



ulm university universität  
**uulm**

---

# **Shimura-Kurven, Endomorphismen und $q$ -Parameter**

---

Dissertation zur Erlangung des Doktorgrades Dr. rer. nat.  
der Fakultät für Mathematik und Wirtschaftswissenschaften  
der Universität Ulm

Vorgelegt von Dominik Josef Ufer aus Nagold

ULM, 2010



**Dekan:** Prof. Dr. Werner Kratz  
**Erstgutachter:** Prof. Dr. Irene I. Bouw  
**Zweitgutachter:** Prof. Dr. Werner Lütkebohmert  
**Tag der Promotion:** 20. Juli 2010



# Inhaltsverzeichnis

<b>Inhaltsverzeichnis</b>	<b>v</b>
<b>Einleitung</b>	<b>vii</b>
<b>1 Quaternionenalgebren</b>	<b>1</b>
1.1 Definitionen und Klassifikation über Zahlkörpern . . . . .	1
1.2 Einbettungen von imaginär quadratischen Körpern . . . . .	6
1.3 Automorphismen . . . . .	12
<b>2 Abelsche Flächen vom Typ <math>\mathcal{QM}</math> und Shimura-Kurven</b>	<b>15</b>
2.1 Abelsche Flächen vom Typ $\mathcal{QM}$ . . . . .	16
2.2 Arithmetische Fuchssche Gruppen . . . . .	20
2.3 Shimura-Kurve $\mathcal{X}(1)$ : Definition und Algebraisierbarkeit . . . . .	22
2.4 Abelsche Flächen vom Typ $\mathcal{QM}$ & CM . . . . .	24
2.5 Konstruktion von abelschen Flächen vom Typ $\mathcal{QM}$ & CM . . . . .	30
2.6 Reduktion modulo $p$ und Liften von Endomorphismen . . . . .	34
2.7 CM-Punkte und abelsche Flächen vom Typ $\mathcal{QM}$ & CM . . . . .	37
<b>3 Dieudonné-Moduln abelscher Varietäten</b>	<b>43</b>
3.1 Lineare gewöhnliche Differentialgleichungen über $\mathbb{C}$ . . . . .	44
3.2 Picard-Fuchs Differentialgleichung . . . . .	48
3.3 Definition von $F$ -Kristallen . . . . .	51
3.4 $F$ -Kristalle gewöhnlicher formaler abelscher Schemata . . . . .	54
3.5 Deformation gewöhnlicher abelscher Varietäten . . . . .	55
3.6 Liftbarkeit von Isogenien . . . . .	58
<b>4 Anwendung I: Abelsche Flächen vom Typ <math>\mathcal{QM}</math></b>	<b>67</b>
4.1 Beschreibung der $q$ -Parameter . . . . .	67
4.2 Beispiel: Diskriminante 6 . . . . .	72
<b>5 Anwendung II: Zyklische Überlagerungen von <math>\mathbb{P}^1</math></b>	<b>77</b>
5.1 Definition der Shimura-Kurve . . . . .	78
5.2 Beschreibung der $q$ -Parameter . . . . .	84
<b>Literaturverzeichnis</b>	<b>89</b>

**Zusammenfassung**

**95**

# Einleitung

In dieser Arbeit studieren wir arithmetische Eigenschaften von Shimura-Kurven in gemischter Charakteristik. Shimura-Kurven sind eine Verallgemeinerung der klassischen Modulkurven. Modulkurven parametrisieren Familien von elliptischen Kurven mit Zusatzstruktur. Sie sind für die Zahlentheorie und die algebraische Geometrie sehr interessante Objekte. Zum Beispiel benutzt Wiles im Beweis der Fermatschen Vermutung ([Wil95]) die Theorie der Modulkurven. Die Modulkurven besitzen eine reiche arithmetische Struktur, die sehr gut untersucht ist. Shimura-Kurven parametrisieren Familien höher-dimensionaler Objekte und besitzen ähnliche Eigenschaften wie die Modulkurven. Wir verallgemeinern in dieser Arbeit eine arithmetische Eigenschaft der Modulkurven auf Shimura-Kurven. Wir geben nämlich eine lokale Beschreibung von Shimura-Kurven in Termen von Gleichungen für den Lokus im Deformationsraum einer abelschen Varietät.

Wir geben nun eine Motivation für das Studium solcher Gleichungen und betrachten dazu den einfachsten Fall der Modulkurven. Eine wichtige Rolle in der Theorie der Modulkurven spielen die Modulformen, insbesondere die  $j$ -Funktion

$$j(\tau) := \frac{1}{q} + 744 + 196884q + 21493760q^2 + \dots,$$

für  $q := e^{i\pi\tau}$  und  $\tau \in \mathcal{H}$  in der komplexen oberen Halbebene. Die  $j$ -Funktion besitzt eine Modulinterpretation. Sie definiert einen Parameter auf der Modulkurve  $X(1)$ , welche Isomorphieklassen von elliptischen Kurven über den komplexen Zahlen  $\mathbb{C}$  parametrisiert. Diese Modulinterpretation der  $j$ -Funktion begründet, dass die  $j$ -Funktion imaginär quadratische Zahlen  $\tau \in \mathcal{H}$  auf algebraische Zahlen abbildet. Man nennt diese algebraischen Zahlen  $j(\tau)$  singuläre Moduli.

In [Zag02] definiert Zagier die verallgemeinerte Spur singulärer Moduli  $t(d) \in \mathbb{C}$  für  $d \in \mathbb{Z}_{<0}$ ,  $d \equiv 0, 1 \pmod{4}$  als gewichtete Summe über singuläre Moduli mit bestimmten Eigenschaften. Diese entsprechen elliptischen Kurven mit vorgegebenen Endomorphismen. Die verallgemeinerte Spur erfüllt interessante Kongruenzrelationen (z.B. [Jen05], [Edi05]). Edixhoven

benutzt zum Beweis der Kongruenzen in [Edi05] einen geometrischen Ansatz. Kroworsch ([Kro09]) verallgemeinert Edixhovens Ansatz auf andere Modulkurven und zeigt ähnliche Kongruenzrelationen. Es stellt sich die Frage, in welcher Allgemeinheit dieser Ansatz funktioniert. Motivation und Ziel dieser Arbeit ist es zu zeigen, dass sich dieser Ansatz in den Kontext von Shimura-Kurven übertragen lässt.

Ein wichtiger Schritt im Beweis der Kongruenzen mittels dem geometrischen Ansatz in [Edi05] und [Kro09] ist es, statt einer Modulkurve die korrespondierende Familie von elliptischen Kurven mit Stufenstruktur zu betrachten. Indem man die Reduktion modulo  $p$  der zugehörigen elliptischen Kurven mit Zusatzstruktur betrachtet, bekommt die Menge der singulären Moduli eine geometrische,  $p$ -adische Struktur.

Diese geometrische Struktur leitet sich aus folgendem Problem der Deformationstheorie ab. Man betrachtet für eine gegebene gewöhnliche elliptische Kurve  $\bar{E}$  in positiver Charakteristik  $p$  die Menge der Lifts von  $\bar{E}$  nach Charakteristik 0. Die Methode ist zunächst nur für den gewöhnlichen Fall ausgearbeitet. Es ist bekannt, dass diese Menge eine geometrische Struktur besitzt und dass die Geometrie durch eine Koordinate, den sogenannten  $q$ -Parameter, beschrieben wird. Das Problem ist nun die Teilmenge der Lifts mit vorgegebenen Endomorphismen durch Gleichungen in  $q$  zu beschreiben.

Wir stellen nun die Fragen und Ergebnisse dieser Arbeit vor. In dieser Arbeit geben wir die benötigten Hilfsmittel zur Lösung analoger Probleme für allgemeinere Shimura-Kurven. Dabei verfolgen wir das Ziel, die geometrischen Grundlagen für die Verallgemeinerung der Kongruenzrelationen in [Kro09] auf Shimura-Kurven zu liefern. Wir beschränken uns auf den Fall einer Shimura-Kurve  $\mathcal{X}$  vom Typ PEL. Diese hat die Eigenschaft, dass sie hauptpolarisierte abelsche Varietäten  $A$  mit einer Einbettung  $\mathcal{O} \hookrightarrow \text{End}(A)$  einer festen Ordnung  $\mathcal{O}$  in den Endomorphismenring parametrisiert. Abelsche Varietäten sind eine Verallgemeinerung der elliptischen Kurven. Über  $\mathbb{C}$  entsprechen ihnen komplexe Tori. Die Ordnung  $\mathcal{O}$  in der Definition der Shimura-Kurve  $\mathcal{X}$  ist dabei so gewählt, dass die parametrisierte Familie eindimensional ist.

Es gibt auch für höherdimensionale gewöhnliche abelsche Varietäten  $\bar{A}$  eine explizite Deformationstheorie. Der Deformationsraum einer gewöhnlichen abelschen Varietät von höherer Dimension ist nicht mehr eindimensional, genauer existieren mehrere Koordinaten auf dem Deformationsraum. Man nennt diese Koordinaten  $q$ -Parameter. Angenommen, eine gewöhnliche abelsche Varietät  $\bar{A}$  ist die Reduktion eines Punktes auf der Shimura-Kurve  $\mathcal{X}$ , dann definiert die Shimura-Kurve einen eindimensionalen Unterraum des Deformationsraums. Um eine Analogie mit dem Fall

von Modulkurven herstellen zu können, muss man also eine explizite Koordinate  $t$  im Deformationsraum finden, welche diesen eindimensionalen Unterraum parametrisiert. Dies entspricht einem analogen Deformationsproblem wie im Fall der Modulkurven. Man betrachtet nämlich die Lifts  $A$  von  $\bar{A}$ , für die  $\mathcal{O} \subset \text{End}(A)$  gilt. So bekommt man Gleichungen für die  $q$ -Parameter. Diese geben im geeigneten Sinn eine lokale Beschreibung der Shimura-Kurve  $\mathcal{X}$  und liefern den Parameter  $t$ .

Auf der Shimura-Kurve  $\mathcal{X}$  existiert eine Menge von speziellen isolierten Punkten, die CM-Punkte. Sie gehören zu abelschen Varietäten, deren Endomorphismenalgebra  $\text{End}(A) \otimes \mathbb{Q} \not\cong \mathcal{O} \otimes \mathbb{Q}$  maximale Dimension hat. Die CM-Punkte auf der Shimura-Kurve verallgemeinern die singulären Moduli. Somit kann man analog zum Fall der Modulkurve die  $p$ -adische Geometrie der CM-Punkte im Deformationsraum von  $\bar{A}$  beschreiben, in dem man wiederum ein Deformationsproblem in der Koordinate  $t$  betrachtet.

Wir betrachten in dieser Arbeit zur Demonstration der Methoden zwei Spezialfälle. Zum einen den Fall, dass die Ordnung  $\mathcal{O}$  aus der Definition der Shimura-Kurve  $\mathcal{X}$  zu einer indefiniten Quaternionenalgebra über  $\mathbb{Q}$  gehört, zum anderen den Fall, dass  $\mathcal{X}$  zyklische Überlagerungen von  $\mathbb{P}^1$  parametrisiert.

Der zentrale Fall in dieser Arbeit ist der, für den  $\mathcal{O} := \mathcal{O}_D$  eine maximale Ordnung in einer indefiniten Quaternionenalgebra  $D$  über  $\mathbb{Q}$  ist. D. h. wir betrachten die Shimura-Kurve  $\mathcal{X}(1) := \mathcal{X}$ , welche abelsche Flächen  $A$  mit einer Einbettung  $\mathcal{O}_D \hookrightarrow \text{End}(A)$  parametrisiert. Wir nennen diese abelschen Flächen  $A$  kurz vom Typ  $\mathcal{QM}$ .

In Kapitel 1 wird zuerst die benötigte Ringtheorie für Quaternionenalgebren studiert. In Kapitel 2 wird diskutiert, was die Struktur der Quaternionenalgebra über die Geometrie der abelschen Flächen vom Typ  $\mathcal{QM}$  aussagt. So korrespondiert die Einbettung eines imaginär quadratischen Körpers  $K$  in die Quaternionenalgebra  $D$  einem CM-Punkt. Dieser wiederum korrespondiert zu einer abelschen Fläche  $A$  vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation. Aus den Struktursätzen über Endomorphismenalgebren von abelschen Varietäten folgt, dass  $A$  isogen zum Produkt zweier isogener elliptischer Kurven  $E, E'$  ist.

In [Mor09] gibt Mori eine Idee, wie man über den komplexen Zahlen  $\mathbb{C}$  eine Isogenie  $A \rightarrow E \times E'$  konstruieren kann. Wir folgen dieser Idee und arbeiten sie für abelsche Flächen über Zahlkörper  $F$  vollständig und explizit aus. In unserer Formulierung kann man diese Konstruktion auch auf positive Charakteristik übertragen.

#### **2.4.12 Theorem (und Prop. 2.4.15).**

*Sei  $A$  eine abelsche Fläche vom Typ  $\mathcal{QM}$  über einem Zahlkörper  $F$  mit komplexer Multiplikation. D.h. es gelte  $\text{End}^0(A) \simeq M_2(K)$  für einen imaginär*

quadratischen Körper  $K$  und  $\text{Zentrum}(\text{End}(A)) \simeq \mathcal{O}_{K,c}$  für eine Ordnung  $\mathcal{O}_{K,c} \subset K$  mit Führer  $c \in \mathbb{N}$  in  $K$ .

Dann existieren isogene elliptische Kurven  $E, E'$  mit

$$\text{End}(E) \simeq \text{End}(E') \simeq \mathcal{O}_{K,c}$$

und eine Isogenie

$$\psi_{e\eta} : A \rightarrow E_e \times E_{\bar{e}}$$

mit  $\deg \psi_{e\eta} \mid (4c^2 \cdot \text{disc}(K))$ .

Somit können wir als Korollar die Deformationsräume von  $A$  und von  $E$  in Verbindung bringen. Dies könnte zum Beispiel interessant sein, um explizit abelsche Varietäten vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation zu konstruieren oder um Gleichungen für Shimura-Kurven zu finden.

Als zweites Thema beschäftigen wir uns mit der Deformationstheorie von gewöhnlichen abelschen Varietäten. Wir formulieren diese in Termen der de-Rham-Kohomologie. Es gibt auch alternative Beschreibungen, zum Beispiel in Termen der  $p$ -divisiblen Gruppen wie z.B. in [Kro09]. Die de-Rham-Kohomologie ist für unsere Zwecke gut geeignet, da sie möglicherweise Verallgemeinerungen auf Shimura-Kurven erlauben, die nicht vom Typ PEL sind. Zudem ist die de-Rham-Kohomologie für explizite Berechnungen geeignet.

In Kapitel 3 fassen wir dann allgemeine Ergebnisse aus der Theorie der Dieudonné-Moduln und der Deformationstheorie von gewöhnlichen abelschen Varietäten benutzerfreundlich zusammen. Wir verstehen die de-Rham-Kohomologie als Realisierung eines Dieudonné-Moduls. Es ist bekannt ([Del81]), dass man mittels der de-Rham-Kohomologie auf dem Deformationsraum einer abelschen Varietät Koordinaten konstruieren kann, die  $q$ -Parameter. Wir benutzen ein Theorem von Messing ([Mes72]), um eine notwendige und hinreichende Liftbarkeitsbedingung für Endomorphismen an die  $q$ -Parameter herzuleiten (Korollar 3.6.16). Diese entspricht der Liftbarkeitsbedingung an den Serre-Tate-Parameter aus der Deformationstheorie von  $p$ -divisiblen Gruppen ([Kat81, Thm. 2.1]). Dies spiegelt wieder, dass die Gruppenstruktur dieser Parameter übereinstimmt (Appendix zu [Del81]).

In den Kapiteln 4 und 5 gehen wir nun auf unsere beiden Spezialfälle von Shimura-Kurven ein.

In Kapitel 4 betrachten wir den Deformationsraum einer gewöhnlichen abelschen Fläche  $\bar{A}$  vom Typ  $\mathcal{QM}$  über einem endlichen Körper. Wir berechnen Gleichungen für den Locus  $V$  der Lifts von  $\bar{A}$ , die ebenfalls vom Typ  $\mathcal{QM}$  sind (Theorem 4.1.6). Dies entspricht einer lokalen Beschreibung

der Shimura-Kurve. Mori leitet in [Mor09] mittels anderer Methoden in dieser Situation ähnliche Gleichungen für den Serre-Tate-Parameter her. In Proposition 4.1.8 benutzen wir Theorem 4.1.6, um darüber hinaus Koordinaten für Lifts von  $\bar{A}$  vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation zu finden. Dies stellt einen wichtigen Schritt im Beweis von Kongruenzen für verallgemeinerte Spuren dar.

Schließlich beschäftigen wir uns in Kapitel 5 mit unserem zweiten Spezialfall, nämlich Shimura-Kurven die Isomorphieklassen zyklischer Überlagerungen von  $\mathbb{P}^1$  parametrisieren. Wir leiten für diese Shimura-Kurven analoge Gleichungen her. Dies zeigt, dass die Methoden auch auf andere Shimura-Kurven anwendbar sind, die nicht zu indefiniten Quaternionenalgebren über  $\mathbb{Q}$  gehören.



# Kapitel 1

## Quaternionenalgebren

In den Kapitel 2 und 4 studieren wir eine bestimmte Klasse von Shimura-Kurven, nämlich Shimura-Kurven, die Familien von abelschen Flächen vom Typ  $\mathcal{QM}$  parametrisieren. Damit meinen wir, dass die Punkte einer Shimura-Kurve  $\mathcal{X}$  zu abelschen Fläche korrespondieren, deren Endomorphismenalgebren eine feste Quaternionenalgebra  $D$  enthalten. Die Struktur der Quaternionenalgebra  $D$  spielt eine wichtige Rolle in dem Studium der Shimura-Kurve  $\mathcal{X}$ . So kann man mittels einer Automorphismengruppe von  $D$  eine Fuchssche Gruppe  $\Gamma$  definieren. Diese liefert eine alternative Definition der Shimura-Kurve  $\mathcal{X}$  (über  $\mathbb{C}$ ) als Quotient  $\mathcal{H}/\Gamma$  der komplexen oberen Halbebene  $\mathcal{H}$  nach  $\Gamma$ . Über dies interessieren wir uns für spezielle Punkte auf  $\mathcal{X}$ , die CM-Punkte. Diese korrespondieren zu Einbettungen von imaginär quadratischen Körpern in  $D$ .

In diesem Kapitel fassen wir Standardergebnisse über Quaternionenalgebren zusammen. In Abschnitt 1.1 geben wir die grundlegende Definitionen für Quaternionenalgebren und zitieren den Satz 1.1.6 über die Klassifikation von Quaternionenalgebren über Zahlkörpern. In Abschnitt 1.2 benutzen wir dies um die Einbettungen von Körpern in eine Quaternionenalgebra zu studieren. In Abschnitt 1.3 definieren und untersuchen wir zwei spezielle Automorphismengruppen von  $D$ , welche in der Definition der Shimura-Kurve  $\mathcal{X}(1)$  (Definition 2.3.2) eine wichtige Rolle spielen.

Als Referenzen für dieses Kapitel dienen die Bücher [AB04], [Vig80] und für den Abschnitt über Idempotenten der Artikel [Mor09].

### 1.1 Definitionen und Klassifikation über Zahlkörpern

In diesem Abschnitt geben wir zunächst die Definition einer Quaternionenalgebra (Definition 1.1.1) und klassifizieren jene über lokalen Körpern (Be-

merkung 1.1.3) und Zahlkörper (Satz 1.1.6). Dann zitieren wir eine äquivalente, explizite Definition einer Quaternionenalgebra als Vektorraum mittels einer Basis (Proposition 1.1.9). Mit Hilfe dieser expliziten Darstellung können wir eine eindeutige Involution auf der Quaternionenalgebra  $D$  definieren, die Konjugation (Proposition 1.1.14). Desweiteren studieren wir positive Involutionen (Definition 1.1.17). Schließlich geben wir die Definition einer Ordnung (Definition 1.1.23).

**1.1.1 Definition.** Eine *Quaternionenalgebra*  $D$  über einem Körper  $F$  ist eine einfache zentrale  $F$ -Algebra von Dimension 4.

Ein Beispiel für eine Quaternionenalgebra über einem beliebigen Körper  $F$  ist die Matrixalgebra  $M_2(F)$ .

**1.1.2 Definition.** Eine Quaternionenalgebra  $D$  über  $F$  nennt man *unverzweigt*, falls  $D \simeq M_2(F)$  ist. Ansonsten nennt man  $D$  *verzweigt*.

Wir wollen die Quaternionenalgebren über Zahlkörpern klassifizieren. Dazu betrachten wir zunächst den lokalen Fall. Wir nennen dabei einen Körper *lokal* falls er vollständig bezüglich einer diskreten Bewertung ist und endlichen Restklassenkörper besitzt.

**1.1.3 Bemerkung.** Über endlichen und algebraisch abgeschlossenen Körpern (insbesondere  $\mathbb{C}$ ) ist jede Quaternionenalgebra unverzweigt. Über lokalen Körpern und  $\mathbb{R}$  gibt es bis auf Isomorphie genau eine verzweigte Quaternionenalgebra. Im Fall der reellen Zahlen  $\mathbb{R}$  ist dies die Algebra der Hamiltonschen Quaternionen.

**1.1.4 Definition.** Sei  $F$  ein Zahlkörper und sei  $v$  eine Primstelle von  $F$ . Wir nennen die Quaternionenalgebra  $D$  *verzweigt* bei  $v$ , falls die Quaternionenalgebra  $D \otimes_F F_v$  über der Vervollständigung  $F_v$  verzweigt ist. Andernfalls, also wenn  $D \otimes F_v \simeq M_2(F_v)$  ist, nennen wir  $D$  *unverzweigt* bei  $v$ . Ist  $D$  verzweigt an allen reellen Primstellen, so nennt man  $D$  *definit*. Ansonsten nennt man  $D$  *indefinit*. Ist  $D$  an allen reellen Primstellen unverzweigt, so nennt man  $D$  *total indefinit*.

**1.1.5 Beispiel.** Im Fall  $F = \mathbb{Q}$  ist die Indefinitheit einer Quaternionenalgebra  $D/\mathbb{Q}$  äquivalent zur Aussage  $D \otimes \mathbb{R} \simeq M_2(\mathbb{R})$ .

Mittels Definition 1.1.4 können wir den Satz 1.1.6 zur Klassifikation der Quaternionenalgebren formulieren:

**1.1.6 Satz ( [Vig80, Thm. III.3.1] ).** Für einen Zahlkörper  $F$  gilt:

- (i) Jede Quaternionenalgebra über  $F$  ist nur in einer endlichen, geraden Anzahl von endlichen oder reellen Primstellen verzweigt. Die Quaternionenalgebra ist durch die Menge  $\Sigma$  dieser Primstellen (bis auf Isomorphie) eindeutig bestimmt.

(ii) Umgekehrt gibt es zu jeder endlichen Menge gerader Mächtigkeit von endlichen oder reellen Primstellen  $\Sigma$  von  $F$  eine Quaternionenalgebra über  $F$  verzweigt genau in  $\Sigma$ .

**1.1.7 Definition.** Sei  $D$  eine Quaternionenalgebra über  $\mathbb{Q}$ . Wir nennen das Produkt der verzweigten Primideale von  $D$  die *reduzierte Diskriminante* von  $D$  (Schreibweise:  $\text{disc}(D)$ ).

**1.1.8 Korollar.** Zu jeder natürlichen quadratfreien Zahl  $d \in \mathbb{N}$  existiert (bis auf Isomorphie) genau eine Quaternionenalgebra  $D$  über  $\mathbb{Q}$  mit  $\text{disc}(D) = d$ . Umgekehrt sind zwei Quaternionenalgebren über  $\mathbb{Q}$  genau dann isomorph, wenn sie die gleiche reduzierte Diskriminante haben. Somit liefert die Abbildung  $D \mapsto \text{disc}(D)$  einen Isomorphismus

$$\left\{ \begin{array}{l} \text{Isomorphieklassen von} \\ \text{Quaternionenalgebren} \\ \text{über } \mathbb{Q} \end{array} \right\} \xrightarrow{\sim} \{d \in \mathbb{N} : d \text{ quadratfrei}\}.$$

Mittels dieser Isomorphie ist  $D$  genau dann indefinit, wenn  $\text{disc}(D)$  ein Produkt von einer geraden Anzahl von Primzahlen ist.

BEWEIS. Die Aussagen folgen direkt aus der Definition der reduzierten Diskriminante und der Klassifikation der Quaternionenalgebren in Satz 1.1.6.  $\square$

Folgender Satz liefert eine explizite Darstellung einer Quaternionenalgebra als  $F$ -Algebra. Sie ist eine erste Version von Satz 1.2.4.

**1.1.9 Proposition ( [AB04, Bemerkung nach Def. 1.1.1] ).**

Sei ein Körper  $F$  der Charakteristik  $\text{char}(F) \neq 2$  und eine Quaternionenalgebra  $D/F$  gegeben. Dann existieren  $a, b \in F^*$  und eine Basis  $B = \{1, i, j, ij\}$  von  $D$  über  $F$ , so dass

$$i^2 = a, \quad j^2 = b, \quad ij = -ji$$

gilt.

Umgekehrt liefert jede  $F$ -Algebra mit einer solchen Basis  $B$  eine Quaternionenalgebra über  $F$ . Wir bezeichnen diese mit  $\left(\frac{a,b}{F}\right)$ .

**1.1.10 Bemerkung.**

- (i) Die Basis  $B$  und das Zahlenpaar  $(a, b)$  in Proposition 1.1.9 sind nicht eindeutig.
- (ii) Man kann die reduzierte Diskriminante von  $D := \left(\frac{a,b}{\mathbb{Q}}\right)$  mit Hilfe des Hilbert-Symbols elementar berechnen. Für die Definition und Eigenschaften des Hilbert-Symbols sei auf [Ser77, Chap. III] verwiesen.

Man zeigt ([Vig80, Cor. II.1.2]), dass für das Hilbert-Symbol genau dann  $(a, b)_p = -1$  gilt, wenn  $D$  bei  $p$  verzweigt ist.

Eine Liste von Repräsentanten  $D := \left(\frac{a, b}{\mathbb{Q}}\right)$  der Isomorphieklassen von Quaternionenalgebren über  $\mathbb{Q}$  mit Diskriminante  $\text{disc}(D) = pq$  für beliebige Primzahlen  $p, q \in \mathbb{N}$  findet man in [AB04, Prop. 1.25].

**1.1.11 Beispiel.** Eine Basis  $B$  wie in Prop. 1.1.9 ist für die Matrixalgebra  $M_2(F) = \left(\frac{1, -1}{F}\right)$  gegeben durch

$$i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

**1.1.12 Beispiel.** Betrachtet man die reduzierte Diskriminante  $(6) \subset \mathbb{Z}$ , dann gibt es wegen der Klassifikation bis auf Isomorphie nur eine Quaternionenalgebra über  $\mathbb{Q}$  mit dieser Diskriminante, nämlich  $\left(\frac{2, -3}{\mathbb{Q}}\right)$ .

Nun betrachten wir spezielle Anti-Automorphismen auf  $D$ , die Involutionsen. Vor allem die positiven Involutionsen sind interessant, weil auf dem Endomorphismenring einer polarisierten abelschen Varietät durch die Polarisation eine eindeutige positive Involution definiert wird.

**1.1.13 Definition.** Sei  $D$  eine Quaternionenalgebra über  $F$ . Eine *Involution* auf  $D$  ist ein Anti-Automorphismus

$$D \rightarrow D, h \mapsto h^\dagger$$

über  $F$ , der die Gleichung  $(h^\dagger)^\dagger = h$  für alle  $h \in D$  erfüllt.

**1.1.14 Proposition.** Sei  $D$  eine Quaternionenalgebra über  $F$ . Es existiert eine eindeutige Involution  $h \mapsto \bar{h}$  auf  $D$ , so dass für eine beliebige Basis  $B = \{1, i, j, ij\}$  wie in Proposition 1.1.9

$$\bar{i} = -i, \bar{j} = -j, \bar{ij} = -ij \tag{1.1}$$

gilt. Diese nennt man Konjugation.

BEWEIS. Wählt man eine beliebige Basis  $B = \{1, i, j, ij\}$  wie in der Proposition, dann kann man elementar nachrechnen, dass durch die Gleichungen (1.1) eine Involution auf  $D$  definiert werden kann.

Um die Unabhängigkeit von der Wahl der Basis  $B$  zu zeigen betrachtet man zunächst ein beliebiges Element  $h \in D \setminus \mathbb{Q}$  mit  $h^2 \in \mathbb{Q}$ . Man schreibt  $h$  in Termen der Basis  $B$  als  $h = h_0 + h_1i + h_2j + h_3ij$  mit  $h_l \in \mathbb{Q}$ . Durch Fallunterscheidung beweist man elementar, dass  $h_0 = 0$  und somit  $\bar{h} = -h$  gilt. Sei nun  $B = \{1, i', j', i'j'\}$  eine weitere Basis von  $D$ . Da  $(i')^2, (j')^2, (i'j')^2 \in \mathbb{Q}$  gilt, folgen die Gleichungen (1.1) und somit die Behauptung der Proposition.  $\square$

**1.1.15 Definition.** Man definiert die *reduzierte Spur*  $\text{tr} : D \rightarrow F$  als die additive Abbildung  $\text{tr}(h) = h + \bar{h} \in F$  für ein Element  $h \in D$  und die *reduzierte Norm*  $n : D \rightarrow F$  als die multiplikative Abbildung  $n(h) = h\bar{h} \in F$ .

**1.1.16 Bemerkung.** Die Spur  $\text{tr} : D \rightarrow F$  definiert durch  $\langle x, y \rangle := \text{tr}(x\bar{y})$  eine symmetrische Form

$$\langle \cdot, \cdot \rangle : D \times D \rightarrow F.$$

**1.1.17 Definition.** Sei  $F \subset \mathbb{R}$  ein Unterkörper und  $D$  eine Quaternionenalgebra über  $F$ . Eine Involution  $\dagger : D \rightarrow D$  nennt man *positiv*, falls  $\text{tr}(hh^\dagger) > 0$  für alle  $h \in D \setminus \{0\}$  gilt, d.h. die quadratische Form  $\text{tr}(hh^\dagger)$  ist positiv definit.

**1.1.18 Bemerkung.** Sei  $F$  und  $D/F$  wie in Definition 1.1.17 gegeben. Die Konjugation ist genau dann eine positive Involution, wenn kein  $h \in D \setminus \{0\}$  mit  $n(h) \leq 0$  existiert.

**1.1.19 Beispiel.**

- (i) Die Konjugation in einer Matrixalgebra  $M_2(F) = \left(\frac{1, -1}{F}\right)$  ist gegeben durch die Adjunktion

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \text{Adj}(A) := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Die Spur entspricht der Spur im Sinne von Matrizen und die Norm entspricht der Determinante.

Ist  $F \subset \mathbb{R}$  dann ist die Konjugation in  $M_2(F)$  keine positive Involution. Eine positive Involution ist durch die Transposition in  $M_2(F)$  gegeben.

- (ii) Sei  $D = \left(\frac{2, -3}{\mathbb{Q}}\right)$ . Dann ist die Konjugation keine positive Involution. Jede positive Involution in  $D$  ist gegeben durch  $h^\dagger = a\bar{h}a^{-1}$  für ein  $a \in D$  mit  $a^2 < 0$ . Allgemeiner gilt folgende Proposition 1.1.21.

**1.1.20 Definition.** Sei  $\alpha \in \mathbb{Q}(\alpha) \subset \mathbb{R}$  eine algebraische Zahl. Wir nennen  $\alpha$  *total positiv*, falls für jede Einbettung  $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{R}$  gilt, dass  $\sigma(\alpha) > 0$  ist.

**1.1.21 Proposition ([Shi63, Prop. 2]).** Sei  $D$  eine total indefinite Quaternionenalgebra über einem Zahlkörper  $F \subset \mathbb{R}$ . Sei  $h \mapsto h^\dagger$  eine positive Involution. Dann existiert ein  $a \in D$  so dass  $a^2 \in F$  total negativ ist und  $h^\dagger = a\bar{h}a^{-1}$  für alle  $h \in D$  gilt.

Sei  $F$  im Rest des Abschnittes ein Zahlkörper oder ein lokaler Körper. Bezeichne  $R$  den Ganzheitsring von  $F$ . Sei  $D$  eine Quaternionenalgebra über  $F$ . Im Folgenden studieren wir bestimmte Teilringe von  $D$ , die Ordnungen (Definition 1.1.23).

**1.1.22 Definition.** Ein Element  $h \in D$  heißt *ganz* über  $F$ , falls sowohl die Norm als auch die Spur von  $h$  ganzalgebraisch sind.

**1.1.23 Definition.** Ein  $R$ -Ideal ist ein vollständiges  $R$ -Gitter in  $D$ . Eine  $R$ -Ordnung  $\mathcal{O}$  ist ein  $R$ -Ideal, das auch ein Ring ist. Eine Ordnung  $\mathcal{O}$  heißt *maximal* falls keine andere Ordnung in  $D$  existiert, die  $\mathcal{O}$  enthält.

Die Definition einer  $R$ -Ordnung  $\mathcal{O}$  ist äquivalent dazu, dass  $\mathcal{O}$  ein Ring aus ganzen Elementen von  $D$  ist, der  $R$  enthält und für den  $\mathcal{O} \otimes_R F \simeq D$  gilt. Damit folgt, dass jede  $R$ -Ordnung in einer maximalen Ordnung enthalten ist.

Die maximalen Ordnungen in indefiniten Quaternionenalgebren sind isomorph. Genauer gilt folgender

**1.1.24 Satz ( [AB04, Thm. 1.59] ).** *Ist  $D$  indefinit, so sind alle maximalen Ordnungen konjugiert.*

## 1.2 Einbettungen von imaginär quadratischen Körpern

In diesem Abschnitt wollen wir Aussagen für Einbettungen von Körpern in eine Quaternionenalgebra  $D/F$  zusammenfassen. Diese Einbettungen definieren CM-Punkte auf Shimura-Kurven (siehe Abschnitt 2.7).

**1.2.1 Definition.** Wir nennen eine  $F$ -Algebra  $D$  *separabel*, falls  $D \otimes_F K$  halbeinfach ist für alle Körpererweiterungen  $K/F$ .

**1.2.2 Bemerkung.** Sei  $F$  ein Körper mit  $\text{char}(F) = 0$  und sei  $D/F$  eine Quaternionenalgebra. Dann ist  $D$  separabel.

Im folgenden Satz zitieren wir zunächst äquivalente Bedingungen für die Existenz einer Einbettung eines Körpers in eine Quaternionenalgebra:

**1.2.3 Satz ( [Vig80, Thm. I.2.8, III.3.8] ).** *Sei  $F$  ein Zahlkörper oder ein lokaler Körper und  $D$  eine Quaternionenalgebra über  $F$  und  $K/F$  eine separable quadratische Körpererweiterung. Sei  $\Sigma$  die Menge der Primstellen in  $F$ , die in  $D$  verzweigen. Folgende Aussagen sind äquivalent:*

- (a) *es existiert eine Einbettung  $\iota : K \hookrightarrow D$ ,*
- (b) *die Quaternionenalgebra  $D \otimes_F K$  ist unverzweigt,*
- (c) *keine Primstelle  $v \in \Sigma$  ist vollständig zerlegt in  $K$ .*

*Ein Körper  $K$ , der die äquivalente Bedingungen erfüllt, heißt Zerfällungskörper von  $D$ .*

Folgender wichtiger Struktursatz ist ein Hilfsmittel in der Beschreibung der Einbettungen  $K \hookrightarrow D$  von separablen Erweiterungen  $K/F$ . Er ist eine genauere Version von Proposition 1.1.9.

**1.2.4 Satz ( [Vig80, Cor. 2.2] ).** Sei  $F$  ein beliebiger Körper der Charakteristik  $\text{char}(F) \neq 2$  und  $D$  eine Quaternionenalgebra über  $F$ . Sei  $K$  eine separable 2-dimensionale  $F$ -Algebra und  $\iota : K \hookrightarrow D$  eine Einbettung. Bezeichne  $m \mapsto \bar{m}$  den nicht-trivialen  $F$ -Automorphismus von  $K$ . Dann existieren Elemente  $\theta \in F^*$  und  $u \in D$  mit folgenden Eigenschaften:

- (i)  $D = K + uK$ ,
- (ii)  $u^2 = \theta$ ,
- (iii)  $um = \bar{m}u$  für alle  $m \in K$ .

Wir schreiben dann  $D = (K, \theta)$ .

Sei  $K$  ein Körper. Die Zahl  $\theta = u^2 \in F^*$  aus Satz 1.2.4 ist nur eindeutig bis auf Multiplikation mit Zahlen  $a \in \mathfrak{n}(K^*)$ . Denn seien  $\theta \in F^*$  und  $u \in D$  wie in der Aussage vom Satz 1.2.4 gegeben. Dann erfüllt  $u' = \gamma \cdot u \in D$  mit  $\gamma \in K^*$  die Bedingungen aus Thm. 1.2.4 und es gilt  $D = (K, \theta')$  für  $\theta' = (u')^2 = \mathfrak{n}(\gamma)\theta$ .

**1.2.5 Proposition.** Sei  $D$  eine Quaternionenalgebra über  $\mathbb{Q}$  und sei ein Zerfällungskörper  $K := \mathbb{Q}(\sqrt{-d})$  von  $D$  gegeben. Bezeichne  $\Sigma \subset \mathbb{N}$  die Menge der Primteiler von  $\text{disc}(D)$  und sei

$$\Sigma_{-1} := \{p \in \Sigma : p \text{ inert in } K\}.$$

Wähle  $u \in D$  wie in der Aussage von Satz 1.2.4, so dass o.B.d.A.  $\theta \in \mathbb{Z}$  gilt. Dann gilt  $p \mid \theta$  für alle ungeraden Primzahlen  $p \in \Sigma_{-1}$ .

BEWEIS. Dies folgt aus den Eigenschaften des Hilbertsymbols  $(\cdot, \cdot)_p$ . Denn für  $\text{ggT}(p, 2d\theta) = 1$  gilt  $(-d, \theta)_p = 1$ .  $\square$

**1.2.6 Bemerkung.** In der Notation von Satz 1.2.4 sei  $D = (K, \theta)$  und  $u \in D$  erfülle die Eigenschaften (i) bis (iii) aus diesem Satz. Dann folgt aus dem Beweis von Proposition 1.1.14, dass die Konjugation auf  $D$  gegeben ist durch

$$m \mapsto \bar{m} \quad \text{und} \quad um \mapsto -um$$

für alle  $m \in K$ . Insbesondere gilt  $\bar{u} = -u$ .

**1.2.7 Proposition.** Sei  $F$  ein beliebiger Körper mit  $\text{char}(F) \neq 2$  und  $D$  eine Algebra über  $F$ . Wir nehmen an, dass eine separable 2-dimensionale  $F$ -Algebra  $K$ , eine Einbettung  $\iota : K \hookrightarrow D$  und ein Element  $u \in D$  mit den Eigenschaften

- (i)  $D = K + uK$ ,
- (ii)  $\theta := u^2 \in F^*$ ,
- (iii)  $um = \bar{m}u$  für alle  $m \in K$

existiere. Dann ist  $D$  eine Quaternionenalgebra und in der Notation von Satz 1.2.4 gilt  $D = (K, \theta)$ .

BEWEIS. Aus der Bedingung (i) folgt, dass  $D$  von Dimension 4 über  $F$  ist. Aus der Bedingung (iii) folgt, dass  $D$  eine zentrale  $F$ -Algebra ist. Aus der Bedingung (ii) folgt, dass  $D$  nicht isomorph zu  $K^2$  und somit einfach ist. Damit ist  $D$  eine Quaternionenalgebra über  $F$ .  $\square$

Folgender Satz 1.2.8 liefert eine einfache Charakterisierung von Matrix-Algebren in Termen der Darstellung der Quaternionenalgebren wie in Satz 1.2.4.

**1.2.8 Satz ( [Vig80, Cor. 2.4] ).** Sei  $F$  ein beliebiger Körper mit  $\text{char} F \neq 2$  und  $D = (K, \theta)$  eine Quaternionenalgebra über  $F$  wie in Satz 1.2.4. Folgende Aussagen sind äquivalent:

- (i)  $D$  ist unverzweigt,
- (ii)  $K$  ist kein Körper oder  $\theta \in \mathfrak{n}(K)$ .

In der Bezeichnung von Satz 1.2.4 ist  $D = K + uK$  ein  $K$ -Vektorraum durch die Multiplikation von rechts

$$\kappa_1 : K \times D \rightarrow D, (x, h) \mapsto h \cdot \iota(x).$$

Die Abbildung

$$\kappa_2 : D \times D \rightarrow D, (h_1, h) \mapsto h_1 \cdot h$$

ist  $K$ -bilinear. Bezeichne  $\alpha \in K$  ein Element mit  $\alpha^2 \in F$ . Dann ist  $K + uK$  eine Zerlegung von  $D$  in den positiven und negativen Eigenraum bezüglich der Abbildung  $\kappa_2(\iota(\alpha)) : D \rightarrow D$ .

**1.2.9 Proposition.** Für den Ring der  $K$ -linearen Abbildungen  $\text{End}_K(D)$  gilt

$$\begin{aligned} \kappa : D \otimes_{\mathbb{Q}} K &\xrightarrow{\sim} \text{End}_K(D) \\ h_1 \otimes x &\longmapsto [h \mapsto \kappa_1(x, h) \circ \kappa_2(h_1, h).] \end{aligned}$$

BEWEIS. Der Morphismus  $\kappa$  ist offensichtlich injektiv. Die Quaternionenalgebra  $D$  ist ein zweidimensionaler  $K$ -Vektorraum. Somit ist  $\text{End}_K(D)$  und  $M_2(K)$  isomorph als  $K$ -Vektorräume. Also ist  $\kappa$  ebenfalls surjektiv.  $\square$

**1.2.10 Proposition.** Sei  $\langle \cdot, \cdot \rangle : D \times D \rightarrow F$  das Skalarprodukt auf  $D$  wie in Bem. 1.1.16. Sei  $D = (K, \theta)$  wie in Satz 1.2.4 gewählt. Dann gilt:

$$\langle m, u \rangle = 0, \quad \forall m \in K.$$

Die Zerlegung  $D = K + uK$  ist somit die orthogonale Zerlegung von  $D$  bezüglich dem Skalarprodukt  $\langle \cdot, \cdot \rangle : D \times D \rightarrow F$ .

BEWEIS. Sei  $m \in K$ . Dann ist

$$\langle m, u \rangle = \text{tr}(m\bar{u}) = m\bar{u} + u\bar{m} = -mu + mu = 0.$$

□

Sei für den Rest des Abschnittes  $F := \mathbb{Q}$  und  $D$  eine indefinite Quaternionenalgebra über  $\mathbb{Q}$ . Bezeichne  $K/\mathbb{Q}$  einen imaginären Zerfällungskörper von  $D$ . Sei also  $K = \mathbb{Q}(\alpha)$  mit  $\alpha^2 = -d$ . Bezeichne  $\iota : K \hookrightarrow D$  eine feste Einbettung. Satz 1.2.3 besagt in dieser Situation, dass alle Primteiler  $p$  der Diskriminante  $\text{disc}(D)$  in  $K$  verzweigt oder inert sind.

