Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen

Dem Fachbereich 6 (Mathematik und Informatik)
der Universität Gesamthochschule Essen
zur Erlangung des Grades eines Doktors
der Naturwissenschaften
(Dr.rer.nat)

vorgelegt im Juli 1994 von

Anne-Monika Spallek

aus Bochum

Einleitung

Aufgrund der zunehmenden Vernetzung von Datenverarbeitungsanlagen entsteht ein erhöhter Bedarf an Verfahren zur Sicherung übertragener Daten, das heißt an Verschlüsselungsalgorithmen und an ein sicheres Key-Management (Vereinbarung geheimer Schlüssel, Schlüsselaustausch, Schlüsselspeicherung). Seit Diffie und Hellmann im Jahre 1976 mit ihrer richtungsgebenden Arbeit 'New Directions in Cryptography' die Idee der Public-Key-Verfahren (auch: asymmetrische Verfahren) präsentierten, haben sich viele Kryptologen mit dem Auffinden solcher Kryptoalgorithmen und deren mathematischen Grundlagen beschäftigt. Das Konzept dieser Public-Key-Systeme ist dadurch gekennzeichnet, daß jeder Teilnehmer ein Schlüsselpaar hat, das aus einem öffentlichen Schlüssel (Public Key) und einem privaten geheimen Schlüssel besteht. Für dieses Paar muß gelten, daß ein potentieller Angreifer aus Kenntnis des Public-Key nur mit extrem hohem Aufwand (der in der Praxis seine Möglichkeiten übersteigt) auf den geheimen privaten Schlüssel schließen kann. Public-Key-Kryptosysteme basieren damit auf mathematischen Funktionen, die einerseits leicht zu berechnen, aber andererseits nur schwer umzukehren sind. Das bekannteste Public-Key-Verfahren ist das RSA-Verfahren. Hierbei wird ausgenutzt, daß man große ganze Zahlen sehr schnell miteinander multiplizieren kann, während hingegen das Faktorisieren einer großen Zahl sehr zeitaufwendig ist. Andere Systeme nutzen die Tatsache aus, daß in einigen Gruppen die diskrete Exponentiation, d.h. die Berechnung von $b = a^n$ in G für $a \in G, n \in \mathbb{Z}$ einfach, die Berechnung der Umkehrfunktion, des diskreten Logarithmus $n = log_a(b)$ in G, aber ungleich schwieriger ist. Diese auf dem Logarithmusproblem basierende Systeme werden allgemein DL-Systeme genannt. Ein Angreifer, der dieses DL-System knacken möchte, muß den diskreten Logarithmus in der zugrunde gelegten Gruppe rechentechnisch lösen können. Gruppen, in denen die diskrete Exponentiation schnell berechnet werden kann, das Logarithmusproblem aber nicht mehr beherrschbar ist, nennen wir *kryptographisch geeignete* Gruppen oder nur *geeignete* Gruppen. Aus den für das Logarithmusproblem heutzutage bekannten Algorithmen erhalten wir explizite Bedingungen für geeignete Gruppen.

Die Menge der Punkte einer Abelschen Varietät über einem endlichen Körper ist eine endliche abelsche Gruppe und die Addition ist stets durch rationale Funktionen gegeben. Demnach können auch Abelsche Varietäten für die DL-Systeme genutzt werden. Wir nennen eine über einem endlichen Körper $\mathbb{F}_q$ definierte Abelsche Varietät A geeignet, falls die

Gruppe $A(\mathbb{F}_q)$ der $\mathbb{F}_q$-rationalen Punkte kryptographisch geeignet ist. Für ihre kryptographische Anwendung müssen noch die folgenden Probleme gelöst werden:

- Herleitung einer schnellen diskreten Exponentiation auf einer Abelschen Varietät
- Realisierung einer kryptographisch geeigneten Abelschen Varietät

Die Addition auf einer Abelschen Varietät ist im allgemeinen für Kryptosysteme viel zu kompliziert. In einer besseren Situation ist man, wenn die Abelsche Varietät A die Jacobische Varietät J_C einer Kurve C ist. Dann ist die Gruppe $J_C(\mathbb{F}_q)$ der $\mathbb{F}_q$-rationalen Punkte der Jacobischen Varietät gleich der Divisorklassengruppe der Kurve und damit die Addition auf $J_C(\mathbb{F}_q)$ durch die Addition in der Divisorklassengruppe gegeben. Durch den Satz von Riemann-Roch kann sie auf das Auffinden von Funktionen auf der Kurve mit gegebenen Null- und Polstellen zurückgeführt werden. Das Problem der Realisierung einer geeigneten Jacobischen Varietät reduziert sich in diesem Fall auf die Realisierung der zugehörigen Kurve.
Für Kurven vom Geschlecht 1, d.h. für **elliptische Kurven**, erhält man bekanntlich sehr kurze Additionsformeln. Eine explizite Gleichung einer geeigneten elliptischen Kurve kann mit Hilfe eines bekannten Verfahrens nach einer Idee von Atkin, das auf der Theorie der komplexen Multiplikation basiert, konstruiert werden.

Es stellt sich nun die Frage, ob **Jacobische Varietäten von Kurven vom Geschlecht 2** für die DL-Systeme geeignet sind. Im ersten Teil dieser Arbeit habe ich die **kryptographischen Eigenschaften** einer Jacobischen Varietät einer Kurve vom Geschlecht 2 genauer untersucht und gezeigt, daß sie gegenüber den elliptischen Kurven einige wesentliche Vorteile haben. Im zweiten Teil habe ich für einen affinen Teil der Jacobischen Varietät sehr **kurze Additionsformeln** hergeleitet, die eine schnelle Berechnung der diskreten Exponentiation ermöglichen. Schließlich habe ich im dritten Teil die Idee von Atkin auf Jacobische Varietäten von Kurven vom Geschlecht 2 ausgeweitet und darauf aufbauend einen **Algorithmus zur Konstruktion von kryptographisch geeigneten Varietäten** entwickelt. Mit diesem Algorithmus konnte ich einige geeignete Varietäten konstruieren. Zuletzt habe ich auf der Basis dieser partiellen Additionsformeln ein **Kryptosystem** implementiert, das diese geeigneten Varietäten benutzt (Authentifikationssystem [Spa II]).

1) Herleitung einer schnellen Addition

1987 veröffentlichte D.G. Cantor [Cant] für die Addition auf der Jacobischen Varietät einer hyperelliptischen Kurve einen Additionsalgorithmus, der ausnutzt, daß den Divisorklassen eindeutig spezielle quadratische Formen zugeordnet werden können. Unabhängig hiervon leitete W. Kampkötter in seiner Dissertation 1991 [Ka] aus den Additionstheoremen der zugehörigen Thetafunktionen eine Additionsformel für die partielle Addition auf der zweidimensionalen affinen Varietät $J_C - \Theta$ her. Zusammen mit einer vollständigen Überdeckung von J_C durch Karten isomorph zu $J_C - \Theta$ definiert dies dann eine Addition auf J_C. Die vollständige Formel erstreckt sich über mehrere Seiten und ist daher für Kryptosysteme ungeeignet.
Meine Idee bestand darin, beide Ansätze zu kombinieren und aus der Addition in der Divisorklassengruppe Additionsformeln für die partielle Addition auf $J_C - \Theta$ herzuleiten. Es zeigt sich, daß man für die rationalen Punkte der affinen Varietät $J_C - \Theta$ eine für die Addition geeignetere Darstellung herleiten kann, die zwar mehrere Fallunterscheidungen nötig macht, aber in den einzelnen Fällen zu sehr kurzen Formeln führt. Diese können anschließend noch so vereinfacht werden, daß die Addition hiermit mehr als 2.5 mal schneller ist als mit dem Cantorschen Algorithmus.

2) Konstruktion einer geeigneten Jacobischen Varietät

Problemstellung :

> Gesucht wird eine explizite Gleichung einer kryptographisch geeigneten Jacobischen Varietät, d.h. ein endlicher Körper $\mathbb{F}_q$ und die Gleichung einer Kurve C vom Geschlecht 2 definiert über $\mathbb{F}_q$, so daß die Gruppe $J_C(\mathbb{F}_q)$ der rationalen Punkte der Jacobischen Varietät J_C von C kryptographisch geeignet ist. Die expliziten Bedingungen hierfür werden im ersten Kapitel hergeleitet und genauer präzisiert.

Der naive Lösungsansatz besteht darin, daß man sich zufällig Kurven C über endlichen Körpern $\mathbb{F}_q$ wählt, die $\mathbb{F}_q$-rationalen Punkte ihrer Jacobischen Varietät J_C zählt und anschließend diese Bedingungen überprüft. Da es aber für Jacobische Varietäten keinen schnellen Punktezählalgorithmus gibt und der anschließende Erfolg vom Zufall abhängt, ist dieses Probierverfahren für die Praxis zu zeitaufwendig und daher ungeeignet.

Erfolgversprechender ist die umgekehrte Strategie.

> Man sucht zunächst eine geeignete Punktegruppe und konstruiert hierzu die Gleichung der zugehörigen Jacobischen Varietät bzw. Kurve.

Für elliptische Kurven löst diese Konstruktionsaufgabe ein bekanntes Verfahren, das auf der Theorie der komplexen Multiplikation basiert. Hierauf aufbauend habe ich in meiner Diplomarbeit [Spa I] einen Algorithmus zur Konstruktion von geeigneten elliptischen Kurven entwickelt. Man geht dabei folgendermaßen vor:

Zunächst wählt man sich einen imaginärquadratischen Zahlkörper K und eine ganze Zahl $\omega \in O_K$, so daß $\omega\bar{\omega} = p$ für eine geeignete Primzahl p ist. In diesem Fall ist ω das Frobeniuselement des Frobeniusendomorphismus π_p auf einer elliptischen Kurve E mit komplexer Multiplikation und Endomorphismenring O_K. Das charakteristische Polynom $f_p(x) = (x - \omega)(x - \bar{\omega})$ des Frobeniusendomorphismus liefert für $x = 1$ die Anzahl N_p der $\mathbb{F}_p$-rationalen Punkte von E. Man kann nun die Bedingungen einer kryptographisch geeigneten Gruppe leicht überprüfen und so testen, ob E über $\mathbb{F}_p$ eine geeignete Gruppe liefern würde.

Mit Hilfe der Theorie der komplexen Multiplikation kann dann die zugehörige Kurvengleichung von E über $\mathbb{F}_p$ explizit konstruiert werden. Man berechnet zunächst analytisch mit Hilfe der bekannten j-Funktion die Invarianten $j_1, ..., j_h$ der Klassengruppe von K, wobei h die Klassenzahl von K bezeichnet. Diese Klasseninvarianten sind die j-Invarianten von über K konjugierten elliptischen Kurven E_j definiert über $K(j)$ mit Endomorphismenring O_K. Zu jeder j-Invariante kennt man direkt die Gleichung einer zugehörigen Kurve $E_j/K(j)$. Die zugehörigen Kurvengleichungen über $\mathbb{F}_p$ erhält man über die Reduktion der j-Invarianten. Nach dem Hauptsatz der komplexen Multiplikation sind die Invarianten ganzalgebraische Zahlen und der von einer Invariante j erzeugte Zahlkörper $K(j)$ ist der Hilbertsche Klassenkörper von K. Das Klassenpolynom $\mathcal{H}(x) := \prod_{i=1}^{h}(x - j_i)$ hat ganzzahlige Koeffizienten und die reduzierten Invarianten $j_{(p)}$ entsprechen den Nullstellen des reduzierten Klassenpolynoms $\mathcal{H}_p(x) = \mathcal{H}(x) \bmod p$. Anschließend kann man direkt zu jeder Invariante $j_{(p)}$ eine Gleichung der Kurve $E_{j_{(p)}}/\mathbb{F}_p$ angeben. Durch Exponentiation eines Punktes $P \in E_{j_{(p)}}(\mathbb{F}_p)$ mit $N_p = f_p(1)$ überprüft man leicht, welche Kurve die gewünschte geeignete Gruppe liefert.

Ziel meiner Arbeit war es, diesen Konstruktionsalgorithmus auf **Jacobische Varietäten von Kurven vom Geschlecht 2** auszuweiten, um so kryptographisch geeignete Varietäten angeben zu können. Dieser Fall ist wesentlich komplizierter, da die Kurve und ihre Jacobische Varietät verschieden sind. Die Jacobische Varietät ist bezüglich der kanonischen Polarisierung eine einfache prinzipal polarisierte Abelsche Varietät der Dimension 2. Für die Verallgemeinerung des Verfahrens wird daher die Theorie der komplexen Multiplikation von Abelschen Varietäten von Shimura/Taniyama (1975) [S-T],[Sh] benötigt. Der Körper der komplexen Multiplikation ist jetzt ein CM-Körper K vom Grad 4 über $\mathbb{Q}$, d.h. eine total imaginärquadratische Erweiterung eines total reellen Zahlkörpers. Die Konstruktion von Jacobischen Varietäten von Kurven vom Geschlecht 2 reduziert sich also auf die Konstruktion von einfachen Abelschen Varietäten A der Dimension 2 mit Endomorphismenring O_K bezüglich eines CM-Körpers K und die Konstruktion von prinzipalen Polarisierungen auf den Abelschen Varietäten. Da die analytische Darstellung von A von der komplexen Darstellung des Endomorphismenrings abhängt, betrachtet man CM-Typen bestehend aus einem CM-Körper K und einer speziellen Menge von Isomorphismen von K nach $\mathbb{C}$.

Im dieser Arbeit wird gezeigt, unter welchen Bedingungen es prinzipale Polarisierungen zu einem gegebenen CM-Typ gibt und wie sie explizit konstruiert werden können (Proposition 4.1, Satz 4.2). Anschließend wird gezeigt, daß die prinzipal polarisierten Abelschen Varietäten von einem CM-Typ eindeutig speziellen Zahlenpaaren entsprechen. Die Isomorphieklassen von prinzipal polarisierten Abelschen Varietäten entsprechen dann den zugehörgigen Zahlklassen, für die schließlich (Satz 4.7) explizit Vertretersysteme konstruiert werden. Zu diesen prinzipal polarisierten Abelschen Varietäten werden in Kapitel 4.3 die zugehörigen Periodenmatrizen aus der zweidimensionalen Siegelschen oberen Halbebene berechnet. Um die Idee von Atkin auf die Konstruktion von Kurven vom Geschlecht 2 zu übertragen, müssen zu diesen Zahlklassen Klasseninvarianten und Klassenpolynome bestimmt werden. Aus der Theorie der projektiven Invarianten von Binärformen sechsten Grades erhält man ein vollständiges Invariantensystem für Kurven vom Geschlecht 2, dargestellt in den Koeffizienten der Kurvengleichung. Bolza zeigte schon 1887 in [Bo II], daß diese Invarianten über den komplexen Zahlen durch die zehn geraden Thetanullwerte bezüglich der zugehörigen Periodenmatrix ausgedrückt werden können. Damit ist die analytische Berechnung der Invarianten von Kurven vom Gechlecht 2 über $\mathbb{C}$ möglich. Der Hauptsatz der komplexen Multiplikation von Abelschen Varietäten besagt, daß diese Invarianten einen unverzweigten Klassenkörper über dem dualen Körper K^* von K erzeu-

gen. Sie sind ganzalgebraische Zahlen, wenn die zugehörige Kurve überall potentiell gute Reduktion hat. Dann haben die zugehörigen Klassenpolynome ganzzahlige Koeffizienten und die Nullstellen der reduzierten Polynome liefern die reduzierten Invarianten der reduzierten Kurven. In vielen Beispielen kann so das Invariantensystem einer über einem Primkörper definierten Kurve berechnet werden.

Ist A eine über einem Primkörper $\mathbb{F}_p$ definierte Abelsche Varietät, so bestimmt das charakteristische Polynom $f_p(x)$ des Frobeniusendomorphismus π_p auf A für $x = 1$ die Anzahl N_p der $\mathbb{F}_p$-rationalen Punkte. Da A komplexe Multiplikation mit $End(A) = O_K$ hat, kann das Frobeniuselement $\omega \in O_K$ explizit berechnet werden. Wenn A Dimension 2 hat, ist $N_p = f_p(1) = \prod_{i=1}^{4}(1 - \omega_i)$, wobei die ω_i die über K konjugierten Elemente von ω sind. Adleman und Huang zeigten in [A-H], daß es unter speziellen Bedingungen an das Frobeniuselement ω eine über $\mathbb{F}_p$ definierte prinzipal polarisierte Abelsche Varietät A mit Endomorphismenring O_K gibt. Diese ist $\mathbb{F}_p$-isomorph zu der Jacobischen Varietät J_C einer über $\mathbb{F}_p$ definierten Kurve C vom Geschlecht 2. Können wir über die analytische Auswertung der Klassenpolynome ein modulo p reduziertes Invariantensystem berechnen, so erhält man durch Lösen des Invariantengleichungssystems die Gleichung der Kurve über $\mathbb{F}_p$. Hieraus wiederum erhält man direkt eine Gleichung der zugehörigen Jacobischen Varietät. Anschließend kann man durch Exponentiation eines Punktes auf der Jacobischen Varietät $J_C(\mathbb{F}_p)$ mit der gewünschten Gruppenordnung $N_p = f_p(1)$ testen, ob sie die gesuchte geeignete Gruppe liefert.

Das erste Kapitel enthält einige Grundlagen der Public-Key-Kryptographie. Hierzu werden die RSA- und DL-Verfahren genauer analysiert und miteinander verglichen. Nachdem die für das Logarithmusproblem bekannten Algorithmen kurz angeführt wurden, werden wir hieraus Bedingungen für kryptographisch geeignete Varietäten ableiten. Anschließend werden die Vor- und Nachteile von DL-Systemen auf Basis von Kurven vom Geschlecht 2 untersucht und die zugehörigen Kryptoprotokolle angegeben.

Das zweite Kapitel liefert die theoretischen Grundlagen des Divisorklassengruppenmodells der Jacobischen Varietät einer hyperelliptischen Kurve. Für die rationalen Punkte der Jacobischen Varietät einer Kurve vom Geschlecht 2 wird hiervon ausgehend eine geeignete rationale Darstellung hergeleitet. Schließlich werden bezüglich dieser Darstellung kurze Additionsformeln berechnet.

Das dritte Kapitel beinhaltet die wesentlichen Sätze und Definitionen aus der Theorie

der komplexen Multiplikation von Abelschen Varietäten von Shimura/Taniyama [S-T],[Sh] (1975). Sämtliche Sätze wurden speziell für prinzipal polarisierte Abelsche Varietäten formuliert und teilweise bewiesen, weil sich ihre Beweise in diesem Spezialfall vereinfachen ließen.

Im vierten Kapitel werden wir für Abelsche Varietäten der Dimension 2 mit komplexer Multiplikation explizit prinzipale Polarisierungen zu einem gegebenen CM-Typ konstruieren. Es wird gezeigt, daß man den Isomorphieklassen eindeutig spezielle Zahlklassen zuordnen kann, für welche wir Vertretersysteme angeben werden. Anschließend werden die zu einem CM-Typ gehörenden Periodenmatrizen bestimmt und die zehn geraden Thetanullwerte an ihnen ausgewertet.

Das fünfte Kapitel enthält die Herleitung der Invariantensysteme einer Kurve vom Geschlecht 2. Man erhält so rationale Darstellungen in den Koeffizienten der Kurvengleichung. Die zugehörigen Darstellungen in den zehn geraden Thetanullwerte werden anschließend angegeben.

Das letzte Kapitel liefert den vollständigen Algorithmus zur Konstruktion von geeigneten Jacobischen Varietäten von Kurven vom Geschlecht 2. Außerdem werden mehrere Beispiele erläutert und berechnet. Mit diesem Konstruktionsalgorithmus gelang es mir, einige kryptographisch geeignete Varietäten zu konstruieren.

An dieser Stelle möchte ich mich bei Herrn Prof.Dr.G.Frey für die Aufgabenstellung und die Unterstützung bei der Bearbeitung des Themas danken. Weiterhin gilt mein Dank Herrn Priv.Doz.H.-G.Rück für wertvolle Anregungen und aufschlußreiche Gespräche.

Inhaltsverzeichnis

Kapitel 1

Kurven vom Geschlecht 2 in Public-Key-Systemen

1.1 Kryptosysteme und Abelsche Varietäten

Die Public-Key-Kryptographie bietet hervorragende Methoden für die Sicherung der **Integrität** (Unversehrtheit), **Authentizität** (Echtheit des Ursprungs) und **Vertraulichkeit von Daten**. Die einzelnen Aufgaben können mit Hilfe der Sicherheitsmechanismen *elektronische Unterschrift* und *Verschlüsselung* erfüllt werden. Die verschiedenen Kryptoalgorithmen eignen sich zur Realisierung dieser Sicherheitsmechanismen unterschiedlich gut. In diesem Abschnitt werden wir das RSA- und DL-Verfahren miteinander vergleichen und dabei speziell die Verwendung von Abelschen Varietäten genauer untersuchen.

Das **RSA-Verfahren** (so benannt nach seinen Erfindern Rivest, Shamir und Adleman) beruht darauf, daß man große ganze Zahlen sehr schnell miteinander multiplizieren kann, die anschließende Faktorisierung allerdings problematisch ist. Dieses Verfahren hat sich unter den asymmetrischen Kryptoverfahren als 'Quasi-Standard' durchgesetzt und ist heutzutage schon auf vielen Prozessorchipkarten implementiert. Leider wurden in jüngster Zeit erhebliche Fortschritte in der Faktorisierung gemacht [Le]. Lange Zeit herrschte die Meinung, RSA-Moduli mit 512 Bit seien sicher. Mittlerweile stimmen die Experten darin überein, daß man bei Verwendung der RSA-Algorithmen größere Modullängen von beispielsweise 1024 Bit vorsehen sollte [Beu]. Größere Modullängen haben immer eine starke Verschlechterung der Performance zur Folge, denn der mit dem RSA-Verfahren verbundene Rechenaufwand wächst mindestens quadratisch mit der Länge des Moduls.

Ein **DL-System** basiert darauf, daß in speziellen Gruppen G die Berechnung der **diskreten Exponentiation** $b = a^n$ in G für $a \in G, n \in \mathbb{Z}$ einfach, aber die Berechnung der Umkehrfunktion, d.h. des **diskreten Logarithmus** $n = log_a(b)$ in G, ungleich schwieriger ist. Leider werden diese Verfahren in der Praxis viel zu wenig beachtet, obwohl sie gegenüber dem RSA-Verfahren einige wesentliche Vorteile haben:

1. Während das RSA-Verfahren auf dem Problem in einer einzigen und dazu noch sehr einfachen mathematischen Struktur (ganze Zahlen) abhängt, ist das Logarithmusproblem in allen Gruppen formulierbar.

2. Allgemein wird das Logarithmusproblem in geeigneten Gruppen für wesentlich schwieriger erkannt als das Faktorisieren ganzer Zahlen, so daß man die Parameter eines solchen Kryptosystems wesentlich kleiner dimensionieren kann [Beu].

Man beachte, daß die diskrete Exponentiation mit einer Zahl $n \in \mathbb{N}$ unabhängig von der Wahl der Gruppe mit $O(log(n))$ elementaren Gruppenoperationen berechnet werden kann. Die Berechnung der Umkehrfunktion hängt jeweils von der speziellen Gruppe ab. Während die Umkehrung in der additiven Gruppe $\mathbb{Z}/m\mathbb{Z}$ ebenfalls in $O(log(n))$ Gruppenoperationen berechnet werden kann, erweist sich schon das Logarithmusproblem in der multiplikativen Untergruppe eines Primkörpers $\mathbb{F}_p$ als wesentlich schwieriger. Ist α ein primitives Element von $\mathbb{F}_p^*$ und $x \in \mathbb{F}_p^*$ beliebig, so benötigt man für die Berechnung von $y = \alpha^x$ in $\mathbb{F}_p^*$ wiederum nur $O(log(x))$ elementare Gruppenoperationen und für die Berechnung von $x = log_\alpha(y)$ sogar schon $O(exp(c \cdot \sqrt{log\ p\ log(log\ p)}))$ elementare Operationen.

Auf Grund der oben genannten Vorteile sucht man nach Gruppen, für die die DL-Systeme höchstes Sicherheitsniveau erlangen, ohne daß sie an Effizienz und Schnelligkeit verlieren. Diese Gruppen müssen einerseits eine **schnelle Exponentiation** haben und andererseits so beschaffen sein, daß kein zur Zeit existierender Algorithmus das **Logarithmusproblem** in ihr **rechentechnisch** lösen kann. Wir werden dies anschließend genauer präzisieren. Derartige Gruppen nennen wir **kryptographisch geeignete** oder einfach nur **geeignete** Gruppen. Die Schwierigkeit besteht nun darin, geeignete Gruppen zu finden. Wir möchten hierfür Abelsche Varietäten über endlichen Körpern genauer untersuchen.

Definition 1.1 *Eine Abelsche Varietät A ist eine komplette algebraische Gruppenvarietät über einem algebraisch abgeschlossenen Körper K; d.h. A ist eine algebraische Mannigfaltigkeit irreduzibel, separiert, komplett und die Gruppenverknüpfung $+ : A \times A \longrightarrow A$ sowie die Inversenbildung $- : A \longrightarrow A$ sind Morphismen algebraischer Mannigfaltigkeiten und dadurch stets lokal durch Polynome gegeben. Sei k ein vollkommener Teilkörper von K, dann ist A über k definiert, wenn es ein k-Gruppenschema A_0 gibt, so daß $A = A_0 \otimes_k K$.*

Die Gruppenverküpfung auf A ist kommutativ. Ist $k = \mathbb{F}_q$ mit $q = p^n$ ein endlicher Körper, so bestimmt das charakteristische Polynom des Frobeniusendomorphismus von q auf einer Abelschen Varietät A die Anzahl der $\mathbb{F}_q$-rationalen Punkte. Damit ist die Ordnung der Punktegruppe $A(\mathbb{F}_q)$ bekannt. Das Problem besteht allerdings in der konkreten Realisierung der Gruppe und der Auswertung der im Allgemeinen viel zu komplizierten Additionsmorphismen. In einer besseren Situation ist man, wenn die Abelsche Varietät A die **Jacobische Varietät J_C einer Kurve C** ist.

Definition 1.2 *Ist C eine über einem vollkommenen Körper k definierte, nicht-singuläre, irreduzible, projektive Kurve vom Geschlecht $g > 0$ mit k-rationalem Punkt, dann gibt es eine Abelsche Varietät J_C der Dimension g über k und einen kanonischen Morphismus $\Phi : C \longrightarrow J_C$ über k mit der folgenden universellen Eigenschaft:*

Sei $h : C \longrightarrow A$ ein Morphismus von C in eine Abelsche Varietät A, dann gibt es genau einen Homomorphismus $\alpha : J_C \longrightarrow A$ und ein Element $a \in A$, so daß $h(x) = \alpha(\Phi(x)) + a$ für alle $x \in C$. Diese bis auf Isomorphie eindeutig bestimmte Abelsche Varietät J_C heißt Jacobische Varietät von C.

Nach dem Satz von Abel [La I] ist die Gruppe $J_C(k)$ der k-rationalen Punkte der Jacobische Varietät zur Picardgruppe $Pic_k^0(C)$ isomorph. Die Addition auf $J_C(k)$ wird durch die Addition in der Divisorklassengruppe $Pic_k^0(C)$ der Kurve definiert. Durch den Satz von Riemann-Roch entspricht sie dem Auffinden von Funktionen auf der Kurve mit gegebenen Null- und Polstellen. Hierfür entwickelten Ming-Deh Huang und Doug Ierardi in [H-I] effiziente Algorithmen.

Es sei nun C eine über k definierte **hyperelliptische Kurve** mit k-rationalem Punkt, d.h. für $char(k) \neq 2$ gibt es ein affines Modell der Kurve der Form $y^2 = f(x)$, wobei $f(x) \in k[x]$ ein normiertes Polynom vom Grad $2g + 1$ mit paarweise verschiedenen Nullstellen ist. In diesem Fall kann man den k-rationalen Punkten der Jacobischen Varietät J_C eindeutig spezielle quadratische Formen zuordnen. Die Addition in $J_C(k)$ entspricht dann

der Komposition der entsprechenden quadratischen Formen und einer anschließenden Reduktion der zusammengesetzten Form. Diese Tatsache nutzte Cantor 1987 [Cant] bei der Entwicklung seines Additionsalgorithmus für Jacobische Varietäten hyperelliptischer Kurven aus. Andererseits kann man aus den Additionstheoremen der hyperelliptischen Thetafunktionen Additionsformeln für die partielle Addition auf einem affinen Teil $J_C - \Theta$ der Jacobischen Varietät herleiten. Zusammen mit einer vollständigen Überdeckung von J_C durch Karten isomorph zu $J_C - \Theta$ definiert dies eine Addition auf J_C.
Speziell für Geschlecht 2 entwickelte W. Kampkötter 1991 [Ka] in seiner Dissertation auf diese Weise partielle Additionsformeln. Leider sind diese Formeln für Kryptosysteme völlig unbrauchbar, da schon die Formel für nur eine Koordinate mehrere Seiten füllt. Für Geschlecht 1, d.h. für elliptische Kurven, sind kurze Additionsformeln wohl bekannt.
Nun ergibt sich natürlich die Frage, unter welchen Bedingungen diese Gruppen für die DL-Systeme geeignet sind.

1.2 Kryptographisch geeignete Jacobische Varietäten

1) Ein bekannter Algorithmus für das Logarithmusproblem ist der **Baby-Step-Giant-Step-Algorithmus** von D.Shanks 1969. Man kann ihn auf **jede endliche Gruppe anwenden**, und seine Laufzeit verhält sich proportional zur Quadratwurzel der Gruppenordnung. Auf Silver und Pohlig, Hellman [P-H] geht ein wichtiger Algorithmus zurück, der mit Hilfe des Chinesischen Restsatzes das Logarithmusproblem in einer endlichen abelschen Gruppe auf das Logarithmusproblem in zyklischen Untergruppen von Primzahlordnung reduziert. In den jeweiligen Untergruppen kann der Baby-Step-Giant-Step-Algorithmus eingesetzt werden. Das gesamte Verfahren führt nur dann zum Erfolg, wenn das Logarithmusproblem in diesen zyklischen Untergruppen von Primzahlordnung rechentechnisch lösbar ist. Um also in einer Gruppe diesen Angriff zu vermeiden, muß sie so gewählt werden, daß sie mindestens eine zyklische Untergruppe von so großer Primzahlordnung l_q hat, daß in dieser Untergruppe der diskrete Logarithmus rechentechnisch nicht mehr berechnet werden kann. Die Größe von l_q hängt wiederum von der verfügbaren Rechentechnik, d.h. von der Leistungsfähigkeit der Hardware und von der Komplexität der verfügbaren Algorithmen ab. Zur Zeit ist das sicherlich dann der Fall, wenn l_q von der Größenordnung $2^{128} \approx 10^{40}$ ist.

2) Mit dem **Index-Kalkül-Verfahren** stehen für das Logarithmusproblem in der **multiplikativen Gruppe eines endlichen Körpers** Logarithmier-Algorithmen von probabilistisch subexponentieller Laufzeit zur Verfügung.

3) Weitere Angriffsmöglichkeiten sind für die Punktegruppen von **Jacobischen Varietäten J_C über endlichen Körpern** $\mathbb{F}_q$ bekannt. Mit Hilfe der **Tate-Paarung** kann das Logarithmusproblem in der Gruppe $J_C(\mathbb{F}_q)$ der $\mathbb{F}_q$-rationalen Punkte der Jacobischen Varietät auf das Logarithmusproblem in der multiplikativen Gruppe eines endlichen Erweiterungskörpers $\mathbb{F}_{q^k}$ reduziert werden [F-R]. Die Zahl k ist dadurch charakterisiert, daß der Körper $\mathbb{F}_{q^k}$ der kleinste Erweiterungskörper von $\mathbb{F}_q$ ist, in dem die l_q-ten Einheitswurzeln liegen. Das ist genau dann der Fall, wenn k die kleinste Zahl mit $l_q \mid q^k - 1$ ist. Dieser Reduktionsalgorithmus ist polynomial in q^k, so daß das Logarithmusproblem in $J_C(\mathbb{F}_q)$ wegen (2) in probabilistisch subexponentieller Laufzeit gelöst werden kann. Ist allerdings k groß genug, so ist der Erweiterungskörper rechentechnisch nicht mehr beherrschbar und der Angriff des Index-Kalkül-Algorithmus ausgeschlossen. Dieser Angriff ist bedeutsam, da damit alle Jacobische Varietäten von supersingulären hyperelliptischen Kurven ungeeignet sind [F-R]. Hierunter fallen insbesondere die schon oft veröffentlichten supersingulären elliptischen Kurven.
Aus diesen Logarithmier-Algorithmen erhalten wir explizite Bedingungen für geeignete Jacobische Varietäten.

Geeignete Jacobische Varietäten

Definition 1.3 *Eine über einem endlichen Körper $\mathbb{F}_q$ definierte Jacobische Varietät J_C einer Kurve C vom Geschlecht g heißt* ***kryptographisch geeignet*** *oder nur* ***geeignet,*** *wenn die folgenden Bedingungen erfüllt sind.*

1. *Die diskrete Exponentiation kann schnell berechnet werden.*
2. *Die Gruppe $J_C(\mathbb{F}_q)$ der $\mathbb{F}_q$-rationalen Punkte von J_C hat eine zyklische Untergruppe von Primzahlordnung $l_q \approx 10^{40}$.*
3. *Die Ordnung k von l_q mod q ist größer als 1000.*

Bemerkung: Speziell für Chipkartensysteme benötigt man eine einfach zu implementierende Addition. Der Cantorsche Additionsalgorithmus für Jacobische Varietäten hyperelliptischer Kurven beispielsweise basiert auf einer Polynomarithmetik. Deren Implementation ist leider sehr Speicherplatz-intensiv und deshalb für Prozessorchipkarten ungeeignet.

Eine Kurve vom Geschlecht 1 ist eine **elliptische Kurve** E. Die Menge der $\mathbb{F}_q$-rationalen Punkte $E(\mathbb{F}_q)$ ist zur Divisorklassengruppe $Pic^0_{\mathbb{F}_q}(E)$ isomorph. Damit ist E selbst eine Abelsche Varietät. Über das Modell der quadratischen Formen und über die Additionstheoreme der Weierstraß'schen-$\mathcal{P}$ Funktion erhält man dieselben und bekanntlich sehr kurzen Additionsformeln. Ein bekanntes Verfahren nach einer Idee von Atkin, das auf der Theorie der komplexen Multiplikation basiert, ermöglicht die Konstruktion von geeigneten elliptischen Kurven. In meiner Diplomarbeit [Spa I] habe ich dieses Verfahren genauer analysiert, den Algorithmus implementiert und geeignete Kurven konstruiert.

