Explizite Gleichungen

für Jacobische Varietäten

hyperelliptischer Kurven

Dissertation
zur
Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr.rer.nat.)

dem Fachbereich 6 – Mathematik der
Universität–Gesamthochschule Essen
vorgelegt im August 1991
von
Wolfgang Kampkötter
aus Oelde

Inhaltsverzeichnis

Einleitung

Jacobische Varietäten hyperelliptischer Kurven werden in der letzten Zeit vermehrt in der algorithmischen Zahlentheorie benutzt, da sie die einfachsten Verallgemeinerungen elliptischer Kurven sind. So wurde etwa das Primzahltestverfahren von Goldwasser und Kilian, siehe [Goldwasser], verallgemeinert, indem intern nicht mehr auf der elliptischen Kurve, sondern auf der Jacobischen Varietät einer hyperelliptischen Kurve vom Geschlecht 2 gerechnet wird, siehe [Adleman]. Auch das Schlüsselaustauschsystem von Diffie und Hellman wurde schon auf Jacobische Varietäten hyperelliptischer Kurven verallgemeinert, siehe [Koblitz]. Beide Beispiele benutzen für die Darstellung der Varietät das Divisorklassengruppenmodell, welches auf Jacobi zurückgeht und etwa in [Mumford] beschrieben wird, und für welches in [Cantor] ein Additionsalgorithmus angegeben wurde.

Neben ihrer klassischen Beschreibung als Divisorklassengruppe studierte Mumford diese Varietäten auch als projektive Varietäten. Er entwickelte insbesondere ein algorithmisches Verfahren, welches die Gleichungen der Varietät berechnet. Möchte man aber diese Darstellung in den obigen Anwendungen nutzen, dann benötigt man zusätzlich noch ein explizites, d.h. durch Gleichungen beschriebenes Additionsgesetz auf ihrer Darstellung als projektive Varietät. In der vorliegenden Arbeit leiten wir ein solches Additionsgesetz für Jacobischen Varietäten hyperelliptischer Kurven vom Geschlecht 2 her. Überraschend ist die Einfachheit des Ergebnisses, sowie die Möglichkeit einer eleganten Herleitung, welche die entsprechende Herleitung im Fall einer elliptischen Kurve verallgemeinert. Die vorgestellten Methoden lassen sich voraussichtlich mit erhöhtem computerunterstützten Rechneraufwand auch auf Jacobische Varietäten hyperelliptischer Kurven höheren Geschlechts verallgemeinern.

Anders als in den oben zitierten Beispielanwendungen, welche mit Varietäten über endlichen Körpern arbeiten, verläuft die Herleitung entsprechender Gleichungen über dem Körper der komplexen Zahlen. Das Ziel ist die Konstruktion universeller Gleichungen, die anschließend auf Gleichungen über endlichen Körpern reduziert werden können. Genauer betrachtet man die Jacobische Varietät als Abelsche Varietät, d.h. sie ist einerseits ein komplexer Torus, dessen Dimension gleich dem Geschlecht der Kurve ist, andererseits auch eine projektive Varietät. Die Methode ist das Studium der Funktionentheorie auf diesen Tori.

Mit Hilfe von Thetafunktionen kann man die Gleichung und das Additionsgesetz einer elliptischen Kurve fast rein algebraisch durch Anwendung spezieller Relationen zwischen den Thetafunktionen herleiten, siehe etwa [Mumford], I oder [Weber], §§22 und 49. Dazu wählt man die Thetafunktion aus, die bei 0 verschwindet, welche im wesentlichen die Weierstraßsche Sigma-Funktion ist, und definiert die Weier-

straßsche $\wp$-Funktion als zweite logarithmische Ableitung der Sigma-Funktion. Mit dieser und ihrer ersten Ableitung läßt sich schon der affine Ring des Torus erzeugen. Eine Differentialgleichung liefert mit den Koordinaten $\wp$ und $\wp'$ die Gleichung der elliptischen Kurve, und aus dem Additionstheorem der Sigma-Funktion berechnet sich ein Additionstheorem der $\wp$-Funktion, welches zu einem Additionsgesetz der elliptischen Kurve führt.

Die Definition von Thetafunktionen auf höherdimensionalen komplexen Räumen ist ebenso wie die Herleitung einiger Thetarelationen elementar. Allerdings wächst die Anzahl der uns interessierenden Thetafunktionen, und daher auch die Komplexität der Relationen zwischen ihnen exponentiell. Jede Vereinfachung der Relationen sollte daher konsequent genutzt werden. In unserem Fall führt das Verschwinden einiger Thetanullwerte zu Vereinfachungen. Etwa konnte damit die Anzahl der Summanden des Additionstheorems einer Thetafunktion von 2^{2g} auf 2^g vereinfacht werden, wenn g das Geschlecht der Kurve bezeichnet, siehe Abschnitt 2.3.

Die wichtigste Verbindung der Darstellungen der Jacobischen Varietät, einerseits als Divisorklassengruppe, andererseits als komplexer Torus, wird zu Beginn des 3. Kapitels zitiert. Sie motiviert die Wahl einer Thetafunktion, die die Rolle der Sigma-Funktion übernehmen soll. Der Tangentialvektor an die Kurve durch den Punkt ∞ führt durch Übertragung auf die Abelsche Varietät zu einer speziellen Derivation. Wenden wir diese zweimal auf den Logarithmus der Sigma-Funktion an, dann erhalten wir eine meromorphe Funktion auf dem komplexen Torus, die $\wp$-Funktion. Diese und ihre ersten $2g-1$ Ableitungen genügen, den affinen Ring einer affinen Karte der Jacobischen Varietät zu erzeugen. Das Wechselspiel zwischen den beiden Darstellungen der Varietät liefert universelle Gleichungen in den Ableitungen der $\wp$-Funktion, welche eine Karte als affine Varietät durch g Gleichungen in $2g$ Koordinaten beschreiben, wobei g wieder das Geschlecht der Kurve bezeichnet. Überdecken wir die gesamte Varietät mit isomorphen Karten, dann erhalten wir eine vollständige Beschreibung der Varietät.

Im 4. Kapitel schließlich leiten wir aus dem Additionstheorem der Thetafunktion, die die Rolle der Sigma-Funktion übernommen hat, ein Additionstheorem der $\wp$-Funktion her. Dabei geben wir ein Verfahren an, welches im Prinzip für hyperelliptische Kurven von beliebigem Geschlecht funktioniert. Da wir aber an einem universellen Additionstheorem interessiert sind, in welchem nicht die Verzweigungspunkte der Kurve vorkommen sollen, müssen wir nach der Berechnung des Additionstheorems dieses noch geeignet umformen, indem Substitutionen mit Hilfe der Gleichungen der Varietät vorgenommen werden. Im Fall einer Kurve vom Geschlecht 2 erreichen wir, daß alle Verzweigungspunkte aus dem Additionstheorem verschwinden. Speziell ist das Additionstheorem der Sigma-Funktion, geschrieben als Polynom in den Ableitungen der $\wp$-Funktion, überraschend einfach. Zweimaliges

logarithmisches Ableiten dieser Gleichung führt anschließend zum Additionstheorem der $\wp$-Funktion.

Die beiden letzten Kapitel beschäftigen sich mit einer speziellen Anwendung der hergeleiteten Gleichungen. Und zwar wird im 6. Kapitel der Algorithmus von Schoof, siehe [Schoof], auf hyperelliptische Kurven vom Geschlecht 2 verallgemeinert. Dieser Algorithmus berechnet das charakteristische Polynom des Frobenius-Endomorphismus der Jacobischen Varietät, wenn diese über einem endlichen Körper definiert ist, in polynomialer Zeit vom Logarithmus der Körperordnung.

Ein wichtiges Hilfsmittel ist die Beschreibung der n-Torsionspunkte durch Gleichungen in den Koordinaten der Jacobischen Varietät als projektive Varietät. Wir beschränken uns im 5. Kapitel auf die Beschreibung der Torsionspunkte auf einer Karte des Atlasses der Varietät, da diese für die spezielle Anwendung im Kapitel 6 ausreicht. Zur Herleitung dieser Gleichungen für den allgemeinen Fall einer hyperelliptischen Kurve können wir nicht auf das Beispiel der elliptischen Kurven zurückgreifen. Wieder müssen wir universelle Gleichungen herleiten, d.h. insbesondere sollen die Verzweigungspunkte der Kurve nicht in die Gleichungen eingehen. Aus dem Modell der Divisorklassengruppe leiten wir ein Verfahren her, mit dem wir universelle Gleichungen mit diesen Eigenschaften definieren können. Ferner beweisen wir Rekursionsformeln, mit denen diese Gleichungen schnell berechnet werden können.

Das 6. Kapitel beschreibt schließlich die Verallgemeinerung des Algorithmus von Schoof auf Jacobische Varietäten hyperelliptischer Kurven vom Geschlecht 2. Da die beschreibenden Gleichungen, sowie das Additionstheorem auf der Varietät und die Beschreibung der Torsionspunkte durch universelle Gleichungen gegeben sind, lassen sich diese leicht zu Gleichungen über einem endlichen Körper reduzieren, wenn die Kurve über diesem Körper gegeben ist. In [Pila] wurde dieser Algorithmus schon auf beliebige Abelsche Varietäten verallgemeinert. Dort wird aber die Existenz expliziter Gleichungen für die Varietät vorausgesetzt, was im allgemeinen gerade die Schwierigkeit ist. Wir werden aber sehen, daß gerade die Spezialisierung in unserem Fall auf Jacobische Varietäten hyperelliptscher Kurven vom Geschlecht 2 den Algorithmus immens beschleunigt. Diesen Algorithmus kann man etwa bei dem Primzahltestverfahren von Adleman und Huang, siehe [Adleman], anwenden.

An dieser Stelle bedanke ich mich bei Herrn Prof. Dr. G. Frey und Herrn Priv.Doz. Dr. H.-G. Rück für die Themenstellung. Mein besonderer Dank gilt Herrn Rück, der mich während der Entstehung dieser Arbeit durch zahlreiche Gespräche und Anregungen betreut hat.

Kapitel 1 : Die Jacobische Varietät einer hyperelliptischen Kurve

In diesem Kapitel beschreiben wir die Jacobische Varietät einer hyperelliptischen Kurve einerseits als Divisorklassengruppe und andererseits als Abelsche Varietät. Die Verbindung zwischen diesen beiden Darstellungen liefert der Satz von Abel, siehe etwa [Lang.2], IV.

1.1 : Die Jacobische Varietät als Divisorklassengruppe

Zunächst werden wir in diesem Abschnitt die Darstellung der Jacobischen Varietät einer hyperelliptischen Kurve als Divisorklassengruppe wiederholen, wie sie von Mumford in [Mumford], IIIa, §§1 und 2 eingeführt wurde. Diese ist über jedem Körper der Charakteristik $\neq 2$ definiert, und mit einem Additionsalgorithmus von Cantor, siehe [Cantor], kann in der Jacobischen Varietät in dieser Darstellung effektiv addiert werden. Durch geringfügige Änderungen der Resultate von Mumford und Cantor kann man hyperelliptische Kurven und deren Jacobische Varietäten auch über Körpern der Charakteristik 2 definieren, was Koblitz in [Koblitz] bei der Definition neuer Kryptographieverfahren ausnutzt.

Sei $C : Y^2 = f(X)$ eine hyperelliptische Kurve vom Geschlecht g über einem algebraisch abgeschlossenen Körper K der Charakteristik $\neq 2$, wobei f ein normiertes Polynom vom Grad $2g+1$ über K mit paarweise verschiedenen Nullstellen sei. Als projektive Varietät hat C eine Singularität bei $\infty = (0:1:0)$. Wir definieren daher die Primdivisoren von C als die Punkte eines nichtsingulären Modells von C. Da wir den Grad von f als ungerade vorausgesetzt haben, liegt über jedem Punkt $P = (x, y)$ von C sowie über $P = \infty$ je genau ein Primdivisor von C. Wir können daher die Primdivisoren mit den Punkten $P = (x, y)$ von C und $P = \infty$ identifizieren.

Die Divisorengruppe $\mathrm{Div}(C)$ von C ist die freie abelsche Gruppe, die von den Primdivisoren von C erzeugt wird. Ein Divisor $D \in \mathrm{Div}(C)$ ist also nach obiger Identifizierung eine formale Summe $D = \sum_{P \in C} n_P P$ mit $n_P \in \mathbb{Z}$ und nur endlich vielen $n_P \neq 0$. Den Grad eines Divisors $D = \sum_{P \in C} n_P P$ definiert man als $\deg(D) = \sum_{P \in C} n_P$. Sei $\mathrm{Div}_0(C)$ die Untergruppe der Divisoren vom Grad 0. Insbesondere Hauptdivisoren, also Divisoren rationaler Funktionen auf C, haben den Grad 0. Wir bezeichnen die Untergruppe der Hauptdivisoren in $\mathrm{Div}_0(C)$ mit H und nennen zwei Divisoren D_1, D_2 linear äquivalent, $D_1 \equiv D_2$, falls $D_1 - D_2 \in H$ ist, und die Faktorgruppe $\mathrm{Div}_0(C)/H$ die Gruppe der Divisorklassen vom Grad 0. Nach dem Satz von Abel-Jacobi ist die Jacobische Varietät $\mathrm{Jac}(C)$ als Gruppe isomorph zur Divisorklassengruppe, siehe etwa [Lang.2], IV.

Ist $P=(x,y)$ ein Punkt der Kurve, dann auch $P'=(x,-y)$. Daher hat die Funktion $X-x$ bei P und P' je eine Nullstelle, d.h. im Fall $P=(x,0)$ bei P eine doppelte Nullstelle, und bei ∞ eine doppelte Polstelle. Daher ist $P+P'-2\cdot\infty\equiv 0 \bmod H$, oder äquivalent $-P'\equiv P-2\cdot\infty \bmod H$. Hieraus und aus dem Satz von Riemann-Roch folgt, daß jedes Element von $\mathrm{Jac}(C)$ genau einen Repräsentanten der Form

$$D=\sum_{i=1}^{r} P_i - r\cdot\infty \qquad \text{mit } P_i\neq\infty$$

mit $r\leq g$ hat, wobei noch die folgende Bedingung erfüllt ist: Für $i,j=1,...,r$ mit $i\neq j$ gilt $P_i'\neq P_j$. Die Menge der Divisorklassen, die einen Repräsentanten in dieser Form mit $r<g$ haben, bezeichnen wir mit Θ.

Die Restriktion der birationalen Abbildung

$$\begin{array}{ccc} Symm^g(C) & \xrightarrow{\ I\ } & \mathrm{Jac}(C) \\ \sum_{i=1}^{g} P_i & \longmapsto & \sum_{i=1}^{g} P_i - g\cdot\infty \bmod H \end{array}$$

mit $Symm^g(C):=C\times ...\times C/S_g$ ist ein Isomorphismus

$$Z \;:=\; \left\{\sum_{i=1}^{g} P_i \mid P_i\neq\infty, P_i\neq P_j' \text{ für } i\neq j\right\} \xrightarrow{\ res(I)\ } \mathrm{Jac}(C)-\Theta\ .$$

Sei $\mathrm{Div}_0^{+,\nu}(C):=\{D=\sum_{i=1}^{\nu} P_i-\nu\cdot\infty \mid P_i\neq\infty \text{ und } P_i'\neq P_j \text{ für alle } i\neq j\}$. Einem solchen Divisor $D=\sum_{i=1}^{\nu} P_i-\nu\cdot\infty\in\mathrm{Div}_0^{+,\nu}(C)$, $P_i=(x_i,y_i)$, ordnen wir drei Polynome zu:

(i) $u(t)=u^D(t):=\prod_{i=1}^{\nu}(t-x_i)$.

(ii) $v(t)=v^D(t)$ sei das eindeutig bestimmte Polynom vom Grad $\leq\nu-1$ mit $v(x_i)=y_i, i=1,...,\nu$, wobei Vielfachheiten zu berücksichtigen sind, falls ein Punkt P_i mehrfacher Summand in D ist. Das heißt, falls die Punkte P_i verschieden sind, dann sei

$$v^D(t):=\sum_{i=1}^{\nu} y_i\,\frac{\prod_{j\neq i}(t-x_j)}{\prod_{j\neq i}(x_i-x_j)}$$

das übliche Interpolationspolynom. Andernfalls können wir $v(t)$ einfach durch einen Grenzwertprozeß berechnen. Auf jeden Fall gilt: Erscheint der Punkt P_i k-mal als Summand von D, dann ist

$$\left(\frac{d}{dt}\right)^j\left(v(t)-\sqrt{f(t)}\right)\Big|_{t=x_i}=0 \quad \text{für} \quad 0\leq j\leq k-1\ .$$

(iii) Nach Konstruktion ist $f(t) - v(t)^2$ ein Vielfaches von $u(t)$; wir definieren also $w(t) = w^D(t)$ durch

$$u(t) \cdot w(t) = f(t) - v(t)^2 \ .$$

Ist $\nu \leq g$, dann ist $\deg(v(t)^2) \leq 2g - 2 < \deg(f(t))$, also ist mit $u(t)$ auch $w(t)$ normiert.

Hat man umgekehrt drei Polynome $u(t), v(t), w(t)$ mit $u(t) \cdot w(t) = f(t) - v(t)^2$, wobei $u(t)$ normiert mit Grad $\nu \leq g$ und $\deg(v(t)) \leq \nu - 1$ ist, dann kann man diesen einen Divisor $D \in \mathrm{Div}_0^{+,\nu}(C)$ zuordnen, indem man

$$D = \sum_{i=1}^{\nu} P_i - \nu \cdot \infty \quad , \quad P_i = (x_i, y_i) \ ,$$

setzt, wobei $x_1, ..., x_\nu$ die Nullstellen von $u(t)$ inklusive Vielfachheiten sind und $y_i = v(x_i)$ ist. Da beide Prozesse invers zueinander sind, ist bewiesen:

Proposition 1.1: *Für $\nu \leq g$ existiert eine Bijektion zwischen den Mengen*

$$Div_0^{+,\nu}(C) \quad \textit{und} \quad \big\{(u(t), v(t), w(t)) \,|u(t) \cdot w(t) = f(t) - v(t)^2, \ u(t) \textit{ normiert vom Grad } \nu, \ \deg(v(t)) \leq \nu - 1, \deg(w(t)) = 2g + 1 - \nu\big\}.$$

Damit wird $\mathrm{Div}_0^{+,\nu}(C)$ eine Varietät mit den Koeffizienten von $u(t), v(t), w(t)$ als Koordinaten. Speziell ist Z eine nichtsinguläre g-dimensionale Varietät (siehe [Mumford],IIIa,1.3), und nach obiger Proposition existiert eine Bijektion zwischen $\mathrm{Jac}(C) - \Theta$ und

$$\big\{(u(t), v(t), w(t)) \,|u(t) \cdot w(t) = f(t) - v(t)^2, u(t) \text{ normiert vom Grad } g, \ \deg(v(t)) \leq g - 1, \deg(w(t)) = g + 1\big\}.$$

Wir werden jetzt $\mathrm{Jac}(C)$ mit affinen Stücken isomorph zu Z überdecken.

Seien $a_1, a_2, ..., a_{2g+1}$ die Nullstellen des Polynoms f der Kurvengleichung. Diese bilden zusammen mit ∞ und der Identifizierung $a_i \longleftrightarrow P_i = (a_i, 0)$ die Menge der Verzweigungspunkte von C. Sei B die Indexmenge $\{1, 2, ..., 2g + 2\}$ der Verzweigungspunkte und L die Divisorklasse vom Grad 2, die $P + P'$ für alle $P \in C$ enthält. Ein Repräsentant von L ist $2 \cdot \infty$. Einer Teilmenge gerader Ordnung T von B ordnen wir die Divisorklasse e_T mit dem Repräsentanten

$$\sum_{i \in T} P_i - \#T \cdot \infty$$

zu. Mit der Bezeichnung CT des Komplements von T in B und der Verknüpfung $T_1 \circ T_2 = (T_1 \cup T_2) - (T_1 \cap T_2)$ zwischen Teilmengen T_1 und T_2 von B haben diese Divisorklassen folgende Eigenschaften:

(i) $2e_T = 0$, d.h. e_T ist 2-Torsionspunkt in $\mathrm{Jac}(C)$
(ii) $e_{T_1} + e_{T_2} = e_{T_1 \circ T_2}$
(iii) Genau dann ist $e_{T_1} = e_{T_2}$, wenn $T_1 = T_2$ oder $T_1 = CT_2$
(iv) Jeder 2-Torsionspunkt von $\mathrm{Jac}(C)$ hat die Form e_T mit einer Teilmenge gerader Ordnung T von B.

Die Überdeckung von $\mathrm{Jac}(C)$ mit affinen Stücken isomorph zu Z lautet mit diesen Bezeichnungen:

Lemma 1.2: *Sei V die Teilmenge $\{2, 4, 6, ..., 2g+2\}$ der geraden Zahlen in B. Dann gilt*

$$\bigcup_T ((Jac(C) - \Theta) + e_T) = Jac(C) \ ,$$

wobei T die Teilmengen gerader Ordnung von V durchläuft.

Beweis : (Eine etwas schwächere Aussage wird in [Mumford], III, 2.5 bewiesen.) Sei $D \in \mathrm{Jac}(C)$ mit dem kanonischen Repräsentanten $\sum_{i=1}^{r} Q_i - r \cdot \infty$, d.h. $Q_i \neq \infty$ und für $i \neq j$ ist $Q_i \neq Q_j'$. Wir wählen $R_1 = (a_{i_1}, 0), ..., R_{g-r} = (a_{i_{g-r}}, 0)$ von den Q_i verschiedene endliche Verzweigungspunkte mit geraden Indizes $i_1, ..., i_{g-r} \in V - \{2g+2\}$, was möglich ist, da die Anzahl der geraden Indizes in B gleich g ist. Dann ist

$$D + \left[\sum_{i=1}^{g-r} R_i - (g-r) \cdot \infty\right] = \left[\sum_{i=1}^{r} Q_i + \sum_{i=1}^{g-r} R_i - g \cdot \infty\right] \in \mathrm{Jac}(C) - \Theta \ ,$$

also $D \in (\mathrm{Jac}(C) - \Theta) + e_T$ mit $T = \{i_1, ..., i_{g-r}\}$, falls $g - r$ gerade ist, bzw. $T = \{i_1, ..., i_{g-r}, 2g+2\}$ sonst.

□

Einem Punkt $P \in C$ ordnen wir eine Derivation des Tangentialraumes $T_{\mathrm{Jac}(C),0}$ von $\mathrm{Jac}(C)$ bei 0 zu, die auf den Koeffizienten von $u(t), v(t), w(t)$ operiert.

Dazu wählen wir ein nichttriviales $\delta_P \in T_{C,P}$. Zu diesem gehören analytische Koordinaten $\varepsilon \mapsto P(\varepsilon) \in C$ in einer kleinen Umgebung von P mit $P(0) = P$, so daß δ_P das Bild des Tangentialvektors $\frac{\partial}{\partial \varepsilon}$ bei 0 in diesen Koordinaten ist. Sei $D_P \in T_{\mathrm{Jac}(C),0}$ der Tangentialvektor zu dieser kleinen analytischen Kurve in $\mathrm{Jac}(C)$ bei 0, d.h. D_P ist das Bild von $\frac{\partial}{\partial \varepsilon}$ unter der Abbildung

$$\varepsilon \longmapsto \text{ Divisorklasse von } P(0) - P(\varepsilon)$$

bei $\varepsilon = 0$. D_P ist bis auf skalare Vielfache dadurch eindeutig bestimmt.

Wir möchten nun beschreiben, wie D_P auf den Koeffizienten von $u(t), v(t), w(t)$ operiert. Wegen der Translationsinvarianz von D_P können wir den Nullpunkt, der in Θ liegt, geeignet verschieben, so daß er bezüglich der oben beschriebenen Überdeckung von $\mathrm{Jac}(C)$ in einem nichtsingulären Stück isomorph zu Z liegt, wo $u(t), v(t), w(t)$ definiert sind.

Sei $0 \longmapsto D = \sum_{i=1}^{g} P_i - g \cdot \infty \in Z$ die gewählte Verschiebung und

$$\sum_{i=1}^{g} P_i(\varepsilon) - g \cdot \infty \equiv D + P(0) - P(\varepsilon) \bmod H \ .$$

Da Z offen ist, kann man $|\varepsilon|$ klein genug wählen, so daß auch $D + P(0) - P(\varepsilon) \in Z$ ist. Seien nun $u_\varepsilon(t), v_\varepsilon(t), w_\varepsilon(t)$ die drei dem Divisor $\sum_{i=1}^{g} P_i(\varepsilon) - g \cdot \infty$ zugeordneten Polynome. Dann repräsentieren

$$\left(\left.\frac{du_\varepsilon}{d\varepsilon}\right|_{\varepsilon=0}, \left.\frac{dv_\varepsilon}{d\varepsilon}\right|_{\varepsilon=0}, \left.\frac{dw_\varepsilon}{d\varepsilon}\right|_{\varepsilon=0} \right) \in T_{Z,D} = T_{\mathrm{Jac}(C),D}$$

die Translation von D_P nach $T_{\mathrm{Jac}(C),D}$.

In [Mumford], IIIa, 3.1. wurde die Wirkung von D_P auf $u(t), v(t), w(t)$ berechnet. Wir zitieren hier nur das spezielle Ergebnis für $P = \infty$:

Satz 1.3: *Nach geeigneter Normierung von D_∞, d.h. Multiplikation mit einem Skalar, und der Bezeichnung $\dot{}$ für D_∞ operiert diese auf den Koeffizienten von $u(t), v(t), w(t)$ folgendermaßen:*

$$\begin{aligned} \dot{u}(t) &= v(t) \\ \dot{v}(t) &= \tfrac{1}{2}\left(-w(t) + (t - u_1 + w_0)u(t)\right) \\ \dot{w}(t) &= -(t - u_1 + w_0)v(t) \ . \end{aligned}$$

Beweis : Den Beweis, siehe [Mumford],IIIa,3.1., führt man durch explizites Ausrechnen der entsprechenden Gleichungen für D_P, $P \in C$, $P \neq \infty$ und anschließendem Übergang zum Grenzwert P gegen ∞.

□

1.2 : Die Jacobische Varietät als Abelsche Varietät

Wir werden jetzt die Jacobische Varietät einer hyperelliptischen Kurve als Abelsche Varietät konstruieren. Eine g-dimensionale Abelsche Varietät ist ein komplexer Torus $\mathbb{C}^g/\Gamma$, wobei Γ ein diskretes Gitter von maximalem Rang $2g$ ist, der auch eine projektive algebraische Varietät ist.

Wählen wir ein nichtsinguläres Modell der hyperelliptischen Kurve C vom Geschlecht g, so kann dieses bekanntlich als kompakte zusammenhängende Riemannsche Fläche S vom Geschlecht g aufgefaßt werden. Ihre erste Homologiegruppe $H_1(S,\mathbb{Z})$ ist eine freie abelsche Gruppe mit $2g$ Erzeugern. Üblicherweise wählt man Erzeugende $A_1,...,A_g,B_1,...,B_g$ als geschlossene Kurven in S, so daß sich zwei verschiedene A_i in keinem Punkt schneiden, ebenso nicht zwei verschiedene B_i, und A_i und B_j schneiden sich nur, wenn $j=i$ ist, und dann in genau einem Punkt.

Zusätzlich betrachtet man den g-dimensionalen Vektorraum $\Omega_1(S)$ der holomorphen Differentiale. In unserem Fall einer hyperelliptischen Riemannschen Fläche, die durch die Gleichung $Y^2 = f(X)$ gegeben ist, ist $\frac{p(X)dX}{Y}$ mit einem Polynom $p(X)$ vom Grad $\leq g-1$ ein holomorphes Differential. Da auch der Vektorraum der so beschriebenen Differentiale die Dimension g hat, gilt

$$\Omega_1(S) = \left\{ \frac{p(X)dX}{Y} \mid p(X) \text{ Polynom vom Grad } \leq g-1 \right\} .$$

$\Omega_1(S)$ hat eine Basis $\omega_1,...,\omega_g$ mit

$$\int_{A_i} \omega_j = \delta_{ij} ,$$

welche wir im folgenden festhalten werden. Definieren wir die $g \times g$-Matrix Ω durch

$$\Omega_{ij} := \int_{B_i} \omega_j ,$$

dann ist Ω symmetrisch mit positiv definitem Imaginärteil. Diese Aussagen findet man z.B. in [Mumford], II,§2. Wir definieren das diskrete Gitter Γ_Ω mit Periodenmatrix Ω durch $\Gamma_\Omega := \mathbb{Z}^g + \Omega \cdot \mathbb{Z}^g$. Die analytische Jacobische Varietät von C definieren wir als den komplexen Torus $\mathbb{C}^g/\Gamma_\Omega$. Da der Imaginärteil von Ω positiv definit ist, ist $\mathbb{C}^g/\Gamma_\Omega$ eine projektive Varietät, siehe etwa [Griffiths], Chapter 2.6.

Mit $\omega := (\omega_1, ..., \omega_g)^t$ ist die Abbildung

$$\begin{array}{rccc} \varphi & : & C^k & \longrightarrow & \mathbb{C}^g/\Gamma_\Omega \\ & & (P_1, ..., P_k) & \longmapsto & \sum_{i=1}^{k} \int_\infty^{P_i} \omega \bmod \Gamma_\Omega \end{array}$$

holomorph. Nach dem Satz von Abel induziert sie einen Isomorphismus

$$\begin{array}{rccc} \overline{\varphi} & : & \mathrm{Jac}(C) & \longrightarrow & \mathbb{C}^g/\Gamma_\Omega \end{array}$$

von der Jacobischen Varietät als Divisorklassengruppe auf die analytische Jacobische Varietät, indem die Divisorklasse von $\sum_{i=1}^{k} P_i - \sum_{i=1}^{k} Q_i$ auf $\varphi(P_1, ..., P_k) - \varphi(Q_1, ..., Q_k)$ abgebildet wird.

In den analytischen Koordinaten $z_1, ..., z_g$ wird die oben gewählte Derivation D_∞ auf eine Linearkombination $\sum_{i=1}^{g} c_i \frac{\partial}{\partial z_i}$ mit komplexen Koeffizienten c_i der partiellen Ableitungen abgebildet. Der Vollständigkeit halber sei hier erwähnt, daß sich die c_i aus der Basis $\omega_1, ..., \omega_g$ von $\Omega_1(S)$ berechnen lassen. Ist nämlich

$$\omega_i = \frac{p_i(X)dX}{Y} \quad \text{mit} \quad p_i(X) = e_i X^{g-1} + \dots ,$$

dann haben wir die Identifizierung

$$D_\infty \quad \longleftrightarrow \quad -\sum_{i=1}^{g} e_i \frac{\partial}{\partial z_i}$$

(siehe [Mumford], IIIa, 5.10).

Kapitel 2 : Thetafunktionen auf hyperelliptischen Tori

Im ersten Kapitel haben wir gesehen, daß die Jacobische Varietät $\mathrm{Jac}(C)$ einer hyperelliptischen Kurve C vom Geschlecht g als komplexe Mannigfaltigkeit ein komplexer Torus $\mathbb{C}^g/\Gamma$ mit einem Gitter $\Gamma \subset \mathbb{C}^g$ ist. Auf diesem möchten wir nichtkonstante meromorphe Funktionen konstruieren. In Vorbereitung hierauf definieren wir Thetafunktionen, denn aus ihrer Quasiperiodizität bezüglich Γ (siehe Lemma 2.1) folgt, daß das Quadrat vom Quotienten zweier Thetafunktionen immer eine meromorphe und bezüglich Γ periodische Funktion ist, also eine meromorphe Funktion auf $\mathbb{C}^g/\Gamma$ definiert.

Nach der Definition der Thetafunktionen zu hyperelliptischen Kurven beweisen wir einige ihrer elementaren Eigenschaften, die sich aus der Reihendarstellung ergeben, insbesondere die Riemannsche Thetaformel, Satz 2.7, aus dem wir als Korollar Additionstheoreme für unsere Thetafunktionen herleiten, siehe Korollar 2.8, Korollar 2.8'. Mit Hilfe der "Fundamental Vanishing Property" von Mumford, Satz 2.11, die nur für Thetafunktionen hyperelliptischer Kurven richtig ist, (siehe [Mumford], IIIa, §9), vereinfachen wir die Additionstheoreme, Satz 2.14, ferner folgt aus ihr und der Riemannschen Thetaformel die Frobeniussche Thetaformel.

2.1 : Definition und elementare Eigenschaften

Sei $\Omega = (\Omega_{i,j})_{i,j=1,\ldots,g}$ die Periodenmatrix von Γ, eine symmetrische komplexe $g \times g$-Matrix, deren Imaginärteil $Im(\Omega) := (Im(\Omega_{i,j}))_{i,j=1,\ldots,g}$ positiv definit ist, d.h. $\Gamma = \Gamma_\Omega = \mathbb{Z}^g + \Omega \cdot \mathbb{Z}^g$. Zwei Vektoren $a, b \in \frac{1}{2}\mathbb{Z}^g$, den Charakteristiken, ordnen wir die auf $\mathbb{C}^g$ holomorphe Thetafunktion mit Periodenmatrix Ω,

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] : \mathbb{C}^g \longrightarrow \mathbb{C} \quad ,$$

$$z \longmapsto \vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z) := \vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) := \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)^t (z+b)\right),$$

zu.