Wir zeigen im Folgenden, dass man einer Einbettung  $\iota : K \rightarrow D$  eine Idempotente in der Algebra  $D \otimes_{\mathbb{Q}} K \simeq M_2(K)$  zuordnen kann. Dabei führen wir Ideen aus [Mor09, §1.3] weiter aus.

**1.2.11 Proposition.** Die Konjugation auf  $D \otimes_{\mathbb{Q}} K$  wie in Proposition 1.1.14 definiert, ist gegeben durch

$$D \otimes_{\mathbb{Q}} K \longrightarrow D \otimes_{\mathbb{Q}} K, \tag{1.2}$$

$$h \otimes x \longmapsto \bar{h} \otimes x. \tag{1.3}$$

Wir bezeichnen die Konjugation auf  $D \otimes_{\mathbb{Q}} K$  ebenfalls mit  $e \mapsto \bar{e}$ .

BEWEIS. Das Zentrum von  $D \otimes_{\mathbb{Q}} K$  ist  $\mathbb{Q} \otimes_{\mathbb{Q}} K$ . Sei  $D = (K, \delta)$  und  $u \in D$  wie in Satz 1.2.4 gewählt. Dann erfüllt  $u \otimes 1 \in D \otimes_{\mathbb{Q}} K$  die Eigenschaften (i) bis (iii) des Satzes und es gilt  $(u \otimes 1)^2 = \delta$ . Mit der Bemerkung 1.2.6 folgt dann die Behauptung. □

**1.2.12 Proposition.** Sei  $\iota : K \hookrightarrow D$  eine Einbettung. Durch

$$e_{\iota} := \frac{1}{2} \left( 1 \otimes 1 - \frac{1}{d} \iota(\alpha) \otimes \alpha \right) \in D \otimes_{\mathbb{Q}} K \tag{1.4}$$

ist eine Idempotente in  $D \otimes_{\mathbb{Q}} K \simeq M_2(K)$  mit  $\text{tr } e_{\iota} = 1$  gegeben.

BEWEIS. Es gilt:

$$e_{\iota}^2 = \frac{1}{4} \left[ 1 \otimes 1 - \frac{2}{d} \iota(\alpha) \otimes \alpha + \frac{1}{d^2} \iota(-d) \otimes (-d) \right] = e_{\iota}$$

und

$$\begin{aligned} \operatorname{tr} e_\iota &= e_\iota + \bar{e}_\iota \\ &= 1 \otimes 1 - \frac{1}{2d}(\iota(\alpha) \otimes \alpha + \iota(\bar{\alpha}) \otimes \alpha) \\ &= 1 \otimes 1. \end{aligned}$$

□

**1.2.13 Definition.** Wir nennen die Idempotente  $e_\iota \in D \otimes_{\mathbb{Q}} K$  wie in (1.4) die zu  $\iota$  gehörende Idempotente. Falls klar ist, welche Einbettung  $\iota : K \rightarrow D$  wir betrachten, schreiben wir auch abkürzend  $e$  für  $e_\iota$ .

**1.2.14 Proposition.** Sei  $e := a \otimes 1 + b \otimes \alpha \in D \otimes_{\mathbb{Q}} K$  eine Idempotente mit  $e \notin \{0, 1\}$ . Dann definiert  $\alpha \mapsto ab^{-1}$  eine Einbettung  $\iota : K \hookrightarrow D$ . Für die zu  $\iota$  gehörende Idempotente  $e_\iota$  wie in Proposition 1.2.12 gilt:

$$e_\iota = e \cdot (2a \otimes 1)^{-1}.$$

BEWEIS. Da  $e$  eine Idempotente ist, gilt

$$\begin{aligned} e^2 &= (a^2 - db^2) \otimes 1 + (ab + ba) \otimes \alpha \\ &= (a \otimes 1 + b \otimes \alpha). \end{aligned}$$

Dies entspricht dem Gleichungssystem

$$a^2 - db^2 = a \tag{1.5}$$

$$ab + ba = b. \tag{1.6}$$

Da (1.6) äquivalent zu  $ab^{-1} = b^{-1}(1 - a)$  ist, folgt die Identität

$$\begin{aligned} ab^{-1}ab^{-1} &\stackrel{(1.6)}{=} b^{-1}(1 - a)ab^{-1} \\ &= b^{-1}ab^{-1} - b^{-1}a^2b^{-1} \\ &\stackrel{(1.5)}{=} b^{-1}ab^{-1} - b^{-1}ab^{-1} - b^{-1}db^2b^{-1} \\ &= -d. \end{aligned}$$

Da  $e \neq 1$  eine Idempotente ist, gilt

$$0 = n(e) = e\bar{e} = (n(a) - d n(b)) \otimes 1 + \operatorname{tr}(a\bar{b}) \otimes \alpha.$$

und folglich  $\operatorname{tr}(ab^{-1}) = \operatorname{tr}(a\bar{b})/n(b) = 0$ . Somit definiert  $\alpha \mapsto ab^{-1}$  eine Einbettung. Die letzte Aussage der Proposition folgt aus den Gleichungen

$$e \cdot (2a \otimes 1)^{-1} = \frac{1}{2}(1 \otimes 1 + ba^{-1} \otimes \alpha) = e_\iota.$$

□

**1.2.15 Korollar.** Folgende Abbildung liefert eine Bijektion von Mengen:

$$\begin{aligned} \{\iota : K \hookrightarrow D\} & \longrightarrow \{e \in D \otimes_{\mathbb{Q}} K : e^2 = e, \operatorname{tr} e = 1\}, \\ \iota : K \hookrightarrow D & \longmapsto e_{\iota} = \frac{1}{2}(1 \otimes 1 - \frac{1}{d}\iota(\alpha)^{-1} \otimes \alpha), \\ \left\{ \begin{array}{l} \iota : K \hookrightarrow D \\ \alpha \mapsto b^{-1} \end{array} \right. & \longleftarrow e = \frac{1}{2}(1 \otimes 1 + b \otimes \alpha). \end{aligned}$$

BEWEIS. Die Behauptung folgt unmittelbar aus Proposition 1.2.12 und Proposition 1.2.14 für  $a = \frac{1}{2}$ . □

**1.2.16 Proposition.** Sei  $\iota : K \hookrightarrow D$  eine Einbettung und  $e_{\iota} \in D \otimes_{\mathbb{Q}} K$  die zugehörige Idempotente nach Korollar 1.2.15. Bezeichne  $\bar{\iota} : K \hookrightarrow D$  die Verknüpfung der komplexen Konjugation auf  $K$  mit  $\iota$  und bezeichne  $e_{\bar{\iota}}$  die zu  $\bar{\iota}$  gehörende Idempotente. Dann gelten folgende Identitäten:

$$e_{\bar{\iota}} = \bar{e}_{\iota} = 1 - e_{\iota}.$$

BEWEIS. Dies folgt unmittelbar aus Proposition 1.2.12 und der Definition der Konjugation auf  $D \otimes_{\mathbb{Q}} K$ . □

Durch den Isomorphismus  $\kappa : D \otimes_{\mathbb{Q}} K \simeq \operatorname{End}_K(D)$  aus Prop. 1.2.9 definiert die Idempotente  $e$  eine Projektion  $\kappa(e)$  auf  $D$ . Die komplementäre Projektion ist gegeben durch  $1 - \kappa(e) = \kappa(\bar{e})$ :

**1.2.17 Korollar (zu Prop. 1.2.10).** In der Notation von Prop. 1.2.10 gilt: Die  $K$ -lineare Abbildung  $\kappa(e_{\iota})$  (resp.  $\kappa(\bar{e}_{\iota})$ ) ist die orthogonale Projektion bzgl. dem Skalarprodukt  $\langle \cdot, \cdot \rangle : D \times D \rightarrow K$  nach  $K$  (resp.  $uK$ ).

BEWEIS. Sei  $x := x_1 + ux_2 \in K + uK = D$  gegeben. Dann gilt

$$\begin{aligned} & \kappa(e)(x_1 + ux_2) \\ &= \kappa\left(\frac{1}{2} \otimes 1 - \frac{1}{2d}\iota(\alpha) \otimes \alpha\right)(x_1 + ux_2) \\ &= \frac{1}{2}(x_1 + ux_2 - \frac{1}{d}\iota(\alpha)x_1\iota(\alpha) - \frac{1}{d}\iota(\alpha)ux_2\iota(\alpha)) \\ &\stackrel{(*)}{=} \frac{1}{2}(x_1 + ux_2 + x_1 - ux_2) \\ &= x_1. \end{aligned}$$

Dabei folgt (\*) aus der Eigenschaft (iii) von Satz 1.2.4. Die Aussage für  $\kappa(\bar{e}_{\iota})$  beweist man analog. □

Sei nun  $\mathcal{O}$  eine Ordnung in  $D$  und  $\mathcal{O}_D$  eine maximale Ordnung, die  $\mathcal{O}$  enthält. Um CM-Punkte einer Shimura-Kurve (siehe Abschnitt 2.7) zu beschreiben, betrachten wir nicht nur Einbettungen  $\iota : K \hookrightarrow D$  von Zerfällungskörpern  $K$ , sondern zusätzlich die Urbilder  $\iota^{-1}(\mathcal{O})$ . Diese Urbilder sind Ordnungen in  $K$ .

Sei  $K := \mathbb{Q}(\sqrt{-d})$  ein Zerfällungskörper von  $D$  und  $\mathcal{O}_{K,c}$  eine Ordnung von  $K$  mit Führer  $c \in \mathbb{N}$ . Sei  $h(\mathcal{O}_{K,c})$  die Klassenzahl von  $\mathcal{O}_{K,c}$ , also die Anzahl der gebrochenen Ideale modulo Hauptideale (für Eigenschaften der Klassenzahl siehe [Neu07, §6]).

**1.2.18 Definition.** Wir bezeichnen mit

$$\mathbb{E}(\mathcal{O}, \mathcal{O}_{K,c}) := \{\iota : K \hookrightarrow D \text{ mit } \iota(\mathcal{O}_{K,c}) \subset \mathcal{O}\}$$

die Menge der Einbettungen von  $\mathcal{O}_{K,c}$  in  $\mathcal{O}$ . Gilt  $\iota(\mathcal{O}_{K,c}) = \mathcal{O}$ , dann nennen wir  $\iota \in \mathbb{E}(\mathcal{O}, \mathcal{O}_{K,c})$  eine *optimale Einbettung* bzgl.  $\mathcal{O}_{K,c}$ . Wir bezeichnen die Menge der optimalen Einbettungen mit  $\mathbb{E}^*(\mathcal{O}, \mathcal{O}_{K,c})$ .

### 1.3 Automorphismen

In diesem Abschnitt wollen wir die Untergruppe  $\mathcal{O}_D^1$  (Definition 1.3.5) der Automorphismengruppe der Quaternionenalgebra  $D$  über  $\mathbb{Q}$  untersuchen. Die Gruppe  $\mathcal{O}_D^1$  liefert eine Fuchssche Gruppe  $\Gamma(1) < \mathrm{SL}_2(\mathbb{R})$ . Der Quotient  $\mathcal{X}(1) := \mathcal{H}/\Gamma(1)$  liefert eine Shimura-Kurve (Definition 2.3.2).

Sei allgemein  $F \subset \mathbb{R}$  ein Zahlkörper und  $D$  eine Quaternionenalgebra über  $F$ . Sei  $\mathcal{O}_F$  der Ganzheitsring von  $F$ .

**1.3.1 Definition.** Bezeichne  $\mathrm{Aut}_F(D)$  die Gruppe der  $F$ -Automorphismen von  $D$ , d.h. der Automorphismen  $\gamma : D \rightarrow D$ , die eingeschränkt auf  $F$  die Identität sind.

**1.3.2 Proposition ( [Vig80, Thm. 2.1, Cor. 2.3] ).** Sei  $\gamma \in \mathrm{Aut}_F(D)$  ein  $F$ -Automorphismus. Dann ist  $\gamma$  ein innerer Automorphismus, dh. es existiert ein  $h \in D$ , so dass  $\gamma(x) = h x h^{-1}$  für alle  $x \in D$  gilt. Insbesondere gilt  $\mathrm{Aut}_F(D) \simeq D^*/F^*$ .

Sei  $\mathcal{O} \subset D$  eine  $\mathcal{O}_F$ -Ordnung. Wir möchten nun zwei bestimmte Gruppen von Automorphismen studieren. Nämlich jene, deren Elemente die Ordnung  $\mathcal{O}$  festlassen und jene, deren Elemente zusätzlich Bilinearformen auf  $D$  festlassen. Diese Gruppen liefern uns Fuchssche Gruppen (Definition 2.2.7), die uns zur Definition der Shimura-Kurven  $\mathcal{X}^*(1)$  und  $\mathcal{X}(1)$  führen (Definition 2.3.2).

**1.3.3 Definition.** Wir definieren den *Normalisator* von  $\mathcal{O}$  als die Gruppe

$$\text{Nor}(\mathcal{O}) := \{h \in D^* : h\mathcal{O} = \mathcal{O}h\}.$$

**1.3.4 Korollar (zu Prop. 1.3.2).**

- (i) Die Gruppe der Automorphismen  $\{\mu \in \text{Aut}_F(D) : \mu(\mathcal{O}) = \mathcal{O}\}$  der Ordnung  $\mathcal{O}$  ist isomorph zum Quotienten  $\text{Nor}(\mathcal{O})/\mathcal{O}_F^*$ .
- (ii) Sei  $h \in \mathcal{O}^*$ . Genau dann ist  $\mathcal{O}h$  Links- und Rechtsideal, wenn  $\mathcal{O}h = h\mathcal{O}$ , i.e.  $h \in \text{Nor}(\mathcal{O})$  ist.

BEWEIS. Der Beweis ist elementar. □

Korollar 1.3.4 besagt, dass  $\text{Nor}(\mathcal{O})$  auf der Menge der beidseitigen Idealen wirkt.

**1.3.5 Definition.** Bezeichne  $\mathcal{O}_D^1 \subset D$  die Gruppe

$$\mathcal{O}_D^1 := \{h \in \mathcal{O}_D : n(h) = 1\} < \text{Nor}(\mathcal{O}).$$

Sei

$$\dagger : D \rightarrow D, x \mapsto x^\dagger$$

eine positive Involution. Dann korrespondiert nach Proposition 1.1.21 zur Involution  $\dagger$  ein Element  $a \in D$ , so dass  $a^2 \in F$  total negativ ist und  $x^\dagger = a\bar{x}a^{-1}$  gilt. Dann definiert

$$E_a : D \times D \longrightarrow \mathbb{R} \tag{1.7}$$

$$(x_1, x_2) \longmapsto \text{tr}(x_1 \cdot a^{-1} \cdot x_2^\dagger) \tag{1.8}$$

eine alternierende Bilinearform. Ein Element  $h \in \mathcal{O}_D^1$  lässt im folgenden Sinne die Bilinearform  $E_a$  fest:

**1.3.6 Proposition.** Sei  $h \in \mathcal{O}_D$ . Dann gilt

$$E_a(x_1h, x_2h) = n(h) \cdot E_a(x_1, x_2)$$

für alle  $x_1, x_2 \in D$ . Insbesondere ist die Bilinearform  $E_a$  invariant unter Rechtsmultiplikation von  $h \in \mathcal{O}_D$ , wenn  $h \in \mathcal{O}_D^1$  ist.

BEWEIS. Es gilt

$$\begin{aligned} E_a(x_1h, x_2h) &= \text{tr}(x_1h \cdot a^{-1} \cdot (x_2h)^\dagger) \\ &= \text{tr}(x_1h\overline{x_2h}a^{-1}) \\ &= n(h) \text{tr}(x_1\overline{x_2}a^{-1}) = n(h) \cdot E_a(x_1, x_2). \end{aligned}$$

□

**1.3.7 Bemerkung.** Sei  $A$  eine abelsche Varietät vom Typ  $\mathcal{Q}M$  und sei eine Polarisierung  $\lambda : A \rightarrow A^t$  gegeben. Die Proposition 1.3.6 besagt, dass für  $h \in \mathcal{O}_D^1$  folgendes Diagramm kommutiert:

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & A^t \\ \downarrow h & & \uparrow h^\dagger \\ A & \xrightarrow{\lambda} & A^t. \end{array}$$

Wir sind im Folgenden daran interessiert, wie die Gruppen  $\text{Nor}(\mathcal{O})$  und  $\mathcal{O}_D^1$  auf den Einbettungen in  $D$  von Zerfällungskörpern wirken. Um die Notation zu vereinfachen betrachten wir nur den Fall, dass  $F = \mathbb{Q}$  gilt.

**1.3.8 Lemma ( [AB04, Cor. 4.17] ).** Sei  $D$  eine Quaternionenalgebra über  $\mathbb{Q}$  und  $\mathcal{O}$  eine Ordnung von  $D$ . Sei desweiteren  $h \in \text{Nor}(\mathcal{O})$  und  $\iota : K \hookrightarrow D$  in  $\mathbb{E}(\mathcal{O}, \mathcal{O}_{K,c})$ . Dann gilt:

- (i) Der Morphismus  $\iota^h := h^{-1}\iota(\cdot)h : K \hookrightarrow D$  definiert eine Einbettung von  $\mathcal{O}_{K,c}$  in  $\mathcal{O}$ .
- (ii) Die Einbettung  $\iota^h$  aus (i) ist genau dann optimal, wenn  $\iota$  optimal ist.

Mit Hilfe von Lemma 1.3.8 kann man folgende Äquivalenzrelation definieren:

**1.3.9 Definition.** Wir nennen zwei Einbettungen  $\iota, \iota' \in \mathbb{E}(\mathcal{O}, \mathcal{O}_{K,c})$  äquivalent, falls ein  $h \in \mathcal{O}_D^1$  existiert so dass  $\iota' = \iota^h$  ist.

Bezeichne  $h(\mathcal{O}, \mathcal{O}_{K,c})$  die Anzahl der Äquivalenzklassen optimaler Einbettungen aus  $\mathbb{E}^*(\mathcal{O}, \mathcal{O}_{K,c})$ .

**1.3.10 Proposition ( [Vig80, Cor. 5.12, 5.13] ).** Bezeichne  $\Sigma_{-1}$  die Menge der Primzahlen  $p \mid \text{disc}(D)$  inert in  $K$  und bezeichne  $b = |\Sigma_{-1}|$ . Es gilt:

$$h(\mathcal{O}_D^1, \mathcal{O}_{K,c}) = 2^{b+1}h(\mathcal{O}_{K,c}).$$

**1.3.11 Bemerkung.** (i) In [Neu07, §12] findet man eine Formel für die Klassenzahl von  $\mathcal{O}_{K,c}$ , die in konkreten Fällen angewendet werden kann. Man kann somit auch  $h(\mathcal{O}_D^1, \mathcal{O}_{K,c})$  konkret angeben.

(ii) In [Vig80, Cor. 5.12] ist auch eine explizite Formel für die Anzahl der optimalen Einbettungen modulo  $\text{Nor}(\mathcal{O}_D)$  gegeben.

## Kapitel 2

# Abelsche Flächen vom Typ QM und die Shimura-Kurve $\mathcal{X}(1)$

In diesem Kapitel benutzen wir die Ergebnisse über Quaternionenalgebren aus Kapitel 1 um die Shimura-Kurve  $\mathcal{X}(1)$  zu studieren. Sei  $\mathcal{O}_D$  eine feste maximale Ordnung in einer Quaternionenalgebra  $D$  über  $\mathbb{Q}$ . Zu der Automorphismengruppe  $\mathcal{O}_D^1$  (Definition 1.3.5) gehört eine Shimura-Kurve  $\mathcal{X}(1)$  (Definition 2.3.2). Diese parametrisiert Isomorphieklassen hauptpolarisierte abelsche Flächen  $A$  mit Einbettungen  $\mathcal{O}_D \hookrightarrow \text{End}(A)$ .

Kroworsch ([Kro09]) zeigt Kongruenzen für verallgemeinerte Spuren singulärer Moduli im Fall von klassischen Modulkurven. Um Spurformeln analog zu denen in [Kro09] definieren zu können, müssen wir einige Informationen über die abelschen Flächen haben, die als Punkte der Shimura-Kurve  $\mathcal{X}(1)$  auftreten. Insbesondere die CM-Punkte auf  $\mathcal{X}(1)$  müssen studiert werden, weil sie eine Verallgemeinerung der singulären Moduli auf die Shimura-Kurve  $\mathcal{X}(1)$  sind.

Im Fall der Modulkurve entsprechen den singulären Moduli die elliptische Kurven mit komplexer Multiplikation. Analog entsprechen den CM-Punkte auf  $\mathcal{X}(1)$  abelsche Flächen deren Endomorphismenalgebra echt größer als die Quaternionenalgebra  $D$  sind. Diese sind dann isogen zum Produkt isogener elliptischer Kurven.

In diesem Kapitel studieren wir die Shimura-Kurve  $\mathcal{X}(1)$  und ihre CM-Punkte, sowohl als Quotient  $\mathcal{H}/\Gamma$  der komplexen oberen Halbebene nach einer Fuchs'schen Gruppe  $\Gamma$ , wie auch mittels der Modulinterpretation von  $\mathcal{X}(1)$ . In Abschnitt 2.1 definieren wir, was wir unter einer abelschen Fläche  $A$  vom Typ QM verstehen. Wir zeigen, dass entweder die Endomorphismenalgebra von  $A$  in Charakteristik 0 isomorph zur Quaternionenalgebra

ist oder  $A$  isogen zum Produkt zweier elliptischer Kurven ist (Proposition 2.1.8). Wir zeigen außerdem, dass  $A$  über endlichen Körpern nicht absolut einfach ist (Satz 2.1.9). In Abschnitt 2.2 fassen wir dann allgemeine Ergebnisse über arithmetische Fuchssche Gruppen und Shimura-Kurven über den komplexen Zahlen zusammen. In Abschnitt 2.3 wenden wir diese allgemeinen Ergebnisse auf die Shimura-Kurve  $\mathcal{X}(1)$  an. In Abschnitt 2.4 und Abschnitt 2.5 betrachten wir die CM-Punkte auf  $\mathcal{X}(1)$  mittels ihrer Modulinterpretation (Satz 2.3.6) und treffen Strukturaussagen über abelsche Flächen vom Typ QM & CM über Zahlkörper (Theorem 2.4.12 und Satz 2.5.7). Diese lassen sich mit etwas Vorsicht auch über endlichen Körpern anwenden. Dies benutzen wir in Abschnitt 2.6 um Aussagen über die Liftbarkeit von Endomorphismen nach Charakteristik 0 zu treffen. Im letzten Abschnitt 2.7 geben wir eine intrinsische Beschreibung der CM-Punkte auf  $\mathcal{X}(1)$  und verbinden diese mit der Modulinterpretation um eine Korrespondenz zwischen CM-Punkten auf  $\mathcal{X}(1)$  und bestimmten elliptischen Kurven explizit zu machen (Theorem 2.7.12).

## 2.1 Abelsche Flächen vom Typ QM

Sei  $A$  eine abelsche Fläche über dem Körper  $F$ . Wir bestimmen in diesem Abschnitt die Möglichkeiten für die Endomorphismenalgebra  $\text{End}^0(A)$ , so dass eine Einbettung  $D \hookrightarrow \text{End}^0(A)$  einer Quaternionenalgebra  $D$  über  $\mathbb{Q}$  existiert (Proposition 2.1.8). In positiver Charakteristik  $\text{char}(F) > 0$  folgt aus der Existenz einer solchen Einbettung, dass  $A$  nicht absolut einfach ist (Satz 2.1.9).

Sei  $F$  ein beliebiger Körper mit  $\text{char}(F) \neq 2$ . Sei  $A$  eine abelsche Varietät von Dimension 2 über  $F$ . Bezeichne  $\text{End}(A)$  den Endomorphismenring von  $A$  und  $\text{End}^0(A) := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$  die Endomorphismenalgebra von  $A$ . Für Allgemeines über Endomorphismenalgebren von abelschen Varietäten sei auf [Mum74, Kap. IV] verwiesen.

Bezeichne  $A^t \simeq \text{Pic}^0(A)$  die duale abelsche Varietät von  $A$ . Bezeichne  $t_P : A \rightarrow A$  die Translation mit  $P$ . Sei  $L$  ein Geradenbündel auf  $A$ . Die Zuordnung

$$\begin{aligned} \varphi_L : A &\longrightarrow \text{Pic}^0(A) \\ P &\longmapsto [t_P^* L \otimes L^{-1}] \end{aligned} \tag{2.1}$$

ist ein Homomorphismus. Ist  $L$  ampel, so ist  $\varphi_L$  eine Isogenie.

**2.1.1 Definition.** Eine *Quasi-Polarisierung* ist ein Morphismus  $\lambda : A \rightarrow A^t$  mit folgender Eigenschaft:

Es existiert eine Körpererweiterung  $F' \supset F$  und ein Geradenbündel  $L$  auf

$A \otimes F'$ , so dass  $\lambda \otimes F' = \varphi_L$  für  $\varphi_L$  wie in (2.1) ist.

Ist das Geradenbündel  $L$  ampel, so nennen wir den Morphismus  $\lambda : A \rightarrow A^t$  eine *Polarisierung*.

Wir nennen  $A$ , falls eine Polarisation gegeben ist, vereinfachend *polarierte abelsche Varietät*. Ist  $\deg \lambda = 1$ , dann nennen wir  $A$  *hauptpolariert*.

Sei nun eine Polarisation  $\lambda : A \rightarrow A^t$  gegeben.

**2.1.2 Proposition ([Mum74, §20, §21]).** *Die Polarisation induziert eine positive Involution*

$$\dagger : \text{End}^0(A) \rightarrow \text{End}^0(A), \alpha \mapsto \alpha^\dagger := \lambda^{-1} \circ \alpha^t \circ \lambda$$

auf  $\text{End}^0(A)$ , die Rosati-Involution.

Betrachte nun also  $\text{End}^0(A)$  ausgestattet mit der Involution  $\dagger$  aus Proposition 2.1.2.

**2.1.3 Definition.** Wir nennen eine abelsche Varietät  $A/F$  *einfach*, falls sie über  $F$  keine echten abelschen Untervarietäten besitzt. Behält  $A$  diese Eigenschaften nach beliebiger Körpererweiterung, so nennen wir  $A$  *absolut einfach*.

Wendet man die allgemeinen Ergebnisse für die Endomorphismenalgebren einer abelschen Varietät aus [Mum74, Thm. 2] auf den Fall  $g = 2$  an, so ergibt sich folgender Satz 2.1.4 für die Endomorphismenalgebra  $\text{End}^0(A) := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ .

**2.1.4 Satz.** *Sei  $A$  eine einfache abelsche Fläche. Bezeichne  $K$  das Zentrum von  $\text{End}^0(A)$  und  $K_0$  den Unterkörper der Elemente von  $K$ , die durch die Involution  $\dagger$  auf  $\text{End}^0(A)$  festgelassen werden. Dann ist  $\text{End}^0(A)$  endlich-dimensional als  $\mathbb{Q}$ -Algebra. Der Körper  $K_0$  ist total reell. Es treten folgende Möglichkeiten für  $\text{End}^0(A)$  auf:*

- (Ia)  $\text{End}^0(A) = K \simeq \mathbb{Q}$ ,
- (Ib)  $\text{End}^0(A) = K \simeq \mathbb{Q}(\sqrt{d})$  mit quadratfreiem  $d \in \mathbb{N}$ ,
- (II)  $\text{End}^0(A)$  ist isomorph zu einer indefiniten Quaternionenalgebra über den rationalen Zahlen  $K = \mathbb{Q}$ ,
- (IIIa)  $\text{End}^0(A)$  ist isomorph zu einer definiten Quaternionenalgebra über den rationalen Zahlen  $K = \mathbb{Q}$ ,
- (IIIb)  $\text{End}^0(A)$  ist isomorph zu einer definiten Quaternionenalgebra über dem Körper  $K_0 \simeq \mathbb{Q}(\sqrt{d})$  mit  $d \in \mathbb{Q}_{>0}$ ,
- (IVa)  $\text{End}^0(A) \simeq \mathbb{Q}(\sqrt{-d})$  mit  $d \in \mathbb{Q}_{>0}$ , i.e.  $\text{End}^0(A)$  ist isomorph zu einem CM-Körper von Grad 2,

## 18 Kapitel 2. Abelsche Flächen vom Typ $\mathcal{QM}$ und Shimura-Kurven

(IVb)  $\text{End}^0(A)$  ist isomorph zu einer Quaternionenalgebra, dessen Zentrum isomorph zu  $K \simeq \mathbb{Q}(\sqrt{-d})$  mit  $d \in \mathbb{Q}_{>0}$  ist,

(IVc)  $\text{End}^0(A)$  ist isomorph zu einem CM-Körper  $K$  von Grad 4, d.h.  $\text{End}^0(A)$  ist isomorph zu einer imaginär quadratischen Erweiterung  $K$  des total reellen Unterkörpers  $K_0 = \mathbb{Q}(\sqrt{d})$  von Grad 2.

Die Fälle (IIIb) und (IVb) treten nur in positiver Charakteristik auf.

Ist die abelsche Fläche  $A$  nicht einfach, dann ist sie isogen zum Produkt  $A \sim E \times E'$  elliptischer Kurven. In diesem Fall gilt für die Endomorphismenalgebra:

- $\text{End}^0(A) \simeq M_2(\text{End}^0(E))$ , falls  $E$  und  $E'$  isogen sind,
- $\text{End}^0(A) \simeq \text{End}^0(E) \times \text{End}^0(E')$ , falls  $E$  und  $E'$  nicht isogen sind.

**2.1.5 Definition.** Eine einfache abelsche Varietät  $A$  hat *komplexe Multiplikation*, falls für die Endomorphismenalgebra  $D := \text{End}^0(A)$  und das Zentrum  $K$  von  $D$  die Gleichung  $\sqrt{\dim_K(D)} \cdot [K : \mathbb{Q}] = 2g$  erfüllt ist. Eine zusammengesetzte abelsche Varietät hat komplexe Multiplikation, falls deren einfache Faktoren komplexe Multiplikation haben.

Eine einfache abelsche Fläche hat im Fall (IIIb), (IVb) und (IVc) komplexe Multiplikation.

**2.1.6 Definition.** Sei  $A$  eine (nicht notwendigerweise einfache) abelsche Fläche und existiere eine Einbettung  $\psi_{\mathcal{QM}} : D \hookrightarrow \text{End}^0(A)$  einer indefiniten Quaternionenalgebra  $D$  über  $\mathbb{Q}$  in die Endomorphismenalgebra  $\text{End}^0(A)$  von  $A$ . Bezeichne  $\dagger$  die positive Involution auf  $\text{End}^0(A)$ . Wir nehmen an dass  $\psi_{\mathcal{QM}}(D)^\dagger = \psi_{\mathcal{QM}}(D)$  erfüllt sei. Dann nennen wir die abelsche Fläche  $A$  vom *Typ  $\mathcal{QM}$*  durch  $\psi_{\mathcal{QM}}$ . Wir nennen die Einbettung  $\psi_{\mathcal{QM}} : D \hookrightarrow \text{End}^0(A)$  den  *$\mathcal{QM}$ -Typ* von  $A$ .

**2.1.7 Bemerkung.** Bezeichne

$$\dagger := \psi_{\mathcal{QM}}^{-1} \circ \dagger \circ \psi_{\mathcal{QM}} : D \longrightarrow D$$

ebenso die positive Involution auf  $D$  induziert durch den  $\mathcal{QM}$ -Typ  $\psi_{\mathcal{QM}}$ . Wenn wir vom  $\mathcal{QM}$ -Typ sprechen, meinen wir, dass die Quaternionenalgebra  $D$  mit jener positiven Involution  $\dagger$  versehen ist.

In der folgender Proposition 2.1.8 bestimmen wir die Möglichkeiten für die Endomorphismenalgebra einer abelschen Fläche  $A$  von Typ  $\mathcal{QM}$  in Charakteristik 0.

**2.1.8 Proposition.** Sei  $F$  ein Körper der Charakteristik  $\text{char}(F) = 0$  und  $A$  eine abelsche Fläche über  $F$  vom Typ  $\mathcal{QM}$  durch  $D$ . Dann gilt folgendes für die Endomorphismenalgebra  $\text{End}^0(A)$ :

- (i) Ist  $A$  über  $F$  einfach, dann ist  $\text{End}^0(A)$  isomorph zu einer Quaternionenalgebra (Fall II in Satz 2.1.4).
- (ii) Ist  $A$  über  $F$  nicht einfach, dann gilt  $\text{End}^0(A) \simeq M_2(K)$ . Und es gilt  $A \sim E^2$  für eine elliptische Kurve mit komplexer Multiplikation durch  $K \subset D$ .

BEWEIS. Ist  $A$  einfach, dann gilt nach der Klassifikation der Endomorphismenalgebren von einfachen abelschen Flächen in Satz 2.1.4, dass  $\text{End}^0(A)$  kommutativ ist oder isomorph zu einer indefiniten Quaternionenalgebra  $D$  über  $\mathbb{Q}$ . Dies beweist (i).

Ist  $A$  über  $F$  nicht einfach, dann gilt  $A \sim_F E \times E'$  für elliptische Kurven  $E, E'$ . Somit ist  $\text{End}^0(A)$  kommutativ oder isomorph zu einer Matrixalgebra  $M_2(K)$ . Es muss also  $D \subset M_2(K)$  gelten und folglich  $K$  ein Zerfällungskörper von  $D$  sein. Da  $\text{End}^0(A) \simeq M_2(K)$  ist, folgt dass  $E \sim E'$  und  $\text{End}^0(E) \simeq K \subset D$  gilt.  $\square$

Im Folgenden betrachten wir den Fall, dass  $A$  eine abelsche Fläche vom Typ  $\mathcal{QM}$  über einem endlichen Körper  $k$  ist. Mittels der Honda-Tate-Theorie ([Tat68]) kann man zeigen, dass  $A$  nicht absolut einfach ist:

**2.1.9 Satz.** Sei  $k$  ein endlicher Körper der Charakteristik  $p := \text{char}(k)$ . Sei  $D$  über  $\mathbb{Q}$  eine indefinite Quaternionenalgebra. Sei  $A$  eine abelsche Fläche über  $k$  vom Typ  $\mathcal{QM}$  durch  $D$ . Dann ist  $A$  (über dem algebraischen Abschluss  $\bar{k}$ ) isogen zum Produkt  $E^2$  einer elliptischen Kurve  $E$  mit komplexer Multiplikation. Insbesondere ist  $A$  entweder gewöhnlich oder supersingulär.

BEWEIS. Mittels der Honda-Tate-Theorie werden in [Oor, Bem. zu Prop. 3.13] die Möglichkeiten für die Endomorphismenalgebren von einfachen abelschen Flächen über endlichen Körpern bestimmt. Dort wird auch bestimmt, ob die zugehörige abelsche Fläche absolut einfach ist. Dies liefert das Ergebnis, dass  $A$  genau dann absolut einfach ist, wenn  $\text{End}^0(A)$  isomorph zu einem CM-Körper  $K$  von Dimension 4 ist. Da eine Einbettung  $D \hookrightarrow \text{End}^0(A)$  existiert ist  $\text{End}^0(A)$  nicht kommutativ. Folglich ist  $A$  nicht absolut einfach.  $\square$

**2.1.10 Bemerkung.** In Charakteristik 0 gibt es absolut einfache abelsche Flächen vom Typ  $\mathcal{QM}$ , siehe [HM95, Example 1.6]. Beispielsweise ist die Jakobische  $J(C)$  der Kurve

$$C : y^2 = x(x^4 + \frac{1+2\sqrt{11}}{2}x^3 + \frac{99}{20}x^2 + \frac{-1+2\sqrt{11}}{2}x + 1)$$

vom Typ  $\mathcal{QM}$  mit der Quaternionenalgebra  $D := \left(\frac{2,-3}{\mathbb{Q}}\right)$ . Sie ist aber absolut einfach, also hat  $J(C)$  nach 2.1.8 insbesondere keine komplexe Multiplikation.

**2.1.11 Korollar.** *Wir benutzen die Notation von Satz 2.1.9. Sei  $A$  desweiteren gewöhnlich. Dann existiert ein imaginärer Zerfällungskörper  $K$  von  $D$ , so dass  $\text{End}^0(E) \simeq K$  gilt. Insbesondere gilt  $\text{End}_{\bar{k}}^0(A) \simeq M_2(K) \simeq D \otimes_{\mathbb{Q}} K$ .*

BEWEIS. Dies folgt aus der selben Überlegung wie in Proposition 2.1.8.  $\square$

Der  $p$ -Rang (Definition 2.1.12) ist eine wichtige Invariante einer abelschen Varietät in positiver Charakteristik.

**2.1.12 Definition.** Sei  $A$  eine abelsche Varietät von Dimension  $g$  über einem Körper  $k$  mit  $\text{char}(k) = p > 0$ . Bezeichne  $A[p](\bar{k})$  die  $p$ -Torsionspunkte von  $A$  über dem algebraischen Abschluss  $\bar{k}$  von  $k$ . Dann nennen wir die natürliche Zahl  $0 \leq r \leq g$ , so dass  $A[p](\bar{k}) \simeq (\mathbb{Z}/p\mathbb{Z})^r$  gilt, den  $p$ -Rang von  $A$ . Wir nennen  $A$  *gewöhnlich* falls  $r = g$  gilt. Wir nennen eine elliptische Kurve *supersingulär*, falls  $r = 0$  gilt. Eine abelsche Varietät von Dimension  $g > 1$  nennen wir *supersingulär*, falls  $A$  über dem algebraischen Abschluss  $\bar{k}$  isogen zum Produkt  $E^g$  einer supersingulären elliptischen Kurve  $E$  ist.

Wir bestimmen den  $p$ -Rang einer abelschen Fläche vom Typ QM:

**2.1.13 Korollar.** *Sei  $D$  über  $\mathbb{Q}$  eine indefinite Quaternionenalgebra. Sei  $A$  eine abelsche Fläche über einem endlichen Körper  $k$  vom Typ QM durch  $D$ . Dann ist  $A$  entweder gewöhnlich oder supersingulär.*

BEWEIS. Dies folgt direkt aus Satz 2.1.9, da die elliptische Kurve  $E \subset A$  entweder gewöhnlich oder supersingulär ist.  $\square$

## 2.2 Arithmetische Fuchssche Gruppen

In diesem Abschnitt zitieren wir allgemeine Ergebnisse über Fuchssche Gruppen (Definition 2.2.7) und geben die Definition einer arithmetischen Fuchsschen Gruppe (Definition 2.2.13). Dieser Abschnitt ist die Vorbereitung für den nächsten Abschnitt 2.3, in dem wir Shimura-Kurven (Definition 2.2.14) über  $\mathbb{C}$  betrachten, die Isomorphieklassen von hauptpolarierten abelschen Flächen vom Typ QM parametrisieren.

Sei  $\mathcal{H} := \{z = a + bi \in \mathbb{C} : b = \text{Im } z > 0\}$  die komplexe obere Halbebene.

**2.2.1 Definition.** Eine *gebrochene lineare Transformation* ist eine Abbildung  $\mathbb{P}_{\mathbb{C}}^1 \rightarrow \mathbb{P}_{\mathbb{C}}^1$ , definiert durch

$$z \mapsto \frac{az + b}{cz + d}, \quad \text{mit } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{C}).$$

**2.2.2 Proposition.** *Die Gruppe  $\text{PSL}_2(\mathbb{R}) := \text{SL}_2(\mathbb{R})/\{\pm 1\}$  wirkt via gebrochener linearer Transformation auf  $\mathbb{P}^1(\mathbb{C})$ .*

BEWEIS. Dies rechnet man elementar nach.  $\square$

Sei  $\Gamma < \mathrm{SL}_2(\mathbb{R})$  im Folgenden eine diskrete Untergruppe und wirke  $\Gamma$  auf  $\mathbb{P}^1(\mathbb{C})$  via gebrochener linearer Transformation.

**2.2.3 Definition.** Sei  $\sigma \in \Gamma \setminus \{\pm 1\}$ . Wir nennen  $\sigma$  genau dann

- *parabolisch*, wenn  $\sigma$  genau einen Fixpunkt in  $\mathbb{R} \cup \{\infty\}$  besitzt,
- *elliptisch*, wenn die Fixpunkte von  $\sigma$  gegeben sind durch  $\zeta, \bar{\zeta}$  für ein  $\zeta \in \mathcal{H}$ ,
- *hyperbolisch*, wenn  $\sigma$  zwei Fixpunkte in  $\mathbb{R} \cup \{\infty\}$  besitzt.

Wir nennen Punkte  $\zeta \in \mathbb{P}^1(\mathbb{C})$ , für die es ein parabolisches (resp. elliptisches) Element  $\sigma \in \Gamma$  mit  $\sigma\zeta = \zeta$  gibt, *Spitzen* (resp. *elliptische Punkte*).

**2.2.4 Proposition ([Shi94, Prop. 1.16, 1.17]).** Sei  $\zeta \in \mathbb{P}^1(\mathbb{C})$  und bezeichne den Stabilisator von  $\zeta$  unter  $\Gamma$  mit  $\Gamma_\zeta := \{\sigma \in \Gamma : \sigma\zeta = \zeta\}$ .

- Sei  $\zeta \in \mathcal{H}$  ein elliptischer Punkt. Dann ist der Stabilisator  $\Gamma_\zeta$  eine endliche zyklische Gruppe. Wir nennen die Zahl  $|\Gamma_\zeta| \in \mathbb{N}$  die Ordnung des elliptischen Punkts  $\zeta$ .
- Sei  $\zeta \in \mathbb{R} \cup \{\infty\}$  eine Spitze. Dann ist  $\Gamma_\zeta / (\Gamma \cap \{\pm 1\})$  isomorph zu  $\mathbb{Z}$ .

**2.2.5 Definition.** Sei  $\Gamma < \mathrm{SL}_2(\mathbb{R})$  eine diskrete Untergruppe. Wir definieren die *erweiterte obere Halbebene* als

$$\mathcal{H}^* := \mathcal{H} \cup \{\text{Spitzen von } \Gamma\}.$$

**2.2.6 Satz ([Shi94, §1.5]).** Sei  $\Gamma$  eine diskrete Untergruppe von  $\mathrm{SL}_2(\mathbb{R})$ . Dann wirkt  $\Gamma$  auf  $\mathcal{H}^*$  und es existiert eine komplexe Struktur auf  $X := \mathcal{H}^*/\Gamma$ , so dass  $X$  eine Riemannsche Fläche ist.

**2.2.7 Definition.** Wir nennen eine diskrete Untergruppe  $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$  eine *Fuchssche Gruppe der ersten Art*, falls  $\mathcal{H}^*/\Gamma$  eine kompakte Riemannsche Fläche ist.