Eine **Kurve C vom Geschlecht 2** ist stets hyperelliptisch. Damit ihre Jacobische Varietät J_C für die DL-Systeme genutzt werden kann, benötigt man noch

- eine schnelle Exponentiation in der Gruppe der rationalen Punkte von J_C und
- eine explizite Realisierung einer geeigneten Jacobischen Varietät.

Es stellt sich natürlich die Frage, welche kryptographischen Vor- und Nachteile Jacobische Varietäten von Kurven vom Geschlecht 2 gegenüber den anderen Gruppen haben. Wir wollen hierfür die Jacobische Varietät einer Kurve vom Geschlecht 2 vom kryptographischen Aspekt her genauer untersuchen.

Kryptographische Analyse

Die Ordnung der Punktegruppe $J_C(\mathbb{F}_q)$ der Jacobischen Varietät J_C einer Kurve C vom Geschlecht g über $\mathbb{F}_q$ wird durch das charakteristische Polynom $f_q(x)$ des Frobeniusendomorphismus π_q auf J_C ausgewertet an $x = 1$ gegeben. Sind $\omega_1, ..., \omega_{2 \cdot g}$ die komplexen Nullstellen von $f_q(x)$, so gilt $|\omega_i| = \sqrt{q}$ ([Mum] IV.21 Application II). Ist $C = E$ eine elliptische Kurve, so gilt für die Gruppenordnung

$$N_q := |E(\mathbb{F}_q)| = \prod_{i=1}^{2}(1 - \omega_i) = 1 + a_1 + q \text{ mit } a_1 := -\sum_{i=1}^{2}\omega_i.$$

Damit ist $|a_1| \leq 2\sqrt{q}$, also $|N_q - 1 - q| \leq 2\sqrt{q}$. Also $|E(\mathbb{F}_q)| \approx q$.
Ist C eine Kurve vom Geschlecht 2, so haben wir

$$N_q := |J_C(\mathbb{F}_q)| = \prod_{i=1}^{4}(1 - \omega_i) = 1 + a_1 + a_2 + a_1 q + q^2$$

$$\text{mit } a_1 := -\sum_{i=1}^{4}\omega_i, a_2 := \sum_{i \neq j}\omega_i\omega_j.$$

Damit ist $|a_1| \leq 4\sqrt{q}$, $|a_2| \leq 6q$, also $|N_q - 1 - q^2| \leq 6q + 4\sqrt{q}(1+q)$. Für den Thetadivisor Θ von J_C gilt:

$$n_q := |\Theta(\mathbb{F}_q)| = |C(\mathbb{F}_q)| = 1 + q + a_1,$$

wobei $|n_q - 1 - q| \leq 4\sqrt{q}$ ([We], [La I], VI,§3). Damit ist $|J_C(\mathbb{F}_q)| \approx q^2$.

Vorteil 1:

Man kann zu einem festen Grundkörper $\mathbb{F}_q$ mit Kurven vom Geschlecht 2 viel größere Gruppen erzeugen. Kryptographisch bedeutet das, daß man die Sicherheit einer großen Gruppe hat, obwohl man nur über einem viel kleineren Körper arbeiten muß. In einer Gruppe mit ungefähr q^2 Punkten muß ja effektiv nur in einem Körper mit q Elementen gerechnet werden. Man benötigt daher weniger Speicherplatz und hat eine schnellere Grundkörperarithmetik zur Verfügung. Dieser Vorteil besteht auch bei anderen Abelschen Varietäten der Dimension 2. Er wirkt sich natürlich um so stärker aus, je größer der Grundkörper ist.

Bemerkung

Für eine kryptographisch geeignete Jacobische Varietät einer Kurve vom Geschlecht 2 haben wir

$$|J_C(\mathbb{F}_q)| = \prod_{i=1}^{4}(1 - \omega_i) = 1 + a_1 + a_2 + a_1 q + q^2 \approx 10^{40}$$

$$\text{und } |\Theta(\mathbb{F}_q)| = |C(\mathbb{F}_q)| = 1 + q + a_1 \approx 10^{20}.$$

Ein beliebiger Punkt auf $J_C(\mathbb{F}_q)$ liegt also nur mit einer Wahrscheinlichkeit von 10^{-20} in dem Thetadivisor. Mumford zeigte [Mum III], daß die Jacobische Varietät J_C mit endlich vielen Karten isomorph zu $J_C - \Theta$ überdeckt werden kann. Liegt die Summe zweier Punkte aus $(J_C - \Theta)(k)$ in $\Theta(k)$, so können diese Punkte mit partiellen Additionsformeln

erst nach einem Kartenwechsel addiert werden. Eine derartige Koordinatentransformation ist allerdings sehr zeitaufwendig und Speicherplatz-intensiv. Weil dieser Fall aber nur mit einer Wahrscheinlichkeit von 10^{-20} auftritt, ist es für ein Kryptosystem völlig ausreichend, wenn in diesem seltenen Fall das Kryptosystem (z.B. der Authentifikationsvorgang) einfach mit einer neuen Zahl wiederholt wird. Damit genügt für die praktische Anwendung in einem DL-System schon eine schnelle partielle Addition.

Im ersten Teil meiner Arbeit habe ich für einen affinen Teil der Jacobischen Varietät sehr kurze Additionsformeln hergeleitet, die eine schnelle Berechnung der disrekten Exponentiation auf J_C ermöglichen. Diese Formeln sind einfach zu implementieren und demnach sogar für Chipkartensysteme geeignet.

Vorteil 2:
Die Gruppenoperation in $J_C(\mathbb{F}_q)$ ist trotz meiner kurzen Additionsformeln immer noch komplizierter als in $\mathbb{F}_q^*$ oder $E(\mathbb{F}_q)$. Bei zukünftig geforderten großen Gruppenordnungen $\approx 10^{80}$ überwiegt der Vorteil des kleineren Grundkörpers, der dann nur $\approx 10^{40}$ Elemente hat, den Nachteil der komplizierteren Arithmetik, so daß man dann sogar ein schnelleres Kryptosystem erhält.

Bemerkung
Für die Punktegruppe einer elliptischen Kurve ist zwar zur Zeit noch kein konkreter Algorithmus für das Logarithmusproblem bekannt, allerdings ist klar, daß das auf der Jacobischen Varietät einer Kurve vom Geschlecht 2 basierende Kryptosystem wegen der komplizierteren Additionsformeln sicherer ist. Außerdem ist über die Struktur einer elliptischen Kurve und über ihre Eigenschaften viel mehr bekannt als über Jacobische Varietäten.

Auf Grund dieser Überlegungen ist es sinnvoll, Jacobische Varietäten von Kurven vom Geschlecht 2 für die Sicherheitsmechanismen zu verwenden, an die höchste Sicherheitanforderungen gestellt werden, die aber nicht zu große Datenmengen benötigen. Das ist sowohl bei dem Schlüsselaustausch als auch bei der digitalen Unterschrift der Fall. Im nächsten Abschnitt werden wir für diese Sicherheitsmechanismen Kryptoprotokolle liefern.

1.3 Kryptoprotokolle

Diffie-Hellman-Schlüsselaustausch-Schema

Angenommen, zwei Personen A und B möchten gemeinsam ein Geheimnis $K_{A,B}$ haben. Es sei $J_C(F_q)$ eine geeignete Jacobische Varietät und P ein Erzeuger der zyklischen Untergruppe der Ordnung l_q. Wir bezeichnen mit $*$ die diskrete Exponentiation auf $J_C(\mathbb{F}_q)$.

A wählt sich einen geheimen Schlüssel in der Form einer Zufallszahl $x_A \in \{1, ..., l_q\}$ und berechnet $Y_A = x_A * P$ in $J_C(\mathbb{F}_q)$. B wählt sich analog einen geheimen Schlüssel $x_B \in \{1, ..., l_q\}$ und berechnet das Element $Y_B = x_B * P$ in $J_C(\mathbb{F}_q)$.
Sowohl Y_A als auch Y_B werden öffentlich bekannt gegeben. Dann berechnet sich das Geheimnis $K_{A,B}$ aus

$$\begin{aligned} K_{A,B} &= (x_A \cdot x_B) * P \text{ in } J_C(\mathbb{F}_q) \\ &= x_B * Y_A \text{ in } J_C(\mathbb{F}_q) \\ &= x_A * Y_B \text{ in } J_C(\mathbb{F}_q). \end{aligned}$$

Somit sind sowohl A als auch B in der Lage, $K_{A,B}$ zu berechnen. Man kennt allerdings zur Zeit kein Verfahren zur Berechnung von $K_{A,B}$ ohne Kenntnis von x_A oder x_B, in welchem man nicht zuerst Y_A oder Y_B logarithmieren muß. Damit muß jeder Angreifer, der das Geheimnis knacken möchte, zunächst den diskreten Logarithmus von Y_B oder Y_A zur Basis P in $J_C(\mathbb{F}_q)$ berechnen.

Signatur-Schema nach ElGamal für Jacobische Varietäten [El]

Wir bezeichnen mit M ein Dokument, das von A unterschrieben werden soll. f_1 und f_2 seien zwei Funktionen, die dem Klartext M sowie einem Punkt $R \in J_C(\mathbb{F}_q)$ ganze Zahlen $f_1(M)$ und $f_2(R)$ zuordnen. Für den Fall der Jacobischen Varietät schlage ich folgende Funktionen vor.

1. $f_1(M)$: Die rechnerinterne Bitmuster-Darstellung von M wird in Blöcke der Größe l_q geteilt, die dann in $\mathbb{Z}/l_q\mathbb{Z}$ addiert werden.

2. $f_2(R)$: Die Koordinaten von R werden hintereinander geschrieben und dann als eine Zahl in $\mathbb{Z}/l_q\mathbb{Z}$ interpretiert.

A berechnet zu einer zufällig gewählten ganzen Zahl $x \in \{1, ..., l_q\}$ den öffentlichen Schlüssel (Public-Key) $Y = x \cdot P$ in $J_C(\mathbb{F}_q)$.
Um jetzt das Dokument M unterschreiben zu können, muß A mit seinem geheimen Schlüssel x (zusammen mit P , J_C und $\mathbb{F}_q$) eine Unterschrift finden, die jeder mit Hilfe des öffentlichen Schlüssels Y verifizieren kann, die aber keiner ohne Kenntnis von x fälschen kann. Das folgende Signatur-Schema erfüllt diese Bedingung:
Die Unterschrift von M besteht aus einem Gruppenelement R und einer ganzen Zahl $s \in \{1, ..., l_q\}$, so daß die Gleichung

$$f_1(M) * P = f_2(R) * Y + s * R \text{ in } J_C(\mathbb{F}_q) \quad (*)$$

erfüllt ist. A berechnet den Punkt R mit Hilfe einer zufällig gewählten ganzen Zahl $k < l_q$ durch

$$R = k * P \text{ in } J_C(\mathbb{F}_q).$$

Dann berechnet A die ganze Zahl s, indem er die Gleichung

$$f_1(M) = x f_2(R) + ks \mod l_q$$

nach s auflöst.

$$\text{D.h. } s = \frac{f_1(M) - x f_2(R)}{k} \mod l_q.$$

Diese Zahlen existieren, da der $ggt(k, l_q) = 1$ ist. Dann gilt :

$$f_1(M) * P = (x f_2(R)) * P + (ks) * P \text{ in } J_C(\mathbb{F}_q)$$

$$\Longrightarrow f_1(M) * P = f_2(R) * Y + s * R \text{ in } J_C(\mathbb{F}_q).$$

Der Empfänger kann die Unterschrift dadurch überprüfen, indem er die Gleichheit von $(*)$ nachrechnet. Ein Betrüger ist ohne die Kenntnis von x nicht in der Lage, den Punkt R und die Zahl s zu berechnen. Möchte jetzt ein Angreifer den geheimen Schlüssel x knacken, um die Unterschrift von A fälschen zu können, so muß er die Gleichung

$$f_1(M) * P = (x f_2(R)) * P + s * R \text{ in } J_C(\mathbb{F}_q)$$

zu gegebenem R, s, D, M und gesuchtem x lösen. Dies ist gerade das Logarithmusproblem in der von D erzeugten Untergruppe von $J_C(\mathbb{F}_q)$.

Kapitel 2

Additionsformeln für die Jacobische Varietät

Im ersten Kapitel haben wir gesehen, daß sich die Jacobische Varietät einer Kurve vom Geschlecht 2 nur dann für ein DL-Chipkartensystem eignet, wenn man für die Punktegruppe eine schnell zu berechnende und einfach zu implementierende Addition findet. Aufbauend auf die Arbeit von D. Cantor [Cant] werden in diesem Kapitel für einen affinen Teil der Jacobischen Varietät geeignete Additionsformeln entwickelt. Die Idee besteht darin, für die Divisorklassen eine geeignete rationale Darstellung herzuleiten und anschließend die Addition in der Divisorklassengruppe in dieser Darstellung rational durch Formeln zu beschreiben. Hierfür müssen für alle einzelnen Fälle seperat Additionsformeln hergeleitet werden. Es zeigt sich, daß die Addition hiermit sogar 2.5-mal schneller ist, als die Addition mit dem Cantorschen Algorithmus.

2.1 Das Diviorklassengruppenmodell

In diesem Abschnitt werden wir die Darstellung der Jacobischen Varietät einer hyperelliptischen Kurve als Divisorklassengruppe wiederholen, wie sie in Mumford in [Mum II] eingeführt wurde.

Es sei C eine über einem algebraisch abgeschlossenen Körper K der Charakteristik $\neq 2$ definierte hyperelliptische Kurve vom Geschlecht g. Jedes nichtsinguläre Modell der Kurve C kann bekanntlich durch zwei affine Karten überdeckt werden. Die erste Karte wird durch eine Gleichung der Form $y^2 = f(x)$, wobei $f(x) \in K[x]$ ein normiertes Polynom vom Grad $2g+1$ mit paarweise verschiedenen Nullstellen $a_1, ..., a_5$ ist, definiert. Damit ist die Diskriminante $disc(f(x))$ ungleich 0. Die zweite Karte liefert die Gleichung $y'^2 = x' \prod_{i=1}^{5}(1 - a_i x')$. Die Transformation $x' = x^{-1}$ und $y' = y \cdot x^{-(g+1)}$ definiert den zugehörigen Isomorphismus zwischen den offenen Mengen $x \neq 0$ auf der ersten und $x' \neq 0$ auf der zweiten Karte.

Die K-rationalen Punkte der Kurve entsprechen den Paaren $P = (x, y) \in K^2$ mit $y^2 = f(x)$ auf der ersten und einem Punkt $P_\infty := (0,0) = (x', y')$ auf der zweiten Karte. Fassen wir x und x' als affine Koordinaten in $\mathbb{P}^1$ auf, so wird durch $(x, y) \longrightarrow x$ auf der ersten und $(x', y') \longrightarrow x'$ auf der zweiten Karte die zweiblättrige Überlagerung $\pi : C \longrightarrow \mathbb{P}^1$ der Kurve definiert. Die Punkte $(a_i, 0)$ für $i = 1, ..., 5$ und P_∞ heißen **Weiertraßpunkte** von C. Ein (K-rationaler) **Divisor** D von C ist eine endliche formale Summe der Form $D = \sum_i m_i P_i$ mit $m_i \in \mathbb{Z}$ und $P_i = (x_i, y_i)$ aus $C(K)$, der Menge der K-rationalen Punkte von C. Der **Grad** von D ist $\sum_i m_i$. Der größte gemeinsame Teiler zweier Divisoren wird durch $ggt(\sum_i n_i P_i, \sum_i m_i P_i) := \sum_i min(m_i, n_i) P_i$ definiert. Die (K-rationalen) Divisoren $Div_K(C)$ von C bilden bezüglich der formalen Addition

$$\sum_i m_i P_i + \sum_i n_i P_i = \sum_i (m_i + n_i) P_i$$

eine additive Gruppe und die Divisoren vom Grad Null bilden eine Untergruppe $Div_K^0(C)$. Die Hauptdivisoren bilden eine Untergruppe H_K von $Div_K^0(C)$ und ihr Quotient ist die **Picardgruppe** $Pic_K^0(C) := Div_K^0(C)/H_K$ von C.

Sei J_C die Jacobische Varietät von C und Φ die zugehörige kanonische Abbildung. Nach dem Satz von Abel [La I] ist die Gruppe der K-rationalen Punkte $J_C(K)$ der Jacobischen Varietät als Gruppe zur Picardgruppe $Pic_K^0(C)$ der Kurve isomorph. Dabei definiert die Abbildung $\sigma_\Phi : \sum n_i P_i \longrightarrow \sum n_i \Phi(P_i)$ den entsprechenden Gruppenisomorphismus.

Mit dem Punkt $P = (x_0, y_0)$ von $C(K)$ ist auch der Punkt $P' = (x_0, -y_0)$ ein Punkt der Kurve. Die beiden Punkte P und P' sind die Nullstellen der Funktion $(x - x_0)$, welche eine doppelte Polstelle an P_∞ hat. Also gilt:

$$P + P' - 2 \cdot P_\infty \equiv 0 \ (mod\ H_K) \text{ bzw. } -P' \equiv P - 2 \cdot P_\infty \ (mod\ H_K).$$

Hieraus folgt, daß jedes Element von $J_C(K)$ in der Form

$$D = \sum_{i=1}^{r} P_i - r \cdot P_\infty \text{ mit } P_i \neq P_j' \text{ für } i \neq j, P_i \neq P_\infty,\ P_i \in C(K)$$

dargestellt werden kann. Diese Divisoren werden **semireduziert** genannt. Ist zusätzlich $r \leq g$, so heißen sie **reduziert.** Aus dem Satz von Riemann-Roch [La I] folgt, daß jedes Element aus $J_C(K)$ eindeutig durch einen derartigen reduzierten Divisor repräsentiert werden kann. Die Menge der Divisorklassen, die als Repräsentanten einen reduzierten Divisor mit $r < g$ haben, heißt Thetadivisor von J_C und wird mit Θ bezeichnet. Definiert man für ein festes r

$$\begin{aligned} Z_r &:= \{\sum_{i=1}^{r} P_i | P_i \neq P_j' \text{ für } i \neq j, P_\infty \neq P_i \in C(K)\}, \\ \text{so ist } (J_C - \Theta)(K) &\cong Z_g \text{ eine g-dimensionale affine Varietät und } J_C(K) \cong \cup_{r=0}^{g} Z_r. \end{aligned}$$

Ist k ein algebraischer Unterkörper von K, dann heißt ein Divisor D rational über k, wenn $D = D^\sigma$ für alle Automorphismen σ von K über k. Die Gruppe der k-rationalen Divisoren vom Grad Null wird mit $Div_k^0(C)$ und die Untergruppe der k-rationalen Hauptdivisoren mit H_k bezeichnet. Sein Bild $J_C(k)$ in $J_C(K)$ ist eine Untergruppe von $J_C(K)$.

Im Folgenden bezeichne k stets einen **vollkommenen algebraischen Unterkörper von** K. Die Jacobische Varietät J_C und die kanonische Abbildung Φ können dann schon über k definiert werden. Die Gruppe der über k definierten Punkte von J_C/k ist zur Picardgruppe $Pic_k^0(C)$ der Kurve isomorph. Die Addition setzt sich also zusammen aus der **Komposition** der Repräsentanten und einer anschließenden **Reduktion** in der Divisorklassengruppe. Für die affine Varietät $(J_C - \Theta)(k)$ wollen wir schnelle Additionsformeln herleiten.

Es seien nun $D_1, D_2, D_1 + D_2 \in (J_C - \Theta)(k)$, dann gibt es Punkte $P_{l_i} \in C(K)$ mit

$$D_l = \sum_{i=1}^{g} P_{l_i} - gP_\infty \text{ mit } P_{l_i} \neq P'_{l_j}, l = 1, 2.$$

Komposition:

$D_1 + D_2 = \sum_{i=1}^{g}(P_{1_i} + P_{2_i}) - 2 \cdot g \cdot P_\infty$.

Reduktion:

1. Reduktion zum semireduzierten Divisor.
   Für $P_{1_i} = P'_{2_j}$ haben wir $P_{1_i} + P_{2_j} - 2P_\infty \equiv 0 \bmod H_K$.
   Dann ist $D_1 + D_2 = \sum_{i=1}^{r} P_i - rP_\infty$ mit $P_i \neq P'_j$ und $r \leq 2g$.

2. Reduktion zum reduzierten Divisor in der Divisorklassengruppe.
   Dann ist $D_1 + D_2 \equiv \sum_{i=1}^{g} Q_i - g \cdot P_\infty \bmod H_K$.

Das Problem der Addition in dieser Darstellung besteht darin, daß nicht die Koordinaten (x_i, y_i) der Punkte P_i selber, sondern erst der Divisor, d.h. das symmetrische Produkt der Koordinaten, über k definiert ist. Wir brauchen also eine

1. **k-rationale Darstellung der Repräsentanten**

2. **k-rationale Beschreibung der Komposition und Reduktion.**

2.2 Die rationale Darstellung

Jeder semireduzierte Divisor $D = \sum_{i=1}^{r} P_i - r \cdot P_\infty$ kann eindeutig durch ein Polynomenpaar $(u(x), v(x))$ mit $D = ggt(div(u(x)), div(v(x) - y))$ repräsentiert werden. Dabei sind die Polynome $u(x)$ und $v(x)$ eindeutig durch die Punkte P_i definiert. Für $P_i = (x_i, y_i)$ ist

$$(i) \quad u(x) = u^D(x) := \prod_{i=1}^{r}(x - x_i) = x^r + \sum_{i=1}^{r} u_i x^{r-i} \text{ und}$$

$$(ii) \quad v(x) = v^D(x) = \sum_{i=1}^{r} v_i x^{r-i}$$

das eindeutig bestimmte Polynom vom Grad kleiner r
mit $v(x_i) = y_i$ mit Vielfachheit.

Das heißt, erscheint der Punkt P_i $k-mal$ als Summand von D,
so ist $(\frac{d}{dx})^j(v(x)-\sqrt{f(x)})|_{x=x_i}=0$ für $0\leq j\leq k-1$.

Nach Konstruktion ist das Polynom $v(x)^2-f(x)$ ein Vielfaches von $u(x)$. Wir definieren ein weiteres Polynom $w^D(x)$ durch den Quotienten

$$(iii)\quad w(x)=w^D(x):=\frac{v(x)^2-f(x)}{u(x)}.$$

Wenn $r\leq g$, d.h. $deg(v(x)^2)\leq 2g-2<deg(f(x))$, so ist mit $u(x)$ auch $w(x)$ normiert. Ist D durch die Polynome $u(x),v(x)$ definiert, so schreiben wir $D=div(u(x),v(x))$. D ist nach Definition genau dann reduziert, wenn $deg(u(x))\leq g$.

Hat man umgekehrt drei Polynome $u(x),v(x),w(x)$ mit $u(x)\,w(x)=v(x)^2-f(x)$ mit $u(x)$ normiert $deg(u(x))=r\leq g, deg(v(x))\leq r-1$, dann kann man diesen Polynomen einen Divisor D der Form

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

zuordnen. Dabei sind $x_1,\cdots,x_r$ die Nullstellen von $u(x)$ inklusive Vielfachheit und $y_i=\sqrt{f(x_i)}$. Diese Abbildung liefert einen Isomorphismus zwischen den einzelnen Mengen

$$\{\sum_{i=1}^{r}P_i\mid P_i\neq P_\infty, P_i\neq P_j'\text{ für }i\neq j\}\ \cong\ \{(u(x),v(x),w(x))|\ u(x)w(x)=v(x)^2-f(x),$$
$$u(x)\text{ normiert vom Grad r,}$$
$$deg(v(x))<r,\ deg(w(x))=2g+1-r\}.$$

Weil die Polynome $u(x)$ und $v(x)$ das Polynom $w(x)$ eindeutig festlegen, kann unter Verwendung des euklidischen Algorithmus folgendes geschrieben werden:

$$f(x)-v(x)^2=u(x)\cdot(x^{2g+1-r}+B_0(u_i,v_j)x^{2g-r}+\cdots)+Rest,$$

wobei $Rest=F_1(u_i,v_j)x^{r-1}+\cdots+F_r(u_i,v_j)$ ein Polynom vom Grad $r-1$ ist und die Koeffizienten $F_l(u_i,v_j)$ und $B_l(u_i,v_j)$ Polynome in den Koeffizienten u_i,v_j von $u(x)$ und $v(x)$ sind. Wir bezeichnen mit $V(F_1,\cdots,F_r)$ die durch die Restpolynome definierte r-dimensionale affine Varietät in k^{2r}. Die Koeffizienten $(u_1,\cdots,u_r,v_1\cdots,v_r)$ der Polynome

$u(x)$ und $v(x)$ sind die Punkte der affinen Varietät. Wir erhalten damit die folgende Mengenisomorphie, die die zweite Menge zu einer affinen Varietät macht.

$$\begin{aligned} V(F_1,\cdots,F_r) \cong \{(u(x),v(x),w(x))|\ & u(x)\cdot w(x) = v(x)^2 - f(x), \\ & u(x) \text{ normiert vom Grad r}, \\ & deg(v(x)) < r,\ deg(w(x)) = 2g+1-r\} \cong Z_r. \end{aligned}$$

Andererseits können wir jedem semireduzierten Divisor $D = (u(x), v(x), w(x))$ eindeutig eine quadratische Form

$$Q^D(X,Y) := u(x)X^2 + 2v(x)XY + w(x)Y^2 \quad \text{mit Diskrimante } f(x)$$

zuordnen. Die Reduktion des Divisors erhält man so über die Reduktion der zugehörigen qudratischen Form. (vgl. [Cant] S.97).
Da D rational über k ist, wenn die Polynome $u(x)$ und $v(x)$ Koeffizienten in k haben, liefern die Koeffizienten $(u_1,\cdots,u_r,v_1\cdots,v_r)$ der Polynome $u(x), v(x)$ eine k-rationale Darstellung der rationalen Punkte von $J_C(k)$. Zwei Elemente $D_1 = div(u_1(x), v_1(x))$ und $D_2 = div(u_2(x), v_2(x))$ werden addiert, indem man die Polynome des zusammengesetzten und semireduzierten Divisors $D_1 + D_2$ berechnet und anschließend die zugehörige quadratische Form reduziert.

Komposition:

Dem zusammengesetzten schon semireduzierten Divisor $D_1 + D_2 = \sum_{i=1}^{r} P_i - r \cdot P_\infty$ ordnen wir die folgende quadratische Form $Q^*(X,Y)$ zu.

$$\begin{aligned} Q^*(X,Y) &:= (u^*(x), v^*(x), \frac{v^*(x)^2 - f(x)}{u(x)}) \text{ mit} \\ u^*(x) &:= \prod_{i=1}^{r}(x - x_i) \text{ und} \\ v^*(x) & \quad \text{ist das eindeutig bestimmte Polynom mit} \\ & \quad v^*(x_i) = y_i \text{ mit Vielfachheit.} \end{aligned}$$

Reduktion:

Jetzt reduzieren wir $Q^*(X,Y)$ mit dem bekannten Gauß-Reduktionsalgorithmus wie folgt (vgl.Cant S.99):

> Wir ersetzen $u^*(x)$ durch $u_{neu}(x) = (v(x)^{*2} - f(x))/u^*(x)$ und $v^*(x)$ durch $v_{neu}(x) \equiv -v^*(x) \pmod{u_{neu}(x)}$. Dann ist $deg(v_{neu}(x)) < deg(u_{neu}(x))$.
> Wenn $deg(u_{neu}(x)) = m$ und $deg(v_{neu}(x)) = n$ mit $m > n$, dann haben wir $deg(u_{neu}(x)) = max\{2g+1, 2\} - m$. Wenn $m > g+1$, dann ist $deg(u_{neu}(x)) \leq 2(m-1) - m = m - 2$ und wenn $m = g+1$, dann ist $deg(u_{neu}(x)) \leq g$.
>
> Diesen Reduktionsschritt wiederholen wir so lange, bis $deg(u_{neu}(x))$ kleiner gleich g ist.
>
> Der reduzierten quadratischen Form $(u_{neu}(x), v_{neu}(x), w_{neu}(x))$ Form kann wieder ein reduzierter Divisor $D_{neu} = \sum_{i=1}^{r} Q_i - rP_\infty$ zugeordnet werden. Dabei ist $Q_i = (x_i, y_i)$, wobei x_i die Nullstellen von $u_{neu}(x)$ sind und $y_i = \sqrt{f(x_i)}$.

Wir suchen als Erstes für die Koeffizienten von $v^*(x)$ k-rationale Formeln. Anschließend müssen wir noch für die Reduktion k-rationale Formeln herleiten.

2.3 Additionsformeln für Geschlecht 2

Sei $C : y^2 = x^5 + f_1x^4 + f_2x^3 + f_3x^2 + f_4x + f_5 =: f(x)$ mit $f_i \in k, disc(f(x)) \neq 0$ eine projektive glatte Kurve vom Geschlecht 2. Wir haben

$$\begin{aligned}(J_C - \Theta)(k) &\cong \{P_1 + P_2 \mid P_1 \neq P_2',\ P_i \neq P_\infty\} \\ &\quad \text{mit } P_i = (x_i, y_i), \text{ wobei } f(x_i) = y_i^2 \\ &\quad \text{und } x_1 + x_2, x_1x_2, y_1 + y_2, y_1y_2 \in k. \\ \Theta(k) &\cong \{P \mid P \neq P_\infty\} \cup \{P_\infty\} \text{ mit } P \in C(k).\end{aligned}$$

Ein Element $D \in (J_C - \Theta)(k)$ kann in verschiedenen Modellen wie folgt dargestellt werden:
Als reduzierter Divisor:

$$D = \sum_{i=1}^{2} P_i - 2 \cdot P_\infty \quad \text{mit } x_1 + x_2, x_1x_2, y_1 + y_2, y_1y_2 \in k.$$

Als Polynomen-Paar:

$$D = div(u(x), v(x)) \qquad \text{mit } u(x), v(x) \in k[x],\ u(x) = \prod_{i=1}^{2}(x - x_i), \ldots$$

Als reduzierte quadratische Form:

$$D = Q(X,Y) = u(x)X^2 + 2 \cdot v(x)XY + w(x)Y^2 \text{ mit } Disk(Q(X,Y)) = f(x).$$

Als Punkt auf der affinen Varietät:

$$D = (u_1, u_2, v_1, v_2) \in V(F_1(u_1, u_2, v_1, v_2), F_2(u_1, u_2, v_1, v_2)) \subseteq k^4.$$

Die definierenden Polynome $F_1(u_1, u_2, v_1, v_2)$ und $F_2(u_1, u_2, v_1, v_2)$ berechnen wir wie folgt (vgl. S.17) :

$$\begin{aligned}((v_1x + v_2)^2 - f(x)) : (x^2 + u_1x + u_2) &= w(x) \\ &= x^3 + x^2(f_1 - u_1) + x(f_2 - f_1u_1 + u_1^2 - u_2) \\ &\quad + f_3 - f_2u_1 + f_1u_1^2 - u_1^3 - f_1u_2 + 2u_1u_2 - v_1^2 \\ \text{mit } Rest &= F_1(u_1, u_2, v_1, v_2)x + F_2(u_1, u_2, v_1, v_2),\end{aligned}$$

$$\begin{aligned}\text{wobei } F_1(u_1, u_2, v_1, v_2) &:= -f_4 + f_3u_1 - f_2(u_1^2 - u_2) + f_1u_1(u_1^2 - 2u_2) - \\ &\quad (u_1^2 - u_2)^2 + u_1^2u_2 - u_1v_1^2 + 2v_1v_2, \\ F_2(u_1, u_2, v_1, v_2) &:= -f_5 + f_3u_2 - f_2u_1u_2 + f_1u_1(u_1^2 - u_2) - \\ &\quad u_1u_2(u_1^2 - 2u_2) - u_2v_1^2 + v_2^2.\end{aligned}$$

Die partielle Addition auf $(J_C - \Theta)(k)$:

$$\begin{aligned}\text{Es sei } D_1, D_2, D_1 + D_2 &\in (J_C - \Theta)(k) \text{ mit} \\ D_1 &= P_1 + P_2 - 2 \cdot P_\infty \leftrightarrow (u_1, u_2, v_1, v_2) \leftrightarrow Q_1(X,Y), \\ D_2 &= P_3 + P_4 - 2 \cdot P_\infty \leftrightarrow (u_3, u_4, v_3, v_4) \leftrightarrow Q_2(X,Y).\end{aligned}$$

Falls $P_i = P_j'$ ist, kann man direkt den reduzierten Divisor angeben. Wir setzen daher $P_i \neq P_j'$ voraus. Damit ist der zusammengesetzte Divisor $D_1 + D_2$ schon semireduziert und

$$D_1 + D_2 = \sum_{i=1}^{4} P_i - 4 \cdot P_\infty \leftrightarrow Q^*(X,Y) = (u^*(x), v^*(x), w^*(x)).$$

Herleitung einer Kompositionsformel:

Während das Polynom $u^*(x)$ durch

$$\begin{aligned} u^*(x) &= \prod_{i=1}^{4}(x - x_i) = (x^2 + u_1x + u_2)(x^2 + u_3x + u_4) \\ &=: x^4 + \sum_{i=1}^{4} u_i^* x^{4-i} \in k[x] \end{aligned}$$

universell gegeben ist, hängt das Polynom $v^*(x)$ davon ab, wie oft ein Punkt P_i in dem zusammengesetzten Divisor $D_1 + D_2$ auftritt.

Berechnung von $v^*(x)$

Es ergibt sich folgende Aufgabe:

1. In sämtlichen möglichen Fällen muß das Polynom

$$v^*(x) = \sum_{l=1}^{4} v_l^* \; x^{4-l}$$

bestimmt werden. Wir berechnen die Koeffizienten von $v^*(x)$, indem wir das durch die jeweiligen Bedingungen

$$v^*(x_i) = y_i \text{ mit Vielfachheit}$$

enstandende 4-dimensionale Gleichungssystem nach den Koeffizienten v_l^* für $l = 1, ..., 4$ auflösen. Diese Koeffizienten sind Polynome $v_l^*(x_i, y_j)$ der Koordinaten der Punkte P_i und in x_i und in y_j symmetrisch.