Bemerkung : Die positive Definitheit des Imaginärteils von Ω sichert die absolute und auf jeder kompakten Teilmenge von $\mathbb{C}^g$ gleichmäßige Konvergenz der Reihe. Den Beweis hierzu findet man z.B. in [Mumford], II, Proposition 1.1.

Das folgende Lemma beschreibt die Quasiperiodizität der Thetafunktionen bezüglich Γ :

Lemma 2.1: *Seien $a, b \in \frac{1}{2}\mathbb{Z}^g$ und $p, q \in \mathbb{Z}^g$. Dann gilt*

$$\vartheta[{}^{a}_{b}](z+\Omega p+q) = e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} \quad \vartheta[{}^{a}_{b}](z) \quad .$$

Beweis : Wir schreiben die linke Seite in der obigen Reihendarstellung und verschieben anschließend den Summationsindex von n nach $n+p$:

$$\begin{aligned}
&\vartheta[{}^{a}_{b}](z+\Omega p+q) = \sum_{n\in\mathbb{Z}^g} e^{\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)^t (z+\Omega p+q+b)} \\
&= e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} \\
&\quad \cdot \sum_{n\in\mathbb{Z}^g} e^{\pi i ((n+a)^t \Omega (n+a) + 2(n+a)^t \Omega p + p^t \Omega p) + 2\pi i ((n+a)^t (z+b) + p^t (z+b) + n^t q)} \\
&= e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} \sum_{n\in\mathbb{Z}^g} e^{\pi i (n+p+a)^t \Omega (n+p+a) + 2\pi i (n+p+a)^t (z+b)}
\end{aligned}$$

Wir haben hier benutzt, daß $e^{2\pi i n^t q} = 1$ für alle $n \in \mathbb{Z}^g$ ist. Nach der Indexverschiebung von n nach $n+p$ bekommen wir das gewünschte Ergebnis.

□

Bemerkung 2.2: Das Quadrat vom Quotienten zweier Thetafunktionen ist nach diesem Lemma eine bzgl. Γ periodische Funktion, d.h. eine meromorphe Funktion auf $\mathbb{C}^g/\Gamma$, denn es gilt

$$\left(\frac{\vartheta[{}^{a_1}_{b_1}](z+\Omega p+q)}{\vartheta[{}^{a_2}_{b_2}](z+\Omega p+q)}\right)^2 = \left(\frac{exp(-2\pi i p^t b_1 + 2\pi i a_1^t q)\ \vartheta[{}^{a_1}_{b_1}](z)}{exp(-2\pi i p^t b_2 + 2\pi i a_2^t q)\ \vartheta[{}^{a_2}_{b_2}](z)}\right)^2 = \left(\frac{\vartheta[{}^{a_1}_{b_1}](z)}{\vartheta[{}^{a_2}_{b_2}](z)}\right)^2 .$$

Verändern wir z in $\vartheta[{}^{a}_{b}](z)$ nur um eine Halbperiode, dann erhalten wir Beziehungen zwischen Thetafunktionen verschiedener Charakteristiken :

Lemma 2.3: *Für $a, b, c, d \in \frac{1}{2}\mathbb{Z}^g$ gilt*

$$\vartheta[{}^{a}_{b}](z+\Omega c+d) = e^{-\pi i c^t \Omega c - 2\pi i c^t (z+b+d)} \quad \vartheta[{}^{a+c}_{b+d}](z) \quad .$$

Beweis : Wir gehen von der Definition der Thetafunktion aus und erhalten

$$\vartheta[{}^{a}_{b}](z+\Omega c+d) = \sum_{n\in\mathbb{Z}^g} e^{\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)^t (z+\Omega c+b+d)}$$

$$= e^{-\pi i c^t \Omega c - 2\pi i c^t (z+b+d)} \cdot$$
$$\sum_{n\in\mathbb{Z}^g} e^{\pi i((n+a)^t\Omega(n+a)+2(n+a)^t\Omega c + c^t\Omega c)+2\pi i((n+a)^t(z+b+d)+c^t(z+b+d))}$$
$$= e^{-\pi i c^t \Omega c - 2\pi i c^t (z+b+d)} \sum_{n\in\mathbb{Z}^g} e^{\pi i(n+a+c)^t\Omega(n+a+c)+2\pi i(n+a+c)^t(z+b+d)}$$
$$= e^{-\pi i c^t \Omega c - 2\pi i c^t (z+b+d)} \quad \vartheta[\begin{smallmatrix} a+c \\ b+d \end{smallmatrix}](z) \quad .$$

□

Verbinden wir die beiden Lemmata, dann erhalten wir :

Korollar 2.4: *Für $a, b \in \frac{1}{2}\mathbb{Z}^g$ und $p, q \in \mathbb{Z}^g$ gilt :*

$$\vartheta[\begin{smallmatrix} a+p \\ b+q \end{smallmatrix}](z) = e^{2\pi i a^t q} \quad \vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](z) \quad .$$

Beweis : Nach Lemma 2.1 ist

$$\vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](z+\Omega p+q) = e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} \quad \vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](z) \quad ,$$

und nach Lemma 2.3 ist

$$\vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](z+\Omega p+q) = e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b+q)} \quad \vartheta[\begin{smallmatrix} a+p \\ b+q \end{smallmatrix}](z) \quad .$$

Das Gleichsetzen der rechten Seiten liefert mit $e^{2\pi i p^t q} = 1$ das Ergebnis.

□

Dieses Korollar besagt, daß wir im wesentlichen, d.h. bis auf ein Vorzeichen, die oben definierten Thetafunktionen schon mit den Charakteristiken $a, b \in \{0, \frac{1}{2}\}^g$ parametrisieren können. Bei festem g und gegebener Periodenmatrix Ω haben wir so also 2^{2g} Thetafunktionen definiert.

Eine weitere wichtige Eigenschaft dieser Thetafunktionen ist, daß sie entweder gerade oder ungerade Funktionen sind, d.h. $\vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](-z) = \pm\vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](z)$. Gerade bei der späteren Berechnung von Thetanullwerten werden wir das folgende Korollar häufig benutzen:

Korollar 2.5: *Für $a, b \in \frac{1}{2}\mathbb{Z}^g$ gilt :*

$$\vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](-z) = e^{4\pi i a^t b}\, \vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](z) \quad ,$$

d.h. $\vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}]$ ist genau dann gerade (ungerade) Funktion, wenn $4a^t b$ gerade (ungerade) ist.

Beweis : Wir schreiben nach Definition

$$\vartheta[{}^{a}_{b}](-z) = \sum_{n\in\mathbb{Z}^g} e^{\pi i(n+a)^t\Omega(n+a)+2\pi i(n+a)^t(-z+b)} \quad ,$$

ersetzen den Summationsindex n durch $-n$ und erhalten

$$= \sum_{n\in\mathbb{Z}^g} e^{\pi i(-n+a)^t\Omega(-n+a)+2\pi i(-n+a)^t(-z+b)}$$
$$= \sum_{n\in\mathbb{Z}^g} e^{\pi i(n-a)^t\Omega(n-a)+2\pi i(n-a)^t(z-b)}$$
$$= \vartheta[{}^{-a}_{-b}](z) = \vartheta[{}^{a-2a}_{b-2b}](z) = e^{-4\pi i a^t b}\vartheta[{}^{a}_{b}](z) = e^{4\pi i a^t b}\vartheta[{}^{a}_{b}](z)$$

nach Korollar 2.4. Da $4a^tb \in \mathbb{Z}$ ist, ist insbesondere $e^{-4\pi i a^t b} = e^{4\pi i a^t b}$, und die Aussage über gerade bzw. ungerade Funktionen folgt unmittelbar.

□

2.2 : Riemannsche Thetaformeln

In diesem Abschnitt werden wir eine der wichtigsten Beziehungen zwischen Produkten von Thetafunktionen beweisen. Sowohl die Additionstheoreme für Thetafunktionen, siehe unten, als auch die Frobeniussche Thetaformel, die wir im nächsten Abschnitt vorstellen werden, leiten sich aus dieser ab.

Jeder symmetrischen Matrix $A \in M_n(\mathbb{Z})$ mit $A^tA = m^2I_n$, $m \in \mathbb{N}$, kann man eine ähnliche Theta-Relation zuordnen. Die meiste Beachtung findet aber die Riemannsche Theta-Relation, die sich aus der Matrix

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

ergibt und die wir unten explizit formulieren und beweisen werden (siehe hierzu auch [Mumford], I, §5 für den Fall $g = 1$).

Zunächst führen wir einige Bezeichnungen ein. Einem Viertupel $(x, y, u, v) \in (\mathbb{C}^g)^4$ ordnen wir ein Viertupel $(\tilde{x}, \tilde{y}, \tilde{u}, \tilde{v}) \in (\mathbb{C}^g)^4$ folgendermaßen zu:

$$\tilde{x} = \tfrac{1}{2}(x + y + u + v)$$
$$\tilde{y} = \tfrac{1}{2}(x + y - u - v)$$
$$\tilde{u} = \tfrac{1}{2}(x - y + u - v)$$
$$\tilde{v} = \tfrac{1}{2}(x - y - u + v)$$

Insbesondere ist dann $(\tilde{\tilde{x}}, \tilde{\tilde{y}}, \tilde{\tilde{u}}, \tilde{\tilde{v}}) = (x, y, u, v)$. Ferner definiert diese Abbildung eine Bijektion zwischen den Mengen

$$\left\{(n,m,p,q) \in a + \mathbb{Z}^g \mid a \in \{0, \tfrac{1}{2}\}^g, n+m+p+q \in 2\mathbb{Z}^g\right\} \text{ und } (\mathbb{Z}^g)^4 \ .$$

Da die Periodenmatrix Ω symmetrisch ist, gelten ferner die beiden Gleichungen

$$n^t\Omega n + m^t\Omega m + p^t\Omega p + q^t\Omega q = \tilde{n}^t\Omega\tilde{n} + \tilde{m}^t\Omega\tilde{m} + \tilde{p}^t\Omega\tilde{p} + \tilde{q}^t\Omega\tilde{q} \ ,$$
$$n^t x + m^t y + p^t u + q^t v = \tilde{n}^t\tilde{x} + \tilde{m}^t\tilde{y} + \tilde{p}^t\tilde{u} + \tilde{q}^t\tilde{v} \ ,$$

die wir im Beweis der folgenden Proposition benutzen werden. Zur Vereinfachung der Schreibweise setzen wir noch $\vartheta(z) := \vartheta[{}^0_0](z)$.

Proposition 2.6: *Für Vektoren $x, y, u, v \in \mathbb{C}^g$ gilt:*

$$2^g\ \vartheta(\tilde{x})\ \vartheta(\tilde{y})\ \vartheta(\tilde{u})\ \vartheta(\tilde{v}) = \sum_{a,b \in \{0,\frac{1}{2}\}^g} \vartheta[{}^a_b](x)\ \vartheta[{}^a_b](y)\ \vartheta[{}^a_b](u)\ \vartheta[{}^a_b](v) \ .$$

Beweis: Da die Summendarstellung der Thetafunktionen absolut und gleichmäßig konvergiert, können wir die Summationsreihenfolge beliebig vertauschen. Wir beginnen wieder mit der Definition der Thetafunktionen:

$$\sum_{a,b \in \{0,\frac{1}{2}\}^g} \vartheta[{}^a_b](x)\ \vartheta[{}^a_b](y)\ \vartheta[{}^a_b](u)\ \vartheta[{}^a_b](v)$$

$$= \sum_{a,b \in \{0,\frac{1}{2}\}^g} \sum_{n,m,p,q \in \mathbb{Z}^g} e^{\pi i[(n+a)^t\Omega(n+a)+\ldots+(q+a)^t\Omega(q+a)]+2\pi i[(n+a)^t x+\ldots+(q+a)^t v]} \cdot e^{2\pi i(n^t+\ldots+q^t)b+8\pi i a^t b}$$

$$= \sum_{a \in \{0,\frac{1}{2}\}^g} \sum_{n,m,p,q \in \mathbb{Z}^g} e^{\pi i[(n+a)^t\Omega(n+a)+\ldots+(q+a)^t\Omega(q+a)]+2\pi i[(n+a)^t x+\ldots+(q+a)^t v]} \cdot \sum_{b \in \{0,\frac{1}{2}\}^g} e^{2\pi i(n+m+p+q)^t b} \ .$$

Nun gilt $\displaystyle\sum_{b \in \{0,\frac{1}{2}\}^g} e^{2\pi i(n+m+p+q)^t b} = \begin{cases} 2^g & \text{, falls } n+m+p+q \in 2\mathbb{Z}^g \\ 0 & \text{, sonst} \end{cases}$,

also ist der obere Ausdruck gleich

$$= 2^g \sum_{a \in \{0,\frac{1}{2}\}^g} \sum_{\substack{n,m,p,q \in \mathbb{Z}^g \\ n+m+p+q \in 2\mathbb{Z}^g}} e^{\pi i[(n+a)^t\Omega(n+a)+\ldots+(q+a)^t\Omega(q+a)]+2\pi i[(n+a)^t x+\ldots+(q+a)^t v]}$$

$$= 2^g \sum_{a \in \{0,\frac{1}{2}\}^g} \sum_{\substack{n,m,p,q \in a+\mathbb{Z}^g \\ n+m+p+q \in 2\mathbb{Z}^g}} e^{\pi i[n^t\Omega n+\ldots+q^t\Omega q]+2\pi i[n^t x+\ldots+q^t v]} .$$

Nach den Vorbemerkungen ist dies gleich

$$= \sum_{\tilde{n},\tilde{m},\tilde{p},\tilde{q} \in \mathbb{Z}^g} e^{\pi i[\tilde{n}^t\Omega\tilde{n}+\ldots+\tilde{q}^t\Omega\tilde{q}]+2\pi i[\tilde{n}^t\tilde{x}+\ldots+\tilde{q}^t\tilde{v}]} = 2^g\ \vartheta(\tilde{x})\ \vartheta(\tilde{y})\ \vartheta(\tilde{u})\ \vartheta(\tilde{v}) .$$

□

Nach dieser Vorbereitung kommen wir zur endgültigen Formulierung der Riemannschen Thetaformel:

Satz 2.7: (Riemannsche Thetaformel)
Seien $c, d \in \frac{1}{2}\mathbb{Z}^g$ *und* $x, y, u, v \in \mathbb{C}^g$. *Dann gilt:*

$$2^g\ \vartheta[\tfrac{c}{d}](\tilde{x})\ \vartheta[\tfrac{c}{d}](\tilde{y})\ \vartheta[\tfrac{c}{d}](\tilde{u})\ \vartheta[\tfrac{c}{d}](\tilde{v})$$

$$= \sum_{a,b \in \{0,\frac{1}{2}\}^g} e^{4\pi i(a^t d - b^t c)}\ \vartheta[\tfrac{a}{b}](x)\ \vartheta[\tfrac{a}{b}](y)\ \vartheta[\tfrac{a}{b}](u)\ \vartheta[\tfrac{a}{b}](v) .$$

Beweis: Wir ersetzen in der Proposition 2.6 x durch $x + 2\Omega c + 2d$. Dadurch werden $\tilde{x}, \ldots, \tilde{v}$ durch $\tilde{x} + \Omega c + d, \ldots, \tilde{v} + \Omega c + d$ resp. ersetzt, und wir erhalten

$$2^g \vartheta(\tilde{x} + \Omega c + d) \cdots \vartheta(\tilde{v} + \Omega c + d)$$

$$= \sum_{a,b \in \{0,\frac{1}{2}\}^g} \vartheta[\tfrac{a}{b}](x + 2\Omega c + 2d)\ \vartheta[\tfrac{a}{b}](y)\ \vartheta[\tfrac{a}{b}](u)\ \vartheta[\tfrac{a}{b}](v) .$$

Dies ist nach Lemma 2.1 und Lemma 2.3 äquivalent zu

$$2^g e^{-4\pi i c^t\Omega c - 4\pi i c^t(\tilde{x}+\ldots+\tilde{v}) - 8\pi i c^t d} \vartheta[\tfrac{c}{d}](\tilde{x}) \cdots \vartheta[\tfrac{c}{d}](\tilde{v})$$

$$= \sum_{a,b \in \{0,\frac{1}{2}\}^g} e^{-4\pi i c^t\Omega c - 4\pi i c^t(x+b) + 4\pi i a^t d} \vartheta[\tfrac{a}{b}](x) \cdots \vartheta[\tfrac{a}{b}](v) .$$

Wegen $x = \frac{1}{2}(\tilde{x} + \ldots + \tilde{v})$ folgt

$$2^g \vartheta[\tfrac{c}{d}](\tilde{x}) \cdots \vartheta[\tfrac{c}{d}](\tilde{v}) = \sum_{a,b \in \{0,\frac{1}{2}\}^g} e^{4\pi i(a^t d - b^t c)} \vartheta[\tfrac{a}{b}](x) \cdots \vartheta[\tfrac{a}{b}](v) .$$

□

Spezialisieren wir die Variablen im vorstehenden Satz geschickt, dann erhalten wir die Additionstheoreme für Thetafunktionen (für den Fall $g = 1$ vergleiche auch [Mumford], I, §5 oder [Weber], §22). J.D. Fay erwähnt in [Fay], I, (3), eine andere Sorte von Additionstheoremen, die allerdings auch die Periodenmatrix Ω verändern.

Korollar 2.8: (Additionstheoreme)
Seien $c, d \in \frac{1}{2}\mathbb{Z}^g$ und $x, u \in \mathbb{C}^g$. Dann gilt:

$$2^g\, \vartheta[\begin{smallmatrix} c \\ d \end{smallmatrix}](x+u)\, \vartheta[\begin{smallmatrix} c \\ d \end{smallmatrix}](x-u)\, \vartheta[\begin{smallmatrix} c \\ d \end{smallmatrix}](0)^2 = \sum_{a,b \in \{0,\frac{1}{2}\}^g} e^{4\pi i(a^t d - b^t c)}\, \vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](x)^2\, \vartheta[\begin{smallmatrix} a \\ b \end{smallmatrix}](u)^2 \ .$$

Beweis : Wir setzen in Satz 2.7 mit den dort verwendeten Bezeichnungen $x = y$ und $u = v$. Dies ersetzt $\tilde{x}$ durch $x + u$, $\tilde{y}$ durch $x - u$ und $\tilde{u}$, $\tilde{v}$ jeweils durch 0.

□

2.3 : Nullstellen von Thetafunktionen

Neben den ungeraden Thetafunktionen verschwinden auch einige gerade am Punkt $0 \in \mathbb{C}^g$. Mumford hat diese für den hyperelliptischen Fall genau klassifiziert; wir stellen hier zunächst seine Ergebnisse vor.

Sei $C : y^2 = f(x) = \prod_{i=1}^{2g+1} (x - a_i)$ mit paarweise verschiedenen a_i eine hyperelliptische Kurve von Geschlecht g mit Verzweigungspunkten $a_1, ..., a_{2g+1}, a_{2g+2} := \infty$. Sei $B := \{1, 2, ..., 2g+2\}$ deren Indexmenge und $B' = B - \{2g+2\}$. Wegen der besonderen Bedeutung des Verzweigungspunktes $a_{2g+2} = \infty$ bezeichnen wir im folgenden auch häufig den Index $2g+2$ mit ∞.

Einem Verzweigungspunkt a_k, $k \in B$, ordnen wir den $2g$-Vektor η_k folgendermaßen zu:

$$\eta_{2i-1} = \begin{pmatrix} (0 & \dots & 0 & \frac{1}{2} & 0 & \dots & 0)^t \\ (\frac{1}{2} & \dots & \frac{1}{2} & 0 & 0 & \dots & 0)^t \end{pmatrix} \quad 1 \le i \le g$$

$$\uparrow \ i \ \downarrow$$

$$\eta_{2i} = \begin{pmatrix} (0 & \dots & 0 & \frac{1}{2} & 0 & \dots & 0)^t \\ (\frac{1}{2} & \dots & \frac{1}{2} & \frac{1}{2} & 0 & \dots & 0)^t \end{pmatrix} \quad 1 \le i \le g$$

$$\eta_{2g+1} = \begin{pmatrix} (0 & \dots & 0) \\ (\frac{1}{2} & \dots & \frac{1}{2})^t \end{pmatrix}$$

$$\eta_{2g+2} = \begin{pmatrix} (0 & \dots & 0)^t \\ (0 & \dots & 0)^t \end{pmatrix}$$

Die η_k, $k \in B'$, erzeugen $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ mit der Relation

$$\sum_{k \in B'} \eta_k = 0 \in \tfrac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g} \ .$$

Wir möchten die Menge der Charakteristiken, die wir später auch als Elemente von $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ auffassen, mit Teilmengen gerader Ordnung von B parametrisieren. Die Potenzmenge von B ist mit der Verknüpfung $S \circ T := (S \cup T) - (S \cap T)$ eine Gruppe. Sei $G := \{S \subseteq B \mid \#S \text{ gerade}\}$ die Untergruppe der Elemente gerader Ordnung der Potenzmenge von B. Jeder Teilmenge S von B ordnen wir eine Charakteristik

$$\eta_S := \sum_{k \in S} \eta_k$$

zu. Dies definiert einen Epimorphismus abelscher Gruppen, η, von G auf $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, denn

$$\eta_{S \circ T} = \sum_{k \in S \circ T} \eta_k \equiv \sum_{k \in S \circ T} \eta_k + 2 \sum_{k \in S \cap T} \eta_k = \sum_{k \in S} \eta_k + \sum_{k \in T} \eta_k = \eta_S + \eta_T \bmod \mathbb{Z}^{2g} \ .$$

Diese Abildung ist surjektiv, da aus obiger Relation zwischen den η_k folgt $\mathrm{Kern}(\eta) = \{\emptyset, B\}$, und da $\#G = 2^{2g+1} = 2 \cdot \#\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ ist. Insbesondere ist $\bar{G} := G/\mathrm{Kern}(\eta) = G/_{(S \sim CS)} \cong \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, d.h. wir können die Charakteristiken mit den Elementen von $\bar{G}$ parametrisieren.

Die Additionstheoreme enthalten auf der rechten Seite einen Faktor der Form $e^{4\pi i(a^t d - b^t c)}$. Um diesen in der neuen Schreibweise der Charakteristiken einfach schreiben zu können, setzen wir

$$\left\langle \binom{a}{b}, \binom{c}{d} \right\rangle := 4(a^t d - b^t c) \ ,$$

bzw. für $\bar{S}, \bar{T} \in \bar{G}$:

$$\langle \eta_S, \eta_T \rangle := 4\big((\eta_S)_1^t (\eta_T)_2 - (\eta_S)_2^t (\eta_T)_1\big) \ ,$$

wobei $(\eta_S)_1$, $(\eta_S)_2$ den Vektor der ersten respektive zweiten g Einträge des Vektors η_S bezeichnen.

Lemma 2.9: *Seien $\bar{S}, \bar{T} \in \bar{G}$. Dann gilt:*

$$\langle \eta_S, \eta_T \rangle \equiv \#S \cap T \ mod\ 2 \ ,$$

insbesondere ist $\langle , \rangle : \bar{G} \times \bar{G} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ eine symmetrische Bilinearform.

Beweis : Da $\eta_S \in \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ unabhängig von der Wahl des Repräsentanten S von $\bar{S}$ ist, ist die linke Seite der Gleichung wohldefiniert. Auch die rechte Seite ist wohldefiniert, denn wegen $\#T$ gerade ist

$$\#(CS \cap T) = \#T - \#S \cap T \equiv \#S \cap T \bmod 2 \ .$$

Als nächstes zeigen wir die Bilinearität der rechten Seite. Es gilt

$$\#(S_1 \cap (S_2 \circ S_3)) \equiv \#S_1 \cap S_2 + \#S_1 \cap S_3 \bmod 2 ,$$

da $S_1 \cap (S_2 \circ S_3) = S_1 \cap [(S_2 \cup S_3) - (S_2 \cap S_3)]$

$$= [(S_1 \cap S_2) - S_3] \quad \dot\cup \quad [(S_1 \cap S_3) - S_2]$$

$$= [(S_1 \cap S_2) - (S_1 \cap S_2 \cap S_3)] \quad \dot\cup \quad [(S_1 \cap S_3) - (S_1 \cap S_2 \cap S_3)] .$$

Dies zeigt, daß die rechte Seite des Lemmas eine symmetrische Bilinearform $\bar{G} \times \bar{G} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ ist.

Um die Gleichung zu beweisen, bemerken wir zunächst, daß für $j, k \in B$

$$\langle \eta_j, \eta_k \rangle \equiv 1 + \delta_{jk} \bmod 2 \quad (\delta_{jk} \text{ Kroneckersymbol})$$

gilt, wie man leicht nachrechnet. Da $\#T$ gerade ist, weist man leicht nach

$$\langle \eta_S, \eta_T \rangle = \sum_{\substack{j \in S \\ k \in T}} \langle \eta_j, \eta_k \rangle = \sum_{\substack{j \in S \\ k \in T}} (1 + \delta_{jk}) \equiv \#S \cap T \bmod 2 .$$

□

Sei $U \subset B$ die Menge $U = \{1, 3, 5, ..., 2g+1\}$ der ungeraden Zahlen in B. Dann läßt sich in unserer neuen Schreibweise auch die Eigenschaft von $\vartheta[\eta_S]$, gerade oder ungerade Funktion zu sein, einfach ausdrücken:

Lemma 2.10: *Sei $S \in G$. $\vartheta[\eta_S]$ ist genau dann gerade Funktion, wenn $\#S \circ U \equiv g+1$ mod 4.*

Beweis : Nach Korollar 2.5 wissen wir, daß $\vartheta[\eta_S]$ genau dann gerade ist, wenn $4(\eta_S)_1^t(\eta_S)_2$ gerade ist. Andererseits ist $\#S \circ U = \#S + \#U - 2\#S \cap U \equiv g+1 \bmod 2$, daher werden wir zeigen, daß für alle $S \in G$ gilt

$$4(\eta_S)_1^t(\eta_S)_2 + \frac{\#S \circ U - (g+1)}{2} \equiv 0 \bmod 2 .$$

Diese Abbildung, $S \longmapsto 4(\eta_S)_1^t(\eta_S)_2 + \frac{\#S \circ U - (g+1)}{2} \bmod 2$ ist ein Gruppenhomomorphismus $\varphi : G \longrightarrow \mathbb{Z}/2\mathbb{Z}$, denn für $S, T \in G$ gilt mit $\#U = g+1$ und dem vorigen Lemma 2.9

$$\varphi(S \circ T) \equiv 4(\eta_S + \eta_T)_1^t(\eta_S + \eta_T)_2 + \frac{\#S \circ T \circ U - (g+1)}{2}$$

$$\equiv 4(\eta_S)_1^t(\eta_S)_2 + 4(\eta_T)_1^t(\eta_T)_2 + \langle \eta_S, \eta_T \rangle - \#S \cap (T \circ U) + \frac{\#S + \#U - (g+1) + (\#T \circ U - (g+1))}{2}$$

$$\equiv 4(\eta_S)_1^t(\eta_S)_2 + 4(\eta_T)_1^t(\eta_T)_2 + \#S \cap T - \#S \cap T - \#S \cap U + \frac{(\#S \circ U - (g+1)) + (\#T \circ U - (g+1)) + 2\#S \cap U}{2}$$

$$\equiv \varphi(S) + \varphi(T) \bmod 2 .$$

Aus der Definition von U und η_k für $k \in B$ errechnen wir leicht, daß $\varphi(S) \equiv 0$ für alle $S = \{k, \infty\}$ ist. Da diese G erzeugen, gilt auch $\varphi(S) \equiv 0$ für alle $S \in G$.

□

Die Verbindung zwischen der Mengenlehre und der Klassifikation der hyperelliptischen Thetafunktionen, die bei 0 verschwinden, liefert der folgende Satz von Mumford, die sogenannte "Fundamental Vanishing Property", den wir hier ohne Beweis vorstellen:

Satz 2.11: ([Mumford], IIIa, 6.7)
Sei $U \subset B$ die Menge der ungeraden Zahlen in B, $U = \{1, 3, ..., 2g+1\}$. Dann gilt für alle $\bar{S} \in \bar{G}$:

$$\vartheta[\eta_S](0) = 0 \qquad \Longleftrightarrow \qquad \#(S \circ U) \neq g+1 \ .$$

Bemerkung : Wegen $CS \circ U = C(S \circ U)$ und $\#B = 2g+2$ ist die Eigenschaft $\#(S \circ U) \neq g+1$ unabhängig von der Wahl des Repräsentanten S von $\bar{S}$.

Mit Hilfe dieses Satzes können wir die Additionstheoreme von Korollar 2.8, die auf den rechten Seiten 2^{2g} Summanden haben, so vereinfachen, daß sich diese Zahl auf 2^g verringert, indem wir mehrere der Gleichungen addieren. Motiviert wurde die Suche nach dieser Möglichkeit durch ein entsprechendes Verfahren im Fall $g = 1$ (siehe etwa [Mumford], I, §5, Gleichungen $(A_i), i = 1, ..., 16$, oder [Weber], §22).

Wir definieren dazu zwei Untergruppen $\mathcal{U}$ und $\mathcal{V}$ von $\bar{G}$:

$$\mathcal{U} = \left\{\bar{S} \in \bar{G} \mid S \subseteq \{1, 3, ..., 2g+1\} \vee CS \subseteq \{1, 3, ..., 2g+1\}\right\}$$
$$\mathcal{V} = \left\{\bar{T} \in \bar{G} \mid T \subseteq \{2, 4, ..., 2g+2\} \vee CT \subseteq \{2, 4, ..., 2g+2\}\right\} \ .$$

Man weist leicht nach, daß $\mathcal{U}$ und $\mathcal{V}$ tatsächlich Untergruppen von $\bar{G}$ sind, die orthogonal zueinander bezüglich der Bilinearform $<,>: \bar{G} \times \bar{G} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ sind.

Wegen $S \sim CS$ ist die Ordnung von $\mathcal{U}$ gleich der Anzahl der Teilmengen gerader Ordnung von $\{a_1, a_3, ..., a_{2g+1}\}$, also gleich 2^g. Analog ist auch $\#\mathcal{V} = 2^g$.

Lemma 2.12: *(i) Ist $\bar{S} \in \mathcal{U} \cup \mathcal{V} - \{\bar{\emptyset}\}$, dann ist $\vartheta[\eta_S](0) = 0$.*
(ii) Für alle $\bar{T} \in \bar{G}$ gilt

$$\sum_{\bar{S} \in \mathcal{U}} e^{\pi i \langle \eta_S, \eta_T \rangle} = \begin{cases} 2^g & , \text{falls } \bar{T} \in \mathcal{V} \\ 0 & , \text{sonst} \end{cases} \ .$$

(iii) Für alle $\bar{S} \in \bar{G}$ gilt

$$\sum_{\bar{T} \in \mathcal{V}} e^{\pi i \langle \eta_S, \eta_T \rangle} = \begin{cases} 2^g & , \text{falls } \bar{S} \in \mathcal{U} \\ 0 & , \text{sonst} \end{cases} \ .$$

Beweis : (i) Zunächst sei $\bar{S} \in \mathcal{U}$, $\bar{S} \neq \bar{\emptyset}$. Wir wählen den Repräsentanten S von $\bar{S}$ so, daß S nur ungerade Elemente enthält. Sei wieder $U = \{1, 3, ..., 2g+1\}$. Dann ist $S \subseteq U$, also $\#U \circ S = \#U - \#S = g + 1 - \#S \neq g + 1$ wegen $\#S \geq 2$. Nach Satz 2.11 gilt also $\vartheta[\eta_S](0) = 0$.

Wir erhalten das analoge Resultat für $\bar{T} \in \mathcal{V}$, indem wir U durch CU ersetzen und beachten, daß $T \circ CU = CT \circ U = C(T \circ U)$ ist. Satz 2.11 und die anschließende Bemerkung liefern dann den Beweis.

(ii) Seien $\bar{S} \in \mathcal{U}$ und $\bar{T} \in \mathcal{V}$. Wegen $\#\mathcal{U} = 2^g$ folgt aus der Orthogonalität von $\mathcal{U}$ und $\mathcal{V}$

$$\sum_{\bar{S} \in \mathcal{U}} e^{\pi i \langle \eta_S, \eta_T \rangle} = \sum_{\bar{S} \in \mathcal{U}} 1 = 2^g \ .$$

Sei nun $\bar{T} \in \bar{G} - \mathcal{V}$. Dann gibt es ein ungerades $a \in T$ und ein ungerades $b \in CT$, und der Gruppenhomomorphismus

$$f_{\bar{T}} : \mathcal{U} \longrightarrow \mathbb{Z}/2\mathbb{Z} \quad , \quad \bar{S} \longmapsto \langle \eta_S, \eta_T \rangle \equiv \#S \cap T \bmod 2$$

ist wegen $\#\{a, b\} \cap T = 1$ surjektiv. Aus dem Homomorphiesatz folgt nun, daß $\#\mathrm{Kern}(f_{\bar{T}}) = \frac{1}{2}\#\mathcal{U}$ ist, also erhalten wir

$$\sum_{\bar{S} \in \mathcal{V}} e^{\pi i \langle \eta_S, \eta_T \rangle} = \sum_{\bar{S} \in \mathrm{Kern}(f_T)} 1 + \sum_{\bar{S} \in \mathcal{U} - \mathrm{Kern}(f_T)} (-1) = 0 \ .$$

(iii) beweist man analog wie (ii).

