Einleitung

Die Untersuchung der abelschen Erweiterungen algebraischer Zahlkörper entspringt der klassischen Fragestellung nach der ganzzahligen Lösbarkeit gewisser diophantischer Gleichungen. So führt beispielsweise Fermats Zwei-Quadrate-Satz sofort zur Untersuchung des Verhaltens von Primzahlen beim Übergang zu den ganzen Zahlen im Gaußschen Zahlkörper. Die Gleichung $p = X^2 + Y^2$ ist nämlich genau dann in ganzen Zahlen lösbar - p ist durch die Form $F(X,Y) = (X - iY)(X + iY)$ darstellbar - wenn p Produkt zweier ganzalgebraischer Gaußzahlen ist. Eine naheliegende Verallgemeinerung des Problems ist die Suche nach Primzahlen, die sich durch ganzzahlige quadratische Formen $aX^2+bXY+cY^2 = a(X + \rho Y)(X + \rho' Y)$ darstellen lassen. Sind ρ und ρ' nicht rational, so erzeugen sie den selben quadratischen Körper, und die Lösbarkeit der Gleichung $p = aX^2 + bXY + cY^2$ übersetzt sich in die Frage nach dem Zerlegungsverhalten von p im Hilbertklassenkörper von $\mathbb{Q}(\rho)$, der maximal unverzweigten abelschen Erweiterung von $\mathbb{Q}(\rho)$, bzw. nach dem Zerlegungsverhalten in abelschen Erweiterungen insb. im Geschlechterkörper und im Ringklassenkörper, siehe [Coh85], 2. Der Fall binärer (Norm-)Formen ist klassisch ausgearbeitet und liefert zusammen mit dem Zerlegungsgesetz im Hilbertklassenkörper[1] eine vollständige Antwort auf die gestellte Frage. Für die Erzeugung von Primzahlen durch Normformen von imaginär abelschen Körpern kennen wir folgendes Kriterium: Ist K imaginär abelsch und p kein Teiler der Diskrimante von K, dann ist p genau dann durch die Normform darstellbar, wenn p im Hilbertklassenkörper H_K voll zerlegt ist, siehe [Gar81], Theorem 7.27. Dabei verstehen wir unter der *Normform* eines algebraischen Zahlkörpers K vom Grad n mit Ganzheitsbasis $\{\alpha_1, \ldots, \alpha_n\}$ die homogene Form

$$F_K(X_1, \ldots, X_n) := N_{K/\mathbb{Q}}(\alpha_1 X_1 + \ldots + \alpha_n X_n) = \prod_\sigma \sum_i \sigma(\alpha_i) X_i,$$

wobei σ die verschiedenen $\mathbb{Q}$-Einbettungen von K in einen fixierten algebraischen Abschluß durchläuft. Im obigen Beispiel ist $F_K(X,Y) = X^2 + Y^2$ die Normform

[1] Der Hilbertklassenkörper zu K ist derjenige über K normale Erweiterungskörper, in dem genau die Primhauptideale vom Trägheitsgrad 1 voll zerlegt sind. Nach [Has65], S. 4, war diese Charakterisierung die Hilbertsche Definition des Klassenkörpers. Mittlerweile wird allgemeiner jeder abelsche Erweiterungskörper eines Zahlkörpers Klassenkörper genannt.

von $K := \mathbb{Q}(i)$ über $\mathbb{Q}$ zur Ganzheitsbasis $\{1, i\}$. K hat Klassenzahl 1, also ist $K = H_K$ und $p \neq 2$ genau dann durch $F_K(X, Y)$ darstellbar, wenn p in K voll zerlegt ist, d.h. wenn $p \equiv 1 \bmod 4$. Betrachten wir ein zweites Beispiel ([Gar81], p. 214). Die Form $F(X, Y) = X^2 + XY + 4Y^2$ ist die Normform von $K = \mathbb{Q}(\sqrt{-15})/\mathbb{Q}$ zur Basis $\{1, \frac{1}{2}(1 + \sqrt{-15})\}$. Eine Primzahl $p \neq 3, 5$ ist somit genau dann durch $F_K(X, Y)$ darstellbar, wenn p im Hilbertklassenkörper $H_K = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ zu K voll zerlegt ist. Letzteres ist genau dann der Fall, wenn $p \equiv 1 \bmod 15$ oder $\equiv 4 \bmod 15$.[2]