2. Anschließend müssen diese Koeffizienten $v_l^*(x_i, y_j)$ als Polynome $v_l^*(u_i, v_j)$ der k-rationalen Koeffizienten u_i, v_j dargestellt werden:
Da die Polynome $v_l^*(x_i, y_j)$ in x_i und y_j symmetrisch sind, kann man sie in den elementarsymmetrischen Funktionen der x_i und y_j darstellen. Der Beweis des Hauptsatzes von symmetrischen Funktionen liefert hierfür einen Algorithmus. Die elementarsymmetrischen Funktionen sind Polynome in den Ausdrücken $x_1 + x_2, x_1x_2, y_1 + y_2, y_1y_2, x_3 + x_4, x_3x_4, y_3 + y_4, y_3y_4$, welche sich wiederum durch die Koordinaten u_i, v_j ausdrücken lassen. Denn

für $P_1 \neq P_2$ haben wir $\quad x_1x_2 = u_2, \quad x_1 + x_2 = -u_1$

$$\begin{aligned}
\text{und da } y_1 &= v_1x_1 + v_2 \text{ und } y_2 = v_1x_2 + v_2 \\
\text{auch } y_1y_2 &= v_1^2u_2 - v_1v_2u_1 + v_2^2,\ y_1 + y_2 = 2v_2 - v_1u_1. \\
\text{Für } P_1 = P_2 \text{ haben wir } \quad x_1^2 &= u_2, 2x_1 = -u_1 \\
\text{und da } y_1 &= v_1x_1 + v_2 \text{ und } v_1 = y_1' = \sqrt{f(x_1)}' = \frac{f'(x_1)}{2 \cdot y_1} \\
\text{auch } y_1^2 &= (v_2 - \frac{v_1u_1}{2})^2, 2y_1 = 2(v_2 - \frac{v_1u_1}{2}).
\end{aligned}$$

Analog für P_3 und P_4.

Wir müssen die folgenden Fälle unterscheiden:

FALL A : $D_1 \neq D_2$

Fall 1: p1234	$P_i \neq P_j$ für $i \neq j,\ i,j \in \{1,\cdots,4\}$
Fall 2: p1134	$P_1 = P_2$ sonst $P_i \neq P_j$ für $i \neq j,\ i,j \in \{1,3,4\}$
Fall 3: p1133	$P_1 = P_2$ und $P_3 = P_4$ und $P_1 \neq P_3$
Fall 4: p1114	$P_1 = P_2 = P_3$ und $P_4 \neq P_1$
Fall 5: p1214	$P_1 = P_3$ sonst $P_i \neq P_j$ für $i \neq j,\ i,j \in \{1,2,4\}$

FALL B : $D_1 = D_2$

Fall 6: p1212	$P_1 = P_3$ und $P_2 = P_4$ und $P_1 \neq P_2$
Fall 7: p1111	$P_1 = P_2 = P_3 = P_4$

Es zeigt sich, daß die ersten drei Fälle dieselben Formeln liefern. In der schnellen diskreten Exponentiation werden am häufigsten die Fälle p1212 und p1234 benötigt. Die anderen Fälle treten hingegen eher selten auf. Nach geschickter Zusammenfassung sind diese Formeln sehr kurz, so daß wir eine sehr schnelle Exponentiation erhalten.

Fall A :

$D_1 := (u_1, u_2, v_1, v_2) \neq D_2 := (u_3, u_4, v_3, v_4)$ und $D_1, D_2, D_1 + D_2 \notin \Theta$

Fall 1 (p1234) = Fall 2 (p1134) = Fall 3 (p1133):

1) Es ist:

$$\begin{aligned} u_1 &= -x_1 - x_2, \quad u_2 = x_1 x_2, \quad v_1 = \frac{y_1 - y_2}{x_1 - x_2}, \quad v_2 = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}, \\ u_3 &= -x_3 - x_4, \quad u_4 = x_3 x_4, \quad v_3 = \frac{y_3 - y_4}{x_3 - x_4}, \quad v_4 = \frac{x_3 y_4 - x_4 y_3}{x_3 - x_4}. \end{aligned}$$

2) Aus dem Gleichungssystem $v^*(x_i) = y_i$ für $i = 1, \cdots, 4$ erhält man

$$v^*(x) := \sum_{i=1}^{r} y_i \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}.$$

3) $v^*(x)$ wurde in den elementarsymmetrischen Funktionen und dann in den Koordinaten u_i, v_j dargestellt. Anschließend wurde die Formel durch Einführung einiger Hilfsvariabeln vereinfacht. Wir definieren

$$\begin{aligned} v_{13} &:= v_1 - v_3, \quad v_{24} := v_2 - v_4, \quad u_{13} := u_1 - u_3, \quad u_{24} := u_2 - u_4, \\ u_{1.4} &:= u_1 u_4, \quad u_{2.3} := u_2 u_3, \quad u_{1.3} := u_1 u_3 \end{aligned}$$

4) und erhalten die folgenden Formeln für die Koeffizienten $v_1^*, ..., v_4^*$ von $v^*(x)$.
Setzen wir $n := u_{24}^2 - u_{13}(u_{2.3} - u_{1.4})$, so ist

$$\begin{aligned} v_4^* &= (u_4(-u_2 u_{13} v_{13} + v_2(u_1 u_{13} - u_{24})) + u_2 v_4(u_{24} - u_3 u_{13}))/n \\ v_3^* &= ((-u_{2.3} u_{13} - u_4 u_{24}) v_1 + (u_{1.3} u_{13} - u_{2.3} + u_{1.4}) v_{24} + \\ &\quad (u_2 u_{24} + u_{1.4} u_{13}) v_3)/n \\ v_2^* &= (v_{13}(u_3 u_4 - u_1 u_2) + v_{24}(u_{13}(u_1 + u_3) - u_{24}))/n \\ v_1^* &= (-v_{13} u_{24} + v_{24} u_{13})/n. \end{aligned}$$

Fall 4 (p1114):

1) Es ist $P_1 = P_2 = P_3 \neq P_4$. Damit sind alle P_i schon über k definiert und es gilt:

$$\begin{aligned} u_1 &= -2x_1,\ u_2 = x_1^2,\ v_1 = \frac{f'(x_1)}{2y_1},\ v_2 = y_1 - v_1x_1, \\ u_3 &= -x_1 - x_4,\ u_4 = x_1x_4,\ v_3 = \frac{y_1 - y_4}{x_1 - x_4},\ v_4 = \frac{x_1y_4 - x_4y_1}{x_1 - x_4}, \\ \text{also}\quad x_1 &= -\frac{u_1}{2},\ y_1 = v_1x_1 + v_2 \in k, \\ x_4 &= -x_1 - u_3,\ y_4 = v_3x_4 + v_4 \in k. \end{aligned}$$

2) Gleichungssystem:

$$\begin{aligned} v^*(x_i) &= y_i \text{ für } i = 1,4 \\ v^{*'}(x_1) &= y_1' = \frac{f'(x_1)}{2 \cdot y_1} = v_1 \\ v^{*''}(x_1) &= y_1'' = (\frac{f'(x_1)}{2 \cdot y_1})' = \frac{-2v_1^2 + f''(x_1)}{2y_1}. \end{aligned}$$

3) Die Formel wurde vereinfacht durch Einführung von zwei Hilfsvariabeln:

$$\text{Setzen wir } y_{14} := y_1 - y_4,\ h_1 := 2v_1^2 - f''(x_1), n := -4u_{13}^3y_1,$$

4) so erhalten wir die folgenden Formeln für die Koeffizienten

$$\begin{aligned} v_4^* &= ((12u_4u_{13} - 4\ x_4^3)\ y_1^2 - 4v_1y_1(2x_1^3x_4 - 3u_4^2 + x_1x_4^3) - \\ &\quad x_1(4u_2y_4y_1 + u_4u_{13}^2h_1))/n \\ v_3^* &= -(h_1(u_2^2 - 3u_4^2 + 2x_1x_4^3) + 8v_1x_1^3y_1 + 4y_1(v_1x_4^2(-3\ x_1 + x_4) - 3\ u_2\ y_{14}))/n \\ v_2^* &= (h_1(2x_1^3 - 3u_2x_4 + x_4^3) + 12y_1(v_1(u_2 - u_4) - x_1y_{14}))/n \\ v_1^* &= (-h_1u_{13}^2 + 4y_1(v_1u_{13} + y_{14}))/n. \end{aligned}$$

Fall 5 (p1214):

1) Es ist $P_1 = P_3, P_i \neq P_j$ für $i \neq j$ und $i,j, \in \{1,2,4\}$. Damit sind alle P_i schon über k definiert und es gilt

$$\begin{aligned}
\text{da } x_1 &= x_3 \text{ ist} \quad x_1 = \frac{u_4 - u_2}{u_1 - u_3} = \frac{v_4 - v_2}{v_1 - v_3} \in k, \quad (i) \\
u_1 &= -x_1 - x_2, \quad u_2 = x_1 x_2, \quad v_1 = \frac{y_1 - y_2}{x_1 - x_2}, \quad v_2 = y_1 - v_1 x_1, \\
u_3 &= -x_1 - x_4, \quad u_4 = x_1 x_4, \quad v_3 = \frac{y_1 - y_4}{x_1 - x_4}, \quad v_4 = y_1 - v_3 x_1. \\
\text{Damit ist} \quad x_2 &= -x_1 - u_1, \quad x_4 = -x_1 - u_3 \in k, \\
y_1 &= v_1 x_1 + v_2, \quad y_2 = v_1 x_2 + v_2, \quad y_4 = v_3 x_4 + v_4 \in k. \quad (ii)
\end{aligned}$$

2) Gleichungssystem:

$$\begin{aligned}
v^*(x_i) &= y_i \text{ für } i = 1,2,4 \\
v^{*'}(x_1) &= y_1' = \frac{f'(x_1)}{2y_1}
\end{aligned}$$

Da die Punkte P_i k-rational sind, kann man die aus diesem Gleichungssystem erhaltenen Formeln zusammen mit den Transformationen $(i),(ii)$ als Additionsformel verwenden.

Fall B: (Verdoppelung)

$D_1 := (u_1, u_2, v_1, v_2) = D_2 := (u_3, u_4, v_3, v_4)$ und $D_1, D_2, D_1 + D_2 \notin \Theta$

Fall 6 (p1212):

1) Es ist $P_1 = P_3, P_2 = P_4, P_1 \neq P_4$, also

$$\begin{aligned}
u_1 &= -x_1 - x_2 = u_3, \quad u_2 = x_1 x_2 = u_4, \\
v_1 &= \frac{y_1 - y_2}{x_1 - x_2} = v_3, \quad v_2 = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2} = v_4.
\end{aligned}$$

2) Gleichungssystem:

$$v^*(x_i) = y_i \text{ für } i = 1,2$$

$$v^{*'}(x_i) = (y_i)' = \frac{f'(x_i)}{2 \cdot y_i} \text{ für } i = 1, 2$$

3) Die Formeln wurden vereinfacht durch Einführung einiger Hilfsvariabeln:

$$\begin{aligned}
u_{12} &:= u_1^2, \quad v_{22} := v_2^2, \quad uu_: = u_1 u_2, \quad uu_2 := 2u_2, \\
w_1 &:= 2u_1, \quad w_4 := u_2^2, \quad w_2 := uu_2 + u_{12}, \\
u_{11} &:= 2uu, \quad n_{11} := v_{12}u_2 - v_1 v_2 u_1 + v_{22}, \quad t_{11} := 2v_2 - v_1 u_1, \\
h_{31} &:= -v_1/(2n_{11}), \quad h_{32} := t_{11}/(4n_{11}) + h_{31}u_1/2, \\
h_{11} &:= -f_2 + f_1 w_1 - 3u_{12} + uu_2.
\end{aligned}$$

4) Wir erhalten die folgenden Formeln für die Koeffizienten

$$\begin{aligned}
v_4^* &= v_2 + h_{31}w_4 h_{11} + h_{32}(f_5 - w_4(f_1 - w_1) - v_{22}), \\
v_3^* &= v_1 + h_{32}(f_4 - 2v_1 v_2 - w_4 - u_{11}(f_1 - w_1)) + \\
&\quad h_{31}(f_5 - f_2 u_{11} + f_1(2u_{12}uu_2 - w_4) - 3w_1(u_{12}u_2 - w_4) - v_{22}), \\
v_2^* &= h_{32}(f_3 - f_1 w_2 + w_1 u_{12} + u_{11} - v_{12}) + \\
&\quad h_{31}(f_4 - 2v_1 v_2 - f_2 w_2 + f_1 w_1(u_{12} + u_2) - 3(u_{12}^2 - w_4)), \\
v_1^* &= -h_{32}h_{11} + h_{31}(f_3 - w_1(f_2 + 2u_{12}) + f_1(3u_{12} - uu2) + 3u_{11} - v_{12})),
\end{aligned}$$

Fall 7 (p1111):

1) Weil $P_1 = P_2 = P_3 = P_4$, ist P_1 schon k-rational und wir haben

$$\begin{aligned}
u_1 &= -2x_1 = u_3, \quad u_2 = x_1^2 = u_4, \\
v_1 &= \frac{f'(x_1)}{2y_1} = v_3, \quad v_2 = y_1 - v_1 x_1 = v_4. \\
\text{Damit ist} \quad x_1 &= -\frac{u_1}{2}, \quad y_1 = v_1 x_1 + v_2 \in k. \quad (*)
\end{aligned}$$

2) Gleichungssystem:

$$\begin{aligned}
v^*(x_1) &= y_1 \\
v^{*'}(x_1) &= y_1' = \frac{f'(x_1)}{2 \cdot y_1} = v_1
\end{aligned}$$

$$
\begin{aligned}
v^{*''}(x_1) &= y_1'' = \left(\frac{f'(x_1)}{2 \cdot y_1}\right)' = \frac{-2v_1^2 + f''(x_1)}{2y_1} \\
v^{*'''}(x_1) &= y_1''' = \left(\frac{f'(x_1)}{2 \cdot y_1}\right)'' = \frac{6v_1^3 - 3v_1 f''(x_1) + y_1 f'''(x_1)}{2y_1^2}
\end{aligned}
$$

Da die Punkte P_i schon k-rational sind, kann man die aus diesem Gleichungssystem erhaltenen Formeln zusammen mit der Transformation $(*)$ als Additionsformel verwenden.

3) Wir schreiben die Formeln vereinfacht auf. Setzen wir

$$h_2 = u_1^2 + 6u_2 \text{ und } n := (u_1 v_1 - 2v_2)^2,$$

4) so erhalten wir die folgenden Formeln für die Koeffizienten:

$$
\begin{aligned}
v_4^* &= (u_2 v_1(-2f_3 u_1 + f_2 h_2 + 20u_2^2) + 2(u_1 u_2 v_1^3 + (f_3 - f_2 u_1)u_2 v_2) + \\
&\quad (u_1^2 - 2u_2)v_1^2 v_2 - 4v_2^2(u_1 v_1 - v_2))/n, \\
v_3^* &= (v_1(-f_3 h_2 + 2(2u_2(3f_2 u_1 + 5u_1 u_2) - 3u_1 v_1 v_2 + 2v_2^2)) \\
&\quad +2((u_1^2 + 3u_2)v_1^3 + (f_3 u_1 - 3f_2 u_2 + 10u_2^2)v_2))/n \\
v_2^* &= 2(v_1(2u_1(-f_3 + v_1^2) + u_2(9f_2 - 5u_1^2) + 30u_2^2) + v_2(f_3 + 10u_1 u_2 - v_1^2))/n, \\
v_1^* &= 2(v_1(-f_3 + f_2 u_1 + v_1^2) + (f_2 + 10u_2)v_2)/n.
\end{aligned}
$$

Herleitung einer Reduktionsformel:

Die Reduktion des zusammengestzten Divisors $(P_1 + P_2 + P_3 + P_4 - 4P_\infty)$ entspricht der Reduktion der zugehörigen im letzten Abschnitt berechneten quadratischen Form

$$Q^*(X,Y) = u^*(x)X^2 + 2v^*(x)XY + w^*(x)Y^2 \text{ mit } w^*(x) = \frac{f(x) - v^*(x)^2}{u^*(x)}.$$

Für D_1, D_2 und $D_1 + D_2 \in J_C - \Theta$ haben wir $deg(u^*(x)) = 4$ und $deg(v^*(x)) = 3$, also $deg(w^*(x)) = deg(v^*(x)^2 - f(x)) - deg(u^*(x)) = 2$. Damit ist $deg(w^*(x)) < deg(v^*(x)) < deg(u^*(x))$.
Die Gauß-Reduktion erfolgt nun in zwei Schritten:

1. Ersetze die Form $(u^*(x), v^*(x), w^*(x))$
   durch die Form $(w^*(x), -v^*(x), u^*(x)) =: (u_{neu}(x), -v^*(x), w_{neu}(x))$.

   Jetzt ist zwar $deg(u_{neu}(x)) < deg(w_{neu}(x))$,
   aber noch $deg(u_{neu}(x)) < deg(v^*(x))$.

2. Setze $v_{neu}(x) := -v^*(x) \bmod u_{neu}(x)$.
   Jetzt ist die Form $(u_{neu}(x), v_{neu}(x), w_{neu}(x))$ reduziert.

Definieren wir $u_{neu}(x) =: x^2 + u_5 x + u_6$ und $v_{neu}(x) =: v_5 x + v_6$, so erhalten wir folgende Formeln für die Koeffizienten u_5, u_6, v_5, v_6:

$$\begin{aligned}
\text{Es ist } u_{neu}(x) &= w^*(x) = \frac{v^*(x)^2 - f(x)}{u^*(x)} \text{ und normiert, also} \\
u_5 &= \frac{(2v_2^*v_1^* - v_1^{*^2}(u_2 + u_1) - 1)}{v_1^{*^2}}, \\
u_6 &= \frac{(v_2^{*^2} + 2v_3^*v_1^* - f_1 + (u_1 + u_2)(1 - 2v_2^*v_1^* + v_1^*(u_1 + u_2)) - v_1^{*^2}u_2u_4)}{v_1^{*^2}}, \\
\text{oder } u_6 &= \frac{v_4^{*^2} - f_5}{v_1^{*^2}u_2u_4} \quad \text{falls } u_2 \neq 0 \text{ und } u_4 \neq 0.
\end{aligned}$$

$$\begin{aligned}
\text{Es ist } v_{neu}(x) &= -v^*(x) \bmod u_{neu}(x) \\
v_5 &= -v_3^* + v_2^*u_5 - v_1^*u_5^2 + v_1^*u_6, \\
v_6 &= -v_4^* + v_2^*u_6 - v_1^*u_5u_6.
\end{aligned}$$

Damit haben wir die partielle Addition durch kurze Formeln beschrieben. Es ist

$$(u_1, u_2, v_1, v_2) + (u_3, u_4, v_3, v_4) = (u_5, v_5, u_6, v_6) \in (J_C - \Theta)(k).$$

Beispiel:

Ich habe diese Addition und Cantors Algorithmus in dem System 'PARI' implementiert und deren Laufzeiten verglichen. Ein Beispiel dazu wird hier angegeben.

$$\begin{aligned}
\text{Für } p &= 15394628755070098943 \text{ und eine Kurve} \\
C/\mathbb{F}_p &: Y^2 = X^5 - 140X^3 + 240X^2 + 3810X - 6928
\end{aligned}$$

$$\begin{aligned}
\text{ist } (J(C) - \Theta)(\mathbb{F}_p) &= V(F_1(u_1,u_2,v_1,v_2), F_2(u_1,u_2,v_1,v_2)), \text{ wobei} \\
F_1(u_1,u_2,v_1,v_2) &:= -3810 + 240u_1 + 140(u_1^2 - u_2) - (u_1^2 - u_2)^2 \\
&\quad + u_1^2u_2 - u_1v_1^2 + 2v_1v_2 \\
F_2(u_1,u_2,v_1,v_2) &:= 6928 + 240u_2 + 140u_1u_2 - u_1u_2(u_1^2 - 2u_2) - u_2v_1^2 + v_2^2
\end{aligned}$$

$$\begin{aligned}
\text{Es ist } D &= (15394628755070098929, 49, \\
&\quad 31694823907497262594, 86028807748921141745) \\
\text{ein Punkt auf} &\quad (J_C - \Theta)(\mathbb{F}_p). \\
\text{Sei } l_p &= 59248648645708686479341865505391744126 79, \\
\text{so ist } (l_p - 1)D &= (15394628755070098929, 49, \\
&\quad 122251463643203727349, 67917479801779848198) \\
&= -D.
\end{aligned}$$

Additionsformel(Spallek) : 7.540 *sek*

Additionsalgorithmus(Cantor) : 20.460 *sek*

Laufzeit genauer spezifizieren!

Kapitel 3

Prinzipal polarisierte Abelsche Varietäten mit CM

3.1 Prinzipal polarisierte Abelsche Varietäten

In diesem Kapitel werden die wichtigsten Grundlagen für die Konstruktion von geeigneten Jacobischen Varietäten über $\mathbb{C}$ geliefert. Wir benötigen sowohl Ergebnisse aus der algebraischen als auch aus der analytischen Theorie von Abelschen Varietäten. Die wesentlichen Definitionen und Sätze findet man in [S-T] Kapitel 1 §3.1 oder [La II] Kapitel 3 §4.

In den folgenden Kapiteln sei A stets eine über einem beliebigen Körper K definierte Abelsche Varietät. Weiterhin wollen wir die folgenden Bezeichnungen vereinbaren:

$\mathcal{D}_a$	Gruppe aller Divisoren auf A algebraisch äquivalent zu Null ($\equiv_a$)
$\mathcal{D}_l$	Gruppe der Hauptdivisoren, d.h. linear äquivalent zu Null ($\sim$)
$\mathcal{D}_a/D_l =: Pic^0(A)$	Picardvarietät von A

Ist X Divisor auf A, dann gibt es einen Homomorphismus

$$\varphi_X : A \longrightarrow Pic^0(A)$$

gegeben durch

$$a \longrightarrow Cl(X_a - X),$$

wobei X_a die Translation von X durch a und Cl die lineare Äquivalenzklasse bezeichnet. Diese Aussage gilt für alle Charakteristiken.

Ein Divisor X heißt **nicht-ausgeartet**, wenn der Kern von φ_X endlich ist. Dann ist die Abbildung φ_X surjektiv. Wir definieren

$$\mathcal{C} = \mathcal{C}(X) := \{Y \in Div(A) \mid \exists m, m' > 0 \text{ ganze Zahlen, mit } mX \equiv_a m'Y\}.$$

Eine **Polarisierung** ist eine Klasse $\mathcal{C}$ von Divisoren, so daß $\mathcal{C} = C(X)$ für einen amplen (oder äquivalent, positiv nicht-ausgearteten) Divisor X. Das Paar $(A, \mathcal{C})$ heißt dann **polarisierte Abelsche Varietät**. Es gibt stets einen Divisor $X_0 \in Div(A)$, genannt **Basispolardivisor von** $\mathcal{C}$, so daß es für alle Divisoren $Y \in \mathcal{C}$ eine positive ganze Zahl m mit $Y \equiv_a mX_0$ gibt. X_0 ist bis auf algebraische Äquivalenz eindeutig bestimmt. Nachdem Satz von Riemann-Roch gibt es stets einen positiven Divisor, der zu X_0 algebraisch äquivalent ist. Ist X_0 ein positiver Basispolardivisor, so bezeichnen wir mit $\mathcal{C}_{X_0}$ die zugehörige Polarisierung.

Ist A über den komplexen Zahlen definiert, so ist bekanntlich die Gruppe der komplexen Punkte $A(\mathbb{C})$ eine kompakte komplexe Lie-Gruppe und daher komplex analytisch isomorph zu einem Torus. Das heißt, es gibt einen komplex analytischen Isomorphismus

$$\theta : \mathbb{C}^n/\Lambda \longrightarrow A,$$

wobei $dim A = n$ und Λ ein Gitter in $\mathbb{C}^n$ ist.

Definition 3.1 *Sei $\mathbb{C}^n/\Lambda$ ein komplexer Torus. Eine $\mathbb{R}$-Bilinear-Form $E(x,y)$ auf $\mathbb{C}^n$ mit Werten in den reellen Zahlen $\mathbb{R}$ heißt (nicht-ausgeartete) Riemannform von $\mathbb{C}^n/\Lambda$, wenn*

(1) $E(x,y) \in \mathbb{Z}$ *für alle* $x, y \in \Lambda$

(2) $E(x,y) = -E(y,x)$

(3) $E(ix,y)$ *ist eine positiv definite symmetrische Form .*

Bekanntlich kommt ein komplexer Torus $\mathbb{C}^n/\Lambda$ genau dann von einer Abelschen Varietät A, wenn es auf ihm eine Riemannform gibt.

Eine meromorphe Funktion ϑ auf $\mathbb{C}$ heißt **Thetafunktion** auf $\mathbb{C}^n/\Lambda$, wenn

$$\vartheta(z+\lambda) = \vartheta(z) \cdot e^{2\pi i(l_\lambda(z)+c_\lambda)} \text{ für alle } \lambda \in \Lambda \text{ ist,}$$

wobei $l_\lambda(z)$ eine $\mathbb{C}-$Linearform auf $\mathbb{C}^n$ und c_λ eine von λ abhängige komplexe Zahl bezeichnet. Da

$$l_{\lambda_1+\lambda_2}(z) = l_{\lambda_1}(z) + l_{\lambda_2}(z),$$

kann man $l_\lambda(z)$ zu einer $\mathbb{R}$-bilinearen Funktion auf $\mathbb{C}^n$ fortsetzen. Ist ϑ holomorph, so wird durch

$$E_\vartheta(x,y) := l_x(y) - l_y(x)$$

wegen

$$l_{\lambda_1}(\lambda_2) \equiv l_{\lambda_2}(\lambda_1) \bmod \mathbb{Z}$$

eine durch ϑ gegebene Riemannform auf $\mathbb{C}^n/\Lambda$ definiert. Ist andererseits $E(x,y)$ eine Riemannform auf $\mathbb{C}^n/\Lambda$, so gibt es eine holomorphe Thetafunktion ϑ auf $\mathbb{C}^n/\Lambda$, so daß E eine durch ϑ definierte Riemannform ist.

Der Divisor (ϑ) ist invariant unter Λ und definiert deshalb einen analytischen Divisor $X := (\vartheta)$ auf $\mathbb{C}^n/\Lambda$. Man kann zeigen, daß die durch ϑ definierte Form E_ϑ eindeutig durch den Divisor X und unabhängig von der Wahl von ϑ bestimmt ist. Wir definieren $E_X := E_\vartheta$. Ebenfalls kann man zeigen, daß zwei Divisoren X, Y genau dann algebraisch äquivalent sind ($X \equiv_a Y$), wenn die zugehörigen Riemannformen E_X, E_Y gleich sind.

Da A über den komplexen Zahlen definiert ist, bestimmt jede Polarisierung $\mathcal{C}$ auf A nicht nur eindeutig die algebraische Äquivalenzklasse eines amplen Basispolardivisors Y, sondern damit auch eindeutig eine Riemannform $E_\mathcal{C} := E_Y$. Die Pfeile verdeutlichen diese eindeutigen Beziehungen.

$$\mathcal{C} = \mathcal{C}_Y \longleftrightarrow [Y]_a \longleftrightarrow E_\mathcal{C} := E_Y \longleftrightarrow \varphi_\mathcal{C} := \varphi_Y$$

Sei der Torus $\mathbb{C}^n/\Lambda$ eine analytische Darstellung von A. Dann gibt es eine symplektische Basis $\{\lambda_1, \cdots, \lambda_{2n}\}$ von Λ, mit

$$(E_\mathcal{C}(\lambda_i, \lambda_j))_{ij} = \begin{pmatrix} & & & e_1 & & \\ & 0 & & & \cdot & \\ & & & & & e_n \\ -e_1 & & & & & \\ & \cdot & & & 0 & \\ & & -e_n & & & \end{pmatrix} \quad \text{mit } e_1, \cdots, e_n \in \mathbb{Z}_+, e_1|e_2|\cdots|e_n$$

Wir haben $\sqrt{det\ E_\mathcal{C}} = e_1 \cdots e_n$ und man kann die Gleichheit $|ker(\varphi_\mathcal{C})| = |det\ E_\mathcal{C}|$ leicht zeigen.

Definition 3.2 *Mit den obigen Bezeichnungen und Voraussetzungen gilt:*
(A, C_Y) *heißt* ***prinzipal polarisiert****, wenn*

$$(E_C(\lambda_i, \lambda_j))_{ij} = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix} =: J, \text{ das heißt } \sqrt{det(E_C)} \text{ gleich } 1 \text{ ist.}$$

Also ist $(A, \mathcal{C})$ genau dann prinzipal polarisiert, wenn $|ker(\varphi_C)| = 1$, d.h. φ_C ein Isomorphismus ist.
Definieren wir $\Omega_1 := (\lambda_1, \cdots, \lambda_n) \in M^{n\times n}(\mathbb{C})$ und $\Omega_2 := (\lambda_n, \cdots, \lambda_{2n}) \in M^{n\times n}(\mathbb{C})$, so ist E_C genau dann prinzipal, wenn $\Omega := \Omega_2^{-1}\Omega_1$ symmetrisch und der Imaginärteil von Ω positiv definit $(Im(\Omega) > 0)$ ist. Man bezeichnet die Menge dieser Matrizen

$$\mathcal{H}_n := \{\Omega \in GL_n(\mathbb{C}) |\ \Omega^t = \Omega, Im(\Omega) > 0\}$$

als die **n-dimensionale Siegelsche obere Halbebene.** Setzen wir

$$Sp(2n, \mathbb{Z}) := \{M \in GL_{2n}(\mathbb{Z}) |\ MJM^t = J\},$$

so entspricht $\mathcal{H}_n / Sp(2n, \mathbb{Z})$ den Isomorphieklassen von prinzipal polarisierten Abelschen Varietäten.

Satz 3.3 *Sei $(A, \mathcal{C})$ eine polarisierte Abelsche Varietät, dann gibt es einen Körper k_0 mit der folgenden Eigenschaft:*

> *Ist k ein Definitionskörper von $(A, \mathcal{C})$, der k_0 enthält, σ ein Isomorphismus von k in einen Körper, dann ist $(A, \mathcal{C})$ zu $(A^\sigma, \mathcal{C}^\sigma)$ isomorph, genau dann wenn σ die Identität auf k_0 ist.*

Falls $char(k) = 0$, dann ist k_0 eindeutig bestimmt und in jedem Definitionskörper enthalten. k_0 heißt **Modulkörper** der polarisierten Abelschen Varietät $(A, \mathcal{C})$. Ist A über $\mathbb{C}$ definiert, so kann der Modulkörper über $\mathbb{Q}$ durch bestimmte Werte von Siegelschen Modulfunktionen erzeugt werden.
Für diesen Satz und die Definition vergleiche man [S-T] Kapitel 1 §4.2 Satz 2.

Beispiel: Die Jacobische Varietät einer hyperelliptischen Kurve

(Vgl. [Mum I],Kapitel 2,§2.)
Es sei C eine hyperelliptische Kurve vom Geschlecht g. Die komplexen Punkte eines nichtsingulären Modells der Kurve können bekanntlich als kompakte zusammenhängende Riemannsche Fläche S vom Geschlecht g aufgefaßt werden. Ihre erste Homologiegruppe $H_1(S,\mathbb{Z})$ ist eine freie abelsche Gruppe mit $2g$ Erzeugern. Nun wählt man als Erzeugende geschlossene Kurven $A_1,\cdots,A_g,B_1,\cdots,B_g$ in S derart, daß sich zwei verschiedene A_i oder zwei B_i oder ein A_i und ein B_j für $i \neq j$ in keinem Punkt, aber die Kurven A_i und B_i in genau einem Punkt schneiden. Bezeichnet $\Omega_1(S)$ den Vektorraum der holomorphen Differentiale von S, so gibt es eine Basis $\omega_1,\cdots,\omega_g$ von $\Omega_1(S)$, mit

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

Definiert man anschließend

$$\Omega_{ij} := \int_{B_i} \omega_j \text{ und } \Omega := (\Omega_{ij}),$$

so liegt Ω in $\mathcal{H}_g$. Nach dem Satz von Abel ist die Gruppe der komplexen Punkte $J_C(\mathbb{C})$ der Jacobischen Varietät J_C komplex analytisch isomorph zu dem Torus $\mathbb{C}^g/L_\Omega$ mit dem Gitter $L_\Omega := \mathbb{Z}^g + \Omega\mathbb{Z}^g \subset \mathbb{C}^{2g}$. Die Abbildung Φ, definiert durch

$$\Phi \;:\; J_C(\mathbb{C}) \longrightarrow \mathbb{C}^g/L_\Omega$$

$$\sum_{i=1}^{r} P_i \longrightarrow \sum_{i=1}^{r} \int_{P_\infty}^{P_i} (\omega_1,\cdots,\omega_g) \; mod \; L_\Omega,$$

liefert den Isomorphismus (vgl. Kapitel 2).
Der analytische Divisor $\Phi(\Theta)$ für den Thetadivisor Θ von C definiert so die kanonische Polarisierung $\mathcal{C}_{\Phi(\Theta)}$ auf $J_C(\mathbb{C})$. Da Ω in $\mathcal{H}_g$, ist $(J_C(\mathbb{C}),\mathcal{C}_{\Phi(\Theta)})$ eine prinzipal polarisierte Abelsche Varietät der Dimension g mit Basispolardivisor $\Phi(\Theta)$.

3.2 CM-Theorie von Abelschen Varietäten

Sei K ein algebraischer Zahlkörper mit $|K:\mathbb{Q}| = 2n$, A eine Abelsche Varietät über $\mathbb{C}$ der Dimension n und $\mathbb{C}^n/\Lambda$ eine komplexe Darstellung von $A(\mathbb{C})$ bezüglich eines Isomorphismus

$$\theta : \mathbb{C}^n/\Lambda \longrightarrow A(\mathbb{C}).$$

K heißt **CM-Körper**, wenn K eine total imaginärquadratische Erweiterung eines total reellen Zahlkörpers ist. Ein Tupel $(K, \{\varphi_1, \cdots, \varphi_n\})$ nennt man einen **CM-Typ**, falls $\{\varphi_1, \bar{\varphi}_1, \cdots, \varphi_n, \bar{\varphi}_n\}$ die Menge aller Einbettungen von K nach $\mathbb{C}$ ist.

Sei e : $K \longrightarrow End(A) \otimes \mathbb{Q} =: End_{\mathbb{Q}}(A)$ ein Isomorphismus von $\mathbb{Q}$-Algebren mit $e(1) = 1_A$

und Φ_1 : $End_{\mathbb{Q}}(A) \longrightarrow End(\mathbb{C}^n, \mathbb{C}) \cong M_n(\mathbb{C})$ eine komplexe Darstellung von $End_{\mathbb{Q}}(A)$,

so ist

S_Φ := $\Phi_1 \circ e$ ein $\mathbb{Q}$ – linearer Isomorphismus von K nach $M_n(\mathbb{C})$ mit $S_\Phi(1) = E_n$,

und es gilt folgender Satz.(vgl. [S-T] Kapitel 2§5.2).

