Additionsformeln für
Jacobi–Varietäten hyperelliptischer Kurven
via Theta–Relationen

Additionsformeln für Jacobi–Varietäten hyperelliptischer Kurven via Theta–Relationen

Gutachter:
Dr. Michael Hortmann
Prof. Dr. Jens Gamst

Diplomarbeit im Fachbereich Mathematik, Universität Bremen,
vorgelegt von Sönke Maseberg im Oktober 1998.

Inhaltsverzeichnis

Einleitung

Ein Grundwerkzeug für die Kryptographie sind endliche Körper sehr hoher Ordnung. Für das ursprüngliche Diffie–Hellman Schlüssel–Austausch Verfahren werden heutzutage Bitlängen von über 1024 benötigt, um die kryptographische Sicherheit zu gewährleisten. Werden hingegen elliptische Kurven für dieses Verfahren genutzt, so reichen 160 Bit bei gleicher Sicherheit und die kryptographischen Operationen sind entsprechend schneller. Diese Ersparnis ist wichtig bei Chipkartenanwendungen, bei der die Prozessoren relativ langsam sind und der Speicherplatz knapp ist. Die Gruppenordnung von Jacobi–Varietäten hyperelliptischer Kurven über endlichen Körpern wächst exponentiell mit dem Geschlecht der Kurven, so daß auf dem Diskreten Logarithmus Problem basierende kryptographische Verfahren bei kleinen Bitlängen besonders effektiv durchführbar sind.

Das Thema meiner Arbeit ist, eine Gruppenstruktur auf Jacobi–Varietäten hyperelliptischer Kurven zu erklären und entsprechende Additionsformeln zur Verfügung zu stellen, womit eine Basis für Kryptosysteme auf Jacobischen Varietäten geschaffen wäre. Obwohl bei diesen Anwendungen mit endlichen Körpern gerechnet wird, benötige ich zur Herleitung der Additionsformeln analytische Funktionen und damit den Körper der komplexen Zahlen. Die entstehenden rationalen Ausdrücke sind dann auch für endliche Körper sinnvoll.

Die Jacobische Varietät einer hyperelliptischen Kurve läßt sich durch Gleichungen beschreiben, die durch die Betrachtung reduzierter Divisoren auf der Kurve zustande kommen. Ein erster Zugang zu einer Additionsformel ist das Verfahren von Cantor, das durch Rückgriff auf die Divisordarstellung eine explizite Addition von Punkten auf der Jacobischen Varietät ermöglicht. Es gibt aber auch eine ganz andere Herleitung, die auf Mumford und Kampkötter zurückgeht.

Zu einer hyperelliptischen Kurve vom Geschlecht $g \geq 1$ wird ein Gitter Γ konstruiert, wodurch eine Isomorphie zwischen dem Torus $\mathbb{C}^g/\Gamma$ und der Jacobischen Varietät der Kurve hergestellt wird. Ziel ist es, die Funktionen zu finden, die den Torus auf die Varietät abbilden und die somit eine Arithmetik auf der Varietät durch die übertragene Gruppenstruktur des Torus erklären.

Aus der Theorie der elliptischen Kurven, also der hyperelliptischen Kurven vom Geschlecht 1, ist bekannt, daß die Weierstraßsche $\wp$–Funktion zusammen mit ihrer Ableitung einen komplex eindimensionalen Torus $\mathbb{C}/\Gamma$ auf die elliptische Kurve abbildet, auf der sich dadurch eine explizite Addition formulieren läßt. Da die elliptische Kurve eine spezielle Jacobi–Varietät ist, wird diese Strategie auf beliebiges Geschlecht $g \geq 1$ verallgemeinert. Es werden ϑ–Funktionen auf dem Torus $\mathbb{C}^g/\Gamma$ betrachtet, durch die sich die Weierstraßsche $\wp$–Funktion für Geschlecht 1 in der Weise verallgemeinern läßt, daß $\mathbb{C}^g/\Gamma$ durch $\wp$ und seine ersten $2g-1$ Ableitungen auf die Jacobi–Varietät abgebildet wird. Eine Additionsformel der ϑ–Funktion führt ob des Zusammenhangs mit $\wp$ zu Additionsformeln für $\wp, \wp', ..., \wp^{(2g-1)}$, wodurch die gewünschten expliziten Additionsformeln auf der Jacobi–Varietät entstehen. Da sich zu einem Punkt des Torus der entprechende Punkt der Varietät durch Auswerten von

$\wp$ und seinen Ableitungen nur mit Mühe finden läßt, werden Punkte der Varietät weiterhin durch die beschreibenden Gleichungen bestimmt. Zwei Punkte können als Koordinaten in $(\wp, \wp', ..., \wp^{(2g-1)})$ aufgefaßt und dadurch mit den Formeln addiert werden.

An der Stelle wäre ich gerne auf allgemeinere Abelsche Varietäten übergegangen und hätte dort eine Arithmetik entwickelt, doch leider fehlen dort die definierenden Gleichungen. Dadurch muß das Programm „Additionsfomeln für Abelsche Varietäten via Theta–Relationen“ in dieser Arbeit auf Jacobische Varietäten hyperelliptischer Kurven eingeschränkt werden.

Zur Struktur meiner Arbeit: Zunächst erläutere ich in Abschnitt 1 einige Grundlagen zu Jacobi–Varietäten hyperelliptischer Kurven und diskutiere anschließend den Fall $g = 1$: Elliptische Kurven und Weierstraßsche $\wp$–Funktionen. Es folgt eine Gliederung für das Vorgehen bei höherem Geschlecht. Dieser folgend definiere ich in Abschnitt 3 die ϑ–Funktion und leite eine Additionsformel für ϑ her, mit der sich in Abschnitt 4 die $\wp$–Funktion derart verallgemeinern läßt, daß $\wp, \wp', ..., \wp^{(2g-1)}$ den Torus $\mathbb{C}^g/\Gamma$ in den $\mathbb{C}^{2g}$ einbettet. In Abschnitt 5 wird die Additionsformel für $\wp$ zu einer Arithmetik für Jacobische Varietäten hyperelliptischer Kurven von beliebigem Geschlecht führen, die zu einem gegebenem Geschlecht konkret entwickelt werden müssen.

Ich werde die Theorie für beliebiges Geschlecht ausführen und stets beispielhaft die Situation für Geschlecht 1 und 2 schildern, was letztendlich in expliziten Additionsformeln für elliptische Kurven und für Jacobi–Varietäten hyperelliptischer Kurven von Geschlecht 2 münden wird, die ich in Abschnitt 6, im Rahmen der Diskussion der kryptographischen Anwendungen, auf einen endlichen Körper einschränken werde.

Die entstehenden expliziten Additionsformeln sind schon bei Geschlecht 2 derart umfangreich, daß die Unterstützung durch einen Computer unumgänglich ist, die ich darum bei einigen Umformungen und Beispielen auch in Anspruch genommen habe. So habe ich zum Beispiel auf die vollständigen Additionsformeln für Jacobi–Varietäten hyperelliptischer Kurven vom Geschlecht 2 verzichtet, da sich sonst die Seitenzahl mehr als verdoppelt hätte.

1 Grundlagen

In diesem Abschnitt möchte ich die im Titel „Additionsformeln für Jacobi–Varietäten hyperelliptischer Kurven via Theta–Relationen“ enthaltenen Begriffe erklären.

Ich werde die hyperelliptische Kurve einführen und Divisoren dazu definieren, die sich durch Polynome und Gleichungen charakterisieren lassen. Die Darstellung durch Gleichungen gestattet es, die Menge der Divisoren als affine Varietät zu betrachten, auf der sich eine Arithmetik durch Addition und Reduktion von Divisoren nach Cantor definieren läßt.

Ziel dieser Arbeit ist eine dazu alternative Addition via ϑ–Funktionen. Hierfür betrachte ich einen von der hyperelliptischen Kurve erzeugten Torus, der die Jacobische Varietät generiert.

Ich kann in diesem Abschnitt nur einen kurzen Streifzug durch die Grundlagen bieten, werde einige Fakten beweisen oder durch Beispiele untermauern, aber auch manche Tatsache nur zitieren. Für weitere Informationen verweise ich auf [Mumford 1975], [Mumford 1983], [Mumford 1984], [Fulton] und [Kampkötter].

1.1 Hyperelliptische Kurven und Divisoren

Definition 1
Eine **hyperelliptische Kurve** C **vom Geschlecht** g **über** $\mathbb{C}$ ist die Menge der Punkte $(x, y) \in \mathbb{C} \times \mathbb{C}$, welche die Gleichung

$$C: \; y^2 = f(x) \tag{1}$$

erfüllen, und der Punkt ∞, wobei $g \in \mathbb{N} - \{0\}$ und $f(x) \in \mathbb{C}[x]$ ein normiertes Polynom vom Grad $2g + 1$ ist und keine Lösungen $(x, y) \in \mathbb{C} \times \mathbb{C}$ existieren, die gleichzeitig (1), $2y = 0$ und $f'(x) = 0$ erfüllen.

$f(x)$ hat stets die Gestalt $f(x) = \prod_{i=1}^{2g+1}(x - a_i)$ mit paarweise verschiedenen Nullstellen $a_i \in \mathbb{C}$. Für Geschlecht $g = 1$ ist die hyperelliptische Kurve eine elliptische Kurve.

Alle endlichen Punkte $(x, y) \in C$, die also (1) erfüllen, sind glatt. Betrachte dazu die projektive Varietät, denn dort ist der Punkt ∞ die einzige Singularität: Sei $f(x) = x^{2g+1} + f_1 x^{2g} + ... + f_{2g+1}$ ohne mehrfache Nullstelle. Betrachte

$$F(X, Y, Z) = Z^{2g-1}Y^2 - X^{2g+1} - f_1 X^{2g} Z - ... - f_{2g+1} Z^{2g+1}$$

und die projektive Varietät

$$\mathbb{P}^2 = \{(X, Y, Z) \in \mathbb{C}^3 \mid F(X, Y, Z) = 0\},$$

die aus allen Äquivalenzklassen $(X, Y, Z) \sim (\lambda X, \lambda Y, \lambda Z)$, $\lambda \in \mathbb{C}$, $\lambda \neq 0$, $(X, Y, Z) \neq (0, 0, 0)$ besteht.

Für $Z \neq 0$ ist $(X,Y,Z) \sim (\frac{X}{Z}, \frac{Y}{Z}, 1) \sim (x,y,1)$. (x,y) erfüllt $y^2 = f(x)$, d.h. für $Z \neq 0$ besteht die projektive Varietät $\mathbb{P}^2$ aus allen Punkten, die (1) genügen.

Für $Z = 0$ muß zwingend $X = 0$ und $Y \neq 0$ sein, d.h. $(0,Y,Z) \sim (0,1,0)$, womit $(0,1,0)$ dem Punkt ∞ entspricht.

Betrachte die partiellen Ableitungen:

$$\frac{\partial F}{\partial X} = -(2g+1)X^{2g} - 2gf_1 ZX^{2g-1} - ... - f_{2g}Z^{2g},$$
$$\frac{\partial F}{\partial Y} = 2Z^{2g-1}Y,$$
$$\frac{\partial F}{\partial Z} = (2g-1)Y^2Z^{2g-2} - f_1X^{2g} - ... - (2g+1)f_{2g+1}Z^{2g}.$$

Für $(x,y,1) \in \mathbb{P}^2$ verschwinden die partiellen Ableitungen in keinem Punkt, aber für $(0,1,0) \in \mathbb{P}^2$ gilt $\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z}$. Also ist C glatt in allen endlichen Punkten $(x,y) \in C$ und nur in ∞ singulär.

Um den Punkt ∞ oder Umgebungen dazu zu betrachten, wird die folgende, zu C verwandte, Kurve betrachtet:

$$C^* \ : y^{*2} = x^* \prod_{i=1}^{2g+1} (1 - a_i x^*),$$

die $C - \{(0, \sqrt{f(0)}), (0, -\sqrt{f(0)}), \infty\}$ und $C^* - \{(0,0)\}$ über den Isomorphismus $x \longmapsto x^* = \frac{1}{x}$, $y \longmapsto y^* = \frac{y}{x^{g+1}}$ ineinander überführt. $x^* = y^* = 0$ auf C^* entspricht ∞ auf C.

Zusammenfassend läßt sich sagen, daß sich für alle endlichen Punkte das Modell C nutzen läßt, denn alle Punkte sind glatt. Nur um den Punkt ∞ selbst oder Umgebungen zu betrachten, wird auf C^* gewechselt, denn dort ist ∞ als $(0,0)$ in Koordinaten gegeben und der Punkt ist glatt.

Definition 2
Für eine hyperelliptische Kurve C vom Geschlecht $g \geq 1$ ist ein **Divisor** die formale endliche Summe

$$D = \sum_{P \in C} \alpha_P P,$$

wobei $\alpha_P \in \mathbb{Z}$ ist und nur endlich viele α_P von 0 verschieden sind.

Divisoren bilden ein Gruppe. Die Verknüpfung $+$ ist die folgende: Es wird für $D_1 = \sum_{P \in C} \alpha_P P$ und $D_2 = \sum_{P \in C} \beta_P P$ definiert: $D_1 + D_2 = \sum_{P \in C} (\alpha_P + \beta_P) P$. Das Nullelement sei $D = \sum_{P \in C} \alpha_P P$ mit $\alpha_P = 0$ für alle $P \in C$. Die Menge der Divisoren bilden mit dieser Verknüpfung eine abelsche Gruppe, die $Div\ C$ genannt wird.

Auf der Kurve C kann jedes Polynom $\tilde{g}(x,y) \in \mathbb{C}[x,y]$ wegen $y^2 = f(x)$ als **Funktion auf** C aufgefaßt und in der Form $g(x,y) = a(x) + yb(x)$ mit $a(x), b(x) \in \mathbb{C}[x]$ geschrieben werden.

Definition 3
Sei $g(x,y) = a(x) + yb(x) \in \mathbb{C}[x,y]$ eine Funktion auf C, $g \not\equiv 0$ und P ein Punkt der Kurve C. Die **Ordnung von** g **auf** P, bezeichnet mit $\mathrm{ord}_P\, g$ wird definiert durch:

i. Ist $P = (x_0, y_0)$ ein endlicher Punkt, so sei r die höchste Potenz von $(x - x_0)$, die $a(x)$ und $b(x)$ teilt, schreibe $g(x,y) = (x - x_0)^r (a_0(x) - yb_0(x))$. Ist $a_0(x_0) - y_0 b_0(x_0) \neq 0$, setze $s = 0$, sonst sei s die höchste Potenz von $(x - x_0)$, die $a_0(x)^2 - f(x) b_0(x)^2$ teilt. Ist $y_0 \neq 0$, d.h. $P \neq \neg P$, so definiere $\mathrm{ord}_P\, g = r + s$. Für $y_0 = 0$ definiere $\mathrm{ord}_P\, g = 2r + s$.

ii. Ist $P = \infty$, so setze $\mathrm{ord}_P\, g = -\max\{2 \deg a, 2g + 1 + 2 \deg b\}$.

Definition 4
Eine **rationale Funktion auf** C ist von der Form

$$f(x,y) = \frac{g(x,y)}{h(x,y)},$$

wobei $g, h \in \mathbb{C}[x,y], h \not\equiv 0$, Funktionen auf C sind.

Definition 5
Einer Funktion $f(x,y) \in \mathbb{C}[x,y]$ auf C, $f \not\equiv 0$, wird der **Divisor von** f zugeordnet:

$$\operatorname{div} f = \sum_{P \in C} \operatorname{ord}_P f \; P.$$

Ist f eine rationale Funktion auf C, so ist $\operatorname{div} f = \operatorname{div} \frac{g}{h} = \operatorname{div} g - \operatorname{div} h$.

Der **Grad eines Divisors** ist erklärt durch die Abbildung

$$\begin{aligned} \deg : \quad & Div\, C \quad \longrightarrow \mathbb{Z}, \\ & \sum_{P \in C} \alpha_P P \longmapsto \sum_{P \in C} \alpha_P. \end{aligned}$$

Die Menge der Divisoren vom Grad 0 bildet eine Untergruppe von $Div\, C$, die mit $Div_0\, C$ bezeichnet wird. Ein Divisor heißt **Hauptdivisor** , wenn es eine rationale Funktion f gibt mit $\operatorname{div} f = D$.
Der **größte gemeinsame Teiler** zweier Divisoren $\sum_{P \in C} \alpha_P P, \sum_{P \in C} \beta_P P \in Div_0\, C$ ist definiert durch $\operatorname{ggT}(\sum_{P \in C} \alpha_P P, \sum_{P \in C} \beta_P P) = \sum_{P \in C} \min(\alpha_P, \beta_P) P - \sum_{P \in C} \min(\alpha_P, \beta_P) \infty$.
Die Menge der Hauptdivisoren in $Div_0\, C$ bildet eine Untergruppe $\mathcal{H}$. Die Faktorgruppe

$$Pic_0\, C := Div_0 C / \mathcal{H},$$

heißt **Picardgruppe**. Sie besteht aus allen Äquivalenzklassen von Divisoren vom Grad 0 modulo Hauptdivisoren. Zwei Divisoren D_1, D_2 heißen demnach äquivalent, wenn $D_1 - D_2 \in \mathcal{H}$ gilt. Sie werden dann mit $D_1 \sim D_2$ bezeichnet.

Zu einem Punkt $P = (x_0, y_0)$ auf C ist auch der an der x–Achse gespiegelte Punkt $\neg P = (x_0, -y_0)$ ein Punkt der Kurve C. Die Funktion $x - x_0$ hat in P und $\neg P$ je eine Null– und in ∞ eine doppelte Polstelle, während der Punkt $P = (x_0, 0)$ eine doppelte Null– und Polstelle besitzt. Also gilt

$$\begin{aligned} & P + \neg P - 2 \cdot \infty \equiv 0 \mod \mathcal{H} \\ \Longleftrightarrow\ & P + \neg P \qquad \equiv 2 \cdot \infty \mod \mathcal{H}. \end{aligned}$$

Daraus folgt, daß jeder Repräsentant aus $Pic_0\, C$ eine Darstellung als

$$D = \sum_{i=1}^{\nu} P_i - \nu \cdot \infty$$

hat, wobei $\nu \geq 1$ beliebig, $P_i \neq \infty, P_i \neq \neg P_j$ für $i \neq j$ und $i, j = 1, ..., \nu$ ist. Eine solche Darstellung wird **semireduziert** genannt. Gilt zusätzlich $\nu \leq g$, so heißt die Darstellung **reduziert**.

Zwei weitere Beschreibungen von $Pic_0\, C$ gestatten es, einen Divisor durch Polynome und durch Gleichungen auszudrücken.

1.2 Darstellung eines Divisors durch Polynome und durch Gleichungen

Betrachte die Menge der semireduzierten Divisoren

$$Div_0^\nu C := \left\{ \sum_{i=1}^{\nu} P_i - \nu \cdot \infty \mid P_i \neq \infty,\ P_i \neq \neg P_j \text{ für } i \neq j \right\},$$

$\nu \in \mathbb{N} - \{0\}$ beliebig. Sei $D = \sum_{i=1}^{\nu} P_i - \nu \cdot \infty \in Div_0^\nu C$. Wie üblich erfüllen $P_i = (x_i, y_i)$ die Gleichung $y_i^2 = f(x_i)$. Ordne diesem Divisor D in einem ersten Schritt zwei Polynome zu:

$$\begin{aligned} u(t) &= \prod_{i=1}^{\nu}(t - x_i), \\ v(t) &= \sum_{i=1}^{\nu} y_i \frac{\prod_{j\neq i}(t - x_j)}{\prod_{j\neq i}(x_i - x_j)}. \end{aligned}$$

$u(t)$ ist normiert vom Grad ν und $v(t)$ ist das eindeutig bestimmte Polynom mit $v(x_i) = y_i$ für $i = 1, ..., \nu$ vom Grad $\leq \nu - 1$. Vielfachheiten werden berücksichtigt. Die Nullstellen von $u(t)$ sind: $x_1, ..., x_\nu$. Hieraus lassen sich berechnen:
$\mathrm{div}(u(t)) = \sum_{i=1}^{\nu_1}(x_i, y_i) + (x_i, -y_i) - 2\nu_1 \cdot \infty + \sum_{i=1}^{\nu_2}(x_i, 0) - \nu_2 \cdot \infty$, wobei $\nu_1 + \nu_2 = \nu$ ist und $\mathrm{div}(v(t) - s) = \sum_{(t,s)\in C} \alpha_{(t,s)}(t, s) - \alpha \cdot \infty$, wobei wegen der Endlichkeitsforderung genau α der $\alpha_{(t,s)}$ von 0 verschieden und alle $P_i \in D$ enthalten sind. Dann ist

$$\mathrm{ggT}(\mathrm{div}(u(t)), \mathrm{div}(v(t) - s)) = \sum_{i=1}^{\nu}(x_i, y_i) - \nu \cdot \infty = D$$

mit der Bezeichnung $D = \mathrm{div}(u(t), v(t))$.

Dabei gilt $u(t) \mid f(t) - v(t)^2$, da wegen $f(x_i) - v(x_i)^2 = 0$ und $u(x_i) = 0$ für $i = 1, ..., \nu$ sowohl $f(t) - v(t)^2$ als auch $u(t)$ dieselben Nullstellen haben. Ist $\deg(u(t)) \leq g$, so ist D reduziert.

In einem zweiten Schritt wird diese Konstruktion umgekehrt und zwei Polynomen eindeutig ein Divisor zugeordnet. Sei das Polynompaar $(u(t), v(t))$ gegeben mit $u(t) \mid f(t) - v(t)^2$ und sei $u(t)$ normiert vom Grad ν und $v(t)$ sei vom Grad $\leq \nu - 1$. Ordne ihnen einen Divisor D in folgender Weise zu:

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

wobei die x_i die Nullstellen von $u(t)$ sind und $y_i = v(x_i)$ gilt für $i = 1, ..., \nu$.

Diese Zuordnungen sind per Konstruktion invers zueinander, womit bewiesen ist:

$$\begin{aligned} Div_0^\nu C \ \cong\ P_\nu := \{(u_1, ..., u_\nu, v_1, ..., v_\nu) \mid\ & u(t) = t^\nu + u_1 t^{\nu-1} + ... + u_\nu, \\ & v(t) = v_1 t^{\nu-1} + ... + v_\nu, \\ & u(t) \mid f(t) - v(t)^2\} \subset \mathbb{C}^{2\nu}. \end{aligned}$$

Die Bedingung $u(t) \mid f(t) - v(t)^2$ läßt sich weiter ausnutzen. Dazu wird $\frac{f(t)-v(t)^2}{u(t)}$ durch Division mit Rest berechnet, wobei $f(t),\ u(t),\ v(t)$ Polynome der Form sind:

$$\begin{aligned} f(t) &= t^{2g+1} + f_1 t^{2g} + ... + f_{2g+1}, \\ u(t) &= t^\nu + u_1 t^{\nu-1} + ... + u_\nu, \\ v(t) &= v_1 t^{\nu-1} + ... + v_\nu. \end{aligned}$$

Sie implizieren

$$f(t) - v(t)^2 = u(t)\ \underbrace{(t^{2g+1-\nu} + B_0 t^{2g-\nu} + ... + B_{2g-\nu})}_{w(t)} + \underbrace{R_1 t^{\nu-1} + ... + R_\nu}_{Rest(t)},$$

wobei $w(t)$ ein Polynom vom Grad $2g + 1 - \nu$, $Rest(t)$ ein Polynom vom Grad $\leq \nu - 1$ und $B_0, ..., B_{2g-\nu}, R_1, ..., R_\nu \in \mathbb{C}[u_1, ..., u_\nu, v_1, ..., v_\nu]$ sind. Also ist P_ν isomorph zu

$$\begin{aligned}\{(u_1, ..., u_\nu, v_1, ..., v_\nu, w_0, ..., w_\nu) \mid u(t) &= t^\nu + u_1 t^{\nu-1} + ... + u_\nu,\\ v(t) &= v_1 t^{\nu-1} + ... + v_\nu,\\ w(t) &= t^{\nu+1} + w_0 t^\nu + ... + w_\nu,\\ f(t) - v(t)^2 &= u(t)\, w(t)\} \subset \mathbb{C}^{3\nu+1}\end{aligned}$$

und heißt auch (u, v, w)–Darstellung. Da das Polynom $u(t)$ den Term $f(t) - v(t)^2$ teilt, muß der Rest verschwinden und es ergeben sich ν Gleichungen in 2ν Variablen, nämlich $u_1, ..., u_g, v_1, ..., v_\nu$. Werden die $w_0, ..., w_g$ mit hinzu genommen, sind es $2\nu + 1$ Gleichungen in $3\nu + 1$ Variablen. Da sich die w_i aus den u_i und v_i in $g + 1$ Gleichungen berechnen lassen, gilt $P_\nu \subset \mathbb{C}^{2\nu} \subset \mathbb{C}^{3\nu+1}$.

Entscheidend an den Polynomen $u(t), v(t)$ und $w(t)$ sind die Koeffizienten $u_1, ..., u_\nu$, $v_1, ..., v_\nu$, $w_0, ..., w_\nu$. Die Unbestimmte t ist eher symbolisch in der Weise zu betrachten, daß die Nullstellen von $u(t)$ eingesetzt in $v(t)$ die entsprechenden Divisoren wiedergeben.

Ganz allgemein gilt:

Definition 6
Sei $\mathcal{P} \subset \mathbb{C}[x_1, ..., x_n]$ ein Primideal. Als **affine Varietät** $V \subset \mathbb{C}^n$ wird die Nullstellenmenge von $\mathcal{P}$ bezeichnet, d.h. $V = \{t \in \mathbb{C}^n \mid f(t) = 0 \text{ für alle } f \in \mathcal{P}\}$. Oft wird V auch mit $V(\mathcal{P})$ oder $V(f_1, ..., f_k)$ bezeichnet, wenn $f_1, ..., f_k$ das Ideal $\mathcal{P}$ erzeugen.

Die affine Varietät läßt sich daher auch durch den **affinen Ring** $R(V) = \mathbb{C}[x_1, ..., x_n]/(\mathcal{P})$ charakterisieren.

Im Sinne der Definition ist P_ν also eine ν–dimensionale affine Varietät, da sie von ν Gleichungen erzeugt wird:

$$\begin{aligned}(u_1, ..., u_\nu, v_1, ..., v_\nu) \in P_\nu \iff & R_1(u_1, ..., u_\nu, v_1, ..., v_\nu) = 0,\\ & \vdots\\ & R_\nu(u_1, ..., u_\nu, v_1, ..., v_\nu) = 0.\end{aligned}$$

Nach [Mumford 1984], 1.3 und 1.5 erzeugen $R_1, ..., R_\nu$ ein Primideal, womit $V(R_1, ..., R_\nu)$ als affine Varietät zu bezeichnen ist. Da P_ν isomorph zu $Div_0^\nu C$ ist, macht es Sinn, $Div_0^\nu C$ und damit $Pic_0\ C$ als Varietät zu bezeichnen:

$$\begin{aligned}Div_0^\nu C &\cong \{(u_1, ..., u_\nu, v_1, ..., v_\nu) \mid R_i(u_1, ..., u_\nu, v_1, ..., v_\nu) = 0 \text{ für } i = 1, ..., \nu\}\\ &\cong V(R_1, ..., R_\nu).\end{aligned}$$

Repräsentanten von $Pic_0\ C$, bzw. Elemente von $Div_0^\nu C$, lassen sich demnach durch Probieren oder mit einem Algorithmus aus den ν Gleichugen $R_1 = 0, ..., R_\nu = 0$ berechnen. Das Problem ist, eine Verknüpfung zu erklären, die zwei Elementen dasjenige Element zuzuordnet, das auf der Varietät liegt und durch die die Verknüpfung assoziativ und kommutativ wird. Ein erster Versuch dazu wird über die Addition von Divisoren beschritten.

1.3 Reduktionsalgorithmus von Cantor

Mit Hilfe des Satzes von Riemann–Roch läßt sich zeigen, daß sich jeder Repräsentant in $Pic_0\, C$ als reduzierter Divisor $D = \sum_{i=1}^{\nu} P_i - \nu \cdot \infty$, $P_i \neq \infty$, $P_i \neq \neg P_j$ für $i \neq j$ und $i, j = 1, ..., \nu$ mit $\nu \leq g$ darstellen läßt. Um einen semireduzierten Divisor zu reduzieren, nutze den

Reduktionsalgorithmus von Cantor
Sei D ein semireduzierter Divisor der Form $D = \sum_{i=1}^{\nu} P_i - \nu \cdot \infty$ mit $P_i \neq \infty$, $P_i \neq \neg P_j$ für $i \neq j$ und $i, j = 1, ..., \nu$, sowie $\nu \geq 1$ beliebig gegeben.

i. Ist $\nu \leq g$, so ist D bereits reduziert.

ii. Ist $\nu > g$, so existieren Polynome $u^*(t), v^*(t)$ mit $D = \operatorname{div}(u^*(t), v^*(t))$. Konstruiere dazu für $P_i = (x_i, y_i)$, $i = 1, ..., \nu$: $u^*(t) = \prod_{i=1}^{\nu}(t - x_i)$ und $v^*(t)$ so, daß $v^*(x_i) = y_i$ gilt. Setze

$$\begin{aligned} u_{neu}(t) &= \frac{f(t) - v^*(t)^2}{u^*(t)}, \\ v_{neu}(t) &\equiv -v^*(t) \mod u_{neu}(t). \end{aligned}$$

Dann ist $\deg v_{neu}(t) < \deg u_{neu}(t)$.

iii. Wiederhole diesen Reduktionsschritt, bis $\deg u_{neu}(t) \leq g$.

iv. Dann ist

$$D_{neu} = \operatorname{div}(u_{neu}(t), v_{neu}(t)) = \sum_{i=1}^{\mu} Q_i - \mu \cdot \infty,\ \mu \leq g,$$

der reduzierte Divisor mit $D_{neu} \equiv D \mod \mathcal{H}$. Dabei sind für die Punkte $Q_i = (x_i, y_i)$ die $x_1, ..., x_\mu$ die Nullstellen von $u_{neu}(t)$ und $y_i = v(x_i)$ für $i = 1, ..., \mu$.

Die Repräsentanten in $Pic_0\, C$ mit $\nu < g$ werden mit Θ bezeichnet, so daß $Pic_0\, C - \Theta$ Repräsentanten der Form hat:

$$\sum_{i=1}^{g} P_i - g \cdot \infty,\ P_i \neq \infty,\ P_i \neq \neg P_j \text{ für } i \neq j \text{ und } i, j = 1, ..., g.$$

Beispiel 1 ($g = 1$)
Jedem endlichen Punkt $P = (x, y) \in C$ entspricht eindeutig ein Divisor $D = P - \infty \in Pic_0\, C$. Also ist

$$\begin{aligned} Pic_0\, C - \Theta &\cong \{P - \infty \mid P \in C, P \neq \infty\}, \\ \Theta &\cong \{\infty\}. \end{aligned}$$

Ein Divisor $D \in Pic_0\, C - \Theta$ läßt sich charakterisieren:

i. als Polynompaar: $D = \operatorname{div}(u(t), v(t))$ mit $u(t) = (t - x)$ und $v(t) = y$,

ii. als Punkt der Varietät: $D = (u_1, v_1) \in V(R_1)$;

dazu wird $\frac{f(t)-v(t)^2}{u(t)}$ via Division mit Rest ausgerechnet. Mit der Gleichung für die elliptische Kurve $f(t) = t^3 + at + b$, $u(t) = t + u_1$, $v(t) = v_1$ folgt aus $f(t) - v(t)^2 \;=\; u(t) \cdot w(t) + Rest(t)$:

$$\begin{aligned} w(t) &= t^2 - u_1 t + (a + u_1^2), \\ Rest(t) &= -u_1^3 - au_1 + b - v_1^2. \end{aligned}$$

Also ist $(u_1, v_1) \in Pic_0\, C - \Theta \iff R_1(u_1, v_1) = 0 \iff v_1^2 = -u_1^3 - au_1 + b$.

Beispiel 2 ($g = 2$)

$$\begin{aligned} Pic_0\, C &\cong \left\{ \sum_{i=1}^{\nu} P_i - \nu \cdot \infty \mid P_i \neq \neg P_j \text{ für } i \neq j,\ P_i \neq \infty,\ 1 \leq i,j \leq \nu,\ \nu = 1,2 \right\}, \\ Pic_0\, C - \Theta &\cong \{P_1 + P_2 - 2 \cdot \infty \mid P_1 \neq \neg P_2, P_1, P_2 \neq \infty\}, \\ \Theta &\cong \{P - \infty \mid P \neq \infty\}. \end{aligned}$$

Für einen Divisor $D \in Pic_0\, C - \Theta$ gibt es drei verschiedene Darstellungen:

i. als reduzierter Divisor: $D = P_1 + P_2 - 2 \cdot \infty$ mit $P_i = (x_i, y_i),\ i = 1, 2$,

ii. als Polynompaar: $D = \operatorname{div}(u(t), v(t))$ mit
$u(t) = (t - x_1)(t - x_2) = t^2 + (-x_1 - x_2)t + x_1 x_2$,
$v(t) = y_1 \frac{t - x_2}{x_1 - x_2} - y_2 \frac{t - x_1}{x_1 - x_2}$,

iii. als Punkt der Varietät: $D = (u_1, u_2, v_1, v_2) \in V(R_1, R_2)$,

mit einer Berechnung von $\frac{f(t)-v(t)^2}{u(t)}$ via Division mit Rest: Seien

$$\begin{aligned} f(t) &= t^5 + f_1 t^4 + f_2 t^3 + f_3 t^2 + f_4 t + f_5, \\ u(t) &= t^2 + u_1 t + u_2, \\ v(t) &= v_1 t + v_2. \end{aligned}$$

Dann ist $f(t) - v(t)^2 \;=\; u(t) \cdot w(t) + Rest(t)$ mit

$$\begin{aligned} w(t) &= t^3 + (f_1 - u_1)t^2 + (f_2 - u_2 - u_1 f_1 + u_1^2)t \\ &\quad + f_3 - v_1^2 - u_2 f_1 + 2u_1 u_2 - u_1 f_2 + u_1^2 f_1 - u_1^3, \\ Rest(t) &= (-3u_1^2 u_2 + u_1 v_1^2 - u_1^3 f_1 - u_1 f_3 + f_4 + u_1^2 f_2 \\ &\quad - 2v_1 v_2 + u_1^4 - u_2 f_2 + u_2^2 + 2u_1 u_2 f_1)t \\ &\quad - u_2 f_3 + f_5 + u_2^2 f_1 - v_2^2 + u_1 u_2 f_2 - u_1^2 u_2 f_1 + u_1^3 u_2 - 2u_1 u_2^2 + u_2 v_1^2. \end{aligned}$$

$Rest(t)$ ist ein Polynom vom Grad 1 und verschwindet, da die Division aufgeht, wodurch die beiden Gleichungen

$$\begin{aligned} R_1(u_1, u_2, v_1, v_2) &= -3u_1^2 u_2 + u_1 v_1^2 - u_1^3 f_1 - u_1 f_3 + f_4 + u_1^2 f_2 - 2v_1 v_2 + u_1^4 - u_2 f_2 \\ &\quad + u_2^2 + 2u_1 u_2 f_1, \\ R_2(u_1, u_2, v_1, v_2) &= -u_2 f_3 + f_5 + u_2^2 f_1 - v_2^2 + u_1 u_2 f_2 - u_1^2 u_2 f_1 + u_1^3 u_2 - 2u_1 u_2^2 + u_2 v_1^2 \end{aligned}$$

gefunden sind. R_1 und R_2 sind Ideale und sogar Primideale, welche den affinen Ring der Varietät beschreiben. Also ist $(u_1, u_2, v_1, v_2) \in Pic_0 C - \Theta \iff R_1(u_1, u_2, v_1, v_2) = R_2(u_1, u_2, v_1, v_2) = 0$.

Beispiel 3
Sei $C\ :\ y^2 = 4x^3 - 144x$ eine elliptische Kurve vom Geschlecht 1. Betrachte die beiden Punkte $P_1 = (-2, -16)$, $P_2 = (6, 0)$ sowie die Divisoren $D_1 = (-2, -16) - \infty$, $D_2 = (6, 0) - \infty$ dazu. Der zusammengesetzte Divisor $D = D_1 + D_2 = (-2, -16) + (6, 0) - 2 \cdot \infty$ ist bereits semireduziert. Wende Cantor zur Reduktion an:

$$\begin{aligned} u^*(t) &= (t+2)(t-6) = t^2 - 4t - 12, \\ v^*(t) &= -16\frac{t-6}{-2-6} = 2t - 12. \end{aligned}$$

Berechne

$$\begin{aligned} u_{neu}(t) &= \frac{f(t) - v^*(t)^2}{u^*(t)} = 4t + 12, \\ v_{neu}(t) &= -2t + 12. \end{aligned}$$

Damit repräsentiert $(u_{neu}(t), v_{neu}(t))$ den Divisor D. Bestimme die Nullstelle von $u_{neu}(t)$: $x = -3$ und $y = v(-3) = 18$. Damit ist $D = (-3, 18) - \infty$.

Beispiel 4
Betrachte die hyperelliptische Kurve $C\ :\ y^2 = x^5 + 2x^3 + 5x^2 + 6x + 3$ vom Geschlecht 2 und die beiden Punkte $P \approx (-10, 9, -31.3803, 35.5034)$, $Q \approx (0, 5, -2.7176, -3.8636)$, die ich näherungsweise angebe.

Stelle nun P und Q als Divisoren dar. Für P ist $u(t) = t^2 - 10t + 9$, $v(t) = -31.3803t + 35.5034$. Die Nullstellen von $u(t)$ sind $x_1 = 1$, $x_2 = 9$ und die zugehörigen y–Koordinaten berechnen sich über $v(t)$: $y_1 = v(x_1) = 4.1231$, $y_2 = v(x_2) = -246.9190$: $P \approx (1, 4.1231) + (9, -246.9190) - 2 \cdot \infty$. Ganz analog läßt sich finden: $Q \approx (\sqrt{5}i, -3.8636 - 6.0768i) + (-\sqrt{5}i, -3.8636 + 6.0768i) - 2 \cdot \infty$.

Addiere die beiden Divisoren: $P + Q$
$\approx (1, 4.1231) + (9, -246.9190) + (\sqrt{5}i, -3.8636 - 6.0768i) + (-\sqrt{5}i, -3.8636 + 6.0768i) - 4 \cdot \infty$.
Dieser Divisor ist bereits semireduziert, nutze nun Cantor zur Reduktion:

$$\begin{aligned} u^*(t) &= (t-1)(t-9)(t)(t-5) = t^4 - 10t^3 + 14t^2 - 50t + 45, \\ v^*(t) &\approx -0.5407t^3 + 2.3248t^2 - 5.4213t + 7.7604, \\ \Longrightarrow\ u_{neu}(t) &\approx -0.2934\,(t^2 - 2.0187t + 4.3490), \\ v_{neu}(t) &\approx 0.5802t - 2.3971. \end{aligned}$$

Daraus folgt $P + Q \approx (-2.0187, 4.3490, 0.5812, -2.3971)$ als Punkt der Varietät. Um eine Darstellung als reduzierter Divisor zu erhalten, berechne die Nullstellen von $u_{neu}(t)$ und setze diese Nullstellen in $v_{neu}(t)$ ein. Es folgt
$P + Q \approx (1.0093 - 1.8249i, -1.8115 - 1.0587i) + (1.0093 + 1.8249i, -1.8115 + 1.0587i) - 2 \cdot \infty$.

1.4 Restriktion auf eine partielle Addition

In dieser Arbeit wird eine Addition auf $Pic_0\, C$ entwickelt, die Theta–Relationen nutzt und damit eine Alternative zur Divisoraddition und –reduktion darstellt. Dieser Abschnitt zeigt, daß es reicht, sich auf $Pic_0\, C - \Theta$ zu beschränken und eine Addition hierauf zu erklären.

Für $D, E \in Pic_0\, C - \Theta$ wird eine partielle Addition entwickelt, die $D + E$ berechnet, sofern $D + E \notin \Theta$ liegt. Falls dies nicht der Fall ist oder $D + E$ mit $D \in \Theta$ und $E \in Pic_0\, C - \Theta$ berechnet werden soll, wird folgender Trick angewandt:

Identifiziere die Nullstellen $a_1, ..., a_{2g+1}$ des Polynoms f mit den Weierstraßpunkten $P_i = (a_i, 0)$: $a_i \longleftrightarrow P_i$. Betrachte die P_i und $\infty =: a_{2g+2}$ mit der Indexmenge $B = \{1, 2, ..., 2g+2\}$. Für alle Weierstraßpunkte P_i gilt $P_i = \neg P_i$. Betrachte die Divisorklasse vom Grad 2, die $P + \neg P$ für alle $P \in C$ enthält. Sie hat einen Repräsentant $2 \cdot \infty$. Definiere dazu die Divisorklasse mit dem Repräsentanten

$$e_T = \sum_{i \in T} P_i - \sharp\, T \cdot \infty \in Pic_0\, C,$$

wobei $T \subseteq B$, $\sharp\, T \in 2\mathbb{Z}$ und $\sharp\, T$ die Anzahl der Elemente von T sei. Die Repräsentanten e_T haben die folgenden Eigenschaften:

i. $2\, e_T = 0$,

ii. $e_{T_1} + e_{T_2} = e_{T_1 \circ T_2}$ mit der Verknüpfung $T_1 \circ T_2 = (T_1 \cup T_2) - (T_1 \cap T_2)$,

iii. $e_{T_1} = e_{T_2} \Longleftrightarrow T_1 = T_2$ oder $T_1 = \mathcal{C}T_2$, wobei $\mathcal{C}T$ das Komplement von T in B ist.

Der folgende Satz zeigt, daß sich $Pic_0\, C$ mit affinen Stücken isomorph zu Z_g überdecken läßt. Im Beweis wird zu einem Divisor $D \in Pic_0\, C$ ein e_T konstruiert, so daß $D \in (Pic_0\, C - \Theta) + e_T$ ist.

Satz 1
Sei $B = \{1, 2, ..., 2g+2\}$ die Indexmenge der Weierstraßpunkte mit ∞ und $V = \{2, 4, ..., 2g+2\}$ die Teilmenge der geraden Zahlen in B. Dann gilt

$$\bigcup_{T \subseteq V,\, \sharp\, T \in 2\mathbb{Z}} (Pic_0\, C - \Theta) + e_T = Pic_0\, C,$$

wobei „+“ die Addition von Divisoren bedeutet.

Beweis „$\subset$“: $D = \sum_{i=1}^{g} P_i - g \cdot \infty + \sum_{i \in T} P_i - \sharp\, T \cdot \infty = \sum_{i=1}^{\nu} P_i^* - \nu \cdot \infty \in Pic_0\, C$ mit dem Reduktionsverfahren von Cantor und $\nu \leq g$.