**2.2.8 Bemerkung.** Falls  $\mathcal{X} := \mathcal{H}^*/\Gamma$  kompakt ist, kann man auf  $\mathcal{X}$  ein Radon-Maß einführen, das *hyperbolische Volumen*  $\mathrm{vol}(\mathcal{X})$ . Wir möchten dies nicht ausführen. Eine Definition wird in [Shi94, §2.5] gegeben. In der Literatur wird das hyperbolische Volumen  $\mathrm{vol}(\mathcal{X})$  häufig benutzt um eine äquivalente Definition der Fuchsschen Gruppen zu geben. Es gilt nämlich für eine diskrete Untergruppe  $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ , dass  $\mathcal{H}^*/\Gamma$  genau dann kompakt ist, wenn  $\mathrm{vol}(\mathcal{X})$  endlich ist ([Shi94, §2.5]). Folglich ist  $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$  eine Fuchssche Gruppe, falls  $\mathcal{H}^*/\Gamma$  endliches Volumen  $\mathrm{vol}(\mathcal{X})$  hat.

**2.2.9 Bemerkung.** Sei  $\zeta \in \mathcal{H}$  ein elliptischer Punkt (bzw. eine Spitze). Wir nennen das Bild  $[\zeta] \in \mathcal{H}^*/\Gamma$  unter der Quotientenabbildung ebenfalls elliptischen Punkt (bzw. Spitze).

**2.2.10 Proposition ([Shi94, Prop. 2.20]).** Bezeichne  $\mathcal{X} := \mathcal{H}^*/\Gamma$ , wobei  $\Gamma < \mathrm{SL}_2(\mathbb{R})$  eine Fuchssche Gruppe der ersten Art sei. Bezeichne mit  $m \in \mathbb{N}$  die Anzahl der Spitzen von  $\mathcal{X}$  und mit  $e_j \in \mathbb{N}$  die Ordnungen der elliptischen Punkte von  $\mathcal{X}$ . Dann hat  $\mathcal{X}$  endliches hyperbolisches Volumen  $\mathrm{vol}(\mathcal{X})$  (Bemerkung 2.2.8). Für das Geschlecht  $g$  von  $\mathcal{X}$  gilt:

$$2g - 2 = \mathrm{vol}(\mathcal{X}) - \sum_j \left(1 - \frac{1}{e_j}\right) - m.$$

**2.2.11 Definition.** Sei  $\Gamma < \mathrm{SL}_2(\mathbb{R})$  eine Fuchssche Gruppe der ersten Art. Bezeichne mit  $x_i \in \mathcal{H}^*$  die elliptischen Punkte und die Spitzen von  $\Gamma$ . Wir nennen  $\Gamma$  eine *Dreiecksgruppe*, falls  $\mathcal{X} := \mathcal{H}^*/\Gamma$  von Geschlecht  $g = 0$  ist und die Anzahl der elliptischen Punkte zusammen mit der Anzahl der Spitzen 3 ist. Falls  $x_i$  ein elliptischer Punkt ist, bezeichne  $e_i$  die Ordnung von  $x_i$ . Falls  $x_i$  eine Spitze ist, setzen wir  $e_i := \infty$ . Dann schreiben wir  $\Gamma = \Delta(e_1, e_2, e_3)$  für die Dreiecksgruppe.

**2.2.12 Definition.** Wir nennen zwei Untergruppen  $G_1, G_2$  einer Gruppe  $G$  *kommensurabel*, falls ihr Schnitt  $G_1 \cap G_2$  endlichen Index in  $G_1$  und  $G_2$  hat.

Sei  $D$  eine Quaternionenalgebra über einem Zahlkörper  $F$ . Sei  $\mathcal{O}$  eine  $\mathcal{O}_F$ -Ordnung und sei  $\mathcal{O}^1 := \{h \in \mathcal{O}^* : \mathrm{n}(h) = 1\}$ . Sei  $\mathcal{O}^1 \hookrightarrow \mathrm{SL}_2(\mathbb{R})$  eine Einbettung und  $\Gamma_{\mathcal{O}} < \mathrm{SL}_2(\mathbb{R})$  ihr Bild.

**2.2.13 Definition.** Sei  $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$  eine Fuchssche Gruppe der ersten Art. Wir nennen  $\Gamma$  *arithmetisch*, falls  $\Gamma$  kommensurabel zu einer Gruppe  $\Gamma_{\mathcal{O}}$  wie oben ist.

**2.2.14 Definition.** Sei  $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$  eine arithmetische Fuchssche Gruppe der ersten Art. Dann nennen wir den Quotienten  $\mathcal{H}^*/\Gamma$  eine *Shimura-Kurve*.

**2.2.15 Bemerkung.** Dies ist die Definition einer Shimura-Kurve über  $\mathbb{C}$ . Man kann diese über beliebigen Körpern definieren. Dazu siehe zum Beispiel [Möl05, Definition 1.1] und [Del71].

## 2.3 Shimura-Kurve $\mathcal{X}(1)$ : Definition und Algebraisierbarkeit

Sei  $D$  eine indefinite Quaternionenalgebra über  $\mathbb{Q}$  und  $\mathcal{O}_D$  eine maximale Ordnung. In Abschnitt 2.2 haben wir gesehen, dass die Gruppe  $\mathcal{O}_D^1$  (Defi-

tion 1.3.5) eine Shimura-Kurve  $\mathcal{X}(1)$  (Definition 2.2.14) über  $\mathbb{C}$  definiert. In diesem Abschnitt zitieren wir bekannte Ergebnisse für  $\mathcal{X}(1)$ . Insbesondere korrespondieren die Punkte von  $\mathcal{X}(1)$  zu hauptpolarisierten abelschen Flächen vom Typ  $\mathcal{QM}$  (Satz 2.3.6). Wir benutzen diese Modulbeschreibung um  $\mathcal{X}(1)$  in Kapitel 4 weiter zu untersuchen.

Sei  $D$  eine indefinite verzweigte Quaternionenalgebra über  $\mathbb{Q}$ , d.h. es gilt  $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$  und  $D$  ist nicht isomorph zur Matrixalgebra  $M_2(\mathbb{Q})$ . Bezeichne  $\emptyset \neq \Sigma \subset \mathbb{N}$  die Menge der Primteiler von  $\text{disc}(D)$ . Sei  $\mathcal{O}_D$  die (bis auf Konjugation eindeutige) maximale Ordnung in  $D$ . Bezeichne

$$\mathcal{O}_D^1 := \{h \in \mathcal{O}_D : n(h) = 1\}, \tag{2.2}$$

$$\text{Nor}(\mathcal{O}_D) := \{[h] \in D^* : n(h) > 0, h\mathcal{O}_D = \mathcal{O}_D h\} \tag{2.3}$$

wie in Definition 1.3.5 (bzw. 1.3.3).

Sei eine Einbettung  $\theta : D \hookrightarrow M_2(\mathbb{R})$ , gegeben. Diese Einbettung ist eindeutig bis auf Konjugation. Mittels der Einbettung  $\theta$  kann man die Gruppen  $\mathcal{O}_D^1$  und  $\text{Nor}(\mathcal{O}_D)$  als diskrete Untergruppen von  $SL_2(\mathbb{R})$  auffassen. Wir bezeichnen diese Untergruppen von  $SL_2(\mathbb{R})$  mit

$$\Gamma(1) := \theta(\mathcal{O}_D^1),$$

$$\Gamma^*(1) := \theta(\text{Nor}(\mathcal{O}_D)/\mathbb{Q}^*).$$

**2.3.1 Satz ([Shi94, Prop. 9.2]).** *Die Gruppen  $\Gamma(1)$  (resp.  $\Gamma^*(1)$ ) sind arithmetische Fuchsische Gruppen. Es existieren keine parabolischen Elemente  $\sigma$  in  $\Gamma(1)$  (resp.  $\Gamma^*(1)$ ).*

**2.3.2 Definition.** Wir definieren die Shimura-Kurven  $\mathcal{X}(1)$  und  $\mathcal{X}^*(1)$  als die Quotienten  $\mathcal{X}(1) := \mathcal{H}/\Gamma(1)$  und  $\mathcal{X}^*(1) := \mathcal{H}/\Gamma^*(1)$ . Diese Quotienten sind nach Satz 2.3.1 kompakte Riemannsche Flächen.

**2.3.3 Proposition ([Vig80, Abschnitt IV.3.A]).** *Das hyperbolische Volumen von  $\mathcal{X}(1)$  ist gegeben durch*

$$\text{vol}(\mathcal{X}(1)) = \frac{1}{6} \prod_{p|\text{disc}(D)} (p-1).$$

*Es gibt nur elliptische Punkte von Ordnung 2 und 3 und die Anzahl  $n_2$  (bzw.  $n_3$ ) der elliptischen Punkte von Ordnung 2 (bzw. Ordnung 3) sind*

$$n_2 = \prod_{p|\text{disc}(D)} \left(1 - \left(\frac{-4}{p}\right)\right), \quad n_3 = \prod_{p|\text{disc}(D)} \left(1 - \left(\frac{-3}{p}\right)\right).$$

Das Geschlecht  $g$  von  $\mathcal{X}(1)$  ist gegeben durch

$$g = 1 + \frac{\text{vol}(\mathcal{X}(1))}{2} - \frac{n_2}{4} - \frac{n_3}{3}.$$

**2.3.4 Beispiel.** Sei  $D$  die Quaternionenalgebra über  $\mathbb{Q}$  mit Diskriminante  $\text{disc}(D) = 6$ . In der Notation von Proposition 2.3.3 gilt

$$\text{vol}(\mathcal{X}(1)) = \frac{1}{3}, \quad n_2 = 2, \quad n_3 = 2.$$

Das Geschlecht von  $\mathcal{X}(1)$  ist somit  $g = 0$ .

Die Kurve  $\mathcal{X}(1)$  ist eine Überlagerung von  $\mathcal{X}^*(1)$ . Tatsächlich gilt nämlich folgende Proposition 2.3.5. Diese werden wir in Satz 2.7.12 benutzen um zu zeigen, dass eine Korrespondenz zwischen den CM-Punkten auf  $\mathcal{X}(1)$  (2.7.4) und den CM-Punkten auf der Modulkurve  $X(1)$  existiert.

**2.3.5 Proposition ( [Vig80, § IV.3.B] ).** Die Gruppe  $\Gamma(1)$  ist eine normale Untergruppe von  $\Gamma^*(1)$  von Index  $2^{|\Sigma|}$ . Der Quotient  $\Gamma(1)/\Gamma^*(1)$  ist eine elementarabelsche 2-Gruppe. Die Elemente von  $\Gamma^*(1)/\Gamma(1)$  korrespondieren zu den Klassen  $[h]$  von Elementen  $h \in D$ , für die  $\mathfrak{n}(h) = \prod_{p \in \Sigma'} p$  für eine Untermenge  $\Sigma' \subset \Sigma$  gilt.

In [Shi67, §4] und [Shi63, §2] wird beschrieben, wie die Shimura-Kurve  $\mathcal{X}(1)$  polarisierte abelsche Flächen  $A$  mit Einbettungen  $\mathcal{O}_D \hookrightarrow \text{End}(A)$  parametrisiert.

**2.3.6 Satz ( [Shi67, Thm. 4.20], [Shi63, Thm. 1] ).** Es gibt eine Bijektion zwischen den Punkten  $\zeta \in \mathcal{X}(1)$  und den Isomorphieklassen hauptpolarisierter abelscher Flächen mit  $\mathcal{QM}$  durch  $\mathcal{O}_D$ .

Die Shimura-Kurven  $\mathcal{X}(1)$  und  $\mathcal{X}^*(1)$  sind algebraisierbar.

**2.3.7 Satz ( [Shi67, Thm. 4.20], auch [Shi94, Thm. 9.6] ).** Es existieren Modelle von  $\mathcal{X}(1)$  und  $\mathcal{X}^*(1)$  als projektive algebraische Kurven über dem Zahlkörper  $\mathbb{Q}$ .

**2.3.8 Bemerkung.** Wir bezeichnen diese algebraischen Kurven ebenfalls mit  $\mathcal{X}(1)$  und  $\mathcal{X}^*(1)$ .

## 2.4 Abelsche Flächen vom Typ $\mathcal{QM}$ mit komplexer Multiplikation

Proposition 2.1.8 impliziert, dass eine abelsche Fläche  $A$  vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation nicht absolut einfach ist. D.h. über einer

Erweiterung des Definitionskörpers ist  $A$  isogen zum Produkt isogener elliptischer Kurven. Wir konstruieren zu einer gegebenen Idempotenten  $e \in \text{End}^0(A)$  mit bestimmten Eigenschaften (Notation 2.4.6) eindeutige elliptische Kurven  $E_e, E_{\bar{e}}$  und eine explizite Isogenie  $\psi : A \rightarrow E_e \times E_{\bar{e}}$  (Theorem 2.4.12).

**2.4.1 Notation.** Sei  $D$  eine indefinite Quaternionenalgebra über  $\mathbb{Q}$  und  $\mathcal{O}_D$  in  $D$  eine maximale Ordnung. Sei  $F$  ein Körper der Charakteristik  $\text{char}(F) \neq 2$  und  $A$  eine abelsche Fläche vom Typ  $\mathcal{QM}$  durch  $\psi_{\mathcal{QM}} : \mathcal{O}_D \hookrightarrow \text{End}(A)$  über  $F$ . Sei  $\lambda : A \rightarrow A^t$  eine Hauptpolarisierung. Dann liefert  $\lambda$  eine Involution auf  $\text{End}(A)$  und durch Einschränken eine Involution auf  $\mathcal{O}_D$ , die wir mit  $a \mapsto a^\dagger$  bezeichnen (siehe Bemerkung 2.1.7). Wir nehmen an, dass die Polarisation  $\lambda : A \rightarrow A^t$  und alle Endomorphismen von  $A$  über  $F$  definiert sind.

**2.4.2 Bemerkung.** Angenommen  $A$  habe zusätzlich komplexe Multiplikation im Sinne von Definition 2.1.5. Dann impliziert Proposition 2.1.8, dass  $A$  isogen zum Produkt  $E^2$  einer elliptischen Kurve  $E$  mit komplexer Multiplikation durch einen imaginär quadratischen Körper  $K$  ist. Die Quaternionenalgebra  $D$  lässt sich in  $\text{End}^0(A) \simeq M_2(K)$  einbetten und folglich ist  $K$  ein Zerfällungskörper von  $D$ .

**2.4.3 Notation.** Wir nehmen an,  $A$  habe komplexe Multiplikation und es gelte  $\text{End}^0(A) \simeq M_2(K)$  für einen imaginär quadratischen Zerfällungskörper  $K = \mathbb{Q}(\alpha)$  mit  $\alpha^2 = -d \in \mathbb{Z}_{<0}$  quadratfrei.

Sei

$$\varepsilon : \text{End}^0(A) \xrightarrow{\sim} D \otimes_{\mathbb{Q}} K$$

ein Isomorphismus, so dass folgendes Diagramm kommutiert:

$$\begin{array}{ccc} D & \xrightarrow{\psi_{\mathcal{QM}}} & \text{End}^0(A) \\ & \searrow \text{can} & \downarrow \varepsilon \\ & & D \otimes_{\mathbb{Q}} K. \end{array} \tag{2.4}$$

**2.4.4 Proposition.** *Es existieren genau 2 Isomorphismen*

$$\varepsilon_1, \varepsilon_2 : \text{End}^0(A) \longrightarrow D \otimes_{\mathbb{Q}} K,$$

die das Diagramm (2.5) kommutativ machen. Dabei ist  $\varepsilon_2$  die Verknüpfung von  $\varepsilon_1$  mit der komplexen Konjugation in  $\mathbb{Q} \otimes_{\mathbb{Q}} K$ .

**BEWEIS.** Seien  $\varepsilon_1, \varepsilon_2 : \text{End}^0(A) \rightarrow D \otimes_{\mathbb{Q}} K$  zwei Isomorphismen, die das

Diagramm (2.5) kommutativ machen. Wir definieren den Isomorphismus

$$\kappa := \varepsilon_2 \circ \varepsilon_1^{-1} : D \otimes_{\mathbb{Q}} K \rightarrow D \otimes_{\mathbb{Q}} K.$$

Nach der Definition der Isomorphismen  $\varepsilon_i$  ist die Einschränkung von  $\kappa$  auf  $D \otimes_{\mathbb{Q}} \mathbb{Q}$  die Identität auf  $D \otimes_{\mathbb{Q}} \mathbb{Q}$ . Für den Morphismus  $\kappa$  muss damit

$$\kappa(d \otimes \alpha) = (d \otimes 1)\kappa(1 \otimes \alpha) = \kappa(1 \otimes \alpha)(d \otimes 1)$$

gelten und folglich ist  $\kappa(1 \otimes \alpha) \in \text{Zentrum}(D \otimes_{\mathbb{Q}} K) = \mathbb{Q} \otimes_{\mathbb{Q}} K$ . Aus der Identität  $\kappa(1 \otimes \alpha)^2 = d \otimes 1$  folgt  $\kappa(1 \otimes \alpha) = \pm 1 \otimes \alpha$ .  $\square$

Bezeichne nun  $\varepsilon : \text{End}^0(A) \rightarrow D \otimes_{\mathbb{Q}} K$  den (bis auf Konjugation) eindeutigen Isomorphismus aus Prop. 2.4.4.

**2.4.5 Proposition.** *Das Zentrum von  $\text{End}(A)$  ist mittels  $\varepsilon$  isomorph zu  $\mathbb{Z} \otimes_{\mathbb{Z}} \mathcal{O}_{K,c}$  für eine Ordnung  $\mathcal{O}_{K,c}$  von  $K$  mit Führer  $c \in \mathbb{N}$ . Somit definiert*

$$\varepsilon^{-1} : \mathcal{O}_D \otimes_{\mathbb{Z}} \mathcal{O}_{K,c} \hookrightarrow \text{End}(A)$$

eine Einbettung.

BEWEIS. Es ist offensichtlich, dass das Zentrum einer  $\mathbb{Z}$ -Ordnung wiederum eine  $\mathbb{Z}$ -Ordnung ist. Der Endomorphismenring  $\text{End}(A)$  ist eine Ordnung in  $\text{End}^0(A)$ . Somit ist  $\text{Zentrum}(\text{End}(A))$  eine Ordnung in  $\varepsilon^{-1}(\mathbb{Q} \otimes_{\mathbb{Q}} K)$ , dem Zentrum von  $\text{End}^0(A)$ . Die Behauptung der Proposition folgt unmittelbar.  $\square$

**2.4.6 Notation.** Sei nun die Ordnung  $\mathcal{O}_{K,c}$  mit Führer  $c \in \mathbb{N}$  wie in Proposition 2.4.5 gegeben, d.h.  $\text{Zentrum}(\text{End}(A)) \simeq \mathcal{O}_{K,c}$ . Sei

$$\iota : K \hookrightarrow D$$

eine optimale Einbettung von  $\mathcal{O}_{K,c}$  in  $\mathcal{O}_D$ , d.h. es gelte  $\mathcal{O}_{K,c} = \iota^{-1}(\mathcal{O}_D)$ . Bezeichne mit

$$e = \frac{1}{2}(1 \otimes 1 + \iota(\alpha)^{-1} \otimes \alpha) \in D \otimes_{\mathbb{Q}} K \tag{2.5}$$

die zu  $\iota$  gehörende Idempotente nach Proposition 1.2.14.

**2.4.7 Definition.** Sei  $A$  eine abelsche Varietät und  $I \subsetneq \text{End}(A)$  ein Ideal in  $\text{End}(A)$ . Wir definieren das *Torsionsuntergruppenschema* bzgl.  $I$  als das Untergruppenschema

$$A[I] := \bigcap_{\gamma \in I} \ker \gamma.$$

**2.4.8 Lemma.** Sei  $A$  eine abelsche Varietät, nicht notwendigerweise einfach, und  $I \subsetneq \text{End}(A)$  ein Ideal. Genau dann existiert eine Isogenie  $\gamma \neq 0$  in  $I$ , wenn  $I$  ein Gitter in  $\text{End}(A)$  ist.

BEWEIS. Sei  $I$  ein Gitter und  $\tilde{\beta} \in \text{End}(A)$  eine Isogenie. Dann existieren  $n \in \mathbb{N} \setminus \{0\}$  und  $\beta \in I$ , so dass  $\beta = \tilde{\beta} \circ [n]$  gilt. Daraus folgt die Gleichheit  $\ker \beta = \ker(\tilde{\beta} \circ [n])$  und somit ist  $\beta \in I \setminus \{0\}$  eine Isogenie.

Sei umgekehrt  $\beta \in I \setminus \{0\}$  eine Isogenie und  $n := \deg \beta$ . Dann existiert ein  $\tilde{\beta} \in \text{End}(A)$ , so dass die Isogenie  $[n]$  faktorisiert als  $[n] = \tilde{\beta} \circ \beta$ . Somit gilt  $[n] = \tilde{\beta} \circ \beta \in I$  und folglich auch  $I \otimes \mathbb{Q} \simeq \text{End}^0(A)$ .  $\square$

**2.4.9 Bemerkung.** Falls  $A$  eine einfache abelsche Varietät ist, sind alle nicht-trivialen Endomorphismen Isogenien, und somit ist  $I$  genau dann ein Gitter wenn  $I$  nicht trivial ist.

**2.4.10 Lemma.** Sei  $A$  eine abelsche Varietät und  $I \subsetneq \text{End}(A)$  ein Ideal.

- (i) Ist  $I$  ein Gitter in  $\text{End}(A)$ , so ist das Untergruppenschema  $A[I]$  endlich.
- (ii) Ist  $A[I]$  endlich, so ist das Ideal  $J = \{\beta \in \text{End}(A) : \beta A[I] = 0\} \supset I$  ein Gitter.

BEWEIS. Ist  $I$  ein Gitter, dann existiert nach Lemma 2.4.8 eine nicht-triviale Isogenie  $\beta \in I$  und folglich ist  $A[I] \subset \ker \beta$  endlich.

Ist  $n := |A[I]|$  endlich, dann gilt  $A[I] \subset \ker [n]$  und somit gilt  $[n] \in J$ . Folglich ist  $J$  ein Gitter nach Lemma 2.4.8. Die Relation  $I \subset J$  gilt nach der Definition des Torsionsuntergruppenschemas  $A[I]$ .  $\square$

Die nächste Proposition liefert eine explizite Konstruktion des Quotienten  $A/A[I]$ . Für weitere Details sei auf [Shi98, §7] verwiesen.

**2.4.11 Proposition ( [Shi98, §7, Prop. 7],[Wat69, § 3.2] ).** Sei  $A$  eine abelsche Varietät und  $I \subsetneq \text{End}(A)$  ein Gitter. Seien  $(\gamma_i)_i \subset \text{End}(A)$  Erzeuger von  $I$  über  $\text{End}(A)$ , dann definiert

$$\begin{aligned} \psi &:= (\gamma_i)_i : A \longrightarrow \prod_i \text{Im } \gamma_i, \\ P &\longmapsto (\gamma_i(P))_i \end{aligned}$$

eine Isogenie mit  $\ker \psi = A[I]$ . Folglich gilt  $\prod_i \text{Im } \gamma_i \simeq A/A[I]$  als abelsche Varietäten. Sind  $A$  und alle  $\gamma \in I$  über  $F$  definiert, dann ist auch  $\psi$  über  $F$  definiert.

Wir konstruieren eine explizite Isogenie

$$A \rightarrow E_e \times E_{\bar{e}}.$$

Dazu erinnern wir an unsere Bezeichnungen. Gegeben ist die abelsche Fläche  $A$  vom Typ  $\mathcal{QM}$  durch  $D$  und die Einbettung  $\iota : \mathcal{O}_{K,c} \hookrightarrow \mathcal{O}_D$ . Dann existiert nach Satz 1.2.4 ein  $u \in D$ , so dass  $D = \iota(K) + u\iota(K)$ ,  $u^2 \in \mathbb{Q}$  und  $ux = \bar{x}u$  für alle  $x \in \iota(K)$  gilt. Sei ein solches Element  $u \in \mathcal{O}_D$  gewählt.

Das Element  $e := e_\iota = \frac{1}{2}(1 \otimes 1 + \iota(\alpha)^{-1} \otimes \alpha) \in D \otimes_{\mathbb{Q}} K$  bezeichne die zu  $\iota$  gehörige Idempotente. Die zu  $\bar{\iota}$  gehörende Idempotente  $e_{\bar{\iota}}$  ist nach Proposition 1.2.16 gegeben durch  $e_{\bar{\iota}} = \bar{e} = 1 - e$ .

**2.4.12 Theorem.** Sei  $\eta \in \iota(\mathcal{O}_{K,c})$ , so dass  $e\eta \in \text{End}(A)$  ist. Dann existieren isogene elliptische Kurven  $E_e, E_{\bar{e}}$  vom Typ CM durch  $\mathcal{O}_{K,c}$  und eine Isogenie

$$\psi_{e\eta} : A \rightarrow E_e \times E_{\bar{e}},$$

von Grad  $\deg \psi_{e\eta} \mid \deg \eta$ .

BEWEIS. Wir definieren  $I = \langle e\eta, \bar{e}\eta \rangle$  als das ganze Ideal in  $\text{End}(A)$  erzeugt von  $e\eta$  und  $\bar{e}\eta$ . Da  $\eta = e\eta + \bar{e}\eta \in I \subsetneq \text{End}(A)$  eine Isogenie definiert, ist  $I$  nach Lemma 2.4.8 ein Gitter. Somit definiert  $I$  nach Lemma 2.4.11 eine Isogenie  $\psi_{e\eta} : A \rightarrow A'$  mit  $\ker \psi_{e\eta} = A[I] \subset \ker \eta$ . Insbesondere folgt  $\deg \psi_{e\eta} \mid \deg \eta$ .

Das Ideal  $eI = \langle e\eta \rangle < \text{End}(A)$  ist kein Gitter, da  $e \neq 1$  eine Idempotente ist, also zu einer Projektion gehört. Dies impliziert dass  $A \rightarrow A/A[eI]$  keine Isogenie ist. Also ist  $A/A[eI]$  eine abelsche Varietät von Dimension  $\leq 1$ . Da aber  $eI \neq \{0\}$  gilt, ist  $E_e := A/A[eI]$  eine elliptische Kurve. Analog definiert man die elliptische Kurve  $E_{\bar{e}} := A/A[\bar{e}I]$ . Damit definiert das Gitter  $I \subset \text{End}(A)$  nach Lemma 2.4.11 eine Isogenie

$$\psi_{e\eta} : A \rightarrow E_e \times E_{\bar{e}}.$$

Wir möchten nun zeigen, dass  $E_e \simeq E_{\bar{e}}$  gilt. Dazu betrachten wir zunächst  $\text{End}(E_e)$ . Die Endomorphismen  $\beta \in \text{End}(A)$ , die mit  $e\eta \in \text{End}(A)$  kommutieren, also  $E_e$  auf sich selbst abbilden, sind  $\psi^{-1}(\beta) \in \iota(\mathcal{O}_{K,c}) \otimes \mathcal{O}_{K,c}$ . Folglich gilt  $\mathcal{O}_{K,c} \simeq \text{End}(E_e)$ . Analog gilt  $\mathcal{O}_{K,c} \simeq \text{End}(E_{\bar{e}})$ .

Für das Element  $u \in \mathcal{O}_D$  gilt  $u\bar{e}\eta = e\eta u$ , d.h. folgendes Diagramm kommutiert

$$\begin{array}{ccc} A & \xrightarrow{e\eta} & E_e \\ \downarrow u & & \downarrow u|_{E_e} \\ A & \xrightarrow{\bar{e}\eta} & E_{\bar{e}}. \end{array} \tag{2.6}$$

Dies liefert eine explizite Isogenie  $u|_{E_e} : E_e \rightarrow E_{\bar{e}}$ . □

Im Folgenden wollen wir Aussagen über die Eindeutigkeit der elliptischen Kurven  $E_e$  und  $E_{\bar{e}}$  treffen.

**2.4.13 Lemma.** Seien  $\eta, \eta' \in \iota(\mathcal{O}_{K,c})$ , so dass  $e\eta, e\eta' \in \text{End}(A)$  ist. Bezeichne

$$\begin{aligned}\psi_{e\eta} &: A \rightarrow E_e \times E_{\bar{e}}, \\ \psi_{e\eta'} &: A \rightarrow E'_e \times E'_{\bar{e}}\end{aligned}$$

die zugehörigen Isogenien aus Satz 2.4.12. Dann gilt  $E_e \simeq E'_e$  und  $E_{\bar{e}} \simeq E'_{\bar{e}}$ .

BEWEIS. Es gilt o.B.d.A.  $\eta' = \beta\eta$  für ein  $\beta \in \iota(\mathcal{O}_K)$  und folglich  $e\eta' = e\eta \cdot e\beta$ . Es ist  $e\eta \in \text{End}(E_e)$  und  $e\eta' \in \text{End}(E'_e)$ . Somit definiert  $e\beta$  eine Isogenie  $e\beta : E_e \rightarrow E'_e$ . Es existiert ein  $N \in \mathbb{N}$ , so dass  $[N] \circ e\beta \in \text{End}(E_e)$  ist:

$$E_e \xrightarrow{e\beta} E'_e \xrightarrow{[N]} E_e.$$

Folglich gilt  $E'_e/E'_e[N] \simeq E_e$  und somit sind  $E_e$  und  $E'_e$  isomorph. Analog gilt  $E_{\bar{e}} \simeq E'_{\bar{e}}$ .  $\square$

**2.4.14 Lemma.** Seien  $\iota, \iota' : K \hookrightarrow D$  zwei äquivalente Einbettungen im Sinne von Definition 1.3.9, d.h. es existiert ein  $h \in \mathcal{O}_D^1$ , so dass  $\iota'(x) = h\iota(x)h^{-1}$  für alle  $x \in K$  gilt. Bezeichne mit  $e, e' \in D \otimes_{\mathbb{Q}} K$  die korrespondierenden Idempotenten. Seien  $\eta, \eta' \in \iota(\mathcal{O}_{K,c})$  so gewählt, dass  $e\eta, e'\eta' \in \text{End}(A)$  ist. In der Bezeichnung von Satz 2.4.12 gilt dann  $E_e \simeq E_{e'}$  und  $E_{\bar{e}} \simeq E_{\bar{e}'}$ .

BEWEIS. Sei  $h \in \mathcal{O}_D^1$  so gewählt, dass  $\iota'(x) = h\iota(x)h^{-1}$  für alle  $x \in K$  gilt. Zu  $h$  korrespondiert ein Isomorphismus  $A \xrightarrow{\sim} A$ . Da  $e \circ (h \otimes 1) = (h \otimes 1) \circ e'$  ist, liefert die Einschränkung von  $h$  auf  $E_e$  (bzw.  $E_{\bar{e}}$ ) einen Isomorphismus  $E_e \simeq E_{e'}$  (bzw.  $E_{\bar{e}} \simeq E_{\bar{e}'}$ ).  $\square$

**2.4.15 Proposition.** Es existiert  $\eta \in \iota(\mathcal{O}_{K,c})$  mit  $e\eta \in \text{End}(A)$ , so dass für die Isogenie  $\psi_{e\eta} : A \rightarrow E_e \times E_{\bar{e}}$  aus Satz 2.4.12 gilt, dass

$$\deg \psi_{e\eta} \mid (4c^2 \cdot \text{disc}(K)).$$

BEWEIS. Angenommen es gilt  $4 \mid \text{disc}(K)$ . Dann ist  $\mathcal{O}_{K,c} = \mathbb{Z} \oplus c\alpha\mathbb{Z}$ . Für  $\eta := 2c\alpha \in \mathcal{O}_{K,c}$  folgt, dass  $e\eta = c\alpha \otimes 1 + 1 \otimes c\alpha \in \mathcal{O}_{K,c} \otimes \mathcal{O}_{K,c}$  gilt. Nach Proposition 2.4.5 ist somit  $e\eta \in \text{End}(A)$ . Es gilt  $\mathfrak{n}(\eta) = 4c^2d = c^2 \cdot \text{disc}(K)$  und folglich  $\deg \eta = c^2 \cdot \text{disc}(K)$ . Mit der Teilbarkeitsbedingung  $\deg \psi_{e\eta} \mid \deg \eta$  aus der Aussage von Satz 2.4.12 folgt somit die Behauptung.

Angenommen es gilt  $4 \nmid \text{disc}(K)$ . Dann ist  $\mathcal{O}_{K,c} = \mathbb{Z} \oplus c\frac{1+\alpha}{2}\mathbb{Z}$ . Für  $\eta := 2c\alpha \in \mathcal{O}_{K,c}$  gilt ebenso  $e\eta \in \text{End}(A)$ . Die Aussage folgt dann aus der Identität  $\deg \eta = 4c^2 \cdot \text{disc}(K)$ .  $\square$

**2.4.16 Bemerkung.** Man kann die elliptische Kurve  $E_e$  (bzw.  $E_{\bar{e}}$ ) nach Proposition 2.4.11 auch als Bild unter der Abbildung  $e\eta$  (bzw.  $\bar{e}\eta$ ) auffassen. Man betrachtet also  $E_e$  (bzw.  $E_{\bar{e}}$ ) als Untervarietät von  $A$ . Die duale

Isogenie  $\psi_{e\eta}^D$  von  $\psi_{e\eta}$  ist dann gegeben durch

$$\begin{aligned} E_e \times E_{\bar{e}} &\longrightarrow A \\ (x, y) &\longmapsto \eta^D(x) + \bar{\eta}^D(y). \end{aligned}$$

Ein Isomorphismus  $\varepsilon : \text{End}^0(A) \rightarrow D \otimes_{\mathbb{Q}} K$  aus Proposition 2.4.4 induziert durch die positive Involution  $\dagger$  auf  $\text{End}^0(A)$  eine positive Involution auf  $D \otimes_{\mathbb{Q}} K$ . Die Proposition 2.4.4 impliziert, dass diese unabhängig von der Wahl des Isomorphismus  $\varepsilon$  ist. Diese Involution auf  $D \otimes_{\mathbb{Q}} K$  sei ebenfalls mit  $\dagger$  bezeichnet. Das folgende Lemma beschreibt die Involution  $\dagger$  auf  $D \otimes_{\mathbb{Q}} K$  in Termen der kanonischen Einbettung  $D \hookrightarrow D \otimes_{\mathbb{Q}} K$ .

**2.4.17 Lemma ([Knu91, Thm. 9.3.5]).** *Sei  $\dagger$  eine positive Involution auf  $D$ . Dann existiert eine eindeutige Fortsetzung von  $\dagger$  zu einer positiven Involution auf  $D \otimes_{\mathbb{Q}} K$ . Sei  $\alpha \in K \setminus \mathbb{Q}$  mit  $\alpha^2 \in \mathbb{Q}$ , dann ist die Involution gegeben durch  $(h \otimes \alpha) \mapsto h^{\dagger} \otimes \bar{\alpha}$ .*

**2.4.18 Bemerkung.** Es sei daran erinnert, dass die positive Involution  $\dagger : D \rightarrow D$  nicht der Konjugation (Lemma 1.1.14) in  $D$  entspricht.

**2.4.19 Bemerkung.** Die Polarisierung von  $A$  entspricht nicht der durch das Produkt  $E_e \times E_{\bar{e}}$  induzierten Polarisierung. Denn wäre die Polarisierung auf  $A$  durch die auf dem Produkt  $E_e \times E_{\bar{e}}$  induziert, so müsste die Involution auf  $\text{End}(E)$  der Konjugation entsprechen. Insbesondere würde dies bedeuten, dass für die Idempotente  $e \in D \otimes_{\mathbb{Q}} K$  die Identität  $e^{\dagger} = \bar{e}$  gilt. Mit Lemma 2.4.17 berechnen wir

$$\begin{aligned} e^{\dagger} &= \frac{1}{2}(1 \otimes 1 + \iota(\alpha^{-1}) \otimes \alpha)^{\dagger} \\ &= \frac{1}{2}(1 \otimes 1 + \iota(\alpha^{-1})^{\dagger} \otimes \bar{\alpha}) \\ &\stackrel{!}{=} \frac{1}{2}(1 \otimes 1 - \iota(\alpha^{-1}) \otimes \alpha) = \bar{e} \end{aligned}$$

Da  $\bar{\alpha} = -\alpha$  gilt, muss  $\iota(\alpha)^{\dagger} = \iota(\alpha)$  erfüllt sein. Dies ist aber ein Widerspruch dazu, dass  $\dagger$  eine positive Involution ist.

## 2.5 Konstruktion abelscher Flächen vom Typ $\mathcal{QM}$ mit komplexer Multiplikation

Unser Ziel in diesem Abschnitt ist es zu zeigen, dass für eine elliptische Kurve  $E$  vom Typ CM durch  $K$  eine abelsche Fläche  $A$  von Typ  $\mathcal{QM}$  und komplexer Multiplikation durch  $M_2(K)$  existiert. In gewissem Sinne ist dies eine Umkehrung von Theorem 2.4.12. Dies wird in Satz 2.5.7 genauer beschrieben. In den folgenden Abschnitten 2.6, 2.7 spielen die Ergebnisse dieses Abschnittes eine entscheidende Rolle.

Sei  $F$  nun ein Zahlkörper und  $E$  eine elliptische Kurve über  $F$  mit komplexer Multiplikation durch einen CM-Körper  $K$ . Sei ein fester Isomorphismus  $\iota : \mathcal{O}_{K,c} \xrightarrow{\sim} \text{End}(E)$  gewählt. Sei  $\theta \in \mathbb{N}$  eine quadratfreie Zahl mit  $\text{ggT}(\theta, n(m)) = 1$  für alle  $m \in K^*$ . Sei eine elliptische Kurve  $E'$  mit  $\text{End}(E') \simeq \mathcal{O}_{K,c}$  und eine Isogenie  $u : E \rightarrow E'$  von Grad  $\deg u \mid \theta^2$  gegeben. Sei  $\tilde{u} : E' \rightarrow E$  eine Isogenie mit  $\tilde{u} \circ u = [\theta]$ . Dann gilt:

$$\text{End}(E') = [\theta]^{-1} u \text{End}(E) \tilde{u}. \tag{2.7}$$

**2.5.1 Bemerkung.** In der Situation von Abschnitt 2.4 gilt  $E = E_e$  und  $E' = E_{\bar{e}}$ . Der genaue Zusammenhang wird in Satz 2.5.7 beschrieben.

Bezeichne  $\bar{\iota} : \mathcal{O}_{K,c} \xrightarrow{\sim} \text{End}(E)$  die Verknüpfung von  $\iota$  mit der komplexen Konjugation. Definiere mittels (2.7)

$$\iota' : \mathcal{O}_{K,c} \longrightarrow \text{End}(E') \tag{2.8}$$

$$\beta \longmapsto [\theta]^{-1} \circ u \bar{\iota}(\beta) \circ \tilde{u}. \tag{2.9}$$

Dann gelten für alle  $\eta \in \mathcal{O}_{K,c}$  die Identitäten

$$u\iota(\eta) = \iota'(\bar{\eta})u,$$

$$\tilde{u}\iota'(\eta) = \iota(\bar{\eta})\tilde{u}.$$

Wir konstruieren eine Quaternionenalgebra  $D$  über  $\mathbb{Q}$  aus geeigneten Teilalgebren von  $\text{Hom}(E, E')$  und  $\text{Hom}(E', E)$ . Dazu identifizieren wir  $\tilde{u}$  und  $u$  (bzw.  $\iota$  und  $\iota'$ ). Dies geschieht formal wie folgt:

Wir definieren eine Algebra  $D'$  und Ideale  $I_K, I_{uK}$  als

$$D' := (\iota(K) \times u\iota(K) \times \iota'(K) \times \tilde{u}\iota'(K)),$$

$$\subset \text{Hom}(E, E') \times \text{Hom}(E', E),$$

$$I_K := ((\iota(\alpha), 1, 1, 1) - (1, 1, \iota'(\alpha), 1)),$$

$$I_{uK} := ((1, u\iota(\alpha), 1, 1) - (1, 1, 1, \tilde{u}\iota'(\alpha))).$$

**2.5.2 Proposition.** Die Algebra

$$D := D' / (I_K + I_{uK})$$

ist eine Quaternionenalgebra über  $\mathbb{Q}$ .

BEWEIS. Für die Algebra  $D$  gilt

(i)  $D = \iota(K) \oplus u\iota(K),$

(ii)  $u^2 = u\tilde{u} = \theta,$

## 32 Kapitel 2. Abelsche Flächen vom Typ $\mathcal{QM}$ und Shimura-Kurven

$$(iii) \quad u\iota(\alpha) = \iota'(\bar{\alpha})u = \iota(\bar{\alpha})u.$$

Damit ist  $D$  nach Prop. 1.2.7 eine Quaternionenalgebra über  $\mathbb{Q}$ .  $\square$

Sei nun  $\mathcal{O}_D$  eine maximale Ordnung, die  $\mathcal{O}_{K,c} \oplus u\mathcal{O}_{K,c}$  enthält. Wir definieren wie folgt eine Wirkung von  $\mathcal{O}_D$  auf  $E \times E'$ :

**2.5.3 Lemma.** *Sei ein Element  $h := \beta_1 + u\beta_2 \in \mathcal{O}_D$  mit  $\beta_i \in K$  gegeben. Dann korrespondiert  $h$  zu einer Isogenie  $\Psi(h) : E \times E' \rightarrow E \times E'$ .*

BEWEIS. Sei zunächst  $h \in \mathcal{O}_{K,c} \oplus u\mathcal{O}_{K,c} \subset \mathcal{O}_D$ , d.h.  $\beta_i \in \mathcal{O}_{K,c}$ . Die Definition von  $D$  liefert uns die Morphismen

$$\begin{aligned} \Psi_E(h) &:= (\iota(\beta_1), u\iota(\beta_2)) : E \rightarrow E \times E', \\ \Psi_{E'}(h) &:= (\iota'(\beta_1), \tilde{u}\iota'(\beta_2)) : E' \rightarrow E' \times E. \end{aligned}$$

Wir definieren den Morphismus

$$\begin{aligned} \Psi(h) : E \times E' &\rightarrow E \times E' \\ (P, Q) &\mapsto \Psi_E(h)(P) + \Psi_{E'}(h)(Q). \end{aligned}$$

Die Verknüpfung von  $\Psi(h)$  mit der Projektion nach  $E$  bzw.  $E'$  ist

$$\begin{aligned} &(\iota(\beta_1) + \tilde{u}\iota'(\beta_2)) : E \times E' \rightarrow E \\ \text{bzw.} & \quad (\iota(\beta_2) + u\iota'(\beta_1)) : E \times E' \rightarrow E'. \end{aligned}$$

Man rechnet mittels der Identifikation  $E' = u(E)$  nach, dass  $\ker \Psi(h)|_E$  und  $\ker \Psi(h)|_{E'}$  endlich sind.  $\square$

**2.5.4 Lemma.** *Die Abbildung*

$$\begin{aligned} \Psi : \mathcal{O}_D &\hookrightarrow \text{End}(E \times E') & (2.10) \\ h &\mapsto \Psi(h) \end{aligned}$$

ist ein Morphismus. Dabei bezeichnet  $\Psi(h) : E \times E' \rightarrow E \times E'$  die Isogenie aus Lemma 2.5.3.

