Konstruktion elliptischer Kurven über endlichen Körpern zu vorgegebener Ordnungszahl

Diplomarbeit

im Studiengang Mathematik
der Universität Bremen
vorgelegt im

Sommersemester 2007

von

Sebastian Lösch

Gutachter:
Prof. Dr. Michael Hortmann (Universität Bremen)
Prof. Dr. Jens Gamst (Universität Bremen)

Vorwort

Elliptische Kurven werden schon lange in der Funktionentheorie, der Algebraischen Geometrie und der Zahlentheorie betrachtet. In den letzten zwanzig Jahren hat sich das ursprünglich rein theoretische Interesse gewandelt.

Das an Bedeutung gewinnende Gebiet der Kryptografie bietet für elliptische Kurven vielfältige Anwendungsmöglichkeiten. So lassen sich elliptische Kurven über endlichen Körpern u. a. zur Faktorisierung von ganzen Zahlen, zu Primzahltests und in Verschlüsselungsverfahren einsetzen.

Die Kryptografie mit elliptischen Kurven (ECC, elliptic curve cryptography) bietet den Vorteil, dass sie bei gleichen Sicherheitsanforderungen mit erheblich kürzeren Schlüssellängen auskommt als andere Public-Key-Verfahren wie etwa RSA: ein ECC-Schlüssel mit nur 384 Bit wird heute als etwa so sicher angesehen wie ein RSA-Schlüssel mit 7680 Bit (siehe [21]). Kryptografie auf elliptischen Kurven kommt daher gerne dort zum Einsatz, wo wenig Speicherplatz oder wenig Rechenleistung zur Verfügung steht, z. B. auf Chipkarten. Als prominentes Beispiel sei hier der neue Reisepass genannt, bei dem die Verschlüsselung der (biometrischen) Daten mittels ECC geschieht.

Kryptografie auf elliptischen Kurven basiert auf dem Diskreten-Logarithmus-Problem (DLP), welches auf elliptischen Kurven über endlichen Körpern schwer zu lösen ist. Benötigt werden dabei Kenntnisse der Gruppenordnung der zum Einsatz kommenden elliptischen Kurve über einem endlichen Körper. Hier lassen sich nun zwei Wege einschlagen. Zum einen können solange zufällig elliptische Kurven gewählt und ihre Gruppenordnungen gesucht werden, bis diese den gewünschten Anforderungen entsprechen. Zum anderen kann zunächst eine Gruppenordnung den gewünschten Anforderungen entsprechend gewählt und dann eine elliptische Kurve dieser Gruppenordnung konstruiert werden. Die hierbei zum Einsatz kommenden Theorien werden in der vorliegenden Arbeit soweit wie möglich entwickelt und dargestellt.

Unsere Konstruktion elliptischer Kurven zu vorgegebener Gruppenordnung erfolgt mit der sogenannten Methode der Komplexen Multiplikation (CM-Methode, Complex-Multiplication-Methode). Es zeigt sich, dass ordinäre elliptische Kurven E über endlichen Körpern durch Reduktion elliptischer Kurven A über $\mathbb{C}$ mit komplexer Multiplikation entstehen. Ausgangspunkt des Konstruktionsverfahrens ist die in diesem Fall auftretende Isomorphie der Endomorphismenringe $End(E) \simeq End(A)$. Die Gruppenordnung von E über $\mathbb{F}_q$ ist eindeutig durch den Frobenius-Endomorphismus ϕ_q von E bestimmt,

$$deg(\phi_q) = q \qquad \text{und} \qquad deg(1 - \phi_q) = |E(\mathbb{F}_q)|.$$

Es ist $End(A)$ eine Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers K und aus den obigen Normgleichungen lässt sich K bestimmen. A ist isomorph zu einem komplexen Torus $\mathbb{C}/L$ für ein Gitter $L \subset \mathbb{C}$. Das Gitter L ist linear äquivalent zu einem eigentlichen gebrochenen Ideal $\mathfrak{a}$ von $\mathcal{O}$. Die j-Invariante $j(\mathfrak{a}) = j(L) = j(A)$ ist algebraisch ganz und erzeugt den Ringklassenkörper $H_{\mathcal{O}}$ über K, über welchem man A als definiert annehmen darf. Die j-Invariante von E ergibt sich dann als Lösung der Klassengleichung von $\mathcal{O}$ über $\mathbb{F}_q$ und führt auf eine definierende Gleichung der reduzierten Kurve $\tilde{A}$ von A. Da E als elliptische Kurve über einem endlichen Körper durch ihre j-Invariante nicht eindeutig bestimmt ist, müssen Twiste von $\tilde{A}$ betrachtet werden. Es offenbart sich dann ein ebensolcher Twist als isomorph zu E.

