Über die Konstruktion algebraischer Kurven mittels komplexer Multiplikation

vorgelegt von
M. Sc. Mathematiker
Osmanbey Uzunkol
aus Kayseri

Von der Fakultät II-Mathematik und Naturwissenschaften
der Technischen Universität Berlin
zur Erlangung des akademischen Grades
Doktor der Naturwissenschaften
–Dr. rer. nat.–
genehmigte Dissertation

Promotionsauschuss:

Vorsitzender: Prof. Dr. Stefan Felsner, Technische Universität Berlin
Berichter: Prof. Dr. Dr. h. c. Michael E. Pohst, Technische Universität Berlin
Berichter: Prof. Dr. Franck Leprévost, Université du Luxembourg

Tag der wissenschaftlichen Aussprache: 29.06.2010

Berlin 2010

D 83

Inhaltsverzeichnis

Einleitung

Im Jahre 1896 bewies Hilbert ([Hil1896]) einen Satz, welcher später wegen der Vorarbeiten von Kronecker im Jahre 1853[1] und Weber im Jahre 1886 ([Wb1886]) als der Satz von **Kronecker-Weber** bekannt wurde. Dieser Satz besagt, dass jede abelsche Erweiterung von $\mathbb{Q}$ in einem Kreisteilungskörper enthalten ist. Dieser Kreisteilungskörper wird durch einen speziellen Wert der Funktion

$$z \mapsto e^{2\pi iz}$$

erzeugt. Dieser spezielle Wert, auch bekannt als der **singuläre Wert**, entspricht genau einem Punkt der endlichen Ordnung im Kreis $\mathbb{R}/\mathbb{Z}$.

Dieser Satz veranlasste Kronecker zu seinem **liebsten Jugendtraum** der Erzeugung aller abelschen Erweiterungen imaginär quadratischer Zahlkörper durch die singulären Werte bestimmter elliptischer Modulfunktionen. Seitdem zehren die Zahlentheoretiker von der Idee, alle abelschen Erweiterungen eines vorgegebenen Zahlkörpers K durch spezielle Werte geeigneter analytischer Funktionen zu erzeugen. Dieses als das 12. Problem von Hilbert[2] bekannte Programm erfuhr seine Bestätigung im Falle imaginär quadratischer Zahlkörper mit Hilfe der klassischen Theorie der komplexen Multiplikation (**CM-Theorie**). Die Theorie der komplexen Multiplikation bringt mittels der Wechselwirkung der Arithmetik des Körpers und der Geometrie der zugehörigen elliptischen Kurve verschiedene Aspekte der *drei großen Gausschen A*, Arithmetik, Algebra und Analysis, in eleganter Weise zusammen[3]. Die CM-Theorie verwirklicht damit den Jugendtraum von Kronecker. Das 12. Problem von Hilbert bleibt jedoch infolge des Fehlens der funktionentheoretischen Hilfsmittel ein offenes Problem für alle anderen Zahlkörper.

[1] in [Kr1853], Seite 10, schrieb Kronecker: ... ergiebt nämlich das bemerkenswerthe ... Resultat: *daß die Wurzel **jeder** Abelschen Gleichung mit ganzzahligen Coëffizienten als rationale Function von Wurzeln der Einheit dargestellt werden*

[2] D. Hilbert, *Mathematische Probleme* Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse, Vandenhoeck-Ruprecht, 1900, 3, 253-297

[3] Hilbert: *'The theory of complex multiplication of elliptic modular forms, which brings together number theory and analysis, was not only the most beautiful part of Mathematics but of all science',* International Congress of Mathematicians at Zürich, 1932, siehe Hilbert-Courant, Constance Reid, Springer Verlag, 1986.

Es ist zu bemerken, dass die eigentliche Vermutung von Hilbert für imaginär quadratische Zahlkörper wegen der Behauptung falsch war, dass jede abelsche Erweiterung eines imaginär quadratischen Zahlkörpers K der Diskriminante D durch die singulären Werte der $j-$Invariante erzeugt werden könne[1]. Nach der Theorie der komplexen Multiplikation elliptischer Modulfunktionen erzeugt der Wert $j(\tau)$ der j-Invariante mit $\tau \in \mathcal{O}_K$ zunächst, im Gegensatz zur Vermutung von Hilbert, die maximale abelsche unverzweigte Erweiterung $\mathcal{H}_K$ von K, den sogenannten **Hilbertklassenkörper**, dessen Galoisgruppe über K nach der Klassenkörpertheorie eine zur Klassengruppe von K isomorphe Gruppe ist. Der Grad von $\mathcal{H}_K$ über K ist daher genau die Klassenzahl h_K von K. Mittels dieser Isomorphie und der Eigenschaft, dass die singulären Werte der $j-$Invariante ganze algebraische Zahlen sind, kann der Körper $\mathcal{H}_K$ durch das **Hilbertklassenpolynom** $H_D(x) \in \mathbb{Z}[x]$, das Minimalpolynom von $j(\tau)$ über K, erzeugt werden. Durch die Adjunktion der geeigneten Werte der Weberschen Funktionen an den Hilbertklassenkörper H_K werden dann alle abelschen Erweiterungen von K erzeugt, siehe z. B. [Sil94].

Shimura und Taniyama ([Sh61]) verallgemeinerten die Theorie der komplexen Multiplikation auf die abelschen Varietäten. Sie ermöglicht es, gewisse abelsche Erweiterungen eines **CM-Körpers** K (eine total imaginäre quadratische Erweiterung eines total reellen Zahlkörpers K_0) zu erzeugen. Aber im Allgemeinen können nicht alle abelschen Erweiterungen mittels der CM-Theorie erzeugt werden.

Im Falle, dass der Grad des CM-Körpers K über $\mathbb{Q}$ vier ist, gibt es allerdings die von Igusa eingeführten absoluten Invarianten j_1, j_2 und j_3 einer hyperelliptischen Kurve $\mathcal{C}$ vom Geschlecht zwei, welche die Rolle der $j-$Invariante spielen und deren singuläre Werte eine unverzweigte Körpererweiterung erzeugen. Daher ist es möglich, explizite Polynome zu konstruieren, die diese Erweiterung erzeugen. Die Koeffizienten dieser Polynome sind rationale Zahlen.

Ursprünglich widmete man sich der Theorie der algebraischen Kurven und auch der Theorie der komplexen Multiplikation aus rein theoretischem Interesse, welches sich im Laufe der letzten 25 Jahren grundlegend änderte, so dass heutzutage die elliptischen Kurven und die hyperelliptischen Kurven vom Geschlecht zwei verschiedene Anwendungen vor allem in der Kryptographie, Codierungstheorie und der algorithmischen Zahlentheorie haben. Die Theorie der komplexen Multiplikation ermöglicht zum Beispiel die Konstruktion elliptischer Kurven und hyperelliptischer Kurven mit komplexer Multiplikation über endlichen Körpern, deren Jacobische vorgegebene Ordnung

[1] siehe auch, N. Schappacher, *On the history of Hilbert's twelfth problem: a comedy of errors*, Matériaux pour l'histoire des mathématiques au XXéme siécle (Nice, 1996), 243-273, Sémin. Congr., 3, Soc. Math. France, Paris.

besitzen. Diese Konstruktion spielt heutzutage sowohl in der Kryptographie, etwa bei der Realisierung gruppen- oder paarungsbasierter Kryptosysteme, siehe [BSS99], [BSS05] und [FST06], als auch bei Primzahlnachweisen, siehe [AtMr93], eine besonders wichtige Rolle. Der aufwendigste Teil dieser Konstruktionen ist die Berechnung der Klassenpolynome, deren Nullstellen nach der Reduktion modulo einer Primzahlpotenz q die Invarianten der reduzierten elliptischen und hyperelliptischen Kurven über $\mathbb{F}_q$ liefern, aus denen die entsprechenden Kurvengleichungen hergeleitet werden können.

Im Falle der elliptischen Kurven wachsen die Koeffizienten des Hilbertklassenpolynoms exponentiell mit dem Betrag der Diskriminante, und sind sogar für kleine Diskriminanten sehr groß. Zum Beispiel für die Diskriminante $D = -260$ haben wir das Hilbertklassenpolynom über $K = \mathbb{Q}(\sqrt{D})$

$$H_{-260}(x) = x^8 - 9997874035270492198400 \cdot x^7 - 9998961618958421018636902174720000 \cdot x^6 - 215070546007239462749413484981714944000000 \cdot x^5 + 463238908732347767153420578775505775886336000000 \cdot x^4 + 1486555780464986511315003407707666416737976320000000 \cdot x^3 + 859800832359880294057832490921895099181280788480000000 \cdot x^2 + 305486088367929951707960768526477860306636557516800000000000 \cdot x + 330294750567571502894677425666147267942635955814400000000000.$$

Eine **Klasseninvariante** ist ein singulärer Wert einer Modulfunktion g der Stufe N mit der Eigenschaft, dass $K(j(\tau)) = K(g(\tau))$ gilt. Die analytische Konstruktion elliptischer Kurven wird in der Praxis mittels singulärer Werte der sogenannten Klasseninvarianten von Weber oder deren Verallgemeinerungen ermöglicht. Der Vorteil dieser singulärer Werte ist also, dass die erzeugenden Klassenpolynome für diese Werte wesentlich 'kleinere' Koeffizienten als die Koeffizienten der Hilbertklassenpolynome besitzen. Für die obige Diskriminante $D = -260$ bekommen wir mit geeigneter Klasseninvariante das folgende Weberklassenpolynom, welches über K den gleichen Körper wie $H_{-260}(x)$ erzeugt:

$$W_{-260}(x) = x^8 - 8 \cdot x^7 + 12 \cdot x^6 + 8 \cdot x^5 - 27 \cdot x^4 + 8 \cdot x^3 + 12 \cdot x^2 - 8 \cdot x + 1.$$

Bei der Konstruktion hyperelliptischer Kurven gab es (im Gegensatz zu den elliptischen Kurven) bisher keine alternativen Invarianten, die Klassenpolynome mit kleineren Koeffizienten liefern, obgleich die Koeffizienten der Igusaklassenpolynome stärker als die Koeffizienten der Hilbertklassenpolynome mit dem Betrag der Diskriminante wachsen.

Die in **dieser Arbeit** entwickelten Algorithmen ermöglichen eine schnellere analytische Konstruktion der Klassenpolynome und damit eine schnellere Konstruktion algebraischer Kurven mit komplexer Multiplikation vom Geschlecht eins und zwei. Die Ergebnissen teilen sich grob in fünf Bereiche ein.

- Wir entwickeln eine Darstellung der Klasseninvariante mittels der The-

tanullwerte, deren singuläre Werte schneller zu berechnen sind als die singulären Werte der Klasseninvariante, die mittels der Quotienten der Dedekindschen $\eta-$Funktion dargestellt werden.

- Wir beweisen die Eigenschaft, dass fast alle Klasseninvarianten im Geschlecht eins Einheiten in den entsprechenden Ringklassenkörpern sind. Wir können somit in einigen Fällen bessere Invarianten erhalten. Mit Hilfe dessen führen wir außerdem einen Algorithmus ein, der die Einheitengruppen dieser Ringklassenkörper berechnet.

- Wir stellen auch die verallgemeinerten Klasseninvarianten mittels der Quotienten der Thetanullwerte dar und zeigen die Eigenschaft, dass die verallgemeinerten Klasseninvarianten Einheiten in den entsprechenden Ringklassenkörpern sind.

- Wir verallgemeinern das Verfahren der Bestimmung der Klasseninvarianten mittels des zweidimensionalen Shimuraschen Reziprozitätsgesetzes auf Geschlecht zwei. Das ermöglicht zum ersten Mal ein konstruktives Verfahren, welches überprüft, ob die singulären Werte bestimmter Siegelscher Modulfunktionen ein Klasseninvariantensystem der einfachen hauptpolarisierten abelschen Varietäten liefern.

- Wir erweitern die CM-Methode im Geschlecht zwei auf alle primitiven CM-Körper.

Zunächst werden im Kapitel 1 die grundlegenden Definitionen und Sätze aus der Theorie der hauptpolarisierten einfachen abelschen Varietäten und der Thetafunktionen bereitgestellt, die wir im Laufe der Arbeit benötigen werden.

Wir werden im zweiten Kapitel den Hauptsatz der CM-Theorie in der ideal- und ideltheoretischen Sprache beschreiben.

Im Kapitel 3 werden wir die Grundidee der CM-Methode der Konstruktion elliptischer und hyperelliptischer Kurven vom Geschlecht zwei einführen. Des Weiteren werden wir die in der Literatur eingeführten Algorithmen zusammenfassen. Ferner werden die Probleme, die bei diesen Konstruktionsmethoden vorkommen, erläutert.

Im Kapitel 4 werden die Verfahren von Schertz und Gee erklärt, die mittels des Shimuraschen Reziprozitätsgesetzes effizient testen, ob der singuläre Wert $g(\tau)$ einer Modulfunktion g der Stufe N an $\tau \in \mathbb{H}$ eine Klasseninvariante ist. Diese Methoden werden wir für beliebige Ordnungen imaginär quadratischer Zahlkörper formulieren. Dabei wird die Reziprozitätsabbildung auf eine Abbildung endlicher Gruppen $(\mathcal{O}_K/N\mathcal{O}_K)^*$ in $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ reduziert. Ferner ermöglicht das Shimurasche Reziprozitätsgesetz, die entsprechenden Konjugierten dieser Invarianten zu bestimmen. Als nächstes wird

die Darstellung der Klasseninvarianten mittels der Thetanullwerte gewährleistet, welche mittels der AGM-Methode (eng.: arithmetic-geometric mean) eine schnellere Berechnung der Klassenpolynome liefert. Ausserdem wird bewiesen, dass viele dieser Invarianten bereits Einheiten in den entsprechenden Ringklassenkörpern sind. Zusätzlich werden wir zeigen, dass wir in einigen Fällen sogar bessere Klasseninvarianten finden können. Im Falle, dass die Klasseninvarianten Einheiten sind, werden wir des Weiteren die Nullstellen eines Klassenpolynoms betrachten, die zusammen mit den Einheitswurzeln eine Untergruppe der Einheitengruppe des entsprechenden Ringklassenkörpers von endlichem Index bilden. Mittels der unteren Regulatorabschätzung und einer Methode der Vergrößerung dieser Gruppe, wird ein Algorithmus entwickelt, der die vollen Einheitengruppen solcher Körper berechnet. Ferner werden wir die Verallgemeinerungen der Klasseninvariante mittels der Thetanullwerte darstellen und zeigen, dass sie, wie im klassischen Fall, Einheiten sind. Abschließend werden wir auf die Frage der Optimalität dieser Invarianten eingehen.

Im Kapitel 5 werden wir das Verfahren von Gee ([GeSt98]) mit Hilfe des mehrdimensionalen Shimuraschen Reziprozitätzgesetzes auf hauptpolarisierte einfache abelsche Flächen verallgemeinern. Eine entsprechende galoistheoretische Interpretation des Körpers der arithmetischen Siegelschen Modulfunktionen der Stufe $(2, 4)$ von Sasaki wird dabei benutzt, um die konkrete Reziprozitätsabbildung von $(\mathcal{O}_K/N\mathcal{O}_K)^*$ in eine passende Untergruppe von $\mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z})$ zu formulieren. Somit erhalten wir unsere reduzierte Abbildung und einen Algorithmus, der mit Hilfe der Operation der Matrizen von $\mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z})$ auf die arithmetischen Siegelschen Modulfunktionen testet, ob ein System der Modulfunktionen (g_1, g_2, g_3) an dem CM-Punkt $\tau \in \mathbb{H}_2$ ein Klasseninvariantensystem liefert.

Abschließend werden wir im Kapitel 6 die Beispiele der Klassenpolynome angeben.

Ich möchte mich an dieser Stelle bei Herrn Prof. Dr. Dr. h. c. Michael E. Pohst ganz herzlich für seine wertvolle Hinweise, Unterstützung, Zusammenarbeit und für die Möglichkeit zu jeder Zeit mit Fragen zu ihm zu kommen, und die Erfahrungen, die ich durch ihn und KANT-Gruppe machen durfte bedanken.

Ferner danke ich Herrn Prof. Dr. Franck Leprévost für die Übernahme der Begutachtung dieser Arbeit und die mathematische Diskussionen, die wir während seiner Berlin Besuche durchgeführt haben. Mein besonderer Dank gebührt Herrn Prof. Dr. Florian Heß. Seine Unterstützung und sein Rat waren für mich sehr wichtig. Ferner danke ich besonders Jens Bauch, Juliane Krämer, Gerriet Möhlmann, Dr. Florin Nicolae und Dr. Marcus Wagner für die Hinweise bei der Erstellung dieser Arbeit.

Bu tez canım eşim Şermin'e ve birtanem küçük kızım Elif'ime ithaf edilmiştir. (Mein besonderer Dank gilt jedoch meiner Frau Şermin und meiner kleinen Tochter Elif. Ihnen ist diese Arbeit gewidmet.)

Kapitel 1

Grundlagen

In diesem Kapitel werden die in dieser Arbeit grundlegenden Definitionen und Aussagen aus der Theorie der hauptpolarisierten abelschen Varietäten mit komplexer Multiplikation und der Thetafunktionen bereitgestellt. Ferner werden wir die Aussagen über Endomorphismenringe dieser abelschen Varietäten zusammenstellen. Sämtliche Aussagen, falls sie nicht bewiesen oder explizit zitiert werden, sind aus [Mum70], [Sh97], [Lang73], [Lang83] und [Mil2] entnommen und werden zweckmäßig so dargelegt, wie wir sie im Laufe der Arbeit benötigen werden.

1.1 Abelsche Varietäten

Eine **Gruppen-Varietät** A über einem Körper k ist eine Varietät mit dem (abelschen) Gruppengesetz $+ : A \times A \to A$, so dass $+$ und ihre Inverse $- : A \to A$ stets $k-$Morphismen der Varietäten sind. Eine **abelsche Varietät** A über k ist eine projektive Gruppen-Varietät. Wir sagen, dass eine abelsche Varietät A über einem Teilkörper k' von k **definiert** ist, falls A als Gruppen-Varietät bereits über k' definiert ist. Der Körper k' heißt in diesem Fall ein **Definitionskörper** von A. Die Dimension einer abelschen Varietät A ist definiert als die Dimension von A als eine projektive Varietät.

Wir werden in dieser Arbeit insbesondere die abelschen Varietäten der Dimension eins und zwei über einem Körper k betrachten.

Es seien A und B zwei abelsche Varietäten über einem Körper k. Ein **Homomorphismus** λ zwischen A und B (ein **Endomorphismus** im Falle $A = B$) ist ein Morphismus von Varietäten $\lambda : A \to B$, für den stets $\lambda(x + y) = \lambda(x) + \lambda(y)$ für alle $x, y \in A$ gilt. Falls λ birational ist, heißt λ ein **Isomorphismus** zwischen A und B (und **Automorphismus** im Falle $A = B$).

Wir bezeichnen mit $\mathrm{Hom}(A,B)$ die Menge aller Homomorphismen von A nach B (und $\mathrm{End}(A) = \mathrm{Hom}(A,A)$). Die Menge der Homomorphismen $\mathrm{Hom}(A,B)$ ist ein freier $\mathbb{Z}-$Modul von endlichem Rang r, welcher durch

$$r \leq 4\ \dim(A)\dim(B) \tag{1.1}$$

nach oben beschränkt ist, siehe [Mum70], S. 178, corollary 1.

$\mathrm{End}(A)_{\mathbb{Q}} := \mathrm{End}(A) \otimes \mathbb{Q}$ hat die Struktur als $\mathbb{Q}-$Algebra, wobei $\mathrm{End}(A)$ als eine Ordnung in dieser Algebra betrachtet werden kann, siehe [Sh97], S. 4. Nun seien A und B zwei abelsche Varietäten der Dimension g. Ein Homomorphismus λ von A in B heißt eine **Isogenie**, falls λ einen endlichen Kern besitzt und surjektiv ist. Gegeben sei eine Isogenie $\lambda \in \mathrm{Hom}(A,B)$. Es sei k ein Definitionskörper für A und B, und $x \in A$ ein generischer Punkt im Sinne von [Weil46]. Dann heißen die Grade

$$v(\lambda) = [k(x) : k(\lambda x)],\ v_s(\lambda) = [k(x) : k(\lambda x)]_s,\ v_i(\lambda) = [k(x) : k(\lambda x)]_i \tag{1.2}$$

Grad, separabler Grad bzw. inseparabler Grad der Isogenie λ. Diese hängen nicht von der Wahl von k und x ab. Ferner gilt $|\mathrm{Kern}(\lambda)| = v_s$, siehe [Sh97], S. 4.

Der Kern ist nach dem Hauptsatz der endlichen abelschen Gruppen isomorph zu einer Gruppe

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \text{ mit } n_{i+1}|n_i,\ 1 \leq i \leq r-1. \tag{1.3}$$

Ist λ eine separable Isogenie, so nennen wir sie eine $(n_1, \cdots, n_r)-$Isogenie, wobei n_i, $1 \leq i \leq r$, wie in 1.3 sind.

Falls eine Untervarietät B einer abelschen Varietät A eine Untergruppe von A ist, heißt B eine **abelsche Untervarietät** von A. Eine abelsche Varität A der Dimension g heißt (absolut) **einfach**, falls sie über $\bar{k}$ nur die abelschen Untervarietäten $\{0\}$ und A hat. Jenes ist, wegen des vollständigen Irreduzibilitätssatzes von Poincaré ([Mum70], S. 173) gleichbedeutend damit, dass $\mathrm{End}(A)$ nullteilerfrei ist, und somit $\mathrm{End}(A)_{\mathbb{Q}} := \mathrm{End}(A) \otimes \mathbb{Q}$ eine Divisionsalgebra ist. Das Zentrum dieser Algebra ist entweder ein total reeller Zahlkörper vom Grad g (über $\mathbb{Q}$) oder eine total imaginäre quadratische Erweiterung K eines total reellen Körpers K_0 mit $[K_0 : \mathbb{Q}] = g$, die wir **CM-Körper** nennen. Wir haben bei dieser Arbeit stets die Annahme, dass $\mathrm{End}(A)_{\mathbb{Q}} := \mathrm{End}(A) \otimes \mathbb{Q}$ ein CM-Körper ist. Wir merken an, dass diese Einschränkung wegen [Lang83], S. 11, theorem 3.3, äquivalent dazu ist, dass A eine einfache abelsche Varietät ist.

Es sei $A(\mathbb{C})$ eine abelsche Varietät der Dimension g über $\mathbb{C}$. Dann ist $A(\mathbb{C})$ eine komplexe Lie-Gruppe und somit isomorph zu einem komplexen Torus

V/Λ, das heißt V ist ein $\mathbb{C}-$Vektorraum der Dimension g, und Λ ist ein Gitter vom Rang $2g$ (über $\mathbb{R}$) in $V \cong \mathbb{C}^g$ mit dem analytischen Isomorphismus

$$\beta : V/\Lambda \to A(\mathbb{C}). \tag{1.4}$$

Komplex-analytische Homomorphismen abelscher Varietäten sind im folgenden Sinne algebraisch:

Es seien $\beta' : V'/\Lambda' \to A'(\mathbb{C})$ ein analytischer Isomorphismus der Varietät A' und $\lambda : A \to A'$ ein algebraischer Homomorphismus. Dann existiert ein analytischer Homomorphismus λ' mit folgendem kommutativen Diagramm

$$\begin{array}{ccc} V/\Lambda & \xrightarrow{\beta} & A(\mathbb{C}) \\ \downarrow{\scriptstyle \lambda'} & & \downarrow{\scriptstyle \lambda} \\ V'/\Lambda' & \xrightarrow[\beta']{} & A'(\mathbb{C}) \end{array} . \tag{1.5}$$

Ferner liefert die Abbildung $\lambda \mapsto \lambda'$ einen Isomorphismus zwischen $\mathrm{Hom}(A, A')$ und $\mathrm{Hom}(V/\Lambda, V'/\Lambda')$. Der Homomorphismus λ kann somit durch eine $\mathbb{C}-$lineare Abbildung

$$\lambda' : V \to V' \tag{1.6}$$

dargestellt werden, welche das Gitter Λ auf Λ' mit $\lambda'\Lambda \subseteq \Lambda'$ abbildet.

Es sei $\beta : V/\Lambda \to A(\mathbb{C})$ ein komplex-analytischer Isomorphismus wie oben. Wir identifizieren V mit $\mathbb{C}^g$. Auf dem komplexen Torus $\mathbb{C}^g/\Lambda$ existiert eine reellwertige nicht-ausgeartete Bilinearform $E(x, y)$ mit folgenden Eigenschaften:

1. $E(ix, y)$ ist eine positiv definite symmetrische Form und $E(x, y) \in \mathbb{Z}$ für $(x, y) \in \Lambda \times \Lambda$ sowie

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

Diese Form heißt **Riemannform** auf Λ. Jede über $\mathbb{C}$ definierte abelsche Varietät ist somit isomorph zu einem komplexen Torus. Umgekehrt ist jeder komplexe Torus, auf dem eine Riemannform existiert, isomorph zu einer abelschen Varietät. Wir identifizieren jede abelsche Varietät A mit dem Paar $(\mathbb{C}^g/\Lambda, E)$ und schreiben $(A, E) = (\mathbb{C}^g/\Lambda, E)$. Dieses Paar heißt **polarisierte abelsche Varietät** mit der Polarisierung E. Wir merken an, dass die polarisierte abelsche Varietät (A, E) über $k \subset \mathbb{C}$ definiert ist, falls die abelsche Varietät A über k definiert ist, siehe [Sh97], S. 26.

Die abelschen Varietäten der Dimension eins sind die **elliptischen Kurven**. Alle eindimensionalen komplexen Tori $\mathbb{C}/\Lambda$ mit $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ sind elliptische Kurven und jede elliptische Kurve über $\mathbb{C}$ ist polarisierbar mit der eindeutigen Polarisierung $\Im(H)$, wobei H durch

$$H(z,\omega) = \left(\frac{z\bar{w}}{\Im(\omega_1\bar{\omega_2})}\right) \tag{1.7}$$

definiert ist, welches man leicht nachweisen kann.

Die Eigenschaft, dass jeder komplexe Torus zu einer elliptischen Kurve isomorph ist, gilt nicht mehr für die komplexen Tori $\mathbb{C}^g/\Lambda$, falls $g \geq 2$ ist.

Beispiel 1.1. *Die folgenden vier Vektoren sind über $\mathbb{R}$ linear unabhängig*

$$\omega_1 = (1,0),\ \omega_2 = (i,0),\ \omega_3 = (0,1),\ \omega_4 = (\alpha,\beta), \tag{1.8}$$

falls $\Im(\beta) \neq 0$ ist.

Es sei $\mathbb{C}^2/\Lambda$ der komplexe Torus, wobei das $4-$dimensionale Gitter Λ durch die vier Vektoren 1.8 erzeugt wird. Dann existiert auf dem Torus $\mathbb{C}^2/\Lambda$ keine Riemannform, daher gibt es keine abelsche Varietät, die zu $\mathbb{C}^2/\Lambda$ analytisch isomorph ist, siehe [Shaf97], S. 163 und 164.

1.2 Hauptpolarisierte abelsche Varietäten

Bezeichne E nun eine Riemannform auf dem Gitter Λ. Nach [Lang82], Kapitel VI, Teil 3, lemma 1, existiert eine sogenannte Frobeniusbasis $\{\lambda_1, \cdots, \lambda_{2g}\}$ von Λ, für die

$$(E(\lambda_i,\lambda_j))_{1\leq i,j\leq 2g} = \begin{pmatrix} 0 & \mathrm{D} \\ \text{-D} & 0 \end{pmatrix} \tag{1.9}$$

mit der Diagonalmatrix $D = \mathrm{diag}(d_1, \cdots, d_g)$, $d_i \in \mathbb{N}$ und $d_i | d_{i+1}$, gilt.

Die **Pfaffsche** einer Riemannform E ist die Determinante der Matrix D. Wir definieren den **Grad** der Polarisierung von $\mathbb{C}^g$ als die Pfaffsche von E. Im Falle, dass der Grad von E eins ist, heißt die abelsche Varietät **hauptpolarisiert**. Wir merken an, dass alle elliptischen Kurven mit 1.7 hauptpolarisiert sind.

Das Gitter mit der Frobeniusbasis $\{\lambda_1, \cdots, \lambda_{2g}\}$ kann in der Form $\omega_1\mathbb{Z}^g + \omega_2\mathbb{Z}^g$ mit

$$\omega_i = (\lambda_{1+(i-1)g}, \cdots, \lambda_{g+(i-1)g}) \tag{1.10}$$

angegeben werden. Die Matrix $\tau = \omega_1\omega_2^{-1}$ ist ein Element der $g-$dimensionalen Siegelschen oberen Halbebene $\mathbb{H}_g$, die aus den Matrizen der Form

$$\Omega = \Omega_1 + i\Omega_2$$

mit reellen $g \times g-$Matrizen Ω_1, Ω_2 besteht, wobei Ω_2 eine positiv definite Matrix ist. Deshalb ist dieses Gitter äquivalent zu $\Delta = \mathbb{Z}^g + \tau\mathbb{Z}^g$. Die Matrix τ heißt eine **Periodenmatrix** der hauptpolarisierten abelschen Varietät.

Für eine glatte projektive algebraische Kurve C ist das **Geschlecht** g von C die Dimension des Vektorraums der holomorphen $1-$Formen $H^0(\omega_C)$ mit der Basis $\{\omega_1, \cdots, \omega_g\}$.

Die **Jacobi-Varietät** von C ist dann definiert durch

$$J(C) = H^0(\omega_C)^*/\mathrm{Per}(\omega_1, \cdots, \omega_n), \tag{1.11}$$

wobei $H^0(\omega_C)^*$ der duale Vektorraum von $H^0(\omega_C)$ ist, und $\mathrm{Per}(\omega_1, \cdots, \omega_n)$ das Periodengitter von C ist.

Allgemein sind die Jacobi-Varietäten der algebraischen Kurven die hauptpolarisierten abelschen Varietäten. Ferner sind zwei algebraische Kurven C_1 und C_2 über einem algebraisch algeschlossenen Körper k nach dem Torellischen Satz ([Weil57]) genau dann isomorph, wenn die Jacobischen dieser Kurven als hauptpolarisierte abelsche Varietäten isomorph sind. Die einfachen Jacobischen Varietäten der hyperelliptischen Kurven vom Geschlecht zwei sind genau die hauptpolarisierten abelschen Varietäten der Dimension zwei. Es gibt allerdings für beliebiges Geschlecht $g > 2$ abelsche Varietäten, die nicht Jacobische einer hyperelliptischen Kurve sind, oder für $g > 3$ gar nicht Jacobische einer algebraischen Kurve sind.

1.3 Komplexe Multiplikation

Wir fixieren nun eine Einbettung $\mathbb{Q}^{\mathrm{al}} \hookrightarrow \mathbb{C}$.

Unter einem **CM-Typ** (K, Φ) verstehen wir einen CM-Körper K, $[K : \mathbb{Q}] = 2g$, mit der Menge $\Phi = \{\varphi_1, \cdots, \varphi_g\}$ der Einbettungen $K \hookrightarrow \mathbb{Q}^{\mathrm{al}}$, für die

$$\mathrm{Hom}(K, \mathbb{Q}^{\mathrm{al}}) = \Phi \cup \bar{\Phi} \tag{1.12}$$

gilt, wobei $\bar{\Phi} = \{\bar{\varphi_1}, \cdots, \bar{\varphi_g}\}$ und $\bar{\varphi_i}$ die komplex Konjugierte von Φ bzw. φ_i bezeichnen.

Es bezeichne nun L die galoissche Hülle von K mit $G = \mathrm{Gal}(L/\mathbb{Q})$,
$H = \mathrm{Gal}(L/K)$ und $H_0 = \mathrm{Gal}(L/K_0)$. Wir betrachten nun die Mengen

$$S := \{\sigma \in G : \sigma|_K = \varphi_i, \varphi_i \in \Phi\} \text{ und}$$

$$S^r := \{\sigma^{-1} : \sigma \in S\}.$$

Der CM-Typ (K, Φ) heißt **primitiv**, falls

$$H = \{\sigma \in G : \sigma S = S\} =: H'$$

gilt, welches nach der Galoistheorie im Falle der Dimension eins und zwei der Aussage entspricht, dass K keine CM-Teilkörper enthält. Der Fixkörper K^r zu $H^r := \{\sigma \in G : \sigma S^r = S^r\}$ heißt der **Reflexivkörper** von K.

Für den Reflexivkörper gilt

$$K^r = \mathbb{Q}(\{\sum_{i=1}^{g} \varphi_i(\xi) : \varphi_i \in \Phi, \xi \in K\}).$$

Der Reflexivkörper K^r ist auch ein CM-Körper. Der CM-Typ (K^r, Ψ) mit $\mathrm{Hom}(K^r, \mathbb{Q}^{\mathrm{al}}) = \Psi \cup \bar{\Psi}$ heißt der **Reflexivtyp** von (K, Φ). Die **Typ-Norm** Abbildung N_Ψ für ein Element $x \in K^r$ ist wie folgt definiert:

$$N_\Psi(x) = \prod_{\psi \in \Psi} \psi(x). \tag{1.13}$$

Dann gelten $y = N_\Psi(x) \in K$ und $y\bar{y} = N_{K^r/\mathbb{Q}}(x)$, siehe [Sh97], S. 63, proposition 29. Ferner bildet $N_\Psi(x)$ die Ideale (Idealklassen) von K^r auf die Ideale (bzw. die Idealklassen) von K im folgenden Sinne ab:

Es sei $\mathfrak{a}$ ein Ideal in K^r. Dann ist $\mathfrak{b}\mathcal{O}_L = \prod_{\psi \in \Psi} \mathfrak{a}^\psi \mathcal{O}_L =: N_\Psi(\mathfrak{a})$ ein Ideal in K, und gilt $\mathfrak{b}\bar{\mathfrak{b}} = N_{K^r/\mathbb{Q}}(\mathfrak{a})\mathcal{O}_K$, wobei $\mathcal{O}_L$ die Maximalordnung von L bezeichnet, siehe [Sh97], S. 63.

Wir sagen, dass eine abelsche Varietät A komplexe Multiplikation hat, falls $K \cong \mathrm{End}(A)_\mathbb{Q}$ gilt, d. h. es existiert eine Einbettung $\mathcal{O} \hookrightarrow \mathrm{End}(A)$, wenn $\mathcal{O}$ eine Ordnung in K (vom Grad $2g$) und A eine abelsche Varietät der Dimension g ist. Eine **abelsche Varietät vom Typ** (K, Φ) ist genau dann eine einfache abelsche Varietät, falls der CM-Typ (K, Φ) primitiv ist. Für die CM-Körper K vom Grad 4 entspricht dies genau den zyklischen und nicht-galoisschen Körpern mit $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$ ([Weng01], S. 22).

$\mathfrak{a}$ sei ein $\mathbb{Z}-$Untermodul eines CM-Körpers K und

$$\Phi(\mathfrak{a}) = \{\Phi(\alpha) = (\varphi_1(\alpha), \cdots, \varphi_g(\alpha))^{tr} \in \mathbb{C}^g : \alpha \in \mathfrak{a}\}. \tag{1.14}$$

Wir setzen nun

$$S_\Phi(\alpha) = S(\alpha) = \begin{pmatrix} \varphi_1(\alpha) & & \\ & \ddots & \\ & & \varphi_g(\alpha) \end{pmatrix}. \tag{1.15}$$

Dann beschreibt $\mathbb{C}^g/\Phi(\mathfrak{a})$ eine abelsche Varietät vom CM-Typ (K, Φ). Umgekehrt kann man jede abelsche Varietät vom CM-Typ (K, Φ) auf diese Art und Weise beschreiben, siehe dazu [Lang83], S. 15.

Wir betrachten nun den Fall $\mathrm{End}(A) = \mathcal{O}_K$. Es seien $\mathfrak{a}$ ein Ideal in $\mathcal{O}_K$ und $A(\mathfrak{a}) = \mathbb{C}^g/\Phi(\mathfrak{a})$ die wie oben definierte abelsche Varietät vom CM-Typ

(K, Φ). Dann gibt es ein Element $\xi \in K$ mit $K = K_0(\xi)$, ξ total imaginär und $-\xi^2$ total positiv in K_0 mit $\Im(\varphi_i(\xi)) > 0$ für $\varphi_i \in \Phi$. Für dieses Element können wir die Riemannform E_ξ für ein geeignetes $r \in \mathbb{Z}$ wie folgt angeben:

$$E_\xi(x, y) = r \cdot \sum_{i=1}^{g} \varphi_i(\xi)(\bar{x}_i y_i - x_i \bar{y_i}). \tag{1.16}$$

Umgekeht kann jede Riemannform, die der Bedingung

$$E(x, S_\Phi(\alpha)y) = E(S_\Phi(\bar{\alpha})x, y) \tag{1.17}$$

genügt, durch ein geeignetes solches $\xi \in K$ angegeben werden. Im Allgemeinen definiert ein solches ξ nicht eine hauptpolarisierte abelsche Varietät. Der folgende Satz charakterisiert, unter welcher Bedingung solche Elemente die hauptpolarisierten abelschen Varietäten im Falle der Dimension zwei definieren, siehe [Sh61], II.6.2, theorem 4:

Satz 1.2. *Es sei (K, Φ) ein CM-Typ, wobei K eine total imaginäre quadratische Körpererweitetung eines reell quadratischen Zahlkörpers K_0 ist. Es sei $\mathfrak{a}$ ein gebrochenes Ideal mit dem Gitter, welches von $\Phi(\mathfrak{a}) \in \mathbb{C}^2$ erzeugt wird. Dann operiert $\mathcal{O}_K$ auf $\Phi(\mathfrak{a})$ durch $a\Phi(u) = \Phi(au)$.*

Ferner ist die durch ein Element $\xi \in K$ induzierte Polarisierung genau dann eine Hauptpolarisierung, falls $\mathcal{D}_K \mathfrak{a}\bar{\mathfrak{a}} = (\xi)$ gilt, wobei $\mathcal{D}_K$ die absolute Differente von K bezeichnet.

Wir haben daher die folgende notwendige und hinreichende Bedingung, dass E_ξ eine Hauptpolarisierung auf $\mathbb{C}^2/\Phi(\mathfrak{a})$ induziert:

$$\exists\, \xi \in K \text{ mit } \mathcal{D}_K \mathfrak{a}\bar{\mathfrak{a}} = (\xi), \bar{\xi} = -\xi \text{ und } \Im(\phi(\xi)) > 0 \text{ für } \phi \in \Phi. \tag{1.18}$$

1.4 Endomorphismenringe über endlichen Körpern

Der Tate-Modul $T_p(A)$ einer abelschen Varietät A ist der $\mathbb{Z}_p-$Modul, der durch den projektiven Limes

$$T_p(A) = \varprojlim A[p^n]$$

definiert ist, wobei p eine Primzahl ist, $A[p^n]$ die p^n-Torsionspunkte von A bezeichnet, und der projektive Limes über allen positiven ganzen Zahlen $N \in \mathbb{N}$ mit dem Transitionsmorphismus, gegeben durch die Multiplikation-mit$-p$ Abbildung $A[p^{n+1}] \to A[p^n]$ gebildet wird, siehe [Tate66].

Es sei $\mathcal{C}$ eine hyperelliptische Kurve über einem endlichen Körper $\mathbb{F}_q$ der Charakteristik p. Die Frobeniusabbildung

$$(x, y) \to (x^q, y^q)$$

auf der Kurve $\mathcal{C}$ induziert einen Endomorphismus π auf der Jacobischen $J_\mathcal{C}$. Nun bezeichne $T_l(J_\mathcal{C})$ den Tate-Modul von $J_\mathcal{C}$ bezüglich $l \neq p$. Dann induziert der Frobenius-Endomorphismus π eine Abbildung auf den Vektorraum $V_l(J_\mathcal{C}) = \mathbb{Q}_l \otimes T_l(J_\mathcal{C})$. Das charakteristische Polynom

$$P(X) = \prod_{i=1}^{2g}(X - \pi_i)$$

dieser Darstellung besitzt ganzzahlige Koeffizienten, siehe [Sh97], S. 4. Die Gruppenordnung von $J_\mathcal{C}$ ist durch $P(1)$ gegeben. Jede abelsche Varietät A ist isogen zu dem Produkt

$$\prod_{i=1}^{r} A_i^{m_i},$$

wobei A_i einfache abelsche Varietäten der Dimension g_i sind. Nun gilt nach [Tate66], S. 139, theorem 1,

$$P_A(X) = \prod_{i=1}^{r} P_{A_i}(X)^{m_i},$$

wobei P_A und P_{A_i}, $1 \leq i \leq t$, die charakteristischen Polynome der jeweiligen Frobenius-Endomorphismen bezeichnen. Insbesondere gilt:

A und B sind genau dann isogen, falls $P_A = P_B$ ist.

Falls die Jacobische $J_\mathcal{C}$ nicht einfach ist, folgt daraus, dass das charakteristische Polynom P_A nicht irreduzibel ist, und die Faktoren von P_A genau zu den einzelnen abelschen Untervarietäten gehören. Die Gruppenordnung $P(1)$ ist in diesem Fall keine Primzahl und kann im Allgemeinen auch nicht annähernd prim sein, was in den vielen Anwendungen eine Voraussetzung ist, siehe Kapitel 3.

Aufgrund unserer Vorüberlegungen setzen wir nun voraus, dass das charakteristische Polynom P_A irreduzibel ist, so dass wir für die Gruppenordnung $P(1)$ eine Primzahl erhalten können. Wir schliessen damit auch den Fall aus, dass das Polynom P_A eine Primpotenz eines einzigen Polynoms ist, welches für den Fall des nicht kommutativen Endomorphismenringes von A vorkommen kann. Daher betrachten wir die einfachen abelschen Varietäten.

Wir setzen $\mathrm{End}(A)_\mathbb{Q} := \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$. Jeder Endomorphismus von A ist eine Isogenie, da A einfach ist. Der Frobenius-Endomorphismus π kommutiert mit jedem Endomorphismus von A. Es gilt ferner, dass $\mathbb{Q}(\pi)$ das gesamte

Zentrum von $\mathrm{End}(A)_{\mathbb{Q}}$ ist, siehe [Tate66], S. 140. Da P_A irreduzibel ist, gilt daher, dass $\mathrm{End}(A)_{\mathbb{Q}} = \mathbb{Q}(\pi)$ ist. Der Satz von Weil besagt, dass für alle Einbettungen von $\mathbb{Q}(\pi)$ stets $|\pi| = \sqrt{q}$ gilt, siehe [Sh97], S. 7.

Eine $q-$**Weil-Zahl** ω ist eine ganzalgebraische Zahl, so dass für alle Einbettungen $\psi : \mathbb{Q}(\omega) \hookrightarrow \mathbb{C}$ stets $|\psi(\omega)| = \sqrt{q}$ gilt. Der Fall $\pi = \pm\sqrt{q}$ tritt nur im Falle der supersingulären elliptischen Kurven auf. Daher muss π in allen Einbettungen echt komplex sein, da $P(X)$ irreduzibel ist. Die Zahlen $q = \pi\bar{\pi}$ und $t = \pi + \bar{\pi}$ sind offensichtlich total reelle Zahlen. Wir haben damit insgesamt die Eigenschaft, dass $\mathbb{Q}(\pi)$ eine total imaginäre Erweiterung des total reellen Körpers $\mathbb{Q}(t)$ ist, welche durch das Polynom

$$X^2 - tX + q$$

über $\mathbb{Q}(t)$ erzeugt ist. Somit ist $\mathbb{Q}(\pi)$ ein CM-Körper.

Für die anwendungsrelevanten hyperelliptischen Kurven über endlichen Körpern haben wir daher die Eigenschaft, dass die Jacobischen dieser Kurven komplexe Multiplikation mit einer Ordnung in einem CM-Körper besitzen.

1.5 Modulkörper

Es seien (A, E) eine polarisierte abelsche Varietät vom CM-Typ (K, Φ) und (K^r, Ψ) der Reflexivtyp von K. Dann existiert ein von (A, E) eindeutig bestimmter Zahlkörper k_0 mit der folgenden Eigenschaft:

k sei der Definitionskörper von (A, E), der den Körper k_0 enthält, und σ ein Isomorphismus von k nach einem anderen Zahlkörper. (A, E) ist isomorph zu (A^σ, E^σ) genau dann, falls σ auf k_0 die Identitätsabbildung ist, siehe [Sh97], S. 27.

Dieser Körper k_0 heißt der **Modulkörper** der polarisierten abelschen Varietät (A, E). Der Modulkörper k_0 ist in jedem Definitionskörper vom (A, E) enthalten, siehe [Sh97], S. 27, proposition 14.

Der Hauptsatz der komplexen Multiplikation beschreibt die Körpererweiterung $k_0^r = K^r k_0$ über K^r klassenkörpertheoretisch, worauf wir im nächsten Kapitel, insbesondere für die polarisierten abelschen Varietäten der Dimension eins und zwei, näher eingehen werden.

Modulkörper elliptischer Kurven

Es seien E eine elliptische Kurve über $\mathbb{C}$ und $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ ein zweidimensionales Gitter über $\mathbb{R}$. Dann ist sie analytisch isomorph zu einem komplexen Torus $\mathbb{C}/\Lambda$, und wegen 1.7 existiert eine Riemannform auf jedem komplexen Torus $\mathbb{C}/\Lambda$, daher ist jeder komplexe Torus isomorph zu einer

elliptischen Kurve über $\mathbb{C}$. Die $j-$Invariante der elliptischen Kurve E entspricht damit der $j-$Invariante vom zu E isomorphen komplexen Torus $\mathbb{C}/\Lambda$, die wir mittels der Eisensteinschen Reihen

$$g_2(\tau) = 60 \sum_{\omega \in \Lambda_\tau, \omega \neq 0} \frac{1}{\omega^4},\ g_3(\tau) = 140 \sum_{\omega \in \Lambda_\tau, \omega \neq 0} \frac{1}{\omega^6} \text{ für } \Lambda_\tau = \tau\mathbb{Z} + \mathbb{Z}, \quad (1.19)$$

durch

$$j(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3^2} \quad (1.20)$$

definieren, wobei $\tau = \frac{\omega_1}{\omega_2}$ ein Element der oberen Halbene $\mathbb{H}$ ist. Wir merken an, dass die Gitter Λ und Λ_τ homothetisch sind, und daher die gleiche $j-$Invariante besitzen.

Satz 1.3. *Im Falle der Dimension eins ist $\mathbb{Q}(j)$ der Modulkörper der elliptischen Kurve E über $\mathbb{C}$, wobei j die $j-$Invariante der Kurve E bezeichnet.*

Beweis: Da jede elliptische Kurve eine eindeutige Polarisierung 1.7 besitzt, folgt aus jeder Isomorphie zwischen E und E^σ als polarisierte abelsche Varietäten auch eine Isomorphie zwischen den Kurven E und E^σ über dem Definitionskörper k von E und E^σ. (Wir merken an, dass k genau der Definitionskörper von E ist, falls k der Definitionskörper von E als polarisierte abelsche Varietät ist.) Nun gilt $E \cong E^\sigma$ genau dann, wenn $j(E) = j(E^\sigma) = \sigma(j(E))$ ist. Dies bedeutet, dass j von σ fixiert wird, somit auch der Körper $\mathbb{Q}(j)$. □

Ferner existiert zu jeder elliptischen Kurve E über $\mathbb{C}$ eine über $\mathbb{Q}(j)$ definierte elliptische Kurve E', siehe [Sil94], S. 50, proposition 1.4. Daher stimmen der Modulkörper und der Definitionskörper der elliptischen Kurven bis auf Isomorphie überein. Im Allgemeinen stimmen diese beiden Körper sogar im Falle, dass die Charakteristik des Körpers $\neq 2, 3$ ist, überein ([Sil94], S. 50). Allerdings ist der Modulkörper einer abelschen Varietät A im Allgemeinen nur ein Teilkörper des Definitionskörpers von A, siehe [DeEm99], S. 42.

Um den Modulkörper über $\mathbb{Q}$ der hauptpolarisierten abelschen Varietäten der Dimension zwei, die hauptpolarisierten **abelschen Flächen**, vom CM-Typ (K, Φ) zu bestimmen, welcher durch die Auswertung bestimmter Modulfunktionen bestimmt wird, brauchen wir einige Aussagen aus der Theorie der Thetafunktionen, die wir im nächsten Abschnitt näher erläutern werden.

1.6 Thetafunktionen

Es bezeichne $\mathbb{H}_g$ die Siegelsche obere Halbebene der Dimension g mit $\Omega \in \mathbb{H}_g$, das heißt die Menge $\mathbb{H}_g$ aus allen $g \times g$ symmetrischen Matrizen besteht, deren

Imaginärteil positiv definit sind. Die **Riemann-Thetafunktion** ist definiert durch

$$\theta(z,\Omega) = \sum_{n\in\mathbb{Z}^g} \exp(\pi i(n^t\Omega n + 2n^t z)) \tag{1.21}$$

für einen Spaltenvektor $z \in \mathbb{C}^g$. Die **Thetacharakteristiken** für $\delta, \epsilon \in (\mathbb{Z}/2\mathbb{Z})^g$ sind durch die folgende Gleichung gegeben, siehe [Weng01], S. 11:

$$\theta\left[\delta,\epsilon\right](z,\Omega) = \sum_{n\in\mathbb{Z}^g} \exp\left(\pi i\left[(n+\frac{1}{2}\delta)^t\Omega(n+\frac{1}{2}\delta) + 2(n+\frac{1}{2}\delta)^t(z+\frac{1}{2}\epsilon)\right]\right). \tag{1.22}$$

Aus der Gleichung 1.22 folgt stets die folgende Gleichung:

$$\theta\left[\delta,\epsilon\right](-z,\Omega) = (-1)^{\delta^t\epsilon}\theta\left[\delta,\epsilon\right](z,\Omega). \tag{1.23}$$

Wir setzen nun $z = 0$, dann erhalten wir die **Thetanullwerte**, siehe [Weng01], S. 11:

Bemerkung 1.4. *1. Die Thetanullwerte für $\delta^t\epsilon \equiv 1 \bmod 2$ verschwinden identisch. Dies kann man leicht aus der Definition 1.22 verifizieren. Diese Werte heißen die **ungeraden** Thetanullwerte. Falls wir im Gegensatz $\delta^t\epsilon \equiv 0 \bmod 2$ haben, dann nennen wir sie die **geraden** Thetanullwerte.*

2. Daher haben wir für ein gegebenes g stets $2^{g-1}(2^g+1)$ gerade und $2^{g-1}(2^g-1)$ ungerade Thetanullwerte in $\mathbb{H}_g$.

Mittels der geeigneten Quotienten der geraden Thetanullwerte kann man die Invarianten der elliptischen Kurven und der hyperelliptischen Kurven vom Geschlecht zwei erhalten.

Elliptische Kurven

Nun betrachten wir die Thetanullwerte für $g = 1$. Es gelten die folgenden Gleichungen für $\tau \in \mathbb{H}$:

1. $\theta_{00}(\tau) := \theta[0,0](0,\tau) = \sum_{n\in\mathbb{Z}} q^{n^2/2}$,
2. $\theta_{10}(\tau) := \theta[1,0](0,\tau) = \sum_{n\in\mathbb{Z}} q^{(n+\frac{1}{2})^2/2}$,
3. $\theta_{01}(\tau) := \theta[0,1](0,\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2/2}$,
4. $\theta_{11}(\tau) := \theta[1,1](0,\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{(n+\frac{1}{2})^2/2}$.

Die $\Delta-$Funktion ist definiert als der Nenner der Gleichung 1.20, d. h. es gilt $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$. Die geraden Thetanullwerte und die $\Delta-$Funktion erfüllen die folgende Identität, siehe [ShGo97], S. 777:

$$\Delta(\tau) = 16\pi^{12}\theta_{00}(\tau)^8\theta_{01}(\tau)^8\theta_{10}(\tau)^8. \tag{1.24}$$

Die absolute Invariante j einer elliptischen Kurve über $\mathbb{C}$ erfüllt die folgende Gleichung für jedes $\tau \in \mathbb{H}$, siehe [Gua04], S. 254:

$$j(\tau) = 32\frac{\theta_{00}(\tau)^8 + \theta_{01}(\tau)^8 + \theta_{10}(\tau)^8}{\theta_{00}(\tau)^8\theta_{01}(\tau)^8\theta_{10}(\tau)^8}. \tag{1.25}$$

Hyperelliptische Kurven

Wir erhalten die folgenden Vektoren, die die geraden Thetanullwerte der Dimension $g = 2$ liefern:

$$a_1 := \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, a_2 := \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, a_3 := \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, a_4 := \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, a_5 := \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

$$a_6 := \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, a_7 := \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, a_8 := \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, a_9 := \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, a_{10} := \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Dann sind die geraden Thetanullwerte

$$\theta_i := \theta[a_i], 1 \leq i \leq 10. \tag{1.26}$$

Es sei T die Menge aller geraden Thetanullwerte der Dimension 2. Dann besteht die Menge

$$S = \{C \subset T : |C| = 4, \sum_{c \in C} c \in \mathbb{Z}^4\} \tag{1.27}$$

aus 15 Untermengen von T. Jede solche Untermenge besteht aus 4 geraden Thetanullwerten, siehe [Str10], S. 30. Eine Menge $\{b, c, d\} \subset T$ heißt **Syzygie**, falls sie eine Untermenge von einem Element der Menge S ist. Insgesamt haben wir daher 60 Syzygie-Untermengen von T. Wir definieren nun

1. $h_4 := \sum_{c \in T} \theta[c]^8$,
2. $h_6 := \sum_{b,c,d \in T, \{b,c,d\}\ \text{Syzygie}} \pm(\theta[b]\theta[c]\theta[d])^4$,
3. $h_{10} := \prod_{c \in T} \theta[c]^2$,
4. $h_{12} := \sum_{C \in S} \prod_{c \in T-C} \theta[c]^4$.