□

Korollar 2.8 lautet in unserer neuen Schreibweise:

Korollar 2.8': *Für alle $\bar{T} \in \bar{G}$ gilt*

$$2^g \, \vartheta[\eta_T](x+u) \, \vartheta[\eta_T](x-u) \, \vartheta[\eta_T](0)^2 = \sum_{\bar{S} \in \bar{G}} e^{\pi i \langle \eta_S, \eta_T \rangle} \vartheta[\eta_S](x)^2 \, \vartheta[\eta_S](u)^2 \ .$$

Man beachte hier, daß keine weiteren Vorzeichen durch das Ersetzen der Charakteristiken durch Repräsentanten der Klassen von $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ entstehen, da sie in den betroffenen Summanden immer doppelt auftreten.

Wir summieren mehrere dieser Gleichungen auf und erhalten:

Proposition 2.13:

$$\begin{aligned} \vartheta[0](x+u) \, \vartheta[0](x-u) \, \vartheta[0](0)^2 &= \sum_{\bar{S} \in \mathcal{U}} \vartheta[\eta_S](x)^2 \, \vartheta[\eta_S](u)^2 \\ &= \sum_{\bar{T} \in \mathcal{V}} \vartheta[\eta_T](x)^2 \, \vartheta[\eta_T](u)^2 \ . \end{aligned}$$

Beweis : Die Summe der Gleichungen von Korollar 2.8' über alle $\bar{T} \in \mathcal{V}$ liefert

$$\sum_{\bar{T}\in\mathcal{V}} 2^g\, \vartheta[\eta_T](x+u)\, \vartheta[\eta_T](x-u)\, \vartheta[\eta_T](0)^2 = \sum_{\bar{T}\in\mathcal{V}} \sum_{\bar{S}\in\bar{G}} e^{\pi i\langle \eta_S, \eta_T\rangle} \vartheta[\eta_S](x)^2\, \vartheta[\eta_S](u)^2 \ .$$

Nach Lemma 2.12(i) ist $\vartheta[\eta_T](0) = 0$ für alle $\bar{T} \in \mathcal{V} - \{\bar{\emptyset}\}$. Also vereinfacht sich die Gleichung zu

$$2^g\, \vartheta[0](x+u)\, \vartheta[0](x-u)\, \vartheta[0](0)^2 = \sum_{\bar{S}\in\bar{G}} \Big(\sum_{\bar{T}\in\mathcal{V}} e^{\pi i\langle \eta_S, \eta_T\rangle} \Big) \vartheta[\eta_S](x)^2\, \vartheta[\eta_S](u)^2 \ .$$

Nach Lemma 2.12(iii) ist dies äquivalent zu

$$2^g\, \vartheta[0](x+u)\, \vartheta[0](x-u)\, \vartheta[0](0)^2 = \sum_{\bar{S}\in\mathcal{U}} 2^g\, \vartheta[\eta_S](x)^2\, \vartheta[\eta_S](u)^2 \ .$$

Analog zeigt man den zweiten Teil der Aussage.

□

Additionstheoreme für die anderen Thetafunktionen berechnen wir aus der vorstehenden Aussage, indem wir zu x eine geeignete Halbperiode addieren:

Satz 2.14: (Additionstheoreme für hyperelliptische Thetafunktionen)
Für $a, b \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ gilt :

$$\begin{aligned} \vartheta[{a \atop b}](x+u)\, \vartheta[{a \atop b}](x-u)\, \vartheta[0](0)^2 &= \sum_{\bar{S}\in\mathcal{U}} e^{4\pi i a^t(\eta_S)_2} \vartheta[\eta_S + \left({a \atop b}\right)](x)^2\, \vartheta[\eta_S](u)^2 \\ &= \sum_{\bar{T}\in\mathcal{V}} e^{4\pi i a^t(\eta_T)_2} \vartheta[\eta_T + \left({a \atop b}\right)](x)^2\, \vartheta[\eta_T](u)^2 \ . \end{aligned}$$

Beweis : Ersetzen wir in Proposition 2.13 x durch $x + \Omega a + b$, dann verändert sich die linke Seite nach Lemma 2.3 zu

$$\begin{aligned} &\vartheta[0](x+u+\Omega a+b)\, \vartheta[0](x-u+\Omega a+b)\, \vartheta[0](0)^2 \\ &\qquad = e^{-2\pi i a^t \Omega a - 4\pi i a^t(x+b)} \vartheta[{a \atop b}](x+u)\, \vartheta[{a \atop b}](x-u) \vartheta[0](0)^2 \end{aligned}$$

und die rechte Seite zu

$$\begin{aligned} &\sum_{\bar{S}\in\mathcal{U}} \vartheta[\eta_S](x+\Omega a+b)^2\, \vartheta[\eta_S](u)^2 \\ &\qquad = e^{-2\pi i a^t \Omega a - 4\pi i a^t(x+b)} \sum_{\bar{S}\in\mathcal{U}} e^{4\pi i a^t(\eta_S)_2} \vartheta[\eta_S + \left({a \atop b}\right)](x)^2\, \vartheta[\eta_S](u)^2 . \end{aligned}$$

Analog zeigt man wieder den zweiten Teil der Aussage.

□

2.4 : Frobeniussche Thetaformel

Als weitere Anwendung der Riemannschen Thetaformel und der "Fundamental Vanishing Property", Satz 2.11, beweist man die Frobeniussche Thetaformel. Im 4. Kapitel beweisen wir Beziehungen zwischen Theta-Null-Werten, das sind Derivationen der Thetafunktionen, ausgewertet an der Stelle 0, indem wir die Parameter der Frobeniusschen Thetaformel geeignet wählen.

Satz 2.15: (Verallgemeinerte Frobeniussche Thetaformel)
Seien $z_1, z_2, z_3, z_4 \in \mathbb{C}^g$ *mit* $z_1 + z_2 + z_3 + z_4 = 0$ *und* $a_1, a_2, a_3, a_4 \in \frac{1}{2}\mathbb{Z}^{2g}$ *mit* $a_1 + a_2 + a_3 + a_4 = 0$. *Dann gilt :*

$$\sum_{j \in B} (-1)^j \prod_{i=1}^{4} \vartheta[a_i + \eta_j](z_i) = 0 \ .$$

Beweis : Siehe [Mumford], IIIa, §7.

□

Eine Anwendung der Frobeniusschen Thetaformel ist das Verschwinden von Ableitungen der Thetafunktionen an der Stelle 0.

Satz 2.16: *Sei* $S \subseteq B$ *gerader Ordnung,* $k \geq 0$ *und* d *eine beliebige Derivation. Ist* $\#S \circ U < g + 1 - 2k$ *oder* $\#S \circ U > g + 1 + 2k$, *dann ist*

$$d^k \vartheta[\eta_S](0) = 0 \ .$$

Beweis : (Vollständige Induktion nach k)
$k = 0$: Satz 2.11.
Sei nun $k > 0$ und die Behauptung für kleinere ganze Zahlen schon bewiesen. Sei $\#S \circ U < g+1-2k$. Ersetzt man S im Fall $\#S \circ U > g+1+2k$ durch sein Komplement in B, dann wird auch dieser Fall in unsere Betrachtung mit eingeschlossen.

Sei $T := S \circ U$, d.h. $\#T < g + 1 - 2k$ und $\#T \equiv g + 1 \bmod 2$. Ist $\#T \equiv g - 1 - 2k \bmod 4$, dann ist nach Lemma 2.10 $d^k \vartheta[\eta_S]$ ungerade Funktion, also trivialerweise $d^k \vartheta[\eta_S](0) = 0$.

Im folgenden nehmen wir daher an, daß $\#T \equiv g + 1 - 2k \bmod 4$ ist.

Wir wählen drei paarweise disjunkte Teilmengen $X, Y, Z \subseteq B-T$ mit je $\frac{1}{2}(g+1-\#T)$ Elementen. Dies ist möglich, denn zunächst ist wegen $\#T \equiv g+1 \bmod 2$ die Zahl $\frac{1}{2}(g+1-\#T)$ ganz, wegen $\#T < g+1-2k$ und $k>0$ sind die Mengen nichtleer, und wegen $3 \cdot \frac{1}{2}(g+1-\#T) < 2g+2-\#T = \#B - \#T$ können X, Y, Z auch paarweise disjunkt in $B-T$ gewählt werden.

Ferner wählen wir ein Element $x \in X$ und setzen in der Frobeniusschen Thetaformel

$$z_1 := z, z_2 := -z, z_3 := 0, z_4 := 0$$

$$\begin{aligned} a_1 &:= \eta_{T \circ U} + \eta_x \\ a_2 &:= \eta_{(T \cup X \cup Y) \circ U} + \eta_x \\ a_3 &:= \eta_{(T \cup X \cup Z) \circ U} + \eta_x \\ a_4 &:= -a_1 - a_2 - a_3 \ . \end{aligned}$$

Wenden wir k-mal die Derivation d nach z auf die Gleichung an und setzen anschließend $z := 0$, dann erhalten wir

$$\sum_{j \in B} (-1)^j \left(\sum_{l=0}^{k} (-1)^l \binom{k}{l} d^{k-l} \vartheta[a_1 + \eta_j](0)\ d^l \vartheta[a_2 + \eta_j](0) \right) \cdot \vartheta[a_3 + \eta_j](0)\ \vartheta[a_4 + \eta_j](0) = 0 \ .$$

Wir werden zeigen, daß in dieser Gleichung auf der linken Seite nur genau ein Summand stehen bleibt. Dazu berechnen wir Repräsentanten $S_1(j), ..., S_4(j) \subseteq B$ der Klassen $\overline{S_i(j)}$ mit $a_i + \eta_j \equiv \eta_{S_i(j)} \bmod \mathbb{Z}^{2g}$, für die $\#S_i(j) \circ U$ minimal wird. Dann gilt $S_1(j) \circ U = (T \cup \{x\}) \circ \{j\}$, und wegen

$$\#S_1(j) \circ U = \#T + 2 - 2 \cdot \left\{ \begin{array}{ll} 0 & , \text{falls } j \notin T \cup \{x\} \\ 1 & , \text{sonst} \end{array} \right\} < g+3-2k$$

folgt nach Induktion $d^l \vartheta[a_1 + \eta_j](0) = 0$ für $0 \leq l < k$. In der obigen Gleichung bleibt also noch

$$\sum_{j \in B} (-1)^j\ d^k \vartheta[a_1 + \eta_j](0)\ \vartheta[a_2 + \eta_j](0)\ \vartheta[a_3 + \eta_j](0)\ \vartheta[a_4 + \eta_j](0) = 0 \ .$$

Wir testen nun, welche Summanden in dieser Summe noch verschwinden. Dazu berechnen wir zunächst die Ordnungen der übrigen $S_i(j) \circ U$, um Satz 2.11 anwenden zu können:

$$
\begin{aligned}
S_2(j) \circ U &= (T \cup X \cup Y) \circ \{x\} \circ \{j\} = (T \cup X \cup Y - \{x\}) \circ \{j\} \\
\#S_2(j) \circ U &= \#T + \#X + \#Y - 1 + 1 - 2 \cdot \begin{cases} 0 & \text{, falls } j \notin T \cup X \cup Y - \{x\} \\ 1 & \text{, sonst} \end{cases} \\
&= g + 1 - 2 \cdot \begin{cases} 0 & \text{, falls } j \notin T \cup X \cup Y - \{x\} \\ 1 & \text{, sonst} \end{cases} \\
S_3(j) \circ U &= (T \cup X \cup Z - \{x\}) \circ \{j\} \\
\#S_3(j) \circ U &= g + 1 - 2 \cdot \begin{cases} 0 & \text{, falls } j \notin T \cup X \cup Z - \{x\} \\ 1 & \text{, sonst} \end{cases} \\
S_4(j) \circ U &= (T \cup Y \cup Z \cup \{x\}) \circ \{j\} \\
\#S_4(j) \circ U &= g + 3 - 2 \cdot \begin{cases} 0 & \text{, falls } j \notin T \cup Y \cup Z \cup \{x\} \\ 1 & \text{, sonst} \end{cases}
\end{aligned}
$$

Zu $\vartheta[a_2 + \eta_j](0)\ \vartheta[a_3 + \eta_j](0)\ \vartheta[a_4 + \eta_j](0) \neq 0$ ist nach Satz 2.11 äquivalent, daß $\#S_2(j) \circ U = \#S_3(j) \circ U = \#S_4(j) \circ U = g + 1$ ist, also

$$
j \notin T \cup X - \{x\} \cup Y, j \notin T \cup X - \{x\} \cup Z \text{ und } j \in T \cup Y \cup Z \cup \{x\} \ ,
$$

also $j = x$.
In der Summe bleibt daher nur der Summand

$$
(-1)^x\ d^k\vartheta[a_1 + \eta_x](0)\ \vartheta[a_2 + \eta_x](0)\ \vartheta[a_3 + \eta_x](0)\ \vartheta[a_4 + \eta_x](0) = 0
$$

übrig, wobei die letzten drei Faktoren ungleich 0 sind. Es folgt, daß $d^k\vartheta[a_1 + \eta_x](0) = 0$ ist, dies ist aber äquivalent zu $d^k\vartheta[\eta_S](0) = 0$.

□

Kapitel 3 : Konstruktion meromorpher Funktionen auf hyperelliptischen Tori

In diesem Kapitel werden wir zunächst eine meromorphe Funktion $\wp : \mathbb{C}^g/\Gamma \longrightarrow \mathbb{C}$ definieren, die sowohl in der Konstruktion, als auch in ihren Eigenschaften als Verallgemeinerung der Weierstraßschen $\wp$-Funktion im Fall $g = 1$ aufgefaßt werden kann. Im wesentlichen ist sie die zweite logarithmische Ableitung einer Thetafunktion, $\vartheta[\delta]$, wobei wir das δ unten noch explizit angeben werden.

Als Einstieg in die Theorie meromorpher Funktionen auf hyperelliptischen Tori beweist man, daß eine nichtkonstante meromorphe Funktion $f : \mathbb{C}^g/\Gamma \longrightarrow \mathbb{C}$ mindestens die Ordnung 2 hat; der Beweis verläuft dabei analog zu dem im Fall $g = 1$. Die Ordnung von f definiert man als die Anzahl der Polstellendivisoren, die auch gleich der Anzahl der Nullstellendivisoren ist, wobei Vielfachheiten jeweils mitgezählt werden.

Im zweiten Abschnitt werden wir dann Gleichungen für die Jacobische Varietät einer hyperelliptischen Kurve mit den Ableitungen der $\wp$-Funktion als Koordinaten herleiten und einen Algorithmus angeben, der diese Gleichungen bei gegebener Kurvengleichung berechnet.

3.1 : Die $\wp$-Funktion

Die Konstruktion meromorpher Funktionen beginnt im Fall $g = 1$ mit der Weierstraßschen σ-Funktion $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$, die holomorph und bezüglich Γ quasiperiodisch ist und nur auf den Gitterpunkten von Γ Nullstellen hat, die einfach sind. Man kann z.B. $\sigma(z) = \vartheta[{}^{1/2}_{1/2}](z)$ wählen. Dann definiert man $\wp(z) := -\frac{d^2}{dz^2}\log(\sigma(z)) + const.$, und man sieht leicht, daß $\wp(z)$ eine gerade elliptische Funktion der Ordnung 2 ist. Wählt man die Konstante so, daß die Laurententwicklung von $\wp(z)$ um $z = 0$ keinen konstanten Term besitzt, dann erfüllt $\wp(z)$ die Differentialgleichung $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, und man kann $\wp(z), \wp'(z)$ als Koordinaten für die elliptische Kurve
$E : Y^2 = 4X^3 - g_2X - g_3$ benutzen. Genauer ist die Abbildung

$$\mathbb{C}/\Gamma \longrightarrow E \subset \mathbb{P}^2(\mathbb{C}) \quad , \quad z \longmapsto [\wp(z), \wp'(z), 1]$$

ein komplex-analytischer Isomorphismus komplexer Liegruppen (siehe [Silverman], VI, 3.6).

Einen Ansatz, diesen Prozeß auf den Fall $g = 2$ zu verallgemeinern, führt Grant in [Grant] explizit aus. Er arbeitet dort mit drei $\wp$-Funktionen, nämlich nach geeigneter

Wahl einer σ-Funktion den drei zweiten partiellen logarithmischen Ableitungen von $-\sigma(z)$. Zusammen mit fünf $\wp'$-Funktionen liefert dieser Ansatz eine Darstellung von $\mathrm{Jac}(C)-\Theta$ als affine Varietät durch 6 Gleichungen in 8 Koordinaten. Diesen Ansatz werden wir hier nicht weiter verfolgen, da Mumford in [Mumford], IIIa, §10 eine niedrigerdimensionale Darstellung von $\mathrm{Jac}(C)-\Theta$ definiert, die für unsere Zwecke, nämlich einen effektiven Algorithmus zu beschreiben, geeigneter ist, und welche auch für größeres g leicht berechnet werden kann.

Wir nehmen dazu die im 1. Kapitel gewählte Derivation, D_∞, und definieren die Verallgemeinerung der Weierstraßschen $\wp$-Funktion durch

$$\wp(z) := -4\, D_\infty^2(\log \vartheta[\delta](z)) + const.$$

mit einem geeigneten $\delta \in \frac{1}{2}\mathbb{Z}^{2g}$. Setzen wir dann noch $\wp^{(k)}(z) := D_\infty^k \wp(z)$, dann erhalten wir mit $\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)$ als Koordinaten eine Einbettung von $\mathrm{Jac}(C)-\Theta$ in den affinen Raum $\mathbb{A}^{2g}$. Mit Hilfe der drei Polynome $u(t), v(t), w(t)$, die wir im ersten Kapitel definiert haben, leiten wir im nächsten Abschnitt beschreibende Gleichungen für die so entstandene Varietät her.

In diesem Kapitel sei wieder $B = \{1, 2, ..., 2g+2\}$ die Indexmenge der Verzweigungspunkte $a_1, a_2, ..., a_{2g+1}, a_{2g+2} = \infty$, $B' = B - \{2g+2\}$ und $U = \{1, 3, 5, ..., 2g+1\}$ die Teilmenge der ungeraden Indizes. Wir kommen nun zur Wahl einer geeigneten Charakteristik δ, die die Menge Θ der Divisorklassen

$$D = \sum_{i=1}^{r} P_i - r \cdot \infty \text{ mit } p_i \neq \infty \ , \ P_i' \neq P_j \text{ für } i \neq j$$

mit $r < g$ mit dem Nulldivisor der $\vartheta[\delta]$-Funktion identifiziert:

$$\delta := \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \cdots & \frac{1}{2} & \frac{1}{2} \\ \frac{g}{2} & \frac{g-1}{2} & \cdots & 1 & \frac{1}{2} \end{pmatrix} = \sum_{k \in U} \eta_k \in \tfrac{1}{2}\mathbb{Z}^{2g} \ .$$

Satz 3.1: ([Mumford], IIIa, 5.3) *Sei $\omega = (\omega_1, ..., \omega_g)^t$ die im 1. Kapitel gewählte Basis der holomorphen Differentiale. Dann gelten :*
(i) Für alle $z \in \mathbb{C}^g$ gilt

$$\vartheta[\delta](z) = 0 \iff \exists\, P_1, ..., P_{g-1} \in C \text{ mit } z \equiv \sum_{i=1}^{g-1} \int_\infty^{P_i} \omega \ mod\ \Gamma \ ,$$

d.h. $Jac(C)-\Theta$ wird mit dem Isomorphismus $Jac(C) \longrightarrow \mathbb{C}^g/\Gamma$ des ersten Kapitels analytisch mit $(\mathbb{C}^g/\Gamma) - (V(\vartheta[\delta])/\Gamma)$ identifiziert, wobei $V(\vartheta[\delta]) \subset \mathbb{C}^g$ den Nulldivisor der $\vartheta[\delta]$-Funktion bezeichnet, welcher von der Vielfachheit 1 ist.

(ii) Zu allen $k \in B'$ existieren Konstanten c_k, so daß für alle Divisoren $D = \sum_{i=1}^{g} P_i \in Div_0^{+,g}(C)$, $P_i = (x_i, y_i)$, mit zugeordnetem Polynom $u^D(t) = \prod_{i=1}^{g}(t - x_i)$ gilt

$$u^D(a_k) = c_k \left(\frac{\vartheta[\delta + \eta_k](z)}{\vartheta[\delta](z)} \right)^2 \quad mit\ z \equiv \sum_{i=1}^{g} \int_{\infty}^{P_i} \omega \ mod\ \Gamma \ .$$

Dies zeigt nach Bemerkung 2.2 insbesondere, daß die Koeffizienten von $u^D(t)$ meromorphe Funktionen auf $\mathbb{C}^g/\Gamma$ sind.

Dieser Satz ist die wichtigste Verbindung zwischen den beiden Darstellungen der Jacobischen Varietät. Der erste Teil motiviert die Wahl von $\vartheta[\delta]$ als Analogon zur Weierstraßschen σ-Funktion. Der zweite Teil liefert, wie wir später noch sehen werden, Beziehungen zwischen der Kurvengleichung und den Thetafunktionen über das Divisorklassengruppenmodell der Jacobischen Varietät. Wegen der Identifizierung von Θ mit $V(\vartheta[\delta])$ bezeichnen wir letzteres im folgenden ebenfalls mit Θ. Analog zum Fall $g = 1$ beweist man leicht, daß die von uns eingeführten Thetafunktionen den Nulldivisorgrad 1 haben, so daß speziell $\vartheta[\delta]$ genau den Nulldivisor Θ mit der Vielfachheit 1 hat.

Zum Beweis des Satzes möchten wir nur anmerken, daß der erste Teil eine Folgerung eines Satzes von Riemann ist, siehe [Mumford], II, §3. Beim Beweis des zweiten Teils wird ausgenutzt, daß nichtkonstante meromorphe Funktionen auf hyperelliptischen Tori mindestens die Ordnung 2 haben.

Interessante Anwendungen des zweiten Teils werden wir durch Spezialisierung der Divisorklasse D auf eine 2-Torsionsklasse bekommen. Ihr kanonischer Repräsentant besteht dann aus Verzweigungspunkten der Kurve und es gilt

Korollar 3.2: *Für eine Teilmenge T von B' gilt*

$$\Omega(\eta_T)_1 + (\eta_T)_2 \equiv \sum_{i \in T} \int_{\infty}^{(a_i,0)} \omega \ mod\ \Gamma \ .$$

Beweis : Dieses ergibt sich aus der Definition der η_i und Integration der rechten Seite dieser Gleichung für spezielle ein- und zweielementige Teilmengen von B. Die expliziten Rechnungen findet man in [Mumford], IIIa, 5.6-5.7.

□

In der folgenden Definition geben wir unsere Verallgemeinerung der Weierstraßschen $\wp$-Funktion an. Im ersten Kapitel haben wir die Derivation D_∞ mit der Derivation $-\sum_{i=1}^{g} e_i \frac{\partial}{\partial z_i}$ identifiziert. Wenden wir diese auf eine meromorphe Funktion $f : \mathbb{C}^g \longrightarrow \mathbb{C}$ an, dann schreiben wir ebenfalls entweder $D_\infty(f(z))$ oder auch einfacher $f'(z)$. Aus dem Zusammenhang wird immer ersichtlich sein, welche Derivation gemeint ist.

Definition und Satz 3.3: *Wir definieren*

$$\wp(z) := -4\, D_\infty^2\Big(\log \vartheta[\delta](z)\Big) + d$$

mit einer Konstanten d, die wir in der folgenden Proposition geeignet bestimmen werden. Dann gilt:
$\wp : \mathbb{C}^g \longrightarrow \mathbb{C}$ ist eine gerade und bezüglich Γ periodische meromorphe Funktion, definiert also insbesondere eine meromorphe Funktion $\wp : \mathbb{C}^g/\Gamma \longrightarrow \mathbb{C}$, mit einem Polstellendivisor der Ordnung 2 entlang Θ.

Beweis : Die Periodizität von $\wp$ folgt aus Lemma 2.1, denn es gilt für $p, q \in \mathbb{Z}^g$

$$\begin{aligned}
\wp(z + \Omega p + q) &= -4\, D_\infty^2\Big(\log \vartheta[\delta](z + \Omega p + q)\Big) + d \\
&= -4\, D_\infty^2\Big(\log(e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q})\Big) - 4\, D_\infty^2\Big(\log \vartheta[\delta](z)\Big) + d \\
&= -4\, D_\infty^2\Big(\log \vartheta[\delta](z)\Big) + d = \wp(z)\ .
\end{aligned}$$

Wir haben hier ausgenutzt, daß die Derivation nach z gleich der Derivation nach $z + \Omega p + q$ ist.

Daß $\wp$ eine gerade Funktion ist, liest man aus der Definition ab. Da $\vartheta[\delta]$ einen Nulldivisor der Ordnung 1 entlang Θ hat, hat $\wp$ als zweite logarithmische Ableitung von $\vartheta[\delta]$ einen Poldivisor der Ordnung 2 entlang Θ.

□

Die folgende Proposition stellt die Verbindung zwischen den Polynomen $u(t)$, $v(t)$, $w(t)$ und der $\wp$-Funktion her. Mit ihr können wir auch die Wahl der Konstanten d in der Definition der $\wp$-Funktion begründen, denn sie wurde so gewählt, daß diese Verbindung möglichst einfach wird. Aus dieser Proposition leiten wir anschließend beschreibende Gleichungen für $\mathrm{Jac}(C) - \Theta$ als affine Varietät her, und die Wahl dieser $\wp$-Funktion und ihrer Ableitungen als Koordinaten führt zu einem effektiven Verfahren, die beschreibenden Gleichungen in den Koeffizienten der Kurvengleichung für C auszudrücken.

Proposition 3.4: *Sei t in dem Modell*

$$Jac(C) - \Theta = \{(u(t), v(t), w(t)) \mid f(t) - v(t)^2 = u(t)w(t), \deg(u) = g, \deg(v) \leq g-1, \deg(w) = g+1\}$$

so gewählt, daß $D_\infty(u(t)) = v(t)$ ist. Mit den Bezeichnungen

$$u(t) = t^g + u_1 t^{g-1} + \cdots + u_g$$
$$w(t) = t^{g+1} + w_0 t^g + \cdots + w_g$$

gilt dann nach geeigneter Wahl der Konstanten d

$$w_0 - u_1 = 2\wp(z) \ .$$

Beweis : Wegen $\dot{u}(t) := D_\infty(u(t)) = v(t)$ gilt nach Satz 1.3,

$$\dot{v}(t) = \tfrac{1}{2}\Big(-w(t) + (t - u_1 + w_0)u(t)\Big) \ .$$

Mit $w(t) = \frac{f(t)}{u(t)} - \frac{v(t)^2}{u(t)}$ können wir $w_0 - u_1$ durch

$$w_0 - u_1 = 2\frac{\dot{v}(t)}{u(t)} + \frac{f(t)}{u(t)^2} - \frac{v(t)^2}{u(t)^2} - t$$

ausdrücken. Setzen wir speziell $t = a_k$ mit einem $k \in B - \{\infty\}$, dann gilt nach Satz 3.1

$$u(a_k) = c_k \cdot \Big(\frac{\vartheta[\delta + \eta_k](z)}{\vartheta[\delta](z)}\Big)^2$$

mit einer Konstanten c_k. Wenden wir D_∞ auf diese Gleichung an, dann bekommen wir

$$v(a_k) = 2c_k \frac{\vartheta[\delta+\eta_k](z)\ \vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta](z)^2} - 2c_k \frac{\vartheta[\delta+\eta_k](z)^2\ \vartheta[\delta]'(z)}{\vartheta[\delta](z)^3} \ ,$$

und nach nochmaliger Anwendung

$$\begin{aligned}\dot{v}(a_k) = {} & 2c_k \frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta](z)^2} + 2c_k \frac{\vartheta[\delta+\eta_k](z)\ \vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta](z)^2} \\ & - 8c_k \frac{\vartheta[\delta+\eta_k](z)\ \vartheta[\delta+\eta_k]'(z)\vartheta[\delta]'(z)}{\vartheta[\delta](z)^3} \\ & - 2c_k \frac{\vartheta[\delta+\eta_k](z)^2\ \vartheta[\delta]''(z)}{\vartheta[\delta](z)^3} + 6c_k \frac{\vartheta[\delta+\eta_k](z)^2\ \vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^4} \ .\end{aligned}$$

Damit erhalten wir

$$\frac{v(a_k)}{u(a_k)} = 2\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)} - 2\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} \ ,$$

sowie

$$\frac{\dot{v}(a_k)}{u(a_k)} = 2\,\frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta+\eta_k](z)^2} + 2\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)}$$

$$- 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} - 2\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} + 6\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2}\ .$$

Wegen $f(a_k) = 0$ können wir die linke Seite der Aussage schreiben als

$$w_0 - u_1 = 4\,\frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta+\eta_k](z)^2} + 4\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)}$$

$$- 16\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} - 4\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} + 12\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2}\ .$$

$$- 4\,\frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta+\eta_k](z)^2} + 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} - 4\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} - a_k$$

$$= 4\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)} - 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)}$$

$$- 4\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} + 8\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} - a_k$$

Mit

$$D_\infty^2(\log(\vartheta[\delta](z))) = \frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} - \frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2}$$

folgt

$$-8\,D_\infty^2(\log(\vartheta[\delta](z))) - (w_0 - u_1) = -4\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)}$$

$$-4\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)} + 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} + a_k\ .$$

Dies zeigt, daß die auf $\mathbb{C}^g/\Gamma$ meromorphe Funktion $-8\,D_\infty^2(\log(\vartheta[\delta](z))) - (w_0 - u_1)$ höchstens einfache Polstellen bei $V(\vartheta[\delta]) \cup V(\vartheta[\delta+\eta_k])$ hat. Da dies für alle $k \in B - \{\infty\}$ richtig ist, hat diese Funktion tatsächlich höchstens eine einfache Polstelle entlang Θ, dann ist sie aber eine Konstante, die wir mit $\tilde{d}$ bezeichnen.

Setzen wir $d := -\frac{1}{2}\tilde{d}$, dann folgt

$$2\wp(z) = -8D_\infty^2(\log(\vartheta[\delta](z))) + 2d = w_0 - u_1\ .$$

□

Bemerkung : (i) Die oben definierte Konstante d, bzw. $\tilde{d}$, können wir auch berechnen. Werten wir nämlich die Definition von $\tilde{d}$ im Beweis der Proposition an

der Stelle $z_0 := \Omega\delta_1 + \delta_2$ aus, dann bekommen wir

$$\begin{aligned}\tilde{d} &= -4\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} - 4\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)} + 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} + a_k\Big|_{z=z_0} \\ &= -4\,\frac{\vartheta[0]''(0)}{\vartheta[0](0)} - 4\,\lim_{z\to 0}\frac{\vartheta[\eta_k]''(z)}{\vartheta[\eta_k](z)} + 8\,\lim_{z\to 0}\frac{\vartheta[\eta_k]'(z)}{\vartheta[\eta_k](z)}\,\frac{\vartheta[0]'(z)}{\vartheta[0](z)} + a_k\ .\end{aligned}$$

Führen wir die Grenzwertberechnung explizit aus und berücksichtigen, daß $\vartheta[\eta_k]$ genau dann ungerade Funktion ist, wenn k gerade und ungleich ∞ ist, dann folgt mit dem Satz von l'Hospital

$$\tilde{d} = \begin{cases} -4\,\frac{\vartheta[0]''(0)}{\vartheta[0](0)} - 4\,\frac{\vartheta[\eta_k]''(0)}{\vartheta[\eta_k](0)} + a_k & \text{falls } k \in B-\{\infty\} \text{ ungerade} \\ -4\,\frac{\vartheta[0]''(0)}{\vartheta[0](0)} - 4\,\frac{\vartheta[\eta_k]'''(0)}{\vartheta[\eta_k]'(0)} + 8\frac{\vartheta[0]''(0)}{\vartheta[0](0)} + a_k & \text{falls } k \in B-\{\infty\} \text{ gerade}\ . \end{cases}$$

Da $\tilde{d}$ nicht von k abhängt, können wir $\tilde{d}$ auch als $\frac{1}{2g+1}\cdot(2g+1)\,\tilde{d}$ schreiben, also

$$\tilde{d} = -\frac{4}{2g+1}\Bigg(\sum_{\substack{k\in B-\{\infty\}\\ k \text{ ungerade}}}\left(\frac{\vartheta[\eta_k]''(0)}{\vartheta[\eta_k](0)} + \frac{\vartheta[0]''(0)}{\vartheta[0](0)}\right) + \sum_{\substack{k\in B-\{\infty\}\\ k \text{ gerade}}}\left(\frac{\vartheta[\eta_k]'''(0)}{\vartheta[\eta_k]'(0)} - \frac{\vartheta[0]''(0)}{\vartheta[0](0)}\right) - \frac{1}{4}\sum_{k\in B-\{\infty\}} a_k\Bigg)\ .$$

(ii) Mumford hat in [Mumford],IIIa,Proposition 10.1 eine ähnliche Aussage wie die in obiger Proposition behauptete bewiesen. Da erstens unser Beweis nicht die Theorie der Neumannschen dynamischen Systeme benutzt und zweitens die Aussage unseres Satzes sich auf die durch Satz 3.1 motivierte $\wp$-Funktion als Verallgemeinerung der Weierstraßschen $\wp$-Funktion stützt, haben wir den hier vorgestellten Beweis dem von Mumford vorgezogen.