Der Ausgangspunkt meiner Diplomarbeit war der Artikel von Bröker und Stevenhagen [15]. Die notwendigen zahlentheoretischen Kenntnisse habe ich mir durch das Buch von Cox [3] angeeignet. Einen einfachen Überblick über elliptische Kurven bot mir das Buch von Washington [13];

ausführlich werden diese in den Büchern [11, 12] von Silverman behandelt. Desweiteren ist die Diplomarbeit von Lay [17] zu erwähnen, welche in der Implementierung ihren Schwerpunkt hat; eine ausführliche Erläuterung seines Verfahren und Beweise der zugrunde liegenden theoretischen Erkenntnisse werden dort nicht gegeben.

In Kapitel 1 meiner Diplomarbeit werden Zahlkörper im Allgemeinen und Ordnungen von Zahlkörpern im Speziellen untersucht, denn diese treten als Endomorphismenringe elliptischer Kurven auf. In Kapitel 2 und 3 werden Ringklassenkörper und deren Konstruktion behandelt. Dies ermöglicht es, uns eine Brücke zu elliptischen Kurven zu schlagen, denn die Werte der j-Modulfunktion entpuppen sich als j-Invarianten von elliptischen Kurven. Das Kapitel 4 stellt elliptische Kurven über $\mathbb{C}$ und endlichen Körpern vor und erläutert das Konzept der Reduktion elliptischer Kurven und ihrer Endomorphismenringe. In Kapitel 5 werden die erworbenen Kenntnisse zusammengetragen, um das Konstruktionsverfahren für elliptische Kurven über endlichen Körpern zu vorgegebener Punktezahl herzuleiten und ausführlich zu erklären. Neben dem allgemeinen Konstruktionsverfahren für elliptische Kurven über beliebigen endlichen Körpern wird ein spezieller Ansatz zur Erzeugung elliptischer Kurven über Primkörpern vorgestellt.

Im Rahmen meiner Diplomarbeit und meines Studiums habe ich von vielen Menschen Hilfe und Unterstützung erfahren.
Herrn Hortmann danke ich für die äußerst spannende Aufgabenstellung und die freundliche und kompetente Betreuung meiner Diplomarbeit. Herrn Gamst danke ich für seine Bereitschaft das Zweitgutachten zu erstellen und seine fachliche Hilfe durch viele klärende Gespräche.
Meinen Eltern möchte ich für die Finanzierung meines Studium danken. Allen Freunden und Bekannten bin ich dankbar für die mentale und seelische Unterstützung, im Besonderen Sonja.

Inhaltsverzeichnis

1 Zahlkörper

Definition 1.0.1. Ein **Zahlkörper** K ist ein Unterkörper von $\mathbb{C}$ von endlichem Grad über $\mathbb{Q}$. Ein Element $\alpha \in K$ heißt (**algebraisch**) **ganz**, wenn es Nullstelle eines normierten Polynoms aus $\mathbb{Z}[X]$ ist. Mit $\mathcal{O}_K$ wird die Menge der ganzen Elemente aus K bezeichnet.

Proposition 1.0.2. *Sei K ein Zahlkörper.*

(i) $\mathcal{O}_K$ ist ein Unterring von $\mathbb{C}$ mit K als Quotientenkörper.

(ii) $\mathcal{O}_K$ ist ein freier $\mathbb{Z}$-Modul vom Rang $[K:\mathbb{Q}]$.

Beweis. Siehe [9, Korollare zu den Theoremen 2 und 9]. □

Es heißt $\mathcal{O}_K$ der **Ganzheitsring** von K. Für α in $\mathcal{O}_K$ definiert man $N_{K/\mathbb{Q}}(\alpha)$, $Tr_{K/\mathbb{Q}}(\alpha)$ und das charakteristische Polynom von α, als Norm, Spur und charakteristisches Polynom des Endomorphismus $m_\alpha : K \to K$, $x \mapsto \alpha x$.
Ist $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$, so ist bekannt ([10, Prop. 1, S. 44]), dass

$$Tr_{K/\mathbb{Q}}(\alpha) = \textstyle\sum_{i=1}^{n} \sigma_i(\alpha) \qquad \text{und} \qquad N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

gilt. Die Spur ist also additiv und die Norm multiplikativ. Da beide invariant unter allen $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ sind, liegen Spur und Norm stets in $\mathbb{Q}$. Ist α sogar aus $\mathcal{O}_K$ gewählt, so sind $Tr_{K/\mathbb{Q}}(\alpha)$, $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, denn Spur und Norm treten als Koeffizienten des charakteristischen Polynoms von α auf, welches ein Vielfaches des Minimalpolynoms von α ist. Aus Proposition 1.0.2.(ii) folgt das