Es sei $\Omega \in \mathbb{H}_2$. Im Falle, dass $h_{10}(\Omega) \neq 0$ ist, welches genau der einfachen polarisierten abelschen Varietät entspricht ([ShGo97], S. 777) definieren die folgenden Funktionen die Invarianten einer hyperelliptischen Kurve $\mathcal{C}$ über $\mathbb{C}$ vom Geschlecht zwei, siehe [Igu60-I], S. 848, und auch [Bol1887]:

1. $I_2(\mathcal{C}) := h_{12}(\Omega)/h_{10}(\Omega)$,
2. $I_4(\mathcal{C}) := h_4(\Omega)$,
3. $I'_6(\mathcal{C}) := h_6(\Omega)$,
4. $I_{10}(\mathcal{C}) := h_{10}(\Omega)$,

Aus diesen Invarianten erhält man die absoluten Igusa-Invarianten durch

$$j_1 = \frac{I_2^5}{I_{10}}, j_2 = \frac{I_2^2}{I_{10}}, j_3 = \frac{I_2^3 I_4}{I_{10}}. \tag{1.28}$$

Man definiert in der Literatur auch andere Klasseninvarianten, die in der $\mathbb{Q}-$Algebra der homogenen Elemente vom Grad 0 von $\mathbb{Q}[I_2, I_4, I'_6, I_{10}^{-1}]$ liegen. Ein alternatives Invariantensystem ist durch

$$i_1 := \frac{2^8 I_4 I'_6}{I_{10}}, i_2 := \frac{2^5 I_2 I_4^2}{I_{10}}, i_3 := \frac{2^{14} I_4^5}{I_{10}^2}. \tag{1.29}$$

gegeben, siehe [Str10].

Es sei nun (A, E) eine hauptpolarisierte abelsche Varietät vom CM-Typ (K, Φ) der Dimension zwei. Dann existiert eine Periodenmatrix $\Omega \in \mathbb{H}_2$, die von $\mathcal{O}_K$, der Polarisierung, und dem Typ Φ abhängig ist, und für die

$$(A, E) \cong \mathbb{C}^2/\Omega\mathbb{Z}^2 + \mathbb{Z}^2$$

gilt. Der Modulkörper vom A ist in diesem Fall von den absoluten Igusa Invarianten erzeugt, siehe [Spa94], S. 75, 76, und [Igu60-II], S. 641. Wir werden daher im nächstem Kapitel die Erweiterung

$$K^r(j_1(\Omega), j_2(\Omega), j_3(\Omega)) = K^r(i_1(\Omega), i_2(\Omega), i_3(\Omega))$$

über dem Reflexivkörper K^r von K klassenkörpertheoretisch mit Hilfe des Hauptsatzes der komplexen Multiplikation beschreiben.

Kapitel 2

Hauptsätze der komplexen Multiplikation

In diesem Kapitel werden wir den Hauptsatz der komplexen Multiplikation erklären. Dieser beschäftigt sich mit der Primidealzerlegung eines Endomorphismus π einer hauptpolarisierten abelschen Varietät (A, E) mit komplexer Multiplikation, welcher modulo p Frobenius-Endomorphismus wird. Der Hauptsatz ermöglicht die klassenkörpertheoretische Beschreibung der Galoisgruppe vom Kompositum $k_0^r = k_0 K^r$ über K^r, wobei k_0 der Modulkörper von (A, E), und K^r der Reflexivkörper von K ist. Ferner beschreibt der Hauptsatz die Galoisgruppe des Körpers $k_0^r(F(A_{\mathrm{tor}}))$ über k_0^r, wobei $F(A_{\mathrm{tor}})$ das Bild der Menge der Torsionspunkte von A unter einer geeigneten Funktion F bezeichnet. Sämtliche Aussagen, die nicht bewiesen oder explizit zitiert werden, sind aus [Sh97], [Sh71], [Lang83] und [Mil1] entnommen. Die Aussagen aus der Klassenkörpertheorie sind in [CaFr67], [Neu92] und [Jan73] zu finden.

2.1 Idealtheoretische Fassung

Es seien $k \subset \mathbb{C}$ ein algebraischer Zahlkörper und $\mathfrak{m}$ ein ganzes Ideal in k. Für ein Element $\alpha \in k$ schreiben wir $\alpha \equiv 1 \bmod {}^{\times}\mathfrak{m}$, falls ganze zu $\mathfrak{m}$ teilerfremden Ideale $\mathfrak{r}$ und $\mathfrak{n}$ mit $(\alpha - 1)\mathfrak{r} = \mathfrak{m}\mathfrak{n}$ existieren. Ferner bezeichne $I_k(\mathfrak{m})$ die Gruppe aller zu $\mathfrak{m}$ teilerfremden Ideale, $P_k(\mathfrak{m})$ die Untergruppe aller Hauptideale (α) mit $\alpha \in k$, $\alpha \equiv 1 \bmod {}^{\times}\mathfrak{m}$ von $I_k(\mathfrak{m})$. Die Faktorgruppe $\mathrm{Cl}_k(\mathfrak{m}) = I_k(\mathfrak{m})/P_k(\mathfrak{m})$ heißt die Gruppe der **Idealklassen** modulo $\mathfrak{m}$. Mit $h_{\mathfrak{m}}$ bezeichnen wir die Ordnung von $\mathrm{Cl}_k(\mathfrak{m})$, welche wir die **Klassenzahl** von k modulo $\mathfrak{m}$ nennen. Eine Untergruppe $C_M(\mathfrak{m})$ von $I_k(\mathfrak{m})$ heißt eine **Kongruenzuntergruppe**, falls $P_k(\mathfrak{m}) \subseteq C_M(\mathfrak{m})$ ist.

Es sei (A, E) eine hauptpolarisierte abelsche Varietät vom primitiven

CM-Typ (K, Φ), $[K : \mathbb{Q}] = 2g$, mit dem Reflexivtyp (K^r, Ψ). Ferner sei K_0 der total reelle Teilkörper von K mit $[K_0 : \mathbb{Q}] = g$ und $\mathcal{O}_K$ die Maximalordnung von K. Dann existiert ein algebraischer Zahlkörper k mit folgenden Eigenschaften:

1. k ist normal über K^r,
2. A ist definiert über k,
3. Zu jedem $\sigma \in \mathrm{Gal}(k/K^r)$, sind alle Elemente von $\mathrm{Hom}(A, A^\sigma)$ definiert über k.

Es sei nun k_0 der Modulkörper von (A, E) und $k_0^r = k_0 K^r$. Dann gilt $K^r \subseteq k_0^r \subseteq k$, siehe [Sh97], S. 65 und 110.

Satz 2.1. *Die Menge*

$$\mathcal{C}(K) = \{(\mathfrak{a}, \alpha) | \mathfrak{a} \textit{ ist gebrochenes } \mathcal{O}_K - \textit{Ideal mit } \mathfrak{a}\bar{\mathfrak{a}} = (\alpha) \textit{ und } \alpha \in K_0 \textit{ ist total positiv}\} / \sim$$

bildet eine Gruppe mit dem Einselement $(\mathcal{O}_K, 1)$, wobei $\sim$

$$(\mathfrak{a}, \alpha) \sim (\mathfrak{b}, \beta) :\Leftrightarrow \exists \mu \in K \textit{ mit } \mu\mathfrak{b} = \mathfrak{a} \textit{ und } \alpha = \beta\mu\bar{\mu}$$

eine Äquivalenzrelation ist. Die Multiplikation in der Gruppe $\mathcal{C}(K)$ ist durch komponentenweise Multiplikation erklärt.

Ferner seien $Cl^0(\mathcal{O}_{K_0})$ die enge Klassengruppe von K_0 und $(\mathcal{O}_{K_0}^*)^+$ die von den positiven Einheiten von $\mathcal{O}_{K_0}$ erzeugte Gruppe. Dann ist die folgende Sequenz exakt:

$$1 \longrightarrow (\mathcal{O}_{K_0}^*)^+ / N_{K/K_0}(\mathcal{O}_K^*) \longrightarrow \mathcal{C}(K) \longrightarrow Cl(\mathcal{O}_K) \longrightarrow Cl^0(\mathcal{O}_{K_0}) \longrightarrow 1, \tag{2.1}$$

wobei die Abbildungen

$$(\mathcal{O}_{K_0}^*)^+ / N_{K/K_0}(\mathcal{O}_K^*) \to \mathcal{C}(K),\ u \mapsto (\mathcal{O}_K, u),$$

und

$$\mathcal{C}(K) \to Cl(\mathcal{O}_K),\ (\mathfrak{a}, \alpha) \mapsto \mathfrak{a}$$

gegeben sind.

Beweis: Die Eigenschaft, dass $\mathcal{C}(K)$ eine Gruppe ist, und die Exaktheit an $(\mathcal{O}_{K_0}^*)^+ / N_{K/K_0}(\mathcal{O}_K^*)$ folgen aus [Sh97], S. 106 und 107. Die Exaktheit an den anderen Gruppen folgt aus [ShGo97], S. 784. □

Die Gruppe $\mathcal{C}(K)$ operiert auf die Menge $\mathcal{K}(K,\Phi)$ aller Isomorphieklassen der hauptpolarisierten abelschen Varietäten, welche für den Typ Φ komplexe Multiplikation mit der Maximalordnung $\mathcal{O}_K$ besitzen. Es gilt nach [Sh97], S. 107, section 14.6:

$$|\mathcal{C}(K)| = |\mathcal{K}(K,\Phi)|. \tag{2.2}$$

Es seien (A,E) und (A',E') zwei abelsche Varietäten vom primitiven CM-Typ (K,Φ). Ferner sei $\lambda \in \mathrm{Hom}(A,B)$. Dann existiert zu λ ein Ideal $\mathfrak{a}$ von $\mathcal{O}_K$, so dass es einen Definitionskörper k von A und A' gibt, für den folgende Eigenschaft gilt (siehe [Sh97], S. 47):

$k(\lambda x)$ ist das Kompositum aller Körper $k(\alpha x)$, $\alpha \in \mathfrak{a}$ für jeden generischen Punkt $x \in A$.

Ein solcher Homomorphismus λ heißt eine $\mathfrak{a}-$**Multiplikation** von A in A'. Ferner heißt A' eine $\mathfrak{a}-$**Transformation** von A, falls es eine $\mathfrak{a}-$Multiplikation λ von A nach A' gibt.

Zu jeder $\mathfrak{a}-$Multiplikation λ existiert ein von λ abhängiges total positives Element α mit $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$, somit ein Element $(\mathfrak{a},\alpha) \in \mathcal{C}(K)$, siehe [Sh97], S.106, proposition 7. Es seien $\mathcal{P} = (A,E)$, $\mathcal{P}_2 = (A_2,E_2)$ und $\mathcal{P}_3 = (A_3,E_3)$ hauptpolarisierte abelsche Varietäten vom primitiven CM-Typ (K,Φ). Mit

$$\{\mathcal{P}_1 : \mathcal{P}\} = (\mathfrak{a},\alpha) \in \mathcal{C}(K)$$

bezeichnen wir die Klasse, die nicht von der Wahl von λ abhängt, siehe [Sh97], S. 107.

Wir haben nun den folgenden Satz ([Sh97], S. 107 bis 109):

Satz 2.2. *Es gelten die folgenden Eigenschaften:*

1. $\{\mathcal{P}_2 : \mathcal{P}_1\}\{\mathcal{P}_1 : \mathcal{P}\} = \{\mathcal{P}_2 : \mathcal{P}\}$,
2. $\mathcal{P} \cong \mathcal{P}_1$ *genau dann, wenn* $\{\mathcal{P}_1 : \mathcal{P}\} = (\mathcal{O}_K, 1)$ *ist,*
3. $\mathcal{P}_1 \cong \mathcal{P}_2$ *genau dann, wenn* $\{\mathcal{P}_1 : \mathcal{P}\} = \{\mathcal{P}_2 : \mathcal{P}\}$ *ist,*
4. $\mathcal{P}, \mathcal{P}_1$ *seien über* k *definiert, und* τ *ein* K^r-*Isomorphismus von* k *nach einem Körper* k'*, dann sind* $\mathcal{P}^\tau, \mathcal{P}_1^\tau$ *vom Typ* (K,Φ)*. Es gilt ferner* $\{\mathcal{P}_1^\tau : \mathcal{P}^\tau\} = \{\mathcal{P}_1 : \mathcal{P}\}$.

Wir wollen nun die Erweiterung k_0^r über K^r beschreiben. Nach 2.2, 4, sind $\mathcal{P}^\sigma$ und $\mathcal{P}$ vom primitiven CM-Typ (K,Φ), wobei $\sigma \in \mathrm{Gal}(k/K^r)$ ist. Wir setzen

$$[\sigma] = \{\mathcal{P}_\sigma : \mathcal{P}\}.$$

Nach 2.2 gilt für $\sigma, \tau \in \mathrm{Gal}(k/K^r)$

$$[\sigma][\tau] = [\sigma\tau].$$

Deshalb haben wir einen Homomorphismus von $\mathrm{Gal}(k/K^r)$ nach $\mathcal{C}(K)$, der durch $\sigma \mapsto [\sigma]$ gegeben ist. Ein Element σ ist genau dann im Kern H dieses Homomorpshimus, wenn $\mathcal{P} \cong \mathcal{P}^\sigma$ gilt. Nach dem ersten Kapitel ist H bereits die Gruppe der Elemente von $\mathrm{Gal}(k/K^r)$, die die Elemente von k_0^r invariant lassen. Dazu ist gleichbedeutend, dass die Abbildung $\sigma \mapsto [\sigma]$ ein injektiver Homomorphismus von $\mathrm{Gal}(k_0^r/K^r)$ in $\mathcal{C}(K)$ ist. Die Erweiterung k_0^r/K^r ist daher abelsch. Die Gruppen $\mathcal{C}(K)$ und $\mathrm{Gal}(k_0^r/K^r)$ sind sogar nach [Sh97], S. 111, isomorph.

Wir betrachten nun die Reduktion von A modulo Primidealen von k. Nach [Sh97], S. 95, proposition 25, hat A gute Reduktion für fast alle Primideale von k. Es sei $\mathfrak{m}$ das Produkt der Primideale $\mathfrak{p}$ von K^r, die eine der folgenden Eigenschaften haben:

1. Es existiert ein Primideal $\mathfrak{P}$ von k über $\mathfrak{p}$, für das A schlechte Reduktion hat,
2. $\mathfrak{p}$ ist in k_0^r verzweigt.

Nun sei $\mathfrak{p}$ ein Ideal in K^r, welches $\mathfrak{m}$ nicht teilt, und $\mathfrak{P}$ ein Ideal in k über $\mathfrak{p}$. Aufgrund unserer Definition hat dann A^σ für jedes Element $\sigma \in \mathrm{Gal}(k/K^r)$ gute Reduktion modulo $\mathfrak{P}$. Mit $\tilde{A}$ bezeichnen wir die Reduktion von A modulo $\mathfrak{P}$. Mit σ bezeichnen wir den Frobenius-Automorphismus σ von k für $\mathfrak{P}/\mathfrak{p}$. Wir identifizieren $\tilde{A}^q$ mit der Reduktion von A^σ modulo $\mathfrak{P}$, wobei $N(\mathfrak{p}) = q$ ist. Wir setzen

$$\mathfrak{q} = g(\mathfrak{p}), \tag{2.3}$$

mit $\mathcal{O}_L g(\mathfrak{p}) = N_\Psi(\mathfrak{p})$, wobei N_Ψ die in 1.13 definierte Typ-Norm Abbildung, und L die galoische Hülle von K ist. Dann ist der $q-$Frobenius Homomorphismus π von $\tilde{A}$ nach $\tilde{A}^q$ die Reduktion modulo $\mathfrak{P}$ einer $\mathfrak{q}-$Multiplikation λ von A in A^σ. Es gilt ferner, siehe [Sh97], S. 111:

$$[\sigma] = (g(\mathfrak{p}), N(\mathfrak{p})). \tag{2.4}$$

Dies bedeutet, dass wir für jedes Ideal $\mathfrak{a} \in I_{K^r}(\mathfrak{m})$ wegen 2.3 und der Eigenschaften von N_Ψ nach dem ersten Kapitel stets

$$[\sigma(\mathfrak{a})] = (g(\mathfrak{a}), N(\mathfrak{a})) \tag{2.5}$$

haben, falls wir für jedes Ideal $\mathfrak{a} \in I_{K^r}(\mathfrak{m})$ mit der Idealfaktorisierung $\mathfrak{a} = \prod \mathfrak{p}^{e(\mathfrak{p})}$ stets

$$\sigma(\alpha) = \prod_{\mathfrak{p}} \sigma(\mathfrak{p})^{e(\mathfrak{p})}$$

setzen. H_1 bezeichne den Kern des Homomorphismus $\mathfrak{a} \mapsto \sigma(\mathfrak{a})$ von $I_{K^r}(\mathfrak{m})$ nach $\mathrm{Gal}(k_0^r)/K^r$. Dann ist H_1 die Menge aller Ideale $\mathfrak{a}$ von $I_{K^r}(\mathfrak{m})$, für die

$$(g(\mathfrak{a}), N(\mathfrak{a})) = (\mathcal{O}_K, 1)$$

gilt, siehe [Sh97], S. 111. Es sei H_0 die Untergruppe von $I_{K^r}((1))$, die aus den Idealen $\mathfrak{a}$ besteht, für die es ein $\mu \in K$ mit $g(\mathfrak{a}) = \mu$ und $N(\mathfrak{a}) = \mu\bar{\mu}$ existiert. Dann gilt $H_0 \cap I_{K^r}(\mathfrak{m}) = H_1$. Außerdem liegen alle Elemente von $P_{K^r}((1))$ bereits in H_0. Deswegen ist k_0^r eine unverzweigte Erweiterung über K^r nach der Klassenkörpertheorie. Damit haben wir den ersten Hauptsatz der komplexen Multiplikation in idealtheoretischer Fassung bewiesen:

Satz 2.3. ***Erster Hauptsatz (idealtheoretisch)***

Es sei (K, Φ) ein primitiver CM-Typ, (K^r, Ψ) der Reflexivtyp, (A, E) eine hauptpolarisierte abelsche Varietät definiert über k mit $K^r \subseteq k$, die die komplexe Multiplikation mit $\mathcal{O}_K$ besitzt. Ferner sei k_0 der Modulkörper von A. Dann ist $k_0^r = k_0 K^r$ eine unverzweigte Erweiterung von K^r, die nach der Klassenkörpertheorie zu der Gruppe I_{K^r}/H_0 korrespondiert, wobei für H_0

$$H_0 = \left\{ \mathfrak{a} \in I(K^r) : \begin{array}{r} \exists \mu \in K^* \text{ mit} \\ N_\Psi(\mathfrak{a}) = \mu\mathcal{O}_K \\ \mu\bar{\mu} = N(\mathfrak{a}) \end{array} \right\}$$

gilt.

Torsionspunkte

$G := \mathrm{Aut}((A, E))$ bezeichne die Menge aller Automorphismen der polarisierten abelschen Varietät (A, E). Dann ist $\mathrm{Aut}((A, E))$ nach [Sh97], S. 32, proposition 17, endlich.

Bemerkung 2.4. *Es gilt $G \cong Tor(K)$, falls (K, Φ) primitiver CM-Typ ist und $Tor(K)$ die Gruppe der Torsionseinheiten bezeichnet. Allgemeiner ist die Automorphismengruppe $G := Aut((A, E))$ genau die Gruppe der Torsionseinheiten der Ordnung $\mathcal{O}$ mit $End(A) \cong \mathcal{O}$ von K, falls (K, Φ) primitiver CM-Typ ist, und $\mathcal{O} \cong End(A)$ gilt, siehe [Sh97], S. 103, und vergleiche für den Fall der elliptischen Kurven mit [Sil86], S. 103, theorem 10.1.*

Eine **Kummer Varietät** von (A, E) ist der Quotient von A durch die Gruppe G. Wir haben nun den folgenden Satz für die Existenz einer **normalisierten** Kummer Varietät von A.

Satz 2.5. *Es sei (A, E) eine polarisierte abelsche Varietät mit dem Modulkörper k_0. Dann existiert eine bis auf Isomorphie eindeutige Kummer Varietät (W, F) von (A, E), die wir die **normalisierte** Kummer Varietät nennen, mit folgenden Eigenschaften:*

1. *W ist über k_0 definiert,*
2. *F ist definiert über jedem Definitionskörper k von (A, E), der nach Kapitel 1 den Modulkörper k_0 enthält,*
3. *Gegeben sei ein Definitionskörper k ($k_0 \subseteq k$). Falls σ ein Isomorphismus von k in einen anderen Körper ist und η ein Isomorphismus von (A, E) in (A^σ, E^σ), dann gilt*

$$F = F^\sigma \circ \eta.$$

Es sei $\mathfrak{b}$ ein ganzes Ideal in $\mathcal{O}_K$. Ferner sei $\mathfrak{g}(\mathfrak{b}, A)$ die Menge aller Punkte t von A, für die $\alpha t = 0$ für jedes Element $\alpha \in \mathfrak{b}$ gilt. Falls $t \in \mathfrak{g}(\mathfrak{b}, A)$ gilt, heißt das Ideal $\mathfrak{b}$ das **Annulatorideal** von t. Ein Punkt $t \in \mathfrak{g}(\mathfrak{b}, A)$ heißt ein **Torsionspunkt** auf A, falls aus $\alpha t = 0$ stets $\alpha \in \mathfrak{b}$ folgt. Wir bezeichnen mit A_{tor} die Menge aller solchen Punkte von A.

Der Satz 2.3 wurde für die Körper, die durch die Adjunktion der Bilder gewisser Torsionspunkten von A unter F an den Körper k_0^r entstehen wie folgt verallgemeinert, siehe [Sh97], S. 118:

Satz 2.6. ***Zweiter Hauptsatz (idealtheoretisch)***

Es sei (K, Φ) ein primitiver CM-Typ, (K^r, Ψ) der Reflexivtyp und (A, E) eine hauptpolarisierte abelsche Varietät definiert über k mit $K^r \subseteq k$, die die komplexe Multiplikation mit $\mathcal{O}_K$ besitzt. Ferner seien k_0 der Modulkörper von A, $\mathfrak{b} \in \mathcal{O}_K$ ein Ideal mit $b = \mathfrak{b} \cap \mathbb{Z}$, $t \in A(\bar{k})$ ein Punkt mit dem Annulatorideal $\mathfrak{b}$, und (W, F) die normalisierte Kummer Varietät von (A, E). Dann ist $k_0^r(F(t))$ eine abelsche Erweiterung von K^r, die nach der Klassenkörpertheorie zu der Gruppe $I_{K^r}((b))/H_{\mathfrak{b}}$ mit

$$H_{\mathfrak{b}} = \left\{ \mathfrak{a} \in I(K^r)((b)) : \begin{array}{r} \exists \mu \in K^* \text{ mit} \\ N_\Psi(\mathfrak{a}) = \mu \mathcal{O}_K \\ \mu\bar{\mu} = N(\mathfrak{a}) \\ \mu \equiv 1 \bmod {}^\times(b) \end{array} \right\}$$

korrespondiert.

Der Hauptsatz für beliebige Ordnungen $\mathcal{O}$ von K, die als Endomorphismenringe hauptpolarisierter abelscher Varietäten vorkommen, findet sich in [Sh61], S. 136 bis 142, section 17.

2.2 Idealtheoretische Fassung

Gegeben sei ein algebraischer Zahlkörper $M \subset \mathbb{C}$ vom Grad g mit der maximal abelschen Erweiterung M^{ab}. Wir bezeichnen mit M_A den Ring der

Adele und mit M_A^* die Idelgruppe von M. Ferner bezeichne M_a^* den archimedisschen und M_∞^* den nicht archimedischen Teil von M_A^*. Wir betrachten M^* und die Lokalisierung $M_{\mathfrak{p}}^*$ als Untergruppen von M_A^*, wobei $\mathfrak{p}$ Primstelle (endlich oder unendlich) von M ist. Für ein Element $x \in M_A^*$ bezeichnen wir mit x_a, x_∞ und $x_{\mathfrak{p}}$ die Komponenten von M_a^*, M_∞^*, bzw. $M_{\mathfrak{p}}^*$. Nach dem Hauptsatz der Klassenkörpertheorie haben wir die exakte Sequenz

$$1 \longrightarrow \overline{M^* M_{\infty+}^*} \longrightarrow M_A^* \xrightarrow{Ar} \mathrm{Gal}(M^{ab}/M) \longrightarrow 1, \tag{2.6}$$

wobei $M_{\infty+}^*$ die zusammenhängende Komponente des Einselements von M_∞^*, $\overline{A}$ den topologischen Abschluss einer Untergruppe von $A \subset M_A^*$, und Ar die Artinsche Abbildung bezeichnen.

Das Bild eines Elements $x \in M_A^*$ in $\mathrm{Gal}(M^{ab}/M)$ unter der Artinabbildung Ar bezeichnen wir mit $[x, M]$. Für jedes Element $t \in M_A^*$, und jede Primzahl p bezeichnen wir mit t_p die $p-$te Komponente von t, welche ein Element von $M_p = M \otimes_{\mathbb{Q}} \mathbb{Q}_p$ ist. Ferner setzen wir für ein $\mathbb{Z}-$Gitter $\mathfrak{a}$ in M die $p-$te Komponente $\mathfrak{a}_p = \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Dann ist auch $t\mathfrak{a}$ ein $\mathbb{Z}-$Gitter mit $(t\mathfrak{a})_p = t_p \mathfrak{a}_p$, welches impliziert, dass $t\mathfrak{a}$ ein gebrochenes Ideal von M ist, falls $\mathfrak{a}$ ein gebrochenes Ideal von M ist. Weil $\mathbb{Q}/\mathbb{Z}$ kanonisch isomorph zu der direkten Summe $\mathbb{Q}_p/\mathbb{Z}_p$, und daher $M/\mathfrak{a}$ isomorph zu $\mathbb{Q}^g/\mathbb{Z}^g$ ist, ist $M/\mathfrak{a}$ isomorph zu der direkten Summe $M_p/\mathfrak{a}_p$ über alle p. Daher sind $M/\mathfrak{a}$ und $M/t\mathfrak{a}$ isomorph, denn die Multiplikation mit t_p liefert eine Isomorphie zwischen $M_p/\mathfrak{a}_p$ und $M_p/t_p\mathfrak{a}_p$.

Das Bild eines Elements $\omega \in M/\mathfrak{a}$ in $M/t\mathfrak{a}$ bezeichnen wir mit $t\omega$. Falls nun $\omega = u(\mathrm{mod}\ \mathfrak{a})$ ist, dann gilt $t\omega = v(\mathrm{mod}\ t\mathfrak{a})$ mit einem Element $v \in M$, so dass $v \cong t_p u(\mathrm{mod}\ t_p\mathfrak{a}_p)$ für alle p ist. Daher schreiben wir

$$t \cdot (u(\mathrm{mod}\ \mathfrak{a})) = tu(\mathrm{mod}\ t\mathfrak{a}). \tag{2.7}$$

Bemerkung 2.7. *Wir merken an, obschon das Element tu ein Element von M_A ist, können wir uns $tu(\mathrm{mod}\ t\mathfrak{a})$ in der rechten Seite von 2.7 als $\{t_p u(\mathrm{mod}\ t_p\mathfrak{a}_p)\}_p \in M/\mathfrak{a}$ für jede $p-$Komponente vorstellen damit die Schreibweise in 2.7 Sinn macht, siehe auch [Sh71], S. 117.*

Es sei nun (A, E) eine hauptpolarisierte abelsche Varietät, (K, Φ) der CM-Typ, wobei $2g$ der Grad von K über $\mathbb{Q}$ ist. Ferner sei ξ die Abbildung $\mathbb{C}^g \to A$, deren Kern wir mit $q(\mathfrak{a})$ bezeichnen. Dann ist $q(a) = (a^{\phi_1}, \cdots, a^{\phi_g})$ für jedes Element $a \in K$, vergleiche mit der Definition 1.14. Es gilt für die Riemannform E stets

$$E(q(x), q(y)) = \mathrm{Tr}_{K/\mathbb{Q}}(\zeta x \bar{y}),$$

wobei für das Element $\zeta \in K$ wegen 1.16 $\bar{\zeta} = -\zeta$ und $\Im(\zeta^{\phi_i}) > 0$, $1 \leq i \leq g$,

gilt. In diesem Fall sagen wir, dass (A, E) vom Typ $\Omega = \{K, \Phi, \mathfrak{a}, \zeta\}$ ist. Dann haben wir die folgende exakte Sequenz, siehe [Sh97], S. 123:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & K_{\mathbb{R}} & \longrightarrow & K_{\mathbb{R}}/\mathfrak{a} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle q} & & \downarrow & & \\ 1 & \longrightarrow & q(\mathfrak{a}) & \longrightarrow & \mathbb{C}^g & \xrightarrow{\xi} & A & \longrightarrow & 1 \end{array} \tag{2.8}$$

wobei $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ ist. Nun sei (K^r, Ψ) der Reflexivtyp von (K, Φ) und $N_\Psi : (K^r)^* \to K^*$ die Typ-Norm Abbildung wie in 1.13. Dann können wir $N_\Psi(a) = \det S_\Psi(a)$ schreiben, wobei $S_\Psi(a)$ die in 1.15 definierte diagonale Matrix ist. Nun sei L die galoische Hülle von K mit $G = \mathrm{Gal}(L/\mathbb{Q})$, $H = \mathrm{Gal}(L/K)$ und $H^r = \mathrm{Gal}(L/K^r)$. Dann existieren Elemente $\tau_j \in G$, $1 \leq j \leq m := [K^r : \mathbb{Q}]/2$ mit

$$\cup_{i=1}^{g} \phi_i^{-1} H = \cup_{j=1}^{m} H^r \tau_j.$$

Ferner liefert die Menge der Elemente von τ_j genau den CM-Typ Ψ zu K^r, siehe [Sh97], S. 124.

Es sei nun $b \in K^r$ ein Element mit $K^r = \mathbb{Q}(b)$. Da die Koeffizienten des Polynoms $P(x) = \prod_{j=1}^{m}(X - b^{\tau_j})$ in K liegen, existiert ein Element $T \in K^{m\times m}$, dessen charakteristische Polynom P ist. Mittels

$$\sum_k c_k b^k \mapsto \sum_k c_k T^k \tag{2.9}$$

haben wir einen injektiven Ringhomorphismus $\Phi^0 : K^r \to K^{m\times m}$ mit $N_\Psi(a) = \det(\Phi^0(a))$. Wir können daher die Abbildung Φ^0 als eine $\mathbb{Q}_p-$lineare, und daher eine $\mathbb{Q}_A-$lineare Abbildung fortsetzen. Insgesamt erhalten wir einen stetigen Homomorphismus von $(K^r)_A^*$ nach K_A^*, den wir auch mit N_Ψ bezeichnen.

Wir können nun den Hauptsatz der komplexen Multiplikation formulieren. Für den Beweis verweisen wir auf [Sh97], S. 125.

Satz 2.8. ***Hauptsatz (ideltheoretisch)***

Es sei $\mathcal{P} = (A, E)$ eine hauptpolarisierte abelsche Varietät vom Typ $\Omega = \{K, \Phi, \mathfrak{a}, \zeta\}$ und Reflexivtyp (K^r, Ψ). Ferner seien $\sigma \in Aut(\mathbb{C}/K^r)$ und $s \in (K^r)_A^*$, so dass $\sigma = [s, K^r]$ in $(K^r)^{ab}$ ist. Dann ist die folgende Sequenz exakt:

$$0 \longrightarrow q(N_\Psi(s)^{-1}\mathfrak{a}) \longrightarrow \mathbb{C}^g \xrightarrow{\xi'} A^\sigma \longrightarrow 0,$$

mit folgenden Eigenschaften:

1. *$\mathcal{P}^\sigma$ ist vom Typ $\{K, \Phi, N_\Psi(s)^{-1}\mathfrak{a}, \zeta'\}$, wobei $\zeta' = N(s\mathcal{O}_{K^r})\zeta$ ist,*
2. *Es gilt $\xi(q(\omega))^\sigma = \xi'(q(N_\Psi(s)^{-1}\omega))$ für jedes Element $\omega \in K/\mathfrak{a}$, das heißt das folgende Diagram ist kommutativ:*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi\circ q} & A \\ {\scriptstyle N_\Psi(s)^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ K/N_\Psi(s)^{-1}\mathfrak{a} & \xrightarrow{\xi'\circ q} & A^\sigma \end{array} \tag{2.10}$$

Ferner ist die Abbildung ξ' für fest gewählte ξ eindeutig.

Bemerkung 2.9. *Wie weisen darauf hin, dass der Satz 2.8 für alle Automorphismen von $\mathbb{C}$, nicht notwendig diejenigen, die K^r fixieren, verallgemeinert wurde, siehe [Mil1]. Dies ist der Hauptsatz der komplexen Multiplikation über $\mathbb{Q}$.*

2.3 Hauptsätze für Geschlecht eins

Es sei k ein imaginär quadratischer Zahlkörper mit der Maximalordnung $\mathcal{O}_k$ und $\tau \in \mathcal{O}_k \cap \mathbb{H}$. Wie wir im Kapitel 1 gesehen haben, ist der Körper $\mathbb{Q}(j(\tau))$ der Modulkörper einer elliptischen Kurve E über $\mathbb{C}$ mit der $j-$Invariante $j(\tau)$, wobei $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$ ein bis auf Homothetie zu E isomorpher komplexer Torus ist. Nach dem ersten Hauptsatz der komplexen Multiplikation 2.3 können wir nun die Erweiterung $k(j(\tau))$ über k klassenkörpertheoretisch beschreiben, falls die elliptische Kurve komplexe Multiplikation mit $\mathcal{O}_k$ besitzt, da in diesem Fall für den Reflexivkörper $k^r = k$ gilt, und jede elliptische Kurve durch die eindeutige Polarisierung 1.7 hauptpolarisiert ist. In diesem Fall ist die Typ-Norm Abbildung die Identitätsabbildung in k. Dann gilt für die Menge H_0 stets

$$H_0 = \left\{ \begin{array}{r} \exists \mu \in K^* \text{ mit} \\ \mathfrak{a} \in I(K^r) : N_\Psi(\mathfrak{a}) = \mu\mathcal{O}_K \\ \mu\bar{\mu} = N(\mathfrak{a}) \end{array} \right\} = I_k((1)),$$

weil $K^r = K = k$ ist, und die Bedingungen für jedes Ideal in $I_k((1))$ erfüllt sind. Somit haben wir nach der Klassenkörpertheorie, 2.3 und 2.8 den folgenden Satz (vergleiche mit [Sh71], S. 123):

Satz 2.10. *Es sei k ein imaginär quadratischer Zahlkörper mit der Maximalordnung $\mathcal{O}_k$ und $\tau \in \mathcal{O}_k \cap \mathbb{H}$. Dann ist $\mathcal{H}_k = k(j(\tau))$ der Hilbertklassenkörper, das heißt $\mathcal{H}_k$ ist die maximale total unverzweigte abelsche Erweiterung von k. Die Isomorphie $Gal(\mathcal{H}_k/k) \cong Cl(k)$ ist mit $\sigma \mapsto \mathfrak{b}$ durch*

$$j(\mathfrak{a})^\sigma = j(\mathfrak{b}^{-1}\mathfrak{a})$$

gegeben. Ferner gilt

1. $[k(j(\tau)) : k] = [\mathbb{Q}(j(\tau)) : \mathbb{Q}]$,
2. *Falls* $[\tau_1, 1], \cdots, [\tau_h, 1]$ *ein Repräsentantensystem der Klassen in* $Cl(k)$ *sind, dann bilden* $j(\tau_1), \cdots, j(\tau_h)$ *ein komplettes System der konjugierten Zahlen über* $\mathbb{Q}$, *und über* k.

Hauptsätze für beliebige Ordnungen

Wir betrachten nun den Fall, dass eine elliptische Kurve E über $\mathbb{C}$ die komplexe Multiplikation mit einer beliebigen Ordnung $\mathcal{O}_t$ hat, wobei $\mathcal{O}_t$ die eindeutige Ordnung mit dem Führer t eines imaginär quadratischen Zahlkörpers k bezeichnet. Wir haben daher $k \cong \mathrm{End}(E) \otimes \mathbb{Q}$. Es existiert eine kanonische Wahl λ aus zwei Isomorphismen von k nach $\mathrm{End}(E) \otimes \mathbb{Q}$, die durch die folgende Bedingung charakterisiert ist:

$$\omega \circ \lambda(\mu) = \mu\omega, \ \mu \in K, \lambda(\mu) \in \mathrm{End}(E), \tag{2.11}$$

wobei $0 \neq \omega$ der Erzeuger des eindimensionalen Vektorraums der holomorphen Differentialformen von E über $\mathbb{C}$ ist, siehe [Sh71], S. 113. Dieser Isomorphismus heißt **normalisiert**. Man bezeichnet mit dem Paar (E, λ) die normalisierte elliptische Kurve.

Wir fixieren einen Isomorphismus ξ von $\mathbb{C}/\mathfrak{a}$ nach E, wobei $\mathfrak{a}$ ein $\mathbb{Z}-$Gitter in k ist. Es gilt $\xi(\alpha v) = \lambda(\alpha)(\xi(v))$ für jedes Element $\alpha \in k$ mit $\alpha\mathfrak{a} \subseteq \mathfrak{a}$ wegen der Auswahl 2.11 des kanonischen Isomorphismus λ. Ferner ist $\xi(K/\mathfrak{a})$ stets die Menge aller Punkte der endlicher Ordnung von E ([Sh71], S. 117). Somit haben wir nach dem Hauptsatz 2.8 den Hauptsatz der komplexen Multiplikation für elliptische Kurven.

Satz 2.11. ***Hauptsatz: Elliptische Kurven (idealtheoretisch)***

Es seien $k, (E, \lambda), \mathfrak{a}$ *und* ξ *wie oben definiert. Ferner sei* σ *ein Automorphismus von* $\mathbb{C}$ *über* k *und* s *ein Element von* k_A^* *mit* $[s, k] \in k^{ab}$. *Dann existiert ein Isomorphismus*

$$\xi' : \mathbb{C}/s^{-1}\mathfrak{a} \longrightarrow E^\sigma, \tag{2.12}$$

wobei für ξ' *stets* $\xi(u) = \xi'(s^{-1}u)$ *für alle* $u \in k/\mathfrak{a}$ *gilt. Des Weiteren ist das folgende Diagramm kommutativ:*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi} & E \\ {\scriptstyle s^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ K/s^{-1}\mathfrak{a} & \xrightarrow{\xi'} & E^\sigma \end{array} . \tag{2.13}$$

Zusätzlich ist die Abbildung ξ' für gegebenes σ eindeutig, wenn ξ fest gewählt wird.

Es gilt für die $j-$Invariante des $\mathbb{Z}-$Gitters $\mathfrak{a}$ in k nach 2.11 $j(\mathfrak{a})^\sigma = j(s^{-1}\mathfrak{a})$, und somit hängt $j(\mathfrak{a})^\sigma$ nur von der Einschränkung $\sigma|_{k^{ab}}$ ab. Für jedes $\mathbb{Z}-$Gitter $\mathfrak{a}$ gelten damit $j(\mathfrak{a}) \in k^{ab}$ und $j(\mathfrak{a})^{[s,k]} = j(s^{-1}\mathfrak{a})$. Ferner ist ein $\mathbb{Z}-$Gitter $\mathfrak{a}$ genau dann ein gebrochenes $\mathcal{O}_t-$Ideal, wenn ein $x \in k_A^*$ mit $\mathfrak{a} = x\mathcal{O}_t$ existiert, siehe [Sh71], S. 122. Wir bezeichnen nun die Gruppe der gebrochenen $\mathcal{O}_t-$Ideale mit I_t und die Untergruppe der Hauptideale von I_t mit $\mathcal{P}_t$. Dann ist die **Ringklassengruppe** $\mathrm{Cl}_t = I_t/\mathcal{P}_t$ isomorph zu der Gruppe k_A^*/k^*W, wobei $W = k_\infty^* \prod_p \mathcal{O}_p^*$ ist, siehe [Sh71], S. 123. Diese Überlegungen liefern den folgenden Satz, welcher den Satz 2.10 für beliebige Ordnungen verallgemeinert:

Satz 2.12. ***Hauptsatz für beliebige Ordnungen***

Es sei k ein imaginär quadratischer Zahlkörper mit der Ordnung $\mathcal{O}_t$ vom Führer t und $\tau \in \mathcal{O}_t \cap \mathbb{H}$. Dann ist $\Omega_t = k(j(\tau))$ der Ringklassenkörper von k, der Körper, welcher nach der Klassenkörpertheorie zu der Gruppe Cl_t korrespondiert. Die Isomorphie $Gal(k(j(\tau))/k) \cong Cl_t$ ist durch $\sigma \mapsto \mathfrak{b}$ mit

$$j(\mathfrak{a})^\sigma = j(\mathfrak{b}^{-1}\mathfrak{a})$$

gegeben. Ferner gilt

1. *Es gibt eine Isomorphie zwischen $Gal(\Omega_t/k)$ und Cl_t, die durch*

   $$\sigma \mapsto \mathfrak{b},$$

   mit $j(\mathfrak{a})^\sigma = j(\mathfrak{b}^{-1}\mathfrak{a})$ gegeben ist,

2. $[k(j(\tau)) : k] = [\mathbb{Q}(j(\tau)) : \mathbb{Q}]$,

3. *Falls $[\tau_1, 1], \cdots, [\tau_{h_t}, 1]$ ein Repräsentantensystem der Klassen in Cl_t sind, dann bilden $j(\tau_1), \cdots, j(\tau_{h_t})$ ein komplettes System der konjugierten Zahlen über $\mathbb{Q}$, und über k, wobei h_t die Ordnung von Cl_t bezeichnet.*

Beweis: Aus $j(\mathfrak{a})^{[s,k]} = j(s^{-1}\mathfrak{a})$ folgt zusammen mit dem Satz von Shimura, [Sh71], S. 122, theorem 5.5, die erste Behauptung, weil der Satz von Shimura besagt, dass k_A^*/k^*W eine zu Cl_t isomorphe Gruppe ist. Aus der ersten Behauptung folgt $h_t = [k(j(\tau)) : k]$.

Es sei nun E eine elliptische Kurve, die zu $\mathbb{C}/\mathfrak{a}$ isomorph ist. Dann sind $\mathrm{End}(E^\sigma)$ und $\mathrm{End}(E)$ isomorph. Nach [Sh71], S. 104, proposition 4.8 gilt nun die Gleichung $j(\mathfrak{a})^\sigma = j(E^\sigma)$, aus der die Ungleichung
$[\mathbb{Q}(j(\tau)) : \mathbb{Q}] \leq h_t$ folgt. Da $[\mathbb{Q}(j(\tau)) : \mathbb{Q}] \geq [k(j(\tau)) : k]$ trivialerweise gilt, haben wir die zweite, und daher die dritte Aussage. □

Bemerkung 2.13. *Wir merken an, dass aus dem Satz 2.12 mit $t = 1$ der Satz 2.11 folgt. Der Ringklassenkörper Ω_1 von k ist daher genau der Hilbertklassenkörper $\mathcal{H}_k$ von k.*

Klassenkörper über Hilbert- und Ringklassenkörper

Es sei nun E eine elliptische Kurve über $\mathbb{C}$, die komplexe Multiplikation mit einer Ornung $\mathcal{O}_t$ eines imaginär quadratischen Zahlkörpers k besitzt. Dann ist die Automorphismengruppe G von E nach 2.4 gerade die Einheitengruppe $\mathcal{O}_t^*$, da für den Einheitenrang r von k stets $r = 0$ gilt. Sie besteht daher nur aus Torsionseinheiten. Es gilt $G \cong \{\pm 1\}$, falls die $j-$Invariante von E der Bedingung $j \neq 1728, 0$ erfüllt. Wir haben

1. Für $j = 1728$: $k = \mathbb{Q}(i)$, $\mathcal{O}_k = \mathbb{Z}[i]$ und somit $\mathcal{O}_k^* = \{\pm 1, \pm i\}$,
2. Für $j = 0$: $k = \mathbb{Q}(\rho)$, $\rho = e^{2\pi i/3}$, $\mathcal{O}_k = \mathbb{Z}[\rho]$ und somit $\mathcal{O}_k^* = \{\pm 1, \pm\rho, \pm\rho^2\}$.

Mit $\mathcal{E}$ bezeichnen wir die Menge aller elliptischer Kurven in kurzer Weierstraß-Form $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$, wobei g_2 und g_3 die in 1.19 definierten Eisensteinschen Reihen sind. Wir klassifizieren die elliptischen Kurven in drei verschiedenen Klassen $\mathcal{E}_1$, $\mathcal{E}_2$ und $\mathcal{E}_3$, deren Automorphismengruppe $2i$ Elemente hat, $i = 1, 2, 3$. Daher entsprechen die Mengen $\mathcal{E}_2$ und $\mathcal{E}_3$ den elliptischen Kurven, deren $j-$Invariante $j = 1728$ bzw. $j = 0$ sind. Wir definieren nun die folgenden Funktionen:

Definition 2.14. *Es sei E eine elliptische Kurve in kurzer Weierstraß-Form $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$. Dann heißen die Funktionen*

1. $h_E^1((x, y)) = (g_2(\tau)g_3(\tau)/\Delta(\tau)) \cdot x$,
2. $h_E^2((x, y)) = (g_2(\tau)^2/\Delta(\tau)) \cdot x^2$,
3. $h_E^3((x, y)) = (g_3(\tau)/\Delta(\tau)) \cdot x^3$

Webersche Funktionen.

Wir haben nun

$$\begin{cases} h_E^1 = h_E^3 = 0 \text{ und } h_E^2((x, y)) = g_2(\tau)^{-1}x^2 \text{ falls } E \in \mathcal{E}_2, \\ h_E^1 = h_E^2 = 0 \text{ und } h_E^3((x, y)) = (-27g_3(\tau))^{-1}x^3 \text{ falls } E \in \mathcal{E}_3. \end{cases}$$

Aus der expliziten Beschreibung der Elemente von G und der obigen Eigenschaft folgen nun die folgenden Eigenschaften dieser Funktionen:

Lemma 2.15. *1. Es sei $E \in \mathcal{E}_i$, $1 \leq i \leq 3$. Dann gilt $h_E^i(t) = h_E^i(t')$ genau dann, wenn ein $\alpha \in G$ mit $t = \alpha t'$ existiert.*

2. Es sei η ein Isomorphismus zwischen zwei elliptischen Kurven E und E' mit $E, E' \in \mathcal{E}$. Dann gilt $h^i = h^i \circ \eta$.

Nach 2.15 haben wir somit eine explizite Beschreibung der normalisierten Kummer Varietät $(E/G, h^i)$, die den Anforderungen des Satzes 2.5 für jede elliptische Kurve $E \in \mathcal{E}$ genügt.

Die Untergruppe $H_{\mathfrak{b}}$ aus dem zweiten Hauptsatzes der komplexen Multiplikation 2.6 ist genau die Gruppe $P_k(\mathfrak{b}) \cap I_k((b))$, falls E die komplexe Multiplikation mit $\mathcal{O}_k$ eines imaginär quadratischen Zahlkörpers k besitzt.

Nun entspricht dem Körper $k(j(\tau), h^i(P))$ genau der Strahlklassenkörper modulo (b), wobei $P \in E$ ein Punkt der Ordnung b ist. Ferner haben wir den folgenden Satz, welcher das 12. Problem von Hilbert im Falle imaginär quadratischer Zahlkörper löst. Wir verweisen für den Beweis auf [Lang73], S. 126, theorem 2. Für eine entsprechende Aussage des Satzes im Falle beliebiger Ordnungen imaginär quadratischer Zahlkörper verweisen wir auf [Sh71], S. 123, corollary 5.6.

Satz 2.16. *Es sei E eine elliptische Kurve in $\mathcal{E}_i$, $1 \leq i \leq 3$, die die komplexe Multiplikation mit der Maximalordnung $\mathcal{O}_k$ eines imaginär quadratischen Zahlkörpers k besitzt. Dann wird k^{ab} durch die Adjunktion der Werte $h^i(P)$ der Punkte $P \in E$ endlicher Ordnung an den Hilbertklassenkörper $\mathcal{H}_k = \Omega_1$ erzeugt.*

Bemerkung 2.17. *1. Im Allgemeinen beschreibt die Untergruppe $H_{\mathfrak{b}}$ des Satzes 2.6 nicht die gesamte Strahlklassengruppe modulo (b). Daher ist es nicht möglich die maximal abelsche Erweiterung $(K^r)^{ab}$ mittels der Theorie der komplexen Multiplikation explizit zu erzeugen.*

2. In den Kapiteln 4 und 5 werden wir, nebst den Eigenschaften der Relativerweiterung $k_0^r(F(t))/k_0^r$ der in 2.6 und 2.3 mittels der CM-Theorie konstruierten Klassenkörper $k_0^r(F(t))$ und k_0^r auch den maximalen abelschen Teilkörper von $(K^r)^{ab}$, der durch die CM-Theorie konstruierbar ist, näher untersuchen.

Kapitel 3

Die CM-Methoden

Ziel dieses Kapitels ist es, einen Überblick über die Methoden der komplexen Multiplikation, die **CM-Methoden**, anzugeben. Ferner wird auf die Probleme, die bei der CM-Konstruktion auftreten, nebst ihren Lösungen eingegangen. Die CM-Methoden ermöglichen die Konstruktion elliptischer Kurven und hyperelliptischer Kurven vom Geschlecht zwei mit komplexer Multiplikation, **Kurven mit CM**, über endlichen Körpern.

Wir werden die in der Literatur eingeführten Algorithmen zur Konstruktion elliptischer und hyperelliptischer Kurven mit CM, insbesondere die analytische Methode der Konstruktion der Klassenpolynome, die Laufzeitaussagen zur Konstruktion dieser Klassenpolynome, die Konstruktion der Igusaklassenpolynome der hyperelliptischen Kurven nebst Laufzeitaussagen, und die Einschränkungen der CM-Methode im Geschlecht zwei zusammenstellen.

Zuvor werden wir auf die Anwendungsgebiete der CM-Konstruktionen nebst ihren Anforderungen eingehen.

3.1 Anwendungen

Wie in der Einleitung erwähnt wurde, gibt es Anwendungen der Konstruktion algebraischer Kurven mit CM im Primzahlnachweis, und in der gruppen- und paarungsbasierten Kryptographie. Bevor wir die CM-Methoden erklären, werden wir in diesem Abschnitt erläutern, welche Anforderungen für diese Anwendungen benötigt werden.

Dass die Jacobischen Varietäten mit vorgegebener Ordnung über endlichen Körpern mittels der speziellen Eigenschaften der komplexen Multiplikation konstruiert werden können, ist der wesentliche Vorteil dieser Methoden. Die CM-Methoden stellen somit eine alternative zu den Punktzählalgorithmen dar. Wir werden sehen, wie spezielle Eigenschaften der Kurven mit komplexer

Multiplikation diese Anwendungen realisieren.

Primzahlnachweis

Lenstra hat im Jahre 1987 einen probabilistischen Algorithmus entwickelt, der ganze Zahlen mit Hilfe elliptischer Kurven faktorisiert, siehe [Len87]. Die Idee seines Verfahrens basiert auf dem Pollard $p-1-$Verfahren, siehe [Coh93], Kapitel 8.8, mit dem Unterschied, dass man statt der Gruppe $(\mathbb{Z}/N\mathbb{Z})^*$ eine elliptische Kurve E über dem Ring $\mathbb{Z}/N\mathbb{Z}$ betrachtet, wobei N die Zahl ist, die faktorisiert wird, und $E(\mathbb{Z}/N\mathbb{Z})$ gewisse Glattheitseigenschaften erfüllt, siehe [Coh93], Kapitel 10.3. Für die Eigenschaften der elliptischen Kurven über endlichen Ringen verweisen wir auf [Coh93], S. 485 bis S. 487. Darin, dass es viele elliptische Kurven über $\mathbb{Z}/N\mathbb{Z}$ gibt, und damit die Wahrscheinlichkeit eine passende Kurve, deren Punkte den Glattheitsanforderungen genügen, zu finden groß ist, liegt die Stärke seines Verfahrens. Auch heute ist dieses Verfahren eine der schnellsten Methoden, um die Primfaktoren mit ca. 50 Dezimalstellen der zu faktorisierender ganzen Zahl N zu berechnen. Deswegen benutzt man in modernen Faktorisierungsverfahren diese Methode mit den quadratische Sieb und Zahlkörpersieb Algorithmen, um zunächst die Faktoren von N bis 50 Dezimalstellen zu bestimmen.

Diese Flexibilität der Auswahl der Kurven E über $\mathbb{Z}/N\mathbb{Z}$ benutzen Goldwasser und Killian, um ein probabilistisches Verfahren zu entwickeln, welches ECPP (elliptic curve primality proving) genannt wurde, siehe [GoKi86]. Dieses verallgemeinerte das $N-1-$Primzahlnachweisverfahren auf das Verfahren des Primzahlnachweises mittels elliptischer Kurven, siehe [Uz04]. Der folgende Satz wird bei diesem Verfahren benutzt, siehe [Uz04], S. 63, theorem 4.9:

Satz 3.1. *Es sei $N \neq 1$ eine zu 6 teilerfremde Zahl und E eine elliptische Kurve über $\mathbb{Z}/N\mathbb{Z}$ mit einem Punkt $P \in E$. Ferner sei m eine Zahl, die den folgenden Bedingungen genügt:*

1. *Es existiert ein Primfaktor q von m mit*
$$q > (\sqrt[4]{N}+1)^2.$$
2. *Es gilt $m \cdot P = \mathcal{O}_E = (0:1:0)$.*
3. *Es gilt $\frac{m}{q} \cdot P = (x:y:t)$ mit $t \in (\mathbb{Z}/N\mathbb{Z})^*$.*

Dann ist die Zahl N prim.