BEWEIS. Dies rechnet man mittels den Relationen in  $D$  aus dem Beweis von Proposition 2.5.2 elementar nach.  $\square$

Wir betrachten weiter für  $\beta \in \mathcal{O}_{K,c}$  die Isogenie

$$(\iota(\beta), \iota'(\beta)) : E \times E' \rightarrow E \times E'. \quad (2.11)$$

Insgesamt bekommen wir den folgenden Satz:

**2.5.5 Satz.** *Mit der Bezeichnung aus (2.10) und (2.11) existiert eine Einbettung*

$$\begin{aligned} \Psi : \mathcal{O}_D \otimes_{\mathbb{Z}} \mathcal{O}_{K,c} &\hookrightarrow \text{End}(E \times E') & (2.12) \\ h \otimes 1 &\mapsto \Psi(h) \\ 1 \otimes \beta &\mapsto (\iota(\beta), \iota'(\beta)). \end{aligned}$$

BEWEIS. Es ist offensichtlich, dass

$$\begin{aligned} \Psi(h \otimes \beta) &= \Psi(h) \circ (\iota(\beta), \iota'(\beta)) \\ &= \Psi(h \otimes 1) \circ \Psi(1 \otimes \beta) \\ &\in \text{End}(E \times E') \end{aligned}$$

für  $h \otimes \beta \in \mathcal{O}_D \otimes_{\mathbb{Z}} \mathcal{O}_{K,c}$  gilt. Damit folgt die Behauptung.  $\square$

Wir möchten der abelschen Fläche  $E \times E'$  mit ihrer  $\mathcal{O}_D$ -Wirkung eine abelsche Fläche vom Typ QM zuweisen. Sei dazu  $e = \frac{1}{2}(1 \otimes 1 + \iota(\alpha)^{-1} \otimes \alpha)$  die zu  $\iota$  gehörende Idempotente und  $\bar{e} = 1 - e$  die zu  $\bar{\iota}$  gehörende Idempotente.

**2.5.6 Bemerkung.** Die abelsche Fläche  $E \times E'$  ist nicht vom Typ QM im Sinne von Definition 2.1.6, da die Produktpolarisation auf  $E \times E'$  keine positive Polarisation auf  $D$  liefert (vgl. Bemerkung 2.4.19).

**2.5.7 Satz.** *Sei  $\eta \in \mathcal{O}_{K,c}$ , so dass  $e\eta \in \mathcal{O}_D \otimes \mathcal{O}_{K,c}$  ist. Desweiteren sei das ganze Ideal  $I = \langle \Psi(e\eta), \Psi(\bar{e}\eta) \rangle$  von  $\text{End}(E \times E')$  und das Torsionsuntergruppenschema  $G := (E \times E')[I]$  gegeben. Dann ist  $G$  endlich und definiert somit eine Isogenie*

$$\tilde{\psi}_e : E \times E' \rightarrow (E \times E')/G.$$

Bezeichne  $A := (E \times E')/G$  die abelsche Fläche. Die Einbettung

$$\Psi : \mathcal{O}_D \otimes_{\mathbb{Z}} \mathcal{O}_{K,c} \hookrightarrow \text{End}(E \times E')$$

aus (2.12) induziert eine Einbettung

$$\mathcal{O}_D \otimes_{\mathbb{Z}} \mathcal{O}_{K,c} \hookrightarrow \text{End}(A).$$

BEWEIS. Das Ideal  $I \subsetneq \text{End}(E \times E')$  enthält die Isogenie  $\Psi(1 \otimes \eta) \neq 0$  (vgl. Beweis von Satz 2.4.12). Daher ist  $I$  nach Lemma 2.4.8 ein Gitter und  $G$  nach Lemma 2.4.10 endlich. Folglich definiert  $\tilde{\psi}_e$  eine Isogenie.

Nun bleibt die Behauptung über die Endomorphismen von  $A$  zu zeigen. Ein Endomorphismus  $\beta$  auf  $E \times E'$  induziert genau dann einen Endomorphismus auf  $A$ , wenn  $\beta G \subset G$  gilt. Dazu argumentieren wir wie folgt:

Offensichtlich kommutieren alle  $\beta \otimes \beta' \in \mathcal{O}_{K,c} \otimes \mathcal{O}_{K,c}$  mit  $e$  und  $\bar{e}$ . Folglich gilt  $\Psi(\beta \otimes \beta')G \subset G$ . Für das Element  $u \in \mathcal{O}_D$  gilt  $ue\eta = \bar{e}\eta u$  und daher

$\Psi(u)G \subset G$ . Somit folgt die Behauptung.  $\square$

Wir möchten jetzt die Konstruktion in Zusammenhang mit dem Abschnitt 2.4 bringen.

Wir erinnern dazu an die Situation von Satz 2.4.12:

Sei  $A$  eine abelsche Fläche von Typ QM mit komplexer Multiplikation durch  $\text{End}^0(A) \simeq M_2(K)$ . Sei  $\iota : K \hookrightarrow D$  eine Einbettung und bezeichne  $\mathcal{O}_{K,c} := \iota^{-1}(\mathcal{O}_D)$ . Sei  $e$  die zu  $\iota$  gehörende Idempotente. Und sei  $\eta \in \iota(K)$  ein Endomorphismus mit  $e\eta \in \mathcal{O}_D \otimes \mathcal{O}_{K,c}$ . Bezeichne  $u \in \mathcal{O}_D$  ein Element, für das

- (i)  $D = \iota(K) + u\iota(K)$ ,
- (ii)  $u^2 = \theta \in \mathbb{Z}$ ,
- (iii)  $um = \bar{m}u$  für alle  $m \in \iota(K)$

gilt.

Dann existiert nach Satz 2.4.12 eine Isogenie  $\psi_e : A \rightarrow E_e \times E_{\bar{e}}$ , wobei  $E_e, E_{\bar{e}}$  isogene elliptische Kurven mit CM sind.

**2.5.8 Satz.** *Wendet man den Satz 2.5.7 auf  $E := E_e, E' := E_{\bar{e}}$  an, dann gilt*

$$E \times E' / G \simeq A.$$

BEWEIS. Der Satz ist eine Umformulierung der Konstruktion der dualen Isogenie aus Bemerkung 2.4.16.  $\square$

## 2.6 Reduktion modulo $p$ und Liften von Endomorphismen

Wir möchten in diesem Abschnitt die möglichen Endomorphismenringe für CM-Liften einer abelschen Fläche  $\bar{A}$  von Typ QM über einem endlichen Körper  $k$  nach  $W(k)$  bestimmen. Die Ergebnisse dieses Abschnittes werden in Abschnitt 4.1 benutzt um die Punkte im Deformationsraum von  $\bar{A}$  explizit zu beschreiben (Proposition 4.1.8). Dies ist wahrscheinlich das richtige Werkzeug um Kongruenzen für verallgemeinerte Spuren auf  $\mathcal{X}(1)$  analog zu Edixhoven ([Edi05]) geometrisch zu zeigen.

Sei dazu  $\mathcal{O}_L$  ein diskreter Bewertungsring,  $L := \text{Quot}(\mathcal{O}_L)$  dessen Quotientenring und gelte  $\text{char}(L) = 0$ . Sei  $\mathfrak{m}$  das maximale Ideal von  $\mathcal{O}_L$ . Bezeichne mit  $k := \mathcal{O}_L/\mathfrak{m}$  den zugehörigen Restklassenkörper der Charakteristik  $p := \text{char}(k) > 0$ . Sei  $A$  ein abelsches Schema von Dimension 2 über  $\mathcal{O}_L$ . Bezeichne mit  $\bar{A} := A \otimes k$  die Reduktion von  $A$  modulo  $\mathfrak{m}$ .

**2.6.1 Definition.** Wir sagen eine abelsche Varietät  $A_L$  hat *gute Reduktion* über  $L$ , falls ein abelsches Schema  $A$  über  $\mathcal{O}_L$  mit  $A \otimes L = A_L$  existiert, so dass  $A \otimes k$  glatt ist. Wir sagen  $A_L$  hat *potentiell gute Reduktion*, falls es eine endliche Erweiterung  $L'/L$  gibt, so dass  $A_L \otimes L'$  gute Reduktion über  $L'$  hat.

Habe  $A_L$  gute Reduktion über  $L$ , d.h.  $A \otimes k$  ist eine abelsche Fläche über  $k$ . Wir nehmen an, die abelsche Fläche  $A \otimes L$  sei vom Typ  $\mathbb{Q}M$  durch die indefinite Quaternionenalgebra  $D$  über  $\mathbb{Q}$ . Dann ist  $\bar{A}$  ebenfalls vom Typ  $\mathbb{Q}M$ . Angenommen  $A$  habe zusätzlich komplexe Multiplikation. Dann existiert nach Proposition 2.1.8 ein imaginärer Zerfällungskörper  $K$  von  $D$ , so dass  $\text{End}^0(A) \simeq D \otimes_{\mathbb{Q}} K$  gilt. Das Zentrum von  $\text{End}(A)$  ist nach Proposition 2.4.5 eine Ordnung  $\mathcal{O}_{K,c} \subset K$ , wobei  $c \in \mathbb{N}$  den Führer von  $\mathcal{O}_{K,c}$  in  $\mathcal{O}_K$  bezeichne. Wir wählen eine optimale Einbettung  $\iota : K \hookrightarrow D$ . Dann existiert nach Satz 2.4.12 eine Isogenie

$$\psi_{e\eta} : A \rightarrow E_e \times E_{\bar{e}},$$

so dass  $\deg \psi_{e\eta} \mid (4c^2 \cdot \text{disc}(K))$  gilt und  $E_e, E_{\bar{e}}$  isogene elliptische Kurven mit komplexer Multiplikation durch  $\text{End}(E) = \mathcal{O}_{K,c}$  sind. Die Reduktion  $\bar{A}$  ist isogen zum Produkt  $\bar{E}_e \times \bar{E}_{\bar{e}}$ , wobei  $\bar{E}_e$  (bzw.  $\bar{E}_{\bar{e}}$ ) die Reduktion von  $E_e$  (bzw.  $E_{\bar{e}}$ ) modulo  $\mathfrak{m}$  bezeichnet. Insbesondere ist  $A$  entweder gewöhnlich oder supersingulär. Dies kann man an  $K$  wie folgt ablesen.

**2.6.2 Satz.** Die Reduktion  $\bar{A}$  ist genau dann gewöhnlich, wenn das Primideal  $(p) \subset \mathbb{Z}$  in  $K$  zerfällt.

Die Reduktion  $\bar{A}$  ist genau dann supersingulär, wenn das Primideal  $(p) \subset \mathbb{Z}$  inert oder verzweigt in  $K$  ist.

BEWEIS. Dies folgt aus den entsprechenden Sätzen für elliptische Kurven vom Typ CM ([Lan87, Kap. 13, Thm. 12]).  $\square$

**2.6.3 Proposition.** Sei die Reduktion  $\bar{A}$  über  $p$  gewöhnlich. Dann ist  $D$  nicht verzweigt in  $p$ .

BEWEIS. Nach Satz 2.6.2 gilt  $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathbb{Q}_p^2$  und aus  $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \subset D \otimes_{\mathbb{Q}} \mathbb{Q}_p$  folgt dann nach Satz 1.2.8, dass  $D \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p)$  ist.  $\square$

Sei im folgenden  $\bar{A}$  über  $k$  gewöhnlich. Wir untersuchen nun, wie sich das Zentrum von  $\text{End}(A) \simeq \mathcal{O}_{K,c}$  bei Reduktion verhält (Proposition 2.6.5), d.h. wir untersuchen die Einbettung  $\text{Zentrum}(\text{End}(A)) \hookrightarrow \text{Zentrum}(\text{End}(\bar{A}))$ . Wir reduzieren dies auf Aussagen über das Verhalten von  $\text{End}(E_e)$  bei Reduktion, welches wir in folgendem Lemma 2.6.4 zitieren.

**2.6.4 Lemma ( [Lan87, Thm. 13.12] ).** Sei  $E$  eine elliptische Kurve über  $\mathcal{O}_L$  mit komplexer Multiplikation durch  $\text{End}(E) \simeq \mathcal{O}_{K,c}$ , wobei  $\mathcal{O}_{K,c}$  die Ordnung mit Führer  $c$  bezeichnet. Schreibe  $c = c_0 \cdot p^n$  mit  $p \nmid c_0$ . Habe  $E$  gute gewöhnliche Reduktion  $\bar{E}$  modulo  $\mathfrak{m}$ . Dann gilt  $\text{End}(\bar{E}) \simeq \mathcal{O}_{K,c_0}$ .

**2.6.5 Proposition.** Sei die Situation wie oben. Insbesondere sei  $\bar{A}$  über  $k$  eine gewöhnliche abelsche Fläche und es gelte  $\text{Zentrum}(\text{End}(A)) \simeq \mathcal{O}_{K,c}$ . Bezeichne  $c = c_0 \cdot p^n$  mit  $p \nmid c_0$ . Dann gilt:

$$\text{Zentrum}(\text{End}(\bar{A})) \simeq \mathcal{O}_{K,c_0}.$$

Folglich existiert eine Einbettung

$$\mathcal{O}_D \otimes_{\mathbb{Z}} \mathcal{O}_{K,c_0} \hookrightarrow \text{End}(\bar{A}).$$

BEWEIS. Die Konstruktion der Isogenie  $\psi_{e\eta} : A \rightarrow E_e \times E_{\bar{e}}$  im Beweis von Satz 2.4.12 liefert eine Isogenie  $u : E_e \rightarrow E_{\bar{e}}$  von Grad  $\deg u \mid (n(u))^2$ , wobei  $u$  als Element von  $\mathcal{O}_D$  aufgefasst wird. Da nach Proposition 2.6.3 die Quaternionenalgebra  $D$  in  $p$  nicht verzweigt ist, kann man  $u$  so wählen, dass  $p \nmid n(u)$  gilt. Somit liefert die Reduktion der Isogenie  $u : E_e \rightarrow E_{\bar{e}}$  eine Isogenie  $u_{\text{red}} : \bar{E}_e \rightarrow \bar{E}_{\bar{e}}$ . Satz 2.5.7 konstruiert zu  $u_{\text{red}} : \bar{E}_e \rightarrow \bar{E}_{\bar{e}}$  eine abelsche Varietät  $\tilde{A}$  über  $k$  vom Typ  $\mathcal{QM}$  durch  $\mathcal{O}_D$ . Dabei wird eine optimale Einbettung  $\iota' : K \hookrightarrow D$  konstruiert. Satz 2.5.8 besagt, dass tatsächlich  $\tilde{A} \simeq \bar{A}$  gilt. Somit folgt die Behauptung aus den Aussagen von Satz 2.5.7 über die Endomorphismen von  $\tilde{A}$ .  $\square$

**2.6.6 Bemerkung.** Man beachte beim Beweis von Proposition 2.6.5, dass die Einbettungen  $\iota : K \hookrightarrow D$  und  $\iota' : K \hookrightarrow D$  nicht äquivalent sind, falls  $c \neq c_0$  gilt. Denn  $\iota$  (bzw.  $\iota'$ ) ist eine optimale Einbettung bezüglich  $\mathcal{O}_{K,c}$  (bzw.  $\mathcal{O}_{K,c_0}$ ) und für  $\mathcal{O}_{K,c} \neq \mathcal{O}_{K,c_0}$  sind  $\iota$  und  $\iota'$  wegen Lemma 1.3.8 nicht äquivalent.

Wir möchten die Liftbarkeit einer ganzen Ordnung  $\mathcal{O}_{K,c}$  des Zentrums von  $\text{End}^0(\bar{A})$  in Termen der Liftbarkeit eines einzigen Endomorphismus' ausdrücken. Dies reduzieren wir wieder auf den Fall für elliptische Kurven.

**2.6.7 Proposition.** Sei die Situation wie oben. Insbesondere sei  $\bar{A}$  eine gewöhnliche abelsche Fläche über  $k$ . Gelte  $\text{Zentrum}(\text{End}(\bar{A})) \simeq \mathcal{O}_{K,c_0}$ , insbesondere gelte  $p \nmid c_0$ . Bezeichne  $\pi \in \mathcal{O}_{K,c_0}$  den absoluten Frobenius-Morphismus. Sei  $\mathcal{O}_{K,c} \subset \mathcal{O}_{K,c_0}$  die eindeutige Unterordnung von  $\mathcal{O}_{K,c_0}$  von Index  $p^n$  für ein  $n \in \mathbb{N}$ , d.h. sei  $c = p^n c_0$ . Genau dann existiert eine Einbettung

$$\mathcal{O}_{K,c} \hookrightarrow \text{Zentrum}(\text{End}(A)),$$

falls  $p^n \pi \in \text{Zentrum}(\text{End}(A))$  ist.

BEWEIS. Die eine Richtung ist trivial. Sei also  $p^n\pi \in \text{Zentrum}(\text{End}(A))$ . Dann gilt  $p^n\pi \in \text{End}(E_e)$  (bzw.  $p^n\pi \in \text{End}(\overline{E}_e)$ ). In [Kro09, Prop. 2.3.13] beweist Kroworsch, dass für einen Lift  $E$  einer gewöhnlichen elliptischen Kurve  $\overline{E}$ , genau dann  $\mathcal{O}_{K,p^n c_0} \subset \text{End}(E)$  gilt, wenn  $p^n\pi \in \text{End}(E)$  ist. In unserer Situation gilt somit  $\mathcal{O}_{K,p^n c_0} \subset \text{End}(E_e)$  (bzw.  $\mathcal{O}_{K,p^n c_0} \subset \text{End}(\overline{E}_e)$ ). Analog zum Beweis von Proposition 2.6.5 zeigt man nun, dass daraus  $\mathcal{O}_{K,c} \subset \text{Zentrum}(\text{End}(A))$  folgt.  $\square$

## 2.7 CM-Punkte und abelsche Flächen vom Typ QM & CM

Wir möchten in diesem Abschnitt die Punkte auf der Shimura-Kurve  $\mathcal{X}(1)$  (Definition 2.3.2), die in der Modulinterpretation zu abelschen Flächen vom Typ QM mit komplexer Multiplikation gehören, intrinsisch beschreiben. Schließlich zeigen wir unter Verwendung der Ergebnisse aus den Abschnitten 2.4 und 2.5 eine Korrespondenz zwischen den CM-Punkten und bestimmten elliptischen Kurven.

Wir erinnern an die Bezeichnungen in der Definition der Shimura-Kurve  $\mathcal{X}(1)$  (Definition 2.3.2). Sei  $D$  eine indefinite Quaternionenalgebra über  $\mathbb{Q}$  und  $\mathcal{O}_D$  eine maximale Ordnung. Sei  $\Psi : D \hookrightarrow M_2(\mathbb{R})$  eine Einbettung von  $D$ . Sei

$$\mathcal{O}_D^1 := \{h \in \mathcal{O}_D : n(h) = 1\} \quad \text{und} \quad \Gamma(1) := \Psi(\mathcal{O}_D^1) \subset \text{SL}_2(\mathbb{R}).$$

Dann ist  $\Gamma(1)$  eine arithmetische Fuchsische Gruppe und die Shimura-Kurve  $\mathcal{X}(1) := \mathcal{H}/\Gamma(1)$  ist eine kompakte Riemannsche Fläche.

**2.7.1 Proposition ([Shi94, Prop. 9.4]).** *Gegeben sei ein imaginärer Zerfällungskörper  $K$  von  $D$  und  $\iota : K \hookrightarrow D$  eine Einbettung. Betrachte  $\iota(K^*/\mathbb{Q}^*)$  als Untergruppe von  $\text{SL}_2(\mathbb{R})$  via  $\Psi : D \hookrightarrow M_2(\mathbb{R})$ . Die zugehörige Wirkung von  $\iota(K^*/\mathbb{Q}^*)$  auf  $\mathcal{H}$  hat einen eindeutigen Fixpunkt  $\zeta \in \mathcal{H}$ .*

*Umgekehrt sei  $\gamma \in D^* \setminus \mathbb{Q}^*$  und existiere ein Fixpunkt  $\zeta \in \mathcal{H}$  der Wirkung von  $\Psi(\gamma) \in \text{GL}_2^+(\mathbb{R})$  auf  $\mathcal{H}$ . Dann ist  $\mathbb{Q}(\gamma)$  ein imaginär quadratischer Zerfällungskörper von  $D$ .*

**2.7.2 Definition.** Wir nennen einen Fixpunkt  $\zeta \in \mathcal{H}$  wie in Prop. 2.7.1 einen *CM-Punkt* unter  $D^*$ .

Wir erinnern an die Definition 1.3.9 der Äquivalenz von Einbettungen  $\iota, \iota' : K \hookrightarrow D$ . Dabei nennen wir diese äquivalent, falls  $h \in \mathcal{O}_D^1$  existiert, so dass  $h\iota(x)h^{-1} = \iota'(x)$  für alle  $x \in K$  gilt.

**2.7.3 Proposition ( [AB04, Prop. 9.11] ).** *Zwei Fixpunkte  $\zeta, \zeta' \in \mathcal{H}$  bezüglich zweier optimal gewählter Einbettungen  $\iota, \iota'$  (Definition 1.2.18) sind genau dann gleich, wenn  $\iota$  äquivalent zu  $\iota'$  oder  $\bar{\iota}'$  modulo  $\mathcal{O}_D^1$  ist.*

Somit kann man CM-Punkte auf  $\mathcal{X}(1)$  wie folgt definieren:

**2.7.4 Definition.** Wir nennen die Bahn unter  $\Gamma(1)$  eines Punktes  $\zeta \in \mathcal{H}$  wie in 2.7.1 einen *CM-Punkt* von  $\mathcal{X}(1)$  mit *CM-Ring*  $\mathcal{O}_{K,c} = \iota^{-1}(\mathcal{O}_D)$ , wobei  $c \in \mathbb{N}$  den Führer von  $\mathcal{O}_{K,c}$  bezeichnet.

**2.7.5 Bemerkung.** Analog kann man CM-Punkte auf der Shimura-Kurve  $\mathcal{X}^*(1)$  definieren.

**2.7.6 Bemerkung.** Nach Satz 2.3.6 korrespondiert zu einem CM-Punkt  $\zeta \in \mathcal{X}(1)$  eine abelsche Fläche  $A$  vom Typ  $\mathcal{QM}$  durch  $\mathcal{O}_D$ . Die Bahn von  $\zeta$  unter  $\Psi(\mathcal{O}_D)$  besitzt eine  $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathcal{O}_{K,c}$ -Wirkung. Damit korrespondiert  $\zeta$  zu einer abelschen Fläche vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation.

**2.7.7 Proposition ( [AB04, Lem.5.13] ).** *Die elliptischen Punkte  $\zeta \in \mathcal{X}(1)$  entsprechen den Einbettungen von  $\mathcal{O}_{K,c} \hookrightarrow \mathcal{O}_D$  mit  $\zeta_3 \in \mathcal{O}_{K,c}$  (bzw.  $\zeta_4 \in \mathcal{O}_{K,c}$ ). Insbesondere hat  $\zeta$  als elliptischer Punkt die Ordnung 3 (bzw. 2). Andere Ordnungen von elliptischen Punkten sind nicht möglich.*

BEWEIS. Sei  $\zeta \in \mathcal{X}(1)$  ein elliptischer Punkt, dh. es existiert eine nicht triviale Transformation  $\gamma \in \Gamma(1)$  mit  $\gamma(\zeta) = \zeta$ . Mittels Proposition 2.7.1 definiert  $\gamma \notin \mathbb{Q}$  eine Einbettung  $\mathbb{Q}(\gamma) \hookrightarrow D$  eines imaginär quadratischen Zerfällungskörpers  $K = \mathbb{Q}(\gamma)$ . Da  $n(\gamma) = 1$  gilt, muss  $K \simeq \mathbb{Q}(\zeta_3)$  oder  $K \simeq \mathbb{Q}(\zeta_4)$  sein.

Die Umkehrung folgt direkt aus Prop. 2.7.1. □

**2.7.8 Bemerkung.** Nach Bemerkung 2.7.6 korrespondieren zu den elliptischen Punkten also abelsche Flächen  $A \sim E^2$  mit  $\zeta_3 \in \text{End}(E)$  (bzw.  $\zeta_4 \in \text{End}(E)$ ).

Folgender Satz bestimmt die Anzahl der CM-Punkte mit CM-Ring  $\mathcal{O}_{K,c}$  in  $\mathcal{X}(1)$ . Die kombinatorische Aussage des Satzes wird im Beweis von Theorem 2.7.12 benutzt.

**2.7.9 Korollar ( zu Prop. 1.3.10, [AB04, Thm. 6.13] ).** *Bezeichne  $b \in \mathbb{N}$  die Anzahl der Primzahlen  $p \mid \text{disc}(D)$ , die verzweigt in  $K$  sind. Dann ist die Anzahl der CM-Punkte von  $\mathcal{X}(1)$  mit CM-Ring  $\mathcal{O}_{K,c} \subset K$  genau  $2^b h(\mathcal{O}_{K,c})$ .*

BEWEIS. Dies folgt elementar aus Proposition 2.7.3 und Proposition 1.3.10 unter Verwendung folgender Tatsache:

Sei  $\iota : K \hookrightarrow D$  eine Einbettung. Dann sind  $\bar{\iota}$  und  $\iota$  nicht äquivalent (modulo  $\mathcal{O}_D^1$ ). □

Wir beweisen in Theorem 2.7.12 eine Korrespondenz zwischen elliptischen Kurven und CM-Punkten. Dazu zitieren wir zunächst ein Ergebnis für sogenannte Isogenie-Graphen aus [Koh96].

**2.7.10 Proposition.** Sei  $l \in \mathbb{N}$  eine Primzahl mit  $p \neq \text{char}(F)$ . Sei  $E$  eine elliptische Kurve über  $F$  und bezeichne  $\mathcal{O} := \text{End}(E)$ . Sei  $c \in \mathbb{N}$  der Führer von  $\mathcal{O}$  in  $\mathcal{O}_K$ .

- (1) Sei  $E \rightarrow E'$  eine Isogenie von Grad  $l$  zu einer elliptischen Kurven  $E'$  mit CM durch  $\mathcal{O}' := \text{End}(E') \subset K$ . Dann gilt  $\mathcal{O} \subset \mathcal{O}'$  oder  $\mathcal{O} \supset \mathcal{O}'$  mit Index  $i \mid l$ .
- (2) Bezeichne  $\text{Isog}_l(E)$  folgende Menge:

$$\text{Isog}_l(E) := \left\{ \begin{array}{l} \text{Isogenien } E \rightarrow E' \text{ von Grad } l \\ \text{zu elliptischen Kurven } E' \end{array} \right\}.$$

Dann gilt  $|\text{Isog}_l(E)| \leq l + 1$ .

- (2a) Gelte  $l \nmid c$ . Dann existieren  $\left(\frac{\text{disc}(K)}{l}\right) + 1$  Isogenien  $E \rightarrow E'$  von Grad  $l$  zu elliptischen Kurven  $E'$  mit  $\mathcal{O}' \simeq \mathcal{O}$ .
- (2b) Gelte  $l \mid c$ . Dann existiert genau eine Isogenie  $E \rightarrow E'$  von Grad  $l$  zu einer elliptischen Kurve  $E'$  mit  $\mathcal{O}' \supsetneq \mathcal{O}$  und Index  $[\mathcal{O}' : \mathcal{O}] = l$ .
- (2c) Existieren zusätzlich zu (1) (bzw. (2)) Isogenien von Grad  $l$  dann sind dies genau  $l - \left(\frac{\text{disc}(K)}{l}\right)$  mit  $\mathcal{O}' \subsetneq \mathcal{O}$  und Index  $[\mathcal{O} : \mathcal{O}'] = l$ .

BEWEIS. Einen Beweis in Charakteristik  $p > 0$  findet man in [Koh96, Prop. 23]. Die Vorgehensweise für den Beweis in Charakteristik 0 findet man in einer Bemerkung in dem Beweis von [Koh96, Prop. 22].  $\square$

**2.7.11 Korollar.** Seien  $E_0, E_s$  zwei elliptische Kurven mit CM durch  $\mathcal{O}_{K,c}$  und sei  $n := p_1 \cdots p_s \in \mathbb{N}$  für paarweise verschiedene Primzahlen  $p_i$  mit  $\left(\frac{p_i}{K}\right) = -1$  oder  $p_i \nmid c$ . Dann existiert keine Isogenie  $\beta : E_1 \rightarrow E_s$  mit  $\deg \beta > 1$  und  $\deg \beta \mid n$ .

BEWEIS. Der Fall, dass  $n = p_1$  eine Primzahl ist, entspricht Teil (2a) in Proposition 2.7.10. Wir beweisen die Behauptung für  $n = p_1 p_2$ , der Rest folgt dann mittels Induktion nach  $s \in \mathbb{N}$ . Wir nehmen o.B.d.A. an, dass eine Isogenie  $\beta : E_0 \rightarrow E_2$  von Grad  $n = p_1 p_2$  existiert, sonst folgt die Behauptung direkt aus Teil (2a) in Proposition 2.7.10. Dann existieren Isogenien  $\beta_i : E_{i-1} \rightarrow E_i$  von Grad  $p_i$ , so dass  $\beta = \beta_2 \circ \beta_1$  ist. Per Annahme gilt  $\left(\frac{p_i}{K}\right) = -1$ , und folglich ist  $[\text{End}(E_0) : \text{End}(E_1)] = p_1$  nach Teil (1) in Proposition 2.7.10. Es folgt aus  $\text{End}(E_2) \simeq \mathcal{O}_{K,c}$ , dass  $[\text{End}(E_1) : \text{End}(E_2)] = p_1$  gilt. Nach Proposition 2.7.10 Teil (1) müsste dann  $p_1 \mid p_2$  gelten. Dies ist aber im Widerspruch dazu, dass die Primzahlen  $p_1$  und  $p_2$  verschieden sind.  $\square$

Sei  $\theta \in \mathbb{N}$  eine quadratfreie Zahl, so dass  $D \simeq (K, \theta)$  in der Notation von Satz 1.2.4 gilt. Sei  $\theta = \theta_{-1} \cdot \theta_1$ . Bezeichne  $\Sigma$  die Menge der Primteiler von  $\text{disc}(D)$  und sei  $b \in \mathbb{N}$  die Anzahl der Primzahlen in  $\Sigma$ , die verzweigt in  $K$  sind. Sei  $\Sigma_{-1} \subset \Sigma$  die Untermenge der Primteiler von  $\text{disc}(D)$ , die in  $K$  inert sind. Dann folgt aus Proposition 1.3.10 die folgende Korrespondenz.

**2.7.12 Theorem.** *Es existiert eine  $2^b$ -1-Korrespondenz*

$$\left\{ \begin{array}{l} \text{CM-Punkte auf} \\ \mathcal{X}(1) \text{ durch } K \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{elliptische Kurven} \\ E \text{ mit komplexer} \\ \text{Multiplikation} \\ \text{durch } K \end{array} \right\} \quad (2.13)$$

$$\zeta \in \mathcal{X}(1) \longmapsto E_\zeta.$$

BEWEIS. Wir gliedern den Beweis in drei Schritte. Zunächst konstruieren wir die Abbildung, dann zeigen wir die Surjektivität und zuletzt zeigen wir die Korrespondenz.

- (1) Zunächst konstruieren wir zu einem CM-Punkt  $\zeta \in \mathcal{X}(1)$  eine elliptische Kurve  $E$  wie in der Aussage des Satzes. Sei dazu  $\zeta \in \mathcal{X}(1)$  ein CM-Punkt. Dann korrespondieren zu  $\zeta$  nach Proposition 2.7.3, bis auf Äquivalenz, genau zwei Einbettung von  $K$  in  $D$ , nämlich

$$\iota : K \hookrightarrow D$$

und die Verknüpfung der komplexen Konjugation mit  $\iota$ . In [Shi94, Seite 246] wird eine Normierungsbedingung genannt, so dass man  $\iota$  (bis auf Äquivalenz) eindeutig wählen kann. Mit der selben Überlegung kann man den Isomorphismus

$$\epsilon : \text{End}^0(A) \xrightarrow{\sim} D \otimes_{\mathbb{Q}} K$$

aus Proposition 2.4.4 eindeutig wählen. Nach Bemerkung 2.7.6 korrespondiert zu  $\zeta$  eine abelsche Fläche  $A_\zeta$  vom Typ  $\mathbb{Q}M$  mit komplexer Multiplikation. Satz 2.4.12 besagt, dass zu der eindeutigen normierten Einbettung  $\iota$  eine Isogenie

$$\psi_{e\eta} : A_\zeta \hookrightarrow E_e \times E_{\bar{e}}$$

existiert. Lemma 2.4.14 besagt, dass die Isomorphieklassen der elliptischen Kurve  $E_e$  unabhängig von der Wahl des Repräsentanten  $\iota$  ist. Dies liefert durch  $\zeta \mapsto E_\zeta := E_e$  die Abbildung aus der Korrespondenz (2.13).

Für die weiteren Teile des Beweises bemerke man, dass die elliptische Kurve  $E_\zeta$  komplexe Multiplikation durch  $\mathcal{O}_{K,c} := \iota^{-1}(\mathcal{O}_D)$  hat, wobei

$\mathcal{O}_{K,c}$  eine Ordnung mit Führer  $c$  in  $K$  ist.

(2) Nun zeigen wir die Surjektivität. Sei also  $E$  eine elliptische Kurve mit komplexer Multiplikation durch  $\mathcal{O}_{K,c}$  und sei  $\theta \in \mathbb{Z}$  quadratfrei, so dass  $D \simeq (K, \theta)$  gilt. Sei  $\theta_{-1} \in \mathbb{N}$  das Produkt der Primteiler von  $\theta$ , die inert in  $K$  sind. Sei  $\theta_1 \in \mathbb{N}$ , so dass  $\theta = \theta_{-1} \cdot \theta_1$  gilt. Nach Proposition 2.7.10 Teil (2a) existiert eine elliptische Kurve  $E'$  mit  $\text{End}(E') \simeq \mathcal{O}_{K,c}$  und eine Isogenie  $u_1 : E \rightarrow E'$  mit  $\deg u_1 = \theta_1$ . Definiere nun die Isogenien  $u := [\theta_{-1}] \circ u_1 : E \rightarrow E'$  und  $\tilde{u} := u_1^t : E' \rightarrow E$ . Dann gilt  $\tilde{u} \circ u = [\theta]$ . Die Konstruktion in Abschnitt 2.5 liefert uns eine abelsche Varietät  $A$  vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation durch  $\mathcal{O}_{K,c}$  und somit nach Bemerkung 2.7.6 einen CM-Punkt  $\zeta \in \mathcal{X}(1)$ . Nach Satz 2.5.8 ist die elliptische Kurve  $E$  isomorph zu  $E_\zeta$ , insbesondere liegt  $E$  im Bild der Abbildung.

(3) Es genügt zu zeigen, dass eine elliptische Kurve  $E$  mit komplexer Multiplikation durch  $K \subset D$  unter obiger Abbildung mindestens  $2^b$  Urbilder besitzt. Dann besitzt  $E$  nach der Formel für die Anzahl der CM-Punkte in Korollar 2.7.9 genau  $2^b$  Urbilder.

Sei also eine elliptische Kurve  $E := E_\zeta$  mit komplexer Multiplikation durch  $\mathcal{O}_{K,c}$  gegeben und sei  $\zeta \in \mathcal{X}(1)$  ein beliebiges Urbild unter der Korrespondenz. Sei  $A := A_\zeta$  die zu  $\zeta$  gehörende abelsche Fläche vom Typ  $\mathcal{QM}$ . Nach Proposition 2.3.5 existieren  $2^b - 1$  nicht-triviale Äquivalenzklassen von  $\Gamma^*(1)/\Gamma$ . Sei nun eine nicht-triviale Äquivalenzklasse  $[h] \in \Gamma^*(1)/\Gamma$  und ein Repräsentant  $h \in \text{Nor}(\mathcal{O}_D)$  gewählt, so dass o.B.d.A.

$$1 < n(h) \mid \prod_{p \in \Sigma_{-1}} p$$

erfüllt ist (Prop. 2.3.5). Die Einbettung

$$\iota' := \iota^h : K \hookrightarrow D, x \mapsto h^{-1} \cdot \iota(x) \cdot h$$

definiert nach Lemma 1.3.8 eine optimale Einbettung von  $\mathcal{O}_{K,c}$ . Somit korrespondiert  $\iota'$  zu einem CM-Punkt  $\zeta' \in \mathcal{X}(1)$ . Da  $n(h) \neq 1$  ist, gilt  $\zeta' \neq \zeta$  (Korollar 2.7.3). Sei  $A'$  die abelsche Fläche vom Typ  $\mathcal{QM}$ , die zu  $\zeta'$  korrespondiert und  $E'$  das Bild unter der Korrespondenz (2.13). Aus der Modulinterpretation folgt, dass eine Isogenie

$$\beta : A \rightarrow A'$$

von Grad  $\deg \beta = n(h)$  existiert und diese durch Einschränkung eine Isogenie  $\beta|_E : E \rightarrow E'$  mit  $\deg \beta|_E \mid (n(h))^2$  liefert. Korollar 2.7.11 besagt, dass zwischen elliptischen Kurven  $E, E'$  mit CM durch  $\mathcal{O}_{K,c}$

keine Isogenie  $\beta : E \rightarrow E'$  mit

$$\deg \beta > 1 \quad \text{und} \quad \deg \beta \mid \prod_{p \in \Sigma_{-1}} p$$

existiert. Somit existiert ein  $N \mid n(h)$  und ein Isomorphismus  $\beta_1$ , so dass  $\beta = [N] \circ \beta_1$  gilt. Insbesondere sind also  $E = E_\zeta$  und  $E_{\zeta'}$  isomorph.

Die  $2^b$  verschiedene Äquivalenzklassen in  $\Gamma^*(1)/\Gamma$  liefern mit dieser Überlegung  $2^b$  paarweise verschiedene CM-Punkte, die auf die elliptische Kurve  $E$  abbilden. Somit existieren  $2^b$  paarweise verschiedene Urbilder von  $E$ . □

## Kapitel 3

# Dieudonné-Moduln abelscher Varietäten und die $q$ -Parameter

In den Kapiteln 4 und 5 studieren wir den Lokus einer Shimura-Kurve im Deformationsraum gewöhnlicher abelscher Varietäten. Dazu fassen wir in diesem Kapitel die benötigten Ergebnisse aus der Theorie der Dieudonné-Moduln ([Oda69, §3]) und der Deformationstheorie gewöhnlicher, abelscher Varietäten zusammen. Dabei interpretieren wir die erste de-Rham-Kohomologie (3.4.1) als Realisierung eines Dieudonné-Moduls ([Oda69, §4]). Wir zitieren die Existenz von Koordinaten auf dem Deformationsraum (Satz 3.5.8) und leiten mittels [Mes72, Thm. V.1.10] eine Liftbarkeitsbedingung für Endomorphismen an diese Koordinaten her (Korollar 3.6.16). Dies kann benutzt werden um den Lokus einer Shimura-Kurve im Deformationsraum auszurechnen (Thm. 4.1.6, bzw. Prop. 5.2.3) und um die Geometrie von CM-Punkten im Deformationsraum zu studieren (Prop. 4.1.8, bzw. Prop. 5.2.4). Solche Gleichungen lassen vermuten, dass man Kongruenzen von verallgemeinerten Spuren von CM-Punkten auf allgemeineren Shimura-Kurven vom Typ PEL mit ähnlichen Methoden wie in [Kro09] beweisen kann.

Wir geben nun einen Überblick über den Inhalt dieses Kapitels. In Abschnitt 3.1 leiten wir eine alternative Uniformisierung von Shimura-Kurven über  $\mathbb{C}$  mittels der uniformisierenden Differentialgleichung (Definition 3.1.12) her. Diese hat den Vorteil, dass sie auch in positiver und gemischter Charakteristik betrachtet werden kann. In Abschnitt 3.2 erklären wir kurz die Interpretation der uniformisierenden Differentialgleichung als Picard-Fuchs Differentialgleichung (Satz 3.2.3). Diese Abschnitte liefern den theoretischen Hintergrund für die Kapitel 4 und 5.

In den restlichen Abschnitten des Kapitels beschäftigen wir uns mit der Deformationstheorie gewöhnlicher abelscher Varietäten. Dazu geben wir in Abschnitt 3.3 zunächst die Definition eines  $F$ -Kristalls. In Abschnitt 3.4 betrachten wir gewöhnliche  $F$ -Kristalle. Dies benutzen wir um in Abschnitt 3.5 die Deformationstheorie einer gewöhnlichen abelschen Varietät  $A$  über einem endlichen Körper zu studieren und auf dem Deformationsraum explizite Koordinaten zu definieren (Satz 3.5.8). Diese Koordinaten ermöglichen uns in Abschnitt 3.6 explizite Bedingungen für die Liftbarkeit von Endomorphismen zu formulieren (Korollar 3.6.16).

### 3.1 Lineare gewöhnliche Differentialgleichungen über $\mathbb{C}$

Wir geben kurz Resultate für lineare gewöhnliche Differentialgleichungen über  $\mathbb{C}$  zweiten Grades an. Dabei orientieren wir uns an [Yos87] und [Elk98, §2.2]. Dieser soll einen Zusammenhang zwischen Shimura-Kurven und Differentialgleichungen über  $\mathbb{C}$  erläutern.

Seien dazu  $p_1, p_2 \in \mathbb{C}(x)$  rationale Funktionen über  $\mathbb{C}$  und sei

$$L : u'' + p_1 u' + p_2 u = 0 \quad (3.1)$$

eine lineare gewöhnliche Differentialgleichung. Sei  $S \subset \mathbb{P}^1(\mathbb{C})$  die Menge der Singularitäten von  $p_1$  und  $p_2$ .

**3.1.1 Definition.** Wir nennen zwei Lösungen  $u_0, u_1$  der Differentialgleichung  $L$  *linear unabhängig*, falls die Wronski-Determinante

$$W(u_0, u_1) := \det \begin{pmatrix} u_0 & u_1 \\ u_0' & u_1' \end{pmatrix}$$

nicht verschwindet.

**3.1.2 Satz ([Beu07, Thm. 2.3]).** Sei  $x_0 \in \mathbb{P}^1(\mathbb{C}) \setminus S$  ein. Dann existieren zwei Potenzreihen  $u_0, u_1$  um  $x_0$  mit positivem Konvergenzradius, die linear unabhängige Lösungen von  $L$  in  $x_0$  sind.

**3.1.3 Definition.** Wir nennen einen Punkt  $x_0 \in S$  *reguläre Singularität*, falls  $\text{ord}_{x_0}(p_i) \geq -i$  für  $i = 1, 2$  gilt. Die Differentialgleichung  $L$  nennt man *Fuchssche Differentialgleichung*, falls jeder Punkt  $x_0 \in S$  eine reguläre Singularität ist.

Sei  $x_0 \in \mathbb{P}^1(\mathbb{C})$  ein regulärer Punkt oder eine reguläre Singularität von  $L$ . Wir wenden eine Koordinatentransformation an, so dass o.B.d.A.  $x_0 = 0$ .