Satz 3.4 *Es gibt Isomorphismen $\varphi_1, \cdots, \varphi_n : K \longrightarrow \mathbb{C}$ mit*

$$S_\Phi(\alpha) = \begin{pmatrix} \varphi_1(\alpha) & & \\ & \ddots & \\ & & \varphi_n(\alpha) \end{pmatrix} \quad \forall \alpha \in K \text{ nach geeigneter Basiswahl.}$$

Man sagt, die **Abelsche Varietät (A, e) ist vom CM-Typ $(K, \{\varphi_1, \cdots, \varphi_n\})$ oder für $\Phi := \oplus_{i=1}^n \varphi_i$ auch vom CM-Typ (K, Φ).** Der Einfachheit halber schreiben wir nur 'A ist vom CM-Typ (K, Φ)' und identifizieren dann jedes Element $\alpha \in K$ mit einem Element $e(\alpha) \in End_{\mathbb{Q}}(A)$. Hierzu definieren wir $\Phi(\alpha) :=^t (\varphi_1(\alpha), \cdots, \varphi_n(\alpha)) \in \mathbb{C}^n$. Ein CM-Typ heißt **primitiv**, wenn alle Abelschen Varietäten von diesem Typ einfach sind, das heißt, wenn sie außer 0 und sich selbst keine Abelschen Untervarietäten enthalten.

Der duale CM-Typ

Sei (K, Φ) ein CM-Typ und L ein Erweiterungskörper von K, so daß $L/\mathbb{Q}$ galoisch ist. K_0 sei der total reelle Teilkörper von K, d.h. $|K : K_0| = 2$. Dann setzen wir $G := Gal(L/\mathbb{Q})$ und bezeichnen mit H und H_0 die zugehörigen Untergruppen von G bezüglich K und K_0.

$$\begin{aligned} \text{Weiterhin sei} \quad S &:= \{\sigma \in G \mid \sigma|_K = \varphi_i \;\; i \in \{1, \cdots, n\}\}, \\ S^* &:= \{\gamma^{-1} \mid \gamma \in S\} \\ \text{und} \quad H^* &:= \{\gamma \in G \mid \gamma S^* = S^*\}. \end{aligned}$$

Definieren wir

$$H' := \{\gamma \in G \mid \gamma S = S\},$$

so kann man leicht zeigen, daß der CM-Typ $(K, \{\varphi_i\})$ genau dann primitiv ist, wenn die Gruppen H und H' gleich sind (vgl. [S-T] Kapitel 2 §8.2).
Einen Beweis des folgenden Satzes 3.5 und der Proposition 3.6 findet man in [S-T] Kapitel 2 §8.3.

Satz 3.5 *K^* bezeichne jetzt den zu H^* gehörenden Unterkörper und $\{\psi_j\}$ die Menge aller Isomorphismen von K^* nach $\mathbb{C}$, die man aus Elementen von S^* erhält. Dann gilt: $(K^*, \{\psi_j\})$ ist auch CM-Typ und*

$$K^* = \mathbb{Q}(\sum_{i=1}^{n} \xi^{\varphi_i} \mid \xi \in K).$$

K^* ist durch $(K, \{\varphi_i\})$ eindeutig bestimmt und unabhängig von der Wahl von L.

Der CM-Typ $(K^*, \{\psi_j\})$ wird der zu $(K, \{\varphi_i\})$ **duale CM-Typ** genannt.

Wir bezeichnen nun mit I_{K^*} und I_K die Gruppen der Ideale von K^* bzw. K und mit H_{K^*} bzw. H_K die Untergruppen der Hauptideale. Dann gilt:

Proposition 3.6

$$\forall \quad \alpha \in K^* \text{ ist } \beta := \prod_j \alpha^{\psi_j} \in K, \text{ also } \beta\bar{\beta} = Norm_{K^*/\mathbb{Q}}(\alpha)$$

$$\forall \quad a \in I_{K^*} \text{ ist } b := \prod_j a^{\psi_j} \in I_K, \text{ also } b\bar{b} = Norm_{K^*/\mathbb{Q}}(a)$$

Wir haben uns zum Ziel gesetzt, Jacobischen Varietäten von Kurven vom Geschlecht 2 mit komplexer Multiplikation explizit zu konstruieren. Im letzten Abschnitt haben wir gesehen, daß das genau die prinzipal polarisierten einfachen Abelschen Varietäten der Dimension 2 von primitiven CM-Typen vom Grad 4 über $\mathbb{Q}$ sind. In dem folgenden Beispiel werden diese CM-Typen mit ihren dualen Typen bestimmt.

Beispiel: CM-Typen und ihre Dualen für Dimension 2

Es sei speziell $n = 2$, d.h. $|K : \mathbb{Q}| = 4$ und $(K, \{1, \varphi\})$ ein $CM-$Typ mit total reellem Teilkörper K_0. Weiterhin sei $K = K_0(\xi)$ mit $-\xi^2$ total positiv in K_0 $(-\xi^2 >> 0)$. Wir können ξ immer so wählen, daß $-\bar{\xi} = \xi > 0$, d.h. ξ rein imaginär mit $Im(\xi) > 0$ ist. Mit ρ bezeichnen wir die Galoiskonjugation von K über K_0.

Fall 1 $K/\mathbb{Q}$ **galoisch**

Da $K/\mathbb{Q}$ galoisch, kann L gleich K gewählt werden. G ist abelsch und die Einbettungen $\{1, \rho, \varphi, \bar{\varphi} = \varphi^\rho\}$ entsprechen den Galoiskonjugationen.

(a) $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

In diesem Fall haben wir

$$\begin{aligned} H_0 &= Gal(K/K_0) = \{1, \rho\}. \\ \text{Setze } S &= \{1, \sigma\} \text{ mit } \sigma = \varphi \text{ oder } \sigma = \bar{\varphi}, \text{ dann ist} \\ S^* &= \{1, \sigma^{-1}\},\ G = \{1, \sigma, \rho, \sigma\rho\} \text{ und } H' = \{1, \sigma\} \neq H = G. \end{aligned}$$

Da $H' \neq H$, ist der CM-Körper K nicht primitiv.
Sei nun K^* der zu $H^* = \{\gamma \in G | \gamma S^* = S^*\} = \{1, \sigma\}$ gehörende Unterkörper von K. Damit ist K^* ein imaginärquadratischer Zahlkörper mit $K = K_0\, K^*$.

(b) $G \cong \mathbb{Z}/4\mathbb{Z}$

Wieder ist $S = \{1, \sigma\}$, also $G = \{1, \sigma, \sigma^2 = \rho, \sigma\rho\} = < \sigma >$.
Daraus folgt $H^* = H' = \{1\}$, so daß $(K, \{1, \sigma\})$ ein primitiver CM-Typ ist.
Da $S^* = (1, \sigma^{-1})$, ist $(K, \{1, \sigma^{-1}\})$ der zu $(K, \{1, \sigma\})$ duale CM-Typ.

Fall 2 $K/\mathbb{Q}$ **nicht galoisch**

Setze $K_0 = \mathbb{Q}(\sqrt{D})$ für ein quadratfreies $D > 0$. Da $-\xi^2$ total positiv in K_0 ist, kann es in der Form $-\xi^2 = A + B\sqrt{D}$ mit rationalen Zahlen A und B dargestellt werden, wobei $A + B\sqrt{D} > 0$ und $A - B\sqrt{D} > 0$ und $\xi = i\sqrt{A + B\sqrt{D}}$, $\xi^\varphi = i\sqrt{A - B\sqrt{D}}$. Da $K/\mathbb{Q}$ nicht galoisch ist, folgt $K_0(\xi^\varphi) \neq K_0(\xi)$. Definieren wir $D' := A^2 - B^2D > 0$, so ist $D' = (\xi\xi^\varphi)^2$ also $\sqrt{D'} \notin K_0$. Also ist $\mathbb{Q}(\sqrt{D'})$ ein total reeller quadratischer Zahlkörper ungleich K_0. Für $L = \mathbb{Q}(\xi, \xi^\varphi)$ ist die Körpererweiterung $L/\mathbb{Q}$ galoisch und $|L : \mathbb{Q}| = 8$. Die Galoisgruppe G von L über $\mathbb{Q}$ besteht aus 8 Automorphismen.

$$\begin{aligned} \text{Sei } \sigma &: (\xi, \xi^\varphi) \longrightarrow (\xi^\varphi, -\xi) \\ \tau &: (\xi, \xi^\varphi) \longrightarrow (\xi^\varphi, \xi). \end{aligned}$$

Wir sehen $\sigma^2 = \rho, \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau$, so daß G von τ, σ erzeugt wird.
Also haben wir $G =< \tau, \sigma >$. Außerdem verifiziert man leicht, daß

$$\begin{aligned} H &= \{1, \sigma\tau\}, S = \{1, \sigma, \tau, \sigma\tau\}, \\ \text{und } H_0 &= \{1, \sigma\tau, \tau\sigma, \rho\}, \quad H' = \{\gamma \in G | \gamma S = S\} = \{1, \sigma\tau\}. \end{aligned}$$

Da $H = H'$, ist $(K, \{1, \varphi\})$ primitiv. Weiterhin haben wir

$$\begin{aligned} S^* &= \{\sigma^{-1} | \sigma \in S\} = \{1, \tau, \sigma^3, \sigma\tau\} \\ \text{und} \quad H^* &= \{\sigma \in G | \sigma S^* = S^*\} = \{1, \tau\}. \end{aligned}$$

Damit ist $S^* = H^* \cup H^{*\sigma\tau}$. Setzen wir $\psi := \sigma\tau$, so ist $(K^*, \{1, \psi\}) = (\mathbb{Q}(\xi + \xi^\varphi), \{1, \sigma\tau\})$ der zu $(K, \{1, \varphi\})$ duale CM-Typ.

Der folgende Satz zeigt, wie polarisierte Abelsche Varietäten über $\mathbb{C}$ konstruiert werden können. Den Beweis findet man in [La II] Kapitel 1 §4.

Satz 3.7 *Es sei $K/\mathbb{Q}$ ein CM-Körper mit $|K:\mathbb{Q}| = 2\cdot n$ und (K,Φ) ein CM-Typ. Dann gilt:*

1. *Sei a ein Gitter in K, dann ist $\Phi(a)$ ein Gitter in $\mathbb{C}^n$ und $\mathbb{C}^n/\Phi(a)$ komplexer Torus vom Typ (K,Φ).*

2. *Sei (A,e) vom Typ (K,Φ), dann gibt es ein Gitter a in K und einen komplex analytischen Isomorphismus θ, so daß das folgende Diagramm für alle $\alpha \in K$ kommutiert:*

$$\begin{array}{ccc} \mathbb{C}^n/\Phi(a) & \xrightarrow{\theta} & A \\ {\scriptstyle S_\Phi(\alpha)}\downarrow & & \downarrow{\scriptstyle e(\alpha)} \\ \mathbb{C}^n/\Phi(a) & \xrightarrow[\theta]{} & A \end{array}$$

In diesem Fall schreiben wir die Abelsche Varietät $(A(a),e)$ oder nur $A(a)$ ist vom CM-Typ (K,Φ). Setzen wir

$$O := \{\alpha \in K | \alpha a \subset a\}, \quad \text{so ist } e(O) = e(K) \cap End(A).$$

Ist K primitiv, so ist $e(K) = End_{\mathbb{Q}}(A)$ und $e(O) = End(A)$.

Folgerung 3.8 *Zwei Abelsche Varietäten vom selben CM-Typ sind isogen zueinander. Ein CM-Typ ist damit primitiv, wenn schon eine Abelsche Varietät von diesem Typ einfach ist.*

Wir wollen Jacobische Varietäten mit Endomorphismenring O_K konstruieren, wobei O_K der Ring der ganzen Zahlen eines primitiven CM-Körpers K ist. Deshalb soll im Folgenden unter einer Abelschen Varietät A vom CM-Typ (K,Φ) stets eine Varietät mit $End(A) = e(O_K)$ bzgl. eines primitiven CM-Körpers K zu verstehen sein. Wir identifizieren dann jeden Endomorphismus mit einer Zahl aus O_K.

Ist K ein CM-Körper, so gibt es ein Element $\xi \in K$ mit $\xi^2 \in K_0$ und $K = K_0(\xi)$. Weil K total imaginär ist, ist $-\xi^2$ total positiv in K_0. Wir können ξ so wählen, daß $Im(\xi^{\varphi_i}) > 0$ für $i = 1, \cdots, n$ ist. Dann definiert

$$E_\xi(x,y) := \sum_{i=1}^{n} \xi^{\varphi_i}(\bar{x}_i y_i - x_i \bar{y}_i) \qquad (E_1)$$

eine $\mathbb{R}$-bilineare Form auf $\mathbb{C}^n$. Man sieht sofort, daß $E_\xi(x,y) = -E_\xi(y,x)$. Weil die ξ^{φ_i} alle rein imaginär sind und positiven Imaginärteil haben, ist die Form

$$E_\xi(ix,y) = -i\sum_{i=1}^{n} \xi^{\varphi_i}(\bar{x}_i y_i + x_i \bar{y}_i)$$

symmetrisch, positiv definit und nicht-ausgartet. Nach Definition ist für alle $\alpha_1, \alpha_2 \in K$

$$E_\xi(\Phi(\alpha_1), \Phi(\alpha_2)) = Tr_{K/\mathbb{Q}}(\xi \bar{\alpha}_1 \alpha_2).$$

Wir können daher eine ganze Zahl r finden, so daß die Werte von $rE_\xi(\alpha_1, \alpha_2)$ für alle $\alpha_1, \alpha_2 \in a$ ganze Zahlen sind. Ersetzen wir ξ durch $r\xi$, dann definiert $E_\xi(x,y)$ eine Riemannform auf $\mathbb{C}^n/\Phi(a)$. Diese Form hat dann die charakteristische Eigenschaft

$$E_\xi(x, S_\Phi(\alpha)y) = E_\xi(S_\Phi(\bar{\alpha})x, y) \quad \text{für alle } \alpha \in K. \qquad (E_2)$$

Bekanntlich ist $E_\xi = E_X$ für eine amplen Divisor $X \in Div(A)$, so daß E_ξ eine Polarisierung $\mathcal{C}_\xi := \mathcal{C}_X$ bestimmt. Damit zeigten wir den ersten Teil von dem folgenden Satz.

Satz 3.9 *1. Sei K ein CM-Körper, dann gibt es stets ein Element $\xi \in K$ mit $K = K_0(\xi)$, $-\xi^2$ total positiv in K_0 und $Im(\xi^{\varphi_i}) > 0$ für $i = 1, \cdots, n$, so daß $(A(a), \xi) := (A(a), \mathcal{C}_\xi)$ eine polarisierte Abelsche Varietät vom CM-Typ (K, Φ) ist.*

2. Umgekehrt: Jede Riemannform E auf $\mathbb{C}^n/\Phi(a)$, die der Bedingung (E_2) genügt, kann durch ein geeignetes Element $\xi \in K$ durch (E_1) definiert werden.

Einen Beweis des zweiten Teils findet man in [S-T] Kapitel 2, §6.2.

Die folgende Proposition und Definition findet man in [S-T] Kapitel 2 §7 , 8.

Proposition 3.10 *Es seien A_1 und A_2 zwei über $\mathbb{C}$ definierte Abelsche Varietäten vom CM-Typ (K,Φ), so gibt es Gitter a_1, a_2 in K mit $A_1(\mathbb{C}) \cong \mathbb{C}^n/\Phi(a_1)$ und $A_2(\mathbb{C}) \cong \mathbb{C}^n/\Phi(a_2)$. Sei nun γ ein Element in K ungleich 0 mit $\gamma \in a_1^{-1}a_2$, so repräsentiert die Matrix $S_\Phi(\gamma)$ einen Homomorphismus von A_1 nach A_2. Umgekehrt gehört jeder Homomorphismus λ von A_1 nach A_2 zu einer Matrix $S_\Phi(\gamma)$ mit $\gamma \in a_1^{-1}a_2$.*

Wir sagen, λ ist eine $\gamma a_2^{-1}a_1$-**Multiplikation** von A_1 nach A_2 und A_2 ist eine $\gamma a_2^{-1}a_1$-**Transformation** von A_1. Die Abelschen Varietäten A_1 und A_2 sind genau dann isomorph, wenn die Gitter a_1 und a_2 äquivalent sind. Dann ist nach Definition A_2 eine O_K-Transformation von A_1.

Folgerung 3.11 *Sei $h = |c_K|$ die Klassenzahl von K, so gibt es genau h nicht zueinander isomorphe Abelsche Varietäten vom CM-Typ (K,Φ).*

Definition 3.12 *Die polarisierten Abelsche Varietäten (A_1, C_{X_1}) und (A_2, C_{X_2}) sind isomorph, falls es einen Isomorphismus λ von A_1 nach A_2 mit $\lambda(X_1) \equiv_a X_2$ gibt.*

Konstruktion der prinzipalen Polarisierung

Es sei im Folgenden stets $A = A(a)$ eine Abelsche Varietät vom CM-Typ (K,Φ) mit Endomorphismenring O_K und komplexer Darstellung $\mathbb{C}^2/\Phi(a)$ für ein Gitter a in K. Aus der analytischen Darstellung der Abelschen Varietät können wir auch direkt eine analytische Darstellung der Picardvarietät ablesen. Einen Beweis des folgenden Satzes findet man in [S-T] Kapitel 4 §14.2.

Satz 3.13 *Es sei $(A(a),\xi)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ (K,Φ). Bezeichnet δ die Differente von K über $\mathbb{Q}$, so wird die Picardvarietät $A^* := Pic^0(A)$ durch den Torus $\mathbb{C}^n/\Phi(a^*)$ mit $a^* = (\delta\bar{a})^{-1}$ und die Polarisierungsabbildung*

$$\varphi_\xi \;:\; A \longrightarrow A^*$$

durch die Matrix $S_\Phi(\xi) \;:\; \mathbb{C}^n/\Phi(a) \longrightarrow \mathbb{C}^n/\Phi(a^*)$ *analytisch dargestellt.*

Damit ist φ_ξ eine $(\xi\delta a\bar{a})$-Multiplikation.

Weil $K = K_0(\xi)$ und ξ rein imaginär ist, wird nach Definition die Relativdifferente δ_{K/K_0} von nur rein imaginären Elementen der Form $(o - \bar{o})$ mit $o \in O_K$ erzeugt. Damit ist das Ideal $\xi\delta_{K/K_0}$ ein Ideal in K_0. Natürlich ist auch $\delta_{K_0/\mathbb{Q}} a\bar{a}$ ein Ideal in K_0, so daß wegen $\delta = \delta_{K_0/\mathbb{Q}} \cdot \delta_{K/K_0}$ das gesamte Ideal von der Form

$$(\xi\delta a\bar{a}) = I_0 O_K \text{ mit } I_0 \in I_{K_0} \text{ ist.}$$

Das Ideal I_0 wird durch das Ideal a und die Polarisierung bestimmt und ist unabhängig von der Wahl des Basispolardivisors. In diesem Fall sagt man, daß die polarisierte Abelsche Varietät $(A(a), \xi)$ vom CM-Typ $(K, \Phi; I_0)$ ist. Nach Definition ist $(A(a), \xi)$ prinzipal polarisiert, genau dann wenn *det* $E_\xi = 1$, d.h. φ_ξ ein Isomoprhismus, also φ_ξ eine O_K-Multiplikation ist. Das ist für $I_0 = O_{K_0}$ der Fall. Damit zeigten wir:

Proposition 3.14 *Genau dann gibt es eine prinzipale Polarisierung C auf $A(a)$ vom CM-Typ (K, Φ), wenn es ein Element ξ in K gibt, das die folgenden zwei Bedingungen erfüllt.*

1. *ξ definiert durch (E_1) eine Riemannform auf $A(a)$.*
   (D.h. $K = K_0(\xi)$, und $\bar{\xi} = -\xi$ und $Im(\xi^{\varphi_i}) > 0$ für $i = 1, \cdots, n$.)
2. *$\xi\delta a\bar{a} = O_{K_0}$.*

Folgerung 3.15 *Es gibt genau dann eine prinzipale Polarisierung auf $A(O_K)$ vom CM-Typ $(K, \{\varphi_i\})$, wenn es ein Element $\gamma \in K$ gibt, das die folgenden Bedingungen erfüllt.*

1. *Die Differente δ von K über $\mathbb{Q}$ ist das Hauptideal (γ),*
2. *$\gamma^{\varphi_i} < 0$ für alle i.*

Dann kann $\xi = \gamma^{-1}$ gesetzt werden. Da γ nach Definition der Differente rein imaginär ist, sind für ξ die Bedingungen der letzten Proposition erfüllt.

Wir nennen einen CM-Typ $(K, \{\varphi_1, ..., \varphi_n\})$ O_K **geeignet** oder einfach nur **geeignet**, falls es eine prinzipale Polarisierung auf $A(O_K)$ von diesem Typ gibt. Es ist klar, daß es genau dann einen geeigneten CM-Typ zu einem CM-Körper K gibt, wenn die Differente δ ein Hauptideal ist. Das ist zum Beispiel der Fall, wenn der Körper K_0 Klassenzahl 1 hat.

Wie viele CM-Typen zu einem CM-Körper geeignet sind, hängt von den Fundamentaleinheiten ab. Und zwar davon, wie sich ihr Vorzeichen unter den Einbettungen verändert. Gibt es von jeder denkbaren Kombination eine Einheit, so ist jeder CM-Typ geeignet und die zugehörigen Polarisierungselemente sind $\varepsilon\xi$ für jede Einheit ε.

Isomorphieklassen von prinzipal polarisierten Abelschen Varietäten

Wir wollen nun die Isomorphieklassen von prinzipal polarisierten Abelschen Varietäten zu gegebenem CM-Typ oder nur zu gegebenem CM-Körper genauer untersuchen.

Satz 3.16 *Sei $(A(a),\xi_1)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ (K,Φ). Ein zweites Element ξ_2 definiert genau dann eine prinzipale Polarisierung auf $A(a)$ vom selben Typ, wenn es eine total positive Einheit ε_0 in K_0 mit $\xi_2 = \varepsilon_0\xi_1$ gibt.*

Beweis: Es seien C_{ξ_1} und C_{ξ_2} zwei prinzipale Polarisierungen auf der Abelschen Varietät $A(a)$. Die Polarisierungsabbildungen φ_{ξ_1} und φ_{ξ_2} sind Isomorphismen und werden nach Satz 3.13 durch die Matrizen $S_\Phi(\xi_1)$ und $S_\Phi(\xi_2)$ komplex dargestellt. Damit ist $\varphi_{\xi_1}^{-1}\,\varphi_{\xi_2}$ ein Automorphismus auf $A(a)$, der durch die Matrix

$$S_\Phi(\xi_1)^{-1}\,S_\Phi(\xi_2) = S_\Phi(\xi_1^{-1}\xi_2)$$

repräsentiert wird. Wir haben $\varphi_{\xi_1}^{-1}\varphi_{\xi_2} = e(\xi_1^{-1}\xi_2)$ und da $K = K_0(\xi)$, $\bar{\xi}_j = -\xi_j$ und $Im(\xi_j)^{\varphi_i} > 0$, ist $\xi_1^{-1}\xi_2$ ein total positives Element in O_{K_0}. Jeder Automorphismus von $A(a)$ kommt bekanntlich von einer Einheit ε in O_K, daher haben wir

$$\xi_1^{-1}\xi_2 = \varepsilon \text{ für eine total positive Einheit } \varepsilon \in K_0.$$

Andererseits definiert jedes Element der Form $\varepsilon\xi_1$ mit einer total positiven Einheit ε in K_0 eine prinzipale Polarisierung auf $A(a)$. Denn auch dann sind die Bedingungen von Proposition 3.14 erfüllt. □

Satz 3.17 *Zwei prinzipal polarisierte Abelsche Varietäten $(A(a),\xi_1)$ und $(A(a),\xi_2)$ vom selben CM-Typ sind genau dann isomorph, wenn $\xi_1^{-1}\xi_2 = \varepsilon\bar{\varepsilon}$ für eine Einheit $\varepsilon \in K$.*

Beweis: Da $(A(a),\mathcal{C}_{\xi_1})$ und $(A(a),\mathcal{C}_{\xi_2})$ zwei prinzipal polarisierte Abelsche Varietäten vom selben Typ sind, ist nach dem letzten Satz $\xi_2\xi_1^{-1} = \varepsilon_0$ für eine total positive Einheit $\varepsilon_0 \in K_0$. Nach Definition sind $(A(a),\mathcal{C}_{\xi_1})$ und $(A(a),\mathcal{C}_{\xi_2})$ genau dann isomorph, wenn es einen Automorphismus λ auf $A(a)$ gibt, so daß $\lambda(X_1) = X_2$ für einen Basispolardivisor X_1 von $\mathcal{C}_{\xi_1}$ und X_2 von $\mathcal{C}_{\xi_2}$. Jeder Automorphismus λ gehört bekanntlich zu einer Matrix $S_\Phi(\varepsilon)$ bezüglich einer Einheit $\varepsilon \in K$. $(A(a),\mathcal{C}_{\xi_1})$ und $(A(a),\mathcal{C}_{\xi_2})$ sind genau dann isomorph, wenn E_{ξ_2} gleich dem Bild von E_{ξ_1} unter $S_\Phi(\varepsilon)$ ist. Das heißt, wenn $E_{\xi_2}(S_\Phi(\varepsilon)x, S_\Phi(\varepsilon)y) = E_{\xi_1}(x,y)$. Aus der Eigenschaft (E_2) folgt:

$$\begin{aligned} E_{\xi_2}(S_\Phi(\varepsilon)x, S_\Phi(\varepsilon)y) &= E_{\xi_2}(S_\Phi(\varepsilon)S_\Phi(\bar{\varepsilon})x, y) \\ &= E_{\xi_2}(S_\Phi(\varepsilon\bar{\varepsilon})x, y). \end{aligned}$$

Nach Definition der Riemannform ist $E_{\xi_2}(S_\Phi(\varepsilon\bar{\varepsilon})x, y)$ genau dann gleich $E_{\xi_1}(x,y)$, wenn $\xi_1 = \varepsilon\bar{\varepsilon}\xi_2$ ist. Da $\xi_2\xi_1^{-1} = \varepsilon_0$ für eine total positive Einheit $\varepsilon_0 \in K_0$ ist, folgt die Behauptung. □

Folgerung 3.18 *Sei U die Gruppe der total positiven Einheiten in K_0 und U_1 die Untergruppe von U, deren Elemente von der Form $\varepsilon\bar{\varepsilon}$ für eine Einheit ε in K sind. Ist $(A(a),\xi)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ (K,Φ), so gibt es genau $d := |U/U_1|$ viele nicht isomorphe prinzipal polarisierte Abelsche Varietäten, mit derselben zugrunde liegenden Abelschen Varietät $A = A(a)$.*

Satz 3.19 *Zwei prinzipal polarisierte Abelsche Varietäten $(A(a_1),\xi_1)$ und $(A(a_2),\xi_2)$ vom selben CM-Typ (K,Φ) sind genau dann zueinander isomorph, wenn es ein Element $\gamma \in K$ gibt, so daß*

1. *$\gamma a_1 = a_2$ (d.h. die Abelschen Varietäten $A(a_1)$ und $A(a_2)$ sind isomorph)*
2. *$\xi_1 = \gamma\bar{\gamma}\xi_2$ (d.h. die Polarisierungen sind isomorph).*

Beweis: Nach Definition sind $(A(a_1),\xi_1)$ und $(A(a_2),\xi_2)$ genau dann isomorph, wenn es einen Isomorphismus λ von $A(a_1)$ nach $A(a_2)$ gibt, so daß $\lambda(X_1) = X_2$ für einen Basispolardivisor X_1 von $\mathcal{C}_{\xi_1}$ und X_2 von $\mathcal{C}_{\xi_2}$. Jeder Automorphismus λ gehört nach Proposition 3.10 zu einer Matrix $S_\Phi(\gamma)$ bezüglich eines Elementes $\gamma \in K$ mit $\gamma a_1 = a_2$. Nun ist wiederum $\lambda(X_1) = X_2$ genau dann, wenn $E_{\xi_2}(S_\Phi(\gamma)x, S_\Phi(\gamma)y) = E_{\xi_1}(x,y)$ ist, was nur für $\xi_1 = \gamma\bar{\gamma}\xi_2$ erfüllt ist. □

Wir definieren eine Untergruppe c'_K der Klassengruppe c_K von K durch

$$c'_K := \{\mathcal{A} \in c_K | \exists\ a \in \mathcal{A} \text{ und ein total positives Element } \alpha \in K_0 \text{ mit } a\bar{a} = (\alpha)\}.$$

Dann gilt folgender Satz:

Satz 3.20 *Sei $(A(a), \xi)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ (K, Φ). Ist A' eine a'-Transformation von A, so gibt es genau dann eine prinzipale Polarisierung $C_{\xi'}$ auf A', wenn a' in c'_K liegt.*

Da A' eine a'-Transformation von A ist, kann man für A' den Torus $\mathbb{C}^n/\Phi(a'^{-1}a)$ als analytische Darstellung wählen. Nach Proposition 3.14 ist $\xi\delta a\bar{a} = O_{K_0}$ und ξ erfüllt Bedingung (1) in 3.14. Damit haben wir

$$\xi'\delta a'^{-1}a\bar{a}'^{-1}\bar{a} = \xi'\xi^{-1}a'^{-1}\bar{a}'^{-1}.$$

Nun definiert ξ' nach 3.14 genau dann eine prinzipale Polarisierung auf A', wenn

$$\xi'\xi^{-1}a'^{-1}\bar{a}'^{-1} = O_{K_0}$$

und Bedingung (1) in 3.14 erfüllt ist. Das ist genau dann der Fall, wenn es ein total positives Element $\alpha \in K_0$ gibt, so daß $(\alpha) = a'\bar{a}'$ ist. □

Folgerung 3.21 *Ist $(K, \{\varphi_i\}) = (K, \Phi)$ ein geeigneter CM-Typ und $(\gamma) = \delta$ wie in 3.15, so gibt es genau $h' := |c'_K|$ verschiedene nicht zueinander isomorphe prinzipal polarisierte Abelsche Varietäten von diesem Typ. Bilden die Ideale $a_1, \ldots a_{h'}$ ein Repräsentantensystem von c'_K und $a_i\bar{a}_i = (\alpha_i)$ mit $\alpha_i >> 0$, so bildet*

$$\mathcal{K}_\Phi := \{(A(a_i), \xi_i) \mid i = 1, \ldots, h'\} \text{ mit } \xi_i := (\alpha_i\gamma)^{-1}$$

ein Repräsentantensystem der zugehörigen prinzipal polarisierten Abelschen Varietäten.

Aus den Ergebnissen von 3.18 und 3.21 erhalten wir den folgenden für uns wichtigen Satz:

Satz 3.22 *Ist (K, Φ) ein geeigneter CM-Typ, so gibt es genau $h' \cdot d$ nicht zueinander isomorphe prinzipal polarisierte Abelsche Varietäten von diesem Typ.*

Bilden die Einheiten $\varepsilon_1, \ldots, \varepsilon_d$ ein Repräsentantensystem von U/U_1, so bildet die Vereinigung $\mathcal{K}_\Phi = \cup_{l=1}^{d} \mathcal{K}_\Phi^l$ der Systeme

$$\mathcal{K}_\Phi^l := \{(A(a_i), \varepsilon_l\xi_i) \mid i = 1, \ldots, h'\} \text{ mit } \xi_i := (\alpha_i\gamma)^{-1},$$

ein Repräsentantensystem aller prinzipal polarisierten Abelschen Varietäten vom CM-Typ (K, Φ).

3.3 Hauptsatz der CM-Theorie

Es sei $(A,\mathcal{C})$ ein polarisierte Abelsche Varietät vom CM-Typ $(K,\{\varphi_i\})$ mit Endomorphismenring O_K. $(K^*,\{\psi_j\})$ bezeichne den zu $(K,\{\varphi_i\})$ dualen CM-Typ und k_0 den Modulkörper von $(A,\mathcal{C})$. Der Hauptsatz der komplexen Multiplikation von Abelschen Varietäten beschreibt für $k_0^* = k_0K^*$ die Körpererweiterung k_0^*/K^* klassenkörpertheoretisch. Einen Beweis des Satzes findet man in [S-T] Kapitel 4 §15. Wir definieren im Folgenden für ein Ideal $a \subset O_K$ den Index $N(a) := |O_K/a|$. Wenn a ein gebrochenes Ideal ist, so liegt $Norm_{K/\mathbb{Q}}(a) \cdot a \subset O_K$ und wir definieren den Index $N(a) := N(Norm_{K/\mathbb{Q}}(a) \cdot a)/N(Norm_{K/\mathbb{Q}}(a))$.

Satz 3.23 *Sei H_0 die Gruppe der Ideale a^* in K^*, so daß es ein Element μ in K gibt mit*

$$\prod_j a^{*\psi_j} = (\mu) \text{ und } N(a^*) = \mu\bar{\mu}.$$

Dann ist H_0 eine Idealgruppe von K^*, die die Hauptideale enthält und damit im Sinne der Klassenkörpertheorie modulo (1) definiert ist, und k_0^* ist die unverzweigte Erweiterung über K^* zur Idealgruppe H_0.

Damit ist $Gal(k_0^*/K^*) \cong I_{K^*}/H_0$. Gehört eine Galoiskonjugation σ von k_0^* über K^* zu der Idealklasse eines Ideals a^* von I_{K^*}/H_0, dann schreiben wir $\sigma(a^*)$. Nach Proposition 3.6 ist $\prod_j a^{*\psi_j}$ ein Ideal in c'_K. Shimura zeigte in [S-T] Kapitel 4 §15, daß $A^{\sigma(a^*)}$ eine $(\prod_j a^{*\psi_j})$-Transformation von A ist. Das heißt, für eine Abelsche Varietät $A = A(b)$ vom CM-Typ $(K,\{\varphi_i\})$ ist $A(b)^{\sigma(a^*)} = A((\prod_j a^{*\psi_j})^{-1}b)$ die bzgl. $\sigma(a^*)$ konjugierte Abelsche Varietät. Definiert ξ eine prinzipale Polarisierung auf $A(b)$, so definiert $N(a_i^*)\xi$ wegen Prop. 3.14 eine prinzipale Polarisierung auf $A((\prod_j a^{*\psi_j})^{-1}b)$ vom selben Typ. Damit folgt:

Proposition 3.24 *Es sei $(A(b),\xi)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ $(K,\{\varphi_i\})$. Bilden die Ideale $\{a_1^*,...,a_{h^*}^*\}$ ein Vertretersystem von I_{K^*}/H_0, dann werden durch*

$$(A((\prod_j a_i^{*\psi_j})^{-1}b), N(a_i^*)\xi)$$

alle zu $(A(b),\xi)$ über K^* konjugierten prinzipal polarisierten Abelschen Varietäten gegeben.