Das Verfahren basiert auf einer DOWN-RUN Strategie, bei der die Primzahleigenschaft einer Zahl $N_1 = N$ aus der Primzahleigenschaft einer

kleineren Zahl $q = N_2 < N_1$ folgt. Nach m Schritten erhält man zum Beispiel eine Zahl $N_m < 10^9$, deren Primzahleigenschaft (und somit auch die von N) leicht nachzuweisen ist. Die aufwendigsten Schritte dieses Verfahrens sind die Bestimmung der Gruppenordnungen verschiedener elliptischer Kurven über endlichen Körpern und die Faktorisierung dieser Gruppenordnungen, die wegen 3.1 bei jedem Reduktionsschritt durchgeführt werden muss. Dabei beginnt man mit einer zufälligen Kurve, bestimmt die Gruppenordnung, und überprüft, ob die Eigenschaften nach 3.1 erfüllt sind. Diesen Prozess wiederholt man solange, bis eine passende Kurve bestimmt wird.

Dieses Verfahren wurde mittels der Konstruktion elliptischer Kurven mit komplexer Multiplikation von Atkin und Morain im Jahre 1993 deutlich verbessert, siehe [AtMr93]. Mit der CM-Konstruktion können stets Kurven mit vorgegebener Ordnung konstruiert werden, die apriori die nötigen Eigenschaften erfüllen. Der Algorithmus liefert zur Zeit den effizientesten Primzahlnachweisalgorithmus in der Praxis. Der Rekord liegt momentan bei ca. 2580 Dezimalstellen, siehe [MorECPP].

Eine Verallgemeinerung dieses Verfahrens, welches den Primzahlnachweis mit Hilfe der hyperelliptischen Kurven vom Geschlecht zwei durchführt, ist unter anderem wegen des Fehlens der effizienten CM-Kontruktion für solche Kurven und ihre Jacobischen bisher nicht möglich, obwohl Adleman und Huang mittels der Jacobischen hyperelliptischer Kurven vom Geschlecht zwei ein Verfahren entwickelt haben, aus dem der folgende Satz folgt , siehe [AdHu92]:

Satz 3.2. *Es existiert ein Algorithmus, der in erwarteter polynomieller Zeit beweist oder widerlegt, dass eine gegebene Zahl N prim ist.*

Dieses Verfahren wurde wegen des Fehlens einer effizienten Arithmetik und einer schnellen Methode der Konstruktion hyperelliptischer Kurven vom Geschlecht zwei (nach dem Kenntnis vom Author dieser Arbeit) nie implementiert.

Bemerkung 3.3. *Wir merken an, dass mit dem Algorithmus von Agrawal, Kayal und Saxena, [AKS04], deterministisch in polynomieller Zeit bewiesen oder widerlegt werden kann, dass eine gegebene Zahl N prim ist. Dieses Verfahren ist aber in der Praxis schlechter als die ECPP-Methode.*

Andererseits wurde das Faktorisierungsverfahren von Lenstra auf die hyperelliptischen Kurven vom Geschlecht zwei verallgemeinert. Dabei ist die Laufzeit mittels spezieller hyperelliptischer Kurven und zugehöriger Kummer Flächen, Satz 2.5, verbessert worden, siehe [Cos10]. Dieses Verfahren bietet sogar schnellere Faktorisierung als das Verfahren von Lenstra für die Faktorisierung größer Zahlen an, siehe [Cos10], S. 1203.

DLP

Es sei $G =< g >$ eine zyklische additiv geschriebene Gruppe. Das Problem für ein gegebenes $\alpha \in G$ ein $x \in \mathbb{Z}$ mit $\alpha = x \cdot g$ zu bestimmen wird **diskretes Logarithmus Problem, DLP**, genannt. Das Lösen von DLP ist eine grundlegende Voraussetzung zum Bearbeiten vieler Probleme aus der konstruktiven Zahlentheorie, insbesondere der Probleme der endlichen abelschen Gruppen. Das ist zum Beispiel in der konstruktiven Klassenkörpertheorie interessant, siehe [Coh00], Kapitel 4.

Im Gegensatz zu den Anwendungen von DLP in der konstruktiven Zahlentheorie basiert die Sicherheit gruppenbasierter kryptographischer Methoden auf der Schwierigkeit von DLP, siehe [Men96], [Avan06]. Die zugrundeliegende Gruppe und ihre Präsentation bestimmen die Schwierigkeit dieses Problems. Im Falle, dass die Gruppenordnung nur kleine Primzahlfaktoren besitzt, ist dieses Problem mittels des chinesischen Restsatzes einfach zu lösen, siehe [Men96] S. 107. Daher benutzt man in der Praxis entweder multiplikative zyklische Untergruppen endlicher Körper $\mathbb{F}_{q^n}$, deren Ordnung einen großen Primteiler besitzt, oder zyklische Untergruppen Jacobischer Varietäten algebraischer Kurven von größer Primzahlordnung.

Die generischen DLP Algorithmen, d. h. Pollard-ρ und seine Varianten, besitzen eine exponentielle Laufzeit im Logarithmus der Gruppenordnung, genauer gesagt liegen ihre Laufzeit in $O(\sqrt{|G|})$, siehe [Avan06]. Das Index-Calculus Verfahren und seine Varianten dagegen nutzen die speziellen Eigenschaften der zugrundeliegenden Gruppen aus, und die Laufzeit dieser Algorithmen ist subexponentiell, falls die Gruppen entweder die multiplikativen Gruppen endlicher Körper, siehe [Avan06] Kapitel 20, oder die Jacobischen hyperelliptischer Kurven vom Geschlecht $g > 2$ sind, siehe [Avan06] Kapitel 21, und [EnGau02]. Es existieren daher zur Zeit für sorgfälltig gewählte elliptische Kurven und hyperelliptische Kurven vom Geschlecht zwei keine Algorithmen, die das DLP in subexponentieller Zeit lösen. Diese Tatsache ist der Grund für die Attraktivität dieser Gruppen in der gruppenbasierten Kryptographie. Deshalb benötigt die Konstruktion dieser Kryptosysteme eine passende Gruppe mit einer Untergruppe von Primzahlordnung. Die CM-Methoden bieten an dieser Stelle eine Alternative, wie in ECPP, zu den Punktzählalgorithmen an.

Bemerkung 3.4. *Obwohl es Spekulationen gibt, dass die speziellen Eigenschaften der komplexen Multiplikiation eventuell zu Angriffen führen könnten, ist kein Angriff solcher Art zur Zeit bekannt, siehe [BSS99], S. 151, VIII.2.*

Paarungen

Mit Hilfe der Weil- und Tate-Lichtenbaum Paarungen ist es möglich das DLP auf der Jacobischen einer hyperelliptischen Kurve vom Geschlecht g über $\mathbb{F}_q$ auf das DLP über dem endlichen Körper $\mathbb{F}_{q^k}$ zu übertragen, wobei k- der **Einbettungsgrad**- von q und von den Torsionspunkten der Primzahlordnung l, $\mathrm{ggT}(l, q) = 1$, auf der Jacobischen abhängt, siehe [Avan06], chapter 6. Ist k klein, so lässt sich das DLP auf diesen Kurven mittels der MOV/Frey-Rück Angriffe, [Avan06], chapter 22.2, lösen, denn wir können für das DLP auf $\mathbb{F}_{q^k}$ das Index-Calculus Verfahren anwenden. Die supersingulären Jacobi-Varietäten der algebraischen Kurven vom Geschlecht eins und zwei besitzen kleine Einbettungsgrade. Daher sind sie für die Konstruktion gruppenbasierter Kryptosysteme nicht geeignet.

Andererseits sind diese Paarungen zur Zeit die einzigen Abbildungen, die identitätsbasierte Kryptosysteme realisieren, siehe [BSS05], Kapitel X, und [Avan06], chapter 24. Dieser konstruktive Aspekt führt dazu, dass man Kurven mit dem optimalen k konstruieren will, der nicht so klein ist, dass das DLP in subexponentieller Zeit gelöst werden kann, aber gleichzeitig nicht groß ist, so dass die Paarungen effizient berechenbar sind. Man braucht die gewöhnlichen Jacobischen algebraischer Kurven, um optimale Einbettungsgrade zu erzielen. Die Konstruktion solcher Kurven basiert auf der CM-Methode, welche kontrolliert Kurven konstruiert, deren Jacobischen optimale Einbettungsgrade haben, siehe dazu [FST06] und [Fre08]. Es existieren zur Zeit, außer den CM-Methoden, keine Methoden, die die Jacobischen mit optimalen Einbettungsgraden konstruieren.

3.2 Konstruktion elliptischer Kurven

In diesem Abschnitt werden wir uns mit der CM-Konstruktion elliptischer Kurven beschäftigen. Neben der Grundidee der CM-Konstruktion, werden wir auch auf die Berechnung der Klassenpolynome eingehen, da die Konstruktion dieser Polynome den aufwendigsten Teil der CM-Konstruktion darstellt. Dafür werden die analytischen Methoden der Konstruktion der Klassenpolynome erklärt. Desweiteren werden wir auch die anderen Probleme, die bei dieser Konstruktion vorkommen nebst ihren Lösungen erläutern.

3.2.1 Algorithmus

Es sei E eine elliptische Kurve über $\mathbb{C}$. Im ersten Kapitel haben wir gesehen, dass jede elliptische Kurve mit komplexer Multiplikation über $\mathbb{C}$ einen Definitionskörper K hat, welcher ein Zahlkörper ist. Ferner ist der Endomorphismenring $\mathrm{End}_K(E)$ genau dann zu einer Ordnung $\mathcal{O}_t$ eines imaginär

quadratischen Zahlkörpers k (mit der Diskriminante d_k) isomorph, falls E komplexe Multiplikation besitzt.

Wir wollen eine gewöhnliche elliptische Kurve mit vorgegebener Ordnung $N = p+1-t$ über einem endlichen Körper $\mathbb{F}_p$, $p > 3$, konstruieren. Zunächst konstruieren wir dazu eine elliptische Kurve E über K, die komplexe Multiplikation mit einem vorgegebenen Endomorphismenring $\mathrm{End}_K(E) \cong \mathcal{O}_t$ besitzt, wobei $\mathcal{O}_t$ die Ordnung modulo t von k mit der Diskriminante $D = t^2 d_k$ ist. Es existiert ein Isomorphismus zwischen der Galoisgruppe des Ringklassenkörpers Ω_t modulo t über k und der Ringklassengruppe Cl_t nach dem Satz 2.12 aus dem zweiten Kapitel. Zu jedem Primideal $\mathfrak{q}$, welches zu (t) teilerfremd ist, haben wir daher die folgende Äquivalenz:

$$\mathfrak{q} \text{ ist Hauptideal in } \mathcal{O}_t \Leftrightarrow \mathfrak{q} \text{ ist voll zerlegt in } \Omega_t. \tag{3.1}$$

Bestimmung der Primzahl: Der Satz von Hasse besagt, dass für die Gruppe $E(\mathbb{F}_p)$ der $\mathbb{F}_p-$rationalen Punkte einer elliptischen Kurve E stets

$$|E(\mathbb{F}_p)| = p + 1 - t \text{ mit } |t| \leq 2\sqrt{p} \tag{3.2}$$

gilt. Wir bestimmen daher eine Primzahl $p \in [N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N}]$, die in $\mathcal{O}_t$ zerlegt ist:

Dazu überprüfen wir, ob die Gleichung $x^2 - Dy^2 = 4p$ ganzzahlige Lösungen (u, v) besitzt.

Die Lösungen dieser Gleichung lassen sich mit Hilfe vom Cornacchias Algorithmus bestimmen, siehe [Coh93], S. 36, algorithm 1.5.3, falls es welche gibt.

Dann gelten für $\pi = \frac{u+v\sqrt{D}}{2}$ die Gleichungen $\pi\bar{\pi} = p$ und $t = \pi + \bar{\pi}$, siehe [Coh93], S. 471. Da es sich um eine gewöhnliche elliptische Kurve handelt, fordern wir, dass $t \neq 0$ gilt. Wir haben daher die Eigenschaft nach der Äquivalenz 3.1, dass (p) in Ω_t voll zerlegt ist.

Berechnung der Klassenpolynome: Die klassische Methode ist die analytische Konstruktion dieser Polynome mittels der Isomorphie $\mathrm{Cl}_t \cong \mathrm{Gal}(\Omega_t/k)$. Da nach dem Hauptsatz 2.12 der komplexen Multiplikation $\Omega_t = k(j(\tau))$ mit $\tau \in \mathcal{O}_t$ gilt, und nach 2.12, (3), die $j(I)$ mit $I \in \mathrm{Cl}_t$ ein komplettes System der konjugierten Zahlen sowohl über k als auch über $\mathbb{Q}$ bilden, kann man durch das Numerieren der Elemente $j_i = j(I_i)$, $I_i \in \mathrm{Cl}_t$, $i = 1, \cdots, h_t$, das Minimalpolynom wie folgt berechnen:

$$H_D(x) = \prod_{i=1}^{h_t} (x - j_i) \in \mathbb{Q}[x]. \tag{3.3}$$

Satz 3.5. *Die $j-$Invariante einer elliptischen Kurve E über $\mathbb{C}$ mit komplexer Multiplikation ist eine ganz algebraische Zahl.*

Beweis: Der Satz 3.5 kann mittels der klassischen analytischen Methode oder der Reduktionstheorie bewiesen werden. Für die jeweiligen Beweise verweisen wir auf [Sil94], S. 140 bis 151. □

Nach dem Satz 3.5 haben wir nun

$$H_D(x) \in \mathbb{Z}[x]. \tag{3.4}$$

Dieses Polynom heißt das **Hilbertklassenpolynom** der Ordnung $\mathcal{O}_t$, da im Falle maximaler Ordnung $\mathcal{O}_k$ nach dem Satz 2.10 das Polynom $H_D(x)$ den Hilbertklassenkörper $\mathcal{H}_k$ über k erzeugt. In der Literatur sagt man im allgemeinen Fall auch, dass das Polynom $H_D(x)$ Ringklassenpolynom ist. Wir benutzen im Folgenden aber in beiden Fällen den Begriff Hilbertklassenpolynom.

Da das Ideal (p) in Ω_t voll zerlegt ist, zerfällt das Hilbertklassenpolynom $H_D(x)$ über $\mathbb{F}_p$ in Linearfaktoren. Zusätzlich gilt für das Polynom $H_D(x)$ der folgende Satz:

Satz 3.6. *Die Nullstellen von $H_D(x)$ modulo p mit $p \in [N+1-2\sqrt{N}, N+1+2\sqrt{N}]$ sind genau die $j-$Invarianten der gewöhnlichen elliptischen Kurven, deren Endomorphismenringe isomorph zu der Ordnung $\mathcal{O}_t$ sind.*

Beweis: Zunächst sei ε eine gewöhnliche elliptische Kurve über $\mathbb{F}_p$. Wir betrachten nun einen Endomorphismus $\phi \in \mathrm{End}_{\mathbb{F}_p}(\varepsilon)$ mit der Eigenschaft, dass $\mathrm{End}_{\mathbb{F}_p}(\varepsilon) = \mathbb{Z}[\phi] = \mathcal{O}_t$ gilt. Nach dem Lifting-Satz von Deuring, [Lang73], S. 184, existiert eine elliptische Kurve E über einem Zahlkörper K, ein Endomorphismus $\phi' \in \mathrm{End}_K(E)$, und ein Primideal $\mathfrak{p}$ über p, so dass E eine gute Reduktion $\overline{E}$ modulo $\mathfrak{p}$ besitzt, und die Endomorphismenringe von $\overline{E}$ und ε isomorph sind. Aus unserer Wahl $\mathrm{End}(\overline{E}) = \mathbb{Z}[\phi]$ und der Kommutativität dieses Endomorphismenrings folgt, dass die Abbildung zwischen dem reduzierten Endomorphismenring von $\mathrm{End}_K(E)$ modulo $\mathfrak{p}$ und $\mathrm{End}_K(E)$ surjektiv ist, und nach [Lang73], S. 182, sie für jede Reduktion injektiv ist. Daher existiert zu jeder gewöhnlichen elliptischen Kurve ε über $\mathbb{F}_p$ eine elliptische Kurve E über einem Zahlkörper K mit $\mathrm{End}_K(E) \cong \mathrm{End}_{\mathbb{F}_p}(\varepsilon)$. Dies impliziert, dass die elliptische Kurve $\varepsilon/\mathbb{F}_p$ als eine Reduktion einer Kurve E/Ω_t vorkommt.

Umgekehrt sei E eine elliptische Kurve über einem Zahlkörper K mit CM, d. h. $\mathrm{End}_K(E)$ ist isomorph zu einer Ordnung $\mathcal{O}_t$ in einem imaginär quadratischen Zahlkörper k. Da p in K voll zerlegt und kein Teiler des Führers von $\mathcal{O}_t$ ist, gilt $\mathrm{End}_K(\varepsilon) \cong \mathrm{End}_{\mathbb{F}_p}(E)$, siehe [Lang73], S. 175 bzw. 182. Wir haben somit die Eigenschaft, dass die Nullstellen von $H_D(x)$ die $j-$Invarianten der elliptischen Kurven über $\mathbb{F}_p$ sind. □

Twists: Nun werden wir aus den $j-$Invarianten die expliziten Gleichungen der elliptischen Kurven bestimmen. Falls für die Charakteristik des endlichen Körpers $\mathbb{F}_q$ stets $\neq 2, 3$ gilt, können wir jede elliptische Kurve über $\mathbb{F}_q$ in der kurzen Weierstraßform

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 + ax + b, a, b \in \mathbb{F}_q\} \cup \{\mathcal{O}_E\} \tag{3.5}$$

mit $4a^3 + 27b^2 \neq 0$ schreiben. Dann ist die $j-$Invariante von 3.5

$$j = 1728\frac{4a^3}{4a^3 + 27b^2}. \tag{3.6}$$

Nicht isomorphe Kurven über $\mathbb{F}_p$ mit der gleichen $j-$Invariante heißen **Twists** voneinander. Nun wollen wir feststellen, wie viele Twists einer elliptischen Kurve mit der $j-$Invariante j existieren, und daraus was die Anzahl r der nicht isomorphen elliptischen Kurven mit der vorgegebenen $j-$Invariante über $\mathbb{F}_p$ ist. In der Literatur existieren dazu falsche Angaben, siehe [Coh93], S. 472. Daher führen wir im Folgenden einen Beweis für diese Anzahl aus. Weil die Aussage für beliebige endliche Körper $\mathbb{F}_q$ nicht schwerer zu zeigen ist, werden wir die Aussage in dieser allgemeinsten Form formulieren:

Satz 3.7. *Es sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik > 3 mit $j \in \mathbb{F}_q$. Dann ist die Anzahl r der Twists einer elliptischen Kurve über $\mathbb{F}_q$ mit der $j-$Invariante j durch*

$$r = \begin{cases} 4 & \text{, falls } j = 1728 \text{ und } q \equiv 1 \bmod 4 \\ 6 & \text{, falls } j = 0 \text{ und } q \equiv 1 \bmod 3 \\ 2 & \text{sonst} \end{cases} \tag{3.7}$$

gegeben. Außerdem sind zwei gewöhnliche elliptische Kurven E und E' über $\mathbb{F}_q$ genau dann isomorph, wenn sie die gleiche Ordnung und die gleiche $j-$Invariante haben.

Beweis: Es sei nun die Zahl n durch

$$n = \begin{cases} 2 & \text{, falls } j \neq 0, 1728, \\ 4 & \text{, falls } j = 1728, \\ 6 & \text{, falls } j = 0 \end{cases} \tag{3.8}$$

gegeben.

Nach [Sil86], S. 308, Proposition 5.4., ist die Anzahl r gleich dem Index der Untergruppe $(\mathbb{F}_q^*)^n$ von $\mathbb{F}_q^*$. Nun sei α ein Erzeuger der Gruppe $\mathbb{F}_q^*$. Dann ist α^n ein Erzeuger von $(\mathbb{F}_q^*)^n$. Wir haben daher
$\text{ord}(\alpha^n) = \frac{q-1}{\text{ggT}(n,q-1)}$.

- Für $j \neq 0, 1728$ gilt $\text{ord}(\alpha^2) = (q-1)/2$ und somit $r = 2$,
- Für $j = 1728$ und $q \equiv 1 \bmod 4$, gilt $\text{ggT}(4, q-1) = 4 \Rightarrow r = 4$. Für $q \not\equiv 1 \bmod 4$ gilt $\text{ggT}(4, q-1) = 2 \Rightarrow r = 2$.
- Für $j = 0$ und $q \equiv 1 \bmod 3$, gilt $\text{ggT}(6, q-1) = 6 \Rightarrow r = 6$. Für $q \not\equiv 1 \bmod 3$ gilt $\text{ggT}(6, q-1) = 2 \Rightarrow r = 2$.

Für die zweite Aussage merken wir an, dass wir $\text{End}_{\overline{\mathbb{F}}_q}(E) = \text{End}_{\mathbb{F}_q}(E)$ haben, da E gewöhnlich ist, und daher einen kommutativen Endomorphismenring besitzt. Eine Richtung folgt nun aus der Eigenschaft, dass es eine über $\mathbb{F}_q$ definierte Isogenie λ zwischen E und E' gibt, falls sie die gleiche Ordnung besitzen, siehe [Tate66], S. 139, theorem 1:

Da $j(E) = j(E')$ gilt, existiert eine Isomorphie γ zwischen E und E' über $\overline{\mathbb{F}}_q$. Dann gilt $\gamma \circ \lambda \in \text{End}_{\mathbb{F}_q}(E)$. Für jedes Element $\sigma \in \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ folgt daher aus

$$\gamma^\sigma \circ \lambda = \gamma^\sigma \circ \lambda^\sigma = (\gamma \circ \lambda)^\sigma = \gamma \circ \lambda$$

stets $\gamma^\sigma = \gamma$, da $(\gamma^\sigma - \gamma) \circ \lambda = 0$ gilt, und λ als Isogenie insbesondere surjektiv ist.

Die andere Richtung ist trivial. □

Korollar 3.8. *Folgende elliptische Kurven haben die $j-$Invariante j über jedem Körper der Charakteristik $\neq 2, 3$:*

$y^2 = x^3 + \frac{27j}{4(1728-j)}x - \frac{27j}{4(1728-j)}$, *falls* $j \neq 0, 1728$,

$y^2 = x^3 + 1$, *falls* $j = 0$,

$y^2 = x^3 + x$, *falls* $j = 1728$.

Beweis: Aus der elementaren Rechnung der $j-$Invariante der angegebenen elliptischen Kurven folgen die Behauptungen. Für die Auswahl dieser Gleichungen der Kurven verweisen wir auf [Lang73], S. 18 und 19. □

Bemerkung 3.9.

1. *Es folgt nach dem Satz 3.7, dass entweder eine der Kurven aus 3.8 oder einer ihrer Twists genau N Punkte hat. Falls nicht die Kurven aus 3.8 sondern einer ihrer Twists die Ordnung N besitzt, kann man die Gleichungen dieser Twists nach [Coh93], S. 472 und 473, angeben.*
2. *Wir merken an, dass in [Coh93], S. 472, für die Fälle $q \not\equiv 1 \bmod 3$ und $q \equiv 3 \bmod 4$, 6 bzw. 4 Kurvengleichungen angegeben wurden, und nach Satz dem 3.7 nur zwei dieser Gleichungen die Twists und die restlichen eine zu diesen elliptischen Kurven isomorphe Kurven liefern.*

Wir haben nun einen Algorithmus, der zu einer vorgegebenen Zahl N stets die Diskriminante $D < 0$ und u, v mit $u^2 - Dv^2 = 4p$, $p > 3$, berechnet, und damit auch eine elliptische Kurve E über $\mathbb{F}_p$, $p \in [N+1-2\sqrt{N}, N+1+2\sqrt{N}]$ der Ordnung N mit Hilfe der CM-Methode konstruiert. Dieser Algorithmus findet eine elliptische Kurve der Ordnung N, falls eine existiert. Der Beweis folgt unmittelbar aus unseren Vorüberlegungen.

Algorithmus 1: Konstruktion elliptischer Kurven

Eingabe: Eine natürliche Zahl N und eine Primzahl $p \in [N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N}]$ mit $p \neq 2, 3$

Ausgabe: Eine elliptische Kurve E über $\mathbb{F}_p$ der Ordnung N

1. Bestimme die Diskriminante $D < 0$ und u, v mit $u^2 - Dv^2 = 4p$
2. Berechne das Hilbertklassenpolynom $H_D(x) \in \mathbb{Z}[x]$.
3. Reduziere das Polynom $H_D(x)$ modulo p und bestimme eine Nullstelle $j \in \mathbb{F}_p$.
4. Setze $a \leftarrow \frac{27j}{4(1728-j)}$ und $E : y^2 = x^3 + ax - a$, falls $j \neq 0, 1728$, $y^2 = x^3 + 1$, falls $j = 0$, $y^2 = x^3 + x$, falls $j = 1728$ ist.
5. Gebe E oder einen ihrer Twists der Ordnung N zurück.

---

1. Schritt: Falls u, v nicht bekannt sind, kann man, wie zuvor erwähnt wurde, den Cornacchias Algorithmus, [Coh93], S. 36, benutzen, um geeignete u und v zu bestimmen.

2. Schritt: Der ist der aufwendigste Schritt. Es gibt drei verschiedene Methoden, um die Klassenpolynome zu berechnen. Die klassische Methode ist die analytische Konstruktion des Polynoms 3.3, auf die wir im nächsten Abschnitt und im vierten Kapitel näher eingehen wollen. Es gibt auch die $p-$adische Methode der Konstruktion dieser Polynome, die sogenannte **nicht archimedische Methode**, siehe [Brö08], und die Konstruktion mit Hilfe des Chinesischen Restsatzes, die sogenannte **CR-Methode**, [Beld08].

Alle Methoden haben unter bestimmten Annahmen die Laufzeit $O(|D|^{1+\epsilon})$ für $\epsilon > 0$. Die Rekorde liegen zur Zeit bei $|D| > 10^{15}$ für speziell ausgewählte Diskriminanten mit einer Kombination der analytischen und CR-Methoden, siehe [EngSut10].

3. Schritt: Die Methoden der Faktorisierung der Polynome über endlichen Körpern, zum Beispiel die Algorithmen von Berlekamp oder Cantor-Zassenhaus, können für kleine Diskriminanten angewendet werden. Außerdem wird die spezielle Eigenschaft, dass wir die Galoisgruppe des Ringklassenkörpers über k kennen, ausgenutzt, um eine Nullstelle dieses Polynoms modulo einer großen Primzahl zu bestimmen, falls die Diskriminante und somit die Klassenzahl größer wird, und daher mittels der klassischen Faktorisierungsmethoden die Nullstellen zu bestimmen nicht mehr möglich ist. Für die Details verweisen wir auf [HanMor01] und [EngMor03].

4. Schritt: Wir wissen, dass entweder die elliptischen Kurven 3.8 oder einer ihrer Twists die Ordnung N hat. Daher ist die Kenntnis, welcher Twist der Kurven 3.8 die Ordnung N besitzt, für die Effizienz des Verfahrens vorteilhaft.

In [RubSil09] wird ein Verfahren beschrieben, welches mittels des Shimuraschen Reziprizitätsgesetzes den richtigen Twist zuvor bestimmt, damit nicht alle Twists ausprobiert werden müssen, um die richtige elliptische Kurve der Ordnung N zu bestimmen.

5. Schritt: Wenn wir nur eine Untergruppe der Primzahlordnung q bestimmen wollen, müssen wir überprüfen, ob die elliptische Kurve E eine Untergruppe hat, die genau q Punkte besitzt. Man wählt dazu einen zufälligen Punkt P der elliptischen Kurve und überprüft, ob $q.P = \mathcal{O}_E$ gilt. Wir verweisen auf [Mor05] für die Details.

3.2.2 Probleme

Um die numerische Berechnung des Hilbertklassenpolynoms $H_D(x)$ durchführen zu können, müssen wir eine obere Schranke für die benötigte Präzision bestimmen, damit wir bei der Berechnung keine Rundungsfehler haben und somit die ganzzahligen Koeffizienten berechnen können. Eine obere Schranke ist nach [Beld08], S. 285, durch

$$\left\lceil \log_2 \left(2.48 h_t + \pi \sqrt{|D|} \sum_{(a,b,c)\in\mathcal{H}(D)} \frac{1}{a} \right) \right\rceil + 1,$$

gegeben, wobei mit $\mathcal{H}(D)$ die **Formklassengruppe**, die Gruppe der reduzierten binären quadratischen Formen der Diskriminante D, bezeichnet wird. Die Formklassengruppe ist isomorph zu der Idealklassengruppe Cl_t durch die folgende Abbildung, siehe [Uz04], S. 25:

$$Q = (a, b, c) \mapsto [\tau = \frac{-b + \sqrt{D}}{2a}, 1], \tag{3.9}$$

wobei für die Diskriminante von τ stets $D(\tau) = D = b^2 - 4ac$ gilt, und $[\tau, 1]$ die entsprechende Idealklasse in der Ringklassengruppe Cl_t ist. Wir merken an, dass man in der Praxis wegen der Isomorphie 3.9 die binären quadratischen Formen benutzt, da die Arithmetik quadratischer Formen schneller durchzuführen ist.

Die Koeffizienten des Hilbertklassenpolynoms sind sehr groß(verglichen mit dem Betrag der Diskriminante D). Wir haben ca. $\sqrt{|D|}$ Koeffizienten zu berechnen, denn der Satz von Brauer-Siegel besagt, dass der Grad h_t des Hilbertklassenpolynoms wie $|D|^{1/2+o(1)}$ wächst, siehe [Br47]. Die Koeffizienten wachsen sogar exponentiell mit dem Betrag der Diskriminante $|D|$, siehe [BrSt08], S. 23. Für die Diskriminante $D = -204$ zum Beispiel haben wir das Hilbertklassenpolynom

$H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 +$
$9586484163799611206755507 2 \cdot x^4 + 7751217562312410416108497305 60 \cdot x^3 +$
$5344849307032098969604469298728140 80 \cdot x^2 +$
$6020337293681148983229932704488367325184 \cdot x +$
$2850804137703453816686245017215309345665 8432.$

Eine **Klasseninvariante** ist ein singulärer Wert $g(\tau)$, $\tau \in \mathcal{O}_k \cap \mathbb{H}$, einer Modulfunktion g der Stufe N mit der Eigenschaft, dass $k(j(\tau)) = k(g(\tau))$ gilt. Die analytische Konstruktion wird in der Praxis mittels singulärer Werten der sogenannten Klasseninvarianten von Weber oder deren Verallgemeinerungen ermöglicht. Der Vorteil dieser singulären Werten ist, dass die von denen erzeugten Klassenpolynome für diese Werte wesentlich kleinere Koeffizienten als die Koeffizienten der Hilbertklassenpolynome besitzen. Für die obige Diskriminante $D = -204$ bekommen wir zum Beispiel mit einer geeigneten Klasseninvariante das folgende Polynom:

$$W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64,$$

welches wir **Weberklassenpolynom** nennen.

Daher benutzt man in der Praxis, soweit es möglich ist, diese alternativen Klassenpolynome. Obwohl, wie wir im nächsten Kapitel sehen werden, die logarithmische Höhe der Weberklassenpolynome asymptotisch für $|D| \to \infty$ nur einen konstanten Faktor kleiner als die logarithmische Höhe der Hilbertklassenpolynome ist, ist die Verbesserung in der Praxis von großer Bedeutung.

Wir werden im nächsten Kapitel auch darauf eingehen, wie man bestimmen kann, ob ein singulärer Wert einer Modulfunktion höherer Stufe eine Klasseninvariante ist und wie wir damit eine Familie imaginär quadratischen Körper bestimmen können, für die diese Polynome als eine alternative zu den entsprechenden Hilbertklassenpolynome benutzt werden können. Wir brauchen im 3. Schritt des Algorithmus 1 aber die $j(\tau)$ Werte um die Kurvengleichung zu konstruieren. Wir werden auch erläutern, wie die Nullstellen

dieser Polynome und die Nullstellen der Hilbertklassenpolynome zusammenhängen, damit wir die j Invariante über $\mathbb{F}_p$ stets aus den Nulstellen dieser neuen Polynome bestimmen können.

Als nächstes stellt sich die Frage, wie gut wir auf diese Weise primitive Elemente kleinerer Höhe des Körpers $\mathbb{Q}(j(\tau))$ mit einer Klasseninvariante konstruieren können. Auf diese Frage der Optimalität wird auch im nächsten Kapitel eingegangen.

3.3 Konstruktion hyperelliptischer Kurven

Die Verallgemeinerung der CM-Konstruktion elliptischer Kurven auf hyperelliptische Kurven vom Geschlecht zwei und ihre Jacobischen wird in diesem Abschnitt erklärt. Wie im Falle der elliptischen Kurven, ist die Konstruktion der Klassenpolynome der aufwendigste Teil der CM-Konstruktion hyperelliptischer Kurven. Desweiteren sind die Algorithmen nur durchführbar, falls die CM-Körper gewisse Eigenschaften erfüllen. Diese machen die Konstruktion in vielen anderen Fällen unmöglich. Wir werden näher erläutern, welche Schwierigkeiten bei der Konstruktion zu diesen Einschränkungen führen.

Die CM-Methode wurde von Spallek, siehe [Spa94], auf die hyperelliptischen Kurven und ihre Jacobischen vom Geschlecht zwei verallgemeinert. Weng hat nach den Vorarbeiten von Spallek einen Algorithmus entwickelt, der die CM-Konstruktion im Geschlecht zwei durchführt, siehe [Weng01]. Wie bei der CM-Konstruktion elliptischer Kurven gibt es drei verschiedene Methoden der Konstruktion der Igusaklassenpolynomen, zum einen die **analytische** von Weng, zum anderen die $p-$**adische** von Kohel et. al., siehe [Gau06] und [CaKoh08], und auch die **CR-Methode**, siehe [EiLa05]. Wir werden in Folgendem die analytische Methode von Weng erklären.

Infolge des Fehlens der Klasseninvariantensysteme ist eine der Konstruktion der alternativen Klassenpolynome, die in Analogie mit der Klasseninvariante im Geschlecht eins die speziellen Werte der Siegelschen Modulfunktionen höherer Stufe im Geschlecht zwei sein sollten, bisher jedoch nicht möglich. Wir werden im Kapitel 5 zum ersten Mal eine Methode entwickeln, die konstruktiv überprüft, ob die Werte solcher Modulfunktionen ein Klasseninvariantensystem bilden.

3.3.1 Algorithmen

Algorithmus von Weng

Wir wollen zunächst eine einfache hauptpolarisierte abelsche Fläche mit komplexer Multiplikation $\mathcal{O}_K$ konstruieren, wobei $\mathcal{O}_K$ die Maximalordnung eines

primitiven CM-Körpers K vom Grad 4 über $\mathbb{Q}$ mit einem reellen quadratischen Teilkörper K_0 ist. Dabei wird die Klassengruppe von K_0 als trivial vorausgesetzt. Diese Fläche ist genau die Jacobische einer hyperelliptischen Kurve vom Geschlecht zwei. Wir wissen, dass K entweder eine zyklische Erweiterung von $\mathbb{Q}$ oder eine nicht-galoissche Erweiterung von $\mathbb{Q}$ ist, deren galoissche Hülle L die Galoisgruppe D_4 über $\mathbb{Q}$ hat.

Wir fixieren zunächst einen solchen CM-Körper K. Wir merken an, dass diese Methode nach der Cohen-Lenstra Heuristik, siehe [CohLe84], auf mehr als 3/4 der primitiven CM-Körper anwendbar ist, da die Dichte der reell quadratischen Zahlkörper mit Klassenzahl eins nach dieser Heuristik größer als 3/4 ist.

Um eine hyperelliptische Kurve C über einem geeigneten endlichen Körper $\mathbb{F}_p$ zu konstruieren, müssen wir den Frobeniusendomorphismus π betrachten. Nach dem ersten Kapitel besitzt π ein irreduzibles charakteristisches Polynom vom Grad 4 über $\mathbb{Q}$, welches über $\mathbb{Q}$ den CM-Körper $K = \mathbb{Q}(\pi)$ erzeugt, da K primitiv ist. Mit Hilfe der Nullstellen π_i, $i = 1, \cdots, 4$, von π können wir die Ordnung der Jacobischen $J(C)$ durch

$$|J(C)| = \prod_{i=1}^{4}(1 - \pi_i) \tag{3.10}$$

bestimmen. Diese Nullstellen π_i sind assoziiert, und je zwei Nullstellen unterscheiden sich um eine Einheitswurzel. Daher haben wir zwei mögliche Gruppenordnungen nach 3.10, falls K keinen Kreisteilungskörper enthält, das heißt $\mathrm{Tor}(K) = \{\pm 1\}$ ist, wobei $\mathrm{Tor}(K)$ die Torsionsgruppe der Einheiten von K bezeichnet. Allgemeiner gibt es daher genau $|\mathrm{Tor}(K)|$ Möglichkeiten für die Gruppenordnung.

Um nun eine geeignete Primzahl p zu bestimmen, lösen wir zunächst die relative Normgleichung zu einem Element $\omega \in \mathcal{O}_K$

$$\omega\bar{\omega} = p. \tag{3.11}$$

Bemerkung 3.10. *Falls es keine nicht trivialen Einheitswurzeln gibt, liefert die Methode von Weng für die Jacobische $J(C)$ über $\mathbb{F}_p$ zwei mögliche Gruppenordnungen N_1 und N_2. Wenn p in K voll zerfällt und K nicht galoissch ist, existieren drei oder vier mögliche Gruppenordnungen, falls die Normgleichung 3.11 zwei verschiedene Lösungen, abgesehen vom Vorzeichen, besitzt, siehe [Weng01], S. 52 und 53, Satz 3.1.8.*

Nach diesen Vorüberlegungen können wir eine hyperelliptische Kurve über $\mathbb{F}_p$ konstruieren, falls p der relativen Normgleichung 3.11 genügt.

Wie bei den elliptischen Kurven, wollen wir nun alle nicht isomorphen hauptpolarisierten abelschen Flächen bestimmen, die die komplexe Multiplikation

durch die Maximalordnung $\mathcal{O}_K$ besitzen. Diese werden durch die Periodenmatrizen τ_i in der Siegelschen oberen Halbebene $\mathbb{H}_2$ gegeben.

Es sei nun $K_0 = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{N}$, der reell quadratische Teilkörper von K. Wir können den CM-Körper K durch $K = \mathbb{Q}(i\sqrt{\alpha})$ mit einem quadratfreien total positiven Element $\alpha = a + b\sqrt{d}$ angeben. Ferner bezeichne U^+ die Gruppe aller Einheiten mit positiver Norm von K_0 und U_1 die Untergruppe der gesamten Normeinheiten bezüglich K/K_0 von U^+. Es gilt $U^+ = U_1$, falls die Fundamentaleinheit in K_0 eine negative Norm hat. Da die Klassenzahl von K_0 eins ist, existiert eine relative Ganzheitsbasis von $\mathcal{O}_K$ von der Form

$$\mathcal{O}_{K_0} + \gamma\mathcal{O}_{K_0} \text{ mit } \gamma \in \mathcal{O}_K. \tag{3.12}$$

Die reelle Konjugation von K_0 hat zwei Fortsetzungen nach K. Wir setzen

$$\hat{\sigma}(i\sqrt{\alpha}^+) = i\sqrt{\sigma(\alpha)} \text{ und } \rho\hat{\sigma}(i\sqrt{\alpha}^+) = -i\sqrt{\sigma(\alpha)}, \tag{3.13}$$

wobei $\sqrt{a}^+$ die positive Quadratwurzel einer reellen Zahl a, σ die reelle Konjugation von K_0 und ρ die komplexe Konjugation von K sind.

Es gilt nun der folgende Satz von Spallek, siehe [Spa94], S. 60, Satz 4.7, und S. 62 Satz 4.8, welcher ein volles Repräsentantensystem nicht isomorpher einfacher hauptpolarisierter abelscher Flächen mit CM durch $\mathcal{O}_K$ und die zugehörigen Periodenmatrizen bestimmt

Satz 3.11. *Es sei K ein primitiver CM-Körper vom Grad 4 über $\mathbb{Q}$ mit der Klassengruppe $\tau_1, \cdots, \tau_{h_K}$ mit $\Im(\tau_j) > 0$, $j = 1, \cdots, h_K$, gegeben. Ferner seien $K_0 = \mathbb{Z} + \mathbb{Z}\omega$ der reelle quadratische Zahlkörper von K, σ die reelle Konjugation von K_0, ρ die komplexe Konjugation von K und $\varphi = \rho\hat{\sigma}$.*

1. *Ein Repräsentantensystem nicht isomorpher einfacher hauptpolarisierter abelscher Flächen mit CM durch $\mathcal{O}_K$, ist durch folgende Menge gegeben*

$$\mathcal{K} = \begin{cases} \mathcal{K}_{1,\varphi} & \text{, falls } K \text{ galoissch ist,} \\ \mathcal{K}_{1,\varphi} \cup \mathcal{K}_{1,\bar{\varphi}} & \text{, sonst} \end{cases}$$

wobei $\mathcal{K}_{1,\varphi}$ und $\mathcal{K}_{1,\bar{\varphi}}$ durch die folgenden Mengen definiert sind:

$$\mathcal{K}_{1,\varphi} = \begin{cases} \{(\tau_j, \tau_j^{\varphi}), (\varepsilon_0\tau_j, \varepsilon_0\tau_j^{\varphi}) : N_{K/K_0}(\tau_j) \text{ ist total positiv}\}, & \text{falls } \varepsilon_0 \in U_1 \text{ ist,} \\ \{(\tau_j, \tau_j^{\varphi}) : N_{K/K_0}(\tau_j) \text{ ist total positiv}\}, & \text{falls } \varepsilon_0 \in U^+\backslash U_1 \text{ ist,} \\ \{(\tau_j, \tau_j^{\varphi}) : N_{K/K_0}(\tau_j) \text{ ist total positiv}\}, & \text{sonst,} \end{cases}$$

$$\mathcal{K}_{1,\bar{\varphi}} = \begin{cases} \{(\tau_j, \tau_j^{\bar{\varphi}}), (\varepsilon_0\tau_j, (\varepsilon_0\tau_j)^{\bar{\varphi}}) : N_{K/K_0}(\tau_j) \text{ ist nicht total pos.}\}, & \text{falls } \varepsilon_0 \in U_1 \text{ ist,} \\ \{(\tau_j, \tau_j^{\bar{\varphi}}) : N_{K/K_0}(\tau_j) \text{ ist nicht total pos.}\}, & \text{falls } \varepsilon_0 \in U^+\backslash U_1 \text{ ist,} \\ \{(\varepsilon_0\tau_j, \varepsilon_0\tau_j^{\bar{\varphi}}) : N_{K/K_0}(\tau_j) \text{ ist total positiv}\}, & \text{sonst.} \end{cases}$$

2. *Die Periodenmatrix einer einfachen hauptpolarisierten abelschen Fläche vom Typ* $(K, \{1, \psi\})$ *der Form* (s_j, s_j^ψ) *ist durch folgende Matrix gegeben:*

$$\Omega_{(s_j, s_j^\psi)} = \frac{1}{\omega - \omega^\sigma} \begin{pmatrix} \omega^2 s_j - (\omega^\psi)^2 s_j^\psi & \omega s_j - \omega^\psi s_j^\psi \\ \omega s_j - \omega^\psi s_j^\psi & s_j - s_j^\psi \end{pmatrix}.$$

Der folgende Satz gibt die Anzahl der Periodenmatrizen nicht isomorpher einfachen abelschen Flächen an:

Satz 3.12. *Es sei* K *ein primitiver CM-Körper vom Grad* 4 *über* $\mathbb{Q}$ *und* $\mathcal{C}(K)$ *die wie in 2.1 definerte Gruppe mit* $h := |\mathcal{C}(K)|$*. Dann gilt für die Anzahl* s *der Periodenmatrizen nicht isomorpher einfacher abelscher Flächen mit dem Endomorhismenring* $\mathcal{O}_K$

$$s = \begin{cases} h, \text{ falls } K \text{ galoissch ist,} \\ 2h, \text{ falls } K \text{ nicht galoissch ist.} \end{cases}$$

Beweis: Nach dem Satz 2.1 und 2.2 haben wir für die Anzahl s_0 der Isomorphieklassen der hauptpolarisierten abelschen Varietäten vom CM-Typ (K, Φ) stets

$$s_0 = \frac{|\mathrm{Cl}(\mathcal{O}_K)|}{|\mathrm{Cl}^0(\mathcal{O}_{K_0})|} |(\mathcal{O}_{K_0}^*)^+ / N_{K/K_0}(\mathcal{O}_K^*)|.$$

Dieser Wert ist offenbar von der Auswahl des CM-Typs Φ unabhängig. Es gibt genau einen CM-Typ im Falle zyklischer primitiver CM-Körper und zwei CM-Typen im Falle nicht galoisscher primitiver CM-Körper bis auf komplexe Konjugation. Daher folgt die Behauptung. □

Satz 3.13. *Es sei* K *ein primitiver CM-Körper vom Grad* 4 *über* $\mathbb{Q}$ *über einem reell quadratischen Zahlkörper* K_0*, dessen Klassenzahl* $h_{K_0} = 1$ *ist. Dann gilt für die Anzahl* s *der Periodenmatrizen nicht isomorpher einfacher abelscher Flächen mit dem Endomorhismenring* $\mathcal{O}_K$

$$s = \begin{cases} h_K, \text{ falls } K \text{ galoissch ist,} \\ 2h_K, \text{ falls } K \text{ nicht galoissch ist,} \end{cases}$$

wobei h_K *die Klassenzahl von* K *bezeichnet.*

Beweis: Es gilt

$$\frac{|(\mathcal{O}_{K_0}^*)^+ / N_{K/K_0}(\mathcal{O}_K^*)|}{|\mathrm{Cl}^0(\mathcal{O}_{K_0})|} = 1$$

nach [Weng01], S. 54. Dann folgt aus 3.12 die Behauptung. □

Invarianten und Klassenpolynom

Nun muss man wie im Falle der $j-$Invariante die Klasseninvarianten j_1, j_2 und j_3 von Igusa berechnen. Diese Invarianten sind rationale Funktionen der geraden Thetanullwerte, wie wir im ersten Kapitel gesehen haben. Man berechnet daher mittels der geraden Thetanullwerte die numerischen Werte dieser Invarianten $j_i^{(l)} = j_i(\Omega_l)$, $i = 1, 2, 3$ und $l = 1, \cdots, s$, und konstruiert die entsprechenden Igusaklassenpolynome durch

$$H_i(x) = \prod_{i=1}^{s}(x - j_i^{(l)}) \tag{3.14}$$

Diese Polynome haben rationale Koeffiziente, weil für jeden Autormorphismus σ von $\mathbb{C}$ die hauptpolarisierte abelsche Varietät (A^σ, E^σ) vom CM-Typ (K, Φ) ist, falls (A, E) vom CM-Typ (K, Φ) ist, siehe [Spa94], S. 75 und 76. Somit haben wir

$$H_i(x) \in \mathbb{Q}[x]. \tag{3.15}$$

Für diese Polynome berechnet man das kleinste gemeinsame Vielfache D der Nenner mittels des Kettenbruchalgorithmus, damit wir durch das Multiplizieren mit D die Polynome $D \cdot H_i(x) = \widehat{H_i}(x) \in \mathbb{Z}[x]$ berechnen können, siehe [Weng01], S. 37. Dann werden die Polynome modulo p reduziert, um die entsprechenden Igusa-Invarianten modulo p zu bestimmen. Im Gegensatz zu den Hilbertklassenpolynomen zerfallen die Igusaklassenpolynome modulo p nicht immer in Linearfaktoren. Der folgende Satz besagt aber, dass die reduzierten Polynome mindestens eine Nullstelle modulo p besitzen, siehe [Weng01], Abschnitt 3.2:

Satz 3.14. *Die Igusaklassenpolynome besitzen mindestens eine Nullstelle modulo p, falls p der relativen Normgleichung 3.11 genügt.*

Bemerkung 3.15. *Aus den Igusa-Invarianten können wir nicht die expliziten Kurvengleichungen direkt bestimmen. Der Algorithmus von Mestre berechnet zu gegebenen Igusa-Invarianten die expliziten Kurvengleichungen, siehe [Weng01], S. 32.*

Als letztes muss man die richtige hyperelliptische Kurve berechnen, deren Jacobische die vorgegebene Ordnung hat. Dieses geschieht wie im Falle der elliptischen Kurven mittels der Betrachtung der Twists solcher Kurven, siehe [Weng01], S. 37 und 38.

Der folgende Algorithmus berechnet stets eine hyperelliptische Kurve über einem endlichen Körper $\mathbb{F}_p$ vom Geschlecht zwei, wobei p der relativen Normgleichung 3.11 genügt.

Algorithmus 2: Konstruktion hyperelliptischer Kurven (analytisch)

Eingabe: Ein primitiver CM-Körper K vom Grad 4 über $\mathbb{Q}$ und eine Primzahl p, die der Gleichung 3.11 genügt.

Ausgabe: Eine hyperelliptische Kurve C vom Geschlecht zwei mit $J(C) = N \in \{N_1, N_2\}$ (oder $N \in \{N_1, \cdots, N_4\}$, siehe 3.10)

1. Bestimme die Liste $L = \{\tau_1, \cdots, \tau_s\}$ aller hauptpolarisierten abelschen Flächen mit CM durch $\mathcal{O}_K$ anhand von 3.11, wobei s wie in 3.12 ist.
2. Berechne die 10 geraden Thetanullwerte mit hinreichender Präzision.
3. Berechne die Klassenpolynome $H_i(x) \in \mathbb{Q}[x]$, $i = 1, 2, 3$.
4. Bestimme $D \in \mathbb{Z}$ mit $\widetilde{H_i}(x) = D \cdot H_i(x) \in \mathbb{Z}[x]$.
5. Bestimme die Nullstellen j_1, j_2, j_3 von $\widetilde{H_i}(x)$ modulo p.
6. Bestimme die Kurvengleichung mittels $\{j_1, j_2, j_3\}$ und des Algorithmus von Mestre, siehe 3.15
7. Gebe C oder einen ihrer Twists der Ordnung N zurück.

Wir werden auf die Probleme, die Einschränkungen und die Laufzeit dieses Verfahrens im nächsten Abschnitt näher eingehen.

Nicht archimedische Methode

In [Gau06] und [CaKoh08], haben Kohel et. al. ein alternatives Verfahren zur Konstruktion der Igusa-Klassenpolynome entwickelt, welches die Methode von [Brö08] auf Geschlecht zwei verallgemeinert.

Im Gegensatz zur klassischen Konstruktion, basiert das $p-$adische Verfahren darauf, dass man, statt mit einem CM-Körper K, mit einer hyperelliptischen Kurve C über $\mathbb{F}_{p^d}$ beginnt, um die Igusa-Klassenpolynome zu berechnen, wobei $p = 2$ in [Gau06] und $p = 3$ in [CaKoh08], d eine kleine natürliche Zahl sind, so dass der Endomorphismenring der Jacobischen von C leicht zu berechnen ist.

Der folgende Satz verallgemeinert 3.6 auf abelsche Varietäten, siehe [Gau06],

Satz 3.16. *1. Es seien $\mathbb{Q}_p$ der Körper der $p-$adischen Zahlen und $\mathbb{Q}_p^d$ die eindeutige unverzweigte Körpererweiterung von $\mathbb{Q}_p$, $\mathbb{Z}_p$ und $\mathbb{Z}_p^d$ die*

Ganzheitringe von $\mathbb{Q}_p$ bzw. $\mathbb{Q}_p^d$. Es gibt eine abelsche Varietät A' über $\mathbb{Z}_p^d$, der sogenannte kanonische Lift einer gewöhnlichen abelschen Varietät A über $\mathbb{F}_p^d$ mit

$$End(A') \cong End(A).$$

Ferner, ist A' nicht nur über $\mathbb{Z}_p^d$ sondern auch über $\overline{\mathbb{Q}}$ definiert.

2. *Es sei $\bar{C}$ eine gewöhnliche hyperelliptische Kurve über $\mathbb{F}_{p^d}$ vom Geschlecht zwei. Dann existiert eine hyperelliptische Kurve vom Geschlecht zwei über $\mathbb{Q}_p^d$, deren Jacobische ein kanonischer Lift der Jacobischen von $\overline{C}$ ist. Ferner existiert eine $(p,p)-$Isogenie zwischen $J(C)$ und $J(C^\sigma)$, welche die Frobeniusabbildung σ von $J(\overline{C})$ in ihren Konjugierten reduziert.*

Der Satz 3.16 besagt nun, dass zu einer gewöhnlichen abelschen Varietät über $\mathbb{F}_{p^d}$ stets der kanonische Lift existiert. Er liefert aber keine explizite Konstruktion.