Korollar 1.0.3. *Ist K ein Zahlkörper und $\mathfrak{a} \neq (0)$ ein Ideal von $\mathcal{O}_K$, so ist der Quotientenring $\mathcal{O}_K/\mathfrak{a}$ endlich.*

Beweis. Sei $\alpha \neq 0$ ein Element aus $\mathfrak{a}$. Dann existieren für $i = 1, \ldots, n$ Zahlen $a_i \in \mathbb{Z}$, $a_n \neq 0$, mit $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$, und folglich ist $a_n \in \mathfrak{a} \cap \mathbb{Z}$. Der Homomorphismus $\mathcal{O}_K/a_n\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$ ist surjektiv und mit Prop. 1.0.2.(ii) sieht man, dass $|\mathcal{O}_K/\mathfrak{a}| \leq |O_K/a_n\mathcal{O}_K| = a_n^{[K:\mathbb{Q}]}$ endlich ist. □

Bemerkung. Ein $\mathcal{O}_K$-Ideal $\mathfrak{a} \neq 0$ ist ein freier $\mathbb{Z}$-Modul von Rang $[K:\mathbb{Q}]$! Es ist nämlich zunächst $\mathfrak{a}$ ein freier $\mathbb{Z}$-Untermodul von $\mathcal{O}_K$. Da $\mathbb{Z}$ ein Hauptidealring ist, muss Rang $\mathfrak{a} \leq$ Rang $\mathcal{O}_K$ sein. Da $|\mathcal{O}_K/\mathfrak{a}|$ endlich ist, muss Gleicheit herrschen.

Angeregt durch Korollar 1.0.3 ist die

Definition 1.0.4. Ist $\mathfrak{a} \neq (0)$ ein $\mathcal{O}_K$-Ideal, so definiert man $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$ als die **Norm** von $\mathfrak{a}$ und setzt für das Nullideal $N((0)) := 0$.

Im Gegensatz zum Ganzheitsring $\mathbb{Z}$ von $\mathbb{Q}$ sind beliebige Ganzheitsringe $\mathcal{O}_K$ im Allgemeinen nicht faktoriell. Es gibt jedoch eine ebenso gute Eigenschaft auf Idealebene.

Theorem 1.0.5. *Ist $\mathcal{O}_K$ der Ganzheitsring eines Zahlkörpers K, so ist $\mathcal{O}_K$ ein Dedekind-Ring. Das bedeutet:*

(i) *$\mathcal{O}_K$ ist ganz abgeschlossen: ist $\alpha \in K$ Nullstelle eines normierten Polynoms mit Koeffizienten in $\mathcal{O}_K$, so gilt schon $\alpha \in \mathcal{O}_K$.*

(ii) *$\mathcal{O}_K$ ist noethersch.*

(iii) *Jedes von Null verschiedene Primideal von $\mathcal{O}_K$ ist maximal.*

Beweis. Siehe [9, Kapitel 3, Thm. 14]. □

Korollar 1.0.6. *Ist K ein Zahlkörper, so besitzt jedes von Null verschiedene Ideal $\mathfrak{a} \in \mathcal{O}_K$ eine Darstellung*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

mit Primidealen $\mathfrak{p}_i \in \mathcal{O}_K$. Die Darstellung ist bis auf die Reihenfolge eindeutig und die $\mathfrak{p}_i$ sind genau die Primideale von $\mathcal{O}_K$, die $\mathfrak{a}$ enthalten.

Beweis. Siehe [9, Kapitel 3, Thm. 16]. □

Definition und Bemerkung 1.0.7. Man „erweitert“ die Definition von Idealen und führt gebrochene Ideale ein. Ein **gebrochenes Ideal** $\mathfrak{a}$ von $\mathcal{O}_K$ ist ein endlich erzeugter $\mathcal{O}_K$-Modul von K ungleich Null.
Der Name gebrochenes Ideal erklärt sich durch die Tatsache, dass $\mathfrak{a} \subseteq K$ genau dann ein gebrochenes $\mathcal{O}_K$-Ideal ist, wenn ein Element $d \in \mathcal{O}_K$ ungleich Null existiert, sodass $d\mathfrak{a}$ ein $\mathcal{O}_K$-Ideal ist.

Die Menge der Ideale bildet bzgl. der Idealmultiplikation ein kommutatives Monoid. Für gebrochene Ideale ergibt sich ein schöneres Bild.