□

3.2 : Gleichungen für die Jacobische Varietät

Wir kommen nun zum Hauptteil dieses Kapitels, nämlich Gleichungen für die Karte $\mathrm{Jac}(C) - \Theta$ der Jacobischen Varietät als affine Varietät in den Koordinaten $p^{(k)}(z)$ herzuleiten. Anstatt hier nur die Ergebnisse zu zitieren, siehe [Mumford],IIIa,10.3 und 10.6, werden wir auch den Beweis unserer $\wp$-Funktion angepaßt übernehmen, da er konstruktiv ist und direkt zu einem Algorithmus zur Berechnung der Gleichungen führt, mit dessen Implementation in Mathematica die Beispiele 3.7 berechnet wurden.

Satz 3.5: *Der Morphismus*

$$\varphi : Jac(C) - \Theta \longrightarrow \mathbb{C}^{2g}$$
$$z \longmapsto \left(\wp(z), \wp'(z), \wp''(z), ..., \wp^{(2g-1)}(z)\right)$$

ist eine Einbettung, d.h. die $\wp^{(i)}(z), 0 \leq i \leq 2g-1$, *erzeugen den affinen Ring von* $Jac(C) - \Theta$. *Speziell können wir mit Hilfe der Koeffizienten der Kurvengleichung* $C : Y^2 = f(X)$ *die* $\wp^{(i)}(z)$ *durch universelle Polynome in den Koeffizienten von* $u(t), v(t), w(t)$ *des Modells*

$$Jac(C) - \Theta = \{(u(t), v(t), w(t)) \mid f(t) - v(t)^2 = u(t)w(t), \deg(u) = g, \deg(v) \leq g-1, \deg(w) = g+1\}$$

ausdrücken, sowie die Koeffizienten von $u(t), v(t), w(t)$ *durch universelle Polynome in den* $p^{(i)}(z)$ *ausdrücken.*

Beweis : Seien

$$u(t) = t^g + u_1 t^{g-1} + \cdots + u_g$$
$$v(t) = v_1 t^{g-1} + \cdots + v_g$$
$$w(t) = t^{g+1} + w_0 t^g + \cdots + w_g$$

und

$$f(t) = t^{2g+1} + f_0 t^{2g} + \cdots + f_{2g}$$

mit

$$f(t) = u(t) \cdot w(t) + v(t)^2 \ .$$

Dividieren wir diese Gleichung durch t^{2g+1}, dann bekommen wir eine Polynomgleichung in t^{-1}, nämlich

$$\frac{f(t)}{t^{2g+1}} = \frac{u(t)}{t^g} \cdot \frac{w(t)}{t^{g+1}} + t^{-1} \cdot \left(\frac{v(t)}{t^g}\right)^2 \ . \qquad (1)$$

Das Polynom $\frac{f(t)}{t^{2g+1}}$ in t^{-1} mit konstantem Term 1 hat im Ring der Potenzreihen in t^{-1} eine eindeutige Quadratwurzel, sei etwa $\frac{f(t)}{t^{2g+1}} = \alpha(t^{-1})^2$ mit $\alpha(t^{-1}) = 1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + ...$. Die Koeffizienten $\alpha_1, \alpha_2, ...$ lassen sich aus den Koeffizienten von $f(t)$ berechnen. In der algorithmischen Beschreibung werden wir dies ausführen.

Dividieren wir die Gleichung (1) durch $\frac{f(t)}{t^{2g+1}} = \alpha(t^{-1})^2$, dann bekommen wir

$$1 = \frac{u(t)\, t^{-g}}{\alpha(t^{-1})} \cdot \frac{w(t)\, t^{-(g+1)}}{\alpha(t^{-1})} + t^{-1} \left(\frac{v(t)\, t^{-g}}{\alpha(t^{-1})}\right)^2 \ .$$

Diese Gleichung schreibt sich mit den Potenzreihen in t^{-1}

$$u^*(t^{-1}) := \frac{u(t)\, t^{-g}}{\alpha(t^{-1})}$$
$$v^*(t^{-1}) := \frac{v(t)\, t^{-g}}{\alpha(t^{-1})}$$
$$w^*(t^{-1}) := \frac{w(t)\, t^{-(g+1)}}{\alpha(t^{-1})}$$

in der Form

$$1 = u^*(t^{-1}) \cdot w^*(t^{-1}) + t^{-1} v^*(t^{-1})^2 \ . \tag{2}$$

Mit Hilfe der α_i können wir die Koeffizienten (u_i, v_i, w_i) durch die Koeffizienten (u_i^*, v_i^*, w_i^*) von u^*, v^*, w^* ausdrücken und umgekehrt, indem wir in den Gleichungen

$$\begin{aligned} u(t)\, t^{-g} &= u^*(t^{-1})\, \alpha(t^{-1}) \\ v(t)\, t^{-g} &= v^*(t^{-1})\, \alpha(t^{-1}) \\ w(t)\, t^{-(g+1)} &= w^*(t^{-1})\, \alpha(t^{-1}) \end{aligned} \tag{3}$$

bzw.

$$\begin{aligned} (1 + u_1 t^{-1} + \cdots + u_g t^{-g}) &= (1 + u_1^* t^{-1} + u_2^* t^{-2} + \cdots)\,(1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + \cdots) \\ (v_1 t^{-1} + v_2 t^{-2} + \cdots + v_g t^{-g}) &= (v_1^* t^{-1} + v_2^* t^{-2} + \cdots)\,(1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + \cdots) \\ (1 + w_0 t^{-1} + \cdots + w_g t^{-(g+1)}) &= (1 + w_0^* t^{-1} + w_1^* t^{-2} + \cdots)\,(1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + \cdots) \end{aligned}$$

die Koeffizienten vor den t^{-n} vergleichen. Insbesondere sind die $u_1, ..., u_g$ Polynome in den $u_1^*, ..., u_g^*$, die $v_1, ..., v_g$ Polynome in den $v_1^*, ..., v_g^*$ und die $w_0, ..., w_g$ Polynome in den $w_0^*, ..., w_g^*$. Zum Beispiel ist $u_1 = u_1^* + \alpha_1$, $v_1 = v_1^*$ und $w_0 = w_0^* + \alpha_1$.

Ebenfalls durch Koeffizientenvergleich in der Gleichung (2), bzw. in

$$(1 + u_1^* t^{-1} + u_2^* t^{-2} + \cdots) \cdot (1 + w_0^* t^{-1} + w_1^* t^{-2} + \cdots) = 1 - t^{-1}(v_1^* t^{-1} + v_2^* t^{-2} + \cdots)^2$$

lassen sich die w_k^* aus den u_i^* und den v_j^* berechnen, und zwar ist $u_1^* + w_0^* = 0$, und für $n \geq 1$ ist $u_{n+1}^* + w_n^*$ universelles Polynom in $u_1^*, ..., u_n^*$, $w_0^*, ..., w_{n-1}^*$ und $v_1^*, ..., v_{n-1}^*$. Da aber w_{n-1}^* schon universelles Polynom in $u_1^*, ..., u_n^*$, $w_0^*, ..., w_{n-2}^*$ und $v_1^*, ..., v_{n-2}^*$ ist, folgt induktiv

$$u_{n+1}^* + w_n^* = W_n(u_1^*, ..., u_n^*; v_1^*, ..., v_{n-1}^*) \tag{4}$$

mit einem universellen Polynom W_n in den Variablen $u_1^*, ..., u_n^*$ und $v_1^*, ..., v_{n-1}^*$. Dies zeigt, daß sich die w_k^* aus den u_i^* und den v_j^* berechnen lassen.

Die Verbindung dieser Modelle mit der $\wp$-Funktion wurde schon in Proposition 3.4 beschrieben, und zwar besagte diese, daß $\wp(z) = \frac{1}{2}(w_0 - u_1)$ ist. Wenden wir die oben genannten Beispiele der Koeffizientenvergleiche hierauf an, dann folgt

$$\wp(z) = \tfrac{1}{2}(w_0 - u_1) = \tfrac{1}{2}(w_0^* - u_1^*) = -u_1^* \ .$$

Wir untersuchen nun den Einfluß der Derivation D_∞ auf die Koeffizienten der Polynome u^*, v^*, w^*. Wegen $\dot{u}(t) = D_\infty(u(t)) = v(t)$ ist auch

$$\dot{u}^*(t^{-1}) = \frac{\dot{u}(t)\, t^{-g}}{\alpha(t^{-1})} = \frac{v(t)\, t^{-g}}{\alpha(t^{-1})} = v^*(t^{-1}) \ ,$$

also $\qquad \dot{u}^* = v^*.$ (5a)

Wegen $\dot{v}(t) = \frac{1}{2}\left(-w(t) + (t - u_1 + w_0)\, u(t)\right)$ folgt mit $\wp(z) = \frac{1}{2}(w_0 - u_1)$

$$\begin{aligned}\dot{v}^*(t^{-1}) = \frac{\dot{v}(t)\, t^{-g}}{\alpha(t^{-1})} &= \frac{1}{2}\left(-t\, \frac{w(t)\, t^{-(g+1)}}{\alpha(t^{-1})} + (t + 2\wp(z)) \cdot \frac{u(t)\, t^{-g}}{\alpha(t^{-1})}\right) \\ &= \tfrac{1}{2} t \left(-w^*(t^{-1}) + (1 + 2\wp(z)\, t^{-1}) \cdot u^*(t^{-1})\right)\ ,\end{aligned}$$

also $\qquad \dot{v}^* = \frac{1}{2} t \left(-w^* + (1 + 2\wp t^{-1}) u^*\right).$ (5b)

Aus $\dot{w}(t) = -(t - u_1 + w_0)\, v(t)$ folgt

$$\begin{aligned}\dot{w}^*(t^{-1}) = \frac{\dot{w}(t)\, t^{-(g+1)}}{\alpha(t^{-1})} &= -(t + 2\wp(z)) \cdot \frac{v(t)\, t^{-g}}{\alpha(t^{-1})} \cdot t^{-1} \\ &= -(1 + 2\wp(z)\, t^{-1}) \cdot v^*(t^{-1})\ ,\end{aligned}$$

also $\qquad \dot{w}^* = -(1 + 2\wp\, t^{-1}) \cdot v^*.$ (5c)

Drücken wir die Identitäten (5a) - (5c) in den Koeffizienten aus, dann erhalten wir für alle $i \geq 1$ mit $\wp(z) = -u_1^*$

$$\begin{aligned}\dot{u}_i^* &= v_i^* \\ \dot{v}_i^* &= \tfrac{1}{2}\left(-w_i^* + u_{i+1}^* - 2\, u_1^*\, u_i^*\right) \\ \dot{w}_i^* &= -v_{i+1}^* + 2\, u_1^*\, v_i^*\ .\end{aligned} \tag{6}$$

Mit dem Anfangswert $-u_1^* = \wp(z)$ folgt induktiv aus den Gleichungen (6), daß sich die $\wp^{(k)}(z)$ aus den u_i^* und v_j^* berechnen lassen, und zwar gilt

$$\begin{aligned}\wp(z) &= -u_1^* \\ \wp'(z) &= -\dot{u}_1^* = -v_1^* \\ \wp''(z) &= -\dot{v}_1^* = -\tfrac{1}{2}\left(-w_1^* + u_2^* - 2(u_1^*)^2\right) = -u_2^* + \tfrac{1}{2}\left(W_1(u_1^*) + 2(u_1^*)^2\right) \\ \wp'''(z) &= -v_2^* + \tfrac{1}{2}\left(\dot{W}_1(u_1^*) + 4u_1^*\, v_1^*\right) \\ &\vdots \\ \wp^{(2k)}(z) &= -u_{k+1}^* + \text{ universelles Polynom in } u_1^*, ..., u_k^*, v_1^*, ..., v_{k-1}^* \\ \wp^{(2k+1)}(z) &= -v_{k+1}^* + \text{ universelles Polynom in } u_1^*, ..., u_{k+1}^*, v_1^*, ..., v_k^*\ .\end{aligned}$$

Umgekehrt zeigen diese Überlegungen, daß sich die u_i^* und v_j^* aus den $\wp^{(k)}(z)$ berechnen lassen, und daher auch die w_i^*.

Wir haben bis jetzt gezeigt, daß die beiden Polynomringe

$$\mathbb{C}[u_1^*, u_2^*, ...; v_1^*, v_2^*, ...; w_0^*, w_1^*, ...] \Big/ (\text{Gleichungen (4)})$$

und

$$\mathbb{C}[\wp(z), \wp'(z), \wp''(z), ...]$$

isomorph sind. Dabei bildet der Isomorphismus die Derivation (6) auf die Derivation $D_\infty\left(\wp^{(k)}(z)\right) = \wp^{(k+1)}(z)$ und den Teilring

$$\mathbb{C}[u_1^*, ..., u_g^*; v_1^*, ..., v_g^*; w_0^*, ..., w_{g-1}^*] \Big/ \left(\{u_{n+1}^* + w_n^* = W_n(...) \mid 0 \leq n \leq g-1\}\right)$$

in den Teilring

$$\mathbb{C}[\wp(z), \wp'(z), \wp''(z), ..., \wp^{(2g-1)}(z)]$$

ab. Da die $u_1, ..., u_g, v_1, ..., v_g$, die den affinen Ring von $\mathrm{Jac}(C) - \Theta$ erzeugen, Polynome in den $u_1^*, ..., u_g^*, v_1^*, ..., v_g^*$ sind und diese wieder Polynome in den $\wp(z)$, $\wp'(z)$, $\wp''(z), ..., \wp^{(2g-1)}(z)$ sind, ist gezeigt, daß die Abbildung φ eine Einbettung ist.

□

Da der Morphismus φ nach dem vorigen Satz eine Einbettung ist, stellt sich die Frage, wie man das Bild von φ in $\mathbb{C}^{2g}$ beschreiben kann. Die Koeffizienten u_i, v_j, w_k lassen sich als universelle Polynome in den $\wp^{(i)}(z)$ schreiben, daher ist ein Punkt

$$\left(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)\right) \in \mathbb{C}^{2g}$$

genau dann im Bild von φ, wenn $f(t) - v(t)^2 = u(t) \cdot w(t)$ gilt. Mit Hilfe der Umrechnungsformeln des vorigen Beweises und dieser Gleichung berechnet der folgende Algorithmus ein System von g Polynomgleichungen in den $\wp^{(i)}(z)$, die genau das Bild von φ beschreiben. Ferner liefert er eine Gleichung der Form

$$\wp^{(2g)}(z) = \text{ Polynom in } \wp(z), \wp'(z), ..., \wp^{(2g-1)}(z) \ ,$$

mit der höhere Ableitungen von $\wp(z)$ in den ersten $2g-1$ Ableitungen ausgedrückt werden können.

Wir benutzen in dem Algorithmus die O-Schreibweise, d.h. wir schreiben für eine Potenzreihe $a(s) = \sum_{n=0}^{\infty} a_n s^n$ das Symbol

$$\sum_{n=0}^{k} a_n s^n + O(s^{k+1}) \ ,$$

wenn die Koeffizienten $a_{k+1}, ...$ die Ausgabedaten nicht mehr beeinflussen können.

Algorithmus 3.6: (Bestimmung der Gleichungen für die affine Varietät $\mathrm{Jac}(C) - \Theta$)

Eingabe : Das Polynom $f(X)$ einer hyperelliptischen Kurve $C : Y^2 = f(X)$ vom Geschlecht $g \geq 1$.

Ausgaben : (i) g Polynome $F_1(X_1, X_2, ..., X_{2g})$,

$$F_2(X_1, X_2, ..., X_{2g}),$$
$$\vdots$$
$$F_g(X_1, X_2, ..., X_{2g}) \in \mathbb{C}[X_1, X_2, ..., X_{2g}],$$

mit $(x_1, x_2, ..., x_{2g}) \in \varphi(\mathrm{Jac}(C) - \Theta)$ genau dann, wenn

$$\begin{aligned} & F_1(x_1, x_2, ..., x_{2g}) = 0 \\ \wedge \quad & F_2(x_1, x_2, ..., x_{2g}) = 0 \\ & \vdots \\ \wedge \quad & F_g(x_1, x_2, ..., x_{2g}) = 0 \ . \end{aligned}$$

(ii) Ein Polynom $F_0(X_1, X_2, ..., X_{2g}) \in \mathbb{C}[X_1, ..., X_{2g}]$ mit

$$\wp^{(2g)}(z) = F_0\left(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)\right) \ ,$$

mit dem wir auftretende höhere Ableitungen von $\wp(z)$ durch Polynome in den niedrigeren ersetzen können.

(iii) Die Koeffizienten $u_1, ..., u_g$, $v_1, ..., v_g$ und $w_0, ..., w_g$ als Polynome in den Ableitungen von $\wp(z)$. Diese Ausgaben werden bei späteren Rechnungen gebraucht.

Verfahren : Zur Vereinfachung der Schreibweise setzen wir $s := t^{-1}$.

1. Schritt : Aus den Definitionen von u^*, v^*, w^*, bzw. aus den Gleichungen (3) des Beweises berechnen wir $u_1, ..., u_g$ als Polynome in $u_1^*, ..., u_g^*$, analog für v und w:

Für $j = 1, ..., g$ setze

$u_j \longleftarrow$ Koeffizient von s^j in

$$\left(1 + \sum_{i=1}^{g} u_i^* s^i + O(s^{g+1})\right) \cdot \left(1 + \sum_{i=1}^{g} \alpha_i s^i + O(s^{g+1})\right)$$

$v_j \longleftarrow$ Koeffizient von s^j in

$$\left(\sum_{i=1}^{g} v_i^* s^i + O(s^{g+1})\right) \cdot \left(1 + \sum_{i=1}^{g} \alpha_i s^i + O(s^{g+1})\right)$$

Für $j = 0, ..., g$ setze

$w_j \longleftarrow$ Koeffizient von s^{j+1} in

$$\left(1 + \sum_{i=0}^{g} w_i^* s^{i+1} + O(s^{g+2})\right) \cdot \left(1 + \sum_{i=1}^{g+1} \alpha_i s^i + O(s^{g+2})\right) .$$

2. Schritt : Schreibe $w_0^*, ..., w_g^*$ als Polynome in $u_1^*, ..., u_{g+1}^*, v_1^*, ..., v_g^*$ nach Gleichung (2) des Beweises:

Für $j = 0, ..., g$ setze

$$w_j^* \longleftarrow -(\text{Koeffizient von } s^{j+1}) + w_j^* \text{ in}$$
$$\left(1 + \sum_{i=1}^{g+1} u_i^* s^i + O(s^{g+2})\right)\left(1 + \sum_{i=1}^{g+1} w_{i-1}^* s^i + O(s^{g+2})\right)$$
$$+ s\left(\sum_{i=1}^{g} v_i^* s^i + O(s^{g+1})\right)^2 - 1 .$$

Dann ist $w_j^* = -u_{j+1}^* +$ Polynom in $u_1^*, ..., u_j^*, v_1^*, ..., v_{j-1}^*$.

3. Schritt : Schreibe nach Gleichung (6) $u_1^*, ..., u_{g+1}^*, v_1^*, ..., v_g^*$ als Polynome in $\wp(z), \wp'(z), ..., \wp^{(2g)}(z)$:

Setze $\quad u_1^* \longleftarrow -\wp(z).$

Für $j = 1, ..., g$ setze rekursiv

$$\left\{ \begin{array}{c} v_j^* \longleftarrow D_\infty(u_j^*) \\ u_{j+1}^* \longleftarrow D_\infty(v_j^*) + \frac{1}{2}(w_j^* + u_{j+1}^*) + u_1^* u_j^* \end{array} \right\} .$$

Wir benutzen hier die Bemerkung zum 2. Schritt, nämlich daß $w_j^* + u_{j+1}^*$ Polynom in $u_1^*, ..., u_j^*$ und $v_1^*, ..., v_{j-1}^*$ist, so daß dieser Schritt tatsächlich explizit ist.

4. Schritt : An dieser Stelle können wir die α_j durch die Koeffizienten der Kurvengleichung ausdrücken. Wir bekommen aus der Definition von α die Gleichung

$$\frac{f(t)}{t^{2g+1}} = \left(\alpha(t^{-1})\right)^2 \quad \text{bzw.} \quad f(s^{-1})\, s^{2g+1} = (\alpha(s))^2 .$$

Die α_j berechnen sich dann folgendermaßen:

Für $j = 1, ..., 2g + 1$ setze

$$\alpha_j \longleftarrow -\tfrac{1}{2}(\text{Koeffizient von } s^j) + \alpha_j \text{ in}$$
$$\left(1 + \sum_{i=1}^{2g+1} \alpha_i s^i + O(s^{2g+2})\right)^2 - f(s^{-1}) s^{2g+1} .$$

5. Schritt : Nach diesen Vorbereitungen haben wir $u_1, ..., u_g, v_1, ..., v_g, w_0, ..., w_g$ als Polynome in $\wp(z), \wp'(z), ..., \wp^{(2g)}(z)$ ausgedrückt. Die Gleichung

$$u(t) \cdot w(t) + v(t)^2 - f(t) = 0$$

liefert nun die gesuchten Lösungen: Setze

$$loesgl \longleftarrow \left(t^g + \sum_{i=0}^{g-1} u_{g-i} t^i\right)\left(t^{g+1} + \sum_{i=0}^{g} w_{g-i} t^i\right)) + \left(\sum_{i=0}^{g-1} v_{g-i} t^i\right)^2 - f(t)$$

$$F_0 \longleftarrow -(\text{Koeffizient von } t^g \text{ der } loesgl) + \wp^{(2g)}(z) .$$

F_0 ist Polynom in $\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)$, und es gilt

$$\wp^{(2g)}(z) = F_0\left(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)\right)) \ .$$

Im folgenden ersetzen wir $\wp^{(2g)}(z)$ sofort durch $F_0\left(\wp(z), ..., \wp^{(2g-1)}(z)\right)$:

Für $j = 0, ..., g-1$ setze

$F_{g-j}\left(\wp(z), ..., \wp^{(2g-1)}(z)\right) \longleftarrow$ Koeffizient von t^j der *loesgl.*

Ersetzen wir in den erhaltenen Polynomen $\wp(z)$ durch $X_1, ..., \wp^{(2g-1)}(z)$ durch X_{2g}, dann erhalten wir die gesuchten Polynomen.

□

Bemerkung : Die erhaltenen Gleichungen reichen aus, $\mathrm{Jac}(C) - \Theta$ zu beschreiben, da dieses eine g-dimensionale Varietät ist.

Beispiele 3.7: Die beiden folgenden Beispiele sind Ausgaben des Algorithmus für die Fälle $g = 1$ bzw. $g = 2$. Wir haben hier für den späteren Gebrauch die ausgegebenen Polynome als Differentialausdrücke

$$F_i(\wp(z), ..., \wp^{(2g-1)}(z))$$

in $\wp(z)$ geschrieben, so wie sie vom vorherigen Algorithmus ohne die letzte Ersetzung bereitgestellt werden.

Speziell die Gleichungen für die Koeffizienten von u, v, w als Polynome in den Ableitungen von $\wp(z)$ werden später noch gebraucht, so daß wir hier schon die Abhängigkeit der Koeffizienten von z durch $u_i(z)$ statt u_i etc. ausdrücken.

(i) Elliptische Kurve : $C : Y^2 = X^3 + A\ X + B$. Das Programm liefert folgende Ausgabe:

$$F_0\left(\wp(z), \wp'(z)\right) = \frac{A}{2} + \frac{3\wp(z)^2}{2}$$

$$F_1\left(\wp(z), \wp'(z)\right) = -B - A\wp(z) - \wp(z)^3 + \wp'(z)^2$$

$$\begin{aligned} u_1(z) &= -\wp(z) \\ v_1(z) &= -\wp'(z) \\ w_0(z) &= \wp(z) \\ w_1(z) &= A + \wp(z)^2 \ . \end{aligned}$$

Die Differentialgleichung

$$F_1\left(\wp(z), \wp'(z)\right) = 0 \quad \text{bzw.} \quad \wp'(z)^2 = \wp(z)^3 + A\wp(z) + B$$

entspricht mit den Koordinaten $\wp(z), \wp'(z)$ genau der Kurvengleichung für C.

(ii) Hyperelliptische Kurve $C : Y^2 = X^5 + f_0\ X^4 + f_1\ X^3 + f_2\ X^2 + f_3\ X + f_4$ vom Geschlecht 2. Hier liefert das Programm die folgende Ausgabe:

$$\begin{aligned} F_0(\wp(z), ..., \wp^{(3)}(z)) = \tfrac{1}{16}\big(& f_1^3 - 4f_1f_2 + 8f_3 + 2f_1^2\wp(z) - 8f_2\wp(z) + 12f_1\wp(z)^2 \\ & - 40\wp(z)^3 + 40\wp'(z)^2 - 8f_1\wp''(z) + 80\wp(z)\wp''(z)\big) \end{aligned}$$

$$\begin{aligned} F_1(\wp(z), ..., \wp^{(3)}(z)) = \tfrac{1}{64}\Big(& 5f_1^4 - 24f_1^2f_2 + 16f_2^2 + 32f_1f_3 - 64f_4 - 8f_1^3\wp(z) \\ & + 32f_1f_2\wp(z) - 64f_3\wp(z) - 8f_1^2\wp(z)^2 + 32f_2\wp(z)^2 \\ & - 32f_1\wp(z)^3 + 80\wp(z)^4 + 32f_1\wp'(z)^2 - 320\wp(z)\wp'(z)^2 \\ & - 64\wp''(z)^2 + 128\wp'(z)\wp^{(3)}(z)\Big) \end{aligned}$$

$$\begin{aligned} F_2(\wp(z), ..., \wp^{(3)}(z)) = \tfrac{1}{64}\Big(& -f_1^5 + 8f_1^3f_2 - 16f_1f_2^2 - 8f_1^2f_3 + 32f_2f_3 - 64f_5 \\ & - 4f_1^4\wp(z) + 16f_1^2f_2\wp(z) - 32f_1f_3\wp(z) + 8f_1^3\wp(z)^2 \\ & - 32f_1f_2\wp(z)^2 + 96f_3\wp(z)^2 - 64f_2\wp(z)^3 + 112f_1\wp(z)^4 \\ & - 192\wp(z)^5 + 24f_1^2\wp'(z)^2 - 32f_2\wp'(z)^2 - 160f_1\wp(z)\wp'(z)^2 \\ & + 480\wp(z)^2\wp'(z)^2 - 8f_1^3\wp''(z) + 32f_1f_2\wp''(z) - 64f_3\wp''(z) \\ & - 16f_1^2\wp(z)\wp''(z) + 64f_2\wp(z)\wp''(z) - 96f_1\wp(z)^2\wp''(z) \\ & + 320\wp(z)^3\wp''(z) + 64\wp'(z)^2\wp''(z) - 128\wp(z)\wp''(z)^2 \\ & + 64f_1\wp'(z)\wp^{(3)}(z) - 384\wp(z)\wp'(z)\wp^{(3)}(z) + 64\wp^{(3)}(z)^2\Big) \end{aligned}$$

$$u_1(z) = \frac{f_1}{2} - \wp(z)$$
$$u_2(z) = -\frac{f_1^2}{8} + \frac{f_2}{2} - \frac{f_1\wp(z)}{2} + \frac{3\wp(z)^2}{2} - \wp''(z)$$

$$v_1(z) = -\wp'(z)$$
$$v_2(z) = -\frac{f_1\wp'(z)}{2} + 3\wp(z)\wp'(z) - \wp^{(3)}(z)$$

$$w_0(z) = \frac{f_1}{2} + \wp(z)$$
$$w_1(z) = -\frac{f_1^2}{8} + \frac{f_2}{2} + \frac{f_1\wp(z)}{2} - \frac{\wp(z)^2}{2} + \wp''(z)$$
$$w_2(z) = \frac{f_1^3}{8} - \frac{f_1 f_2}{2} + f_3 + \frac{f_1\wp(z)^2}{2} - 2\wp(z)^3 - \wp'(z)^2 + 2\wp(z)\wp''(z)$$

□

Kapitel 4 : Additionstheorem für die $\wp$-Funktion

Nach der Beschreibung der Jacobischen Varietät durch g Gleichungen in $2g$ Koordinaten ist der nächste Schritt, die abelsche Varietät $\mathrm{Jac}(C)$ als solche zu beschreiben, d.h. die Addition zweier Elemente in der gewählten Darstellung anzugeben. Fassen wir $\mathrm{Jac}(C)$ als komplexen Torus $\mathbb{C}^g/\Gamma$ auf, dann liefert die Vektorraumaddition auf $\mathbb{C}^g$ trivialerweise eine Addition auf $\mathbb{C}^g/\Gamma$. Von Cantor wurde in [Cantor] ein Additionsalgorithmus für das Modell

$$\mathrm{Jac}(C) - \Theta = \{(u(t), v(t), w(t)) \mid f(t) - v(t)^2 = u(t)w(t), \deg(u) = g, \\ \deg(v) \leq g-1, \deg(w) = g+1\}$$

beschrieben. Diesen könnte man zwar mit den Mitteln des vorigen Kapitels benutzen, um ein Additionstheorem für die $\wp$-Funktion herzuleiten, und damit der Varietät $\mathrm{Jac}(C) - \Theta$ eine durch Gleichungen in den Koordinaten dargestellte partielle Addition geben. Dies führt aber schon in kleinen allgemeinen Beispielen zu immens hohen Rechenzeiten.

Wir werden wieder dem Beispiel $g = 1$ folgen und aus dem Additionstheorem der $\vartheta[\delta]$-Funktion ein Additionstheorem für die $\wp$-Funktion herleiten. Unter einem Additionstheorem verstehen wir eine Gleichung der Form

$$\wp(x+u) = \text{ rationale Funktion in } \wp(x), ..., \wp^{(2g-1)}(x), \wp(u), ..., \wp^{(2g-1)}(u) \ ,$$

wobei $x, u, x+u \in (\mathbb{C}^g - \Theta)/\Gamma$ sind. Leiten wir diese Gleichung z.B. nach x ab und ersetzen $\wp^{(2g)}$ und höhere Ableitungen durch $F_0(\wp, ..., \wp^{(2g-1)})$ bzw. dessen Ableitungen, wobei F_0 eine der Ausgaben von Algorithmus 3.6 ist, dann erhalten wir die Additionstheoreme für $\wp', \wp'', ..., \wp^{(2g-1)}$. Insgesamt ergeben diese dann eine partielle Addition auf der Varietät $\mathrm{Jac}(C) - \Theta$; zusammen mit der im 1. Kapitel erwähnten Überdeckung von $\mathrm{Jac}(C)$ durch Karten isomorph zu $\mathrm{Jac}(C) - \Theta$ definiert dies dann eine Addition auf $\mathrm{Jac}(C)$.

Für eine Variable x sei D_∞^x die Derivation D_∞ nach x.