„$\supset$“: $D = \sum_{i=1}^{\nu} P_i - \nu \cdot \infty \in Pic_0\, C, \nu \leq g$. Für $\nu = g$ ist nichts zu zeigen. Sei also $\nu \neq g$:

Wähle Weierstraßpunkte $R_1 = (a_1, 0), ..., R_{g-\nu} = (a_{g-\nu}, 0)$, die von den P_i verschieden sind mit geraden Indizes $i_1, ..., i_{g-\nu} \in V - \{2g-2\}$. Das ist möglich, da es g gerade Indizes in B gibt. Es ist

$$\begin{aligned} D + \sum_{i=1}^{g-\nu} R_i - (g-\nu) \cdot \infty &= \sum_{i=1}^{\nu} P_i - \nu \cdot \infty + \sum_{i=1}^{g-\nu} R_i - (g-\nu) \cdot \infty \\ &= \sum_{i=1}^{\nu} P_i + \sum_{i=1}^{g-\nu} R_i - g \cdot \infty \in Pic_0\, C - \Theta. \end{aligned}$$

Folglich ist $D \in (Pic_0\, C - \Theta) + e_T$ mit $T = \begin{cases} i_1, ..., i_{g-\nu}, & \text{falls } g-\nu \text{ gerade,} \\ i_1, ..., i_{g-\nu}, 2g+2, & \text{falls } g-\nu \text{ ungerade.} \end{cases}$

$\square$

Ist nun $E \in \Theta$, so berechne $E = E + \underbrace{(e_T + e_T)}_{0} = (\underbrace{E + e_T}_{\in Pic_0\, C - \Theta}) + e_T$. Damit ist für $D \in Pic_0\, C - \Theta$: $D + E = (D + (E + e_T)) + e_T$. Da D und $E + e_T$ aus $Pic_0\, C - \Theta$ sind, wird hier die noch zu entwickelnde Addition auf $Pic_0\, C - \Theta$ angewandt und die letzte Addition $+e_T$ wird mit Cantor ausgeführt.

Beispiel 5 ($g = 2$)
Sei $E = (x_E, y_E) - \infty \in \Theta$. Betrachte $e_T = (a_R, 0) - \infty$ und $E + e_T = (x_E, y_E) + (a_R, 0) - 2 \cdot \infty$. Konstruiere Polynome $u(t), v(t)$:

$$u(t) = (t - x_E)(t - a_R) = t^2 + (-x_E - a_R)t + x_E a_R \ ,$$
$$v(t) = y_E \frac{t - a_R}{x_E - a_R} = \frac{y_E}{x_E - a_R} t \ - \frac{y_E a_R}{x_E - a_R}.$$

Damit ist $E + e_T = (-x_E - a_R, x_E a_R, \frac{y_E}{x_E - a_R}, -\frac{y_E a_R}{x_E - a_R}) \in Pic_0\ C - \Theta$ und läßt sich zu einem $D \in Pic_0\, C - \Theta$ partiell addieren. Unter der Annahme, am Ende dieser Arbeit eine partielle Addition zu erhalten, sei $(\zeta_1, \zeta_2, \zeta_3, \zeta_4) \in Pic_0\ C - \Theta$ das Ergebnis und x_1 und x_2 seien die Nullstellen von $u(t) = t^2 + \zeta_1 t + \zeta_2$, $v(t) = \zeta_3 t + \zeta_4$. Dann ist $D + E + e_T = (x_1, v(x_1)) + (x_2, v(x_2)) - 2 \cdot \infty$. Berechne schließlich mit Reduktionsverfahren von Cantor: $D + E = D + E + e_T + e_T = (x_1, v(x_1)) + (x_2, v(x_2)) + (a_R, 0) - 3 \cdot \infty = (x_1^*, y_1^*) + (x_2^*, y_2^*) - 2 \cdot \infty \in Pic_0\, C$. Für $D + D' \in \Theta$ wird analog $(D + (D' + e_T)) + e_T$ berechnet.

Die Vorstellung, eine partielle Addition auf $Pic_0\, C - \Theta$ mit ϑ–Funktionen alternativ zur Divisoraddition zu entwickeln, in der bei einigen Additionen das Additions– und Reduktionsverfahren von Cantor bemüht werden muß, scheint unbefriedigend zu sein. Es scheint, als ob das Konzept des Addierens und Reduzierens von Divisoren dem der ϑ–Funktionen überlegen ist. Dennoch ist es sinnvoll, eine partielle Addition zu entwickeln, denn für Anwendungen wird auf einem endlichen Körper gerechnet und ein zufälliges Element aus $Pic_0\ C$ liegt nur mit sehr geringer Wahrscheinlichkeit in Θ.

Für die Anzahl der Punkte auf einem endlichen Körper $\mathbb{F}_q$, $q = p^r$, p prim, $r \in \mathbb{N} - \{0\}$, gilt

$$|Pic_0\ C| \approx q^g,$$
$$|\Theta| \approx q^{g-1}.$$

Ein zufälliger Punkt aus $Pic_0\ C$ liegt nur mit einer Wahrscheinlichkeit von q^{-1} in Θ. Bei einer Größenordnung des endlichen Körpers von $q \approx 2^{100} \approx 10^{30}$ ist diese Wahrscheinlichkeit bei Geschlecht 2 nur 10^{-30}, wodurch die partielle Addition für Anwendungen völlig ausreicht.

1.5 Jacobi–Varietät einer hyperelliptischen Kurve

In diesem Abschnitt werde ich die Jacobische Varietät einer hyperelliptischen Kurve definieren. Für nähere Details verweise ich auf die Arbeiten von Mumford und Bost ([Mumford 1983], II, §2, [Mumford 1984], IIIa, §5 und [Bost]).

Eine hyperelliptische Kurve C läßt sich als kompakte zusammenhängende Riemannsche Fläche auffassen. Sei g das Geschlecht von C. Die erste Homologiegruppe von C, $H_1(C, \mathbb{Z})$, ist eine abelsche Gruppe mit $2g$ Erzeugern. Als Erzeugende werden in C geschlossene Kurven $A_1, ..., A_g, B_1, ..., B_g$ gewählt, so daß sich die Kurven A_i und A_j, B_i und B_j oder A_i und B_j für $i \neq j$ nie, aber A_i und B_i in genau einem Punkt schneiden. Darüber hinaus können die Kurven A_i und B_j in Beziehung zu den Weierstraßpunkten $a_1, ..., a_{2g+2}$ konstruiert werden, was hier am Beispiel $g = 2$ in Abbildung 1 gezeigt werden soll:

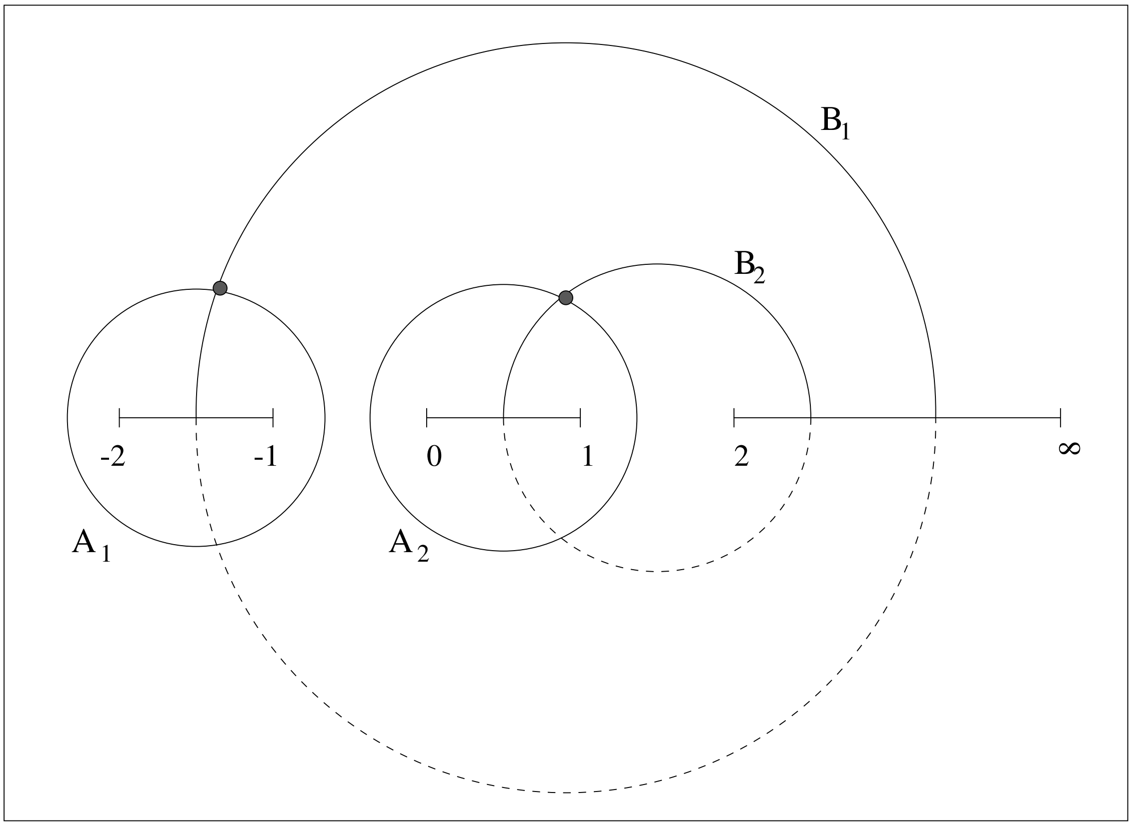

Abbildung 1: Beispiel für die Wahl der Kurven A_1, A_2, B_1, B_2 in Beziehung zu den Weierstraßpunkten $-2, -1, 0, 1, 2, \infty$ für $g = 2$

Sei der Vektorraum der holomorphen Differentiale von C mit $\Omega_1(C)$ bezeichnet. Jedes $\omega \in \Omega_1(C)$ hat die Form $\omega = P(x)\frac{dx}{y}$, mit einem Polynom $P(x)$ vom Grad $\leq g-1$. Ein Beweis dazu findet sich bei [Mumford 1984], IIIa, 5.2. Es läßt sich dann eine Basis $\omega_1, ..., \omega_g$ von $\Omega_1(C)$ finden, so daß

$$\int\limits_{A_i} \omega_j = \delta_{ij}$$

gilt. Es wird dann definiert:

$$\Omega_{ij} := \int\limits_{B_i} \omega_j \text{ und } \Omega := (\Omega_{ij})_{i,j=1,...,g}.$$

Ω ist eine symmetrische $(g \times g)$–Matrix mit positiv definitem Imaginärteil, d.h. Ω ist Element der **oberen Siegelschen Halbebene** $\mathbb{H} = \{A \in GL_g(\mathbb{C}) \mid A^t = A,\ \mathrm{Im}\ A \text{ positiv definit}\}$. Hieraus wird definiert:

Definition 7
Der **Jacobi–Torus von** C ist definiert durch

$$T_C = \mathbb{C}^g/\Gamma$$

mit $\Gamma = \mathbb{Z}^g + \Omega\mathbb{Z}^g,\ \Omega \in \mathbb{H}$.

Die Verbindung zur Picardgruppe $Pic_0\ C$ wird durch den Satz von Abel hergestellt.

Satz 2 (Satz von Abel)
Sei $D = \sum_{i=1}^{\nu} P_i - \nu \cdot \infty$ ein Divisor vom Grad 0 auf $Pic_0\, C$, $\nu \geq 1$. Dann ist

$$\begin{aligned} \Phi : Pic_0\, C &\longrightarrow T_C, \\ \sum_{i=1}^{\nu} P_i - \nu \cdot \infty &\longmapsto \sum_{i=1}^{\nu} \int_{\infty}^{P_i} \omega \quad \mathrm{mod}\ \Gamma,\ \omega = (\omega_1, ..., \omega_g)^t. \end{aligned}$$

wohldefiniert und ein Isomorphismus.

Ein Beweis dazu ist unter anderem bei [Bost], II.3.2, zu finden.

Durch diesen Isomorphismus läßt sich die Picardgruppe $Pic_0\, C$ mit dem Jacobi–Torus T_C identifizieren, d.h.

$$\begin{aligned} &Pic_0\, C \cong T_C, \\ &Div_0^g C \cong Pic_0\, C - \Theta \cong T_C - \Phi(\Theta). \end{aligned}$$

Betrachte $Pic_0\, C - \Theta$ in der Darstellung:

$$\begin{aligned} Pic_0\, C - \Theta \cong \{(u_1, ..., u_g, v_1, ..., v_g) \mid\ & u(t) = t^g + u_1 t^{g-1} + ... + u_g, \\ & v(t) = v_1 t^{g-1} + ... + v_g, \\ & u(t) \mid f(t) - v(t)^2\}. \end{aligned}$$

Die Koeffizienten $u_1, ..., u_g, v_1, ..., v_g$ können demnach als komplexe Funktionen auf $T_C - \Phi(\Theta)$ aufgefaßt werden. Sie sind sogar holomorph und lassen sich meromorph auf den gesamten Torus fortsetzen, ergeben also eine holomorphe Einbettung von $T_C - \Phi(\Theta)$ in den $\mathbb{C}^{2g}$.

Die Kompaktifizierung dieser g–dimensionalen eingebetteten Mannigfaltigkeit wird üblicherweise die **Jacobi–Varietät der hyperelliptischen Kurve** C, $Jac\,C$, genannt. Es ergibt sich ein analytischer Isomorphismus

$$T_C \longrightarrow Jac\, C,$$

wobei $T_C - \Phi(\Theta)$ der affinen Untermannigfaltigkeit entspricht, die natürlicherweise $Jac C - \Theta$ heißt.

Ziel ist nun eine genauere analytische Beschreibung dieser einbettenden Funktionen. Dazu wird in Abschnitt 2.1 illustriert, daß es sich im Fall $g = 1$ gerade um die Weierstraßschen Funktionen $\wp$ und $\wp'$ handelt. Diese Funktionen gehen durch Differentialoperationen aus einer ϑ–Funktion hervor. Dieses Vorhaben läßt sich auch für höheres Geschlecht durchführen.

Die Additionsformeln für die ϑ–Funktion werden auf die gesuchten Additionsformeln für $Jac C - \Theta$ führen. Dazu wird ein spezieller Differentialoperator benötigt.

1.6 Spezieller Differentialoperator

Die Jacobische Varietät $Jac\, C$ läßt sich durch die (u, v, w)–Darstellung auf $Pic_0\, C$ und durch den Torus $\mathbb{C}^g/\Gamma$ charakterisieren. In diesem Abschnitt wird eine spezielle Derivation auf der Varietät eingeführt. Dieser entspricht mittels der durch den Satz von Abel gegebenen Isomorphie eine Derivation auf dem Torus.

Das dieser Derivation entsprechende Vektorfeld X auf $Pic_0\, C$ entsteht durch Parallelverschiebung eines Tangentialvektors im Punkt ∞ der ursprünglichen hyperelliptischen Kurve C, die eine eindimensionale Untermannigfaltigkeit von $Pic_0\, C$ ist. Dieses invariante Vektorfeld X ist offensichtlich bis auf ein skalares Vielfaches eindeutig bestimmt. Die folgenden Sätze geben die Gestalt von X auf dem Torus und in der (u, v, w)–Darstellung an.

Satz 3 ([Mumford 1984], IIIa, 5.10)
Sei $\omega_i = (h_i x^{g-1} + ...)\frac{dx}{y}$ für $i = 1, ..., g$ die normierte Basis von $\Omega_1(C)$ aus 1.5. Das invariante Vektorfeld X hat auf $T_C = \mathbb{C}^g/\Gamma$ die Form:

$$X(z_1, ..., z_g) = (-h_1, ..., -h_g).$$

Damit wirkt der zugehörige Differentialoperator D auf eine Funktion $f : \mathbb{C}^g/\Gamma \longrightarrow \mathbb{C}$ wie folgt:

$$\mathrm{D}\, f = -\sum_{i=1}^{g} h_i \frac{\partial f}{\partial z_i}$$

und $f'(z) = \mathrm{D}\, f(z)$ heißt auch **Ableitung** von f.

Satz 4 ([Mumford 1984], IIIa, §3)
Auf $Pic_0\, C - \Theta$ hat das invariante Vektorfeld X die Form:

$$X(u_1, ..., u_g, v_1, ..., v_g, w_0, ..., w_g) = (u'_1, ..., u'_g, v'_1, ..., v'_g, w'_0, ..., w'_g)$$

mit

$$\begin{aligned}
u'_i &= v_i, \text{ für } i = 1, ..., g,\\
v'_i &= \frac{1}{2}(-w_i + u_{i+1} - u_1 u_i + w_0 u_i), \text{ für } i = 1, ..., g-1,\\
v'_g &= \frac{1}{2}(-w_g - u_1 u_g + w_0 u_g),\\
w'_0 &= -v_1,\\
w'_i &= -v_{i+1} + u_1 v_i - w_0 v_i, \text{ für } i = 1, ..., g-1,\\
w'_g &= u_1 v_g - w_0 v_g.
\end{aligned}$$

Der zugehörige Differentialoperator D wirkt damit auf eine Funktion g
auf $\mathbb{C}[u_1, ..., u_g, v_1, ..., v_g, w_0, ..., w_g]/(\text{Abhängigkeiten der } u_i, v_j, w_k)$ folgendermaßen:

$$\mathrm{D}\, g = \left(\sum_{i=1}^{g} u'_i \frac{\partial}{\partial u_i} + \sum_{i=1}^{g} v'_i \frac{\partial}{\partial v_i} + \sum_{i=0}^{g} w'_i \frac{\partial}{\partial w_i} \right) g,$$

wobei die Abhängigkeiten zwischen den u_i, v_j, w_k wie erwähnt dadurch zustande kommen, daß für die daraus gebildeten Polynome

$$\begin{aligned}
u(t) &= t^g + u_1 t^{g-1} + ... + u_g,\\
v(t) &= v_1 t^{g-1} + ... + v_g,\\
w(t) &= t^{g+1} + w_0 t^{g-1} + ... + w_g
\end{aligned}$$

gilt:

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

Beispielsweise erzielt der Differentialoperator D auf $u(t), v(t)$ und $w(t)$ folgenden Wirkungen:

$$\begin{aligned}
\mathrm{D}\,u(t) &= \left(\sum_{i=1}^{g} u_i' \frac{\partial}{\partial u_i} \;+\; \sum_{i=1}^{g} v_i' \frac{\partial}{\partial v_i} \;+\; \sum_{i=0}^{g} w_i' \frac{\partial}{\partial w_i}\right) \big(t^g + u_1 t^{g-1} + \dots + u_g\big) \\
&= u_1' t^{g-1} + \dots + u_g' \\
&= v_1 t^{g-1} + \dots + v_g \\
&= v(t), \\
\mathrm{D}\,v(t) &= \mathrm{D}\,\big(v_1 t^{g-1} + v_2 t^{g-2} + \dots + v_g\big) \\
&= v_1' t^{g-1} + v_2' t^{g-2} + \dots + v_g' \\
&= \frac{1}{2}(-w_1 + u_2 - u_1 u_1 + w_0 u_1) t^{g-1} + \frac{1}{2}(-w_2 + u_3 - u_1 u_2 + w_0 u_2) t^{g-2} \\
&\quad + \dots + \frac{1}{2}(-w_g - u_1 u_g + w_0 u_g) \\
&= \frac{1}{2}(-w_1 t^{g-1} - w_2 t^{g-2} - \dots - w_g + t(u_2 t^{g-2} + u_3 t^{g-3} + \dots + u_g) \\
&\quad - u_1(u_1 t^{g-1} + u_2 t^{g-2} + \dots + u_g) + w_0(u_1 t^{g-1} + u_2 t^{g-2} + \dots + u_g) \\
&\quad - t^{g+1} - w_0 t^g + t(t^g + u_1 t^{g-1}) - u_1 t^g + w_0 t^g) \\
&= \frac{1}{2}(-w(t) + (t - u_1 + w_0) u(t)), \\
\mathrm{D}\,w(t) &= \mathrm{D}\,\big(t^{g+1} + w_0 t^g + w_1 t^{g-1} + \dots + w_g\big) \\
&= w_0' t^g + w_1' t^{g-1} + \dots + w_g' \\
&= -v_1 t^g + (-v_2 + u_1 v_1 - w_0 v_1) t^{g-1} + \dots + u_1 v_g - w_0 v_g \\
&= -v_1 t^g - v_2 t^{g-1} - \dots - v_g t + (u_1 - w_0)(v_1 t^{g-1} + \dots + v_g) \\
&= -t v(t) + (u_1 - w_0) v(t) \\
&= -(t - u_1 + w_0) v(t).
\end{aligned}$$

2 Konzept für eine Arithmetik auf Jacobi–Varietäten

In diesem Abschnitt 2.1 diskutiere ich den Fall für Geschecht 1. Dort ist die elliptische Kurve bereits die Jacobische Varietät und die Weierstraßsche $\wp$–Funktion bildet zusammen mit ihrer Ableitung den Torus ohne Nullpunkt auf den affinen Teil der elliptische Kurve im $\mathbb{C}^2$ ab. Anschließend entwerfe ich in Abschnitt 2.2 ein Konzept, wie diese bei Geschlecht 1 studierte Vorgehensweise auf beliebiges Geschlecht $g \geq 1$ zu verallgemeinern ist.

2.1 Motivation durch elliptische Kurven

Definition 8
Eine **elliptische Kurve** C **über** $\mathbb{C}$ ist die Menge der Punkte $(x, y) \in \mathbb{C}^2$, die der Gleichung

$$y^2 = \prod_{i=1}^{3}(x - a_i) \tag{2}$$

genügen, und dem besonderen Punkt ∞, wobei $a_1, a_2, a_3 \in \mathbb{C}$ paarweise verschieden sind.

Die Kurve ist eine komplex eindimensionale Fläche im $\mathbb{C}^2$. Eine elliptische Kurve der Form (2) läßt sich mittels Koordinatentransformation folgendermaßen auf $y^2 = x^3 + \tilde{a}x + \tilde{b}$ transformieren:
Eliminiere den Koeffizienten von x^2 durch $x \longmapsto x + \frac{1}{3}A$ mit $A = (a_1 + a_2 + a_3)$:

$$\begin{aligned}
\prod_{i=1}^{3}(x - a_i) &= (x - a_1)(x - a_2)(x - a_3) \\
&= x^3 - Ax^2 + (a_1a_2 + a_2a_3 + a_1a_3)x - (a_1a_2a_3) \\
&\overset{x \mapsto x + \frac{1}{3}A}{\longmapsto} \left(x + \frac{A}{3}\right)^3 - A\left(x + \frac{A}{3}\right)^2 + (a_1a_2 + a_2a_3 + a_1a_3)\left(x + \frac{A}{3}\right) - (a_1a_2a_3) \\
&= x^3 + Ax^2 + x\frac{A^2}{3} + \frac{A^3}{27} - Ax^2 - 2x\frac{A^2}{3} - \frac{A^3}{9} \\
&\quad + (a_1a_2 + a_2a_3 + a_1a_3)x + (a_1a_2 + a_2a_3 + a_1a_3)\frac{A}{3} - (a_1a_2a_3) \\
&= x^3 + \tilde{a}x + \tilde{b}
\end{aligned}$$

mit $\tilde{a} = a_1a_2 + a_2a_3 + a_1a_3 - \frac{1}{3}A^2$, $\tilde{b} = (a_1a_2 + a_2a_3 + a_1a_3)\frac{1}{3}A - \frac{2}{27}A^3 - a_1a_2a_3$, und bringe diese reduzierte Form $y^2 = x^3 + \tilde{a}x + \tilde{b}$ durch eine weitere Koordinatentransformation $x \longmapsto \sqrt[3]{4}x$ auf $y^2 = 4x^3 + ax + b$. Die Bedingung, daß $4x^3 + ax + b$ keine mehrfache Nullstelle besitzt, läßt sich mit der Lösungsformel für $x^3 + \frac{a}{4}x + \frac{b}{4} = 0$ durch $a^3 + 27b^2 \neq 0$ ausdrücken.

Definition 9
Eine elliptische Kurve C über $\mathbb{C}$ in **Weierstraßscher Normalform** ist die Menge der Punkte $(x, y) \in \mathbb{C}^2$, die der Gleichung

$$y^2 = 4x^3 + ax + b \tag{3}$$

genügen, und dem Punkt ∞, wobei $a, b \in \mathbb{C}$, $a^3 + 27b^2 \neq 0$.

Ich betrachte von nun an stets eine elliptische Kurve in Weierstraßscher Normalform. Wie in Abschnitt 1.5 gezeigt, gehört zu jeder Kurve in eineindeutiger Weise ein Gitter Γ, so daß der affine Teil der Kurve, $C - \{\infty\}$, isomorph zum Torus ohne Nullpunkt, $(\mathbb{C}/\Gamma) - \Gamma$, ist.

Definition 10
Für ein Gitter $\Gamma = \mathbb{Z} + \tau\mathbb{Z}$, $\tau \in \mathbb{C}$, $\operatorname{Im}\tau > 0$, heißt die Funktion

$$\begin{aligned} \wp : \quad \mathbb{C} - \{0\} \quad &\longrightarrow \mathbb{C}, \\ z \qquad &\longmapsto \frac{1}{z^2} + {\sum_{\omega\in\Gamma}}' \frac{1}{(z-\omega)^2} - \frac{1}{w^2} \end{aligned}$$

Weierstraßsche $\wp$–Funktion . $\sum'$ bezeichne die Summation über alle von 0 verschiedenen Gitterpunkte.

Lemma 1
${\sum\limits_{\omega\in\Gamma}}' \frac{1}{\omega^\lambda}$ konvergiert absolut $\Longleftrightarrow \lambda > 2$.

Beweis
Betrachte die Partialsummen

$$S_n = \sum_{\substack{0\neq\omega\in\Gamma \\ |\omega|\leq n}} \frac{1}{|\omega|^\lambda} \text{ für } n = N, N+1, ...,$$

wobei $N = \min\{k \in \mathbb{N} \mid k \geq |\omega|\}$. Setze $T_n = S_n - S_{n-1}$, $n \geq 1$, mit $S_0 = 0$. Es gilt:
S_n konvergiert genau dann, wenn $\sum\limits_{n=1}^{\infty} T_n$ konvergiert.
Da die Summe S_n genau $(2n+1)^2 - 1$ Terme enthält, enthält T_n genau
$(2n+1)^2 - 1 - ((2(n-1)+1)^2 - 1) = 8n$ Terme.
Zu jedem τ, das das Gitter $\Gamma = \mathbb{Z} + \tau\mathbb{Z}$ erzeugt, existieren $a, b > 0$, so daß zu jedem ω ein $n \geq 0$ existiert mit $a \cdot n \geq |\omega| \geq b \cdot n$. Dies impliziert:

$$\begin{aligned} (nb)^{-\lambda} \leq \quad & \frac{1}{|\omega|^\lambda} && \leq (na)^{-\lambda} \\ \Longrightarrow \quad 8n(nb)^{-\lambda} \leq \quad & \sum_{an<|\omega|<bn} \frac{1}{|\omega|^\lambda} && \leq 8n(na)^{-\lambda} \\ \Longrightarrow \quad 8b^{-\lambda}\sum_{n=1}^{\infty} n^{1-\lambda} \leq \quad & \sum_{0\neq\omega\in\Gamma} \frac{1}{|\omega|^\lambda} && \leq 8a^{-\lambda}\sum_{n=1}^{\infty} n^{1-\lambda}. \end{aligned}$$

Und $\sum\limits_{n=1}^{\infty} \frac{1}{n^{\lambda-1}}$ konvergiert für $\lambda > 2$, woraus die Behauptung folgt.

$\square$

Korollar 1
$\wp$ konvergiert lokal gleichmäßig.

Beweis
Sei $|z| \leq R$. Für fast alle ω gilt dann: $|\omega| \geq 2R$. Für diese ω gilt

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{\omega^2 - (z-\omega)^2}{\omega^2(z-\omega)^2}\right| = \frac{|z||2\omega - z|}{|\omega|^2|z-\omega|^2} \leq \frac{R3|\omega|}{|\omega|^2\frac{|\omega|^2}{4}} \leq 12R\frac{1}{|\omega|^3},$$

denn aus $|z| \leq R$ und $|\omega| \geq 2R$ folgen $|z-\omega| \geq \frac{|\omega|}{2}$ und $|2\omega - z| \leq 3|\omega|$.

□

$\wp$ ist eine meromorphe Funktion mit einer doppelten Polstelle in jedem Gitterpunkt und keinen weiteren Polstellen. $\wp$ ist gerade, d.h. $\wp(z) = \wp(-z)$ für alle $z \in \mathbb{C}$.

Eine Funktion f heißt **periodisch** oder **elliptisch** bzgl. $\Gamma = \mathbb{Z} + \tau\mathbb{Z}$, $\tau \in \mathbb{C}$, $\operatorname{Im}\tau > 0$, wenn gilt:

$$f(z+\omega) = f(z) \text{ für } \omega \in \Gamma \text{ und alle } z \in \mathbb{C}.$$

Das Ziel, eine konkrete Abbildung zu definieren, die einen Torus ohne 0 auf die dazu isomorphe elliptische Kurve ohne ∞ abbildet, läßt sich durch $\wp(z)$ und $\wp'(z)$ finden, wie der folgende Satz zeigt.

Satz 5
Sei $\Gamma = \mathbb{Z} + \tau\mathbb{Z}$, $\tau \in \mathbb{C}$, $\operatorname{Im}\tau > 0$. Der Morphismus

$$\begin{aligned} \varphi:\ \ \mathbb{C} - \{0\} &\longrightarrow \mathbb{C}^2, \\ z &\longmapsto (\wp(z), \wp'(z)) \end{aligned}$$

ist bzgl. Γ periodisch und eine Einbettung in den $\mathbb{C}^2$, d.h. für die Kurve $C : y^2 = x^3 - g_2x - g_3$ mit $g_2 = 60 \sum\limits_{0 \neq \omega \in \Gamma} \frac{1}{\omega^4}$ und $g_3 = 140 \sum\limits_{0 \neq \omega \in \Gamma} \frac{1}{\omega^6}$ wird $(\mathbb{C}/\Gamma) - \Gamma$ via φ auf $C - \{\infty\}$ abgebildet:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \text{ gilt für } z \in (\mathbb{C}/\Gamma) - \Gamma.$$

Beweis
Betrachte die Differentiation von $\wp$:

$$\wp'(z) = -2\frac{1}{z^3} - 2\sum_{0 \neq \omega \in \Gamma} \frac{1}{(z-\omega)^3} = -2\sum_{\omega \in \Gamma} \frac{1}{(z-\omega)^3}.$$

Offensichtlich gilt $\wp'(z+\omega) = \wp'(z)$ für $\omega \in \Gamma$ und alle $z \in \mathbb{C}$. $\wp'(z)$ ist also periodisch. Daraus folgt $\wp(z+\omega) = \wp(z) + c$ durch Integration. Speziell gilt für $z = -\frac{\omega}{2}$: $\wp(\frac{\omega}{2}) = \wp(-\frac{\omega}{2}) + c$. Da $\wp$ gerade ist, muß $c = 0$ sein. Also ist $\wp$ periodisch bzgl. Γ und damit ist $\varphi : (\mathbb{C}/\Gamma) - \Gamma \longrightarrow \mathbb{C}^2$. Ein $z \in (\mathbb{C}/\Gamma) - \Gamma$ repräsentiert somit stets eine Äquivalenzklasse.

Betrachte die Laurententwicklung von $\wp$ um $z = 0$,

$$\wp(z) = \frac{1}{z^2} + a_2z^2 + a_4z^4 + \ldots, \tag{4}$$

differenziere und quadriere nacheinander:

$$\Longrightarrow \wp'(z) \quad = -2\frac{1}{z^3} + 2a_2 z + 4a_4 z^3 + ...$$

$$\Longrightarrow \wp'(z)^2 = \frac{4}{z^6} - 8a_2\frac{1}{z^2} - 16a_4 + ... \, . \tag{5}$$

Weiter gilt wegen Gleichung (4)

$$\wp(z)^3 = \frac{1}{z^6} + 3a_2\frac{1}{z^2} + 3a_4 + ... \, . \tag{6}$$

Betrachte unter Berücksichtigung von (5) und (6) die Funktion

$$\begin{aligned} f(z) &= \wp'(z)^2 - 4\wp(z)^3 + 20a_2\wp(z) + 28a_4 \\ &= \frac{4}{z^6} - 8a_2\frac{1}{z^2} - 16a_4 + ... - \frac{4}{z^6} - 12a_2\frac{1}{z^2} - 12a_4 + ... + 20a_2\frac{1}{z^2} + ... + 28a_4. \end{aligned}$$

$f(z)$ verschwindet in $z = 0$ und ist in einer Umgebung von $z = 0$ holomorph.

Andererseits ist die Funktion periodisch mit Periode Γ. Polstellen hätte sie höchstens in Γ haben dürfen, dort hat sie aber keine. Also ist $f(z)$ in der ganzen Ebene holomorph. Nach Liouville ist sie damit konstant, da sie in $z = 0$ verschwindet. Also gilt

$$\wp'(z)^2 = 4\wp(z)^3 - 20a_2\wp(z) - 28a_4.$$

Die Werte a_2, a_4 lassen sich berechnen, betrachte dazu

$$\wp(z) - \frac{1}{z^2} = \sum_{0\neq\omega\in\Gamma} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = a_2 z^2 + a_4 z^4 + ..., \tag{7}$$

differenziere (7) zweimal und werte in $z = 0$ aus:

$$\begin{aligned} &6\sum_{0\neq\omega\in\Gamma} \frac{1}{(z-\omega)^4} = 2a_2 + 12a_4 z^2 + ... \\ \Longrightarrow\ &a_2 = 3\sum_{0\neq\omega\in\Gamma} \frac{1}{\omega^4}. \end{aligned}$$

Nun differenziere ich die Formel (7) viermal und werte in $z = 0$ aus:

$$\begin{aligned} &120\sum_{0\neq\omega\in\Gamma} \frac{1}{(z-\omega)^6} = 24a_4 + ... \\ \Longrightarrow\ &a_4 = 5\sum_{0\neq\omega\in\Gamma} \frac{1}{\omega^6}. \end{aligned}$$

Mit $g_2 = 60 \sum\limits_{0\neq\omega\in\Gamma} \frac{1}{\omega^4}$ und $g_3 = 140 \sum\limits_{0\neq\omega\in\Gamma} \frac{1}{\omega^6}$ gilt $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.

□

Um φ auch in den Gitterpunkten zu erklären, wird $\mathbb{C}^2$ zum projektiven Raum $\mathbb{P}^2$ erweitert und φ eindeutig mit $\varphi(0) = \infty$ zu $\varphi : \mathbb{C}/\Gamma \longrightarrow \mathbb{P}^2$ fortgesetzt. Damit ist nun $\varphi(\mathbb{C}/\Gamma) = C$ und die Gruppenstruktur des Torus $\mathbb{C}/\Gamma$ läßt sich auf die elliptische Kurve C im $\mathbb{P}^2$ übertragen.

Zunächst die Addition auf dem affinen Teil der elliptischen Kurve $C - \{\infty\}$. Rechnen auf dem Torus ist einfach: Sind $z_1, z_2 \in \mathbb{C}/\Gamma$, $z_1, z_2, z_1 + z_2 \notin \Gamma$, so ist $z_1 + z_2$ modulo Γ aus $\mathbb{C}/\Gamma$. φ überträgt diese Struktur auf $C - \{\infty\}$, wodurch dort zwei Elementen $(\wp(z_1), \wp'(z_1))$ und $(\wp(z_2), \wp'(z_2))$ als Ergebnis der Addition $(\wp(z_1 + z_2), \wp'(z_1 + z_2))$ zugeordnet wird.

Der folgende Satz zeigt, wie sich $\wp(z_1 + z_2)$ in einer expliziten Formel als rationale Kombination der $\wp(z_1)$, $\wp'(z_1)$, $\wp(z_2)$, $\wp'(z_2)$ berechnen läßt, aus der durch Differentiation eine Formel für $\wp'(z_1 + z_2)$ entsteht.

Satz 6 (Additionsformeln)
Seien $z_1, z_2 \in (\mathbb{C}/\Gamma) - \Gamma$. Für die Punkte $(\wp(z_1), \wp'(z_1))$, $(\wp(z_2), \wp'(z_2)) \in C$ sei $\wp(z_1) \neq \wp(z_2)$. Dann ist das Ergebnis der Addition der beiden Punkte auf der Kurve $(\wp(z_1 + z_2), \wp'(z_1 + z_2))$ mit

$$\begin{aligned}
\wp(z_1 + z_2) &= -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2, \\
\wp'(z_1 + z_2) &= -\wp'(z_1) + \frac{\wp'(z_1) - \wp'(z_2)}{(\wp(z_1) - \wp(z_2))^2}\left(3\wp(z_1)^2 + \frac{a}{4}\right) - \frac{1}{2}\frac{(\wp'(z_1) - \wp'(z_2))^2}{(\wp(z_1) - \wp(z_2))^3}\wp'(z_1).
\end{aligned}$$

Beweis
Seien $z_1, z_2 \in (\mathbb{C}/\Gamma) - \Gamma$, $\wp(z_1) \neq \wp(z_2)$. Betrachte $f(z) = \wp'(z) - a\wp(z) - b$ und bestimme a und b so, daß $f(z_1) = 0$ und $f(z_2) = 0$ gilt:

$$\begin{aligned}
f(z_1) &= \wp'(z_1) - a\wp(z_1) - b = 0, \\
f(z_2) &= \wp'(z_2) - a\wp(z_2) - b = 0.
\end{aligned} \tag{8}$$

Lösen des Gleichungssystems ergibt für a:

$$\begin{aligned}
0 &= \wp'(z_1) - \wp'(z_2) - a\wp(z_1) + a\wp(z_2) \\
\Longleftrightarrow \quad a &= \frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}
\end{aligned}$$

und für b:

$$\begin{aligned}
b &= \wp'(z_1) - \frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\wp(z_1) \\
&= \wp'(z_1)\frac{\wp(z_1) - \wp(z_2)}{\wp(z_1) - \wp(z_2)} - \frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\wp(z_1) \\
&= -\frac{\wp'(z_1)\wp(z_2) - \wp(z_1)\wp'(z_2)}{\wp(z_1) - \wp(z_2)}.
\end{aligned}$$

f ist periodisch, hat in den Gitterpunkten Pole der Ordnung 3 und ist sonst holomorph.

Für das halboffene Periodenparallelogramm $P = \{\rho_1 + \tau\rho_2 \mid 0 \leq \rho_1 < 1,\ 0 \leq \rho_2 < 1\}$ gelten bekanntlich $\sum_{k=1}^{K} m_k a_k - \sum_{l=1}^{L} n_l b_l \in \mathbb{Z} + \tau\mathbb{Z}$, wobei a_k die K Nullstellen mit ihren Vielfachheiten m_k und b_l die L Polstellen mit ihren Vielfachheiten n_l sind, und $\sum_{k=1}^{K} m_k = \sum_{l=1}^{L} n_l$. In P hat f in

0 die einzige Polstelle mit Vielfachheit 3, deshalb existieren auch drei Nullstellen. z_1, z_2 sind je zur Vielfachheit 1 bereits bekannt und $\tilde{z}_3 = -z_1 - z_2 \mod \mathbb{Z} + \tau\mathbb{Z}$ ist die dritte Nullstelle. Es gilt:

$$\begin{aligned} & f(-z_1 - z_2) = 0 \\ \Longleftrightarrow \quad & \wp'(-z_1 - z_2) = a\wp(-z_1 - z_2) + b \\ \Longleftrightarrow \quad & -\wp'(z_1 + z_2) = a\wp(z_1 + z_2) + b, \text{ da } \wp \text{ gerade und } \wp' \text{ ungerade.} \end{aligned}$$

Mit $z_3 = z_1 + z_2$ folgt:

$$\begin{aligned} \wp'(z_1) &= a\wp(z_1) + b, \\ \wp'(z_2) &= a\wp(z_2) + b, \\ -\wp'(z_3) &= a\wp(z_3) + b, \end{aligned}$$
bzw. $(\wp'(z_i))^2 = (a\wp(z_i) + b)^2$ für $i = 1, 2, 3$.

Da $\wp$ die Gleichung der elliptische Kurve löst, gilt für $i = 1, 2, 3$:

$$\wp'(z_i)^2 = 4\wp(z_i)^3 - g_2\wp(z_i) - g_3.$$

Betrachte das Polynom $g(w) = 4w^3 - g_2 w - g_3 - (aw + b)^2$. Nullstellen von $g(w)$ sind die $\wp(z_i)$ für $i = 1, 2, 3$. Sei $\wp(z_3) \neq \wp(z_1), \wp(z_2)$. Zu gegebenem z_1 werden in jedem Periodenparallelogramm P nur endlich viele z_2 ausgeschlossen, da $z_3 = z_1 + z_2$. Dann sind $\wp(z_1), \wp(z_2), \wp(z_3)$ sämtliche Nullstellen, d.h. $g(w) = 4(w - \wp(z_1))(w - \wp(z_2))(w - \wp(z_3))$. Ein Koeffizientenvergleich dieser beiden Darstellungen

$$\begin{aligned} g(w) &= 4(w - \wp(z_1))(w - \wp(z_2))(w - \wp(z_3)) \\ &= 4w^3 - 4(\wp(z_1) + \wp(z_2) + \wp(z_3))w^2 + 4(\wp(z_1)\wp(z_2) + \wp(z_2)\wp(z_3) + \wp(z_1)\wp(z_3))w \\ &\quad - 4\wp(z_1)\wp(z_2)\wp(z_3), \\ g(w) &= 4w^3 - g_2 w - g_3 - (aw + b)^2 \\ &= 4w^3 - a^2 w^2 - (2ab + g_2)w - (b^2 + g_3) \end{aligned}$$

ergibt

$$\begin{aligned} & a^2 && = 4(\wp(z_1) + \wp(z_2) + \wp(z_3)) \\ \Longleftrightarrow\ & \wp(z_3) && = -\wp(z_1) - \wp(z_2) + \frac{1}{4}a^2 \\ \Longleftrightarrow\ & \wp(z_1 + z_2) && = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2. \end{aligned}$$

Aus Gründen der Stetigkeit lassen sich die gerade ausgeschlossenen Werte für z_2 wieder zulassen und die Formel für $\wp(z_1 + z_2)$ ist gefunden. Die zweite Koordinate $\wp'(z_1 + z_2)$ läßt sich durch Differentiation von $\wp(z_1 + z_2)$ nach einer Veränderlichen, z.B. z_1, erzielen:

$$\begin{aligned} & \wp'(z_1 + z_2) \\ &= \frac{\partial}{\partial z_1}\wp(z_1 + z_2) \\ &= -\wp'(z_1) + \frac{1}{2}\,\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\,\frac{\wp''(z_1)(\wp(z_1) - \wp(z_2)) - (\wp'(z_1) - \wp'(z_2))\wp'(z_1)}{(\wp(z_1) - \wp(z_2))^2} \qquad (9) \\ &= -\wp'(z_1) + \frac{1}{2}\,\frac{\wp'(z_1) - \wp'(z_2)}{(\wp(z_1) - \wp(z_2))^2}\wp''(z_1) - \frac{1}{2}\,\frac{(\wp'(z_1) - \wp'(z_2))^2}{(\wp(z_1) - \wp(z_2))^3}\wp'(z_1). \end{aligned}$$

Um den Term $\wp''(z)$ zu ersetzen, wird die Kurvengleichung differenziert,

$$\begin{aligned}
&\wp'(z)^2 &&= 4\wp(z)^3 + a\wp(z) + b \\
\Longrightarrow\ &2\wp'(z)\wp''(z) &&= 12\wp(z)^2\wp'(z) + a\wp'(z),\ \wp'(z) \neq 0 \\
\Longleftrightarrow\ &\wp''(z) &&= 6\wp(z)^2 + \frac{a}{2},
\end{aligned}$$

und in (9) eingesetzt:

$$\begin{aligned}
&\wp'(z_1 + z_2) \\
&= -\wp'(z_1) + \frac{1}{2}\,\frac{\wp'(z_1) - \wp'(z_2)}{(\wp(z_1) - \wp(z_2))^2}\wp''(z_1) \ - \ \frac{1}{2}\,\frac{(\wp'(z_1) - \wp'(z_2))^2}{(\wp(z_1) - \wp(z_2))^3}\wp'(z_1) \\
&= -\wp'(z_1) + \frac{1}{2}\,\frac{\wp'(z_1) - \wp'(z_2)}{(\wp(z_1) - \wp(z_2))^2}\left(6\wp(z_1)^2 + \frac{a}{2}\right) \ - \ \frac{1}{2}\,\frac{(\wp'(z_1) - \wp'(z_2))^2}{(\wp(z_1) - \wp(z_2))^3}\wp'(z_1) \\
&= -\wp'(z_1) + \frac{\wp'(z_1) - \wp'(z_2)}{(\wp(z_1) - \wp(z_2))^2}\left(3\wp(z_1)^2 + \frac{a}{4}\right) \ - \ \frac{1}{2}\,\frac{(\wp'(z_1) - \wp'(z_2))^2}{(\wp(z_1) - \wp(z_2))^3}\wp'(z_1).
\end{aligned}$$

$\square$

In Satz 6 müssen die zwei Punkte $\wp(z_1)$ und $\wp(z_2)$ verschieden sein. Ist dies nicht der Fall und gilt $\wp'(z_1) = \wp'(z_2)$, d.h. sind die beiden Punkte identisch, so wende die folgende Verdopplungsformel an.