Proposition 1.0.8. *Sei $\mathfrak{a}$ ein gebrochenes $\mathcal{O}_K$-Ideal ungleich Null.*

(i) *$\mathfrak{a}$ besitzt eine eindeutige Darstellung als $\prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$ mit $r_i \in \mathbb{Z}$ und paarweise verschiedenen $\mathcal{O}_K$-Primidealen $\mathfrak{p}_i$.*

(ii) *$\mathfrak{a}$ ist invertierbar: es existiert ein gebrochenes $\mathcal{O}_K$-Ideal $\mathfrak{a}^{-1}$, sodass $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$ ist.*

Beweis. Siehe [10, Kapitel 3.4, Thm. 3]. □

Bezeichnet man mit I_K die Menge der gebrochenen $\mathcal{O}_K$-Ideale, so zeigt Proposition 1.0.8 gerade, dass I_K eine kommutative Gruppe unter der Idealmultiplikation ist.
Bezeichnet weiter $P_K \subseteq I_K$ die Untergruppe der gebrochenen $\mathcal{O}_K$-Hauptideale, d. h. solche der Gestalt $\alpha\mathcal{O}_K$ für ein $\alpha \in K^*$, so kann man den Quotienten bilden.

Definition 1.0.9. Es heißt $\mathcal{C}(\mathcal{O}_K) := I_K/P_K$ die **Idealklassengruppe** von $\mathcal{O}_K$.

Es gilt das bemerkenswerte

Theorem 1.0.10. *Die Idealklassengruppe eines Zahlkörpers ist endlich.*

Beweis. Siehe [9, Kapitel 5, Kor. 2]. □

1.1 Verzweigungstheorie

Betrachten wir eine endliche Zahlkörpererweiterung $L \supseteq K$, so stellt sich die Frage, wie sich ein $\mathcal{O}_K$-Primideal $\mathfrak{p}$, aufgefasst als Ideal $\mathfrak{p}\mathcal{O}_L$, in $\mathcal{O}_L$ verhält. Sicher muss $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$ in ein Produkt von Primidealen zerfallen, besitzt also eine Darstellung

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r},$$

wobei die $\mathfrak{P}_i$ die paarweise verschiedenen Primideale von $\mathcal{O}_L$ sind, die $\mathfrak{p}\mathcal{O}_L$ enthalten. Die Zahl $e_{\mathfrak{P}_i|\mathfrak{p}} = e_i$ heißt **Verzweigungsindex** von $\mathfrak{P}_i$ über $\mathfrak{p}$.
Weiter gibt uns ein über $\mathfrak{p}$ liegendes $\mathcal{O}_L$-Primideal $\mathfrak{P}_i$ die Kette endlicher Körper $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{P}_i$. Der Grad $f_{\mathfrak{P}_i|\mathfrak{p}}$ dieser Körpererweiterung heißt **Restklassengrad** von $\mathfrak{P}_i$ über $\mathfrak{p}$.

Die Verzweigungsindizes und Restklassengrade verhalten sich bei Idealketten multiplikativ. Sind $K \subseteq L \subseteq M$ Zahlkörper mit Primidealen $\mathfrak{p} \subseteq \mathfrak{P} \subseteq \mathfrak{Q}$, so gilt $e_{\mathfrak{Q}|\mathfrak{p}} = e_{\mathfrak{Q}|\mathfrak{P}} e_{\mathfrak{P}|\mathfrak{p}}$ und $f_{\mathfrak{Q}|\mathfrak{p}} = f_{\mathfrak{Q}|\mathfrak{P}} f_{\mathfrak{P}|\mathfrak{p}}$.

Theorem 1.1.1. *Sei $K \subseteq L$ eine Erweiterung von Zahlkörpern und $\mathfrak{p}$ ein Primideal von K (d. h. von $\mathcal{O}_K$). Bezeichnen $e_{\mathfrak{P}_i|\mathfrak{p}}$ und $f_{\mathfrak{P}_i|\mathfrak{p}}$ die oben definierten Verzweigungsindizes bzw. Restklassengrade, so gilt*

$$\sum_{i=1}^{r} e_{\mathfrak{P}_i|\mathfrak{p}} f_{\mathfrak{P}_i|\mathfrak{p}} = [L : K].$$

Beweis. Siehe [9, Kapitel 3, Thm. 21]. □

Ist L/K eine normale Erweiterung, also galois'sch, so vereinfacht sich die Darstellung.

Theorem 1.1.2. *Seien K, L Zahlkörper und L/K galois'sch, sowie $\mathfrak{p}$ ein Primideal von K.*

(i) Die Galois-Gruppe $Gal(L : K)$ operiert transitiv auf den über $\mathfrak{p}$ liegenden Primidealen von L: sind $\mathfrak{P}$ und $\mathfrak{P}'$ zwei Primideale von L über $\mathfrak{p}$, so existiert ein $\sigma \in Gal(L : K)$, sodass $\sigma(\mathfrak{P}) = \mathfrak{P}'$ gilt.