Wir wollen jetzt die Klassengruppe $I_{K^\bullet}/H_0$ genauer untersuchen:

(1) Wir definieren für ein Ideal $a^* \in I_{K^\bullet}$ durch $\vartheta(a^*) := \prod_j a^{*\psi_j}$ in Prop. 3.6 einen Homomorphismus

$$\vartheta : I_{K^\bullet}/H_{K^\bullet} \longrightarrow c'_K.$$

Es sei I_K^{**} die Gruppe der Ideale $b \in I_K$ der Form $b = \prod_j a^{*\psi_j}$ für ein Ideal $a^* \in I_{K^\bullet}$ und H_K^{**} die Untergruppe der Hauptideale von I_K^{**}. Dann ist $I_K^{**} = \vartheta(I_{K^\bullet})$ gerade das Bild von $I_{K^\bullet}$ unter ϑ. Da nach Proposition 3.6 $b\bar{b} = N_{K^\bullet/\mathbb{Q}}(a^*)$, gibt es ein total positives Element $\beta \in K_0$ mit $(\beta) = b\bar{b}$. Das Element $N(b)(\beta)^{-1}$ ist dann eine total positive Einheit in K_0. Die Gruppe dieser Einheiten $\varepsilon = N(b)(\beta)^{-1}$ für $b \in I_K^{**}$ bezeichnen wir mit U_0.

Falls $b = (\mu) \in H_K$ für ein Element $\mu \in K$, so ist $N(b)(\mu\bar{\mu})^{-1} = N(a^*)(\mu\bar{\mu})^{-1} \in U_0$. Ist a^* ein Ideal aus H_0, so muß $N(a^*)(\mu\bar{\mu})^{-1}$ schon eine Einheit ε_0 von der Form $\varepsilon_0 = \varepsilon\bar{\varepsilon}$ sein, d.h. $N(a^*)(\mu\bar{\mu})^{-1} \in U_1$. Wir können die Idealgruppe H_0 damit auch folgendermaßen beschreiben:

$$H_0 = \{a^* \in I_{K^\bullet} | \prod_j a^{*\psi_j} = (\mu) \in H_K \text{ und } N(a^*)(\mu\bar{\mu})^{-1} \in U_1\}.$$

Dann ist

$$H_{0K}^{**} := \vartheta(H_0) = \{b = (\mu) \in H_K | \exists a^* \in I_{K^\bullet} \text{ mit } b = \prod_j a^{*\psi_j} \text{ und } N(b)(\mu\bar{\mu})^{-1} \in U_1\},$$

oder anders geschrieben

$$H_{0K}^{**} = \{b \in I_K^{**} | b = (\mu) \in H_K \text{ und } N(b)(\mu\bar{\mu})^{-1} \in U_1\}$$

eine Untergruppe von I_K^{**}. Damit ist nach Konstruktion die induzierte Abbildung

$$\vartheta : I_{K^\bullet}/H_0 \longrightarrow I_K^{**}/H_{0K}^{**}$$

ein Isomorphismus, also

$$I_{K^\bullet}/H_0 \cong I_K^{**}/H_{0K}^{**}. \qquad (i)$$

Mit diesen Bezeichnungen werden wir nun den folgenden wichtigen Satz zeigen.

Satz 3.25 *Die folgenden Gruppen sind isomorph:*

$$I_{K^*}/H_0 \cong I_K^{**}/H_K^{**} \times U_0/U_1.$$

Da U_0/U_1 eine Untergruppe von U/U_1 und I_K^{**}/H_K^{**} von c'_K ist, gilt:

$$I_K^{**}/H_K^{**} \times U_0/U_1 \subset c'_K \times U/U_1.$$

Mit Satz 3.23 haben wir : $|Gal(k_0^*/K^*)| = |I_{K^*}/H_0| = |U_0/U_1| \cdot |I_K^{**}/H_K^{**}| =: d_0 \cdot h_0$ teilt die Zahl $|U/U_1| \cdot |c'_K| = d \cdot h'$. Das heißt, die Anzahl d_0h_0 der über K^* konjugierten polarisierten Abelschen Varietäten ist ein Teiler der Anzahl dh' aller nicht isomorphen prinzipal polarisierten Abelschen Varietäten vom gegebenen CM-Typ (K, Φ).

Beweis: Wegen (i) genügt es, die Isomorphie von I_K^{**}/H_{0K}^{**} und $I_K^{**}/H_K^{**} \times U_0/U_1$ zu zeigen. Wir sahen unter (1), daß es für jedes Ideal $\mathfrak{b} \in I_K^{**}$ ein total positives Element $\beta \in K_0$ mit $(\beta) = \mathfrak{b}\bar{\mathfrak{b}}$ und $N(\mathfrak{b})(\beta)^{-1} \in U_0$ gibt. Nach Konstruktion liegt $\mathfrak{b}$ genau dann in H_{0K}^{**}, wenn $\mathfrak{b} \in H_K^{**}$ und $N(\mathfrak{b})(\beta)^{-1}$ in U_1 ist. So können wir durch $\delta(\mathfrak{b}) := (\mathfrak{b}\ ,\ N(\mathfrak{b})(\beta)^{-1})$ einen injektiven Homomorphismus δ zwischen den Gruppen

$$\delta : I_K^{**}/H_{0K}^{**} \longrightarrow I_K^{**}/H_K^{**} \times U_0/U_1$$

definieren. Die Abbildung ist surjektiv, da, wie wir nun zeigen werden, die Mengen dieselbe Ordnung haben.

Es sei $(A(\mathfrak{b}), \xi)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ $(K, \{\varphi_i\})$. Bezeichne nun $h_0 = |I_K^{**}/H_K^{**}|$ die Anzahl der Idealklassen von K, die Ideale der Form $\prod_j \mathfrak{a}^{*\psi_j}$ mit $\mathfrak{a}^* \in I_{K^*}$ enthalten. Dann gibt es genau h_0 konjugierte Abelsche Varietäten A^σ von A über K^*, die zueinander nicht isomorph sind. $A^{\sigma(\mathfrak{a}^*)}$ ist eine $(\prod_j \mathfrak{a}^{*\psi_j})$-Transformation von A. $A^{\sigma(\mathfrak{a}^*)}$ ist isomorph zu A, falls das Ideal $(\prod_j \mathfrak{a}^{*\psi_j})$ ein Hauptideal (μ) in K ist. Dann ist $N(\mathfrak{a}^*)(\mu\bar{\mu})^{-1}$ eine total positive Einheit $\varepsilon \in U_0$ von K_0. Jetzt sind die prinzipal polarisierten Abelschen Varietäten isomorph, wenn ε in U_1 liegt. Dann definieren wir $d_0 = |U_0 : U_1|$ und sehen, daß es genau d_0h_0 über K^* konjugierte nicht isomorphe prinzipal polarisierte Abelsche Varietäten gibt, was zu beweisen war. □

Shimura zeigte [S-T] Kapitel 4, daß für $|K:\mathbb{Q}| = 4$ und $K/\mathbb{Q}$ nicht galoisch mit Klassenzahl $|c_K| = h \equiv 1 \bmod 2$ die Ordnungen der Klassengruppen h_0 und h' gleich sind. Ist die Norm der Fundamentaleinheit von K_0 negativ, so werden wir sehen, daß die Gruppen U und U_1 gleich sind. Damit ist $d = d_0 = 1$ und die Gleichheit von $d_0 h_0$ und dh' in diesem Fall gezeigt.

(2) Es sei $(A(a), \xi)$ eine prinzipal polarisierte Abelsche Varietät vom CM-Typ (K, Φ). Dann gibt es eine von dem Ideal a, der Polarisierung ξ und dem Typ Φ abhängige Matrix Ω_ξ^Φ in der n-dimensionalen oberen Siegelschen Halbebene $\mathcal{H}_n$, so daß

$$(A(a), \xi) \cong \mathbb{C}^n / \mathbb{Z}^n \Omega_\xi^\Phi + \mathbb{Z}^n.$$

Der Modulkörper kann in diesem Fall durch bestimmte Siegelsche Modulfunktionen j ausgewertet an der Periodenmatrix Ω_ξ^Φ über $\mathbb{Q}$ erzeugt werden.

Für $n = 2$ können diese Modulfunktionen durch die zugehörigen zweidimensionalen Thetanullwerte erzeugt werden. Wir werden in Kapitel 5 darauf genauer eingehen. Im nächsten Abschnitt werden wir für diesen Fall für die Gruppe $c'_K \times U/U_1$ explizit ein Vertretersystem konstruieren.

Kapitel 4

Explizite Konstruktion für Dimension 2

In diesem Kapitel wollen wir einen

1. O_K-geeigneten CM-Typ $(K, \{1, \varphi\})$ mit $|K : \mathbb{Q}| = 4$ explizit bestimmen,
2. prinzipale Polarisierungen zu diesem Typ konstruieren,
3. ein Repräsentantensystem für die Isomorphieklassen der prinzipal polarisierten Abelschen Varietäten von diesem Typ angeben,
4. die zugehörigen Periodenmatrizen $\Omega \in \mathcal{H}_2$ berechnen und
5. die Thetafunktionen an ihnen auswerten.

4.1 Konstruktion der prinzipalen Polarisierung

(I) Konstruktion eines geeigneten CM-Typs $(K, \{1, \varphi\})$.

Proposition 4.1 *Sei $K_0 = \mathbb{Q}(\sqrt{D})$ für ein quadratfreies $D > 0$ ein quadratischer Zahlkörper mit Klassenzahl $|c_{K_0}| = 1$ und K über K_0 eine total imaginärquadratische Erweiterung. Dann gibt es eine Zahl $\omega > 0$ mit $O_{K_0} = \mathbb{Z} + \omega\mathbb{Z}$ und eine Zahl η mit $Im(\eta) > 0$ und $O_K = O_{K_0} + \eta O_{K_0}$. Es sei φ die Einbettung von K nach $\mathbb{C}$ mit $Im(\eta^\varphi) < 0$, die nicht gleich der komplexen Konjugation ρ ist. Dann ist die Differente δ von K über $\mathbb{Q}$ ein Hauptideal (γ) in K und $(K, \{1, \varphi\})$ ein geeigneter CM-Typ.*

Beweis: Da K ein CM-Körper ist, haben wir $K = K_0(\eta)$ und $-Im(\eta)^2 >> 0$. Es sei δ_0 die Differente von K_0 über $\mathbb{Q}$ und δ_1 die Differente von K über K_0. Wir haben dann $\delta = \delta_0 \cdot \delta_1$. Das Ideal δ_1 wird von den Elementen der Form $o - \bar{o}$ mit $o \in O_K$ erzeugt, damit ist $\delta_1 = (\eta - \bar{\eta})$. Analog haben wir $\delta_2 = (\omega - \omega^\varphi)$. Definieren wir nun

$$\gamma := -(\eta - \bar{\eta})(\omega - \omega^\varphi) \in K,$$

so ist $(\gamma) = \delta$ und $\gamma = -2iIm(\eta)(\omega - \omega^\varphi)$ rein imaginär und negativ. Außerdem ist $\gamma^\varphi = -2iIm(\eta^\varphi)(\omega^\varphi - \omega) = 2iIm(\eta^\varphi)(\omega - \omega^\varphi) < 0$, so daß das Element $\xi := \gamma^{-1}$ nach 3.15 eine prinzipale Polarisierung auf $A(O_K)$ definiert. Damit ist der CM-Typ $(K, \{1, \varphi\})$ geeignet. □

Für jedes Ideal a einer Idealklasse von c'_K gibt es ein total positives Element α in K_0 mit $a\bar{a} = (\alpha)$. Nach Satz 3.21 definiert dann das Element $\xi := (\gamma\alpha)^{-1}$ eine prinzipale Polarisierung auf $A(a)$ vom CM-Typ $(K, \{1, \varphi\})$.

(II) Konstruktion von prinzipal polarisierten Abelschen Varietäten.

Satz 4.2 *Sei $(K, \{1, \varphi\})$ der in Proposition 4.1 konstruierte geeignete CM-Typ. Dann gibt es in jeder Idealklasse von c'_K ein Ideal a_τ der Form $a_\tau = O_{K_0} + \tau O_{K_0}$ mit $Im(\tau) > 0$ und $Im(\tau^\varphi) < 0$. Es ist weiterhin $a_\tau \bar{a}_\tau = (\alpha_\tau)$ für das total positive Element*

$$\alpha_\tau := \frac{\tau - \bar{\tau}}{\eta - \bar{\eta}} = \frac{Im(\tau)}{Im(\eta)}$$

und das Element

$$\xi_\tau := -((\tau - \bar{\tau})(\omega - \omega^\varphi))^{-1}$$

definiert eine prinzipale Polarisierung C_τ auf $A(a_\tau)$ vom CM-Typ $(K, \{1, \varphi\})$.

Wir bezeichnen mit $\boldsymbol{A(\tau)}$ die so definierte prinzipal polarisierte Abelsche Varietät $(A(a_\tau), \xi_\tau))$ vom CM-Typ $(K, \{1, \varphi\})$. Damit wir den Typ der Varietät festlegen, ordnen wir jeder prinzipal polarisierten Abelschen Varietät $A(\tau)$ vom CM-Typ $(K, \{1, \varphi\})$ das zugehörige Zahlenpaar (τ, τ^φ) mit $Im(\tau) > 0$ und $Im(\tau^\varphi) < 0$ zu.

Beweis: Sei nun a ganzes Ideal in c'_K, so gibt es ganze Zahlen $\alpha, \beta, \gamma, \delta \in O_{K_0}$ mit

$$a = (\alpha\eta + \beta)O_{K_0} + (\gamma\eta + \delta)O_{K_0}.$$

Da $a\bar{a} = (\alpha\delta - \beta\gamma)$ und $a \in c'_K$, finden wir eine Relativbasis, so daß $\alpha\delta - \beta\gamma$ total positiv in K_0 ist. Jedem Ideal a aus c'_K ordnen wir so eine Zahl τ zu, und zwar den Quotienten

$$\tau = \frac{\alpha\eta + \beta}{\gamma\eta + \delta} \text{ mit } \alpha\delta - \beta\gamma >> 0 \text{ in } K_0$$

zweier Relativbasiszahlen. Weil $Im(\eta) > 0$ und $Im(\eta^\varphi) < 0$, ist stets $Im(\tau) > 0$ und $Im(\tau^\varphi) < 0$. Für das zu a äquivalente Ideal $a_\tau := O_{K_0} + \tau O_{K_0}$ gilt

$$a_\tau \bar{a}_\tau = \left(\frac{\alpha\delta - \beta\gamma}{N_{K/K_0}(\gamma\eta + \delta)}\right).$$

Da

$$Im(\tau) = Im(\frac{\alpha\eta + \beta}{\gamma\eta + \delta}) = \frac{Im((\alpha\eta + \beta)(\gamma\bar{\eta} + \delta))}{N_{K/K_0}(\gamma\eta + \delta)} = Im(\eta)\frac{\alpha\delta - \beta\gamma}{N_{K/K_0}(\gamma\eta + \delta)},$$

ist für $\alpha_\tau := \frac{Im(\tau)}{Im(\eta)}$ die Relativnorm $a_\tau \bar{a}_\tau = (\alpha_\tau)$. Nach Definition von η und τ ist das Element α_τ total positiv, so daß das Element

$$\xi_\tau := (\gamma\alpha_\tau)^{-1} = (\gamma\frac{Im(\tau)}{Im(\eta)})^{-1} = -((\tau - \bar{\tau})(\omega - \omega^\varphi))^{-1}$$

nach Satz 3.21 eine prinzipale Polarisierung $C_\tau := C_{\xi_\tau}$ vom CM-Typ $(K, \{1, \varphi\})$ auf der Abelschen Varietät $A(a_\tau)$ definiert. □

Wir wollen nun untersuchen, wann zwei so definierte prinzipal polarisierte Abelsche Varietäten $A(\tau)$, $A(\tau')$ vom selben CM-Typ isomorph sind. Wir können die Isomorphismen zwischen prinzipal polarisierten Abelschen Varietäten vom selben Typ $(K, \{1, \varphi\})$ über die zugehörigen Zahlenpaare (τ, τ^φ), (τ', τ'^φ) beschreiben.

Nach Proposition 3.10 sind zwei Abelsche Varietäten $A(a_\tau)$ und $A(a_{\tau'})$ genau dann isomorph, wenn die Ideale a_τ und $a_{\tau'}$ äquivalent sind. Das heißt, wenn es ganze Zahlen $\alpha, \beta, \gamma, \delta \in O_{K_0}$ gibt mit

$$\tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta} \text{ und } \tau'^\varphi = \frac{\alpha^\varphi\tau^\varphi + \beta^\varphi}{\gamma^\varphi\tau^\varphi + \delta^\varphi},$$

deren Determinante $\alpha\delta - \beta\gamma$ wegen des festgelegten Vorzeichens der Imaginärteile eine total positive Einheit ist.

Für die zugehörigen Polarisierungen gilt nach Definition in Satz 4.2

$$\xi_{\tau'}\,\xi_{\tau}^{-1} = \frac{N_{K/K_0}(\gamma\tau+\delta)}{\alpha\delta-\beta\gamma}.(*)$$

Nun sind nach Satz 3.19 die prinzipal polarisierten Abelschen Varietäten $A(\tau)$ und $A(\tau')$ isomorph, wenn es ein Element μ in K mit $\xi_{\tau'} = \xi_{\tau}\mu\bar{\mu}$ gibt. Diese Gleichung ist wegen $(*)$ genau dann erfüllt, wenn die Determinante $\alpha\delta - \beta\gamma$ schon eine Einheit aus U_1 ist. Wir zeigten damit folgenden Satz:

Satz 4.3 *Es seien $A(\tau)$ und $A(\tau')$ zwei wie in Satz 4.2 definierte prinzipal polarisierte Abelsche Varietäten vom selben CM-Typ $(K,\{1,\varphi\})$. $A(\tau)$ und $A(\tau')$ sind genau dann isomorph, wenn*

$$\tau' = \frac{\alpha\tau+\beta}{\gamma\tau+\delta} \text{ und } \tau'^{\varphi} = \frac{\alpha^{\varphi}\tau^{\varphi}+\beta^{\varphi}}{\gamma^{\varphi}\tau^{\varphi}+\delta^{\varphi}}$$

für $\alpha,\beta,\gamma,\delta \in O_{K_0}$ und $\alpha\delta-\beta\gamma \in U_1$.

Ist $N(\varepsilon_0) = -1$, so ist jede Einheit in U_1 das Quadrat einer anderen Einheit. Also haben wir

$$A(\tau) \cong A(\tau') \Longleftrightarrow \tau' = \frac{\alpha\tau+\beta}{\gamma\tau+\delta} \text{ mit } A := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in PSL_2(O_K).$$

4.2 Konstruktion der Repräsentantensysteme

Als Erstes müssen wir ein Vertretersystem $\mathcal{K}_\Phi = \mathcal{K}_{\{1,\varphi\}}$ **aller** nicht isomorphen prinzipal polarisierten Abelschen Varietäten **vom CM-Typ $(K,\{1,\varphi\})$** bestimmen.

Satz 4.4 *Es sei $(K,\{1,\varphi\})$ der in Proposition 4.1 konstruierte geeignete CM-Typ und $\varepsilon_0 > 0$ eine Fundamentaleinheit von K_0. Weiterhin sei $\{\tau_1,...,\tau_{h'}\}$ ein Repräsentantensystem von c'_K mit $Im(\tau_i) > 0$ und $Im(\tau_i^\varphi) < 0$. Wir setzen*

$$\mathcal{K}_{\{1,\varphi\}} = \{(\tau_i,\tau_i^\varphi) \mid i = 1,\cdots,h'\} \text{ falls } N(\varepsilon_0) = -1 \text{ oder } \varepsilon_0 \in U_1, \text{ d.h. für } d = 1,$$
$$\mathcal{K}_{\{1,\varphi\}} = \{(\tau_i,\tau_i^\varphi),(\varepsilon_0\tau_i,(\varepsilon_0\tau_i)^\varphi \mid i = 1,\cdots,h'\} \text{ sonst, d.h. für } d = 2.$$

*Dann ist $\mathcal{K}_{\{1,\varphi\}}$ ein Repräsentantensystem **aller nicht isomorphen prinzipal polarisierten Abelschen Varietäten** vom CM-Typ $(K,\{1,\varphi\})$.*

Beweis: Jede Einheit ε in K_0 ist von der Form $\varepsilon = \pm\varepsilon_0^n$ mit $n \in \mathbb{N}_0$.

1. **$N(\varepsilon_0) = -1$, damit ist $c'_K = c_K$.**

   In diesem Fall ist jede total positive Einheit $\varepsilon_p \in U$ schon das Quadrat einer anderen Einheit in K_0, so daß

   $$\varepsilon_p = \varepsilon^2 = N_{K/K_0}(\varepsilon) \in U_1 \text{ gilt.}$$

   Damit sind die Gruppen U und U_1 gleich, also $d = 1$. Das heißt, daß wir zu jeder Abelschen Varietät $A(a_{\tau_i})$ keine weitere zu $\xi_i := \xi_{\tau_i} = -((\tau_i - \bar{\tau_i})(\omega - \omega^\varphi))^{-1}$ **nicht isomorphe prinzipale Polarisierung** vom selben Typ finden. Damit ist

   $$\mathcal{K}_\Phi = \mathcal{K}_{\{1,\varphi\}} := \{(\tau_i,\tau_i^\varphi) \mid i = 1,\cdots,h'\}.$$

2. **$N(\varepsilon_0) = 1$**, dann ist $|c'_K/c_K| \leq 2$.

   Da alle Einheiten aus U der Form $\varepsilon = \varepsilon^n$ mit n gerade schon in U_1 liegen, ist $d = |U/U_1|$ stets kleiner gleich 2.

   (a) d ist genau dann gleich 1, wenn $\varepsilon_0 = \varepsilon\bar{\varepsilon}$ für eine Einheit $\varepsilon \in K$. Wir können $\mathcal{K}_\Phi = \mathcal{K}_{\{1,\varphi\}}$ wie im ersten Fall definieren.

(b) Ist Fall (a) nicht erfüllt, so definiert das Element $\varepsilon_0\xi_i$ eine zu C_{ξ_i} **nicht isomorphe** prinzipale Polarisierung auf der Abelschen Varietät $A(a_{\tau_i})$ vom selben Typ. Damit ist

$$\mathcal{K}_\Phi = \mathcal{K}_{\{1,\varphi\}} := \{(\tau_i, \tau_i^\varphi), (\varepsilon_0\tau_i, (\varepsilon_0\tau_i)^\varphi) \mid i = 1, \cdots, h'\}.$$

Als Zweites müssen wir ein Vertretersystem $\mathcal{K}'_\Phi = \mathcal{K}_{\{1,\bar{\varphi}\}}$ **aller** nicht isomorphen prinzipal polarisierten Abelschen Varietäten **vom CM-Typ $(K, \{1, \bar{\varphi}\})$** konstruieren.

Satz 4.5 *Es sei $(K, \{1, \varphi\})$ der in Proposition 4.1 konstruierte geeignete CM-Typ und $\varepsilon_0 > 0$ eine Fundamentaleinheit von K_0. Es sei $\{\tau_1, ..., \tau_{h'}\}$ ein Repräsentantensystem von c'_K mit $Im(\tau_i) > 0$ und $Im(\tau_i^\varphi) < 0$. Für $h'_2 := |c_K/c'_K| = 2$ bezeichne $\{\tau'_1, ..., \tau'_{h'}\}$ ein Vertretersystem von $c'_K - c_K$ mit $Im(\tau'_i) > 0$ und $Im(\tau_i'^{\bar{\varphi}}) < 0$. Wir setzen*

$$\begin{aligned}
\mathcal{K}_{\{1,\bar{\varphi}\}} &= \{(\varepsilon_0\tau_i, (\varepsilon_0\tau_i)^{\bar{\varphi}}) \mid i = 1, \cdots, h'\} \text{ falls } N(\varepsilon_0) = -1, \\
\mathcal{K}_{\{1,\bar{\varphi}\}} &= \{(\tau'_i, \tau_i'^{\bar{\varphi}}) \mid i = 1, \cdots, h'\} \text{ falls } h'_2 = 2, d = 1, \\
\mathcal{K}_{\{1,\bar{\varphi}\}} &= \{(\tau'_i, \tau_i'^{\bar{\varphi}}), (\varepsilon_0\tau'_i, (\varepsilon_0\tau'_i)^{\bar{\varphi}}) \mid i = 1, \cdots, h'\} \text{ falls } h'_2 = 2, d = 2, \\
\mathcal{K}_{\{1,\bar{\varphi}\}} &= \{\,\} \text{ falls } h'_2 = 1.
\end{aligned}$$

Dann ist $\mathcal{K}_{\{1,\bar{\varphi}\}}$ ein Repräsentantensystem aller nicht isomorphen prinzipal polarisierten Abelschen Varietäten vom CM-Typ $(K, \{1, \bar{\varphi}\})$.

Beweis:

1. $N(\varepsilon_0) = -1$

   Es ist $\varepsilon_0 > 0$ und $\varepsilon_0^\varphi < 0$, außerdem für $\xi_i := \xi_{\tau_i}$ ist $Im(\xi_i) > 0$, $Im(\xi_i)^\varphi > 0$, also $Im(\xi_i)^{\bar{\varphi}} < 0$. Multiplizieren wir ξ_i mit ε_0, so gilt $Im(\varepsilon_0\xi_i) > 0$, und $Im(\varepsilon_0\xi_i)^{\bar{\varphi}} > 0$. Damit ist

   $$\begin{aligned}
   \mathcal{K}_{\Phi'} = \mathcal{K}_{\{1,\bar{\varphi}\}} &= \{(A(a_{\tau_i}), \varepsilon_0\xi_i) \mid i = 1, \cdots, h'\} \\
   &= \{(\varepsilon_0\tau_i, (\varepsilon_0\tau_i)^{\bar{\varphi}}) \mid i = 1, \cdots, h'\}
   \end{aligned}$$

   ein Vertretersystem **aller nicht isomorphen prinzipal polarisierten Abelschen Varietäten vom CM-Typ $(K, \{1, \bar{\varphi}\})$.**

2. $N(\varepsilon_0) = 1 \Longrightarrow |c_K : c'_K| \leq 2$

In diesem Fall ist die obige Konstruktion nicht möglich. Der CM-Typ $(K, \{1, \bar{\varphi}\})$ ist nicht O_K geeignet. Das heißt, es gibt keine prinzipale Polarisierung C_ξ auf $A(O_K)$ vom CM-Typ $(K, \{1, \bar{\varphi}\})$.

(a) Falls $c_K = c'_K$, so gibt es auch kein anderes Ideal a in c_K, so daß es zu $A(a)$ eine prinzipale Polarisierung vom CM-Typ $(K, \{1, \bar{\varphi}\})$ gibt.

(b) Anderenfalls ist $|c_K/c'_K| = 2$. Es sei nun $\{\tau'_1, ..., \tau'_{h'}\}$ ein Vertretersystem von $c'_K - c_K$ mit $Im(\tau'_i) > 0$ und $Im(\tau_i'^{\bar{\varphi}}) < 0$. Dieses gibt es, weil für das Element $\alpha_i := \frac{Im(\tau'_i)}{Im(\eta)} > 0$ wegen $a_{\tau'_i}\bar{a}_{\tau'_i} = (\alpha_i)$ und $a_{\tau'_i} \notin c'_K$ gilt:

$$\alpha_i^{\bar{\varphi}} < 0, \text{ also } Im(\tau_i'^{\bar{\varphi}}) < 0.$$

In diesem Fall ist $\gamma < 0$ und $\gamma^{\bar{\varphi}} > 0$, so daß wieder nach 3.21 $\xi_i := (\gamma\alpha'_i)^{-1}$, d.h.

$$\xi_i = -((\tau'_i - \bar{\tau}'_i)(\omega - \omega^{\varphi}))^{-1},$$

eine prinzipale Polarisierung auf $A(a_{\tau'_i})$ definiert. Dann ist

$$\begin{aligned}
\mathcal{K}_{\Phi'} &= \mathcal{K}_{\{1,\bar{\varphi}\}} = \{(A(a_{\tau'_i}), \xi_i) \mid i = 1, \cdots, h'\} \\
&= \{(\tau'_i, \tau_i'^{\bar{\varphi}}) \mid i = 1, \cdots, h'\} \text{ falls } \varepsilon_0 \in U_1 \\
\mathcal{K}_{\Phi'} &= \mathcal{K}_{\{1,\bar{\varphi}\}} = \{(A(a_{\tau'_i}), \xi_i), (A(a_{\tau'_i}), \varepsilon_0\xi_i) \mid i = 1, \cdots, h'\} \\
&= \{(\tau'_i, \tau_i'^{\bar{\varphi}}), (\varepsilon_0\tau'_i, (\varepsilon_0\tau'_i)^{\bar{\varphi}}) \mid i = 1, \cdots, h'\} \text{ falls } \varepsilon_0 \notin U_1
\end{aligned}$$

ein Vertretersystem von **nicht isomorphen prinzipal polarisierten Abelschen Varietäten vom CM-Typ $(K, \{1, \bar{\varphi}\})$.** □

Unser Ziel besteht darin, ein Vertretersystem aller nicht isomorphen prinzipal polarisierten Abelschen Varietäten A mit $End(A) = O_K$ konstruieren, d.h. unabhängig von der Wahl des Typs und damit unabhängig von der Wahl der Einbettungen. Hierzu müssen wir für alle CM-Typen die zugehörigen Repräsentantensysteme konstruieren. Wir haben für den Körper K insgesamt vier verschiedene CM-Typen

$$(K,\{1,\varphi\}),\ (K,\{1,\bar{\varphi}\}),\ (K,\{\rho,\varphi\}),\ (K,\{\rho,\bar{\varphi}\}),$$

die wir mit (K,Φ), (K,Φ'), $(K,\bar{\Phi})$, $(K,\bar{\Phi}')$ bezeichnen. Ist a_i in c'_K, so liegt auch das komplex konjugierte Ideal $\bar{a}_i$ in c'_K, also $\bar{a}_i = a_j$ für ein $j \in \{1,\cdots,h'\}$. Die Menge der Isomorphieklassen von Abelschen Varietäten $A(a_i)$ vom Typ (K,Φ) und vom CM-Typ $(K,\bar{\Phi})$ sind gleich. Nach Definition der Riemannform sind damit auch die Mengen der Isomorphieklassen von prinzipal polarisierten Abelschen Varietäten vom CM-Typ (K,Φ) und vom CM-Typ $(K,\bar{\Phi})$ gleich.
Außerdem gilt $\Phi(a) = \{(\alpha,\alpha^{\varphi}) \mid \alpha \in a\}$ und $\Phi'(a) = \{(\alpha,\bar{\alpha}^{\varphi}) \mid \alpha \in a\}$. Definieren wir $\beta := \alpha^{\varphi} \in a^{\varphi} =: b \in c'_K$, so ist $\Phi'(b) = \{(\beta,\bar{\beta}^{\varphi}) \mid \beta \in b\} = \{(\alpha^{\varphi},\bar{\alpha}^{\varphi^2}) \mid \alpha \in a\}$. Falls $K/\mathbb{Q}$ galoisch mit zyklischer Galoisgruppe, haben wir

$$\alpha^{\varphi^2} = \bar{\alpha},\ \text{so daß}\ \Phi'(b) = \{(\alpha^{\varphi},\alpha) \mid \alpha \in a\}.$$

Damit sind natürlich die Gitter $\Phi(a)$ und $\Phi'(b)$ äquivalent. Also sind auch die Mengen der Isomorphieklassen von Abelschen Varietäten $A(a_i)$ vom Typ $(K,\{1,\varphi\})$ und Typ $(K,\{1,\bar{\varphi}\})$ gleich. Hiermit zeigten wir:

Proposition 4.6 *Die Repräsentantensysteme $\mathcal{K}$ aller nicht isomorphen prinzipal polarisierten Abelschen Varietäten der folgenden CM-Typen sind gleich:*

1. $\mathcal{K}_{\Phi} = \mathcal{K}_{\bar{\Phi}}$ *und* $\mathcal{K}_{\Phi'} = \mathcal{K}_{\bar{\Phi}'}$.

2. *Falls $K/\mathbb{Q}$ galoisch mit zyklischer Galoisgruppe ist* $\mathcal{K}_{\Phi} = \mathcal{K}_{\Phi'}$ *und* $\mathcal{K}_{\bar{\Phi}} = \mathcal{K}_{\bar{\Phi}'}$.

In diesem Abschnitt haben wir zusammengefaßt den folgenden Satz gezeigt:

Satz 4.7 *Es sei $(K,\{1,\varphi\})$ der in Proposition 4.1 konstruierte geeignete CM-Typ und $\varepsilon_0 > 0$ eine Fundamentaleinheit von K_0. Weiterhin sei $\{\tau_1,...,\tau_{h'}\}$ ein Repräsentantensystem von c'_K mit $Im(\tau_i) > 0$ und $Im(\tau_i^\varphi) < 0$. Falls $h'_2 := |c_K/c'_K| = 2$ sei $\{\tau'_1,...,\tau'_{h'}\}$ ein Vertretersystem von $c'_K - c_K$ mit $Im(\tau'_i) > 0$ und $Im(\tau_i'^{\bar\varphi}) < 0$. Dann ist*

$$\begin{aligned}
\mathcal{K}_{\{1,\varphi\}} &= \{(\tau_i,\tau_i^\varphi) \mid i=1,\cdots,h'\} \text{ falls } N(\varepsilon_0)=-1 \text{ oder } \varepsilon_0 \in U_1,\ d.h.d=1,\\
\mathcal{K}_{\{1,\varphi\}} &= \{(\tau_i,\tau_i^\varphi),(\varepsilon_0\tau_i,(\varepsilon_0\tau_i)^\varphi \mid i=1,\cdots,h'\} \text{ für } d=2.
\end{aligned}$$

$$\begin{aligned}
\mathcal{K}_{\{1,\bar\varphi\}} &= \{(\varepsilon_0\tau_i,(\varepsilon_0\tau_i)^{\bar\varphi}) \mid i=1,\cdots,h'\} \text{ falls } N(\varepsilon_0)=-1,\\
\mathcal{K}_{\{1,\bar\varphi\}} &= \{(\tau'_i,\tau_i'^{\bar\varphi}) \mid i=1,\cdots,h'\} \text{ falls } h'_2=2, d=1,\\
\mathcal{K}_{\{1,\bar\varphi\}} &= \{(\tau'_i,\tau_i'^{\bar\varphi}),(\varepsilon_0\tau'_i,(\varepsilon_0\tau'_i)^{\bar\varphi}) \mid i=1,\cdots,h'\} \text{ falls } h'_2=2, d=2,\\
\mathcal{K}_{\{1,\bar\varphi\}} &= \{\,\} \text{ falls } h'_2=1.
\end{aligned}$$

1. $\mathcal{K} := \mathcal{K}_{\{1,\varphi\}}$, *falls $K/\mathbb{Q}$ galoisch und $Gal(K/\mathbb{Q})$ zyklisch.*
2. $\mathcal{K} := \mathcal{K}_{\{1,\varphi\}} \cup \mathcal{K}_{\{1,\bar\varphi\}}$ *sonst.*

Dann ist $\mathcal{K}$ ein Repräsentantensystem aller prinzipal polarisierten Abelschen Varietäten mit Endomorphismenring O_K. Ist K primitiv, so sind diese prinzipal polarisierten Abelschen Varietäten die Jacobischen Varietäten von Kurven vom Geschlecht 2.