Satz 7 (Verdopplungsformeln)
Sei $z_1 \in (\mathbb{C}/\Gamma) - \Gamma$. Dann ist das Ergebnis der Verdopplung eines Punktes $(\wp(z_1), \wp'(z_1)) \in C$ auf der Kurve $(\wp(2z_1), \wp'(2z_1))$ mit

$$\begin{aligned}
\wp(2z_1) &= -2\wp(z_1) + \frac{1}{16}\left(\frac{12\wp(z_1)^2 + a}{\wp'(z_1)}\right)^2, \\
\wp'(2z_1) &= -\wp'(z_1) + \frac{3}{2}\,\frac{\wp(z_1)}{\wp'(z_1)}\left(12\wp(z_1)^2 + a\right) - \frac{1}{32}\,\left(\frac{12\wp(z_1)^2 + a}{\wp'(z_1)}\right)^3.
\end{aligned}$$

Beweis
Durch Betrachtung des Grenzprozesses und Differentiation:

$$\begin{aligned}
\wp(2z_1) &= \lim_{z_2 \to z_1} \wp(z_1 + z_2) \\
&= -2\wp(z_1) + \frac{1}{4}\lim_{z_2 \to z_1}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 \\
&= -2\wp(z_1) + \frac{1}{4}\left(\lim_{z_2 \to z_1}\frac{\wp'(z_1) - \wp'(z_2)}{z_1 - z_2}\,\frac{z_1 - z_2}{\wp(z_1) - \wp(z_2)}\right)^2 \\
&= -2\wp(z_1) + \frac{1}{4}\left(\frac{\wp''(z_1)}{\wp'(z_1)}\right)^2 \\
&= -2\wp(z_1) + \frac{1}{16}\left(\frac{12\wp(z_1)^2 + a}{\wp'(z_1)}\right)^2,
\end{aligned}$$

$$
\begin{aligned}
\wp'(2z_1) &= \frac{1}{2}\,\frac{\mathrm{d}}{\mathrm{d}\,z_1}\wp(2z_1) \\
&= -\wp'(z_1) + \frac{1}{16}\,\frac{12\wp(z_1)^2+a}{\wp(z_1)}\,\frac{24\wp(z_1)\wp'(z_1)^2-(12\wp(z_1)^2+a)\wp''(z_1)}{\wp'(z_1)^2} \\
&= -\wp'(z_1) + \frac{3}{2}\,\frac{\wp(z_1)}{\wp'(z_1)}\left(12\wp(z_1)^2+a\right) - \frac{1}{32}\left(\frac{12\wp(z_1)^2+a}{\wp'(z_1)}\right)^3 .
\end{aligned}
$$

□

Gilt hingegen $\wp(z_1) = \wp(z_2)$ und $\wp'(z_1) = -\wp'(z_2)$, so werden zwei Punkte auf $C - \{\infty\}$ addiert, die durch Spiegelung an der x–Achse aus einander hervorgehen, und das Ergebnis der Addition ist ∞, wegen $P + \neg P = \infty$. In diesem Fall verläßt die partielle Addition den affinen Teil der Kurve. Desweiteren gilt $P + \infty = P$, wodurch ∞ das neutrale Element der Addition ist. Mit dieser Addition bilden die Punkte auf der elliptischen Kurve eine abelsche Gruppe. Anhand der Additionsformeln läßt sich die Kommutativität direkt ablesen, während der Nachweis der Assoziativität einen enormen Aufwand bedeutet. Es ist mir nicht gelungen, $(P + Q) + R = P + (Q + R)$ mit den noch relativ überschaubaren expliziten Additionsformeln, selbst mit Computer–Einsatz, nachzuweisen. Die Assoziativität muß aber wegen der Konstruktion gewährleistet sein.

Soll auf dem affinen Teil einer elliptischen Kurve gerechnet werden, müssen zunächst Punkte bestimmt werden. Selbstverständlich läßt sich zu einer Kurve C das Gitter Γ bestimmen, so daß sich $\wp(z)$ wie auch $\wp'(z)$ anhand der Definitionen als Grenzwert einer unendlichen Reihe über alle Gitterpunkte mit einem Rechner für ein $z \in (\mathbb{C}/\Gamma) - \Gamma$ berechnen lassen. Es gibt aber auch eine viel einfachere Methode: Zu einem x wird $y = \sqrt{f(x)}$ oder $y = -\sqrt{f(x)}$ berechnet und (x, y) ist folglich ein Punkt der Kurve $C - \{\infty\}$. Das Studium der $\wp$–Funktion war für die Bestimmung der Additionsformeln von Wichtigkeit. Zwei Punkte $P, Q \in C - \{\infty\}$ werden demnach in $(\wp, \wp')$–Koordinaten geschrieben, etwa $P = (\wp(z_1), \wp'(z_1))$ und $Q = (\wp(z_2), \wp'(z_2))$, so daß die Formeln zur Addition angewendet werden können.

Beispiel 6
Sei die elliptische Kurve C: $y^2 = 4x^3 - 144x$ gegeben. Betrachte die Punkte $P_1 = (-2, -16)$, $P_2 = (6, 0)$ und $P_3 = (-3, 18)$. Die Additionsformeln aus Satz 6 berechnen daraus:

$$
\begin{aligned}
&P_1 + P_2 = (-3, 18), \\
&P_1 + P_3 = (294, 10080), \\
&P_2 + P_3 = (-2, -16).
\end{aligned}
$$

Das Ergebnis von $P_1 + P_2$ überrascht nicht, da es bereits durch Addition der entsprechenden Divisoren mit dem Cantorschen Reduktionsverfahren in Beispiel 3 berechnet wurde. Um die Assoziativität beispielhaft zu testen, wird $P_1 + P_2 + P_3$ mit drei verschiedenen Klammerungen berechnet, wobei auch die Verdopplungsformeln aus Satz 7 benutzt werden.

$$
\begin{aligned}
&(P_1 + P_2) + P_3 = (-3, 18) + (-3, 18) = (6.25, -8.75), \\
&P_1 + (P_2 + P_3) = (-2, -16) + (-2, -16) = (6.25, -8.75), \\
&(P_1 + P_3) + P_2 = (294, 10080) + (6, 0) = (6.25, -8.75).
\end{aligned}
$$

Beispiel 7
Betrachte für die elliptische Kurve $C\colon y^2 = 4x^3 + 4x - 14$ die Punkte $P_1 = (2, \sqrt{26})$, $P_2 = (1, \sqrt{6}i)$, $P_3 = (-2, 3\sqrt{6}i)$ und addiere, wobei die Ergebnisse näherungsweise angegeben werden:

$$\begin{aligned}
P_1 + P_2 &\approx (2. - 6.2450i, 10.1980 + 31.8434i),\\
P_1 + P_3 &\approx (-0.4375 - 1.1709i, 0.1593 - 2.9853i),\\
P_2 + P_3 &\approx (0.3333, -3.5382i),
\end{aligned}$$

$$\begin{aligned}
(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3) &= (P_1 + P_3) + P_2\\
&\approx (-1.1200 + 3.2474i, 11.3402 - 3.3117i).
\end{aligned}$$

Diese Addition auf der elliptischen Kurve hat eine geometrische Anschauung. Betrachte die auf $\mathbb{R}^2$ projizierte elliptische Kurve in Abbildung 2. Zwei Punkte $P, Q \in C$ werden durch eine Gerade $\overline{P\,Q}$ verbunden, die die elliptische Kurve in einem dritten Punkt schneidet. Die Addition der zwei Punkte P, Q ist der an der x–Achse gespiegelte Schnittpunkt der Geraden $\overline{P\,Q}$ mit der Kurve, welcher mit $P + Q$ bezeichnet wird. Für einen Punkt $R \in C$ wird die Tangente an die Kurve C in R betrachtet. Der weitere Schnittpunkt mit C wird an der x–Achse gespiegelt und ist das Ergebnis der Addition $R{+}R = 2R$. Für einen Punkt $P = (x, y)$ und den gespiegelten Punkt $\neg P = (x, -y)$ ist $P{+}\neg P = \infty$.

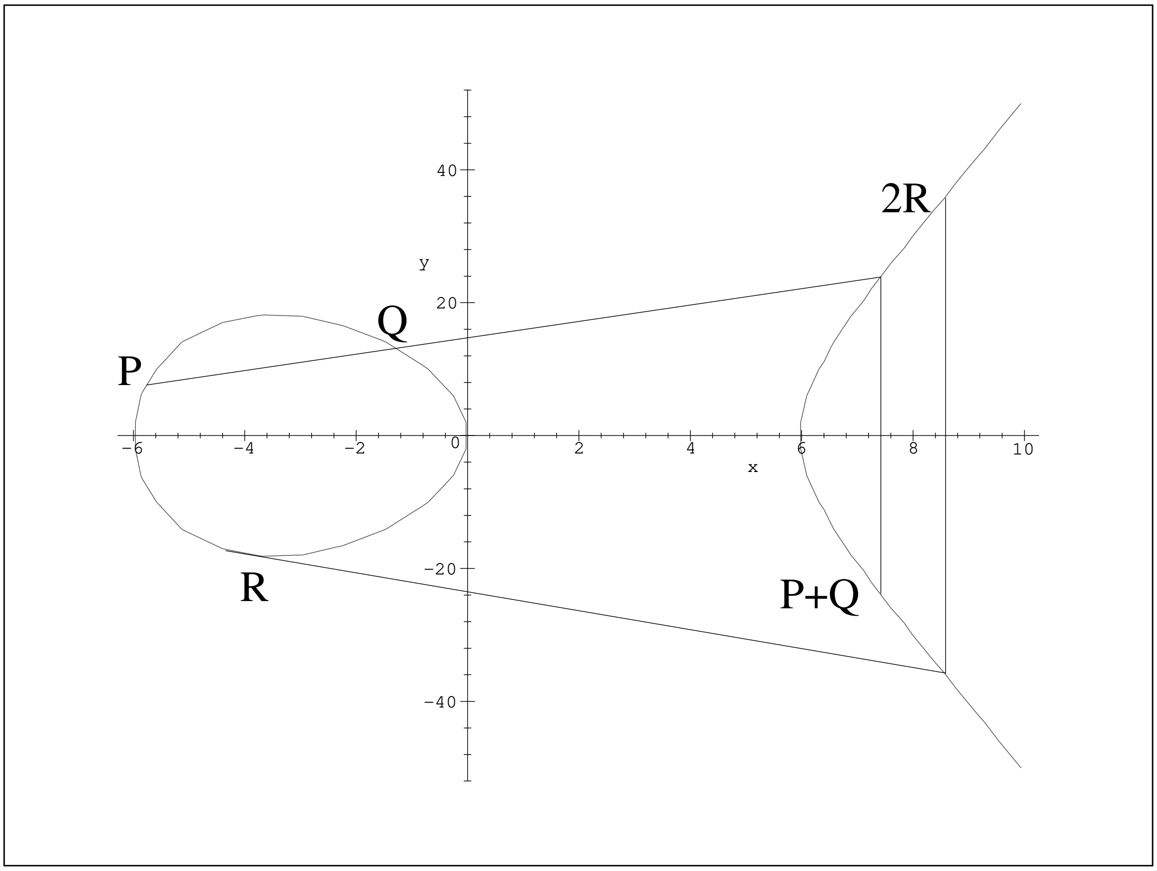

Abbildung 2: Die elliptische Kurve $C\colon y^2 = 4x^3 - 144x$

In Abschnitt 1 wurde gezeigt, daß für eine elliptische Kurve $C : y^2 = f(x) = 4x^3 + ax + b$ gilt:

$$\begin{aligned} Jac\, C &\cong C, \\ Jac\, C - \Theta &\cong \{(x,y) \mid y^2 = f(x)\} = C - \{\infty\}, \\ \Theta &\cong \{\infty\}. \end{aligned}$$

Ein Element $D \in Jac\ C - \Theta$ hat nach Beispiel 1 die Darstellung $D = (u_1(z), v_1(z)) \in V(R_1)$ mit $R_1(u_1(z), v_1(z)) = 0 \iff v_1^2(z) = -4u_1^3(z) - au_1(z) + b$. Das Problem, $u_1(z)$ und $v_1(z)$ zu realisieren, wurde in diesem Abschnitt durch $u_1(z) = -\wp(z)$ und $v_1(z) = \wp'(z)$ gelöst. Dadurch gilt $D = (\wp(z), \wp'(z)) \in V(\tilde{R}_1)$ mit $\tilde{R}_1(\wp(z), \wp'(z)) = \wp'(z)^2 - 4\wp(z)^3 - a\wp(z) - b$ und $\tilde{R}_1(\wp(z), \wp'(z)) = 0$ für alle $z \in (\mathbb{C}/\Gamma) - \Gamma$.

Dieses Verfahren soll für beliebiges Geschlecht $g \geq 1$ verallgemeinert werden.

2.2 Entwurf für eine Arithmetik bei hyperelliptischen Kurven

Sei nun C eine hyperelliptische Kurve vom Geschlecht $g \geq 1$ und $Jac\, C - \Theta$ die Jacobische Varietät zu C. Analog zu Geschlecht $g = 1$, wo eine Addition auf $Jac\ C - \Theta \cong C - \{\infty\} \cong (\mathbb{C}/\Gamma) - \Gamma$ definiert wurde, soll eine partielle Addition auf $Jac\ C - \Theta$ für beliebiges Geschlecht entwickelt werden.

$Jac\ C - \Theta$ ist nach Abschnitt 1 die Einbettung von $T_C - \Phi(\Theta)$ in den $\mathbb{C}^{2g}$ und läßt sich durch die g Gleichungen $R_i(u_1(z), ..., u_g(z), v_1(z), ..., v_g(z)) = 0$, $i = 1, ..., g$, mit den $2g$ Funktionen $u_1, ..., u_g, v_1, ..., v_g : T_C - \Phi(\Theta) \longrightarrow \mathbb{C}$ charakterisieren.

Während sich Punkte auf der Varietät relativ leicht durch die Gleichungen bestimmen lassen, besteht das Problem in einer zur Divisoraddition alternativen Arithmetik.

Dazu soll analog zu $g = 1$ folgendes erreicht werden:

i. Definition einer Verallgemeinerung der Weierstraßschen $\wp$–Funktion in g Variablen in Zusammenhang zu $u_1(z), ..., u_g(z), v_1(z), ..., v_g(z)$ in der Weise, daß $(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z))$ den Torus $T_C - \Phi(\Theta)$ in den $\mathbb{C}^{2g}$ einbettet. Dabei sollen die Ableitungen $\wp^{(k)}(z) = \mathrm{D}^k(\wp(z))$, $k = 0, ..., 2g-1$, durch den Differentialoperator D aus 1.6 erklärt sein.
$\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)$ erfüllen damit die g Gleichungen $R_i = 0$, die $Jac C - \Theta$ definieren, wodurch $Jac\ C - \Theta$ die Gruppenstruktur von $T_C - \Phi(\Theta)$ erhielte. Dort gilt:
Sei $x, u \in T_C$, $x, u, x + u \notin \Phi(\Theta)$. Dann ist $x + u$ modulo Γ die Addition von x und u auf $T_C - \Phi(\Theta)$. Übertragen auf $Jac\ C - \Theta$ würde den beiden Elementen

$$(\wp(x), \wp'(x), ..., \wp^{(2g-1)}(x)) \text{ und } (\wp(u), \wp'(u), ..., \wp^{(2g-1)}(u))$$

als Ergebnis der Addition auf $Jac\ C - \Theta$ der Punkt

$$(\wp(x+u), \wp'(x+u), ..., \wp^{(2g-1)}(x+u))$$

zugeordnet werden.

ii. Explizite Additionsformeln für $\wp(x+u), \wp'(x+u), ..., \wp^{(2g-1)}(x+u)$, die sich als rationale Kombination der $\wp(x), \wp'(x), ..., \wp^{(2g-1)}(x), \wp(u), \wp'(u), ..., \wp^{(2g-1)}(u)$ schreiben lassen, wobei **rationale Kombination** einen Ausdruck $\wp(x+u) = \frac{f}{g}$ mit
$f, g \in \mathbb{C}[\wp(x), \wp'(x), ..., \wp^{(2g-1)}(x), \wp(u), \wp'(u), ..., \wp^{(2g-1)}(u)]$ bedeuten soll.

Ist beides erreicht, ließe sich auf dem affinen Teil der Jacobischen Varietät einer hyperelliptischen Kurve rechnen. Und zwar ohne die $\wp$–Funktion und ihre $2g-1$ ersten Ableitungen konkret auswerten zu müssen. Zwei Punkte P und Q würden sich über die Gleichungen bestimmen und als Koordinaten in $\wp, \wp', ..., \wp^{(2g-1)}$ schreiben lassen. Etwa

$$P = (\wp(x), \wp'(x), ..., \wp^{(2g-1)}(x)) \text{ und } Q = (\wp(u), \wp'(u), ..., \wp^{(2g-1)}(u)).$$

Mit den Additionsformeln würde sich daraus das Ergebnis

$$P + Q = (\wp(x+u), \wp'(x+u), ..., \wp^{(2g-1+u)}(x))$$

berechnen lassen und eine Arithmetik auf dem affinen Teil der Jacobischen Varietät wäre somit erzielt. Für die nach Abschnitt 1.4 sehr seltenen Fällen der Addition auf Θ wird die Divisoraddition nach Cantor genutzt.

Soweit die Formulierung des Konzepts, wie für eine Jacobi–Varietät eine Arithmetik erklärt werden kann. Um eine Verallgemeinerung der $\wp$–Funktion zu definieren und Additionsformeln bestimmen zu können, wird im nächsten Abschnitt die ϑ–Funktion studiert. Aus ihr wird sich das gewünschte $\wp$ definieren lassen und eine Additionsformel für ϑ führt auf ein Analogon für $\wp$.

3 Die ϑ–Funktion

In diesem Abschnitt definiere ich die ϑ–Funktion als Vorbereitung auf die Verallgemeinerung der Weierstraßschen $\wp$–Funktion. Zunächst beweise ich einige Eigenschaften und insbesondere die Riemannsche Theta–Formel, die aufgrund von Relationen zwischen ϑ–Funktionen auf eine Additionsformel für ϑ führen wird. Da für eine kryptographische Anwendung kurze Rechenzeiten von Vorteil sind, sollte diese Additionsformel so weit wie möglich vereinfacht werden. Deshalb werde ich eine neue Notation einführen, die die Anzahl der Summanden in der Additionsformel für ϑ entscheidend verkleinert und die Formel vereinfacht.

3.1 Definitionen, Eigenschaften und Theta–Relationen

Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 1$. Nach Abschnitt 1.5 läßt sich das Gitter $\Gamma = \mathbb{Z}^g + \Omega\mathbb{Z}^g$, $\Omega \in \mathbb{H}$, $\mathbb{H} = \{A \in GL_g(\mathbb{C}) \mid A^t = A,\ \operatorname{Im} A \text{ positiv definit}\}$, so wählen, daß der Jacobi–Torus $\mathbb{C}^g/\Gamma$ isomorph zur Jacobi–Varietät $Jac\,C$ ist.

Definition 11
Die **ϑ–Funktion** ist durch

$$\begin{aligned} \vartheta\begin{bmatrix} a \\ b \end{bmatrix}: \quad \mathbb{C}^g \times \mathbb{H} &\longrightarrow \mathbb{C}, \\ (z, \Omega) &\longmapsto \sum_{n \in \mathbb{Z}^g} e^{\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)^t (z+b)} \end{aligned}$$

definiert, wobei $a, b \in \frac{1}{2}\mathbb{Z}^g$ die **Charakteristik von** ϑ und n^t der transponierte Vektor von n ist.

Satz 8
Auf $\mathbb{C}^g \times \mathbb{H}$ konvergiert $\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z, \Omega)$ absolut und lokal gleichmäßig und ist eine holomorphe Funktion.

Beweis
Für $\operatorname{Im}\Omega \geq c_2 I_g > 0$, die g–dimensionale Einheitsmatrix I_g, und
$\max\{|\operatorname{Im} z_i| : i = 1, ..., g\} < c_1 - \max\{|b_i| : i = 1, ..., g\}$ gilt

$$\begin{aligned} & |e^{\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)^t (z+b)}| \\ &= |e^{\pi i (n+a)^t (\operatorname{Re}\Omega + i \operatorname{Im}\Omega)(n+a) + 2\pi i (n+a)^t (\operatorname{Re} z + i \operatorname{Im} z + b)}| \\ &= e^{-\pi (n+a)^t \operatorname{Im}\Omega (n+a) - 2\pi i (n+a)^t (\operatorname{Im} z + b)}, \text{ da } |e^\zeta| = e^{\operatorname{Re}\zeta} \\ &\leq e^{-\pi (n+a)^t c_2 I_g (n+a) + 2\pi |n+a|^t (\max_i |\operatorname{Im} z_i| + \max_i |b_i| 1_g)}, \text{ mit } 1_g = (1 \ldots 1)^t \\ &\leq e^{-\pi c_2 \sum_{i=1}^g |n_i + a_i|^2 + 2\pi c_1 \sum_{i=1}^g |n_i + a_i|} \\ &= \prod_{i=1}^g e^{-\pi c_2 |n_i + a_i|^2 + 2\pi c_1 |n_i + a_i|}. \end{aligned}$$

Daraus folgt

$$\begin{aligned}
|\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z,\Omega)| &\leq \sum_{n\in\mathbb{Z}^g} |e^{\pi i(n+a)^t\Omega(n+a)+2\pi i(n+a)^t(z+b)}| \\
&\leq \sum_{n\in\mathbb{Z}^g}\prod_{i=1}^{g} e^{-\pi c_2|n_i+a_i|^2+2\pi c_1|n_i+a_i|} \\
&\leq \left(\sum_{n\geq 0} e^{-\pi c_2|n+a|^2+2\pi c_1|n+a|}\right)^g, \text{ wobei } a=\max_i |a_i|,
\end{aligned}$$

und $\sum_{n\geq 0} e^{-\pi c_2|n+a|^2+2\pi c_1|n+a|} = \sum_{n\geq 0} e^{-\pi c_2(|n+a|-\frac{c_1}{c_2})^2} e^{\pi\frac{c_1^2}{c_2}}$ konvergiert.
Eine g–dimensionale Funktion ist dann holomorph, wenn sie stetig und in jeder Komponente holomorph ist. Da $\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z,\Omega)$ in jeder Komponente holomorph ist und aufgrund der absoluten und lokal gleichmäßigen Konvergenz auf $\mathbb{C}^g\times\mathbb{H}$ stetig ist, ist $\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z,\Omega)$ also holomorph.

□

Bemerkung
Bei $g=2$ sind $a,b\in\frac{1}{2}\mathbb{Z}^2$, d.h. $a=\begin{pmatrix}a_1\\a_2\end{pmatrix}$, $b=\begin{pmatrix}b_1\\b_2\end{pmatrix}$ mit $a_1,a_2,b_1,b_2\in\frac{1}{2}\mathbb{Z}$. Ausführlich geschrieben gilt für $z\in\mathbb{C}^2$

$$\begin{aligned}
\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z) &= \vartheta\begin{bmatrix}a_1\\a_2\\b_1\\b_2\end{bmatrix}\begin{pmatrix}z_1\\z_2\end{pmatrix} \\
&= \sum_{n_1,n_2\in\mathbb{Z}} e^{\pi i\begin{pmatrix}n_1+a_1\\n_2+a_2\end{pmatrix}^t\Omega\begin{pmatrix}n_1+a_1\\n_2+a_2\end{pmatrix}+2\pi i\begin{pmatrix}n_1+a_1\\n_2+a_2\end{pmatrix}^t\begin{pmatrix}z_1+b_1\\z_2+b_2\end{pmatrix}} \\
&= \sum_{n_1,n_2\in\mathbb{Z}} e^{\pi i(n_1+a_1\ n_2+a_2)\Omega\begin{pmatrix}n_1+a_1\\n_2+a_2\end{pmatrix}+2\pi i(n_1+a_1\ n_2+a_2)\begin{pmatrix}z_1+b_1\\z_2+b_2\end{pmatrix}}.
\end{aligned}$$

Künftig werde ich abkürzend $\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z)$ statt $\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z,\Omega)$ schreiben.
Eine Funktion $f:\mathbb{C}^g\longrightarrow\mathbb{C}$ heißt **periodisch** bzgl. $\Gamma=\mathbb{Z}^g+\Omega\mathbb{Z}^g$, $\Omega\in\mathbb{H}$, wenn für $\omega\in\Gamma$ und alle $z\in\mathbb{C}$ gilt:

$$f(z+\omega)=f(z)$$

und sie heißt **Theta–Funktion**, wenn f die sogenannte **Theta–Relation** erfüllt, d.h. wenn für $\omega\in\Gamma$ und alle $z\in\mathbb{C}^g$ gilt:

$$f(z+\omega)=e^{2\pi i(l(z,\omega)+j(\omega))}\,f(z)$$

mit Linearformen l und j, wobei l $\mathbb{C}$-linear in z und $\mathbb{R}$-linear in ω ist und j nur von ω abhängt. Die Eigenschaft einer solchen Theta–Relation heißt auch **quasi–periodisch**, also periodisch bis auf einen einfachen multiplikativen Faktor.

Ich zeige, daß die definierte ϑ–Funktion die Theta–Relation erfüllt und gebe dazu l und j konkret an.

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

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

Beweis
Einsetzen von $z + \Omega p + q$ in die Definition von ϑ beweist die Aussage:

$$\begin{aligned}
&\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z + \Omega p + q) \\
&= \sum_{n\in\mathbb{Z}^g} e^{\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)^t (z + \Omega p + q + b)} \\
&= e^{2\pi i a^t q} \sum_{n\in\mathbb{Z}^g} e^{\pi i ((n+a)^t \Omega (n+a) + 2(n+a)^t \Omega p) + 2\pi i ((n+a)^t (z+b) + n^t q)} \\
&= e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} \\
&\quad \sum_{n\in\mathbb{Z}^g} e^{\pi i ((n+a)^t \Omega (n+a) + 2(n+a)^t \Omega p + p^t \Omega p) + 2\pi i ((n+a)^t (z+b) + p^t (z+b) + n^t q)} \\
&= e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} \\
&\quad \sum_{n\in\mathbb{Z}^g} e^{\pi i ((n+a)^t \Omega (n+a) + (n+a)^t \Omega p + p^t \Omega (n+a) + p^t \Omega p) + 2\pi i ((n+a)^t (z+b) + p^t (z+b) + n^t q)} \\
&= e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} \sum_{n\in\mathbb{Z}^g} e^{\pi i ((n+a)+p)^t \Omega ((n+a)+p) + 2\pi i ((n+a)+p)^t (z+b)}\ \underbrace{e^{2\pi i n^t q}}_{=1} \\
&\overset{n\mapsto n-p}{=} e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} \sum_{n-p\in\mathbb{Z}^g} e^{\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)(z+b)} \\
&= e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q}\ \vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z).
\end{aligned}$$

□

Speziell gelten mit obigen Bezeichnungen:

$$\begin{aligned}
&\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z + \Omega p) = e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b)}\ \vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z), \\
&\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z + q) = e^{2\pi i a^t q}\ \vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z).
\end{aligned}$$

Mit der Umformung $e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q} = e^{2\pi i (-p^t (z+b) + a^t q - \frac{1}{2} p^t \Omega p)}$ sind die Linearformen gegeben durch: $l(z, \Omega p + q) = -p^t(z+b)$ und $j(\Omega p + q) = a^t q - \frac{1}{2} p^t \Omega p$. Also erfüllt die Funktion ϑ die Theta-Relation und hat somit ihren Namen verdient. Um die Rolle der Charakteristik zu verstehen, wird zunächst das Quadrat vom Quotienten zweier Theta–Funktionen betrachtet.

Korollar 2
Seien $a, b, c, d \in \frac{1}{2}\mathbb{Z}^g$, $p, q \in \mathbb{Z}^g$ und $z \in \mathbb{C}^g$. Dann gilt

$$\left(\frac{\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z + \Omega p + q)}{\vartheta \begin{bmatrix} c \\ d \end{bmatrix} (z + \Omega p + q)} \right)^2 = \left(\frac{\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z)}{\vartheta \begin{bmatrix} c \\ d \end{bmatrix} (z)} \right)^2 .$$

Beweis

$$\begin{aligned} \left(\frac{\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z + \Omega p + q)}{\vartheta \begin{bmatrix} c \\ d \end{bmatrix} (z + \Omega p + q)} \right)^2 &= \left(\frac{\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z)\ e^{-\pi i p^t \Omega p - 2\pi i p^t (z+b) + 2\pi i a^t q}}{\vartheta \begin{bmatrix} c \\ d \end{bmatrix} (z)\ e^{-\pi i p^t \Omega p - 2\pi i p^t (z+d) + 2\pi i c^t q}} \right)^2 \\ &= e^{2\pi i p^t (2d-2b) + 2\pi i (2c-2a)^t q} \left(\frac{\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z)}{\vartheta \begin{bmatrix} c \\ d \end{bmatrix} (z)} \right)^2 \\ &= \left(\frac{\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z)}{\vartheta \begin{bmatrix} c \\ d \end{bmatrix} (z)} \right)^2 , \end{aligned}$$

da $e^{2\pi i p^t (2d-2b) + 2\pi i (2c-2a)^t q} = 1$ ist, wegen $2d - 2b,\ 2c - 2a \in \mathbb{Z}$.

□

Das Quadrat vom Quotienten zweier Theta–Funktionen ist meromorph und bezüglich Γ periodisch, also eine meromorphe Funktion auf dem Torus $\mathbb{C}^g / \Gamma$. Als nächstes wird das Verhalten von ϑ untersucht, wenn sich die Charakteristik um halbe Perioden verändert.

Lemma 3
Seien $a, b, c, d \in \frac{1}{2}\mathbb{Z}^g$ und $z \in \mathbb{C}^g$. Dann gilt

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z + \Omega c + d) = e^{-\pi i c^t \Omega c - 2\pi i c^t (z+b+d)}\ \vartheta \begin{bmatrix} a + c \\ b + d \end{bmatrix} (z).$$

Beweis
Verifikation anhand der Definition zeigt die Behauptung:

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

□

Korollar 3
Seien $a,b\in\frac{1}{2}\mathbb{Z}^g$, $p,q\in\mathbb{Z}^g$ und $z\in\mathbb{C}^g$. Dann gilt

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

Beweis
Aus den Lemmata 2 und 3 folgt

$$\begin{aligned}
\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z+\Omega p+q)&=e^{-\pi i p^t\Omega p-2\pi i p^t(z+b)+2\pi i a^t q}\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(z),\\
\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z+\Omega p+q)&=e^{-\pi i p^t\Omega p-2\pi i p^t(z+b+q)}\ \vartheta\begin{bmatrix}a+p\\b+q\end{bmatrix}(z).
\end{aligned}$$

Also ist

$$\begin{aligned}
\vartheta\begin{bmatrix}a+p\\b+q\end{bmatrix}(z)&=e^{-\pi i p^t\Omega p-2\pi i p^t(z+b)+2\pi i a^t q+\pi i p^t\Omega p+2\pi i p^t(z+b+q)}\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(z)\\
&=e^{2\pi i a^t q}\ \underbrace{e^{2\pi i p^t q}}_{=1}\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(z).
\end{aligned}$$

□

Die Relation in Korollar 3 ist unabhängig von p. Es reicht im wesentlichen sogar, $\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z)$ nur für Charakteristiken $a,b\in\{0,\frac{1}{2}\}^g$ zu betrachten, denn für beliebiges $p,q\in\mathbb{Z}^g$ ist $\vartheta\begin{bmatrix}a+p\\b+q\end{bmatrix}(z)$ bis auf das Vorzeichen $e^{2\pi i a^t q} = \pm 1$ mit $\vartheta \begin{bmatrix} a \\ b \end{bmatrix}(z)$ identisch. Das motiviert die Frage, ob ϑ eine gerade oder eine ungerade Funktion ist.

Korollar 4
Seien $a, b \in \frac{1}{2}\mathbb{Z}^g$ und $z \in \mathbb{C}^g$. Dann gilt

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix}(-z) = e^{4\pi i a^t b}\, \vartheta \begin{bmatrix} a \\ b \end{bmatrix}(z).$$

Beweis
Durch Umformen und Ausnutzen von Korollar 3:

$$\begin{aligned}
\vartheta \begin{bmatrix} a \\ b \end{bmatrix}(-z) &= \sum_{n \in \mathbb{Z}^g} e^{\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)^t(-z+b)} \\
&= \sum_{n \in \mathbb{Z}^g} e^{\pi i (-n-a)^t \Omega (-n-a) + 2\pi i (-n-a)^t(z-b)} \\
&\overset{n \mapsto -n}{=} \sum_{-n \in \mathbb{Z}^g} e^{\pi i (n-a)^t \Omega (n-a) + 2\pi i (n-a)^t(z-b)} \\
&= \vartheta \begin{bmatrix} -a \\ -b \end{bmatrix}(z) \\
&= \vartheta \begin{bmatrix} a - 2a \\ b - 2b \end{bmatrix}(z)
\end{aligned}$$

$$\begin{aligned}
&= e^{2\pi i a^t(-2b)}\, \vartheta \begin{bmatrix} a \\ b \end{bmatrix}(z) \\
&= e^{4\pi i a^t b}\, \vartheta \begin{bmatrix} a \\ b \end{bmatrix}(z), \text{ denn für } a, b \in \frac{1}{2}\mathbb{Z}^g \text{ gilt } 4a^t b \in \mathbb{Z}.
\end{aligned}$$

$\square$

Bemerkung
Wegen $e^{n\pi i} = (-1)^n$ ist $\vartheta \begin{bmatrix} a \\ b \end{bmatrix}(z)$ genau dann eine gerade (ungerade) Funktion, wenn $4a^t b$ gerade (ungerade) ist, d.h. es gilt $\vartheta \begin{bmatrix} a \\ b \end{bmatrix}(-z) = \vartheta \begin{bmatrix} a \\ b \end{bmatrix}(z) \Longleftrightarrow 4a^t b \in 2\mathbb{Z}$.

3.2 Riemannsche Theta–Formel

Sei $(x,y,u,v) \in (\mathbb{C}^g)^4$ und ordne diesem Quadrupel ein weiteres in folgender Weise zu:

$$\begin{aligned} \phi : (\mathbb{C}^g)^4 \quad &\longrightarrow (\mathbb{C}^g)^4, \\ (x,y,u,v) &\longmapsto (\widetilde{x},\widetilde{y},\widetilde{u},\widetilde{v}) = \frac{1}{2}\,(x,y,u,v)\,\underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}}_{A}. \end{aligned}$$

Lemma 4
Für $(x,y,u,v) \in (\mathbb{C}^g)^4$, $(n,m,p,q) \in (\mathbb{Z}^g)^4$, $(\widetilde{x},\widetilde{y},\widetilde{u},\widetilde{v}) = \phi(x,y,u,v)$ und $(\widetilde{n},\widetilde{m},\widetilde{p},\widetilde{q}) = \phi(n,m,p,q)$ gelten

i. $(\widetilde{\widetilde{x}},\widetilde{\widetilde{y}},\widetilde{\widetilde{u}},\widetilde{\widetilde{v}}) = (x,y,u,v)$, d.h. ϕ ist bijektiv,

ii. $\phi((\mathbb{Z}^g)^4) \;=\; \{(\widetilde{n},\widetilde{m},\widetilde{p},\widetilde{q}) \in (\{0,\frac{1}{2}\}^g + \mathbb{Z}^g)^4 \mid \widetilde{n}+\widetilde{m}+\widetilde{p}+\widetilde{q} \in 2\mathbb{Z}^g\}$,

iii. $n^t\Omega n + m^t\Omega m + p^t\Omega p + q^t\Omega q = \widetilde{n}^t\Omega\widetilde{n} + \widetilde{m}^t\Omega\widetilde{m} + \widetilde{p}^t\Omega\widetilde{p} + \widetilde{q}^t\Omega\widetilde{q}$,

iv. $n^tx + m^ty + p^tu + q^tv = \widetilde{n}^t\widetilde{x} + \widetilde{m}^t\widetilde{y} + \widetilde{p}^t\widetilde{u} + \widetilde{q}^t\widetilde{v}$.

Beweis

ad i. $\phi\circ\phi = \frac{1}{4}A^2 = \frac{1}{4}\,4\,I = I$.

ad ii. $(\widetilde{n},\widetilde{m},\widetilde{p},\widetilde{q}) = (\frac{n+m+p+q}{2}, \frac{n+m-p-q}{2}, \frac{n-m+p-q}{2}, \frac{n-m-p+q}{2}) \in (\{0,\frac{1}{2}\}^g + \mathbb{Z}^g)^4$
und $\widetilde{n}+\widetilde{m}+\widetilde{p}+\widetilde{q} \in 2\mathbb{Z}^g$.

ad iii. $n^t\Omega n + m^t\Omega m + p^t\Omega p + q^t\Omega q$
$= n^t\Omega\widetilde{\widetilde{n}} + m^t\Omega\widetilde{\widetilde{m}} + p^t\Omega\widetilde{\widetilde{p}} + q^t\Omega\widetilde{\widetilde{q}}$
$= n^t\Omega\,\frac{1}{2}\,(\widetilde{n}+\widetilde{m}+\widetilde{p}+\widetilde{q}) + m^t\Omega\,\frac{1}{2}\,(\widetilde{n}+\widetilde{m}-\widetilde{p}-\widetilde{q}) + p^t\Omega\,\frac{1}{2}\,(\widetilde{n}-\widetilde{m}+\widetilde{p}-\widetilde{q}) + q^t\Omega\,\frac{1}{2}\,(\widetilde{n}-\widetilde{m}-\widetilde{p}+\widetilde{q})$
$= \frac{1}{2}\,(n+m+p+q)\Omega\widetilde{n} + \frac{1}{2}\,(n+m-p-q)\Omega\widetilde{m} + \frac{1}{2}\,(n-m+p-q)\Omega\widetilde{p} + \frac{1}{2}\,(n-m-p+q)\Omega\widetilde{q}$
$= \widetilde{n}^t\Omega\widetilde{n} + \widetilde{m}^t\Omega\widetilde{m} + \widetilde{p}^t\Omega\widetilde{p} + \widetilde{q}^t\Omega\widetilde{q}$.

ad iv. $(n^t,\ m^t,\ p^t,\ q^t)\ (x,\ y,\ u,\ v)^t$
$= (n^t,\ m^t,\ p^t,\ q^t)\ \frac{1}{4}\,4\,I\ (x,\ y,\ u,\ v)^t$
$= (\frac{1}{2}\,(n^t,\ m^t,\ p^t,\ q^t)\ A^t)\ (\frac{1}{2}\ A\ (x,\ y,\ u,\ v)^t)$
$= (\widetilde{n}^t,\ \widetilde{m}^t,\ \widetilde{p}^t,\ \widetilde{q}^t)\ (\widetilde{x},\ \widetilde{y},\ \widetilde{u},\ \widetilde{v})^t$.