Wir werden uns in dieser Arbeit mit abelschen Erweiterungen total imaginär quadratischer Erweiterungen total reeller Zahlkörper, sogenannter *CM-Körper*, beschäftigen. In dieser Sitution kommutiert jede Einbettung nach $\mathbb{C}$ mit der komplexen Konjugation, und wir können den Beweis des Kriteriums für imaginär abelsche Zahlkörper, [Gar81], Beweis von Theorem 7.27, unmittelbar auf CM-Körper übertragen.

Satz 0.0.1. *Sei K ein galoisscher CM-Körper vom Grad $[K : \mathbb{Q}] = n$, p eine rationale Primzahl, die in K nicht verzweigt, und sei $F_K(X_1, \ldots, X_n)$ die Normform zu K. Es gibt genau dann eine ganzzahlige Lösung der Gleichung $F_K(X_1, \ldots, X_n) = p$, wenn p im Hilbertklassenkörper H_K voll zerlegt ist.*

Beweis. Nach Voraussetzung ist K eine rein imaginär quadratische Erweiterung eines total reellen Zahlkörpers, die Menge der Einbettungen $K \hookrightarrow \mathbb{C}$ ist daher durch $\{\sigma_1, \ldots, \sigma_{n/2}, \bar{\sigma}_1, \ldots, \bar{\sigma}_{n/2}\}$, wobei $\bar{\sigma}_i := {}^- \circ \sigma_i$, gegeben. Die Existenz eines Tupels ${}^t(x_1, \ldots, x_n) \in \mathbb{Z}^n$ mit $p = F_K(x_1, \ldots, x_n)$ ist zur Existenz eines ganzen $\alpha \in \mathcal{O}_K$ mit Norm $N_{K/\mathbb{Q}}(\alpha) = p$ äquivalent. Da

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n/2} \sigma_i(\alpha)\bar{\sigma}_i(\alpha) > 0,$$

ist die letzte Bedingung genau dann erfüllt, wenn die Ideale $p\mathbb{Z} = N_{K/\mathbb{Q}}(\alpha)\mathbb{Z}$ übereinstimmen, was wiederum zur Existenz eines Primhauptideals $\mathfrak{p}$ von $\mathcal{O}_K$ der Norm p gleichwertig ist. $\mathfrak{p}$ ist daher vom Trägheitsgrad 1 (p ist unverzweigt in K). Die Galoisgruppe operiert transitiv auf der Menge aller Primideale von $\mathcal{O}_K$, die p teilen. Folglich stimmen die Trägheitsindizes aller Primteiler von p überein. Daher ist $p = F_K(X_1, \ldots, X_n)$ dann und nur dann ganzzahlig lösbar, wenn jeder Primteiler von p Trägheitstgrad und Verzweigungszahl 1 hat und ein Primhauptideal ist. Ein Primideal $\mathfrak{p}$ ist genau dann ein Hauptideal, wenn es im Hilbertklassenkörper H_K voll zerlegt ist. Insgesamt ist somit p genau dann durch die Normform darstellbar, wenn p in H_K voll zerlegt ist. □

[2] $p = 3$ und 5 sind nicht durch $F_K(X, Y)$ darstellbar.