Seien nun die Gleichung

$$s(s-1) + sq_1 + q_2 = 0 \quad (3.2)$$

für  $q_0 := \frac{p_1}{x}|_{x=0}$  und  $q_1 := \frac{p_2}{x^2}|_{x=0}$  gegeben. Wir nennen (3.2) die *charakteristische Gleichung* von  $L$  bei  $x_0 = 0$ . Die Lösungen  $s_0, s_1 \in \mathbb{C}$  von (3.2) nennen wir die *charakteristischen Exponenten*.

**3.1.4 Satz ([Beu07, Thm 2.9]).** Sei eine reguläre Singularität  $x_0 \in S$  gegeben. Dann besitzt  $L$  zwei linear unabhängige Lösungen  $u_0, u_1$  als Laurent-Reihen um  $x_0$ .

**3.1.5 Proposition ([Yos87, § 2.4]).** Seien  $u_0, u_1$  zwei linear unabhängige Funktionen. Dann liefert die Gleichung

$$\det \begin{pmatrix} u_0 & u_0' & u_0'' \\ u_1 & u_1' & u_1'' \\ u & u' & u'' \end{pmatrix} = 0$$

eine lineare Differentialgleichung  $u'' + pu' + q = 0$  mit Lösungsraum  $\mathbb{C}u_0 \oplus \mathbb{C}u_1$ .

Seien  $u_0$  und  $u_1$  zwei linear unabhängige Lösungen in einem regulären Punkt  $x_0 \in \mathbb{P}^1(\mathbb{C}) \setminus S$  von  $L$ . Sei  $\gamma$  eine Schleife mit Anfangs- und Endpunkt in  $x_0$ , die  $S$  nicht schneidet. Die analytische Fortsetzung von  $u_0$  und  $u_1$  entlang der Kurve  $\gamma$  liefert wieder zwei linear unabhängige Lösungen, denn die Wronski-Determinante ist eine nicht-verschwindende holomorphe Abbildung in  $x_0$ . Damit bekommen wir eine Wirkung der Fundamentalgruppe  $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, x_0)$  auf dem Lösungsraum von  $L$  in  $x_0$ .

**3.1.6 Definition.** Wir nennen den Homomorphismus

$$\rho : \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, x_0) \rightarrow \mathrm{GL}(2, \mathbb{C})$$

wie oben die *Monodromie-Darstellung* von  $L$  bezüglich  $u_0, u_1$ . Wir nennen das Bild  $\Gamma := \rho(\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, x_0))$  die *Monodromie-Gruppe*.

**3.1.7 Bemerkung.** Die Konjugationsklasse der Monodromie-Gruppe  $\Gamma$  ist offensichtlich unabhängig von der Wahl der linear unabhängigen Lösungen  $u_0, u_1$  und ebenso von der Wahl des Punktes  $x_0 \in \mathbb{P}^1(\mathbb{C}) \setminus S$ .

Wir wollen nun eine Uniformisierung von Quotienten  $\mathcal{H}^*/\Gamma$  für eine Fuchssche Gruppen  $\Gamma$  in Termen von linearen Differentialgleichungen beschreiben. Wir folgen dazu [Elk98, §2.2].

**3.1.8 Notation.** Bezeichne  $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$  die erweiterte komplexe obere Halbebene. Sei  $z$  eine Koordinate auf  $\mathcal{H}$ . Sei  $\Gamma < \mathrm{SL}_2(\mathbb{R})$  eine Fuchssche

Gruppe (Definition 2.2.7). Existiere ein projektives, glattes Modell  $C$  über  $\mathbb{C}$  von  $\mathcal{X} := \mathcal{H}^*/\Gamma$  und sei der Einfachheit halber  $C$  von Geschlecht 0. Wir wählen einen Parameter  $t$  auf  $C$ .

Wir betrachten die Überlagerung  $\mathcal{H}^* \rightarrow C$ . Die Zuordnung  $z := z(t)$  ist nur modulo  $\Gamma$  wohldefiniert. Wir fassen  $t \mapsto z(t)$  jedoch als mehrwertige Funktion auf und definieren  $z' := \frac{dz}{dt}$ . Die folgende Ableitung ist aber wohldefiniert und holomorph außerhalb einer endlichen Menge  $S$  von Punkten auf  $\mathcal{H}^*$ :

**3.1.9 Definition.** Man nennt die meromorphe Funktion

$$S_t(z) = \frac{2z'z''' - 3(z'')^2}{(z')^2}$$

die *Schwarzsche Ableitung* von  $z := z(t)$ .

**3.1.10 Proposition ([Yos87, §4.1]).** Die Schwarzsche Ableitung  $S_t(z)$  erfüllt folgende Eigenschaften:

- (i) Die Schwarzsche Ableitung  $S_t(z)$  verschwindet genau dann, wenn  $z$  eine gebrochene lineare Transformation von  $t$  ist.
- (ii) Ist  $t_1$  eine nicht-konstante Funktion in  $t$ , dann gilt die Regel

$$S_{t_1}(z) = \left( \frac{dt}{dt_1} \right)^2 S_t(z) + S_{t_1}(t).$$

BEWEIS. Beide Eigenschaften (i) und (ii) kann man elementar nachrechnen. Ein alternativer Beweis wird in [Yos87, §4.2] bzw. [Yos87, § 4.3] gegeben.  $\square$

Aus Proposition 3.1.10 folgt, dass  $S_t(z)$  unabhängig von der Wahl des Parameters  $t$  und der Wahl der Abbildung  $t \mapsto z(t)$  ist. Somit können wir  $S_t(z)$  als meromorphe Funktion auf  $C$  auffassen. Wir ordnen der Schwarzschen Ableitung in Definition 3.1.12 eine Fuchssche Differentialgleichung zu. Zunächst bestimmen wir dazu in Proposition 3.1.11 die Pole von  $S_t(z)$ .

**3.1.11 Proposition ([Yos87, §4.4]).** Die Pole der Schwarzschen Ableitung  $S_t(z)$  in  $C$  liegen genau in den Spitzen und in den elliptischen Punkten von  $C \simeq \mathcal{X}$  (Definition 2.2.3). In einer Spitze hat  $S_t(z)$  einen doppelten Pol mit Leitkoeffizient  $-1$ . In einem elliptischen Punkt von Ordnung  $e$  hat  $S_t(z)$  einen doppelten Pol mit Leitkoeffizient  $(1 - e^{-2})$ .

BEWEIS. In einem elliptischen Punkt  $x_j \in C$  ist  $\mathcal{H} \rightarrow C$  verzweigt mit Index  $e_j$ , da der Stabilisator genau  $e_j$  Elemente hat. Lokal in diesem Punkt ist  $z = t^{1/e_j} \cdot h$  mit holomorpher Funktion  $h = c_0 + c_1 t + \dots$ . Damit rechnet man die Proposition elementar nach. Für die Spitzen zeigt man dies ähnlich.  $\square$

**3.1.12 Definition.** Wir nennen die Fuchssche Differentialgleichung

$$L: u'' + S_t(z)u = 0 \quad (3.3)$$

die *uniformisierende Differentialgleichung* von  $\mathcal{X}$ .

Die Lösungen von  $L$  hängen wie folgt mit der Funktion  $z(t)$  zusammen.

**3.1.13 Satz ( [Yos87, §4.2] ).** Sei  $\Gamma < \mathrm{SL}_2(\mathbb{R})$  eine Fuchssche Gruppe und  $z(t)$  die mehrwertige Funktion wie in 3.1.8. Sei  $L$  die uniformisierende Differentialgleichung von  $\mathcal{X} := \mathcal{H}^*/\Gamma$  wie in Definition 3.1.12. Dann existieren zwei linear unabhängige Lösungen  $u_0(t)$  und  $u_1(t)$  von  $L$  über  $\mathbb{C}$ , so dass  $z(t) = \frac{u_0(t)}{u_1(t)}$  gilt.

BEWEIS. Setze  $u_0 = (z')^{-1/2}$  und  $u_1 = z \cdot u_0$ . Man rechnet nach, dass  $W(u_0, u_1) = 1$ . Man berechnet die Differentialgleichung mit Lösungsraum  $\mathbb{C}u_0 \oplus \mathbb{C}u_1$  aus Proposition 3.1.5. Man rechnet elementar nach, dass dies die obige Gleichung (3.3) ergibt.  $\square$

**3.1.14 Satz.** Seien die Annahmen und Bezeichnungen wie in Satz 3.1.13. Sei desweiteren  $\Gamma(L)$  die Monodromie-Gruppe der uniformisierenden Differentialgleichung (3.3). Dann sind  $\Gamma(L)$  und  $\Gamma$  konjugiert.

BEWEIS. Man betrachtet die Lösungen  $u_0, u_1$  aus dem Beweis von Satz 3.1.13. Ändert sich  $z$  projektiv, so ändert sich der Lösungsraum von  $L$  linear. Das liefert die Behauptung.  $\square$

**3.1.15 Beispiel ( [Yos87, §5.3] ).** Sei  $\Gamma := \Delta(e_1, e_2, e_3) < \mathrm{SL}_2(\mathbb{R})$  eine Dreiecksgruppe wie in Definition 2.2.11. Insbesondere korrespondiert zu  $e_i$  eine Spitze, falls  $e_i = \infty$  ist, und sonst ein elliptischer Punkt von Ordnung  $e_i$ . Dann ist die uniformisierende Differentialgleichung  $L$  von  $\mathcal{H}^*/\Gamma$  eindeutig bestimmt. Seien nämlich o.B.d.A. nach Transformation die elliptischen Punkte bzw. Spitzen zu  $e_i$  gegeben durch die Punkte  $0, 1, \infty \in \mathbb{P}^1(\mathbb{C})$ . Dann ist  $L$  gegeben durch die *hypergeometrische Differentialgleichung*

$$L: x(x-1)u'' + [c - (a+b+1)x]u' - abu = 0$$

für  $a, b, c \in \mathbb{C}$  mit

$$|1-c| = \frac{1}{e_1}, \quad |c-a-b| = \frac{1}{e_2}, \quad |a-b| = \frac{1}{e_3}.$$

Die Lösungen von  $L$  können mit Hilfe der hypergeometrischen Funktionen (für die Definition siehe [Yos87, §1.1]) explizit angegeben werden.

Zum Beispiel ist die uniformisierende Differentialgleichung zu  $\Delta(\infty, \infty, \infty)$

gegeben durch die *Gaußsche hypergeometrische Differentialgleichung*

$$L : x(x-1)u'' + [2x-1]u' + \frac{1}{4}u = 0.$$

Diese entspricht der Modulkurve  $X(2)$ . Eine Basis von Lösungen von  $L$  um  $\lambda_0 := \frac{1}{2}$  ist für den Parameter  $t := 1 - 2\lambda$  wie folgt gegeben:

$$\begin{aligned} f_1(\lambda) &= F\left(\frac{1}{4}, \frac{1}{4}, \frac{1}{2}; t^2\right) \\ &= 1 + \frac{1}{8}t^2 + \frac{25}{384}t^4 + \frac{45}{1024}t^6 + \frac{7605}{229376}t^8 + \dots, \\ f_2(\lambda) &= -\frac{1}{2}t \cdot F\left(\frac{3}{4}, \frac{3}{4}, \frac{3}{2}; t^2\right) \\ &= -\left(\frac{1}{2}t + \frac{3}{16}t^3 + \frac{147}{1280}t^5 + \frac{847}{10240}t^7 + \dots\right). \end{aligned}$$

## 3.2 Picard-Fuchs Differentialgleichung

In diesem Abschnitt geben wir eine alternative Interpretation der uniformisierenden Differentialgleichung (3.3) als Picard-Fuchs Differentialgleichung. Dies liefert den Hintergrund für die Anwendungen in den Kapiteln 4 und 5. Wir folgen dem Artikel [Möl05].

Sei  $\Gamma < \mathrm{SL}_2(\mathbb{R})$  eine arithmetische Fuchssche Gruppe und  $\mathcal{X} := \mathcal{H}^*/\Gamma$  die korrespondierende Shimura-Kurve über  $\mathbb{C}$ . Sei  $\tilde{\mathcal{X}}$  eine endliche Überlagerung von  $\mathcal{X}$ , z.B. gegeben durch Hinzufügen einer Stufenstruktur, so dass eine endliche Menge  $S \subset \tilde{\mathcal{X}}$  und eine Familie

$$\mathfrak{A} \rightarrow \tilde{\mathcal{X}} \setminus S$$

von abelschen Varietäten mit Stufenstruktur existiert ([Möl05, Seite 5]).

Bezeichne  $\Omega_{\tilde{\mathcal{X}}}^1(\log S)$  die Garbe der Differenzialformen auf  $\tilde{\mathcal{X}}$  mit höchstens logarithmischen Singularitäten in  $S \subset \tilde{\mathcal{X}}$ .

**3.2.1 Definition.** Wir nennen ein Paar  $(\mathcal{E}, \nabla)$  bestehend aus einem Vektorbündel  $\mathcal{E}$  über  $\tilde{\mathcal{X}}$  und einem logarithmischen Zusammenhang (Definition 3.3.2)

$$\nabla : \mathcal{E} \rightarrow \mathcal{E} \otimes \Omega_{\tilde{\mathcal{X}}}^1(\log S)$$

ein *flaches Vektorbündel* über  $\mathcal{X}$ .

Wir betrachten das flache Vektorbündel  $H := H_{\mathrm{dR}}^1(\mathfrak{A}/\tilde{\mathcal{X}} \setminus S)$  mit seinem Gauß-Manin-Zusammenhang  $\nabla : H \rightarrow H \otimes \Omega_{\tilde{\mathcal{X}}}^1(\log S)$  ([KO68, §2]). Das Vektorbündel  $H$  ist mit einer kanonischen Filtrierung

$$H := \mathrm{Fil}^0(H) \supset \mathrm{Fil}^1(H)$$

versehen, der *Hodge-Filtrierung*. Man sagt,  $H$  definiert zusammen mit der Hodge-Filtrierung eine Variation von Hodge-Strukturen (VHS). Dabei muss

man besondere Rücksicht auf die Singularitäten  $x \in S$  nehmen. Für eine genaue Definition siehe zum Beispiel [Möl05] oder [BDIP02, § 7A]. An der VHS kann man ablesen, ob eine Familie von abelschen Varietäten zu einer Shimura-Kurve gehört ([Möl05, Thm. 1.2]).

**3.2.2 Definition.** Sei  $(\mathcal{E}, \nabla)$  ein flaches Vektorbündel von Rang 2 mit einem Geradenbündel  $\text{Fil}^1(\mathcal{E}) \subset \mathcal{E}$ , so dass  $\text{Gr}^1(\mathcal{E}) := \mathcal{E}/\text{Fil}^1(\mathcal{E})$  ebenfalls ein Geradenbündel ist. Dann nennen wir den Morphismus

$$\kappa : \text{Fil}^1(\mathcal{E}) \rightarrow \text{Gr}^1(\mathcal{E}) \otimes \Omega_{\tilde{\mathcal{X}}}^1(\log S)$$

gegeben durch

$$\kappa : \text{Fil}^1(\mathcal{E}) \hookrightarrow \mathcal{E} \xrightarrow{\nabla} \mathcal{E} \otimes \Omega_{\tilde{\mathcal{X}}}^1(\log S) \xrightarrow{\text{proj}} \text{Gr}^1(\mathcal{E}) \otimes \Omega_{\tilde{\mathcal{X}}}^1(\log S)$$

die Kodaira-Spencer Abbildung.

**3.2.3 Satz ( [Möl05, Thm. 1.2] ).** Seien die Bezeichnungen wie oben, insbesondere korrespondiere die Familie  $\mathfrak{A} \rightarrow \tilde{\mathcal{X}} \setminus S$  zu einer Shimura-Kurve. Dann existiert ein flaches Untervektorbündel  $(\mathcal{E}, \nabla|_{\mathcal{E}}) \subset (H, \nabla)$  von Rang 2 mit folgenden Eigenschaften:

- (i)  $\text{Fil}^1(\mathcal{E}) := \text{Fil}^1(H) \cap \mathcal{E}$  ist ein Geradenbündel,
- (ii) die Kodaira-Spencer Abbildung  $\kappa : \text{Fil}^1(\mathcal{E}) \rightarrow \text{Gr}^1(\mathcal{E}) \otimes \Omega_{\tilde{\mathcal{X}}}^1(\log S)$  ist ein Isomorphismus.

**3.2.4 Bemerkung.** Man kann sich die Bedingung an die Kodaira-Spencer Abbildung wie folgt erklären. Sei die Familie  $E_t$  von elliptischen Kurven für ein Parameter  $t$  über  $\mathbb{C} \setminus \{0, \infty\}$  gegeben durch

$$E_t : y^2 = t \cdot x(x-1)(x+1).$$

Wähle  $D := \frac{d}{dt}$  und den globalen Schnitt  $\omega := \frac{dx}{2y} \in H^0(E_t, \Omega_{E_t})$ . Dann gilt  $\nabla(D)(\omega) = \omega$  und folglich verschwindet die Kodaira-Spencer Abbildung. Dies liegt daran, dass die Familie  $E_t$  isotrivial ist, d.h. die Fasern  $E_t$  zueinander isomorph sind. Dies kann aber in einer Familie, die zu einer Shimura-Kurve gehört, nicht auftreten.

**3.2.5 Definition ( [BW06, Def. 2.1] ).** Wir nennen ein flaches Vektorbündel  $(\mathcal{E}, \nabla)$  von Rang 2 mit den Eigenschaften (i) und (ii) aus Satz 3.2.3 ein *ursprüngliches Bündel*.

Wir stellen jetzt den Zusammenhang zwischen dem ursprünglichen Bündel  $\mathcal{E} \subset H$  und einer gewöhnlichen linearen Differentialgleichung her. Dazu folgen wir [BW06, §5]. Wir nehmen an, dass  $\tilde{\mathcal{X}} \simeq \mathbb{P}^1$  und  $S \neq \emptyset$

gilt. Bezeichne  $t$  den Standard-Parameter auf  $\mathbb{P}^1$  und  $D := \frac{d}{dt}$ . Sei o.B.d.A. nach Koordinatentransformation  $\infty \in S$ . Sei  $\omega \in \text{Fil}^1(\mathcal{E})(\mathbb{P}^1 \setminus \{\infty\})$  ein globaler Schnitt. Dann erfüllt  $\omega$  bezüglich  $D$  eine Fuchssche Differentialgleichung zweiter Ordnung  $L$ . Man nennt diese die *Picard-Fuchs Differentialgleichung*.

In [BM10, Prop. 2.2] ist ein explizites Kriterium für das Verschwinden der Kodaira-Spencer Abbildung an die lokalen Exponenten der Picard-Fuchs Differentialgleichung gegeben.

**3.2.6 Beispiel.** Wir betrachten erneut die Fuchssche Gruppe  $\Gamma(2)$  also die Dreiecksgruppe  $\Delta(\infty, \infty, \infty)$ . Diese gehört zur Modulkurve  $X(2) := \mathcal{H}^*/\Gamma(2)$ . In Beispiel 3.1.15 haben wir die uniformisierende Differentialgleichung berechnet. Tatsächlich existiert eine universelle Familie

$$E_\lambda : y^2 = x(x-1)(x-\lambda) \quad (3.4)$$

über  $C := \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ . Man betrachtet das 2-dimensionale Vektorbündel  $H := H_{\text{dR}}^1(E_\lambda/C)$ . Dieses ist gegeben durch den Quotient der Differentiale zweiter Gattung auf  $E_\lambda$  modulo den exakten Differentialen. Eine Basis der globalen Schnitte von  $H$  ist gegeben durch

$$\omega_0 := \frac{dx}{2y} \quad \text{und} \quad \omega_1 := \frac{x dx}{2y}.$$

Für den Parameter  $\lambda$  auf  $C$  ist der Gauß-Manin-Zusammenhang gegeben durch

$$\nabla\left(\frac{d}{d\lambda}\right) : H \rightarrow H,$$

also durch formales Differenzieren. Man rechnet damit folgende Identität aus:

$$\lambda(\lambda-1)\omega_0'' + (2\lambda-1)\omega_0' + \frac{1}{4}\omega_0 = d\left(\frac{y}{(x-\lambda)^2}\right).$$

Das Ergebnis ist ein exaktes Differential, somit erfüllt  $\omega_0$  die Differentialgleichung

$$L : \lambda(\lambda-1)u'' + [2\lambda-1]u' + \frac{1}{4}u = 0. \quad (3.5)$$

Vergleicht man dies mit Beispiel 3.1.15 sieht man also, dass die Picard-Fuchs Differentialgleichung und die uniformisierende Differentialgleichung gleich sind.

Man kann mittels der Picard-Fuchs Differentialgleichung arithmetische Eigenschaften der universellen Familie beweisen.

**3.2.7 Beispiel ( [BW06, Exa. 4.5] ).** Wir betrachten wiederum das Beispiel der Modulcurve  $X(2)$  und ihrer Picard-Fuchschen Differentialgleichung  $L$  (3.5). Die Modulcurve  $X(2)$  sowie ihre universelle Familie  $E_\lambda \rightarrow C$  (3.4) sind über  $\mathbb{Z}[\frac{1}{2}]$  definiert. Folglich macht es Sinn, die Familie  $E_\lambda$  und ihre Picard-Fuchs Differentialgleichung auch in positiver Charakteristik  $p \neq 2$  zu betrachten. Die Theorie der Lösungen von Differentialgleichungen in positiver Charakteristik ist etwas anders ([Hon81]): Sei  $k$  ein endlicher Körper der Charakteristik  $\text{char}(k) = p$ . Das Hasse-Polynom

$$\Phi := \sum_{i=0}^m \binom{m}{i}^2 \lambda^i \quad \text{für} \quad m := \frac{p-1}{2}$$

liefert eine Basis des Lösungsraums von  $L$  über  $k[\lambda^p]$ . Für  $\Phi$  gilt, dass dessen Nullstellen alle in  $\mathbb{F}_{p^2}$  liegen. Der Zusammenhang mit der universellen Familie ist wie folgt gegeben: Ein Element  $\lambda_0 \in \mathbb{F}_{p^2}$  ist genau dann Nullstelle von  $\Phi$ , falls die elliptische Kurve  $E_{\lambda_0}$  supersingulär ist. Der Grund dafür liegt darin, dass der Frobenius-Morphismus  $F$  auf  $H_{\text{dr}}^1(E_\lambda/R)$  horizontal ist. Dabei sei  $R := W[[\lambda, 1/\lambda(\lambda-1)\tilde{\Phi}]]$  für einen beliebigen Lift  $\tilde{\Phi}$  des Hasse-Polynoms  $\Phi$ .

**3.2.8 Bemerkung.** Die Berechnungen in Kapitel 5, vor allem Proposition 5.1.3, sind eine direkte Verallgemeinerung der Berechnungen für  $X(2)$ .

### 3.3 Definition von $F$ -Kristallen

In diesem Abschnitt fassen wir Allgemeines zu  $F$ -Kristallen zusammen. Wir orientieren uns dabei an [Del81, §1].

Sei  $k$  ein algebraisch abgeschlossener Körper der Charakteristik  $p$ . Bezeichne  $W := W(k)$  den Ring der Witt-Vektoren und  $\sigma$  den Frobenius-Morphismus auf  $W$ . Seien  $R := W[[t]]$  und  $\bar{R} := k[[t]]$  die Potenzreihenringe zu den Variablen  $t := (t_1, \dots, t_n)$ .

Wir möchten nun definieren, was wir unter einem  $F$ -Kristall auf  $\bar{R}$  verstehen. Dazu benötigen wir folgende Definitionen:

**3.3.1 Definition.** Ein Lift  $\varphi : R \rightarrow R$  des Frobenius-Morphismus  $k \rightarrow k$  zu einem Morphismus von  $R$  nennen wir  $\sigma$ -linear oder auch *kompatibel* mit  $\sigma$ , falls  $\varphi \circ \sigma$  linear ist.

Zum Beispiel ist ein  $\sigma$ -linearer Lift gegeben durch

$$\begin{aligned} \varphi(t_i) &:= t_i^p, & \text{für } i = 1, \dots, n, \\ \varphi(a) &:= \sigma(a), & \text{für } a \in W. \end{aligned}$$

**3.3.2 Definition.** Sei  $H$  ein freier  $R$ -Modul. Ein *Zusammenhang* auf  $H$  ist ein Morphismus

$$\nabla : H \rightarrow H \otimes \Omega_{R/W}^1,$$

der die Leibniz-Regel erfüllt, d.h. es gilt

$$\nabla(c \cdot a) = c\nabla(a) + a \otimes dc$$

für alle  $a \in H$  und  $c \in R$ .

**3.3.3 Bemerkung.** Mittels der Isomorphie  $\text{Hom}(\Omega_{R/W}^1, R) \simeq \text{Der}(R)$  kann man den Zusammenhang auch als einen Morphismus  $\nabla : \text{Der}_W(R) \rightarrow \text{End}(H)$  interpretieren.

In Abschnitt 3.2, insbesondere Beispiel 3.2.6, haben wir bereits Beispiele für einen Zusammenhang gesehen.

**3.3.4 Definition.** Wir nennen einen Zusammenhang

$$\nabla : H \rightarrow H \otimes \Omega_{R/W}^1$$

- *integrierbar*, falls für die zugehörigen Endomorphismen

$$\nabla(d/dt_i)\nabla(d/dt_j) = \nabla(d/dt_j)\nabla(d/dt_i)$$

gilt,

- und *topologisch nilpotent*, falls die Reduktion

$$\nabla \otimes_W k : H \otimes_W k \rightarrow H \otimes \Omega_{R/W}^1 \otimes_W k$$

nilpotent ist.

**3.3.5 Definition.** Ein *Kristall* auf  $\bar{R}$  ist ein freier  $R$ -Modul  $H$  endlichen Typs mit einem integrierbaren, topologisch nilpotenten Zusammenhang

$$\nabla : H \rightarrow H \otimes \Omega^1(A/R).$$

**3.3.6 Definition.** Wir nennen einen Morphismus  $\alpha : H \rightarrow H'$  zwischen Kristallen  $(H, \nabla)$  und  $(H', \nabla')$  *horizontal*, falls folgendes Diagramm kommutiert:

$$\begin{array}{ccc} H & \xrightarrow{\nabla} & H \otimes \Omega^1(A/R) \\ \alpha \downarrow & & \downarrow \alpha \otimes 1 \\ H' & \xrightarrow{\nabla'} & H' \otimes \Omega^1(A/R). \end{array}$$

**3.3.7 Bemerkung.** Sei  $\varphi : R \rightarrow R$  ein  $\sigma$ -linearer Lift des Frobenius-Morphismus auf  $\overline{R}$ . Und sei  $(H, \nabla)$  ein Kristall. Dann induziert  $\varphi$  auf  $\varphi^*H$  einen Zusammenhang  $\varphi^*\nabla$  und eine Struktur als Kristall.

**3.3.8 Lemma ( [Kat73, §1.2] ).** Seien  $\varphi, \psi : R \rightarrow R$  zwei  $\sigma$ -lineare Lifts des Frobenius-Morphismus auf  $\overline{R}$ . Dann existiert ein eindeutiger Isomorphismus

$$\chi(\varphi, \psi) : \varphi^*H \xrightarrow{\sim} \psi^*H.$$

**3.3.9 Definition.** Ein  $F$ -Kristall ist ein Kristall  $(H, \nabla)$  über  $\overline{R}$ , so dass für alle  $\sigma$ -kompatible Lifts  $\varphi : R \rightarrow R$  des Frobenius-Morphismus auf  $\overline{R}$  ein horizontaler Homomorphismus  $F(\varphi) : \varphi^*H \rightarrow H$  existiert, der einen Isomorphismus  $F(\varphi) \otimes \mathbb{Q}_p : \varphi^*H \otimes \mathbb{Q}_p \rightarrow H \otimes \mathbb{Q}_p$  induziert.

Ausserdem fordern wir, dass für zwei  $\sigma$ -kompatible Lifts  $\varphi, \psi : R \rightarrow R$  folgendes Diagramm kommutiert

$$\begin{array}{ccc} \varphi^*H & \xrightarrow{F(\varphi)} & H \\ \chi(\varphi, \psi) \downarrow & & \nearrow F(\psi) \\ \psi^*H & & . \end{array}$$

**3.3.10 Definition.** Wir nennen einen Untermodul  $H_0$  eines  $F$ -Kristalls  $H$  (topologisch) *nilpotent*, falls ein Morphismus  $\varphi : R \rightarrow R$  wie in Definition 3.3.9 existiert, für den  $F(\varphi)$  auf  $H_0$  topologisch nilpotent ist.

Sei nun ein Lift  $\varphi : R \rightarrow R$  des Frobenius-Morphismus wie in der Definition 3.3.9 fest gewählt und sei  $H$  ein  $F$ -Kristall. Bezeichne dann  $F(\varphi)$  den horizontalen Morphismus von  $H$ .

Bezeichne  $\overline{s} : \overline{R} \rightarrow k'$  einen Punkt in  $\mathrm{Spf}(\overline{R})$  mit Werten in einer algebraisch abgeschlossenen Erweiterung  $k'/k$ . Bezeichne  $s : R \rightarrow W(k')$  den Teichmüller-Lift von  $\overline{s}$  bezüglich  $\varphi$ , d.h. den eindeutigen Lift  $s$  von  $\overline{s}$  nach  $W(k')$  für den  $s\varphi = \sigma s$  gilt. Aus dieser Eigenschaft beweist man elementar das folgende Lemma.

**3.3.11 Lemma ( [Del81, §1.1.4] ).** Das Tripel  $(s^*H, s^*\nabla, s^*F(\varphi))$  ist ein  $F$ -Kristall.

Sei  $\varphi'$  ein weiterer Lift des Frobenius-Morphismus wie in Definition 3.3.9 und  $F(\varphi')$  der zugehörige Morphismus. Sei  $s' : R \rightarrow W(k')$  der zu  $\varphi'$  gehörende Teichmüller-Lift von  $\overline{s}$ . Dann existiert ein eindeutiger Isomorphismus  $s^*H \rightarrow (s')^*H$  von  $F$ -Kristallen. Man nennt deshalb  $s^*H$  das von  $H$  induzierte  $F$ -Kristall bei  $\overline{s}$ .

### 3.4 $F$ -Kristalle gewöhnlicher formaler abelscher Schemata

In diesem Abschnitt beschreiben wir die Struktur von gewöhnlichen  $F$ -Kristallen, d.h. von  $F$ -Kristallen gewöhnlicher abelscher Schemata. Sei dazu  $\pi : A \rightarrow \mathrm{Spf}(R)$  ein formales abelsches Schema von relativer Dimension  $g$ .

**3.4.1 Definition.** Sei

$$H_{\mathrm{dR}}^i(A/R) := \mathbb{R}^i \pi_* (\Omega_{A/R}^\bullet),$$

wobei  $\mathbb{R}^i \pi_*$  den hyper-abgeleiteten Funktor von  $\pi_*$  bezeichnet. Wir bezeichnen die  $R$ -Moduln  $H_{\mathrm{dR}}^i(A/R)$  mit ihrer Graduierung als die relative *de-Rham-Kohomologie* von  $A$  über  $R$ .

Wir betrachten im Folgenden den Modul  $H := H_{\mathrm{dR}}^1(A/R)$  von Rang  $2g$  über  $R$ . Die folgenden zwei Sätze definieren eine  $F$ -Kristall-Struktur auf  $H$ .

**3.4.2 Satz ( [KO68, Thm. 1] ).** *Es existiert ein kanonischer integrierbarer Zusammenhang*

$$\nabla : H \rightarrow H \otimes \Omega^1(A/R)$$

auf  $H$ . Dieser Zusammenhang wird Gauß-Manin-Zusammenhang genannt.

Der Vergleich mit der kristallinen Kohomologie ([BO78, §7]) liefert den folgenden Satz.

**3.4.3 Satz ( [Kat73, §8] ).** *Der Gauß-Manin-Zusammenhang  $\nabla$  auf  $H$  ist topologisch nilpotent und  $(H, \nabla)$  ist ein  $F$ -Kristall.*

Betrachte im Folgenden den  $R$ -Modul  $H$  mit ihrer Struktur als  $F$ -Kristall, definiert in Satz 3.4.3. Wähle einen festen Lift  $\varphi : R \rightarrow R$  des Frobenius-Morphismus auf  $\bar{R}$  und einen horizontalen Morphismus  $F(\varphi)$  wie in der Definition 3.3.9. Bezeichne die Reduktion von  $H$  mit  $\bar{H} := H \otimes_R k$  und sei  $F_0 := F(\varphi) \otimes_R k$ . Es gilt  $\bar{H} = \bar{H}^{\mathrm{nil}} \oplus \bar{H}^{\mathrm{ss}}$ , wobei  $\bar{H}^{\mathrm{nil}} := \bigcup \mathrm{Ker} F_0^n$  den nilpotenten und  $\bar{H}^{\mathrm{ss}} := \bigcap \mathrm{Im} F_0^n$  den semistabilen Teil von  $\bar{H}$  bezeichnet. Im Fall, dass  $H$  zu einem gewöhnlichen abelschen Schema  $A/\mathrm{Spf} W$  gehört, induziert diese Zerlegung auf der Reduktion  $\bar{H}$  eine Zerlegung auf dem  $F$ -Kristall  $H$  (siehe Proposition 3.4.8). Im Folgenden wollen wir dies diskutieren.

**3.4.4 Definition.** Definiere die *Hodge-Filtrierung* auf  $\bar{H}$  als

$$\mathrm{Fil}^i(\bar{H}) := \{x \in \bar{H} : \exists y \in H, y \text{ reduziert zu } x \text{ und } F(\varphi)\varphi^* y \in p^i H\}.$$

**3.4.5 Definition.** Wir nennen eine Filtrierung

$$H = \text{Fil}^0(H) \supseteq \text{Fil}^1(H) \supseteq \dots$$

durch freie  $R$ -Moduln  $\text{Fil}^i(H)$  auf  $H$  *Hodge-Filtrierung*, falls folgende Eigenschaften erfüllt sind:

- (i)  $\text{Fil}^i(H) \otimes k = \text{Fil}^i(\overline{H})$ ,
- (ii)  $\nabla \text{Fil}^i(H) \subset \text{Fil}^{i-1}(H) \otimes \Omega_{R/W}^1$ , für  $i > 0$ .

**3.4.6 Satz ([Del81, §2.1A]).** Auf  $H$  existiert eine Hodge-Filtrierung, die wir wie in Definition 3.4.5 bezeichnen. Sie hat Stufe  $\leq 1$ , d.h.  $\text{Fil}^i(H)$  ist trivial für  $i \geq 2$ . Die Filtrierung ist eindeutig und unabhängig von der Wahl des  $\sigma$ -linearen Lifts  $\varphi : R \rightarrow R$  des Frobenius-Morphismus auf  $\overline{R}$ .

**3.4.7 Definition.** Wir nennen ein  $F$ -Kristall  $H$  ein *Unit-Root  $F$ -Kristall*, falls es einen Morphismus  $\varphi : R \rightarrow R$  wie in Definition 3.3.9 gibt, für den  $F(\varphi)$  einen Isomorphismus auf  $H$  definiert.

**3.4.8 Proposition ([Del81, Prop. 1.3.2]).** Sei  $s^*A \otimes k$  gewöhnlich für alle Punkte  $s : R \rightarrow k'$  in  $\text{Spf } R$ . Dann existiert ein Unit-Root- $F$ -Kristall  $U \subset H$  von Rang  $g$ , für das  $H = U \oplus \text{Fil}^1(H)$  erfüllt ist.

**3.4.9 Bemerkung.** Im Beweis von [Kat73, Thm. 4.1] wird das  $R$ -Modul  $U$  explizit konstruiert.

## 3.5 Deformation gewöhnlicher abelscher Varietäten

In diesem Abschnitt definieren wir die  $q$ -Parameter (Satz 3.5.8). Dies sind explizite Koordinaten des Modulraums von Lifts einer gewöhnlichen abelschen Varietät (Definition 3.5.1).

Sei dazu  $\overline{A}$  eine gewöhnliche abelsche Varietät der Dimension  $g$  über einem endlichen Körper  $k$  der Charakteristik  $p$ . Bezeichne mit  $W := W(k)$  den Ring der Witt-Vektoren über  $k$ . Sei  $\mathcal{S}$  die Kategorie der Mengen und sei  $\mathcal{C}_W$  die Kategorie der artinschen, lokalen  $W$ -Algebren  $R$ , zusammen mit Isomorphismen  $R/\mathfrak{m}_R \simeq k$ , so dass folgendes Diagramm kommutiert:

$$\begin{array}{ccc} W & \longrightarrow & R \\ \downarrow & & \downarrow \\ k & \xrightarrow{\cong} & R/\mathfrak{m}_R. \end{array}$$

Sei  $\hat{\mathcal{C}}_W$  die Kategorie der vollständigen, lokalen, noetherschen  $W$ -Algebren  $R$ , so dass  $R/\mathfrak{m}_R^n \in \mathcal{C}_W$  für jede natürliche Zahl  $n \in \mathbb{N}$  ist.

**3.5.1 Definition.** Wir definieren den lokalen Modulfunktor  $M$  als den kovarianten Funktor  $M : \mathcal{C}_W \rightarrow \mathcal{S}$  durch

$$M(R) := \left\{ \begin{array}{l} \text{Isomorphieklassen von } (A_0, \rho_0), \text{ wobei} \\ A_0 \rightarrow \text{Spec}(R) \text{ ein abelsches Schema} \\ \text{und } \rho_0 : A_0 \otimes k \xrightarrow{\sim} \bar{A} \text{ ein Isomorphismus ist} \end{array} \right\}.$$

**3.5.2 Theorem ([Oor71, Thm. 2.2.1]).** Der Funktor  $M$  ist darstellbar durch das formale Schema  $\text{Spf } R$  mit  $R := W[[t_1, \dots, t_{g^2}]]$ , d.h. es gibt eine natürliche Isomorphie

$$\hat{\mathcal{C}}_W(R, -) \xrightarrow{\sim} M(-)$$

und ein universelles formales abelsches Schema  $A \rightarrow \text{Spf } R$ .

**3.5.3 Satz.** Sei  $A_0$  ein formales abelsches Schema über  $W$  mit  $A_0 \otimes_W k = \bar{A}$ , dann existiert ein  $s \in \text{Spf}(R)$  mit  $A_0 \simeq s^*A$ . Sei umgekehrt ein  $s \in \text{Spf}(R)$  gegeben, dann existiert eine (nicht notwendigerweise separable) Erweiterung  $W'/W$  und ein formales abelsches Schema  $A_0$  über  $W'$ , so dass  $A_0 \simeq s^*A$  gilt.

BEWEIS. Sei  $W_n := W/\mathfrak{m}^{n+1}$ . Der Modulfunktor  $M$  ist darstellbar, Wir nennen ein System von abelschen Schemata  $X$  über  $S \otimes W_n$  kompatibel Nach [GD60, Thm. 10.12.3] und [GD61, Thm. 5.4.1] existiert eine Äquivalenz von Kategorien zwischen formalen abelschen Schemata über  $W$  und dem inversen Limes von kompatiblen abelschen Schemata über  $W_n$ . D.h. sei  $A$  ein formales abelsches Schema über  $W$  dann definiert  $A \otimes_W W_n$  ein kompatibles System, d.h. von abelschen Schemata und es gilt  $A = \varprojlim A_n$ . Da der lokale Modulfunktor darstellbar ist liefert dies auch kompatible Koordinaten im Deformationsraum.  $\square$

Es existiert eine formale Deformation  $A_{\text{can}}/\text{Spf } W$  von  $\bar{A}$ , die sich besonders auszeichnet. Tatsächlich ist  $A_{\text{can}}$  sogar algebraisierbar.

**3.5.4 Satz ([Mes72, Thm. V.3.3]).** Sei  $\bar{A}$  eine gewöhnliche abelsche Varietät über dem (perfekten) Körper  $k$ . Dann existiert ein eindeutiger Lift  $A_{\text{can}}$  von  $\bar{A}$  zu einem projektiven abelschen Schema über  $W$ , so dass der Morphismus  $\text{End}(A_{\text{can}}) \leftrightarrow \text{End}(\bar{A})$  ein Isomorphismus ist.

**3.5.5 Definition.** Wir nennen den eindeutigen Lift  $A_{\text{can}}$  aus Satz 3.5.4 den kanonischen Lift von  $\bar{A}$ . Wir bezeichnen den Punkt in  $M$  der zu  $A_{\text{can}}$  korrespondiert mit  $s_{\text{can}}$ . Wir nennen das Urbild  $\beta \in \text{End}(A_{\text{can}})$  eines Endomorphismus  $\bar{\beta} : \bar{A} \rightarrow \bar{A}$  unter dem Isomorphismus  $\text{End}(A_{\text{can}}) \xrightarrow{\sim} \text{End}(\bar{A})$  den kanonischen Lift von  $\bar{\beta}$ .

Sei die Situation wie in Satz 3.5.2 gegeben. D.h. sei  $A/M$  die universelle formale Deformation von  $\bar{A}$  und sei der Funktor  $M$  dargestellt durch das formale Schema  $\mathrm{Spf} R$  mit  $R := W[[t_1, \dots, t_{g^2}]]$ . Dann sind wir in der Situation von Abschnitt 3.4. Insbesondere gilt (Proposition 3.4.8), dass das  $F$ -Kristall  $H := H_{\mathrm{dR}}^1(A/M)$  eine Zerlegung  $H = \mathrm{Fil}^1(H) \oplus U$  in einen nilpotenten  $R$ -Modul  $\mathrm{Fil}^1(H)$  von Rang  $g$  und ein Unit-Root- $F$ -Kristall  $U$  über  $R$  von Rang  $g$  besitzt.

Wir möchten im folgenden eine Gruppenstruktur auf dem Deformationsraum  $\mathrm{Spf} R$  definieren (Satz 3.5.10). Diese soll die Eigenschaft besitzen, dass der Frobenius-Morphismus  $F(\Phi)$  auf  $R$  ein Gruppenhomomorphismus ist. Da der Frobenius-Morphismus auf  $\bar{A}$  sich zu einem Endomorphismus auf dem kanonischen Lift  $A_{\mathrm{can}}$  liften lässt, muss dieser dem neutralen Element der Gruppe entsprechen. Folgender Satz 3.5.6 zeigt die Existenz eines Frobenius-Morphismus  $F(\Phi)$  mit gewissen Eigenschaften, welche tatsächlich die notwendigen sind (Satz 3.5.10).

**3.5.6 Satz ( [Del81, §A3] ).** *In der Situation und Bezeichnung wie oben, existiert ein eindeutiger  $\sigma$ -kompatibler Lift  $\Phi : R \rightarrow R$  des Frobenius-Morphismus auf  $\bar{R}$ , so dass*

$$F(\Phi)(\Phi^*(\mathrm{Fil}^1(H))) \subset \mathrm{Fil}^1(H)$$

*gilt.*

Bezeichne  $\Phi : R \rightarrow R$  den Morphismus wie in Satz 3.5.6. Dann liefert uns die spezielle Wahl von  $\Phi$  eine Verfeinerung von [Del81, Satz 1.4.2].