$\square$

Satz 9
Seien $x,y,u,v \in \mathbb{C}^g$ und sei $(\widetilde{x},\widetilde{y},\widetilde{u},\widetilde{v}) = \phi(x,y,u,v)$. Dann gilt

$$2^g\ \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{x})\ \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{y})\ \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{u})\ \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{v}) = \sum_{a,b\in\{0,\frac{1}{2}\}^g} \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x)\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(y)\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(u)\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v).$$

Beweis
Da ϑ absolut und lokal gleichmäßig konvergiert, läßt sich die Summationsreihenfolge beliebig vertauschen. Betrachte die rechte Seite mit $a, b \in \{0, \frac{1}{2}\}^g$ und $n, m, p, q \in \mathbb{Z}^g$:

$$\begin{aligned}
&\sum_{a,b} \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (x)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (y)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (u)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (v) \\
&= \sum_{a,b} \left(\sum_{n} e^{\pi i (n+a)^t \Omega (n+a) + 2\pi i (n+a)^t (x+b)} + \dots + \sum_{q} e^{\pi i (q+a)^t \Omega (q+a) + 2\pi i (q+a)^t (v+b)} \right) \\
&= \sum_{a,b} \left(\sum_{n,m,p,q} e^{\pi i ((n+a)^t \Omega (n+a) + \dots + (q+a)^t \Omega (q+a)) + 2\pi i ((n+a)^t x + \dots + (q+a)^t v) + 2\pi i (n^t + \dots + q^t) b}\ \underbrace{e^{8\pi i a^t b}}_{=1} \right) \\
&= \sum_{a,b} \left(\sum_{n,m,p,q} e^{\pi i ((n+a)^t \Omega (n+a) + \dots + (q+a)^t \Omega (q+a)) + 2\pi i ((n+a)^t x + \dots + (q+a)^t v)}\ e^{2\pi i (n + \dots + q)^t\, b} \right).
\end{aligned}$$

Für $b \in \{0, \frac{1}{2}\}^g$ gilt $e^{2\pi i (n + \dots + q)^t\, b} = \begin{cases} 2^g, & n + \dots + q \in 2\mathbb{Z}^g, \\ 0, & n + \dots + q \notin 2\mathbb{Z}^g, \end{cases}$

und also gilt weiter

$$\begin{aligned}
&\sum_{a,b \in \{0, \frac{1}{2}\}^g} \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (x)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (y)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (u)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (v) \\
&= 2^g \sum_{a \in \{0, \frac{1}{2}\}^g} \left(\sum_{\substack{n,m,p,q \in \mathbb{Z}^g \\ n+m+p+q \in 2\mathbb{Z}^g}} e^{\pi i ((n+a)^t \Omega (n+a) + \dots + (q+a)^t \Omega (q+a)) + 2\pi i ((n+a)^t x + \dots + (q+a)^t v)} \right) \\
&= 2^g \sum_{a \in \{0, \frac{1}{2}\}^g} \left(\sum_{\substack{n,m,p,q \in a + \mathbb{Z}^g \\ n+m+p+q \in 2\mathbb{Z}^g}} e^{\pi i (n^t \Omega n + \dots + q^t \Omega q) + 2\pi i (n^t x + \dots + q^t v)} \right) \\
&= 2^g \sum_{\widetilde{n}, \widetilde{m}, \widetilde{p}, \widetilde{q} \in \mathbb{Z}^g} e^{\pi i (\widetilde{n}^t \Omega \widetilde{n} + \dots + \widetilde{q}^t \Omega \widetilde{q}) + 2\pi i (\widetilde{n}^t \widetilde{x} + \dots + \widetilde{q}^t \widetilde{v})}, \text{ wegen Lemma 4} \\
&= 2^g\ \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\widetilde{x})\ \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\widetilde{y})\ \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\widetilde{u})\ \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\widetilde{v}).
\end{aligned}$$

□

Satz 10 (Riemannsche Theta–Formel)
Seien $c, d \in \frac{1}{2}\mathbb{Z}^g$, $x, y, u, v \in \mathbb{C}^g$ und sei $(\widetilde{x}, \widetilde{y}, \widetilde{u}, \widetilde{v}) = \phi(x, y, u, v)$. Dann gilt

$$\begin{aligned}
&2^g\ \vartheta \begin{bmatrix} c \\ d \end{bmatrix} (\widetilde{x})\ \vartheta \begin{bmatrix} c \\ d \end{bmatrix} (\widetilde{y})\ \vartheta \begin{bmatrix} c \\ d \end{bmatrix} (\widetilde{u})\ \vartheta \begin{bmatrix} c \\ d \end{bmatrix} (\widetilde{v}) \\
&= \sum_{a,b \in \{0, \frac{1}{2}\}^g} e^{4\pi i (a^t d - b^t c)} \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (x)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (y)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (u)\ \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (v).
\end{aligned}$$

Beweis
Ersetze in Satz 9 x durch $x + 2\Omega c + 2d$ und verändere y, u, v nicht. Wegen $\widetilde{x} = \frac{1}{2}(x + y + u + v)$ verändert sich $\widetilde{x}$ zu $\widetilde{x} + \Omega c + d$ und $\widetilde{y}, \widetilde{u}, \widetilde{v}$ verändern sich analog:

$$\begin{aligned}
&2^g\, \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{x} + \Omega c + d)\; \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{y} + \Omega c + d)\; \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{u} + \Omega c + d)\; \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{v} + \Omega c + d)\\
&= \sum_{a,b\in\{0,\frac{1}{2}\}^g} \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x + 2\Omega c + 2d)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(y)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(u)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v).
\end{aligned}$$

Durch Anwenden von Lemma 3 auf die linke Seite folgt:

$$\begin{aligned}
&2^g\, \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{x} + \Omega c + d)\; \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{y} + \Omega c + d)\; \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{u} + \Omega c + d)\; \vartheta\begin{bmatrix}0\\0\end{bmatrix}(\widetilde{v} + \Omega c + d)\\
&= 2^g e^{-4\pi i c^t \Omega c - 2\pi i c^t(\widetilde{x} + \ldots + \widetilde{v}) - 8\pi i c^t d}\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(\widetilde{x})\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(\widetilde{y})\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(\widetilde{u})\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(\widetilde{v}).
\end{aligned}$$

Anwenden von Lemma 2 auf die rechte Seite ergibt:

$$\begin{aligned}
&\sum_{a,b\in\{0,\frac{1}{2}\}^g} \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x + 2\Omega c + 2d)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(y)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(u)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v)\\
&= \sum_{a,b\in\{0,\frac{1}{2}\}^g} e^{-\pi i (2c)^t \Omega (2c) - 2\pi i (2c)^t (x+b) + 2\pi i a^t (2d)}\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(y)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(u)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v).
\end{aligned}$$

Also gilt zusammen:

$$\begin{aligned}
&2^g\, \vartheta\begin{bmatrix}c\\d\end{bmatrix}(\widetilde{x})\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(\widetilde{y})\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(\widetilde{u})\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(\widetilde{v})\\
&= \sum_{a,b\in\{0,\frac{1}{2}\}^g} e^{4\pi i c^t \Omega c + 2\pi i c^t(\widetilde{x} + \ldots + \widetilde{v}) + 8\pi i c^t d - 4\pi i c^t \Omega c - 4\pi i c^t (x+b) + 4\pi i a^t d}\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x) \ldots \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v)\\
&= \sum_{a,b\in\{0,\frac{1}{2}\}^g} e^{2\pi i c^t(\widetilde{x} + \ldots + \widetilde{v}) - 4\pi i c^t x + 8\pi i c^t d - 4\pi i c^t b + 4\pi i a^t d}\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x) \ldots \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v)\\
&= \sum_{a,b\in\{0,\frac{1}{2}\}^g} e^{2\pi i c^t(\widetilde{x} + \ldots + \widetilde{v}) - 4\pi i c^t \frac{1}{2}(\widetilde{x} + \ldots + \widetilde{v}) + 8\pi i c^t d - 4\pi i c^t b + 4\pi i a^t d}\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x) \ldots \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v)\\
&= \sum_{a,b\in\{0,\frac{1}{2}\}^g} \underbrace{e^{8\pi i c^t d}}_{=1}\; e^{-4\pi i c^t b + 4\pi i a^t d}\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(y)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(u)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v)\\
&= \sum_{a,b\in\{0,\frac{1}{2}\}^g} e^{4\pi i (a^t d - c^t b)}\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(y)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(u)\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(v).
\end{aligned}$$

$\square$

Speziell $x = y$ und $u = v$ implizieren $\widetilde{x} = x + u, \widetilde{y} = x - u$ und $\widetilde{u} = \widetilde{v} = 0$, so daß gilt

$$2^g\, \vartheta\begin{bmatrix}c\\d\end{bmatrix}(x + u)\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(x - u)\; \vartheta\begin{bmatrix}c\\d\end{bmatrix}(0)^2 = \sum_{a,b\in\{0,\frac{1}{2}\}^g} e^{4\pi i (a^t d - c^t b)}\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x)^2\; \vartheta\begin{bmatrix}a\\b\end{bmatrix}(u)^2. \tag{10}$$

Nach Korollar 3 kommt es bis auf ein Vorzeichen nur auf die Charakteristiken $a, b \in \{0, \frac{1}{2}\}^g$ an. Seien also $c, d \in \frac{1}{2}\mathbb{Z}^g$, so zerlege c und d eindeutig in folgender Weise: $c = a + p$ und $d = b + q$ mit $a, b \in \{0, \frac{1}{2}\}^g$ und $p, q \in \mathbb{Z}^g$. Dann ist

$$\vartheta \begin{bmatrix} c \\ d \end{bmatrix} (z) = \vartheta \begin{bmatrix} a+p \\ b+q \end{bmatrix} (z) = e^{2\pi i a^t q}\, \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z), \ z \in \mathbb{C}^g.$$

Betrachte die linke Seite der Gleichung (10):

$$2^g\, \vartheta \begin{bmatrix} c \\ d \end{bmatrix} (x+u)\, \vartheta \begin{bmatrix} c \\ d \end{bmatrix} (x-u)\, \vartheta \begin{bmatrix} c \\ d \end{bmatrix} (0)^2 = 2^g\, \underbrace{e^{8\pi i a^t q}}_{=1}\, \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (x+u)\, \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (x-u)\, \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (0)^2$$

und erhalte eine Additionsformel für ϑ:

Korollar 5 (Erste Additionsformel für ϑ)
Seien $c, d \in \{0, \frac{1}{2}\}^g$ und $x, u \in \mathbb{C}^g$. Dann gilt

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

□

In dieser ersten Additionsformel wird die Summe über 2^{2g} Glieder gebildet, während die noch folgende zweite Formel die Anzahl der Summanden verringern und deshalb die Formel verbessern wird.

3.3 Additionsformel für die ϑ–Funktion

Die Additionsformel für ϑ aus Korollar 5 bietet noch Möglichkeiten zur Vereinfachung. Ich werde die verschiedenen Charakteristiken durch ein Erzeugendensystem parametrisieren, so daß letztendlich deutlich weniger Charakteristiken zur Summation zugelassen werden.

Ich erinnere an die Indexmenge $B = \{1, 2, ..., 2g+2\}$ der Nullstellen von $f(x) = \prod_{i=1}^{2g+1}(x - a_i)$, $a_{2g+2} = \infty$ aus Abschnitt 1.4. Sei $B' = B - \{2g+2\} = \{1, 2, ..., 2g+1\}$. Den Nullstellen a_i, $i \in B$, werden Vektoren der Länge $2g$ in folgender Weise zugeordnet:

$$\begin{aligned}
\eta_{2i-1} &= \begin{pmatrix} (0...0\ \frac{1}{2}\ 0...0)^t \\ (\frac{1}{2}...\frac{1}{2}\ 0\ 0...0)^t \end{pmatrix}, \ i = 1, ..., g, \\
&\qquad\qquad \uparrow \\
&\qquad\qquad i \\
&\qquad\qquad \downarrow \\
\eta_{2i} &= \begin{pmatrix} (0...0\ \frac{1}{2}\ 0...0)^t \\ (\frac{1}{2}...\frac{1}{2}\ \frac{1}{2}\ 0...0)^t \end{pmatrix}, \ i = 1, ..., g, \\
\eta_{2g+1} &= \begin{pmatrix} (0...0)^t \\ (\frac{1}{2}...\frac{1}{2})^t \end{pmatrix}, \\
\eta_{2g+2} &= \begin{pmatrix} (0...0)^t \\ (0...0)^t \end{pmatrix}.
\end{aligned}$$

Beispiel 8 ($g = 1$)

$$\eta_1 = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}, \ \eta_2 = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \ \eta_3 = \begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix}, \ \eta_4 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Beispiel 9 ($g = 2$)

$$\eta_1 = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; \eta_2 = \begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix}, \; \eta_3 = \begin{pmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix}, \; \eta_4 = \begin{pmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \; \eta_5 = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \; \eta_6 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Ziel ist, aus der Menge $\{\eta_1, ..., \eta_{2g+2}\}$ ein Erzeugendensystem für die Charakteristiken aus $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ zu bilden. Betrachte die Potenzmenge $\mathcal{P}(B) = \{T \mid T \subseteq B\}$ von B und für $S, T \in \mathcal{P}(B)$ die Verknüpfung

$$S \circ T = (S \cup T) - (S \cap T).$$

$\mathcal{P}(B)$ ist mit dieser Verknüpfung eine Gruppe, denn:
$S, T \in \mathcal{P}(B) \implies S \circ T \in \mathcal{P}(B)$,
$\emptyset \in \mathcal{P}(B)$ ist das neutrale Element: $\emptyset \circ S = S = S \circ \emptyset$ für alle $S \in \mathcal{P}(B)$,
$S \in \mathcal{P}(B)$ ist zu sich selbst invers: $S \circ S = (S \cup S) - (S \cap S) = S - S = \emptyset$. $\mathcal{P}(B)$ ist sogar abelsch.

Üblicherweise wird mit $\sharp\, H$ die Anzahl der Elemente in einer Gruppe H bezeichnet. Betrachte die Gruppe $G = \{S \subseteq B \mid \sharp\, S \text{ gerade}\} \subset \mathcal{P}(B)$. Es gilt $\sharp\, G = 2^{2g+1}$.

Beispiel 10 ($g = 1$)

$$\begin{aligned} B &= \{1, 2, 3, 4\}, \\ G &= \{\emptyset, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3, 4\}\}, \\ \sharp\, G &= 8. \end{aligned}$$

Beispiel 11 ($g = 2$)

$$\begin{aligned} B &= \{1, 2, 3, 4, 5, 6\}, \\ G &= \{\emptyset, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{1, 6\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{2, 6\}, \{3, 4\}, \{3, 5\}, \\ &\quad \{3, 6\}, \{4, 5\}, \{4, 6\}, \{5, 6\}, \{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{1, 2, 3, 6\}, \{1, 2, 4, 5\}, \\ &\quad \{1, 2, 4, 6\}, \{1, 2, 5, 6\}, \{1, 3, 4, 5\}, \{1, 3, 4, 6\}, \{1, 3, 5, 6\}, \{1, 4, 5, 6\}, \{2, 3, 4, 5\}, \\ &\quad \{2, 3, 4, 6\}, \{2, 3, 5, 6\}, \{2, 4, 5, 6\}, \{3, 4, 5, 6\}, \{1, 2, 3, 4, 5, 6\}\}, \\ \sharp\, G &= 32. \end{aligned}$$

Die folgende Funktion wird die verschiedenen Charakteristiken aus $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ mit Elementen aus G darstellen.

Lemma 5
Durch die Zuordnung

$$\begin{aligned} \eta : G &\longrightarrow \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}, \\ S &\longmapsto \sum_{k \in S} \eta_k \end{aligned}$$

wird jedem $S \in G$ eine Charakteristik zugeordnet und η ist ein Epimorphismus abelscher Gruppen.

Beweis
Wegen

$$
\begin{aligned}
\eta_{S\circ T} &= \sum_{k\in S\circ T} \eta_k \\
&\equiv \sum_{k\in S\circ T} \eta_k \;+\; 2 \sum_{k\in S\cap T} \eta_k, \text{ da Einträge } \eta_k \in \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g} \\
&\equiv \sum_{k\in (S\cup T)-(S\cap T)} \eta_k \;+\; 2 \sum_{k\in S\cap T} \eta_k \\
&\equiv \sum_{k\in S\cup T} \eta_k \;-\; \sum_{k\in S\cap T} \eta_k \;+\; 2 \sum_{k\in S\cap T} \eta_k \\
&\equiv \sum_{k\in S\cup T} \eta_k \;+\; \sum_{k\in S\cap T} \eta_k \\
&\equiv \sum_{k\in S} \eta_k \;+\; \sum_{k\in T} \eta_k \\
&\equiv \eta_S \;+\; \eta_T \mod \mathbb{Z}^{2g}
\end{aligned}
$$

ist η ein Morphismus, der wegen $\sharp\, G = 2^{2g+1} = 2 \cdot 2^{2g} = 2 \cdot \sharp\, (\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g})$ und $\ker(\eta) = \{\emptyset, B\}$ sogar ein Epimorphismus ist.

$\square$

Dies impliziert

Korollar 6

$$\eta : \overline{G} = G/\ker(\eta) = G/(S \sim \mathcal{C}S) \longrightarrow \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$$

ist ein Isomorphismus.

Hierdurch lassen sich die Charakteristiken mit Elementen aus $\overline{G}$ parametrisieren. Im weiteren wird die Notation $\eta_{i,j}$ für $\eta_i + \eta_j$ benutzt.

Beispiel 12 ($g = 1$)

$$\overline{G} = G/\{1,2,3,4\} = \{\overline{\emptyset}, \overline{\{1,4\}}, \overline{\{2,4\}}, \overline{\{3,4\}}\},\ \sharp\, \overline{G} = 2^2 = 4,$$

$$\eta_{1,4} = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix},\ \eta_{2,4} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix},\ \eta_{3,4} = \begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix},\ \eta_{\emptyset} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Beispiel 13 ($g = 2$)

$$
\begin{aligned}
\overline{G} &= G/\{1,2,3,4,5,6\} \\
&= \{\overline{\emptyset}, \overline{\{1,2\}}, \overline{\{1,3\}}, \overline{\{1,4\}}, \overline{\{1,5\}}, \overline{\{1,6\}}, \overline{\{2,3\}}, \overline{\{2,4\}}, \overline{\{2,5\}}, \overline{\{2,6\}}, \overline{\{3,4\}}, \\
&\quad \overline{\{3,5\}}, \overline{\{3,6\}}, \overline{\{4,5\}}, \overline{\{4,6\}}, \overline{\{5,6\}}\},
\end{aligned}
$$

$$\sharp\, \overline{G} = 16,$$

$$\eta_{1,2} = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix},\ \eta_{1,3} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix},\ \eta_{1,4} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix},\ \eta_{1,5} = \begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix},\ \eta_{1,6} = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$\eta_{2,3} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 0 \end{pmatrix}, \ \eta_{2,4} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \end{pmatrix}, \ \eta_{2,5} = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{1}{2} \end{pmatrix}, \ \eta_{2,6} = \begin{pmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix}, \ \eta_{3,4} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{2} \end{pmatrix},$$

$$\eta_{3,5} = \begin{pmatrix} 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \end{pmatrix}, \ \eta_{3,6} = \begin{pmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix}, \ \eta_{4,5} = \begin{pmatrix} 0 \\ \frac{1}{2} \\ 0 \\ 0 \end{pmatrix}, \ \eta_{4,6} = \begin{pmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \ \eta_{5,6} = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \ \eta_{\emptyset} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Ziel ist an dieser Stelle, den neuen Formalismus in die erste Additionsformel einfließen zu lassen. Dabei wird für den dort vorkommenen Ausdruck $e^{4\pi i(a^t d - b^t c)}$ in der neuen Notation gesetzt:

$$\left\langle \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \right\rangle := 4(a^t d - b^t c) \text{ für } a, b, c, d \in \left\{0, \frac{1}{2}\right\}^g.$$

Für $\overline{S}, \overline{T} \in \overline{G}$ gilt $\langle \eta_S, \eta_T \rangle = \left\langle \begin{pmatrix} (\eta_S)_1 \\ (\eta_S)_2 \end{pmatrix}, \begin{pmatrix} (\eta_T)_1 \\ (\eta_T)_2 \end{pmatrix} \right\rangle = 4\left((\eta_S)_1^t (\eta_T)_2 - (\eta_S)_2^t (\eta_T)_1\right)$, wobei $(\eta_S)_1$ bzw. $(\eta_S)_2$ der Vektor der ersten bzw. zweiten g Einträge von (η_S) sein soll und S bzw. T Repräsentanten der Äquivalenzklassen von $\overline{S}$ bzw. $\overline{T}$ sind. In der neuen Notation lautet Korollar 5 nun:

Korollar 7
Seien $\overline{T} \in \overline{G}$ und $x, u \in \mathbb{C}^g$. Dann gilt

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

Daraus ergibt sich

Lemma 6
Seien $\overline{S}, \overline{T} \in \overline{G}$. Dann gilt

$$\langle \eta_S, \eta_T \rangle \ \equiv \ \sharp\,(S \cap T) \mod 2, \tag{11}$$

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

Beweis
$\langle \cdot, \cdot \rangle$ ist wohldefiniert, da von der Wahl der Repräsentanten S aus $\overline{S}$ bzw. T aus $\overline{T}$ unabhängig, wegen $\eta_S, \eta_T \in \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$. Desweiteren ist $\sharp\,(S \cap T)$ wohldefiniert wegen

$$\begin{aligned} \sharp\,(\mathcal{C}S \cap T) &= \sharp\,T - \sharp\,(S \cap T) \equiv \sharp\,(S \cap T) \mod 2, \\ \sharp\,(S \cap \mathcal{C}T) &= \sharp\,S - \sharp\,(T \cap S) \equiv \sharp\,(T \cap S) \mod 2. \end{aligned}$$

Zeige nun: $\langle \eta_j, \eta_k \rangle \ \equiv \ 1 + \delta_{j\,k} \mod 2$ für $j, k \in B'$ ($\delta_{j\,k}$ Kroneckersymbol).
Damit ist:

$$\langle \eta_S, \eta_T \rangle = \sum_{\substack{j \in S \\ k \in T}} \langle \eta_j, \eta_k \rangle = \sum_{\substack{j \in S \\ k \in T}} 1 + \delta_{j\,k} \mod 2.$$

Es folgt:

$$\begin{aligned}\sum_{\substack{j\in S\\k\in T}} 1+\delta_{j\,k} &= \sum_{j\in S}\left(\sum_{\substack{j\in S\cap T\\ j\in T}} 1+\delta_{j\,k} \;+\; \sum_{\substack{j\notin S\cap T\\ j\in T}} 1+\delta_{j\,k}\right)\\ &= \sharp\, T - \sharp\,(S\cap T)\\ &\equiv \sharp\,(S\cap T) \mod 2, \text{ da } \sharp\, T \text{ gerade.}\end{aligned}$$

$\langle\cdot,\cdot\rangle : \overline{G}\times\overline{G} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ ist eine symmetrische Bilinearform. Die Symmetrie ist nach der Definition modulo $2\mathbb{Z}$ klar. Zu zeigen ist, daß $\langle\eta_S,\eta_{R\circ T}\rangle \equiv \langle\eta_S,\eta_R\rangle + \langle\eta_S,\eta_T\rangle \mod 2$ gilt, $\overline{S},\overline{T},\overline{R}\in\overline{G}$:

$$\begin{aligned}\langle\eta_S,\eta_{R\circ T}\rangle &\equiv \sharp\,(S\cap(R\circ T))\\ &= \sharp\,(S\cap((R\cup T)-(R\cap T)))\\ &= \sharp\,(((S\cap R)-T)\cup((S\cap T)-R))\\ &= \sharp\,(((S\cap R)-(S\cap R\cap T))\cup((S\cap T)-(S\cap R\cap T)))\\ &\equiv \sharp\,(S\cap R)+\sharp\,(S\cap T)\\ &\equiv \langle\eta_S,\eta_R\rangle+\langle\eta_S,\eta_T\rangle \mod 2.\end{aligned}$$

□ Es bezeichne $U\subset B$ die Menge der ungeraden Zahlen in B, d.h. $U=\{1,3,...,2g+1\}$. Nach wie vor ist $V\subset B$ die Menge der geraden Zahlen in B, d.h. $V=\{2,4,...,2g+2\}$.

Lemma 7
Sei $S\in G$. Dann gilt

$$\vartheta[\eta_S] \text{ ist eine gerade Funktion } \iff \sharp\,(S\circ U)\ \equiv\ g+1 \mod 4.$$

Beweis
Nach Korollar 4 gilt $\vartheta[\eta_S](-z) = e^{4\pi i(\eta_S)_1^t(\eta_S)_2}\ \vartheta[\eta_S](z)$, also ist $\vartheta[\eta_S]$ genau dann gerade, wenn $4\,(\eta_S)_1^t(\eta_S)_2$ gerade ist. Also gilt

$$4\,(\eta_S)_1^t(\eta_S)_2\equiv 0 \mod 2 \iff \vartheta \text{ ist eine gerade Funktion.}$$

Betrachte $\sharp\,(S\circ U)=\sharp\,((S\cup U)-(S\cap U))=\sharp\,S+\sharp\,U-2\,\sharp\,(S\cap U)$.
Es ist $\sharp\,(S\circ U)\ \equiv\ g+1 \mod 2$, da $S\in G$ und $\sharp\,U=g+1$. Wegen

$$\sharp\,(S\circ U)-(g+1)\equiv 0 \mod 4 \iff \frac{\sharp\,(S\circ U)-(g+1)}{2}\equiv 0 \mod 2$$

wird also die zur Behauptung äquivalente Aussage bewiesen:

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

Betrachte dazu die Abbildung

$$\begin{aligned}&\varphi : G\longrightarrow \mathbb{Z}/2\mathbb{Z},\\ &\qquad S\longmapsto 4\,(\eta_S)_1^t(\eta_S)_2+\frac{\sharp\,(S\circ U)-(g+1)}{2} \mod 2.\end{aligned}$$

φ ist ein Gruppenisomorphismus, denn für $S, T \in G$ gilt:

$$
\begin{aligned}
&\varphi(S \circ T) \\
&\equiv 4\,(\eta_S + \eta_T)_1^t(\eta_S + \eta_T)_2 + \frac{\sharp\,(S \circ T \circ U) - (g+1)}{2}, \text{ da } \eta_{S\circ T} \equiv \eta_S + \eta_T \mod 2, \\
&\equiv 4\,(\eta_S)_1^t(\eta_S)_2 + 4\,(\eta_T)_1^t(\eta_T)_2 + 4\,(\eta_S)_1^t(\eta_T)_2 + 4\,(\eta_T)_1^t(\eta_S)_2 \\
&\quad + \frac{\sharp\,(S \cup (T \circ U) - S \cap (T \circ U)) - (g+1)}{2} \\
&\equiv 4\,(\eta_S)_1^t(\eta_S)_2 + 4\,(\eta_T)_1^t(\eta_T)_2 + 4\,(\eta_S)_1^t(\eta_T)_2 - 4\,(\eta_S)_2^t(\eta_T)_1 \\
&\quad + \frac{\sharp\,(S \cup (T \circ U) - S \cap (T \circ U)) - (g+1)}{2} \\
&\equiv 4\,(\eta_S)_1^t(\eta_S)_2 + 4\,(\eta_T)_1^t(\eta_T)_2 + \langle \eta_S, \eta_T \rangle \\
&\quad + \frac{\sharp\,S + \sharp\,(T \circ U) - 2\,\sharp\,(S \cap (T \circ U)) - (g+1)}{2} + \frac{\sharp\,U - (g+1)}{2}, \text{ wegen } \sharp\,U = g+1 \\
&\equiv 4\,(\eta_S)_1^t(\eta_S)_2 + 4\,(\eta_T)_1^t(\eta_T)_2 + \langle \eta_S, \eta_T \rangle - \sharp\,(S \cap (T \circ U)) \\
&\quad + \frac{\sharp\,S + \sharp\,(T \circ U) - (g+1)}{2} + \frac{\sharp\,U - (g+1)}{2} \\
&\equiv 4\,(\eta_S)_1^t(\eta_S)_2 + 4\,(\eta_T)_1^t(\eta_T)_2 + \sharp\,(S \cap T) - (\sharp\,(S \cap T) + \sharp\,(S \cap U) - 2\sharp(S \cap T \cap U)) \\
&\quad + \frac{\sharp\,S + \sharp\,U - (g+1) + \sharp\,(T \circ U) - (g+1)}{2} \\
&\equiv 4\,(\eta_S)_1^t(\eta_S)_2 + 4\,(\eta_T)_1^t(\eta_T)_2 - \sharp\,(S \cap U) \\
&\quad + \frac{\sharp\,(S \circ U) - 2\sharp\,(S \cap U) - (g+1) + \sharp\,(T \circ U) - (g+1)}{2} \\
&\equiv 4\,(\eta_S)_1^t(\eta_S)_2 + 4\,(\eta_T)_1^t(\eta_T)_2 + \frac{\sharp\,(S \circ U) - (g+1)}{2} + \frac{\sharp\,(T \circ U) - (g+1)}{2} \\
&\equiv \varphi(S) + \varphi(T) \mod 2.
\end{aligned}
$$

Betrachte nun für $S = \{k, \infty\},\ k \in B' = \{1, 2, ..., 2g-1\}, U = \{1, 3, ..., 2g+1\},\ \sharp\,U = g+1:$

$$\sharp\,(S \circ U) = \sharp\,((S \cup U) - (S \cap U)) = \sharp U + 1 + (-1)^k = g + 2 + (-1)^k.$$

$$\frac{\sharp\,(S \circ U) - (g+1)}{2} = \frac{g + 2 + (-1)^k - (g+1)}{2} = \frac{1 + (-1)^k}{2} = \begin{cases} 1, & k \text{ gerade}, \\ 0, & k \text{ ungerade}. \end{cases}$$

Andererseits gibt es für $4\,(\eta_S)_1^t(\eta_S)_2$ folgende Fälle:

$k = 2i-1 : 4\,(\eta_{2i-1})_1^t(\eta_{2i-1})_2 = 0,$ für $i = 1, ..., g$

$k = 2i : \quad 4\,(\eta_{2i})_1^t(\eta_{2i})_2 = 1,$ für $i = 1, ..., g$

$k = 2g+1 : 4\,(\eta_{2g+1})_1^t(\eta_{2g+1})_2 = 0.$

Somit ist

$$4\,(\eta_S)_1^t(\eta_S)_2 = \begin{cases} 1, & k \text{ gerade}, \\ 0, & k \text{ ungerade}. \end{cases}$$

Zusammen gilt also für $S\{k, \infty\}$:

$$\varphi(S) = 4\,(\eta_S)_1^t(\eta_S)_2 + \frac{\sharp\,(S \circ U) - (g+1)}{2} \equiv 0 \mod 2.$$

Da $S = \{k, \infty\}$ alle Elemente von G via ϕ erzeugt, ist $\varphi(S) \equiv 0 \mod 2$ für alle $S \in G$. □

Mumford stellte fest, daß die ϑ–Funktion in 0 genau dann verschwindet, wenn an die Charakteristik eine Bedingung geknüpft ist. Ich zitiere den entscheidenden Satz:

Satz 11 ([Mumford 1984], IIIa, 6.7)
Sei $\overline{S} \in \overline{G}$. Dann gilt

$$\vartheta[\eta_S](0) = 0 \iff \sharp\,(S \circ U) \neq g+1.$$

Die Bedingung $\sharp\,(S \circ U) \neq g+1$ ist unabhängig von der Wahl des Repräsentanten S von $\overline{S}$, denn nach der Mengentheorie gilt:
$\sharp\,(\mathcal{C}S \circ U) = \sharp\,\mathcal{C}(S \circ U) = \sharp\,B - \sharp\,(S \circ U) = 2g+2-\sharp\,(S \circ U) \neq g+1,$ da $\sharp\,(S \circ U) \neq g+1$.

Ziel soll nun sein, die Anzahl der Summanden in der Additionsformel zu verringern. Nach wie vor ist $U = \{1, 3, ..., 2g+1\},\ V = \{2, 4, ..., 2g+2\}$. Ich definiere

$$\mathcal{U} = \{\overline{S} \in \overline{G} \mid S \subseteq U \vee \mathcal{C}S \subseteq U\},$$
$$\mathcal{V} = \{\overline{T} \in \overline{G} \mid T \subseteq V \vee \mathcal{C}T \subseteq V\}.$$

Beispiel 14 ($g = 1$)

$$\mathcal{U} = \{\overline{\emptyset}, \overline{\{1,3\}}\},$$
$$\mathcal{V} = \{\overline{\emptyset}, \overline{\{2,4\}}\}.$$

Beispiel 15 ($g = 2$)

$$\mathcal{U} = \{\overline{\emptyset}, \overline{\{1,3\}}, \overline{\{1,5\}}, \overline{\{3,5\}}\},$$
$$\mathcal{V} = \{\overline{\emptyset}, \overline{\{2,4\}}, \overline{\{2,6\}}, \overline{\{4,6\}}\}.$$

$\mathcal{U},\ \mathcal{V}$ sind Untergruppen von $\overline{G}$ und sie sind bezüglich der Bilinearform $\langle\cdot,\cdot\rangle$ zueinander orthogonal, d.h. für $U \in \mathcal{U},\ V \in \mathcal{V}$ gilt $\langle \eta_U, \eta_V\rangle = \sharp\,(U \cap V) = 0$. Es ist $\sharp\,\mathcal{U} = 2^g$, denn wegen $S \sim \mathcal{C}S$ ist die Ordnung von $\mathcal{U}$ gleich der Anzahl der Teilmengen gerader Ordnung in $\{a_1, a_3, ..., a_{2g+1}\}$. Analog ist $\sharp\,\mathcal{V} = 2^g$.

Lemma 8
Es gelten die folgenden Aussagen:

i. Für $\overline{S} \in (\mathcal{U} \cup \mathcal{V}) - \overline{\{\emptyset\}}$ gilt $\vartheta[\eta_S](0) = 0$.

ii. Für alle $\overline{T} \in \overline{G}$ gilt $\sum\limits_{\overline{S}\in\mathcal{U}} e^{\pi i\langle \eta_S, \eta_T\rangle} = \begin{cases} 2^g, & \overline{T} \in \mathcal{V}, \\ 0, & \overline{T} \notin \mathcal{V}. \end{cases}$

iii. Für alle $\overline{S} \in \overline{G}$ gilt $\sum\limits_{\overline{T}\in\mathcal{V}} e^{\pi i\langle \eta_S, \eta_T\rangle} = \begin{cases} 2^g, & \overline{S} \in \mathcal{U}, \\ 0, & \overline{S} \notin \mathcal{U}. \end{cases}$

Beweis
ad i. Sei $\overline{S} \in \mathcal{U}, \overline{S} \neq \overline{\emptyset}$. Wähle einen Repräsentanten S von $\overline{S}$, der nur ungerade Elemente enthält. Dann ist $S \subseteq U$ und $\sharp\,S \neq 0$ impliziert:
$\sharp\,(S \circ U) = \sharp\,((S \cup U) - (S \cap U)) = \sharp\,U - \sharp\,S = g+1-\sharp\,S \neq g+1$. Nach Satz 11 ist $\vartheta[\eta_S](0) = 0$. Analog für $\overline{T} \in \mathcal{V}$.

ad ii. Sei $\overline{T} \in \mathcal{V}$. Dann ist $\sum_{\overline{S}\in\mathcal{U}} e^{\pi i \langle \eta_S, \eta_T \rangle} = \sum_{\overline{S}\in\mathcal{U}} 1 = \sharp\, \mathcal{U} = 2^g$, da $\mathcal{U}$ und $\mathcal{V}$ orthogonal zueinander sind.
Sei nun $\overline{T} \in \overline{G} - \mathcal{V}$. Dann existieren ungerade Elemente $a \in T$ und $b \in \mathcal{C}T$. Betrachte

$$\begin{aligned} f_{\overline{T}} : \mathcal{U} &\longrightarrow \mathbb{Z}/2\mathbb{Z}, \\ \overline{S} &\longmapsto \langle \eta_S, \eta_T \rangle \equiv \sharp\,(S \cap T) \mod 2. \end{aligned}$$

$f_{\overline{T}}$ ist surjektiv, da wegen $\sharp\,(\{a,b\} \cap T) = 1$ der Schnitt von S und T nicht leer ist. Nach dem Homomorphiesatz ist $\sharp\, \ker(f_{\overline{T}}) = \frac{1}{2} \cdot \sharp\, \mathcal{U}$. Für $\overline{S} \in \ker(f_{\overline{T}})$ gilt $\langle \eta_S, \eta_T \rangle = 0$ und für $\overline{S} \in \mathcal{U} - \ker(f_{\overline{T}})$ gilt $\langle \eta_S, \eta_T \rangle = 1$. Dies impliziert
$\sum\limits_{\overline{S}\in\mathcal{U}} e^{\pi i \langle \eta_S, \eta_T \rangle} = \sum\limits_{\overline{S}\in\ker(f_{\overline{T}})} e^{\pi i \langle \eta_S, \eta_T \rangle} + \sum\limits_{\overline{S}\in\mathcal{U}-\ker(f_{\overline{T}})} e^{\pi i \langle \eta_S, \eta_T \rangle} = \frac{1}{2} \cdot \sharp\, U - (\sharp\, U - \frac{1}{2} \cdot \sharp\, U) = 0.$

ad iii. Analog zu ii.

$\square$

Mit diesen Eigenschaften lassen sich die Summanden in der ersten Additionsformel, die ich in Korollar 7 bereits in die neue Notation umgewandelt habe, dezimieren. Ich erhalte daraus eine erste Vereinfachung.

Satz 12
Seien $x, u \in \mathbb{C}^g$. Dann gelten

i. $\vartheta[0](x+u)\ \vartheta[0](x-u)\ \vartheta[0](0)^2 = \sum\limits_{\overline{S}\in\mathcal{U}} \vartheta[\eta_S](x)^2\ \vartheta[\eta_S](u)^2,$

ii. $\vartheta[0](x+u)\ \vartheta[0](x-u)\ \vartheta[0](0)^2 = \sum\limits_{\overline{T}\in\mathcal{V}} \vartheta[\eta_T](x)^2\ \vartheta[\eta_T](u)^2,$

wobei die Charakteristik von $\vartheta[0](z)$, $z \in \mathbb{C}^g$, ein $2g$–dimensionaler Null–Vektor ist.

Beweis

ad i. Summiere die Gleichung aus Korollar 7 über $\overline{T} \in \mathcal{V}$, teile auf und nutze Lemma 8 aus.

$$\begin{aligned}
&\sum_{\overline{T}\in\mathcal{V}} 2^g\ \vartheta[\eta_T](x+u)\ \vartheta[\eta_T](x-u)\ \vartheta[\eta_T](0)^2 \\
&= \sum_{\overline{T}\in\mathcal{V}} \sum_{\overline{S}\in\overline{G}} e^{\pi i \langle \eta_S, \eta_T \rangle}\ \vartheta[\eta_S](x)^2\ \vartheta[\eta_S](u)^2 \\
\Longleftrightarrow\ & 2^g\ \vartheta[\eta_\emptyset](x+u)\ \vartheta[\eta_\emptyset](x-u)\ \vartheta[\eta_\emptyset](0)^2 \\
&\quad + \sum_{\overline{T}\in\mathcal{V}-\overline{\emptyset}} 2^g\ \vartheta[\eta_T](x+u)\ \vartheta[\eta_T](x-u)\ \vartheta[\eta_T](0)^2 \\
&= \sum_{\overline{S}\in\mathcal{U}} \left(\sum_{\overline{T}\in\mathcal{V}} e^{\pi i \langle \eta_S, \eta_T \rangle} \right) \vartheta[\eta_S](x)^2\ \vartheta[\eta_S](u)^2 \\
&\quad + \sum_{\overline{S}\in\overline{G}-\mathcal{U}} \left(\sum_{\overline{T}\in\mathcal{V}} e^{\pi i \langle \eta_S, \eta_T \rangle} \right) \vartheta[\eta_S](x)^2\ \vartheta[\eta_S](u)^2
\end{aligned}$$

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

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

ad ii. Analog zu i.

□

An dieser Stelle folgt die zweite Additionsformel für ϑ. Für spätere Zwecke und aus beweistechnischen Gründen ist es sinnvoll, sich der alten Bezeichung $a, b \in \{0, \frac{1}{2}\}^g$ für die Charakteristik zu bedienen.

Satz 13 (Zweite Additionsformel für ϑ)
Seien $a, b \in \{0, \frac{1}{2}\}^g$ und $x, u \in \mathbb{C}^g$. Dann gelten

i. $$\vartheta\begin{bmatrix}a\\b\end{bmatrix}(x+u)\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x-u)\ \vartheta[0](0)^2 = \sum_{\overline{S}\in\mathcal{U}} e^{4\pi i a^t(\eta_S)_2}\ \vartheta\left[\eta_S + \begin{pmatrix}a\\b\end{pmatrix}\right](x)^2\ \vartheta[\eta_S](u)^2,$$

ii. $$\vartheta\begin{bmatrix}a\\b\end{bmatrix}(x+u)\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x-u)\ \vartheta[0](0)^2 = \sum_{\overline{T}\in\mathcal{V}} e^{4\pi i a^t(\eta_T)_2}\ \vartheta\left[\eta_T + \begin{pmatrix}a\\b\end{pmatrix}\right](x)^2\ \vartheta[\eta_T](u)^2.$$

Beweis
ad i. In Satz 12 i. ersetze ich x durch $x + \Omega a + b$,

$$\vartheta[0](x+u+\Omega a+b)\ \vartheta[0](x-u+\Omega a+b)\ \vartheta[0](0)^2 = \sum_{\overline{S}\in\mathcal{U}} \vartheta[\eta_S](x+\Omega a+b)^2\ \vartheta[\eta_S](u)^2,$$

und wende auf beide Seiten Lemma 3 an:

$$\begin{aligned}
&\left(e^{-\pi i a^t\Omega a - 2\pi i a^t(z+b)}\right)^2\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x+u)\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x-u)\ \vartheta[0](0)^2\\
&= \sum_{\overline{S}\in\mathcal{U}} \left(e^{-\pi i a^t\Omega a - 2\pi i a^t(z+(\eta_S)_2+b)}\right)^2\ \vartheta\left[\eta_S + \begin{pmatrix}a\\b\end{pmatrix}\right](x)^2\ \vartheta[\eta_S](u)^2\\
\iff &\vartheta\begin{bmatrix}a\\b\end{bmatrix}(x+u)\ \vartheta\begin{bmatrix}a\\b\end{bmatrix}(x-u)\ \vartheta[0](0)^2\\
&= \sum_{\overline{S}\in\mathcal{U}} e^{4\pi i a^t(\eta_S)_2}\ \vartheta\left[\eta_S + \begin{pmatrix}a\\b\end{pmatrix}\right](x)^2\ \vartheta[\eta_S](u)^2,
\end{aligned}$$

wobei $e^{-4\pi i a^t(\eta_s)_2} = e^{4\pi i a^t(\eta_s)_2}$ gilt, da es nur die Werte ± 1 annehmen kann.

ad ii. Analog zu i.

□

In dieser zweiten Additionsformel wird durch Ausnutzen der Theta–Relationen nur noch über 2^g statt 2^{2g} Summanden summiert. Diese Additionsformel bildet die Basis für die Addition auf der Jacobischen Varietät einer hyperelliptischen Kurve, denn im nächsten Abschnitt wird die Verallgemeinerung der $\wp$–Funktion mit Hilfe von ϑ so erklärt, daß diese Additionsformel zu einer Additionsformel für $\wp$ führen wird.

4 Die $\wp$–Funktion

In diesem Abschnitt werde ich mit Hilfe der ϑ–Funktion eine Verallgemeinerung der Weierstraßschen $\wp$–Funktion für Geschlecht $g \geq 1$ definieren. Als Motivation dient wiederum der Fall $g = 1$, denn hier gewährleisten die bekannte Weierstraßsche $\wp$–Funktion und ihre Ableitung $\wp'$ die Abbildung des Torus ohne Nullpunkt auf den affinen Teil der elliptische Kurve, wodurch die Kurve eine Gruppenstruktur erhält. Bekanntlich läßt sich die $\wp$–Funktion als negative zweite logarithmische Ableitung der Weierstraßschen σ–Funktion erklären, welche die Theta–Relation erfüllt.