(ii) Die $\mathcal{O}_L$-Primideale $\mathfrak{P}_1, \dots \mathfrak{P}_r$ über $\mathfrak{p}$ besitzen alle den selben Verzweigungsindex e und Restklassengrad f, sodass sich die Formel aus Theorem 1.1.1 zu

$$ref = [L : K]$$

vereinfacht.

Beweis. Siehe [9, Kapitel 3, Thm. 23 und folgendes Korollar]. □

Bezeichnung. Ist eine Zahlkörpererweiterung L/K gegeben, so heißt ein Primideal $\mathfrak{p}$ von K **verzweigt** in L, wenn $e_{\mathfrak{P}|\mathfrak{p}} > 1$ für ein Primideal $\mathfrak{P} \subset \mathcal{O}_L$ über $\mathfrak{p}$ gilt.
Ist $e_{\mathfrak{P}|\mathfrak{p}} = 1$ für alle $\mathcal{O}_L$-Prinideale $\mathfrak{P}$ über $\mathfrak{p}$, so heißt $\mathfrak{p}$ **unverzweigt**. Gilt stets die stärkere Bedingung $e_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{p}} = 1$, so heißt $\mathfrak{p}$ **vollständig zerlegt** in L.
Die Eigenschaft eines Primideals verzweigt zu sein tritt jedoch selten auf, denn es gilt

Proposition 1.1.3. *Ist L/K eine Erweiterung von Zahlkörpern, so sind nur endlich viele Primideale $\mathfrak{p} \subset \mathcal{O}_K$ verzweigt in $\mathcal{O}_L$.*

Beweis. Siehe [9, Kor. 3 zu Thm. 24]. □

Ist L/K eine Zahlkörpererweiterung, so existiert ein Element $\alpha \in L$ mit $K(\alpha) = L$. Da auch $[L : \mathbb{Q}] = m$ endlich ist, existiert ein Polynom $g(X) \in \mathbb{Q}[X]$ mit $g(\alpha) = \alpha^m + b_1\alpha^{m-1} + \dots + b_m = 0$.
Ist $b \in \mathbb{Z}$ der Hauptnenner der Koeffizienten, so ist auch $(b\alpha)^m + b_1 b(b\alpha)^{m-1} + \dots + b_m b^m = 0$.

Da die $b_i b^i$ in $\mathbb{Z}$ liegen, ist $b\alpha$ eine ganze Zahl, also aus $\mathcal{O}_L$. Weiter ergibt sich schnell, dass $\mathbb{Q}(\alpha) = \mathbb{Q}(b\alpha)$ ist und damit auch $L = K(b\alpha)$ gilt.
Ist eine Zahlkörpererweiterung L/K gegeben, so können wir also o. B. d. A. annehmen, dass diese von einem Element α aus $\mathcal{O}_L$ erzeugt wird. Es ist dann $\mathcal{O}_K[\alpha]$ eine Untergruppe von $\mathcal{O}_L$ mit endlichem Index (denn beide Gruppen sind freie abelsche Gruppen von Rang $[L : \mathbb{Q}]$).

Wie die Zerlegung eines Primideals von $\mathcal{O}_K$ in $\mathcal{O}_L$ aussieht, lässt sich explizit angeben.

Theorem 1.1.4. *Seien $K \subseteq L$ Zahlkörper und $L = K(\alpha)$ mit $\alpha \in \mathcal{O}_L$, sowie $g(X) \in \mathcal{O}_K[X]$ das Minimalpolynom von α über K.*

Weiter sei $\mathfrak{p}$ ein $\mathcal{O}_K$-Primideal, es werde $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$ nicht von $p = \mathfrak{p} \cap \mathbb{Z}$ geteilt und $g(X)$ zerfalle modulo $\mathfrak{p}$ in paarweise verschiedene, irreduzible Polynome $g_i(X) \in \mathcal{O}_K[X]$,

$$g(X) \equiv \prod_{i=1}^{r} g_i(X)^{e_i} \bmod \mathfrak{p}.$$

Die $g_i(X)$ seien normiert und es gelte $deg(g_i(X)) = deg(g_i(X)) \bmod \mathfrak{p}$.

Dann gilt:

(i) Die Ideale

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$$

sind die paarweise verschiedenen $\mathcal{O}_L$-Primideale mit $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$.