**3.5.7 Satz ( [Del81, Kor. A2.1 zu 1.4.2] ).** *Es existieren Basen  $(a_i)_{1 \leq i \leq g}$  von  $U$ ,  $(b_i)_{1 \leq i \leq g}$  von  $\mathrm{Fil}^1 H$  und Elemente  $\eta_{i,j} \in \Omega_{R/W}^1$  mit folgenden Eigenschaften:*

$$\nabla a_i = 0, \tag{3.6}$$

$$\nabla b_i = \sum_j a_j \otimes \eta_{i,j} \in H \otimes \Omega_{R/W}^1, \tag{3.7}$$

$$F(\Phi)(\Phi^*(a_i)) = a_i, \tag{3.8}$$

$$F(\Phi)(\Phi^*(b_i)) = pb_i, \tag{3.9}$$

$$\Phi^*(\eta_{i,j}) = p\eta_{i,j}, \tag{3.10}$$

$$d\eta_{i,j} = 0. \tag{3.11}$$

**3.5.8 Satz ( [Del81, Kor. A2.1 zu 1.4.2] ).** *Seien die Basen  $(a_i)_{1 \leq i \leq g}$  von  $U$  und  $(b_i)_{1 \leq i \leq g}$  von  $\mathrm{Fil}^1 H$  wie in Satz 3.5.7 gewählt. Dann existiert eine eindeutige Familie  $\tau := (\tau_{i,j})$  von formalen Potenzreihen  $\tau_{i,j} \in \mathrm{Quot}(W)[[t]]$*

mit

$$d\tau_{i,j} = \eta_{i,j}, \quad (3.12)$$

$$\Phi^*(\tau_{i,j}) = p\tau_{i,j}, \quad (3.13)$$

$$s_{\text{can}}^* \tau_{i,j} = 0. \quad (3.14)$$

Desweiteren sind die Potenzreihen  $q_{i,j} := \exp(\tau_{i,j}) \in R$  wohldefiniert und es gilt:

$$\Phi^*(q_{i,j}) = q_{i,j}^p,$$

$$s_{\text{can}}^* q_{i,j} = 1.$$

**3.5.9 Definition.** Wir nennen die Familie  $q = (q_{i,j})$  aus Satz 3.5.8 die  $q$ -Parameter von  $A/M$ .

Die  $q$ -Parameter definieren im folgenden Sinne ein Koordinatensystem und eine Gruppenstruktur auf dem Deformationsraum.

**3.5.10 Satz ( [Del81, 2.1.3] ).** Die  $q$ -Parameter  $q = (q_{i,j})$  aus Satz 3.5.8 bilden mit  $p$  ein System regulärer Parameter von  $\text{Spf}(R)$ , d.h. der  $W$ -Morphismus

$$\begin{aligned} \text{Spf}(W[[x_{i,j}]]_{(i,j=1,\dots,g)}) &\longrightarrow \text{Spf}(R), \\ x_{i,j} &\longmapsto q_{i,j} - 1 \end{aligned}$$

ist ein Isomorphismus.

**3.5.11 Bemerkung ( [Del81, A2.2] ).** Satz 3.5.10 induziert eine Gruppenstruktur auf der formalen Faser des Deformationsraums von  $M$ , so dass der Frobenius-Morphismus  $F(\Phi)$  ein Gruppenhomomorphismus ist. Insbesondere entspricht  $s_{\text{can}} \in \text{Spf } R$  dem neutralen Element.

**3.5.12 Bemerkung.** Katz vergleicht im Appendix zu [Del81] die  $q$ -Parameter für den Deformationsraum von  $\bar{A}$  wie in Satz 3.5.8 mit den Serre-Tate-Parametern aus [Dwo71]. Er zeigt ([Del81, A3.1]), dass die Gruppenstruktur auf dem Deformationsraum  $M$ , induziert durch diese zwei verschiedenen Familien von Parametern, übereinstimmen.

## 3.6 Liftbarkeit von Isogenien

In diesen Abschnitt beschreiben wir Lifts von gewöhnlichen abelschen Varietäten zusammen mit zusätzlichen Morphismen. In [Mes72, Appendix Prop. 3.3] und [Kat81, Thm. 2.1] sind Bedingungen für die Liftbarkeit eines Morphismus  $\bar{\eta}$  in Termen der Wirkung von  $\bar{\eta}$  auf den Serre-Tate-Parametern gegeben.

Sei die Situation wie in Abschnitt 3.5 gegeben. Insbesondere sei  $\bar{A}$  eine gewöhnliche abelsche Varietät über  $k$ . Bezeichne  $A$  über  $\mathrm{Spf} R$  die universelle formale Deformation von  $\bar{A}$  (Satz 3.5.3). Wir schreiben  $H := H_{\mathrm{dR}}^1(A/R)$ . Das  $k$ -Modul  $\bar{H} := H \otimes_R k$  besitzt eine kanonische Filtrierung  $\mathrm{Fil}^1(\bar{H}) \subsetneq \bar{H}$ , die Hodge-Filtrierung. Und es existiert ein Komplement  $\bar{U} \subset \bar{H}$ , so dass  $\bar{H} = \mathrm{Fil}^1(\bar{H}) \oplus \bar{U}$  gilt. Da  $\bar{A}$  gewöhnlich ist, kann man diese Zerlegung von  $\bar{H}$  zu einer Zerlegung  $H = \mathrm{Fil}^1(H) \oplus U$  liften (Proposition 3.4.8). Dabei ist  $\mathrm{Fil}^1(H)$  nilpotent und  $U$  ein Unit-Root  $F$ -Kristall.

Angenommen  $\bar{A}$  besitzt eine Hauptpolarisierung  $\bar{\lambda} : \bar{A} \rightarrow \bar{A}^t$ . Diese Polarisierung definiert nach Prop. 2.1.2 eine Involution auf  $\mathrm{End}(\bar{A})$ , die wir mit

$$\dagger : \alpha \mapsto \alpha^\dagger$$

bezeichnen. Ausserdem liefert die Polarisierung  $\bar{\lambda}$  mittels folgender Proposition 3.6.1 eine Paarung

$$\langle \cdot, \cdot \rangle : H \times H \rightarrow R$$

auf  $H$ .

**3.6.1 Proposition ([Oda69, Prop. 3.24],[KO68, §2]).** *Es existiert eine symplektische Form  $\langle \cdot, \cdot \rangle : H \times H \rightarrow R$  auf  $H$ , d.h. die Paarung  $\langle \cdot, \cdot \rangle$  ist perfekt, bilinear und alternierend. Für beliebige  $\omega_1, \omega_2 \in H$  gelten außerdem folgende Identitäten:*

$$\langle F\omega_1, F\omega_2 \rangle = p \langle \omega_1, \omega_2 \rangle, \quad (3.15)$$

$$(\mathrm{Fil}^1(H))^\perp = \mathrm{Fil}^1(H), \quad (3.16)$$

$$U^\perp = U, \quad (3.17)$$

$$\langle \nabla \omega_1, \omega_2 \rangle + \langle \omega_1, \nabla \omega_2 \rangle = d \langle \omega_1, \omega_2 \rangle. \quad (3.18)$$

Sei  $(a_i) \subset U$ ,  $(b_i) \subset \mathrm{Fil}^1(H)$  die Basis wie in Satz 3.5.7. Wir bezeichnen mit  $s_{\mathrm{can}} \in \mathrm{Spf} R$  den Punkt im Deformationsraum, so dass  $s_{\mathrm{can}}^* A$  der kanonische Lift von  $\bar{A}$  ist. Nach geeigneter Wahl der Indizes ist die folgende Identität erfüllt:

$$\langle s_{\mathrm{can}}^* a_i, s_{\mathrm{can}}^* b_j \rangle = \delta_{i,j}. \quad (3.19)$$

Für  $s \in \mathrm{Spf} R$  möchten wir die Variation von Hodge-Strukturen im Sinne von Abschnitt 3.2 studieren. D.h. wir möchten für Punkte  $s \in \mathrm{Spf} R$  die Einbettungen  $s^* \mathrm{Fil}^1(H) \hookrightarrow s^* H$  von  $R$ -Moduln bezüglich dem Zusammenhang  $\nabla$  mittels der Paarung  $\langle \cdot, \cdot \rangle$  vergleichen. Dies können wir nur im offenen Einheitskreis um einen Punkt machen (Bemerkung 3.6.3). Diese korrespondiert zum folgenden Ring:

Sei  $R_0$  der folgende Unterring von  $R$ :

$$R_0 := \{f \in R : f \text{ konvergiert in } x \in W^n \text{ mit } |x_i| < 1 \forall i \in \{1, \dots, g\}\}. \quad (3.20)$$

Bezeichne  $L_0 := R_0 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$  den Quotientenkörper von  $R_0$ .

**3.6.2 Proposition ( [Kat73, Prop. 3.1] ).** *Es existieren Basisvektoren  $b'_i$  von  $\text{Fil}^1(H) \otimes_R L_0$  mit folgenden Eigenschaften:*

- (i) *die Vektoren  $b'_i$  sind horizontal, d.h. es gilt  $\nabla b'_i = 0$ ,*
- (ii) *die Vektoren  $b'_i$  sind Lifts von  $s_{\text{can}}^* b_i$  nach  $L_0$ , d.h. es gilt  $s_{\text{can}}^* b'_i = s_{\text{can}}^* b_i$ .*

**3.6.3 Bemerkung.** Satz 3.5.7 besagt, dass eine horizontale Fortsetzung nach  $R$  der Vektoren  $(s_{\text{can}}^* a_i)$  zu einer Basis von  $U$  existiert, also insbesondere nach  $L_0$ . Die horizontale Basis  $(s_{\text{can}}^* b_i)$  von  $s_{\text{can}}^* \text{Fil}^1(H)$  lässt sich aber nicht nach  $R$  zu einer horizontalen Basis von  $\text{Fil}^1(H)$  fortsetzen.

**3.6.4 Korollar ( [Kat73, Rem. 3.2] ).** *Sei  $L$  die Vervollständigung des algebraischen Abschlusses des Quotientenkörpers  $\text{Quot}(W)$  von  $W$ . Sei  $\mathcal{O}_L$  der lokale Ring von  $L$  und  $\mathfrak{m}_L$  dessen maximales Ideal. Sei  $s \in \text{Spf}(R_0)$  mit  $s \equiv s_{\text{can}} \pmod{\mathfrak{m}_L}$ . Dann liefert die Abbildung*

$$\begin{aligned} s^* H \otimes_R L &\xrightarrow{\sim} s_{\text{can}}^* H \otimes_R L \\ s^* b'_i &\longmapsto s_{\text{can}}^* b'_i \\ s^* a_i &\longmapsto s_{\text{can}}^* a_i. \end{aligned}$$

einen Isomorphismus von  $L$ -Vektorräumen, welcher eine Einbettung

$$\rho : s^* \text{Fil}^1(H) \hookrightarrow s_{\text{can}}^* H \otimes \text{Quot}(W)$$

von  $W$ -Moduln induziert.

**3.6.5 Proposition.** *In der Bezeichnung aus Prop. 3.6.2 erfüllen die Vektoren  $b'_i \in \text{Fil}^1(H) \otimes_R L_0$  und  $a'_i := a_i \otimes 1 \in H \otimes_R L_0$  folgende zusätzliche Eigenschaften:*

- (iii) *die Vektoren  $a'_i$  und  $b'_i$  bilden eine symplektische Basis von  $H \otimes_R L_0$ , d.h.*

$$\langle a'_i, a'_j \rangle = 0, \quad \langle b'_i, b'_j \rangle = 0, \quad \langle a'_i, b'_j \rangle = \delta_{i,j}. \quad (3.21)$$

- (iv) *die Vektoren  $b'_i$  sind Eigenvektoren von  $F(\Phi)$  mit  $F(\Phi)(\Phi^* b'_i) = p b'_i$ .*

BEWEIS. Die Eigenschaft (iii) folgt aus der Überlegung:

$$d\langle a'_i, b'_j \rangle \stackrel{(3.18)}{=} \langle \nabla a'_i, b'_j \rangle + \langle a'_i, \nabla b'_j \rangle = 0 \quad (3.22)$$

in  $H \otimes \Omega_{R/W}^1$ . Dabei folgt die letzte Identität daraus, dass  $a'_i$  und  $b'_j$  horizontal sind (Satz 3.5.7 und Proposition 3.6.2). Das impliziert, dass  $\langle a'_i, b'_j \rangle$  konstant ist. Ausserdem liften  $a'_i$  und  $b'_j$  die Vektoren  $s_{\text{can}}^* a_i$  und  $s_{\text{can}}^* b_j$ . Somit folgt aus (3.19) und (3.22) die Identität

$$\langle a'_i, b'_j \rangle = \langle s_{\text{can}}^* a_i, s_{\text{can}}^* b_j \rangle = \delta_{i,j}.$$

Die Eigenschaft (iv) zeigt man analog zur Eigenschaft (iii). Bezeichne mit  $c_{i,j} \in L_0$  und  $c'_{i,j} \in L_0$  die Koeffizienten in der Zerlegung

$$F(\Phi)(\Phi^* b'_i) = \sum c_{j,i} a'_i + \sum c'_{j,i} b'_j.$$

Der Frobenius-Morphismus ist horizontal, insbesondere gilt

$$\nabla \circ F(\Phi)(\Phi^* b'_i) = 0,$$

also sind die Koeffizienten  $c_{i,j}$  und  $c'_{i,j}$  konstant. Die Vektoren  $b'_i$  sind aber Lifts von  $s_{\text{can}}^* b_i$ , also folgt die Behauptung  $F(\Phi)(\Phi^* b'_i) = p b'_i$  aus (3.9).  $\square$

**3.6.6 Proposition.** Sei  $\tau := (\tau_{i,j})$  die Familie von formalen Potenzreihen mit Koeffizienten in  $\text{Quot}(W)$  aus Satz 3.5.8 und  $(b_i) \subset \text{Fil}^1(H)$  die Basis von  $\text{Fil}^1(H)$  aus Satz 3.5.7. Dann gelten für die Elemente  $b_i \otimes 1, b'_j \in H \otimes_R L_0$  folgende Identitäten

$$\tau_{i,j} = \langle b_i \otimes 1, b'_j \rangle. \quad (3.23)$$

Desweiteren gilt

$$b_i \otimes 1 = b'_i - \sum_j \tau_{i,j} a'_j. \quad (3.24)$$

BEWEIS. Wir schreiben für die Elemente  $b_i \otimes 1 \in H \otimes_R L_0$  abkürzend ebenfalls  $b_i$ . Es gilt

$$\begin{aligned} d\langle b_i, b'_j \rangle &\stackrel{(3.18)}{=} \langle \nabla b_i, b'_j \rangle + \langle b_i, \nabla b'_j \rangle \\ &\stackrel{\nabla b'_j=0}{=} \langle \nabla b_i, b'_j \rangle \\ &\stackrel{(3.7)}{=} \sum_l \langle a'_l, b'_j \rangle \eta_{i,l} \\ &\stackrel{(3.21)}{=} \eta_{i,j} \\ &\stackrel{(3.12)}{=} d\tau_{i,j}. \end{aligned}$$

Und da  $\langle s_{\text{can}}^* b_i, s_{\text{can}}^* b'_j \rangle = 0 = s_{\text{can}}^* \tau_{i,j}$  gilt, folgt (3.23). Die Gleichung (3.24) folgt elementar aus  $\langle a_i, b_j \rangle = \delta_{i,j}$ .  $\square$

**3.6.7 Definition.** Sei  $\text{Defo}(\bar{A})$  die Kategorie der formalen abelschen Schemata  $A_0$  über  $W$  mit  $A_0 \otimes_W k = \bar{A}$ . Die Morphismen von  $\text{Defo}(\bar{A})$  seien die Morphismen  $\eta : A_0 \rightarrow A_1$ , die zu Endomorphismen  $\eta \otimes_W k : \bar{A} \rightarrow \bar{A}$  reduzieren.

Der formale Deformationsraum von  $\bar{A}$  ist nach Satz 3.5.2 darstellbar durch das formale Schema  $\text{Spf } R$  und es existiert ein universelles formales abelsches Schema  $A$  über  $R$ . Bezeichne  $s_{\text{can}} \in \text{Spf } R$  den Punkt im Deformationsraum, so dass  $s_{\text{can}}^* A$  isomorph zum kanonischen Lift von  $\bar{A}$  (Definition 3.5.5) ist. Sei eine solche Isomorphie fest gewählt.

**3.6.8 Definition.** Bezeichne  $\text{Defo}'_{\text{Fil}}(\bar{A})$  folgende Kategorie: Die Objekte von  $\text{Defo}'_{\text{Fil}}(\bar{A})$  sind  $W$ -Moduln  $\mathcal{B} \subset H$  von Rang  $g$  und Einbettungen

$$\rho : \mathcal{B} \hookrightarrow s_{\text{can}}^* H \otimes \text{Quot}(W),$$

so dass

- der Quotient  $(s_{\text{can}}^* H \otimes \text{Quot}(W)) / (\rho(\mathcal{B}) \otimes \text{Quot}(W))$  frei ist,
- die Reduktion  $\mathcal{B} \otimes_W k$  kanonisch isomorph zu  $\text{Fil}^1(\bar{H})$  ist und
- die Reduktion  $\rho \otimes k$  die Identität auf  $\text{Fil}^1(\bar{H})$  ist.

Die Morphismen  $\mathcal{B} \rightarrow \tilde{\mathcal{B}}$  von  $\text{Defo}'_{\text{Fil}}(\bar{A})$  sind Paare  $(\beta_{\text{Fil}}, \bar{\beta})$ , wobei

- $\bar{\beta} : \bar{A} \rightarrow \bar{A}$  ein Endomorphismus von  $\bar{A}$  ist,
- $\beta_{\text{Fil}} : \mathcal{B} \rightarrow \tilde{\mathcal{B}}$  ein Morphismus von  $W$ -Moduln ist, der

$$\bar{\beta}^* : \text{Fil}^1(\bar{H}) \rightarrow \text{Fil}^1(\bar{H})$$

liftet und

- für den kanonischen Lift  $\beta_{\text{can}} : s_{\text{can}}^* A \rightarrow s_{\text{can}}^* A$  von  $\bar{\beta}$  (Definition 3.5.5) folgendes Diagramm kommutiert:

$$\begin{array}{ccc} \mathcal{B} & \xrightarrow{\rho} & s_{\text{can}}^* H \otimes \text{Quot}(W) \\ \downarrow \beta_{\text{Fil}} & & \downarrow \beta_{\text{can}}^* \\ \tilde{\mathcal{B}} & \xrightarrow{\tilde{\rho}} & s_{\text{can}}^* H \otimes \text{Quot}(W). \end{array}$$

Sei  $A_0 \in \text{Defo}(\bar{A})$  eine formale Deformation von  $\bar{A}$  nach  $W$ . Dann existiert nach Proposition 3.5.3 genau ein  $s \in \text{Spf } R$  im Deformationsraum und ein Isomorphismus  $\rho_0 : s^* A \xrightarrow{\sim} A_0$ . Wählt man einen solchen Isomorphismus fest, dann liefert dies einen kanonischen Isomorphismus  $s^* \text{Fil}^1(H) \otimes_W k \simeq \text{Fil}^1(\bar{H})$ . Sei nun  $\text{Defo}'(\bar{A})$  die Unterkategorie von  $\text{Defo}(\bar{A})$ , so dass  $s \in \text{Spf } R_0$  gilt, wobei  $R_0$  den Ring aus (3.20) bezeichnet.

**3.6.9 Theorem.** *Der Funktor  $\mathcal{F}$ , definiert durch*

$$\begin{aligned} \mathcal{F} : \text{Defo}'(\bar{A}) &\longrightarrow \text{Defo}'_{\text{Fil}}(\bar{A}) \\ [A_0 \simeq s^*A] &\longmapsto [\rho : s^*\text{Fil}^1(H) \hookrightarrow s^*_{\text{can}}H \otimes \text{Quot}(W)] \\ [\beta : s_1^*A \rightarrow s_2^*A] &\longmapsto \left[ \begin{array}{l} \beta_{\text{Fil}} : s_1^*\text{Fil}^1(H) \rightarrow s_2^*\text{Fil}^1(H) \\ \bar{\beta} : s_1^*A \otimes_W k \rightarrow s_2^*A \otimes_W k \end{array} \right], \end{aligned}$$

*ist eine Äquivalenz von Kategorien. Dabei bezeichnet  $\rho : s^*\text{Fil}^1(H) \hookrightarrow s^*_{\text{can}}H \otimes \text{Quot}(W)$  die horizontale Einbettung aus Korollar 3.6.4.*

**BEWEIS.** In [Mes72, Thm. V.1.10] ist die Äquivalenz für infinitesimale Deformationen gezeigt, d.h. für Lifts von  $\bar{A}$  (bzw.  $s^*\text{Fil}^1(H)$ ) zu einem artinsch, lokalem Ring (z.B.  $W_n := W/\mathfrak{m}^n$ ). Das Theorem folgt dann mittels Grenzwertbildung analog zu der im Beweis von Proposition 3.5.3.  $\square$

**3.6.10 Bemerkung.** Der Funktor  $\mathcal{F}$  vergleicht eine Deformation von  $\bar{A}$  mit dem Lift der Hodge-Filtrierung. Dies ist eine analoge Situation zur Variation von Hodge-Strukturen (VHS) aus Abschnitt 3.2.

**3.6.11 Bemerkung.** In [Mes72, Thm. V.1.10] wird die Äquivalenz aus Satz 3.6.9 in Termen der sogenannten universellen Erweiterung und den dazugehörigen Kristallen formuliert. Tatsächlich liefert dies durch Ersetzen von  $\text{Defo}'_{\text{Fil}}$  eine Äquivalenz für den Funktor  $\text{Defo}'(\bar{A})$ . Mittels [MM74, §1.4] kann man die Äquivalenz in Termen der Hodge-Filtrierung  $\text{Fil}^1(H) \subset H$ , wie in Theorem 3.6.9, übersetzen. Für eine einfachere Formulierung beschränken wir uns in Satz 3.6.9 auf den Subfunktor  $\text{Defo}'(\bar{A})$ .

Nun formulieren wir die Bedingung aus Satz 3.6.9 für die Liftbarkeit von Endomorphismen in Termen der  $q$ -Parameter um. Aus technischen Gründen beschränken wir uns auf die Lifts von  $\bar{A}$ , welche die Polarisierung  $\bar{\lambda} : \bar{A} \rightarrow \bar{A}^t$  liften. Genauer betrachten wir folgenden Funktor.

**3.6.12 Definition.** Wir definieren den Funktor  $M_{\text{pp}}$  als den kovarianten Funktor  $M_{\text{pp}} : \mathcal{C}_W \rightarrow \mathcal{S}$  durch

$$M_{\text{pp}}(R_0) := \left\{ \begin{array}{l} \text{Isomorphieklassen von } (A_0, \rho_0, \lambda_0), \text{ wobei} \\ A_0 \rightarrow \text{Spec}(R_0) \text{ ein formales abelsches Schema,} \\ \rho_0 : A_0 \otimes k \xrightarrow{\sim} \bar{A} \text{ ein Isomorphismus und} \\ \lambda_0 : A_0 \rightarrow A_0^t \text{ eine Quasi-Polarisierung mit } \lambda_0 \otimes k = \bar{\lambda} \text{ ist} \end{array} \right\}.$$

**3.6.13 Satz ( [Oor71, Thm. 2.3.3, §2.4] ).** *Der Funktor  $M_{\text{pp}}$  ist ein Unterfunktor des lokalen Modulfunktors  $M$ . Er ist darstellbar durch das formale Schema  $\text{Spf}(R/\mathfrak{a}_{\text{pp}})$  mit  $\mathfrak{a}_{\text{pp}} := \langle q_{i,j}q_{j,i}^{-1} - 1 \rangle_{(i,j=1,\dots,g)}$ .*

Sei nun  $\beta : \bar{A} \rightarrow \bar{A}$  ein Endomorphismus und identifiziere  $\text{End}(\bar{A})$  mit  $\text{End}(s_{\text{can}}^* A)$ . Der Endomorphismus  $\beta$  wirkt auf der de-Rham-Kohomologie  $s_{\text{can}}^* H$ . Bezeichne

$$\Psi : \text{End}(\bar{A}) \hookrightarrow \text{GL}_g(W)$$

die Darstellung der Wirkung der Endomorphismen auf der Basis  $s_{\text{can}}^* a_i$  von  $s_{\text{can}}^* U$  via Projektion. Wir benutzen folgendes Lemma 3.6.14, um die Wirkung von  $\text{End}(\bar{A})$  auf der Basis  $s_{\text{can}}^* b_i = s_{\text{can}}^* b'_i$  zu bestimmen.

**3.6.14 Lemma ([Oda69, Prop.3.24], [KO68, §2]).** *Sei  $s \in \text{Spf } R \cap V(\mathfrak{a}_{\text{pp}})$  ein Punkt im Deformationsraum von  $M_{\text{pp}}$ . Seien beliebige Elemente  $\omega_1, \omega_2 \in s^* H$  und ein Endomorphismus  $\beta \in \text{End}(s^* A)$  gegeben. Dann gilt folgende Identität:*

$$\langle \beta^* \omega_1, \omega_2 \rangle = \langle \omega_1, (\beta^\dagger)^* \omega_2 \rangle. \quad (3.25)$$

Es gilt  $\langle s_{\text{can}}^* b_i, s_{\text{can}}^* a_j \rangle = \delta_{i,j}$ . Somit wirkt  $\text{End}(\bar{A})$  nach Lemma 3.6.14 auf der Basis  $s_{\text{can}}^* b_i = s_{\text{can}}^* b'_i$  durch

$$\Psi^\dagger := \Psi \circ \dagger : \text{End}(\bar{A}) \hookrightarrow \text{GL}_g(W). \quad (3.26)$$

Mit Hilfe dieser Vorbereitungen kann man eine Bedingung für die Liftbarkeit von Isogenien angeben.

**3.6.15 Satz.** *Sei  $s \in \text{Spf } R_0 \cap V(\mathfrak{a}_{\text{pp}})$  für  $\mathfrak{a}_{\text{pp}}$  wie in Satz 3.6.13. Bezeichne  $A_s = s^* A$  die zugehörige abelsche Varietät in  $\text{Defo}'(\bar{A})$  und  $\tau \in M_g(R)$  die Matrix  $(\tau_{i,j})$ , definiert in Satz 3.5.8. Der Endomorphismus  $\bar{\beta} \in \text{End}(\bar{A})$  ist genau dann zu einem Endomorphismus  $A_s \rightarrow A_s$  liftbar, wenn*

$$\Psi(\bar{\beta}) s^* \tau = (\Psi^\dagger(\bar{\beta}) s^* \tau)^t \quad (3.27)$$

für die Matrix  $\Psi(\bar{\beta}) \in \text{GL}_g(W)$  gilt.

BEWEIS. Sei die Einbettung

$$\rho : s^* \text{Fil}^1(H) \hookrightarrow s_{\text{can}}^* H \otimes \text{Quot}(W)$$

aus Korollar 3.6.4 gegeben. Die abelsche Varietät  $A_s$  bildet unter der Äquivalenz der Kategorien  $\text{Defo}'(\bar{A})$  und  $\text{Defo}'_{\text{Fil}}(\bar{A})$  aus Theorem 3.6.9 auf  $\rho$  ab. Wir zeigen nun die Notwendigkeit der Identität (3.27) für die Existenz eines Lifts. Angenommen es existiere ein Lift  $\beta \in \text{End}(A_s)$  des Endomorphismus  $\bar{\beta}$  von  $\bar{A}$  nach  $A_s$ . Dann ist der Lift  $\beta$  unter der Äquivalenz aus Satz 3.6.9 gegeben durch einen Lift

$$\beta_{\text{Fil}} : s^* \text{Fil}^1(H) \rightarrow s^* \text{Fil}^1(H)$$

von  $\bar{\beta}^* : \text{Fil}^1(\bar{H}) \rightarrow \text{Fil}^1(\bar{H})$  der in folgendes kommutative Diagramm passt:

$$\begin{array}{ccc} s^*\text{Fil}^1(H) & \xrightarrow{\rho} & s^*_{\text{can}} H \otimes \text{Quot}(W) \\ \downarrow \beta_{\text{Fil}} & & \downarrow \beta^*_{\text{can}} \\ s^*\text{Fil}^1(H) & \xrightarrow{\rho} & s^*_{\text{can}} H \otimes \text{Quot}(W). \end{array} \quad (3.28)$$

Der Endomorphismus  $\beta_{\text{can}}$  wirkt auf den Vektoren  $(s^*_{\text{can}} b_i)_i$  durch die Matrix  $\Psi^\dagger(\bar{\beta}) \in M_g(W)$  aus (3.26). Wegen der Kommutativität von (3.28) und der Definition von  $\rho : s^*\text{Fil}^1(H) \hookrightarrow s^*_{\text{can}} H \otimes \text{Quot}(W)$  wirkt  $\beta_{\text{Fil}}$  auf den Vektoren  $(s^* b'_i)_i$  durch die Matrix  $\Psi^\dagger(\bar{\beta})$ .

Nach Proposition 3.6.6 gilt

$$s^* \tau_{ij} = \langle s^* b_i, s^* b'_j \rangle$$

und aus Lemma 3.6.14 folgt somit

$$\langle s^* b_i, \Psi^\dagger(\bar{\beta}) s^* b'_j \rangle = \langle \Psi(\bar{\beta}) s^* b_i, s^* b'_j \rangle. \quad (3.29)$$

Schreiben wir  $\Psi(\bar{\beta}) = (c_{i,j})$  (bzw.  $\Psi^\dagger(\bar{\beta}) = (c'_{i,j})$ ) für die Koeffizienten der Matrix  $\Psi(\bar{\beta})$  (bzw.  $\Psi^\dagger(\bar{\beta})$ ). Dann folgt aus (3.29) unter Verwendung der Linearität der Paarung  $\langle \cdot, \cdot \rangle$  die Identität

$$s^* \left( \sum_k c_{i,k} \tau_{k,j} \right) = s^* \left( \sum_k c'_{j,k} \tau_{i,k} \right). \quad (3.30)$$

In Termen der Matrix  $\tau = (\tau_{i,j})$  ist (3.30) äquivalent zur Identität

$$\Psi(\bar{\beta}) \cdot s^* \tau = s^* \tau \cdot (\Psi^\dagger(\bar{\beta}))^t = (\Psi^\dagger(\bar{\beta}) \cdot s^* \tau^t)^t.$$

Und da  $s \in V(\mathfrak{a}_{\text{pp}})$  ist, gilt

$$(\Psi^\dagger(\bar{\beta}) \cdot s^* \tau^t)^t = (\Psi^\dagger(\bar{\beta}) \cdot s^* \tau)^t.$$

Wir zeigen nun, dass die Identität (3.27) hinreichend für die Existenz eines Lifts ist. Gelte also (3.27) für  $s^* \tau$ . Definiere  $\beta_{\text{Fil}}$  wie folgt: Wirke  $\beta_{\text{Fil}}$  auf den Vektoren  $(s^* b'_i)_i$  durch die Matrix  $\Psi^\dagger(\bar{\beta})$ . Es bleibt zu zeigen, dass  $\beta_{\text{Fil}}$  das Diagramm (3.28) kommutativ macht. Auf den Vektoren  $s^*_{\text{can}} a_i$  wirkt  $\beta_{\text{can}}$  durch  $\Psi(\bar{\beta})$ . Man rechnet elementar nach, dass aus (3.27) die Identität

$$\Psi^\dagger(\bar{\beta}) s^* b_i = \Psi^\dagger(\bar{\beta}) s^* b'_i + \sum_j \tau_{i,j} \Psi(\bar{\beta}) s^* a_j \quad (3.31)$$

auf der Basis  $(s^* b_i)$  von  $s^*\text{Fil}^1(H)$  folgt. Wegen der Gleichung (3.24) aus Proposition 3.6.6 folgt, dass das Diagramm (3.28) kommutiert. Nach Theorem 3.6.9 existiert folglich ein Lift  $\beta \in \text{End}(A_s)$  von  $\bar{\beta} \in \text{End}(\bar{A})$ .  $\square$

**3.6.16 Korollar.** Sei  $s \in \text{Spf } R_0 \cap V(\mathfrak{a}_{\text{pp}})$  für  $\mathfrak{a}_{\text{pp}}$  wie in Satz 3.6.13. Bezeichne  $A_s = s^*A$  die zugehörige abelsche Varietät in  $\text{Defo}'(\bar{A})$ . Genau dann ist der Endomorphismus  $\beta \in \text{End}(\bar{A})$  zu einer Isogenie  $A_s \rightarrow A_s$  liftbar, wenn

$$s^*(q_{i,j}^{\Psi(\beta)}) = s^*(q_{i,j}^{\Psi^\dagger(\beta)})^t$$

für alle  $i, j \in \{1, \dots, g\}$  gilt.

BEWEIS. Dies folgt unmittelbar aus der Definition der  $q$ -Parameter in Satz 3.5.8 als  $(q_{i,j}) := (\exp(\tau_{i,j}))$ .  $\square$

**3.6.17 Bemerkung.** In [Kat81, Thm. 2.1] sind entsprechende Liftbarkeitsbedingungen für den Serre-Tate-Parameter mittels der Deformationstheorie von  $p$ -divisiblen Gruppen formuliert (Bemerkung 3.5.12).

Eine ausführliche Diskussion des Serre-Tate-Parameters für den Fall von elliptischen Kurven findet man in [Kro09].

## Kapitel 4

# Anwendung I: Abelsche Flächen vom Typ $\mathcal{QM}$

In diesem Kapitel geben wir eine Anwendung der Ergebnisse aus Kapitel 3. Wir betrachten dazu wie in Kapitel 2 die Shimura-Kurve  $\mathcal{X}(1)$  (Definition 2.3.2), die Isomorphieklassen von abelschen Flächen  $A$  vom Typ  $\mathcal{QM}$  parametrisiert, d.h. abelsche Flächen  $A$  mit Einbettung  $\mathcal{O}_D \hookrightarrow \text{End}(A)$  einer festen maximalen Ordnung in der indefiniten Quaternionenalgebra  $D$  (Definition 2.1.6). Wir interessieren uns für den Ort  $V$  der Shimura-Kurve im Deformationsraum einer abelschen Fläche  $\bar{A}$  vom Typ  $\mathcal{QM}$  über einem endlichen Körper. Konkret bestimmen wir Gleichungen für den Ort der Lifts  $A$  von  $\bar{A}$  nach Charakteristik 0, welche vom Typ  $\mathcal{QM}$  sind (Theorem 4.1.6). Mori bestimmt in [Mor09] mittels anderer Methoden ähnliche Gleichungen. Wir gehen darüber hinaus und betrachten die Geometrie der CM-Lifts von  $\bar{A}$ . In Abschnitt 4.2 zeigen wir für das Beispiel der Quaternionenalgebra  $D/\mathbb{Q}$  mit Diskriminante 6, wie man diese Gleichungen explizit berechnet.

### 4.1 Beschreibung der $q$ -Parameter

Sei in diesem Abschnitt  $\bar{A}$  eine hauptpolarisierte, gewöhnliche abelsche Fläche über  $k = \mathbb{F}_q$ . Sei  $D/\mathbb{Q}$  eine indefinite, verzweigte Quaternionenalgebra und  $\mathcal{O}_D$  eine maximale Ordnung, so dass durch  $\Psi : \mathcal{O}_D \hookrightarrow \text{End}(\bar{A})$  ein  $\mathcal{QM}$ -Typ (Definition 2.1.6) gegeben ist.

Sei  $\bar{\lambda} : \bar{A} \rightarrow \bar{A}^t$  eine Hauptpolarisierung auf  $\bar{A}$ . Dann definiert  $\bar{\lambda}$  eine Involution auf  $\text{End}(\bar{A})$  und somit auf  $\mathcal{O}_D$ . Wir bezeichnen diese Involution mit  $x \mapsto x^\dagger$ .

Sei  $W = W(k)$  der Ring der Witt-Vektoren. Wir interessieren uns nun für die Lifts von  $\bar{A}$  nach  $W$  vom Typ  $\mathcal{QM}$ . Das heißt, wir möchten die abelsche Varietät  $\bar{A}$ , den  $\mathcal{QM}$ -Typ  $\Psi_{\mathcal{QM}} : \mathcal{O}_D \hookrightarrow \text{End}(\bar{A})$  und die Polarisierung  $\bar{\lambda} :$

$\bar{A} \rightarrow \bar{A}$  nach  $W$  liften. Sei  $M$  der lokale Modulfunktor (Definition 3.5.1) der Lifts von  $\bar{A}$  nach  $W$ . Der Funktor  $M$  ist darstellbar durch das formale Schema  $\mathrm{Spf} R$  mit  $R := W[[q-1]]$  für  $q := (q_{i,j})_{i,j=1,2}$ . Dabei wählen wir die Koordinaten im Deformationsraum  $\mathrm{Spf} R$  von  $M$  mittels Satz 3.5.10, d.h.  $q_{i,j}$  bezeichnen die  $q$ -Parameter auf  $\mathrm{Spf} R$  aus Satz 3.5.8. Wie in Abschnitt 3.6 beschränken wir uns auf den Funktor  $M_{\mathrm{pp}}$  (Definition 3.6.12) also auf den Unterlokus  $V(\mathfrak{a}) \subset \mathrm{Spf} R$  mit  $\mathfrak{a} = \langle q_{1,2}q_{2,1}^{-1} - 1 \rangle$ .

**4.1.1 Definition.** Wir definieren den Funktor  $N$  als den kovarianten Funktor  $N : \mathcal{C}_W \rightarrow \mathcal{S}$  durch

$$N(R_0) := \left\{ \begin{array}{l} \text{Isomorphieklassen von } (A_0, \rho_0, \Psi_0, \lambda_0), \text{ wobei} \\ A_0 \rightarrow \mathrm{Spec}(R_0) \text{ ein formales abelsches Schema,} \\ \rho_0 : A_0 \otimes k \xrightarrow{\sim} \bar{A} \text{ ein Isomorphismus,} \\ \Psi_0 : \mathcal{O}_D \hookrightarrow \mathrm{End}(A_0) \text{ ein } \mathcal{QM}\text{-Typ mit } \Psi_0 \otimes k = \Psi_{\mathcal{QM}} \text{ und} \\ \lambda_0 : A_0 \rightarrow A_0^t \text{ eine Quasi-Polarisierung mit } \lambda_0 \otimes k = \bar{\lambda} \text{ ist} \end{array} \right\}.$$

**4.1.2 Lemma.** Sei  $(A_0, \rho_0, \Psi_0, \lambda_0) \in N(R_0)$  und  $(A_1, \rho_1, \lambda_1) \in M(R_0)$  mit Isomorphismus  $\gamma : A_0 \xrightarrow{\sim} A_1$  quasi-polarisierter abelscher Schemata. Dann existiert höchstens ein  $\mathcal{QM}$ -Typ  $\Psi_1 : \mathcal{O}_D \rightarrow \mathrm{End}(A_1)$ , so dass  $(A_1, \rho_1, \Psi_1, \lambda_1) \in N(R_0)$  ist. D.h. der Funktor  $N$  ist ein Unterfunktor von  $M_{\mathrm{pp}}$ , in dem man den  $\mathcal{QM}$ -Typ vergisst.

BEWEIS. Angenommen es existiert ein  $\mathcal{QM}$ -Typ  $\Psi_1 : \mathcal{O}_D \rightarrow \mathrm{End}(A_1)$  auf  $A_1$  und ein Isomorphismus  $\gamma : A_0 \xrightarrow{\sim} A_1$  wie in der Aussage des Lemmas. Da  $A_0 \otimes k \simeq A_1 \otimes k$  gilt, ist  $\bar{\gamma} := \gamma \otimes k$  ein Automorphismus von  $\bar{A}$ . Die Bedingungen  $\Psi_1 \otimes k = \Psi_{\mathcal{QM}}$  und  $\lambda_1 \otimes k = \bar{\lambda}$  implizieren, dass  $\bar{\gamma}$  im Zentrum von  $\mathrm{End}(\bar{A})$  liegt und  $\bar{\gamma}^\dagger = \bar{\gamma}$  gelten muss. Da  $D$  eine Quaternionenalgebra ist, muss  $\bar{\gamma} \in \mathbb{Q}$  (Definition 1.1.1) und folglich  $\bar{\gamma} = \mathrm{id}$  gelten.  $\square$

Bezeichne  $s_{\mathrm{can}} \in \mathrm{Spf} R$  den Punkt im Deformationsraum, welcher zum kanonische Lift von  $\bar{A}$  korrespondiert. Dieser ist gegeben durch den Nullpunkt in der Gruppenstruktur auf dem Deformationsraum, d.h.  $s_{\mathrm{can}}^* q_{i,j} = 1$  für alle  $i, j$ . Sei der  $W$ -Modul  $s_{\mathrm{can}}^* H := H_{\mathrm{dR}}^1(s_{\mathrm{can}}^* A/W)$  gegeben und bezeichne

$$\Psi : \mathrm{End}(\bar{A}) \hookrightarrow M_2(W)$$

die Darstellung der Wirkung der Endomorphismen auf der Basis  $(a_1, a_2) \subset s_{\mathrm{can}}^* U$  des Unit-Root-Kristalls  $s_{\mathrm{can}}^* U \subset s_{\mathrm{can}}^* H$  wie in Satz 3.5.7.

**4.1.3 Proposition.** Sei  $t \in \mathcal{O}_D \setminus \mathbb{Q}$  wie in Proposition 1.1.21, d.h. es gilt  $x^\dagger = t\bar{x}t^{-1}$  für alle  $x \in \mathcal{O}_D$ . Bezeichne

$$\Lambda := \Psi(\Psi_{\mathcal{QM}}(t)) = (a_{ij}) \in M_2(W)$$

die Matrix der Wirkung des Endomorphismus  $\Psi_{\text{QM}}(t) \in \text{End}(A)$  auf der Basis  $(s_{\text{can}}^* a_i)$  von  $s_{\text{can}}^* U$ .

(i) Dann gilt  $a_{11} = -a_{22}$  und  $a_{11}^2 + a_{12}a_{21} \in W^*$ .

(ii) Die Identität  $\Lambda s^* \tau = (\Lambda^\dagger s^* \tau)^t$  ist genau dann erfüllt, wenn einer der folgenden Fälle eintritt:

(I) Es gilt  $a_{12} \in W^*$  und

$$s^* \tau = \begin{pmatrix} s^* \tau_{11} & -\frac{a_{11}}{a_{12}} s^* \tau_{12} \\ -\frac{a_{11}}{a_{12}} \tau_{11} & -\frac{a_{21}}{a_{12}} s^* \tau_{11} \end{pmatrix}, \quad (4.1)$$

wobei  $s^* \tau_{11}, s^* \tau_{12} \in W$  beliebig sind.

(II) Es gilt  $a_{12} \notin W^*$  und

$$s^* \tau = \begin{pmatrix} -\frac{a_{12}}{a_{11}} s^* \tau_{12} & s^* \tau_{12} \\ s^* \tau_{12} & \frac{a_{21}}{a_{11}} s^* \tau_{12} \end{pmatrix}, \quad (4.2)$$

wobei  $s^* \tau_{12}, s^* \tau_{21} \in W$  beliebig sind.