Durch diese im ersten Teil studierte Vorgehensweise werde ich im zweiten Teil eine Verallgemeinerung der Weierstraßschen $\wp$–Funktion analog als im wesentlichen zweite logarithmische Ableitung der ϑ–Funktion definieren, wobei mit Ableitung die Anwendung des in Abschnitt 1.6 definierten Differentialoperators D gemeint ist.

Diese so verallgemeinerte $\wp$–Funktion soll zusammen mit ihren ersten $2g - 1$ Ableitungen die gewünschte Abbildung von $T_C - \Phi(\Theta)$ auf $Jac\,C - \Theta$ herstellen. Dazu werde ich die Konstante in der Definition von $\wp$ so wählen, daß sich ein Zusammenhang zu den Funktionen $u_1(z), ..., u_g(z)$, $v_1(z), ..., v_g(z)$ einstellt, denn diese $2g$ Funktionen beschreiben durch g Gleichungen den affinen Ring von $Jac\,C - \Theta$.

Durch diesen Zusammenhang kann ich im dritten Teil zeigen, daß sich $Jac\,C - \Theta$ durch $\wp(z)$, $\wp'(z), ..., \wp^{(2g-1)}(z)$ in g Gleichungen darstellen läßt. Der Vorteil gegenüber der Beschreibung durch g Gleichung in $u_1(z), ..., u_g(z)$, $v_1(z), ..., v_g(z)$ ist der, daß sich durch die Additionsformel der ϑ–Funktion wegen des Zusammenhangs von ϑ zu $\wp$ auch Additionsformeln für $\wp, \wp', ..., \wp^{(2g-1)}$ finden lassen, was schließlich zu einer Arithmetik auf dem affinen Teil der Jacobischen Varietät führen wird.

4.1 $\wp$ bei Geschlecht 1

Sei C eine elliptische Kurve und Γ das Gitter, so daß $C - \{\infty\}$ isomorph zu $(\mathbb{C}/\Gamma) - \Gamma$ ist, und betrachte die von Weierstraß eingeführte $\wp$–Funktion,

$$\begin{aligned} \wp : \quad \mathbb{C} - \{0\} \quad &\longrightarrow \mathbb{C}, \\ z \qquad &\longmapsto \frac{1}{z^2} + \sum_{\omega \in \Gamma}{}' \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}, \end{aligned}$$

wobei $\sum'$ die Summation über alle Gitterpunkte $\neq 0$ bedeutet. $\wp$ ist bezüglich Γ periodisch und induziert die Funktion $\wp : (\mathbb{C}/\Gamma) - \Gamma \longrightarrow \mathbb{C}$. Daneben gibt es noch die dazu verwandte σ–Funktion,

$$\begin{aligned} &\sigma : \mathbb{C} \longrightarrow \mathbb{C}, \\ &\quad z \longmapsto z \prod_{\omega \in \Gamma}{}' \left(1 - \frac{z}{\omega}\right)\; e^{\frac{z}{\omega} + \frac{z^2}{2\omega^2}}, \end{aligned}$$

die holomorph und bezüglich Γ quasi-periodisch ist, d.h. die Theta–Relation erfüllt. σ hat dann die Form: $\sigma(z+\omega) = e^{c(z+\frac{\omega}{z})}\sigma(z)$. Sie verschwindet nur in den Gitterpunkten von Γ. Zusammen mit der ζ–Funktion,

$$\begin{aligned} \zeta : \mathbb{C} - \{0\} &\longrightarrow \mathbb{C}, \\ z \quad &\longmapsto \frac{1}{z} \prod_{\omega\in\Gamma}{}' \left(\frac{1}{z-\omega} + \frac{1}{\omega} \right) + \frac{z}{\omega^2}, \end{aligned}$$

ergeben sich die Beziehungen

$$\begin{aligned} \zeta(z) &= \frac{\sigma'(z)}{\sigma(z)} = (\log(\sigma(z)))', \\ \zeta'(z) &= -\wp(z), \\ \Longrightarrow \wp(z) &= -\frac{\mathrm{d}^2}{\mathrm{d}\,z^2}(\log(\sigma(z))) + c. \end{aligned}$$

Die Konstante c wird so gewählt, daß die Laurententwicklung von $\wp(z)$ um $z=0$ keinen konstanten Term besitzt, denn dann ist $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_4$ für alle $z \in \mathbb{C}$ erfüllt.

Vergleiche $\sigma(z)$ mit $\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z)$: Beide Funktionen sind holomorph und bezüglich Γ quasi-periodisch. Die einzige Nullstelle von $\sigma(z)$ im Periodenparallelogramm ist 0. Das folgende Lemma gibt an, für welche der vier möglichen Charakteristiken $(a,b) \in \{0, \frac{1}{2}\}^2$ die Funktion $\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z)$ auch bei 0 eine Nullstelle hat.

Lemma 9
Für die Charaktistik $\delta = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$ gilt

$$\vartheta[\delta](0) = 0.$$

Beweis
Verifiziere die Behauptung direkt über die Definition von ϑ für $g=1$:
$\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z) = \sum\limits_{n\in\mathbb{Z}} e^{\pi i(n+a)^2\Omega + 2\pi i(n+a)(z+b)}$ mit $z \in \mathbb{C}$, $a, b \in \{0, \frac{1}{2}\}$, $\Omega \in \mathbb{C}$, $\operatorname{Im}\Omega > 0$.

$$\begin{aligned} \vartheta\begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix}(0) &= \sum_{n\in\mathbb{Z}} e^{\pi i\Omega n^2 + \pi i\Omega n + \pi i\Omega\frac{1}{4} + \pi i n + \pi i\frac{1}{2}} \\ &= \underbrace{e^{\pi i\Omega\frac{1}{4} + \pi i\frac{1}{2}}}_{=:c} \sum_{n\in\mathbb{Z}} e^{\pi i n}\ e^{\pi i\Omega n(n+1)} \\ &= c \lim_{n\to\infty} \left(\sum_{k=0}^{n} e^{\pi i k}\ e^{\pi i\Omega k(k+1)} + \sum_{l=1}^{n} e^{\pi i(-l)}\ e^{\pi i\Omega(-l)(-l+1)} \right) \\ &= c \lim_{n\to\infty} \left(\sum_{k=0}^{n} (-1)^k\ e^{\pi i\Omega k(k+1)} + \sum_{l=1}^{n} (-1)^l\ e^{\pi i\Omega l(l-1)} \right) \\ &= c \lim_{n\to\infty} \left(\sum_{k=0}^{n} (-1)^k\ e^{\pi i\Omega k(k+1)} + \sum_{k=0}^{n} (-1)^{k+1}\ e^{\pi i\Omega(k+1)k} \right) \\ &= 0. \end{aligned}$$

□

Für die verbleibenden Charakteristiken $\begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix}$, $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ hat ϑ keine Nullstelle. Also haben $\vartheta[\delta](z)$ und $\sigma(z)$ in allen Gitterpunkten Nullstellen. Da der Quotient $\frac{\sigma(z)}{\vartheta[\delta](z)}$ weder Null- noch Polstellen hat und ebenfalls quasi–periodisch ist, gilt $\frac{\sigma(z)}{\vartheta[\delta](z)} = e^{l(z,\omega)+j(\omega)}$ mit Linearformen l, j. Betrachte dazu

$$\begin{aligned}
\sigma(z) &= e^{l(z,\omega)+j(\omega)}\ \vartheta[\delta](z) \\
\Longrightarrow \frac{\mathrm{d}^2}{\mathrm{d}\,z^2}\left(\log(\sigma(z))\right) &= \frac{\mathrm{d}^2}{\mathrm{d}\,z^2}\left(\log\left(e^{l(z,\omega)+j(\omega)}\ \vartheta[\delta](z)\right)\right) \\
&= \frac{\mathrm{d}}{\mathrm{d}\,z}\left(l'(z,\omega) + \frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)}\right) \\
&= 0 + \frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} + \frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2},\ \text{da } l(z,\omega) \text{ linear in } z \\
&= \frac{\mathrm{d}^2}{\mathrm{d}\,z^2}\left(\log(\vartheta[\delta](z))\right).
\end{aligned}$$

Also ist $\wp(z) = -\frac{\mathrm{d}^2}{\mathrm{d}\,z^2}\left(\log(\vartheta[\delta](z))\right) + c$.

4.2 $\wp$ bei beliebigem Geschlecht

Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 1$ und $\mathbb{C}^g/\Gamma$ der Jacobi–Torus zu C. Nach Abschnitt 1.5 ist $\mathbb{C}^g/\Gamma - \Phi(\Theta)$ isomorph zu $Jac\ C - \Theta$. Um eine $\wp$–Funktion auf $\mathbb{C}^g/\Gamma - \Phi(\Theta)$ zu erklären, werde ich analog zu Geschlecht 1 die Nullstellen von $\vartheta(z)$ studieren. Dazu zitiere ich einen Satz von Mumford, der genau die Charakteristik der ϑ–Funktion angibt, für welche die Nullstellenmenge von $\vartheta[\delta](z)$ in $\mathbb{C}^g/\Gamma$ gleich $\Phi(\Theta)$ ist und die mit Θ aus $Jac\,C - \Theta$ identifiziert werden kann.

Satz 14 ([Mumford 1984], IIIa, 5.3)

i. Sei $\omega = (\omega_1, ..., \omega_g)^t$ die Basis der holomorphen 1–Formen. Dann gilt für

$$\delta \equiv \begin{pmatrix} (\frac{1}{2}\ \frac{1}{2}\ \cdots\ \frac{1}{2}\ \frac{1}{2})^t \\ (\frac{g}{2}\ \frac{g-1}{2}\ \cdots\ 1\ \frac{1}{2})^t \end{pmatrix} \mod \mathbb{Z}^{2g}$$

und alle $z \in \mathbb{C}^g$:

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

ii. Sei $V(\vartheta[\delta])$ die Nullstellenmenge von $\vartheta[\delta](z)$, so kann $Jac\ C - \Theta$ analytisch beschrieben werden als $\mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$.

iii. Zu jedem Weierstraßpunkt a_k, $k \in B'$, existiert ein $\eta_k \in \frac{1}{2}\mathbb{Z}^{2g}$ und eine Konstante c_k, so daß zu jedem Divisor $D(z) = \sum_{i=1}^{g}(x_i(z), y_i(z)) - g \cdot \infty \in Pic_0\ C - \Theta$ und entsprechendem Punkt $z \equiv \sum_{i=1}^{g} \int_{\infty}^{(x_i(z),y_i(z))} \omega \mod \Gamma \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ mit zugehörigem Polynom $u(t,z) = \prod_{i=1}^{g}(t - x_i(z))$ gilt:

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

Insbesondere sind die Koeffizienten von $u(t,z)$ meromorphe Funktionen auf $\mathbb{C}^g/\Gamma$ mit Polstellen bei $V(\vartheta[\delta])$.

$u(t,z)$ kann also als eine Funktion in z mit Parameter t betrachtet werden. Desweiteren beweist Mumford:

Korollar 8 ([Mumford 1984], IIIa, 5.7)
Für eine Teilmenge $T \subseteq B' = \{1, ..., 2g-1\}$ gilt

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

d.h. zu einem Divisor $D = \sum_{i \in T}(a_i, 0) - \sharp\, T \cdot \infty \in Pic_0\, C$ gehört $z \equiv \Omega(\eta_T)_1 + (\eta_T)_2 \in \mathbb{C}^g/\Gamma$.

Beispiel 16 ($g = 1$)
Die Aussage aus Satz 14 ist bereits aus Lemma 9 bekannt: für $\delta = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \in \frac{1}{2}\mathbb{Z}^2$ verschwindet $\vartheta[\delta](z)$ genau dann, wenn $z = 0$ ist. $V(\vartheta[\delta]) = \{0\}$ ist die Nullstellenmenge von $\vartheta[\delta](z)$ und entspricht $\Theta = \{\infty\}$ auf der elliptischen Kurve bzw. der Jacobi–Varietät. Also ist $Jac\, C - \{\infty\} \cong (\mathbb{C}/\Gamma) - \Gamma$, wie in Kapitel 2.1 gesehen, und die meromorphen Funktionen $u_1(z), v_1(z)$ bzw. $\wp(z), \wp'(z)$ haben Polstellen bei $z = 0$.

Beispiel 17 ($g = 2$)
Für die Charakteristik $\delta = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \end{pmatrix}$ gilt:

$\vartheta[\delta](z) = 0 \Longleftrightarrow$ Es existiert ein $P \in C$ mit $z \equiv \int_\infty^P \omega \mod \Gamma \Longleftrightarrow z \in V(\vartheta[\delta]) \Longleftrightarrow P - \infty \in \Theta$.

Definition 12
Die Funktion

$$\begin{aligned} \wp : \mathbb{C}^g - V(\vartheta[\delta]) &\longrightarrow \mathbb{C}, \\ z &\longmapsto -4\ \mathrm{D}^2(\log(\vartheta[\delta](z))) + c \end{aligned}$$

heißt **verallgemeinerte Weierstraßsche $\wp$–Funktion** mit einer Konstanten c.

Nach Satz 3 wirkt der Differentialoperator D auf eine Funktion $f : \mathbb{C}^g/\Gamma \longrightarrow \mathbb{C}$ in folgender Weise: $f'(z) = \mathrm{D}\, f(z) = -\sum_{i=1}^g h_i \frac{\partial f}{\partial z_i}(z)$ und wird Ableitung genannt. Entsprechend wird zweimaliges Ableiten mit $f''(z) = \mathrm{D}^2 f(z) = \mathrm{D}(\mathrm{D}\, f)(z)$ bezeichnet.

Satz 15
$\wp$ ist gerade und bezüglich Γ eine periodische meromorphe Funktion. Sie definiert also eine meromorphe Funktion

$$\wp : \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma \longrightarrow \mathbb{C}$$

und hat Polstellen der Ordnung 2 bei $z \in V(\vartheta[\delta])/\Gamma$.

Beweis
$\wp$ ist gerade, da ϑ es ist.

$\wp$ ist periodisch: Seien $p, q \in \mathbb{Z}^g$ und $z \in \mathbb{C}^g$. Dann gilt mit Lemma 2:

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

Polstellen von $\wp$: $\vartheta[\delta](z)$ hat Nullstellen der Ordnung 1 bei $z \in V(\vartheta[\delta])/\Gamma$, also hat $\wp(z)$ als zweite logarithmische Ableitung von $\vartheta[\delta](z)$ dort Polstellen 2. Ordnung.

□

Nach Abschnitt 1 läßt sich der affine Teil der Jacobi–Varietät durch die Polynome $u(t)$ und $v(t)$ darstellen, indem $\frac{f(t)-v(t)^2}{u(t)}$ via Division mit Rest ausgerechnet wird. Der Rest muß verschwinden und liefert somit g Gleichungen in den $2g$ Variablen $u_1, ..., u_g, v_1, ..., v_g$, die den affinen Ring von $Jac\,C - \Theta$ beschreiben. Aufgrund der gegebenen Isomorphie von $Jac\,C - \Theta$ und $T_C - \Phi(\Theta)$ sind die Koeffizienten der Polynome als meromorphe Funktionen auf dem Torus aufzufassen.

Da die verallgemeinerten $\wp$–Funktionen diese Isomorphie explizit angeben sollen, wird die Konstante c in der Definition von $\wp$ nun so gewählt, daß ein Zusammenhang zu den meromorphen Funktionen $u_1(z), ..., u_g(z), v_1(z), ..., v_g(z)$ besteht. Dieser Zusammenhang, im folgenden Satz beschrieben, wird $\mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ in den $\mathbb{C}^{2g}$ einbetten.

Satz 16
Betrachte die Darstellung

$$\begin{aligned}
Jac\,C - \Theta \cong \{(u_1(z), ..., u_g(z), v_1(z), ..., v_g(z), w_0(z), ..., w_g(z)) \mid \\
u(t,z) = t^g + u_1(z)t^{g-1} + ... + u_g(z), \\
v(t,z) = v_1(z)t^{g-1} + ... + v_g(z), \\
w(t,z) = t^{g+1} + w_0(z)t^g + ... + w_g(z), \\
u(t,z)\ w(t,z) = f(t) - v(t,z)^2 \text{ für } z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma\}.
\end{aligned}$$

Die Konstante c aus der Definition von $\wp$ läßt sich so wählen, daß für $z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ gilt

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

Beweis
Satz 4 beschreibt die Anwendung des Differentialoperators D auf $v(t,z) = v_1(z)t^{g-1} + ... + v_g(z)$, wobei $v(t,z)$ als Funktion in z mit Parameter t aufgefaßt wird:

$$\begin{aligned}
\mathrm{D}\,v(t,z) &= \left(\sum_{i=1}^{g} u_i'(z)\frac{\partial}{\partial u_i(z)} + \sum_{i=1}^{g} v_i'(z)\frac{\partial}{\partial v_i(z)} + \sum_{i=0}^{g} w_i'(z)\frac{\partial}{\partial w_i(z)}\right)\big(v_1(z)t^{g-1} + ... + v_g(z)\big) \\
&= v_1'(z)t^{g-1} + ... + v_g'(z) \\
&= \frac{1}{2}(-w_1(z) + u_2(z) - u_1(z)u_1(z) + w_0(z)u_1(z))t^{g-1} \\
&\quad + ... + \frac{1}{2}(-w_g(z) - u_1(z)u_g(z) + w_0(z)u_g(z)) \\
&= \frac{1}{2}(-w(t,z) + (t - u_1(z) + w_0(z))u(t,z)).
\end{aligned}$$

Eine Umformung ergibt

$$w_0(z) - u_1(z) = \frac{2\,\mathrm{D}\,v(t,z) + w(t,z)}{u(t,z)} - t = 2\frac{\mathrm{D}\,v(t,z)}{u(t,z)} + \frac{w(t,z)}{u(t,z)} - t,$$

wobei sich der Parameter t auf der rechten Seite weghebt. Es bleibt eine Gleichheit zwischen Funktionen. Mit $w(t,z) = \frac{f(t)-v(t,z)^2}{u(t,z)}$ folgt daraus

$$w_0(z) - u_1(z) = 2\frac{\mathrm{D}\,v(t,z)}{u(t,z)} + \frac{f(t)}{u(t,z)^2} - \frac{v(t,z)^2}{u(t,z)^2} - t. \tag{12}$$

Ziel ist, $\frac{\mathrm{D}\,v(t,z)}{u(t,z)}$ und $\left(\frac{v(t,z)}{u(t,z)}\right)^2$ auszuwerten. Nutze dazu Satz 14, der für den Parameter $t = a_k$ eingesetzt, $k \in B'$, besagt:

$$u(a_k, z) = c_k \left(\frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)}\right)^2 \text{ mit Konstante } c_k \text{ für } z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma. \tag{13}$$

D.h. für einen Weierstraßpunkt a_k ist $u(a_k,z) = a_k^g + u_1(z)a_k^{g-1} + ... + u_g(z) = c_k \left(\frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)}\right)^2$ eine Gleichheit zwischen Funktionen auf dem Torus.

Auf diese Gleichheit (13) wird der Differentialoperator D zweimal angewendet: Auf der linken Seite gilt nach Satz 14:

$$\mathrm{D}^2\,u(a_k,z) = \mathrm{D}(\mathrm{D}\,u)(a_k,z) = \mathrm{D}\,v(a_k,z)$$

und auf der rechten mit $\mathrm{D}\,f(z) = f'(z)$ und der üblichen Kettenregel für die Differentiation:

$$\begin{aligned}
&\mathrm{D}^2\,u(a_k,z)\\
&= \mathrm{D}^2\left(\left(c_k\frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)}\right)^2\right)\\
&= \mathrm{D}\left(2\,c_k\,\frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)}\;\frac{\vartheta[\delta+\eta_k]'(z)\,\vartheta[\delta](z) - \vartheta[\delta+\eta_k](z)\,\vartheta[\delta]'(z)}{\vartheta[\delta](z)^2}\right)\\
&= \mathrm{D}\left(2\,c_k\,\frac{\vartheta[\delta+\eta_k](z)\,\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta](z)^2} - 2c_k\frac{\vartheta[\delta+\eta_k](z)^2\vartheta[\delta]'(z)}{\vartheta[\delta](z)^3}\right)\\
&= 2\,c_k\,\frac{(\vartheta[\delta+\eta_k]'(z)^2 + \vartheta[\delta+\eta_k](z)\,\vartheta[\delta+\eta_k]''(z))\,\vartheta[\delta](z)^2}{\vartheta[\delta](z)^4}\\
&\quad - 2\,c_k\,\frac{2\vartheta[\delta+\eta_k](z)\,\vartheta[\delta+\eta_k]'(z)\,\vartheta[\delta](z)\,\vartheta[\delta]'(z)}{\vartheta[\delta](z)^4}\\
&\quad - 2\,c_k\,\frac{(2\vartheta[\delta+\eta_k](z)\,\vartheta[\delta+\eta_k]'(z)\,\vartheta[\delta]'(z) + \vartheta[\delta+\eta_k](z)^2\,\vartheta[\delta]''(z))\,\vartheta[\delta](z)^3}{\vartheta[\delta](z)^6}\\
&\quad - 2\,c_k\,\frac{3\vartheta[\delta+\eta_k](z)^2\,\vartheta[\delta]'(z)\,\vartheta[\delta](z)^2\,\vartheta[\delta]'(z)}{\vartheta[\delta](z)^6}
\end{aligned}$$

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

Division von $\mathrm{D}\,v(a_k,z) = 2\,c_k\,\frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta](z)^2} + 2\,c_k\,\frac{\vartheta[\delta+\eta_k](z)\,\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta](z)^2}$ $- 8\,c_k\,\frac{\vartheta[\delta+\eta_k](z)\,\vartheta[\delta+\eta_k]'(z)\,\vartheta[\delta]'(z)}{\vartheta[\delta](z)^3} - 2\,c_k\,\frac{\vartheta[\delta+\eta_k](z)^2\,\vartheta[\delta]''(z)}{\vartheta[\delta](z)^3} + 6\,c_k\,\frac{\vartheta[\delta+\eta_k](z)^2\,\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^4}$ durch $u(a_k,z) = c_k\left(\frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)}\right)^2$:

$$
\begin{aligned}
\frac{\mathrm{D}\,v(a_k,z)}{u(a_k,z)} &= 2\,\frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta+\eta_k](z)^2} + 2\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)} - 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)}\\
&\quad - 2\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} + 6\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2}
\end{aligned}
\tag{14}
$$

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

$$
\frac{v(a_k,z)}{u(a_k,z)} = \frac{\mathrm{D}\,u(a_k,z)}{u(a_k,z)} = 2\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)} - 2\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)}. \tag{15}
$$

ergibt für Gleichung (12) mit $f(a_k) = 0$:

$$
\begin{aligned}
&w_0(z) - u_1(z)\\
&= 2\,\frac{\mathrm{D}\,v(a_k,z)}{u(a_k,z)} + \frac{f(a_k)}{u(a_k,z)^2} - \frac{v(a_k,z)^2}{u(a_k,z)^2} - a_k\\
&= 4\,\frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta+\eta_k](z)^2} + 4\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)} - 16\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} - 4\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)}\\
&\quad + 12\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} - 4\,\frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta+\eta_k](z)^2} + 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} - 4\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} - a_k\\
&= 4\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)} - 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\,\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} - 4\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} + 8\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} - a_k.
\end{aligned}
$$

Betrachte daneben die zweite logarithmische Ableitung von $\vartheta[\delta](z)$:

$$\begin{aligned}
\mathrm{D}^2(\log(\vartheta[\delta](z))) &= \mathrm{D}\left(\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)}\right) \\
&= \frac{\vartheta[\delta]''(z)\,\vartheta[\delta](z) - \vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} \\
&= \frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} - \frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2}.
\end{aligned}$$

$w_0(z) - u_1(z)$ und $\mathrm{D}^2(\log(\vartheta[\delta](z)))$ haben beide doppelte Polstellen bei $V(\vartheta[\delta])$. Die Funktion

$$\begin{aligned}
&-8\ \mathrm{D}^2(\log(\vartheta[\delta](z))) - (w_0(z) - u_1(z)) \\
&= -8\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} + 8\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} - 4\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)} \\
&\quad + 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} + 4\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} - 8\,\frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} + a_k \\
&= -4\,\frac{\vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta+\eta_k](z)} + 8\,\frac{\vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta+\eta_k](z)}\frac{\vartheta[\delta]'(z)}{\vartheta[\delta](z)} - 4\,\frac{\vartheta[\delta]''(z)}{\vartheta[\delta](z)} + a_k
\end{aligned}$$

ist auf $\mathbb{C}^g/\Gamma$ meromorphe und hat höchstens einfache Polstellen bei $V(\vartheta[\delta]) \cup V(\vartheta[\delta+\eta_k])$, da für alle $k \in B'$ gilt: $\delta \neq \delta + \eta_k$. $-8\ \mathrm{D}^2(\log(\vartheta[\delta](z))) - (w_0(z) - u_1(z))$ hat daher tatsächlich höchstens einen einfachen Pol bei $V(\vartheta[\delta])$ und ist folglich konstant:

$$\begin{aligned}
& -8\ \mathrm{D}^2(\log(\vartheta[\delta](z))) - (w_0(z) - u_1(z)) = \tilde{c} \\
\Longleftrightarrow\quad & -8\ \mathrm{D}^2(\log(\vartheta[\delta](z))) - \tilde{c} = w_0(z) - u_1(z) \\
\overset{c \mapsto -\frac{1}{2}\tilde{c}}{\Longleftrightarrow}\quad & 2(-4\ \mathrm{D}^2(\log(\vartheta[\delta](z))) + c) = w_0(z) - u_1(z) \\
\Longleftrightarrow\quad & 2\wp(z) = w_0(z) - u_1(z).
\end{aligned}$$

$\square$

Zusammenfassend läßt sich sagen: Die verallgemeinerte Weierstraßsche $\wp$–Funktion wird im folgenden durch $\wp(z) = -4\ \mathrm{D}^2(\log(\vartheta[\delta](z))) + c$ für $z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ gegeben, wobei c so gewählt wird, daß $w_0(z) - u_1(z) = 2\wp(z)$ erfüllt ist. Die Konstante c läßt sich berechnen. Die Idee ist, dazu

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

an der Stelle $\Omega\delta_1 + \delta_2$ auszuwerten und $c = -\frac{1}{2}\tilde{c}$ zu berücksichtigen. Um ähnliche Relationen zu Lemma 3 für die Terme $\vartheta[\delta]'(\Omega\delta_1 + \delta_2)$ und $\vartheta[\delta]''(\Omega\delta_1 + \delta_2)$ zu erhalten, wird ein Lemma benötigt:

Lemma 10
Sei $a, b, c, d \in \frac{1}{2}\mathbb{Z}^g$. Dann gilt mit $h = (-h_1, ..., -h_g)^t$

i. $$\vartheta\begin{bmatrix}a\\b\end{bmatrix}'(z + \Omega c + d) = e^{-\pi i c^t \Omega c - 2\pi i c^t(z+b+d)}\left(\vartheta\begin{bmatrix}a+c\\b+d\end{bmatrix}'(z) - 2\pi i c^t h\,\vartheta\begin{bmatrix}a+c\\b+d\end{bmatrix}(z)\right),$$

ii. $$\begin{aligned}\vartheta\begin{bmatrix}a\\b\end{bmatrix}''(z + \Omega c + d) = e^{-\pi i c^t \Omega c - 2\pi i c^t(z+b+d)}\Bigg(&\vartheta\begin{bmatrix}a+c\\b+d\end{bmatrix}''(z) - 4\pi i c^t h\,\vartheta\begin{bmatrix}a+c\\b+d\end{bmatrix}'(z) \\ &-4\pi^2(c^t h)^2\,\vartheta\begin{bmatrix}a+c\\b+d\end{bmatrix}(z)\Bigg).\end{aligned}$$

Beweis

ad i. Durch Anwenden des Differentialoperators D auf Lemma 3:

$$\vartheta\begin{bmatrix}a\\b\end{bmatrix}'(z+\Omega c+d) = \mathrm{D}\left(e^{-\pi i c^t\Omega c-2\pi i c^t(z+b+d)}\,\vartheta\begin{bmatrix}a+c\\b+d\end{bmatrix}(z)\right)$$
$$= \left(-2\pi i c^t h\,\vartheta\begin{bmatrix}a+c\\b+d\end{bmatrix}(z)+\vartheta\begin{bmatrix}a+c\\b+d\end{bmatrix}'(z)\right)e^{-\pi i c^t\Omega c-2\pi i c^t(z+b+d)}.$$

ad ii. Erneutes Anwenden von D auf Gleichung i.

□

Damit gilt nun nach Lemmata 3 und 10 durch sorgfältiges Aufschreiben, Ausmultiplizieren und Wegkürzen:

$$\begin{aligned}\tilde c = &-4\,\frac{\vartheta[\delta+\eta_k]''(\Omega\delta_1+\delta_2)}{\vartheta[\delta+\eta_k](\Omega\delta_1+\delta_2)}+8\,\frac{\vartheta[\delta+\eta_k]'(\Omega\delta_1+\delta_2)}{\vartheta[\delta+\eta_k](\Omega\delta_1+\delta_2)}\frac{\vartheta[\delta]'(\Omega\delta_1+\delta_2)}{\vartheta[\delta](\Omega\delta_1+\delta_2)}\\ &-4\,\frac{\vartheta[\delta]''(\Omega\delta_1+\delta_2)}{\vartheta[\delta](\Omega\delta_1+\delta_2)}+a_k\\ =&-4\,\lim_{z\to 0}\frac{\vartheta[\eta_k]''(z)}{\vartheta[\eta_k](z)}+8\,\lim_{z\to 0}\frac{\vartheta[\eta_k]'(z)}{\vartheta[\eta_k](z)}\,\frac{\vartheta[0]'(0)}{\vartheta[0](0)}-4\,\frac{\vartheta[0]''(0)}{\vartheta[0](0)}+a_k,\end{aligned}$$

dabei muß der Grenzwert betrachtet werden, da nach Satz 11 aus $\sharp\,(k\circ U)=g+1+(-1)^k\neq g+1$ folgt $\vartheta[\eta_k](0)=0$. $\tilde c$ ist für alle $k\in B'$ gleich, also läßt sich $\tilde c$ für ein spezielles k mit der Regel von de l'Hospital ausrechnen.

Zurück zur verallgemeinerten $\wp$–Funktion, die für $g=1$: $\wp(z)=-4\frac{\mathrm{d}^2}{\mathrm{d}\,z^2}\left(\log\left(\vartheta\begin{bmatrix}\frac12\\\frac12\end{bmatrix}(z)\right)\right)+c$ lautet und mit der klassischen Weierstraßsche $\wp$–Funktion aus Abschnitt 2.1, hier mit $\tilde\wp$ bezeichnet, bis auf den Faktor 4 übereinstimmt: $\tilde\wp=-\frac{\mathrm{d}^2}{\mathrm{d}\,z^2}\left(\log(\sigma(z))\right)+c$. Der Unterschied im Faktor 4 liegt darin begründet, daß $(\tilde\wp(z),\tilde\wp'(z))$ die Gleichung der elliptischen Kurve in Weierstraßscher Normalform $y^2=4x^3-\tilde g_2x-\tilde g_3$ löst. Ein leichter Koordinatenwechsel überführt die beiden Definitionen von $\wp$ und $\tilde\wp$ ineinander:

$$\begin{aligned}&\tilde\wp'(z)^2 &&= 4\tilde\wp(z)^3-\tilde g_2\wp(z)-\tilde g_3\\ \Longleftrightarrow\ &16\tilde\wp'(z)^2 &&= 64\tilde\wp(z)^3-16\tilde g_2\tilde\wp(z)-16\tilde g_3\\ \Longleftrightarrow\ &(4\tilde\wp'(z))^2 &&= (4\tilde\wp(z))^3-4\tilde g_2\,4\tilde\wp(z)-16\tilde g_3\\ \Longleftrightarrow\ &\wp'(z)^2 &&= \wp(z)^3-g_2\wp(z)-g_3\end{aligned}$$

mit $\tilde\wp(z)=\frac14\wp(z),\ \tilde g_2=\frac14 g_2$ und $\tilde g_3=\frac{1}{16}g_3$.

4.3 Einbettung

In diesem Teil zeige ich, daß die verallgemeinerte $\wp$–Funktion und ihre ersten $2g-1$ Ableitungen den Torus $\mathbb{C}^g/\Gamma-V(\vartheta[\delta])/\Gamma$ in den $\mathbb{C}^{2g}$ einbetten, daß also $(\wp(z),\wp'(z),...,\wp^{(2g-1)}(z))$ die g beschreibenden Gleichungen des affinen Teils der Jacobischen Varietät erfüllen. Dabei wird wie üblich die Ableitung von $\wp$ durch Anwenden des Differentialoperators $\wp^{(k)}(z)=\mathrm{D}^k(\wp(z))$, $k=0,...,2g-1$, erklärt. Die Gleichungen, die den affinen Ring von $Jac\,C-\Theta$ beschreiben, gestatten es, Punkte zu bestimmen und dadurch $(\wp(z), ..., \wp^{(2g-1)}(z))$ als Koordinaten zu nutzen. Ich gebe einen auf dem Beweis basierenden Algorithmus an, der die Polynome $u(t,z)$, $v(t,z)$ und $w(t,z)$ und damit die g beschreibenden Gleichungen von $Jac\,C - \Theta$ bestimmen.

Satz 17
Der Morphismus

$$\begin{aligned}\varphi: \quad \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma &\longrightarrow \mathbb{C}^{2g}, \\ z &\longmapsto (\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z))\end{aligned}$$

ist eine Einbettung.

Beweis
Nach Satz 14 ist $\mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ isomorph zu $Jac\,C - \Theta$. $Jac\,C - \Theta$ wird durch die Polynome $u(t,z), v(t,z)$ bzw. deren Koeffizienten $u_1(z), ..., u_g(z), v_1(z), ..., v_g(z)$ bestimmt, die meromorphe Funktionen auf dem Torus $\mathbb{C}^g/\Gamma$ sind. Dabei gilt $u(t,z)|f(t) - v(t,z)^2$, wodurch der Rest bei Division mit Rest verschwindet. Dieser Rest besteht aus g Gleichungen in $u_1(z), ..., u_g(z), v_1(z), ..., v_g(z)$.

Die Relation $w_0(z) - u_1(z) = 2\wp(z)$ aus Satz 16 wird zwischen $(u_1(z), ..., u_g(z), v_1(z), ..., v_g(z))$ und $(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z))$ einen Zusammenhang herstellen, so daß schließlich g Gleichungen in den $\wp(z), ..., \wp^{(2g-1)}(z)$ entstehen, die für jedes $z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ verschwinden. Dadurch erzeugt $(\wp(z), ..., \wp^{(2g-1)}(z))$ den affinen Teil der Jacobi–Varietät $Jac\,C$ und φ ist eine Einbettung in den $\mathbb{C}^{2g}$.

In diesem Beweis schreibe ich die Funktionen $u_1(z), ..., u_g(z), v_1(z), ..., v_g(z)$, $\wp(z), ..., \wp^{(2g-1)}(z)$ ohne (z), um die Rechnungen noch einigermaßen übersichtlich gestalten zu können. Gleichungen sind daher als Gleichungen zwischen Funktionen aufzufassen.

Zum Beweis werden die Polynome

$$\begin{aligned}u(t) &= t^g + u_1 t^{g-1} + ... + u_g = t^g + \sum_{i=1}^{g} u_i t^{g-i}, \\ v(t) &= v_1 t^{g-1} + ... + v_g = \sum_{i=1}^{g} v_i t^{g-i}, \\ w(t) &= t^{g+1} + w_0 t^g + w_1 t^{g-1} + ... + w_g = t^{g+1} + \sum_{i=1}^{g+1} w_{i-1} t^{g+1-i}\end{aligned}$$

und das die hyperelliptische Kurve definierende Polynom betrachtet:

$$f(t) = t^{2g+1} + f_1 t^{2g} + ... + f_{2g+1} = t^{2g+1} + \sum_{i=1}^{2g+1} f_i t^{2g+1-i}.$$

Dividiere

$$f(t) = u(t)\,w(t) \;+\; v(t)^2 \tag{16}$$

durch die „buchhaltende“ Variable $t^{2g+1} \neq 0$:

$$\frac{f(t)}{t^{2g+1}} = \frac{u(t)}{t^g}\,\frac{w(t)}{t^{g+1}} \;+\; \frac{1}{t}\left(\frac{v(t)}{t^g}\right)^2 \tag{17}$$

mit den folgenden Identitäten:

$$\frac{u(t)}{t^g} = 1 + \sum_{i=1}^{g} u_i t^{-i},$$
$$\frac{v(t)}{t^g} = \sum_{i=1}^{g} v_i t^{-i},$$
$$\frac{w(t)}{t^{g+1}} = 1 + \sum_{i=1}^{g+1} w_{i-1} t^{-i},$$
$$\frac{f(t)}{t^{2g+1}} = 1 + \sum_{i=1}^{2g+1} f_i t^{-i}.$$

Betrachte $\frac{f(t)}{t^{2g+1}}$ als Polynom in t^{-1} mit konstantem Term 1. $\frac{f(t)}{t^{2g+1}}$ hat eine eindeutige Quadratwurzel im Ring der Potenzreihen, d.h.

$$\frac{f(t)}{t^{2g+1}} = \left(\alpha(t^{-1})\right)^2 \text{ mit } \alpha(t^{-1}) = 1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + \ldots \text{ und } \alpha_i \in \mathbb{C}.$$

Die Koeffizienten α_i berechnen sich aus den Koeffizienten von f. Ich benutze im folgenden die für ein Polynom $f(x) = \sum_{n=0}^{\infty} a_n x^n$ übliche Schreibweise $\sum_{n=0}^{k} a_n x^n + \mathcal{O}\left(x^{k+1}\right)$, wenn die Terme ab Ordnung $k+1$ die Ausgabe nicht mehr beeinflussen können.

$$\begin{aligned}
0 &= f(t)t^{-(2g+1)} - \left(1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + \ldots\right)^2 \\
&= \left(1 + \sum_{i=1}^{2g+1} f_i t^{-i}\right) - \left(1 + 2\sum_{i=1}^{2g+1} \alpha_i t^{-i} + \sum_{i=1}^{4g+2} \left(\sum_{\substack{j,k\geq 1\\ j+k=i}} \alpha_j\, \alpha_k\right) t^{-i}\right) + \mathcal{O}\left(t^{2g-2}\right) \\
&= \sum_{i=1}^{2g+1} \left(f_i - 2\alpha_i - \sum_{\substack{j,k\geq 1\\ j+k=i}} \alpha_j\, \alpha_k\right) t^{-i} + \mathcal{O}\left(t^{2g-2}\right)
\end{aligned}$$

$$\Longrightarrow \alpha_i = \frac{1}{2} f_i - \frac{1}{2} \sum_{\substack{j,k\geq 1\\ j+k=i}} \alpha_j\, \alpha_k,\ i = 1, \ldots, 2g+1.$$

Division von (17) durch $(\alpha(t^{-1}))^2$ führt auf:

$$1 = \frac{u(t)\, t^{-g}}{\alpha(t^{-1})}\, \frac{w(t)\, t^{-(g+1)}}{\alpha(t^{-1})} \;+\; t^{-1} \left(\frac{v(t)\, t^{-g}}{\alpha(t^{-1})}\right)^2, \tag{18}$$

was sich als Potenzreihe in t^{-1} schreiben läßt:

$$1 = u^*(t^{-1})\, w^*(t^{-1}) \;+\; t^{-1}\, (v^*(t^{-1}))^2 \tag{19}$$

mit

$$\begin{aligned}
u^*(t^{-1}) &= \frac{u(t)\; t^{-g}}{\alpha(t^{-1})} = 1 + \sum_{i=1}^{g} u_i^* t^{-i} + \mathcal{O}\left(t^{-(g+1)}\right) = 1 + u_1^* t^{-1} + u_2^* t^{-2} + ...,\\
v^*(t^{-1}) &= \frac{v(t)\; t^{-g}}{\alpha(t^{-1})} = \sum_{i=1}^{g} v_i^* t^{-i} + \mathcal{O}\left(t^{-(g+1)}\right) = v_1^* t^{-1} + v_2^* t^{-2} + ...,\\
w^*(t^{-1}) &= \frac{w(t)\; t^{-(g+1)}}{\alpha(t^{-1})} = 1 + \sum_{i=1}^{g+1} w_{i-1}^* t^{-i} + \mathcal{O}\left(t^{-(g+2)}\right) = 1 + w_0^* t^{-1} + w_1^* t^{-2} + ... \,.
\end{aligned} \tag{20}$$

Die Koeffizienten u_i^*, v_j^*, w_k^* sind wie die u_i, v_j, w_k meromorphe Funktionen auf $\mathbb{C}^g/\Gamma$. Durch einen Koeffizientenvergleich lassen sich (u_i^*, v_j^*, w_k^*) und (u_i, v_j, w_k) ineinander überführen:

$$\begin{aligned}
&1 + u_1 t^{-1} + u_2 t^{-2} + ... + u_g t^{-g}\\
&\quad = \;\; (1 + u_1^* t^{-1} + u_2^* t^{-2} + ...)\; (1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + ...),\\
&v_1 t^{-1} + v_2 t^{-2} + ... + v_g t^{-g}\\
&\quad = \;\; (v_1^* t^{-1} + v_2^* t^{-2} + ...)\; (1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + ...),\\
&1 + w_0 t^{-1} + w_1 t^{-2} + ... + w_g t^{-g-1}\\
&\quad = \;\; (1 + w_0^* t^{-1} + w_1^* t^{-2} + ...)\; (1 + \alpha_1 t^{-1} + \alpha_2 t^{-2} + ...).
\end{aligned} \tag{21}$$

Also gelten

$$\begin{aligned}
u_i &= u_i^* + \alpha_i + \sum_{\substack{j,k\geq 1\\ j+k=i}} u_j^* \alpha_k,\; i = 1, ..., g,\\
v_i &= v_i^* + \sum_{\substack{j,k\geq 1\\ j+k=i}} v_j^* \alpha_k,\; i = 1, ..., g,\\
w_i &= w_i^* + \alpha_{i+1} + \sum_{\substack{j,k\geq 1\\ j+k=i+1}} w_{j-1}^* \alpha_k,\; i = 0, ..., g.
\end{aligned}$$

Zum Beispiel sind

$$\begin{aligned}
u_1 &= u_1^* + \alpha_1,\\
v_1 &= v_1^*,\\
w_0 &= w_0^* + \alpha_1.
\end{aligned}$$

Die w_k^* lassen sich aus den u_i^*, v_j^* durch Gleichung (19) bestimmen:

$$
\begin{aligned}
1 &= u^*(t^{-1})\, w^*(t^{-1}) \;+\; t^{-1}\, v^*(t^{-1})^2 \\
&= \left(1 + \sum_{i=1}^{g} u_i^* t^{-i} + \mathcal{O}\left(t^{-(g+1)}\right)\right) \left(1 + \sum_{i=1}^{g+1} w_{i-1}^* t^{-i} + \mathcal{O}\left(t^{-(g+2)}\right)\right) \\
&\quad + \; t^{-1} \left(\sum_{i=1}^{g} v_i^* t^{-i} + \mathcal{O}\left(t^{-(g+1)}\right)\right)^2 \\
&= 1 + \sum_{i=1}^{g} \left(u_i^* + w_{i-1}^* + \sum_{\substack{j,k\geq 1 \\ j+k=i}} u_j^* w_{k-1}^* \right) t^{-i} + \sum_{i=2}^{g} \left(\sum_{\substack{j,k\geq 1 \\ j+k=i}} v_j^* v_k^* \right) t^{-(i+1)} + \mathcal{O}\left(t^{-(g+1)}\right).
\end{aligned}
$$

Durch Koeffizientenvergleich ergibt sich für $i = 0, 1, ..., g$:

$$
\begin{aligned}
& 0 = u_{i+1}^* + w_i^* + \sum_{\substack{j,k\geq 1 \\ j+k=i+1}} u_j^* w_{k-1}^* + \sum_{\substack{j,k\geq 1 \\ j+k=i}} v_j^* v_k^* \\
\iff \; & w_i^* = -\, u_{i+1}^* - \sum_{\substack{j,k\geq 1 \\ j+k=i+1}} u_j^* w_{k-1}^* - \sum_{\substack{j,k\geq 1 \\ j+k=i}} v_j^* v_k^*.
\end{aligned}
\tag{22}
$$

Explizit:

$$
\begin{aligned}
0 &= u_1^* + w_0^*, \\
0 &= u_2^* + w_1^* + u_1^* w_0^*, \\
0 &= u_3^* + w_2^* + u_2^* w_0^* + u_1^* w_1^* + v_1^{*2}, \\
&\;\vdots \\
0 &= u_n^* + w_{n-1}^* + (\text{Polynom in } u_1^*, ..., u_{n-1}^*, v_1^*, ..., v_{n-2}^*, w_0^*, ..., w_{n-2}^*).
\end{aligned}
\tag{23}
$$

Da nach (22) der Term w_{n-1}^* bereits durch ein Polynom in $u_1^*, ..., u_n^*, v_1^*, ..., v_{n-2}^*, w_0^*, ..., w_{n-2}^*$ ausgedrückt werden kann, und $w_{n-2}^*, ..., w_0^*$ analog, wird induktiv definiert:

$$
u_n^* + w_{n-1}^* =: W_{n-1}(u_1^*, ..., u_{n-1}^*, v_1^*, ..., v_{n-2}^*), \tag{24}
$$

wobei W_{n-1} ein Polynom in $u_1^*, ..., u_{n-1}^*, v_1^*, ..., v_{n-2}^*$ ist.