An die Frage nach der Existenz von Klassenkörpern schließt sich unmittelbar der Wunsch nach einer expliziten Beschreibung dieser Erweiterungen an. Im Grundbereich der rationalen Zahlen wird dieses Verlangen von der Exponentialfunktion gestillt, denn nach dem Theorem von Kronecker und Weber ist jede abelsche Erweiterung in einem Kreisteilungskörper enthalten, und Kreisteilungskörper sind durch Einheitswurzeln, also durch Werte der Funktion $f(z) := e^{2\pi iz}$ in rationalen Argumenten, erzeugt. Im nächst schwierigeren Fall der imaginär quadratischen Zahlkörper hatte Kronecker die Idee, daß die elliptische Modulfunktion j diese Rolle übernimmt, was er als seinen liebsten Jugendtraum bezeichnete. Ist ein singulärer Modul τ, d.h. ein Punkt der oberen Halbebene, der einen imaginär quadratischen Körper K erzeugt, gegeben, so ist die Erweiterung $K(j(\tau))/K$ abelsch, und $K(j(\tau))$ ist der Hilbertklassenkörper zu K, wenn $\mathbb{Z} + \tau\mathbb{Z}$ ein Ideal von K ist.[3] In beiden Fällen erhalten wir Klassenkörper eines Zahlkörpers durch Adjunktion von Werten analytischer Funktionen in speziellen Argumenten.[4] Die Ausweitung dieses Prinzips stellte Hilbert der mathematischen Gesellschaft in seinem berühmten Paris-Vortrag - 20 Jahre vor dem Takagischen Beweis von Kroneckers Jugendtraum - als Problem 12 als Aufgabe. Man finde analytische Funktionen, welche für beliebige Grundkörper zur Exponentialfunktion und zur elliptischen Modulfunktion analoge Eigenschaften aufweisen.[5] Es dauerte bis in die 1950er Jahre ehe André Weil [Wei55], Goro Shimura [Shm55] und Yutaka Taniyama [Tan55] die prinzipiellen Ideen einer geeigneten Verallgemeinerung der Theorie der komplexen Multiplikation elliptischer Kurven auf Dimension > 1 entwickeln konnten, die Shimura und Taniyama in [ST61] weiter ausgearbeitet haben. Sie konnten zeigen, daß Funktionen existieren, die auf dem Modulraum polarisierter abelscher Varietäten mit einer gewissen Endomorphismenstruktur leben, die in speziellen Punkten abelsche Erweiterungen von Zahlkörpern, die

[3] ansonsten ist $K(j(\tau))/K$ ein Ringklassenkörper.

[4] Die rationalen Zahlen besitzen bekanntermaßen keine unverzweigten abelschen Erweiterungen, insofern ist es möglicherweise richtiger von $K(j(\tau))$, $\mathbb{Z} + \mathbb{Z}\tau$ ein Ideal des imaginär quadratischen Zahlkörpers K, als dem geeigneten Substitut für $\mathbb{Q}$ zu sprechen. Die maximale abelsche Erweiterung von K erhalten wir durch zusätzliche Adjunktion von Werten der Weberfunktionen in Torsionspunkten der entsprechenden elliptischen Kurve an $K(j(\tau))$.

[5] In Hilberts Rede heißt es „... Von der höchsten Bedeutung endlich erscheint mir die Ausdehnung des Kroneckerschen Satzes auf den Fall, *daß an Stelle des Bereichs der rationalen Zahlen oder des imaginär quadratischen Zahlenbereichs ein beliebiger algebraischer Zahlkörper als Rationalitätsbereich zu Grunde gelegt wird; ich halte dies Problem für eines der tiefgehendsten und weittragendsten Probleme der Zahlen- und Funktionentheorie. ...*“ und später „... Wie wir sehen, treten in dem eben gekennzeichneten Problem die drei grundlegenden Disziplinen der Mathematik, nämlich Zahlentheorie, Algebra und Funktionentheorie in die innigste gegenseitige Berührung und ich bin sicher, daß insbesondere die Theorie der analytischen Funktionen mehrerer Variablen eine wesentliche Bereicherung erfahren würde, wenn es gelänge, *diejenigen Funktionen aufzufinden und zu diskutieren, die für einen beliebigen algebraischen Zahlkörper die entsprechende Rolle spielen, wie die Exponentialfunktion für den Körper der rationalen Zahlen und die elliptische Modulfunktion für den imaginären quadratischen Zahlkörper.*“, zitiert nach [Hil00].