Die Richelot-Isogenie liefert die Relationen zwischen den definierenden Gleichungen hyperelliptischer Kurven vom Geschlecht zwei, deren Jacobischen $(2,2)-$isogen sind. Sie ermöglicht eine explizite Beschreibung des Satzes 3.16 mittels einer Menge der Gleichungen, die den kanonischen Lift definieren, falls 2 in $\mathcal{O}_K \cong \mathrm{End}(J(\overline{C}))$ voll zerlegt ist. Danach werden diese Gleichungen mittels einer Variante des Newton-Verfahrens gelöst, welches die expliziten Igusa-Invarianten des kanonischen Lifts mit höher Präzision nebst dem Grad s der Igusa-Klassenpolynome mit Hilfe einer Variante des LLL-Algorithmus berechnet. Für die Details verweisen wir auf [Gau06].

Diese explizite Konstruktion des kanonischen Lifts wurde in [CaKoh08] auf $p = 3$ verallgemeinert. Die nicht analytische Methode ermöglicht deshalb die Konstruktion der Igusa-Klassenpolynome, falls $p = 2$ oder $p = 3$ in $\mathcal{O}_K$ voll zerlegt ist. Eine eventuell explizite Konstruktion der Invariante des kanonischen Lifts würde die Verallgemeinerung dieser Methode für in $\mathcal{O}_K$ zerlegte $p > 3$ erweitern.

Algorithmus 3: Nicht archimedische Konstruktion

Eingabe: Eine gewöhnliche hyperelliptische Kurve $\overline{C}$ über $\mathbb{F}_{p^d}$ vom Geschlecht zwei mit CM durch $\mathrm{End}(J(\overline{C})) \cong \mathcal{O}_K$, $d \in \mathbb{N}$, und eine Primzahl p, die der Gleichung 3.11 genügt.

Ausgabe: Eine hyperelliptische Kurve C vom Geschlecht zwei mit $J(C) = N \in \{N_1, N_2\}$ (oder $N \in \{N_1, \cdots, N_4\}$, siehe 3.10)

1. Berechne die Igusa-Invarianten $\bar{j_1}, \bar{j_2}, \bar{j_3}$ von $\overline{C}$ und wähle einen beliebigen Lift auf $\mathbb{Z}_p^d$.

2. Berechne die Invarianten j_1, j_2, j_3 des kanonischen Lifts aus dem Lift im ersten Schritt.

3. Bestimme den Grad s von $H_i(x)$.

4. Wende den LLL-Algorithmus mit den Eingaben s und den Potenzen von j_1, j_2, j_3 an.

5. Bestimme mit den Ergebnissen des vierten Schritts die Polynome $H_i(x)$.

6. Bestimme $D \in \mathbb{Z}$ mit $\widetilde{H_i(x)} = D \cdot H_i(x) \in \mathbb{Z}[x]$.

7. Bestimme die Kurvengleichung mittels $\{j_1, j_2, j_3\}$ und des Mestre-Algorithmus, siehe 3.15

8. Gebe C oder einen ihrer Twists der Ordnung N zurück.

Siehe [Gau06] und [CaKoh08] für die Details, wie man den LLL-Algorithmus anwenden kann, um die entsprechenden Potenzen von j_1, j_2, j_3 nebst dem Grad s dieser Polynome zu bestimmen.

3.3.2 Einschränkungen und Probleme

Klassenzahl von K_0: Der Algorithmus von Weng setzt voraus, dass der reell quadratische Zahlkörper K_0 die Klassenzahl eins hat. In diesem Fall existiert eine relative Ganzheitsbasis von K über K_0. Aber schon die Existenz einer solchen ist eine hinreichende Bedingung dafür, dass wir die Menge aller nicht isomorpher hauptpolarisierter abelscher Varietäten bestimmen können. Wir werden im fünften Kapitel die Bedingungen für die Existenz einer relativen Ganzheitsbasis von K über K_0 herleiten, um die CM-Methode auf alle primitiven CM-Körper K zu erweitern.

Berechnung der Periodenmatrizen und Thetanullwerte: Um die Werte $j(\tau_i)$ schneller berechnen zu können, wendet man im Geschlecht eins die $\mathrm{SL}(2,\mathbb{Z})$ äquivalenten Elemente von $\tau_i \in \mathrm{Cl}_{\mathcal{O}}$ an, welche im Fundamentalbereich von $\mathbb{H}$ liegen, da die $j-$Invariante in diesem Fall schneller konvergiert. Seit der Arbeit von Gottschling [Got59] ist es möglich, auch im Geschlecht zwei die Peridodenmatrizen zunächst auf den Fundamentalbereich $\mathcal{B}$ abzubilden.

Die MAGMA-Funktion, [MAGMA], `To2DUpperHalfSpaceFundamentalDomain` bildet zum einen jede Periodenmatrix nach $\mathcal{B}$ ab und gibt zum anderen die Transformationen aus, welche uns eine schnellere Konvergenz unserer Igusaklasseninvariante ermöglichen.

Im Schritt 3 des Algorithmus 2 müssen wir die Thetanullwerte mit hinreichender Präzision berechnen, damit die Werte der Igusa-Klasseninvariante im Schritt 4 berechnet werden können. Weng hat Schranken für die Thetanullwerte mit vorgegebener Präzision im Geschlecht zwei angegeben, [Weng01] S. 27. Eine verbesserte Version der Schranken der Thetanullwerte ist in der Arbeit von Dupont zu finden. Damit ist es möglich, die Thetanullwerte (und somit die Igusa-Klassenpolynome) mit absolutem Fehler $< 10^{-s}$ zu berechnen, [Dup06], S. 138 bis 141. Schließlich hat Streng, [Str10], S. 35, mit Hilfe dieser Schranken eine verbesserte Version der Berechnung der Igusa-Klasseninvarianten gegeben:

Korollar 3.17. *Es seien* $\Omega = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_3 & \tau_2 \end{pmatrix} \in \mathcal{B}$, x_j *und* y_j *der reelle bzw. imaginäre Teil von* z_j, $j = 1, 2, 3$, *und* j_k *die in 1.28 definierten Igusa-Invarianten. Dann gilt*

- $\log_2 |h_4(\Omega)| < 8$,
- $\log_2 |h_6(\Omega)| < 13$,
- $\log_2 |h_{10}(\Omega)| < 11$,
- $\log_2 |h_{12}(\Omega)| < 17$,
- $-\log_2 |h_{10}(\Omega)| < \pi(y_1 + y_2 - y_3) + 3 + max\{2, -\log_2 |z_3|\}$,
- $\log_2 |j_k(\Omega)| < 2\pi(y_1 + y_2 - y_3) + 64 + 2max\{2, -\log_2 |z_3|\}$, $k = 1, 2, 3$

Schranken für die Nenner der Klassenpolynome: Um die gesamte Laufzeit der Konstruktion der Igusa-Klassenpolynomen bestimmen zu können, brauchen wir eine obere Schranke D der Igusa-Klassenpolynome für die

$$D \cdot H_i(x) \in \mathbb{Z}[x]$$

gilt. Diese Schranken werden in [GoLau10] gegeben. Sie ermöglichen es Streng ([Str10]), die Laufzeit der Konstruktion der Igusaklassenpolynome durch folgenden Satz anzugeben:

Satz 3.18. *Es sei* Δ_0 *die Diskriminante des reell quadratischen Teilkörpers* K_0 *eines CM-Körpers* K *vom Grad vier über* $\mathbb{Q}$ *mit der Diskriminante* $\Delta = \Delta_1 \Delta_0^2$. *Die Igusaklassenpolynome* $H_i(x)$, *(*$i = 1, 2, 3$*) im Schritt 3 des Algorithmus 2 werden für jeden primitiven CM-Körper* K *vom Grad vier über* $\mathbb{Q}$ *in* $O(\Delta_1^{7/2} \Delta_0^{11/2})$ *berechnet, falls die Bedingung 1.18 erfült ist. Die Länge der Ausgabe ist* $O(\Delta_1^2 \Delta_0^3)$.

Nicht-archimedische Methoden:

Um diese Methode anwenden zu können, benötigt man die Eigenschaft, dass p in $\mathcal{O}_K$ voll zerlegt ist. Wie wir erwähnt haben, braucht man die explizite Konstruktion der Invariante des kanonischen Lifts, um diese Methode auf in $\mathcal{O}_K$ zerlegte $p > 3$ erweitern zu können. Selbst für $p = 3$ ist diese explizite Beschreibung sehr kompliziert, siehe [CaKoh08]. Deswegen ist diese Methode zur Zeit nur sinnvoll, falls 2 oder 3 in $\mathcal{O}_K$ voll zerlegt ist. In [Koh07], hat Kohel die nicht-archmedische und analytische Methode implementiert. Wegen der leider zur Zeit fehlenden effizienten Arithmetik der Thetafunktionen, insbesondere der Thetanullwerte, führte es dazu, dass die Igusa-Klassenpolynome mit der nicht-archimedischen Methode in dieser Datenbank nur bis zum Grad 96 bestimmt sind.

Kapitel 4

Klassenpolynome vom Geschlecht eins

In diesem Kapitel beschäftigen wir uns mit der Konstruktion von Klassenpolynomen vom Geschlecht eins.

Es sei k ein imaginär quadratischer Zahlkörper. Im ersten Abschnitt erklären wir das Reziprozitätsgesetz von Shimura, welches uns ermöglichen wird, effizient zu überprüfen, ob ein singulärer Wert $g(\tau)$ einer Modulfunktion g der Stufe N eine Klasseninvariante ist, das heißt ob $k(g(\tau)) = k(j(\tau))$ gilt.

Weber hat schon im Jahre 1908 in seinem 'Lehrbuch der Algebra' ([Wb1908]) solche Modulfunktionen höherer Stufe eingeführt. Es ist allerdings bei seinen Formulierungen nicht klar, ob es sich um einen Satz oder um eine numerische Beobachtung handelte.

Aufgrund dieser Unklarheit führte Heegner ([Heeg52], S. 22 bis 27) einen lückenhaften Nachweis des Klassenzahleinsproblems. Diese Unklarheiten wurden nach den Vorarbeiten von Weber und Heegner von Birch ([Birch69]) und von Stark ([St69]) geklärt.

Shimura entwickelte in seinem Buch 'Introduction to the Arithmetic Theory of Automorphic Functions' seine abstrakte Theorie, insbesondere sein Reziprozitätsgesetz ([Sh71]) welches Gee und Stevenhagen ermöglichte, die Klasseninvarianteneigenschaft konstruktiv zu überprüfen und die Verallgemeinerung der Klasseninvariante von Weber einzuführen ([GeSt98]).

Schertz ([Sch02]) hat mittels dieses Reziprozitätsgesetzes die von Weber eingeführten Klasseninvarianten vollständig bewiesen. Schertz, Enge und Morain benutzten seine Methoden verallgemeinerte Klasseninvarianten zu entwickeln, die einerseits statt einfachen $\eta-$Quotienten mittels der Doppel $\eta-$Quotienten ([EnSch04]), und andererseits mittels verallgemeinerter Weberscher Funktionen konstruiert sind ([EngMor09]).

Das zur Zeit schnellste Verfahren, welches die Klasseninvarianten als singuläre Werte gewisser $\eta-$Quotienten numerisch berechnet, basiert auf der Berechnung der geraden Thetanullwerte mit hinreichender Präzision mittels der AGM-Methode von Dupont ([Dup07]) und mittels einer Identität zwischen den Thetanullwerten und der Funktion η^{12}. Aus dieser Identität lässt sich die Werte der Dedekinschen $\eta-$Funktion und die Klasseninvarianten etwa mit Hilfe des 12ten Wurzelziehens durch eine Variante der Newton Iteration berechnen. Dieses Verfahren berechnet die $N-$signifikanten Bits eines Thetanullwerts in $O(\mathcal{M}(N)\log N)$, wobei $\mathcal{M}(N)$ die Komplexität der Multiplikation zweier $N-$Bit Zahlen bezeichnet.

Im zweiten Abschnitt werden wir zeigen, dass wir die klassischen Klasseninvarianten als singuläre Werte von Quotienten gewisser Thetanullwerte darstellen können, und somit der zweite Schritt, nämlich die 12ten Wurzeln von η zu ziehen, gespart werden kann. Dadurch erhalten wir das schnellste Verfahren, welches die Klasseninvarianten mittels der Thetanullwerte berechnet. Insgesamt sparen wir in der Laufzeit $O(\mathcal{M}(N))-$Bit Operationen.

Im dritten Abschnitt werden wir zeigen, dass fast alle Klasseninvarianten von Weber stets Einheiten in den entsprechenden Ringklassenkörpern sind. Diese Ergebnisse ermöglichen es, neue Klasseninvarianten zu erhalten, auf die wir auch im dritten Abschnitt eingehen werden.

Die Eigenschaft, dass eine Klasseninvariante eine Einheit in dem entsprechenden Ringklassenkörper ist, liefert ein Verfahren, mit dem die Einheitengruppen solcher Ringklassenkörper berechnet werden können. Wir werden dieses Verfahren im Abschnitt vier entwickeln. Wir wenden dabei die untere Regulatorabschätzung von Fieker und Pohst ([FiPohst08]) und ein Verfahren an, welches aus einer Untergruppe von endlichem Index der Einheitengruppe die volle Einheitengruppe berechnet ([PhZs89], s. 371 und 372).

Die von Gee ([Gee01]), Enge und Morain ([EngMor09]) entwickelten verallgemeinerten Klasseninvarianten werden wir im fünften Abschnitt mittels der Thetanullwerte darstellen. Dies ermöglicht, auch in diesen Fällen schnellere Berechnung der numerischen Werte dieser verallgemeinerten Invarianten durchzuführen. Des Weiteren werden wir auch zeigen, dass die von Gee eingeführten Klasseninvarianten Einheiten in den entsprechenden Hilbertklassenkörpern sind.

Im letzten Abschnitt werden wir auf die Frage der Optimalität der Klasseninvariante eingehen. Dabei werden wir uns mit der Frage beschäftigen, wie gut wir die alternativen Klassenpolynome im Vergleich zu den Hilbertklassenpolynomen mittels der CM-Konstruktion erhalten können.

Teile der Ergebnisse der Abschnitte zwei, drei und vier hat uns zu dem Artikel 'On the computation of class polynomials with "Thetanullwerte" and its applications to the unit group computation' geführt ([LePoUz09]). Wir

merken an, dass die Ergebnissen der Darstellung der Invarianten mittels der Thetanullwerte dieses Artikels, [LePoUz09], S. 5, im Abschnitt drei mit Hilfe der Duplikationsformel der Thetafunktionen verbessert sind.

4.1 Shimurasches Reziprozitätsgesetz

Wie wir im dritten Kapitel erwähnt haben, wachsen die Koeffizienten der Hilbertklassenpolynome exponentiell mit dem Betrag der Diskriminante, welche die Erzeugung der Hilbert- oder Ringklassenkörper für große Diskriminanten unausführbar macht. Unser Ziel ist es nun, statt der $j-$Invariante die Modulfunktionen g höherer Stufe zu betrachten. Die Hoffnung ist, dass sowohl die singulären Werte $g(\tau)$ dieser Funktionen die Hilbert- bzw. Ringklassenkörper erzeugen, als auch die Minimalpolynome dieser Werte kleinere Koeffizienten als die Koeffizienten der Hilbertklassenpolynome besitzen. Um die Anwendungen realisieren zu können, auf die wir im dritten Kapitel eingegangen sind, müssen wir zusätzlich in der Lage sein, aus den Nullstellen der Minimalpolynome dieser neuen Klasseninvarianten die entsprechenden $j-$Werte zu bestimmen.

Um die Minimalpolynome solcher Klasseninvarianten bestimmen zu können, müssen wir in der Lage sein, die Konjugierten dieser Invarianten zu bestimmen. Dies bedeutet, dass allein die Tatsache, dass die Klasseninvarianten die Ringklassenkörper erzeugen, uns keine Methode liefert, mit der wir die Klassenpolynome berechnen können.

Modulfunktionen

Sämtliche Aussagen in diesem Abschnitt sind in [Lang73] zu finden, falls sie nicht explizit zitiert oder bewiesen sind.

Die Modulfunktionen der beliebigen Stufe $N > 1$ erhält man durch die Kongruenzuntergruppe $\Gamma(N) = \ker[\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})]$. Die kompaktifizierte Riemannsche Fläche $(\Gamma(N)/H)^*$ ist isomorph zu der Modulkurve $X(N)$ der Stufe N über $\mathbb{C}$. Der Funktionenkörper $\mathcal{F}_{N,\mathbb{C}}$ von $X(N)$ über $\mathcal{F}_{1,\mathbb{C}}$ hat die Galoisgruppe $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$, wobei 1_2 die 2×2 Einheitenmatrix bezeichnet. Die Modulfunktionen der Stufe N sind somit $\Gamma(N)-$Invariante Modulfunktionen auf $\mathbb{H}$, die auch im 'Unendlichen' meromorph sind. Wir merken an, dass diese Funktionen unter der Abbildung $\tau \to \tau + N$ invariant und daher periodisch sind.

Wir werden uns mit den arithmetischen Modulfunktionen beschäftigen, das heißt Modulfunktionen, deren Fourierkoeffizienten im Kreisteilungskörper $\mathbb{Q}(\zeta_N)$ liegen . Im Falle $N = 1$ ist der Funktionenkörper von $X(1)$ bekanntlich $\mathcal{F}_1 = \mathbb{Q}(j)$, da die Modulkurve $X(1)$ über $\mathbb{Q}$ definiert ist. Für $N > 1$

müssen wir aber neben der geometrischen Operation der Kongruenzuntergruppe $\Gamma(N)$ auf den Funktionenkörper $\mathcal{F}_N$ der arithmetischen Modulfunktionen der Stufe N auch die Operation der Galoisgruppe $(\mathbb{Z}/N\mathbb{Z})^*$ des $N-$ten Kreisteilungskörpers $\mathbb{Q}(\zeta_N)$ betrachten, da die Fourierkoeffizienten der Modulfunktionen von $\mathcal{F}_N$ in $\mathbb{Q}(\zeta_N)$ liegen.

Mittels der Operation der Galoisgruppe $G(\mathbb{Q}(\zeta_N, j)/\mathbb{Q}(j))$ und des Basiswechsels von $\mathbb{Q}(\zeta_N)$ nach $\mathbb{C}$ erhalten wir die Galoisgruppe $G(\mathcal{F}_N/\mathcal{F}_1)$ als semidirektes Produkt

$$\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \rtimes (\mathbb{Z}/N\mathbb{Z})^* \cong \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}. \tag{4.1}$$

Wir merken an, dass die Gruppe $(\mathbb{Z}/N\mathbb{Z})^*$ in $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ so eingebettet ist, dass wir die Untergruppe der Elemente der Form
$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ mit $d \in (\mathbb{Z}/N\mathbb{Z})^*$ betrachten.

Daher erhalten wir das folgende exakte Diagramm von Gruppen:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1(\zeta_N)) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \det} & & \downarrow & & \downarrow \\
1 & \longrightarrow & 1 & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathcal{F}_1(\zeta_N)/\mathcal{F}_1) & \longrightarrow & 1.
\end{array} \tag{4.2}$$

Nun können wir die Galoisgruppe aller arithmetischen Modulfunktionen $\mathcal{F} = \cup_{N\geq 1}\mathcal{F}_N$ über $\mathcal{F}_1$ durch den projektiven Limes wie folgt beschreiben:

$$\lim_{\leftarrow N}(\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}) = \mathrm{GL}(2,\widehat{\mathbb{Z}})/\{\pm 1_2\} \cong \mathrm{Gal}(\mathcal{F}/\mathbb{Q}(j)). \tag{4.3}$$

Wir erhalten somit die folgende exakte Sequenz

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{GL}(2,\widehat{\mathbb{Z}}) \longrightarrow \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1. \tag{4.4}$$

Reziprozitätsgesetz

Es sei k ein imaginär quadratischer Zahlkörper mit der Diskriminannte d. Ferner bezeichne $\mathcal{O}_t$ für ein $t \in \mathbb{N}$ die Ordnung mit dem Führer t in k, Cl_t die Idealklassengruppe von $\mathcal{O}_t$. Wir können diese Ordnung explizit wie folgt angeben:

$$\mathcal{O}_t = \left[t \cdot \frac{d + \sqrt{d}}{2}, 1 \right], \tag{4.5}$$

wobei für $\mathbb{Q}-$linear unabhängige Vektoren ω_1, ω_2 mit $[\omega_1, \omega_2] := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ das von diesen Vektoren erzeugte Gitter zu verstehen ist.

Nach dem Hauptsatz der komplexen Multiplikation für die Ordnungen der imaginär quadratischen Zahlkörper 2.12 folgt

$$k(j(\mathcal{I})) = \Omega_t \text{ für alle } \mathcal{I} \in \mathrm{Cl}_t.$$

Ω_t ist eine abelsche Körpererweiterung von k, welche zu der Untergruppe $\mathcal{U}_t$ der Idealgruppe von k gehört, die durch die Ideale der Form (λ), $\lambda \in \mathbb{Z}$, mit $\mathrm{ggT}(\lambda, t) = 1$ und $\lambda \equiv r \bmod t$ für ein geeignetes $r \in \mathbb{Z}$ erzeugt wird, [Sch02], S. 328.

Nun können wir den Hauptsatz der komplexen Multiplikation 2.12 mit dem folgenden Satz verallgemeinern, [Lang73], S. 128:

Satz 4.1. *Es seien k und $\mathcal{O}_t$ wie oben und $N \geq 1$. Dann ist der Strahlklassenkörper $H_{N,\mathcal{O}_t}$ bezüglich der Ordnung $\mathcal{O}_t$ des Führers N über Ω_t durch die Werte $g(\tau)$ der Funktionen $g \in \mathcal{F}_N$ erzeugt, welche keine Pole an τ besitzen. Ferner wird die maximal abelsche Erweiterung k^{ab} über k durch die endlichen Werte der Funktionen $f \in \mathcal{F}$ erzeugt.*

Es sei g nun eine arithmetische Modulfunktion der Stufe N und $\tau \in \mathcal{O}_t$. Nach 4.1 gilt $g(\tau) \in H_{N,\mathcal{O}_t}$. Falls alle Automorphismen der Gruppe $\mathrm{Gal}(k^{ab}/\Omega_t)$ auf $g(\tau)$ trivial operieren, dann liegt $g(\tau)$ bereits im Ringklassenkörper Ω_t. Somit ist $g(\tau)$ eine Klasseninvariante.

Die Galoisgruppe $\mathrm{Gal}(k^{ab}/\Omega_t)$ können wir mittels der Klassenkörpertheorie beschreiben.

Wir wählen $\tau \in k \cap \mathbb{H}$ mit dem Minimalpolynom $AX^2 + BX + C \in \mathbb{Z}[X]$ mit $A > 0$. Wir haben $\mathcal{O}_t = \mathbb{Z}[A\tau]$ mit der Diskriminante

$$D(\tau) = B^2 - 4AC = t^2 d.$$

Es seien k_a^* die Idelgruppe von k, k_∞^* der archimedische Teil von k_a^*, $k_{\infty+}^*$ die zusammenhängende Komponente des Einselements von k_∞^*. Dann liefert der Hauptsatz der Klassenkörpertheorie in der idelischen Sprache die folgende exakten Sequenz (wie wir im zweiten Kapitel 2.6 gesehen haben):

$$1 \longrightarrow \overline{k^* k_{\infty+}^*} \longrightarrow k_a^* \xrightarrow{Ar} \mathrm{Gal}(k^{ab}/k) \longrightarrow 1, \tag{4.6}$$

wobei Ar die Artinabbildung auf die Idelgruppe k_a^* von k bezeichnet. Weil die Einheitengruppe von k endlich ist, gilt zunächst $\overline{k^* k_{\infty+}^*} = k^* k_{\infty+}^*$. Ausserdem ist k insbesondere ein total komplexer Zahlkörper. Deswegen können wir die exakte Sequenz 4.6 mittels der endlichen Idelgruppe $\widehat{k^*} = (k \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^*$ von k beschreiben, da das Bild des unendlichen Teils unter der Artinabbildung trivial ist. Der Hauptsatz der Klassenkörpertheorie für die imaginär quadratischen Zahlkörper kann daher durch die folgende exakte Sequenz formuliert werden:

$$1 \longrightarrow k^* \longrightarrow \widehat{k^*} \xrightarrow{Ar} \mathrm{Gal}(k^{ab}/k) \longrightarrow 1. \tag{4.7}$$

Innerhalb des endlichen Rings der Adele $\widehat{k} = \prod_p'(K \otimes_{\mathbb{Q}} \mathbb{Q}_p)$ haben wir die proendliche Vervollständigung $\widehat{\mathcal{O}_t} = \mathcal{O}_t \otimes_Z \widehat{\mathbb{Z}} = \lim_{\leftarrow N}(\mathcal{O}_k/N\mathcal{O}_k) = \widehat{\mathbb{Z}} + \widehat{\mathbb{Z}} \cdot A\tau$ der Ordnung $\mathcal{O}_t$ von k, wobei mit $\prod'$ das eingeschränkte Produkt bezeichnet wird, siehe [CaFr67], S. 62. Die Untergruppe $\widehat{\mathcal{O}_t}^* = \prod_p(\mathcal{O}_t \otimes_{\mathbb{Z}} \mathbb{Z}_p)^*$ von $\widehat{k}^*$ ist nach dem Satz 2.11 (und nach der Diskussion nach diesem Satz im zweiten Kapitel) das Urbild unter der Artinabblidung Ar, siehe auch [Sh71], S. 123.

Wir schreiben (einfachheitshalber) $\mathcal{O}_t = \mathcal{O}$.

Wir müssen überprüfen, ob die Operation von $\widehat{\mathcal{O}}^*$ auf den singulären Wert $g(\tau)$ einer Modulfunktion g trivial ist, um zu entscheiden, ob $g(\tau)$ eine Klasseninvariante ist. Diese können wir mit Hilfe des Shimuraschen Reziprozitätsgesetzes testen, welches besagt, dass das Bild von $g(\tau)$ unter $x \in \widehat{\mathcal{O}}^*$ durch den Wert an τ einer zu g über $\mathbb{Q}(j)$ konjugierten Modulfunktion bestimmt ist. Genauer gesagt existiert eine Abbidung h_τ, welche die exakte Sequenz 4.4 mit der exakten Sequenz 4.7 der Klassenkörpertheorie wie folgt verbindet:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & \widehat{\mathcal{O}}^* & \longrightarrow & \mathrm{Gal}(k^{ab}/\Omega_t) & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle h_\tau} & & & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}(2,\widehat{\mathbb{Z}}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) & \longrightarrow & 1 \end{array} \tag{4.8}$$

Wir können nun das Reziprozitätsgesetz von Shimura durch den folgenden Satz formulieren, siehe [Sh71], S. 157, theorem 6.31 und S. 160, proposition 6.33:

Satz 4.2. *Die Voraussetzungen seien wie oben. Es gilt*

$$g(\tau)^{[x^{-1}:k]} = g(\tau)^{h_\tau(x)}(\tau). \tag{4.9}$$

Ferner sei $G \subseteq GL(2,\widehat{\mathbb{Z}})$ eine offene Untergruppe mit dem Fixkörper $F \subseteq \mathcal{F}$. Bezüglich der Artinabbildung wird die Untergruppe von $\prod_p \mathcal{O}_p^*$, die trivial auf

$k(F(\tau))$ operiert, von $\mathcal{O}^*$ erzeugt. Ferner gilt:

$$h_\tau^{-1}(G) = \{x \in \prod_p \mathcal{O}_p^* : h_\tau(x) \in G\}.$$

Wir können die Abbildung h_τ wie folgt explizit angeben: $h_\tau(x) \in \mathrm{GL}(2, \widehat{\mathbb{Z}})$ ist die Transponierte der Matrix, welche die Multiplikation mit $x \in \widehat{\mathcal{O}_k^*}$ auf den freien $\widehat{\mathbb{Z}}-$Modul $\widehat{\mathcal{O}} = \widehat{\mathbb{Z}} + \widehat{\mathbb{Z}}A\tau$ bezüglich der Basis $\{\tau, 1\}$ beschreibt. Falls $AX^2 + BX + C$ das Minimalpolynom von τ über $\mathbb{Z}$ ist, dann haben wir

$$h_\tau : x = s\tau + t \mapsto \begin{pmatrix} t - Bs & -Cs \\ sA & t \end{pmatrix}. \tag{4.10}$$

Da $g \in \mathcal{F}_N$ ist, ist der Wert $g(\tau) \in H_{N,\mathcal{O}}$. Die Operation von $\widehat{\mathcal{O}}^*$ kann durch den endlichen Quotient $(\mathcal{O}/N\mathcal{O})^*$ beschrieben werden. Das ist die Verallgemeinerung von [GeSt98], S. 448 für beliebige Ordnungen. Wir können damit 4.8 auf die folgende exakte Sequenz der endlichen Gruppen reduzieren:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & (\mathcal{O}/N\mathcal{O})^* & \longrightarrow & \mathrm{Gal}(H_{N,\mathcal{O}}/\Omega_t) & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle h_{\tau,N}} & & & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) & \longrightarrow & 1 \end{array} \tag{4.11}$$

Dieses gilt wegen der Eigenschaft, dass k^{ab} die Vereinigung aller endlichen Erweiterungen $H_{N,\mathcal{O}}$ über Ω_t nach dem Satz 4.9 ist, welche den endlichen Quotienten $\widehat{\mathcal{O}}^* \twoheadrightarrow (\widehat{\mathcal{O}}/N\widehat{\mathcal{O}})^* = (\mathcal{O}/N\mathcal{O})^*$ von $\widehat{\mathcal{O}}^*$, $N \in \mathbb{Z}^{\geq 1}$ entsprechen, siehe auch [Stev01], S. 167.

Falls nun alle Bilder von $(\mathcal{O}/N\mathcal{O})^*$ unter $h_{\tau,N}$ auf der Modulfunktion g trivial operieren, liegt $g(\tau)$ bereits in Ω_t und ist daher eine Klasseninvariante.

Nun können wir mittels des folgenden Verfahrens überprüfen, ob $g(\tau)$ eine Klasseninvariante ist, dessen Beweis unmittelbar aus unseren Vorüberlegungen folgt:

Algorithmus 4: Konstruktion der Klasseninvariante

Eingabe: Eine Modulfunktion g der Stufe N und $\tau \in \mathcal{O}_t \cap \mathbb{H}$

Ausgabe: $g(\tau)$ liefert eine Klasseninvariante oder nicht

1. Berechne die Erzeuger $x_1, \cdots, x_k$ von $(\mathcal{O}/N\mathcal{O})^*$

2. Bilde mittels $h_{\tau,N}$ die Erzeuger in $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ ab
3. Für $i = 1$ bis k überprüfe, ob $h_{\tau,N}(x_i) \in \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ auf $g(\tau)$ trivial operiert
4. Falls es ein j mit einer $h_{\tau,N}(x_j)$ gibt, welche auf $g(\tau)$ nicht trivial operiert, gebe '$g(\tau)$ ist keine Klasseninvariante' aus. Sonst gebe '$g(\tau)$ ist eine Klasseninvariante' aus.

Nach [GeSt98], S. 448, und [Stev01], S. 169, 170, gilt nun der folgende Satz:

Satz 4.3. *Es sei $g(\tau)$ eine Klasseninvariante für eine Ordnung eines imaginär quadratischen Zahlkörpers k der Diskriminante D. Dann ist $g(\tau)$ Klasseninvariante für alle imaginär quadratischen Zahlkörper, deren Diskriminante modulo $4N$ zu D kongruent sind.*

Bemerkung 4.4. *Der Satz 4.3 besagt, dass wir für eine Familie von imaginär quadratischen Zahlkörpern $\mathcal{K}$ eine Klasseninvariante $g(\tau)$ haben, falls sie für einen Körper $k \in \mathcal{K}$ eine Klasseninvariante ist.*

Minimalpolynome, $N-$Systeme

Das Reziprozitätsgesetz von Shimura ermöglicht auch, die Konjugierten einer Klasseninvariante zu bestimmen, welche Schertz mittels der $N-$Systeme beschrieben hat, auf die wir nun eingehen.

Definition 4.5. *Eine imaginär quadratische Zahl $\tau \in \mathbb{H} \cap k$ ist die Nullstelle einer quadratischen Gleichung $Ax^2 + Bx + C = 0$, welche durch τ eindeutig bestimmt ist, falls wir folgende Normalisierung annehmen:*

$$A, B, C \in \mathbb{Z}, \mathrm{ggT}(A, B, C) = 1, A > 0.$$

*Wir nennen diese Gleichung **primitiv**.*

Definition 4.6. *Es seien $N \in \mathbb{N}$ und $\tau_1, \tau_2, \cdots, \tau_{h_t} \in \mathbb{H}$, so dass*

$$[\tau_1, 1], [\tau_2, 1], \cdots, [\tau_{h_t}, 1]$$

ein volles Repräsentantensystem der Idealklassen von Cl_t ist. Ferner seien $A_i x^2 + B_i x + C_i = 0$ die primitiven Gleichungen für τ_i, welche der folgenden Eigenschaft genügen:

$$\mathrm{ggT}(A_i, N) = 1 \text{ und } B_i \equiv B_j \mod 2N, 1 \leq i, j \leq h_t.$$

*Wir nennen dann die Elemente $\tau_1, \tau_2, \cdots, \tau_{h_t}$ ein **N-System modulo** t.*

Nach [Sch02], S. 335, proposition 3, existiert für jede natürliche Zahl N ein $N-$System. Für die gegebene Klasseninvariante $g(\tau)$ liefert das $N-$System die Werte τ_i so, dass $g(\tau_i)$ die konjugierten Elemente von $g(\tau)$ sind.

Die Klasseninvarianten von Weber

Wir können nun mit dem Algorithmus 4 und der $N-$Systeme die klassischen Weberschen Klasseninvarianten angeben, welche die ersten expliziten Klasseninvarianten der Ordnungen imaginär quadratischer Zahlkörper liefern, deren Diskriminante durch 4 teilbar sind.

Die Dedekindsche $\eta-$Funktion wird durch

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{k=1}^{\infty}(1-q^k), q = \exp(2\pi i\tau) \text{ mit } \Im(\tau) > 0. \tag{4.12}$$

definiert. Die Schläflischen Funktionen $\mathfrak{f}, \mathfrak{f}_1$ und $\mathfrak{f}_2$ von Weber können nun als die folgenden Quotienten der Dedekindschen $\eta-$Funktion definiert werden:

$$\mathfrak{f}(\tau) = \exp(-\frac{\pi i}{24})\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)}, \mathfrak{f}_1(\tau) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)}, \mathfrak{f}_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}. \tag{4.13}$$

Diese Funktionen erfüllen die folgenden Gleichungen, siehe [Wb1908], S. 114:

Satz 4.7. *Es gelten die folgenden Gleichungen für jedes Element $\tau \in \mathbb{H}$:*

1. $\mathfrak{f}(\tau)^8 = \mathfrak{f}_1(\tau)^8 + \mathfrak{f}_2(\tau)^8$,
2. $\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$.

Die Funktionen γ_2 und γ_3 definieren wir nun mittels der $j-$Invariante wie folgt:

$$\gamma_2 = \sqrt[3]{j(\tau)}, \gamma_3 = \sqrt{j(\tau) - 12^3}. \tag{4.14}$$

Nach [Sch02], S. 327, haben wir nun das folgende Lemma

Lemma 4.8. *Die Schläflischen Funktionen von Weber erfüllen die folgenden Identitäten:*

$$\gamma_2 = \frac{\mathfrak{f}^{24} - 16}{\mathfrak{f}^8} = \frac{\mathfrak{f}_1^{24} + 16}{\mathfrak{f}_1^8} = \frac{\mathfrak{f}_2^{24} + 16}{\mathfrak{f}_2^8}. \tag{4.15}$$

g sei eine der Funktionen $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2, \gamma_2, \gamma_3$. Dann gilt nach dem Lemma 4.8 stets $\mathbb{Q}(j(\tau)) \subseteq \mathbb{Q}(g(\tau))$.

Offenbar sind die singulären Werte der 72ten Potenzen dieser Funktionen Klasseninvarianten. Die Koeffizienten der Minimalpolynome dieser Klasseninvarianten sind aber wegen 4.15 nicht wesentlich kleiner. Allerdings untersuchte Weber die kleineren Potenzen dieser Modulfunktionen, welche Klasseninvarianten liefern. Schertz hat in [Sch02] mit Hilfe des Shimuraschen Reziprozitätsgesetzes den folgenden Satz bewiesen, welcher es ermöglicht, die Ringklassenkörper mit Polynomen mit 'kleineren' Koeffizienten zu erzeugen. Dieser Satz umfasst alle Ergebnissen von Weber, siehe [Sch02], S. 329:

Satz 4.9. *$\tau \in \mathbb{H}$ sei die Nullstelle einer primitiven Gleichung*

$$Ax^2 + Bx + C = 0 \text{ mit } \mathrm{ggT}(A, 2) = 1, B \equiv 0 \bmod 32$$

mit der Diskriminante $D(\tau) = B^2 - 4AC = -4m = t^2 d$. Dann sind die folgenden algebraischen Zahlen $g(\tau)$ Klasseninvarianten:

1. $\left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} \mathfrak{f}(\tau)^2\right)^3$, *falls* $m \equiv 1 \bmod 8$,
2. $\mathfrak{f}(\tau)^3$, *falls* $m \equiv 3 \bmod 8$,
3. $\left(\frac{1}{2}\mathfrak{f}(\tau)^4\right)^3$, *falls* $m \equiv 5 \bmod 8$,
4. $\left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} \mathfrak{f}(\tau)\right)^3$, *falls* $m \equiv 7 \bmod 8$,
5. $\left(\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} \mathfrak{f}_1(\tau)^2\right)^3$, *falls* $m \equiv 2 \bmod 4$,
6. $\left(\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} \mathfrak{f}_1(\tau)^4\right)^3$, *falls* $m \equiv 4 \bmod 8$,

wobei der Faktor $\left(\frac{2}{A}\right)$ das Legendre Symbol bezeichnet.

Falls $\tau = \tau_1, \cdots, \tau_{h_t}$ ein $16-$System modulo t ist, dann sind die oben beschriebenen singulären Werte $g(\tau_i)$ ein komplettes System der Konjugierten über $\mathbb{Q}$. Daher ist das Minimalpolynom über $\mathbb{Q}$ durch

$$W_{D(\tau)} = \prod_i (x - g(\tau_i))$$

gegeben. Ferner besitzt dieses Polynom ganzzahlige Koeffizienten.

Beispiel: Wir betrachten die Diskriminante -204, wie im dritten Kapitel. Da $-204 = -4 \cdot 51$ und $51 \equiv 3 \bmod 8$ ist, ist $f(\tau)^3$ nach dem Satz 4.9 eine Klasseninvariante. Mittels eines $16-$Systems erhalten wir die Konjugierten von $\mathfrak{f}(\tau)^3$. Daher haben wir das Minimalpolynom:

$$W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64.$$

welches im Gegensatz zu dem Hilbertklassenpolynom

$H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 +$
$9586484163799611206755507 2 \cdot x^4 + 7751217562312410416108497305 60 \cdot x^3 +$
$5344849307032098969604469298728140 80 \cdot x^2 +$
$6020337293681148983229932704488367325184 \cdot x +$
$2850804137703453816686245017215309345665 8432.$

wesentlich kleinere Koeffizienten besitzt.

Bemerkung 4.10. *Im Falle, dass* 3 *die Diskriminannte* $D(\tau)$ *nicht teilt, liefern die Funktionen im Satz 4.9 ohne die* $3-$*ten Potenzen die Klasseninvarianten, siehe [Sch02], S. 330, theorem 2.*

4.2 Klassenivarianten mittels der Thetanullwerte

Im ersten Kapitel haben wir die Riemannschen Thetafunktionen und Thetanullwerte für beliebiges Geschlecht betrachtet. Nun betrachten wir die Thetanullwerte für $g = 1$, $\tau \in \mathbb{H}$ und $q = \exp(2\pi i\tau)$, die wir im ersten Kapitel eingeführt haben:

Definition 4.11. *Es gelten für* $\tau \in \mathbb{H}$

1. $\theta_{00}(\tau) := \theta[0,0](0,\tau) = \sum_{n\in\mathbb{Z}} q^{n^2/2}$,
2. $\theta_{10}(\tau) := \theta[1,0](0,\tau) = \sum_{n\in\mathbb{Z}} q^{(n+\frac{1}{2})^2/2}$,
3. $\theta_{01}(\tau) := \theta[0,1](0,\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2/2}$,
4. $\theta_{11}(\tau) := \theta[1,1](0,\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{(n+\frac{1}{2})^2/2}$.

Wir merken an, dass die Funktionen $\theta_{00}, \theta_{10}, \theta_{01}$ die geraden Thetanullwerte sind und die Funktion θ_{11} der einzige ungerade Thetanullwert ist.

Die Frage, mit der wir uns beschäftigen, ist zwischen den Schläflischen Funktionen von Weber (4.13) und den Thetanullwerten (4.11) Identitäten zu bestimmen. Dabei stützen wir uns auf den folgenden Satz, siehe [Wb1908], S. 112 und 114:

Satz 4.12. *Es bezeichne* θ'_{11} *die Ableitung der Funktion* θ_{11}*. Dann gelten die folgenden Gleichungen für* $\tau \in \mathbb{H}$ *:*

1. $\theta'_{11}(\tau) = 2\pi\eta(\tau)^3$,
2. $\theta_{00}(\tau) = \eta(\tau)\mathfrak{f}(\tau)^2$,
3. $\theta_{01}(\tau) = \eta(\tau)\mathfrak{f}_1(\tau)^2$,
4. $\theta_{10}(\tau) = \eta(\tau)\mathfrak{f}_2(\tau)^2$.

Ferner gilt für die Schläflischen Funktionen von Weber (4.13) der folgende Satz:

Satz 4.13. *Es gelten für* $\tau \in \mathbb{H}$

1. $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$,

2. $\mathfrak{f}(\tau)\mathfrak{f}_2(\frac{\tau+1}{2}) = \exp(\frac{\pi i}{24})\sqrt{2}$.

Beweis: Als erstes folgt aus $\mathfrak{f}_1(2\tau) = \frac{\eta(\tau)}{\eta(2\tau)}$ stets $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$, denn es gilt $\mathfrak{f}_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}$.

Für die zweite Aussage haben wir zunächst aus [Sch02], S. 335, proposition 2, die Transformationsformel $\eta(\tau+1) = \exp(\frac{\pi i}{12})\eta(\tau)$, welche bedeutet, dass wir stets

$$\mathfrak{f}_1(\tau+1) = \frac{\eta(\frac{\tau+1}{2})}{\eta(\tau+1)} = \exp(\frac{-\pi i}{12})\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)} = \exp(\frac{-\pi i}{24})\mathfrak{f}(\tau) \tag{4.16}$$

haben. Nun folgt aus dem ersten Teil

$$\mathfrak{f}(\tau)\mathfrak{f}_2(\frac{\tau+1}{2}) = \sqrt{2}\frac{\mathfrak{f}(\tau)}{\mathfrak{f}_1(\tau+1)} = \sqrt{2}\exp(\frac{\pi i}{24}).\square$$

Wir führen nun die folgenden Quotienten der geraden Thetanullwerte ein, die wir **modifizierte Schläflische Funktionen** nennen:

Definition 4.14. *Für $\tau \in \mathbb{H}$ definieren wir die modifizierten Schläflischen Funktionen wie folgt:*

1. $\mathfrak{F}(\tau) = e^{\frac{\pi i}{8}}\sqrt{2}\frac{\theta_{00}(\tau)}{\theta_{10}(\frac{\tau+1}{2})}$,
2. $\mathfrak{F}_1(\tau) = \frac{2\theta_{01}(\tau)}{\theta_{10}(\tau/2)}$,
3. $\mathfrak{F}_2(\tau) = \frac{\sqrt{2}\theta_{10}(\tau)}{\theta_{01}(2\tau)}$.

Satz 4.15. *Es gelten für $\tau \in \mathbb{H}$ die folgenden Gleichungen:*

1. $\mathfrak{F}(\tau) = \mathfrak{f}(\tau)^3$,
2. $\mathfrak{F}_1(\tau) = \mathfrak{f}_1(\tau)^3$,
3. $\mathfrak{F}_2(\tau) = \mathfrak{f}_2(\tau)^3$.

Beweis: Wir multiplizieren die drei Funktionen θ_{00}, θ_{01} und θ_{10} und erhalten nach dem Satz 4.7,(2), und dem Satz 4.12 :

$$\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau) = \eta(\tau)^3(\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau))^2 = (\sqrt{2})^2\eta(\tau)^3 = 2\eta(\tau)^3.$$

Damit gilt

$$\eta(\tau)^3 = \frac{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}{2}.$$

Nun ist die dritte Potenz von $\theta_{00}(\tau)$ nach dem Satz 4.12, (2), $\theta_{00}(\tau)^3 = \eta(\tau)^3 \mathfrak{f}(\tau)^6$.

Dann gilt

$$\mathfrak{f}(\tau)^6 = \frac{\theta_{00}(\tau)^3}{\eta(\tau)^3} = \frac{2\theta_{00}(\tau)^3}{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)} = \frac{2\theta_{00}(\tau)^2}{\theta_{01}(\tau)\theta_{10}(\tau)}.$$

Analog haben wir mit dem Satz 4.12, (3) und (4),

$$\mathfrak{f}_1(\tau)^6 = \frac{2\theta_{01}(\tau)^2}{\theta_{00}(\tau)\theta_{10}(\tau)}, \text{ bzw. } \mathfrak{f}_2(\tau)^6 = \frac{2\theta_{10}(\tau)^2}{\theta_{00}(\tau)\theta_{01}(\tau)}.$$

Andererseits folgt aus der Definition 4.11 von $\theta_{00}(\tau)$ und $\theta_{01}(\tau)$ zusammen mit der Identität $2(n^2+m^2) = (n+m)^2 + (n-m)^2$ die sogenannte Duplikationsformel, siehe auch [RaFa74], S. 63:

$$\theta_{10}(\tau)^2 = 2\theta_{00}(2\tau)\theta_{10}(2\tau). \tag{4.17}$$

Daher gilt

$$\mathfrak{f}_1(\tau)^6 = \frac{2\theta_{01}(\tau)^2}{\theta_{00}(\tau)\theta_{10}(\tau)} = \frac{4\theta_{01}(\tau)^2}{\theta_{10}(\tau/2)^2} = \left(\frac{2\theta_{01}(\tau)}{\theta_{10}(\tau/2)}\right)^2 = \mathfrak{F}_1^2.$$

Nun folgt aus dem Vergleich des Vorzeichens mittels der jeweiligen $q-$Entwicklungen $\mathfrak{F}_1(\tau) = \mathfrak{f}_1(\tau)^3$.

Nach dem Satz 4.13, (1), haben wir für die dritte Potenz von $\mathfrak{f}_2$

$$\mathfrak{f}_2(\tau)^3 = \frac{2\sqrt{2}}{\mathfrak{f}_1(2\tau)^3} = \frac{2\sqrt{2}\theta_{10}(\tau)}{2\theta_{01}(2\tau)} = \mathfrak{F}_2(\tau).$$

Abschließend betrachten wir analog die dritte Potenz von $\mathfrak{f}(\tau)$. Nach 4.13, (2), gilt daher

$$\mathfrak{f}(\tau)^3 = \frac{e^{\frac{\pi i}{8}} 2\sqrt{2}}{\mathfrak{f}_2(\frac{\tau+1}{2})^3} = \frac{e^{\frac{\pi i}{8}} 2\sqrt{2}\theta_{01}(\tau+1)}{\sqrt{2}\theta_{10}(\frac{\tau+1}{2})} = \mathfrak{F}(\tau).\square$$

Wir können nach dem Satz 4.15 und dem Satz 4.9 die Klasseninvarianten von Weber stets als Quotienten der Thetanullwerte durch den folgenden Satz angeben, dessen Beweis auch unmittelbar aus 4.15 und 4.9 folgt:

Satz 4.16. *$\tau \in \mathbb{H}$ sei die Nullstelle einer primitiven Gleichung*

$$Ax^2 + Bx + C = 0 \text{ mit } \mathrm{ggT}(A, 2) = 1, B \equiv 0 \bmod 32$$

mit der Diskriminante $D(\tau) = B^2 - 4AC = -4m = t^2 d$. Dann sind folgende Zahlen $g(\tau)$ Klasseninvarianten:

1. $\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} \mathfrak{F}(\tau)^2$, *falls* $m \equiv 1 \bmod 8$,
2. $\mathfrak{F}(\tau)$, *falls* $m \equiv 3 \bmod 8$,
3. $\frac{1}{8} \mathfrak{F}(\tau)^4$, *falls* $m \equiv 5 \bmod 8$,
4. $\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} \mathfrak{F}(\tau)$, *falls* $m \equiv 7 \bmod 8$,
5. $\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} \mathfrak{F}_1(\tau)^2$, *falls* $m \equiv 2 \bmod 4$,
6. $\left(\frac{2}{A}\right) \frac{1}{16\sqrt{2}} \mathfrak{F}_1(\tau)^4$, *falls* $m \equiv 4 \bmod 8$,

wobei der Faktor $\left(\frac{2}{A}\right)$ *das Legendre Symbol bezeichnet.*

Falls $\tau = \tau_1, \cdots, \tau_{h_t}$ *ein* $16-$*System modulo* t *ist, dann sind die oben beschriebenen singulären Werte* $g(\tau_i)$ *ein komplettes System der Konjugierten über* $\mathbb{Q}$*. Daher ist das Minimalpolynom über* $\mathbb{Q}$ *durch das Polynom*

$$W_{D(\tau)} = \prod_i (x - g(\tau_i))$$

gegeben. Ferner besitzt dieses Polynom ganzzahlige Koeffizienten.

4.2.1 Laufzeitaussagen

Mittels der naiven Methode der Berechnung der $N-$signifikanten Bits der Thetanullwerte erhält man ein Verfahren, welches die Bit-Komplexität in $O(\mathcal{M}(N)\sqrt{N})$ hat, siehe [Dup07], S. 5, wobei $\mathcal{M}(N)$ die Komplexität der Multiplikation zweier $N-$Bit Zahlen bezeichnet.

Mittels der Relationen der Thetanullwerte und der Newton-Iteration hat Dupont ein Verfahren entwickelt, welches die $N-$signifikanten Bits der Thetanullwerte in $O(\mathcal{M}(N) \log N)$ berechnet, siehe [Dup07], S. 14. Dieses Verfahren ist somit die zur Zeit asymptotisch schnellste Methode der Berechnung der $N-$signifikanten Bits von den Thetanullwerten.

Diese Methode ermöglicht, die numerischen Werte der $j-$ Invariante und der Dedekindschen $\eta-$Funktion zu bestimmen. Wir definieren dazu die folgenden Funktionen:

Definition 4.17. *Für* $\tau \in \mathbb{H}$ *definieren wir* κ *und* κ' *wie folgt:*

- $\kappa(\tau) = \left(\frac{\theta_{10}(\tau)}{\theta_{00}(\tau)}\right)^2$,
- $\kappa'(\tau) = \left(\frac{\theta_{01}(\tau)}{\theta_{00}(\tau)}\right)^2$.

Nach [BorBor87], S. 112 bis 116, haben wir den folgenden Satz, welcher ermöglicht, die $j-$Funktion rational in κ' darzustellen. Zusammen mit dem Verfahren von Dupont haben wir nun den folgenden Satz:

Satz 4.18. *Mittels der Identität*

$$j(\tau) = 256\frac{\left(1-\kappa'(\tau)^2+\kappa'(\tau)^4\right)}{\kappa'(\tau)^4(1-\kappa'(\tau)^2)}$$

können wir die $N-$signifikanten Bits von $j(\tau)$ in $O(\mathcal{M}(N)\sqrt{N})$ berechnen.

Analog haben wir die folgende Aussage für die Berechnung der $N-$signifikanten Bits von $\eta(\tau)^{12}$:

Satz 4.19. *Mittels der Identität*

$$\eta(\tau)^{12} = \frac{\kappa'(\tau)^2(1-\kappa'(\tau)^2)\theta_{00}(\tau)^{12}}{16}$$

können wir die $N-$signifikanten Bits von $\eta(\tau)^{12}$ in $O(\mathcal{M}(N)\log N)$ berechnen.

Beweis: Nach [Dup07], S. 19, gilt zunächst

$$\mathfrak{f}(\tau)^{24}\kappa'(\tau)^2(1-\kappa'(\tau)^2) = 16.$$

Nach dem Satz 4.12, 2, gilt nun $\mathfrak{f}(\tau)^{24}\eta(\tau)^{12} = \theta_{00}(\tau)^{12}$. Daher erhalten wir

$$\eta(\tau)^{12} = \frac{\kappa'(\tau)^2(1-\kappa'(\tau)^2)\theta_{00}(\tau)^{12}}{16}.\square$$

Bemerkung 4.20. *Um den Wert $\eta(\tau)^{12}$ numerisch zu berechnen, müssen wir nach dem Satz 4.19 sowohl $\theta_{00}(\tau)$ als auch $\theta_{01}(\tau)$ zuerst mittels des Verfahrens von Dupont mit hinreichender Präzision berechnen.*

Um die Klasseninvarianten in 4.9 berechnen zu können müssen wir zusätzlich die 12−ten Wurzeln aus $\eta(\tau)^{12}$ ziehen. Da die Klasseninvarianten die Quotienten von zwei Werten der Dedekindschen $\eta-$Funktion sind, müssen wir das 12−te Wurzelnziehen zweimal durchführen. Das kann man mittels der Newton-Iteration in $O(\mathcal{M}(N))$ berechnen, siehe [Dup07]. S. 10 bis 12. Insgesamt haben wir das folgende Korollar:

Korollar 4.21. *Um die $N-$signifikanten Bits von $\eta(\tau)$ und damit die $N-$signifikanten Bits einer Klasseninvariante in 4.9 zu berechnen, müssen wir zusätzlich $O(\mathcal{M}(N))-$Bit Operationen durchführen.*

Wenn wir im Gegensatz zu dem Satz 4.9 die Klasseninvarianten als die Quotienten der Thetanullwerte im Satz 4.16 benutzen, erhalten wir den folgenden Satz, dessen Beweis aus unseren Vorüberlegungen und dem Verfahren von Dupont folgt:

Satz 4.22. *Wir sparen $O(\mathcal{M}(N))-$Bit Operationen, wenn wir die Klasseninvariante im Satz 4.16 statt den Satz 4.9 benutzen.*

Bemerkung 4.23. *Mit dem Satz 4.22 haben wir die zur Zeit effizienteste Berechnung der Klasseninvarianten in der Darstellung aus dem Satz 4.16.*

Wir werden im Abschnitt 5 auf die Darstellungen der anderen Klasseninvarianten mittels der Thetanullwerte eingehen. Die Methode liefert auch in diesen Fällen die bisher schnellste Methode bei der Berechnung solcher Klasseninvarianten.