Betrachte $\wp$. Nach Satz 16 gilt $2\wp = w_0 - u_1$, d.h.

$$
\begin{aligned}
\wp &= \frac{1}{2}\,(w_0 - u_1) = \frac{1}{2}\,(w_0^* + \alpha_1 - (u_1^* + \alpha_1)) = \frac{1}{2}\,(w_0^* - u_1^*) \\
&= \frac{1}{2}\,(\underbrace{w_0^* + u_1^*}_{0} - 2u_1^*) = -\, u_1^*.
\end{aligned}
\tag{25}
$$

Nun ist $\wp$ mit u_1^* verbunden, woraus sich aus den Relationen zu den anderen Koeffizienten, auch nicht–gesternte, ein Zusammenhang zwischen u_i, v_j, w_k zu $\wp$ herstellen läßt. Um einen Zusammenhang zu den Ableitungen $\wp', ..., \wp^{(2g-1)}$ herzustellen, nutze $w_0 - u_1 = 2\wp$ und Satz 4:

$$
\begin{aligned}
\mathrm{D}\, u(t) &= v(t), \\
\mathrm{D}\, v(t) &= \frac{1}{2}(-w(t) + (t + 2\wp)u(t)), \\
\mathrm{D}\, w(t) &= -(t + 2\wp)v(t).
\end{aligned}
$$

Für gesternte Polynome bedeutet dies:

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

Die Koeffizienten von $\mathrm{D}\,u^*(t^{-1})$, $\mathrm{D}\,v^*(t^{-1})$ und $\mathrm{D}\,w^*(t^{-1})$ werden mit u_i^*, v_j^* und w_k^* bezeichnet. Sie sind meromorphe Funktionen auf $\mathbb{C}^g/\Gamma$ und aufgrund der Gleichungen (20) gelten die folgenden Relationen:

$$
\begin{aligned}
u_i^{*\prime} &= v_i^*, \\
v_i^{*\prime} &= \frac{1}{2}\,(-w_i^* + u_{i+1}^* - 2\,u_1^*\,u_i^*), \\
w_i^{*\prime} &= -v_{i+1}^* + 2\,u_1^*\,v_i^*.
\end{aligned}
\tag{26}
$$

Damit lassen sich induktiv die $\wp^{(k)}$, $k \geq 0$, mit dem Anfangswert $\wp = -u_1^*$ berechnen:

$$
\begin{aligned}
\wp &= -u_1^*, \\
\wp' &= -u_1^{*\prime} \\
&= -v_1^*, \\
\wp'' &= -v_1^{*\prime} \\
&= -\frac{1}{2}\,(-w_1^* + u_2^* - 2\,u_1^{*2}) \\
&= -\frac{1}{2}\,(-u_2^* - w_1^* + 2\,u_2^* - 2\,u_1^{*2}) \\
&= \frac{1}{2}\,(W_1(u_1^*) - 2\,u_2^* + 2\,u_1^{*2}) \\
&= -u_2^* + \frac{1}{2}(W_1(u_1^*) + 2\,u_1^{*2}), \\
\wp''' &= -u_2^{*\prime} + \frac{1}{2}\,({W_1}'(u_1^*) + 4\,u_1^*\,u_1^{*\prime}) \\
&= -v_2^* + \frac{1}{2}\,({W_1}'(u_1^*) + 4\,u_1^*\,u_1^{*\prime}), \\
&\;\vdots \\
\wp^{(2n)} &= -u_{n+1}^* + \text{ (Polynom in } u_1^*, ..., u_n^*, v_1^*, ..., v_{n-1}^*), \\
\wp^{(2n+1)} &= -v_{n+1}^* + \text{ (Polynom in } u_1^*, ..., u_{n+1}^*, v_1^*, ..., v_n^*).
\end{aligned}
\tag{27}
$$

Umgekehrt lassen sich die u_i^* und v_j^* aus den $\wp^{(k)}$ ermitteln:

$$
\begin{aligned}
u_1^* &= -\wp, \\
v_1^* &= -\wp', \\
u_2^* &= -\wp'' + \frac{1}{2}(W_1(u_1^*) + 2\,u_1^{*2}) \\
&= -\wp'' + \frac{1}{2}(W_1(-\wp) + 2\,\wp^2), \\
v_2^* &= -\wp''' + \frac{1}{2}(W_1'(-\wp) + 4\,\wp\,\wp'), \\
&\;\vdots \\
u_{n+1}^* &= \wp^{(2n)} + \text{ (Polynom in } \wp, \wp', ..., \wp^{(2n-1)}), \\
v_{n+1}^* &= \wp^{(2n+1)} + \text{ (Polynom in } \wp, \wp', ..., \wp^{(2n)}).
\end{aligned}
\tag{28}
$$

Insbesondere ist

$$
\begin{aligned}
&\wp^{(2g)} = -u_{g+1}^* + \text{ (Polynom in } u_1^*, ..., u_g^*, v_1^*, ..., v_{g-1}^*) \\
\Longleftrightarrow\ &\wp^{(2g)} = \text{Polynom in } \wp, \wp', ..., \wp^{2g-1},
\end{aligned}
$$

wodurch höhere Ableitungen $\wp^{(2g)}, \wp^{(2g+1)}, ...$ in den ersten $2g-1$ Ableitungen ausgedrückt werden können.

Durch dieses konstruktive Verfahren ist eine Isomorphie zwischen

$$\mathbb{C}[u_1^*, u_2^*, ..., v_1^*, v_2^*, ...] \text{ und } \mathbb{C}[\wp, \wp', ...]$$

gegeben. Dabei werden die Ableitungen (26) auf die Ableitungen D $\wp^{(k)} = \wp^{(k+1)}$ und

$$\mathbb{C}[u_1^*, ..., u_g^*, v_1^*, ..., v_g^*] \text{ auf } \mathbb{C}[\wp, \wp', ..., \wp^{(2g-1)}]$$

abgebildet. Die u_i^*, v_j^* lassen sich wiederum aus den u_i, v_j berechnen. Damit ist

$$\mathbb{C}[u_1, ..., u_g, v_1, ..., v_g] \text{ zu } \mathbb{C}[\wp, \wp', ..., \wp^{(2g-1)}]$$

isomorph.

Die g Gleichungen in den $u_1, ...u_g, v_1, ..., v_g$, die den affinen Ring von $Jac\,C - \Theta$ erzeugen und so die Jacobi–Varietät beschreiben, werden durch die Isomorphie auf g Gleichungen abgebildet, die aus den $\wp, \wp', ..., \wp^{(2g-1)}$ bestehen und die weiterhin den affinen Ring der Varietät $Jac\,C - \Theta$ erzeugen. Also ist φ eine Einbettung.

□

Mit diesem konstruktiven Beweis lassen sich nun zwei Algorithmen angeben. Der erste beschreibt zu einer hyperelliptischen Kurve C die meromorphen Funktionen $u_1(z), ..., u_g(z)$, $v_1(z), ..., v_g(z)$, $w_0(z), ..., w_g(z)$ als Polynome in $\wp(z), \wp'(z), ..., \wp^{(2g)}(z)$. Der zweite Algorithmus gibt die g Gleichungen explizit an, welche $Jac\,C - \Theta$ beschreiben. Ein Punkt $(x_0, ..., x_{2g-1}) \in \mathbb{C}^{2g}$ liegt also genau dann auf dem affinen Teil der Jacobi–Varietät, wenn dieser Punkt die g Gleichungen erfüllt. Dabei wird $\wp^{(2g)}(z)$ durch ein Polynom aus $\mathbb{C}[\wp(z), \wp', ..., \wp^{(2g-1)}(z)]$ dargestellt. Dieses Verfahren zum Finden von Punkten auf der Varietät, läßt sich konkret mit Hilfe eines Computers umsetzen und ist deutlich einfacher und schneller, als die $\wp$–Funktion und ihre Ableitungen direkt durch unendliche Reihen und Differentiationen zu realisieren.

In Abschnitt 1.2 wurde diese Methode, durch Gleichungen Punkte auf der Varietät zu finden, schon beschrieben und benutzt. Der Vorteil ist hier, daß sich explizite Additionsformeln finden lassen. Werden die Punkte $(x_0, ..., x_{2g-1})$ und $(y_0, ..., y_{2g-1})$ auf $Jac\,C - \Theta$ als $(\wp(x), \wp'(x), ..., \wp^{(2g-1)}(x))$ und $(\wp(y), \wp'(y), ..., \wp^{(2g-1)}(y))$ interpretiert, so ist $(\wp(x+y), \wp'(x+y), ..., \wp^{(2g-1)}(x+y))$ das Ergebnis der Addition.

Zunächst der Algorithmus 1, der zu einer gegebener hyperelliptischen Kurve vom Geschlecht $g \geq 1$, $C : y^2 = f(x) = x^{2g+1} + f_1 x^{2g} + ... + f_{2g+1}$, die Koeffizienten der Polynome $u(t,z), v(t,z)$ und $w(t,z)$ in einer Darstellung der $\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)$ ermittelt. Dabei wird der Algorithmus in einer Pseudo–Code Schreibweise notiert, der die übliche FOR–Schleifen Routine, das Symbol := als Zuweisungsoperator und $'$ als Ableitungsoperator nutzt.

Algorithmus 1
Eingabe: $f_1, ..., f_{2g+1}$.
Berechne:

$u_1^*(z) := -\wp(z);$

$w_0^*(z) := -u_1^*(z);$

$\texttt{for } i := 1 \texttt{ to } g \texttt{ do}$

$$v_i^*(z) := u_i^{*'}(z);$$

$$u_{i+1}^*(z) := v_i^{*'}(z) + u_1^*(z)\,u_i^*(z) - \frac{1}{2}\sum_{\substack{j,k\geq 1\\ j+k=i+1}} u_j^*(z) w_{k-1}^*(z) - \frac{1}{2}\sum_{\substack{j,k\geq 1\\ j+k=i}} v_j^*(z) v_k^*(z);$$

$$w_i^*(z) := -u_{i+1}^*(z) - \sum_{\substack{j,k\geq 1\\ j+k=i+1}} u_j^*(z) w_{k-1}^*(z) - \sum_{\substack{j,k\geq 1\\ j+k=i}} v_j^*(z) v_k^*(z);$$

$\texttt{end};$

for $i := 1$ to $g+1$ do

$$\alpha_i := \frac{1}{2} f_i - \frac{1}{2} \sum_{\substack{j,k \geq 1 \\ j+k=i}} \alpha_j \alpha_k;$$

end;

for $i := 1$ to g do

$$u_i(z) := u_i^*(z) + \alpha_i + \sum_{\substack{j,k \geq 1 \\ j+k=i}} u_j^*(z) \alpha_k;$$

$$v_i(z) := v_i^*(z) + \sum_{\substack{j,k \geq 1 \\ j+k=i}} v_j^*(z) \alpha_k;$$

end;

for $i := 0$ to g do

$$w_i(z) := w_i^*(z) + \alpha_{i+1} + \sum_{\substack{j,k \geq 1 \\ j+k=i+1}} w_{j-1}^*(z) \alpha_k;$$

end;

Ausgabe: $u_1(z), ..., u_g(z), v_1(z), ..., v_g(z), w_0(z), ..., w_g(z) \in \mathbb{C}[\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)]$.

Während der erste Algorithmus u_i, v_j, w_k durch $\wp, \wp', ..., \wp^{(2g)}$ ausdrückt, ermittelt der folgende zweite Algorithmus die definierenden Gleichungen des affinen Teils der Jacobi–Varietät und eine Darstellung von $\wp^{(2g)}$ in $\wp, \wp', ..., \wp^{(2g-1)}$:

Algorithmus 2
Eingabe:

$f_1, ..., f_{2g+1}$,
$u_1(z), ..., u_g(z), v_1(z), ..., v_g(z), w_0(z), ..., w_g(z) \in \mathbb{C}[\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)]$

nach Algorithmus 1. Dies impliziert:

$$\begin{aligned} u(t,z) &= t^g + u_1(z) t^{g-1} + ... + u_g(z), \\ v(t,z) &= v_1(z) t^{g-1} + ... + v_g(z), \\ w(t,z) &= t^{g+1} + w_0(z) t^g + ... + w_g(z), \\ f(t) &= t^{2g+1} + f_1 t^{2g} + ... + f_{2g+1}. \end{aligned}$$

Multipliziere die rechte Seite aus:

$$\begin{aligned} 0 &= u(t,z)\, w(t,z) \; - \; f(t) \; + \; v(t,z)^2 \\ &= \left(t^g + \sum_{i=1}^{g} u_i(z) t^{g-i} \right) \left(t^{g+1} + \sum_{i=1}^{g+1} w_{i-1}(z) t^{g+1-i} \right) \\ &\quad - \left(t^{2g+1} + \sum_{i=1}^{2g+1} f_i t^{2g+1-i} \right) \; + \; \left(\sum_{i=1}^{g} v_i(z) t^{g-i} \right)^2 \\ &= t^{2g+1}(1-1) \; + \; t^{2g}(w_0(z) - f_1 + u_1(z)) \\ &\quad + \; t^{2g-1}(w_1(z) + w_0(z) u_1(z) + u_2(z) - f_2) \; + \; ... \end{aligned} \tag{29}$$

Setze

$$F_0 := -(\text{Koeffizient von } t^g \text{ der Gleichung (29)}) + \wp^{(2g)}(z).$$

Es gilt $F_0 \in \mathbb{C}[\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)]$ und $\wp^{(2g)}(z) = F_0(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z))$, so daß im folgenden stets $\wp^{(2g)}(z)$ durch diesen Ausdruck ersetzt wird.

Setze

```
for i := 1 to g do
    F_i := Koeffizient von t^{g-i} der Gleichung (29);
end;
```

Ausgabe: $F_0, F_1, ..., F_g \in \mathbb{C}[\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)]$.

Nach Konstruktion der $u_1(z), ..., u_g(z)$, $v_1(z), ..., v_g(z)$, $w_0(z), ..., w_g(z)$ verschwinden in (29) die Koeffizienten von $t^{2g+1}, ..., t^{g+1}$ für alle $z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ und die linke Seite ist dort 0. Desweiteren ist auch der Koeffizient von $t^g = 0$ wegen $\wp^{(2g)}(z) = -(\text{Koeffizient von } t^g) + \wp^{(2g)}(z)$, so daß die g Gleichungen

$$F_i(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)) = 0,\ i = 1, ..., g,$$

den affinen Teil der Jacobischen Varietät beschreiben.

Ein beliebiger Punkt $(x_0, ..., x_{2g-1}) \in \mathbb{C}^{2g}$ liegt damit genau dann auf $Jac\, C - \Theta$, wenn gilt:

$$\begin{aligned} &F_1(x_0, ..., x_{2g-1}) = 0, \\ &\vdots \\ &F_g(x_0, ..., x_{2g-1}) = 0. \end{aligned}$$

Die Gleichungen $F_i(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)) = 0, i = 1, ..., g$, stellen bereits die zweite Möglichkeit dar, $Jac\, C - \Theta$ durch g Gleichungen zu beschreiben, denn nach Abschnitt 1.2 lassen sich die Gleichungen $R_i(u_1(z), ..., u_g(z), v_1(z), ..., v_g(z), w_0(z), ..., w_g(z)) = 0, i = 1, ..., g$, durch Division mit Rest bestimmen. Diese neu konstruierten Gleichungen F_i haben den wichtigen Vorteil, daß durch die Additionsformeln für $\wp, \wp', ..., \wp^{(2g-1)}$, die im nächsten Abschnitt entwickelt werden, eine Arithmetik auf $Jac\, C - \Theta$ erklärt werden kann.

Beispiel 18 ($g = 1$)
Betrachte die elliptische Kurve $C:\ y^2 = x^3 + ax + b$ und wende den Algorithmus 1 auf die Eingabewerte $f_1 = 0,\ f_2 = a,\ f_3 = b$ an. Das Programm gibt folgende Ausgabedaten:

$$\begin{aligned} u_1^*(z) &= -\wp(z), \\ w_0^*(z) &= \wp(z), \\ v_1^*(z) &= -\wp'(z), \\ u_2^*(z) &= -\wp''(z) + \wp(z)^2 + \frac{1}{2}\wp(z)^2 = -\wp''(z) + \frac{3}{2}\wp(z)^2, \\ w_1^*(z) &= \wp''(z) - \frac{3}{2}\wp(z)^2 + \wp(z)^2 = \wp''(z) - \frac{1}{2}\wp(z)^2, \end{aligned}$$

$$\alpha_1 = \frac{1}{2}f_1 = 0,$$
$$\alpha_2 = \frac{1}{2}f_2 - \frac{1}{2}\alpha_1^2 = \frac{a}{2},$$
$$\alpha_3 = \frac{1}{2}f_3 - \frac{1}{2}(2\alpha_1\alpha_2) = \frac{b}{2},$$

$$\begin{aligned}
u_1(z) &= u_1^*(z) + \alpha_1 = -\wp(z),\\
v_1(z) &= v_1^*(z) = -\wp'(z),\\
w_0(z) &= w_0^*(z) + \alpha_1 = \wp(z),\\
w_1(z) &= w_1^*(z) + \alpha_2 + w_0^*(z)\,\alpha_1 = \wp''(z) - \frac{1}{2}\wp(z)^2 + \frac{a}{2}.
\end{aligned}$$

$u(t,z), v(t,z), w(t,z)$ sind nun bekannt und durch Ausmultiplizieren,

$$\begin{aligned}
0 &= u(t,z)\,w(t,z) - f(t) + v(t,z)^2\\
&= (t + u_1(z))\,\left(t^2 + w_0(z)t + w_1(z)\right)\\
&\quad - \left(t^3 + at + b\right) + (v_1(z))^2\\
&= t^2(w_0(z) + u_1(z)) + t(w_1(z) + w_0(z)u_1(z) - a) + u_1(z)w_1(z) - b + v_1(z)^2\\
&= t\,\left(\wp''(z) - \frac{3}{2}\wp(z)^2 - \frac{a}{2}\right) + \wp'(z)^2 - \wp(z)^3 - a\wp(z) - b,
\end{aligned}$$

und Algoritmus 2 berechnen sich:

$$\begin{aligned}
\wp''(z) &= F_0(\wp(z), \wp'(z)) = -\left(\wp''(z) - \frac{3}{2}\wp(z)^2 - \frac{a}{2}\right) + \wp''(z) = \frac{3}{2}\wp(z)^2 + \frac{a}{2},\\
F_1(\wp(z), \wp'(z)) &= \wp'(z)^2 - \wp(z)^3 - a\wp(z) - b.
\end{aligned}$$

$F_1((\wp(z), \wp'(z)) = 0$ spiegelt damit die elliptische Kurve $\wp'(z)^2 = \wp(z)^3 + a\wp(z) + b$ wider.

Beispiel 19 **($g = 2$)**
Für die hyperelliptische Kurve $C:\ y^2 = f(x)$ mit $f(t) = t^5 + f_1t^4 + f_2t^3 + f_3t^2 + f_4t + f_5$ liefern die Algorithmen 1 und 2 die folgende Ausgabe:

$$\begin{aligned}
u_1(z) &= \frac{f_1}{2} - \wp(z),\\
u_2(z) &= -\frac{f_1^2}{8} + \frac{f_2}{2} - \frac{f_1}{2}\wp(z) + \frac{3}{2}\wp(z)^2 - \wp''(z),\\
v_1(z) &= -\wp'(z),\\
v_2(z) &= -\frac{f_1}{2}\wp'(z) + 3\wp(z)\wp'(z) - \wp'''(z),\\
w_0(z) &= \frac{f_1}{2} + \wp(z),\\
w_1(z) &= -\frac{f_1^2}{8} + \frac{f_2}{2} + \frac{f_1}{2}\wp(z) + \frac{1}{2}\wp(z)^2 + \wp''(z),\\
w_2(z) &= \wp^{(4)}(z) - 3\wp''(z)\wp(z) - \frac{7}{2}\wp'(z)^2 + \frac{1}{2}\wp(z)^3 + \frac{1}{2}f_3 - \frac{1}{4}f_1f_2 + \frac{1}{16}f_1^3 + \frac{1}{2}f_2\wp(z)\\
&\quad - \frac{1}{8}f_1^2\wp(z) + \frac{1}{2}f_1\wp''(z) - \frac{1}{4}f_1\wp(z)^2.
\end{aligned}$$

$$
\begin{aligned}
&\wp^{(4)}(z) \\
&= F_0(\wp(z),\wp'(z),\wp''(z),\wp'''(z)) \\
&= \frac{1}{16}\ \big(f_1^3 - 4f_1f_2 + 8f_3 + 2f_1^2\wp(z) \\
&\qquad - 8f_2\wp(z) + 12f_1\wp(z)^2 - 40\wp(z)^3 + 40\wp'(z)^2 \\
&\qquad -8f1\wp''(z) + 80\wp(z)\wp''(z)\big)\ ,
\end{aligned}
$$

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

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

Nachdem also per Konstruktion die Gruppentruktur von $\mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ auf $JacC - \Theta$ übertragen wurde, soll diese Struktur dort explizit sichtbar gemacht werden.

5 Additionsformeln für die $\wp$–Funktion

In diesem Kapitel werde ich die Additionsformeln für den affinen Teil der Jacobi–Varietät einer hyperelliptischen Kurven entwickeln. Nach Konstruktion der $\wp$–Funktion für Geschlecht $g \geq 1$ wird $\mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ durch $(\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z))$ auf $Jac\,C - \Theta$ abgebildet, wodurch diese die Gruppenstruktur des Torus übernimmt. Zwei Elementen von $Jac\,C - \Theta$,

$(\wp(z_1), \wp'(z_1), ..., \wp^{(2g-1)}(z_1))$ und
$(\wp(z_2), \wp'(z_2), ..., \wp^{(2g-1)}(z_2))$,

wird als Ergebnis der partiellen Addition auf $Jac\,C - \Theta$ das Element

$$(\wp(z_1 + z_2), \wp'(z_1 + z_2), ..., \wp^{(2g-1)}(z_1 + z_2))$$

zugeordnet. Ziel ist es, $\wp(z_1+z_2)$ als rationale Kombination der $\wp(z_1), \wp'(z_1), ..., \wp^{(2g-1)}(z_1), \wp(z_2), \wp'(z_2), ..., \wp^{(2g-1)}(z_2)$ mit $z_1, z_2, z_1+z_2 \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ darzustellen. Aus einer solchen Formel lassen sich durch Anwenden des Differentialoperators D Formeln für $\wp'(z_1+z_2), ..., \wp^{(2g-1)}(z_1+z_2)$ herleiten. Der bei der Differentiation auftretende Term $\wp^{(2g)}$ wird durch die im Algorithmus 2 aus Abschnitt 4.3 ermittelte Darstellung F_0 ersetzt, so daß sich $\wp'(z_1 + z_2), ..., \wp^{(2g-1)}(z_1 + z_2)$ ebenfalls durch $\wp(z_1), ..., \wp^{(2g-1)}(z_1)$, $\wp(z_2), ..., \wp^{(2g-1)}(z_2)$ ausdrücken lassen.

Diese Additionsformeln bilden dann eine partielle Addition auf $Jac\,C - \Theta$, die mit der in Abschnitt 1.4 beschriebenen Überdeckungseigenschaft zu einer Addition auf $JacC$ führt, d.h. zu einem Element $E \in \Theta$ wird ein e_T addiert, so daß $E+e_T \in JacC-\Theta$ ist. $E+e_T$ kann dann zu einem $D \in JacC-\Theta$ mit der partiellen Addition auf $Jac\,C - \Theta$ addiert werden: $D + E = (D + (E + e_T)) + e_T$. Für die Addition auf Θ wird das Additions– und Reduktionsverfahren von Cantor genutzt. Dies stellt bei Anwendungen auf einem endlichen Körper nur eine Ausnahme dar, da es, wie erwähnt, nur mit geringer Wahrscheinlichkeit vorkommt.

Ich werde im ersten Teil dieses Abschnitts eine Additionsformel für beliebiges Geschlecht $g \geq 1$ herleiten, die jedoch bei gegebenem Geschlecht konkret entwickelt werden muß. Ich werde in den folgenden Abschnitten explizite Additionsformeln für Geschlecht 1 und 2 angeben. Bei Geschlecht 1 bietet das Ergebnis wegen der bereits in Abschnitt 2.1 präsentierten Addition wenig Neues, während bei Geschlecht 2 die Formeln derart umfangreich werden, daß ich lediglich $\wp(z_1 + z_2)$ angeben kann. Mit Einsatz eines Computer–Algebra–Systems lassen sich die ermittelten Additionsformeln implementieren und Beispiele rechnen.

5.1 Aussagen bei beliebigem Geschlecht

Für $x, u \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ wird D^x bzw. D^u durch das Anwenden des Differentialoperators D nach x bzw. u erklärt und $\mathrm{D}^x + \mathrm{D}^u$ sei die Summe dieser partiellen Differentiationen. Es gelten die üblichen Kettenregeln für die Differentiation, die ihrerseits auch als Ableitung mit $f'(z) = \mathrm{D}\,f(z)$ bezeichnet wird.

Satz 18

Seien $x, u, x+u \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$. Dann gelten

i. $\wp(x+u)$ ist rationale Kombination der $\wp(x), ..., \wp^{(2g-1)}(x), \wp(u), ..., \wp^{(2g-1)}(u)$,

d.h. $\wp(x+u) = \dfrac{f}{g}$ mit $f, g \in \mathbb{C}[\wp(x), ..., \wp^{(2g-1)}(x), \wp(u), ..., \wp^{(2g-1)}(u)]$,

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

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

Beweis

Setze für die Charakteristik $\begin{pmatrix} a \\ b \end{pmatrix}$ in der Additionsformel aus Satz 13 ii. speziell δ aus Satz 14 ein:

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

und dividiere beide Seiten durch $\vartheta[\delta](x)^2\ \vartheta[\delta](u)^2$:

$$\frac{\vartheta[\delta](x+u)}{\vartheta[\delta](x)^2} \frac{\vartheta[\delta](x-u)}{\vartheta[\delta](u)^2} \vartheta[0](0)^2 = \sum_{\overline{T} \in \mathcal{V}} e^{4\pi i \delta_1^t (\eta_T)_2} \frac{\vartheta[\delta + \eta_T](x)^2}{\vartheta[\delta](x)^2} \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2}, \tag{30}$$

was möglich ist, da $\vartheta[\delta](x)^2,\ \vartheta[\delta](u)^2 \neq 0$ für $x, u \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$.

Die Terme $\frac{\vartheta[\delta+\eta_T](z)^2}{\vartheta[\delta](z)^2}$ und $\frac{\vartheta[\eta_T](z)^2}{\vartheta[\delta](z)^2}$ sind nach Korollar 2 meromorphe Funktionen $\mathbb{C}^g/\Gamma \longrightarrow \mathbb{C}$ mit Polstellen höchstens bei $V(\vartheta[\delta])$, und sie haben nach Satz 17 eine Darstellung als rationale Kombination in $\wp(z), \wp'(z), ..., \wp^{(2g-1)}(z)$. Deshalb ist auch

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

als rationale Kombination darstellbar. Das impliziert die erste Behauptung i. Wie diese rationale Kombination konkret aussieht, ist Bestandteil der nun zu beweisenden Behauptung ii.

Wende auf die Gleichung (30) die Operation $-(\mathrm{D}^x + \mathrm{D}^u)^2(\log)$ an:

$$\begin{aligned} &-(\mathrm{D}^x + \mathrm{D}^u)^2 \left(\log \left(\frac{\vartheta[\delta](x+u)}{\vartheta[\delta](x)^2} \frac{\vartheta[\delta](x-u)}{\vartheta[\delta](u)^2} \vartheta[0](0)^2 \right) \right) \\ &= -(\mathrm{D}^x + \mathrm{D}^u)^2 \left(\log \left(\sum_{\overline{T} \in \mathcal{V}} e^{4\pi i \delta_1^t (\eta_T)_2} \frac{\vartheta[\delta + \eta_T](x)^2}{\vartheta[\delta](x)^2} \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2} \right) \right). \end{aligned} \tag{31}$$

Die rechte Seite ist schon so, wie in ii. behauptet, fehlt noch die linke. Behauptung:

$$\begin{aligned}
&-(\mathrm{D}^x+\mathrm{D}^u)^2\left(\log\left(\frac{\vartheta[\delta](x+u)}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\delta](x-u)}{\vartheta[\delta](u)^2}\ \vartheta[0](0)^2\right)\right)\\
&=-4\ \left(\frac{\vartheta[\delta]''(x+u)}{\vartheta[\delta](x+u)}\ -\ \frac{\vartheta[\delta]'(x+u)^2}{\vartheta[\delta](x+u)^2}\right)\\
&\quad+2\ \left(\frac{\vartheta[\delta]''(x)}{\vartheta[\delta](x)}\ -\ \frac{\vartheta[\delta]'(x)^2}{\vartheta[\delta](x)^2}\right)\\
&\quad+2\ \left(\frac{\vartheta[\delta]''(u)}{\vartheta[\delta](u)}\ -\ \frac{\vartheta[\delta]'(u)^2}{\vartheta[\delta](u)^2}\right).
\end{aligned}\tag{32}$$

Denn:

$$\begin{aligned}
&-(\mathrm{D}^x+\mathrm{D}^u)^2\left(\log\left(\frac{\vartheta[\delta](x+u)}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\delta](x-u)}{\vartheta[\delta](u)^2}\ \vartheta[0](0)^2\right)\right)\\
&=-(\mathrm{D}^x+\mathrm{D}^u)\ \left(\frac{\vartheta[\delta](x)^2}{\vartheta[\delta](x+u)}\ \frac{\vartheta[\delta](u)^2}{\vartheta[\delta](x-u)}\right.\\
&\quad\left(\frac{1}{\vartheta[\delta](u)^2}\ \mathrm{D}^x\left(\frac{\vartheta[\delta](x+u)\ \vartheta[\delta](x-u)}{\vartheta[\delta](x)^2}\right)\right.\\
&\quad\left.\left.+\frac{1}{\vartheta[\delta](x)^2}\,\mathrm{D}^u\left(\frac{\vartheta[\delta](x+u)\ \vartheta[\delta](x-u)}{\vartheta[\delta](u)^2}\right)\right)\right)\\
&=-(\mathrm{D}^x+\mathrm{D}^u)\ \left(\frac{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^2}{\vartheta[\delta](x+u)\ \vartheta[\delta](x-u)}\right.\\
&\quad\left(\frac{(\vartheta[\delta]'(x+u)\ \vartheta[\delta](x-u)\ +\ \vartheta[\delta](x+u)\ \vartheta[\delta]'(x-u))\ \vartheta[\delta](x)^2}{\vartheta[\delta](u)^2\ \vartheta[\delta](x)^4}\right.\\
&\quad-\ \frac{2\ \vartheta[\delta](x+u)\ \vartheta[\delta](x-u)\ \vartheta[\delta](x)\ \vartheta[\delta]'(x)}{\vartheta[\delta](u)^2\ \vartheta[\delta](x)^4}\\
&\quad+\ \frac{(\vartheta[\delta]'(x+u)\ \vartheta[\delta](x-u)\ -\ \vartheta[\delta](x+u)\ \vartheta[\delta]'(x-u))\ \vartheta[\delta](u)^2}{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^4}\\
&\quad\left.\left.-\ \frac{2\ \vartheta[\delta](x+u)\ \vartheta[\delta](x-u)\ \vartheta[\delta](u)\ \vartheta[\delta]'(u)}{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^4}\right)\right)\\
&=-(\mathrm{D}^x+\mathrm{D}^u)\ \left(\frac{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^2}{\vartheta[\delta](x+u)\ \vartheta[\delta](x-u)}\right.\\
&\quad\left(\frac{\vartheta[\delta]'(x+u)\ \vartheta[\delta](x-u)}{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^2}\ +\ \frac{\vartheta[\delta](x+u)\ \vartheta[\delta]'(x-u)}{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^2}\right.\\
&\quad-\ 2\,\frac{\vartheta[\delta](x+u)\ \vartheta[\delta](x-u)\ \vartheta[\delta]'(x)}{\vartheta[\delta](x)^3\ \vartheta[\delta](u)^2}\\
&\quad+\ \frac{\vartheta[\delta]'(x+u)\ \vartheta[\delta](x-u)}{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^2}\ -\ \frac{\vartheta[\delta](x+u)\ \vartheta[\delta]'(x-u)}{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^2}\\
&\quad\left.\left.-\,2\,\frac{\vartheta[\delta](x+u)\ \vartheta[\delta](x-u)\ \vartheta[\delta]'(u)}{\vartheta[\delta](x)^2\ \vartheta[\delta](u)^3}\right)\right)\\
&=-(\mathrm{D}^x+\mathrm{D}^u)\ \left(\frac{\vartheta[\delta]'(x+u)}{\vartheta[\delta](x+u)}\ -\ 2\frac{\vartheta[\delta]'(x)}{\vartheta[\delta](x)}\ +\frac{\vartheta[\delta]'(x+u)}{\vartheta[\delta](x+u)}\ -\ 2\frac{\vartheta[\delta]'(u)}{\vartheta[\delta](u)}\right)
\end{aligned}$$

$$
\begin{aligned}
&= -2\ \left(\mathrm{D}^x \left(\frac{\vartheta[\delta]'(x+u)}{\vartheta[\delta](x+u)}\right) +\ \mathrm{D}^u \left(\frac{\vartheta[\delta]'(x+u)}{\vartheta[\delta](x+u)}\right)\right.\\
&\qquad \left. -\ \mathrm{D}^x \left(\frac{\vartheta[\delta]'(x)}{\vartheta[\delta](x)}\right) -\ \mathrm{D}^u \left(\frac{\vartheta[\delta]'(u)}{\vartheta[\delta](u)}\right)\right)
\end{aligned}
$$

$$
\begin{aligned}
&= -2\ \left(\frac{\vartheta[\delta]''(x+u)\ \vartheta[\delta](x+u)\ -\ \vartheta[\delta]'(x+u)^2}{\vartheta[\delta](x+u)^2}\right.\\
&\qquad +\ \frac{\vartheta[\delta]''(x+u)\ \vartheta[\delta](x+u)\ -\ \vartheta[\delta]'(x+u)^2}{\vartheta[\delta](x+u)^2}\\
&\qquad -\ \frac{\vartheta[\delta]''(x)\ \vartheta[\delta](x)\ -\ \vartheta[\delta]'(x)^2}{\vartheta[\delta](x)^2}\\
&\qquad \left. -\ \frac{\vartheta[\delta]''(u)\ \vartheta[\delta](u)\ -\ \vartheta[\delta]'(u)^2}{\vartheta[\delta](u)^2}\right)
\end{aligned}
$$

$$
\begin{aligned}
&= -2\ \left(2\frac{\vartheta[\delta]''(x+u)}{\vartheta[\delta](x+u)}\ -\ 2\frac{\vartheta[\delta]'(x+u)^2}{\vartheta[\delta](x+u)^2}\ -\ \frac{\vartheta[\delta]''(x)}{\vartheta[\delta](x)}\ +\ \frac{\vartheta[\delta]'(x)^2}{\vartheta[\delta](x)^2}\right.\\
&\qquad \left. -\ \frac{\vartheta[\delta]''(u)}{\vartheta[\delta](u)}\ +\ \frac{\vartheta[\delta]'(u)^2}{\vartheta[\delta](u)^2}\right).
\end{aligned}
$$

Damit ist die Behauptung (32) bewiesen.

Um einen Ausdruck zu erhalten, in dem $\wp(z)$ vorkommt, betrachte die Definition von $\wp$,

$$
\begin{aligned}
\wp(z) \quad &= -4\ \mathrm{D}^2(\log(\vartheta[\delta](z))) + c\\
&= -4\ \mathrm{D}\left(\frac{\vartheta'[\delta](z)}{\vartheta[\delta](z)}\right) + c\\
&= -4\ \frac{\vartheta''[\delta](z)\ \vartheta[\delta](z)\ -\ \vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} + c\\
&= -4\ \frac{\vartheta''[\delta](z)}{\vartheta[\delta](z)}\ + 4\ \frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} + c\\
\iff \quad \frac{\vartheta''[\delta](z)}{\vartheta[\delta](z)}\ -\ \frac{\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^2} &= \frac{1}{4}\ (-\wp(z)\ + c),
\end{aligned}
$$

und setze dieses Ergebnis in (32) ein:

$$
\begin{aligned}
&-(\mathrm{D}^x + \mathrm{D}^u)^2 \left(\log\left(\frac{\vartheta[\delta](x+u)}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\delta](x-u)}{\vartheta[\delta](u)^2}\ \vartheta[0](0)^2\right)\right)\\
&= -4\ \frac{1}{4}\ (-\wp(x+u)\ + c)\ + 2\ \frac{1}{4}\ (-\wp(x)\ + c)\ + 2\ \frac{1}{4}\ (-\wp(u)\ + c)\\
&= \wp(x+u)\ -\frac{1}{2}\wp(x)\ -\frac{1}{2}\wp(u).
\end{aligned}
$$

Damit folgt die Behauptung ii. aus (31):

$$
\begin{aligned}
\wp(x+u) &= \frac{1}{2}\wp(x)\ + \frac{1}{2}\wp(u)\\
&\qquad -(\mathrm{D}^x + \mathrm{D}^u)^2 \left(\log\left(\sum_{\overline{T}\in\mathcal{V}} e^{4\pi i\delta_1^t(\eta_T)_2}\ \frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2}\right)\right).
\end{aligned}
\tag{33}
$$

ad iii.
Auf $\mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ ist $-x$ das Inverse zu x. Also ist auf $Jac\, C - \Theta$
$\neg\left(\wp(x), \wp'(x), ..., \wp^{(2g-2)}(x), \wp^{(2g-1)}(x)\right) = \left(\wp(-x), \wp'(-x), ..., \wp^{(2g-2)}(-x), \wp^{(2g-1)}(-x)\right)$ das Inverse zu $\left(\wp(x), \wp'(x), ..., \wp^{(2g-2)}(x), \wp^{(2g-1)}(x)\right)$. $\wp$ ist nach Satz 3 eine gerade Funktion, dadurch sind alle geraden Ableitungen gerade Funktionen und die ungeraden Ableitungen sind ungerade Funktionen, woraus die Behauptung iii. folgt.

□

Für eine Additionsformel $\wp(x+u)$ als rationale Kombination der $\wp(x), \wp'(x), ..., \wp^{(2g-1)}(x)$, $\wp(u)$, $\wp'(u), ..., \wp^{(2g-1)}(u)$ muß die rechte Seite von (33) umgeformt werden, die im wesentlichen aus den beiden Termen

$$\frac{\vartheta[\delta+\eta_T](z)^2}{\vartheta[\delta](z)^2} \text{ und } \frac{\vartheta[\eta_T](z)^2}{\vartheta[\delta](z)^2}, \overline{T} \in \mathcal{V}$$

besteht. Es reicht, nur einen dieser Terme explizit zu berechnen, wie das folgende Lemma zeigt. Ich erinnere dabei an die in Abschnitt 3.3 benutzten Bezeichnungen:

$$\begin{aligned}
B &= \{1, 2, 3, ..., 2g+2\},\\
B' &= \{1, 2, 3, ..., 2g+1\},\\
U &= \{1, 3, ..., 2g+1\},\ \sharp\, U = g+1,\\
V &= \{2, 4, ..., 2g+2\},\ \sharp\, V = g+1,\\
G &= \{S \subseteq B \mid \sharp\, S \text{ gerade}\},\\
\overline{G} &= G/(S \sim \mathcal{C}S),\\
\mathcal{U} &= \{\overline{S} \in \overline{G} \mid S \subseteq U \vee \mathcal{C}S \subseteq U\},\\
\mathcal{V} &= \{\overline{T} \in \overline{G} \mid T \subseteq V \vee \mathcal{C}T \subseteq V\},\\
\eta_S &= \sum_{k \in S} \eta_k,\\
\eta_\infty &:= \eta_{2g+2}.
\end{aligned}$$

Lemma 11
Zu $\overline{T} \in \mathcal{V}$ existiert ein $\overline{S} \in \mathcal{V}$, so daß gilt:

$$\delta + \eta_T \equiv \eta_S \mod \mathbb{Z}^{2g}.$$

Beweis
Sei g ungerade. Dann gilt für $\overline{U} =\in \mathcal{V}$ mit $\sharp\, U = g+1 \in 2\mathbb{Z}$: $\delta = \eta_U = \sum_{k\in U} \eta_k$ und

$$\delta + \eta_T = \sum_{k\in U} \eta_k + \sum_{k\in T} \eta_k = \sum_{k \in U\cup T} \eta_k + \sum_{k\in U\cap T} \eta_k = \sum_{k \in T\circ U} \eta_k,$$

da $2\eta_k \equiv 0 \mod \mathbb{Z}^{2g}$. Sei $t = \sharp\, T \cap U$. Dann ist

$$\sharp\, T \circ U = \sharp\left((T\cup U) - (T \cap U)\right) = \sharp\, U - (\sharp\, T - t) - t = \sharp\, U - \sharp\, T - 2t.$$

Insbesondere ist $\sharp\, T \circ U$ gerade und somit ist $\overline{T \circ U} \in \mathcal{V}$.