wiederum in engem Zusammenhang mit der Endomorphismenstruktur der parametrisierten Varietät stehen, liefern. Bislang ist es allerdings nur in wenigen Fällen gelungen, die entsprechenden Modulfunktionen und die damit einhergehenden *Shimuraklassenkörper* explizit zu konstruieren.

Ziel der vorliegenden Arbeit ist es, Modulfunktionen zweier Kurvenfamilien vorzustellen, die obige Eigenschaften aufweisen, deren Werte in Parametern von CM-Kurven also Klassenkörper erzeugen, sowie die auftretenden Körper eingehender zu studieren. Dazu werden wir zunächst einige grundlegende Eigenschaften abelscher Varietäten mit komplexer Multiplikation bereitstellen, was insbesondere der Klärung der Begrifflichkeit dienen soll. Im darauffolgenden Kapitel stellen wir die Konstruktion Picardscher Modulfunktionen zu zwei Kurvenfamilien (Picardkurven, eine Familie hyperelliptischer Kurven) dar. Dabei werden wir unser Augenmerk in erster Linie auf die weniger bekannte Konstruktion der Modulfunktion zur hyperelliptischen Kurvenfamilie legen. Für die Picardsche Kurvenfamilie geben wir die notwendigen Daten an und verweisen auf die Literatur. In Kapitel 3 werden die auftretenden Grundkörper (*Reflexkörper*) eingehender untersucht, die, wenn wir der Einfachheit halber *galoissch* voraussetzen, als Multiplikationskörper bzw. Endomorphismenalgebren von Jacobischen der Kurvenfamilien vorkommen. Das Hauptresultat dieses Abschnitts besagt, daß jeder sextische CM-Körper, der die dritten oder vierten Einheitswurzeln enthält, als Multiplikationskörper auftritt, und daß jeder solche durch einen singulären Modul projektiv erzeugt wird. Ausgehend von einem singulären Modul ist es dann nicht schwer, die Jacobi-Varietät einer CM-Kurve mit vorgegebenem Multiplikationstyp zu konstruieren und mit Hilfe der Modulfunktion die Gleichung der Kurve anzugeben. Im letzten Abschnitt befassen wir uns genauer mit den durch die Werte der Picardschen Modulfunktionen erzeugten Klassenkörpern. Es ist znächst nicht klar, daß wir überhaupt echte Erweiterungen der zugrunde liegenden Körper erhalten, so fällt beispielsweise der Modulkörper einer CM-Kurve mit Gleichung $y^2 = 1 - x^l$, l eine ungerade Primzahl, mit $\mathbb{Q}$ zusammen, vgl. [ST61], Chapter IV, 15.4 Example 2), insofern rechtfertigt Beispiel 4.3.3 die vorangegangenen und weiteren Untersuchungen. Um explizite Resultate zu erhalten, setzen wir im vierten Kapitel voraus, daß der Endomorphismenring der CM-Varietät isomorph zur Hauptordnung des Multiplikationskörpers ist. In diesem Fall ist der Shimuraklassenkörper unverzweigt über dem Reflexkörper, und er ist Klassenkörper zu einer Idealgruppe, die wir für zyklische Klassengruppen und ungerade Klassenzahlen genauer bestimmen können. Es zeigt sich, daß das Haupthindernis zur Bestimmung der Modulkörper in der Unkenntnis der Wirkung der komplexen Konjugation auf der Klassengruppe besteht. Abschließend werden wir für kleine Klassenzahlen dieses Problem lösen und die fraglichen Shimuraklassenkörper bis zur Klassenzahl 11 bestimmen.