Satz 4.1: *Für $x, u \in \mathbb{C}^g$ mit $x, u, x+u \notin \Theta$ ist $\wp(x+u)$ rationale Kombination von $\wp(x), ..., \wp^{(2g-1)}(x), \wp(u), ..., \wp^{(2g-1)}(u)$, und es gilt*

$$\wp(x+u) = \tfrac{1}{2}\,\wp(x) + \tfrac{1}{2}\,\wp(u) \\ - (D_\infty^x + D_\infty^u)^2 \log\left(\sum_{T \in \mathcal{V}} e^{4\pi i \delta_1^t (\eta_T)_2} \cdot \frac{\vartheta[\delta + \eta_T](x)^2}{\vartheta[\delta](x)^2} \cdot \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2} \right) .$$

Beweis : Das Additionstheorem für $\vartheta[\delta]$ lautet nach Satz 2.14

$$\vartheta[\delta](x+u)\,\vartheta[\delta](x-u)\,\vartheta[0](0)^2 = \sum_{T\in\mathcal{V}} e^{4\pi i \delta_1^t(\eta_T)_2}\vartheta[\delta+\eta_T](x)^2\vartheta[\eta_T](u)^2 \ .$$

Wir dividieren diese Gleichung durch $\vartheta[\delta](x)^2\,\vartheta[\delta](u)^2$ und erhalten

$$\frac{\vartheta[\delta](x+u)\,\vartheta[\delta](x-u)}{\vartheta[\delta](x)^2\,\vartheta[\delta](u)^2}\,\vartheta[0](0)^2 = \sum_{T\in\mathcal{V}} e^{4\pi i \delta_1^t(\eta_T)_2}\cdot\frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\cdot\frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2} \ .$$

Als meromorphe Funktion $\mathbb{C}^g/\Gamma \longrightarrow \mathbb{C}$ mit Polstellen höchstens bei Θ sind

$$\frac{\vartheta[\delta+\eta_T](z)^2}{\vartheta[\delta](z)^2} \quad \text{sowie} \quad \frac{\vartheta[\eta_T](z)^2}{\vartheta[\delta](z)^2}$$

nach Satz 3.5 Polynome in $\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)$. Daher ist

$$-(D_\infty^x + D_\infty^u)^2 \log\left(\sum_{T\in\mathcal{V}} e^{4\pi i \delta_1^t(\eta_T)_2}\cdot\frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\cdot\frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2}\right)$$

rationaler Ausdruck in $\wp(x), ..., \wp^{(2g-1)}(x), \wp(u), ..., \wp^{(2g-1)}(u)$. Andererseits ist dieser gleich

$$\begin{aligned}
&-(D_\infty^x + D_\infty^u)^2 \log\left(\frac{\vartheta[\delta](x+u)\,\vartheta[\delta](x-u)}{\vartheta[\delta](x)^2\,\vartheta[\delta](u)^2}\,\vartheta[0](0)^2\right) \\
&\quad = -4\left(\frac{\vartheta[\delta]''(x+u)}{\vartheta[\delta](x+u)} - \frac{\vartheta[\delta]'(x+u)^2}{\vartheta[\delta](x+u)^2}\right) + 2\left(\frac{\vartheta[\delta]''(x)}{\vartheta[\delta](x)} - \frac{\vartheta[\delta]'(x)^2}{\vartheta[\delta](x)^2}\right) \\
&\qquad\qquad + 2\left(\frac{\vartheta[\delta]''(u)}{\vartheta[\delta](u)} - \frac{\vartheta[\delta]'(u)^2}{\vartheta[\delta](u)^2}\right) \\
&\quad = \wp(x+u) - d - \tfrac{1}{2}\,(\wp(x)+d) - \tfrac{1}{2}\,(\wp(u)+d) \\
&\quad = \wp(x+u) - \tfrac{1}{2}\,\wp(x) - \tfrac{1}{2}\,\wp(u) \ .
\end{aligned}$$

Also gilt:

$$\begin{aligned}
\wp(x+u) &= \tfrac{1}{2}\,\wp(x) + \tfrac{1}{2}\,\wp(u) \\
&\quad - (D_\infty^x + D_\infty^u)^2 \log\left(\sum_{T\in\mathcal{V}} e^{4\pi i \delta_1^t(\eta_T)_2}\cdot\frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\cdot\frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2}\right) \ ,
\end{aligned}$$

und $\wp(x+u)$ ist rationaler Ausdruck in $\wp(x), ..., \wp^{(2g-1)}(x), \wp(u), ..., \wp^{(2g-1)}(u)$.

□

Der nächste Schritt, das Additionstheorem explizit zu machen, ist der, die Quadrate von Thetaquotienten

$$\frac{\vartheta[\eta_T](z)^2}{\vartheta[\delta](z)^2} \quad \text{für } \bar{T} \in \mathcal{V}$$

als Polynome in den Ableitungen von $\wp(z)$ zu schreiben. Dies ist möglich, da diese Funktionen nur Polstellen bei Θ haben. Automatisch haben wir dann aber auch schon die anderen im Satz auftretenden Quotienten

$$\frac{\vartheta[\delta+\eta_T](z)^2}{\vartheta[\delta](z)^2} \quad \text{für } \bar{T} \in \mathcal{V}$$

berechnet, da diese ebenfalls von der Form

$$\frac{\vartheta[\eta_S](z)^2}{\vartheta[\delta](z)^2} \quad \text{mit einem } \bar{S} \in \mathcal{V}$$

sind. Denn da $\bar{U} \in \mathcal{V}$ im Fall g ungerade bzw. $\overline{U \circ \{\infty\}} \in \mathcal{V}$ im Fall g gerade ist, gilt dies mit $\delta = \eta_U$ bzw. $\delta = \eta_{U\circ\{\infty\}}$.

Zuvor müssen wir allerdings noch einige Konstanten berechnen. In diesem Kapitel sei $B' = \{1,2,3,...,2g+1\}$, $B = B' \cup \{2g+2\}$, $U = \{1,3,5,...,2g+1\}$ und $V = \{2,4,6,...,2g\}$. Für $k \in B'$ sei c_k die Konstante, die in Satz 3.1(ii) definiert wurde.

4.1 : Bestimmung von Quotienten von Thetanullwerten

In diesem Abschnitt werden wir einige allgemeine Quotienten von Thetanullwerten berechnen. Im nächsten Abschnitt werden wir dann durch Spezialisierung dieser Lemmata das Additionstheorem der $\wp$-Funktion explizit machen.

Das erste Lemma beschreibt die Quasiperiodizität der ersten beiden Ableitungen der ϑ-Funktionen

Lemma 4.2: *Für $a,b,c,d \in \frac{1}{2}\mathbb{Z}^g$ gilt mit $D_\infty = -\sum_{i=1}^{g} e_i \frac{\partial}{\partial z_i}$ und $e = (-e_1,...,-e_g)^t$*

(i) $$\vartheta[\tfrac{a}{b}]'(z+\Omega c+d) = e^{-\pi i c^t \Omega c - 2\pi i c^t (z+b+d)} \left(\vartheta[\tfrac{a+c}{b+d}]'(z) - 2\pi i c^t e \cdot \vartheta[\tfrac{a+c}{b+d}](z) \right),$$

(ii) $$\vartheta[\tfrac{a}{b}]''(z+\Omega c+d) = e^{-\pi i c^t \Omega c - 2\pi i c^t (z+b+d)} \Big(\vartheta[\tfrac{a+c}{b+d}]''(z) - 4\pi i c^t e \cdot \vartheta[\tfrac{a+c}{b+d}]'(z) - 4\pi^2 (c^t e)^2 \cdot \vartheta[\tfrac{a+c}{b+d}](z) \Big).$$

Beweis : Wir wenden D_∞ nach z auf die Gleichung von Lemma 2.3 an.

□

Lemma 4.3: *Seien $T \subseteq B'$ mit $\#T = g-1$ und $k,l \in B'-T$ verschieden. Dann gilt*

$$c_k \frac{\vartheta[\eta_{T\circ U} + \eta_{\{k,l\}}](0)^2}{\vartheta[\eta_{T\circ U} + \eta_l](0)^2} = e^{4\pi i(\eta_T)_1^t(\eta_k)_2} e^{4\pi i(\eta_l)_1^t(\eta_k)_2} \prod_{i\in T\cup\{l\}} (a_k - a_i) \ .$$

Beweis : Die linke Seite ist wegen $\#(T \circ U \circ \{l,\infty\}) \circ U = \#T + 2 = g+1$ nach Satz 2.11 definiert. Wir erinnnern daran, daß $\eta_l = \eta_{\{l,\infty\}}$ für $l \in B'$.

Sei $W := T \cup \{l\}$. Wegen $\#T = g-1$ und $\infty \notin T \cup \{l\} = W$ können wir Satz 3.1(ii) mit $D = \sum_{i\in W}(a_i, 0) - g\cdot\infty$ anwenden. Mit Korollar 3.2 lautet er

$$\begin{aligned} u^D(a_k) = \prod_{i\in W}(a_k - a_i) &= c_k \frac{\vartheta[\delta+\eta_k](\Omega(\eta_W)_1 + (\eta_W)_2)^2}{\vartheta[\delta](\Omega(\eta_W)_1 + (\eta_W)_2)^2} \\ &= c_k\, e^{-4\pi i(\eta_W)_1^t(\eta_k)_2} \frac{\vartheta[\eta_{T\circ U} + \eta_{\{k,l\}}](0)^2}{\vartheta[\eta_{T\circ U} + \eta_l](0)^2} \end{aligned}$$

nach Lemma 2.3.

□

Lemma 4.4: *Seien $T \subseteq B'$ mit $\#T = g-1$ und $k \in B'-T$. Dann gilt*

$$c_k \frac{\vartheta[\eta_{T\circ U}]'(0)^2}{\vartheta[\eta_{T\circ U} + \eta_k](0)^2} = -\tfrac{1}{4} e^{4\pi i(\eta_T)_1^t(\eta_k)_2} e^{4\pi i(\eta_k)_1^t(\eta_k)_2} \prod_{i\in B'-T-\{k\}} (a_k - a_i) \ .$$

Beweis : Die linke Seite ist wieder wegen $\#(T\circ U\circ\{k,\infty\})\circ U = g+1$ definiert. Wir leiten die Gleichung

$$u(a_k) = c_k \frac{\vartheta[\delta+\eta_k](z)^2}{\vartheta[\delta](z)^2}$$

von Satz 3.1(ii) zweimal nach z ab. Auf der linken Seite entspricht dies dem Ableitungsoperator $\dot{}$ aus Satz 1.3. Wir erhalten daher

$$\begin{aligned} &\tfrac{1}{2}(-w(a_k) + (a_k - u_1 + w_0)u(a_k)) \\ &\qquad = 2c_k \frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta](z)^2} + 2c_k \frac{\vartheta[\delta+\eta_k](z)\,\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta](z)^2} \\ &\qquad + 6c_k \frac{\vartheta[\delta+\eta_k](z)^2\,\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^4} - 2c_k \frac{\vartheta[\delta+\eta_k](z)^2\,\vartheta[\delta]''(z)}{\vartheta[\delta](z)^3} \\ &\qquad - 8c_k \frac{\vartheta[\delta+\eta_k](z)\,\vartheta[\delta+\eta_k]'(z)\vartheta[\delta]'(z)}{\vartheta[\delta](z)^3} \ . \end{aligned}$$

Sei $W := T \cup \{k\}$. Wegen $\#T = g-1$ und $\infty \notin T \cup \{k\} = W$ können wir anschließend $D = \sum_{i \in W} (a_i, 0) - g \cdot \infty$ einsetzen. Diesem sind die drei Polynome

$$\begin{aligned} u^D(a_k) &= \prod_{i \in W} (a_k - a_i) = 0 \text{ , da } k \in W, \\ v^D(a_k) &= 0, \\ w^D(a_k) &= \prod_{i \in B'-W} (a_k - a_i) \neq 0 \end{aligned}$$

zugeordnet. Wir erhalten daher mit Korollar 3.2

$$-\tfrac{1}{2} \prod_{i \in B'-W} (a_k - a_i) = -\tfrac{1}{2} w(a_k) = 2c_k \, \frac{\vartheta[\delta + \eta_k]'(\Omega(\eta_W)_1 + (\eta_W)_2)^2}{\vartheta[\delta](\Omega(\eta_W)_1 + (\eta_W)_2)^2} \, ,$$

da nach Satz 2.11 $\vartheta[\delta + \eta_k + \eta_W](0) = 0$ ist, denn $\#(U \circ \{k\} \circ W) \circ U = \#T = g-1$.

Aus Lemma 2.3 folgt dann die Behauptung.

□

Das folgende Lemma verschärft die Aussage von Satz 2.16 über das Verschwinden erster Ableitungen der ϑ-Funktionen bei Anwendung der speziellen Derivation D_∞.

Lemma 4.5: *Sei $T \subseteq B$ mit $\#T$ gerade, $\#T \circ U = g-1$ und $\infty \in T$. Dann gilt*

$$\vartheta[\eta_T]'(0) = 0 \, .$$

Beweis : Mumford beweist in [Mumford], IIIa, §9 diese Ausage mit Hilfe von Neumanns dynamischen Systemen. Man kann sich auch einen Beweis überlegen, der diese Theorie nicht benutzt. Dazu wählen wir $k, l \in B - T \circ U$ verschieden und setzen in der Frobeniusschen Thetaformel, Satz 2.15,

$$z_1 := z, z_2 := -z, z_3 := 0, z_4 := 0$$

$$a_1 := \eta_T, a_2 := -\eta_T, a_3 := \eta_T + \eta_{\{k,l\}}, a_4 := -\eta_T - \eta_{\{k,l\}} \, ,$$

leiten diese zweimal nach z ab und setzen anschließend $z := 0$. Streichen wir die verschwindenden Summanden, dann bekommen wir

$$\vartheta[\eta_T]'(0)^2 = - \sum_{j \in B - T \circ U - \{k,l\}} (-1)^j e^{4\pi i (\eta_j)_1^t (\eta_k + \eta_l)_2} \cdot \frac{\vartheta[\eta_T + \eta_j]'(0)^2}{\vartheta[\eta_T + \eta_{\{k,l\}}](0)^2} \cdot$$

$$\cdot \frac{\vartheta[\eta_T + \eta_{\{k,l\}} + \eta_j](0)^2}{\vartheta[\eta_T + \eta_{\{k,l\}}](0)^2} \, .$$

Aus Lemma 4.3 und Lemma 4.4 folgt dann nach einigen Rechnungen die Behauptung.

□

Im folgenden Lemma berechnen wir die Quadrate der Konstanten von Satz 3.1(ii):

Lemma 4.6: *Für $k \in B'$ gilt*

$$c_k^2 = e^{4\pi i(\eta_k)_1^t(\eta_k)_2} \prod_{i \in B'-\{k\}} (a_k - a_i) \ .$$

Beweis : Wir wählen $T \subseteq B'$ mit $\#T = g+1$ und $k \in T$. Satz 3.1(ii) lautet mit $D_1 = \sum_{i \in T-\{k\}} (a_i, 0) - g \cdot \infty$ nach Korollar 3.2

$$u^{D_1}(a_k) = \prod_{i \in T-\{k\}} (a_k - a_i) = c_k \ \frac{\vartheta[\delta + \eta_k](\Omega(\eta_{T-\{k\}})_1 + (\eta_{T-\{k\}})_2)^2}{\vartheta[\delta](\Omega(\eta_{T-\{k\}})_1 + (\eta_{T-\{k\}})_2)^2}$$

$$= c_k e^{4\pi i(\eta_T)_1^t(\eta_k)_2} e^{4\pi i(\eta_k)_1^t(\eta_k)_2} \cdot \frac{\vartheta[\eta_{T\circ U}](0)^2}{\vartheta[\eta_{T\circ U} + \eta_k](0)^2} \ .$$

Mit $D_2 = \sum_{i \in B'-T} (a_i, 0) - g \cdot \infty$ lautet Satz 3.1(ii) mit Korollar 3.2

$$u^{D_2}(a_k) = \prod_{i \in B'-T} (a_k - a_i) = c_k \ \frac{\vartheta[\delta + \eta_k](\Omega(\eta_{B'-T})_1 + (\eta_{B'-T})_2)^2}{\vartheta[\delta](\Omega(\eta_{B'-T})_1 + (\eta_{B'-T})_2)^2}$$

$$= c_k e^{4\pi i(\eta_{B'-T})_1^t(\eta_k)_2} \cdot \frac{\vartheta[\eta_{U\circ\{k\}\circ(B'-T)}](0)^2}{\vartheta[\eta_{U\circ\{\infty\}\circ(B'-T)}](0)^2} \ .$$

Wegen

$$U \circ \{k\} \circ (B' - T) \equiv U \circ \{k\} \circ B \circ \{\infty\} \circ T \equiv U \circ T \circ \{k, \infty\} \bmod (S \sim \mathcal{C}S)$$

sowie analog $U \circ \{\infty\} \circ (B' - T) \equiv U \circ T \bmod (S \sim \mathcal{C}S)$ folgt

$$u^{D_2}(a_k) = \prod_{i \in B'-T} (a_k - a_i) = c_k e^{4\pi i(\eta_T)_1^t(\eta_k)_2} \cdot \frac{\vartheta[\eta_{T\circ U} + \eta_k](0)^2}{\vartheta[\eta_{T\circ U}](0)^2} \ .$$

Multiplizieren wir beide Gleichungen für D_1 und D_2, dann erhalten wir

$$u^{D_1}(a_k) \cdot u^{D_2}(a_k) = \prod_{i \in B'-\{k\}} (a_k - a_i) = c_k^2 e^{4\pi i(\eta_k)_1^t(\eta_k)_2} \ ,$$

woraus die Behauptung folgt.

□

4.2 : Quadrate von Thetaquotienten

In diesem Abschnitt werden wir einen rekursiven Prozeß herleiten, der die auf $\mathbb{C}^g/\Gamma$ meromorphen Funktionen

$$\frac{\vartheta[\eta_T](z)^2}{\vartheta[\delta](z)^2} \quad \text{für } \bar{T} \in \mathcal{V}$$

als Polynome in $\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)$ ausdrückt. Dies ist möglich, da diese Funktionen meromorph mit einer Polstelle höchstens bei Θ sind.

Wegen $\bar{U} \in \mathcal{V}$ im Fall g ungerade bzw. $\overline{U \circ \{\infty\}} \in \mathcal{V}$ im Fall g gerade ist ein Fall trivial, nämlich

$$\frac{\vartheta[\delta](z)^2}{\vartheta[\delta](z)^2} = 1 \ .$$

Aus Satz 3.1(ii) leiten wir die nächsten Fälle her, denn es gilt für $k \in B'$, k gerade,

$$u(a_k) = a_k^g + u_1 \, a_k^{g-1} + ... + u_g = c_k \, \frac{\vartheta[\delta + \eta_k](z)^2}{\vartheta[\delta](z)^2} \ ,$$

wobei die Koeffizienten $u_1, ..., u_g$ Polynome in den Ableitungen von $\wp(z)$ sind, die bei Algorithmus 3.6 mit ausgegeben werden.

Beispiel : $g = 2$.
In diesem Fall ist

$$\mathcal{V} = \left\{ \bar{\emptyset}, \overline{\{2,6\}}, \overline{\{4,6\}}, \overline{\{2,4\}} \right\} \ ,$$

$$\eta_\emptyset \equiv 0 \ , \ \eta_{\{2,6\}} \equiv \eta_2 \ , \ \eta_{\{4,6\}} \equiv \eta_4 \ , \ \eta_{\{2,4\}} \equiv \delta \bmod \mathbb{Z}^{2g} \ .$$

Obige Ausführungen ergeben

$$c_4 \, \frac{\vartheta[\delta + \eta_4](z)^2}{\vartheta[\delta](z)^2} = c_4 \, \frac{\vartheta[\eta_2](z)^2}{\vartheta[\delta](z)^2} = a_4^2 + u_1 \, a_4 + u_2$$

$$c_2 \, \frac{\vartheta[\delta + \eta_2](z)^2}{\vartheta[\delta](z)^2} = c_2 \, \frac{\vartheta[\eta_4](z)^2}{\vartheta[\delta](z)^2} = a_2^2 + u_1 \, a_2 + u_2 \ .$$

Im Fall $g = 2$ fehlt also nur noch neben der Bestimmung der Konstanten die Berechnung von $\dfrac{\vartheta[0](z)^2}{\vartheta[\delta](z)^2}$.

□

Wir führen nun einige Bezeichnungen ein. V sei wieder die Menge $\{2, 4, 6, ..., 2g\}$ der geraden Zahlen in $B' = B - \{2g + 2\}$. Für $\bar{T} \in \mathcal{V}$ sei T in der folgenden Definition der Repräsentant, der nur gerade Zahlen enthält. Wir definieren

$$f[\eta_T](z) := \left(\prod_{i \in V - T} c_i \right) \cdot \frac{\vartheta[\eta_T](z)^2}{\vartheta[\delta](z)^2} \ ,$$

wobei die Konstanten c_i wieder die Konstanten von Satz 3.1(ii) bezeichnen. Zum Beispiel ist $f[\delta](z) = 1$, und für $k \in V$ ist $f[\delta + \eta_k](z) = u(a_k)$.

Aus der folgenden Proposition können wir einen Algorithmus herleiten, der die weiteren Funktionen $f[\eta_T](z)$ für $\bar{T} \in \mathcal{V}$ aus den schon bestimmten rekursiv berechnet.

Proposition 4.7: *Seien $T \subseteq B'$ mit $\#T = g-1$, $k, l \in B' - T$ verschieden. Dann gilt:*

$$\vartheta[\eta_k]'(z)\,\vartheta[\eta_l](z) - \vartheta[\eta_k](z)\,\vartheta[\eta_l]'(z) = \pm \frac{\vartheta[\eta_{T\circ U}]'(0)\,\vartheta[\eta_{T\circ U}+\eta_{\{k,l\}}](0)}{\vartheta[\eta_{T\circ U}+\eta_k](0)\,\vartheta[\eta_{T\circ U}+\eta_l](0)} \cdot \vartheta[0](z)\,\vartheta[\eta_{\{k,l\}}](z) \ .$$

Bemerkung : Wir wenden später nur das Quadrat dieser Gleichung an, so daß das Vorzeichen für unsere Zwecke nicht interessiert.

Beweis : Siehe [Mumford], IIIa, 9.9 mit $c = \infty$. Der Beweis stützt sich auf die Frobeniussche Thetaformel und ist sonst elementar.

□

Satz 4.8: *Sei $\tilde{W} \subseteq V$ mit $\#\tilde{W} \leq g-2$. Sei $W := \tilde{W}$ im Fall $\#\tilde{W}$ gerade, sonst sei $W := \tilde{W} \cup \{2g+2\}$. Dann gilt für $k, l \in V - \tilde{W}$ mit $k > l$*

$$f[\eta_W](z) = \frac{\Big(f[\eta_W+\eta_k]'(z)\,f[\eta_W+\eta_l](z) - f[\eta_W+\eta_k](z)\,f[\eta_W+\eta_l]'(z)\Big)^2}{(a_k-a_l)\,f[\eta_W+\eta_k](z)\,f[\eta_W+\eta_l](z)\,f[\eta_W+\eta_{\{k,l\}}](z)} \ .$$

Beweis : Wir ersetzen z in Proposition 4.7 mit einer Menge $T \subseteq B'$ der Ordnung $g-1$ mit $k, l \notin T$ durch $z + \Omega(\eta_W)_1 + (\eta_W)_2$ und erhalten nach Lemma 4.2(i) und Lemma 2.3 :

$$\vartheta[\eta_W+\eta_k]'(z)\,\vartheta[\eta_W+\eta_l](z) - \vartheta[\eta_W+\eta_k](z)\,\vartheta[\eta_W+\eta_l]'(z) = \pm \frac{\vartheta[\eta_{T\circ U}]'(0)}{\vartheta[\eta_{T\circ U}+\eta_k](0)} \cdot \frac{\vartheta[\eta_{T\circ U}+\eta_{\{k,l\}}](0)}{\vartheta[\eta_{T\circ U}+\eta_l](0)} \cdot \vartheta[\eta_W](z) \cdot \vartheta[\eta_W+\eta_{\{k,l\}}](z) \ .$$

Quadrieren wir diese Gleichung, dann folgt mit

$$c_k \frac{\vartheta[\eta_{T\circ U}]'(0)^2}{\vartheta[\eta_{T\circ U}+\eta_k](0)^2} = -\tfrac{1}{4} e^{4\pi i(\eta_T)_1^t(\eta_k)_2} e^{4\pi i(\eta_k)_1^t(\eta_k)_2} \cdot \prod_{i \in B'-T-\{k\}} (a_k - a_i)$$

nach Lemma 4.4 und

$$c_k \frac{\vartheta[\eta_{T\circ U}+\eta_{\{k,l\}}](0)^2}{\vartheta[\eta_{T\circ U}+\eta_l](0)^2} = e^{4\pi i(\eta_T)_1^t(\eta_k)_2} e^{4\pi i(\eta_l)_1^t(\eta_k)_2} \cdot \prod_{i\in T\cup\{l\}} (a_k - a_i)$$

nach Lemma 4.3 und aus Lemma 4.6

$$\begin{aligned}\Big(\vartheta[\eta_W+\eta_k]'(z)\,\vartheta[\eta_W+\eta_l](z) - \vartheta[\eta_W+\eta_k](z)\,\vartheta[\eta_W+\eta_l]'(z)\Big)^2 \\ = -\tfrac{1}{4} e^{4\pi i(\eta_l)_1^t(\eta_k)_2} \cdot (a_k - a_l) \cdot \vartheta[\eta_W](z)^2 \cdot \vartheta[\eta_W+\eta_{\{k,l\}}](z)^2 \\ = \tfrac{1}{4} \cdot (a_k - a_l) \cdot \vartheta[\eta_W](z)^2 \cdot \vartheta[\eta_W+\eta_{\{k,l\}}](z)^2 \ ,\end{aligned}$$

da nach Definition von η_k und η_l mit $k > l$ folgt $e^{4\pi i(\eta_l)_1^t(\eta_k)_2} = -1$.

Wir dividieren diese Gleichung durch $\vartheta[\delta](z)^4$ und multiplizieren sie mit

$$4 \cdot \left(\prod_{i\in V-T} c_i\right)\left(\prod_{i\in V-T-\{k,l\}} c_i\right) = 4 \cdot \left(\prod_{i\in V-T-\{k\}} c_i\right)\left(\prod_{i\in V-T-\{l\}} c_i\right) .$$

Einfaches Nachrechnen nach Einsetzen der Definitionen für $f[...](z)$ liefert

$$\begin{aligned}\frac{\Big(f[\eta_W+\eta_k]'(z)\,f[\eta_W+\eta_l](z) - f[\eta_W+\eta_k](z)\,f[\eta_W+\eta_l]'(z)\Big)^2}{f[\eta_W+\eta_k](z)\,f[\eta_W+\eta_l](z)} = \\ = (a_k - a_l)\,f[\eta_W](z)\,f[\eta_W+\eta_{\{k,l\}}](z) \ ,\end{aligned}$$

woraus die Behauptung folgt.

□

Die Funktionen $f[\eta_W](z)$ mit $\overline{W} \in \mathcal{V}$ können wir nun folgendermaßen induktiv berechnen: Wir setzen zunächst $f[\delta](z) := 1$, sowie $f[\delta+\eta_k](z) := u(a_k)$ für $k \in V$.

Wir können nun für $r \geq 2$ verschiedene Indizes $k_1, ..., k_r \in V$ $f[\delta+\eta_{k_1}+...+\eta_{k_r}](z)$ mit Hilfe von Satz 4.8 aus den schon berechneten Funktionen

$$f[\delta+\eta_{k_1}+...+\eta_{k_{r-2}}](z) \ ,$$

$$f[\delta+\eta_{k_1}+...+\eta_{k_{r-2}}+\eta_{k_{r-1}}](z) \quad \text{und} \quad f[\delta+\eta_{k_1}+...+\eta_{k_{r-2}}+\eta_{k_r}](z)$$

berechnen. Nach den Notationen von Satz 4.8 ist hier $\eta_W \equiv \delta+\eta_{k_1}+...+\eta_{k_r}$, $k = k_r$ und $l = k_{r-1}$ (oder umgekehrt, falls $k_r < k_{r-1}$ ist). Damit ist

$$\begin{aligned}\eta_W+\eta_k &\equiv \delta+\eta_{k_1}+...+\eta_{k_{r-2}}+\eta_{k_{r-1}} \ , \\ \eta_W+\eta_l &\equiv \delta+\eta_{k_1}+...+\eta_{k_{r-2}}+\eta_{k_r} \ , \\ \eta_W+\eta_k+\eta_l &\equiv \delta+\eta_{k_1}+...+\eta_{k_{r-2}} \ .\end{aligned}$$

Bemerkung : Da die Polstellen von $f[\eta_W](z)$ höchstens entlang Θ liegen können, sind diese Funktionen Polynome in den Ableitungen von $\wp(z)$, obwohl in der Gleichung von Satz 4.8 Nenner auftreten.

Beispiele 4.9: (i) Zunächst möchten wir die Berechnung des Additionstheorems der $\wp$-Funktion im Fall $g = 1$ wiederholen. Es sind $f[\delta](z) = 1$, sowie $f[0](z) = a_2 - \wp(z)$ nach Beispiel 3.7(i). Das Additionstheorem der $\vartheta[\delta]$-Funktion lautet nun

$$\frac{\vartheta[\delta](x+u)\,\vartheta[\delta](x-u)}{\vartheta[\delta](x)^2\,\vartheta[\delta](u)^2}\,\vartheta[0](0)^2\,c_2 = f[0](u) - f[0](x) = \wp(x) - \wp(u)\,,$$

aus welcher mit Satz 4.1 und Beispiel 3.7(i) die bekannte Additionsformel für die $\wp$-Funktion,

$$\begin{aligned}
\wp(x+u) &= \tfrac{1}{2}\wp(x) + \tfrac{1}{2}\wp(u) - (D_\infty^x + D_\infty^u)^2 \log\Big(\wp(x) - \wp(u)\Big) \\
&= \tfrac{1}{2}\wp(x) + \tfrac{1}{2}\wp(u) - \frac{\wp''(x) - \wp''(u)}{\wp(x) - \wp(u)} + \left(\frac{\wp'(x) - \wp'(u)}{\wp(x) - \wp(u)}\right)^2 \\
&= \tfrac{1}{2}\wp(x) + \tfrac{1}{2}\wp(u) - \tfrac{3}{2}\,(\wp(x) + \wp(u)) + \left(\frac{\wp'(x) - \wp'(u)}{\wp(x) - \wp(u)}\right)^2 \\
&= -\wp(x) - \wp(u) + \left(\frac{\wp'(x) - \wp'(u)}{\wp(x) - \wp(u)}\right)^2\,,
\end{aligned}$$

folgt.

(ii) Im nächsten Beispiel möchten wir nun das Additionstheorem der $\wp$-Funktion im Fall $g = 2$ berechnen. Dazu benutzen wir dieselben Bezeichnungen wie in Beispiel 3.7(ii). Im Fall $g = 2$ läßt sich die Funktion $f[0](z)$ aus $f[\delta](z) = 1$,

$$f[\eta_2](z) = \tfrac{1}{8}\big(8a_4^2 + 4a_4 f_1 - f_1^2 + 4f_2 - 8a_4\wp(z) - 4f_1\wp(z) + 12\wp(z)^2 - 8\wp''(z)\big)$$

und

$$f[\eta_4](z) = \tfrac{1}{8}\big(8a_2^2 + 4a_2 f_1 - f_1^2 + 4f_2 - 8a_2\wp(z) - 4f_1\wp(z) + 12\wp(z)^2 - 8\wp''(z)\big)$$

mit einem Computer-Algebra-System schnell berechnen, und zwar erhalten wir

$$\begin{aligned}
f[0](z) = \tfrac{1}{16}\Big(&-32a_2^4 - 32a_2^3a_4 - 16a_2^2a_4^2 - 32a_2^3f_1 - 24a_2^2a_4f_1 - 8a_2a_4^2f_1 - 2a_2^2f_1^2 \\
&+ 2a_4^2f_1^2 + a_2f_1^3 - a_4f_1^3 - 24a_2^2f_2 - 16a_2a_4f_2 - 8a_4^2f_2 - 4a_2f_1f_2 + 4a_4f_1f_2 \\
&- 16a_2f_3 - 16a_4f_3 - 16f_4 - 16a_2^2a_4\wp(z) + 16a_2a_4^2\wp(z) - 8a_2^2f_1\wp(z) \\
&+ 8a_4^2f_1\wp(z) - 6a_2f_1^2\wp(z) + 6a_4f_1^2\wp(z) + 8a_2f_2\wp(z) - 8a_4f_2\wp(z) \\
&+ 24a_2^2\wp(z)^2 - 24a_4^2\wp(z)^2 + 12a_2f_1\wp(z)^2 - 12a_4f_1\wp(z)^2 - 8a_2\wp(z)^3 \\
&+ 8a_4\wp(z)^3 - 16a_2\wp'(z)^2 + 16a_4\wp'(z)^2 - 16a_2^2\wp''(z) + 16a_4^2\wp''(z) \\
&- 8a_2f_1\wp''(z) + 8a_4f_1\wp''(z) + 16a_2\wp(z)\wp''(z) - 16a_4\wp(z)\wp''(z)\Big)
\end{aligned}$$

Zur Berechnung dieses Ausdruck ist es notwendig, die auftretenden Terme der Formen $\wp'(z)\wp'''(z)$, sowie $\wp'''(z)^2$ mit Hilfe der Gleichungen für die Jacobische Varietät, siehe Beispiel 3.7(ii), durch Polynome in $\wp(z)$, $\wp'(z)$, $\wp''(z)$ zu ersetzen.

Damit können wir nun die rechte Seite des Additionstheorems der $\vartheta[\delta]$-Funktion als Polynom in den Ableitungen von $\wp(z)$ berechnen. Wir bekommen folgendes Ergebnis:

$$2 \cdot \frac{\vartheta[\delta](x+u)\,\vartheta[\delta](x-u)}{\vartheta[\delta](x)^2\,\vartheta[\delta](u)^2}\,\vartheta[0](0)^2\,\frac{c_2\,c_4}{a_4-a_2} =$$

$$= \frac{2}{a_4-a_2}\Big(f[0](u) - f[0](x) + f[\eta_2](x)\,f[\eta_4](u) - f[\eta_4](x) f[\eta_2](u)\Big)$$

$$= \big(\wp(u)-\wp(x)\big)^3 + 2\big(\wp'(u)^2 - \wp'(x)^2\big) + 2\big(\wp(x)-\wp(u)\big)\big(\wp''(x)+\wp''(u)\big)\ .$$

Das Additionstheorem der $\wp$-Funktion lautet nach Satz 4.1 nun

$$\wp(x+u) = \tfrac{1}{2}\wp(x) + \tfrac{1}{2}\wp(u) - \big(D_\infty^x + D_\infty^u\big)^2 \log$$

$$\Big(\big(\wp(u)-\wp(x)\big)^3 + 2\big(\wp'(u)^2 - \wp'(x)^2\big) + 2\big(\wp(x)-\wp(u)\big)\big(\wp''(x)+\wp''(u)\big)\Big)\ ,$$

woran wir erkennen, daß die Verzweigungspunkte der Kurve nur symbolisch in die Rechnungen eingehen, auf keinen Fall aber berechnet werden müssen.