4.3 Konstruktion der Periodenmatrix

Es sei wieder $(K, \{1, \varphi\}) = (K, \Phi)$ der in Proposition 4.1 konstruierte geeignete CM-Typ und $a_\tau = O_{K_0} + \tau O_{K_0}$ ein Ideal in K mit $\tau = \frac{\alpha\eta+\beta}{\gamma\eta+\delta}$, wobei $Im(\tau) > 0$ und $Im(\tau^\varphi) < 0$. Wir zeigten Satz in 4.2, daß das Element ξ_τ eine prinzipale Polarisierung auf $A(a_\tau)$ vom CM-Typ (K, Φ) definiert. Nach Abschnitt 3.2 gibt es dann eine $\mathbb{Z}$-Basis $\alpha_1, \cdots, \alpha_4$ von a_τ, so daß

$$E_{\xi_\tau}(\Phi(\alpha_i), \Phi(\alpha_j)) = \begin{pmatrix} & 0 & & 1 \\ & & & 1 \\ -1 & & & \\ & -1 & & 0 \end{pmatrix}.$$

Die Elemente $\tau\omega, \tau, 1, -\omega^\varphi$ bilden offensichtlich eine $\mathbb{Z}$-Basis von a_τ. Wir werden nun zeigen, daß diese Basis die symplektische Basis aus Abschnitt 3.2 ist. Wir erhalten durch

$$\Phi(a_\tau) = \left\langle \begin{matrix} \tau\omega & \tau & 1 & -\omega^\varphi \\ \tau^\varphi\omega^\varphi & \tau^\varphi & 1 & -\omega \end{matrix} \right\rangle$$

ein Gitter in $\mathbb{C}^2$. Definieren wir zwei quadratische Matrizen

$$\mathcal{A}_1 := \begin{pmatrix} \tau\omega & \tau \\ \tau^\varphi\omega^\varphi & \tau^\varphi \end{pmatrix} \text{ und } \mathcal{A}_2 := \begin{pmatrix} 1 & -\omega^\varphi \\ 1 & -\omega \end{pmatrix},$$

so ist $\Phi(a_\tau) = \mathcal{A}_1\mathbb{Z}^2 + \mathcal{A}_2\mathbb{Z}^2$. Nach Konstruktion ist $\xi_\tau \cdot (\tau - \bar{\tau}) = -(\omega - \omega^\varphi)^{-1}$ und $\xi_\tau^\varphi \cdot (\tau^\varphi - \bar{\tau}^\varphi) = (\omega - \omega^\varphi)^{-1}$. Damit erhalten wir die folgenden Ergebnisse:

$$E_{\xi_\tau}(\Phi(\alpha_1), \Phi(\alpha_3)) = \xi_\tau\omega(\bar{\tau} - \tau) + \xi_\tau^\varphi\omega^\varphi(\bar{\tau}^\varphi - \tau^\varphi) = \frac{\omega - \omega^\varphi}{\omega - \omega^\varphi} = 1,$$

$$E_{\xi_\tau}(\Phi(\alpha_2), \Phi(\alpha_4)) = -\xi_\tau\omega^\varphi(\bar{\tau} - \tau) - \xi_\tau^\varphi\omega(\bar{\tau}^\varphi - \tau^\varphi) = \frac{-\omega^\varphi + \omega}{\omega - \omega^\varphi} = 1,$$

$$E_{\xi_\tau}(\Phi(\alpha_2), \Phi(\alpha_3)) = \xi_\tau(\bar{\tau} - \tau) + \xi_\tau^\varphi(\bar{\tau}^\varphi - \tau^\varphi) = \frac{1 - 1}{\omega - \omega^\varphi} = 0,$$

$$E_{\xi_\tau}(\Phi(\alpha_1), \Phi(\alpha_4)) = -\omega\omega^\varphi\xi_\tau(\bar{\tau} - \tau) - \omega\omega^\varphi\xi_\tau^\varphi(\bar{\tau}^\varphi - \tau^\varphi) = -\omega\omega^\varphi\frac{1 - 1}{\omega - \omega^\varphi} = 0,$$

$$E_{\xi_\tau}(\Phi(\alpha_1), \Phi(\alpha_2)) = E_{\xi_\tau}(\Phi(\alpha_3), \Phi(\alpha_4)) = 0,$$

$$E_{\xi_\tau}(\Phi(\alpha_i), \Phi(\alpha_i)) = 0 \quad \text{und} \quad E_{\xi_\tau}(\Phi(\alpha_i), \Phi(\alpha_j)) = E_{\xi_\tau}(\Phi(\alpha_j), \Phi(\alpha_i)),$$

$$\text{also} \quad E_{\xi_\tau}(\Phi(\alpha_i), \Phi(\alpha_j)) = \begin{pmatrix} 0 & E_2 \\ -E_2 & 0 \end{pmatrix}$$

□

Jetzt können wir die zugehörige Periodenmatrix aus der zweidimensionalen Siegelschen oberen Halbebene bestimmen. Die Gitter

$$\Phi(a_\tau) = \mathcal{A}_1\mathbb{Z}^2 + \mathcal{A}_2\mathbb{Z}^2 \text{ und } \mathcal{A}_2^{-1}\mathcal{A}_1\mathbb{Z}^2 + \mathbb{Z}^2$$

sind äquivalent. Wir invertieren die Matrix $\mathcal{A}_1$ und erhalten

$$\mathcal{A}_1^{-1} = \frac{1}{(\omega - \omega^\varphi)} \begin{pmatrix} \omega & -\omega^\varphi \\ 1 & -1 \end{pmatrix}$$

und damit

$$\Omega_{\tau,\tau^\varphi} := \mathcal{A}_1^{-1}\mathcal{A}_2 = \frac{1}{(\omega - \omega^\varphi)} \begin{pmatrix} (\omega^2\tau - \omega^{\varphi^2}\tau^\varphi) & (\omega\tau - \omega^\varphi\tau^\varphi) \\ (\omega\tau - \omega^\varphi\tau^\varphi) & (\tau - \tau^\varphi) \end{pmatrix}.$$

$\Omega_{\tau,\tau^\varphi}$ ist die Periodenmatrix der prinzipal polarisierten Abelschen Varietät $A(\tau)$ vom CM-Typ $(K, \Phi) = (K, \{1, \varphi\})$. Es ist

$$\begin{aligned} det(Im(\Omega_{\tau,\tau^\varphi})) &= \frac{1}{\omega - \omega^\varphi}(Im(\omega^2\tau - \omega^{\varphi^2}\tau^\varphi)Im(\tau - \tau^\varphi) - Im(\omega\tau - \omega^\varphi\tau^\varphi)^2) \\ &= -Im(\tau\tau^\varphi)(\omega - \omega^\varphi) > 0. \end{aligned}$$

Damit liegt $\Omega_{\tau,\tau^\varphi}$ in $\mathcal{H}_2$ und der folgende Satz gezeigt.

Satz 4.8 *Es sei $(K, \{1, \varphi\})$ ein geeigneter CM-Typ aus 4.1 und $A(\tau) = A(a_\tau, \xi_\tau)$ eine durch Satz 4.2 definierte prinzipal polarisierte Abelsche Varietät vom CM-Typ $(K, \{1, \varphi\})$. Dann ist $A(\tau)$ als prinzipal polarisierte Abelsche Varietät zu $\mathbb{C}^2/\Omega_{\tau,\tau^\varphi}\mathbb{Z}^2 + \mathbb{Z}^2$ isomorph, wobei*

$$\Omega_{\tau,\tau^\varphi} := \frac{1}{(\omega - \omega^\varphi)} \begin{pmatrix} (\omega^2\tau - \omega^{\varphi^2}\tau^\varphi) & (\omega\tau - \omega^\varphi\tau^\varphi) \\ (\omega\tau - \omega^\varphi\tau^\varphi) & (\tau - \tau^\varphi) \end{pmatrix}.$$

Wir werden jetzt für den einfacheren Fall $D \equiv 2,3 \ mod\ 4$ die Isomorphismen genauer beschreiben. Es ist $O_{K_0} = \mathbb{Z} + \sqrt{D}\mathbb{Z}$ und damit

$$\Omega_{\tau,\tau^\varphi} = \frac{1}{2\sqrt{D}} \begin{pmatrix} D(\tau - \tau^\varphi) & \sqrt{D}(\tau + \tau^\varphi) \\ \sqrt{D}(\tau + \tau^\varphi) & (\tau - \tau^\varphi) \end{pmatrix}.$$

Transformieren wir τ durch $\tau' = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$ mit $\alpha, \beta, \gamma, \delta \in O_{K_0}$ und $\alpha\delta - \beta\gamma$ total positiv, so transformiert sich die Periodenmatrix $\Omega_{\tau,\tau^\varphi}$ durch die Matrix

$$M := \begin{pmatrix} a_1 & a_2 D & b_2 D & b_1 \\ a_2 & a_1 & b_1 & b_2 \\ c_2 & c_1 & d_1 & d_2 \\ c_1 & c_2 D & d_2 D & d_1 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

wobei $\alpha = a_1 + a_2\sqrt{D}$, $\beta = b_1 + b_2\sqrt{D}$, $\gamma = c_1 + c_2\sqrt{D}$, $\delta = d_1 + d_2\sqrt{D}$. Es ist

$$\Omega_{\tau',\tau'^\varphi} = M\Omega_{\tau,\tau^\varphi} = \frac{A\Omega_{\tau,\tau^\varphi} + B}{C\Omega_{\tau,\tau^\varphi} + D}.$$

Man kann leicht nachrechnen, daß für $\alpha\delta - \beta\gamma = 1$ die zugehörige Matrix M in $Sp(4,\mathbb{Z})$ liegt. Bekanntlich sind die prinzipal polarisierten Abelschen Varietäten $A(\tau)$ und $A(\tau')$ vom selben Typ (K, Φ) genau dann zueinander isomorph, wenn es eine Matrix $M \in Sp(4,\mathbb{Z})$ gibt, die die zugehörigen Periodenmatrizen durch $\Omega_{\tau',\tau'^\varphi} = M\Omega_{\tau,\tau^\varphi}$ ineinander transformiert. Ist die Norm der Fundamentaleinheit von K_0 negativ, so zeigten wir in Satz 4.3

$$A(\tau') \cong A(\tau) \Longleftrightarrow \exists A \in PSl_2(O_{K_0}) \text{ mit } \tau' = A\tau.$$

Das bedeutet, daß die $PSl_2(O_{K_0})$ Transformationen eindeutig den $Sp(4,\mathbb{Z})$ Transformationen entsprechen.

4.4 Bestimmung der Thetanullwerte

Im fünften Kapitel wird gezeigt, daß die absoluten Invarianten einer prinzipal polarisierten Abelschen Varietät $A(\tau)$ vom CM-Typ $(K, \{1, \varphi\})$ spezielle Siegelsche Modulfunktionen sind, die durch die zugehörigen Thetanullwerte dargestellt werden können. Wir werden in diesem Kapitel angeben, wie man die Thetanullwerte bezüglich dieser CM-Periodenmatrizen $\Omega_{\tau,\tau^\varphi}$ explizit bestimmen kann. E. Hecke untersuchte schon 1912 derartige Reihenentwicklungen [He]. Damit können die absoluten Invarianten einer prinzipal polarisierten Abelschen Varietät $A(\tau)$ analytisch berechnet werden.

Sei $\Omega \in \mathcal{H}_2$ die Periodenmatrix eines Gitters in $\mathbb{C}^2$. Zwei Vektoren $a, b \in \frac{1}{2}\mathbb{Z}^2$, den **Charakterisiken**, ordnen wir eine auf $\mathbb{C}^2$ holomorphe Thetafunktion mit Periodenmatrix Ω,

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} : \mathbb{C}^2 \longrightarrow \mathbb{C},$$

durch

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) := \sum_{n \in \mathbb{Z}^2} exp(\pi(n+a)^t \Omega (n+a) + 2\pi i (n+a)^t (z+b)) \text{ zu.}$$

Die positive Definitheit des Imaginärteils sichert die absolute und auf jeder Teilmenge von $\mathbb{C}^2$ gleichmäßige Konvergenz der Reihe [Mum II].

Man kann weiterhin zeigen, daß auf Grund der Quasiperiodizität der Thetafunktionen die soeben definierten Thetafunktionen schon mit den Charakteristiken $a, b \in \{\frac{1}{2}, 0\}^2$ parametrisiert werden können. Wir haben damit für jede Periodenmatrix 16 Thetafunktionen definiert. Wir sprechen für $z = 0$ von dem zur jeweiligen Charakteristik gehörenden **Thetanullwert**

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (\Omega) := \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (0, \Omega).$$

Für die Definition der Thetafunktion und ihre Eigenschaften vergleiche [Mum II]. Es gilt folgende Proposition:

Proposition 4.9 *Für $a, b \in \frac{1}{2}\mathbb{Z}^2$ gilt :*

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

Damit ist

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (0, \Omega) \neq 0 \Longleftrightarrow 4a^t b \equiv 0 \ mod\ 2.$$

Von den 16 definierten Thetafunktionen sind damit genau 6 ungerade und haben Thetanullwert Null. Wir führen die folgenden Bezeichnungen in Anlehnung an die Bezeichnungsweise von Otto Staude [Sta] ein:

$$v_1 := \vartheta\begin{bmatrix}1&0\\0&0\end{bmatrix},\ v_2 := \vartheta\begin{bmatrix}1&0\\1&0\end{bmatrix},\ v_3 := \vartheta\begin{bmatrix}0&1\\1&0\end{bmatrix},\ v_4 := \vartheta\begin{bmatrix}0&1\\1&1\end{bmatrix}$$

$$v_5 := \vartheta\begin{bmatrix}0&0\\1&1\end{bmatrix},\ v_0 := \vartheta\begin{bmatrix}0&0\\0&0\end{bmatrix},\ v_{45} := \vartheta\begin{bmatrix}0&1\\0&0\end{bmatrix},\ v_{35} := \vartheta\begin{bmatrix}0&1\\0&1\end{bmatrix}$$

$$v_{43} := \vartheta\begin{bmatrix}0&0\\0&1\end{bmatrix},\ v_{21} := \vartheta\begin{bmatrix}0&0\\1&0\end{bmatrix},\ v_{25} := \vartheta\begin{bmatrix}1&0\\0&1\end{bmatrix},\ v_{24} := \vartheta\begin{bmatrix}1&1\\0&1\end{bmatrix}$$

$$v_{13} := \vartheta\begin{bmatrix}1&1\\1&0\end{bmatrix},\ v_{23} := \vartheta\begin{bmatrix}1&1\\0&0\end{bmatrix},\ v_{41} := \vartheta\begin{bmatrix}1&1\\1&1\end{bmatrix},\ v_{51} := \vartheta\begin{bmatrix}1&0\\1&1\end{bmatrix}$$

Mit dieser Bezeichnungsweise sprechen wir von den 10 geraden Thetanullwerten $v_1, v_3, v_5, v_0, v_{45}, v_{43}, v_{21}, v_{25}, v_{23}, v_{41}$. Speziell für die im letzten Abschnitt definierte CM-Periodenmatrix $\Omega = \Omega_{\tau,\tau^\varphi}$ haben wir für $a = (a_1, a_2) = (\frac{a_1'}{2}, \frac{a_2'}{2})$.

$$\begin{aligned}
&(n+a)^t\Omega(n+a) = \\
&= \frac{-\tau^\varphi(\omega^{\varphi^2}(n_1+a_1)^2 + 2\,\omega^\varphi(n_1+a_1)(n_2+a_2) + (n_2+a_2)^2)}{\omega-\omega^\varphi} \\
&\quad + \frac{\tau(\omega^2(n_1+a_1)^2 + 2\,\omega(n_1+a_1)(n_2+a_2) + (n_2+a_2)^2)}{\omega-\omega^\varphi} \\
&= \frac{\tau((n_1+a_1)\omega + (n_2+a_2))^2 - \tau^\varphi((n_1+a_1)\omega^\varphi + (n_2+a_2))^2}{\omega-\omega^\varphi} \\
&= \frac{\tau((2n_1+a_1')\omega + (2n_2+a_2'))^2 - \tau^\varphi((2n_1+a_1')\omega^\varphi + (2n_2+a_2'))^2}{4(\omega-\omega^\varphi)} \\
&= \frac{\tau o^2 - \tau^\varphi o^{\varphi^2}}{4(\omega-\omega^\varphi)} \text{ mit } o \in O_{K_0}, o \equiv a_1'\omega + a_2' \bmod 2
\end{aligned}$$

Setzen wir

$$q := exp(\frac{\pi i \tau}{4(\omega - \omega^\varphi)}) \text{ und } q' := exp(-\frac{\pi i \tau^\varphi}{4(\omega - \omega^\varphi)}),$$

so können wir die Thetanullwerte durch

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (\Omega) = \sum_{o \equiv a_1' \omega + a_2' \, mod 2} \pm q^{o^{\varphi^2}} q'^{o^2}$$

als Potenzreihen über dem Körper K_0 darstellen. Das Vorzeichen ist jeweils positiv oder negativ, je nachdem ob $exp(2\pi i(n+a)^t b)$ gleich 1 oder gleich -1 ist. Dieser Ausdruck ist natürlich gleich 1, falls $2(n+a)^t b \equiv 0 \; mod \; 2$ und anderenfalls -1. Der Übergang zu gewöhnlichen Potenzreihen über $\mathbb{Q}$ ist durch

$$q_1 := qq' = exp(\frac{\pi i(\tau - \tau^\varphi)}{4(\omega - \omega^\varphi)}) \text{ und } q_2 := q^{\omega^\varphi} q'^{\omega} = exp(\frac{\pi i(\omega^\varphi \tau - \omega \tau^\varphi)}{4(\omega - \omega^\varphi)})$$

sofort wieder gegeben. Wir erhalten folgende zweidimensionale q-Entwicklungen:

1. $D \equiv 2, 3 \; mod \; 4$

$$q_1 = exp(\frac{\pi i(\tau - \tau^\varphi)}{8\sqrt{D}}) \text{ und } q_2 = exp(-\frac{\pi i(\tau + \tau^\varphi)}{8})$$

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (\Omega) = \sum_{l=0}^{\infty} \sum_{l = (2n_1 + a_1')^2 D + (2n_2 + a_2')^2} \pm q_1^l q_2^{2(2n_1 + a_1')(2n_2 + a_2')}.$$

2. $D \equiv 1 \; mod \; 4$

$$q_1 = exp(\frac{\pi i(\tau - \tau^\varphi)}{4\sqrt{D}}) \text{ und } q_2 = exp(-\frac{\pi i((\sqrt{D}-1)\tau + (\sqrt{D}+1)\tau^\varphi)}{8\sqrt{D}})$$

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (\Omega) = \sum_{l=0}^{\infty} \sum_{l = (2n_1 + a_1')^2 \frac{D-1}{4} + (2n_2 + a_2')^2} \pm q_1^l q_2^{(2n_1 + a_1')^2 + 2(2n_1 + a_1')(2n_2 + a_2')}.$$

Kapitel 5

Invariantensysteme für Kurven vom Geschlecht 2

5.1 Invariantensysteme über beliebigen Körpern

In diesem Kapitel werden wir ein vollständiges Invariantensystem für eine Kurve vom Geschlecht 2 herleiten. Zur Erforschung dieser Invarianten benutzen wir die Theorie der projektiven Invarianten von Binärformen sechsten Grades. Man vergleiche hierzu insbesondere die Arbeiten von O. Bolza [Bo II] und Igusa [Ig], die wesentliche Aussagen über die Invarianten von Kurven vom Geschlecht 2 liefern. Falls die Kurve C über $\mathbb{C}$ definiert ist, sind die ganzen Invarianten zweidimensionale Siegelsche Modulfunktionen. Bolza zeigte schon 1887 [Bo II], daß sie durch die zugehörigen zehn geraden Thetanullwerte dargestellt werden können. Mit Hilfe dieser Darstellung können wir schließlich das Invariantensystem einer Kurve vom Geschlecht 2, deren Jacobische Varietät von einem gegebenen CM-Typ $(K, \{1, \varphi\})$ ist, über die in Kapitel 4.3 bestimmte Periodenmatrix und in Kapitel 4.4 hergeleiteten Reihenentwicklungen analytisch berechnen.

Es sei C eine über einem algebraisch abgeschlossenen Körper K definierte projektive glatte Kurve vom Geschlecht 2. Igusa zeigte in [Ig] S. 616, daß es für beliebige Charakteristik stets ein affines Modell der Kurve der Form

$$C : XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

mit Koeffizienten $a, b, c, d \in K$ gibt. Als projektive Kurve hat C eine Singularität bei $P_\infty := (0 : 1 : 0)$. Die anderen fünf Weierstraßpunkte der Kurve liefern die Werte von X,

an denen die Gleichung in Y eine doppelte Nullstelle hat. Das sind die Nullstellen $a_1, ..., a_5$ des Polynoms

$$f(x) := (1 + aX + bX^2) + 4X^2(c + dX + X^2).$$

M bezeichne die Menge der sechs Weierstraßpunkte der Kurve $a_1, ..., a_5$ und $a_6 := P_\infty$ aufgefaßt als Punkte in $\mathbb{P}_1(K)$.

Da jede Kurve C vom Geschlecht 2 hyperelliptisch ist, gibt es für $char(K) \neq 2$ ein affines Modell der Kurve der Form $y^2 = f(x)$, wobei $f(x)$ ein normiertes quadratfreies Polynom vom Grad 5 ist. M besteht dann aus einem Punkt $P_\infty := (0 : 1 : 0)$ der zugehörigen projektiven Gleichung und den fünf verschiedenen Nullstellen von $f(x)$.

Zwei Mengen M, M' aus je sechs Punkten in $\mathbb{P}_1(K)$ führen genau dann zu isomorphen Kurven, wenn sie durch einen Automorphismus $s \in PGL_2(K)$ von $\mathbb{P}_1(K)$ ineinander überführt werden können. Das ist genau dann der Fall, wenn die zu M bzw. zu M' zugehörigen Binärformen sechsten Grades $F(x,z) = \prod_{i=1}^{6}(x - a_i z)$ und $F'(x,z) = \prod_{i=1}^{6}(x - a_i' z)$ projektiv äquivalent sind.

Eine **ganze Invariante** von C ist eine Funktion J auf der Menge aller 6–elementigen Teilmengen von $\mathbb{P}_1(K)$, die nur von den $PGL_2(K)$ Bahnen abhängt. Damit ist jede in den a_i symmetrische Funktion der Form

$$I_m := \sum (a_i - a_j)(a_l - a_k) \cdots (a_n - a_p) \text{ mit } i,j,l,k,n,p... \in \{1, ..., 6\},$$

in der jedes a_i für $i = 1, ..., 6$ in jedem Produkt $(a_i - a_j)(a_l - a_k) \cdots (a_n - a_p)$ genau m-mal auftritt, eine ganze Invariante vom Grad m (vgl. [Ig] S. 620). Der Fundamentalsatz über symmetrische Funktionen besagt, daß man die Summanden von I_m als Polynome der Koeffizienten der Kurvengleichung rational darstellen kann.

Kürzen wir $(a_i - a_j)$ durch (ij) ab, so definieren die folgenden Ausdrücke die ganzen Invarianten der Grade 2,4,6,10 einer Kurve C vom Geschlecht 2 (vgl. [Ig] S. 620).

(1) $I_2 = \sum_{15} (12)^2(34)^2(56)^2$

Summiert wird über die Produkte, die man aus $(12)^2(34)^2(56)^2$ durch Operation der 15 Transpositionen-Tripel $(ij)(i'j')(i''j'')$ mit $\{i, j, i', j', i'', j''\} = \{1, 2, 3, 4, 5, 6\}$ erhält.

(2) $I_4 = \sum_{10}(12)^2(23)^2(31)^2\,(45)^2(56)^2(64)^2$

Summiert wird über die Produkte, die man aus $(12)^2(23)^2(31)^2\,(45)^2(56)^2(64)^2$ durch Operation der zehn Paare von 3-er Zykeln $(ijk)(i'j'k')$ mit $\{i,j,k,i',j',k'\} = \{1,2,3,4,5,6\}$ erhält.

(3) $I_6 = \sum_{60}(12)^2(23)^2(31)^2\,(45)^2(56)^2(64)^2\,(14)^2(25)^2(36)^2$

Summiert wird über die Produkte, die man aus
$(12)^2(23)^2(31)^2\,(45)^2(56)^2(64)^2\,(14)^2(25)^2(36)^2$
durch Operation der 60 Permutationen der Form $(ijk)(i'j'k')(il)(jm)(ko)$ mit $\{i,j,k,i',j',k'\} = \{1,2,3,4,5,6\}, \{l,m,o\} = \{i',j',k'\}$ erhält.

(4) $I_{10} = \prod_{i<j}(ij)^2$.

Sei $char(K) \neq 2$ und C eine Kurve vom Geschlecht 2 gegeben durch

$$C : y^2 = x^5 + f_1x^4 + f_2x^3 + f_3x^2 + f_4x + f_5.$$

Es ist $a_6 = P_\infty$, so können wir $(a_i - a_6) = -1$ für alle i setzen. Damit gilt:

1. $I_2 = 6f_2^2 - 16f_1f_3 + 40f_4$
2. $I_4 = 4(f_1^2f_3^2 - 3f_2f_3^2 - 3f_1^2f_2f_4 + 9f_2^2f_4 + f_1f_3f_4 - 20f_4^2 + 12f_1^3f_5 - 45f_1f_2f_5 + 75f_3f_5)$
3. $I_6 = -2(-4f_1^2f_2^2f_3^2 + 12f_2^3f_3^2 + 12f_1^3f_3^3 - 38f_1f_2f_3^3 + 18f_3^4 + 12f_1^2f_2^3f_4 - 36f_2^4f_4 - 38f_1^3f_2f_3f_4 + 119f_1f_2^2f_3f_4 - 14f_1^2f_3^2f_4 - 13f_2f_3^2f_4 + 18f_1^4f_4^2 - 13f_1^2f_2f_4^2 - 88f_2^2f_4^2 - 32f_1f_3f_4^2 + 160f_4^3 - 30f_1^3f_2^2f_5 + 99f_1f_2^3f_5 + 80f_1^4f_3f_5 - 246f_1^2f_2f_3f_5 - 165f_2^2f_3f_5 + 320f_1f_3^2f_5 - 308f_1^3f_4f_5 + 930f_1f_2f_4f_5 - 800f_3f_4f_5 + 450f_1^2f_5^2 - 1125f_2f_5^2)$
4. $I_{10} = f_1^2f_2^2f_3^2f_4^2 - 4f_2^3f_3^2f_4^2 - 4f_1^3f_3^3f_4^2 + 18f_1f_2f_3^3f_4^2 - 27f_3^4f_4^2 - 4f_1^2f_2^3f_4^3 + 16f_2^4f_4^3 + 18f_1^3f_2f_3f_4^3 - 80f_1f_2^2f_3f_4^3 - 6f_1^2f_3^2f_4^3 + 144f_2f_3^2f_4^3 - 27f_1^4f_4^4 + 144f_1^2f_2f_4^4 - 128f_2^2f_4^4 - 192f_1f_3f_4^4 + 256f_4^5 - 4f_1^2f_2^2f_3^3f_5 + 16f_2^3f_3^3f_5 + 16f_1^3f_3^4f_5 - 72f_1f_2f_3^4f_5 + 108f_3^5f_5 + 18f_1^2f_2^3f_3f_4f_5 - 72f_2^4f_3f_4f_5 - 80f_1^3f_2f_3^2f_4f_5 + 356f_1f_2^2f_3^2f_4f_5 + 24f_1^2f_3^3f_4f_5 - 630f_2f_3^3f_4f_5 - 6f_1^3f_2^2f_4^2f_5 + 24f_1f_2^3f_4^2f_5 + 144f_1^4f_3f_4^2f_5 -$

$$746f_1^2f_2f_3f_4^2f_5+560f_2^2f_3f_4^2f_5+1020f_1f_3^2f_4^2f_5-36f_1^3f_4^3f_5+160f_1f_2f_4^3f_5-1600$$
$$f_3f_4^3f_5-27f_1^2f_2^4f_5^2+108f_2^5f_5^2+144f_1^3f_2^2f_3f_5^2-630f_1f_2^3f_3f_5^2-128f_1^4f_3^2f_5^2+$$
$$560f_1^2f_2f_3^2f_5^2+825f_2^2f_3^2f_5^2-900f_1f_3^3f_5^2-192f_1^4f_2f_4f_5^2+1020f_1^2f_2^2f_4f_5^2-900f_2^3f_4f_5^2+$$
$$160f_1^3f_3f_4f_5^2-2050f_1f_2f_3f_4f_5^2+2250f_3^2f_4f_5^2-50f_1^2f_4^2f_5^2+2000f_2f_4^2f_5^2+256f_1^5f_5^3-$$
$$1600f_1^3f_2f_5^3+2250f_1f_2^2f_5^3+2000f_1^2f_3f_5^3-3750f_2f_3f_5^3-2500f_1f_4f_5^3+3125f_5^4$$

Werten wir die ganzen Invarianten $I_2,...,I_{10}$ an dem universellen Modell in den Koeffizienten a,b,c,d aus, so können wir in dem Ausdruck von I_2 die Zahl 2^3, von I_4 die Zahl 2^2, von I_6 die Zahl 2^3 und von I_{10} die Zahl 2^{12} ausklammern. Da demnach alle Invarianten modulo 2 verschwinden, sind diese Invarianten für $char(k)=2$ ungeeignet definiert. Da auch $I_{10}\equiv 0 \bmod 2$ sind keine absoluten Invarianten definierbar. Wir korrigieren die Invarianten um diese Faktoren und erhalten folgende Kongruenzen modulo 2.

$$\begin{aligned}
2^{-3}I_2 &\equiv a^2b^2 \ mod\ 2\\
2^{-2}I_4 &\equiv a^4b^4 \ mod\ 2\\
2^{-3}I_6 &\equiv a^6b^6 \ mod\ 2\\
2^{-12}I_{10} &\equiv 1+ac+bc+a(b+bc+bc+bc)+a(bc+d)+\\
&\quad a^5(1+bc+b^3d+b^4cd)+a^4(b^3+c^2+b^5c^2+b^4d^2)\ mod\ 2.
\end{aligned}$$

Wir definieren uns also neue ganze Invarianten durch

$$J_2:=2^{-3}I_2,\ \ J_4:=2^{-2}I_4,\ \ J_6:=2^{-3}I_6,\ \ J_{10}:=2^{-12}I_{10}.$$

Aus der klassischen Invariantentheorie von Binärformen sechsten Grades folgt (vgl. [Ig] S.622), daß sich jede ganze Invariante vom geraden Grad als Polynom in J_2,J_4,J_6,J_{10} mit rationalen Koeffizienten darstellen läßt. Igusa zeigte in [Ig] S.632 den folgenden Satz:

Satz 5.1 *Zwei Kurven C und C' vom Geschlecht 2 sind genau dann isomorph, wenn es ein $r\in K^*$ gibt, mit $J_{2i}=r^{2i}J'_{2i}$ für $i=1,2,3,5$.*

Der Quotient von ganzen Invarianten gleichen Grades heißt **absolute Invariante** von C. Damit ist jede Funktion j der Form

$$j=J_2^{e_2}J_4^{e_4}J_6^{e_6}J_{10}^{e_{10}} \text{ mit } -5e_{10}=e_2+2e_4+3e_6$$

eine absolute Invariante von C. Da $-5e_{10}=e_2+2e_4+3e_6$ haben wir

$$j=(\frac{J_2^5}{J_{10}})^{e_{10}-e_4-e_6}(\frac{J_2^3J_4}{J_{10}})^{e_4}(\frac{J_2^2J_6}{J_{10}})^{e_6}.$$

Weil die Diskriminainte stets ungleich Null ist, haben wir $J_{10} \neq 0$, so daß diese Quotienten für alle Kurven definiert sind. Für $J_2 \neq 0$ erzeugen die drei absoluten Invarianten

$$j_1 = (\frac{J_2^5}{J_{10}}),\ j_2 = (\frac{J_2^3 J_4}{J_{10}}),\ j_3 = (\frac{J_2^2 J_6}{J_{10}})$$

alle absoluten Invarianten. Für den Sonderfall $J_2 = 0$ führen wir noch drei weitere absolute Invarianten ein.

$$j_4 = (\frac{J_4 J_6}{J_{10}}),\ j_5 = (\frac{J_4^5}{J_{10}^2}),\ j_3 = (\frac{J_6^5}{J_{10}^3}).$$

Damit gilt

Satz 5.2 *Falls J_2' und J_2 ungleich Null sind, so sind die Kurven C und C' genau dann isomorph, wenn die absoluten Invarianten $j_i = j_i'$ für $i = 1,2,3$ gleich sind.*

Beweis: Für $r = \sqrt{J_2(J_2')^{-1}}$ haben wir sofort $J_m = r^m J_m'$ für $m = 2,4,6,10$, so daß der Satz 5.1 die Isomorphie liefert.

Satz 5.3 *Es sei C eine über einem algebraischen Zahlkörper K definierte Kurve vom Geschlecht 2. Die absoluten Invarianten von C sind genau dann ganz, wenn sie überall potentiell gute Reduktion hat.*

Beweisskizze: Bekanntlich findet man immer einen endlichen Erweiterungskörper K' über K und ein Modell C' über K' mit $f'(x)$ in $O_{K'}[x]$. Die ganzen Invarianten von C' sind Polynome in den Koeffizienten a, b, c, d und damit ganzalgebraische Zahlen. Jetzt hat nach Definition C überall potentiell gute Reduktion, wenn C' gute Reduktion modulo jedem Primideal $\mathcal{P}$ hat. Das ist genau dann der Fall, wenn die Diskriminante und damit J_{10} in $O_{K'}^*$ liegt. Also sind die soeben definierten absoluten Invarianten ganz in K' und damit auch ganz in K. Die umgekehrte Richtung ist sehr viel schwieriger zu zeigen, einen Beweis findet man in [Ig] Lemma 5.