4.3 Einheiteneigenschaft der Klasseninvarianten

Beispiel: Wir hatten im ersten Abschnitt mit Hilfe der Klasseninvariante $\mathfrak{F}(\tau)$ das Weberklassenpolynom

$$W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64.$$

der Diskriminante -204 berechnet. Falls wir die Koeffizienten und Nullstellen α_i, $1 \leq i \leq 6$, dieses Polynoms näher untersuchen, dann sehen wir schnell, dass das Polynom

$$\widetilde{W}_{-204}(x) = x^6 - 8 \cdot x^5 - 3 \cdot x^4 + 6 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x + 1$$

stets die Nullstellen $\frac{\alpha_i}{2}$ besitzt, welche Einheiten sind. In diesem Fall können wir $\mathfrak{F}(\tau)/2$ als eine Klasseninvariante benutzen und daher das Klassenpolynom $\widetilde{W}_{-204}$ erhalten. Wir werden in diesem Abschnitt sehen, dass das obige Beispiel kein Zufall ist. Wir erhalten somit in einigen Fällen des Satzes 4.16 bessere Klasseninvarianten.

Ein Satz von Deuring

Es bezeichne $\mathcal{P}_s$ die Menge aller $2 \times 2-$Matrizen der Determinante s mit den folgenden Eigenschaften:

$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ mit $\det(M) = s$ und $\mathrm{ggT}(a, b, c, d) = 1$. Diese Matrizen heißen primitive Matrizen.

Nach [Sch10], S. 63 und S. 64, theorem 2.2.2., theorem 2.2.4, ist die Untergruppe

$$\Gamma_M = \Gamma \cap M^{-1}\Gamma M$$

eine Kongruenzuntergruppe modulo s. Ferner haben wir auf $\mathcal{P}_s$ die Äquivalenzrelation

$$M \sim M' :\Longleftrightarrow \Gamma M = \Gamma M',$$

mit der $\mathcal{P}_s$ in eine endliche Anzahl von $\psi(s)$ Äquivalenzklassen zerfällt, wobei $\psi(s)$ die Anzahl der positiven Teiler von s bezeichnet. Das Vertretersystem ist gegeben durch die Dreiecksmatrizen

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, a > 0, ad = s, \mathrm{ggT}(a, b, d) = 1,$$

wobei b aus einem vollen Restsystem modulo d etwa $0 \leq b < d$ ist.

Mittels der Eisensteinschen Reihen g_2, g_3, schreiben wir die Diskriminantenfunktion für $\tau \in \mathbb{H}$ und die absolute Invariante j an τ wie folgt, siehe [Deu58], S. 3:

$$\Delta(\tau) := g_2(\tau)^3 - 27g_3(\tau)^2, j(\tau) := 2^6 3^3 g_2(\tau)^3 \Delta(\tau)^{-1}. \tag{4.18}$$

Aus der Theorie der elliptischen Modulfunktionen folgt, siehe [Deu58], S. 3, die Identität

$$\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}. \tag{4.19}$$

zwischen $\Delta(\tau)$ und $\eta(\tau)$. Für die $\Delta-$Funktion haben wir die folgende Aussage:

Lemma 4.24. *Es sei $\{\omega_1, \omega_2\}$ eine $\mathbb{Z}-$Basis eines Gitters $L \subset \mathbb{C}$ mit $\tau = \frac{\omega_1}{\omega_2}$. Dann gilt*

$$\Delta \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \omega_2^{-12}\Delta(\tau). \tag{4.20}$$

Beweis: Es gelten nach [Lang73], S. 17,

$$g_2(\tau) = \omega_2^{-4} g_2(\omega_1, \omega_2) \text{ und } g_3(\tau) = \omega_2^{-6} g_3(\omega_1, \omega_2).$$

Aus der Definition (4.18) folgt unmittelbar die Behauptung.□

Wir definieren für eine primitive Matrix M der Determinante s den folgenden Quotient der $\Delta-$Funktion

$$\varphi_M(\tau) := s^{12} \frac{\Delta\left(M\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right)}{\Delta\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}}. \tag{4.21}$$

Jede primitive Matrix M kann in der Form

$$M = P_1 P_2 \cdots P_m$$

dargestellt werden, wobei $\det(P_i) = p_i$ stets eine Primzahl ist, siehe [Deu58], S. 43. Es gilt ferner, auch nach [Deu58], S. 43:

$$\varphi_{AB}(\tau) = \varphi_A(B(\tau))\varphi_B(\tau).$$

Deuring hat die Bestimmung des Divisors eines singulären Wertes $\varphi_M(\tau)$ daher mittels der Divisoren der $\varphi_{P_i}(\tau)$ durch den folgenden Satz explizit angegeben, welcher von dem Zerfällungsverhalten der Primzahlen p_i in k abhängt, siehe [Deu58], S. 43:

Satz 4.25. *Es seien $t > 0$ eine ganze Zahl, p eine Primzahl und $l \geq 0$ der maximale Exponent von p mit $p^l | t$. Ferner seien a, b, c und d ganze Zahlen, so dass die Matrix $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ die Determinante p hat. Es sei $\{\omega_1, \omega_2\}$ eine Basis eines gebrochenen $\mathcal{O}_t$-Ideals I mit $\tau := \frac{\omega_1}{\omega_2} \in \mathbb{H}$.*

1. *Falls p in k zerlegt mit $p = \mathfrak{p}\overline{\mathfrak{p}}$ ist, dann gelten die folgenden Aussagen:*
   (a) *$\varphi_P(\tau)$ ist eine Einheit, falls $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ eine Basis eines gebrochenen $\mathcal{O}_{tp}$-Ideals ist,*
   (b) *$\frac{\varphi_P(\tau)}{p^{12}}$ ist eine Einheit, falls $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ eine Basis eines gebrochenen $\mathcal{O}_{tp^{-1}}$-Ideals ist,*
   (c) *Im Falle $l = 0$, ist $\frac{\varphi_P(\tau)}{p^{12}}$ eine Einheit, falls $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ eine Basis eines gebrochenen Ideals $I_{\mathcal{O}_t}\mathfrak{p}_{\mathcal{O}_t}$ oder $I_{\mathcal{O}_t}\overline{\mathfrak{p}}_{\mathcal{O}_t}$ ist.*
2. *Falls p in k verzweigt mit $p = \mathfrak{p}^2$ ist, dann gelten die folgenden Aussagen:*
   (a) *$\frac{\varphi_P(\tau)}{p^{\frac{6}{l+1}}}$ ist eine Einheit, falls $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ eine Basis eines gebrochenen $\mathcal{O}_{tp}$-Ideals ist,*

(b) $\frac{\varphi_P(\tau)}{p^{12-\frac{6}{p^l}}}$ *ist eine Einheit, falls* $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ *eine Basis eines gebrochenen* $\mathcal{O}_{tp^{-1}}$*-Ideals ist,*

(c) $\frac{\varphi_P(\tau)}{p^6}$ *ist eine Einheit, falls* $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ *eine Basis des Ideals* $I_{\mathcal{O}_t}\mathfrak{p}_{\mathcal{O}_t}$ *ist.*

3. *Falls* p *in* k *träge ist, dann gelten die folgenden Aussagen:*

(a) $\frac{\varphi_P(\tau)}{p^{12/p^l(p+1)}}$ *ist eine Einheit, falls* $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ *eine Basis eines gebrochenen* $\mathcal{O}_{tp}$*-Ideals ist,*

(b) $\frac{\varphi_P(\tau)}{p^{12\left[1-\frac{1}{p^{l-1}(p+1)}\right]}}$ *ist eine Einheit, falls* $P\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ *eine Basis eines gebrochenen* $\mathcal{O}_{tp^{-1}}$*-Ideals ist.*

Wir haben nun den folgenden Satz:

Satz 4.26. *Es sei* $g(\tau)$ *eine der Klasseninvarianten aus dem Satz 4.9 oder 4.16. Dann ist* $g(\tau)$ *eine Einheit, falls* $m \equiv 1, 5, 7 \bmod 8$ *oder* $m \equiv 2 \bmod 4$ *gelten, wobei* $D(\tau) = -4m$ *ist.*

Beweis: Es sei $\tau \in \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'}) =: k$ mit $D(\tau) = -4m = t^2 d = t'^2 d'$, wobei d' quadratfrei ist. Dann haben wir nach [Coh93], S. 218, 219

$$t' = \begin{cases} t & \text{falls } d' \equiv 1 \bmod 4, \text{ d. h. } d' = d, \text{ ist} \\ 2t & \text{falls } d \equiv 0 \bmod 4, \text{ i. e. } d' \equiv 2, 3 \bmod 4 \text{ ist.} \end{cases} \tag{4.22}$$

Für die Fälle $m \equiv 1, 5 \bmod 8$ haben wir zunächst $m \equiv 1 \bmod 4$. Es gilt $t' \equiv 0 \bmod 2$, weil sonst d' keine quadratfreie Zahl wäre.

Wir setzen $t' = 2s$, woraus stets $s^2 d' \equiv -1 \bmod 4$ folgt und daher $\mathrm{ggT}(s, 2) = 1$ ist. Daraus folgt $s^2 \equiv 1 \bmod 4$ und $d' \equiv -1 \bmod 4$.

Insgesamt haben wir für $m \equiv 1 \bmod 4$ die Maximalordnung $\mathcal{O}_k = \mathbb{Z}[\sqrt{d'}]$ und $(2) = \mathfrak{p}^2$, da 2 in $\mathcal{O}_k$ verzweigt ist. Mittels der Betrachtung der Basis $\{\tau, 1\}$ von $\mathcal{O}_t$ zusammen mit der Matrix $P = \begin{pmatrix}1 & s\\ 0 & 2\end{pmatrix}$ haben wir $P\begin{pmatrix}\tau\\ 1\end{pmatrix} = [\tau + s, 2]$ als eine Basis des Ideals $\mathfrak{p}\mathcal{O}_t$.

Nach dem Satz 4.25, (2(c)), haben wir die Eigenschaft, dass $\frac{\varphi_P(\tau)}{2^6}$ eine Einheit ist, die wegen der Identität 4.19 gleichbedeutend damit ist, dass

$$2^{-6}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)}$$

eine Einheit ist, da s eine ungerade Zahl ist. Nun machen wir eine Fallunterscheidung

- Im Falle $m \equiv 1 \bmod 8$, erhalten wir damit die Gleihung

$$2^{-6}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)} = g(\tau)^4 = \left(\left(\left(\frac{2}{A}\right)\frac{\mathfrak{f}(\tau)^2}{\sqrt{2}}\right)^3\right)^4.$$

  Diese impliziert, dass $g(\tau)$ eine Einheit ist.

- Im Falle $m \equiv 5 \bmod 8$, erhalten wir die Gleichung

$$2^{-6}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)} = g(\tau)^2 = \left(\left(\frac{\mathfrak{f}(\tau)^4}{2}\right)^3\right)^2,$$

  woraus folgt, dass $g(\tau)$ eine Einheit ist.

Für $m \equiv 7 \bmod 8$, haben wir auch $t' \equiv 0 \mod 2$. Wir setzen $t' = 2s$ wie oben, und erhalten $s^2 d' = -m$ mit $\mathrm{ggT}(s,2) = 1$. Es gelten daher $s^2 \equiv 1 \bmod 8$ und somit $-d' \equiv 3 \mod 4$. Aus diesen Kongruenzen folgt, dass

$\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{d'}}{2}]$ und $(2) = \mathfrak{p}\overline{\mathfrak{p}}$ gelten, da 2 in $\mathcal{O}_k$ zerfällt.

Mittels der Betrachtung der Basis $\{\tau+s, 1\}$ eines $\mathcal{O}_{2t}-$Ideals zusammen mit der Matrix $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ erhalten wir $P\begin{pmatrix} \tau+s \\ 1 \end{pmatrix} = [\tau+s, 2]$ als eine Basis eines $\mathcal{O}_t$-Ideals.

Nach dem Satz 4.25, (1(b)) und der Identität 4.19 ist

$$\frac{\varphi_P(\tau+s)}{2^{12}} = g(\tau)^8 = \left(\left(\left(\frac{2}{A}\right)\frac{\mathfrak{f}(\tau)}{\sqrt{2}}\right)^3\right)^8$$

eine Einheit. Somit ist auch $g(\tau)$ eine Einheit in diesem Fall.

Im Falle $m \equiv 2 \mod 4$ haben wir $t^2 d' \equiv 2 \mod 4$ mit einer ungeraden t, welche bedeutet, dass $d' \equiv 2 \mod 4$ gilt, und daher $\mathcal{O}_k = \mathbb{Z}[\sqrt{d}]$ und $(2) = \mathfrak{p}^2$.

Für die Basis $\{\tau, 1\}$ von $\mathcal{O}_t$ mit der Matrix $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ haben wir $P\begin{pmatrix} \tau \\ 1 \end{pmatrix} = [\tau, 2]$ als eine Basis von $\mathfrak{p}\mathcal{O}_t$. Nach dem Satz 4.25, (2(c)) und der Identität 4.19, erhalten wir die Einheit $\frac{\varphi_P(\tau)}{2^6}$. Daher gilt

$$2^{-6}\frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)} = g(\tau)^4 = \left(\left(\left(\frac{2}{A}\right)\frac{\mathfrak{f}_1(\tau)^2}{\sqrt{2}}\right)^3\right)^4.$$

Somit ist $g(\tau)$ eine Einheit. $\square$

Bemerkung 4.27. *1. Nach Satz 4.26 und 4.9 liegen diese Einheiten zusammen in den entsprechenden Ringklassenkörpern.*

2. Für die Fälle $m \equiv 3 \bmod 8$ und $m \equiv 12 \bmod 16$ werden wir beweisen, dass die Invarianten keine Einheiten in den Ringklassenkörpern sind. Aber wir werden mit Hilfe des Satzes 4.25 zeigen, dass es Einheiten gibt, welche eine Beziehung zu den Klasseninvarianten haben. Wir werden also damit beweisen, dass die konstanten Koeffizienten der Minimalpolynome der Klasseninvarianten Potenzen von 2 sind, und für diese Koeffizienten 2^l stets $l|h_t$ gilt, wobei h_t die Klassenzahl der Ringklassengruppe modulo t ist.

Ferner werden wir zeigen, dass für $m \equiv 4 \bmod 16$ die Klasseninvarianten auch Einheiten sind.

Die Klasseninvarianten, die Einheiten sind, nennen wir nun **Klasseneinheiten**.

4.3.1 Neue Klasseneinheiten

Satz 4.28. *Es sei $g(\tau)$ eine der Klasseninvarianten aus dem Satz 4.9 oder 4.16.*

1. *Für $m \equiv 3 \bmod 8$ gelten die folgenden Aussagen:*
   (a) *$\tilde{g}(\tau) := g(\tau)/2$ ist eine Klasseninvariante und eine Einheit, falls $m \equiv 3 \bmod 24$ ist,*
   (b) *$g(\tau)$ hat die Norm 2^l mit $h_t = 3l$, falls $m \equiv 11, 19 \bmod 24$ ist.*
2. *Für $m \equiv 4 \bmod 8$ gelten die folgenden Aussagen:*
   (a) *$g(\tau)$ ist eine Einheit, falls $m \equiv 4 \bmod 16$ ist,*
   (b) *Für $m \equiv 12 \bmod 16$, schreiben wir $m = 16a + 12$. Dann gelten die folgenden Aussagen:*
      - *$g(\tau)$ hat die Norm 2^l mit $h_t = 2l$, falls $a \equiv 0, 1, 5 \bmod 6$ ist,*
      - *$g(\tau)$ hat die Norm 2^l mit $h_t = 6l$, falls $a \equiv 2, 4 \bmod 6$ ist,*
      - *$\tilde{g}(\tau) := g(\tau)/2$ ist eine Klasseninvariante mit der Norm 2^l mit $h_t = 2l$, falls $a \equiv 3 \bmod 6$ ist.*

Beweis: Wie im Beweis des Satzes 4.26, setzen wir zunächst $-4m = t'^2 d'$. Falls $m \equiv 3 \bmod 8$ gilt, dann haben wir $-m = s^2 d'$ für eine ungerade s. Wir erhalten daher, dass $d' \equiv 5 \bmod 8$ mit $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{d'}}{2}]$ gilt.

Wir merken an, dass 2 in $\mathcal{O}_k$ träge ist. Ferner gilt $t \equiv 2 \bmod 4$ wegen $d = d'$ und $-4m = t^2 d$, da sonst $m \not\equiv 3 \bmod 8$ wäre. Mittels der Basis $\{\tau + s, 1\}$

eines $\mathcal{O}_{2t}$-Ideals und der Matrix $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, erhalten wir $P \begin{pmatrix} \tau+s \\ 1 \end{pmatrix} = [\tau+s, 2]$ als eine Basis eines $\mathcal{O}_t$-Ideals. Nach dem Satz 4.25, 3(b), und der Identität 4.19 ist

$$2^{-8}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)}$$

eine Einheit, weil $t \equiv 2 \bmod 4$ stets $l = 1$ impliziert und wir $12\left(1-(1/2^{1-1}3)\right) = 8$ haben.

Insgesamt gilt

$$2^{-8}\frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)} = \left(\frac{\mathfrak{f}(\tau)^3}{2}\right)^8 = (\frac{g(\tau)}{2})^8.$$

Für $m \equiv 11, 19 \bmod 24$ ist die Funktion $\mathfrak{f}(\tau)$ nach der Bemerkung 4.10 selbst eine Klasseninvariante, denn es gilt $\gcd(3, D(\tau)) = 1$. Wir erhalten daher, dass $g(\tau)$ die Norm $\pm 2^{8h_t/24}$ hat, und daher $l = h_t/3$ ist.

Im Falle $m \equiv 3 \bmod 24$ gilt $3|D(\tau)$, daher $l = h_t$ für die Klasseninvariante $\mathfrak{f}(\tau)^3$. Dies impliziert, dass $\tilde{g}(\tau) = \mathfrak{f}(\tau)^3/2$ eine Klasseninvariante und eine Einheit ist.

Für den Fall $m \equiv 4 \bmod 8$, schreiben wir $m = 8a+4$. Es gilt damit $-4(8a+4) = t'^2 d'$ und daher $t' = t = 4s$. Wir erhalten nun $-2k-1 = s^2 d'$. Dies bedeutet

$$d' \equiv \begin{cases} 3 \bmod 4 & \text{falls } m \equiv 4 \bmod 16, \\ 1 \bmod 4 & \text{falls } m \equiv 12 \bmod 16. \end{cases} \tag{4.23}$$

Wir betrachten zunächst den Fall $m \equiv 4 \bmod 16$.

Wir haben die Eigenschaften, dass $\mathcal{O}_k = \mathbb{Z}[\sqrt{d'}]$ gilt, und 2 in $\mathcal{O}_k$ verzweigt ist. Ferner gilt $-4m = t^2 d = t^2(4d')$ und daher $-m = t^2 d' \equiv 4 \mod 16$ und somit $t \equiv 2 \mod 4$. Dies bedeutet, dass $l = 1$ ist.

Mit der Basis $\{\tau, 1\}$ eines $\mathcal{O}_{2t}$-Ideals zusammen mit $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ haben wir $P \begin{pmatrix} \tau \\ 1 \end{pmatrix} = [\tau, 2]$ als eine Basis eines $\mathcal{O}_t-$Ideals.

Nun nach dem Satz 4.25, (2(b)), und 4.19 erhalten wir

$$2^{-9}\frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)} = \left(\left(\left(\frac{2}{A}\right)\frac{\mathfrak{f}_1(\tau)^4}{2\sqrt{2}}\right)^3\right)^2 = g(\tau)^2,$$

weil $2^{12-\frac{6}{2}} = 2^9$ gilt. Daher ist $g(\tau)$ eine Einheit im Falle $m \equiv 4 \bmod 16$.

Für den letzten Fall $m \equiv 12 \bmod 16$ mit $d = d' \equiv 1 \mod 4$ haben wir $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{d'}}{2}]$. Wir müssen die folgenden zwei Fälle betrachten:

$$d \equiv \begin{cases} 1 \bmod 8, \text{ d. h. 2 ist zerfällt,} & \text{falls } a \equiv 1,3,5 \bmod 6 \\ 5 \bmod 8, \text{ d. h. 2 ist träge,} & \text{falls } a \equiv 0,2,4 \bmod 6. \end{cases} \tag{4.24}$$

Außerdem gilt $s^2 d \equiv 2a \mod 3$. Dies bedeutet, dass für $a \equiv 1,2,4,5 \bmod 6$ stets $\mathrm{ggT}(3,d) = 1$ gilt. Wegen der Bemerkung 4.10 betrachten wir in diesem Fall die Klasseninvarianten ohne die 3−ten Potenzen.

- Falls $a \equiv 0 \mod 6$ ist, dann ist 2 träge in $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{d'}}{2}]$.

  Mittels der Basis $\{\tau, 1\}$ eines $\mathcal{O}_{2t}$-Ideals und der Matrix $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ haben wir $P \begin{pmatrix} \tau \\ 1 \end{pmatrix} = [\tau, 2]$ als eine Basis eines $\mathcal{O}_t-$Ideals.

  Nach dem Satz 4.25 (3(b)) erhalten wir die Einheit

  $$2^{-10} \frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)} = \frac{\mathfrak{f}_1(\tau)^{24}}{2^{10}} = \frac{g(\tau)^2}{2},$$

  da $t = 2$ und somit $12(1 - \frac{1}{2^{2-1}3}) = 10$ gelten. Somit ist $h_t = 2l$.

- Falls $a \equiv 2,4 \mod 6$ gilt, haben wir die Einheit

  $$2^{-10} \frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)} = \frac{\mathfrak{f}_1(\tau)^{24}}{2^{10}} = \frac{g(\tau)^6}{2}.$$

  In diesem Fall haben wir $g(\tau) = \left(\left(\frac{2}{A}\right) \frac{1}{2\sqrt{2}} \mathfrak{f}_1(\tau)^4 \right)$. Es gilt daher $h_t = 6l$ wegen

  $$\prod_{i=1}^{h_t} \frac{g(\tau_i)^6}{2} = \pm 1.$$

- Falls $a \equiv 1,5 \bmod 6$ ist, dann ist 2 zerfällt in $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{d'}}{2}]$.

  Es seien $\{\tau, 1\}$ die Basis eins $\mathcal{O}_{2t}-$Ideals und $P = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Dann ist $P \begin{pmatrix} \tau \\ 1 \end{pmatrix} = [\tau, 2]$ eine Basis eines $\mathcal{O}_t-$Ideals.

  Nach dem Satz 4.25 (1(b)) ist

  $$2^{-12} \frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)} = \frac{\mathfrak{f}_1(\tau)^{24}}{2^{12}} = \frac{g(\tau)^6}{2^3},$$

eine Einheit. Damit erhalten wir analog

$$\prod_{i=1}^{h_t} \frac{g(\tau_i)^6}{2^3} = \pm 1,$$

welche impliziert, dass wir stets $h_t = 2l$ haben.

- Falls $a \equiv 3 \bmod 6$ ist, erhalten wir die neue Klasseninvariante

$$\tilde{g}(\tau) = \frac{g(\tau)}{2} = \left(\left(\frac{2}{A} \right) \frac{1}{4\sqrt{2}} \mathfrak{f}_1(\tau)^4 \right)^3$$

und die Einheit

$$2^{-12} \frac{\Delta(\frac{\tau}{2})}{\Delta(\tau)} = \frac{\mathfrak{f}_1(\tau)^{24}}{2^{12}} = \frac{\tilde{g}(\tau)^2}{2^{12}}$$

welche bedeutet, dass

$$\prod_{i=1}^{h_t} \frac{\tilde{g}(\tau_i)^2}{2^{12}} = \pm 1$$

gilt, und daher wir $h_t = 2l$ haben. □

Beispiel: Für die Diskriminante $D = -204 = -4 \cdot 51$ haben wir $51 \equiv 3 \bmod 24$.

Es gilt nach dem Satz 4.28, (1(a)) und dem Satz 4.16, dass $\mathfrak{F}(\tau)/2$ eine Klasseninvariante ist. Daher erhalten wir das Minimalpolynom

$$\widetilde{W}_{-204}(x) = x^6 - 8 \cdot x^5 - 3 \cdot x^4 + 6 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x + 1,$$

welches wir mittels der Betrachtung der Koeffizienten von $W_{-204}(x)$ am Anfang dieses Abschnitts festgestellt hatten.

Wir haben nun nach dem Satz 4.28 das folgende Korollar für die Klassenzahl h_t der Ringklassengruppe Cl_t:

Korollar 4.29. *Es gelten die folgenden Teilbarkeitsaussagen für die Klassenzahl h_t der Ringklassengruppe Cl_t modulo t:*

1. $3|h_t$, *falls für die Diskriminante* $D = -4m$ *die Kongruenzbedingung* $m \equiv 3 \bmod 8$ *gilt,*
2. $2|h_t$, *falls für die Diskriminante* $D = -4m$ *die Kongruenzbedingung* $m \equiv 4 \bmod 16$ *gilt,*
3. $6|h_t$, *falls für die Diskriminante* $D = -4m$ *die Kongruenzbedingung* $m \equiv 4 \bmod 16$ *und für a mit* $m = 16a+12$ *die Bedingung* $a \equiv 2, 4 \bmod 6$ *gilt.*

4.4 Berechnung der Einheitengruppe

Da die Klasseninvarianten nach dem Satz 4.26 und 4.28, (2(a)) für $m \equiv 1, 5, 7 \bmod 8$, $m \equiv 2 \bmod 4$ und $m \equiv 4 \bmod 16$ Klasseneinheiten sind, stellt sich die Frage, ob wir die Einheitengruppe der entsprechenden Ringklassenkörper mit diesen Einheiten und ihren Konjugierten berechnen können.

In diesem Abschnitt betrachten wir dazu die Nullstellen der Klassenpolynome dieser Klasseneinheiten und die Untergruppe der Einheitengruppe, welche von diesen Nullstellen und Einheitswurzeln erzeugt wird. Wir führen mittels einer Methode der Vergrößerung dieser Gruppe ein Verfahren ein, wodurch sich die gesammte Einheitengruppe berechnen läßt, falls die Nullstellen eines Klassenpolynoms eine Untergruppe vom endlichen Index der Einheitengruppe des entsprechenden Ringklassenkörpers bilden.

L sei ein Ringklassenkörper vom Grad n über k, welcher von einer Klasseneinheit erzeugt ist. Ferner seien h_L die Klassenzahl und E_L die Einheitengruppe von L.

Nach dem Dirichletschen Einheitensatz, siehe [PhZs89], S. 334, ist die Einheitengruppe E_L das direkte Produkt der Untergruppe der Torsionseinheiten $\mathcal{W}_L$ und der $r = n - 1$ Grundeinheiten, da L unter anderem eine total komplexe Erweiterung von k ist.

Es seien $\epsilon_1, \cdots, \epsilon_{n-1} \in E_L$ unabhängige Einheiten. Die Matrix

$$\mathcal{R}(\varepsilon_1, \cdots, \varepsilon_{n-1}) = \mathcal{R}_\varepsilon,$$

deren ijten Eintrag $\log |\varepsilon_i^{(j)}|^2$ ist, heißt die **Regulatormatrix**.

Nach [PhZs89], S. 360, ist der Betrag der Determinante von $\mathcal{R}(\varepsilon_1, \cdots, \varepsilon_{n-1})$ positiv.

Umgekehrt folgt daraus, falls die Regulatormatrix $\mathcal{R}(\varepsilon_1, \cdots, \varepsilon_{n-1})$ nicht singulär ist, dass $\epsilon_1, \cdots, \epsilon_{n-1} \in E_L$ unabhängige Einheiten sind.

Die unabhängigen Einheiten $\epsilon_1, \cdots, \epsilon_{n-1} \in E_L$ bilden zusammen mit der Untergruppe der Torsionseinheiten $\mathcal{W}_L$ eine Untergruppe

$$\mathcal{E}_L = \mathcal{W}_L \times < \varepsilon_1 > \times \cdots \times < \varepsilon_{n-1} > .$$

in E_L von endlichem Index.

Es gilt die folgende Identität für den Index dieser Untergruppe in E_L:

$$(E_L : \mathcal{E}_L) = \frac{|\det(\mathcal{R}_\varepsilon|}{R_E}, \tag{4.25}$$

wobei wir mit R_E den Regulator von L bezeichnen, siehe [Wa82], lemma 4.15.

Falls man eine untere Schranke für den Regulator $|R_E|$ des Körpers L hat, erhält man damit wegen der Gleichung 4.25 eine obere Schranke B für den Index $(E_L : \mathcal{E}_L)$.

Das von Pohst und Fieker ([FiPohst08]) eingeführte Verfahren liefert eine verbesserte untere Schranke für $|R_E|$, und daher auch eine obere Schranke für $(E_L : \mathcal{E}_L)$.

Wir benutzen dazu die Computeralgebra Systeme KANT/KASH ([Pohst]) und MAGMA ([MAGMA]). In beiden Systemen haben wir die Funktion `RegulatorLowerBound`, mit der wir eine untere Regulatorabschätzung für $|R_E|$ bestimmen können.

Wir haben nun den folgenden Satz für die Grundeinheiten von L, siehe [LePoUz09], S. 14 und 15:

Satz 4.30. *Es seien $\epsilon_1, \cdots, \epsilon_{n-1} \in E_L$ unabhängige Einheiten. Dann existieren die Grundeinheiten $u_1, \cdots, u_r$ of E_L so dass*

$$\begin{aligned} \varepsilon_1 &= \zeta_1 u_1^{b_{11}} \\ \varepsilon_2 &= \zeta_2 u_1^{b_{21}} u_2^{b_{22}} \\ &\vdots \\ \varepsilon_r &= \zeta_t u_1^{b_{r1}} \cdots u_r^{b_{rr}}, \end{aligned}$$

mit $b_{ij} \in \mathbb{Z}, b_{ii} > 0, \zeta_i \in \mathcal{W}_L$. Ferner, haben wir

$$(E_K : \mathcal{E}_K) = b_{11} \cdots b_{rr}.$$

Es sei nun $W(x)$ das Klassenpolynom einer Klasseneinheit, welche über k den Körper L erzeugt.

Wir wählen $n-1$ Nullstellen $\epsilon_1, \cdots, \epsilon_{n-1}$ dieses Polynoms $W(x)$, so dass $\det(\mathcal{R}(\varepsilon_1, \cdots, \varepsilon_{n-1})) = \det(\mathcal{R}_\varepsilon)$ nicht Null und minimal ist, falls wir solche Nullstellen von $W(x)$ haben. Da wir die n Nullstellen von $W(x)$ explizit wegen der Konstruktion des Klassenpolynoms $W(x)$ numerisch berechnet haben, ist es nicht schwer die $n-1$ Nullstellen mit der Eigenschaft zu wählen, dass $\det(\mathcal{R}_\varepsilon)$ minimal ist.

Wir haben die folgenden drei Lemmata, welche uns ermöglichen zu testen, ob eine Einheit eine $p-$Potenz ist, wobei p eine Primzahl ist, siehe [Haj88], lemma 5.2.1, 5.2.2 und 5.2.3 :

Lemma 4.31. *$M = \mathbb{Q}(\alpha)$ sei ein algebraischer Zahlkörper vom Grad $n > 1$, wobei $\alpha^{(1)}, \cdots, \alpha^{(n)}$ die Konjugierten von α sind. Ferner sei $f_\alpha(x) = \prod_{j=1}^{n}(x - \alpha^{(j)})$ das Minimalpolynom von α.*

Für jede positive ganze Zahl m gilt $\alpha \in {M^*}^m$ genau dann, wenn $f_\alpha(x^m)$ einen irreduziblen Faktor in $\mathbb{Z}[x]$ hat, dessen Grad ein positiver Teiler von n ist.

Lemma 4.32. *Es bezeichne E_{L^+} die Gruppe der Einheiten in $L^+ = L \cap \mathbb{R}$. Es seien p eine Primzahl und $\varepsilon \in E_{L^+}$. Genau dann gilt $\varepsilon \in E_L^p$, wenn $\varepsilon \in E_{L^+}^p$ oder $\varepsilon/d \in E_{L^+}^p$ ist, wobei d die Diskriminante des imaginär quadratischen Zahlkörpers k ist.*

Lemma 4.33. *Es sei $\mathbb{Q}(\varepsilon)$ einer der Konjugierten des maximal reellen Teilkörpers von L für eine Einheit $\varepsilon \in E_L$ und $-d \in \mathbb{P}$, wobei d die Diskriminante des imaginär quadratischen Zahlkörpers k ist. Ferner sei $f_\varepsilon(x)$ das Minimalpolynom von ε.*

Genau dann gilt für jede Primzahl p stets $\varepsilon \in E_L^p$, wenn $f_\varepsilon(x^p)$ einen irreduziblen Faktor in $\mathbb{Z}[x]$ hat, dessen Grad ein positiver Teiler von n ist.

Algorithmus

Überprüfung der $p-$ten Potenzen:

Wir listen zunächst die Primzahlen $p \leq B$, wobei B die obere Schranke für den Index der Untergruppe $\mathcal{E}_L$ von E_L ist.

Durch die folgenden Schritte finden wir den $p-$Teil von $(E_L : \mathcal{E}_L)$:

Schritt 1: Teste ob $\varepsilon_1 \in \mathcal{W}_L E_L^p$ gilt.

Falls NEIN, setze $\theta_1 = \varepsilon_1$.

Falls JA, teste ob $\varepsilon_1' \in \mathcal{W}_L E_L^p$ gilt, wobei für $\varepsilon_1' \in E_L$ $\varepsilon_1'^p = \zeta\varepsilon_1$ für ein $\zeta \in \mathcal{W}_L$ gilt.

Wir folgen dem Schritt bis wir $\varepsilon_1 \in \mathcal{W}_L E_L^{p^{j_1}}$ mit $\varepsilon_1 \notin \mathcal{W}_L E_L^{p^{j_1+1}}$ haben.

Nun gilt für θ_1 stets $\theta_1^{p^{j_1}} = \zeta\varepsilon_1$ für ein $\zeta \in \mathcal{W}_L$.

Schritt 2: Wir nehmen an, dass wir θ_{m-1} gefunden haben.

Finde die größte ganze Zahl j_m, so dass ganze Zahlen $c_1, \ldots, c_{m-1}$ existieren, welche der Ungleichung $0 \leq c_i \leq p^{j_m - 1}$ genügen und und für die

$$\varepsilon_m^{-1}\theta_1^{c_1} \cdots \theta_{m-1}^{c_{m-1}} \in \mathcal{W}_L E_L^{p^{j_m}}$$

gilt.

Nun sei θ_m eine Einheit in E_L, für die $\theta_{m-1}^{p^{j_m}} = \zeta\varepsilon_m\theta_1^{-c_1} \cdots \theta_{m-1}^{-c_{m-1}}$ mit $\zeta \in \mathcal{W}_L$ gilt.

Wir merken an, dass wir in diesem Schritt die Anzahl der Schritte zur Überprüfung der $p-$ten Potenzen mittels des Verfahrens von Pohst und Zassenhaus, siehe [PhZs89], p. 371-372, von $p^{(m-1)(j_{m-1})}$ Schritten auf Maximum $(m-1)j_m$ Schritte reduzieren um das geeignete j_m zu bestimmen.

Schritt 3: Der p-Teil von $[E_L : \mathcal{E}_L]$ ist $p^{j_1+\cdots+j_t}$, und $< \mathcal{W}_L, \theta_1, \cdots, \theta_{n-1} >$ hat den Index $[E_L : \mathcal{E}_L]/(p^{j_1} \cdots p^{j_t})$.

Grundeinheiten: Wir können nun durch den folgenden Algorithmus die Einheitengruppe E_L berechnen:

Algorithmus 5: Berechnung der Einheitengruppe

Eingabe: Eine Ordnung $\mathcal{O}_t$ eines imaginär quadratischen Zahlkörpers k mit dem Führer t, $\tau \in \mathcal{O}_t$ und $D(\tau) = -4m$, wobei m die Kongruenzbedingungen nach dem Satz 4.26 oder 4.28, (1(a)), (2(a)) erfüllt und wir somit eine Klasseneinheit $g(\tau)$ haben.

Ausgabe: Die Erzeuger der Einheitengruppe E_{Ω_t} des Ringklassenkörpers Ω_t modulo t vom Grad h_t über k.

1. Berechne das Klassenpolynom $W(g(\tau))$ von $g(\tau)$
2. Bestimme eine untere Schranke l des Regulators von $\Omega_t = k(g(\tau))$.
3. Bestimme $h_t - 1$ Nullstellen $\epsilon_1, \cdots, \epsilon_{h_t-1}$ von $W(g(\tau))$, so dass die Determinante der Regulatormatrix den kleinsten von Null verschiedenen Betrag m hat.
4. Bestimme aus (3) eine obere Schranke $B = m/l$ für den Index der Untergruppe von E_{Ω_t}, welche von $\epsilon_1, \cdots \epsilon_{h_t-1}$ und den Einheitenwurzeln erzeugt sind.
5. Liste alle Primzahlen $p_i \leq B$, $i = 1, \cdots, n$ auf.
6. Für $i = 1$ bis n
   (a) Bestimme mittels der Überprüfung der $p-$ten Potenzen e_i von p_i, sowie die Einheiten $\gamma_1, \cdots, \gamma_{h_t-1}$, die zusammen mit den Einheitswurzeln eine Untergruppe vom Index $(E_{\Omega_t} : \mathcal{E}_{\Omega_t})/p_i^{e_i}$ bilden.
   (b) Setze $\gamma_1, \cdots, \gamma_{h_t-1} := \epsilon_1, \cdots, \epsilon_{h_t-1}$.
7. Gebe die Grundeinheiten $\gamma_1, \cdots, \gamma_{h_t-1}$ und die Untergruppe der Einheitswurzeln von Ω_t aus.

Beispiel: Wir betrachten noch einmal das Beispiel $m = 24 \cdot 3 + 3$. Das Klassenpolynom von $\mathfrak{F}(\tau)/2$ war

$$\widetilde{W}_{-204}(x) = x^6 - 8x^5 - 3x^4 + 6x^3 + 9x^2 + 2x + 1.$$

Es sei $L = K(\mathfrak{F}(\tau)/2)$. Mittels der Benutzung der Funktion `RegulatorLowerBound` von KANT/KASH erhalten wir 43.3706 als untere Schranke des Regulators von L.

Die Konjugierten $(\mathfrak{F}(\tau)/2)^{(i)}$, für $i = 1, \cdots, 5$ liefern die Determinante der Regulatormatrix $\det(\mathcal{R}) = 74.6592$.

Nach der Gleichung 4.25 haben wir damit die obere Schranke

$$B = 74.6592/43.3706 = 1.7214$$

für den Index der Untergruppe $\mathcal{E}_L$ von E_L, welche von $(\mathfrak{F}(\tau)/2)^{(i)}$ und den Einheitenwurzeln von L erzeugt ist.

Dies bedeutet aber, dass bereits $(\mathfrak{F}(\tau)/2)^{(i)}$ mit $\mathcal{W}_L$ die Einheitengruppe E_L erzeugen, da es keine Primzahl $p \leq B$ existiert.

4.5 Verallgemeinerte Klasseninvarianten mittels Thetanullwerte

Mittels der Verallgemeinerungen der in 4.13 definierten Funktionen $\mathfrak{f}, \mathfrak{f}_1$ und $\mathfrak{f}_2$ für $l \in \mathbb{Z}^{>2}$

$$\mathfrak{m}_l(\tau) = \sqrt{l}\frac{\eta(l\tau)}{\eta(\tau)}, \mathfrak{m}_j(\tau) = \zeta\frac{\eta(\frac{\tau+j}{l})}{\eta(\tau)}, 0 \leq j \leq l-1, \tag{4.26}$$

sind die **verallgemeinerten Schläflischen Funktionen** der Stufe l definiert, wobei ζ eine geeignete Einheitswurzel ist, siehe [Gee01], S. 73.

Die singulären Werte der kleineren Potenzen dieser Funktionen liefern wie im Satz 4.9 Klasseninvarianten, siehe [EngMor09].

Die Stufe $l = 3$: Für diesen Fall haben wir die Funktionen

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)}, \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)}, \mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)}, \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)}. \tag{4.27}$$

Für diese Funktionen haben wir nun den folgenden Satz:

Satz 4.34. *Es sei $\tau \in \mathbb{H}$. Dann gelten die folgenden Gleichungen:*

1. $\mathfrak{g}_0(\tau)\mathfrak{g}_1(\tau)\mathfrak{g}_2(\tau)\mathfrak{g}_3(\tau) = \sqrt{3}$,
2. $\prod_{i=0}^{3}(x - \mathfrak{g}_i(\tau)^{12}) = x^4 + 36x^3 + 270x^2 + (756 - j(\tau))x + 3^6$,
3. $\mathfrak{g}_0(3\tau)\mathfrak{g}_3(\tau) = \sqrt{3}$,

4. $\mathfrak{g}_3(\frac{\tau+1}{3})\mathfrak{g}_1(\tau) = \sqrt{3}$,

5. $\mathfrak{g}_3(\frac{\tau+2}{3})\mathfrak{g}_2(\tau) = \zeta_{12}\sqrt{3}$.

Beweis: Für die Beweise der ersten zwei Aussagen verweisen wir auf [Wb1908], S. 255. Nun folgt die dritte Aussage aus

$$\mathfrak{g}_0(3\tau)\mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(\tau)}{\eta(3\tau)}\frac{\eta(3\tau)}{\eta(\tau)} = \sqrt{3}.$$

Mittels der Transformation der Dedekindschen $\eta-$Funktion $\eta(\tau+1) = \zeta_{24}\eta(\tau)$, $\tau \in \mathbb{H}$, haben wir

$$\mathfrak{g}_3(\frac{\tau+1}{3})\mathfrak{g}_1(\tau) = \sqrt{3}\zeta_{24}^{-1}\frac{\eta(\tau+1)}{\eta(\frac{\tau+1}{3})}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)} = \sqrt{3}\zeta_{24}^{-1}\zeta_{24} = \sqrt{3}.$$

Analog erhalten wir die letzte Aussage. □

Der folgende Satz erweitert den Satz 4.9 für die kleineren Potenzen der Funktionen $\mathfrak{g}_i$, $0 \leq i \leq 2$, siehe [Gee01], S. 73:

Satz 4.35. *Es sei $\mathcal{O}_k = [\tau, 1]$ die Maximalordnung eines imaginär quadratischen Zahlkörpers k der Diskriminante D mit $Tr_{k/\mathbb{Q}}(\tau) \in \{-1, 0\}$.*

Dann liefern die singulären Werte der folgenden Funktionen an τ in der Tabelle Klasseninvarianten, deren Klassenpolynome ganzzahlige Koeffizienten besitzen:

	$D \equiv 1(9)$	$D \equiv 4(9)$	$D \equiv 7(9)$	$D \equiv 3(9)$	$D \equiv 6(9)$
$D \equiv 1(4)$	$\zeta_3\mathfrak{g}_0^2, \zeta_3^2\mathfrak{g}_1^2$	$\mathfrak{g}_0^2, \mathfrak{g}_1^2$	$\zeta_3^2\mathfrak{g}_0^2, \zeta_3\mathfrak{g}_1^2$	$\frac{1}{3\sqrt{-3}}\mathfrak{g}_2^6$	$\frac{1}{\sqrt{-3}}\mathfrak{g}_2^2$
$D \equiv 0(8)$	$\zeta_3^2\zeta_4\mathfrak{g}_1^2, \zeta_3\zeta_4\mathfrak{g}_2^2$	$\zeta_3\zeta_4\mathfrak{g}_1^2, \zeta_3^2\mathfrak{g}_2^2$	$\zeta_4\mathfrak{g}_1^2, \zeta_4\mathfrak{g}_2^2$	$\frac{1}{3\sqrt{3}}\mathfrak{g}_0^6$	$\frac{1}{\sqrt{3}}\mathfrak{g}_0^2$
$D \equiv 4(8)$	$\zeta_3\mathfrak{g}_1^4, \zeta_3^2\mathfrak{g}_2^4$	$\zeta_3^2\mathfrak{g}_1^4, \zeta_3\mathfrak{g}_2^4$	$\mathfrak{g}_1^4, \mathfrak{g}_2^4$	$\frac{1}{3^3}\mathfrak{g}_0^{12}$	$\frac{1}{3}\mathfrak{g}_0^4$

Die Stufe $l = 5$: In diesem Fall haben wir die Funktionen

$$\mathfrak{h}_0(\tau) = \frac{\eta(\frac{\tau}{5})}{\eta(\tau)}, \mathfrak{h}_1(\tau) = \zeta_8\frac{\eta(\frac{\tau+1}{5})}{\eta(\tau)}, \mathfrak{h}_2(\tau) = \zeta_{12}\frac{\eta(\frac{\tau+2}{5})}{\eta(\tau)}, \tag{4.28}$$

$$\mathfrak{h}_3(\tau) = \zeta_{24}\frac{\eta(\frac{\tau+3}{5})}{\eta(\tau)}, \mathfrak{h}_4(\tau) = \zeta_3^{-1}\frac{\eta(\frac{\tau+4}{5})}{\eta(\tau)}, \mathfrak{h}_5(\tau) = \sqrt{5}\frac{\eta(5\tau)}{\eta(\tau)}.$$

Für diese Funktionen haben wir nun die folgenden Identitäten:

Satz 4.36. *Es sei $\tau \in \mathbb{H}$. Dann gelten die folgenden Gleichungen:*

1. $\mathfrak{h}_0(\tau)\mathfrak{h}_1(\tau)\mathfrak{h}_2(\tau)\mathfrak{h}_3(\tau)\mathfrak{h}_4(\tau)\mathfrak{h}_5(\tau) = \sqrt{5}$,

2. $\mathfrak{h}_0(\tau)^6 + \mathfrak{h}_1(\tau)^6 + \mathfrak{h}_2(\tau)^6 + \mathfrak{h}_3(\tau)^6 + \mathfrak{h}_4(\tau)^6 + \mathfrak{h}_5(\tau)^6 = -30$,
3. $\mathfrak{h}_0(5\tau)\mathfrak{h}_5(\tau) = \sqrt{5}$,
4. $\mathfrak{h}_5(\frac{\tau+1}{5})\mathfrak{h}_1(\tau) = \zeta_6\sqrt{5}$,
5. $\mathfrak{h}_5(\frac{\tau+2}{5})\mathfrak{h}_2(\tau) = \zeta_8\sqrt{5}$,
6. $\mathfrak{h}_5(\frac{\tau+3}{5})\mathfrak{h}_3(\tau) = \zeta_{12}\sqrt{5}$,
7. $\mathfrak{h}_5(\frac{\tau+4}{5})\mathfrak{h}_4(\tau) = \zeta_3^{-1}\zeta_{24}\sqrt{5}$.

Beweis: Für die Beweise der ersten zwei Aussagen verweisen wir auf [Hr08], S. 439 und 440. Nun folgt die dritte Aussage aus

$$\mathfrak{h}_0(5\tau)\mathfrak{h}_5(\tau) = \sqrt{5}\frac{\eta(\tau)}{\eta(5\tau)}\frac{\eta(5\tau)}{\eta(\tau)} = \sqrt{5}.$$

Mittels der Transformation $\eta(\tau+1) = \zeta_{24}\eta(\tau)$ haben wir

$$\mathfrak{h}_5(\frac{\tau+1}{5})\mathfrak{h}_1(\tau) = \sqrt{5}\zeta_8\frac{\eta(\tau+1)}{\eta(\frac{\tau+1}{5})}\frac{\eta(\frac{\tau+1}{5})}{\eta(\tau)} = \sqrt{5}\zeta_8\zeta_{24} = \zeta_6\sqrt{5}.$$

Analog folgen die anderen Aussagen. □

Der folgende Satz erweitert den Satz 4.9 für die Funktion $\mathfrak{h}_5^2$, siehe [EngMor09], S. 17:

Satz 4.37. *Es sei $\mathcal{O}_t = [\tau, 1]$ die Ordnung eines imaginär quadratischen Zahlkörpers k der Diskriminante $D = t^2 d_k$, wobei d_k die Diskriminannte des Körpers k ist. Dann liefert $\mathfrak{h}_5^2(\tau)$ eine Klasseninvariante, falls $3 \nmid D$ ist.*

Im Gegensatz zu den anderen Klasseninvarianten, sind die Koeffizienten des Klassenpolynoms von $\mathfrak{h}_5^2$ im Satz 4.37 nicht ganzzahlig. Sie liegen in $\mathcal{O}_k$.

Bemerkung 4.38. *Wir verweisen auf [EngMor09] für die anderen verallgemeinerten Funktionen der Stufe l, deren Potenzen Klasseninvarianten liefern. Die hinreichende Bedingung dafür, dass die Klassenpolynome solcher Invarianten ganzzahlige Koeffizienten haben, wurde auch in [EngMor09] angegeben, theorem 10 und theorem 21 .*

Quotienten der Thetanullwerte

Wir haben gesehen, dass sich die Quotienten der Thetanullwerte schneller als die Quotienten der Dedekindschen $\eta-$Funktionen berechnen lassen. Wir wollen deshalb die verallgemeinerten Schläflischen Funktionen als Quotienten der Thetanullwerte darstellen.

Wir werden die Darstellungen der Schläflischen Funktionen der Stufe $l = 3$ und $l = 5$ als Quotienten der Thetanullwerte herleiten. Die Idee der Beweise dieser Darstellungen wird uns ermöglichen, auch die verallgemeinerten Schläflischen Funktionen beliebiger Stufe l als Quotienten gewisser Thetanullwerte darzustellen.

Die Stufe $l = 3$: Wir haben in diesem Fall den folgenden Satz:

Satz 4.39. *Es gelten die folgenden Identitäten für $\tau \in \mathbb{H}$:*

1. $\mathfrak{g}_0(\tau) = \frac{\theta_{10}(\tau/6)}{\theta_{10}(\tau/2)} \frac{\mathfrak{f}_1(\tau/3)}{\mathfrak{f}_1(\tau)}$, $\mathfrak{g}_0(\tau)^3 = \frac{\theta_{10}(\tau/6)^2}{\theta_{10}(\tau/2)^2} \frac{\theta_{01}(\tau/3)}{\theta_{01}(\tau)}$,
2. $\mathfrak{g}_1(\tau) = \zeta_{48} \frac{\theta_{10}(\frac{\tau+1}{6})\mathfrak{f}_1(\frac{\tau+1}{3})}{\theta_{10}(\frac{\tau+1}{2})\mathfrak{f}(\tau)}$, $\mathfrak{g}_1(\tau)^3 = \frac{\theta_{10}(\frac{\tau+1}{6})^2\theta_{01}(\frac{\tau+1}{3})}{\theta_{10}(\frac{\tau+1}{2})^2\theta_{00}(\tau)}$,
3. $\mathfrak{g}_2(\tau) = \frac{\theta_{10}(\frac{\tau+2}{6})\mathfrak{f}_1(\frac{\tau+2}{3})}{\theta_{10}(\frac{\tau}{2})\mathfrak{f}_1(\tau)}$, $\mathfrak{g}_2(\tau)^3 = \frac{\theta_{10}(\frac{\tau+2}{6})^2\theta_{01}(\frac{\tau+2}{3})}{\theta_{10}(\frac{\tau}{2})^2\theta_{01}(\tau)}$,
4. $\mathfrak{g}_3(\tau) = \sqrt{3}\frac{\theta_{10}(\frac{3\tau}{2})\mathfrak{f}_1(3\tau)}{\theta_{10}(\frac{\tau}{2})\mathfrak{f}_1(\tau)}$, $\mathfrak{g}_3(\tau)^3 = 3\sqrt{3}\frac{\theta_{10}(\frac{3\tau}{2})^2\theta_{01}(3\tau)}{\theta_{10}(\frac{\tau}{2})^2\theta_{01}(\tau)}$.