(ii) Die Primideale $\mathfrak{P}_i$ besitzen die Restklassengrade $f_{\mathfrak{P}_i|\mathfrak{p}} = deg(g_i(X))$ und Verzweigungsindizes $e_{\mathfrak{P}_i|\mathfrak{p}} = e_i$.

Beweis. Siehe [9, Kapitel 3, Thm. 27]. □

1.2 Imaginär-quadratische Zahlkörper

In diesem Abschnitt bezeichne K stets einen imaginär-quadratischer Zahlkörper, d. h. eine quadratische Erweiterung von $\mathbb{Q}$ die nicht in $\mathbb{R}$ liegt.
Es ist also $K = \mathbb{Q}(\sqrt{N})$ für ein $-N \in \mathbb{N}$ nach den Erläuterungen auf Seite 3 und N kann o. B. d. A. als quadratfrei vorausgesetzt werden. Die **Diskriminante** $discr(K) = d_K$ von K ist definiert als

$$d_K := \begin{cases} 4N & : \quad N \not\equiv 1 \bmod 4 \\ N & : \quad N \equiv 1 \bmod 4. \end{cases}$$

Die Diskriminante charakterisiert den Zahlkörper eindeutig, denn es ist $K = \mathbb{Q}(\sqrt{d_K})$. Außerdem gilt stets $d_K \equiv 0, 1 \bmod 4$.
Der Ganzheitsring eines quadratischen Zahlkörpers besitzt folgende Gestalt:

$$\mathcal{O}_K = \left\{ \begin{array}{lcl} \mathbb{Z}[\sqrt{N}] & : & N \not\equiv 1 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & : & N \equiv 1 \bmod 4. \end{array} \right\} = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right].$$

Mit $\omega_K := \frac{d_K + \sqrt{d_K}}{2}$ können wir allgemeingültig $\mathcal{O}_K = \mathbb{Z}[\omega_K]$ schreiben. Es ist

$$f_K(X) := \begin{cases} X^2 - N & : \quad N \not\equiv 1 \bmod 4 \\ X^2 - X + \frac{-N+1}{4} & : \quad N \equiv 1 \bmod 4, \end{cases}$$

das Minimalpolynom von $\sqrt{N}$ bzw. $(1 + \sqrt{N})/2$ über $\mathbb{Q}$. Für die Einheiten von $\mathcal{O}_K$ gilt folgende Charakterisierung

$$\alpha \in \mathcal{O}_K^* \quad \Longleftrightarrow \quad \alpha \in \mathcal{O}_K \text{ und } N_{K/\mathbb{Q}}(\alpha) = 1.$$

Lemma 1.2.1. *Für die Einheitengruppe $\mathcal{O}_K^*$ gilt einer der folgenden Fälle.*

- *Ist $K = \mathbb{Q}(\sqrt{-3})$, so ist $\mathcal{O}_K^* = \{\pm 1, \pm\omega, \pm\omega^2\}$ für $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$.*
- *Ist $K = \mathbb{Q}(\sqrt{-1})$, so ist $\mathcal{O}_K^* = \{\pm 1, \pm i\}$.*
- *In allen anderen Fällen gilt $\mathcal{O}_K^* = \{\pm 1\}$.*

Beweis. Siehe [3, Übung 5.9]. □

Als Spezialisierung des Theorems 1.1.4 erhalten wir

Proposition 1.2.2. *Bezeichne $\alpha \mapsto \overline{\alpha}$ den nichttrivialen Automorphismus von K und $p \in \mathbb{Z}$ eine Primzahl.*

(i) Ist $(d_K/p) = 0$, so ist $p\mathcal{O}_K = \mathfrak{p}^2$ für ein Primideal $\mathfrak{p}$ von $\mathcal{O}_K$.
(ii) Ist $(d_K/p) = 1$, so ist $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ für Primideale $\mathfrak{p} \neq \overline{\mathfrak{p}}$ von $\mathcal{O}_K$.
(iii) Ist $(d_K/p) = -1$, so ist $p\mathcal{O}_K$ ein Primideal von $\mathcal{O}_K$.

Beweis. Siehe [3, Prop. 5.16]. □

Wir wissen bereits, das $\mathcal{O}_K$-Ideale $\mathbb{Z}$-Moduln von Rang 2 sind. Über eine explizite Darstellung gibt das folgende Lemma Auskunft.