Sei g gerade, wähle $\delta = \eta_U + \underbrace{\eta_\infty}_{0} = \eta_{U\circ\{\infty\}}$ und verfahre analog. □

Jeder Term $\frac{\vartheta[\eta_T](z)^2}{\vartheta[\delta](z)^2}$, $\overline{T} \in \mathcal{V}$, läßt sich durch ein $\frac{\vartheta[\delta+\eta_S](z)^2}{\vartheta[\delta](z)^2}$, $\overline{S} \in \mathcal{V}$, ausdrücken und mittels Satz 14 berechnen: Für $a_k \in B'$ und $z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ gilt

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

Um den Term $\frac{\vartheta[\delta+\delta](z)^2}{\vartheta[\delta](z)^2} = \frac{\vartheta[0](z)^2}{\vartheta[\delta](z)^2}$ auszuwerten, beweise und zitiere ich die folgenden Lemmata und Sätze.

Lemma 12
Sei $T \subseteq B'$, $\sharp\, T = g-1$, $k, l \in B' - T$ und $k \neq l$. Dann gilt

$$c_k \left(\frac{\vartheta[\eta_{T\circ U} + \eta_{\{k,l\}}](0)}{\vartheta[\eta_{T\circ U} + \eta_{\{l,\infty\}}](0)}\right)^2 = e^{4\pi i(\eta_T)_1^t(\eta_k)_2}\ e^{4\pi i(\eta_l)_1^t(\eta_k)_2} \prod_{i\in T\cup\{l\}} (a_k - a_i). \tag{34}$$

Beweis
Zunächst ist $\overline{T\circ U \circ \{k,l\}} \in \overline{G}$, denn

$$\begin{aligned}
\sharp\,(T\circ U\circ\{k,l\}) &= \sharp\,(((T\cup U) - (T\cap U))\circ\{k,l\}) \\
&= \sharp\, U + (\sharp\, T - t) - t \pm 1 \pm 1, \text{ wobei } t = \sharp\, T\cap U \\
&= g+1+g-1-2t \pm 1 \pm 1 \text{ ist gerade.}
\end{aligned}$$

Desweiteren ist die linke Seite von (34) definiert, d.h. der Nenner ist von 0 verschieden, weil nach Satz 11 aus $\sharp\,(T\circ U\circ\{l,\infty\})\circ U = \sharp\,(T\circ\{l,\infty\}) = \sharp\, T + 2 = g+1$ folgt $\vartheta[\eta_{T\circ U} + \eta_l](0) \neq 0$.
Betrachte nun $W = T\cup\{l\}$. Es ist $\sharp\, T = g-1$, $\sharp\, W = g$ und $\infty \notin W$. Nach Satz 14 ii. und Korollar 8 gilt: Sei $k \in B' - T$. Zu $D = \sum_{i\in W}(a_i, 0) - g\cdot\infty \in Pic_0\ C - \Theta$ korrespondiert $\Omega(\eta_W)_1 + (\eta_W)_2 \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ und es gilt

$$u(a_k, \Omega(\eta_W)_1 + (\eta_W)_2) = \prod_{i\in W}(a_k - a_i) = c_k \left(\frac{\vartheta[\delta+\eta_k](\Omega(\eta_W)_1 + (\eta_W)_2)}{\vartheta[\delta](\Omega(\eta_W)_1 + (\eta_W)_2)}\right)^2.$$

Dabei bezeichne $(\eta_W)_1$ die ersten und $(\eta_W)_2$ die zweiten g Einträge des $2g$–dimensionalen Vektors η_W. Wende Lemma 3 an. Dann folgt mit $\delta = \eta_U$:

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

da $e^{4\pi i a^t b} = e^{-4\pi i a^t b}$ für $a, b \in \frac{1}{2}\mathbb{Z}^g$.

□

Lemma 13
Sei $T \subseteq B'$, $\sharp\, T = g-1$ und $k \in B' - T$. Dann gilt

$$c_k \left(\frac{\vartheta[\eta_{T\circ U}]'(0)}{\vartheta[\eta_{T\circ U} + \eta_{\{k,\infty\}}](0)}\right)^2 = -\frac{1}{4}\ e^{4\pi i(\eta_T)_1^t(\eta_k)_2}\ e^{4\pi i(\eta_k)_1^t(\eta_k)_2} \prod_{i\in B'-T-\{k\}} (a_k - a_i). \tag{35}$$

Beweis
Die linke Seite ist definiert, da nach Satz 11 aus $\sharp\,(T \circ U \circ \{k,\infty\}) \circ U = \sharp\, T + 2 = g+1$ gerade $\vartheta[\eta_{T\circ U} + \eta_{\{k,\infty\}}](0) \neq 0$ folgt. Betrachte aus Satz 14 ii:

$$u(a_k, z) = c_k \left(\frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)} \right)^2 \text{ für } z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma. \tag{36}$$

Wende den Differentialoperator D zweimal auf (36) an. Wie schon im Beweis von Satz 16 gezeigt, gelten nach Satz 4:

$$\mathrm{D}^2\, u(a_k, z) = \mathrm{D}\, v(a_k, z) = \frac{1}{2} \left(-w(a_k, z) + (a_k - u_1(z) + w_0(z)) u(a_k, z) \right), \tag{37}$$

$$\begin{aligned}
\mathrm{D}^2\, u(a_k, z) &= \left(c_k \left(\frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)} \right)^2 \right)'' \\
&= \left(2\, c_k\, \frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)}\; \frac{\vartheta[\delta+\eta_k]'(z)\, \vartheta[\delta](z) \;-\; \vartheta[\delta+\eta_k](z)\, \vartheta[\delta]'(z)}{\vartheta[\delta](z)^2} \right)' \\
&= \left(2\, c_k\, \frac{\vartheta[\delta+\eta_k](z)\, \vartheta[\delta+\eta_k]'(z)}{\vartheta[\delta](z)^2} \;-\; 2\, c_k\, \frac{\vartheta[\delta+\eta_k](z)^2\, \vartheta[\delta]'(z)}{\vartheta[\delta](z)^3} \right)' \\
&= 2\, c_k\, \frac{\vartheta[\delta+\eta_k]'(z)^2}{\vartheta[\delta](z)^2} \;+ 2\, c_k\, \frac{\vartheta[\delta+\eta_k](z)\, \vartheta[\delta+\eta_k]''(z)}{\vartheta[\delta](z)^2} \\
&\quad - 8\, c_k\, \frac{\vartheta[\delta+\eta_k](z)\, \vartheta[\delta+\eta_k]'(z)\, \vartheta[\delta]'(z)}{\vartheta[\delta](z)^3} \\
&\quad - 2\, c_k\, \frac{\vartheta[\delta+\eta_k](z)^2\, \vartheta[\delta]''(z)}{\vartheta[\delta](z)^3} \;+ 6\, c_k\, \frac{\vartheta[\delta+\eta_k](z)^2\, \vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^4}.
\end{aligned} \tag{38}$$

Sei $W = T \cup \{k\}$. Es ist $\sharp T = g-1$, $\sharp W = g$ und $\infty \notin W$. $D = \sum_{i\in W}(a_i, 0) - g\cdot\infty \in Pic_0\, C - \Theta$ entspricht $\Omega(\eta_W)_1 + (\eta_W)_2 \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$ nach Korollar 8. Es gelten

$$\begin{aligned}
u(a_k, \Omega(\eta_W)_1 + (\eta_W)_2) &= \prod_{i \in W} (a_k - a_i) = 0, \text{ da } k \in W, \\
w(a_k, \Omega(\eta_W)_1 + (\eta_W)_2) &= \prod_{i \in B' - W} (a_k - a_i) \neq 0.
\end{aligned}$$

Damit ist $\mathrm{D}^2\, u(a_k, \Omega(\eta_W)_1 + (\eta_W)_2) = -\frac{1}{2} w(a_k, \Omega(\eta_W)_1 + (\eta_W)_2) = -\frac{1}{2} \prod_{i\in B'-W}(a_k - a_i)$. Durch $u(a_k, \Omega(\eta_W)_1 + (\eta_W)_2) = c_k \left(\frac{\vartheta[\delta+\eta_k](\Omega(\eta_W)_1+(\eta_W)_2)}{\vartheta[\delta](\Omega(\eta_W)_1+(\eta_W)_2)} \right)^2 = 0$ folgt $\frac{\vartheta[\delta+\eta_k](\Omega(\eta_W)_1+(\eta_W)_2)}{\vartheta[\delta](\Omega(\eta_W)_1+(\eta_W)_2)} = 0$ und (38) impliziert:

$$\mathrm{D}^2\, u(a_k, \Omega(\eta_W)_1 + (\eta_W)_2) = 2\, c_k \left(\frac{\vartheta[\delta+\eta_k]'(\Omega(\eta_W)_1 + (\eta_W)_2)}{\vartheta[\delta](\Omega(\eta_W)_1 + (\eta_W)_2)} \right)^2.$$

Mit Korollar 8 und Lemmata 3 und 10 gilt

$$\begin{aligned}
&\mathrm{D}^2\, u(a_k, \Omega(\eta_W)_1 + (\eta_W)_2) \\
&= 2\, c_k \left(\frac{\vartheta[\delta+\eta_k]'(\Omega(\eta_W)_1 + (\eta_W)_2)}{\vartheta[\delta](\Omega(\eta_W)_1 + (\eta_W)_2)} \right)^2 \\
&= 2\, c_k\, e^{-4\pi i (\eta_W)_1^t (\eta_k)_2} \left(\frac{\vartheta[\delta+\eta_k+\eta_W]'(0) - 2\pi i (\eta_W)_1^t\, h\, \vartheta[\delta+\eta_k+\eta_W](0)}{\vartheta[\delta+\eta_W](0)} \right)^2 \\
&= 2\, c_k\, e^{-4\pi i (\eta_W)_1^t (\eta_k)_2} \left(\frac{\vartheta[\delta+\eta_k+\eta_W]'(0)}{\vartheta[\delta+\eta_W](0)} \right)^2,
\end{aligned}$$

da $\vartheta[\delta+\eta_k+\eta_W](0)=0$ ist, nach Satz 11 und $\sharp\,(U\circ\{k\}\circ W)\circ U=\sharp\,T=g-1\neq g+1$. Also gilt insgesamt

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

□

Lemma 14
Sei $k\in B'$. Dann 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
Wähle $T\subseteq B'$ mit $\sharp\,T=g+1$, $k\in T$. Betrachte die beiden Divisoren mit zugehörigem Punkt des Torus:

$$D_1=\sum_{i\in T-\{k\}}(a_i,0)-g\cdot\infty\in Pic_0\,C-\Theta\sim\Omega(\eta_{T-\{k\}})_1+(\eta_{T-\{k\}})_2\in\mathbb{C}^g/\Gamma-V(\vartheta[\delta])/\Gamma,$$
$$D_2=\sum_{i\in B'-T}(a_i,0)-g\cdot\infty\in Pic_0\,C-\Theta\sim\Omega(\eta_{B'-T})_1+(\eta_{B'-T})_2\in\mathbb{C}^g/\Gamma-V(\vartheta[\delta])/\Gamma.$$

Nach Satz 14 ii, Korollar 8 und Lemma 3 gilt

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

Analog für D_2:

$$\begin{aligned}
&u(a_k,\Omega(\eta_{B'-T})_1+(\eta_{B'-T})_2)\\
&=\prod_{i\in B'-T}(a_k-a_i)\\
&=c_k\,e^{4\pi i(\eta_{B'-T})_1^t(\eta_k)_2}\left(\frac{\vartheta[\delta+\eta_k+\eta_{B'-T}](0)}{\vartheta[\delta+\eta_{B'-T}](0)}\right)^2\\
&=c_k\,e^{4\pi i(\eta_{B'-T})_1^t(\eta_k)_2}\left(\frac{\vartheta[\eta_{U\circ\{k\}\circ(B'-T)}](0)}{\vartheta[\eta_{U\circ\{\infty\}\circ(B'-T)}](0)}\right)^2\\
&=c_k\,e^{4\pi i(\eta_T)_1^t(\eta_k)_2}\left(\frac{\vartheta[\eta_{T\circ U}+\eta_k](0)}{\vartheta[\eta_{T\circ U}](0)}\right)^2,\ \text{da gelten:}
\end{aligned}$$

$U \circ \{k\} \circ (B' - T) \equiv U \circ \{k\} \circ B \circ \{\infty\} \circ T \equiv \mathcal{C}(U \circ T \circ \{k, \infty\}) \equiv T \circ U \circ k \mod (S \sim \mathcal{C}S)$,
$U \circ \{\infty\} \circ (B' - T) \equiv U \circ T \circ B \equiv \mathcal{C}(U \circ T) \equiv T \circ U \mod (S \sim \mathcal{C}S)$ und
$\eta_{B'-T} = \eta_\infty + \eta_{B-T} = 0 + \eta_T$.

Durch Multiplikation der beiden Gleichungen folgt die Behauptung:

$$\begin{aligned}
&u(a_k, \Omega(\eta_{T-\{k\}})_1 + (\eta_{T-\{k\}})_2)\, u(a_k, \Omega(\eta_{B'-T})_1 + (\eta_{B'-T})_2) \\
&= \prod_{i \in T-\{k\}+B'-T} (a_k - a_i) \\
&= \prod_{i \in B'-\{k\}} (a_k - a_i) \\
&= c_k^2\, e^{4\pi i (\eta_k)_1^t (\eta_k)_2}\, \underbrace{e^{8\pi i (\eta_T)_1^t (\eta_k)_2}}_{=1}.
\end{aligned}$$

□

Ich führe eine neue Bezeichnung ein. Für $\overline{T} \in \mathcal{V}$ sei T der Repräsentant, der nur gerade Zahlen enthält. Sei $V' = \{2, 4, ..., 2g\} \subset B'$ und definiere

$$f[\eta_T](z) = \left(\prod_{i \in V'-T} c_i \right) \left(\frac{\vartheta[\eta_T](z)}{\vartheta[\delta](z)} \right)^2.$$

Beispielsweise sind dann

$$\begin{aligned}
f[\delta](z) \quad &= \left(\prod_{i \in V'-V'} c_i \right) \left(\frac{\vartheta[\delta](z)}{\vartheta[\delta](z)} \right)^2 = 1, \text{ mit } \delta = \eta_{V'} \text{ bzw. } \delta = \eta_{V' \circ \{\infty\}}, \\
f[\delta + \eta_k](z) &= \left(\prod_{i \in V'-(V'-\{k\})} c_i \right) \left(\frac{\vartheta[\delta + \eta_k](z)}{\vartheta[\delta](z)} \right)^2 = u(a_k, z),\ k \in V', \\
f[0](z) \quad &= \left(\prod_{i \in V'} c_i \right) \left(\frac{\vartheta[0](z)}{\vartheta[\delta](z)} \right)^2 = c_2 \cdot ... \cdot c_{2g} \left(\frac{\vartheta[0](z)}{\vartheta[\delta](z)} \right)^2.
\end{aligned}$$

Wie angekündigt, zitiere ich den Satz von Mumford und formuliere anschließend einen Satz, aus dem sich ein Algorithmus herleiten läßt, um $\left(\frac{\vartheta[0](z)}{\vartheta[\delta](z)} \right)^2$ zu bestimmen. Der Beweis stützt sich auf den Satz von Mumford und die gerade bewiesenen Lemmata.

Satz 19 ([Mumford 1984], IIIa, 9.9)
Sei $T \subseteq B'$, $\sharp\, T = g - 1$, $k, l \in B' - T$ und $k \neq l$. Dann gilt für $z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$:

$$\begin{aligned}
&\vartheta[\eta_k]'(z)\, \vartheta[\eta_l](z) \;-\; \vartheta[\eta_k](z)\, \vartheta[\eta_l]'(z) \\
&= \pm \frac{\vartheta[\eta_{T \circ U}]'(0)\, \vartheta[\eta_{T \circ U} + \eta_{\{k,l\}}](0)}{\vartheta[\eta_{T \circ U} + \eta_{\{k,\infty\}}](0)\, \vartheta[\eta_{T \circ U} + \eta_{\{l,\infty\}}](0)}\, \vartheta[0](z)\, \vartheta[\eta_{\{k,l\}}](z).
\end{aligned}$$

Satz 20
Sei $\tilde{W} \subseteq V'$, $\sharp\, \tilde{W} \leq g - 2$, $W = \begin{cases} \tilde{W}, & \text{falls } \sharp\, \tilde{W} \text{ gerade}, \\ \tilde{W} \cup \{\infty\}, & \text{falls } \sharp\, \tilde{W} \text{ ungerade}. \end{cases}$
Dann gilt für $k, l \in V' - \tilde{W}$ mit $k > l$ und $z \in \mathbb{C}^g/\Gamma - V(\vartheta[\delta])/\Gamma$:

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

Beweis
Benutze Satz 19,

$$\begin{aligned}&\vartheta[\eta_k]'(z)\,\vartheta[\eta_l](z) \;-\; \vartheta[\eta_k](z)\,\vartheta[\eta_l]'(z)\\&= \pm\,\frac{\vartheta[\eta_{T\circ U}]'(0)\;\vartheta[\eta_{T\circ U}+\eta_{\{k,l\}}](0)}{\vartheta[\eta_{T\circ U}+\eta_{\{k,\infty\}}](0)\;\vartheta[\eta_{T\circ U}+\eta_{\{l,\infty\}}](0)}\;\vartheta[0](z)\;\vartheta[\eta_{\{k,l\}}](z),\end{aligned} \tag{39}$$

und setze für z speziell $z+\Omega(\eta_W)_1+(\eta_W)_2$ ein, wobei $T\subseteq B'$, $\sharp\, T = g-1$ und $k,l\in T$ sind. Anwenden der Lemmata 3 und 10 impliziert für die linke Seite von (39):

$$\begin{aligned}&\vartheta[\eta_k]'(z+\Omega(\eta_W)_1+(\eta_W)_2)\;\vartheta[\eta_l](z+\Omega(\eta_W)_1+(\eta_W)_2)\\&-\vartheta[\eta_k](z+\Omega(\eta_W)_1+(\eta_W)_2)\;\vartheta[\eta_l]'(z+\Omega(\eta_W)_1+(\eta_W)_2)\\&= e^{-2\pi i(\eta_W)_1^t\Omega(\eta_W)_2\;-\;2\pi i(\eta_W)_1^t(2z+(\eta_k)_2+(\eta_l)_2+2(\eta_W)_2)}\\&\quad\Big(\big(\vartheta[\eta_W+\eta_k]'(z)\;-\;2\pi i(\eta_W)_1^t\;h\;\vartheta[\eta_W+\eta_k](z)\big)\,\big(\vartheta[\eta_W+\eta_l](z)\big)\\&\quad-\;\big(\vartheta[\eta_W+\eta_k](z)\big)\,\big(\vartheta[\eta_W+\eta_l]'(z)\;-\;2\pi i(\eta_W)_1^t\;h\;\vartheta[\eta_W+\eta_l](z)\big)\Big)\\&= e^{-2\pi i(\eta_W)_1^t\Omega(\eta_W)_2\;-\;2\pi i(\eta_W)_1^t(2z+(\eta_k)_2+(\eta_l)_2+2(\eta_W)_2)}\\&\quad\big(\vartheta[\eta_W+\eta_k]'(z)\,\vartheta[\eta_W+\eta_l](z)\;-\;\vartheta[\eta_W+\eta_k](z)\,\vartheta[\eta_W+\eta_l]'(z)\big)\end{aligned}$$

und für die rechte:

$$\begin{aligned}&\pm\;\frac{\vartheta[\eta_{T\circ U}]'(0)\;\vartheta[\eta_{T\circ U}+\eta_{\{k,l\}}](0)}{\vartheta[\eta_{T\circ U}+\eta_{\{k,\infty\}}](0)\;\vartheta[\eta_{T\circ U}+\eta_{\{l,\infty\}}](0)}\\&\quad\vartheta[0](z+\Omega(\eta_W)_1+(\eta_W)_2)\;\vartheta[\eta_{\{k,l\}}](z+\Omega(\eta_W)_1+(\eta_W)_2)\\&=\pm\,\frac{\vartheta[\eta_{T\circ U}]'(0)\;\vartheta[\eta_{T\circ U}+\eta_{\{k,l\}}](0)}{\vartheta[\eta_{T\circ U}+\eta_{\{k,\infty\}}](0)\;\vartheta[\eta_{T\circ U}+\eta_{\{l,\infty\}}](0)}\;e^{-2\pi i(\eta_W)_1^t\Omega(\eta_W)_2\;-\;2\pi i(\eta_W)_1^t(2z+(\eta_k)_2+(\eta_l)_2+2(\eta_W)_2)}\\&\quad\vartheta[\eta_W](z)\;\vartheta[\eta_W+\eta_{\{k,l\}}](z).\end{aligned}$$

Daraus ergibt sich

$$\begin{aligned}&\vartheta[\eta_W+\eta_k]'(z)\;\vartheta[\eta_W+\eta_l](z)\;-\;\vartheta[\eta_W+\eta_k](z)\;\vartheta[\eta_W+\eta_l]'(z)\\&=\pm\,\frac{\vartheta[\eta_{T\circ U}]'(0)\;\vartheta[\eta_{T\circ U}+\eta_{\{k,l\}}](0)}{\vartheta[\eta_{T\circ U}+\eta_{\{k,\infty\}}](0)\;\vartheta[\eta_{T\circ U}+\eta_{\{l,\infty\}}](0)}\;\vartheta[\eta_W](z)\;\vartheta[\eta_W+\eta_{\{k,l\}}](z).\end{aligned}\tag{40}$$

Durch Quadrieren von (40) verschwindet das Vorzeichen $\pm$ und durch Lemmata 12, 13 und 14 folgt:

$$\begin{aligned}&\big(\vartheta[\eta_W+\eta_k]'(z)\;\vartheta[\eta_W+\eta_l](z)\;-\;\vartheta[\eta_W+\eta_k](z)\;\vartheta[\eta_W+\eta_l]'(z)\big)^2\\&=\left(\frac{\vartheta[\eta_{T\circ U}]'(0)}{\vartheta[\eta_{T\circ U}+\eta_{\{k,\infty\}}](0)}\right)^2\;\left(\frac{\vartheta[\eta_{T\circ U}+\eta_{\{k,l\}}](0)}{\vartheta[\eta_{T\circ U}+\eta_{\{l,\infty\}}](0)}\right)^2\;\vartheta[\eta_W](z)^2\;\vartheta[\eta_W+\eta_{\{k,l\}}](z)^2\\&=-\,\frac{1}{4}\;\frac{1}{c_k^2}\;\underbrace{e^{8\pi i(\eta_T)_1^t(\eta_k)_2}}_{=1}\;e^{4\pi i(\eta_l)_1^t(\eta_k)_2}\;\underbrace{e^{4\pi i(\eta_k)_1^t(\eta_k)_2}\prod_{i\in B'-T-\{k\}}(a_k-a_i)\;\prod_{i\in T}(a_k-a_i)}_{c_k^2}\\&\quad(a_k-a_l)\;\vartheta[\eta_W](z)^2\;\vartheta[\eta_W+\eta_{\{k,l\}}](z)^2\\&=-\,\frac{1}{4}\;e^{4\pi i(\eta_l)_1^t(\eta_k)_2}\;(a_k-a_l)\;\vartheta[\eta_W](z)^2\;\vartheta[\eta_W+\eta_{\{k,l\}}](z)^2.\end{aligned}$$

Es gilt $(\eta_l)_1^t(\eta_k)_2 = \frac{1}{4}$ für $k > l$, $k, l \in B'$, denn nach Definition sind

$$\eta_{2i-1} = \begin{pmatrix} (0...0\ \frac{1}{2}\ 0...0)^t \\ (\frac{1}{2}...\frac{1}{2}\ 0\ 0...0)^t \end{pmatrix},\ i = 1, ..., g,$$

$$\begin{array}{c} \uparrow \\ i \\ \downarrow \end{array}$$

$$\eta_{2i} = \begin{pmatrix} (0...0\ \frac{1}{2}\ 0...0)^t \\ (\frac{1}{2}...\frac{1}{2}\ \frac{1}{2}\ 0...0)^t \end{pmatrix},\ \text{für } i = 1, ..., g.$$

Damit folgt durch $e^{4\pi i(\eta_l)_1^t(\eta_k)_2} = e^{\pi i} = -1$ die Gleichung:

$$\begin{aligned} &\big(\vartheta[\eta_W + \eta_k]'(z)\ \vartheta[\eta_W + \eta_l](z)\ -\ \vartheta[\eta_W + \eta_k](z)\ \vartheta[\eta_W + \eta_l]'(z)\big)^2 \\ &= \frac{1}{4}\ (a_k - a_l)\ \vartheta[\eta_W](z)^2\ \vartheta[\eta_W + \eta_{\{k,l\}}](z)^2. \end{aligned} \tag{41}$$

Teile (41) durch $\vartheta[\delta](z)^4$ und multipliziere mit
$4\ \left(\prod_{i\in V'-W-\{k\}} c_i\right)\ \left(\prod_{i\in V'-W-\{l\}} c_i\right) = 4\ \left(\prod_{i\in V'-W} c_i\right)\ \left(\prod_{i\in V'-W-\{k,l\}} c_i\right)$,
so daß die zu (41) äquivalente Gleichung gilt:

$$\begin{aligned} &4\ \left(\prod_{i\in V'-W-\{k\}} c_i\right)\ \left(\prod_{i\in V'-W-\{l\}} c_i\right) \\ &\quad\left(\frac{\vartheta[\eta_W + \eta_k]'(z)\ \vartheta[\eta_W + \eta_l](z)\ -\ \vartheta[\eta_W + \eta_k](z)\ \vartheta[\eta_W + \eta_l]'(z)}{\vartheta[\delta](z)^2}\right)^2 \\ &= (a_k - a_l)\ \left(\prod_{i\in V'-W} c_i\right)\ \left(\frac{\vartheta[\eta_W](z)}{\vartheta[\delta](z)}\right)^2\ \left(\prod_{i\in V'-W-\{k,l\}} c_i\right)\ \left(\frac{\vartheta[\eta_W + \eta_k](z)}{\vartheta[\delta](z)}\right)^2 \\ &= (a_k - a_l)\ f[\eta_W](z)\ f[\eta_W + \eta_{\{k,l\}}](z). \end{aligned} \tag{42}$$

Die letzte Zeile ist schon ein Schritt für den Beweis des Satzes. Noch zu zeigen ist:

$$\begin{aligned} &4\ \left(\prod_{i\in V'-W-\{k\}} c_i\right)\ \left(\prod_{i\in V'-W-\{l\}} c_i\right) \\ &\quad\left(\frac{\vartheta[\eta_W + \eta_k]'(z)\ \vartheta[\eta_W + \eta_l](z)\ -\ \vartheta[\eta_W + \eta_k](z)\ \vartheta[\eta_W + \eta_l]'(z)}{\vartheta[\delta](z)^2}\right)^2 \\ &= \frac{\big(f[\eta_W + \eta_k]'(z)\ f[\eta_W + \eta_l](z)\ -\ f[\eta_W + \eta_k](z)\ f[\eta_W + \eta_l]'(z)\big)^2}{f[\eta_W + \eta_k](z)\ f[\eta_W + \eta_l](z)}. \end{aligned}$$

Betrachte dazu

$$\begin{aligned}
f[\eta_T](z) \; &= \left(\prod_{i\in V'-T} c_i\right) \left(\frac{\vartheta[\eta_T](z)}{\vartheta[\delta](z)}\right)^2, \\
f[\eta_T]'(z) \; &= 2 \left(\prod_{i\in V'-T} c_i\right) \left(\frac{\vartheta[\eta_T](z)\;\vartheta[\eta_T]'(z)}{\vartheta[\delta](z)^2} - \frac{\vartheta[\eta_T](z)^2\;\vartheta[\delta]'(z)}{\vartheta[\delta](z)^3}\right), \\
f[\eta_T]'(z)^2 &= 4 \left(\prod_{i\in V'-T} c_i\right)^2 \left(\frac{\vartheta[\eta_T](z)^2\;\vartheta[\eta_T]'(z)^2}{\vartheta[\delta](z)^4} - 2\,\frac{\vartheta[\eta_T](z)^3\;\vartheta[\eta_T]'(z)\;\vartheta[\delta]'(z)}{\vartheta[\delta](z)^5}\right. \\
&\qquad\qquad \left. + \frac{\vartheta[\eta_T](z)^4\;\vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^6}\right).
\end{aligned}$$

Dies impliziert:

$$\begin{aligned}
&4 \left(\prod_{i\in V'-W-\{k\}} c_i\right) \left(\prod_{i\in V'-W-\{l\}} c_i\right) \\
&\left(\frac{\vartheta[\eta_W+\eta_k]'(z)\;\vartheta[\eta_W+\eta_l](z) \;-\; \vartheta[\eta_W+\eta_k](z)\;\vartheta[\eta_W+\eta_l]'(z)}{\vartheta[\delta](z)^2}\right)^2 \\
&= 4 \left(\prod_{i\in V'-W-\{k\}} c_i\right) \left(\prod_{i\in V'-W-\{l\}} c_i\right) \\
&\left(\frac{\vartheta[\eta_W+\eta_k]'(z)^2}{\vartheta[\delta](z)^2}\;\frac{\vartheta[\eta_W+\eta_l](z)^2}{\vartheta[\delta](z)^2}\right. \\
&- 2\,\frac{\vartheta[\eta_W+\eta_k](z)\;\vartheta[\eta_W+\eta_k]'(z)\;\vartheta[\eta_W+\eta_l](z)\;\vartheta[\eta_W+\eta_l]'(z)}{\vartheta[\delta](z)^4} \\
&\left. + \frac{\vartheta[\eta_W+\eta_l]'(z)^2}{\vartheta[\delta](z)^2}\;\frac{\vartheta[\eta_W+\eta_k](z)^2}{\vartheta[\delta](z)^2}\right)
\end{aligned}$$

$$
\begin{aligned}
&= 4 \left(\prod_{i \in V' - W - \{k\}} c_i \right)^2 \frac{\prod_{i \in V' - W - \{l\}} c_i}{\prod_{i \in V' - W - \{k\}} c_i} \left(\frac{\vartheta[\eta_W + \eta_k]'(z)^2 \ \vartheta[\eta_W + \eta_l](z)^2}{\vartheta[\delta](z)^4} \right. \\
&\qquad - \ 2 \, \frac{\vartheta[\eta_W + \eta_k](z) \ \vartheta[\eta_W + \eta_k]'(z) \ \vartheta[\delta]'(z) \ \vartheta[\eta_W + \eta_l](z)^2}{\vartheta[\delta](z)^5} \\
&\qquad \left. + \ \frac{\vartheta[\eta_W + \eta_k](z)^2 \ \vartheta[\delta]'(z)^2 \ \vartheta[\eta_W + \eta_l](z)^2}{\vartheta[\delta](z)^6} \right) \\
&\quad - \ 2 \left(2 \prod_{i \in V' - W - \{k\}} c_i \right) \left(2 \prod_{i \in V' - W - \{l\}} c_i \right) \\
&\qquad \left(\frac{\vartheta[\eta_W + \eta_k](z) \ \vartheta[\eta_W + \eta_k]'(z) \ \vartheta[\eta_W + \eta_l](z) \ \vartheta[\eta_W + \eta_l]'(z)}{\vartheta[\delta](z)^4} \right. \\
&\qquad - \ \frac{\vartheta[\eta_W + \eta_k](z) \ \vartheta[\eta_W + \eta_k]'(z) \ \vartheta[\eta_W + \eta_l](z)^2 \ \vartheta[\delta]'(z)}{\vartheta[\delta](z)^5} \\
&\qquad - \ \frac{\vartheta[\eta_W + \eta_k](z)^2 \ \vartheta[\delta]'(z) \ \vartheta[\eta_W + \eta_l](z) \ \vartheta[\eta_W + \eta_l]'(z)}{\vartheta[\delta](z)^5} \\
&\qquad \left. + \ \frac{\vartheta[\eta_W + \eta_k](z)^2 \ \vartheta[\eta_W + \eta_l](z)^2 \ \vartheta[\delta]'(z)^2}{\vartheta[\delta](z)^6} \right) \\
&\quad + \ 4 \left(\prod_{i \in V' - W - \{l\}} c_i \right)^2 \frac{\prod_{i \in V' - W - \{k\}} c_i}{\prod_{i \in V' - W - \{l\}} c_i} \left(\frac{\vartheta[\eta_W + \eta_l]'(z)^2 \ \vartheta[\eta_W + \eta_k](z)^2}{\vartheta[\delta](z)^4} \right. \\
&\qquad - \ 2 \, \frac{\vartheta[\eta_W + \eta_l](z) \ \vartheta[\eta_W + \eta_l]'(z) \ \vartheta[\delta]'(z) \ \vartheta[\eta_W + \eta_k](z)^2}{\vartheta[\delta](z)^5} \\
&\qquad \left. + \ \frac{\vartheta[\eta_W + \eta_l](z)^2 \ \vartheta[\delta]'(z)^2 \ \vartheta[\eta_W + \eta_k](z)^2}{\vartheta[\delta](z)^6} \right)
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{f[\eta_W + \eta_k]'(z)^2 \ f[\eta_W + \eta_l](z)}{f[\eta_W + \eta_k](z)} \ - \ 2 \ f[\eta_W + \eta_k]'(z) \ f[\eta_W + \eta_l]'(z) \\
&\quad + \ \frac{f[\eta_W + \eta_l]'(z)^2 \ f[\eta_W + \eta_k](z)}{f[\eta_W + \eta_l](z)}
\end{aligned}
$$

$$
= \frac{\left(f[\eta_W + \eta_k]'(z) \ f[\eta_W + \eta_l](z) \ - \ f[\eta_W + \eta_k](z) \ f[\eta_W + \eta_l]'(z) \right)^2}{f[\eta_W + \eta_k](z) \ f[\eta_W + \eta_l](z)}.
$$

Damit folgt aus (42)

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

und somit die Behauptung des Satzes.

$\square$

Diese allgemeinen Betrachtungen zu beliebigem Geschlecht $g \geq 1$ werde ich in den beiden folgenden Abschnitten zur Herleitung der Additionsformeln für Geschlecht 1 und 2 nutzen.

5.2 Explizite Additionsformeln für Geschlecht 1

Die in Abschnitt 2.1 in Satz 6 entwickelten Additionsformeln für das Rechnen auf einer elliptischen Kurve $C\ :\ y^2 = x^3 + ax + b$ werde ich durch Anwenden der auf den vorangegangenen Seiten beschriebenen Theorie für Geschlecht 1 wiederholen, obwohl das Ergebnis nicht überraschen wird.

Ich betrachte die Gleichung aus Satz 18 ii. mit $\mathrm{D}^x = \frac{\partial}{\partial x}$ und $\mathrm{D}^u = \frac{\partial}{\partial u}$:

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

und werde dazu den Term

$$-\left(\frac{\partial}{\partial x} + \frac{\partial}{\partial u}\right)^2 \left(\log\left(\sum_{\overline{T}\in\mathcal{V}} e^{4\pi i \delta_1^t (\eta_T)_2}\ \frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2}\right)\right) \tag{43}$$

explizit berechnen. Für Geschlecht 1 gelten bekanntlich: $B = \{1,2,3,4\},\ U = \{1,3\},\ V = \{2,4\}$, $\mathcal{U} = \{\overline{\emptyset}, \overline{\{1,3\}}\},\ \mathcal{V} = \{\overline{\emptyset}, \overline{\{2,4\}}\}$, $\eta_1 = \begin{pmatrix}\frac{1}{2}\\ 0\end{pmatrix}, \eta_2 = \begin{pmatrix}\frac{1}{2}\\ \frac{1}{2}\end{pmatrix}, \eta_3 = \begin{pmatrix}0\\ \frac{1}{2}\end{pmatrix}, \eta_4 = \begin{pmatrix}0\\ 0\end{pmatrix}, \delta = \begin{pmatrix}\frac{1}{2}\\ \frac{1}{2}\end{pmatrix}$ mit $\delta = \eta_U = \eta_1 + \eta_3$. Für die Summe besteht ein besonderes Interesse an den η_T für $\overline{T} \in \mathcal{V}$, die da sind: $\eta_\emptyset = 0,\ \eta_{\{2,4\}} = \eta_2 = \delta$. Damit besteht die Summe in (43) aus zwei Summanden:

$$\begin{aligned}
&\sum_{\overline{T}\in\mathcal{V}} e^{4\pi i \delta_1^t (\eta_T)_2}\ \frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2}\\
&= e^{4\pi i \frac{1}{2}\cdot 0}\ \frac{\vartheta[\delta+0](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[0](u)^2}{\vartheta[\delta](u)^2} +\ e^{4\pi i \frac{1}{2}\cdot\frac{1}{2}}\ \frac{\vartheta[\delta+\delta](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\delta](u)^2}{\vartheta[\delta](u)^2}\\
&= \frac{\vartheta[\delta](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[0](u)^2}{\vartheta[\delta](u)^2}\ -\ \frac{\vartheta[\delta+\delta](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\delta](u)^2}{\vartheta[\delta](u)^2}.
\end{aligned}$$

Es sind für $z \in (\mathbb{C}/\Gamma) - \Gamma$:

$$\begin{aligned}
\frac{\vartheta[\delta](z)^2}{\vartheta[\delta](z)^2} &= 1,\\
\frac{\vartheta[\delta+\eta_2](z)^2}{\vartheta[\delta](z)^2} = \frac{\vartheta[\delta+\delta](z)^2}{\vartheta[\delta](z)^2} = \frac{\vartheta[0](z)^2}{\vartheta[\delta](z)^2} &= \frac{1}{c_2}u(a_k, z) = \frac{1}{c_2}(a_2 + u_1(z)) = \frac{1}{c_2}(a_2 - \wp(z)).
\end{aligned}$$

Also folgt:

$$\begin{aligned}
&\sum_{\overline{T}\in\mathcal{V}} e^{4\pi i \delta_1^t (\eta_T)_2}\ \frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2}\\
&= \frac{\vartheta[0](u)^2}{\vartheta[\delta](u)^2}\ -\ \frac{\vartheta[0](x)^2}{\vartheta[\delta](x)^2}\\
&= \frac{1}{c_2}(a_2 - \wp(u)) - \frac{1}{c_2}(a_2 - \wp(x))\\
&= \frac{1}{c_2}\left(\wp(x) - \wp(u)\right).
\end{aligned} \tag{44}$$

Wende $-\left(\frac{\partial}{\partial x}+\frac{\partial}{\partial u}\right)^2(\log)$ auf (44) an:

$$\begin{aligned}
&-\left(\frac{\partial}{\partial x}+\frac{\partial}{\partial u}\right)^2\left(\log\left(\frac{1}{c_2}\left(\wp(x)-\wp(u)\right)\right)\right)\\
&=-\left(\frac{\partial}{\partial x}+\frac{\partial}{\partial u}\right)\left(\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\right)\\
&=-\frac{\left(\wp''(x)-\wp''(u)\right)\left(\wp(x)-\wp(u)\right)\;-\;\left(\wp'(x)-\wp'(u)\right)^2}{\left(\wp(x)-\wp(u)\right)^2}\\
&=-\frac{\wp''(x)-\wp''(u)}{\wp(x)-\wp(u)}+\left(\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\right)^2
\end{aligned}\tag{45}$$

und ersetze $\wp''(z)$ durch $F_0(\wp(z),\wp'(z))=\frac{3}{2}\wp(z)^2+\frac{a}{2}$:

$$\begin{aligned}
&-\frac{\wp''(x)-\wp''(u)}{\wp(x)-\wp(u)}+\left(\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\right)^2\\
&=-\frac{3}{2}\,\frac{\wp(x)^2-\wp(u)^2}{\wp(x)-\wp(u)}+\left(\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\right)^2\\
&=-\frac{3}{2}\,\frac{\left(\wp(x)-\wp(u)\right)\left(\wp(x)+\wp(u)\right)}{\wp(x)-\wp(u)}+\left(\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\right)^2\\
&=-\frac{3}{2}\left(\wp(x)+\wp(u)\right)+\left(\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\right)^2.
\end{aligned}$$

Dadurch ist (43) als rationale Kombination der $\wp(x),\wp'(x),\wp(u),\wp'(u)$ dargestellt und es folgt durch Satz 18 die Additionsformel

$$\begin{aligned}
\wp(x+u)&=\frac{1}{2}\wp(x)+\frac{1}{2}\wp(u)-\frac{3}{2}\left(\wp(x)+\wp(u)\right)+\left(\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\right)^2\\
&=-\wp(x)-\wp(u)+\left(\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\right)^2.
\end{aligned}$$

Das ist die Additionsformel für $\wp(x+u)$. Eine Formel für $\wp'(x+u)$ läßt sich durch Differentiation nach z.B. x ermitteln:

$$\begin{aligned}
&\wp'(x+u)\\
&=\frac{\partial}{\partial x}\wp(x+u)\\
&=-\wp'(x)+2\frac{\wp'(x)-\wp'(u)}{\wp(x)-\wp(u)}\,\frac{\wp''(x)(\wp(x)-\wp(u))\;-\;(\wp'(x)-\wp'(u))\wp'(x)}{(\wp(x)-\wp(u))^2}\\
&=-\wp'(x)+2\frac{\wp'(x)-\wp'(u)}{(\wp(x)-\wp(u))^2}\,\wp''(x)\;-2\frac{(\wp'(x)-\wp'(u))^2}{(\wp(x)-\wp(u))^3}\,\wp'(x)\\
&=-\wp'(x)\;+\frac{\wp'(x)-\wp'(u)}{(\wp(x)-\wp(u))^2}\,(3\wp(x)^2+a)\;-2\frac{(\wp'(x)-\wp'(u))^2}{(\wp(x)-\wp(u))^3}\,\wp'(x).
\end{aligned}$$

Das Resultat fasse ich in einem Satz zusammen.