Beweis: Wir haben im Beweis des Satzes 4.15 gezeigt, dass die folgende Gleichung

$$\eta(\tau)^3 = \frac{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}{2}$$

gilt. Daraus folgt die Gleichung

$$\mathfrak{g}_0(\tau)^3 = \frac{\theta_{00}(\tau/3)\theta_{01}(\tau/3)\theta_{10}(\tau/3)}{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}.$$

Nach der Duplikationsformel 4.17 und der Transformationsformel 4.12, (3), erhalten wir

$$\mathfrak{g}_0(\tau)^3 = \frac{\theta_{10}(\tau/6)^2\theta_{01}(\tau/3)}{\theta_{10}(\tau/2)^2\theta_{01}(\tau)} = \frac{\eta(\tau/3)}{\eta(\tau)} \frac{\theta_{10}(\tau/6)^2\mathfrak{f}_1(\tau/3)^2}{\theta_{10}(\tau/2)^2\mathfrak{f}_1(\tau)^2} = \mathfrak{g}_0(\tau)\frac{\theta_{10}(\tau/6)^2\mathfrak{f}_1(\tau/3)^2}{\theta_{10}(\tau/2)^2\mathfrak{f}_1(\tau)^2}.$$

Es gilt daher mittels des Vergleichs des Vorzeichens beider Seiten

$$\mathfrak{g}_0(\tau) = \frac{\theta_{10}(\tau/6)\mathfrak{f}_1(\tau/3)}{\theta_{10}(\tau/2)\mathfrak{f}_1(\tau)}.$$

Wir haben somit wegen des Satzes 4.15, (2),

$$\mathfrak{g}_0(\tau)^3 = \frac{\theta_{10}(\tau/6)^3}{\theta_{10}(\tau/2)^3} \frac{\theta_{01}(\tau/3)}{\theta_{10}(\tau/6)} \frac{\theta_{10}(\tau/2)}{\theta_{01}(\tau)} = \frac{\theta_{10}(\tau/6)^2}{\theta_{10}(\tau/2)^2} \frac{\theta_{01}(\tau/3)}{\theta_{01}(\tau)}.$$

Aus dem Satz 4.34, (3), folgt nun

$$\mathfrak{g}_3(\tau) = \frac{\sqrt{3}}{\mathfrak{g}_0(3\tau)} = \sqrt{3}\frac{\theta_{10}(\frac{3\tau}{2})\mathfrak{f}_1(3\tau)}{\theta_{10}(\frac{\tau}{2})\mathfrak{f}_1(\tau)},$$

und

$$\mathfrak{g}_3(\tau)^3 = 3\sqrt{3}\frac{3\sqrt{3}}{\mathfrak{g}_0(3\tau)^3} = 3\sqrt{3}\frac{\theta_{10}(\frac{3\tau}{2})^2\theta_{01}(3\tau)}{\theta_{10}(\frac{\tau}{2})^2\theta_{01}(\tau)}.$$

Die Aussagen der Sätze 4.34, (4), und 4.16 implizieren die Gleichungen

$$\mathfrak{g}_1(\tau) = \frac{\sqrt{3}}{\mathfrak{g}_3(\frac{\tau+1}{3})} = \frac{\theta_{10}(\frac{\tau+1}{6})\mathfrak{f}_1(\frac{\tau+1}{3})}{\theta_{10}(\frac{\tau+1}{2})\mathfrak{f}_1(\tau+1)} = \zeta_{48}\frac{\theta_{10}(\frac{\tau+1}{6})\mathfrak{f}_1(\frac{\tau+1}{3})}{\theta_{10}(\frac{\tau+1}{2})\mathfrak{f}(\tau)},$$

und

$$\mathfrak{g}_1(\tau)^3 = \frac{3\sqrt{3}}{\mathfrak{g}_3(\frac{\tau+1}{3})^3} = \frac{\theta_{10}(\frac{\tau+1}{6})^2\theta_{01}(\frac{\tau+1}{3})}{\theta_{10}(\frac{\tau+1}{2})^2\theta_{01}(\tau+1)}.$$

Mittels der folgenden Transformationsformel der Thetanullwerte

$$\theta_{01}(\tau+1) = \theta_{00}(\tau), \theta_{00}(\tau+1) = \theta_{01}(\tau) \text{ und } \theta_{10}(\tau+1) = \zeta_8\theta_{10}(\tau) \quad (4.29)$$

erhalten wir den zweiten Teil der zweiten Aussage

$$\mathfrak{g}_1(\tau)^3 = \frac{\theta_{10}(\frac{\tau+1}{6})^2\theta_{01}(\frac{\tau+1}{3})}{\theta_{10}(\frac{\tau+1}{2})^2\theta_{00}(\tau)}.$$

Der Satz 4.34, (5), besagt

$$\mathfrak{g}_2(\tau) = \frac{\zeta_{12}\sqrt{3}}{\mathfrak{g}_3(\frac{\tau+2}{3})} = \zeta_{12}\frac{\theta_{10}(\frac{\tau+2}{6})\mathfrak{f}_1(\frac{\tau+2}{3})}{\theta_{10}(\frac{\tau+2}{2})\mathfrak{f}_1(\tau+2)}.$$

Aus der Transformationsformel 4.16 und den Transformationsformeln 4.29 erhalten wir die Gleichungen

$$\mathfrak{f}_1(\tau+2) = \zeta_{48}^{-1}\mathfrak{f}(\tau+1) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+2}{2})}{\eta(\tau+1)} = \zeta_{24}^{-1}\mathfrak{f}_1(\tau), \theta_{10}(\frac{\tau+2}{2}) = \zeta_8\theta_{10}(\tau/2),$$

aus denen der erste Teil der dritten Aussage folgt:

$$\mathfrak{g}_2(\tau) = \zeta_{12}\frac{\theta_{10}(\frac{\tau+2}{6})\mathfrak{f}_1(\frac{\tau+2}{3})}{\theta_{10}(\frac{\tau+2}{2})\mathfrak{f}_1(\tau+2)} = \zeta_{12}\frac{\theta_{10}(\frac{\tau+2}{6})\mathfrak{f}_1(\frac{\tau+2}{3})}{\zeta_8\theta_{10}(\frac{\tau}{2})\zeta_{24}^{-1}\mathfrak{f}_1(\tau)} = \frac{\theta_{10}(\frac{\tau+2}{6})\mathfrak{f}_1(\frac{\tau+2}{3})}{\theta_{10}(\frac{\tau}{2})\mathfrak{f}_1(\tau)}.$$

Letztlich nach dem Satz 4.34, (5), gilt

$$\mathfrak{g}_2(\tau)^3 = \frac{\zeta_4 3\sqrt{3}}{\mathfrak{g}_3(\frac{\tau+2}{3})^3} = \zeta_4 \frac{\theta_{10}(\frac{\tau+2}{6})^2\theta_{01}(\frac{\tau+2}{3})}{\theta_{10}(\frac{\tau+2}{2})^2\theta_{01}(\tau+2)}.$$

Aus den Transformationsformeln 4.29 folgt somit die letzte Aussage:

$$\mathfrak{g}_2(\tau)^3 = \zeta_4 \frac{\theta_{10}(\frac{\tau+2}{6})^2\theta_{01}(\frac{\tau+2}{3})}{\zeta_4\theta_{10}(\frac{\tau}{2})^2\theta_{01}(\tau)} = \frac{\theta_{10}(\frac{\tau+2}{6})^2\theta_{01}(\frac{\tau+2}{3})}{\theta_{10}(\frac{\tau}{2})^2\theta_{01}(\tau)}.\square$$

Die Stufe $l = 5$: Mit Hilfe des folgenden Satzes können wir die verallgemeinerten Schläflischen Funktionen der Stufe 5 mittels Quotienten der Thetanullwerte darstellen, dessen Beweis, wie im Beweis des Satzes 4.39, aus der Betrachtung der Transformationen von $\mathfrak{f}_1$ zusammmen mit den Transformationen 4.29 folgt:

Satz 4.40. *Es gelten die folgenden Identitäten für $\tau \in \mathbb{H}$:*

1. $\mathfrak{h}_0(\tau) = \frac{\theta_{10}(\tau/10)}{\theta_{10}(\tau/2)}\frac{\mathfrak{f}_1(\tau/5)}{\mathfrak{f}_1(\tau)}$, $\mathfrak{h}_0(\tau)^3 = \frac{\theta_{10}(\tau/10)^2}{\theta_{10}(\tau/2)^2}\frac{\theta_{01}(\tau/5)}{\theta_{01}(\tau)}$,
2. $\mathfrak{h}_1(\tau) = \zeta_6\zeta_{48}\frac{\theta_{10}(\frac{\tau+1}{10})\mathfrak{f}_1(\frac{\tau+1}{5})}{\theta_{10}(\frac{\tau+1}{2})\mathfrak{f}(\tau)}$, $\mathfrak{h}_1(\tau)^3 = -\frac{\theta_{10}(\frac{\tau+1}{10})^2\theta_{01}(\frac{\tau+1}{5})}{\theta_{10}(\frac{\tau+1}{2})^2\theta_{00}(\tau)}$,
3. $\mathfrak{h}_2(\tau) = \zeta_{24}\frac{\theta_{10}(\frac{\tau+2}{10})\mathfrak{f}_1(\frac{\tau+2}{5})}{\theta_{10}(\frac{\tau}{2})\mathfrak{f}_1(\tau)}$, $\mathfrak{h}_2(\tau)^3 = \zeta_8\frac{\theta_{10}(\frac{\tau+2}{10})^2\theta_{01}(\frac{\tau+2}{5})}{\theta_{10}(\frac{\tau}{2})^2\theta_{01}(\tau)}$,
4. $\mathfrak{h}_3(\tau) = \zeta_{48}\frac{\theta_{10}(\frac{\tau+3}{10})\mathfrak{f}_1(\frac{\tau+3}{5})}{\theta_{10}(\frac{\tau+1}{2})\mathfrak{f}(\tau)}$, $\mathfrak{h}_3(\tau)^3 = \frac{\theta_{10}(\frac{\tau+3}{10})^2\theta_{01}(\frac{\tau+3}{5})}{\theta_{10}(\frac{\tau+1}{2})^2\theta_{00}(\tau)}$,
5. $\mathfrak{h}_4(\tau) = \zeta_{24}^{-1}\frac{\theta_{10}(\frac{\tau+4}{10})\mathfrak{f}_1(\frac{\tau+4}{5})}{\theta_{10}(\frac{\tau}{2})\mathfrak{f}_1(\tau)}$, $\mathfrak{h}_4(\tau)^3 = \zeta_8\frac{\theta_{10}(\frac{\tau+4}{10})^2\theta_{01}(\frac{\tau+4}{5})}{\theta_{10}(\frac{\tau}{2})^2\theta_{01}(\tau)}$,
6. $\mathfrak{h}_5(\tau) = \sqrt{5}\frac{\theta_{10}(\frac{5\tau}{2})\mathfrak{f}_1(5\tau)}{\theta_{10}(\frac{\tau}{2})\mathfrak{f}_1(\tau)}$, $\mathfrak{h}_5(\tau)^3 = 5\sqrt{5}\frac{\theta_{10}(\frac{5\tau}{2})^2\theta_{01}(5\tau)}{\theta_{10}(\frac{\tau}{2})^2\theta_{01}(\tau)}$.

Beliebige Stufe l: Aus der Idee des Beweises des Satzes 4.39 können wir die Funktionen

$$\mathfrak{m}_l(\tau) = \sqrt{l}\frac{\eta(l\tau)}{\eta(\tau)} \text{ und } \mathfrak{m}_0(\tau) = \frac{\eta(\frac{\tau}{l})}{\eta(\tau)} \tag{4.30}$$

mittels des folgenden Satzes als Quotienten der Thetanullwerte darstellen.

Satz 4.41. *Es gelten die folgenden Identitäten für $\tau \in \mathbb{H}$:*

1. $\mathfrak{m}_0(5\tau)\mathfrak{m}_l(\tau) = \sqrt{l}$,
2. $\mathfrak{m}_0(\tau) = \frac{\theta_{10}(\tau/2l)\mathfrak{f}_1(\tau/l)}{\theta_{01}(\tau/2)\mathfrak{f}_1(\tau)}$,

3. $\mathfrak{m}_0(\tau)^3 = \frac{\theta_{10}(\tau/2l)^2}{\theta_{10}(\tau/2)^2}\frac{\theta_{01}(\tau/l)}{\theta_{01}(\tau)}$,

4. $\mathfrak{m}_l(\tau) = \sqrt{l}\frac{\theta_{10}(l\tau/2)\mathfrak{f}_1(l\tau)}{\theta_{10}(\tau/2)\mathfrak{f}_1(\tau)}$,

5. $\mathfrak{m}_l(\tau)^3 = l\sqrt{l}\frac{\theta_{10}(l\tau/2)^2\theta_{01}(l\tau)}{\theta_{10}(\tau/2)^2\theta_{01}(\tau)}$.

Beweis: Analoge an den Beweisen der Sätze 4.34 und 4.39 folgen sämtliche Aussagen. □

Bemerkung 4.42. *Die Funktionen*

$$\zeta\frac{\eta(\frac{\tau+k}{l})}{\eta(\tau)}$$

der beliebigen Stufe l kann man mittels des Satzes 4.41 mit einer geeigneten Einheitswurzel ζ sowie der Transformationen 4.29 als gewisse Quotienten der Thetanullwerte darstellen.

4.5.1 Klasseneinheiten

Wir werden nun mit Hilfe des Satzes 4.25 zeigen, dass die im Satz 4.35 eingeführten Klasseninvarianten stets Einheiten sind.

Satz 4.43. *Die im Satz 4.35 eingeführten Klasseninvarianten sind Einheiten in den entsprechenden Hilbertklassenkörpern.*

Beweis: Wir betrachten zunächst den Fall $D \equiv 1 \bmod 3$ und $D \equiv 1 \bmod 4$. Wir haben daher die Bedingung $D \equiv 1 \bmod 12$.

Es gilt somit, dass $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ ist und 3 in $\mathcal{O}_k$ zerfällt.

Ferner gilt für die Zahl l des Satzes 4.25 stets $l = 0$, da wegen der Voraussetzungen im Satz 4.35 für den Führer $t = 1$ gilt.

Nach dem Satz 4.25, 1. (c), sind die Quotienten $\frac{\varphi_P(\tau)}{3^{12}}$ und $\frac{\varphi_Q(\tau)}{3^{12}}$ mit den Matrizen $P = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$ bzw. $Q = \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}$ Einheiten.

Nun erhalten wir nach dem Satz 4.24 daher die Einheiten

$$\frac{\varphi_P(\tau)}{3^{12}} = 3^{-12}\frac{\Delta(\tau/3)}{3^{-12}\Delta(\tau)} = \frac{\Delta(\tau/3)}{\Delta(\tau)} \text{ und } \frac{\varphi_Q(\tau)}{3^{12}} = \frac{\Delta(\frac{\tau+1}{3})}{\Delta(\tau)}.$$

Wegen der Identität 4.19 sind die $12-$ten Wurzeln dieser Einheiten die Klasseninvarianten für die Fälle $D \equiv 1 \bmod 4$ und $D \equiv 1, 4, 7 \bmod 9$.

Analog erhalten wir für die Fälle $D \equiv 0, 4 \bmod 8$ und $D \equiv 1, 4, 7 \bmod 9$ die Einheiteneigenschaften der Klasseninvarianten, da wir stets $D \equiv 4 \bmod 12$

haben. Denn auch in diesem Fall zerfällt 3 in $\mathcal{O}_k$, und wir können neben Q auch die Matrix $R = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ mit dem Satz 4.25, 1. (c), betrachten, um die Einheiteneigenschaft von $\mathfrak{g}_2(\tau)^2$ nachzuweisen.

Nun haben wir für die Fälle $D \equiv 0 \bmod 3$ und $D \equiv 0 \bmod 4$ stets $D \equiv 0 \bmod 12$.

Es gilt daher, dass 3 in $\mathcal{O}_k$ verzweigt ist. Nach dem Satz 4.25, 1. (c), und dem Satz 4.24 erhalten wir mit der Matrix $P = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$ die Einheit

$$\frac{\varphi_P(\tau)}{3^6} = \frac{1}{3^6}\frac{\Delta(\frac{\tau}{3})}{\Delta(\tau)}.$$

Es folgt daraus wegen der Identität 4.24 die Gleichung

$$\left(\frac{\mathfrak{g}_0(\tau)^2}{\sqrt{3}}\right)^{12} = \frac{1}{3^6}\frac{\Delta(\frac{\tau}{3})}{\Delta(\tau)}.$$

Wir haben insgesamt die Eigenschaft, dass die Klasseninvarianten

$$\frac{\mathfrak{g}_0(\tau)^2}{\sqrt{3}}, \frac{\mathfrak{g}_0(\tau)^4}{3}, \frac{\mathfrak{g}_0(\tau)^6}{3\sqrt{3}} \text{ und } \frac{\mathfrak{g}_0(\tau)^{12}}{3^3}$$

Einheiten für $D \equiv 24 \bmod 72$, $D \equiv 60 \bmod 72$, $D \equiv 48 \bmod 72$ bzw. $D \equiv 12 \bmod 72$ sind.

Letztlich erhalten wir für den Fall $D \equiv 1 \bmod 4$ und $D \equiv 0 \bmod 3$ die Kongruenzbedingung $D \equiv 9 \bmod 12$, und damit $3|D$. Wieder nach dem Satz 4.25, 1. (c), dem Satz 4.24 haben wir mit der Matrix $R = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ die Einheit

$$\frac{\varphi_R(\tau)}{3^6} = \frac{1}{3^6}\frac{\Delta(\frac{\tau+2}{3})}{\Delta(\tau)},$$

und wegen der Identität 4.24

$$\left(\frac{\mathfrak{g}_2(\tau)^2}{\sqrt{3}}\right)^{12} = \frac{1}{3^6}\frac{\Delta(\frac{\tau+2}{3})}{\Delta(\tau)}.$$

Somit sind die Klasseninvarianten

$$\frac{\mathfrak{g}_2(\tau)^2}{\sqrt{-3}} \text{ und } \frac{\mathfrak{g}_2(\tau)^6}{3\sqrt{-3}}$$

Einheiten für $D \equiv 33 \bmod 72$ bzw. $D \equiv 57 \bmod 72$. □

Bemerkung 4.44. *Enge und Schertz haben in [EnSch03] und [EnSch04] die Klasseninvarianten mittels der Doppel $\eta-$Quotienten*

$$\mathfrak{m}^s_{p_1,p_2}(\tau) = \left(\frac{\eta(\frac{\tau}{p_1})\eta(\frac{\tau}{p_1})}{\eta(\tau)\eta(\frac{\tau}{p_1 p_2})} \right)^s$$

eingeführt, wobei $p_1 \neq p_2$ Primzahlen sind, und
$s = 24/\operatorname{ggT}(24, (p_1-1)(p_2-1)) \in \mathbb{Z}$ gilt.

Diese Quotienten sind nach [EnSch03], S. 7, auch Einheiten. Wir merken an, dass wir für gegebenes s auch diese Invarianten mittels der Thetanullwerte, wie in 4.39, mit Hilfe der Transformationsformeln 4.16 und 4.29 darstellen können.

4.6 Optimale Klasseninvarianten

Wir werden uns nun mit der Frage beschäftigen, wie gut wir mittels einer Klasseninvariante als ein singulärer Wert der Modulfunktion g der Stufe N im Vergleich zu dem Wert der absoluten Invariante j ein Klassenpolynom erhalten können.

Es sei g eine Modulfunktion, deren singuläre Werte $g(\tau)$ Klasseninvarianten sind. Dann unterscheidet asymptotisch, $|D| \to \infty$, die logarithmische Höhe der Nullstellen des Klassenpolynoms von $g(\tau)$ von der logarithmischen Höhe des Hilbertklassenpolynoms von $j(\tau)$ um einen konstanten Faktor, wie wir früher diskutiert haben. Daher wollen wir feststellen, ob dieser konstante Faktor beliebig gut sein kann. Wir werden aber sehen, dass dieser Faktor nach oben durch 100.82 beschränkt ist.

Zu jeder Modulfunktion $g \in \mathcal{F}$ existiert ein Polynom mit

$$\Phi(g, j) = 0,$$

welches wir **Modulpolynom** nennen, siehe [EnSch05], S. 132. Für die Modulfunktion g der Stufe N definieren wir den folgenden Quotienten, welcher uns ermöglicht, die Klasseninvariante $g(\tau)$ mit $j(\tau)$ zu vergleichen:

$$r(g) = \frac{\deg_g(\Phi(g, j))}{\deg_j(\Phi(g, j))}. \tag{4.31}$$

Nach [HinSil00], Proposition B.3.5, haben wir den folgenden Satz:

Satz 4.45. *Voraussetzungen seien wie oben. Dann ist $r(g)$ asymptotisch gleich dem Faktor*

$$\lim_{\mathcal{H}(j(\tau))\to\infty} \frac{\mathcal{H}(g(\tau))}{\mathcal{H}(j(\tau))},$$

wobei der Limes über alle CM-Punkte $\tau \in \mathbb{H}$ gebildet wird, welche durch den Betrag der Diskriminante der entsprechenden Ordnungen geordnet sind, und $\mathcal{H}$ die absolute logarithmische Höhe ist.

Mit Hilfe des Satzes 4.45 haben Bröker und Stevenhagen den folgenden Satz bewiesen, siehe [BrSt08]:

Satz 4.46. *Es gilt*

$$r(g) \leq 32768/325 \approx 100.82,$$

wobei g eine beliebige Modulfunktion einer beliebigen Stufe ist.

Es bezeichne $\Gamma(g)$ den Stabilisator von g in $\Gamma = \mathrm{Sl}(2,\mathbb{Z})$. Um den Satz 4.46 zu beweisen, haben Bröker und Stevenhagen eine obere Schranke durch

$$r(g) \leq \frac{24}{\lambda_1(\Gamma(g))}, \tag{4.32}$$

erhalten, wobei $\lambda_1(\Gamma(g))$ den Selbergschen Eigenwert bezeichnet, d. h. $\lambda_1(H)$ für eine Kongruenzuntergruppe H von Γ der kleinste positive Eigenwert des Laplace-Operators auf der Modulkurve X_H ist, siehe auch [Sar95]. Die zur Zeit beste untere Schranke für den Selbergschen Eigenwert beträgt

$$\lambda_1(\Gamma(g)) \geq 975/4096.$$

Daher hat man die obere Schranke 100.82 für $r(g)$.

Nach der Vermutung über den Selbergschen Eigenwert gilt für die untere Schranke, siehe [Sar95]:

$$\lambda_1(\Gamma(g)) \geq 1/4.$$

Daher haben wir den folgenden Satz, wessen Beweis aus der Ungleichung 4.32 folgt:

Satz 4.47. *Falls die Vermutung über den Selbergschen Eigenwert gilt, dann gilt*

$$r(g) \leq 96.$$

Der Satz 4.47 besagt, dass wir zumindest theoretisch einen optimalen konstanten Faktor 96 gewinnen können, falls es eine Modulfunktion gibt, deren singulären Werte Klasseninvarianten liefern.

Die Schläflische Funktion $\mathfrak{f}$ aus dem Satz 4.9 nach der Bemerkung 4.10 und dem Lemma 4.8 liefert den Faktor $r(\mathfrak{f}) = 72$, falls für die Diskriminante $3 \not| D$ und $D = -4m$ mit $m \equiv 1 \bmod 8$ gilt. Im Sinne des Satzes 4.47 ist diese Klasseninvariante die zur Zeit mittels der CM-Methode konstruierbare beste Klasseninvariante.

Die Aufgabe besteht also darin, die Modulfunktionen g zu bestimmen, für die $r(g) = 96$ gilt und deren singulären Werte Klasseninvarianten sind.

Dieses ist zur Zeit ein offenes Problem, welches vermutlich mittels der Untersuchung gewisser Quotienten der Thetanullwerte gelöst werden könnte.

Falls wir für die Optimalität noch die Bedingung haben wollen, dass die Klasseninvarianten Einheiten sein sollten, erhalten wir nach dem Satz 4.9, der Bemerkung 4.10, und dem Lemma 4.8

$$\left(\frac{2}{A}\right) \frac{1}{\sqrt{2}} \mathfrak{f}(\tau)$$

als im Sinne des Satzes 4.47 beste Klasseninvariante, falls $m \equiv 7 \bmod 8$ und $3 \not| D$ gilt.

Kapitel 5

Klasseninvarianten im Geschlecht zwei

Hauptziel dieses Kapitels ist es, das Verfahren der Bestimmung einer Klasseninvariante vom Geschlecht eins mittels des zweidimensionalen Reziprozitätsgesetzes von Shimura und einer von Sasaki ([Sa99]) bestimmten Arithmetik gewisser Siegelschen Modulfunktionen auf die einfachen hauptpolarisierten abelschen Flächen (A, E) von vorgegebenem primitiven CM-Typ (K, Φ) zu verallgemeinern. Des Weiteren werden wir beweisen, dass alle primitiven CM-Körper K vom Grad vier über $\mathbb{Q}$ eine relative Ganzheitsbasis über ihrem reell quadratischen Zahlkörpern K_0 besitzen, falls $A = \mathbb{C}^2/\Phi(\mathcal{O}_K)$ ist. Dies wird es ermöglichen, die im dritten Kapitel eingeführte CM-Konstruktion auf alle primitiven CM-Körper zu erweitern.

Wir schreiben (einfachheitshalber) $F = K^r$, wobei K^r der im ersten Kapitel eingeführte Reflexivkörper des primitiven CM-Körpers K ist. Dann gilt nach dem ersten Kapitel, dass K entweder zyklisch mit $K = F$ oder nicht-galoissch mit der galoisschen Hülle L ist, wobei die absolute Galoisgruppe von L stets die Diedergruppe D_4 ist. Im nicht-galoisschen Fall ist F wieder ein primitiver CM-Körper vom Grad vier mit $K \neq F$, welcher in L enthalten ist.

Wie wir im dritten Kapitel erläutert haben, ist es hinreichend, die CM-Konstruktion durchzuführen, falls der primitive CM-Körper K eine relative Ganzheitsbasis über seinem reell quadratischen Zahlkörper K_0 besitzt. Wir werden im ersten Abschnitt zeigen, dass die Steinitzklasse, siehe 5.1, für jeden primitiven CM-Körper K vom Grad vier ein Hauptideal ist, falls für die hauptpolarisierte abelsche Fläche A stets $A = \mathbb{C}^2/\Phi(\mathcal{O}_K)$ gilt. Aus dieser Eigenschaft der Steinitzklasse folgt, dass K eine relative Ganzheitsbasis über seinem reell quadratischen Zahlkörper K_0 besitzt. Damit erweitern wir die CM-Konstruktion auf alle primitiven CM-Körper, deren reell quadratischen Zahlkörper nicht notwendig die Klassenzahl eins besitzen soll.

Das in diesem Kapitel entwickelte Verfahren überprüft, ob der Wert einer Siegelschen Modulfunktion g der Stufe $(2N, 4N)$, $\mathrm{ggT}(2, N) = 1$ an einem CM-Punkt $\tau \in \mathbb{H}_2$ in dem Modulkörper $H_F = F(j_1(\tau), j_2(\tau), j_3(\tau))$ der hauptpolarisierten abelschen Fläche (A, E) vom primitiven CM-Typ (K, Φ) liegt. Damit können wir entscheiden, ob $g(\tau)$ eine Klasseninvariante ist. Im Falle, dass wir ein Klasseninvariantensystem $(g_1(\tau), g_2(\tau), g_3(\tau))$ mittels dieses Verfahrens mit $F(g_1(\tau), g_2(\tau), g_3(\tau)) = H_F$ bestimmen können, dann können wir, wie im Geschlecht eins, statt der Igusa-Klassenpolynome, die Klassenpolynome von $g_1(\tau), g_2(\tau)$ und $g_3(\tau)$ berechnen, welche kleinere Koeffizienten als die Koeffizienten der Igusa-Klassenpolynome besitzen.

Wir werden im zweiten Abschnitt die von Sasaki bestimmte Arithmetik der Siegelschen Modulfunktionen beschreiben.

Als nächstens werden wir im dritten Abschnitt, den maximal mittels der CM-Theorie konstruierbaren Klassenkörper F^{cm} idealtheoretisch beschreiben, welcher in den Arbeiten [Ov74], [Sh97] und [Sh62] zu finden ist. Im Prinzip besagt die Theorie der komplexen Multiplikation, dass die Klassenkörper, die mittels der komplexen Multiplikation konstruiert werden, die Körper sind, die nicht aus den Klassenkörpern der total reellen Teilkörper stammen.

Ferner wird im vierten Abschnitt auf die arithmetischen Siegelschen Modulfunktionen mit komplexer Multiplikation nebst ihren Eigenschaften eingegangen. Des Weiteren werden wir uns mit dem zwei dimensionalen Reziprozitätsgesetz von Shimura beschäftigen, welches uns ermöglicht, unser Verfahren zu beschreiben.

Im fünften Abschnitt werden wir ein Verfahren entwickeln, welches die aus den vorherigen Abschnitten erläuterten Eigenschaften benutzt, um eine explizite Abbildung von $(\mathcal{O}/N\mathcal{O})^*$ nach $U \leq \mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z})$ zu beschreiben. Falls die Bilder dieser Abbildung auf den Wert $g(\tau)$ einer arithmetischen Siegelschen Modulfunktion der Stufe $(2N, 4N)$ trivial operieren, dann liefert dieser Wert $g(\tau)$ eine Klasseninvariante. Wir werden somit abschließend überprüfen, ob ein System $(g_1(\tau), g_2(\tau), g_3(\tau))$ der arithmetischen Siegelschen Modulfunktionen der Stufe $(2N, 4N)$ bereits den Körper H_F erzeugt.

Wir werden abschließend auf die praktischen Betrachtungen dieses Verfahrens im sechsten Abschnitt eingehen.

5.1 Steinitzklasse

Wir haben im dritten Kapitel erläutert, dass die Existenz einer relativen Ganzheitsbasis des primitiven Körpers K über seinem reell quadratischen Zahlkörper eine hinreichende Bedingung dafür ist, dass wir die Menge aller nicht isomorphen hauptpolarisierten abelschen Flächen bestimmen können. In diesem Abschnitt werden wir zeigen, dass jeder primitive CM-Körper K

vom Grad vier über $\mathbb{Q}$ stets eine relative Ganzheitsbasis über seinem reell quadratischen Zahlkörper K_0 besitzt, falls $A = \mathbb{C}^2/\Phi(\mathcal{O}_K)$ ist. Dabei stützen wir uns auf die Tatsache, dass die Existenz einer relativen Ganzheitsbasis äquivalent dazu ist, dass das Ideal, welches die sogenannte Steinitzklasse repräsentiert, ein Hauptideal ist.

Relative Ganzheitsbasis

Es sei nun K ein primitiver CM-Körper, $[K : \mathbb{Q}] = 4$, mit dem reell quadratischen Zahlkörper K_0. Dann existieren Elemente $\omega_1, \omega_2 \in K$ und ein gebrochenes Ideal $\mathfrak{a}$ von K_0 mit

$$\mathcal{O}_K = \omega_1 \mathcal{O}_{K_0} + \omega_2 \mathfrak{a}, \tag{5.1}$$

siehe [PohstVL], S. 38. Die Idealklasse von $\mathfrak{a}$ heißt die **Steinitzklasse** von K. Nach [PohstVL], S. 38, theorem 1.43, haben wir folgende notwendige und hinreichende Bedingung für die Existenz einer relativen Ganzheitsbasis von K über K_0:

Satz 5.1. *Es existiert genau dann eine relative Ganzheitsbasis von K über K_0, wenn das in 5.1 definierte Ideal $\mathfrak{a}$ ein Hauptideal ist.*

Bemerkung 5.2. *Mit der Einführung der idealtheoretischen Diskriminante liefert Fröhlich, siehe [Fr60], eine Vereinfachung des obigen Kriteriums. Der Satz von ihm besagt, dass K/K_0 genau dann eine relative Ganzheitsbasis besitzt, wenn die idealtheoretische Diskriminante durch ein Hauptidel dargestellt werden kann, siehe [Fr60], S. 26, theorem 3.7.*

Wir merken an, dass es in der Praxis schwierig ist dieses Kriterium zu überprüfen, da es zur Zeit keine effizienten Algorithmen für Idele gibt.

Im Falle der Existenz einer relativen Ganzheitsbasis gibt Streng, [Str10], das volle Repräsentantensystem hauptpolarisierter abelscher Flächen mit CM an, deren primitive CM-Körper nicht notwendig einen reell quadratischen Zahlkörper K_0 mit der Klassenzahl eins haben. Für den Beweis verweisen wir auf [Str10], S. 28 und 29:

Satz 5.3. *Es seien K ein primitiver CM-Körper vom Grad 4 über $\mathbb{Q}$, $\Phi = (\phi_1, \phi_2)$ ein CM-Typ von K und $\epsilon \in \mathcal{O}_K^*$, so dass $< -1 > \times < \epsilon >$ in $\mathcal{O}_K^*$ einen endlichen Index besitzt. Ferner sei $\mathcal{K}' = \{z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}\} \subset K$ ein volles Repräsentantensystem der Idealklassen von K, die ein Ideal der Form $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ besitzen, und es sei $\mathcal{K} = \pm\mathcal{K}' \cup \pm\epsilon\mathcal{K}'$. Ein volles Repräsentantensystem hauptpolarisierter abelscher Flächen wird wie folgt angegeben:*

1. $\{\Omega(z) | z \in \mathcal{K}, \Im(\phi_1(z)) > 0 > \Im(\phi_2(z))\}$, *falls K galoissch ist,*

2. $\{\Omega(z)|z \in \mathcal{K}, \Im(\phi_1(z)) > 0\}$, *falls* K *nicht galoissch ist,*

wobei

$$\Omega(z) = (\phi_1 + \phi_2)(z\delta^{-1} \begin{pmatrix} \omega^2 & \omega \\ \omega & 1 \end{pmatrix}) \in \mathbb{H}_2,$$

$\mathcal{O}_{K_0} = \mathbb{Z}[\omega]$ *und* δ *das erzeugende Element der Differente* $\mathcal{D}_{K_0/\mathbb{Q}}$ *sind.*

Wir merken an, dass die Differente $\mathcal{D}_{K_0/\mathbb{Q}}$ stets ein Hauptideal ist, falls K ein primitiver CM-Körper ist. Dies folgt aus der Eigenschaft, dass jeder primitive CM-Körper die Form

$$K = \mathbb{Q}(\sqrt{\Delta_0}, \sqrt{-a + b\Delta_0}) \tag{5.2}$$

hat, wobei Δ_0 die Fundamentaldiskriminante des reell quadratischen Zahlkörpers, und $-a + b\Delta_0$ ein total negatives Element mit $a, b \in \mathbb{Z}$ ist, siehe [Str10], S. 38. Dann wird $\mathcal{D}_{K_0/\mathbb{Q}}$ von dem Element $\delta = \sqrt{\Delta_0}$ erzeugt. Außerdem gilt für das Element a die Ungleichung $0 < a < \Delta$, wobei $\Delta = \Delta_1\Delta_0^2$ die Diskriminante von K ist.

Nach Satz 5.1 und 5.3 können wir die Menge aller nicht isomorphen hauptpolarisierten abelschen Flächen konstruieren:

Bemerkung 5.4. *Wir können bei der Konstruktion hyperelliptischer Kurven im Algorithmus 3 alle primitiven CM-Körper* K *benutzen, deren Steinitzklasse trivial ist.*

Satz 5.5. *Es seien die Voraussetzungen wie im Satz 1.2. Ferner sei* $(A, E) = (\mathbb{C}^2/\Phi(\mathcal{O}_K), E)$ *eine einfache hauptpolarisierte abelsche Fläche vom CM-Typ* (K, Φ)*. Dann besitzt jeder solche primitive Zahlkörper* K *vom Grad* 4 *(über* $\mathbb{Q}$*) eine relative Ganzheitsbasis über seinem reell quadratischen Teilkörper* K_0*.*

Beweis: Zu der Maximalordnung $\mathcal{O}_K$ existieren wegen 5.1 Elemente $\omega_1, \omega \in K$ und ein gebrochenes Ideal $\mathfrak{a} \subseteq K_0$ mit

$$\mathcal{O}_K = \omega_1\mathcal{O}_{K_0} + \omega\mathfrak{a}.$$

Wir können o. E. $\mathcal{O}_K$ mit $\omega_1^{-1}\mathcal{O}_K$ und ξ mit $\omega_1\bar{\omega_1}\xi$, wegen [Spa94], S. 46, Satz 4.1, vertauschen. Daher haben wir

$$\mathcal{O}_K = \mathcal{O}_{K_0} + \omega\mathfrak{a}.$$

Nach dem ersten Kapitel haben wir die Riemannform

$$E_\xi : \mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z},\ (x,y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\xi x \bar{y}).$$

Nun seien $x, y \in \mathcal{O}_{K_0}$. Dann gilt

$$E(x,y) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi x\bar{y}) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi yx) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi y\bar{x}) = E(y,x).$$

Da E eine Riemannform ist, gilt aber $E(x,y) = -E(y,x)$. Wir erhalten somit $E(x,y) = 0$.

Analog gilt $E(x,y) = 0$ für $x,\ y \in \omega\mathfrak{a}$.

Diese implizieren, dass die Riemannform E durch die Elemente $\mathcal{O}_{K_0} \times \omega\mathfrak{a}$ bestimmt sind, da E insbesondere alternierend ist.

Es sei $T : K_0 \times K_0 \to \mathbb{Q}$ die $\mathbb{Q}-$lineare Spurform mit $(a,b) \mapsto \mathrm{Tr}_{K_0/\mathbb{Q}}(ab)$. Weil $\xi(\omega - \bar{\omega})$ ein Element von K_0 ist, gilt

$$E_\xi(\omega a, b) = T(\xi(\omega - \bar{\omega})a, b)$$

für alle $a \in \mathfrak{a}$, $b \in \mathcal{O}_{K_0}$.

Da die Riemannform E_ξ die Hauptpolarisierung liefert und somit die Determinante eins besitzt, gilt nach der Bedingung 1.18 die Eigenschaft, dass $\xi(\omega - \bar{\omega})\mathfrak{a}$ das duale gebrochene Ideal von $\mathcal{O}_{K_0}$ bezüglich der Form T ist. Dies impliziert wegen [Neu92], III.2, S. 205 bis 207, dass

$$\xi(\omega - \bar{\omega})\mathfrak{a} = \mathcal{D}^{-1}(K_0/\mathbb{Q}) = \delta^{-1}\mathcal{O}_{K_0}$$

gilt. Daher ist das Ideal $\mathfrak{a}$ ein Hauptideal. Die Behauptung folgt somit aus dem Satz 5.1□

Korollar 5.6. *Man kann die Menge aller einfachen hauptpolarisierten abelschen Flächen vom CM-Typ (K,Φ) bestimmen, falls K ein primitiver CM-Körper vom Grad vier über $\mathbb{Q}$ ist.*

Beweis: Aus dem Satz 5.5 und 5.3 folgt unmittelbar die Behauptung. □

5.2 Die Arithmetik der Siegelschen Modulfunktionen

Wir werden in diesem Abschnitt eine Arithmetik des Körpers der Siegelschen Modulfunktionen bestimmen, die auf der Arbeit von Sasaki ([Sa99]) basiert und uns ermöglichen wird, die exakte Sequenz 4.4 der eindimensionalen arithmetischen Modulfunktionen auf die zweidimensionalen arithmetischen Siegelschen Modulfunktionen der Stufe $(2N, 4N)$ zu verallgemeinern. Für die Aussagen der Siegelschen Modulfunktionen verweisen wir auf [Kli90].

In [Kr68] untersuchte Kronecker die Körper über $\mathbb{Q}$, die durch

$$\sqrt{\kappa} = \frac{\theta_{10}(2\tau)}{\theta_{00}(2\tau)} \tag{5.3}$$

und

$$\frac{\theta_{11}(2\tau, 2(\tau h_1 + h_2))}{\theta_{01}(2\tau, 2(\tau h_1 + h_2))} \text{ mit } h = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \in \frac{1}{N}\mathbb{Z}^2 \tag{5.4}$$

erzeugt werden.

Die Funktionen 5.3 und 5.4 entsprechen der $j-$Funktion und den Weberschen Funktionen 2.14 in der modernen Sprache.

Die Menge aller symmetrischen $2 \times 2-$Matrizen $\tau \in \mathbb{C}^{2\times 2}$ mit positiv definitem Imaginärteil bildet eine drei-dimensionale komplexe Mannigfaltigkeit $\mathbb{H}_2$, die wir im ersten Kapitel als die Siegelsche obere Halbebene der Dimension zwei definiert haben.

Da wir keine entsprechenden Funktionen der $j-$ Invariante für die Modulfunktionen höherer Dimension haben, aber eine entsprechende Theorie der Thetafunktionen für ein beliebiges Geschlecht existiert, werden wir die Körper über $\mathbb{Q}$ betrachten, die durch die folgenden Quotienten der zwei dimensionalen Thetanullwerte der zweiten Ordnung und der Thetafunktionen erzeugt werden:

$$\kappa_i = \frac{\theta_{a_i}(2\tau)}{\theta_{a_0}(2\tau)},\ 1 \leq i \leq 3,\ \tau \in \mathbb{H}_2 \tag{5.5}$$

und

$$f_i(h)[\tau] = \frac{\theta_{a_i}(2(\tau h_1 + h_2), 2\tau)}{\theta_{a_0}(2(\tau h_1 + h_2), 2\tau)} : i = 1, 2, 3, h = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \in \frac{1}{N}\mathbb{Z}^4/\mathbb{Z}^4,\ \tau \in \mathbb{H}_2 \tag{5.6}$$

wobei $a_1 = [1,0,0,0]^t, a_2 = [0,1,0,0]^t, a_3 = [1,1,0,0]^t$ und $a_0 = [0,0,0,0]^t$ die im ersten Kapitel definierten geraden Thetacharakteristiken sind und $\tau \in \mathbb{H}_2$ ist.

Diese Funktionen stellen somit Verallgemeinerungen der Funktionen 5.3 und 5.4 im Falle der Dimension zwei dar.

Die symplektische Gruppe $\mathrm{Sp}(4, \mathbb{R})$ operiert auf $\mathbb{H}_2$ durch

$$M \cdot \tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = (a\tau + b)(c\tau + d)^{-1}, \tag{5.7}$$

wobei $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(4, \mathbb{R})$ und a, b, c und d stets $2 \times 2-$Matrizen sind.

Wir betrachten die Kongruenzuntergruppe $\Gamma(2,4)$ der Siegelschen Modulgruppe $\Gamma = \mathrm{Sp}(4, \mathbb{Z})$, welche aus den Matrizen $M \in \mathrm{Sp}(4, \mathbb{Z})$ der Form

$$M \equiv 1_4 \bmod 2, \ \{a^t b\} \equiv \{c^t d\} \equiv 0 \bmod 4 \tag{5.8}$$

besteht, wobei 1_4 die 4×4 Einheitsmatrix und $\{A\}$ den Vektor der quadratischen Matrix A bezeichnen, welcher aus den diagonalen Elementen von A besteht.

Der Quotient $\mathbb{H}_2/\Gamma(2,4)$ ist der Modulraum der hauptpolarisierten abelschen Varietäten mit der Stufe $(2,4)-$Struktur. Die Funktionen κ_1, κ_2 und κ_3 der Gleichung 5.5 erzeugen den Modulkörper bezüglich der Kongruenzuntergruppe $\Gamma(2,4)$, siehe [Sa99], S. 81.

Explizite Kummer Fläche

Es sei nun $(A, E) = \mathbb{C}^2/(\tau\mathbb{Z}^2 + \mathbb{Z}^2)$ eine einfache hauptpolarisierte abelsche Varietät vom CM-Typ (K, Φ) mit der wie im ersten Kapitel definierten Periodenmatrix $\tau \in \mathbb{H}_2$. Dann liefert das Bild der holomorphen Abbildung

$$\Psi : (A, E)/\mathrm{Tor}(K) \to \mathbb{P}^3, z \mapsto (\theta_{a_0}(2z, 2\tau) : \theta_{a_1}(2z, 2\tau) : \theta_{a_2}(2z, 2\tau) : \theta_{a_3}(2z, 2\tau)) \tag{5.9}$$

die explizite Kummer Fläche $W(\tau)$ im Falle der Dimension zwei, siehe [Igu60-I]. Für das Produkt der Thetafunktionen existiert die folgende Identität ([Sa99], S. 91):

$$f(\tau) = \theta_{a_0}(2z, 2\tau)^i \theta_{a_1}(2z, 2\tau)^j \theta_{a_2}(2z, 2\tau)^k \theta_{a_3}(2z, 2\tau)^l \text{ mit } i + j + k + l = 4, \tag{5.10}$$

welche die definierende Gleichung der Kummer Fläche $W(\tau)$ beschreibt, aus der der folgende Satz folgt, siehe [Sa99], S. 93:

Satz 5.7. *Es sei τ wie oben. Dann ist die Kummer Fläche $W(\tau)$ über dem folgenden Körper definiert*

$$\mathbb{Q}\left(\left\{\frac{\theta_{a_i}(2\tau)}{\theta_{a_j}(2\tau)} : i, j = 0, 1\right\}\right). \tag{5.11}$$

Teilungspunkte

Es sei N eine ungerade positive ganze Zahl mit dem wie im zweiten Kapitel definierten Annulatorideal $\mathfrak{n}$ mit $N = \mathfrak{n} \cap \mathbb{Z}$. Es bezeichne ferner $W(\tau)[N]$

die Untermenge der Kummer Fläche $W(\tau)$, die aus den Punkten

$$\Psi(\tau h_1 + h_2) = (\cdots : \theta_{a_i}(2(\tau h_1 + h_2), 2\tau) : \cdots) \tag{5.12}$$

besteht, wobei $h = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \in \frac{1}{N}\mathbb{Z}^4/\mathbb{Z}^4$ wie in der Gleichung 5.6 definiert ist.

Es sei $W[N]$ die Untermenge der Kummer Fläche W, die aus den Untermengen $W(\tau)[N]$ der Kummer Fläche $W(\tau)$ für die CM-Punkte $\tau \in \mathbb{H}_2$ besteht. Wir bezeichnen den Modulkörper der Elemente $W[N]$ mit $\mathcal{F}_N$.

Dann gilt der folgende Satz, [Sa99], S. 101 und 102:

Satz 5.8. *Voraussetzungen seien wie oben. Dann gilt*

$$\mathcal{F}_N = \mathbb{Q}\left(\left\{f_1(h), f_2(h), f_3(h) : h \in \frac{1}{N}\mathbb{Z}^4/\mathbb{Z}^4\right\}\right).$$

Ferner ist $\mathcal{F}_N$ der Körper der arithmetischen Siegelschen Modulfunktionen der Stufe $(2N, 4N)$.

Aus dem Satz 5.8 und der Gleichung 5.5 folgt unmittelbar, dass

$$\mathcal{F}_1 = \mathbb{Q}(\kappa_1, \kappa_2, \kappa_3) \tag{5.13}$$

gilt.

Die exakte Sequenz

Der folgende Satz verallgemeinert die galoistheoretische Betrachtung 4.2 der Körper arithmetischer Modulfunktionen vom Geschlecht eins auf den Körper der arithmetischen Siegelschen Modulfunktionen der Stufe $(2N, 4N)$, siehe [Sa99], S. 103:

Satz 5.9. *Der Körper $\mathcal{F}_N$ hat die folgenden Eigenschaften:*

1. *$\mathcal{F}_N$ ist eine Galoiserweiterung des Körpers $\mathcal{F}_1$,*
2. *$\zeta_N \in \mathcal{F}_N$,*
3. *$\mathbb{Q}(\zeta_N)$ ist in $\mathcal{F}_N$ algebraisch abgeschlossen,*
4. *$Gal(\mathcal{F}_N/\mathcal{F}_1) = U(4, \mathbb{Z}/N\mathbb{Z}) \leq GL(4, \mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\}$, wobei $U(4, \mathbb{Z}/N\mathbb{Z})$ aus den Matrizen*

   $R \in GL(4, \mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\}$ besteht, für die ein $n \in \mathbb{N}$ existiert mit

$$\mathrm{ggT}(n, N) = 1, \ \textit{und}$$
$$n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv R^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} R \bmod N.$$

Wir können somit die Galoisgruppe des Körpers aller arithmetischen Siegelschen Modulfunktionen bezüglich aller Stufen $(2N, 4N)$

$$\mathcal{F} = \cup_{N \geq 1} \mathcal{F}_N$$

über $\mathcal{F}_1$ durch den projektiven Limes (wie im Geschlecht eins 4.3) wie folgt beschreiben:

$$\lim_{\leftarrow N}(\mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\}) = U(4, \widehat{\mathbb{Z}})/\{\pm 1_4\} \cong \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1). \tag{5.14}$$

Wir erhalten somit die folgende exakte Sequenz

$$1 \longrightarrow \{\pm 1\} \longrightarrow U(4, \widehat{\mathbb{Z}}) \longrightarrow \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1. \tag{5.15}$$

5.3 Konstruierbare Klassenkörper mit CM

In diesem Abschnitt werden wir den maximal mittels der Theorie der komplexen Multiplikation konstruierbaren Klassenkörper F^{cm} beschreiben, wobei F der Reflexivkörper eines primitiven CM-Körpers K vom Grad 4 über $\mathbb{Q}$ ist.

Der maximale Klassenkörper

Im zweiten Kapitel haben wir diskutiert, dass die Typ-Norm Abbildung 1.13 als eine $\mathbb{Q}_A-$lineare Abbildung fortgesetzt werden kann, deren Fortsetzung

$$N_\Psi : F_A^* \to K_A^* \tag{5.16}$$

auch einen stetigen Homomorphismus der Idelklassengruppe
$C_F = F_A^*/F^*$ nach der Idelklassengruppe $C_K = K_A^*/K^*$,
und somit einen stetigen Homomorphismus

$$N_\Psi : C_F/D_F \to C_K/D_K \tag{5.17}$$

liefert, wobei D_M die zusammenhängende Komponente des Einselements der Idelgruppe M_A^* eines Zahlkörpers M bezeichnet.

Es sei (A, E) eine einfache hauptpolarisierte abelsche Fläche vom primitiven CM-Typ (K, Φ). Wir können die Untergruppe $G_{\mathfrak{n}}$ der Idelgruppe F_A^*, die

dem Klassenkörper des Hauptsatzes 2.6 $H_F(f(t))$ über F entspricht, durch den folgenden Satz von Ovseevich beschreiben, [Ov74], S. 17, theorem 3.2.3:

Satz 5.10. *Dem Körper $H_F(f(t))$ über F entspricht die Untergruppe $G_\mathfrak{n}$ der Idelgruppe F_A^* mit $G_\mathfrak{n} = N_\Psi^{-1}(H_\mathfrak{n})$, wobei*

$$H_\mathfrak{n} = PU_\mathfrak{n} \text{ mit}$$
$$P = \{\xi \in K^* \subseteq K_A^* : \xi\bar{\xi} \in \mathbb{Q}\} \text{ und}$$
$$U_\mathfrak{n} = \{u \in K_A^* : u \equiv 1 \bmod \mathfrak{n} \text{ ein ganzes Idel ist}\}.$$

Im Falle, dass der Endomorphismenring von (A, E) nicht der Maximalordnung $\mathcal{O}_K$, sondern einer beliebigen Ordnung $\mathcal{O} \subseteq \mathcal{O}_K$ entspricht, kann man die Hauptsätze der komplexen Multiplikation auch formulieren (siehe Kapitel 2). Es gilt insbesondere, dass diese Klassenkörper stets im Kompositum F^{cm} aller Klassenkörper $H_F(f(t))$ liegen. Daher ist die Betrachtung der Maximalordnung und des entsprechenden Klassenkörpers $H_F(f(t))$ genügend, um den maximal mittels der CM-Theorie konstruierbaren Teilkörper $F^{cm} \subseteq F^{ab}$ idealtheoretisch beschreiben zu können.

Nun haben wir für die Untergruppe G_Ψ der Idelgruppe F_A^*, die dem Körper F^{cm} entspricht den folgenden Satz, siehe [Ov74], S. 17, theorem 3.2.4, und [Sh97], S. 129:

Satz 5.11. *1. Es seien die Voraussetzungen wie oben. Dann gilt $G_\Psi = Kern(N_\Psi)$, wobei N_Ψ die Typ-Norm Abbildung $C_F/D_F \to C_K/D_K$ ist.*

2. Die folgende Sequenz ist exakt:

$$1 \longrightarrow Tor(F) \longrightarrow M_\infty N_\Psi^{-1}(\textstyle\prod_p \mathcal{O}_p^*) \longrightarrow Gal(F^{cm}/H_F) \longrightarrow 1, \tag{5.18}$$

wobei $M_\infty \subseteq F_\infty^*$ den unendlichen Teil bezeichnet.

Wir schreiben (einfachheitshalber) $\mathcal{O}_K = \mathcal{O}$ und $L_\mathfrak{n} = H_F(f(t))$, wobei $\mathfrak{n}$ das im zweiten Kapitel definierte Annulatorideal vom Punkt $t \in A$ bezeichnet.

Weil F ein total komplexer Zahlkörper ist, haben wir die Eigenschaft, dass der im zweiten Kapitel definierte nicht archimedische Teil F_∞^* der Idelgruppe F_A^* von F unter der Artinabbildung trivial ist. Daher haben wir nach dem Satz 5.11 die folgende exakte Sequenz (Wir vergessen den unendlichen Teil, vgl. mit dem vierten Kapitel):

$$1 \longrightarrow \mathrm{Tor}(F) \longrightarrow N_\Psi^{-1}(\textstyle\prod_p \mathcal{O}_p^*) \longrightarrow \mathrm{Gal}(F^{cm}/H_F) \longrightarrow 1. \tag{5.19}$$

Bemerkung 5.12. *Die exakte Sequenz 5.19 entspricht genau der Verallgemeinerung der exakten Sequenz 4.8 imaginär quadratischer Körper k, da wir in diesem Fall stets $F = K = k$, $N_\Psi = Id$ und $Tor(k) = \mathcal{O}_k^*$ haben.*

Relative Erweiterung

Zuvor werden wir die relative Körpererweiterung $H_F(f(t))/H_F$ galoistheoretisch beschreiben, wobei nach dem zweiten Hauptsatz der komplexen Multiplikation 2.6 die Galoisgruppe $\mathrm{Gal}(H_F(f(t))/F)$, und nach dem ersten Hauptsatz der komplexen Multiplikation 2.3 die Galoisgruppe $\mathrm{Gal}(H_F/F)$ der Kongruenzuntergruppe

$$H_{\mathfrak{n}} = \left\{ \mathfrak{a} \in I(F)((N)) : \begin{array}{r} \exists \mu \in K^* \text{ mit} \\ N_\Psi(\mathfrak{a}) = \mu \mathcal{O}_K \\ \mu\bar{\mu} = N_{F/\mathbb{Q}}(\mathfrak{a}) \\ \mu \equiv 1 \bmod {}^\times(N) \end{array} \right\}$$

von $I_F((N))$, bzw. der Kongruenzuntergruppe

$$H_0 = \left\{ \mathfrak{a} \in I(F) : \begin{array}{r} \exists \mu \in K^* \text{ mit} \\ N_\Psi(\mathfrak{a}) = \mu \mathcal{O}_K \\ \mu\bar{\mu} = N_{F/\mathbb{Q}}(\mathfrak{a}) \end{array} \right\}$$

von I_F entsprechen.