Satz 5.4 *Sei C eine Kurve vom Geschlecht 2 mit der Eigenschaft, daß der Endomorphismenring ihrer Jacobischen Varietät J_C dem Ring der ganzen Zahlen eines CM-Körpers vom Grad 4 über $\mathbb{Q}$ entspricht. Das heißt, J_C bzw. C hat komplexe Multiplikation. Dann hat J_C überall potentiell gute Reduktion.*

Beweisskizze: Es sei A eine über einem algebraischen Zahlkörper K definierte Abelschen Varietät, dann gibt es nach dem Satz von Grothendiek (vgl. [B-L-R]) einen endlichen algebraischen Erweiterungkörper L über K und ein semistabiles Modell A' über L. Für ein Primideal $\mathcal{P}$ bezeichne A'_p das reduzierte Gruppenschema und $A'_{0,p}$ das Gruppenschema, daß gleich der Zusammenhangskomponente der Identität von A'_p ist.

Das heißt dann: A' hat entweder gute Reduktion modulo $\mathcal{P}$ oder es gibt einen Torus T, eine Abelsche Varietät B und eine injektive Abbildung

$$i : End(A'_p) \longrightarrow End(A'_{0,p}) \text{ gibt,}$$

so daß die folgende Sequenz exakt ist:

$$0 \longrightarrow T \longrightarrow A'_{0,p} \longrightarrow B_p \longrightarrow 0$$

$$\begin{aligned} \text{Damit gilt: } End(A'_{0,p}) \otimes \mathbb{Q} &\cong End(T) \otimes \mathbb{Q} \oplus End(B_p) \otimes \mathbb{Q} \\ &\cong \mathbb{Q}^{dimT} \oplus End(B_p) \otimes \mathbb{Q} \\ \text{also } Zen(End(A'_{0,p}) \otimes \mathbb{Q}) &\cong \mathbb{Q}^{dimT} \oplus Zen(End(B_p) \otimes \mathbb{Q}) \end{aligned}$$

Für $dimA' = 2$ und $K = Zen(End(A') \otimes \mathbb{Q})$ primitiver CM-Körper gilt :

1. Falls $dim(T) = 2$,d.h. $dim(B_p) = 0$,
   so ist $K = Zen(End(A') \otimes \mathbb{Q}) \subseteq Zen(End(A'_p) \otimes \mathbb{Q})$, wobei $Zen(End(A'_p) \otimes \mathbb{Q})$ injektiv nach $Zen(End(A'_{0,p}) \otimes \mathbb{Q}) = \mathbb{Q}^2$ abgebildet wird.
   Das ist natürlich für $|K : \mathbb{Q}| = 4$ nicht möglich.

2. Falls $dim(T) = 1$,d.h. $dim(B_p) = 1$,
   so kann $K = Zen(End(A') \otimes \mathbb{Q})$ injektiv in einen der beiden Summenden $\mathbb{Q} \oplus Zen(End(B_p) \otimes \mathbb{Q})$ abgebildet werden. Da $dim(B_p) = 1$, ist B_p eine elliptische Kurve, d.h. $Zen(End(B_p) \otimes \mathbb{Q})$ ist ein imaginärquadratischer Zahlkörper $Q(\sqrt{-d})$. Da ein Körper vom Grad 4 über $\mathbb{Q}$ nicht in einen Körper vom Grad 2 über $\mathbb{Q}$ eingebettet werden kann, ist auch $dim(T) = 1$ nicht möglich.

3. Da $dim(T) \leq 2$, folgt $T = 0$.

Damit hat A' gute Reduktion mod $\mathcal{P}$, d.h. A potentiell gute Reduktion mod $\mathcal{P}$. □

Bemerkung 5.5 *Die absoluten Invarianten einer Kurve C vom Geschlecht 2 definiert über einem algebraischen Zahlkörper K mit komplexer Multiplikation sind ganz, wenn für alle Primideale $\mathcal{P}$ die Jacobische Varietät $\bar{J}_C = J_C \bmod \mathcal{P}$ wieder eine prinzipal polarisierte Abelsche Varietät der Dimension 2 ist. Nach dem letzten Satz ist $\bar{J}_C$ eine Abelsche Varietät der Dimension 2. Ist $\bar{J}_C$ für ein Primideal $\mathcal{P}$ nicht prinzipal polarisiert, so ist sie als Abelsche Varietät isomorph zu dem Produkt von zwei elliptischen Kurven [We]. In diesem Fall ist $J_{10} \equiv 0 \bmod \mathcal{P}$ und $\bar{C}$ zerfällt in diese zwei elliptischen Kurven. Sei $\prod \mathcal{P}$ das Produkt über alle solche schlechten Stellen, so liegt J_{10} in $\prod \mathcal{P}$.*

5.2 Invarianten repräsentiert durch Thetanullwerte

Ist eine Kurve C vom Geschlecht 2 über $\mathbb{C}$ definiert, so ist ihre Jacobische Varietät $J_C(\mathbb{C})$ als prinzipal polarisierte Abelsche Varietät isomorph zu dem durch die zugehörige Periodenmatrix $\Omega_C \in \mathcal{H}_2$ definierten Torus

$$J_C(\mathbb{C}) \cong \mathbb{C}^2/\mathbb{Z}^2\Omega_C + \mathbb{Z}^2.$$

Zwei über $\mathbb{C}$ definierte Kurven C, C' vom Geschlecht 2 sind genau dann zueinander isomorph, wenn ihre Jacobischen Varietäten $J_C(\mathbb{C})$ und $J_{C'}(\mathbb{C})$ als prinzipal polarisierte Abelsche Varietäten isomorph sind [We]. Das ist wiederum genau dann der Fall, wenn

$$\Omega_{C'} = M\Omega_C \text{ für } M \in Sp(4,\mathbb{Z}).$$

Die Invarianten von $C/\mathbb{C}$ sind damit zweidimensionale Siegelsche Modulfunktionen. Schon Bolza zeigte 1887 in [Bo II], wie die Invarianten durch die Thetanullwerte der zugehörigen Periodenmatrix dargestellt werden können. Mit den Bezeichnungen aus Kapitel 4.4 und mit Bolzas Aussagen können wir die Darstellungen für unsere ganzen Invarianten entwickeln.

Wir definieren zunächst die folgenden Modulformen der Grade 4,10,12,16:

Definition 5.6 1. $h_4 := \sum_{10} v_\alpha$ *Summation über alle zehn geraden Thetanullwerte*

2. $h_{10} := \prod_{10} v_\alpha$ *Produkt über alle zehn geraden Thetanullwerte*

3. $h_{12} := (v_0v_1v_{21}v_{23}v_{25}v_{41})^4 + (v_0v_{21}v_{23}v_{25}v_3v_{43})^4 + (v_1v_{23}v_{25}v_3v_{41}v_{45})^4$
$+ (v_1v_{21}v_{25}v_3v_{43}v_{45})^4 + (v_0v_1v_{21}v_{41}v_{43}v_{45})^4 + (v_0v_{23}v_3v_{41}v_{43}v_{45})^4$
$+ (v_0v_1v_{21}v_3v_{41}v_5)^4 + (v_0v_1v_{23}v_3v_{43}v_5)^4 + (v_1v_{23}v_{25}v_{41}v_{43}v_5)^4$
$+ (v_{21}v_{25}v_3v_{41}v_{43}v_5)^4 + (v_0v_{21}v_{23}v_{25}v_{45}v_5)^4 + (v_0v_1v_{25}v_3v_{45}v_5)^4$
$+ (v_{21}v_{23}v_3v_{41}v_{45}v_5)^4 + (v_1v_{21}v_{23}v_{43}v_{45}v_5)^4 + (v_0v_{25}v_{41}v_{43}v_{45}v_5)^4$
Summation über die 15 Komplemente der Göpelquadrupel

4. $h_{16} := v_3^2(v_0v_1v_{21}v_{23}v_{25}v_3v_{41})^4 + v_1^2(v_0v_1v_{21}v_{23}v_{25}v_3v_{43})^4 + v_{41}^2(v_0v_{21}v_{23}v_{25}v_3v_{41}v_{43})^4$
$+ v_{43}^2(v_0v_1v_{21}v_{23}v_{25}v_{41}v_{43})^4 + v_0^2(v_0v_1v_{23}v_{25}v_3v_{41}v_{45})^4 + v_{21}^2(v_1v_{21}v_{23}v_{25}v_3v_{41}v_{45})^4$
$+ v_0^2(v_0v_1v_{21}v_{25}v_3v_{43}v_{45})^4 + v_{23}^2(v_1v_{21}v_{23}v_{25}v_3v_{43}v_{45})^4 + v_{23}^2(v_0v_1v_{21}v_{23}v_{41}v_{43}v_{45})^4$
$+ v_{25}^2(v_0v_1v_{21}v_{25}v_{41}v_{43}v_{45})^4 + v_1^2(v_0v_1v_{23}v_3v_{41}v_{43}v_{45})^4 + v_{21}(v_0v_{21}v_{23}v_3v_{41}v_{43}v_{45})^4$
$+ v_{25}^2(v_0v_{23}v_{25}v_3v_{41}v_{43}v_{45})^4 + v_3^2(v_0v_1v_{21}v_3v_{41}v_{43}v_{45})^4 + v_{41}^2(v_1v_{21}v_{25}v_3v_{41}v_{43}v_{45})^4$
$+ v_{43}^2(v_1v_{23}v_{25}v_3v_{41}v_{43}v_{45})^4 + v_{45}^2(v_0v_1v_{21}v_{23}v_{25}v_{41}v_{45})^4 + v_{45}^2(v_0v_{21}v_{23}v_{25}v_3v_{43}v_{45})^4$
$+ v_{23}^2(v_0v_1v_{21}v_{23}v_3v_{41}v_5)^4 + v_{25}^2(v_0v_1v_{21}v_{25}v_3v_{41}v_5)^4 + v_{21}^2(v_0v_1v_{21}v_{23}v_3v_{43}v_5)^4$
$+ v_{25}^2(v_0v_1v_{23}v_{25}v_3v_{43}v_5)^4 + v_0^2(v_0v_1v_{23}v_{25}v_{41}v_{43}v_5)^4 + v_{21}^2(v_1v_{21}v_{23}v_{25}v_{41}v_{43}v_5)^4$
$+ v_0^2(v_0v_{21}v_{25}v_3v_{41}v_{43}v_5)^4 + v_1^2(v_1v_{21}v_{25}v_3v_{41}v_{43}v_5)^4 + v_{23}^2(v_{21}v_{23}v_{25}v_3v_{41}v_{43}v_5)^4$
$+ v_3^2(v_1v_{23}v_{25}v_3v_{41}v_{43}v_5)^4 + v_{41}^2(v_0v_1v_{23}v_3v_{41}v_{43}v_5)^4 + v_{43}^2(v_0v_1v_{21}v_3v_{41}v_{43}v_5)^4$
$+ v_1^2(v_0v_1v_{21}v_{23}v_{25}v_{45}v_5)^4 + v_{21}^2(v_0v_1v_{21}v_{25}v_3v_{45}v_5)^4 + v_{23}^2(v_0v_1v_{23}v_{25}v_3v_{45}v_5)^4$
$+ v_3^2(v_0v_{21}v_{23}v_{25}v_3v_{45}v_5)^4 + v_0^2(v_0v_{21}v_{23}v_3v_{41}v_{45}v_5)^4 + v_1^2(v_1v_{21}v_{23}v_3v_{41}v_{45}v_5)^4$
$+ v_{25}^2(v_{21}v_{23}v_{25}v_3v_{41}v_{45}v_5)^4 + v_{41}^2(v_0v_{21}v_{23}v_{25}v_{41}v_{45}v_5)^4 + v_{41}^2(v_0v_1v_{25}v_3v_{41}v_{45}v_5)^4$
$+ v_0^2(v_0v_1v_{21}v_{23}v_{43}v_{45}v_5)^4 + v_{25}^2(v_1v_{21}v_{23}v_{25}v_{43}v_{45}v_5)^4 + v_3^2(v_1v_{21}v_{23}v_3v_{43}v_{45}v_5)^4$
$+ v_1^2(v_0v_1v_{25}v_{41}v_{43}v_{45}v_5)^4 + v_{21}^2(v_0v_{21}v_{25}v_{41}v_{43}v_{45}v_5)^4 + v_{23}^8(v_0v_{23}v_{25}v_{41}v_{43}v_{45}v_5)^4$
$+ v_3^2(v_0v_{25}v_3v_{41}v_{43}v_{45}v_5)^4 + v_{41}^2(v_1v_{21}v_{23}v_{41}v_{43}v_{45}v_5)^4 + v_{43}^2(v_0v_{21}v_{23}v_{25}v_{43}v_{45}v_5)^4$
$+ v_{43}^2(v_0v_1v_{25}v_3v_{43}v_{45}v_5)^4 + v_{43}^2(v_{21}v_{23}v_3v_{41}v_{43}v_{45}v_5)^4 + v_{45}^2(v_0v_1v_{21}v_3v_{41}v_{45}v_5)^4$
$+ v_{45}^2(v_0v_1v_{23}v_3v_{43}v_{45}v_5)^4 + v_{45}^2(v_1v_{23}v_{25}v_{41}v_{43}v_{45}v_5)^4 + v_{45}^2(v_{21}v_{25}v_3v_{41}v_{43}v_{45}v_5)^4$
$+ v_5^2(v_0v_1v_{21}v_{23}v_{25}v_{41}v_5)^4 + v_5^2(v_0v_{21}v_{23}v_{25}v_3v_{43}v_5)^4 + v_5^2(v_1v_{23}v_{25}v_3v_{41}v_{45}v_5)^4$
$+ v_5^2(v_1v_{21}v_{25}v_3v_{43}v_{45}v_5)^4 + v_5^2(v_0v_1v_{21}v_{41}v_{43}v_{45}v_5)^4 + v_5^2(v_0v_{23}v_3v_{41}v_{43}v_{45}v_5)^4$

Mit Hilfe der Umrechnungstabelle von Bolza [Bo II] Seite 483, erhalten wir die folgenden Darstellungen für unsere ganzen Invarianten als Funktionen der zugehörigen Thetanullwerte:

$$\begin{aligned} I_2(C/\mathbb{C}) &= 2^3 J_2(C/\mathbb{C}) = h_{12}(\Omega_C)/h_{10}(\Omega_C) \\ I_4(C/\mathbb{C}) &= 2^2 J_4(C/\mathbb{C}) = h_4(\Omega_C) \\ I_6(C/\mathbb{C}) &= 2^3 J_6(C/\mathbb{C}) = h_{16}(\Omega_C)/h_{10}(\Omega_C) \\ I_{10}(C/\mathbb{C}) &= 2^{12} J_{10}(C/\mathbb{C}) = h_{10}(\Omega_C) \end{aligned}$$

Zusammenfassung der Ergebnisse aus Kapitel 4 und 5:

Satz 5.7 *Es sei $\Omega_{\tau,\tau^\varphi}$ die CM-Periodenmatrix von Satz 4.8 einer prinzipal polarisierten Abelschen Varietät $A(\tau)$ aus Satz 4.2 vom geeigneten primitiven CM-Typ $(K,\{1,\varphi\})$ aus Proposition 4.1. Dann können die Modulfunktionen $j_l(\tau,\tau^\varphi) := j_l(\Omega_{\tau,\tau^\varphi})$ für $l = 1,...,6$ über die Thetanullwerte mit Hilfe der in Kapitel 4.4 hergeleiteten Reihenentwicklung explizit analytisch berechnet werden. Diese Werte sind die absoluten Invarianten einer Kurve C vom Geschlecht 2 mit $J_C(\mathbb{C}) \cong \mathbb{C}^2/\Omega_{\tau,\tau^\varphi}\mathbb{Z}^2 + \mathbb{Z}^2 \cong A(\tau)$.*

Shimura zeigte [S-T], daß eine polarisierte Abelsche $(A,\mathcal{C})$ Varietät vom CM-Typ (K,Φ) schon über einem endlich algebraischen Erweiterungskörper L von $k_0^* = K^* k_0$ definiert ist, wobei k_0 der Modulkörper von $(A,\mathcal{C})$ ist. Wir können nun mit dem Hauptsatz der komplexen Multiplikation 3.23 zusammen mit dem Satz 3.25 den folgenden Satz zeigen:

Satz 5.8 *Es sei $\mathcal{K}_1 = \mathcal{K}_{1,\varphi} = \{(\tau_i,\tau_i^\varphi)|i = 1,...,d\cdot h'\}$ das in Kapitel 4 Satz 4.4 konstruierte Repräsentantensystem aller prinzipal polarisierten Abelschen Varietäten vom geeigneten primitiven CM-Typ $(K,\{1,\varphi\})$ und $\mathcal{K}_2 = \mathcal{K}_{1,\bar\varphi} = \{(\tau_j,\tau_j^{\bar\varphi})|i = 1,...,d\cdot h'\}$ das Vertretersystem zum primitiven CM-Typ $(K,\{1,\bar\varphi\})$ aus Satz 4.5. Falls $K/\mathbb{Q}$ galoisch und zyklisch, so ist nach Satz 4.7 $\mathcal{K} = \mathcal{K}_1 = \mathcal{K}_2$, anderenfalls ist $\mathcal{K} = \mathcal{K}_1 \cup \mathcal{K}_2$. Dann ist*

$$\mathcal{H}_l^1(x) := \prod_{(\tau,\tau^\varphi)\in\mathcal{K}_1} (x - j_l(\tau,\tau^\varphi)) \in K_0^*[x] \text{ für } l \le 6,$$

$$\mathcal{H}_l^2(x) := \prod_{(\tau,\tau^\varphi)\in\mathcal{K}_2} (x - j_l(\tau,\tau^\varphi)) \in K_0^*[x] \text{ für } l \le 6,$$

$$\mathcal{H}_l(x) := \prod_{(\tau,\tau^\varphi)\in\mathcal{K}} (x - j_l(\tau,\tau^\varphi)) \in \mathbb{Q}[x] \text{ für } l \le 6.$$

Beweis: Nach Konstruktion ist $\mathcal{K}_1$ ein Vertretersystem von $c'_K \times U/U_1$. Wir zeigten in Kapitel 3.3 Satz 3.25, daß $I_K^{**}/H_K^{**} \times U_0/U_1$ eine Untergruppe von $c'_K \times U/U_1$ ist. Nach Satz 3.23 und (i) in 3.3 und 3.25 haben wir $Gal(k_0^*/K^*) \cong I_{K^*}/H_0 \cong I_K^{**}/H_K^{**} \times U_0/U_1$, so daß die Polynome $\mathcal{H}_l^k(x)$ für $k = 1,2$ und $l \leq 6$ Koeffizienten in K^* haben.

Es sei ρ die Galoiskonjugation von K^*/K_0^*, die der komplexen Konjugation entspricht, und σ eine Fortsetzung von der Galoiskonjugation von $K_0^*/\mathbb{Q}$. Für $l = 1, ..., 6$ ist die Zahl $j = j_l(\tau, \tau^\varphi) \in k_0^*$ (Satz 3.23) eine absolute Invariante der zugehörigen Kurve C vom Geschlecht 2 mit $J_C(\mathbb{C}) \cong \mathbb{C}^2/\Omega_{\tau,\tau^\varphi}\mathbb{Z}^2 + \mathbb{Z}^2$. C ist schon über einem endlich algebraischen Erweiterungskörper L von k_0^* definiert. Damit ist j eine Funktion der Koeffizienten $f_i \in L$ der Kurvengleichung und $\bar{j} = j^\rho$ bzw. j^σ Funktion der entsprechenden konjugierten Koeffizienten f_i^ρ, f_i^σ. Das heißt, j^ρ ist die entsprechende absolute Invariante von C^ρ und j^σ von C^σ. Betrachtet man die q-Entwicklungen aus Kapitel 4.4, so sieht man leicht, daß $\bar{j}(\tau, \tau^\varphi) = j(-\bar{\tau}, -\bar{\tau}^\varphi)$, also $j(A(\bar{\tau})) = \bar{j}(A(\tau))$ ist. Das Ideal $a_{\bar{\tau}}$ liegt allerdings auch schon in c'_K, so daß damit die Koeffizienten von dem Polynom $\mathcal{H}_l^k(x)$ für $k = 1,2$ schon in dem dualen reellen quadratischen Zahlkörper K_0^* liegen.

Betrachten wir jetzt die Menge aller prinzipal polarisierten Abelschen Varietäten mit Endomorphismenring O_K, so sind darin natürlich auch die bezüglich σ konjugierten Varietäten enthalten. Wir haben damit bezüglich eines vollständigen Repräsentantensystems $\mathcal{K}$ ein Polynom in $\mathbb{Q}[x]$. □

Für die Konstruktion geeigneter Kurven müssen wir diese Polynome explizit analytisch zu berechnen. Nach Satz 5.3 hat das Polynom $\mathcal{H}_l(x)$ ganzzahlige Koeffizienten, wenn die zugehörigen Kurven vom Geschlecht 2 mit Enddomorphismenring O_K überall potentiell gute Reduktion haben. Nach Bemerkung 5.5 liegt die ganze Invariante J_{10} dieser Kurven in $\prod \mathcal{P}$ dem Produkt der schlechten Stellen. Die Primzahlen p mit $\mathcal{P}|p$ können dann nach Definition der Invarianten im Nenner der Polynome auftreten. Leider benötigen wir aber für die Reduktion der Polynome deren Ganzzahligkeit. In vielen Beispielen sind diese Polynome auch schon ganzzahlig, anderenfalls kann man noch versuchen den Nenner durch Probieren zu finden.

Kapitel 6

Algorithmus und Beispiele für g=2

6.1 Der Algorithmus

Teil A: (Suche einer geeigneten Gruppenstruktur)

1. Wir wählen uns einen primitiven CM Körper K vom Grad 4 über $\mathbb{Q}$, das heißt entweder ist $K/\mathbb{Q}$ nicht galoisch oder zyklisch. Der total reelle Teilkörper K_0 soll Klassenzahl 1 haben. Weiterhin berechnen wir eine relative Ganzheitsbasis von K/K_0 in der Form, daß $O_K = O_{K_0} + \eta O_{K_0}$ und $Im(\eta) > 0$ ist. Zuletzt konstruieren wir uns einen geeigneten CM-Typ $(K, \{1, \varphi\})$. Hierzu wählen wir eine Einbettung φ von K nach $\mathbb{C}$ mit $Im(\eta^\varphi) < 0$. Dann gibt es nach Proposition 4.1 eine prinzipale Polarisierung auf $A(O_K)$ von diesem Typ.

2. Wir suchen eine Zahl $\omega \in O_K$, deren 4 konjugierte ω_i für $i = 1, .., 4$ echt verschieden sind, mit $\omega\bar{\omega} = p$ für eine Primzahl $p \approx 10^{20}$, so daß es eine weitere Primzahl $l \approx 10^{40}$ gibt, mit

   (a) $l \mid \prod_{i=1}^{4}(1 - \omega_i) =: N$.

   (b) $l \mid p^k - 1$ nur für $k > 1000$.

   Dann ist ω eine 'gute' Weil-Zahl für p in der von Adlemann und Huang in [A-H] definierten Bedeutung. Dann gibt es nach Satz 11 in Kapitel 5.5 in [A-H] eine über $\mathbb{F}_p$ definierte prinzipal polarisierte Abelsche Varietät A, die $f_\omega(1) = \prod_{i=1}^{4}(1 - \omega_i)$ $\mathbb{F}_p$-rationale Punkte hat.

Teil B: (Konstruktion der zugehörigen Kurvengleichung über $\mathbb{F}_p$)

1. Wir berechnen zu dem Körper K in Kapitel 4 Satz 4.7 konstruierte Repräsentantensystem $\mathcal{K}$ aller prinzipal polarisierten Abelschen Varietäten mit Endomorphismenring O_K. $\mathcal{K}$ besteht aus Zahlenpaaren (τ_j, τ_j') mit $Im(\tau_j) > 0$ und $Im(\tau_j') < 0$.

$$\mathcal{K} = \{(\tau_j, \tau_j') | j \leq 2 \cdot d \cdot h'\}$$

2. Wir berechnen jetzt analytisch mit ausreichender Genauigkeit die zehn geraden Thetanullwerte und anschließend die Invariantensysteme bezüglich der Vertreterpaare aus $\mathcal{K}$. Das heißt, wir berechnen

$$j_l(\tau, \tau') := j_l(\Omega_{\tau,\tau'}) \text{ für alle Paare } (\tau, \tau') \in \mathcal{K} \text{ und für } l = 1,2,3,4,5,6,$$

wobei die Matrix $\Omega_{\tau,\tau'}$ in Kapitel 4.3 Satz 4.8 gegeben und die Reihenentwicklung der Thetanullwerte in Kapitel 4.4 hergeleitet wurde.

3. Anschließend werten wir die zugehörigen Polynome aus Satz 5.8

$$H_l(x) = \prod_{(\tau,\tau') \in \mathcal{K}} (x - j_l(\tau, \tau')) \in \mathbb{Q}[x] \text{ aus.}$$

Falls $H_l(x) \notin \mathbb{Z}[x]$, suchen wir mit kleinen Primzahlen den Nenner ab. können wir den Nenner n so herausfinden, so setzen wir $H_l(x) := n * H_l(x)$ und modifizieren die Invarianten.

4. Wir reduzieren das Polynom $H_l^0(x) \equiv H_l(x) \bmod p$, wobei p die in Schritt 2 gefundene Primzahl ist.

5. Für geeignete Nullstellen j_l^0 von $H_l^0(x)$ ist das Tripel (j_1^0, j_2^0, j_3^0) das Invariantensystem einer Kurve vom Geschlecht 2 über $\mathbb{F}_p$. In diesem Fall gibt es Koeffizienten $f_i \in \mathbb{F}_p$, die das Invariantengleichungssystem lösen und somit entweder Koeffizienten der gesuchten Kurve C oder der zu ihr getwisteten Kurve sind.

6. Zuletzt testen wir durch Multiplikation eines Punktes auf der zugehörigen Jacobischen Varietät $J_C(\mathbb{F}_p)$ mit der gewünschten Ordnung N, ob C oder erst ihr Twist die kryptographisch geeignete Kurve ist.

Bemerkungen

1) *Ein geeignetes Element ω in O_K habe ich auf die folgende Art und Weise gefunden: Man setze $\omega = \sum_{i=1}^{4} x_i \mu_i$, wobei $\mu_1, ...\mu_4$ eine Ganzheitsbasis von K über $\mathbb{Z}$ ist. Durch die Bedingung $\omega\omega^{\varphi} = p = \bar{\omega}\bar{\omega}^{\varphi}$ erhalten wir die Gleichungen:*

$$\omega\omega^{\varphi} - \bar{\omega}\bar{\omega}^{\varphi} = 0 \text{ und } \omega\omega^{\varphi} + \bar{\omega}\bar{\omega}^{\varphi} = 2p.$$

Nun setze ich zwei der x_i sinnvoll fest und inkrementiere die anderen solange, bis diese beiden Gleichungen für eine geeignete Primzahl p erfüllt sind. Anschließend teste ich, ob die Zahl $\prod_{i=1}^{4}(1 - \omega_i) =: N$ von einer Primzahl $l \approx 10^{40}$ geteilt wird und ob die Ordnung k von l mod p größer als 1000 ist.

2) *Eine schnelle algorithmische Berechnung eines Relativbasis-Repräsentantensystems wird zur Zeit von Herrn Sachar Paulus im Institut für Experimentelle Mathematik erforscht. Generell sind aber Algorithmen für die Berechnung einer absoluten Ganzheitsbasis bekannt, aus denen kann man dann anschließend Relativbasiszahlen berechnen.*

3) *Wir zeigten in Satz 3.25, daß die Idealklassengruppe I_{K^*}/H_0 aus 3.23 dem Hauptsatz der komplexen Multiplikation ein Repräsentantensystem liefert, welches das Vertretersystem $\mathcal{K}_{\Phi}$ als Teiler enthält. Es genügt daher eigentlich, wenn man über diese kleinere Klassengruppe geht. Es ist allerdings sehr viel komplizierter, hierfür ein Vertretersystem zu bestimmen.*

4) *Die Berechnung der Invariantensysteme ist nur ein rechentechnisches Problem und hängt von der gewählten Genauigkeit ab.*

5) *Größere Schwierigkeiten macht das Lösen des nichtlinearen Gleichungssystems zu gegebenen Invarianten. In meinen Fällen nahm ich den Buchbergeralgorithmus zur Berechnung einer Gröbnerbasis zur Hilfe. Beispielweise ist in dem System 'Maple' ein Algorithmus implementiert, der mit Hilfe des Buchbergeralgorithmus die Lösungsmenge -leider nur über $\mathbb{Z}$ - liefert.*

Im ersten Schritt suchen wir einen primitiven CM-Körper vom Grad 4 über $\mathbb{Q}$. Wir zeigten, daß K über $\mathbb{Q}$ entweder nicht galoisch oder zyklisch sein muß. Um dies zu überprüfen, verwenden wir folgende Kriterien:

1. Sei $1 \neq \sigma \in Gal(K_0/\mathbb{Q})$. Für $K_0 = \mathbb{Q}(\sqrt{D})$ ist $\sigma(\sqrt{D}) = -\sqrt{D}$. Wir haben $K = K_0(\sqrt{a})$ für ein quadratfreies $a \in K_0$ und definieren so $\tilde{\sigma}$ als die Fortsetzung von σ auf K mit $\tilde{\sigma}(\sqrt{a}) := -\sqrt{\sigma(a)}$. Bekanntlich ist K/K_0 genau dann galoisch, wenn $\frac{\sigma(a)}{a} = q^2$ für ein Element $q \in K_0$.

2. Sei nun $K/\mathbb{Q}$ galoisch und $\sigma(a) = q^2 a$ für ein q in K, so gilt

$$\tilde{\sigma}^2(\sqrt{a}) = \tilde{\sigma}(-\sqrt{\sigma(a)}) = \tilde{\sigma}(-\sqrt{aq^2}) = \tilde{\sigma}(-q\sqrt{a}) = -\sigma(q)(-\sqrt{\sigma(a)}) = \sigma(q)q\sqrt{a}.$$

Also ist:

(a) $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \iff \tilde{\sigma}^2 = id \iff \sigma(q)q = 1$,

(b) $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \iff \tilde{\sigma}^2 = \rho \iff \sigma(q)q = -1$.

6.2 Beispiele

Beipiel 1:

Teil A: (Suche einer geeigneten Gruppenstruktur)

1) Wir setzen

$$\begin{aligned} K_0 &= \mathbb{Q}(\sqrt{2}) \text{ ist total reeller Teilkörper mit } |c_{K_0}| = 1, \\ K &= K_0(\sqrt{a}) \text{ mit } a = -(2+\sqrt{2}) \text{ ist } CM - \text{Körper mit Klassenzahl } |c_K| = 1, \\ O_K &= O_{K_0} + \eta\, O_{K_0} \text{ mit } \eta = i\sqrt{2+\sqrt{2}} = \sqrt{a}, \\ O_{K_0} &= \mathbb{Z} + \sqrt{2}\mathbb{Z} \text{ mit Fundamentaleinheit } \varepsilon_0 = 1+\sqrt{2} \text{ d.h. } N(\varepsilon_0) = -1. \end{aligned}$$

φ sei die folgende Fortsetzung der Galoiskonjugation von $K_0/\mathbb{Q}$:

$$\eta^\varphi = -\sqrt{a^\varphi} = -i\sqrt{2-\sqrt{2}}.$$

Damit ist $(K, \{1, \varphi\})$ nach 3.15 ein geeigneter CM-Typ, d.h. zu diesem Typ gibt es prinzipale Polarisierungen. η ist geeigneter Repräsentant der Idealklassengruppe $c'_K = c_K$. Das Element $\xi_\eta = -((\eta - \eta^\varphi)(2\sqrt{2}))^{-1}$ definert nach Satz 4.2 eine prinzipale Polarisierung E_{ξ_η} auf $A(O_K) = A(\eta)$. Weil $aa^\varphi = \sqrt{2}^2$ ein Quadrat in K_0 ist, ist $K/\mathbb{Q}$ galoisch. Außerdem ist

$$\frac{a}{a^\varphi} = \frac{a^2}{N(a)} = 3 + 2\sqrt{2} = \varepsilon_0^2 \text{ und } N(\varepsilon_0) = -1,$$

so daß $K/\mathbb{Q}$ zyklisch ist. Damit ist K ein primitiver CM-Körper, so daß $\mathbb{C}^2/\mathbb{Z}^2\Omega_{\eta,\eta^\varphi} + \mathbb{Z}^2$ die Jacobische Varietät einer Kurve vom Geschlecht 2 ist.

2) Wir setzen $\omega = x_1 + x_2\sqrt{2} + i\sqrt{2+\sqrt{2}}(x_3 + x_4\sqrt{2})$ und erhalten

$$\begin{aligned}
\omega\bar{\omega} &= (x_1 + x_2\sqrt{2})^2 + (2+\sqrt{2})(x_3 + x_4\sqrt{2})^2 = p, \\
\omega^\varphi\bar{\omega}^\varphi &= (x_1 - x_2\sqrt{2})^2 + (2-\sqrt{2})(x_3 - x_4\sqrt{2})^2 = p, \\
\text{also } p &= x_1^2 + 2x_2^2 + 2x_3^2 + 4x_3x_4 + 4x_4^2 \text{ und } 0 = 2x_1x_2 + x_3^2 + 4x_3x_4 + 2x_4^2.
\end{aligned}$$

$$\text{Setzen wir } x_1 = -\frac{x_3^2 + 4x_3x_4 + 2x_4^2}{2x_2} \in \mathbb{Z}, \text{ so muß } x_3 \equiv 0 \bmod 2$$

$$\text{z.B. } x_2 = 1 \text{ und } x_3 = 2, \text{ also } x_1 = -\frac{4 + 8x_4 + 2x_4^2}{2} = -(2 + 4x_4 + x_4^2).$$

$$\text{Damit haben wir } p = 14 + 24x_4 + 24x_4^2 + 8x_4^3 + x_4^4.$$

$$\text{Es ist } N := \prod_{i=1}^{4}(1-\omega_i) = 1 + a_1 + a_2 + a_1p + p^2 \text{ mit}$$

$$a_1 = = -4x_1 = 4(2 + 4x_4 + x_4^2) \text{ und } a_2 = 4x_1^2 - 8 + 2p.$$

Wir erhalten zum Beispiel für $x_4 = 111387$ die Zahlen:

$$\begin{aligned}
p &= 153946287550700989943 \\
|J_C(\mathbb{F}_p)| &= N = 4 \cdot l_p = 4 \cdot 592486486457086864793418655053917441267 9,
\end{aligned}$$

$$
\begin{aligned}
|J_C(\mathbb{F}_p)| &= 1 + a_1 + a_2 + a_1 \cdot p + p^2 \text{ und} \\
|C(\mathbb{F}_p)| &= 1 + a_1 + p = 15394628760033102722 0 \quad \text{mit} \\
a_1 &= 49630037276 \text{ und } a_2 = 92367772510568935492 2.
\end{aligned}
$$

Wir faktorisieren l_p

$$l_p = 2 * 3049 * 971607882022116865846865619963787211.$$

Die kleinste Zahl k mit l_p teilt $p^k - 1$ ist die Zahl 971607882022116865846865619963787211. Wir haben also eine geeignete Punktegruppe gefunden.