Lemma 1.2.3. *Ist $\mathfrak{a} \neq 0$ ein $\mathcal{O}_K$-Ideal des imaginär-quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{N})$ und setzen wir $a = min(\mathfrak{a} \cap \mathbb{N})$, so existiert ein Element $v \in \mathcal{O}_K - \mathbb{Z}$ mit $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}v$.*
Schreiben wir $\mathcal{O}_K = \mathbb{Z}[w]$, wobei ω eine Nullstelle des Polynoms $f_K(X)$ ist, und ist $v = b + c\omega$ mit $b, c \in \mathbb{Z}$, so gilt:

$$a \equiv b \equiv 0 \bmod c \qquad \text{und} \qquad N_{K/\mathbb{Q}}(b + c\omega) \equiv 0 \bmod ac.$$

Beweis. Zunächst ist $\mathbb{Z}a = \mathfrak{a} \cap \mathbb{Z}$ ein $\mathbb{Z}$-Ideal ungleich Null. Schreiben wir $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ wie oben, so ist

$$C = \{c \in \mathbb{Z} : \exists\, b \in \mathbb{Z} \text{ mit } b + c\omega \in \mathfrak{a}\}$$

ebenfalls ein Ideal in $\mathbb{Z}$. Da wegen $a \in \mathfrak{a}$ auch $a\omega \in \mathfrak{a}$ liegt, gilt $\mathbb{Z}a \subseteq C$. Es wird C von einem Element $c \in \mathbb{N}$ erzeugt, $C = \mathbb{Z}c$. Da $c \in C$ liegt, gibt es ein $b \in \mathbb{Z}$ mit $b + c\omega =: v \in \mathfrak{a}$. Dann ist $v \in \mathcal{O}_K - \mathbb{Z}$ und $\mathbb{Z}a + \mathbb{Z}v \subseteq \mathfrak{a}$.
Ist andererseits $x \in \mathfrak{a} \subset \mathcal{O}_K$ beliebig gewählt, so existieren zunächst Zahlen $f, g \in \mathbb{Z}$ mit $x = f + g\omega$. Es ist dann $g \in C$, also $g = hc$ für ein $h \in \mathbb{Z}$. Folglich ist $x = f + hc\omega = f + h(v - b)$, also

$$x - hv = f - hb \in \mathfrak{a} \cap \mathbb{Z} = \mathbb{Z}a,$$

und deshalb $x \in \mathbb{Z}a + \mathbb{Z}v$.
Mit a und $b + c\omega$ liegen auch ωa und $\omega(b + c\omega)$ in $\mathfrak{a}$. Also ist

$$\omega a = \alpha a + \beta(b + c\omega) \qquad \text{und} \qquad \omega(b + c\omega) = \gamma a + \delta(b + c\omega) \qquad \text{für } \alpha, \beta, \gamma, \delta \in \mathbb{Z}.$$

Aus der ersten Gleichung folgt $a = \beta c$ und $\alpha a + \beta b = 0$. Da $\mathfrak{a}$ ein $\mathbb{Z}$-Modul von Rang 2 ist, ist $\beta \neq 0$ und Einsetzen liefert $-b = \alpha c$. Dies zeigt $a \equiv b \equiv 0 \bmod c$.
Multiplikation der zweiten Gleichung mit dem Konjugierten $(b + c\overline{\omega})$ gibt

$$\omega N_{K/\mathbb{Q}}(b + c\omega) = \gamma a(b + c\overline{\omega}) + \delta N_{K/\mathbb{Q}}(b + c\omega).$$

Ist $\omega = \frac{1+\sqrt{N}}{2}$, so ist $\overline{\omega} = 1 - \omega$. Wir erhalten

$$\omega N_{K/\mathbb{Q}}(b + c\omega) = \gamma a(b + c(1 - \omega)) + \delta N_{K/\mathbb{Q}}(b + c\omega)$$

und es folgt $N_{K/\mathbb{Q}}(b + c\omega) = -\gamma ac$. Der Fall $\omega = \sqrt{N}$ liefert ebenfalls $N_{K/\mathbb{Q}}(b + c\omega) = -\gamma ac$. Deshalb gilt $N_{K/\mathbb{Q}}(b + c\omega) \equiv 0 \bmod ac$. □

Definition und Bemerkung 1.2.4. Wir schreiben entsprechend den obigen Bezeichnungen Ideale $\mathfrak{a}$ auch in der Gestalt $\mathfrak{a} = [a, b + c\omega]$ als $\mathbb{Z}$-Moduln.
Gilt $ggT(a, b, c) = 1$, so nennen wir $\mathfrak{a}$ ein **primitives** Ideal. Ein Element $\alpha \in \mathcal{O}_K$ heißt primitiv, wenn das von ihm erzeugte Hauptideal (α) primitiv ist. Es ist offensichtlich, dass jedes $\mathcal{O}_K$-Ideal $\mathfrak{a}$ eine Darstellung $\mathfrak{a} = d\mathfrak{b}$ mit $d \in \mathbb{Z}$ und einem primitiven $\mathcal{O}_K$-Ideal $\mathfrak{b}$ besitzt.Über die Darstellung primitiver Ideale als $\mathbb{Z}$-Moduln gibt das folgende Lemma Auskunft.