Nun gilt der folgende Satz:

Satz 5.13. $I_F/H_0 \cong \frac{I_F((N))/H_{\mathfrak{n}}}{(I_F((N)) \cap H_0)/H_{\mathfrak{n}}}$.

Wir beweisen den Satz 5.13, nach dem wir die folgenden zwei Lemmata beweisen:

Lemma 5.14. *Es seien $\mathfrak{m}_1$ und $\mathfrak{m}_2$ zwei Moduln eines Zahlkörpers M im Sinne der Klassenkörpertheorie mit $\mathfrak{a} \in I_M(\mathfrak{m}_1)$. Dann existiert ein Element $\alpha \equiv 1 \bmod {}^\times\mathfrak{m}_1$ mit der Eigenschaft, dass $\alpha\mathfrak{a}$ ein zu dem Modul $\mathfrak{m}_1\mathfrak{m}_2$ teilerfremdes ganzes Ideal ist.*

Beweis: Wir fordern für die reellen unendlichen Stellen $\mathfrak{p}_\infty | \mathfrak{m}_1$ die Eigenschaft $\nu_{\mathfrak{p}_\infty}(\alpha) > 0$. Falls wir nun ein Primideal $\mathfrak{p}$ mit $\mathfrak{p}|\mathfrak{m}_1$ haben, dann fordern wir $\nu_{\mathfrak{p}}(\alpha) = 0 = -\nu_{\mathfrak{p}}(\mathfrak{a})$, da wir $\mathfrak{a} \in I_M(\mathfrak{m}_1)$ haben. Falls nun $\mathfrak{p} \nmid \mathfrak{m}_1\mathfrak{m}_2$ gilt, ist die Forderung $\nu_{\mathfrak{p}}(\alpha) \geq -\nu_{\mathfrak{p}}(\mathfrak{a})$. Sämtliche Forderungen folgen aus einem Korollar des starken Approximationssatzes, siehe [Coh00], S. 4, corollary 1.2.9. □

Lemma 5.15. *Es seien $\mathfrak{m}_1$ und $\mathfrak{m}_2$ zwei Moduln eines Zahlkörpers M im Sinne der Klassenkörpertheorie.*

1. *Es gelten* $I_M(\mathfrak{m}_2) \subseteq I_M(\mathfrak{m}_1)P_M(\mathfrak{m}_2)$ *und* $I_M(\mathfrak{m}_1) \subseteq I_M(\mathfrak{m}_2)P_M(\mathfrak{m}_1)$.
2. *Es gilt* $I_M(\mathfrak{m}_2) = I_M(\mathfrak{m}_1)C_M(\mathfrak{m}_2)$, *falls* $\mathfrak{m}_2|\mathfrak{m}_1$ *und* $C_M(\mathfrak{m}_2)$ *eine wie im zweiten Kapitel definierte Kongruenzuntergruppe modulo* $\mathfrak{m}_2$ *sind.*

Beweis: Nach dem Lemma 5.14 existiert zu jedem Ideal $\mathfrak{a} \in I_M(\mathfrak{m}_2)$ ein Element α mit $\alpha \equiv 1 \bmod {}^{\times}\mathfrak{m}_2$ und $\alpha\mathfrak{a} \in I_M(\mathfrak{m}_1)$. Damit erhalten wir $\mathfrak{a} \in I_M(\mathfrak{m}_1)P_M(\mathfrak{m}_2)$, weil $\alpha\mathcal{O}_M \in P_M(\mathfrak{m}_2)$ ist. Es gilt daher für jede Kongruenzuntergruppe $C_M(\mathfrak{m}_2)$ modulo $\mathfrak{m}_2$

$$I_M(\mathfrak{m}_2) \subseteq I_M(\mathfrak{m}_1)P_M(\mathfrak{m}_2) \subseteq I_M(\mathfrak{m}_1)C_M(\mathfrak{m}_2).$$

Umgekehrt ist $I_M(\mathfrak{m}_1) \subseteq I_M(\mathfrak{m}_2)$ und $C_M(\mathfrak{m}_2) \subseteq I_M(\mathfrak{m}_2)$, falls $\mathfrak{m}_2|\mathfrak{m}_1$ ist. Daher folgt die Behauptung. □

Beweis des Satzes 5.13: Nach dem Lemma 5.15 gilt zunächst

$$I_F = I_F((N))H_0.$$

Daher folgt aus den Isomorphiesätzen die Behauptung:

$$\frac{I_F}{H_0} = \frac{I_F((N))H_0}{H_0} \cong \frac{I_F((N))}{I_F((n)) \cap H_0} \cong \frac{I_F((N))/H_{\mathfrak{n}}}{(I_F((N)) \cap H_0)/H_{\mathfrak{n}}}.\square$$

Aus dem Satz 5.13 und der Galoistheorie folgt unmittelbar das folgende Korollar:

Korollar 5.16. *Es gilt* $Gal(H_F(f(t))/H_F) \cong (I_F((N)) \cap H_0)/H_{\mathfrak{n}}$.

Nun haben wir das folgende Lemma nach [Sh97], S. 118,:

Lemma 5.17. *Es gilt* $\mathcal{L}_N := Gal(H_F(f(t))/H_F) \subseteq N_\Psi^{-1}((\mathcal{O}_K/N\mathcal{O}_K)^*)/Tor(F)$, *wobei* $Tor(F)$ *die Untergruppe der Torsionseinheiten von* F *bezeichnet.*

Wegen der Injektivität der Typ-Norm Abbildung identifizieren wir das Bild $N_\Psi(\mathcal{L}_N) \subseteq (\mathcal{O}_K/N\mathcal{O}_K)^*/\mathrm{Tor}(F)$ mit der Gruppe $\mathrm{Gal}(H_F(f(t))/H_F)$, falls $\mathrm{Tor}(F) = \mathrm{Tor}(K)$ ist. Wir betrachten daher nur die CM-Körper K und ihre Reflexivkörper F mit $\mathrm{Tor}(F) = \mathrm{Tor}(K)$.

Wir erhalten nach dem Lemma 5.17 und dem Korollar 5.16 ein $\mathcal{L} = N_\Psi(\mathcal{L}_N)/\mathrm{Tor}(K)$ mit der folgenden exakten Sequenz:

$$1 \longrightarrow \mathrm{Tor}(K) \longrightarrow \mathcal{L} \longrightarrow \mathrm{Gal}(H_F(f(t))/H_F) \longrightarrow 1. \qquad (5.20)$$

Bemerkung 5.18. *Die exakte Sequenz 5.20 entspricht der Verallgemeinerung der exakten Sequenz 4.11.*

5.4 Zweidimensionales Reziprozitätsgesetz

In diesem Abschnitt werden wir das mehrdimensionale Reziprozitätsgesetz von Shimura erklären, welches im nächsten Abschnitt ermöglichen wird, die exakten Sequenzen 5.15 und 5.19 miteinander zu verbinden.

Arithmetische Modulfunktionen

Eine **Siegelsche Modulform** $f(z)$ vom Gewicht k ist eine holomorphe Funktion auf $\mathbb{H}_2$ (und endlich an den Spitzen, falls $n = 1$ ist), die der folgenden Bedingung genügt:

$$f(z) = (f|_k\gamma)(z) = \det(cz + d)^{-1} f(\gamma(z)), \tag{5.21}$$

für alle γ in einer Kongruenzuntergruppe $\Gamma(N)$ von $\Gamma = \mathrm{Sp}(4, \mathbb{Z})$, wobei γ auf den Punkt $z \in \mathbb{H}_2$ wie in 5.7 operiert. Eine Siegelsche Modulform hat folgende Fourierentwicklung:

$$f(z) = \sum_{\alpha^t=\alpha, \alpha\in\mathbb{Z}^{2\times 2}} c_\alpha \exp(2\pi i(\mathrm{Tr}(\alpha z)/N)). \tag{5.22}$$

Wir verstehen unter einer arithmetischen Modulform $f(z)$ eine Modulform, deren Fourierentwicklung 5.22 stets Koeffizienten aus Kreisteilungskörpern hat (vergleiche mit dem vierten Kapitel).

Der Raum der arithmetischen **automorphen Formen** $\mathcal{A}_k(\mathbb{Q}^{ab})$ vom Gewicht k ist die Menge aller Quotienten $g(z)/h(z)$, wobei $g(z)$ und $0 \neq h(z)$ stets arithmetische Modulformen des Gewichts $k + m$ bzw. m sind.

Es sei nun J die 4×4 Matrix

$$J = \begin{pmatrix} 0 & -1_2 \\ 1_2 & 0 \end{pmatrix}. \tag{5.23}$$

Wir definieren die Gruppe der eingeschränkten symplektischen Ähnlichkeiten (eng.: similitudes)

$$G_{A_{\mathbb{Q}}^+} = \{\gamma \in \mathrm{GL}(4, A_{\mathbb{Q}}) | \gamma^t J \gamma = \nu(\gamma) J, \text{ wobei } \nu(\gamma) \in A_{\mathbb{Q}}^* \text{ und } \nu(\gamma)_\infty > 0\},$$

$$G_{\mathbb{Q}^+} = G_{A_{\mathbb{Q}}^+} \cap \mathrm{GL}(4, \mathbb{Q}). \tag{5.24}$$

Nach [Sh78], S. 39, existiert eine assoziative Rechtsoperation von $G_{A_{\mathbb{Q}}^+}$ auf dem Raum $\mathcal{A}_k(\mathbb{Q}^{ab})$, $f \mapsto f^u$, $f \in \mathcal{A}_k(\mathbb{Q}^{ab})$ und $u \in G_{A_{\mathbb{Q}}^+}$ mit folgenden Eigenschaften:

1. $f^\gamma = f|_k\gamma = \det(cz+d)^{-k} f(\gamma(z))$ für $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_{\mathbb{Q}^+}$.

2. $f^{\iota(t)} = f^{[t,\mathbb{Q}]}$ mit $t \in \widehat{\mathbb{Z}}$ und
$$\iota(t) = \begin{pmatrix} 1_2 & 0 \\ 0 & t^{-1}1_2 \end{pmatrix},$$
wobei $f^{[t,\mathbb{Q}]}$ die Modulform ist, die durch die Operation des Elements $[t,\mathbb{Q}]$ auf die Fourierkoeffizienten von f erhalten wird.

3. Die Untergruppe von $G_{A_{\mathbb{Q}}^+}$, die die Modulform fixiert, ist offen.

CM Fall

Es sei nun (A,E) eine polarisierte abelsche Fläche mit der im ersten Kapitel erwähnten Frobeniusbasis $\{\lambda_1, \cdots, \lambda_4\}$ und

$$(E(\lambda_i,\lambda_j))_{1\le i,j\le 4} = \begin{pmatrix} 0 & \mathrm{D} \\ \text{-D} & 0 \end{pmatrix}$$

mit der Diagonalmatrix $D = \mathrm{diag}(d_1,d_2)$, $d_1|d_2$. Dann existiert (nach dem ersten Kapitel) eine $2\times 4-$Matrix $\Omega = (\omega_1,\omega_2)$ mit $2\times 2-$Matrizen ω_1 und ω_2, die das Gitter Λ mit $(A,E) = (\mathbb{C}^2/\Lambda, E)$ erzeugen. Wir haben daher

$$E(\Omega x, \Omega y) = x^t J y \text{ für } x,y \in \mathbb{R}^4,$$
$$\Lambda = \Omega \begin{pmatrix} 1_2 & 0 \\ 0 & D \end{pmatrix} \mathbb{Z}^4.$$

Der CM-Punkt $\tau = \omega_1\omega_2^{-1}$, welcher der polarisierten abelschen Fläche (A,E) entspricht, ist dann bis auf Translationen durch

$$\Gamma \cap \begin{pmatrix} 1_2 & 0 \\ 0 & D \end{pmatrix}^{-1} \mathrm{GL}(4,\mathbb{Z}) \begin{pmatrix} 1_2 & 0 \\ 0 & D \end{pmatrix}$$

eindeutig.

Wir nehmen an, dass (A,E) stets hauptpolarisiert vom primitiven CM-Typ (K,Φ) ist. Wir fixieren einen Anti-Isomorphismus

$$\varsigma : K \to \mathrm{End}(A) \otimes \mathbb{Q}.$$

Die Wahl des Anti-Isomorphismus statt einem Isomorphismus ist mit dem Hauptsatz der CM-Theorie 2.8 kompatibel, siehe [Sh70], I,2.7.3 und II, 6.2.3.

Dann liefert die Formel

$$\varsigma(k)\Omega x = \Omega^t \xi(k) x \text{ für } x \in \mathbb{R}^4,\ k \in K \tag{5.25}$$

eine Darstellung ξ von K in $\mathrm{GL}(4, \mathbb{Q})$. Es gilt nun, siehe [Rum83], S. 216:

$$E(\Omega^t \xi(k)u, \Omega v) = E(\Omega u, \Omega^t \xi(\bar{k})v). \tag{5.26}$$

Wir haben den folgenden Satz, siehe [Rum83], S. 216:

Satz 5.19. *Für alle Elemente $k \in K^*$ mit $k\bar{k} \in \mathbb{Q}$ gilt $\xi(k) \in G_{\mathbb{Q}^+}$, und die Gleichung*

$$\xi(k)(\tau) = \tau.$$

Wegen des Satzes 5.19, heißt ξ die Einbettung an dem CM-Fixpunkt τ in der Siegelschen oberen Halbebene $\mathbb{H}_2$.

Reziprozitätsgesetz

Wir können nun das zwei-dimensionale Reziprozitätsgesetz von Shimura mittels der Typ-Norm Abbildung 1.13 $N_\Psi : F^* \to K^*$ formulieren. Die Kompositionsabbildung $\xi \circ N_\Psi$ bildet die Elemente von F^* in $G_{\mathbb{Q}^+}$ ab. Ferner, wegen der Diskussion im zweiten Kapitel nach der Gleichung 2.9, bildet die $\mathbb{Q}-$lineare Fortsetzung von $\xi \circ N_\Psi$ die Elemente von F_A^* in $G_{A_\mathbb{Q}^+}$ ab. Diese Fortsetzung bezeichnen wir auch mit $\xi \circ N_\Psi$.

Das zwei dimensionale Reziprozitätsgesetz von Shimura besagt, dass wir stets für jedes $s \in F_A^*$ und eine arithmetische Siegelsche Modulfunktion $f \in \mathcal{A}_0(\mathbb{Q}^{ab})$, welche an τ endlich ist, folgende Gleichung haben:

$$f(\tau)^{[s,F]} = f^{\xi \circ N_\Psi(s^{-1})}(\tau). \tag{5.27}$$

Wir haben nun die folgende Version des Hauptsatzes der komplexen Multiplikation: (Für den Beweis verweisen wir auf [Sh70], I, 4.3, und [Sh76], S. 685, proposition 2.3.)

Satz 5.20. *Es seien die Voraussetzungen wie oben. Ferner seien $s \in F_A^*$ mit $\sigma|_{F^{ab}} = [s, F]$ für jeden Automorphismus σ von $\mathbb{C}$. Dann existiert eine hauptpolarisierte abelsche Fläche $(A^\sigma, N_{F/\mathbb{Q}}E)$ mit $A^\sigma = \mathbb{C}^2/N_\Psi(s^{-1})\Lambda$. Ferner gilt für jedes Element $v \in A$ stets $v^\sigma = N_\Psi(s^{-1})v$.*

5.5 Algorithmus

Der Wert $g(\tau)$ einer arithmetischen Siegelschen Modulfunktion $g \in \mathcal{A}_0(\mathbb{Q}^{ab})$ heißt eine **Klasseninvariante**, falls

$$g(\tau) \in H_F = F(j_1(\tau), j_2(\tau), j_3(\tau))$$

gilt, wobei $j_1(\tau)$, $j_2(\tau)$ und $j_3(\tau)$ die im ersten Kapitel betrachteten absoluten Klasseninvarianten 1.28 von Igusa sind.

Außerdem sagen wir, dass die Werte $g_1(\tau), g_2(\tau), g_3(\tau)$ der drei arithmetischen Siegelschen Modulfunktionen $g_1, g_2, g_3 \in \mathcal{A}_0(\mathbb{Q}^{ab})$ ein **Klasseninvariantensystem** ist, wenn

$$H_F = F(g_1(\tau), g_2(\tau), g_3(\tau))$$

mit $F(j_i(\tau)) \subseteq F(g_i(\tau))$ für den CM-Punkt $\tau \in \mathbb{H}_2$, $1 \leq i \leq 3$, gilt.

Die Abbildungen

Es sei g eine aritmetische Siegelsche Modulfunktion der Stufe $(2N, 4N)$. Dann gilt $g(\tau) \in \mathcal{F}_N$, wie wir im ersten Abschnitt diskutiert haben, wenn N eine ungerade positive ganze Zahl ist.

Nach dem Satz 5.7 und der Riemannschen Additionsformel der Thetafunktionen ([Sa99], S. 92) folgt, dass der Körper

$$\mathbb{Q}\left(\left\{\frac{\theta_{a_i}(2\tau)}{\theta_{a_j}(2\tau)} : i, j = 0, 1\right\}\right)$$

über dem Modulkörper H_F von (A, E) definiert ist. Daher erhalten wir nach dem Satz 2.5 die normalisierte Kummer Fläche (W, F) der Dimension zwei.

Bemerkung 5.21. *Nun erhalten wir nach dem Satz 5.8 die Eigenschaft, dass der Körper $F\mathcal{F}$ durch die Elemente $f(\tau)$, $f \in \mathcal{F}_N$, erzeugt wird, wobei $f(\tau)$ endlich ist. Da wir uns mit der arithmetischen Siegelschen Modulfunktion g der Stufe $(2N, 4N)$ beschäftigen, ist der Körper nach dem Hauptsatz der CM-Theorie 2.8 ein Teilkörper von F^{cm}, falls $\mathfrak{n}$ das Annulatorideal von $t \in A$ mit $N = \mathfrak{n} \cap \mathbb{Z}$ ist.*

Folglich erhalten wir nach den exakten Sequenzen 5.19 und 5.15 zusammen mit dem zweidimensionalen Reziprozitätsgesetz von Shimura 5.27 die folgende Reziprozitätsabbildung:

$$\xi \circ N_\Psi : N_\Psi^{-1}(\prod_p \mathcal{O}_p^*) \to \mathrm{GL}(4, \widehat{\mathbb{Z}}). \tag{5.28}$$

Für die Argumentation, warum das Bild von $N_\Psi^{-1}(\prod_p \mathcal{O}_p^*)$ unter $\xi \circ N_\Psi$ gerade in $\mathrm{GL}(4, \widehat{\mathbb{Z}})$ liegt verweisen wir auf [ShGo97], S. 787.

Wir merken an, dass die Bilder $N_\Psi^{-1}(\prod_p \mathcal{O}_p^*)$ unter $\xi \circ N_\Psi$, wegen der Bemerkung 5.21 und der Gleichung 5.27, gerade in $U(4, \widehat{\mathbb{Z}})$ liegen, falls $g \in \mathcal{F}$ ist. Falls diese Bilder auf $g(\tau)$ trivial operieren, ist $g(\tau)$, wegen der Bemerkung 5.21, eine Klasseninvariante, da in diesem Fall $g(\tau) \in H_F$ gilt.

Wir erinnern uns, dass wir $\mathrm{Tor}(K) = \mathrm{Tor}(F)$ wie im vorherigen Abschnitt fordern.

Die exakte Sequenz 5.19 zeigt, dass die Galoisgruppe von F^{cm} eine unkomplizierte Struktur besitzt. Da $\mathrm{Tor}(F)$ eine endliche Gruppe ist, ist die Galoisgruppe $\mathrm{Gal}(F^{cm}/H_F)$ im wesentlichen das Urbild der Einheitengruppe der proendlichen Vervollständigung $\widehat{\mathcal{O}}^*$ von $\mathcal{O}^*$. Dies bedeutet, dass das Kompositum F^{cm} die Vereinigung der endlichen Erweiterungen $H_F(f(t))$ über H_F ist, die den endlichen Quotienten

$$\widehat{\mathcal{O}}^* \twoheadrightarrow (\widehat{\mathcal{O}}/N\widehat{\mathcal{O}})^* = (\mathcal{O}/N\mathcal{O})^*$$

entsprechen, falls wir die Galoisgruppe $\mathrm{Gal}(H_F(f(t))/H_F)$ mit dem Bild $N_\Psi(\mathcal{L}_N/\mathrm{Tor}(K)) \subseteq (\mathcal{O}_K/N\mathcal{O}_K)^*/\mathrm{Tor}(F)$ identifizieren.

Insgesamt erhalten wir eine modulo N reduzierte Abbildung

$$\bar{\xi} : N_\Psi(\mathcal{L}_N/\mathrm{Tor}(K)) \to \mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z}).$$

Nach der Bemerkung 5.21 liegt der endliche Wert $g(\tau)$ einer arithmetischen Modulfunktion der Stufe $(2, 4)$ in $H_F(f(t))$, falls $\mathfrak{n}$ das Annulatorideal des Punktes $t \in A$ mit einer ungeraden positiven Zahl mit N, die das Ideal $\mathfrak{n} \cap \mathbb{Z}$ erzeugt. Dies bedeutet, dass das Bild von $g(\tau)$ stets in der wie im Satz 5.9 definierten Gruppe $U(4, \mathbb{Z}/N\mathbb{Z})$ liegt, die aus den Matrizen

$$R \in \mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\} \text{ besteht, für die ein } n \in \mathbb{N} \text{ existiert mit}$$
$$\mathrm{ggT}(n, N) = 1, \text{ und}$$
$$n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv R^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} R \bmod N.$$

Bemerkung 5.22. *Die obige Betrachtung impliziert, dass $g(\tau)$ eine Klasseninvariante ist, falls die Bilder von $N_\Psi(\mathcal{L}_N/\mathrm{Tor}(K))$ auf $g(\tau)$ trivial operieren.*

Da wir im Allgemeinen die Untergruppe $N_\Psi(\mathcal{L}_N/\mathrm{Tor}(K))$ von $(\mathcal{O}/N\mathcal{O})^*$ nicht explizit beschreiben können, müssen wir die reduzierte Abbildung

$$\bar{\xi} : (\mathcal{O}/N\mathcal{O})^* \to GL(4, \mathbb{Z}/N\mathbb{Z}) \tag{5.29}$$

betrachten, um entscheiden zu können, ob $g(\tau)$ eine Klasseninvariante ist.

Es sei $(g_1(\tau), g_2(\tau), g_3(\tau))$ ein System der Werte der arithmetischen Siegelschen Modulfunktionen der Stufe $(2N, 4N)$ für einen CM-Punkt $\tau \in \mathbb{H}_2$ mit den folgenden Eigenschaften:

1. Es gilt $F(j_1(\tau)) \subseteq F(g_1(\tau))$.
2. Es gilt $F(j_2(\tau)) \subseteq F(g_2(\tau))$.
3. Es gilt $F(j_3(\tau)) \subseteq F(g_3(\tau))$.
4. Es gilt $F(g_1(\tau), g_2(\tau), g_3(\tau)) = F(j_1(\tau), j_2(\tau), j_3(\tau))$.

Wir können nun überprüfen, ob $g_i(\tau)$ eine Klasseninvariante ist, $1 \leq i \leq 3$. Falls alle $g_i(\tau)$ Klasseninvarianten sind, folgt aus der Eigenschaft (4.), dass $H_F = F(g_1(\tau), g_2(\tau), g_3(\tau))$ gilt und $(g_1(\tau), g_2(\tau), g_3(\tau))$ somit ein Klasseninvariantensystem bildet.

Daher können wir die Klassenpolynome der Elemente $g_1(\tau), g_2(\tau), g_3(\tau)$ statt der Igusa-Klassenpolynome berechnen. Wie im Fall der elliptischen Kurven, erwarten wir somit, dass diese neuen Klassenpolynome kleinere Koeffizienten als die Koeffizienten der entsprechenden Igusa-Klassenpolynome besitzen, falls wir $N > 1$ haben.

Insgesamt erhalten wir den folgenden Algorithmus, welcher überprüft, ob die Werte $g_1(\tau), g_2(\tau), g_3(\tau)$ Klasseninvarianten sind. Im Falle einer positiven Antwort erhalten wir ein Klasseninvariantensystem $(g_1(\tau), g_2(\tau), g_3(\tau))$.

Algorithmus 6: Konstruktion des Klasseninvariantensystems

Eingabe: Ein System der arithmetischen Siegelschen Modulfunktionen $(g_1(\tau), g_2(\tau), g_3(\tau))$ der Stufe $(2N, 4N)$ und ein CM-Punkt $\tau \in \mathbb{H}_2$, der einer einfachen hauptpolarisierten abelschen Fläche (A, E) vom primitiven CM-Typ (K, Φ) mit dem Reflexivtyp (F, Ψ) entspricht.

Ausgabe: $(g_1(\tau), g_2(\tau), g_3(\tau))$ ist ein Klasseninvariantensystem oder nicht.

1. Überprüfe, ob $F(j_1(\tau)) \subseteq F(g_1(\tau))$ gilt. Falls JA gehe zu (2), falls NEIN gehe zu (8).
2. Überprüfe, ob $F(j_2(\tau)) \subseteq F(g_2(\tau))$ gilt. Falls JA gehe zu (3), falls NEIN gehe zu (8).
3. Überprüfe, ob $F(j_3(\tau)) \subseteq F(g_3(\tau))$ gilt. Falls JA gehe zu (4), falls NEIN gehe zu (8).

4. Berechne die Erzeuger $x_1, \cdots, x_k$ von $(\mathcal{O}/N\mathcal{O})^*$.
5. Bilde mittels $\bar{\xi}$ die Erzeuger in $U(4, \mathbb{Z}/N\mathbb{Z})$ ab.
6. Für $l = 1, \cdots, k$ überprüfe, ob $\bar{\xi}(x_l) \in \mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z})$ auf $g_i(\tau)$, $i = 1, 2, 3$, trivial operiert. Falls JA gehe zu (7), falls NEIN gehe zu (8).
7. Gebe '$(g_1(\tau), g_2(\tau), g_3(\tau))$ bildet ein Klasseninvariantensystem' aus.
8. Gebe '$(g_1(\tau), g_2(\tau), g_3(\tau))$ bildet kein Klasseninvariantensystem' aus.

Nach der Bemerkung 5.22 ist es hinreichend, die Bilder von $N_\Psi(\mathcal{L}_N/\mathrm{Tor}(K))$ zu untersuchen, um zu entscheiden, ob sie auf einem Wert $g(\tau)$ einer arithmetischen Siegelschen Modulfunktion g der Stufe $(2N, 4N)$ trivial operieren. Da wir im Allgemeinen die Untergruppe $N_\Psi(\mathcal{L}_N/\mathrm{Tor}(K))$ von $(\mathcal{O}/N\mathcal{O})^*$ nicht explizit beschreiben können, betrachten wir die reduzierte Abbildung

$$\bar{\xi} : (\mathcal{O}/N\mathcal{O})^* \to \mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z}),$$

die offenbar zusätzliche Bilder unter der Abbildung $\bar{\xi}$ in $U(4, \mathbb{Z}/N\mathbb{Z})$ besitzt.

Daher ist es möglich, dass der Algorithmus 6 '$(g_1(\tau), g_2(\tau), g_3(\tau))$ bildet kein Klasseninvariantensystem' ausgibt, im Falle, dass alle Bilder der Abbildung $\bar{\xi}$ von $N_\Psi(\mathcal{L}_N/\mathrm{Tor}(K))$ auf $g(\tau)$ trivial operieren, aber nicht alle Bilder von $(\mathcal{O}/N\mathcal{O})^*$ auf $g(\tau)$ trivial operieren. In diesem Fall gibt der Algorithmus 6 eine falsche Antwort, was die Suche nach einem geeigneten Klasseninvariantensystem erschwert.

5.6 Praktische Betrachtungen

Wir untersuchen in diesem Abschnitt die einzelnen Teile vom Algorithmus 6.

Die Modulfunktionen

Wir müssen mit einem System $(g_1(\tau), g_2(\tau), g_3(\tau))$ der Werte der arithmetischen Siegelschen Modulfunktionen anfangen, die den Anforderungen der Schritte (1), (2), (3) und (4) genügen. Wie im Falle der elliptischen Kurven sind die rationalen Funktionen $g = u/v$ der Quotienten der Thetanullwerte mit $j_i = u/v$, die die arithmetischen Siegelschen Modulfunktionen der Stufe $(2N, 4N)$ sind, die natürlichen Kandidaten eines Klasseninvariantensystems.

Die Gleichung 4.19 lehrt uns, dass wir eine Analogie der $\Delta-$Funktion in diesem Fall brauchen, deren Quotienten arithmetische Siegelsche Modulfunktionen der Stufe $(2N, 4N)$ sein sollten. Falls wir eine zusätzliche Eigenschaft haben, dass wir gewisse Wurzeln der Quotienten dieser zur $\Delta-$Funktion analogen Funktion erhalten, dann sind die Werte dieser Funktionen gute Kandidaten, die ein Klasseninvariantensystem liefern können. (Wir verweisen auf die Definition der Schläflischen Funktionen 4.13.)

Wir betrachten nun die im ersten Abschnitt gegebene Gleichung 1.24

$$\Delta(\tau) = 16\pi^{12}\theta_{00}(\tau)^8\theta_{01}(\tau)^8\theta_{10}(\tau)^8. \tag{5.30}$$

Dieses Produkt besteht im Wesentlichen aus dem Produkt der $8-$ten Potenzen eindimensionaler gerader Thetanullwerte. Wir definieren daher

$$\theta_{ev}(\tau) = \theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau) \tag{5.31}$$

für $\tau \in \mathbb{H}$. Nun können wir, wie in der Gleichung 5.31, das Produkt aller zehn zweidimensionalen geraden Thetanullwerte mit $\tau \in \mathbb{H}^2$ wie folgt definieren:

$$\theta_{ev}(\tau) = \prod_{i=1}^{10} \theta[a_i](\tau). \tag{5.32}$$

Aus der Gleichung von h_{10} aus dem erstem Kapitel folgt

$$h_{10}(\tau) = \theta_{ev}(\tau)^2. \tag{5.33}$$

Deshalb ist die Funktion h_{10} aus dem erste Kapitel, S. 19, eine natürliche Verallgemeinerung der $\Delta-$Funktion, die wir im Folgenden auch mit $\Delta(\tau) = h_{10}(\tau)$ bezeichnen, wobei $\tau \in \mathbb{H}_2$ ist.

Die Werten der zu den eindimensionalen Modulfunktionen anologen Quotienten der $\Delta-$Funktion sind damit natürliche Kandidaten eines Klasseninvariantensystems, falls sie arithmetische Siegelsche Modulfunktionen der Stufe $(2N, 4N)$ sind und den Anforderungen der Schritte (1), (2), (3) und (4) von Algorithmus 6 genügen.

Um geeignete Wurzeln der Quotienten der $\Delta-$Funktion zu erhalten, betrachten wir die Gleichung

$$\Delta\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \omega_2^{-12}\Delta(\tau), \tag{5.34}$$

die wir im Satz 4.24 bewiesen haben. Wir wollen eine verallgemeinerte $\eta-$Funktion für die Dimension zwei definieren:

Für die $2 \times 2-$Matrizen ω_1 und ω_2 mit $\Omega = (\omega_1, \omega_2)$, die das Gitter Λ mit $(A, E) = (\mathbb{C}^2/\Lambda, E)$ erzeugen, haben wir

$$E(\Omega x, \Omega y) = x^t J y \text{ für } x, y \in \mathbb{R}^4,$$
$$\Lambda = \Omega \begin{pmatrix} 1_2 & 0 \\ 0 & D \end{pmatrix} \mathbb{Z}^4.$$

wie wir im vierten Abschnitt erklärt haben. Dann gilt für den CM-Punkt $\tau = \omega_1 \omega_2^{-1}$ stets die folgende Gleichung, siehe [ShGo97], S. 778:

$$\Delta \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \det(\omega_2)^{-10} \Delta(\tau). \tag{5.35}$$

Inspiriert von den Gleichungen 5.34, 5.35 und der Gleichung

$$\frac{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}{2} = \eta(\tau)^3,$$

die wir im Beweis des Satzes 4.15 gezeigt haben, definieren wir für $\tau \in \mathbb{H}_2$ die folgende Funktion, die die analoge verallgemeinerte Funktion der $\eta-$Funktion der Dimension zwei ist:

$$\eta(\tau) = \sqrt[5]{\theta_{ev}(\tau)}. \tag{5.36}$$

Daher sind die Quotienten der $\eta-$Funktion 5.36 die natürlichen Kandidaten eines Klasseninvariantensystems, falls sie arithmetische Siegelsche Modulfunktionen der Stufe $(2N, 4N)$ sind, und den Anforderungen der Schritte (1), (2) und (3) von Algorithmus 6 genügen.

Die explizite Abbildung

Wir müssen im Schritt (5) vom Algorithmus 6 die Erzeuger der Gruppe $(\mathcal{O}/N\mathcal{O})^*$ berechnen. Nach dem Chinesischen Restsatz haben wir

$$(\mathcal{O}/N\mathcal{O})^* \cong \prod_{i=1}^{r} (\mathcal{O}/p_i^{l_i}\mathcal{O})^*, \tag{5.37}$$

wobei $N = \prod_{i=1}^{r} p_i^{l_i}$ die Primfaktorzerlegung von N ist.

Cohen hat einen Algorithmus entwickelt, der die Erzeuger von $(\mathcal{O}/p_i^i\mathcal{O})^*$ berechnet, siehe [Coh00], S. 188, Algorithm 4.2.2. Mit diesem Algorithmus können wir stets die Erzeuger $x_1, \cdots, x_k$ von $(\mathcal{O}/N\mathcal{O})^*$ mittels der Isomorphie 5.37 berechnen.

Mit Hilfe der reduzierten Abbildung $\bar{\xi}$ erhalten wir nach dem Satz 5.9 schließlich eine kleine Untermenge der Gruppe $U(4, \mathbb{Z}/N\mathbb{Z})$, die aus den Matrizen

$$R \in \mathrm{GL}(4, \mathbb{Z}/N\mathbb{Z})/\{\pm 1_4\} \text{ besteht, für die ein } n \in \mathbb{N} \text{ existiert mit}$$

$$\mathrm{ggT}(n, N) = 1, \text{ und}$$

$$n \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv R^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} R \bmod N.$$

Abschließend wenden wir den letzten Schritt vom Algorithmus 6 an, um entscheiden zu können, ob wir ein Klasseninvariantensystem erhalten haben.

Die wesentliche Schwierigkeit besteht darin, die geeigneten CM-Punkte $\tau \in \mathbb{H}_2$ mit der Eigenschaft zu finden, dass die Bilder von $\bar{\xi}$ auf dem System $(g_1(\tau), g_2(\tau), g_3(\tau))$ trivial operieren.

Kapitel 6

Beispiele

In diesem Kapitel werden wir Beispiele der Klassenpolynome angeben, die wir nach dem Satz 4.16 mittels der Quotienten der Thetanullwerte konstruiert haben. Außerdem werden die Beispiele der verbesserten Klasseninvarianten nach dem Satz 4.28 angegeben. Abschließend werden wir die obere Schranken für die Indizes der Untergruppen in der Einheitengruppe angeben, die durch die Klasseneinheiten und die Untergruppen der Torsionseinheiten wie im Algorithmus 5 konstruiert sind.

Diese Beispiele werden mit Hilfe der Computeralgebra Systemen KANT/KASH ([Pohst]) und MAGMA ([MAGMA]) implementiert.

6.1 Klasseninvarianten

In diesem Abschnitt werden wir für gegebene Diskriminante $D = -4m$ die Weberklassenpolynome wie im Satz 4.16 angeben, die mittels der Quotienten der Thetanullwerte konstruiert werden.

Der Fall $m \equiv 1 \bmod 8$

- $D = -4(8+1) = -36$:
  $W_{-36}(x) = x^2 - 4x + 1.$
- $D = -4(8 \cdot 2 + 1) = -68$:
  $W_{-68}(x) = x^4 - x^3 - 2x^2 - x + 1.$
- $D = -4(8 \cdot 5 + 1) = -164$:
  $W_{-164}(x) = x^8 - 5x^7 + 7x^6 - 12x^5 + 14x^4 - 12x^3 + 7x^2 - 5x + 1.$
- $D = -4(8 \cdot 17 + 1) = -548$:

$W_{-548}(x) = x^8-21x^7+103x^6-236x^5+302x^4-236x^3+103x^2-21x+1.$

- $D = -4(8 \cdot 38 + 1) = -1220$:

  $W_{-1220}(x) = x^{16}-60x^{15}-540x^{14}-2340x^{13}-5997x^{12}-11800x^{11}-18780x^{10}-23960x^9-26712x^8-23960x^7-18780x^6-11800x^5-5997x^4-2340x^3-540x^2-60x+1.$

- $D = -4(8 \cdot 103 + 1) = -3300$:

  $W_{-3300}(x) = x^{24}-2216341500x^{23}-1420926197800x^{22}+15432002107500x^{21}-101874159288214x^{20}-122366073946020x^{19}+682118853627000x^{18}-555206230915500x^{17}-230074208623025x^{16}+630650404619880x^{15}-127643499555920x^{14}-1580010485061000x^{13}+2781233380405900x^{12}-1580010485061000x^{11}-127643499555920x^{10}+630650404619880x^9-230074208623025x^8-555206230915500x^7+682118853627000x^6-122366073946020x^5-101874159288214x^4+15432002107500x^3-1420926197800x^2-2216341500x+1.$

- $D = -4(8 \cdot 247 + 1) = -7908$:

  $W_{-7908}(x) = x^{36}-518419280722370x^{35}-208424233716637741 50x^{34}-77878848955222985837 0x^{33}-65694435534630946013191x^{32}-87347541943332665387 0960x^{31}-77359986652275086626452 00x^{30}-31455243002787053984846960x^{29}-31773852733219851001872364x^{28}+11725871836456732354612 5640x^{27}-20774622679634650318778 8200x^{26}-39108752787085524478418360x^{25}-48478525960080174743317711 6x^{24}-53323060709738330082864872 0x^{23}-49643195032970415808773240 0x^{22}-15399722436211663594813527 20x^{21}-32689393241302129446122618 74x^{20}-43373098066003694815058459 00x^{19}-62297073567437841027976305 00x^{18}-43373098066003694815058459 00x^{17}-32689393241302129446122618 74x^{16}-15399722436211663594813527 20x^{15}-49643195032970415808773240 0x^{14}-53323060709738330082864872 0x^{13}-48478525960080174743317711 6x^{12}-39108752787085524478418360x^{11}-20774622679634650318778 8200x^{10}+11725871836456732354612 5640x^9-31773852733219851001872364x^8-31455243002787053984846960x^7-77359986652275086626452 00x^6-87347541943332665387 0960x^5-65694435534630946013191x^4-77878848955222985837 0x^3-20842423371663774150x^2-518419280722370x+1.$

- $D = -4(8 \cdot 1303 + 1) = --41700$:

  $W_{-41700}(x) = x^{72}-23721762625445845201846527744008500x^{71}-34079975910374282250111121450179450659885090 00x^{70}-46180336026150391684289106859723422144725957350 0x^{69}-61582404507096785755983328039050318735317338004464 2x^{68}+21665426330516245202240350227598266573860927536097 8500x^{67}-34095326420008799105744963293391866743923029759956813000x^{66}+11010423440339739184444687101740394951131569345966441755 00x^{65}-42167702699272616552764391382853486368922444365154521 9687x^{64}+$

  $\ldots$

  $22646686744177815192843060159007068460351097181656120502241600x^{10}+20873424295284130038610482729725829008100223065183066146800 0x^9-42167702699272616552764391382853486368922444365154521 9687x^8$

$+ 1101042344033973918444468710174039495113156934596644175500x^7 -$
$34095326420008799105744963293391866743923029759956813000x^6 +$
$21665426330516245202240350227598266573860927536097850 0x^5 -$
$61582404507096785755983328039050318735317338004464 2x^4 -$
$46180336026150391684289106859723422144725957350 0x^3 -$
$34079975910374282250111121450179450659885090 00x^2 -$
$23721762625445845201846527744008500x + 1.$

- $D = -4(831447 + 1) = -1006308$:

$W_{-1006308}(x) = x^{240} -$
$42910048205143797251929550029384226217862283760601433177274446228433324772339906314192$
$00598030674755794761932859519252282852235628661057708096146721308293132957176707969 20x^{239} +$
$15502475010870192710640585892493510548544418000285700212140582941535458787827931990 6737$
$29141972961797396441135489161502626125918579777411859976262686195350145473469329849 3454$
$4989150635150400x^2 - 42910048205143797251929550029384226217862283760601433177274446 22$
$84333247723399063141920059803067475579476193285951925228285223562866105770809614672130$
$829313295717670796920x + 1.$

- $D = -4(8 \cdot 1378567 + 1) = -44114148$:

$W_{-44114148}(x) = x^{1376} + \cdots +$
$19771517784610070596317699525513118627303957222200427239350049564657440394129393279826$
$29517267664135739382685301914414472646587700895616297323888427133270261106630054112954$
$03937829588833696373850374674302712768008569576042910729012300371624478802160852861710$
$16489004272024687880894512706168499475206416218152567167755996409642093387299842529221$
$76911600382168057802780362173630219758942964228342182021807330133045836299675530058904$
$40903090952229295240022905990981259170107607946296120602902657392620677291269148676211$
$57887331264708652502593346270664531385098675874322286046508392364956989920411637611341$
$04456568816918547579454815020144384563700774102479272659618061398020877415672833465640$
$75055608078703660728772337653156535555778754681374381520333836983441373541274878540610$
$11196100163127729026126836533158532713035232537729583098815380669276744346859485003963$
$71176811749371653612843735932138607963369883077293319174358130078177424196661523221939$
$91163411751547047982450830048177956633302764509027397237676982003094661293893860937136$
$55767552724357993217505972674481694273046599302630651393946513997834829108046280541275$
$347501316406720x + 1.$

Der Fall $m \equiv 5 \bmod 8$

- $D = -4(8 + 5) = -52$:
  $W_{-52}(x) = x^2 - 3x - 1.$
- $D = -4(8 \cdot 2 + 5) = -84$:
  $W_{-84}(x) = x^4 - 168x^3 + 142x^2 + 168x + 1.$

- $D = -4(8 \cdot 8 + 5) = -276$:
  $W_{-276}(x) = x^8 - 58032x^7 + 596444x^6 - 468720x^5 + 1316166x^4 + 468720x^3 + 596444x^2 + 58032x + 1.$

- $D = -4(8 \cdot 36 + 5) = -1172$:
  $W_{-1172}(x) = x^{18} - 3881x^{17} - 84475x^{16} - 610566x^{15} - 1261181x^{14} - 370065x^{13} + 761469x^{12} - 903894x^{11} - 423730x^{10} + 2486316x^9 + 423730x^8 - 903894x^7 - 761469x^6 - 370065x^5 + 1261181x^4 - 610566x^3 + 84475x^2 - 3881x - 1.$

- $D = -4(8 \cdot 103 + 5) = -3316$:
  $W_{-3316}(x) = x^{22} - 1762935x^{21} - 20890163x^{20} - 81110082x^{19} + 320016313x^{18} - 3356535321x^{17} - 884146755x^{16} - 13875732036x^{15} - 315027759x^{14} - 26945965971x^{13} - 3356933115x^{12} - 32926936158x^{11} + 3356933115x^{10} - 26945965971x^9 + 315027759x^8 - 13875732036x^7 + 884146755x^6 - 3356535321x^5 - 320016313x^4 - 81110082x^3 + 20890163x^2 - 1762935x - 1.$

- $D = -4(8 \cdot 245 + 5) = -7860$:

$$W_{-7860}(x) = x^{40} - 217353267589383339688880133168x^{39} + 3267403861316155357547273854312599952 12x^{38} - 4664021250582593132170795168521817182133233 6x^{37} + 1450071851929863507062999698327844252313255790 06x^{36} - 2926350009907426513803481484393439232460289684738 72x^{35} - 3808310789597459521060648644196078849450768473765 4548x^{34} - 1092572602427655489065104272330728655309807736989 634128x^{33} + 1688338460954830681741394966640262120292680782091157322 9x^{32} + 3051700216865800352335481120324613311980374082934280 6336x^{31} + 1757332500829883051518685679780075067086539800394268 99696x^{30} + 1424348274016084995702921044533445396264442945063014457408x^{29} + 6707600139911165882350866863039818677296246293071547692648x^{28} + 2556719356010430687320586849089601503223787753387087401081 6x^{27} + 5232114818020253816343933196601686451129243681590663358 9424x^{26} - 4864908935993962517857254565701347160539044432081945899072x^{25} - 1230190803826682101174071087311724043765391258991945553044 30x^{24} - 3755298663369929229574561258398632086682113052109105510 2880x^{23} + 1363797030805670841965688589263033396855327159006853190 20840x^{22} + 3538525830434762762591432803282069876912598814559678351 5360x^{21} - 1144567692298769061504308310238868765952028569983296633796 60x^{20} - 3538525830434762762591432803282069876912598814559678351 5360x^{19} + 1363797030805670841965688589263033396855327159006853190 20840x^{18} + 3755298663369929229574561258398632086682113052109105510 2880x^{17} - 1230190803826682101174071087311724043765391258991945553044 30x^{16} +$$

$$4864908935993962517857254565701347160539044432081945899072x^{15} +$$
$$5232114818020253816343933196601686451129243681590663358942 4x^{14} -$$
$$2556719356010430687320586849089601503223787753387087401081 6x^{13} +$$
$$6707600139911165882350866863039818677296246293071547692648x^{12} -$$
$$1424348274016084995702921044533445396264442945063014457408x^{11} +$$
$$1757332500829883051518685679780075067086539800394268996 96x^{10} -$$
$$3051700216865800352335481120324613311980374082934280633 6x^9 +$$
$$1688338460954830681741394966640262120292680782091157322 9x^8 +$$
$$1092572602427655489065104272330728655309807736989634128x^7 -$$
$$3808310789597459521060648641960788494507684737654548x^6 +$$
$$2926350009907426513803481484393439232460289684738 72x^5 +$$
$$1450071851929863507062999698327844252313255790 06x^4 +$$
$$4664021250582593132170795168521817182133233 6x^3 +$$
$$3267403861316155357547273854312599952 12x^2 +$$
$$2173532675893833396888801331 68x + 1.$$

- $D = -4(8 \cdot 1371 + 5) = -43892$:

$$W_{-43892}(x) = x^{102} - 3305080558681906396173 13x^{101} +$$
$$2205507317815301424608872811995 5x^{100} -$$
$$6270001708615340711681045727555555585580x^{99} +$$
$$1739198024131330534004833128743607949686 70x^{98} +$$
$$2867709974196635390739776051215600288719582x^{97} -$$
$$\dots$$
$$3319947086487670288108920388238284665204536974763 55x^9 +$$
$$1237302961327793685490326094292328093482142573429 5x^8 -$$
$$2623732558166678876908148327635343545628695639 38x^7 +$$
$$1622410979517041923113880424662959055287376360x^6 +$$
$$2867709974196635390739776051215600288719582x^5 -$$
$$1739198024131330534004833128743607949686 70x^4 -$$
$$6270001708615340711681045727555555585580x^3 -$$
$$2205507317815301424608872811995 5x^2 -$$
$$3305080558681906396173 13x - 1.$$

- $D = -4(8 \cdot 756986 + 5) = -24223572$:

$$W_{-24223572}(x) = x^{1136} + \cdots +$$
$$7498432554285378497971339763769939815520724868704336264109773416019334491636816111320454234669$$
$$3219922883361952306544589065560998991311128169398303457003990202233343948947192253274290474 27$$
$$0246392409383299238289099517174223836310318435205653949444935724034177086564652536570772027 78$$
$$3642356843517753272230537340544171512208987545710332750547820278557848839007559003643162368 90$$
$$7437049135034162635909187706746243497235766802939420421213723529361420071671923435448873207 50$$
$$3442054522964812324476374181746305377937064902329630347920022275356350599495916385484668164 57$$
$$5267062944584862406318794068774827134349922634759143906502578321886318858617200935424264901 61$$
$$6144142899341047902320176822024620247762694230307505396168535865586765400907262678869619535 7$$
$$5594691090411987583523088857045928685776230724637762815929050967725154218772461978739651358 98$$

$$623921053561600055283246329103370045685591962580504505572478698208630297044451546114308788426$$
$$058978439311802057005744079807802137447388440992876775482666033570616005708045025689943568368$$
$$437814841141096391901525626709266842099328361533856536844817379172359000590318281263969235603$$
$$992221096121166561827394783760804668811336813783056709920103075277355140421506059281393289804$$
$$478198628722468801582878331720115743204108408764493425435917525519274718750932743681092226004$$
$$777242642656541140166241745075947680038123924336132204318250099661041137337241558484392017003$$
$$385299789134883290366707696808764519228065706071727199601986131243650888588063425873824205500$$
$$435346714078730152916333513837866738346714418633435806602651813908566257287061491518706623020$$
$$404211430840939857455006781659832203598677947965086695646939237740793105455962276639022544159$$
$$088800x + 1.$$

Der Fall $m \equiv 7 \bmod 8$

- $D = -4(8 + 7) = -60$:
  $W_{-60}(x) = x^2 - x - 1.$
- $D = -4(8 \cdot 2 + 7) = -92$:
  $W_{-92}(x) = x^3 - x - 1.$
- $D = -4(8 \cdot 8 + 7) = -284$:
  $W_{-284}(x) = x^7 - 2x^6 - x^5 + x^4 + x^3 + x^2 - x - 1.$
- $D = -4(8 \cdot 891284 + 7) = -28521116$:

  $W_{-28521116}(x) = x^{2912} + \cdots +$
  $105150172257429112468583143080185177188010328325469005827828356802283214413486256995067721702$
  $68474120993112392646788511036958105x^5+709843448095929513067960823900443292866767663888755 5$
  $185885911291365018617733094688864471389616860287131383898014 30x^4 +$
  $642674704388513552339388928898477095554392318231585981014267875527886861270840305245182226$
  $58736x^3 + 795746365650622010910588117912502563063746293123834685756891662584005762664 8x^2 -$
  $174871628837414077194805239406811979 84x + 1.$

Der Fall $m \equiv 2 \bmod 4$

- $D = -4(4 + 2) = -24$:
  $W_{-24}(x) = x^2 - 2x - 1.$
- $D = -4(4 \cdot 21 + 2) = -344$:
  $W_{-344}(x) = x^{10} - 8x^9 + 2x^8 - 18x^7 + 9x^6 - 4x^5 - 9x^4 - 18x^3 - 2x^2 - 8x - 1.$
- $D = -4(4 \cdot 1023751 + 2) = -16380024$:

  $W_{-16380024}(x) = x^{1816} + \cdots +$
  $617426757073178346488847543215877034331675282475340869518759847574583259966270405815761854286$
  $150064501435653570179478268636028371649248938611274360190836226700734881845462756189102600392$

$$0168971229566928459040863575665754698622536853488471544369286030612062166871624683661622558937590515033965012058932054344558018410744154769967179888204910601842039783083661936811014066260686798981873664123133736231287318777894943067719738561583725909272325349604563211084831706978978532628197134573601851877980202648079346237850306879502355599441782758464899612443028958231204496683183537513128813929252985853203578865146364608483812394772683205301221890862580175589392747045085835286313641474965695866080x + 1.$$

Der Fall $m \equiv 4 \bmod 16$

- $D = -4(16 + 4) = -80$:
  $W_{-80}(x) = x^4 - 2x^3 - 5x^2 - 4x - 1.$
- $D = -4(16 \cdot 17 + 4) = -1104$:
  $W_{-1104}(x) = x^{16} - 9521956360x^{15} - 2422629573672x^{14} + 26219327498664x^{13} -$
  $84375886568580x^{12} - 393712002485544x^{11} - 3254944618368 88x^{10} +$
  $187439192911816x^9 - 154132266526074x^8 + 47748165387496x^7 -$
  $15489293319448x^6 + 2215927447800x^5 - 332337094020x^4 +$
  $11432970312x^3 - 61341672x^2 + 163736x + 1.$
- $D = -4(16 \cdot 214967 + 4) = -13757904$:

$$W_{-13757904}(x) = x^{2256} + \cdots +$$
$$1366341918983399219537248730095677627425377649488946893805635161465719399110248167186825980541736852946196185055997652237854812120625739210402936958640316268735951033744155117304524197211202262576090450692111582393043416176779309850770129503084155569394774797083816269171479438257488516599590763097620619890226987646016537897420908185267297575965688112326344087920975405634433565097118987663872230384134037382525019748617923941276080329011715984473189354086248680177437503027135436712560649410000448332660543927461832840087388849263141148332943577123946092021917859620170791535005492366167234237810127339383189843577546027804408384 40x + 1.$$

Der Fall $m \equiv 11 \bmod 24$

- $D = -4(24 + 11) = -140$:
  $W_{-140}(x) = x^6 - 2x^5 - 2x^4 + 4x^3 - 4x + 2^2.$
- $D = -4(24 \cdot 13 + 11) = -1292$:
  $W_{-1292}(x) = x^{12} - 8x^{11} - 28x^{10} + 12x^9 + 56x^8 - 72x^7 + 16x^6 + 144x^5 -$
  $80x^4 - 96x^3 + 32x^2 + 32x + 2^4.$
- $D = -4(24 \cdot 307 + 11) = -29516$:
  $W_{-29516}(x) = x^{84} - 76368x^{83} - 6478884x^82 - 166900768x^{81} -$
  $560587544x^{80} + 3962192744x^{79} + 24019103736x^{78} -$

$\cdots +$
$9314173452288x^2 + 84288733184x + 2^{28}$.