□

Das Ergebnis des letzten Beispiels ist überraschend kurz. Wegen der Wichtigkeit dieses Resultats formulieren wir es nochmals als Satz :

Satz : (Additionstheorem für die $\wp$-Funktion im Fall $g = 2$)
Für $x, u \in \mathbb{C}^2$ mit $x, u, x+u \notin \Theta$ gilt

$$\wp(x+u) = \tfrac{1}{2}\wp(x) + \tfrac{1}{2}\wp(u) - \big(D_\infty^x + D_\infty^u\big)^2 \log$$

$$\Big(\big(\wp(u)-\wp(x)\big)^3 + 2\big(\wp'(u)^2 - \wp'(x)^2\big) + 2\big(\wp(x)-\wp(u)\big)\big(\wp''(x)+\wp''(u)\big)\Big)\ .$$

□

Expandiert man allerdings dieses Resultat, indem man die Derivationen symbolisch ausrechnet und auftretende vierte Ableitungen von $\wp$ substituiert, dann füllt das Ergebnis mehr als eine Seite. Wir verzichten daher hier auf eine Ausgabe, da diese, etwa mit Mathematica, innerhalb weniger Minuten aus dem Satz berechnet werden kann.

4.3 : Das Inverse eines Punktes

Die Addition, die wir oben auf der affinen Karte $\mathrm{Jac}(C) - \Theta$ in den Koordinaten $\wp, \wp', ..., \wp^{(2g-1)}$ beschrieben haben, läßt sich durch eine Überdeckung von $\mathrm{Jac}(C)$ mit Karten isomorph zu $\mathrm{Jac}(C) - \Theta$ zu einer Addition auf $\mathrm{Jac}(C)$ erweitern.

Möchten wir aber bei zwei Punkten $P, Q \in \mathrm{Jac}(C) - \Theta$ nur feststellen, ob deren Summe gleich 0 in $\mathrm{Jac}(C)$ ist, dann genügt es, wie wir gleich zeigen werden, nur in den Koordinaten von $\mathrm{Jac}(C) - \Theta$ zu rechnen. Und zwar ist genau dann $P + Q = 0$, wenn $P = -Q$ gilt. Diese Identität können wir testen, wenn wir das Inverse eines Punktes P berechnen können. Hier gilt der folgende einfache Satz:

Satz 4.10: *Sei $z \in (\mathbb{C}^g - \Theta)/\Gamma$. Dann läßt sich das Inverse des Punktes $(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)) \in Jac(C) - \Theta$ folgendermaßen berechnen:*

$$-\left(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)\right) = \left(\wp(z), -\wp'(z), \wp''(z), -\wp'''(z), ..., -\wp^{(2g-1)}(z)\right) .$$

Beweis : Da $\wp$ nach Definition und Satz 3.3 eine gerade Funktion ist, sind auch alle geraden Ableitungen von $\wp$ gerade Funktionen, und alle ungeraden Ableitungen von $\wp$ sind ungerade Funktionen. Daher gilt

$$\begin{aligned} -\left(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)\right) &= \left(\wp(-z), \wp'(-z), ..., \wp^{(2g-1)}(-z)\right) \\ &= \left(\wp(z), -\wp'(z), \wp''(z), -\wp'''(z), ..., -\wp^{(2g-1)}(z)\right) . \end{aligned}$$

□

Kapitel 5 : Beschreibung der n-Torsionspunkte

In diesem Kapitel werden wir für $n \in \mathbb{Z}$ Polynome herleiten, deren Verschwindungsmenge eine Teilmenge der n-Torsionspunkte der Jacobischen Varietät einer hyperelliptischen Kurve C ist. Genauer werden wir g Polynome in den $2g$ Koordinaten, die wir schon im Kapitel 3 zur Beschreibung der affinen Karte $\mathrm{Jac}(C) - \Theta$ benutzt haben, herleiten, welche zusammen mit den g Polynomen, die wir zur Beschreibung von $\mathrm{Jac}(C) - \Theta$ benutzen, die n-Torsionspunkte auf $\mathrm{Jac}(C) - \Theta$ beschreibt. Die so beschriebene Menge der n-Torsionspunkte ist nur in den Fällen $n = -1, 1$ leer, denn 0 ist der einzige 1-Torsionspunkt, er liegt aber nicht in $\mathrm{Jac}(C) - \Theta$.

Für die Fälle $g = 1, 2$ leiten wir die Gleichungen explizit her. Ferner werden wir Hinweise geben, wie man in den Fällen $g \geq 3$ vorzugehen hat.

Aus dem Additionstheorem für die $\wp$-Funktion, Satz 4.1, lassen sich solche Gleichungen erst dann herleiten, wenn wir die gesamte Jacobische Varietät mit Karten isomorph zu $\mathrm{Jac}(C) - \Theta$ überdecken und in diesem Modell rechnen. In diesem Fall startet man mit einem generischen Punkt, summiert diesen n-mal auf und testet anschließend, unter welchen Bedingungen man den Nullpunkt erreicht. Dieses Verfahren wird von Pila in [Pila], Kapitel 3, vorgeschlagen. Wie man leicht sieht, ist der hierzu notwendige Rechenaufwand ungeheuer groß.

Wir werden anders vorgehen und insbesondere die Gleichungen für die n-Torsionspunkte nur in den Koordinaten von $\mathrm{Jac}(C) - \Theta$ schreiben. D.h. ist $z \in (\mathbb{C}^g - \Theta)/\Gamma$ und $P = (\wp(z), ..., \wp^{(2g-1)}(z))$ der zugehörige Punkt in der affinen Varietät $\mathrm{Jac}(C) - \Theta$, dann werden wir Polynome $\psi_{1,n}, ..., \psi_{g,n}$ in $\wp(z), ..., \wp^{(2g-1)}(z)$ mit der Eigenschaft

$$n \cdot z = 0 \Longleftrightarrow n \cdot P = 0 \Longleftrightarrow \psi_{i,n}(\wp(z), ..., \wp^{(2g-1)}(z)) = 0 \text{ für alle } i = 1, ..., g$$

herleiten.

Ist $n \cdot P \neq 0$, aber $n \cdot P \in \Theta$, dann können wir $n \cdot P$ nicht in unseren Koordinaten ausdrücken. Wir werden aber die Polynome $\psi_{i,n}$ so konstruieren, daß das Polynom $\psi_{1,n}$ genau die $P \in \mathrm{Jac}(C) - \Theta$ mit $n \cdot P \in \Theta$ beschreibt, d.h. daß gilt

$$n \cdot z \in \Theta \Longleftrightarrow n \cdot P \in \Theta \Longleftrightarrow \psi_{1,n}(\wp(z), ..., \wp^{(2g-1)}(z)) = 0 \, .$$

Betrachten wir nochmals die Jacobische Varietät $\mathrm{Jac}(C)$ als komplexen Torus $\mathbb{C}^g/\Gamma$ mit $\Gamma = \Omega\mathbb{Z}^g + \mathbb{Z}^g$, dann sind genau die n^{2g} Punkte

$$\frac{1}{n}(\Omega a + b) \mod \Gamma \quad \text{mit } a, b \in \{0, 1, ..., n-1\}^g$$

die n-Torsionspunkte von $\mathbb{C}^g/\Gamma$. Diese Überlegung führt aber nur im Fall $g = 1$ zu expliziten Gleichungen, indem man etwa

$$\psi_n(z)^2 := n^2 \cdot \prod_{\substack{a,b \in \{0,1,\ldots,n-1\} \\ (a,b) \neq (0,0)}} \left(\wp(z) - \wp(\tfrac{1}{n}(\Omega a + b)) \right)$$

ansetzt, was zu Polynomen P_n in der Unbestimmten $\wp(z)$ führt, die die Menge der n-Torsionspunkte beschreiben. Aus dem Additionstheorem für die $\vartheta[\delta]$-Funktion leitet man Rekursionsformeln für die ψ_n her. Dieser Ansatz wird in [Weber], §58 beschrieben.

Unser Ansatz stützt sich auf Überlegungen, wie man den Nullpunkt der Divisorklassengruppe $\mathrm{Div}_0(C)/H$, die wir im 1. Kapitel beschrieben haben, von anderen Punkten unterscheiden kann. Anders ausgedrückt fragen wir uns, wie ein generischer Punkt spezialisiert werden kann, so daß er gleich dem Nullpunkt wird.

Ausgehend von $D = \sum_{i=1}^{g} P_i - g \cdot \infty \bmod H$ mit Punkten $P_i \neq \infty$ von C mit $P_i \neq P_j'$ für $i \neq j$ betrachten wir den Grenzwert der $P_i \longrightarrow \infty$ von D. Führt man diesen Grenzwertprozeß schrittweise durch, dann durchläuft D folgende Stufen:

$$\begin{array}{lcll}
\left[\sum_{i=1}^{g} P_i - g \cdot \infty\right] & \in & \mathrm{Div}_0(C)/H & = \left\{ \left[\sum_{i=1}^{r} P_i - r \cdot \infty\right] \,\middle|\, P_i \neq \infty, P_i \neq P_j', r \leq g \right\} \\
 & & \| & \\
\lim_{P_g \to \infty} \downarrow & & \cup & \\
\left[\sum_{i=1}^{g-1} P_i - g \cdot \infty\right] & \in & \Theta_{g-1} = \Theta & = \left\{ \left[\sum_{i=1}^{r} P_i - r \cdot \infty\right] \,\middle|\, \ldots, \ldots, r \leq g-1 \right\} \\
\lim_{P_{g-1} \to \infty} \downarrow & & \cup & \\
\left[\sum_{i=1}^{g-2} P_i - g \cdot \infty\right] & \in & \Theta_{g-2} & = \left\{ \left[\sum_{i=1}^{r} P_i - r \cdot \infty\right] \,\middle|\, \ldots, \ldots, r \leq g-2 \right\} \\
\lim_{P_{g-2} \to \infty} \downarrow & & \cup & \\
\vdots & & \vdots & \qquad\qquad \vdots \\
\lim_{P_1 \to \infty} \downarrow & & \cup & \\
[0] & \in & \Theta_0 = \{[0]\} & = \left\{ \left[\sum_{i=1}^{r} P_i - r \cdot \infty\right] \,\middle|\, \ldots, \ldots, r \leq 0 \right\}
\end{array}$$

Unser nächstes Ziel ist nun die Beschreibung der Teilmengen Θ_k, $k = 0, 1, 2, \ldots, g$, als Verschwindungsmengen gewisser Polynome in den Thetafunktionen. Nach Satz

3.1(i) wissen wir schon, daß die Teilmenge $\Theta_{g-1} = \Theta$ genau die Verschwindungsmenge der $\vartheta[\delta]$-Funktion ist.

Zur Beschreibung der weiteren Θ_k bedienen wir uns des (u,v,w)-Modells, das wir ebenfalls im 1. Kapitel beschrieben haben, da dieses nach Satz 3.1(ii) eine Verbindung zwischen den Divisorklassen und den Thetafunktionen herstellt. Und zwar ist einer Divisorklasse $D = \left[\sum_{i=1}^{g} P_i - g \cdot \infty\right]$ mit $P_i = (x_i, y_i) \neq \infty$ und $P_i \neq P_j'$ für $i \neq j$ einerseits das Polynom

$$u^D(t) = \prod_{i=1}^{g}(t - x_i) = t^g + u_1 t^{g-1} + ... + u_g \ ,$$

andererseits der Punkt $z = \overline{\varphi}(D) = \sum_{i=1}^{g} \int_{\infty}^{P_i} \omega \bmod \Gamma$ in dem Torus $\mathbb{C}^g/\Gamma$ zugeordnet. Nach Satz 3.1(ii) gilt mit einem $k \in B'$

$$c_k \, \frac{\vartheta[\delta + \eta_k](z)^2}{\vartheta[\delta](z)^2} = u^D(a_k) \ ,$$

was für $z \in \Theta$ nicht definiert ist. Multiplizieren wir diese Gleichung aber mit $\vartheta[\delta](z)^2$, dann lassen sich beide Seiten zu holomorphen Funktionen auf $\mathbb{C}^g$ fortsetzen:

$$c_k \vartheta[\delta + \eta_k](z)^2 = \vartheta[\delta](z)^2 \, a_k^g + (u_1 \vartheta[\delta](z)^2) a_k^{g-1} + ... + (u_g \, \vartheta[\delta](z)^2) \ ,$$

wobei die Koeffizienten $u_1, ..., u_g$ ebenfalls Funktionen $u_1(z), ..., u_g(z)$ von z sind.

Setzen wir $\tilde{u}_i(z) := u_i(z) \, \vartheta[\delta](z)^2$ für $i = 1, ..., g$ und $\tilde{u}_0(z) := \vartheta[\delta](z)^2$, dann sind die $\tilde{u}_i$ zu holomorphen Funktionen auf $\mathbb{C}^g$ fortsetzbar, insbesondere lassen sie sich durch ϑ-Funktionen ausdrücken, genauer sind sie Linearkombinationen der $\vartheta[\delta + \eta_k](z)^2$ mit $k \in V = \{2, 4, ..., 2g\}$:

Lemma 5.1: *Für $i = 1, ..., g$ gilt*

$$\tilde{u}_i = \frac{\begin{vmatrix} 1 & a_2 & ... & a_2^{g-i-1} & (c_2\vartheta[\delta+\eta_2](z)^2 - \tilde{u}_0 a_2^g) & a_2^{g-i+1} & ... & a_2^{g-1} \\ 1 & a_4 & ... & a_4^{g-i-1} & (c_4\vartheta[\delta+\eta_4](z)^2 - \tilde{u}_0 a_4^g) & a_4^{g-i+1} & ... & a_4^{g-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{2g} & ... & a_{2g}^{g-i-1} & (c_{2g}\vartheta[\delta+\eta_{2g}](z)^2 - \tilde{u}_0 a_{2g}^g) & a_{2g}^{g-i+1} & ... & a_{2g}^{g-1} \end{vmatrix}}{\prod_{i,k \in V, i<k} (a_k - a_i)} \ .$$

Beweis : Die g Gleichungen

$$c_k\,\vartheta[\delta+\eta_k](z)^2 = \tilde{u}_0(z)\,a_k^g + \tilde{u}_1(z)a_k^{g-1} + ... + \tilde{u}_g(z)$$

für $k \in V = \{2,4,...,2g\}$ bilden ein lineares Gleichungssystem in den Unbestimmten $\tilde{u}_1(z),...,\tilde{u}_g(z)$, nämlich

$$\begin{pmatrix} 1 & a_2 & a_2^2 & ... & a_2^{g-1} \\ 1 & a_4 & a_4^2 & ... & a_4^{g-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{2g} & a_{2g}^2 & ... & a_{2g}^{g-1} \end{pmatrix} \begin{pmatrix} \tilde{u}_g \\ \tilde{u}_{g-1} \\ \vdots \\ \tilde{u}_1 \end{pmatrix} = \begin{pmatrix} c_2\,\vartheta[\delta+\eta_2](z)^2 - \tilde{u}_0 a_2^g \\ c_4\,\vartheta[\delta+\eta_4](z)^2 - \tilde{u}_0 a_4^g \\ \vdots \\ c_{2g}\,\vartheta[\delta+\eta_{2g}](z)^2 - \tilde{u}_0 a_{2g}^g \end{pmatrix},$$

welches wir mit der Cramerschen Regel lösen. Dabei benutzen wir, daß die Determinante der Matrix auf der linken Seite die Vandermondsche Determinante ist, d.h. gleich

$$\prod_{i,k\in V, i<k} (a_k - a_i)\ ,$$

also insbesondere ungleich 0 ist.

□

Im Folgenden seien $\tilde{u}_1,...,\tilde{u}_g$ die in diesem Lemma berechneten Linearkombinationen der $\vartheta[\delta+\eta_k]$-Funktionen mit $k \in V$.

Satz 5.2: *Seien $n \in \{0,1,...,g\}$ und $D \in \Theta_{g-n}$. Sei $z \in \mathbb{C}^g$ mit $z \equiv \overline{\varphi}(D)$ mod Γ. Dann gelten mit $\tilde{u}_{-1}(z) := 0$:*
(i) $\tilde{u}_0(z) = \tilde{u}_1(z) = ... = \tilde{u}_{n-1}(z) = 0$.
(ii) Genau dann ist $D \in \Theta_{g-n-1}$, wenn $\tilde{u}_n(z) = 0$ ist.
(iii) Ist $D \notin \Theta_{g-n-1}$, und ist $\sum_{j=1}^{g-n} P_j - (g-n)\cdot\infty$ der kanonische Repräsentant von D mit Punkten $P_j = (x_j, y_j) \neq \infty$ von C mit $P_j \neq P_i'$ für $i \neq j$. Dann gilt für $k \in B'$

$$u^D(a_k) := \prod_{j=1}^{g-n}(a_k - x_j) = c_k \frac{\vartheta[\delta+\eta_k](z)^2}{\tilde{u}_n(z)}\ .$$

(Die Konstanten c_k für $k \in B'$ wurden in Satz 3.1(ii) definiert.)

Beweis : Vollständige Induktion nach $n \in \{0,1,...,g\}$:
Sei $n = 0$. Dann besagt (i) nichts, (ii),(iii) sind genau die Aussagen von Satz 3.1(ii).
Sei $1 \leq n \leq g$ und die Aussage für kleinere n schon bewiesen. Sei $D \in \Theta_{g-n}$. Wegen $\Theta_{g-n} \subset \Theta_{g-(n-1)}$ folgt nach Induktion (i) und (ii)

$$\tilde{u}_0(z) = \tilde{u}_1(z) = ... = \tilde{u}_{n-1}(z) = 0\ .$$

Sei nun $D \notin \Theta_{g-n-1}$ mit dem oben erwähnten kanonischen Repräsentanten. Wir nehmen einen Punkt $P = (x, y) \neq \infty$ von C mit $P \neq P_j'$ und setzen

$$\tilde{D} := \left[\sum_{j=1}^{g-n} P_j + P - (g-n+1) \cdot \infty \right] .$$

Zu $\tilde{D}$ gehöre $\tilde{z} \in \mathbb{C}^g$ mit $\tilde{z} \equiv \overline{\varphi}(\tilde{D}) \bmod \Gamma$, wobei wir den Repräsentanten so wählen, daß $\lim\limits_{P \to \infty} \tilde{z} = z$ gilt. Da $\tilde{D} \in \Theta_{g-n+1} - \Theta_{g-n}$ ist, gilt nach Induktion

$$u^{\tilde{D}}(a_k) = c_k \, \frac{\vartheta[\delta + \eta_k](\tilde{z})^2}{\tilde{u}_{n-1}(\tilde{z})} = u^D(a_k) \cdot (a_k - x) ,$$

bzw. nach einer weiter oben hergeleiteten Gleichung

$$c_k \, \vartheta[\delta+\eta_k](\tilde{z})^2 = \tilde{u}_{n-1} a_k^{g-(n-1)} + \tilde{u}_n(\tilde{z}) a_k^{g-n} + \ldots + \tilde{u}_g(\tilde{z}) = u^D(a_k) \cdot \tilde{u}_{n-1}(\tilde{z})(a_k - x) .$$

Betrachten wir diese Gleichung unter dem Grenzprozeß $P \to \infty$, dann folgt

$$c_k \, \vartheta[\delta + \eta_k](z)^2 = \tilde{u}_n(z) a_k^{g-n} + \ldots + \tilde{u}_g(z) = u^D(a_k) \cdot \lim_{P \to \infty} \left(\tilde{u}_{n-1}(\tilde{z}) \cdot (a_k - x) \right) .$$

Der Grenzwert auf der rechten Seite ist wegen $\lim_{P \to \infty} x = \infty$ unabhängig von a_k, was man auch durch Anwendung des Satzes von l'Hospital erkennt. Betrachten wir daher diese Gleichung als Polynom in der Unbestimmten a_k vom Grad $g - n$, dann ist sie für alle $k \in B'$ richtig, so daß wir durch Koeffizientenvergleich

$$\tilde{u}_n(z) = \lim_{P \to \infty} \left(\tilde{u}_{n-1}(\tilde{z}) \cdot (a_k - x) \right)$$

erhalten. Wählen wir k so, daß $\vartheta[\delta + \eta_k](z) \neq 0$ ist, dann folgt auch $\tilde{u}_n(z) \neq 0$. Einfaches Umformen der obigen Gleichung liefert

$$u^D(a_k) = a_k^{g-n} + \ldots + \frac{\tilde{u}_g(z)}{\tilde{u}_n(z)} = c_k \, \frac{\vartheta[\delta + \eta_k](z)^2}{\tilde{u}_n(z)} ,$$

womit (iii) und eine Richtung von (ii) bewiesen sind.

Nun sei $D \in \Theta_{g-n-1}$. Wir wählen Punkte $Q_1, \ldots, Q_r \neq \infty$ von C, so daß

$$\tilde{D} := D + \left[\sum_{j=1}^{r} Q_j - r \cdot \infty \right] \in \Theta_{g-n} - \Theta_{g-n-1}$$

mit $\lim\limits_{Q_1 \to \infty} \ldots \lim\limits_{Q_r \to \infty} \tilde{D} = D$ ist. Gleichung (iii) lautet mit $\tilde{D}$ anstelle von D

$$u^{\tilde{D}}(a_k) = \prod_{j=1}^{g-n} (a_k - x_j) = c_k \, \frac{\vartheta[\delta + \eta_k](\tilde{z})^2}{\tilde{u}_n(\tilde{z})} .$$

Wenden wir einen der Grenzprozesse, etwa $\lim_{Q_r \to \infty}$, auf diese Gleichung an, dann wird der mittlere Term unendlich, so daß jedenfalls $\lim_{Q_r \to \infty} \tilde{u}_n(\tilde{z}) = 0$ ist. Daher folgt $\tilde{u}_n(z) = \lim_{Q_1 \to \infty} ... \lim_{Q_r \to \infty} \tilde{u}_n(\tilde{z}) = 0$, womit auch die zweite Richtung von (ii) bewiesen ist.

□

Wir kommen nun zur Definition der ψ-Polynome. Die Basis ist der vorhergehende Satz, denn nach ihm gilt für ein $z \in \mathrm{Jac}(C) - \Theta$ und ein $n \in \mathbb{Z}$: $n \cdot z = 0 \iff \tilde{u}_0(nz) = \tilde{u}_1(nz) = ... = \tilde{u}_{g-1}(nz) = 0$.

Satz 5.3: *Setzen wir für $n \in \mathbb{Z}$*

$$\psi_{1,n}(z) := c_1(n) \cdot \frac{\vartheta[\delta](nz)}{\vartheta[\delta](z)^{n^2}} ,$$

$$\psi_{i,n} := c_i(n) \cdot \frac{\tilde{u}_{i-1}(nz)}{\vartheta[\delta](z)^{2n^2}} \text{ für } i = 2, ..., g$$

mit von z unabhängigen Konstanten $c_i(n) \neq 0$, $i = 1, ..., g$, dann gilt:
(i) Die $\psi_{i,n}(z)$, $i = 1, ..., g$, sind meromorphe Funktionen $(\mathbb{C}^g - \Theta)/\Gamma \longrightarrow \mathbb{C}$.
(ii) Für $z \in (\mathbb{C}^g - \Theta)/\Gamma$ gilt : Genau dann ist $n \cdot z = 0$, wenn $\psi_{1,n}(z) = ... = \psi_{g,n}(z) = 0$ ist. Anders ausgedrückt bedeutet dies, daß die Verschwindungsmenge von $\psi_{1,n}, ..., \psi_{g,n}$ genau die n-Torsionspunkte von $Jac(C) - \Theta$ beschreibt.

Beweis : (i) Zu zeigen ist die Periodizität der $\psi_{i,n}$ bezüglich des Gitters $\Gamma = \Omega\mathbb{Z}^g + \mathbb{Z}^g$. Seien $p, q \in \mathbb{Z}^g$. Dann folgt aus Lemma 2.1

$$\psi_{1,n}(z + \Omega p + q) = c_1(n) \cdot \frac{\vartheta[\delta](nz + n\Omega p + nq)}{\vartheta[\delta](z + \Omega p + q)^{n^2}}$$

$$= c_1(n) \cdot e^{2\pi i (n^2 - n)(p^t(\delta)_2 - (\delta)_1^t q)} \frac{\vartheta[\delta](nz)}{\vartheta[\delta](z)^{n^2}}$$

$$= c_1(n) \frac{\vartheta[\delta](nz)}{\vartheta[\delta](z)^{n^2}} = \psi_{1,n}(z),$$

da $n^2 - n$ für alle $n \in \mathbb{Z}$ gerade ist, und da $p^t(\delta_2) - (\delta)_1^t q \in \frac{1}{2}\mathbb{Z}^g$ ist.

Die Periodizität der übrigen $\psi_{i,n}$, $i = 2, ..., g$, ist klar, da $\tilde{u}_{i-1}(z)$ nach Lemma 5.1 Linearkombination von Quadraten von Thetafunktionen ist.

(ii) Die Äquivalenz folgt direkt aus Satz 5.2.

□

Die hier vorgestellten Funktionen $\psi_{i,n}$, die nach Satz 3.5 Polynome in den Ableitungen von $\wp(z)$ sind, sind der erste Ansatz zur Beschreibung der n-Torsionspunkte

in $\mathrm{Jac}(C) - \Theta$. Aus diesen läßt sich durch geeignete Wahl der Konstanten $c_i(n)$, sowie durch einfache Linearkombinationen dieser Funktionen ein Polynomsystem in den Ableitungen von $\wp(z)$ konstruieren, welches leicht mittels Rekursionsformeln berechnet werden kann. Hierbei muß berücksichtigt werden, daß die resultierenden Polynome nur noch Ausdrücke in den Koeffizienten der Kurvengleichung, sowie in den Ableitungen von $\wp(z)$ sind. Exemplarisch werden wir diese Konstruktion in den Fällen $g = 1, 2$ behandeln.

5.1 : Explizite Beschreibung der n-Torsionspunkte im Fall $g = 1$

Wir wählen im Fall $g = 1$ wieder die in Beispiel 3.7(i) behandelte Kurvengleichung

$$C : Y^2 = X^3 + A\,X + B\ .$$

In diesem Fall setzen wir für $n \in \mathbb{Z}$

$$\psi_n(z) := \psi_{1,n}(z) = c_1(n)\frac{\vartheta[\delta](nz)}{\vartheta[\delta](z)^{n^2}}\ .$$

Aus dem Additionstheorem der $\vartheta[\delta]$-Funktion (Beispiel 4.9(i)),

$$\frac{\vartheta[\delta](x+u)\,\vartheta[\delta](x-u)}{\vartheta[\delta](x)^2\,\vartheta[\delta](u)^2}\,\vartheta[0](0)^2\,c_2 = \wp(x) - \wp(u)\ ,$$

bekommen wir mit $m, n \in \mathbb{Z}$, $z \in \mathbb{C}/\Gamma$ mit $z, x := mz, u := nz \neq 0$ in $\mathbb{C}/\Gamma$

$$\frac{\psi_{m+n}(z)\,\psi_{m-n}(z)}{\psi_m(z)^2\,\psi_n(z)^2} \cdot \frac{c_1(m)^2\,c_1(n)^2}{c_1(m+n)\,c_1(m-n)}\,\vartheta[0](0)^2\,c_2 = \wp(mz) - \wp(nz)\ .$$

Wir definieren $d := -2\vartheta[\delta]'(0)$, was ungleich 0 nach Lemma 4.4 mit $T = \emptyset$ und $k = 2$ ist, und setzen

$$c_1(n) := d^{n^2-1} \qquad \text{für } n \in \mathbb{Z}\ .$$

Lemma 5.4: *Für $m, n \in \mathbb{Z}$ gilt*

$$\frac{c_1(m)^2\,c_1(n)^2}{c_1(m+n)\,c_1(m-n)}\,\vartheta[0](0)^2\,c_2 = \frac{\vartheta[0](0)^2\,c_2}{d^2} = -1\ .$$

Beweis : Wir berechnen

$$\begin{aligned}\frac{c_1(m)^2\,c_1(n)^2}{c_1(m+n)\,c_1(m-n)}\,\vartheta[0](0)^2\,c_2 &= \frac{d^{2m^2-2}\,d^{2n^2-2}}{d^{(m+n)^2-1}\,d^{(m-n)^2-1}}\,\vartheta[0](0)^2\,c_2 \\ &= \frac{\vartheta[0](0)^2\,c_2}{d^2} = \frac{1}{4c_2}\,\frac{\vartheta[0](0)^2}{\vartheta[\delta]'(0)^2}\,c_2^2 = -1\end{aligned}$$

nach Lemma 4.4 mit $T = \emptyset$, $k = 2$, und nach Lemma 4.6 mit $k = 2$.

□

Wir erhalten somit folgende erste Version einer Rekursionsformel

Proposition 5.5: *Für $m,n \in \mathbb{Z}$, $z \in \mathbb{C}/\Gamma$ mit $z, mz, nz \neq 0$ in $\mathbb{C}/\Gamma$ gilt*

$$\psi_{m+n}(z)\,\psi_{m-n}(z) = (\wp(nz) - \wp(mz))\;\psi_m(z)^2\;\psi_n(z)^2 \;.$$

Korollar 5.6: *Für $m \in \mathbb{Z}$, $z \in \mathbb{C}/\Gamma$ mit $z, mz \neq 0$ in $\mathbb{C}/\Gamma$ gilt*

$$\wp(mz) = \wp(z) - \frac{\psi_{m+1}(z)\,\psi_{m-1}(z)}{\psi_m(z)^2} \;.$$

Beweis : Mit $\psi_1(z) = 1$ folgt die Behauptung aus Proposition 5.5, indem wir dort $n = 1$ setzen.

□

Unser nächstes Ziel ist, die $\psi_n(z)$ als Polynome in den Ableitungen von $\wp(z)$ zu schreiben. Wir erhalten diese Ausdrücke aus der Rekursionsformel, wenn wir geeignete Anfangswerte berechnen.

Satz 5.7: (*i*) *Für $n \in \mathbb{Z}$ gilt* $\psi_{-n}(z) = -\psi_n(z)$.

(*ii*) $\psi_0(z) = 0$

(*iii*) $\psi_1(z) = 1$

(*iv*) $\psi_2(z) = 2\wp'(z)$

(*v*) $\psi_3(z) = 3\wp(z)^4 + 6A\wp(z)^2 + 12B\wp(z) - A^2$

(*vi*) $\psi_4(z) = 4\wp'[z]\Big(\wp[z]^6 + 5A\wp(z)^4 + 20B\wp(z)^3 - 5A^2\wp(z)^2 - 4AB\wp(z) - 8B^2 - A^3\Big)$

(*vii*) $\psi_{2n+1}(z) = \psi_{n+2}(z)\,\psi_n(z)^3 - \psi_{n+1}(z)^3\,\psi_{n-1}(z)$

(*viii*) $\psi_{2n}(z) = \psi_n(z)\Big(\psi_{n+2}(z)\,\psi_{n-1}(z)^2 - \psi_{n-2}(z)\psi_{n+1}(z)^2\Big)/\psi_2(z)$

Beweis : (i) - (iii) folgen direkt aus der Definition von $\psi_n(z)$.
(iv) Wir wenden den Grenzprozeß $u \to z$ auf das Additionstheorem der $\vartheta[\delta]$-Funktion (Beispiel 4.9(i))

$$\frac{\vartheta[\delta](z+u)\,\vartheta[\delta](z-u)}{\vartheta[\delta](z)^2\,\vartheta[\delta](u)^2}\,\vartheta[0](0)^2\,c_2 = \wp(z) - \wp(u)$$

an und bekommen wegen $\vartheta[\delta](0) = 0$ nach l'Hospital

$$\frac{\vartheta[\delta](2z)}{\vartheta[\delta](z)^4}\ \vartheta[0](0)^2\ c_2\ \vartheta[\delta]'(0) = \wp'(z)\ .$$

Wegen $\dfrac{\vartheta[0](0)^2\ c_2\ \vartheta[\delta]'(0)}{c_1(2)} = \dfrac{\vartheta[0](0)^2\ c_2}{d^2}\ \dfrac{\vartheta[\delta]'(0)}{d} = \dfrac{1}{2}$ nach Lemma 5.4 folgt

$$\psi_2(z) = 2\wp'(z)\ .$$

(v) Nach Proposition 5.5 ist $\psi_3(z) = (\wp(z) - \wp(2z))\psi_2(z)^2$. Aus dem Additionstheorem für die $\wp$-Funktion (Beispiel 4.9(i)),

$$\wp(z+u) = -\wp(z) - \wp(u) + \left(\frac{\wp'(z) - \wp'(u)}{\wp(z) - \wp(u)}\right)^2\ ,$$

berechnet man durch Grenzwertbildung $u \to z$

$$\wp(2z) = -2\wp(z) + \left(\frac{\wp''(z)}{\wp'(z)}\right)^2\ .$$

Eingesetzt ergibt dies mit $\wp''(z) = \frac{1}{2}(3\wp(z)^2 + A)$, sowie $\wp'(z)^2 = \wp(z)^3 + A\wp(z) + B$ die Behauptung.