Satz 21 (Additionsformeln für elliptische Kurven)
Für $x, u, x+u \in (\mathbb{C}/\Gamma) - \Gamma$ und $(\wp(x), \wp'(x)) \neq (\wp(u), \wp'(u))$ gelten die Gleichungen

$$\wp(x+u) = -\wp(x) - \wp(u) + \left(\frac{\wp'(x) - \wp'(u)}{\wp(x) - \wp(u)}\right)^2,$$
$$\wp'(x+u) = -\wp'(x) \; + \; \frac{\wp'(x) - \wp'(u)}{(\wp(x) - \wp(u))^2}\,(3\wp(x)^2 + a) \; - \; 2\,\frac{(\wp'(x) - \wp'(u))^2}{(\wp(x) - \wp(u))^3}\,\wp'(x).$$

□

Additionsformeln für die $\wp$–Funktion beim Geschlecht 1 habe ich bereits in Abschnitt 2.1 hergeleitet. Satz 6 faßt die Ergebnisse zusammen, unterscheidet sich jedoch von den Formeln aus Satz 21. Wie schon erwähnt, liegt der Grund darin begründet, daß die klassische Weierstraßsche $\wp$–Funktion, hier mit $\tilde{\wp}$ bezeichnet, durch $\tilde{\wp}(z) = -\frac{\mathrm{d}^2}{\mathrm{d}\,z^2}(\log(\sigma(z)))$ definiert wird und die Differentialgleichung $\tilde{\wp}'(z)^2 = 4\tilde{\wp}(z)^3 + \tilde{a}\tilde{\wp}(z) + \tilde{b}$ löst, während die in Abschnitt 4 verallgemeinerte $\wp$–Funktion für $g = 1$ die Form $\wp(z) = -4\,\frac{\mathrm{d}^2}{\mathrm{d}\,z^2}(\log(\vartheta\begin{bmatrix}\frac{1}{2}\\ \frac{1}{2}\end{bmatrix}(z)))$ hat und die Differentialgleichung ohne Faktor 4 löst: $\wp'(z)^2 = \wp(z)^3 + a\wp(z) + b$.

Die Relationen $\tilde{\wp}(z) = \frac{1}{4}\wp(z)$, $\tilde{a} = \frac{1}{4}a$ und $\tilde{b} = \frac{1}{16}b$ überführen beide Definitionen und Differentialgleichungen ineinander und die Additionsformeln aus Satz 6 in die aus Satz 21:

$$\begin{aligned}
& \tilde{\wp}(x+u) = -\tilde{\wp}(x) - \tilde{\wp}(u) - \frac{1}{4}\left(\frac{\tilde{\wp}'(x) - \tilde{\wp}'(u)}{\tilde{\wp}(x) - \tilde{\wp}(u)}\right)^2 \\
\Longleftrightarrow\; & 4\tilde{\wp}(x+u) = -4\tilde{\wp}(x) - 4\tilde{\wp}(u) - \left(\frac{4\,\tilde{\wp}'(x) - 4\,\tilde{\wp}'(u)}{4\,\tilde{\wp}(x) - 4\,\tilde{\wp}(u)}\right)^2 \\
\Longleftrightarrow\; & \wp(x+u) = -\wp(x) - \wp(u) - \left(\frac{\wp'(x) - \wp'(u)}{\wp(x) - \wp(u)}\right)^2,
\end{aligned}$$

$$\begin{aligned}
& \tilde{\wp}'(x+u) = -\tilde{\wp}'(x) + \frac{\tilde{\wp}'(x) - \tilde{\wp}'(u)}{(\tilde{\wp}(x) - \tilde{\wp}(u))^2}\left(3\tilde{\wp}(x)^2 + \frac{\tilde{a}}{4}\right) \\
& \qquad - \frac{1}{2}\,\frac{(\tilde{\wp}'(x) - \tilde{\wp}'(u))^2}{(\tilde{\wp}(x) - \tilde{\wp}(u))^3}\,\tilde{\wp}'(x) \\
\Longleftrightarrow\; & 4\tilde{\wp}'(x+u) = -4\tilde{\wp}'(x) + 4\,\frac{4\,(4\,\tilde{\wp}'(x) - 4\,\tilde{\wp}'(u))}{(4\,\tilde{\wp}(x) - 4\,\tilde{\wp}(u))^2}\left(3\tilde{\wp}(x)^2 + \frac{\tilde{a}}{4}\right) \\
& \qquad - 2\,\frac{4\,(4\,\tilde{\wp}'(x) - 4\,\tilde{\wp}'(u))^2}{(4\,\tilde{\wp}(x) - 4\,\tilde{\wp}(u))^3}\,\tilde{\wp}'(x) \\
\Longleftrightarrow\; & \wp'(x+u) = -\wp'(x) + \frac{\wp'(x) - \wp'(u)}{(\wp(x) - \wp(u))^2}\left(3\wp(x)^2 + a\right) \\
& \qquad - 2\frac{(\wp'(x) - \wp'(u))^2}{(\wp(x) - \wp(u))^3}\,\wp'(x).
\end{aligned}$$

In Satz 21 ist vorausgesetzt, daß $(\wp(x), \wp'(x))$ und $(\wp(u), \wp'(u))$ zwei verschiedene Punkte sind. Analog zu Abschnitt 2.1 gelten für $(\wp(x), \wp'(x)) = (\wp(u), \wp'(u))$ die Verdopplungsformeln.

Satz 22 (Verdopplungsformeln für elliptische Kurven)
Für $x, 2x \in (\mathbb{C}/\Gamma) - \Gamma$ gelten

$$\begin{aligned}
\wp(2x) &= -2\wp(x) + \frac{1}{4}\left(\frac{3\wp(x)^2 + a}{\wp'(x)}\right)^2, \\
\wp'(2x) &= -\wp'(x) + \frac{3}{2}\frac{\wp(x)}{\wp'(x)}\ \big(3\wp(x)^2\ +\ a\big) - \frac{1}{8}\left(\frac{3\wp(x)^2\ +\ a}{\wp'(x)}\right)^3.
\end{aligned}$$

Beweis

$$\begin{aligned}
\wp(2x) &= \lim_{u\to x} \wp(x+u) \\
&= -2\wp(x) + \left(\frac{\wp''(x)}{\wp'(x)}\right)^2 \\
&= -2\wp(x) + \frac{1}{4}\left(\frac{3\wp(x)^2\ +\ a}{\wp'(x)}\right)^2, \\
\wp'(2x) &= \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}\,x}\wp(2x) \\
&= -\wp'(x) + \frac{1}{4}\frac{3\wp(x)^2\ +\ a}{\wp'(x)}\ \frac{6\wp(x)\ \wp'(x)^2\ -\ (3\wp(x)^2\ +\ a)\wp''(x)}{\wp'(x)^2} \\
&= -\wp'(x) + \frac{3}{2}\frac{\wp(x)}{\wp'(x)}\ \big(3\ \wp(x)^2\ +\ a\big) - \frac{1}{8}\left(\frac{3\wp(x)^2\ +\ a}{\wp'(x)}\right)^3.
\end{aligned}$$

□

Diese Formeln lassen sich auf die Verdopplungsformeln zur klassischen Weierstraßschen $\wp$–Funktion aus Satz 7 ganz analog mit $\tilde{\wp}(z) = \frac{1}{4}\wp(z)$ und $\tilde{a} = \frac{1}{4}a$ übertragen.

Zu $P = (\wp(x), \wp'(x))$ ist $\neg P = (\wp(x), -\wp'(x))$ der inverse Punkt und es gilt $P + \neg P = \infty$.

5.3 Explizite Additionsformeln für Geschlecht 2

In diesem Abschnitt leite ich Additionsformeln für eine Jacobi–Varietät her, die von der hyperelliptischen Kurve $C:\ y^2 = x^5 + f_1x^4 + f_2x^3 + f_3x^2 + f_4x + f_5$ vom Geschlecht 2 erzeugt wird. Wieder ist die Gleichung

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

aus Satz 18 der Ausgangspunkt, wobei der Term

$$\sum_{T\in\mathcal{V}} e^{4\pi i\delta_1^t(\eta_T)_2}\ \frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2} \qquad (46)$$

konkret ausgerechnet werden soll. Aus den vorigen Beispielen 9, 11 und 15 ist bekannt:

$$\begin{aligned}
&B = \{1,2,3,4,5,6\},\ U = \{1,3,5\},\ V = \{2,4,6\}, \\
&\mathcal{U} = \{\overline{\emptyset}, \overline{\{1,3\}}, \overline{\{1,5\}}, \overline{\{3,5\}}\},\ \mathcal{V} = \{\overline{\emptyset}, \overline{\{2,4\}}, \overline{\{2,6\}}, \overline{\{4,6\}}\},
\end{aligned}$$

$$\eta_1 = \begin{pmatrix} \frac12 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ \eta_2 = \begin{pmatrix} \frac12 \\ 0 \\ \frac12 \\ 0 \end{pmatrix},\ \eta_3 = \begin{pmatrix} 0 \\ \frac12 \\ \frac12 \\ 0 \end{pmatrix},\ \eta_4 = \begin{pmatrix} 0 \\ \frac12 \\ \frac12 \\ \frac12 \end{pmatrix},\ \eta_5 = \begin{pmatrix} 0 \\ 0 \\ \frac12 \\ \frac12 \end{pmatrix},\ \eta_6 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$\delta = \eta_U = \eta_1 + \eta_3 + \eta_5 = \begin{pmatrix} \frac12 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \frac12 \\ \frac12 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \frac12 \\ \frac12 \end{pmatrix} \equiv \begin{pmatrix} \frac12 \\ \frac12 \\ 0 \\ \frac12 \end{pmatrix} \quad \mathrm{mod}\ \ \mathbb{Z}^4.$$

In der Summe in (46) wird über die folgenden η_T summiert:

$$\eta_\emptyset = 0,\ \eta_{\{2,4\}} = \eta_2 + \eta_4 = \delta,\ \eta_{\{2,6\}} = \eta_2 + \eta_6 = \eta_2,\ \eta_{\{4,6\}} = \eta_4 + \eta_6 = \eta_4.$$

Sie implizieren

$$\begin{aligned}
&\sum_{T\in\mathcal{V}} e^{4\pi i\delta_1^t(\eta_T)_2}\ \frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2} \\
&= e^{4\pi i(\frac12\cdot 0\,+\,\frac12\cdot 0)}\ \frac{\vartheta[\delta](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[0](u)^2}{\vartheta[\delta](u)^2} \\
&\quad + e^{4\pi i(\frac12\cdot 0\,+\,\frac12\cdot\frac12)}\ \frac{\vartheta[\delta+\eta_{\{2,4\}}](x)^2}{\vartheta[\eta_{\{2,4\}}](x)^2}\ \frac{\vartheta[\eta_{\{2,4\}}](u)^2}{\vartheta[\delta](u)^2} \\
&\quad + e^{4\pi i(\frac12\cdot\frac12\,+\,\frac12\cdot 0)}\ \frac{\vartheta[\delta+\eta_{\{2,6\}}](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_{\{2,6\}}](u)^2}{\vartheta[\delta](u)^2} \\
&\quad + e^{4\pi i(\frac12\cdot\frac12\,+\,\frac12\cdot\frac12)}\ \frac{\vartheta[\delta+\eta_{\{4,6\}}](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_{\{4,6\}}](u)^2}{\vartheta[\delta](u)^2} \\
&= \frac{\vartheta[0](u)^2}{\vartheta[\delta](u)^2} - \frac{\vartheta[0](x)^2}{\vartheta[\delta](x)^2} - \frac{\vartheta[\delta+\eta_2](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_2](u)^2}{\vartheta[\delta](u)^2} + \frac{\vartheta[\delta+\eta_4](x)^2}{\vartheta[\delta](x)^2}\ \frac{\vartheta[\eta_4](u)^2}{\vartheta[\delta](u)^2}.
\end{aligned}$$

Nach Lemma 11 gelten die Kongruenzen

$$\begin{aligned}
\delta + \eta_2 &\equiv \delta + \eta_{\{2,6\}} \equiv \eta_{\{1,2,3,5,6\}} \equiv \eta_4 \quad \mathrm{mod}\ \mathbb{Z}^4, \\
\delta + \eta_4 &\equiv \delta + \eta_{\{4,6\}} \equiv \eta_{\{1,3,4,5,6\}} \equiv \eta_2 \quad \mathrm{mod}\ \mathbb{Z}^4,
\end{aligned}$$

so daß über die Summanden aus (46) nach Satz 14 bekannt ist:

$$\begin{aligned}
\frac{\vartheta[\delta+\eta_2](z)^2}{\vartheta[\delta](z)^2} &= \frac{\vartheta[\eta_4](z)^2}{\vartheta[\delta](z)^2} = \frac{1}{c_2}u(a_2,z), \\
\frac{\vartheta[\delta+\eta_4](z)^2}{\vartheta[\delta](z)^2} &= \frac{\vartheta[\eta_2](z)^2}{\vartheta[\delta](z)^2} = \frac{1}{c_4}u(a_4,z).
\end{aligned}$$

Die Terme $u(a_2,z)$ und $u(a_4,z)$ lassen sich konkret aus $u(t,z) = t^2 + u_1(z)t + u_2(z)$ mit Algorithmus 1 aus Abschnitt 4.3 bestimmen. Für $z \in \mathbb{C}^2/\Gamma - V(\vartheta[\delta])/\Gamma$ gelten:

$$\begin{aligned}
&u_1(z) = \frac{f_1}{2} - \wp(z), \\
&u_2(z) = -\frac{f_1^2}{8} + \frac{f_2}{2} - \frac{f_1}{2}\wp(z) + \frac32\wp(z)^2 - \wp''(z), \\
\Longrightarrow\ &u(t,z) = t^2 + \frac{f_1}{2}\,t - \wp(z)\,t - \frac{f_1^2}{8} + \frac{f_2}{2} - \frac{f_1}{2}\wp(z) + \frac32\wp(z)^2 - \wp''(z).
\end{aligned}$$

Mit $f[\delta+\eta_k](z) = u(a_k,z) = c_k \left(\frac{\vartheta[\delta+\eta_k](z)}{\vartheta[\delta](z)}\right)^2$, $k \in V$, gelten somit

$$\begin{aligned}
f[\eta_2](z) &= f[\delta+\eta_4](z)\\
&= u(a_4,z)\\
&= a_4^2 + \frac{1}{2}a_4 f_1 - \frac{1}{8}f_1^2 + \frac{1}{2}f_2 - a_4\wp(z) - \frac{1}{2}f_1\wp(z) + \frac{3}{2}\wp(z)^2 - \wp''(z),\\
f[\eta_4](z) &= f[\delta+\eta_2](z)\\
&= u(a_2,z)\\
&= a_2^2 + \frac{1}{2}a_2 f_1 - \frac{1}{8}f_1^2 + \frac{1}{2}f_2 - a_2\wp(z) - \frac{1}{2}f_1\wp(z) + \frac{3}{2}\wp(z)^2 - \wp''(z).
\end{aligned}$$

Es bleibt der Term $\frac{\vartheta[0](z)^2}{\vartheta[\delta](z)^2}$ zu bestimmen. Benutze dazu Satz 20; in der dortigen Notation sind

$$\begin{aligned}
\eta_W &\equiv \delta + \eta_2 + \eta_4 = 0 \mod \mathbb{Z}^4,\\
\eta_W + \eta_4 &\equiv \delta + \eta_2 \mod \mathbb{Z}^4,\\
\eta_W + \eta_2 &\equiv \delta + \eta_4 \mod \mathbb{Z}^4,\\
\eta_W + \eta_4 + \eta_2 &\equiv \delta \mod \mathbb{Z}^4,
\end{aligned}$$

mit $k = 4 > 2 = l$. Die Identitäten $f[0](z) = c_2\, c_4\, \frac{\vartheta[0](z)^2}{\vartheta[\delta](z)^2}$, $f[\delta+\eta_k](z) = u(a_k,z)$, $k \in V$, und $f[\delta](z) = 1$ implizieren

$$\begin{aligned}
f[0](z) &= \frac{\left(f[\delta+\eta_2]'(z)\ f[\delta+\eta_4](z)\ -\ f[\delta+\eta_2](z)\ f[\delta+\eta_4]'(z)\right)^2}{(a_4-a_2)\ f[\delta+\eta_2](z)\ f[\delta+\eta_4](z)\ f[\delta](z)}\\
&= \frac{(u'(a_2,z)\ u(a_4,z)\ -\ u(a_2,z)\ u'(a_4,z))^2}{(a_4-a_2)\ u(a_2,z)\ u(a_4,z)}.
\end{aligned} \tag{47}$$

Werden konkret $u(a_2,z)$, $u'(a_2,z)$, $u(a_4,z)$ und $u'(a_4,z)$ eingesetzt und die Terme $\wp'''(z)^2$ und $\wp'(z)\wp'''(z)$, mittels der in Algorithmus 2 in Beispiel 19 ermittelten Gleichungen $F_1 = 0$ und $F_2 = 0$, durch rationale Kombinationen in $\wp(z)$, $\wp'(z)$, $\wp''(z)$ und $\wp'''(z)$ersetzt, so läßt sich berechnen:

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

Mit diesem Ergebnis für $f[0](z)$ wertet Maple (46) aus:

$$
\begin{aligned}
&\sum_{T\in\mathcal{V}} e^{4\pi i\delta_1^t(\eta_T)_2}\,\frac{\vartheta[\delta+\eta_T](x)^2}{\vartheta[\delta](x)^2}\,\frac{\vartheta[\eta_T](u)^2}{\vartheta[\delta](u)^2}\\
&=\frac{\vartheta[0](u)^2}{\vartheta[\delta](u)^2}\;-\;\frac{\vartheta[0](x)^2}{\vartheta[\delta](x)^2}\;-\;\frac{\vartheta[\delta+\eta_2](x)^2}{\vartheta[\delta](x)^2}\,\frac{\vartheta[\eta_2](u)^2}{\vartheta[\delta](u)^2}\;+\;\frac{\vartheta[\delta+\eta_4](x)^2}{\vartheta[\delta](x)^2}\,\frac{\vartheta[\eta_4](u)^2}{\vartheta[\delta](u)^2}\\
&=\frac{1}{c_2c_4}f[0](u)\;-\;\frac{1}{c_2c_4}f[0](x)\;-\;\frac{1}{c_2}f[\eta_2](x)\,\frac{1}{c_4}f[\eta_4](u)\;+\;\frac{1}{c_4}f[\eta_4](x)\,\frac{1}{c_2}f[\eta_2](u)\\
&=\frac{1}{c_2c_4}\;\left(f[0](u)\;-\;f[0](x)\;-\;f[\eta_2](x)\,f[\eta_4](u)\;+\;f[\eta_4](x)\,f[\eta_2](u)\right)\\
&=\frac{1}{c_2c_4}\frac{1}{a_4-a_2}\,\Big(-\wp'(x)^2\;+\;\wp'(u)^2\;+\;\frac{1}{2}\wp(u)^3\;-\;\frac{1}{2}\wp(x)^3\;-\;\frac{3}{2}\wp(x)\wp(u)^2\\
&\quad+\frac{3}{2}\wp(x)^2\wp(u)\;-\;\wp''(x)\wp(u)\;+\;\wp(x)\wp''(x)\;+\;\wp(x)\wp''(u)\;-\;\wp(u)\wp''(u)\Big)\\
&=\frac{1}{2c_2c_4(a_4-a_2)}\\
&\quad\left((\wp(u)-\wp(x))^3\;+\;2(\wp'(u)^2-\wp'(x)^2)\;+\;2(\wp(x)-\wp(u))(\wp''(x)+\wp''(u))\right),
\end{aligned}
$$

womit eine Additionsformel für $g=2$ erreicht ist, in der der Faktor $\frac{1}{2c_2c_4(a_4-a_2)}$ unter logarithmischem Ableiten verschwindet.

Satz 23 (Additionsformel für Jacobi–Varietäten bei Geschlecht 2**)**
Für $x, u, x+u \in \mathbb{C}^2/\Gamma - V(\vartheta[\delta])/\Gamma$ gilt

$$
\begin{aligned}
\wp(x+u) = {}&\frac{1}{2}\wp(x)+\frac{1}{2}\wp(u)\\
&-(\mathrm{D}^x+\mathrm{D}^u)^2\left(\log\left((\wp(u)-\wp(x))^3\right.\right.\\
&\qquad\left.\left.+2\left(\wp'(u)^2-\wp'(x)^2\right)+2\left(\wp(x)-\wp(u)\right)(\wp''(x)+\wp''(u))\right)\right).
\end{aligned}
$$

Satz 23 ist nicht vollständig bis zu Ende ausformuliert. Während ich im Abschnitt 5.2 die zweite logarithmische Ableitung für Geschlecht 1 konkret errechnete, möchte ich hier darauf verzichten, denn das Ergebnis ist sehr platzraubend und ein Computer–Algebra–System berechnet dies schnell. Desweiteren beschränke ich mich auf die Angabe von $\wp(x+u)$, obwohl die Additionsformel erst mit $\wp'(x+u)$, $\wp''(x+u)$ und $\wp'''(x+u)$ vollständig wäre. Da das vollständige Ergebnis jedoch die Seitenzahl meiner Arbeit mehr als verdoppeln würde, verzichte ich hier darauf.

Der zu $(\wp(x), \wp'(x), \wp''(x), \wp'''(x)) \in Jac\,C - \Theta$ inverse Punkt ist $(\wp(x), -\wp'(x), \wp''(x), -\wp'''(x))$ und die Verdopplung eines Punktes P wird via $2P = (P + (P + Q)) + \neg Q$ ausgeführt.

□

Beispiel 20
Die hyperelliptische Kurve sei durch $C : y^2 = x^5+1$ gegeben. Punkte von $JacC-\Theta$ sind diejenigen Punkte, für die die beiden Gleichungen verschwinden:

$$
\begin{aligned}
F_1(z_1,z_2,z_3,z_4) &= \frac{5}{4}z_1^4-5z_1z_2^2-z_3^2+2z_2z_4,\\
F_2(z_1,z_2,z_3,z_4) &= -1-3z_1^5+\frac{15}{2}z_1^2z_2^2+5z_1^3z_3+z_2^2z_3-2z_1z_3^2-6z_1z_2z_4+z_4^2.
\end{aligned}
$$

Maple besitzt die Funktion „solve“ zum Lösen von Gleichungssystemen und ermittelt daraus zum Beispiel die Lösungen $\left(z_1, 0, \frac{1}{2}\sqrt{5}z_1^2, \frac{1}{2}\sqrt{4 - 10\sqrt{5}z_1^5 + 22z_1^5}\right)$. Drei Punkte der Varietät sind näherungsweise:

$$
\begin{aligned}
P &\approx (15, 0, 251.5576, 261.6712i),\\
Q &\approx (2i, 0, -4.4721, 1.4237 - 1.0134i),\\
R &\approx (3, 0, 10.0623, 4.5729i).
\end{aligned}
$$

Mit der Additionsformel aus Satz 23 und den zugehörigen Ableitungen, die zu umfangreich zum Aufschreiben, für den Rechner aber gut zu handhaben sind, folgt:

$$
\begin{aligned}
P + Q &\approx (0.4025 + 1.9625i, -0.5353 - 1.7060i, -3.4220 + 2.6126i, 9.4690 - 6.4706i),\\
Q + R &\approx (1.0250 + 0.5331i, -2.7206 - 0.8566i, 3.1586 - 0.7109i, -8.6978 - 2.5775i),\\
P + R &\approx (2.2777, 2.6067i, 3.7816, 18.5542i).
\end{aligned}
$$

Interessant ist die Assoziativität, es gilt

$$
\begin{aligned}
&P + (Q + R) = (P + Q) + R = (P + R) + Q\\
&\approx (0.7205 - 0.3895i, -1.6978 + 1.0004i, 1.4640 - 3.1792i, -1.5248 + 6.3741i).
\end{aligned}
$$

Für die Verdopplung eines Punktes berechne $2P = (P + (P + Q)) + \neg Q$:

$$
\begin{aligned}
\neg Q &\approx (2i, 0, -4.4721, -1.4237 + 1.0134i),\\
P + (P + Q) &\approx (1.2889 + 1.3588i, -2.4343 - 2.0444i, 2.3489 + 4.9570i, -2.9654 - 18.2375i),\\
2P &\approx (6.0000, 18.0848i, 9.0008, 313.8227i).
\end{aligned}
$$

Beispiel 21
Betrachte die hyperelliptische Kurve $C : y^2 = x^5 + x^4 + 3x^3 + 5x^2 + 4x + 10$. Der affine Teil der Jacobi–Varietät wird durch die zwei Gleichungen $F_1 = 0$ und $F_2 = 0$ beschrieben, für die Maple mit „solve“ Lösungen ermittelt: $(z_1, g_1(z_1, z_3), z_3, g_2(z_1, z_3))$. Ich verzichte an dieser Stelle auf die umfangreiche Angabe der Funktionen g_1 und g_2, wähle drei Punkte aus und addiere nach der Additionsformel:

$$
\begin{aligned}
P &\approx (1, -3.3247 + 0.8230i, 7, -14.6788 + 0.0699i),\\
Q &\approx (3 + 4i, -1.3314 - 3.9518i, 4, -42.6422 + 14.2087i),\\
R &\approx (3, 1.8884 + 0.2053i, i, -9.8482 + 4.0479i),
\end{aligned}
$$

$$
\begin{aligned}
P + Q &\approx (-0.3548 + 0.5320i, -0.0163 - 0.5232i, 0.7000 + 0.4320i, -2.0766 + 0.3004i),\\
Q + R &\approx (36.8577 - 12.0651i, 230.2701 - 90.5583i,\\
&\qquad 2068.4731 - 1135.1747i, 23977.1102 - 17475.5238i),\\
P + R &\approx (40.8802 - 0.5445i, 265.1202 - 3.4745i,\\
&\qquad 2553.0837 - 46.0243i, 32796.9996 - 734.4269i),\\
P + (Q + R) &= (P + Q) + R = (P + R) + Q\\
&\approx (0.6101 + 3.5381i, 1.7006 - 5.8211i, -15.7600 + 10.5314i, 70.2406 + 1.4194i),
\end{aligned}
$$

$$
\begin{aligned}
\neg Q &\approx (3 + 4i, 1.3314 + 3.9518i, 4, 42.6422 - 14.2087i),\\
P + (P + Q) &\approx (2.1039 + 0.1651i, 0.0984 + 1.5686i, 3.1503 + 0.8551i, -0.7938 + 10.3926i),\\
P + P &\approx (-1.0578 - 2.0344i, 4.7858 + 0.0791i, -5.9549 + 11.1474i, -21.0041 - 36.2258i).
\end{aligned}
$$

6 Kryptographische Anwendungen

Im Zuge des weltweiten Datenaustausches werden Verfahren benötigt, welche die Sicherheit beim Transfer von Daten gewährleisten. Ich möchte zwei bekannte Public–Key Kryptosysteme vorstellen, die sich auch auf Jacobischen Varietäten nutzen lassen: das Diffie–Hellman Schlüssel–Austausch Verfahren und das System von ElGamal.

6.1 Kryptosysteme

Für das **Diffie–Hellman Schlüssel–Austausch Verfahren** wird eine Gruppe G mit einem erzeugenden Element $g \in G$ vereinbart. G und g werden veröffentlicht.

Alice und Bob möchten über einen öffentlichen Kanal kommunizieren, so daß Catherine Nachrichten nicht entziffern kann. Für den geheimen Schlüssel wählt Alice zufällig $k_A \in \mathbb{N}$, berechnet $g^{k_A} \in G$ und sendet g^{k_A} an Bob. Analog wählt Bob zufällig eine natürliche Zahl k_B, berechnet daraus $g^{k_B} \in G$ und sendet g^{k_B} an Alice. Der gemeinsame geheime Schlüssel ist $h = g^{k_A k_B}$. Bob berechnet h aus $(g^{k_A})^{k_B}$ und Alice aus $(g^{k_B})^{k_A}$. Catherine muß h aus g^{k_A}, g^{k_B} und g bestimmen, um in den Besitz des geheimen Schlüssels zu gelangen.

Dieses Verfahren läßt sich zum **ElGamal–System** modifizieren. Eine Nachricht wird auf eine vereinbarte Weise als Gruppenelement dargestellt: sei $N \in G$ die Nachricht. Alice und Bob besitzen wie oben g^{k_A} und g^{k_B}. Bob wählt zufällig eine ganze Zahl l und sendet Alice das Paar $(g^l, N(g^{k_A})^l)$. Zum Entschlüsseln potenziert Alice die erste Komponente des Paares mit ihrem geheimen k_A, multipliziert das Inverse dieses Resultat zu der zweiten Komponente und kann so die verschlüsselte Nachricht lesen: $N = N(g^{k_A})^l((g^l)^{k_A})^{-1}$.

Beide Verfahren lassen sich brechen, wenn sich das Diskrete Logarithmus Problem lösen läßt, nämlich aus g und g^l das l zu bestimmen.

Definition 13
Das **Diskrete Logarithmus Problem** der Gruppe G zur Basis $g \in G$ ist das Problem, zu gegebenem $y \in G$ ein ganzzahliges l zu finden, so daß

$$g^l = y$$

gilt, falls ein solches l existiert.

Um die kryptographische Sicherheit dieser Systeme zu garantieren, sind Gruppen gefragt, in denen eine diskrete Exponentation schnell durchgeführt werden kann, in denen aber das Diskrete Logarithmus Problem nur schwer zu lösen ist.

Wird etwa die multiplikative Gruppe eines endlichen Körpers $\mathbb{F}_q$, $q = p^r$, p prim, $r \in \mathbb{N} - \{0\}$, genutzt, so muß die Ordnung des Körpers bei der gegenwärtigen Computer–Technik mindestins 1024 Bit betragen, da bei dieser Größenordnung die derzeitigen Mittel nicht ausreichen, das Logarithmus Problem in akzeptabler Zeit zu lösen.

Wird dagegen die Jacobi–Varietät einer hyperelliptischen Kurve vom Geschlecht g über einem endlichen Körper $\mathbb{F}_q$ als Ausgangsgruppe genutzt, so hat diese größenordnungsmäßig q^g Elemente, so daß es ausreicht, mit kleineren Körpern zu rechnen. Damit das Diskrete Logarithmus Problem hier schwierig ist, muß gewährleistet sein, daß die Gruppenordnung durch einen großen Primfaktor teilbar ist.

Für kryptographische Anwendungen sind also Additionsformeln für Jacobische Varietäten über endlichen Körpern von Interesse.

6.2 Arithmetik auf Jacobi–Varietäten über endlichen Körpern

Definition 14
Sei $\mathbb{F}_q$ ein endlicher Körper, $q = p^r$, p prim, $r \in \mathbb{N} - \{0\}$, und sei $\overline{\mathbb{F}}_q$ der algebraische Abschluß von $\mathbb{F}_q$. Eine **hyperelliptische Kurve** C **vom Geschlecht** g **über** $\mathbb{F}_q$ ist durch die Gleichung

$$C : y^2 + h(x)y = f(x) \tag{48}$$

gegeben, wobei $g \in \mathbb{N} - \{0\}$, $h(x) \in \mathbb{F}_q[x]$ ein Polynom vom Grad $\leq g$ und $f(x) \in \mathbb{F}_q[x]$ ein normiertes Polynom vom Grad $2g + 1$ ist und keine Lösungen $(x, y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ existieren, die gleichzeitig (48), $2y + h(x) = 0$ und $h'(x)\, y - f'(x) = 0$ lösen.

Die Menge der $\mathbb{F}_q$**–rationalen Punkte auf** C ist die Menge aller Punkte $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$, die (48) erfüllen, zuzüglich ∞.

Hat der endliche Körper $\mathbb{F}_q$ eine von 2 verschiedene Charakteristik, so läßt sich die Kurvengleichung (48) durch die Koordinatentransformation $x \longmapsto x$, $y \longmapsto \left(y - \frac{h(x)}{2}\right)$ auf die Form $C : y^2 = f(x)$ bringen. Andererseits impliziert $h(x) \equiv 0$ eine von 2 verschiedene Charakteristik, so daß für $p \neq 2$ die Definitionen 1 und 14 identisch sind. Für Geschlecht 1 sind darüber hinaus bei Charakteristik 3 Änderungen in der Definition der elliptischen Kurve vorzunehmen.

Ich beschränke mich auf einen endlichen Körper $\mathbb{F}_q$ mit $q = p^r$, $p \neq 2, 3$ und $r \in \mathbb{N} - \{0\}$. Die Additionsformeln, die durch Betrachtungen über dem Körper der komplexen Zahlen in rationalen Ausdrücken mündeten, sind auch auf einem endlichen Körper $\mathbb{F}_q$ sinnvoll. Explizit gebe ich die Formeln für $g = 1$ und $g = 2$, samt Beispielen, an.

Additionsformeln für elliptische Kurven

Sei $C : y^2 = x^3+ax+b$ eine elliptische Kurve über $\mathbb{F}_q$ und seien (x_1, y_1), (x_2, y_2) zwei verschiedene $\mathbb{F}_q$–rationale Punkte auf C. Sei (x_3, y_3) das Ergebnis der Addition von (x_1, y_1) und (x_2, y_2) und sei (x_4, y_4) das Ergebnis der Verdopplung von (x_1, y_1). Dann gilt

$$x_3 = -x_1 - x_2 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2,$$

$$y_3 = -y_1 + \frac{y_1 - y_2}{(x_1 - x_2)^2}(3x_1^2 + a) - 2\frac{(y_1 - y_2)^2}{(x_1 - x_2)^3}y_1,$$

$$x_4 = -2x_1 + \frac{1}{4}\left(\frac{3x_1^2 + a}{y_1}\right)^2,$$

$$y_4 = -y_1 + \frac{3}{2}\frac{x_1}{y_1}\left(3x_1^2 + a\right) - \frac{1}{8}\left(\frac{3x_1^2 + a}{y_1}\right)^3.$$

Beispiel 22
Betrachte über $\mathbb{F}_7$ die elliptische Kurve $C\,:\; y^2 = x^3 - x$. $\mathbb{F}_7$–rationale Punkte auf C lassen sich schnell berechnen, indem alle 49 Elemente in $\mathbb{F}_7 \times \mathbb{F}_7$ auf Erfüllung der Kurvengleichung C getestet werden, zuzüglich ∞. Mit obigen Formeln läßt sich die Verknüpfungstabelle ausfüllen:

	$(0,0)$	$(1,0)$	$(4,2)$	$\neg(4,2) = (4,5)$	$(5,1)$	$\neg(5,1) = (5,6)$	$(6,0)$	∞
$(0,0)$	∞	$(6,0)$	$(5,1)$	$(5,6)$	$(4,2)$	$(4,5)$	$(1,0)$	$(0,0)$
$(1,0)$	$(6,0)$	∞	$(4,5)$	$(4,2)$	$(5,6)$	$(5,1)$	$(0,0)$	$(1,0)$
$(4,2)$	$(5,1)$	$(4,5)$	$(1,0)$	∞	$(6,0)$	$(0,0)$	$(5,6)$	$(4,2)$
$(4,5)$	$(5,6)$	$(4,2)$	∞	$(1,0)$	$(0,0)$	$(6,0)$	$(5,1)$	$(4,5)$
$(5,1)$	$(4,2)$	$(5,6)$	$(6,0)$	$(0,0)$	$(1,0)$	∞	$(4,5)$	$(5,1)$
$(5,6)$	$(4,5)$	$(5,1)$	$(0,0)$	$(6,0)$	∞	$(1,0)$	$(4,2)$	$(5,6)$
$(6,0)$	$(1,0)$	$(0,0)$	$(5,6)$	$(5,1)$	$(4,5)$	$(4,2)$	∞	$(6,0)$
∞	$(0,0)$	$(1,0)$	$(4,2)$	$(4,5)$	$(5,1)$	$(5,6)$	$(6,0)$	∞

Additionsformeln für Jacobische Varietäten bei Geschlecht 2

Sei $C\,:\; y^2 = x^5 + f_1x^4 + f_2x^3 + f_3x^2 + f_4x + f_5$ eine hyperelliptische Kurve vom Geschlecht 2, die zunächst über $\mathbb{C}$ betrachtet wird. $Jac\, C - \Theta$ läßt sich nach Satz 19 durch 2 Gleichungen charakterisieren, so daß gilt:
Ein beliebiger Punkt $(z_0, z_1, z_2, z_3) \in \mathbb{C}^4$ ist genau dann $\in Jac\, C - \Theta$, wenn gilt:

$$(z_0, z_1, z_2, z_3) \in Jac\, C - \Theta \iff F_1(z_0, z_1, z_2, z_3) = 0 \text{ und } F_2(z_0, z_1, z_2, z_3) = 0.$$

Nach Satz 23 gelten folgende Additionsformeln für $x, u, x+u \in \mathbb{C}^2/\Gamma - V(\vartheta[\delta])/\Gamma$:

$$\begin{aligned}\wp(x+u) = {} & \frac{1}{2}\wp(x) + \frac{1}{2}\wp(u) \\ & - (\mathrm{D}^x + \mathrm{D}^u)^2 \Big(\log\big((\wp(u) - \wp(x))^3 \\ & \qquad + 2\left(\wp'(u)^2 - \wp'(x)^2\right) + 2\left(\wp(x) - \wp(u)\right)(\wp''(x) + \wp''(u))\big)\Big),\end{aligned}$$

zuzüglich der Formeln für $\wp'(x+u), \wp''(x+u), \wp'''(x+u)$.

Die Addition auf $JacC$ induziert also auf $JacC - \Theta$ eine Verknüpfung, die assoziativ und kommutativ ist und „fast nie“ aus $Jac\, C - \Theta$ hinaus führt. Beispielsweise erzeugt ein zufällig gewähltes Element eine Untergruppe, deren einziges zu Θ gehöriges Element der Nullpunkt ist. Für kryptographische Anwendungen reicht also die Kenntnis von Additions– und Verdopplungsformeln auf $Jac\, C - \Theta$, wobei ich mich hinsichtlich der Verdopplung des Tricks $2P = (P + (P+Q)) + \neg Q$ bediene. Die rationalen Ausdrücke, die hierfür in Satz 23 entwickelt wurden, sind wiederum auch für endliche Körper sinnvoll, wobei bei der Charakteristik darauf zu achten ist, daß keine Nenner verschwinden. Es ergibt sich also eine partielle Gruppenstruktur auf der Menge

$$\{(x_0, x_1, x_2, x_3) \in \mathbb{F}_q^4 \mid F_1(x_0, x_1, x_2, x_3) = 0,\ F_2(x_0, x_1, x_2, x_3) = 0\}$$

Außerdem ist $(x_0, -x_1, x_2, -x_3)$ das Inverse zu (x_0, x_1, x_2, x_3).

Beispiel 23
Sei über $\mathbb{F}_7$ die hyperelliptische Kurve $C : y^2 = x^5 + 2x^3 + 5x^2 + 6x + 3$ vom Geschlecht 2 gegeben. Die $JacC - \Theta$ entsprechenden Punkte von $\mathbb{F}_7$ lassen sich mit einem Computer berechnen, indem alle 7^4 Elemente auf Erfüllung der Gleichungen $F_1(z_0, z_1, z_1, z_1) = 0$ und $F_2(z_0, z_1, z_2, z_3) = 0$, nach Beispiel 19, durchsucht werden, zuzüglich ∞:

$$\begin{aligned}
&P_1 = (0,0,4,2), \neg P_1 = (0,0,4,5), P_2 = (6,1,2,1), \neg P_2 = (6,6,2,6),\\
&P_3 = (0,2,0,3), \neg P_3 = (0,5,0,4), P_4 = (3,3,6,5), \neg P_4 = (3,4,6,2),\\
&P_5 = (1,1,3,3), \neg P_5 = (1,6,3,4), P_6 = (4,2,3,4), \neg P_6 = (4,5,3,3),\\
&P_7 = (2,0,4,3), \neg P_7 = (2,0,4,4), P_8 = (0,6,6,4), \neg P_8 = (0,1,6,3),\\
&P_9 = (1,2,0,3), \neg P_9 = (1,5,0,4), \infty.
\end{aligned}$$

Die Numerierung der Punkte habe ich so gewählt, da sich durch eine Implementation obiger Additionsformeln mit Hilfe eines Rechners zeigt, daß P_1 eine zyklische Gruppe erzeugt, wobei ich in diesem Beispiel das Glück habe, daß außer ∞ keine weiteren Punkte aus Θ vorkommen:

$$\begin{aligned}
2 \cdot P_1 &= P_2,\\
3 \cdot P_1 &= P_3,\\
4 \cdot P_1 &= P_4,\\
5 \cdot P_1 &= P_5,\\
6 \cdot P_1 &= P_6,\\
7 \cdot P_1 &= P_7,\\
8 \cdot P_1 &= P_8,\\
9 \cdot P_1 &= P_9,\\
10 \cdot P_1 &= \neg P_9,\\
11 \cdot P_1 &= \neg P_8,\\
12 \cdot P_1 &= \neg P_7,\\
13 \cdot P_1 &= \neg P_6,\\
14 \cdot P_1 &= \neg P_5,\\
15 \cdot P_1 &= \neg P_4,\\
16 \cdot P_1 &= \neg P_3,\\
17 \cdot P_1 &= \neg P_2,\\
18 \cdot P_1 &= \neg P_1,\\
19 \cdot P_1 &= \infty.
\end{aligned}$$

□

Literatur

[Brieskorn, Knörrer] Egbert Brieskorn und Horst Knörrer. *Ebene algebraische Kurven*. Birkhäuser, Boston, 1981.

[Bost] Jean-Benoït Bost. *Introduction to Compact Riemann Surfaces, Jacobians, and Abelian Varieties*. In Michel Waldschmidt, Hrsg., *From Number Theory to Physics*, Springer, Berlin, 1992, Seiten 64 – 211.

[Cantor] David Cantor. *Computing in the Jacobian of a Hyperelliptic Curve*. Mathematics of Computation Vol. 48, 1987.

[Chandrasekharan] Komaravolu Chandrasekharan. *Elliptic Functions*. Springer, Berlin, 1985.

[Fischer, Lieb] Wolfgang Fischer und Ingo Lieb. *Funktionentheorie*. Vieweg, Braunschweig, 1994.

[Fulton] William Fulton. *Algebraic Curves*. Benjamin, New York, 1969.

[Kampkötter] Wolfgang Kampkötter. *Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven*. Essen, 1991.

[Kummar Murty] V. Kummar Murty. *Introduction to Abelian Varieties*. CRM Monograph Series Vol. 3, 1993.

[Koblitz] Neal Koblitz. *Algebraic Aspects to Cryptography*. Springer, Berlin, 1998.

[Lang 1959] Serge Lang. *Abelian Varieties*. Interscience, New York, 1959.

[Lang 1978] Serge Lang. *Elliptic Curves – Diophantine Analysis*. Springer, Berlin, 1978.

[Mumford 1970] David Mumford. *Abelian Varieties*. Oxford University Press, Oxford, 1970.

[Mumford 1975] David Mumford. *Curves and their Jacobians*. University of Michigan Press, Michigan, 1975.

[Mumford 1983] David Mumford. *Tata Lectures on Theta I*. Birkhäuser, Boston, 1983.

[Mumford 1984] David Mumford. *Tata Lectures on Theta II*. Birkhäuser, Boston, 1984.

[Spallek] Anne-Monika Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public–Key–Kryptoverfahren*. Essen, 1994.

[Swinnerton-Dyer] H.P.F. Swinnerton-Dyer. *Analytic Theory of Abelian Varieties*. Cambridge University Press, Cambridge, 1974.

Index