BEWEIS. In  $\mathcal{O}_D$  gilt  $t^2 \in \mathbb{Q}$  und  $t \notin \mathbb{Q}$ . Folglich muss  $\text{tr}(t) = \text{tr}(\Lambda) = 0$  also  $a_{11} = -a_{22}$  erfüllt sein. Da außerdem  $t^\dagger = \bar{t}t^{-1} = \bar{t} = -t$  gilt, folgt für die Polarisierung auf den Matrizen  $\Lambda^\dagger = -\Lambda$ . Die Polarisierung  $\bar{\lambda} : \bar{A} \rightarrow \bar{A}^t$  ist eine Hauptpolarisierung, folglich muss  $\det(\Lambda) = a_{11}^2 + a_{12}a_{21} \in W^*$  sein.

Die Identität

$$\Lambda s^* \tau = (\Lambda^\dagger s^* \tau)^t = -(\Lambda s^* \tau)^t$$

liefert folgendes lineares Gleichungssystem für die Koeffizienten  $s^* \tau_{ij}$ :

$$\begin{cases} a_{11} s^* \tau_{11} + a_{12} s^* \tau_{12} & = 0, \\ a_{21} s^* \tau_{11} & + a_{12} s^* \tau_{22} = 0, \\ & -a_{21} s^* \tau_{12} + a_{11} s^* \tau_{22} = 0. \end{cases}$$

Ist  $a_{12} \in W^*$ , folgt (4.1) direkt. Also nehmen wir an, dass  $a_{12} \in (p)$  ist. Da  $a_{11}^2 + a_{12}a_{21} \in W^*$  ist, muss folglich  $a_{11} \in W^*$  sein. Somit folgt (4.2).  $\square$

Sei  $\beta \in \text{End}(\bar{A})$  und bezeichne mit  $B := \Psi(\beta) \in M_2(W)$  die Matrix der Wirkung von  $\beta$  auf der Basis  $(s_{\text{can}}^* a_i)$  von  $s_{\text{can}}^* U$ . In der Bezeichnung von Proposition 4.1.3 ist die Matrix  $\Psi^\dagger(\beta) \in M_2(W)$  gegeben durch

$$\Lambda \cdot \text{Adj}(B) \cdot \Lambda^{-1} \in M_2(W).$$

Benutzt man die Bedingungen aus Satz 3.6.15 für die Liftbarkeit von  $\beta \in \text{End}(\bar{A})$  an die Matrix  $s^*\tau$ , dann liefert dies ein lineares Gleichungssystem in  $s^*\tau_{i,j}$ . Dieses ist durch

$$B \cdot s^*\tau = (\Lambda \cdot \text{Adj}(B) \cdot \Lambda^{-1} \cdot s^*\tau)^t \quad (4.3)$$

gegeben. Wir benutzen diese Überlegung um folgende Proposition 4.1.4 zu zeigen.

**4.1.4 Proposition.** *Gegeben die formale Deformation  $s^*A$  von  $\bar{A}$ . Dann lässt sich die Polarisierung  $\bar{\lambda} : \bar{A} \rightarrow \bar{A}^t$  und der  $\mathcal{QM}$ -Typ  $\Psi_{\mathcal{QM}} : \mathcal{O}_D \hookrightarrow \text{End}(\bar{A})$  genau dann zu einer Polarisierung  $\lambda : s^*A \rightarrow s^*A^t$  und einem  $\mathcal{QM}$ -Typ  $\mathcal{O}_D \hookrightarrow \text{End}(s^*A)$  liften, wenn für die Koordinaten  $s^*q_{ij}$  im Deformationsraum folgende Identitäten erfüllt sind:*

$$\begin{aligned} s^*q_{2,1} &= s^*q_{1,2}, \\ s^*q_{1,2}^{a_{12}} &= s^*q_{1,1}^{-a_{11}}, \\ s^*q_{2,2}^{a_{12}} &= s^*q_{1,1}^{a_{21}}. \end{aligned} \quad (4.4)$$

BEWEIS. Die Varietät  $\bar{A}$  ist gewöhnlich. Damit gilt nach Proposition 2.6.3 insbesondere, dass  $\mathcal{O}_D \otimes_{\mathbb{Z}} W \simeq M_2(W)$  gilt. Es ist also zu zeigen, dass die Bedingungen (4.4) äquivalent zur Erfüllbarkeit der Gleichung (4.3) für jede Matrix  $B \in M_2(W)$  sind. Dies kann man elementar überprüfen. Die Liftbarkeit der Polarisierung folgt nach Satz 3.6.13 aus den Bedingungen (4.4).  $\square$

**4.1.5 Lemma.** *Sei  $\mathfrak{a}$  das Ideal in  $R$  erzeugt von den Elementen*

$$\begin{aligned} q_{2,1} \cdot q_{1,2}^{-1} - 1, \\ q_{1,2}^{a_{12}} \cdot q_{1,1}^{a_{11}} - 1, \\ q_{2,2}^{a_{12}} \cdot q_{1,1}^{-a_{21}} - 1. \end{aligned}$$

*Sei  $s \in \text{Spf } R$  ein Punkt im Deformationsraum von  $\bar{A}$  und sei  $(A_0, \rho_0) \in M(R_0)$  mit  $\rho_0 : A_0 \xrightarrow{\sim} s^*A$ . Es existiert genau dann ein  $\mathcal{QM}$ -Typ  $\Psi_0 : \mathcal{O}_D \hookrightarrow \text{End}(A_0)$  und eine Polarisierung  $\lambda_0 : A_0 \rightarrow A_0^t$ , so dass  $(A_0, \rho_0, \Psi_0, \lambda_0) \in N(R_0)$  gilt, wenn  $(s^*q_{i,j} - 1)$  in der Nullstellenmenge  $V(\mathfrak{a})$  von  $\mathfrak{a}$  liegt.*

BEWEIS. Sei  $(A_0, \rho_0, \Psi_0, \lambda_0) \in N(R_0)$ , insbesondere ist  $(A_0, \rho_0) \in M(R_0)$ . Dann existiert wegen der Darstellbarkeit von  $M$  ein  $s \in \text{Spf } R(R_0)$ , so dass  $s^*A \simeq A_0$  ist. Mit Lemma 4.1.2 können wir  $s^*A = A_0$  annehmen. Somit folgt die Behauptung aus Proposition 4.1.4.  $\square$

**4.1.6 Theorem.** *Der Funktor  $N$  ist darstellbar durch das formale Schema*

$\mathrm{Spf}(R/\mathfrak{a})$ , d.h. es gibt eine natürliche Äquivalenz

$$\hat{C}_W(\mathrm{Spf}(R/\mathfrak{a}), -) \xrightarrow{\sim} N(-).$$

Das formale Schema  $\mathrm{Spf} R/\mathfrak{a}$  ist die formale Faser eines eindimensionalen Torus.

BEWEIS. Die Darstellbarkeit von  $N$  folgt aus Lemma 4.1.5. Aus den Gleichungen (4.4) ist offensichtlich, dass das formale Schema  $\mathrm{Spf} R/\mathfrak{a}$  formal glatt ist. Folglich ist  $\mathrm{Spf} R/\mathfrak{a}$  isomorph zu einem Torus. Da  $\mathrm{Spf} R/\mathfrak{a}$  offensichtlich von Ko-Dimension 3 in  $\mathrm{Spf} R$  ist, folgt dass  $\mathrm{Spf} R/\mathfrak{a}$  eindimensional ist.  $\square$

**4.1.7 Bemerkung.** In [Mor09] bestimmt Mori unter Benutzung anderer Methoden ähnliche Gleichungen ([Mor09, Thm. 7]). Sein Ansatz beruht dabei sehr darauf, dass die CM-Punkte zu abelschen Flächen korrespondieren, die nicht absolut einfach sind.

Wir beschäftigen uns im Folgenden mit den Lifts einer abelschen Fläche vom Typ  $\mathcal{QM}$  nach Charakteristik 0, die ebenfalls vom Typ  $\mathcal{QM}$  sind und komplexe Multiplikation haben.

Nach Satz 2.1.9 ist die abelsche Fläche  $\bar{A}$  nicht absolut einfach. O.B.d.A. sei nach Ersetzen von  $k$  durch eine endliche Erweiterung die abelsche Fläche  $\bar{A}$  über  $k$  nicht einfach, d.h. es existiere eine gewöhnliche elliptische Kurve  $E$  über  $k$ , so dass  $A \sim E^2$  gilt. Die Endomorphismenalgebra  $\mathrm{End}^0(\bar{A})$  ist folglich isomorph zur Matrixalgebra  $M_2(K)$  für einen imaginär quadratischen Körper  $K \simeq \mathrm{End}^0(E)$ . Nach der Honda-Tate-Theorie gilt  $K = \mathbb{Q}(\pi)$ , wobei  $\pi \in \mathrm{End}(\bar{A})$  den absoluten Frobenius-Morphismus von  $\bar{A}$  bezeichnet. Insbesondere existiert eine Ordnung  $\mathcal{O}_{K,c_0} \subset K$  mit Führer  $c_0 \in \mathbb{N}$  in  $\mathcal{O}_K$ , so dass  $\pi \in \mathcal{O}_{K,c_0}$  und  $\mathcal{O}_{K,c_0}$  im Zentrum von  $\mathrm{End}(\bar{A})$  liegt. Nach Proposition 2.6.5 gilt  $p \nmid c_0$  für den Führer von  $\mathcal{O}_{K,c_0}$ .

Sei  $A$  ein Lift von  $\bar{A} = A \otimes k$  nach  $W$  und besitze  $A$  komplexe Multiplikation. Dann gilt  $\mathrm{End}^0(A) \simeq \mathrm{End}^0(\bar{A}) \simeq M_2(K)$ . Nach Proposition 2.6.5 existiert ein  $n \in \mathbb{N}$ , so dass das Zentrum von  $\mathrm{End}(A)$  isomorph zur Ordnung  $\mathcal{O}_{K,c}$  von  $K$  mit Führer  $c := p^n c_0$  in  $\mathcal{O}_K$  ist.

**4.1.8 Proposition.** Gegeben sei die formale Deformation  $s^*A$  von  $\bar{A}$  vom Typ  $\mathcal{QM}$ . Sei  $\mathcal{O}_{K,c} \subset \mathcal{O}_{K,c_0} \simeq \mathrm{Zentrum}(\mathrm{End}(\bar{A}))$  eine Unterordnung in  $K$  mit Führer  $c := p^n c_0$ . Genau dann lässt sich eine Unterordnung  $\mathcal{O}_{K,c}$  zu einer Teilmenge von  $\mathrm{Zentrum}(\mathrm{End}(A))$  liften, wenn im Deformationsraum folgende

Identitäten erfüllt sind:

$$\begin{aligned}
s^* q_{1,1}^{p^n} &= 1, \\
s^* q_{2,1} &= s^* q_{1,2}, \\
s^* q_{1,2}^{a_{12}} &= s^* q_{1,1}^{-a_{11}}, \\
s^* q_{2,2}^{a_{12}} &= s^* q_{1,1}^{a_{21}}.
\end{aligned} \tag{4.5}$$

BEWEIS. Im Zentrum von  $\text{End}(A)$  ist die Involution  $\dagger$  nach Lemma 2.4.17 gegeben durch die komplexe Konjugation, d.h. für  $\beta \in \text{Zentrum}(\text{End}(\bar{A}))$  gilt  $\Psi(\beta)^\dagger = \Psi(\bar{\beta})^t$ .

Bezeichne  $\pi \in \mathcal{O}_{K,c_0}$  den absoluten Frobenius-Morphismus. Nach Proposition 2.6.7 ist die Liftbarkeit von  $\mathcal{O}_{K,c}$  äquivalent zur Liftbarkeit des Morphismus  $p^n \pi$ . Benutzt man die Bedingungen aus Satz 3.6.15 für die Liftbarkeit von Endomorphismen an die Matrix  $s^* \tau$ , dann liefert dies folgendes lineare Gleichungssystem in  $s^* \tau_{i,j}$ :

$$p^n \Psi(\pi) \cdot s^* \tau = (p^n \Psi(\bar{\pi})^t \cdot s^* \tau)^t. \tag{4.6}$$

Es gelten für die Parameter  $s^* \tau \in W$  die Relationen (4.1) bzw. (4.2) aus Proposition 4.1.3. Da  $\Psi(\pi) - \Psi(\bar{\pi})^t \in W^*$  gilt, ist das Gleichungssystem (4.6) äquivalent zur Gleichung  $p^n s^* \tau_{1,2} \equiv 0 \pmod{p^{n+1}}$ . Somit folgt die Behauptung.  $\square$

## 4.2 Beispiel: Diskriminante 6

Wir betrachten nun das Beispiel der Shimura-Kurve  $\mathcal{X}(1)$  bezüglich der Quaternionenalgebra  $D/\mathbb{Q}$  mit  $\text{disc}(D) = 6$ . Wir berechnen dabei konkrete Gleichungen für die  $q$ -Parameter von  $\mathcal{QM}$ -Lifts für bestimmte CM-Punkte. Insbesondere berechnen wir die Gleichung für die Reduktion der elliptischen Punkte.

Folgende Proposition gibt eine explizite Basis einer Quaternionenalgebra  $D$  (wie in Proposition 1.1.9) und eine explizite Basis einer maximalen Ordnung in  $D$  an. Dies gehört zu einem expliziten Modell der Shimura-Kurve  $\mathcal{X}(1)$  ([Has95]), auf das wir hier nicht näher eingehen wollen.

**4.2.1 Proposition ([Has95, §2]).** Sei  $D/\mathbb{Q}$  eine Quaternionenalgebra mit  $\text{disc}(D) = \delta$ . Dann gilt:

- (i) Es existiert eine Primzahl  $p_0 \in \mathbb{N}$  und eine Basis  $\{1, i, j, ij\}$  von  $D$  als  $\mathbb{Q}$ -Vektorraum mit den Eigenschaften  $i^2 = -\delta$ ,  $j^2 = p_0$  und  $ij = -ji$ .
- (ii) Sei  $a_0 \in \mathbb{Z}$ , so dass  $a_0 \delta \equiv -1 \pmod{p_0}$  gilt. Dann ist

$$\mathcal{O}_D := \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3 \oplus \mathbb{Z}e_4$$

für die Elemente

$$\epsilon_1 := 1, \quad \epsilon_2 := \frac{1+j}{2}, \quad \epsilon_3 := \frac{i+ij}{2}, \quad \epsilon_4 := \frac{a_0\delta j + ij}{p_0}$$

eine maximale Ordnung von  $D$ .

(iii) Sei  $a \in D$ , so dass  $a^2 \in \mathbb{Q}_{<0}$  gilt. Dann gilt: Die alternierende Form

$$\begin{aligned} E_t : D \times D &\longrightarrow \mathbb{Q} \\ (h_1, h_2) &\longmapsto \operatorname{tr}(h_1 \bar{h}_2 a) \end{aligned}$$

definiert genau dann eine nicht-degenerierte Form

$$E_t : \mathcal{O}_D \times \mathcal{O}_D \longrightarrow \mathbb{Z}$$

mit Werten in  $\mathbb{Z}$ , falls  $a \cdot i \in \mathcal{O}_D^*$  gilt.

(iv) Durch

$$\Theta(i) := \begin{pmatrix} 0 & -1 \\ \delta & 0 \end{pmatrix}, \quad \Theta(j) := \begin{pmatrix} \sqrt{p_0} & 0 \\ 0 & -\sqrt{p_0} \end{pmatrix}$$

ist eine konkrete Einbettung  $\Theta : D \hookrightarrow M_2(\mathbb{R})$  gegeben.

**4.2.2 Bemerkung.** Die Aussage (iii) in Proposition 4.2.1 korrespondiert dazu, dass die Riemann-Form auf  $A_z := \mathbb{C}^2/\Lambda_z$  nicht degeneriert ist. Dabei ist  $\Lambda_z$  eine Familie von Gittern in  $\mathbb{C}^2$ , welche der Ordnung  $\mathcal{O}_D$  zugeordnet wird. Dies entspricht einer konkreten Interpretation von  $\mathcal{X}(1)$  als Moduli von abelschen Flächen vom Typ QM (siehe [Has95]).

Wichtig für unsere Berechnungen ist, dass für  $a := i$  die Abbildung

$$D \rightarrow D, \quad h \mapsto h^\dagger := \bar{t} h t^{-1} \tag{4.7}$$

eine Involution auf  $\mathcal{O}_D$  definiert, die zu einer Hauptpolarisierung von  $A_z$  gehört.

Man rechnet mittels dem Hilbertsymbol aus, dass  $D := \left(\frac{-6,2}{\mathbb{Q}}\right)$  die Diskriminante  $\operatorname{disc}(D) = 6$  hat. Somit können wir in der Proposition 4.2.1 die Primzahl  $p_0 = 2$  wählen. D.h. es existiert eine Basis  $\{1, i, j, ij\}$  von  $D$  als  $\mathbb{Q}$ -Vektorraum mit den Eigenschaften  $i^2 = -6$ ,  $j^2 = 2$  und  $ij = -ji$ . Sei die Einbettung  $\Theta : D \hookrightarrow M_2(\mathbb{R})$  mit

$$\Theta(i) := \begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix}, \quad \Theta(j) := \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}$$

gegeben.

Um unsere Ergebnisse in Proposition 4.2.4 mit [Mor09, Thm. 7] vergleiche

chen zu können, modifizieren wir die maximale Ordnung  $\mathcal{O}_D$  aus (ii) in Proposition 4.2.1 und setzen

$$\epsilon_1 := 1, \quad \epsilon_2 := \frac{i+j}{2}, \quad \epsilon_3 := \frac{i-j}{2}, \quad \epsilon_4 := \frac{2+2j+ij}{4}. \quad (4.8)$$

Dann gehört  $a := i \in \mathcal{O}_D$  weiterhin zu einer Hauptpolarisierung wie in Bemerkung 4.2.2. Bezeichne die arithmetische Fuchsische Gruppe  $\Theta(\mathcal{O}_D^1) \subset \mathrm{SL}_2(\mathbb{R})$  mit  $\Gamma(1)$ .

Zunächst möchten wir unsere Ergebnisse aus Abschnitt 4.1 auf die elliptischen Punkte von  $\mathcal{X}(1)$  anwenden. Wir haben bereits in Beispiel 2.3.4 gesehen, dass  $\mathcal{X}(1)$  genau zwei elliptische Punkte von Ordnung 2 und zwei elliptische Punkte von Ordnung 3 besitzt. Die elliptischen Punkte  $z_i \in \mathcal{X}(1)$  von Ordnung 2 (bzw. 3) korrespondieren (Proposition 2.7.7) zu Einbettungen  $\iota : K \hookrightarrow D$  von  $K = \mathbb{Q}(\zeta_4)$  (bzw.  $K = \mathbb{Q}(\zeta_3)$ ), wobei  $\zeta_4 := \sqrt{-1} \in \mathbb{C}$  (bzw.  $\zeta_3 := \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ ) seien.

Repräsentanten  $\xi_i \in \mathcal{H}$  der elliptischen Punkte  $z_i := [\xi_i] \in \mathcal{X}(1)$  der Ordnung 2 (bzw. 3) sind in folgender Tabelle gegeben. Dabei definieren  $\iota_i(\zeta_4)$  (bzw.  $\iota_i(\zeta_3)$ ) Einbettungen  $\iota_i : K \hookrightarrow D$  von  $K = \mathbb{Q}(\zeta_4)$  (bzw.  $K = \mathbb{Q}(\zeta_3)$ ) in  $D$ . Und die  $u_i \in D$  aus der Tabelle erfüllen die Eigenschaften von Satz 1.2.4, d.h. es gilt  $D \simeq (\iota_i(K), u_i^2)$ .

$\mathrm{ord}_{\mathrm{ell}}(z_i) = 2 :$	$\iota_i(\zeta_4)$	$u_i$	$u_i^2$	$\xi_i$
$i = 1$	$\epsilon_3$	$\epsilon_2 - 2\epsilon_3$	3	$\frac{-\sqrt{2}+2\sqrt{-1}}{6}$
$i = 2$	$\epsilon_2$	$2\epsilon_2 - \epsilon_3$	3	$\frac{\sqrt{2}+2\sqrt{-1}}{6}$
$\mathrm{ord}_{\mathrm{ell}}(z_i) = 3 :$	$\iota_i(\zeta_3)$	$u_i$	$u_i^2$	$\xi_i$
$i = 1$	$\epsilon_2 - \epsilon_4$	$\epsilon_2 - \epsilon_3$	2	$\frac{(2+\sqrt{2})\sqrt{-3}}{6}$
$i = 1$	$\epsilon_3 + \epsilon_4 - 1$	$\epsilon_2 - \epsilon_3$	2	$\frac{(2-\sqrt{2})\sqrt{-3}}{6}$

**4.2.3 Proposition.** Sei  $z \in \mathcal{X}(1)$  ein elliptischer Punkt und  $A_z$  die zugehörige abelsche Fläche vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation durch  $\mathcal{O}_{\zeta_4}$  (bzw.  $\mathcal{O}_{\zeta_3}$ ). Bezeichne  $E$  die eindeutige elliptische Kurve mit komplexer Multiplikation durch  $\mathcal{O}_{\zeta_4}$  (bzw.  $\mathcal{O}_{\zeta_3}$ ). Dann existiert eine Isogenie  $\psi : A \rightarrow E \times E$  von Grad 2.

BEWEIS. Bezeichne  $n$  die reduzierte Norm von  $D$  über  $\mathbb{Q}$ . Da  $n(\sqrt{\zeta_4}) = 1$  und  $n(\zeta_3) = 1$  ist, gilt in allen Fällen  $e, \bar{e} \in \frac{1}{2}\mathcal{O}_D \otimes \mathcal{O}_K$ . Somit folgt die Behauptung mit Satz 2.4.12.  $\square$

Nun wenden wir Satz 4.1.6 auf diese Situation an. Zunächst betrachten wir die elliptischen Punkte von Ordnung 2.

Sei also  $z \in \mathcal{X}(1)$  ein elliptischer Punkt von Ordnung 2 und  $A_z$  die zugehörige abelsche Fläche vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation durch  $\mathcal{O}_{\zeta_4} \subset \text{Zentrum}(\text{End}(A))$ . Sei  $p \in \mathbb{N}$  eine Primzahl, für die  $p \equiv 1 \pmod{4}$  gilt. Dann hat die abelsche Fläche  $A_z$  gute gewöhnliche Reduktion modulo  $p$ . Tatsächlich existiert eine abelsche Fläche  $\bar{A}$  über dem endlichen Körper  $k = \mathbb{F}_p$ , so dass  $\bar{A} = A_z \otimes k$  gilt.

Wir betrachten nun die Lifts von  $\bar{A}$  nach  $W := W(k)$ . Bezeichne  $A_{\text{can}}$  den kanonischen Lift von  $\bar{A}$  nach  $W$ . Dann gilt  $A_{\text{can}} \simeq A_z \otimes W$ . Bezeichne mit  $s^*H := H_{\text{dR}}^1(s_{\text{can}}^*A/W)$  und mit

$$\Psi : \text{End}(\bar{A}) \hookrightarrow M_2(W)$$

die Darstellung der Wirkung der Endomorphismen  $\text{End}(A_{\text{can}})$  auf der Basis  $(s^*a_1, s^*a_2)$  des Unit-Root-Kristalls  $s_{\text{can}}^*U \subset s_{\text{can}}^*H$ , wie in Satz 3.5.7. Wir können die Basis so wählen, dass  $s^*a_1$  (bzw.  $s^*a_2$ ) ein Eigenvektor zum Endomorphismus  $\zeta_4 \in \mathcal{O}_D$  mit Eigenwert  $\zeta_4$  (bzw.  $-\zeta_4$ ) ist. Nun können wir Satz 4.1.6 anwenden, um den Locus der  $\mathcal{QM}$ -Punkte im Modulraum von  $\bar{A}$  konkret anzugeben. Wir benutzen dabei die Notationen und Bezeichnungen von Abschnitt 4.1. Beispielhaft rechnen wir dies im Fall  $z := \left[ \frac{-\sqrt{2}+2\sqrt{-1}}{6} \right] \in \mathcal{X}(1)$  nach.

**4.2.4 Proposition.** Sei  $z := \left[ \frac{-\sqrt{2}+2\sqrt{-1}}{6} \right] \in \mathcal{X}(1)$ . Bezeichne  $\mathfrak{a} \subset R$  das Ideal, erzeugt von den Elementen

$$\begin{aligned} q_{2,1} \cdot q_{1,2}^{-1} - 1, \\ q_{1,2} \cdot q_{1,1}^{3\zeta_4} - 1, \\ q_{2,2} \cdot q_{1,1}^{-3} - 1. \end{aligned}$$

Dann ist der Locus von  $N \subset M$  gegeben durch die Nullstellenmenge  $V(\mathfrak{a})$  von  $\mathfrak{a}$ .

BEWEIS. O.B.d.A. gelte

$$\Psi(u) = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}.$$

Dann wirkt  $a = \epsilon_2 + \epsilon_3$  auf  $(a_1, a_2)$  durch

$$\Psi(a) = \begin{pmatrix} 3\zeta_4 & 1 \\ 3 & -3\zeta_4 \end{pmatrix}.$$

Die Gleichungen folgen dann direkt aus Proposition 4.1.4.  $\square$

**4.2.5 Bemerkung.** Dies sind analoge Gleichungen wie in [Mor09, Thm. 7] für die Serre-Tate-Parameter.

Für die restlichen elliptischen Punkte geht man völlig analog vor und

leitet folgende Relationen her.

$\text{ord}_{\text{ell}}(z) = 2 :$	Relationen		
$\frac{-\sqrt{2}+2\sqrt{-1}}{6}$	$q_{1,2} = q_{1,1}^{3\zeta_4}$	$q_{2,1} = q_{1,1}^{3\zeta_4}$	$q_{2,2} = q_{1,1}^{-3}$
$\frac{\sqrt{2}+2\sqrt{-1}}{6}$	$q_{1,2} = q_{1,1}^{-3\zeta_4}$	$q_{2,1} = q_{1,1}^{-3\zeta_4}$	$q_{2,2} = q_{1,1}^3$
$\text{ord}_{\text{ell}}(\zeta) = 3 :$			
$\frac{(2+\sqrt{2})\sqrt{-3}}{6}$	$q_{1,2} = q_{1,1}^2$	$q_{2,1} = q_{1,1}^2$	$q_{2,2} = q_{1,1}^{-14}$
$\frac{(2-\sqrt{2})\sqrt{-3}}{6}$	$q_{1,2} = q_{1,1}^{-2}$	$q_{2,1} = q_{1,1}^{-2}$	$q_{2,2} = q_{1,1}^{14}$

## Kapitel 5

# Anwendung II: Zyklische Überlagerungen von $\mathbb{P}^1$

In diesem Kapitel geben wir eine zweite Anwendung der Ergebnisse aus Kapitel 3. Dabei betrachten wir die Shimura-Kurve  $\mathcal{X}_5$  (bzw.  $\mathcal{X}_7$ ), welche Isomorphieklassen von hauptpolarisierten abelschen Varietäten  $A$  von Dimension  $g = 4$  (bzw.  $g = 6$ ) mit einer festen Wirkung von  $\mathbb{Z}[\zeta_5]$  (bzw.  $\mathbb{Z}[\zeta_7]$ ) auf  $H^0(A, \Omega_A)$  parametrisieren. Diese unterscheiden sich von den Shimura-Kurven  $\mathcal{X}(1)$  aus Kapitel 4 zum Beispiel dadurch, dass ihre CM-Punkte generisch gewöhnlich sind (Proposition 5.1.9). Wir benutzen wie im Fall von  $\mathcal{X}(1)$  in Kapitel 4 das Korollar 3.6.16, um Gleichungen für den Lokus von  $\mathcal{X}_N$  im Deformationsraum (Proposition 5.2.3) für  $N = 5, 7$  zu finden. Dies ist ein Indiz dafür, dass man mittels unserer Methoden allgemeine Shimura-Kurven vom Typ PEL studieren kann.

Wir betrachten dazu für  $N \in \mathbb{N}$  mit  $N \geq 2$  die Familien von Kurven

$$\mathfrak{C}_N : y^N = x(x-1)(x-\lambda) \tag{5.1}$$

über der projektiven Gerade  $\mathbb{P}_\lambda^1$ . Sei  $\mathfrak{A}_N := \text{Jac}(\mathfrak{C}_N)$  die Jakobische von  $\mathfrak{C}_N$ . Die Überlagerung  $\pi : \mathfrak{C}_N \rightarrow \mathbb{P}^1(\mathbb{C}), (x, y) \mapsto x$  ist galoisch mit Galois-Gruppe  $G \simeq \mathbb{Z}/N\mathbb{Z}$ . Sie ist verzweigt bei  $0, 1, \lambda$  und  $\infty$ . Das Geschlecht von  $\mathfrak{C}_N$  ist nach der Riemann-Hurwitz-Formel durch  $g = N - \frac{1+\text{gcd}(N-3, N)}{2}$  gegeben. Bezeichne  $\zeta_N \in \mathbb{C}$  eine fest gewählte primitive  $N$ -te Einheitswurzel. Wir wählen einen Erzeuger  $\sigma$  von  $G$  so, dass

$$\sigma(y) = \zeta_N y, \quad \sigma(x) = x$$

gilt.

## 5.1 Definition der Shimura-Kurve

Wir möchten in diesem Abschnitt für spezielle  $N$  zu einem gegebenen CM-Punkt  $\lambda_0 \in \mathbb{P}^1(\mathbb{F}_q)$  in Charakteristik  $p$  eine Gleichung für die CM-Lifts im Deformationsraum von  $\lambda_0^* \mathfrak{A}_N$  herleiten. Dazu gehen wir ähnlich wie in Abschnitt 4.1 vor. Für  $N \in \{2, 4, 5, 6, 7\}$  korrespondiert  $\mathfrak{A}_N$  zu einer Shimura-Kurve (Satz 5.1.1) im Sinne von Abschnitt 3.2. D.h. es existiert eine arithmetische Fuchssche Gruppe  $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$  und eine Einbettung  $j$  von der Riemannschen Fläche  $\mathcal{X} := \mathcal{H}^*/\Gamma$  in den Modulraum der abelschen Varietäten  $\mathcal{A}_N$  über  $\mathbb{C}$ , so dass  $\mathfrak{A}_N \rightarrow \mathbb{P}^1(\mathbb{C})$  den Morphismus  $j(\mathcal{X}) \rightarrow \mathcal{X}$  darstellt. Fasst man Ergebnisse aus [Möl05, §3] zusammen, dann gilt folgender Satz.

**5.1.1 Satz ( [Möl05] ).** *Die Familie  $\mathfrak{C}_N$  korrespondiert genau dann zu einer Shimura-Kurve, wenn*

$$N \in \{2, 4, 5, 6, 7\}$$

*ist.*

**5.1.2 Bemerkung.** Nach [JN91, Lemma 2.2] parametrisiert  $\mathbb{P}_\lambda^1 \setminus \{0, 1, \infty\}$  durch  $\mathfrak{A}_N$  für  $N = 5$  (bzw.  $N = 7$ ) die Isomorphieklassen von hauptpolarierten abelschen Varietäten  $A$  von Dimension  $g = 4$  (bzw.  $g = 6$ ) mit einer festen Wirkung von  $\mathbb{Z}[\zeta_5]$  (bzw.  $\mathbb{Z}[\zeta_7]$ ) auf  $H^0(A, \Omega_A)$ .

Dies liefert folglich Beispiele von Shimura-Kurven vom PEL-Typ, die sich sehr von denen in Kapitel 4 unterscheiden. Dies ist ein Indiz dafür, dass man mittels unserer Methoden allgemeine Shimura-Kurven vom Typ PEL studieren kann.

**5.1.3 Proposition.** *Sei  $N \in \{2, 4, 5, 6, 7\}$ . Dann ist die Monodromiegruppe der Picard-Fuchs Differentialgleichung  $L$  der Familie  $\mathfrak{A}_N$  (Abschnitt 3.2) gegeben durch eine arithmetische Fuchssche Gruppe  $\Gamma \subset \mathrm{SL}^2(\mathbb{R})$ .*

*In der folgenden Tabelle ist zu  $N \in \mathbb{N}$  die arithmetische Gruppe  $\Gamma$  angegeben. Dabei bezeichnet  $\Delta(a, b, c)$  die Fuchssche Dreiecksgruppe mit lokalen Exponenten  $a, b, c$ . Die korrespondierende Quaternionenalgebra  $D$  über dem reellen Körper  $F$  ist genau in  $\Sigma$  verzweigt.*

$N$	$\Gamma$	$F$	$\Sigma$
2	$\Delta(\infty, \infty, \infty)$	$\mathbb{Q}$	$\emptyset$
4	$\Delta(\infty, \infty, \infty)$	$\mathbb{Q}$	$\emptyset$
5	$\Delta(5, 5, 5)$	$\mathbb{Q}(\sqrt{5})$	$\{(\sqrt{5}), \infty_1\}$
6	$\Delta(\infty, \infty, \infty)$	$\mathbb{Q}$	$\emptyset$
7	$\Delta(7, 7, 7)$	$\mathbb{Q}(\cos \frac{\pi}{7})$	$\emptyset$

**BEWEIS.** Dies folgt aus der Berechnung [Bou05, Lem. 1.1.2] einer Basis der Eigenräume  $\mathcal{L}_i$  von  $H_{\mathrm{dR}}^1(\mathfrak{A}_n/\mathbb{P}_\lambda^1)$  bezüglich der Wirkung von  $\sigma \in G$  und der elementaren Berechnung der Differentialgleichung aus [Bou05,

Lem. 1.1.4]. Die Monodromie-Gruppen korrespondieren nach der Liste der arithmetischen Fuchsschen Gruppen aus [Tak77] zu den entsprechenden Quaternionenalgebren.  $\square$

Wir interessieren uns für den Fall, dass  $\Gamma$  nicht zu einer Modulkurve gehört, d.h. dass  $\mathfrak{A}_N$  kein Produkt der Legendre-Familie von elliptischen Kurven mit einer isotrivialen Deformation ist. Somit betrachten wir die Fälle  $N = 5$  (resp.  $N = 7$ ). Dann ist das Geschlecht von  $\mathfrak{C}_N$  gegeben durch  $g = 4$  (resp.  $g = 6$ ). Bezeichne  $H := H_{\text{dR}}^1(\mathfrak{A}_n/\mathbb{P}_\lambda^1)$  und für  $1 \leq i < N$  sei  $\mathcal{L}_i \subset H$  der Eigenraum von  $H$  bezüglich der Wirkung von  $\sigma$  mit Eigenwert  $\zeta_N^i$ .

**5.1.4 Bemerkung.** Die Dimensionen  $n_i$  von  $H^0(\mathfrak{C}_N, \Omega_{\mathfrak{C}_N}) \cap \mathcal{L}_i$  (resp.  $n'_i$  von  $H^1(\mathfrak{C}_N, \mathcal{O}_{\mathfrak{C}_N}) \cap \mathcal{L}_i$ ) sind nach [Bou05, Lem. 1.1.2] gegeben durch folgende Tabellen:

$\mathfrak{C}_5 :$	$i$	1	2	3	4
$H^0(\mathfrak{C}_5, \Omega_{\mathfrak{C}_5}) :$	$n_i$	2	1	1	0
$H^1(\mathfrak{C}_5, \mathcal{O}_{\mathfrak{C}_5}) :$	$n'_i$	0	1	1	2

$\mathfrak{C}_7 :$	$i$	1	2	3	4	5	6
$H^0(\mathfrak{C}_7, \Omega_{\mathfrak{C}_7}) :$	$n_i$	2	2	1	1	0	0
$H^1(\mathfrak{C}_7, \mathcal{O}_{\mathfrak{C}_7}) :$	$n'_i$	0	0	1	1	2	2

In Proposition 5.1.9 zeigen wir, dass  $\mathfrak{A}_5$  (bzw.  $\mathfrak{A}_7$ ) generisch einfach ist. Genauer treffen wir Aussagen über die Möglichkeiten für die Endomorphismenalgebren. Um dies für  $\mathfrak{A}_7$  zu beweisen, benötigen wir zunächst eine Reihe von Lemmata.

Die Situation ist die folgende: Bezeichne  $K := \mathbb{Q}(\zeta_7)$ . Sei  $\tilde{K} \neq K$  ein CM-Körper von Grad 6 und sei  $K' := K\tilde{K}$  ebenfalls ein CM-Körper. In Lemma 5.1.7 geben wir zunächst die möglichen Galoisgruppen für die Erweiterung  $(K')^{\text{Gal}}/\mathbb{Q}$  an, um in Lemma 5.1.8 im Fall  $[\tilde{K} : \mathbb{Q}] = 6$  Aussagen für Lifts eines CM-Typs von  $\tilde{K}$  nach  $K'$  mit gewissen Eigenschaften treffen zu können.

**5.1.5 Definition.** Definiere  $\tilde{A}_4 < S_6$  als die Untergruppe, erzeugt durch  $(14), (123456) \in S_6$ .

**5.1.6 Bemerkung.** Die Gruppe  $\tilde{A}_4$  ist eine zentrale Erweiterung von  $A_4$  durch  $\text{Zentrum}(\tilde{A}_4) \simeq \mathbb{Z}/2\mathbb{Z}$ . Folglich ist  $|\tilde{A}_4| = 24$ .

**5.1.7 Lemma.**

Sei  $G < S_6$  eine transitive Untergruppe der Ordnung  $|G| = n \cdot 12$ , so dass ein Normalteiler  $N < G$  mit Faktorgruppe  $G/N \simeq \mathbb{Z}/6\mathbb{Z}$  und ein davon verschiedener Normalteiler  $\langle s \rangle < G$  von Index 2 mit  $s \in \text{Zentrum}(G)$  existiert. Dann ist  $G$  isomorph zu  $\tilde{A}_4$ . Insbesondere gilt  $n = 2$ .

BEWEIS. Mittels dem Computeralgebrasystem GAP kann man die 16 transitiven Untergruppen von  $S_6$  auflisten und auf die geforderten Eigenschaften hin überprüfen.  $\square$

**5.1.8 Lemma.**

Bezeichne  $K := \mathbb{Q}(\zeta_7)$ . Dann existiert kein CM-Körper  $\tilde{K} \neq K$  und CM-Typ  $I_{\tilde{K}}$  auf  $\tilde{K}$  mit folgenden Eigenschaften:

- (i) es existiert eine Körpererweiterung  $K'/K$  von Grad 2, so dass  $\tilde{K} \subsetneq K'$ ,
- (ii) es existiert ein Lift  $I_{K'} := (\iota_1, \dots, \iota_6)$  des CM-Typs  $I_{\tilde{K}}$  nach  $K'$ ,
- (iii) für den CM-Typ  $I_{K'}$  gilt nach Permutation

$$(\iota_1(\zeta_7), \dots, \iota_6(\zeta_7)) = (\zeta_7, \zeta_7, \zeta_7^2, \zeta_7^2, \zeta_7^3, \zeta_7^4).$$

BEWEIS. Wir führen folgende Bezeichnungen ein: Sei  $K'_0 \subset K'$  (resp.  $K_0 \subset K$ , resp.  $\tilde{K}_0 \subset \tilde{K}$ ) der reelle Unterkörper von  $K'$  (resp.  $K$ , resp.  $\tilde{K}$ ) von Index 2. Sei  $L$  der Galois-Abschluss von  $K'$  und  $\text{Gal}(L/\mathbb{Q})$  die korrespondierende Galois-Gruppe. Sei  $\tilde{n} := [\tilde{K} : \mathbb{Q}]$ .

Es gilt  $\tilde{K} \subsetneq K'$ , folglich ist  $\tilde{n}$  ein echter Teiler von 12. Ausserdem ist  $\tilde{K}$  ein CM-Körper, folglich gilt  $\tilde{n} \in \{2, 4, 6\}$ . Wir unterscheiden folgende Fälle:

$\tilde{n} = 2$  (siehe Abb. 5.1):

Sind  $K$  und  $\tilde{K}$  algebraisch unabhängig, dann enthält  $\{\iota_i(\zeta_7)\}$  alle sieben Einheitswurzeln. Dies ist ein Widerspruch zu (iii).

Gilt andererseits  $\tilde{K} \subset K$ , dann ist  $\tilde{K} \simeq \mathbb{Q}(\sqrt{-7})$ . In diesem Fall wird  $\text{Gal}(K/\tilde{K})$  erzeugt durch  $\zeta_7 \mapsto \zeta_7^2$ . Der CM-Typ  $I_{K'}$  liftet einen CM-Typ  $I_{\tilde{K}}$  auf  $\tilde{K}$ , d.h. es existieren  $\sigma_i \in \text{Gal}((K')^{\text{Gal}}/\tilde{K})$  mit  $\iota_i|_{\tilde{K}} = \sigma_i \circ \iota_1|_{\tilde{K}}$  für alle  $i$ . Da  $\iota_i(K) = K$  ist, folgt  $\sigma_i|_K \in \text{Gal}(K/\tilde{K})$ . Somit ist entweder  $\iota_i(\zeta_7) \in \{\zeta_7^j, j = 1, 2, 4\}$  für alle  $i$  oder  $\iota_i(\zeta_7) \in \{\zeta_7^j, j = 6, 5, 3\}$  für alle  $i$ . Dies ist im Widerspruch zu (iii). Folglich ist  $\tilde{n} = 2$  nicht möglich.

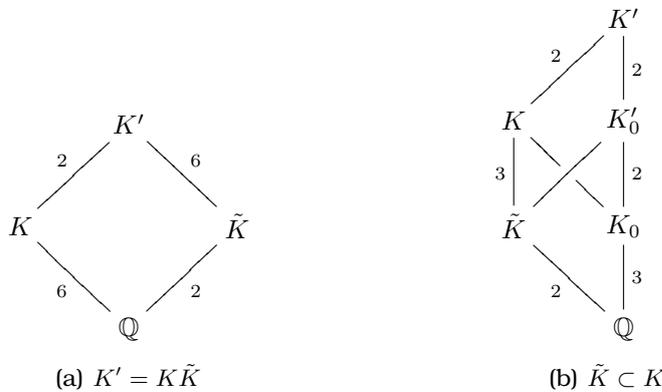


Abbildung 5.1: Fall:  $\tilde{n} = 2$

$\tilde{n} = 4$  (siehe Abb. 5.2):

Es gilt  $[K_0 : \mathbb{Q}] = 3$  und  $[\tilde{K} : \mathbb{Q}] = 4$ . Die Zahlen 3 und 4 sind teilerfremd, somit gilt  $[\tilde{K}K_0 : \mathbb{Q}] = 12$ . Außerdem ist  $\tilde{K}K_0 \subset K'$  und  $[K' : \mathbb{Q}] = 12$ , folglich gilt  $K' = \tilde{K}K_0$ . Ebenso gilt  $K' = K\tilde{K}_0$ . Da  $K/\mathbb{Q}$  und  $\tilde{K}_0/\mathbb{Q}$  galoisch sind, ist folglich  $K'/\mathbb{Q}$  galoisch. Das Element  $\sqrt{-7} \in K \subset K'$  ist auch in  $\tilde{K}$  enthalten, da  $[K' : \tilde{K}] = 3$  gilt. Somit ist  $\tilde{K}$  eine bzyklische Erweiterung von  $\mathbb{Q}$ , da  $\tilde{K}_0, \mathbb{Q}(\sqrt{-7}) \subset \tilde{K}$  gilt. Dann existiert ein  $\sigma \in \text{Gal}(\tilde{K}, \mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$  mit  $\sigma I_{\tilde{K}} = I_{\tilde{K}}$ . Folglich liftet  $I_{\tilde{K}}$  den CM-Typ  $I_{\tilde{K}}^\sigma := I_{\tilde{K}}/\langle \sigma \rangle$  von  $\tilde{K}^{(\sigma)}$ . Wir können diesen Fall also auf den Fall  $\tilde{n} = 2$  reduzieren.