(vi) Nach Proposition 5.5 ist $\psi_4(z)\ \psi_2(z) = (\wp(z) - \wp(3z))\psi_3(z)^2$. Setzen wir im Additionstheorem für die $\wp$-Funktion,

$$\wp(x+u) = -\wp(x) - \wp(u) + \left(\frac{\wp'(x) - \wp'(u)}{\wp(x) - \wp(u)}\right)^2\ ,$$

$x := 2z$ und $u := z$, dann bekommen wir $\wp(3z)$. Setzen wir dies in die Gleichung

$$\begin{aligned}\psi_4(z) &= \frac{(\wp(z) - \wp(3z))\psi_3(z)^2}{\psi_2(z)} = \frac{(\wp(z) - \wp(3z))\psi_3(z)^2}{2\wp'(z)} \\ &= \frac{(\wp(z) - \wp(3z))\psi_3(z)^2\wp'(z)}{2\wp'(z)^2}\end{aligned}$$

ein und ersetzen $\wp'(z)^2 = \wp(z)^3 + A\wp(z) + B$, dann bekommen wir das Ergebnis.

(vii) und (viii) In der Gleichung von Proposition 5.5 ersetzen wir $\wp(mz)$ und $\wp(nz)$ durch den entsprechenden Ausdruck aus Korollar 5.6. Damit bekommen wir

$$\psi_{m+n}(z)\ \psi_{m-n}(z) = \psi_{m+1}(z)\ \psi_{m-1}(z)\ \psi_n(z)^2 - \psi_{n+1}(z)\ \psi_{n-1}(z)\ \psi_m(z)^2\ .$$

Ersetzen wir in dieser Gleichung m durch $n+1$, dann folgt (vii). Ersetzen wir m durch $k+1$ und n durch $k-1$, dann folgt (viii).

□

5.2 : Explizite Beschreibung der n-Torsionspunkte im Fall $g = 2$

In dem Fall $g = 2$ sei

$$C : Y^2 = X^5 + f_0\, X^4 + f_1\, X^3 + f_2\, X^2 + f_3\, X + f_4$$

wieder die Kurvengleichung, die wir schon in Beispiel 3.7(ii) behandelt haben. Wir setzen für $n \in \mathbb{Z}$

$$\psi_n(z) := \psi_{1,n}(z) = c_1(n)\frac{\vartheta[\delta](nz)}{\vartheta[\delta](z)^{n^2}} ,$$

sowie

$$\tilde{\chi}_n(z) := \psi_{2,n}(z) = c_2(n)\frac{\tilde{u}_1(nz)}{\vartheta[\delta](z)^{2n^2}} .$$

Nach Beispiel 3.7(ii) ist

$$\frac{\tilde{u}_1(nz)}{\vartheta[\delta](z)^{2n^2}} = u_1(nz)\frac{\vartheta[\delta](nz)^2}{\vartheta[\delta](z)^{2n^2}} = \left(\frac{f_0}{2} - \wp(nz)\right)\psi_n(z)^2 .$$

Aus dieser Gleichung lesen wir ab, daß für $z \in (\mathbb{C}^2 - \Theta)/\Gamma$ genau dann $\psi_n(z) = 0$ und $\tilde{\chi}_n(z) = 0$ ist, wenn $\psi_n(z) = 0$ und $\wp(nz)\psi_n(z)^2 = 0$ ist. Daher verändern wir $\tilde{\chi}_n$ zu

$$\chi_n(z) := \wp(nz)\psi_n(z)^2 .$$

Aus dem Additionstheorem der $\vartheta[\delta]$-Funktion (Beispiel 4.9(ii)),

$$2 \cdot \frac{\vartheta[\delta](x+u)\,\vartheta[\delta](x-u)}{\vartheta[\delta](x)^2\,\vartheta[\delta](u)^2}\,\vartheta[0](0)^2\,\frac{c_2\,c_4}{a_4 - a_2} =$$

$$= \big(\wp(u) - \wp(x)\big)^3 + 2\big(\wp'(u)^2 - \wp'(x)^2\big) + 2\big(\wp(x) - \wp(u)\big)\big(\wp''(x) + \wp''(u)\big) ,$$

bekommen wir mit $m, n \in \mathbb{Z}$, $z \in \mathbb{C}^2/\Gamma$ mit $z, x := mz, u := nz \notin \Theta$

$$\frac{\psi_{m+n}(z)\,\psi_{m-n}(z)}{\psi_m(z)^2\,\psi_n(z)^2} \cdot \frac{c_1(m)^2\,c_1(n)^2}{c_1(m+n)\,c_1(m-n)}\,\vartheta[0](0)^2\,\frac{c_2\,c_4}{a_4 - a_2} =$$

$$= \big(\wp(nz) - \wp(mz)\big)^3 + 2\big(\wp'(nz)^2 - \wp'(mz)^2\big) + 2\big(\wp(mz) - \wp(nz)\big)\big(\wp''(mz) + \wp''(nz)\big) .$$

Wir definieren $d := -2\vartheta[\delta]'''(0)$ und setzen $d_1 := \dfrac{\vartheta[0](0)^2\,c_2\,c_4}{(a_4 - a_2)d^2}$, sowie

$$c_1(n) := d^{n^2-1} \qquad \text{für } n \in \mathbb{Z} .$$

Daß $c_1(n) \neq 0$ ist, werden wir später im Beweis von Satz 5.11(iv) beweisen. Es gilt wieder

Lemma 5.8: *Für $m, n \in \mathbb{Z}$ gilt*

$$\frac{c_1(m)^2\, c_1(n)^2}{c_1(m+n)\, c_1(m-n)}\, \vartheta[0](0)^2\, \frac{c_2\, c_4}{a_4 - a_2} = \frac{\vartheta[0](0)^2\, c_2\, c_4}{(a_4 - a_2)d^2} = d_1 \ .$$

Beweis : Analog zum 1. Teil des Beweises von Lemma 5.4.

□

Es gilt damit folgende erste Version einer Rekursionsformel

Proposition 5.9: *Für $m, n \in \mathbb{Z}$, $z \in \mathbb{C}/\Gamma$ mit $z, mz, nz \neq 0$ in $\mathbb{C}/\Gamma$ gilt*

$$\psi_{m+n}(z)\, \psi_{m-n}(z)\, d_1 = \psi_m(z)^2\, \psi_n(z)^2 \cdot$$

$$\Big(\big(\wp(nz) - \wp(mz)\big)^3 + 2\big(\wp'(nz)^2 - \wp'(mz)^2\big) + 2\big(\wp(mz) - \wp(nz)\big)\big(\wp''(mz) + \wp''(nz)\big) \Big) \ .$$

Sei für $x, u, x+u \in (\mathbb{C}^2 - \Theta)/\Gamma$

$$\wp(x+u) = F_{add}\big(\wp(x), \wp(u), \wp'(x), \wp'(u), \wp''(x), \wp''(u), \wp'''(x), \wp'''(u)\big)$$

mit einer rationalen Funktion F_{add} das Additionstheorem von $\wp$ nach Beispiel 4.9(ii). Dann erfüllen die χ_n folgende Rekursionsformel :

Proposition 5.10: *Für $m, n \in \mathbb{Z}$, $z \in \mathbb{C}^2/\Gamma$ mit $z, mz, nz \notin \Theta$ gilt*

$$\chi_{m+n}(z) = F_{add}\big(\wp(mz), \wp(nz), ..., \wp'''(mz), \wp'''(nz)\big) \cdot \psi_{m+n}(z)^2 \ .$$

Beweis : Folgt direkt aus der Definition von χ_n.

□

Mit diesen Vorbereitungen können wir nun sowohl die $\psi_n(z)$, als auch die $\chi_n(z)$ als Polynome in den Ableitungen von $\wp(z)$ schreiben. Wie im Fall $g = 1$ geben wir zunächst geeignete Anfangswerte und anschließend Rekursionsformeln an.

Satz 5.11: (*i*) *Für* $n \in \mathbb{Z}$ *gilt* $\psi_{-n}(z) = -\psi_n(z)$, $\chi_{-n}(z) = \chi_n(z)$.

(*ii*) $\psi_0(z) = 0$

$\chi_0(z) = 0$

(*iii*) $\psi_1(z) = 1$

$\chi_1(z) = \wp(z)$

(*iv*) $\psi_2(z) = \frac{1}{d_1}\Big(3\wp'(z)^3 + \wp''(z)\wp^{(3)}(z) - \wp'(z)\wp^{(4)}(z)\Big)$

$$\begin{aligned}\chi_2(z) = \tfrac{1}{d_1^2}\Big(&-27\wp'(z)^4\wp''(z)^2 + 27\wp'(z)^5\wp^{(3)}(z) + 18\wp'(z)\wp''(z)^3\wp^{(3)}(z)\\ &- 9\wp'(z)^2\wp''(z)\wp^{(3)}(z)^2 - \wp^{(3)}(z)^4 - 18\wp'(z)^2\wp''(z)^2\wp^{(4)}(z)\\ &- 3\wp'(z)^3\wp^{(3)}(z)\wp^{(4)}(z) + 2\wp''(z)\wp^{(3)}(z)^2\wp^{(4)}(z)\\ &- 2\wp'(z)\wp^{(3)}(z)\wp^{(4)}(z)^2 + 15\wp'(z)^3\wp''(z)\wp^{(5)}(z)\\ &- \wp''(z)^2\wp^{(3)}(z)\wp^{(5)}(z) + 2\wp'(z)\wp^{(3)}(z)^2\wp^{(5)}(z)\\ &+ \wp'(z)\wp''(z)\wp^{(4)}(z)\wp^{(5)}(z) - \wp'(z)^2\wp^{(5)}(z)^2 - 3\wp'(z)^4\wp^{(6)}(z)\\ &- \wp'(z)\wp''(z)\wp^{(3)}(z)\wp^{(6)}(z) + \wp'(z)^2\wp^{(4)}(z)\wp^{(6)}(z)\Big)\end{aligned}$$

$$\begin{aligned}(v)\psi_{2n+1}(z) = \frac{1}{d_1}&\psi_n(z)^2\psi_{n+1}(z)^2\cdot\\ &\Big(\Big(\wp(nz) - \wp\big((n+1)z\big)\Big)^3 + 2\Big(\wp'(nz)^2 - \wp'\big((n+1)z\big)^2\Big)\\ &+ 2\Big(\wp\big((n+1)z\big) - \wp(nz)\Big)\Big(\wp''(nz) + \wp''\big((n+1)z\big)\Big)\Big)\end{aligned}$$

$$\chi_{2n+1}(z) = F_{add}\Big(\wp\big((n+1)z\big), \wp(nz), ..., \wp'''(nz)\Big)\cdot\psi_{2n+1}(z)^2$$

$$\begin{aligned}(vi)\ \psi_{2n}(z) = \frac{1}{d_1}&\frac{\psi_{n-1}(z)^2\ \psi_{n+1}(z)^2}{\psi_2(z)}\cdot\\ &\Big(\Big(\wp\big((n-1)z\big) - \wp\big((n+1)z\big)\Big)^3 + 2\Big(\wp'\big((n-1)z\big)^2 - \wp'\big((n+1)z\big)^2\Big)\\ &+ 2\Big(\wp\big((n+1)z\big) - \wp\big((n-1)z\big)\Big)\Big(\wp''\big((n-1)z\big) + \wp''\big((n+1)z\big)\Big)\Big)\end{aligned}$$

$$\chi_{2n}(z) = F_{add}\Big(\wp\big((n+1)z\big), \wp\big((n-1)z\big), ..., \wp'''\big((n-1)z\big)\Big)\cdot\psi_{2n}(z)^2$$

Dabei ist

$$(vii)\quad \wp(nz) = \frac{\chi_n(z)}{\psi_n(z)^2}$$

$$(viii)\,\wp'(nz) = \frac{1}{n}\left(\frac{\chi_n'(z)}{\psi_n(z)^2} - 2\frac{\chi_n(z)\psi_n'(z)}{\psi_n(z)^3}\right)$$

$$(ix)\quad \wp''(nz) = \frac{1}{n^2}\left(\frac{\chi_n''(z)}{\psi_n(z)^2} - 4\frac{\chi_n'(z)\psi_n'(z)}{\psi_n(z)^3} + 6\frac{\chi_n(z)\psi_n'(z)^2}{\psi_n(z)^4} - 2\frac{\chi_n(z)\psi_n''(z)}{\psi_n(z)^3}\right)$$

Beweis : (i) - (iii) folgen direkt aus der Definition von $\psi_n(z)$.
(iv) Wir wenden den Grenzprozeß $u \to z$ auf das Additionstheorem der $\vartheta[\delta]$-Funktion (Beispiel 4.9(ii))

$$2 \cdot \frac{\vartheta[\delta](z+u)\,\vartheta[\delta](z-u)}{\vartheta[\delta](z)^2\,\vartheta[\delta](u)^2}\,\vartheta[0](0)^2\,\frac{c_2\,c_4}{a_4-a_2} =$$

$$= \big(\wp(u)-\wp(z)\big)^3 + 2\big(\wp'(u)^2-\wp'(z)^2\big) + 2\big(\wp(z)-\wp(u)\big)\big(\wp''(z)+\wp''(u)\big)$$

an und bekommen wegen $\vartheta[\delta](0) = \vartheta[\delta]'(0) = \vartheta[\delta]''(0) = 0$ nach Lemma 4.5 nach dreimaliger Anwendung des Satzes von l'Hospital

$$-2 \cdot \frac{\vartheta[\delta](2z)}{\vartheta[\delta](z)^4}\,\vartheta[0](0)^2\,\frac{c_2\,c_4\,\vartheta[\delta]'''(0)}{a_4-a_2} = 3\wp'(z)^3 + \wp''(z)\wp^{(3)}(z) - \wp'(z)\wp^{(4)}(z)\ .$$

Da die rechte Seite nicht identisch 0 wird, ist insbesondere $\vartheta[\delta]'''(0) \neq 0$ bewiesen (siehe oben). Wegen

$$-\frac{\vartheta[0](0)^2\,c_2\,c_4\,\vartheta[\delta]'''(0)}{(a_4-a_2)\,c_1(2)} = -\frac{\vartheta[0](0)^2\,c_2\,c_4}{(a_4-a_2)\,d^2}\,\frac{\vartheta[\delta]'''(0)}{d} = \frac{1}{2}d_1$$

nach Definition von $c_1(2)$ und d_1 folgt

$$\psi_2(z) = (3\wp'(z)^3 + \wp''(z)\wp^{(3)}(z) - \wp'(z)\wp^{(4)}(z))/d_1\ .$$

Nach Definition ist $\chi_2(z) = \wp(2z)\cdot\psi_2(z)^2$. Aus dem Additionstheorem für die $\wp$-Funktion, welches wir ja abkürzend $\wp(z+u) = F_{add}\big(\wp(z),\ldots,\wp'''(u)\big)$ schreiben, bekommen wir durch den Grenzprozeß $u \to z$ nach sechsmaliger Anwendung von l'Hospital

$$\begin{aligned}
\wp(2z) = \Big(&-27\wp'(z)^4\wp''(z)^2 + 27\wp'(z)^5\wp^{(3)}(z) + 18\wp'(z)\wp''(z)^3\wp^{(3)}(z)\\
&- 9\wp'(z)^2\wp''(z)\wp^{(3)}(z)^2 - \wp^{(3)}(z)^4 - 18\wp'(z)^2\wp''(z)^2\wp^{(4)}(z)\\
&- 3\wp'(z)^3\wp^{(3)}(z)\wp^{(4)}(z) + 2\wp''(z)\wp^{(3)}(z)^2\wp^{(4)}(z) - 2\wp'(z)\wp^{(3)}(z)\wp^{(4)}(z)^2\\
&+ 15\wp'(z)^3\wp''(z)\wp^{(5)}(z) - \wp''(z)^2\wp^{(3)}(z)\wp^{(5)}(z) + 2\wp'(z)\wp^{(3)}(z)^2\wp^{(5)}(z)\\
&+ \wp'(z)\wp''(z)\wp^{(4)}(z)\wp^{(5)}(z) - \wp'(z)^2\wp^{(5)}(z)^2 - 3\wp'(z)^4\wp^{(6)}(z)\\
&- \wp'(z)\wp''(z)\wp^{(3)}(z)\wp^{(6)}(z) + \wp'(z)^2\wp^{(4)}(z)\wp^{(6)}(z)\Big)\\
&\Big/\big(3\wp'(z)^3 + \wp''(z)\wp^{(3)}(z) - \wp'(z)\wp^{(4)}(z)\big)^2
\end{aligned}$$

(v) und (vi) folgen aus den Propositionen 5.9 und 5.10, indem wir dort m durch $n+1$ ersetzen, bzw. m durch $k+1$ und n durch $k-1$.

(vii) - (ix) Folgt direkt aus der Definition von $\chi_n(z) = \wp(nz)\psi_n(z)^2$ durch Ableiten nach z.

□

Aus den Gleichungen des Satzes ersieht man nicht sofort, daß sowohl die ψ_n, als auch die χ_n Polynome in den Ableitungen von $\wp$ sind. Nach ihrer Definition wissen wir allerdings schon, daß sie es sind. Bei der rekursiven Berechnung der ψ_n und der χ_n wird man sich daher bemühen müssen, frühzeitig zu kürzen.

Nach der Herleitung sollten die berechneten Polynome noch mit einer geeigneten Potenz von d_1 multipliziert werden, so daß diese im Resultat nicht mehr erscheint. Welche Potenz man nimmt, das hängt von der Herleitung der Polynome ab, d.h. wie m und n in Proposition 5.9 gewählt werden.

Anders als im Fall $g = 1$ genügen in diesem Fall die im Satz erwähnten Anfangswerte, wie man etwa folgendem Algorithmus entnehmen kann.

Algorithmus 5.12: zur Berechnung der ψ_n, χ_n :

Ein Algorithmus, der die ψ_n und χ_n für $n \in \mathbb{Z}$ berechnet, läuft etwa folgendermaßen:

1. Schritt : Berechne die Anfangswerte, d.h. (i)-(iii) des obigen Satzes, sowie $\wp(2z), ..., \wp'''(2z)$, und setze $n = 1$.

2. Schritt : An dieser Stelle sind schon alle $\psi_1(z), ..., \psi_{2n}(z)$, $\chi_1(z), ..., \chi_{2n}(z)$ berechnet. In diesem Schritt berechnen wir

$$\psi_{2n+1}(z) \qquad \text{aus} \qquad \psi_n(z), \psi_{n+1}(z), \chi_n(z), \chi_{n+1}(z) \ ,$$

sowie

$$\chi_{2n+1}(z) \qquad \text{aus} \qquad \psi_n(z), \psi_{n+1}(z), \chi_n(z), \chi_{n+1}(z), \psi_{2n+1}(z) \ .$$

Wegen $n \geq 1$ sind alle benötigten Werte ungleich 0 und schon berechnet.

3. Schritt : Ersetze $n \longleftarrow n + 1$.
An dieser Stelle sind schon alle $\psi_1(z), ..., \psi_{2n-1}(z), \chi_1(z), ..., \chi_{2n-1}(z)$ berechnet. Jetzt berechnen wir

$$\psi_{2n}(z) \qquad \text{aus} \qquad \psi_2(z), \psi_{n-1}(z), \psi_{n+1}(z), \chi_{n-1}(z), \chi_{n+1}(z) \ ,$$

sowie

$$\chi_{2n}(z) \qquad \text{aus} \qquad \psi_{n-1}(z), \psi_{n+1}(z), \chi_{n-1}(z), \chi_{n+1}(z), \psi_{2n}(z) \ .$$

Wegen $n \geq 2$ sind alle benötigten Werte ungleich 0 und schon berechnet.

Weiter mit Schritt 2.

□

Kapitel 6 : Der Schoof-Algorithmus im Fall $g = 2$

In diesem Kapitel werden wir die in den Kapiteln 3-5 hergeleiteten Gleichungen benutzen, um das charakteristische Polynom des Frobenius-Endomorphismus der Jacobischen Varietät einer hyperelliptischen Kurve vom Geschlecht 2, die über einem endlichen Körper definiert ist, zu berechnen. Die benötigte Laufzeit ist ein Polynom im Logarithmus der Körperordnung. Die Idee stützt sich auf den Algorithmus von Schoof, der dieses für den Fall einer elliptischen Kurve ebenfalls in polynomialer Zeit vom Logarithmus der Körperordnung löst (siehe [Schoof]).

Pila hat in [Pila] eine Verallgemeinerung des Schoof-Algorithmus auf beliebige Abelsche Varietäten beschrieben; diese Arbeit enhält allerdings die starke Voraussetzung, daß die Abelsche Varietät, sowie die Addition auf ihr, explizit durch Gleichungen gegeben sind; allerdings werden in der Arbeit keine Gleichungen angegeben. Diese Voraussetzungen haben wir in den Kapiteln 3 und 4 erfüllt. Es stellt sich aber heraus, daß in unserem Fall $g = 2$ der Algorithmus gegenüber dem von Pila vorgeschlagenen sehr vereinfacht werden kann.

Die erste Vereinfachung ist, daß wir Rekursionsformeln für die n-Torsionspunkte auf einer Karte im Kapitel 5 bewiesen haben. Diese stützen sich auf das recht einfache Additionstheorem der $\vartheta[\delta]$-Funktion, sowie auf das Additionstheorem der $\wp$-Funktion.

Ferner werden wir beweisen, daß es genügt, nur auf einer Karte zu rechnen, nämlich auf $\mathrm{Jac}(C) - \Theta$. Pilas Algorithmus benötigt die Beschreibung der gesamten Varietät; allein die Beschreibung der n-Torsionspunkte in seinem Fall führt zu vielen Fallunterscheidungen, da er alle von 0 verschiedenen n-Torsionspunkte auf der Varietät beschreiben möchte.

Wegen der speziellen Form des charakteristischen Polynoms können wir aus dem Minimalpolynom direkt das charakteristische Polynom herleiten, siehe Lemma 6.3. Zur Bestimmung des Minimalpolynoms wenden wir nur Mitgliedschaftstests eines Polynoms im Radikal eines Ideals an, Pila dagegen benötigt neben dem Idealmitgliedschaftstest eines Polynoms auch die Berechnung der Dimension des Polynomrings in den Koordinaten der Varietät modulo einem Ideal.

Sei nun $\mathbb{F}_q$ der endliche Körper mit q Elementen der Charakteristik $p \neq 2$ und $\overline{C} : Y^2 = f(X)$ eine hyperelliptische Kurve über $\mathbb{F}_q$ vom Geschlecht 2, d.h. $f(X) \in \mathbb{F}_q[X]$ sei normiert, vom Grad 5 und mit paarweise verschiedenen Nullstellen.

Sei $\mathrm{Jac}(\overline{C})$ die Jacobische Varietät von $\overline{C}$ über dem algebraischen Abschluß $\overline{\mathbb{F}}_q$ von $\mathbb{F}_q$. Wir wählen ein p-modulares System $(K, R, \mathbb{F}_q)$ mit einem Körper K der Cha-

rakteristik 0 und einem Bewertungsring R einer vollständigen diskreten Bewertung von K mit $\mathbb{F}_q \cong R/\mathrm{Rad}(R)$. Sei C eine hyperelliptische Kurve vom Geschlecht 2 über K, die schon über R definiert ist und deren Reduktion gleich $\overline{C}$ ist. Nach dem Lefschetz-Prinzip bekommen wir eine Beschreibung der Jacobischen Varietät von C, indem wir $\mathrm{Jac}(C)$ nach Lemma 1.2 mit 2^g Karten isomorph zu $\mathrm{Jac}(C) - \Theta$ überdecken und die Gleichungen der Kapitel 3–5 über dem Quotientenkörper K von R lesen. Nach Konstruktion hat C bei Reduktion nach $\overline{C}$ gute Reduktion, so daß nach [Igusa] auch $\mathrm{Jac}(C)$ gute Reduktion hat. Es folgt, daß die Gleichungen, die $\mathrm{Jac}(C)$, sowie ihr Additionsgesetz beschreiben, nach der Reduktion die Jacobische Varietät und ihr Additionsgesetz von $\overline{C}$ beschreiben. Diese Gleichungen sind dann schon über $\mathbb{F}_q$ definiert.

Nach diesen Überlegungen werden wir im Folgenden $\mathbb{F}_q$ festhalten und der Einfachheit halber C für $\overline{C}$ schreiben.

Sei $m \in \mathbb{Z}$ und $\mathrm{Jac}(C)[m]$ die Untergruppe der m-Torsionspunkte von $\mathrm{Jac}(C)$. Für eine Primzahl $l \neq p$ sei $T_l\mathrm{Jac}(C)$ der Tatemodul, das ist der projektive Limes der Gruppen $\mathrm{Jac}(C)[l^n]$ unter der durch die Multiplikation mit l induzierten Abbildung

$$\mathrm{Jac}(C)[l^{n+1}] \longrightarrow \mathrm{Jac}(C)[l^n] \ .$$

$T_l\mathrm{Jac}(C)$ ist freier $\mathbb{Z}_l$-Modul vom Rang 4. Sei $T_l\mathrm{Jac}(C) \otimes \mathbb{Q}_l$ der $\mathbb{Q}_l$-Vektorraum der Dimension 4.

Da die Jacobische Varietät, sowie die Addition auf ihr, durch Gleichungen über F_q beschrieben sind, läßt sich der Frobenius-Automorphismus

$$\phi : \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q \ , \ x \longmapsto x^q \ ,$$

zunächst zu dem Frobenius-Endomorphismus auf $\mathrm{Jac}(C)$, dann zu dem Frobenius-Endomorphismus auf $T_l\mathrm{Jac}(C) \otimes \mathbb{Q}_l$ erweitern. Auf $T_l\mathrm{Jac}(C) \otimes \mathbb{Q}_l$ ist dieser ein $\mathbb{Q}_l$-Vektorraumautomorphismus, den wir ebenfalls mit ϕ bezeichnen.

Satz 6.1 : *Das charakteristische Polynom des $\mathbb{Q}_l$-Automorphismus ϕ auf $T_l Jac(C) \otimes \mathbb{Q}_l$ lautet*

$$ch(t) = t^4 + a_1 t^3 + a_2 t^2 + a_1 q t + q^2 \quad mit \quad a_1, a_2 \in \mathbb{Z} \ .$$

Es ist unabhängig von l, und das gestürzte Polynom $t^4\, ch(1/t)$ ist gleich dem Zähler der Zetafunktion des nichtsingulären Modells von C.

Beweis : Siehe [Weil] oder [Lang.1], VI, §3.

□

Als Korollar aus der Riemannschen Vermutung für Kurven über endlichen Körpern, die bewiesen ist, und diesem Satz bekommen wir Abschätzungen der Koeffizienten a_1 und a_2 von $\mathrm{ch}(t)$.

Korollar 6.2 :

$$|a_1| \leq 4\sqrt{q}$$
$$|a_2| \leq 6q \ .$$

Beweis : Der Zähler der Zetafunktion des nichtsingulären Modells von C hat nach der Riemannschen Vermutung die Form

$$P(t) = (1-\omega_1 t)(1-\omega_2 t)(1-\omega_3 t)(1-\omega_4 t)$$

mit $\omega_i \in \mathbb{C}$ vom Betrag $|\omega_i| = \sqrt{q}$ für $i = 1,...,4$. Koeffizientenvergleich in der Gleichung $\mathrm{ch}(t) = t^4 P(1/t)$ liefert zusammen mit den Eigenschaften der ω_i die Behauptung.

□

Schränken wir ϕ auf die Untergruppe $\mathrm{Jac}(C)[l]$ der l-Torsionspunkte ein, d.h. $\phi_l := \phi\,|_{\mathrm{Jac}(C)[l]}$, dann ist ϕ_l nach Konstruktion von $\mathrm{ch}(t)$ ein $\mathbb{F}_l$-Vektorraumautomorphismus mit charakteristischem Polynom

$$\mathrm{ch}_l(t) \equiv \mathrm{ch}(t) \bmod l \ .$$

Die Strategie ist, für genügend viele kleine Primzahlen l die Koeffizienten a_1 und a_2 mod l des charakteristischen Polynoms zu berechnen. Anschließend können wir wegen der Beschränktheit von a_1 und a_2 diese mit dem Chinesichen Restsatz bestimmen.

Diese Strategie verfolgen wir etwa so, daß wir bei gegebener Primzahl $l \neq 2, l \neq p$, die von der Größenordnung $O(\log(q))$ ist, alle Polynome $r(t) \in \mathbb{F}_l[t]$ der Form

$$r(t) = t^4 + \tilde{a}_1 t^3 + \tilde{a}_2 t^2 + \tilde{a}_1 q t + q^2 \quad \text{mit} \quad \tilde{a}_1, \tilde{a}_2 \in \mathbb{F}_l$$

testen, ob $r(\phi_l) = 0$ ist, oder äquivalent, ob $r(\phi_l)x = 0$ für alle $x \in \mathrm{Jac}(C)[l]$ ist. Die möglichen Kandidaten sind Vielfache des Minimalpolynoms $\mu_l(t)$ von ϕ_l, welches wir anschließend durch Faktorisierung des gefundenen $r(t)$ in irreduzible Faktoren als normierten Teiler kleinsten Grades von $r(t)$ mit $\mu_l(\phi_l) = 0$ bestimmen können. Wegen der speziellen Form des charakteristischen Polynoms können wir aus dem Minimalpolynom sofort das charakteristische Polynom bestimmen:

Lemma 6.3 : *Für eine Primzahl $2 \neq l \neq p$ sei*

$$ch_l(t) = t^4 + a_1 t^3 + a_2 t^2 + a_1 q t + q^2$$

mit $a_1, a_2 \in \mathbb{F}_l$ das charakteristische Polynom und $\mu_l(t)$ das Minimalpolynom von ϕ_l. Dann gelten

(a) Ist $\deg(\mu_l(t)) = 1$, *dann ist* $ch_l(t) = \mu_l(t)^4$.
(b) Ist $\deg(\mu_l(t)) = 2$, *dann ist* $ch_l(t) = \mu_l(t)^2$.
(c) Ist $\deg(\mu_l(t)) = 3$ *und* $r(t) = t^4 + \tilde{a}_1 t^3 + \tilde{a}_2 t^2 + \tilde{a}_1 qt + q^2 \in \mathbb{F}_l[t]$ *mit* $r(\phi_l) = 0$, *dann ist* $ch_l(t) = r(t)$.
(d) Ist $\deg(\mu_l(t)) = 4$, *dann ist* $ch_l(t) = \mu_l(t)$.

Beweis : (a) trivial.

(b) Hier unterscheiden wir drei Fälle:

1. Fall : $\mu_l(t) = (t-e)^2$ mit dem Eigenwert $e \in \mathbb{F}_l$. Dann folgt trivial $\mathrm{ch}_l(t) = \mu_l(t)^2$.

2. Fall : $\mu_l(t) = (t-e_1)(t-e_2)$ mit den zwei verschiedenen Eigenwerten $e_1, e_2 \in \mathbb{F}_l$. Nehmen wir ohne Einschränkung $\mathrm{ch}_l(t) = (t-e_1)^3(t-e_2)$ an, also

$$\mathrm{ch}_l(t) = t^4 - (3e_1 + e_2)t^3 + (3e_1^2 + 3e_1e_2)t^2 - (e_1^3 + 3e_1^2e_2)t + e_1^3e_2 \ .$$

Wegen der speziellen Form von $\mathrm{ch}_l(t)$ gilt einerseits

$$a_1^2q^2 = (3e_1 + e_2)^2e_1^3e_2 = 9e_1^5e_2 + 6e_1^4e_2^2 + e_1^3e_2^3 \ ,$$

sowie andererseits

$$(a_1q)^2 = (e_1^3 + 3e_1^2e_2)^2 = e_1^6 + 6e_1^5e_2 + 9e_1^4e_2^2 \ .$$

Da kein Eigenwert gleich 0 ist, folgt nach Division der entstehenden Gleichung durch e_1^3, daß $(e_1 - e_2)^3 = 0$, also $e_1 = e_2$ ist, was im Widerspruch zur Voraussetzung steht. Daher gilt in diesem Fall

$$\mathrm{ch}_l(t) = (t-e_1)^2(t-e_2)^2 = \mu_l(t)^2 \ .$$

3. Fall : $\mu_l(t)$ irreduzibel vom Grad 2. Dann folgt wieder trivial $\mathrm{ch}_l(t) = \mu_l(t)^2$.

(c) Wir nehmen $\mathrm{ch}_l(t) \neq r(t)$ an. Da $\mu_l(t)$ sowohl $r(t)$, als auch $\mathrm{ch}_l(t)$ teilt, teilt es auch deren Differenz,

$$\mu_l(t) \Big| \mathrm{ch}_l(t) - r(t) = (a_1 - \tilde{a}_1)t^3 + (a_2 - \tilde{a}_2)t^2 + (a_1 - \tilde{a}_1)qt \ ,$$

die nach unserer Annahme ungleich 0 ist. Aus $\deg(\mu_l(t)) = 3$ würde dann aber $a_1 \neq \tilde{a}_1$ folgen, also $(a_1 - \tilde{a}_1)\mu_l(t) = \mathrm{ch}_l(t) - r(t)$. Dann wäre aber $\mu_l(0) = 0$ und 0 Eigenwert von ϕ_l, was im Widerspruch zur Bijektivität von ϕ_l steht. Daher ist $\mathrm{ch}_l(t) = r(t)$.