Teil B: (Konstruktion der Kurvengleichung)

1) Wir haben nach Satz 4.4 $\mathcal{K} = \{(\eta, \eta^\varphi)\}$. Bezüglich der Matrix $\Omega_{\eta,\eta^\varphi}$ werten wir mit ausreichender Genauigkeit die zehn geraden Thetanullwerte, dann die ganzen Invarianten und schließlich die absoluten Invarianten aus. Diese sind ganzzahlig. Wir erhalten:

$q =$
0.59864526010607935471534678720936983353337679059127076010030488347094752144 1
25843746112053323447062383802437962917611350652146422021535122665063220 55
08389514684816842330184135750448537013353224036613085694791203532430547 14
69406720188193147921058418796959527985

$q' =$
0.80853831444428824034342704218013375939894386802812905996976497960319002675 1
08210494634257631581818659489515010806368220058474706379270739125061020 65
17530173131275476493522818776191694465036249757879364902573746569175765 03
37819200567084043257605308217553563238 8

$J_2 =$
2.67401867304433865730093929887878479447379592060159393747525598477083 59
63205406299353064779527423325095737215777875748411141159716162155238686 2
31884346101938185739499966593635721909030048759383468338464041265422120 0
69985209951017247197510072168328586878255 6

$J_4 =$
1.765524904639458203486144406867665961909869953216643948993645465301828832573017713073623261711528759712093620053974964525453661752311358692013531447754632642391791231014545746186542582559079304799697041574288689871842326834076035201056374532385297681654304918

$J_6 =$
6.504553041984570388678669143242966403268717837561589820701316006636138914621007072947125180683673479932385498228047243064831946203310014456446896415752928229325401683323166652318602352233790572841075860912936926086979152278082020489763512468422935278649560 1

$J_{10} =$
5.955022063945777333721696950593500642647672613402426738339146204460784808471759504839504491263330285355877931985080969366074190376633411964266815819066269036295902325873519522885899992127335940255045619681220495874325901858587325888472120298354487648612866021 0^{-7}

$$\begin{aligned} j_1 &= J_2^5/J_{10} = 229582512 \\ j_2 &= J_2^3 * J_4/J_{10} = 56687040 \\ j_3 &= J_2^2 * J_6/J_{10} = 78102144 \\ j_4 &= J_4 * J_6/J_{10} = 19284480 \\ j_5 &= J_4^5/J_{10}^2 = 48372940800000 \\ j_6 &= J_6^5/J_{10}^3 = 55136243389886361501696 \end{aligned}$$

2) Wir finden mit Hilfe des Buchbergeralgorithmus folgende Kurvengleichungen über $\mathbb{Z}$ zu diesem Invariantensystem:

$$C : y^2 = x^5 - 140c^2x^3 - 240c^3x^2 + 3810c^4x + c^5 6928 \text{ mit } c \in \mathbb{Z}.$$

Wir werten an dieser Kurve die ganzen Invarianten aus:

$$\begin{aligned} J_2 &= c^4 33750 = c^4 2\,3^3 5^4, \quad J_4 = c^8 281250000 = c^8 2^4 3^2 5^9 \\ J_6 &= c^{12} 13078125000000 = c^{12} 2^6 3^3 5^{12} 31, \quad J_{10} = c^{20} 190734863281250 = c^{20} 2\,5^{20} \end{aligned}$$

$$C : y^2 = x^5 - 1560r^2x^3 + 37920r^3x^2 - 338040r^4x + 1042304r^5 \text{ mit } r \in \mathbb{Z}.$$

$$\begin{aligned} J_2 &= r^4 135000 = r^4 2^3 3^3 5^4, \quad J_4 = r^8 4500000000 = r^8 2^8 3^2 5^9 \\ J_6 &= 2^{12} 837000000000000 = r^{12} 2^{12} 3^3 5^{12} 31, \quad J_{10} = r^{20} 2^{11} 5^{20} \end{aligned}$$

Damit unterscheiden sich die ganzen Invarianten vom Grad m dieser beiden Kurvengleichungen gerade um den Faktor $2^m(\frac{r}{c})^{m^2}$.

Für die erste Kurve erhalten wir folgende Gleichungen für die affine Varietät

$$\begin{aligned} (J_C - \Theta)(K) &: \{F_1[u_1,u_2,v_1,v_2] = 0, F_2[u_1,u_2,v_1,v_2] = 0\}, \text{ wobei} \\ F_1[u_1,u_2,v_1,v_2] &:= -u_1^4 + (3u_2 + 140)u_1^2 + (-v_1^2 + 240)u_1 + \\ &\quad (-u_2^2 - 140u_2 + (2v_2v_1 - 3810)) \\ F_2[u_1,u_2,v_1,v_2] &:= 6928 + 240u_2 + 140u_1u_2 - u_1u_2(u_1^2 - 2u_2) - u_2v_1^2 + v_2^2 \end{aligned}$$

3) **Multiplikation auf der Jacobischen Varietät $J_C(\mathbb{F}_p)$:**

$$\begin{aligned} D &= (15394628755070098 9929, 49, \\ &\quad 31694823907497262594, 86028807748921141745) \\ (l_p - 1) \cdot D &= (15394628755070098 9929, 49, \\ &\quad 12225146364320372 7349, 67917479801779848198) \\ &= -D \end{aligned}$$

Es ist klar, daß damit $l_p \cdot D = 0$ auf $J_C(\mathbb{F}_p)$ und D die für ein Kryptosystem gesuchte Untergruppe erzeugt.

Beispiel 2:

Teil A: (Suche einer geeigneten Gruppenstruktur)

1) Wir setzen

$$\begin{aligned} K_0 &= \mathbb{Q}(\sqrt{5}) \text{ total reeller Teilkörper mit } |c_{K_0}| = 1, \\ K &= K_0(\sqrt{a}) \text{ mit } a = -(5+\sqrt{5}) \text{ ist } CM - \text{Körper mit Klassenzahl } |c_K| = 1, \\ O_K &= O_{K_0} + \eta\, O_{K_0} \text{ mit } \eta = i\sqrt{5+\sqrt{5}} = \sqrt{a}, \\ O_{K_0} &= \mathbb{Z} + \sqrt{5}\mathbb{Z} \text{ mit Fundamentaleinheit } \varepsilon_0 = \frac{1+\sqrt{5}}{2} \text{ d.h. } N(\varepsilon_0) = -1. \end{aligned}$$

φ sei die folgende Fortsetzung der Galoiskonjugation von $K_0/\mathbb{Q}$:

$$\eta^\varphi = -\sqrt{a^\varphi} = -i\sqrt{5-\sqrt{5}}.$$

Damit ist $(K, \{1, \varphi\})$ ein geeigneter CM-Typ. η ist geeigneter Repräsentant der Idealklassengruppe $c'_K = c_K$. Das Element $\xi_\eta = -((\eta - \eta^\varphi)(\sqrt{5}))^{-1}$ definert eine prinzipale Polarisierung E_{ξ_η} auf $A(O_K) = A(\eta)$. Weil $aa^\varphi = 25 - 5 = 2^2\sqrt{5}^2$ ein Quadrat in K_0 ist, ist $K/\mathbb{Q}$ galoisch. Außerdem ist

$$\frac{a}{a^\varphi} = \frac{a^2}{N(a)} = \frac{3+\sqrt{5}}{2} = \frac{1+\sqrt{5}^2}{2} = \varepsilon_0^2 \text{ und } N(\varepsilon_0) = -1,$$

so daß $K/\mathbb{Q}$ zyklisch ist. Damit ist K ein primitiver CM-Körper und $\mathbb{C}^2/\mathbb{Z}^2\Omega_{\eta,\eta^\varphi} + \mathbb{Z}^2$ die Jacobische Varietät einer Kurve vom Geschlecht 2.

2) Wir setzen $\omega = x_1 + x_2\frac{1+\sqrt{5}}{2} + i\sqrt{5+\sqrt{5}}(x_3 + x_4\frac{1+\sqrt{5}}{2})$ und erhalten

$$\begin{aligned} \omega\bar{\omega} &= x_1^2 + x_1x_2 + \frac{3}{2}x_2^2 + 5x_3^2 + 10x_3x_4 + 10x_4^2 + \\ &\quad \sqrt{5}(x_1x_2 + \frac{x_2^2}{2} + x_3^2 + 6x_3x_4 + 4x_4^2), \\ \text{also lösen wir } p &= x_1^2 + x_1x_2 + \frac{3}{2}x_2^2 + 5x_3^2 + 10x_3x_4 + 10x_4^2 \\ \text{und } 0 &= x_1x_2 + \frac{x_2^2}{2} + x_3^2 + 6x_3x_4 + 4x_4^2. \\ \text{Setzen wir } x_2 &= 2, x_3 = 2, \text{ so folgt } x_1 = -3 - 6x_4 - 2x_4^2, \end{aligned}$$

$$\text{so ist } p = 29 + 44x_4 + 54x_4^2 + 24x_4^3 + 4x_4^4.$$

$$\text{Damit haben wir } N := \prod_{i=1}^{4}(1-\omega_i) = 1 + a_1 + a_2 + a_1 p + p^2 \text{ mit}$$

$$a_1 = = -4x_1 - 2x_2 \text{ und } a_2 = 4(x_1^2 + x_1x_2 - x_2^2) + 2p.$$

Wir erhalten zum Beispiel für $x_4 = 100697$ die Zahlen:

$$\begin{aligned} p &= 411293642771748015259 \\ |J_C(\mathbb{F}_p)| &= N = 4 \cdot l_p = 4 \cdot 42290615154454756740973122525028076098619, \\ |J_C(\mathbb{F}_p)| &= 1 + a_1 + a_2 + a_1 \cdot p + p^2 \text{ und} \\ |C(\mathbb{F}_p)| &= 1 + a_1 + p \quad \text{mit} \\ a_1 &= 81121503208 \text{ und } a_2 = 2467761856224884603314. \end{aligned}$$

Wir überprüfen leicht, daß die kleinste Zahl k mit l_p teilt $p^k - 1$ größer als 1000 ist. Wir haben also eine geeignete Punktegruppe gefunden.

Teil B: (Konstruktion der Kurvengleichung)

1) Wir haben nach Satz 4.7 $\mathcal{K} = \{(\eta, \eta^\varphi)\}$. Bezüglich der Matrix $\Omega_{\eta,\eta^\varphi}$ werten wir mit ausreichender Genauigkeit die zehn geraden Thetanullwerte, dann die ganzen Invarianten und schließlich die absoluten Invarianten aus. Diese sind ganzzahlig.

$$\begin{aligned} j_1 &= 6202728393750 \\ j_2 &= 126586293750 \\ j_3 &= 36194303250 \\ j_4 &= 738659250 \\ j_5 &= 136202515664062500 \\ j_6 &= 161449079998774892615392500 0 \end{aligned}$$

2) Wir finden mit Hilfe des Buchbergeralgorithmus folgende Ergebnisse:

$$J_2 = 630 \cdot f,$$

$$\begin{aligned} J_4 &= 8100 \cdot f^2, \\ J_6 &= 1459080 \cdot f^3, \\ J_{10} &= 16 \cdot f^5. \end{aligned}$$

Hierzu erhalten wir dann folgende Kurvengleichungen über $\mathbb{Z}$:

$$C : y^2 = x^5 - 30c^2x^3 + 180c^4x - 176c^5 \text{ mit } c \in \mathbb{Z} \text{ und } f = 20c^4.$$

$$C : y^2 = x^5 - 7190r^2x^3 + 385440r^3x^2 - 7746540r^4x + 55342672r^5 \text{ mit } r \in \mathbb{Z} \text{ und } f = 500r^4.$$

Für die erste Kurve haben wir

$$\begin{aligned} (J_C - \Theta)(K) &: \{F_1[u_1, u_2, v_1, v_2] = 0, F_2[u_1, u_2, v_1, v_2] = 0\}, \text{ wobei} \\ F_1[u_1, u_2, v_1, v_2] &:= -u_1^4 + (3u_2 + 30)u_1^2 + (-v_1^2)u_1 + \\ &\quad (-u_2^2 - 30u_2 + (2v_2v_1 - 810)) \\ F_2[u_1, u_2, v_1, v_2] &:= -176 + 30u_1u_2 - u_1u_2(u_1^2 - 2u_2) - u_2v_1^2 + v_2^2 \end{aligned}$$

3) **Multiplikation auf der Jacobischen Varietät $J_C(\mathbb{F}_p)$:**

$$\begin{aligned} D &= (41129364277174801524 9, 25 \\ &\quad 195589823550795439685, 17794148863612957589) \\ (l_p - 1) \cdot D &= (41129364277174801524 9, 25 \\ &\quad 215703819220952575574, 39349949390813505767 0) \\ &= -D \end{aligned}$$

Es ist klar, daß damit $l_p \cdot D = 0$ auf $J_C(\mathbb{F}_p)$ und D die für ein Kryptosystem gesuchte Untergruppe erzeugt.

Beispiel 3:

Es sei K der Körper der 5-ten Einheitswurzeln.

$$\begin{aligned}
\text{Setze } a &= -\frac{5+\sqrt{5}}{2},\\
\text{so ist } \xi_5 &= \frac{1}{2}(-\frac{1+\sqrt{5}}{2}+\sqrt{a}) \text{ eine 5-te Einheitswurzel},\\
K_0 &= \mathbb{Q}(\sqrt{5}) \text{ ist total reeller Körper mit } |c_{K_0}| = 1,\\
K &= \mathbb{Q}(\sqrt{a}) \text{ ist } CM\text{-Körper mit } |c_K| = 1,\\
O_K &= O_{K_0} + \eta O_{K_0} \text{ mit } \eta = \frac{1}{2}(1+\frac{1+\sqrt{5}}{2}+\sqrt{a}),\\
O_{K_0} &= \mathbb{Z} + \frac{1+\sqrt{5}}{2}\mathbb{Z} \text{ mit Fundamentaleinheit } \varepsilon_0 = \frac{3+\sqrt{5}}{2}, \text{ wobei } N(\varepsilon_0) = 1.\\
&\quad \varphi \text{ sei die folgende Fortsetzung der Galoiskonjugation von } K_0/\mathbb{Q}:\\
(\sqrt{a})^\varphi &= -\sqrt{a^\varphi} = -\sqrt{\frac{5-\sqrt{5}}{2}}.
\end{aligned}$$

Damit ist $(K, \{1, \varphi\})$ ein geeigneter CM-Typ. η ist geeigneter Repräsentant der Idealklassengruppe $c'_K = c_K$. Das Element $\xi_\eta = -((\eta - \eta^\varphi)(\sqrt{5}))^{-1}$ definiert nach Satz 4.2 eine prinzipale Polarisierung E_{ξ_η} auf $A(O_K) = A(\eta)$. Weil $aa^\varphi = \sqrt{5}^2$ ein Quadrat in K_0 ist, ist $K/\mathbb{Q}$ galoisch. Außerdem ist

$$\frac{a}{a^\varphi} = \frac{a^2}{N(a)} = (\frac{a}{\sqrt{5}})^2 \text{ und } \frac{N(a)}{N(\sqrt{5})} = \frac{5}{-5} = -1,$$

so daß $K/\mathbb{Q}$ zyklisch ist. Damit ist K ein primitiver CM-Körper. Nach Satz 4.7 haben wir $\mathcal{K}\{(\eta, \eta^\varphi)\}$. Bezüglich der Matrix $\Omega_{\eta,\eta^\varphi}$ werten wir mit ausreichender Genauigkeit die absoluten Invarianten aus. Wir erhalten:

$$j_1 = j_2 = j_3 = j_4 = j_5 = j_6 = 0.$$

So daß $C : y^2 = x^5 - 1$ die zugehörige leider supersinguläre Kurve definiert.

Beispiel 4: $K/\mathbb{Q}$ nicht galoisch und $N(\varepsilon) = -1$

$$\begin{aligned}
\text{Setze } a &= -(5+2\sqrt{2}),\\
K_0 &= \mathbb{Q}(\sqrt{2}) \text{ damit ist } |c_{K_0}| = 1,\\
K &= \mathbb{Q}(\sqrt{a}) \text{ damit ist } |c_K| = 1,\\
O_K &= O_{K_0} + \eta O_{K_0} \text{ mit } \eta = \frac{1}{2}(1+\sqrt{2}+\sqrt{a}),\\
O_{K_0} &= \mathbb{Z} + \sqrt{2}\mathbb{Z} \text{ mit Fundamentaleinheit } \varepsilon_0 = 1+\sqrt{2}, N(\varepsilon_0) = -1.
\end{aligned}$$

φ sei die folgende Fortsetzung der Galoiskonjugation von $K_0/\mathbb{Q}$:

$$(\sqrt{a})^{\varphi} = -\sqrt{a^{\varphi}} = -\sqrt{5-2\sqrt{2}}$$

Damit ist $(K, \{1, \varphi\})$ ein geeigneter CM-Typ. Weil $aa^{\varphi} = 25 - 8 = 17$ kein Quadrat in K_0 ist, ist $K/\mathbb{Q}$ nicht galoisch und damit ein primitiver CM-Körper und $(K, \{1, \varphi\})$ ein primitiver CM-Typ. Wir haben weiterhin

$$K^* = \mathbb{Q}(\sqrt{a} + (\sqrt{a})^{\varphi}) = \mathbb{Q}(\sqrt{a^*}) \text{ mit } a^* = -\frac{5-\sqrt{17}}{2}$$

$$K_0^* = \mathbb{Q}(\sqrt{17}).$$

Das Element $\xi_\eta = -((\eta - \eta^{\varphi})(2\sqrt{2}))^{-1}$ definert also eine prinzipale Polarisierung vom Typ $(K, \{1, \varphi\})$ durch E_{ξ_η} auf $A(O_K) = A(a_\eta)$ und das Element $\xi_{\varepsilon_0\eta}$ definert eine prinzipale Polarisierung vom Typ $(K, \{1, \bar{\varphi}\})$ auf $A(O_K)$. Damit ist nach Satz 4.7

$$\mathcal{K}_1 = \mathcal{K}_{\{1,\varphi\}} = \{(\eta, \eta^{\varphi})\} \text{ und } \mathcal{K}_2 = \mathcal{K}_{\{1,\bar{\varphi}\}} = \{(\varepsilon_0\eta, (\varepsilon_0\eta)^{\bar{\varphi}})\}.$$

Bezüglich der zugehörigen Matrizen berechnen wir nun die Invarianten

$$j_{l,1} := j_l(\eta, \eta^{\varphi}) \in O_{K_0^*} \text{ und } j_{l,2} := j_l(\varepsilon_0\eta, (\varepsilon_0\eta)^{\bar{\varphi}}) \in O_{K_0^*}$$

$$H_l(x) = (x - j_{l,1})(x - j_{l,2}) \text{ für } l = 1, 2, 3, \ldots.$$

Es ist

$$\begin{aligned}
H_1(x) &= x^2 - 531441x + 55788550416\\
&= (x - \frac{531441 + 59049\sqrt{17}}{2})(x - \frac{531441 - 59049\sqrt{17}}{2})
\end{aligned}$$

$$
\begin{aligned}
H_2(x) &= x^2 - 426465x - 68874753600 \\
&= (x - \frac{426465 + 164025\sqrt{17}}{2})(x - \frac{426465 - 164025\sqrt{17}}{2}) \\
H_3(x) &= x^2 - 216513x - 221011431552 \\
&= (x - \frac{216513 + 234009\sqrt{17}}{2})(x - \frac{216513 - 234009\sqrt{17}}{2}) \\
H_4(x) &= x^2 - 1165185x + 272853619200 \\
&= (x - \frac{1165185 + 125145\sqrt{17}}{2})(x - \frac{1165185 - 125145\sqrt{17}}{2}) \\
H_5(x) &= x^2 - 865990490625x - 8926168066560000000000 \\
&= (x - \frac{865990490625 + 214975265625\sqrt{17}}{2})(x - \frac{865990490625 - 214975265625\sqrt{17}}{2})
\end{aligned}
$$

Andererseits haben wir ausgehend von $K^*(\sqrt{a^*})$ über $K_0^* = \mathbb{Q}(\sqrt{17})$

$$
\begin{aligned}
O_K &= O_{K_0} + \eta^* O_{K_0} \text{ mit } \eta^* = \frac{5 + \sqrt{17}}{4}(1 + \sqrt{a^*}) \\
O_{K_0} &= \mathbb{Z} + \frac{1 + \sqrt{17}}{2}\mathbb{Z} \text{ mit Fundamentaleinheit } \varepsilon_0 = 4 + \sqrt{17}, N(\varepsilon_0) = -1 \\
&\quad \varphi \text{ sei die folgende Fortsetzung der Galoiskonjugation von } K_0/\mathbb{Q}: \\
(\sqrt{a^*})^{\varphi^*} &= -i\frac{\sqrt{5 - \sqrt{17}}}{2}
\end{aligned}
$$

Weil $a^* a^{\varphi *} = (25 - 17)/4 = 2$ kein Quadrat in K_0 ist, ist $K/\mathbb{Q}$ nicht galoisch Es ist

$$\mathcal{K}_1 = \{(\eta^*, (\eta^*)^{\varphi^*})\} \text{ und } \mathcal{K}_2 = \{(\varepsilon_0\eta^*, (\varepsilon_0\eta^*)^{\bar{\varphi^*}})\}.$$

$$
\begin{aligned}
H_1(x) &= x^2 + 11337408x + 3570467226624 \\
&= (x - (-5668704 + 3779136\sqrt{2}))(x + 5668704 + 3779136\sqrt{2}) \\
H_2(x) &= x^2 - 2099520x + 1101996057600 \\
&= (x - 1049760)^2 \\
H_3(x) &= x^2 - 2239488x + 1244031105024 \\
&= (x - (1119744 + 69984\sqrt{2}))(x - (1119744 - 69984\sqrt{2})) \\
H_4(x) &= x^2 + 3421440x + 383960217600 \\
&= (x - (-1710720 + 1127520\sqrt{2}))(x - (-1710720 - 1127520\sqrt{2}))
\end{aligned}
$$

$$\begin{aligned} H_5(x) &= x^2 + 37413446400000x + 35704672266240000000000 \\ &= (x - (-18706723200000 + 13226976000000\sqrt{2})) \\ &\quad (x - (-18706723200000 - 13226976000000\sqrt{2})) \end{aligned}$$

Wir erhalten beispielsweise modulo p = 13:

$$\begin{aligned} H_1(x) &= (x+3)(x+9) \\ H_2(x) &= (x+4)(x+9) \\ H_3(x) &= (x+10)(x+5) \end{aligned}$$

und mit

$$y^2 = x^5 + 2x^3 + 2x^2 + 11x + 6$$

eine zugehörige Kurvengleichung für $C/\mathbb{F}_{13}$.

Beispiel 5:

$$\begin{aligned} \text{Setze } a &= -(3+\sqrt{2}), \\ K &= \mathbb{Q}(\sqrt{a}) \text{ damit ist } |c_K| = 2, N(\varepsilon_0) = N(1+\sqrt{2}) = -1 \\ &\Longrightarrow c_K = c'_K \\ K_0 &= \mathbb{Q}(\sqrt{2}) \text{ damit ist } |c_{K_0}| = 1 \\ O_K &= O_{K_0} + \eta O_{K_0} \text{ mit } \eta = \sqrt{a} \\ O_{K_0} &= \mathbb{Z} + \sqrt{2}\mathbb{Z} \text{ mit Fundamentaleinheit} \\ & \varphi \text{ sei die folgende Fortsetzung der Galoiskonjugation von } K_0/\mathbb{Q}: \\ (\sqrt{a})^\varphi &= -i\sqrt{3-\sqrt{2}} \end{aligned}$$

Weil $aa^\varphi = 9 - 2 = 7$ kein Quadrat in K_0 ist, ist $K/\mathbb{Q}$ nicht galoisch und damit ein primitiver CM-Körper und $(K, \{1, \varphi\})$ ein primitiver CM-Typ.

Das Element $\xi_\eta = -((\eta - \eta^\varphi)(2\sqrt{2}))^{-1}$ definert also eine prinzipale Polarisierung vom Typ $(K, \{1, \varphi\})$ durch E_{ξ_η} auf $A(O_K)$. Setze

$$\tau = \frac{1 + \sqrt{2} + \eta}{2} \text{ also } \tau^\varphi = \frac{1 - \sqrt{2} + \eta^\varphi}{2},$$

so haben wir

$$c_K =< O_{K_0} + \eta O_{K_0}, O_{K_0} + \tau O_{K_0} >$$

und

$$Im(\tau) > 0, Im(\tau^\varphi) < 0 \text{ und } Im(\varepsilon_0\tau) > 0, Im((\varepsilon_0\tau)^{\bar\varphi}) < 0.$$

Es ist

$$\mathcal{K}_1 = \{(\eta, \eta^\varphi), (\tau, \tau^\varphi)\} \text{ und } \mathcal{K}_2 = \{(\varepsilon_0\eta, (\varepsilon_0\eta)^{\bar\varphi}), (\varepsilon_0\tau, (\varepsilon_0\tau)^{\bar\varphi})\}.$$

Bezüglich dieser 4 Matrizen werten wir mit ausreichender Genauigkeit die absoluten Invarianten aus. Diese sind nicht sofort ganzzahlig, aber wir erkennen leicht die Zahl 3 als Nenner. Modifizieren wir $J_{10} = J_{10}/3^{10}$, so erhalten die Klassenpolynome ganzzahlige Koeffizienten.

$$\begin{aligned} H_1(x) &= -4436122759429753678599202540581722260054091836075474944 + \\ &\quad 381525124273795424338347585840230353111990272 * x + \\ &\quad 1114382831049881588644758757324 8 * x^2 - 12334779372287808 * x^3 + x^4 \end{aligned}$$

$$\begin{aligned} H_2(x) &= 992654810593085060923463266307771301834742824960000 - \\ &\quad 133157110713263153449611819544786894848000 * x + \\ &\quad 247215734483711854403519078400 * x^2 - 1184821385368320 * x^3 + x^4 \end{aligned}$$

$$\begin{aligned} H_3(x) &= 14998206047319118390384059091654559685792634968735744 - \\ &\quad 63272800568049529647784138686415907271475 2 * x + \\ &\quad 383328516161318855543139041280 * x^2 - 1479517382536704 * x^3 + x^4 \end{aligned}$$

$$\begin{aligned} H_4(x) &= -335609319004765824343284248330910235619229696000 0 + \\ &\quad 873550130386029652139661245169008640 00 * x + \\ &\quad 8127571136230077635690496000 * x^2 - 180366370375680 * x^3 + x^4 \end{aligned}$$

$$\begin{aligned} H_5(x) &= -1104029278218237189423272549645710893281266520705139 82 \\ &\quad 65274385706673766400000000000000000000 - 860128644934310070904 58 \\ &\quad 139678440237018017496118372209786880000000000000000 * x + \end{aligned}$$

$$591224668260456845101340958483839663619440640000000000 * x^2 -$$
$$1787890486522918138675200000 * x^3 + x^4$$

$$\begin{aligned} H_6(x) = {} & 385646564661177160370852903897568999543372041878329393 80 \\ & 265038903450326413858852918778561424675228260032830530577817604558 \\ & 95189567010647962453339956838 4 - 650527883056462950809321555836112 \\ & 768754808507880616233021170682251631959520667240604903669434666623 \\ & 722345932899764666368 * x + 600577173498453772021388881363362776566 79 \\ & 125794975012088248966659016832854550999203840 * x^2 \\ & -192232941838861716164685070490349114815938 56 * x^3 + x^4 \end{aligned}$$

Wir faktorisieren $H_1(x)$ und erhalten als Nullstelle eine in K^* ganzalgebraische Zahl.

$$\begin{aligned} j_0 = {} & 3^3 * (114210920113776 + 36043491068064\sqrt{7} + \\ & 320 * \sqrt{2} * (109351761656229340623787 + 40675435753200366690881 * \sqrt{7})^{1/2}). \end{aligned}$$

Beispiel 6: Es ist $\varepsilon \in U_1$

$$\begin{aligned} \text{Setze } a &= -(5 + 2\sqrt{6}), \\ K_0 &= \mathbb{Q}(\sqrt{6}) \text{ damit ist } |c_{K_0}| = 1, \\ K &= \mathbb{Q}(\sqrt{a}) \text{ damit ist } |c_K| = 1, \\ & \quad \text{mit Fundamentaleinheit } \varepsilon_0 = (5 + 2\sqrt{6}), \\ & \quad \text{also } N(\varepsilon_0) = N(5 + 2\sqrt{6}) = 1, \\ O_K &= O_{K_0} + \eta O_{K_0} \text{ mit } \eta = \frac{1 + \sqrt{6} + \sqrt{a}}{2}, \\ O_{K_0} &= \mathbb{Z} + \sqrt{6}\mathbb{Z} \\ & \quad \varphi \text{ sei die folgende Fortsetzung der Galoiskonjugation von } K_0/\mathbb{Q}: \\ (\sqrt{a})^{\varphi} &= -\sqrt{a^{\varphi}}. \end{aligned}$$

Weil $aa^{\varphi} = 1$ ein Quadrat in K_0 ist, ist $K/\mathbb{Q}$ galoisch. Weiterhin ist $q = a$ und $N(a) = 1$, so daß $K/\mathbb{Q}$ nicht zyklisch und damit K kein primitiver CM-Körper ist. Da $\varepsilon \in U_1$, sind die prinzipal polarisierten Abelschen Varietäten $A(\eta)$ und $A(\varepsilon_0\eta)$ isomorph. Es ist

$$\mathcal{K} = \{(\eta, \eta^{\varphi})\}$$

und wir berechnen

$$\begin{aligned} j_1 &= 50000, \quad j_2 = -40000 \\ j_3 &= -16000, \quad j_4 = 12800 \\ j_5 &= -819200000, \quad j_6 = -419430400000. \end{aligned}$$

Mit dem Buchbergeralgorithmus ist:

$$\begin{aligned} J_2 &= 10\, f, J_4 = -80\, f^2, \\ J_6 &= -320\, f^3, J_{10} = 2\, f^5 \text{ mit } f \in \mathbb{Z}. \end{aligned}$$

Hierzu gibt es allerdings keine Koeffizienten $f_2, f_3, ..., f_5$, die das Invariantengleichungssystem lösen. Das ist natürlich klar, da der zugrundegelegte CM-Körper nicht primitiv ist.

Literaturverzeichnis

[A-H] **L.M. Adleman, M-D.A. Huang**, Primality Testing and Abelian Varieties Over Finite Fields, Lecture Notes in Math. Springer Verlag Berlin Heidelberg 1992

[B-L-R] **S.Bosch, W. Lütkebohmert und M.Raynaud**, Neron models, Springer-Verlag Berlin Heidelberg New York, 1990.

[Beu] **Beutelsbacher, A. Pfau**, Chipkartensysteme, Springer-Verlag

[Bo I] **O. Bolza**, On binary sextics with linear transformations into themselves, Amer. J. Math.,10 (1888),47 - 70.

[Bo II] **O. Bolza**, Darstellung der rationalen ganzen Invarainten der Binärform sechsten Grades durch die Nullwerthe der zugehörigen ϑ-Function, Math. Ann. Bd. 30

[Cant] **D. Cantor**, Computing in the Jacobian of a hyperelliptic curve, Math. Comp., vol 48, number 177, (1987) 95 - 101

[El] **T.ElGamal**, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans.Inform.Theory, IT 31,1985,pp 469-472.

[F-R] **Gerhard Frey, Hans-Georg Rück** , A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves, preprint.

[He] **Erich Hecke**, Höhere Modulfunktionen und ihre Anwendung auf die Zahlentheorie, Math. Ann.,71 (1912),453-476.
Über die Konstruktion relativ-Abelscher Zahlkörper durch Modulfunktionen von zwei Variabeln, Math. Ann. 74 (1913),465-510.

[H-I] **M-D. Huang, Doug Ierardi**, Efficient Algorithms for the Riemann-Roch Problem and for Addition in the Jacobian of a Curve, IEEE Trans.Inform.Theory, July 1991, pp 678 - 687.

[Igusa] **J.I. Igusa** Arithmetic variety of moduli of genus two, Ann. Math. 72. 612-649 (1960).

[Ka] **W. Kampkötter**, Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven, Dissertation, Institut für Experimentelle Mathematik, Essen (1991) .

[La I] **Serge Lang**, Abelian Varieties, Interscience Pub., New-York 1959.

[La II] **Serge Lang**, Complex Multiplication , Springer-Verlag New York Berlin Heidelberg Tokyo, 1983.

[Le] **A.K. Lenstra. M.S. Manasse**, Factoring by electronic mail. Advances in Cryptology - Eurocrypt '89. Springer Lecture Notes in Computer Science 434 (1990),355-371. Berlin: Springer-Verlag 1990.

[Mi] **V.Miller**, Short programs for functions on curves, unpublishes manuscript, 1986

[Mum] **D.Mumford**, Ablian varieties, Second Edition, Oxford University Press, Oxford 1974

[Mum I,II] **D. Mumford**, Tata Lectures on Theta I,II, Birkhäuser, Boston, 1983/1984.

[P-H] **S.Pohlig, M.Hellman**, an improved algorithm for computing logarithms over GF(p) and its cryptographic significance, IEEE Trans.Inform.Theory, vol.IT-24,pp.106-110,1978.

[S-T] **Goro Shimura, Yutaka Taniyama**, Complex Multiplication of Abelian Varieties , the mathematical society of Japan, 1975

[Sh] **Goro Shimura** , Automorphic Functions and Number Theory, Lecture Notes in Mathematics, Springer-Verlag Berlin Heidelberg New York, 1968

[Spa I] **Anne-Monika Spallek**, Konstruktion einer elliptischen Kurve über einem endlichen Körper zu gegebener Punktegruppe, Diplomarbeit (1992), Institut für Experimentelle Mathematik, Essen

[Spa II] **Anne-Monika Spallek**, Dokumentation und Programme des Authentifikationssystems 'KASPA' basierend auf Kurven vom Geschlecht 2, Anhang zur Dissertation (1994), Institut für Experimentelle Mathematik, Pfad: /home/fitzel/anne/CEBIT, Dokumentation: Doku

[Sta] **Otto Staude**, Über die Parameterdarstellung der Verhältnisse der Thetafunktionen zweier Veränderlicher. Mathematische Annalen, Bd 24 Seite 286.

[We] **A. Weil**, Zum Beweis des Torellischen Satzes, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. (1957),33-53.