- $D = -4(24 \cdot 115752 + 11) = -11112236$:

$W_{-11112236}(x) = x^{1674} + \cdots +$
$120449668318353751312881392925298585320357886514636460848381239477268320530122189086258017558$
$267215429217335692049155997902389091259493210432167505238595406628761548536450421876409817048$
$077860912420798499755006996413063938901730677919645275867639168565460223337858806818003141887$
$866141355961789829452606951261223981117551827440517196319039045533273130270 72x^2 -$
$619534187684350972636514715681140735223217154689791206169434306329251819212714839381961768887$
$181205119822005977880971952241346372973064315141521686449873139869686263430258663749997706646$
$210555563599920183303680819 20x + 2^{558}$.

Der Fall $m \equiv 19 \bmod 24$

- $D = -4(24 + 19) = -172$:
  $W_{-172}(x) = x^3 - 2x^2 - 2$.

- $D = -4(24 \cdot 19 + 19) = -1900$:
  $W_{-1900}(x) = x^{12} - 20x^{11} + 52x^{10} - 108x^9 + 124x^8 - 152x^7 + 152x^6 - 176x^5 + 160x^4 - 48x^3 + 16x^2 + 64x + 2^4$.

- $D = -4(24 \cdot 287 + 19) = -27628$:
  $W_{-27628}(x) = x^{51} - 53036x^{50} - 374352x^{49} - 1220446x^{48} - 2397560x^{47} - 5023592x^{46} + 11340104x^{45} +$
  $\cdots$
  $8860663808x^3 - 3582984192x^2 + 42205184x - 2^{17}$.

- $D = -4(24 \cdot 531519 + 19) = -51025900$:

$W_{-51025900}(x) = x^{1728} + \cdots +$
$114005983394606252856780513507410839763538053784227139906320328444251636651060649419159889589$
$702439991328373602832826840926149792738721872689346892222107334658882321665309914151444304184$
$240086329421460445386878336889180481424306065863877287449239730647513758542831776989970432x+$
2^{576}.

Der Fall $m = 16a + 12$ **mit** $a \equiv 0, 1, 5 \bmod 6$

- $D = -4(16(6 \cdot 1) + 12) = -432$:
  $W_{-432}(x) = x^6 - 543090x^5 - 482106x^4 - 215840x^3 - 55788x^2 - 9960x - 2^3$.

- $D = -4(16(6 \cdot 1 + 1) + 12) = -496$:
  $W_{-496}(x) = x^6 - 122x^5 + 194x^4 - 180x^3 + 112x^2 - 112x + 2^3$.

- $D = -4(16(6 \cdot 1 + 5) + 12) = -752$:

  $W_{-752}(x) = x^{10} - 460x^9 - 1752x^8 - 9880x^7 - 20316x^6 - 23800x^5 - 19552x^4 - 12080x^3 - 4096x^2 - 640x + 2^5$.

- $D = -4(16(6 \cdot 43245 + 0) + 12) = -16606128$:

  $W_{-16606128}(x) = x^{1104} + \cdots +$
  509030210854166184241253877109678932751499860458041801744012848418856398772554492578049931996
  069683270792909400034625694543439525759708197552651511543606336922226660041618154668961775670
  515014161401350908918711048191163904381364640001185404704795922073903953882151179655907817251
  438857517546108314818184258008194788277732314066717697258059928454477105915826530156919198764
  784458314051447967343533095748620016027833348219068388239245142290161615850122052300836140064
  459722125516891130610518715136050816871572769365834458100645670024278163532493037292823230480
  760524284162469048529719706405301295020717036228717317191819819767378940350234025128650607673
  004966525587605365970474708831415817692802817098697800772279293124504907688946536819197127919
  667282275160097585639862430719880674993138503231506387920648031245623954535459771764877843009
  801259961330710955950080$x + 2^{552}$.

- $D = -4(16(6 \cdot 153192 + 1) + 12) = -58825840$:

  $W_{-58825840}(x) = x^{2736} + \cdots +$
  477663272286852766263250069864514966988319070894381151495530399758061178125993300282927660896
  548099383477820899937584083726556420269307611386026187347553708756763682854768262282234186454
  929735485835630997346956987261888915064717102471957889104669922241245141999822792288240792743
  788233194450911627444822890370393593707333699415739369954602084013867734503467495649563261435
  847326389124171808096715333397549107944348041129445803341791774887555170018630191966600245368
  537455116464906950141925861207900214819940691184164146066430213737019034193679627962238187977
  263763672347144390993934073564142019022744628349100541946147088109224905517719809497494699299
  897184267357361776374978258487438685202592637934573147453056152581430968311850142556772304348
  979839820003805205070342711881206751499856768394412040633376629360806933615035549141403057048
  93447929856$x + 2^{1368}$.

- $D = -4(16(6 \cdot 90125 + 5) + 12) = -34608368$:

  $W_{-34608368}(x) = x^{1664} + \cdots +$
  553111234404668346794447669191223804174068966622661542395578217748742566722120133504108942152
  388390163202830652736536591847690026631201827678971936136754828430946780885759030253391683821
  268234227472235069423953473412785996023858544115557576833284231252046356002830575850952313208
  102845693530830648077642790386512908868261724253139451833464702687120388794410820649912285790
  009187063129287235237434774146057155340137546300463606159931054658238091022417793039910652798
  578289897874149501171270136909383376600699304230625505596637127097351122749894667356740108718
  567107712715293908497596416$x + 2^{832}$.

Der Fall $m = 16a + 12$ **mit** $a \equiv 2, 4 \bmod 6$

- $D = -4(16(6 \cdot 2) + 12) = -560$:

$W_{-560}(x) = x^{12} - 180x^{11} + 1160x^{10} - 2620x^9 + 1740x^8 + 1260x^7 - 3504x^6 + 3680x^5 - 2360x^4 + 1000x^3 - 280x^2 + 40x + 2^2$.

- $D = -4(16(6 \cdot 4) + 12) = -688$:
  $W_{-688}(x) = x^6 - 340x^5 + 200x^4 - 70x^3 + 80x^2 - 40x - 2$.
- $D = -4(16(6 \cdot 12 + 2) + 12) = -4784$:
  $W_{-4784}(x) = x^{48} - 25855016x^{47} - 1648271584x^{46} - 586739518648x^{45} + + \cdots +$
  $- 4844421120x^4 + 684366848x^3 - 47669248x^2 + 1540096x + 2^8$.
- $D = -4(16(6 \cdot 21 + 4) = - - 8368$:
  $W_{-8368}(x) = x^{30} - 8895776032x^{29} - 211988625088x^{28} - 1924006079878x^{27} + + \cdots +$
  $190277728x^3 + 32118464x^2 - 3588928x - 2^5$.
- $D = -4(16(6 \cdot 38562 + 2) + 12)) = -14807984$:

$W_{-14807984}(x) = x^{1890} + \cdots +$
272547799193369770249843757024345932659750265194693507537665374853249428368868046313656588655
040501228528597663042632942526024339085738642765510659631509193228884111839566322382801178602
325592318092914388482699477938636101681790724854218075423619986066939759085740294571902956038
9184292836259141970863842630251315 2x − 2^315.

- $D = -4(16(6 \cdot 81025 + 4) + 12)) = -31113904$:

$W_{-31113904}(x) = x^{2376} + \cdots +$
144627298530652657288921349455234442367454106324163468671991883126036861095472218406767228257
423275178324214541574255123226841636323059333613336019510600519749686947892937846947997908851
956224069939918443877403909882091372013854230915808864172849929679943433786340613405381862822
026309394757772057200632042193698531643474707531681653853629965019539410565019962576209772125 2
007614756518447000483254423971856102181320837086410135043257139 2x + 2^396.

6.2 Neue Klasseneinheiten

Wir werden in diesem Abschnitt die mittels des Satzes 4.28, 1.(a) und 2.(b) verbesserten Klassenpolynome der neuen Klasseninvarianten angeben, die nach dem Satz 4.16 mittels der Quotienten der Thetanullwerte konstruiert werden. Um die Koeffizienten dieser neuen Polynome mit den entsprechenden Weberklassenpolynomen vergleichen zu können, geben wir die Weberklassenpolynome in den Beispielen auch an.

Am Ende dieses Abschnitts stellen wir zwei Tabellen vor, die zu der gegebenen Diskriminante D den Quotienten der größten Beträge der Koeffizienten der neuen Klassenpolynome und der Weberklassenpolynome vergleichen.

Der Fall $m \equiv 3 \bmod 24$

- $D = -4(24+3) = -108$:

  $W_{-108}(x) = x^3 - 6x^2 - 12x - 8,$

  $\widetilde{W}_{-108}(x) = x^3 - 3x^2 - 3x - 1.$

- $D = -4(24 \cdot 3 + 3) = -300$:

  $W_{-300}(x) = x^6 - 32x^5 + 60x^4 + 240x^2 + 128x + 64,$

  $\widetilde{W}_{-300}(x) = x^6 - 16x^5 + 15x^4 + 15x^2 + 4x + 1.$

- $D = -4(24 \cdot 27 + 3) = -2604$:

  $W_{-2604}(x) = x^{24} - 22480x^{23} + 394144x^{22} + 6141728x^{21} +$
  $21897312x^{20} - 118225664x^{19} - 365260544x^{18} +$
  $86675968x^{17} - 1274671360x^{16} - 2554568704x^{15} +$
  $7379943424x^{14} - 4408459264x^{13} - 4044079104x^{12} +$
  $46980530176x^{11} - 62486872064x^{10} + 30277894144x^9 +$
  $145046306816x^8 - 248412897280x^7 + 400335831040x^6 -$
  $254801870848x^5 + 224737099776x^4 - 36624662528x^3 +$
  $46321893376x^2 + 973078528x + 16777216,$

  $\widetilde{W}_{-2604}(x) = x^{24} - 11240x^{23} + 98536x^{22} + 767716x^{21} + 1368582x^{20} -$
  $3694552x^{19} - 5707196x^{18} + 677156x^{17} - 4979185x^{16} - 4989392x^{15} +$
  $7206976x^{14} - 2152568x^{13} - 987324x^{12} + 5734928x^{11} - 3813896x^{10} +$
  $924008x^9 + 2213231x^8 - 1895240x^7 + 1527160x^6 - 485996x^5 +$
  $214326x^4 - 17464x^3 + 11044x^2 + 116x + 1.$

- $D = -4(24 \cdot 71 + 3) = -6828$:

  $W_{-6828}(x) = x^{30} - 11125128x^{29} + 2224856348x^{28} + 55651302016x^{27} +$
  $461320536848x^{26} + 921130310400x^{25} - 2593045062208x^{24} -$
  $838537973760x^{23} + 48348753437952x^{22} + 112987683063808x^{21} +$
  $376518787779584x^{20} + 1175574943727616x^{19} + 2977647233028096x^{18} +$
  $7427572669480960x^{17} + 15503544159354880x^{16} + 30014020194926592x^{15} +$
  $48467269256413184x^{14} + 75333799118372864x^{13} + 99304313885818880x^{12} +$
  $109346366412554240x^{11} + 134246376257093632x^{10} + 76561183380865024x^9 +$
  $129294010530398208x^8 + 19871624241086464x^7 + 9986293030400819 2x^6 +$
  $8960933732810752x^5 + 44011600469819392x^4 - 2571583751192576x^3 +$
  $1495578210992128x^2 - 1408749273088x + 1073741824,$

  $\widetilde{W}_{-6828}(x) = x^{30} - 5562564x^{29} + 556214087x^{28} + 6956412752x^{27} +$
  $28832533553x^{26} + 28785322200x^{25} - 40516329097x^{24} - 6551077920x^{23} +$
  $188862318117x^{22} + 220679068484x^{21} + 367694128691x^{20} + 574011202992x^{19} +$
  $726964656501x^{18} + 906686116880x^{17} + 946261240195x^{16} + 915955206144x^{15} +$
  $739551838019x^{14} + 574751275012x^{13} + 378815894645x^{12} + 208561642480x^{11} +$
  $128027321107x^{10} + 36507217112x^9 + 30826094277x^8 + 2368882208x^7 +$

$5952294487x^6 + 267056636x^5 + 655823953x^4 - 19159792x^3 + 5571463x^2 - 2624x + 1.$

- $D = -4(24 \cdot 411371 + 3) = -39491628$:

$W_{-39491628}(x) = x^{1728} + \cdots +$
517065119393952923019770729453449721046148273534772636476424926954431038265800317193454624454
247870753483168561054900478331037431757368284400197738478282148634264869619001948272630849071
409647364754274241693290074112525848209982265018447999186748281867026871686850243923698000458
157145311868175069995459853444422092123635074002190872388172171018329603683737655274624100129
706131453502201631440631381508987473773840495592258150126985267201650070380436823184753283962
723086188603849672974121490554819424492759621386255780584800987697750519957791442150553483803
334356600309186684086497599923495793156153603246093319100656622072718980213050589878858928823
045315423300071041133722841470575484164564153918618011249312549565426095391221514032983089503
655643624659115371126493167791089879644897 28x + 2^{1728},$

$\widetilde{W}_{-39491628}(x) = x^{1728} + \cdots +$
683506627634567185467910601988687218251237974450481260991873328476812105437934665037421855463
103357870040560171267950799281727658153709115519341044736510094982306975748541858543102837179
733934555563206532816028634206436852811232886724732321756057055277357535536182012 6x + 1.$

- $D = -4(24 \cdot 654214 + 3) = -62804556$:

$W_{-62804556}(x) = x^{3540} + \cdots +$
477926508418243493885213660921776525875197340988245607402706974605327485066753319271263531748
201783632953148531538286231393282296646311296865561191961320493632831907360683159029421446799
510937621488991819380609674531874529866816457036354700699041590756521247360526540834080523913
562936079707614391730617347963639849819373004140924787881103196689838196575483433976376510992
315820488509092226470358532451994663973831902650279332236486990773614930421230207882706835783
222480125961210896723324693929107206437067514160205383932374563922478426101051969738804910195
125529858530324302630687873760664213264565930422447323516298040767912284193234827201281340207
057193766560870375821612779890058037444279739699941729270143160131528042795735533916334932954
337208494032464109698701279712571558670291827934679119206898272619895263434299643888114189865
436618283468467116196410184044684566569509897671319767801762947013559020827800887092486720598
133644472572080326272516358137622353262005536918449228232372640706571412468910284376982799591
672157692205963356499528081708601295570260486017732786831491616907329642968855198574850414322
185079948062449801048718736491384732392398115910908803944902029619323817311471058519249916425
810127858460159304122010988770964498419911944998423526979813501657767815654300155175271497962
447424137166758830698778259623055099617068601190904271524889028076594676428947425191208936982
28879360x + 2^{3540},$

$\widetilde{W}_{-62804556}(x) = x^{3540} + \cdots +$
215877045023218448274401692322740584605802340522039555909848311050854015758034495521157999883
018163974989405818550628068435287649084287241887900732995132367917806359313533724118159081088
889112303601123349006967719617699603766707639431942375023716913175992755982188535069724678012
984822015544172859486913655880526044560780070769698638107 20x + 1.$

Der Fall $m = 16a + 12$ **mit** $a \equiv 3 \bmod 6$

- $D = -4(16 \cdot 3 + 12) = -240$:

  $W_{-240}(x) = x^4 - 8500x^3 - 25464x^2 - 9760x + 64,$

  $\widetilde{W}_{-240}(x) = x^4 - 4250x^3 - 6366x^2 - 1220x + 4.$

- $D = -4(16 \cdot (6 + 3) + 12) = -624$:

  $W_{-624}(x) = x^8 - 14651828x^7 - 398682872x^6 + 1450059200x^5 - 1935551872x^4 - 321277696x^3 - 251052032x^2 - 26329088x + 4096,$

  $\widetilde{W}_{-624}(x) = x^8 - 7325914x^7 - 99670718x^6 + 181257400x^5 - 120971992x^4 - 10039928x^3 - 3922688x^2 - 205696x + 16.$

- $D = -4(16 \cdot (6 \cdot 19 + 3) + 12) = -7536$:

  $W_{-7536}(x) = x^{32} - 1802145255027580747541433679 6x^{31} - 5906451848827005535289805423482367032x^{30} - 1349109122110819706100769328926574312447 36x^{29} - 8058910160015754734399600860842051777432606400x^{28} - 8862735242692382192911376863063879108495125324 8x^{27} - 9830646900822027644436641321687643076258957532 16x^{26} - 6004490383421103898493846071660430555931245654016x^{25} - 1995189361974720946113393597478671359825575315046 4x^{24} - 2671715632291547055927778014076154239469392022732 8x^{23} - 1053917824101898744916045957643985873966307016704 0x^{22} + 3673935914714211412883479993354961526723791814656x^{21} + 5953161337527635986111191571807147094993042407424x^{20} + 8355514940928366009511181771611056359492839014400x^{19} - 5486572084584758871368705190350037111496473837568x^{18} + 2556990256273446842401215199544199371829811347456x^{17} - 2624312103584501577741011229107463302835779665920x^{16} + 3340714630312413718401085775116179105506886942 72x^{15} - 2665261255872841789812667667365460600262680903 68x^{14} + 2310760214031902893671792136338615276539792588 8x^{13} - 3528980677091800422226618192222562336481319321 6x^{12} + 1156718960557890384653299481390213546928766976 0x^{11} - 4356097898189006828679893867703677729198047232x^{10} + 8307626831610876831876192070961516434140692 48x^9 - 1271896942908941248034840651712283618930851 84x^8 + 7130029745804866632203788148643045398544384x^7 - 2555791673108776145210474272645653536440 32x^6 + 1052122574671385824239640676874346666393 6x^5 - 2507410980336142899052386682246738739 20x^4 + 1093147640934179069417125879767629824x^3 -

$$189861050391512914628173832074035 2^2 - 635487752388626760486942146 56x + 2^{48},$$

$$\widetilde{W}_{-7536}(x) = x^{32} - 9010726275137903737707168398x^{31} - 1476612962206751383822451355870591758x^{30} - 1686386402638524632625961661158217890559 2x^{29} - 5036818850009846708999750538026282360895379 00x^{28} - 2769604763341369435284805269707462221404726664x^{27} - 1536038578253441819443225206513694230665462114 4x^{26} - 4691008112047737420698317243484711371821285667 2x^{25} - 7793708445213753695755443740151059999318653574 4x^{24} - 5218194594319427843608941433742488748963656294 4x^{23} - 1029216625099510493082076130511704955045221696 0x^{22} + 1793914020856548541447011715505352307970601472x^{21} + 1453408529669833004421677629835729271238535744x^{20} + 1019960319937544678895407931104865278258403200x^{19} - 3348737844595189740825625726532005072934859 52x^{18} + 7803314991068868537601364744702756872039219 2x^{17} - 4004382482276155971894853560039464268243072 0x^{16} + 2548762993097239470215672130673354420094976x^{15} - 1016716482495438304829661433168586959939072x^{14} + 4407425334991269862502655289342146447257 6x^{13} - 3365498234836388036944025222990572292 6016x^{12} + 5515665819920970843569276244116847738880x^{11} - 1038574671313525874299977747846526558208x^{10} + 9903462924493404426427116478635688345 6x^9 - 7581096547299273300378564904405377024x^8 + 2124914451183338949741061970187141 12x^7 - 3808426369888746954814306307801088x^6 + 7838924040432168723938172138291 2x^5 - 9340833799303110312865624883 20x^4 + 2036146150779312605815242752x^3 - 1768218822698229128757248x^2 - 29592204484558979072x + 2^{16}.$$

- $D = -4(16 \cdot (6 \cdot 31457 + 3) + 12) = -12079728$:

$$W_{-12079728}(x) = x^{1024} + \cdots +$$

$$48104156011038657013073113425670404682861319014015521098100769330112149700605165808971778570 8$$

$$71430412295823916014514055643204662171259143731578605047740899568624862517772945672324052346$$

$$87134305180668495140730848119460418954336523888932345100225174099922483610377054970549239899 2$$

$$30845846130074645759506555786605000770574455371289391691833405575152250005877095989485635672$$

$$96624509822077882972732249815479752453952488504566759706408088795227121077058861250049832248 7$$

$$96682993326323352856168991225061907756816885307935182136048124534832026462676439771840639220 0$$

$$31483487553820544836231427950813803423779404992553678181928526772583882935644350510321143247 8$$

$$737983414505405374471207398580695607028977769136934436130281676963248032010308289737069787170$$
$$122665432169980802018010356350582620864312432168242402728050348563884319200968891033373713898$$
$$223612685861507647464376641088115758815359091930802748884083487759653076465871587564526528282$$
$$980748217203466721108821557958667192794993686561169351848160672527602672327741169486539182441$$
$$631346220794072456633495899340 80x + 2^{1536},$$

$$\widetilde{W}_{-12079728}(x) = x^{1024} + \cdots +$$
$$535176500128570848042022438707396463859782841276845218582026474082361250013367785203007244345$$
$$695124652577362418390778465182544311302678012801939511332971240904538184552063842484226621924$$
$$363422083740798815076655332635712009089510455683551987445073868303293039519695736943284453785$$
$$323958517749147053363512205122875925001996374859228425838654344589745843723776293066382690445$$
$$427760218189917261029334110291145353460086658752100075093520149824514228220756765781431745620$$
$$626724469873639713644991877461733719442814806892056474417009323875551101436160572194971138746$$
$$231613996838198559396494615841899013401571539157304288359715387978573428596201535772982549628$$
$$483312369512061992659306172144371541457150515588036765051912741763886811006975029759293794549$$
$$760x + +2^{512}.$$

- $D = -4(16 \cdot (6 \cdot 189532 + 3) + 12) = -72780528$:

$$W_{-72780528}(x) = x^{2272} + \cdots +$$
$$263738392553978067007372185467162066743639577279892026314644136673267739076008334050573052760$$
$$015266144975699326341536523743737596092796284181717362221339650688108693816443129370305332967$$
$$409563406880325137203616729243296994112043036072552981896967638100974385795544940303384118758$$
$$071365974169606252850978876948476092683251446715782321698617396105279736919646621894013233873$$
$$915147412015768067082684565797384486806500533260802821064169645695376439039793986637291551062$$
$$005095593035659560992512177378915329076581657244899043513377006236521967275788668918442890241$$
$$772085686624954641274100414923203978072600909322164931309242899899584714718874781517337255339$$
$$326044837432555398937265869480910970803635236312140349278206648229179192896055732082649484534$$
$$705799089987827554992840951695956808779013022626828735973620016030010170045107868763408295566$$
$$768962259100822656066421410328565213981653660418270502204790987498645667801279821168545124077$$
$$802602430397737451640346003384700359790840711782598905292134313151844540370335079592781753774$$
$$634408802096520455814840322603358843583260758702242512720956770023304342935326505870660205169$$
$$932073322865805545355022773706076699153853380312273498307354562118153086371060422723797648797$$
$$755636036485610075182820009583670289206406807861766267356453266795738276001375246518805411710$$
$$962264000281091669547431719971935298300304600116909745753755659681301198877196869998712948131$$
$$745763428967647402695632132906185755634824127861600214054989845254004057948227765110649223809$$
$$750097950156013083108204875462661631733623719460534985582271608087071832593430545926793212829$$
$$908209726648989363537516860680872200351672980226938707821839986061797749023846456346290618587$$
$$764059573748402582091126980431359279941997686407196714430674110654882831250047324631359993648$$
$$822821925801358253195071238555987693535011289747458261092913824861867788427300558635853704373$$
$$266563594019493028207387591060958075360457519981724072465458081592158442472970725182512138258$$
$$655857506877608054355476641981428088449702987797048729801873747150660811334019197189809410910$$
$$111443758655755901676029686801709870911878066430380216012584400967488369163354426325236717814$$
$$843863667353368836730024837231775592210094752319363227870315187892411442899447354799596563776$$
$$857643490151634299721279805185872666909306654331820920290882829231360371943279692240104013553$$

$$19965754892357271642659036581378362889994625863192222971881552134988671148530586059590018986743639986431515884354128641433375395400347145104456517255430144 0x + 2^{3408},$$

$$\widetilde{W}_{-72780528}(x) = x^{2272} + \cdots +$$
$$60541503484264059975584880271331866685398821563773093107178226437892418035764684822149297122512675470956208940672498991050285501184366375792688518129391488162976269092859061340058681712462524180371344972482202949525677174528055644144601554972970640032441586806512612853322328980791027535947772620215804033860589686006412510665425595669624699917351661624834106889817339974890335341519809276981149405513384542408408465946967688499307945045277289029908580681940376489861742990624257305493907663036722465316097518354525012720752743077853638236719364747549349522528690816745618055205145255472980143061886114587314533888921424046424389674790484022406222906480582003667753421253465595038016829359335042141301600239505538146374124531754819116276124271281120766370141402104677857689270040349740815736519064742964847788482539462215673934490763120496535102737897554171584425425287591332731998577100696404387464122695975765062845143712916001271356996040744881784703005540788304847768962009201220434043892988587820039894625942233047892914787175092684142669218195955643769641771719542797752398585070930734226919548208675597472334713615108863541061291364101458894772465520193546239539905090691912930508320845114596882135711046783822802579714845630558689116544833554569412770579411156955363757255044201910077620012817496295058380919090207294245703046720552572967850020506340509270791031790062261286241111651106410900988626435839467987634338533952462698442204543071191541342337539965530831364999083835471428924598004953973714988385845548774451440975848901274546143510598964446394793952970339433307777078544304446074380634379430698148829083396550521617642176010047542831612136474251719731228006173923173764667803786639845134857418397696713735921517262426919875717898714612267381979148116346431381415031272613347328 0x + 2^{1136}.$$

Vergleichstabellen

Es bezeichne l den größten Betrag der Koeffizienten von $W_D(x)$ und l' den größten Betrag der Koeffizienten von $\widetilde{W}_D(x)$ und $t = l/l'$.

Wir erhalten die folgende Tabelle für den Fall $m \equiv 3 \bmod 24$:

D	h_D	l	l'	t
-108	3	12	3	4.0
-204	6	144	9	16.0
-684	12	86016	139	618.8201
-780	12	381952	1283	297.7023
-972	9	48000	1548	31.0078
-1164	12	1573632	15484	101.930
-1356	18	86114304	25812	3336.212
-1644	18	193265664	120776	1600.20
-2604	24	400335831040	7206976	55548.38
-3660	24	3382296117248	129495040	26119.12
-6828	30	134246376257093632	946261240195	141870.31
-11496	36	3473333201993488924672	4984737146959232	696793.65
-59436	96	$\leq 2,3 \cdot 10^{66}$	$\leq 3.92 \cdot 10^{47}$	$\geq 5,63 \cdot 10^{17}$
-5867436	744	$\leq 7.9 \cdot 10^{777}$	$\leq 5.25 \cdot 10^{644}$	$\geq 1.5 \cdot 10^{133}$
-62506668	1992	$\leq 5.20 \cdot 10^{2346}$	$6.79 \cdot 10^{1987}$	$\geq 7.65 \cdot 10^{358}$

Wir erhalten die folgende Tabelle für den Fall $m = 16a + 12$ mit $a \equiv 3 \bmod 6$ (Bezeichnungen seien wie oben):

D	h_D	l	l'	t
-240	4	25464	6336	4.0
-624	8	1935551872	181257400	10.68
-1008	8	4915855232	1491889320	3.30
-1392	12	1784894646530240	111555915408140	16.0
-1776	16	1023491167730943859712	15992049495795997808	64.0
-2544	20	55484597680811578390315 4176	63274617958088936702898 40	87.69
-3696	24	74755617052866132003463559779287 04	25164662252199417184585914872912	297.07
-6384	32	$\leq 1.35 \cdot 10^{48}$	$\leq 5.7 \cdot 10^{44}$	≥ 2384.15
-12528	36	$\leq 1.44 \cdot 10^{60}$	$\leq 4.04 \cdot 10^{56}$	≥ 3535.18
-123888	104	$\leq 7.03 \cdot 10^{235}$	$\leq 8.30 \cdot 10^{224}$	$\geq 8.45 \cdot 10^{10}$
-203376	240	$\leq 1.16 \cdot 10^{482}$	$\leq 1.36 \cdot 10^{460}$	$\geq 8.45 \cdot 10^{21}$
-3148656	736	$\leq 3.98 \cdot 10^{2067}$	$\leq 5.84 \cdot 10^{2002}$	$\geq 6.81 \cdot 10^{64}$
-4266864	1056	$\leq 1.98 \cdot 10^{2652}$	$\leq 3.65 \cdot 10^{2555}$	$\geq 5.41 \cdot 10^{96}$
-12677616	2000	$\leq 2 \cdot 10^{5308}$	$\leq 3.4 \cdot 10^{5127}$	$\geq 5.8 \cdot 10^{180}$
-45657072	2500	$\leq 2.6 \cdot 10^{7848}$	$\leq 3.7 \cdot 10^{7626}$	$\geq 7.1 \cdot 10^{221}$

Bemerkung 6.1. *Mit Hilfe der im Kapitel 4 betrachteten Klasseninvarianten können wir die Klassenpolynome bis zur Klassenzahl ca.* 4000 *und zum Betrag der Diskriminante ca.* 10^8 *im Computeralgebra-System MAGMA, [MAGMA], berechnen. Darüber hinaus war es sogar möglich für speziell gewählte Diskriminanten die Klassenpolynome vom Grad ca.* 6600 *zu*

konstruiren. Analog erhält man für die Diskriminanten $< -10^9$ *mit kleiner Klassenzahl (ca.* 3500*) die Klassenpolynome zu berechnen.*

6.3 Einheitengruppe

Wir werden in diesem Abschnitt die Indizes der Untergruppen der Einheitengruppen von Ringklassenkörpern angeben, die durch die Nullstellen eines Klassenpolynomes (welches von einer Klasseneinheit erzeugt wird) zusammen mit den Einheitswurzeln wie im Kapitel 4 (Abschnitt 4) konstruiert werden.

Beispiel 6.2. *Wir betrachten das Weberklassenpolynom*

$$W_{-164}(x) = x^8 - 5x^7 + 7x^6 - 12x^5 + 14x^4 - 12x^3 + 7x^2 - 5x + 1,$$

welches mittels des Satzes 4.16 und nach der Bemerkung 4.10 durch die Klasseninvariante

$$g(\tau) = \sqrt[3]{\left(\frac{2}{A}\right)\frac{1}{2\sqrt{2}}\mathfrak{F}(\tau)^2}$$

erzeugt wird.

Als untere Regulatorabschätzung des entsprechenden Ringklassenkörpers erhalten wir 6.966709.

Aber die Determinante der Regulatormatrix beträgt 0 *für jede Wahl der Nullstellen von* $W_{-164}(x)$*. Daher bilden die Nullstellen von* $W_{-164}(x)$ *zusammen mit den Einheitswurzeln eine Untergruppe der Einheitengruppe von unendlichem Index. In diesem Fall können wir den Algorithmus 5 aus dem vierten Kapitel nicht anwenden.*

Es sei nun B die obere Schranke für den Index der Untergruppe der Einheitengruppe, die durch die Nullstellen des Klassenpolynoms einer Klasseneinheit zusammen mit den Einheitswurzeln erzeugt werden. Wir bestimmen B mittels der unteren Regulatorabschätzung, wie wir im vierten Kapitel erklärt haben. Ferner seien D die Diskriminante und h_D die Klassenzahl wie im vorherigen Abschnitt.

Wir geben nun zu gegebener Diskriminante D, die Klassenzahl h_D, eine untere Schranke R für den Regulator, die Determinante der Regulatormatrix $\mathcal{R}$ und B an.

1. Für $D = -116$ gilt $h_D = 6$ mit

$$R = 2.84108928,\ \mathcal{R} = 0.$$

Daher bilden die Nullstellen von $W_D(x)$ zusammen mit den Einheitswurzeln keine Untergruppe von endlichem Index.

2. Für $D = -188$ gilt $h_D = 5$ mit

$$R = 0.30220245,\ \mathcal{R} = -0.5267712 \text{ und } B = 1.74310.$$

Daher bilden die Nullstellen von $W_D(x)$ zusammen mit den Einheitswurzeln die gesammte Einheitengruppe.

3. Für $D = -204$ gilt $h_D = 6$ mit

$$R = 43.3706,\ \mathcal{R} = 74.6592 \text{ und } B = 1.7214.$$

Daher bilden die Nullstellen von $W_D(x)$ zusammen mit den Einheitswurzeln die gesamte Einheitengruppe.

4. Für $D = -404$ gilt $h_D = 14$ mit

$$R = 6.966709379,\ \mathcal{R} = -991452246.217 \text{ und } B = 142312847.03.$$

5. Für $D = -636$ gilt $h_D = 10$ mit

$$R = 11.27469586,\ \mathcal{R} = -94032.7146707 \text{ und } B = 8340.155323.$$

6. Für $D = -780$ gilt $h_D = 8$ mit

$$R = 4.959567428,\ \mathcal{R} = 371242225.327301 \text{ und } B = 74853750.999611.$$

7. Für $D = -972$ gilt $h_D = 6$ mit

$$R = 26.756805737,\ \mathcal{R} = -10241.05192424 \text{ und } B = 382.74568.$$

8. Für $D = -1164$ gilt $h_D = 12$ mit

$$R = 263.3490957,\ \mathcal{R} = 205006262.750542 \text{ und } B = 778458.19914.$$

9. Für $D = -1236$ gilt $h_D = 12$ mit

$$R = 2156.932362,\ \mathcal{R} = 18808192352229204.295 \text{ und}$$
$$B = 8719880458340.866.$$

10. Für $D = -5292$ gilt $h_D = 18$ mit

$$R = 6529.292738\ \mathcal{R} = -29488290.73 \text{ und}$$
$$B = 4516.31.$$

Bemerkungen für Geschlecht zwei

In diesem Abschnitt werden wir auf die Probleme eingehen, die bei der CM-Konstruktion der einfachen hauptpolarisierten abelschen Flächen vorkommen.

Wir merken zunächst an, dass es uns trotz unserer zahlreichenden experimentellen Bemühungen nicht gelungen ist, geeignete CM-Punkte $\tau \in \mathbb{H}_2$ eines Systems $(g_1(\tau), g_2(\tau), g_3(\tau))$ der Werte der arithmetischen Siegelschen Modulfunktionen der Stufe $(2N, 4N)$ zu finden, so dass das System $(g_1(\tau), g_2(\tau), g_3(\tau))$ ein Klasseninvariantensystem ist.

Dass die Betrachtungen von Weber ([Wb1908]) schon vor der Einführung der Klassenkörpertheorie und der Theorie der komplexen Multiplikation stattgefunden sind, war der Vorteil des Verfahrens im Falle der elliptischen Kurven, da man stets die Kandidaten hat, für die man das Reziprozitätsgesetz von Shimura anwenden könnte.

Aufgrund des Fehlens der galoistheoretischen Beschreibung des Modulkörpers aller arithmetischen Modulfunktionen, sind wir gezwungen, uns mit der zur Zeit existierenden Arithmetik der arithmetischen Modulfunktionen der Stufe $(2N, 4N)$ zu beschäftigen. Dabei wird als Zukunftsprojekt die genauere Untersuchung der Thetafunktionen und Thetarelationen notwendig, da die Transformationsverhalten der Thetafunktionen uns, wie im Falle der elliptischen Kurven, die Konstruktion expliziter Klasseninvarianten ermöglichen könnte. Ferner würde eine genauere Beschreibung der Untergruppe $N_\Psi(\mathcal{L}_N/\mathrm{Tor}(K))$ von $(\mathcal{O}/N\mathcal{O})^*$ die Suche nach einem Klasseninvariantensystem effizienter als der Algorithmus 6 bewerkstelligen, wie wir im fünften Kapitel erläutert haben.

Zusammenfassung

Es seien k ein imaginär quadratischer Zahlkörper und $\mathcal{O}_t$ die Ordnung von k mit dem Führer t und der Diskriminante D_t. Mit Hilfe der Theorie der komplexen Multiplikation zeigen wir, dass der singuläre Wert des Quotienten gewisser Thetafunktionen den Ringklassenkörper Ω_t modulo t über k erzeugt. Dies ermöglicht eine schnellere Konstruktion der Klassenpolynome der Ringklassenkörper als die Konstruktion mittels der klassischen Quotienten von Funktionswerten der Dedekindschen $\eta-$Funktion. Ferner beweisen wir, dass die verallgemeinerten $\eta-$Quotienten mittels der Quotienten der Thetanullwerte darstellbar sind. Diese Darstellungen lassen sich auch zur schnelleren Konstruktion der Klassenpolynome verwenden.

Im Falle, dass D_t gewissen Kongruenzbedingungen genügt, beweisen wir, dass diese singulären Werte Einheiten in den entsprechenden Ringklassenkörpern sind. Diese Eigenschaft wird benutzt, um die Einheitengruppen solcher Ringklassenkörper mittels der in der Konstruktion des Klassenpolynoms explizit bestimmten Nullstellen zu berechnen.

Es sei (A, E) eine einfache hauptpolarisierte abelsche Fläche vom primitiven CM-Typ (K, Φ) mit $[K : \mathbb{Q}] = 4$. Wir erweitern die CM-Konstruktion hyperelliptischer Kurven vom Geschlecht zwei über endlichen Körpern mittels einer Bedingung an die Steinitzklasse auf alle primitiven CM-Körper.

Mit Hilfe des zweidimensionalen Reziprozitätsgesetzes von Shimura, der Theorie der komplexen Multiplikation abelscher Varietäten, und einer Arithmetik der Siegelschen Modulfunktionen g der Stufe $(2N, 4N)$, $\mathrm{ggT}(2, N) = 1$, verallgemeinern wir das Verfahren, welches im Falle der elliptischen Kurven überprüft, ob ein singulärer Wert einer arithmetischen Modulfunktion $g(\tau)$ ein Erzeuger des Ringklassenkörpers Ω_t ist. Damit erhalten wir ein Verfahren, welches überprüft, ob ein System der Werte der Siegelschen Modulfunktionen $g_1(\tau),\ g_2(\tau)$ und $g_3(\tau)$ der Stufe $(2N, 4N)$ mit $\tau \in \mathbb{H}_2$ den über dem Reflexivkörper K^r von K unverzweigten Klassenkörper nach dem ersten Hauptsatz der Theorie der komplexen Multiplikation erzeugt.

Den Abschluss bilden einige Beispiele der Klassenpolynome nebst den Untergruppen der Einheitengruppen entsprechender Ringklassenkörper, die wir mittels der singulären Werte der Quotienten der Thetanullwerte berechnen.

Literaturverzeichnis

[AdHu92] L. M. Adleman, M. A. Huang, *Primality Testing and Abelian Varieties over Finite Fields*, Springer-Verlag, 1992

[AKS04] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Ann. Math., **160**, no. 2, 781-793, 2004

[AtMr93] A. O. L. Atkin, F. Morain, *Elliptic Curves and Primality Proving*, Math. Comp. **61**, 29-67, 1993

[Avan06] R. Avanzi, C. Doche, T. Lange, K. Nguyen , F. Vercaueteren, *Handbook of elliptic and hyperelliptic Curve Cryptography*, Chappman-Hall/CRC, 2006.

[Beld08] J. Belding, R. Bröker, A. Enge, K. Lauter, *Computing Hilbert Class Polynomials*, Springer ANTS-VIII, vol. 5011 of Lect. Notes Comp. Sci., 282-295, 2008

[Birch69] B. Birch, *Weber's Class Invariants*, Mathematika **16**, 283-294, 1969

[Bol1887] O. Bolza, *Darstellung der Binärform sechsten Grades durch die Nullwerthe der zugehörigen $\theta-$Functionen*, Math. Ann., **30(4)**, 478-495, 1887

[BorBor87] J. M. Borwein, P. B. Borwein, *Pi and the AGM*, John Willey, 1987

[Br47] R. Brauer, *On the Zeta-Function of Algebraic Number Fields*, American Journal of Mathematics **69**, 243-250, 1947

[Brö08] R. M. Bröker, *A $p-$adic Algorithm to Compute the Hilbert Class Polynomial*, Math. Comp., **77**, 2417-2435, 2008

[BrSt08] R. M. Bröker, P. Stevenhagen, *Constructing Elliptic Curves of Prime Order*, Computational Arithmetic Geometry, edited by K. E. Lauter and K. A. Ribet, Contemp. Math., **463**, 17-28, 2008

[BSS99] I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press (1999)

[BSS05] I. Blake, G. Seroussi, N. Smart, *Advances in Elliptic Curves in Cryptography*, Cambridge University Press (2005)

[CaFr67] J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Acad. Press, 1967

[CaKoh08] R. Carls, D. Kohel, D. Lubicz, *Higher Dimensional* $3-$*adic CM Construction*, J. Algebra **319**, no. 3, 971-1006, 2008

[Coh93] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993

[Coh00] H. Cohen, *Advanced Topics in Computational Algebraic Number Theory*, Springer-Verlag, 2000

[CohLe84] H. Cohen, H. W. Lenstra, *Heuristics on class groups of number fields*, Number Theory, Noordwijkerhout 1983, vol. **1068** of Lec. Notes in Math., p. 33-62, Springer, Berlin, 1984

[Cos10] R. Cosset, *Factorization with Genus 2 Curves*, Math. Comp., vol. **79**, no. 270, 1191-1208, 2010

[DeEm99] P. Debes, M. Emsalem, *On Fields of Moduli of Curves*, Journal of Algebra, vol. **211**, Issue 1, 42-56, 1999

[Deu58] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzykl. d. math. Wiss., 2. Auflage, **Heft 10**, Stuttgart (1958)

[Dup06] R. Dupont, *Moyenne arithmético-géométrique, suites de Borchardt et applications*, Phd Thesis, École Polytexhnique, 2006

[Dup07] R. Dupont, *Fast Evaluation of Modular Functions Using Newton Iterations and the AGM*, to appear in Mathematics of Computation, 2007

[EiLa05] K. Eisenträger, K. Lauter, *A CRT Algorithm for Constructing Genus 2 Curves over Finite Fields*, to appear in Proceedings of Arithmetic, Geometry, and Coding Theory, (AGCT-10), Marseille (2005), Online unter http://arxiv.prg/abs/math.NT/0405305

[EnGau02] A. Enge, P. Gaudry, *A General Framework for Subexponential Discrete Logarithm Algorithms*, Acta Arith. **102**, 83-103, 2002.

[EngMor03] A. Enge, F. Morain, *Fast Decomposition of Polynomials with Known Galois Group*, Springer, Appl. Alg., vol. **2643** of Lect. Notes in Comp. Sci., 254-264, 2003

[EngMor09] A. Enge, F. Morain, *Generalised Weber Functions I*, preprint

[EnSch03] A. Enge, R. Schertz, *Constructing Elliptic Curves from Modular Curves of Positive Genus*, preprint, 2003

[EnSch04] A. Enge, R. Schertz, *Constructing Elliptic Curves over Finite Fields Using Double eta-quotients*, Journal de Théorie des Nombres de Bordeaux **16**, 555-568, 2004

[EnSch05] A. Enge, R. Schertz, *Modular Curves of Composite Level*, Acta Arith. **118**, no. 2, 129-141, 2005

[EngSut10] A. Enge, A. V. Sutherland, *Class Invariants by the CRT Method*, preprint http://hal.inria.fr/docs/00/44/87/29/PDF/classinv.pdf

[FiPohst08] C. Fieker, M. Pohst, *A Regulator Lower Bound for Number Fields*, Journal of Number Theory **128**, 2767-2775, 2008

[Fr60] A. Fröhlich, *Discriminants of Algebraic Number Fields*, Math Zeit., **74**, 18-28, 1960

[Fre08] D. S. Freeman, *Constructing Abelain Varieties for Pairing-Based Cryptography*, Phd Thesis, University of California, Berkeley, 2008

[FST06] D. Freeman, M. Scott, E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*, http://eprint.iacr.org/2006/372.pdf (2006)

[Gau06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, A. Weng, *The* $2-$*adic CM Method for Genus 2 Curves with Apllication to Cryptography*, Asiacrypt 2006 (Shanghai) Lect. Notes in Comp. Sci. **4284**, 114-129, Springer-Verlag, 2006

[Gee01] A. Gee, *Class Fields by Shimura Reciprocity*, Phd Thesis, Universiteit Leiden, 2001

[GeSt98] A. Gee, P. Stevenhagen, *Generating Class Fields Using Shimura Reciprocity*, LNCS 1423, (ANTS-III), 441-453, 1998

[Got59] E. Gottschling, *Explizite Bestimmung der Randflächen des Fundamentalbereichs der Modulgruppe zweiten Grades*, Math. Annalen, **138**, 103-124, 1959

[GoKi86] S. Goldwasser, J. Kilian, *Almost all Primes can be quickly Certified*, Proc. 18th Annual ACM Symp. on Theory of Computing, 1986

[GoLau10] E. Z. Goren, K. Lauter, *in 2010 wird veröffentlicht*

[Gua04] J. Guardia, E. Torres, M. Vela, *Stable Models of Elliptic Curves, Ring Class Fields, and Complex Multiplication*, ANTS-VI, Lec. Notes in Comp. Sci, **3076**, Springer Verlag, Berlin, 250-262, 2004

[Haj88] F. Hajir, *Unramified Elliptic Units*, PhD Thesis, Princeton University, 1988

[HanMor01] G. Hanrot, F. Morain, *Solvability by Radicals from an Algorithmic Point of View*, Sym. and Alg. Comp., ISSAC 2001, 254-264, 2001

[Heeg52] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Mathematische Zeitschrift, **56**, 227-253, 1952

[HinSil00] M. Hindry, J. Silverman, *Diophantine Geometry-An Introduction*, Springer-Verlag, New York, 2000

[Hil1896] D. Hilbert, *Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Körper*, Nach. K. Ges. Wiss. Göttingen, 29-39, 1896, (Ges. Abh., 53-62)

[Hr08] W. B. Hart, *Schläfli Modular Equations for Generalized Weber Functions*, Ramanujan Journal, **15**, 435-468, 2008

[Igu60-I] J. I. Igusa, *Modular Forms and Projective Invariants*, Amer. Jour. Math., **89(3)**, 817-855, 1967

[Igu60-II] J. I. Igusa, *Arithmetic Variety of Moduli for Genus Two*, The Annals of Math., secon ser., Vol. **72**, No. 3, 612-649, 1960

[Jan73] G. J. Janusz, *Algebraic Number Fields*, AMS, Grad. Studies, vol. **7**, 1973

[Kim03] H. H. Kim, *Functoriality for the Exterior Square of GL_4 and the Symmetric fourth of GL_2*, J. Amer. Math. Soc., **16(1)**, 139-183. 2003

[Kli90] H. Klingen, *Introductory Lectures on Siegel Modular Forms*, Cambridge St. in Adv. Math. **No. 20**, 1990

[Koh07] D. Kohel et. al., *ECHIDNA algorithms for algebra and geometry experimentation*

[Kr1853] L. Kronecker, *Über die algebraisch auflösbaren Gleichungen*, Akad. Berlin, 365-374, 20.06.1853 (Werke IV, 3-11)

[Kr68] L. Kronecker, *Zur Theorie der elliptischen Functionen XI*, Math. Werke IV, Chelsea Pub., 1968

[Lang73] S. Lang, *Elliptic Functions*, Addison-Wesley, 1973

[Lang83] S. Lang, *Complex Multiplication*, Springer Verlag, 1983.

[Lang82] S. Lang, *Introduction to Algebraic and Abelian Functions*, Springer Verlag, 1982

[LePoUz09] F. Leprévost, M. Pohst, O. Uzunkol, *On the computation of class polynomials with "Thetanullwerte" and its applications to the unit group computation*, eingereichter Preprint, 2009

[Len87] H. W. Lenstra, *Factoring integers with elliptic curves*, Ann. of Math. **126(2)**, 649-473, 1987

[MAGMA] MAGMA Computational Algebra System, http://magma.maths.usyd.edu.au/magma/

[Men96] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRS Press, 1996

[Mil1] J. S. Milne, *The Fundamental Theorem of Complex Multiplication*, abrufbar unter http://www.jmilne.org/math/articles/2007c.pdf

[Mil2] J. S. Milne, *Abelian Varieties*, abrufbar unter http://www.jmilne.org/math/CourseNotes/AV.pdf

[Mor05] F. Morain, *Implementing the Asymptotically fast Version of the Elliptic Curve Primality Proving Algorithm*, Math. Comp. **76**, 493-505, 2007

[MorECPP] F. Morain, *The ECPP home page*, http://www.lix.polytechnique.fr/ morain/Prgms/ecpp.english.html

[Mum70] D. Mumford, *Abelian Varieties*, Oxford University Press, 1970

[Mum83] D. Mumford, *Tata Lectures on Theta I*, volume 28 of Progress in Mathematics. Birkhäuser, 1983

[Mum84] D. Mumford, *Tata Lectures on Theta II*, volume 43 of Progress in Mathematics. Birkhäuser, 1984

[Neu92] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, 1992

[Ov74] A. I. Ovseevich, *Abelian extensions of fields of CM-type*, Funkts. Anal. Prilozh., **8(1)**, 16-24, 1974

[PhZs89] M. Pohst, H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989

[Pohst] M. Pohst, et al., *KANT/KASH*, http://www.math.tu-berlin.de/ kant/kash.html

[PohstVL] M. Pohst, *Algorithmische Zahlentheorie, Vorlesung-Skript*, Local Fields and Applications, TU-Berlin

[RaFa74] H. E. Rauch, H. M. Farkas, *Theta Functions with Applications to Riemann Surfaces*, The Williams-Wilkins Company, 1974

[RubSil09] K. Rubin, A. Silverberg, *Point Counting on Reductions of CM Elliptic Curves*, J. Num. Theory, vol. 129, 12, 2903-2923, 2009

[Rum83] R. S. Rumely, *On the Grössencharacter of an Abelian Variety in a Parametrized Family*, Trans. of AMS, vol. **276 (1)**, 213-233, 1983

[Sa99] R. Sasaki, *An arithmetic of modular function fields of degree two*, Acta Arith., Vol. **7**, 79-105, 1999

[Sar95] P. Sarnak, *Selberg's Eigenvalue Conjecture*, Notices of AMS, vol. **42**, 1272-1277, 1995

[Sch02] R. Schertz, *Weber's Class Invariants Revisited*, Journal de Théorie des Nombres de Bordeaux **14**, 325-343, 2002

[Sch10] R. Schertz, *Complex Multiplication*, Cambridge University Press, Cambridge, 2010

[Sh61] G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of Publications of the Mathematical Society of Japan. The Mathematica1 Society of Japan,, Tokyo, 1961

[Sh62] G. Shimura, *On the class-fields obtained by complex multiplication of abelian varieties*, Osaka Math., **14**, 33-44, 1962

[Sh70] G. Shimura, *On canonical models of arithmetic quotients of bounded symetric domains*, Ann. of Math. (2) **91**, 144-222, 1970, **92** 528-549, 1970

[Sh71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971

[Sh76] G. Shimura, *Theta functions with complex multiplication*, Duke Math., **43**, 673-696, 1976

[Sh78] G. Shimura, *On certain reciprocity laws for theta functions and modular forms*, Acta Arith. **141**, 35-71, 1978

[Sh97] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton University Press, 1997

[Shaf97] I. Shafarevich, *Basic Algebraic Geometry 2*, Springer-Verlag, Third Printing, 1997

[ShGo97] E. Shalit, E. Z. Goren, *On Special Values of Theta Functions of Genus Two*, Annales de l'institut Fourier, tome **47**, no. 3, 775-799, 1997

[Sil86] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer Verlag, 1986

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer Verlag, Chapter II, 1994

[Spa94] A. M. Spallek, *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, Dissertation, Universität GH Essen, 1994

[St69] H. M. Stark, *On a gap in a Theorem of Heegner*, J. Number Theoy 1, 16-27, 1969

[Stev01] P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity,* Advanced Studies in Pure. Math. 30, 'Class Field Theory - its centenary and prospect', 161-176, 2001

[Str10] M. Streng, *Computing Igusa Class Polynomials*, preprint, 2010

[Tate66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2**, 134-144, 1966

[Uz04] O. Uzunkol, *Atkin's ECPP Algorithm*, M. Sc. Thesis TU-Kaiserslautern, 2004

[Wa82] L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982

[Wb1886] H. Weber, *Theorie der Abelschen Zahlkörper*, Acta Math., **8**, 193-263, 1886

[Wb1908] H. Weber, *Lehrbuch der Algebra*, Bd. **3**, 2. Aufl. Braunschweig, 1908

[Weil46] A. Weil, *Foundations of Algebraic Geometry*, AMS, vol. 29, New York, 1946

[Weil57] A. Weil, *Zum Beweis des Torellischen Satzes*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. **IIa**: 32-53, 1957

[Weng01] A. Weng, *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*, Dissertation, Universität GH Essen, 2001