(d) trivial.

□

Wir beschreiben nun, wie man bei gegebenem $r(t) \in \mathbb{F}_l[t]$ testet, ob $r(\phi_l)x = 0$ für alle $x \in \mathrm{Jac}(C)[l]$ ist. Da $\mathrm{Jac}(C)[l]$ ein $\mathbb{F}_l$-Vektorraum ist, genügt offenbar das Testen dieser Gleichung für eine Basis von $\mathrm{Jac}(C)[l]$. Andererseits haben wir im Kapitel 5 Gleichungen hergeleitet, die die l-Torsionspunkte in $\mathrm{Jac}(C) - \Theta$ beschreiben. Nach der Reduktion beschreiben diese Gleichungen zusammen mit den beiden beschreibenden Gleichungen für $\mathrm{Jac}(C) - \Theta$, die alle über $\mathbb{F}_q$ definiert sind, nun die l-Torsionspunkte in $\mathrm{Jac}(C) - \Theta$ über $\overline{\mathbb{F}}_q$.

Lemma 6.4 : *Für $2 \neq l \neq p$ enthält $Jac(C) - \Theta$ eine $\mathbb{F}_l$-Basis von $Jac(C)[l]$.*

Beweis : Sei $b_1, ..., b_4$ eine beliebige $\mathbb{F}_l$-Basis von $\mathrm{Jac}(C)[l]$. Ist einer der Basisvektoren in Θ, etwa $b_i \in \Theta$, dann ersetzen wir ihn durch $2b_i$. Da b_i ein l-Torsionspunkt ist, ist $2b_i \neq 0$. Daher ist $2b_i \notin \Theta$, wie man leicht mit Hilfe des Divisorklassengruppenmodells sieht, denn entspricht die Divisorklasse $[P - \infty] \in \Theta$ dem Basisvektor b_i, dann entspricht $[2 \cdot P - 2 \cdot \infty] \in \mathrm{Jac}(C) - \Theta$ dem neuen Basisvektor $2 \cdot b_i$. Die resultierenden Vektoren bilden natürlich weiterhin eine $\mathbb{F}_l$-Basis von $\mathrm{Jac}(C)[l]$.

Iterieren wir diesen Prozeß, solange noch Basisvektoren in Θ liegen, dann erhalten wir endlich eine Basis, die auch in $\mathrm{Jac}(C) - \Theta$ liegt.

□

Wir testen nun die Gleichung $r(\phi_l)x = 0$ für alle l-Torsionspunkte x in $\mathrm{Jac}(C) - \Theta$. Abkürzend schreiben wir $(\mathrm{Jac}(C) - \Theta)[l] := (\mathrm{Jac}(C) - \Theta) \cap \mathrm{Jac}(C)[l]$. Dies bedeutet insbesondere, daß wir nur auf einer Karte der Überdeckung von $\mathrm{Jac}(C)$ rechnen werden, nämlich auf $\mathrm{Jac}(C) - \Theta$. Wegen der Wichtigkeit des Resultats formulieren wir

Korollar 6.5 : *Für ein Polynom $r(t) \in \mathbb{F}_l[t]$ sind äquivalent*

$$r(\phi_l) = 0 \qquad \textit{und} \qquad r(\phi_l)x = 0 \textit{ für alle } x \in (Jac(C) - \Theta)[l] \ .$$

Wir ersetzen in den Gleichungen der Kapitel 3–5 die Koordinaten $X_1 := \wp(z)$, $X_2 := \wp'(z)$, $X_3 := \wp''(z)$, $X_4 := \wp^{(3)}(z)$ und setzen $X := (X_1, X_2, X_3, X_4)$. Sei I_l das Ideal in $\mathbb{F}_q[X] = \mathbb{F}_q[X_1, ..., X_4]$, das die Verschwindungsmenge $V(I_l) = (\mathrm{Jac}(C) - \Theta)[l]$ hat. Mit den Bezeichnungen von oben und denen von Beispiel 3.7(ii) und Kapitel 5 wird I_l von den Polynomen $F_1(X), F_2(X), \psi_l(X), \chi_l(X) \in \mathbb{F}_q[X]$ erzeugt,

$$I_l = \langle F_1(X), F_2(X), \psi_l(X), \chi_l(X) \rangle \ .$$

An dieser Stelle fügen wir zum Verständnis der weiteren Verfahrensweise einen kurzen Überblick über idealtheoretische Rechnungen ein.

Idealtheoretische Rechnungen

In diesem Unterabschnitt werden wir einige idealtheoretische Algorithmen vorstellen, die wir bei der weiteren Beschreibung benötigen. Zu nennen sind hier Mitgliedschaftstests eines Polynoms in einem Ideal bzw. im Radikal eines Ideals und Reduktion eines Polynoms auf eine Normalform modulo einem Ideal. Diese Rechnungen lassen sich nach der Bestimmung einer Gröbner-Basis des Ideals recht einfach durchführen und elegant beschreiben. Da die Ideale, die in unserer Anwendung vorkommen, nulldimensional sind, sie beschreiben nur eine Teilmenge von $\mathrm{Jac}(C)[l]$ und $\#\mathrm{Jac}(C)[l] = l^4$, ist eine Laufzeitabschätzung möglich, siehe etwa [Giusti]. Für die Implementation sollte allerdings auf [Hermann] zurückgegriffen werden, so daß zusammen mit [Mayr] die idealtheoretischen Methoden, die [Pila] benutzt, imitiert werden können. Der kurze Überblick, den wir hier geben, stützt sich auf [Buchberger].

Seien K ein Körper, $K[X_1, ..., X_n] = K[X]$ der Polynomring in n Unbestimmten und $<_T$ eine totale Ordnung auf der Menge der Monome, $M_n := \{X_1^{i_1} ... X_n^{i_n} | i_1, ..., i_n \geq 0\}$, die die beiden Bedingungen

$$1 <_T t \text{ für alle Monome } t \in M_n - \{1\}$$

und

$$\text{ist } s <_T t \text{ , dann ist } s \cdot u <_T t \cdot u \text{ für alle } s, t, u \in M_n$$

erfüllt.

Sei $F := \{f_1(X), ..., f_m(X)\}$ eine endliche Menge von Polynomen $f_1(X), ..., f_m(X) \in K[X]$, $I = \langle F \rangle = \langle f_1(X), ..., f_m(X) \rangle$ das von F erzeugt Ideal in $K[X]$ und $g(X) \in K[X]$. Es stellt sich hier die Frage, wie ein kanonischer Repräsentant von $g(X)$ modulo I ausgezeichnet und berechnet werden kann. Der erste Schritt ist ein Reduktionsschritt, wie er schon im Fall einer Unbestimmten bekannt ist:

Definition : (i) Wir sagen, daß $g(X)$ unter Benutzung von $f(X) \in F$, $b \in K$ und $u(X) \in M_n$ reduzierbar ist, in Zeichen $g \longrightarrow_{f,b,u}$, falls der Koeffizient von $g(X)$ vor dem Monom $u(X)$·(größtes Monom von f) ungleich 0 ist, und falls dieser Koeffizient gleich b·(führender Koeffizient von f) ist. (Die Begriffe "führender Koeffizient" und "größtes Monom" hängen von der gewählten Ordnung $<_T$ ab.)

(ii) In dem Fall (i), d.h. wenn $g(X)$ mit f, b, u reduzierbar ist, definieren wir

$$h(X) := g(X) - b \cdot u(X) \cdot f(X)$$

und bezeichnen die Reduktion von $g(X)$ zu $h(X)$ mit $g \longrightarrow_F h$.

(iii) $h(X)$ ist in Normalform modulo F (diese Bedingung hängt nicht nur vom Ideal I, sondern auch vom Erzeugendensystem F ab), falls kein $h'(X) \in K[X]$ mit $h \longrightarrow_F h'$ existiert.

$h(X)$ ist eine Normalform von $g(X)$ modulo F, falls eine Sequenz

$$g = k_0 \longrightarrow_F k_1 \longrightarrow_F \ldots \longrightarrow_F k_r = h$$

existiert, so daß $h(X)$ in Normalform modulo F ist.

□

Teil (ii) der Definition ist ein üblicher Reduktionsschritt, da ein Monom von $g(X)$ durch Subtraktion eines geeigneten Vielfachen $b \cdot u(X) \cdot f(X)$ eines Polynoms $f(X) \in F$ gelöscht wird.

Jedes $g(X) \in K[X]$ kann in endlich vielen Schritten zu einer Normalform $h(X)$ reduziert werden. Dieses Verfahren ist algorithmisch:

Algorithmus : (Reduktion eines Polynoms auf eine Normalform)

Eingabe : Eine endliche Menge F von Polynomen in $K[X]$ und ein $g(X) \in K[X]$.

Ausgabe : Eine Normalform $h(X) \in K[X]$ von $g(X)$.

Verfahren : 1. Schritt : Setze $h(X) := g(X)$

2. Schritt : Teste, ob $h(X)$ in Normalform ist, d.h. teste, ob ein $f(X) \in F$, $b \in K$ und ein $u(X) \in M_n$ mit $h(X) \longrightarrow_{f,b,u}$ existieren. Falls nicht, dann gebe $h(X)$ aus, sonst ersetze $h(X)$ durch $h(X) - b \cdot u(X) \cdot f(X)$ und wiederhole diesen Schritt.

□

In diesem Algorithmus wird nicht festgelegt, welches $f(X) \in F$ zur Reduktion gewählt werden soll. Daher ist es denkbar und anhand von Beispielen auch belegbar, daß ein Polynom zu verschiedenen Normalformen modulo F reduziert werden kann. Erzeugendensysteme F, für die es solche Beispiele nicht gibt, werden wir nun definieren.

Definition : Wir nennen F eine Gröbner-Basis, falls für alle $g(X) \in K[X]$ gilt, daß zwei Normalformen von $g(X)$ modulo F stets gleich sind.

Diese Definition ist neben ihrer Motivation der eindeutigen Reduktion eines Polynoms auf eine Normalform modulo F auch universell, da jedes Ideal eine Gröbner-Basis besitzt. Diese läßt sich auch aus einem beliebigen Erzeugendensystem des Ideals algorithmisch berechnen, und man kann algorithmisch testen, ob ein Erzeugendensystem eines Ideals eine Gröbner-Basis ist. Für nähere Einzelheiten zu dem Algorithmus zur Berechnung einer Gröbner-Basis siehe etwa [Buchberger].

Nach Wahl einer Gröbner-Basis läßt sich jedes Polynom $g(X) \in K[X]$ auf eine kanonische Normalform reduzieren. Daher ist der Mitgliedschaftstest eines Polynoms zu einem Ideal trivial, denn es ist genau dann $g(X) \in I$, wenn die Normalform von $g(X)$ gleich 0 ist.

Den Test auf Mitgliedschaft eines Polynoms $g(X)$ im Radikal $\sqrt{I}$ eines Ideals I führt man mit Hilfe des Tricks von Rabinowitsch folgendermaßen aus. Genau dann gilt nämlich $g(X) \in \sqrt{I}$, wenn $1 \in \langle I, 1 - Z \cdot g(X) \rangle$, welches ein Ideal in $K[X, Z]$ mit einer neuen Unbestimmten Z ist, siehe etwa [Robbiano].

Nach diesem Einschub über idealtheoretische Rechnungen kehren wir zu unserem speziellen Ideal I_l zurück. Der nächste Schritt nach der Erzeugung von I_l ist die Berechnung einer Gröbner-Basis dieses Ideals, denn anschließend können wir auftretende Polynome $g(X) \in \mathbb{F}_q[X]$ modulo dem Ideal I_l algorithmisch auf eine eindeutige Normalform, die von der gewählten Gröbner-Basis abhängt, $N(g)(X) \in \mathbb{F}_q[X]$ reduzieren.

Insbesondere berechnen wir so mit Hilfe der "repeated squaring method" die Normalformen der Koordinaten von $\phi_l^i(X) = (X_1^{q^i}, ..., X_4^{q^i})$ für $i = 1, ..., 4$, also

$$\phi_l^i(X) \equiv (N(X_1^{q^i}), ..., N(X_4^{q^i})) \bmod I_l \qquad \text{für } i = 1, ..., 4.$$

Sei nun $r(t) = t^4 + \tilde{a}_1 t^3 + \tilde{a}_2 t^2 + \tilde{a}_1 q t + q^2 \in \mathbb{F}_l[t]$ und X ein generischer Punkt von $\mathrm{Jac}(C) - \Theta$. Der Übersichtlichkeit halber schreiben wir $\oplus$,$\ominus$ für die Addition bzw. Subtraktion in $\mathrm{Jac}(C)$. Wir möchten $r(\phi_l)X = 0$ testen, wenn wir X zu einem Punkt x in $(\mathrm{Jac}(C) - \Theta)[l]$ spezialisieren. Diese Gleichung ist äquivalent zu

$$\phi_l^4(X) = \ominus(\tilde{a}_1 \phi_l^3(X) \oplus \tilde{a}_2 \phi_l^2(X) \oplus \tilde{a}_1 q \phi_l(X) \oplus q^2 X) \ ,$$

welche wir idealtheoretisch koordinatenweise testen werden. Die Koordinaten der linken Seite sind Polynome in X, während die der rechten Seite rationale Funktionen in X sind. Wir schreiben abkürzend obige Gleichung etwa folgendermaßen

$$\phi_l^4(X) = \left(\frac{z_1(X)}{n(X)}, ..., \frac{z_4(X)}{n(X)} \right) \text{ mit Polynomen } z_i(X), n(X) \in \mathbb{F}_q[X] \ ,$$

wobei $n(X)$ der gemeinsame Nenner der Komponenten ist. Bei der rechnerischen Aufstellung dieser Gleichung werden wir allerdings die Zähler- und Nennerpolynome schon frühzeitig auf eine Normalform modulo I_l reduzieren müssen. Dies bedeutet, daß wir anschließend nicht mehr kürzen dürfen.

Haben wir die vier Gleichungen modulo I_l aufgestellt, etwa

$$N(X_i^{q^4}) = \frac{N(z_i)(X)}{N(n)(X)} \qquad \text{für } i = 1, ..., 4 \ ,$$

dann multiplizieren wir jede Gleichung mit dem gemeinsamen Nenner der rechten Seite, so daß auf beiden Seiten Polynome in $\mathbb{F}_q[X]$ stehen. Nun spezialisieren wir den generischen Punkt X zu einem Punkt $x \in (\mathrm{Jac}(C) - \Theta)[l]$, wir testen also, ob die vier Gleichungen modulo dem Radikal $\sqrt{I_l}$ von I_l richtig sind, d.h. wir testen, ob

$$N(X_i^{q^4}) \cdot N(n)(X) - N(z_i)(X) \in \sqrt{I_l} \text{ für } i = 1, ..., 4 \ .$$

Falls dieses für ein i nicht erfüllt ist, dann existiert ein l-Torsionspunkt $x \in (\mathrm{Jac}(C) - \Theta)[l]$, der die Gleichung $r(\phi_l)x = 0$ nicht erfüllt, d.h. $r(t)$ ist falsch gewählt.

Sind andererseits alle Koordinatengleichungen erfüllt, dann können wir noch nicht auf die Richtigkeit der Gleichung $r(\phi_l) = 0$ schließen. Denn es kann ja einen l-Torsionspunkt $x \in (\mathrm{Jac}(C) - \Theta)[l]$ mit $n(x) = z_i(x) = 0$ für alle i, aber $r(\phi_l)x \neq 0$ geben.

Wir betrachten nun nur noch die $x \in (\mathrm{Jac}(C) - \Theta)[l]$, für die $n(x) = 0$ ist. Diese werden durch das Ideal in $\mathbb{F}_q[X]$,

$$\tilde{I}_l := \langle I_l, n(X) \rangle = \langle I_l, N(n)(X) \rangle \ ,$$

beschrieben. Da sowohl die $z_i(X)$, als auch $n(X)$ Potenzreihen in einem lokalen Parameter der Kurve C zum Punkt ∞ sind, können wir die Regel von l'Hospital anwenden, was bedeutet, daß wir $z_i(X)$ durch $D_\infty z_i(X)$ und $n(X)$ durch $D_\infty n(X)$ ersetzen. Dabei operiert die Derivation D_∞ in der üblichen Weise auf den Koordinaten, nämlich

$$D_\infty(X_1) = X_2, D_\infty(X_2) = X_3, D_\infty(X_3) = X_4, D_\infty(X_4) = F_0(X_1, X_2, X_3, X_4)$$

mit der Bezeichnung F_0 aus Beispiel 3.7(ii). Beim Ableiten der Polynome sollte man die Linearität des Frobenius-Endomorphismus ϕ_l ausnutzen.

Wir testen also, ob die Gleichungen

$$X_i^{q^4} = \frac{D_\infty z_i(X)}{D_\infty n(X)} \ , i = 1, ..., 4$$

für $x \in V(\tilde{I}_l)$ richtig sind. Dazu wählen wir wieder eine Gröbner-Basis von $\tilde{I}_l$ und bezeichnen die Normalform eines Polynoms $g(X) \in \mathbb{F}_q[X]$ modulo $\tilde{I}_l$ mit $\tilde{N}(g)(X)$. Wie oben testen wir dann

$$\tilde{N}(D_\infty n)(X) \cdot \tilde{N}(X_i^{q^4}) - \tilde{N}(D_\infty z_i)(X) \in \sqrt{\tilde{I}_l} \ .$$

Wir dürfen bei diesem Schritt nicht die Normalformen $N(z_i)(X)$ bzw. $N(n)(X)$ ableiten, sondern müssen zunächst formal $z_i(X)$ und $n(X)$ ableiten und diese anschließend mit Hilfe der gewählten Gröbner-Basis auf die neuen Normalformen reduzieren.

Diesen Prozeß iterieren wir, bis das Ideal, modulo dem wir reduzieren, gleich $\mathbb{F}_q[X]$ ist. Dieses stellen wir bei der Berechnung einer Gröbner-Basis fest, denn dann ist $1 \in \mathbb{F}_q[X]$ ein Element der Gröbner-Basis.

Haben wir ein $r(t) \in \mathbb{F}_l[t]$ mit $r(\phi_l) = 0$ gefunden, dann faktorisieren wir dieses und berechnen analog zu oben das Minimalpolynom $\mu_l(t) \in \mathbb{F}_l[t]$ als Teiler kleinsten Grades von $r(t)$ mit $\mu_l(\phi_l) = 0$. Anschließend wenden wir Lemma 6.3 an und bekommen das charakteristische Polynom $\mathrm{ch}_l(t)$ von ϕ_l.

Diesen Prozeß führen wir für kleine Primzahlen $l_1, ..., l_k$ mit $2 < l_1 < ... < l_k$, $l_i \neq p$, und

$$\prod_{i=1}^{k} l_i > 8\sqrt{q}$$

durch, denn dann läßt sich $a_1 \in \mathbb{Z}$ mit $|a_1| \leq 4\sqrt{q}$ aus $a_1 \bmod l_1, ..., a_1 \bmod l_k$ mit dem Chinesischen Restsatz berechnen.

Zur Berechnung von a_2 wählen wir weitere Primzahlen $l_{k+1}, ..., l_m$ mit $l_k < l_{k+1} < ... < l_m$, $l_i \neq p$, und

$$\prod_{i=1}^{m} l_i > 12\, q\ .$$

Sei l nun eine der weiteren Primzahlen. Wir wählen dann $\tilde{a}_2 \in \mathbb{F}_l$ und setzen

$$r(t) = t^4 + a_1 t^3 + \tilde{a}_2 t^2 + a_1 q t + q^2 \in \mathbb{F}_l[t]\ .$$

Gilt für ein $x \in (\mathrm{Jac}(C) - \Theta)[l]$ die Gleichung $r(\phi)x = 0$, dann folgt

$$(r(\phi) - \mathrm{ch}_l(\phi))x = (\tilde{a}_2 - a_2)\phi_l^2(x) = 0\ .$$

Da ϕ_l invertierbar ist, folgt daraus schon $\tilde{a}_2 \equiv a_2 \bmod l$.

Zur weiteren Berechnung von $\mathrm{ch}_l(t)$ brauchen wir nun nicht mehr das Minimalpolynom von ϕ_l bestimmen. Andererseits genügt es, $r(\phi)(x) = 0$ für ein $x \in (\mathrm{Jac}(C) - \Theta)[l]$ zu testen, so daß, wenn überhaupt, nur wenige Anwendungen von l'Hospital (s.o.) genügen, die Gleichung zu testen.

Wir werden anschließend den gesamten Algorithmus nochmals formal beschreiben.

Algorithmus 6.6 :

1. Schritt : Setze $l_0 := 2$ und $k := 1$.

2. Schritt : Wähle eine Primzahl $l_k > l_{k-1}$, $l_k \neq p$ und setze zur Abkürzung $l := l_k$. Ferner setze

$$I_{l,0} := \langle F_1(X), F_2(X), \psi_l(X), \chi_l(X) \rangle$$

als Ideal in $\mathbb{F}_q[X]$ und berechne eine Gröbner Basis GB_0 von $I_{l,0}$.

3. Schritt : Wähle $\tilde{a}_1, \tilde{a}_2 \in \mathbb{F}_l$ und setze

$$r(t) := t^4 + \tilde{a}_1 t^3 + \tilde{a}_2 t^2 + \tilde{a}_1 q t + q^2 \ .$$

4. Schritt : Berechne

$$\left(\frac{z_1(X)}{n(X)}, ..., \frac{z_4(X)}{n(X)}\right) := \ominus(\tilde{a}_1 \phi_l^3(X) \oplus \tilde{a}_2 \phi_l^2(X) \oplus \tilde{a}_1 q \phi_l(X) \oplus q^2 X)$$

mit dem gemeinsamen Nennerpolynom $n(X) \in \mathbb{F}_q[X]$.

5. Schritt : Setze $j := 0$. Diese Variable indiziert die sich bei jeder Anwendung von l'Hospital vergrößernden Ideale $I_{l,j}$ in $\mathbb{F}_q[X]$.

6. Schritt : Berechne für $i = 1, ..., 4$ Normalformen

$$N(N(X_i^{q^4}) \cdot N(n)(X) - N(z_i)(X)) \bmod I_{l,j}$$

in Abhängigkeit von der gewählten Gröbner-Basis GB_j und teste, ob diese Polynome im Radikal $\sqrt{I_{l,j}}$ sind. Falls nicht, dann gehe zu Schritt 3 und wähle ein neues Paar $\tilde{a}_1, \tilde{a}_2$.

7. Schritt : Ersetze j durch $j+1$, definiere $I_{l,j} := \langle I_{l,j-1}, N(n(X))\rangle$ und berechne wieder eine Gröbner-Basis GB_j von $I_{l,j}$. Enthält diese als Basiselement die $1 \in \mathbb{F}_q[X]$, dann ist die Richtigkeit der Gleichungen des 4. Schrittes bewiesen. In diesem Fall fahren wir bei Schritt 9 fort.

8. Schritt : In diesem Schritt wenden wir den Satz von l'Hospital an. Dazu ersetzen wir $z_i(X)$ durch $D_\infty z_i(X)$ für $i = 1, ..., 4$, sowie $n(X)$ durch $D_\infty n(X)$ unter Ausnutzung der Linearität von ϕ_l und fahren mit Schritt 6 fort.

9. Schritt : Berechne durch Faktorisierung von $r(t)$ das Minimalpolynom $\mu_l(t)$, indem analog zu den Schritten 4 bis 8 verfahren wird, nur mit einem Teiler von $r(t)$ anstelle von $r(t)$. Anschließend berechnen wir $\mathrm{ch}_l(t)$ aus $\mu_l(t)$ nach Lemma 6.3. Aus $\mathrm{ch}_l(t)$ bestimmen wir a_1 und a_2 mod l.

10. Schritt : Ist $\prod_{m=1}^{k} l_m \leq 8\sqrt{q}$, dann erhöhe k um 1 und springe zu Schritt 2.

11. Schritt : Bestimme $a_1 \in \mathbb{Z}$, $|a_1| \leq 4\sqrt{q}$ nach dem Chinesischen Restsatz aus $a_1 \bmod l_1$, ..., $a_1 \bmod l_k$. Erhöhe anschließend ebenfalls k um 1.

12. Schritt : Analog zum 2. Schritt; aber in diesem Fall genügt die Indizierung der Ideale mit den Primzahlen l: $I_l := \langle F_1(X), F_2(X), \psi_l(X), \chi_l(X)\rangle$

13. Schritt : Wähle $\tilde{a}_2 \in \mathbb{F}_l$ und setze

$$r(t) := t^4 + a_1 t^3 + \tilde{a}_2 t^2 + a_1 q t + q^2 \ .$$

14. Schritt : Analog zum 4. Schritt mit a_1 anstelle von $\tilde{a}_1$.

15. Schritt : Analog zum 6. Schritt berechnen wir für $i = 1, ..., 4$ Normalformen

$$N(N(X_i^{q^4}) \cdot N(n)(X) - N(z_i)(X)) \bmod I_{l,j}$$

in Abhängigkeit von der gewählten Gröbner-Basis GB und testen, ob diese Polynome im Radikal $\sqrt{I_l}$ sind. Falls nicht, dann gehen wir zurück zu Schritt 13 und wählen ein neues $\tilde{a}_2$.

16. Schritt : Teste, ob $n(X) \in \sqrt{I_l}$ ist. Falls nicht, dann ist die Richtigkeit der Gleichung des 14. Schrittes bewiesen. In diesem Fall fahren wir bei Schritt 18 fort.

17. Schritt : Der Fall $n(X) \in \sqrt{I_l}$, den wir in diesem Schritt behandeln, wird wohl nur sehr selten auftreten. Wir verfahren analog zu Schritt 8, d.h. wir wenden den Satz von l'Hospital an. Das bedeutet die Ersetzung von $z_i(X)$ durch $D_\infty z_i(X)$, sowie $n(X)$ durch $D_\infty n(X)$. Das Ideal I_l wird in diesem Fall nicht verändert und wir springen zurück zu Schritt 15.

18. Schritt : An dieser Stelle ist bewiesen, daß ein $x \in (\mathrm{Jac}(C) - \Theta)[l]$ mit $r(\phi_l)x = 0$ existiert, d.h. $\mathrm{ch}_l(t) = r(t)$. Wieder bestimmen wir $a_2 \bmod l$ aus $\mathrm{ch}_l(t)$.

19. Schritt : Ist $\prod_{m=1}^{k} l_m \leq 12q$, dann erhöhe k um 1 und springe zu Schritt 12.

20. Schritt : Bestimme $a_2 \in \mathbb{Z}$, $|a_2| \leq 6q$ nach dem Chinesischen Restsatz aus $a_2 \bmod l_1$, ..., $a_2 \bmod l_k$.

□

Zum Abschluß bemerken wir noch, daß dieser Algorithmus auch terminiert und geben eine sehr grobe Laufzeitabschätzung an.

Satz 6.7 : *Algorithmus 6.6 terminiert, und die Anzahl elementarer Operationen, die höchstens benötigt werden, ist für $q \to \infty$ polynomial im Logarithmus von q.*

Beweis : Da nur endlich viele Primzahlen l benötigt werden, da ferner im 3. Schritt bzw. im 13. Schritt nur endlich viele Kandidaten $r(t)$ bereitgestellt werden, und da jede Nullstelle eines nichtverschwindenen Polynoms nur endliche Ordnung hat, terminiert der Algorithmus.

Die Anzahl der Primzahlen l, die in Schritt 2 bzw. Schritt 12 benötigt werden, ist $O(\log q)$, dabei ist jede dieser Primzahlen ebenfalls von der Größenordnung $O(\log q)$, so daß auch nur polynomial in $\log(q)$ viele Kandidaten $r(t)$ getestet werden müssen.

Aus den Rekursionsformeln von Satz 5.11 für ψ_l und χ_l folgt sofort, daß deren Grade nur die Größenordnung eines Polynoms in $\log(q)$ haben. Daher benötigt der Buchberger-Algorithmus zur Berechnung einer Gröbner-Basis, sowie zur Berechnung von Normalformen von Polynomen bzgl. dieser Gröbner-Basis, ebenfalls nur eine Laufzeit, die polynomial im Logarithmus von q ist, da alle auftretenden Ideale nulldimensional sind, siehe etwa [Giusti]. Dabei sollte allerdings an geeigneten Stellen die sogenannte "repeated squaring method" angewandt werden.

Wegen der Linearität des Frobenius-Endomorphismus ist die Ordnung eines l-Torsionspunktes als Nullstelle von $z_i(X)$ bzw. $n(X)$ höchstens polynomial in $\log(q)$, so daß auch nur polynomial in $\log(q)$ viele Anwendungen des Satzes von l'Hospital in den Schritten 7 bzw. 17 angewandt werden müssen.

Schließlich wird die Berechnung von a_1 und a_2 mit Hilfe des Chinesischen Restsatzes laufzeitmäßig von den vorhergehenden Schritten dominiert. Damit ist bewiesen, daß für $q \to \infty$ das Laufzeitverhalten von Algorithmus 6.6 polynomial in $\log(q)$ ist.

□

Literaturverzeichnis

[Adleman] Leonard M. Adleman & Ming-Deh A. Huang, "Recognizing Primes In Random Polynomial Time", Preprint, 1988.

[Bosch] Siegfried Bosch, Werner Lütkebohmert & Michel Raynaud, *Néron Models*, Springer-Verlag, Berlin, Heidelberg, 1990.

[Buchberger] Bruno Buchberger, "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory", *Multidimensional Systems Theory*, (N. K. Bose Ed.), Reidel, 1985.

[Cantor] David G. Cantor, "Computing in the Jacobian of a Hyperelliptic Curve", *Math. Comp.*, v. 48, 1987, pp. 95-101.

[Fay] John D. Fay, *Theta Functions on Riemann Surfaces*, Springer-Verlag, Berlin, 1973.

[Giusti] Marc Giusti, "Complexity of Standard Bases in Projective Dimension Zero", *Proc. EUROCAL 87, Leipzig, Juni 1987, Lecture Notes in Computer Science, Vol. 378.*

[Goldwasser] S. Goldwasser & J. Kilian, "Almost all primes can be quickly certified", *Proc. 18th Annual ACM Symp. on Theory of Computing*, 1986, pp. 316-329.

[Grant] David Grant, "Formal Groups in Genus Two", Preprint.

[Griffiths] Phillip Griffiths & Joseph Harris, *Principles of Algebraic Geometry*, Wiley, 1978.

[Hermann] Grete Hermann, "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale", *Math. Ann.*, v. 95, 1926, pp. 736-788.

[Igusa] Jun-ichi Igusa, "Fibre systems of Jacobian varieties I,II", *Amer. J. Math.*, v. 78, 1956, pp. 171-199 und 745-760.

[Koblitz] Neal Koblitz, "Hyperelliptic Cryptosystems", *J. Cryptology*, v. 1, 1989, pp. 139-150.

[Lang.1] Serge Lang, *Abelian Varieties*, Springer Verlag, New York, 1983.

[Lang.2] Serge Lang, *Introduction to Algebraic and Abelian Functions*, 2nd ed., Springer-Verlag, New York, 1982.

[Mayr] Ernst W. Mayr & Albert R. Meyer, "The Complexity of the Word Problems

for Commutative Semigroups and Polynomial Ideals", *Adv. Math.*, v. 46, 1982, pp. 305-329.

[Mumford] David Mumford, *Tata Lectures on Theta I, II*, Birkhäuser, Boston, 1983/1984.

[Pila] J. Pila, "Frobenius Maps of Abelian Varieties and Finding Roots of Unity in Finite Fields", *Math. Comp.*, v. 55, 1990, pp. 745-763.

[Robbiano] Lorenzo Robbiano, "Gröbner Bases: a foundation for Commutative Algebra", Tutorial Minicours, gehalten während der Tagung *Computers and Mathematics 1989* am MIT in Cambridge, Massachusetts.

[Schoof] René Schoof, "Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p", *Math. Comp.*, v. 44, 1985, pp. 483-494.

[Silverman] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[Swinnerton-Dyer] H.P.F. Swinnerton-Dyer, *Analytic Theory of Abelian Varieties*, Cambridge University Press, 1974.

[Tate] John Tate, "Endomorphisms of Abelian Varieties over Finite Fields", *Invent. Math.*, v. 2, 1966, pp. 134-144.

[Weber] Heinrich Weber, *Lehrbuch der Algebra, Vol. III*, Chelsea Publishing Company, New York, 1908.

[Weil] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.

[Wolfram] Stephen Wolfram, *Mathematica: A System for Doing Mathematics by Computer*, Addison-Wesley Publishing Company, 1988.