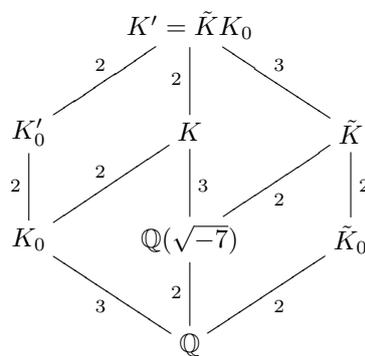


Abbildung 5.2: Fall:  $\tilde{n} = 4$

Wir schließen, dass  $\tilde{n} \neq 4$ . Also ist nur noch der Fall  $\tilde{n} = 6$  zu überprüfen. Aus Überlegungen zu den Graden von  $K_0$  und  $\tilde{K}$  folgt  $K_0 \subset \tilde{K}$ . Der Galois-Abschluss von  $K_0$  ist  $K$  und somit enthält der Galois-Abschluss  $\tilde{K}_{\text{Gal}}$  von  $\tilde{K}$  den Körper  $K$ . Da  $K_0 \subset \tilde{K}$  gilt und  $K$  der Galois-Abschluss von  $K_0$  ist, gilt  $K \subset \tilde{K}_{\text{Gal}}$ . Aus  $K' = K\tilde{K}$  folgt für den Galois-Abschluss  $L$  von  $K'$  somit die Identität  $L = \tilde{K}_{\text{Gal}}$ .

Wir nehmen zunächst an, dass die Galoisgruppe  $G := \text{Gal}(L/\mathbb{Q}) \subset S_6$  eine transitive Untergruppe ist. Da  $K/\mathbb{Q}$  galoisch ist, mit Galoisgruppe  $\text{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ , muss ein Normalteiler  $N \triangleleft G$  existieren mit  $G/N \simeq \mathbb{Z}/6\mathbb{Z}$ . Somit können wir Lemma 5.1.7 anwenden. Es ist folglich  $\text{Gal}(L, \mathbb{Q}) \simeq \tilde{A}_4$ :

$\tilde{n} = 6$ ,  $\text{Gal}(L, \mathbb{Q}) \simeq \tilde{A}_4$  (siehe Abb. 5.3b):

Sei  $G := \tilde{A}_4 \subset S_6$  erzeugt durch  $(14), (123456) \in S_6$ . Bezeichne  $K_{\text{Gal}}$  den Galois-Abschluss von  $K'$ . Der komplexen Konjugation entspricht das Element  $(14)(25)(36) \in \text{Zentrum}(G)$ . Wir suchen Untergruppen  $H_{K'}, H_K, H_{\tilde{K}} < G$ , so dass folgende Eigenschaften erfüllt sind:

- $|H_{K'}| = 2, |H_K| = 4, |H_{\tilde{K}}| = 4,$
- $H_{K'} = H_K \cap H_{\tilde{K}}, \text{ d.h. } K\tilde{K} = K',$
- $H_K \triangleleft G$  und  $G/H_K \simeq \mathbb{Z}/6\mathbb{Z},$

- $|\langle H_K \cup \{(14)(25)(36)\} \rangle| = 8$ , d.h.  $K$  ist CM-Körper,
- $|\langle H_{\tilde{K}} \cup \{(14)(25)(36)\} \rangle| = 8$ , d.h.  $\tilde{K}$  ist CM-Körper,
- $\langle H_K \cup \{(14)(25)(36)\} \rangle = \langle H_{\tilde{K}} \cup \{(14)(25)(36)\} \rangle$ , d.h.  $K_0 \subset K, \tilde{K}$ .

Man zeigt, dass folgende Gruppen diese Eigenschaften erfüllen und bis auf Konjugation eindeutig sind:

$$\begin{array}{c|c} H_{K'} := \langle (25)(36) \rangle & K' = L^{H_{K'}} \\ \hline H_K := \langle (14)(36), (25)(36) \rangle & K = L^{H_K} \\ \hline H_{\tilde{K}} := \langle (25), (36) \rangle & \tilde{K} = L^{H_{\tilde{K}}} \end{array}$$

Wir sind nun in der Lage zu zeigen, dass in dieser Situation die Eigenschaften (ii) und (iii) aus dem Lemma nicht gleichzeitig erfüllt sein können. Dazu nehmen wir an, dass (ii) gilt, d.h. dass ein Lift  $I_{K'} := (\iota_1, \dots, \iota_6)$  eines CM-Typs  $I_{\tilde{K}}$  nach  $K'$  existiert.

Seien also  $\iota_1, \iota_2 \in G$ . Damit  $\iota_1$  und  $\iota_2$  zu einem CM-Typ auf  $K'$  gehören, muss  $\iota_1|_{K'} \neq \iota_2|_{K'}$  und  $\iota_2|_{K'} \neq \bar{\iota}_1|_{K'}$  gelten. D.h. für die Rechtsnebenklassen gilt folgendes:

$$\begin{aligned} \iota_2 H_{K'} &\neq \iota_1 H_{K'} \\ \iota_2 H_{K'} &\neq \iota_1 (14)(25)(36) H_{K'}. \end{aligned}$$

Für  $\iota_1|_{\tilde{K}} = \iota_2|_{\tilde{K}}$  muss

$$\iota_1 H_{\tilde{K}} = \iota_2 H_{\tilde{K}}$$

gelten. Seien  $\iota_1|_K = \text{id}$  und  $\iota_1|_{\tilde{K}} = \iota_2|_{\tilde{K}}$ , dann gilt

$$\iota_1 \in H_K \qquad \text{und} \qquad \iota_2 \in \iota_1 H_{\tilde{K}} \setminus \iota_1 H_{K'}.$$

Für  $h \in H_{\tilde{K}} \setminus \iota_1 H_{K'}$  entspricht  $h|_K$  der komplexen Konjugation auf  $K$ . Also gilt  $\iota_2(\zeta_7) = \bar{\zeta}_7 \notin \{\zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4\}$ . Dies steht im Widerspruch zu (iii).

Wir schließen daraus, dass die Galoisgruppe  $\text{Gal}(L, \mathbb{Q})$  keine transitive Untergruppe von  $S_6$  ist. Daraus folgt, dass  $\tilde{K}$  das Produkt  $\tilde{K}_1 K_0$  für eine quadratischen Erweiterung  $\tilde{K}_1$  von  $\mathbb{Q}$  ist. Dann sind wir im folgendem Fall:

$\tilde{n} = 6$ ,  $\text{Gal}(L, \mathbb{Q}) \simeq (\mathbb{Z}/6\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$  (siehe Abb. 5.3a):

Dann ist  $K'/\mathbb{Q}$  galoisch und bezeichne  $G := (\mathbb{Z}/6\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ . Seien  $r, s \in G$  Erzeuger von  $G$  mit  $r^6 = s^2 = \text{id}$ . O.B.d.A. gelte  $K = (K')^{(s)}$  und  $r(\zeta_7) = \zeta_7^3$ . Dann entspricht das Element  $r^3 \in G$  der komplexen Konjugation auf  $K'$  und es gilt  $\tilde{K}_1 = (K')^{(rs)}$ . Angenommen es existiert ein CM-Typ  $I_{K'}$  auf  $K'$ , der (iii) erfüllt. Insbesondere sind alle

Einbettungen von  $I_{K'}$  modulo  $r^3$  verschieden. Folglich gilt

$$I_{K'} = (\text{id}, s, r^2, r^2s, r, r^4s) \tag{5.2}$$

oder 
$$I_{K'} = (\text{id}, s, r^2, r^2s, rs, r^4). \tag{5.3}$$

Nach der Wahl von  $r, s \in G$  ist  $\tilde{K} = (K')^{\langle r^3s \rangle}$ . Dann liftet  $I_{K'}$  genau dann einen CM-Typ  $I_{\tilde{K}}$  auf  $\tilde{K}$ , wenn sich die Automorphismen aus (5.2) (resp. (5.3)) in genau 3 Rechtsnebenklassen von  $\langle r^3s \rangle$  zerlegen lassen. Dies ist aber offensichtlich nicht möglich.

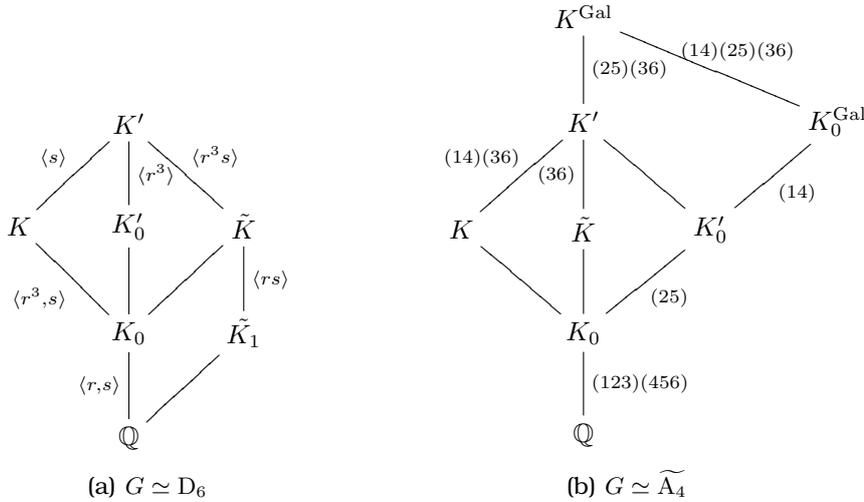


Abbildung 5.3: Fall:  $\tilde{n} = 6$

Insgesamt folgt also die Behauptung des Lemmas. □

Nun sind wir in der Lage folgende Proposition 5.1.9 zu beweisen.

**5.1.9 Proposition.** *Die Menge*

$$\{\text{End}^0(\lambda^*\mathfrak{A}_N) : \lambda \in \mathbb{P}^1(\mathbb{C})\}$$

*enthält unendlich viele CM-Körper. Insbesondere ist das abelsche Schema  $\mathfrak{A}_N$  für  $N \in \{5, 7\}$  generisch einfach.*

**BEWEIS.** Die Aussage für den Fall  $N = 5$  wird zum Beispiel in Proposition 2.7 in [JN91] gezeigt. Wir beweisen die Aussage für  $N = 7$  mit einer ähnlichen Argumentation.

Sei  $\lambda \in \mathbb{C}$  und  $A_\lambda := \lambda^*\mathfrak{A}_7$  mit komplexer Multiplikation im Sinne von Definition 2.1.5. Wir möchten also zeigen, dass unendlich viele  $\lambda \in \mathbb{C}$  existieren, so dass  $A_\lambda$  komplexe Multiplikation besitzt und absolut einfach ist. Sei  $A_\lambda$  so gewählt, dass  $A_\lambda$  komplexe Multiplikation besitzt und nicht einfach ist. Bezeichne  $K := \mathbb{Q}(\zeta_7)$  und  $K_0 := \mathbb{Q}(\zeta_7 + \zeta_7^6)$ . Man unterscheidet zwei Fälle:

1. Angenommen es existiert keine echte Untervarietät  $\tilde{A}$  mit komplexer Multiplikation durch  $K$ . Dann sind wir in der Situation von [Wol88, Satz 4]. Dieser Satz besagt, dass in unserer Situation eine Untervarietät  $\tilde{A} \subset A_\lambda$  von Dimension  $\frac{6}{m}$  mit komplexer Multiplikation existiert, so dass  $A_\lambda \sim \tilde{A}^m$  gilt. Dann gilt  $\text{End}^0(A_\lambda) \simeq M_m(\tilde{K})$  für ein CM-Körper  $\tilde{K}$  und es existiert ein CM-Körper  $K'$  von Grad 12, der  $K$  und  $\tilde{K}$  enthält. Insbesondere gilt  $[K' : K] = 2$ . Die Wirkung von  $\sigma$  auf  $H^0(\mathcal{C}_N, \Omega_{\mathcal{C}_N})$  ist durch den CM-Typ  $I_{K'} := (K'; \iota_1, \dots, \iota_6)$  von  $A_\lambda$  auf  $K'$  bestimmt. D.h. man kann die Matrix der Wirkung von  $\sigma$  auf  $H^0(\mathcal{C}_N, \Omega_{\mathcal{C}_N})$  so diagonalisieren, dass die Einträge durch  $(\iota_i(\zeta_7))_i$  gegeben sind. Aus den Werten  $n_i$  aus Bemerkung 5.1.4 folgt für die Einbettungen  $\iota_i$ , dass nach Permutation

$$(\iota_1(\zeta_7), \dots, \iota_6(\zeta_7)) = (\zeta_7, \zeta_7, \zeta_7^2, \zeta_7^2, \zeta_7^3, \zeta_7^4)$$

gilt. Die Varietät  $A_\lambda$  ist isogen zu einer Potenz von  $\tilde{A}$  und somit ist der CM-Typ  $I_{K'}$  ein Lift des CM-Typs  $I_{\tilde{K}}$  von  $\tilde{A}$  auf  $\tilde{K}$ . Lemma 5.1.8 besagt, dass kein CM-Typ  $I_{\tilde{K}}$  mit diesen Eigenschaften existiert.

2. Angenommen es existiert  $\tilde{A} \subset A_\lambda$  mit komplexer Multiplikation durch  $K$ . Dann sind wir in der Situation von Satz 5 aus [Wol88]. Dieser Satz besagt, dass in unserer Situation eine abelsche Varietät  $\tilde{A}'$  von Dimension 3 mit komplexer Multiplikation durch  $K$  existiert, so dass  $A_\lambda \sim \tilde{A} \times \tilde{A}'$  gilt. Die CM-Typen von  $\tilde{A}$  und  $\tilde{A}'$  müssen somit  $(\zeta_7, \zeta_7^2, \zeta_7^3)$  und  $(\zeta_7, \zeta_7^2, \zeta_7^4)$  sein. Satz 7 in [Wol88] besagt, dass in dieser Situation nach einer geeigneten Normierung des Parameters  $\lambda$  die abelsche Varietät  $A_\lambda$  genau dann eine Untervarietät mit CM-Typ  $(\zeta_7, \zeta_7^2, \zeta_7^3)$  enthält, wenn  $\lambda \in \mathbb{Q}(\zeta_7)$  gilt.

Wählt man nun einen CM-Körper  $\tilde{K} \supset K_0$  mit  $\tilde{K} \neq K$ , dann ist die abelsche Varietät  $\lambda^* A_\lambda$  nach geeigneter Normierung des Parameters  $\lambda$  vom Typ  $K\tilde{K}$ . Dies folgt aus einer völlig analogen Argumentation wie im Beweis für  $N = 5$  in [JN91, Prop. 2.7].  $\square$

## 5.2 Beschreibung der $q$ -Parameter

### 5.2.1 Proposition.

Sei  $p \in \mathbb{N}$  eine Primzahl mit  $(p, N) = 1$ . Für den generischen  $p$ -Rang der Kurven  $\mathcal{C}_5$  und  $\mathcal{C}_7$  gilt folgendes:

$\mathfrak{C}_5$	$p \bmod 5$	generischer $p$ -Rang
	1 mod 5	$g(\mathfrak{C}_5) = 4$
	-1 mod 5	2
	2, 3 mod 5	0
$\mathfrak{C}_7$	$p \bmod 7$	generischer $p$ -Rang
	1 mod 7	$g(\mathfrak{C}_7) = 6$
	2, 4 mod 7	3
	-1 mod 7	2
	3, 5 mod 7	0

BEWEIS. Die Aussage folgt aus [Bou05, Prop. 2.3.5] und der Berechnung der Schranken für den  $p$ -Rang mittels der Dimensionen  $n_i$  und  $n'_i$ .  $\square$

Wir berechnen nun den Locus der abelschen Varietäten  $A_\lambda$  mit  $\mathcal{O}_{\zeta_5} \subset \text{End}(A_\lambda)$  im Deformationsraum einer Kurve  $\overline{A}_\lambda$  über einem endlichen Körper  $k$ .

Sei dazu  $\lambda_0 \in \mathbb{F}_q$  und  $C : y^5 = x(x-1)(x-\lambda_0)$  die Faser von  $\mathfrak{C}_5$  über  $\lambda_0$ . Sei  $\lambda_0$  so gewählt, dass die abelsche Varietät  $\overline{A} := \text{Jac}(C)$  über  $k = \mathbb{F}_q$  einfach und gewöhnlich ist. Dann folgt aus der Honda-Tate-Theorie, dass  $\overline{A}$  komplexe Multiplikation durch ein CM-Körper  $K' \supset K$  besitzt. Wir nehmen außerdem an, dass eine Hauptpolarisierung  $\overline{\lambda} : \overline{A} \rightarrow \overline{A}^t$  existiert. Sei eine Einbettung

$$\Psi_{\zeta_5} : \mathcal{O}_{\zeta_5} \hookrightarrow \text{End}(\overline{A})$$

fest gewählt.

Wir benutzen die Bezeichnungen aus den Abschnitten 3.5 und 3.6. Insbesondere bezeichnet  $M$  den lokalen Modulfunktor von  $\overline{A}$ , wie in Definition 3.5.1. D.h.  $M$  ist der kovariante Funktor  $M : \mathcal{C}_W \rightarrow \mathcal{S}$ , gegeben durch

$$M(R) = \left\{ \begin{array}{l} \text{Isomorphieklassen von } (A_0, \rho_0), \text{ wobei} \\ A_0 \rightarrow \text{Spec}(R) \text{ ein formales abelsches Schema} \\ \text{und } \rho_0 : A_0 \otimes k \xrightarrow{\sim} \overline{A} \text{ ein Isomorphismus ist} \end{array} \right\}.$$

Der zu betrachtende Funktor für die Shimura-Kurve  $\mathbb{P}_\lambda^1$ , die zu  $\mathfrak{A}_5$  korrespondiert, ist nach Bemerkung 5.1.2 wie folgt zu definieren.

**5.2.2 Definition.** Wir definieren den Subfunktor  $N_{\zeta_5}$  vom lokalen Modul-

funktor  $M$  als den kovarianten Funktor  $N_{\zeta_5} : \mathcal{C}_W \rightarrow \mathcal{S}$  durch

$$N_{\zeta_5}(R_0) = \left\{ \begin{array}{l} \text{Isomorphieklassen von } (A_0, \rho_0, \Psi_0, \lambda_0), \text{ wobei} \\ A_0 \rightarrow \text{Spec}(R_0) \text{ ein formales abelsches Schema,} \\ \rho_0 : A_0 \otimes k \xrightarrow{\sim} \bar{A} \text{ ein Isomorphismus,} \\ \Psi_0 : \mathcal{O}_{\zeta_5} \hookrightarrow \text{End}(A_0) \text{ eine Einbettung mit } \Psi_0 \otimes k = \Psi_{\zeta_5} \\ \mathcal{O}_{\zeta_5} \text{ auf } H^0(A_0, \Omega_{A_0}^1) \text{ via } \Psi_0 \text{ durch } (\zeta_5, \zeta_5, \zeta_5^2, \zeta_5^3) \text{ wirkt und} \\ \lambda_0 : A_0 \rightarrow A_0^t \text{ eine Hauptpolarisierung mit } \lambda_0 \otimes k = \bar{\lambda} \text{ ist} \end{array} \right\}.$$

**5.2.3 Proposition.** Sei  $\mathfrak{a}$  das Ideal in  $R$ , erzeugt von den Elementen

$$\begin{aligned} q_{3,4} \cdot q_{4,3}^{-1} - 1, \\ q_{i,j} - 1, \quad \text{für } (i, j) \in \{1, \dots, 4\}^2 \setminus \{(3, 4), (4, 3)\}. \end{aligned}$$

Der Funktor  $N_{\zeta_5}$  ist darstellbar durch das eindimensionale formale Schema  $\text{Spf}(R/\mathfrak{a})$ , d.h. es gibt eine natürliche Äquivalenz

$$\hat{\mathcal{C}}_W(\text{Spf}(R/\mathfrak{a}), -) \xrightarrow{\sim} N_{\zeta_5}(-).$$

BEWEIS. Das Vorgehen ist ähnlich zu jenem aus Abschnitt 4.1 für abelsche Flächen vom Typ  $\mathcal{Q}\mathcal{M}$ . Zunächst bemerkt man, dass für einen Lift  $A_0$  von  $\bar{A}$  nach  $W$  für den  $\mathcal{O}_{\zeta_5} \subset \text{Zentrum}(\text{End}(A_0))$  gilt, der Frobenius-Morphismus  $F$  auf dem  $W$ -Modul  $s^*\text{Fil}^1(H)$  mit  $\zeta_5$  kommutiert. Da die Wirkung von  $\sigma$  auf  $s^*\text{Fil}^1(H)$  diagonalisierbar ist, kommutiert  $\mathcal{O}_{\zeta_5} \subset \text{End}(A_0)$  mit dem Zusammenhang  $\nabla$ . Folglich können wir Eigenvektoren  $s^*a_i, s^*b_i \in s^*H$  von  $\sigma$  wählen, die die Eigenschaften aus Satz 3.5.8 erfüllen. Die Vektoren  $s^*b_i \in s^*\text{Fil}^1(H)$  haben dann die Eigenwerte  $\zeta_5, \zeta_5, \zeta_5^2, \zeta_5^3$  bezüglich  $\sigma$ . Mit Korollar 3.6.16 folgt, dass die Liftbarkeit von  $\sigma$  nach  $A_0$  äquivalent zur Erfüllbarkeit der Gleichungen

$$s^*q_{i,j} = 1, \quad \text{für } (i, j) \in \{1, \dots, 4\}^2 \setminus \{(3, 4), (4, 3)\}$$

ist. Die Gleichung  $q_{3,4} = q_{4,3}$  folgt aus Satz 3.6.13. □

**5.2.4 Proposition.** In der Bezeichnung dieses Abschnittes sei  $\bar{A} := \text{Jac}(C)$  eine abelsche Varietät von Dimension 4, wobei  $C$  eine Faser von  $\mathcal{C}_5$  sei. Besitze  $A$  komplexe Multiplikation durch  $K' \supset K$ . Bezeichne  $\mathcal{O} := \text{End}(\bar{A}) \subset K'$ , d.h. insbesondere gilt  $\mathcal{O}_{\zeta_5} \subset \mathcal{O}$ . Sei  $A_0$  ein Lift von  $\bar{A}$  mit Einbettung  $\mathcal{O}_{\zeta_5} \subset \text{End}(A_0)$ , der zu  $s \in \text{Spf}(R)$  im Deformationsraum korrespondiert. Eine Unterordnung  $\mathcal{O}' \subset \mathcal{O}$  mit  $\mathcal{O}_{\zeta_5} \subset \mathcal{O}'$  lässt sich genau dann zu einer Teilmenge von  $\text{End}(A_0)$  liften, wenn im Deformationsraum folgende Identitäten erfüllt

sind:

$$\begin{aligned} s^* q_{3,4}^{p^n} &= 1, \\ s^* q_{3,4} &= s^* q_{4,3}, \\ s^* q_{i,j} &= 1, \quad \text{für } (i,j) \in \{1, \dots, 4\}^2 \setminus \{(3,4), (4,3)\}. \end{aligned}$$

BEWEIS. Sei die Basis  $s^* a_i, s^* b_i \in s^* H$  von  $s^* H$  wie im Beweis von Proposition 5.2.3 gegeben. Sei  $\pi \in \mathcal{O} \subset K'$  der absolute Frobenius-Morphismus. Wähle  $n \in \mathbb{N}$  minimal so dass  $p^n \pi \in \text{End}(A)$  ist und setze  $\beta := p^n \pi$ . Da  $\beta$  mit  $\sigma$  kommutiert, lässt  $\beta$  die Eigenräume von  $\sigma$  fest. Folglich sind  $s^* b_3$  und  $s^* b_4$  Eigenvektoren zu  $\beta$  und auf  $s^* b_1, s^* b_2$  wirkt  $\beta$  durch eine Matrix  $p^n \psi(\pi) \in M_2(W)$ . Wir bezeichnen die Eigenwerte von  $s^* b_3$  (bzw.  $s^* b_4$ ) mit  $p^n \pi_3 \in W$  (bzw.  $p^n \pi_4 \in W$ ). Nach Korollar 3.6.16 ist die Liftbarkeit nach einer elementaren Rechnung äquivalent zur Erfüllbarkeit der Gleichungen

$$\begin{aligned} p^n \pi_3 (1 - \det(\psi(\pi))) \cdot s^* \tau_{3,4} &\equiv 0 \pmod{p^{n+1}}, \\ p^n \pi_4 (1 - \det(\psi(\pi))) \cdot s^* \tau_{3,4} &\equiv 0 \pmod{p^{n+1}}. \end{aligned}$$

Da  $(1 - \det(\psi(\pi)))$  unipotent ist und  $\pi_3, \pi_4$  invertierbar sind, folgt somit die Behauptung.  $\square$

**5.2.5 Beispiel.** Wir wählen uns eine Faser von  $\mathfrak{C}_5$  mit komplexer Multiplikation. Sei die Kurve  $C : y^5 = x(x-1)(x-\lambda_0)$  mit  $\lambda_0 := \zeta_6$ . Dann ist durch  $\zeta_3 : y \mapsto y, x \mapsto \zeta_3 x + 1$  ein Automorphismus der Ordnung 3 von  $C$  gegeben, der mit  $\zeta_5 : y \mapsto \zeta_5 y, x \mapsto x$  kommutiert. Also gibt es eine Einbettung  $\mathbb{Q}(\zeta_5, \zeta_3) \hookrightarrow \text{End}(\text{Jac}(C))$ . Eine Basis von  $H^0(C, \Omega_C)$  ist durch

$$\begin{aligned} \omega_1^1 &= \frac{dx}{y^4}, \quad \omega_2^1 = \frac{xdx}{y^4} && \in \mathcal{L}_1, \\ \omega_1^2 &= \frac{dx}{y^3} && \in \mathcal{L}_2, \\ \omega_1^3 &= \frac{dx}{y^2} && \in \mathcal{L}_3 \end{aligned}$$

gegeben. Man überprüft, dass  $(\omega_1^1, \omega_2^1, \omega_1^2, \omega_1^3)$  Eigenvektoren zum Automorphismus  $\zeta_3$  mit Eigenwerten  $(\zeta_3, \zeta_3^2, \zeta_3, \zeta_3)$  sind.

Bezeichne  $N_{\zeta_7} \subset M$  den analogen Subfunktorkomplex wie in Definition 5.2.2 für eine Faser  $A_\lambda/\mathbb{F}_q$  der Familie  $\mathfrak{A}_7$  von abelschen Varietäten von Dimension 6. Dann folgt völlig analog wie für Proposition 5.2.3 und Proposition 5.2.4 folgende Proposition.

**5.2.6 Proposition.** Sei  $\mathfrak{a}$  das Ideal in  $R$ , erzeugt von den Elementen

$$\begin{aligned} q_{5,6} \cdot q_{6,5}^{-1} - 1, \\ q_{i,j} - 1, \quad \text{für } (i, j) \in \{1, \dots, 6\}^2 \setminus \{(5, 6), (6, 5)\}. \end{aligned}$$

Der Funktor  $N_{\zeta_7}$  ist darstellbar durch das formale Schema  $\text{Spf}(R/\mathfrak{a})$ .

**5.2.7 Proposition.** Sei  $\bar{A}$  eine abelsche Varietät von Dimension 6 mit komplexer Multiplikation durch eine Ordnung  $\mathcal{O} \subset K'$  mit  $\mathcal{O}_{\zeta_7} \subset \mathcal{O}$ . Sei  $A_0$  ein Lift von  $\bar{A}$  mit Einbettung  $\mathcal{O}_{\zeta_7} \subset \text{End}(A_0)$ . Genau dann lässt sich eine Unterordnung  $\mathcal{O}' \subset \mathcal{O}$  mit  $\mathcal{O}_{\zeta_7} \subset \mathcal{O}'$  zu einer Teilmenge von  $\text{End}(A_0)$  liften, wenn im Deformationsraum folgende Identitäten erfüllt sind:

$$\begin{aligned} s^* q_{3,4}^p &= 1, \\ q_{5,6} \cdot q_{6,5}^{-1} &= 1, \\ q_{i,j} &= 1, \quad \text{für } (i, j) \in \{1, \dots, 6\}^2 \setminus \{(5, 6), (6, 5)\}. \end{aligned}$$

# Literaturverzeichnis

- [AB04] ALSINA, M. und BAYER, P.: *Quaternion orders, quadratic forms, and Shimura curves*. CRM Monograph Series, Bd. 22. Providence, RI : American Mathematical Society, 2004
- [BDIP02] BERTIN, J., DEMAILLY, J.-P., ILLUSIE, L. und PETERS, C.: *Introduction to Hodge theory*. SMF/AMS Texts and Monographs, Bd. 8. Providence, RI : American Mathematical Society, 2002. – Translated from the 1996 French original by James Lewis and Peters
- [Beu07] BEUKERS, F.: Gauss' hypergeometric function. *Arithmetic and geometry around hypergeometric functions* Bd. 260. Basel : Birkhäuser, 2007, S. 23–42
- [BM10] BOUW, I. und MÖLLER, M.: Teichmüller curves, triangle groups, and Lyapunov exponents. *Ann. of Math.* **172** (2010)
- [BO78] BERTHELOT, P. und OGUS, A.: *Notes on crystalline cohomology*. Princeton, N.J. : Princeton University Press, 1978
- [Bou05] BOUW, I.: *Pseudo-elliptic bundles, deformation data, and the reduction of Galois covers*, Fakultät für Mathematik, Universität Duisburg-Essen, Habil., Mai 2005
- [BW06] BOUW, I. und WEWERS, S.: Indigenous bundles with nilpotent  $p$ -curvature. *Int. Math. Res. Not.* (2006), S. 1–37
- [Del71] DELIGNE, P.: Travaux de Shimura. *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389* Bd. 244. Berlin : Springer, 1971, S. 123–165
- [Del81] DELIGNE, P.: Cristaux ordinaires et coordonnées canoniques. *Algebraic surfaces (Orsay, 1976–78)* Bd. 868. Berlin : Springer, 1981, S. 80–137. – With the collaboration of L. Illusie, With an appendix by Nicholas M. Katz
- [Dwo71] DWORK, B.: Normalized period matrices. I. Plane curves. *Ann. of Math. (2)* **94** (1971), S. 337–388

- [Edi05] EDIXHOVEN, B.: On the  $p$ -adic geometry of traces of singular moduli. *Int. J. Number Theory* **1** (2005), Nr. 4, S. 495–497
- [Elk98] ELKIES, N.: Shimura curve computations. *Algorithmic number theory (Portland, OR, 1998)* Bd. 1423. Berlin : Springer, 1998, S. 1–47
- [GD60] GROTHENDIECK, A. und DIEUDONNÉ, J.: EGA I. *Publ. Math. IHES* **4** (1960), S. 5–228
- [GD61] GROTHENDIECK, A. und DIEUDONNE, J.: EGA III. *Pub. Math. IHES* **11** (1961)
- [Has95] HASHIMOTO, K.: Explicit form of quaternion modular embeddings. *Osaka J. Math.* **32** (1995), Nr. 3, S. 533–546
- [HM95] HASHIMOTO, K. und MURABAYASHI, N.: Shimura curves as intersections of Humbert surfaces and defining equations of  $\mathcal{Q}M$ -curves of genus two. *Tohoku Math. J. (2)* **47** (1995), Nr. 2, S. 271–296
- [Hon81] HONDA, T.: Algebraic differential equations. *Symposia Mathematica, Vol. XXIV (Sympos., INDAM, Rome, 1979)*. London : Academic Press, 1981, S. 169–204
- [Jen05] JENKINS, P.:  $p$ -adic properties for traces of singular moduli. *Int. J. Number Theory* **1** (2005), Nr. 1, S. 103–107
- [JN91] DE JONG, J. und NOOT, R.: Jacobians with complex multiplication. *Arithmetic algebraic geometry (Texel, 1989)* Bd. 89. Boston, MA : Birkhäuser Boston, 1991, S. 177–192
- [Kat73] KATZ, N.: Travaux de Dwork. *Séminaire Bourbaki, 24ème année (1971/1972), Exp. No. 409*. Berlin : Springer, 1973, S. 167–200. *Lecture Notes in Math.*, Vol. 317
- [Kat79] KATZ, N.: Slope filtration of  $F$ -crystals. *Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I* Bd. 63. Paris : Soc. Math. France, 1979, S. 113–163
- [Kat81] KATZ, N.: Serre-Tate local moduli. *Algebraic surfaces (Orsay, 1976–78)* Bd. 868. Berlin : Springer, 1981, S. 138–202
- [Ked01] KEDLAYA, K.: Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.* **16** (2001), Nr. 4, S. 323–338
- [Knu91] KNUS, M.-A.: *Quadratic and Hermitian forms over rings*. *Grundlehren der Mathematischen Wissenschaften*, Bd. 294. Berlin : Springer-Verlag, 1991. – With a foreword by I. Bertuccioni

- [KO68] KATZ, N. und ODA, T.: On the differentiation of de Rham cohomology classes with respect to parameters. *J. Math. Kyoto Univ.* **8** (1968), S. 199–213
- [Koh96] KOHEL, D.: *Endomorphism rings of elliptic curves over finite fields*, University of California at Berkeley, Diss., 1996
- [Kro09] KROWORSCH, W: *Congruences of singular moduli*, Universität Ulm, Diss., 2009
- [Lan87] LANG, S.: *Elliptic functions*. Graduate Texts in Mathematics, Bd. 112. Second. New York : Springer-Verlag, 1987. – With an appendix by J. Tate
- [Mes72] MESSING, W.: *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Berlin : Springer-Verlag, 1972 (Lecture Notes in Mathematics, Vol. 264)
- [MM74] MAZUR, B. und MESSING, W.: *Universal extensions and one dimensional crystalline cohomology*. Berlin : Springer-Verlag, 1974 (Lecture Notes in Mathematics, Vol. 370)
- [Möl05] MÖLLER, M.: Shimura- and Teichmüller curves. *Arxiv preprint math/0501333* (2005)
- [Moo98] MOONEN, B.: Models of Shimura varieties in mixed characteristics. *Galois representations in arithmetic algebraic geometry (Durham, 1996)* Bd. 254. Cambridge : Cambridge Univ. Press, 1998, S. 267–350
- [Moo01] MOONEN, B.: Group schemes with additional structures and Weyl group cosets. *Moduli of abelian varieties (Texel Island, 1999)* Bd. 195. Basel : Birkhäuser, 2001, S. 255–298
- [Moo04] MOONEN, B.: Serre-Tate theory for moduli spaces of PEL type. *Ann. Sci. École Norm. Sup. (4)* **37** (2004), Nr. 2, S. 223–269
- [Mor81] MORITA, Yasuo: Reduction modulo  $P$  of Shimura curves. *Hokkaido Math. J.* **10** (1981), Nr. 2, S. 209–238
- [Mor09] MORI, A.: An Expansion Principle for Quaternionic Modular Forms. *Arxiv preprint math/0406388v2* (2009)
- [Mum74] MUMFORD, D.: *Abelian Varieties*. Oxford University Press, 1974
- [Neu07] NEUKIRCH, J.: *Algebraische Zahlentheorie*. Springer-Verlag Berlin Heidelberg, 2007
- [Oda69] ODA, T.: The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. École Norm. Sup. (4)* **2** (1969), S. 63–135

- [Oor] OORT, F.: Endomorphism algebras of abelian varieties. *Algebraic geometry and commutative algebra, Vol. II*. Tokyo : Kinokuniya, S. 469–502
- [Oor71] OORT, F.: Finite group schemes, local moduli for abelian varieties, and lifting problems. *Compositio Math.* **23** (1971), S. 265–296
- [Ser77] SERRE, J.-P.: *Cours d'arithmétique*. Paris : Presses Universitaires de France, 1977. – Deuxième édition revue et corrigée, Le Mathématicien, No. 2
- [Shi63] SHIMURA, G.: On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math. (2)* **78** (1963), S. 149–192
- [Shi67] SHIMURA, G.: Construction of class fields and zeta functions of algebraic curves. *Ann. of Math. (2)* **85** (1967), S. 58–159
- [Shi94] SHIMURA, G.: *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, Bd. 11. Princeton, NJ : Princeton University Press, 1994
- [Shi98] SHIMURA, G.: *Abelian varieties with complex multiplication and modular functions*. Princeton Mathematical Series, Bd. 46. Princeton, NJ : Princeton University Press, 1998
- [Tak77] TAKEUCHI, K.: Arithmetic triangle groups. *J. Math. Soc. Japan* **29** (1977), Nr. 1, S. 91–106
- [Tat68] TATE, J.: Classes d'isogénie des variétés abéliennes sur un corps fini. *Séminaire Bourbaki* **352** (1968), S. 95–110
- [Vig80] VIGNÉRAS, M.-F.: *Arithmétique des algèbres de quaternions*. Lecture Notes in Mathematics, Bd. 800. Berlin : Springer, 1980
- [Wat69] WATERHOUSE, W.: Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)* **2** (1969), S. 521–560
- [Wil95] WILES, A.: Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)* **141** (1995), Nr. 3, S. 443–551
- [Wol88] WOLFART, Jürgen: Werte hypergeometrischer Funktionen. *Invent. Math.* **92** (1988), Nr. 1, S. 187–216
- [Yos87] YOSHIDA, M.: *Fuchsian differential equations*. Braunschweig : Friedr. Vieweg & Sohn, 1987 (Aspects of Mathematics, E11). – With special emphasis on the Gauss-Schwarz theory

- [Zag02] ZAGIER, D.: Traces of singular moduli. *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)* Bd. 3. Int. Press, Somerville, MA, 2002, S. 211–244



# Zusammenfassung

In dieser Arbeit studieren wir arithmetische Eigenschaften von Shimura-Kurven vom Typ PEL in gemischter Charakteristik. Eine Shimura-Kurve  $\mathcal{X}$  vom Typ PEL besitzt die Eigenschaft, dass sie eine Familie hauptpolarisierter abelscher Varietäten  $A$  mit einer Einbettung  $\mathcal{O} \hookrightarrow \text{End}(A)$  einer festen Ordnung  $\mathcal{O}$  parametrisiert. Sei eine solche abelsche Varietät  $A$  mit guter, gewöhnlicher Reduktion  $\bar{A}$  gegeben. Wir untersuchen den Lokus  $V$  der Shimura-Kurve  $\mathcal{X}$  im Deformationsraum von  $\bar{A}$  und besonders die Geometrie der CM-Punkte in  $V$ . Dies entspricht dem wichtigsten Schritt im Beweis der Kongruenzen von verallgemeinerten Spuren singulärer Moduli auf Modulkurven in [Kro09]. Dies lässt vermuten, dass man analog Kongruenzen von verallgemeinerten Spuren von CM-Punkten auf Shimura-Kurven beweisen kann.

Wir fassen dazu die Deformationstheorie gewöhnlicher abelscher Varietäten benutzerfreundlich zusammen. Im Gegensatz zu [Kro09] formulieren wir diese in Termen der de-Rham-Kohomologie. Der Vorteil ist, dass die de-Rham-Kohomologie geeigneter für explizite Berechnungen ist. Mittels der de-Rham-Kohomologie lassen sich analog zur Serre-Tate-Theorie für  $p$ -divisible Gruppen Parameter auf dem Deformationsraum von  $\bar{A}$  definieren ([Del81]). Wir leiten aus [Mes72] Bedingungen für die Liftbarkeit von Endomorphismen an diese Parameter her (Korollar 3.6.16). Diese entsprechen den Bedingungen an die Serre-Tate-Parameter ([Kat81, Thm. 2.1]).

Die Bestimmung des Lokus  $V$  der Shimura-Kurve entspricht einem Deformationsproblem. Man betrachtet nämlich die Lifts von  $\bar{A}$ , welche die Ordnung  $\mathcal{O}$  liften. Mittels der Liftbarkeitsbedingung für Endomorphismen an die Parameter des Deformationsraum kann man Gleichungen für den Lokus  $V$  angeben.

Mittels dieser Überlegung bestimmen wir in zwei Spezialfällen explizite Gleichungen für den Lokus  $V$  (Thm. 4.1.6, bzw. Prop. 5.2.3). In dem Fall dass  $\mathcal{X}$  zu einer maximalen Ordnung  $\mathcal{O}$  in einer indefiniten Quaternionenalgebra ist, liefert uns diese andere Methode ähnliche Gleichungen wie in [Mor09]. Im Fall dass  $\mathcal{X}$  zyklische Überlagerung von  $\mathbb{P}^1$  parametrisiert liefert uns diese Methode neue Gleichungen, die ein Indiz dafür geben, dass

sich die Methode in allgemeinere Kontexte übertragen lässt. Überdies geben wir die Geometrie der CM-Punkte auf  $V$  an (Prop. 4.1.8, bzw. Prop. 5.2.4).

Auf dem Weg zu diesen Ergebnissen studieren wir abelsche Flächen  $A$  mit Einbettungen  $\mathcal{O} \hookrightarrow \text{End}(A)$  einer maximalen Ordnung  $\mathcal{O}$  in einer indefiniten Quaternionenalgebra. Wir nennen diese abelsche Flächen  $A$  vom Typ  $\mathcal{QM}$ . Besitzt eine abelsche Fläche  $A$  vom Typ  $\mathcal{QM}$  zusätzlich komplexe Multiplikation, so ist sie isogen zum Produkt zweier isogener elliptischer Kurven. Wir benutzen eine Idee von Mori ([Mor09]), um explizit eine solche Isogenie zu konstruieren (Thm. 2.4.12). Diese könnte interessant sein, um explizit abelsche Flächen vom Typ  $\mathcal{QM}$  mit komplexer Multiplikation zu konstruieren oder um Gleichungen für Shimura-Kurven zu beweisen.

## **Danksagung**

Allen voran möchte ich mich an dieser Stelle herzlich bei Frau Prof. Dr. Irene I. Bouw für ihre stete Ermutigung und ihre intensive persönliche Betreuung bedanken, insbesondere auch für die Unterstützung, die sie mir gab.

Weiterer Dank gilt dem gesamten Institut für Reine Mathematik für die Unterstützung und freundliche Atmosphäre, die ich dort erfahren durfte.

Ebenfalls danke ich der *Graduate School Mathematical Analysis of Evolution, Information and Complexity*, die half einen Rahmen für angenehmes wissenschaftliches Arbeiten zu schaffen.

Zuletzt möchte ich meiner Familie danken, besonders meiner Frau Sabine, für die Unterstützung, für die Geduld und Ermunterung. Aber vor allem für die kleinen und großen Dinge, die scheinbar neben der Arbeit abliefen, welche jedoch einen hellen und warmen Ort für das Arbeiten schufen.