Lemma 1.2.5. *Ist $\mathfrak{a}$ ein $\mathcal{O}_K$-Ideal und sind $f_K(X)$ und ω wie oben gewählt, so gilt:*

$$\mathfrak{a} \text{ ist primitiv mit } N(\mathfrak{a}) = N_0 \iff \begin{array}{c}\mathfrak{a} = [N_0, \omega - r] \text{ für ein } r \in \mathbb{Z} \\ \text{mit } f_K(r) \equiv 0 \bmod N_0.\end{array}$$

Beweis. „⇐“: Da $ggT(N_0, -r, 1) = 1$ gilt, ist $\mathfrak{a}$ primitiv. Außerdem ist $N(\mathfrak{a}) = det \begin{pmatrix} N_0 & 0 \\ -r & 1 \end{pmatrix} = N_0$ nach Lemma A.0.2. „⇒“: Es besitzt $\mathfrak{a}$ nach Lemma 1.2.3 die Gestalt $\mathfrak{a} = [a, b + c\omega]$ und es gilt $c|a$, $c|b$ und $N_{K/\mathbb{Q}}(b + c\omega) \equiv 0 \bmod ac$. Da $\mathfrak{a}$ primitiv ist, gilt $ggT(a, b, c) = 1$ und es folgt $c = \pm 1$. Da $N(\mathfrak{a}) = ac = N_0$ gilt, muss $a = \pm N_0$ sein. O. B. d. A. sei wir $c = 1$ und $a = N_0$. Es ist dann $\mathfrak{a} = [N_0, \omega - r]$ mit $-r := b$ und $f_K(r) = N_{K/\mathbb{Q}}(\omega - r) \equiv 0 \bmod N_0$. □

1.3 Ordnungen in quadratischen Zahlkörpern

In diesem Abschnitt bezeichne K stets einen quadratischen Zahlkörper.

Definition 1.3.1. Eine **Ordnung** von K ist eine Teilmenge $\mathcal{O} \subseteq K$ und es gilt

(i) $\mathcal{O}$ ist ein Unterring von K mit 1.
(ii) $\mathcal{O}$ ist ein endlich erzeugter $\mathbb{Z}$-Modul.
(iii) $\mathcal{O}$ enthält eine $\mathbb{Q}$-Basis von K.

Da K torsionsfrei ist, ist $\mathcal{O}$ ein freier $\mathbb{Z}$-Modul, der wegen Bedingung (iii) von Rang $2 = [K : \mathbb{Q}]$ ist.
Aus der Charakterisierung des Ganzheitsringes $\mathcal{O}_K$ in Proposition 1.0.2 ist ersichtlich, dass $\mathcal{O}_K$ stets eine Ordnung ist. Ist x ein Element einer Ordnung $\mathcal{O}$, so ist $\mathbb{Z}[x]$ ein $\mathbb{Z}$-Untermodul von $\mathcal{O}$. Da $\mathbb{Z}$ ein Hauptidealring ist, ist $\mathbb{Z}[x]$ ein endlich erzeugter $\mathbb{Z}$-Modul. Theorem A.0.1 sagt dann, dass x in $\mathcal{O}_K$ liegt. Es gilt also stets $\mathcal{O} \subseteq \mathcal{O}_K$, und $\mathcal{O}_K$ heißt deshalb auch **Maximalordnung**. Es gilt das

Lemma 1.3.2. *Sei $\mathcal{O}$ eine Ordnung von K, so besitzt $\mathcal{O}$ endlichen Index f in $\mathcal{O}_K$ und es ist*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, fw_K].$$

Beweis. Es sind $\mathcal{O}$ und $\mathcal{O}_K$ freie $\mathbb{Z}$-Moduln von Rang 2. Wir können daher $\mathcal{O}_K \cong \mathbb{Z} \times \mathbb{Z}$ annehmen, und da $\mathcal{O} \subseteq \mathcal{O}_K$ gilt, ist $\mathcal{O} \cong d_1\mathbb{Z} \times d_2\mathbb{Z}$ mit d_1, $d_2 \in \mathbb{Z}$. Folglich besitzt $\mathcal{O}$ endlichen Index $f = |d_1 d_2|$ in $\mathcal{O}_K$.
Ist $f = [\mathcal{O}_K : \mathcal{O}]$, so gilt $f\mathcal{O}_K \subseteq \mathcal{O}$, also auch $\mathbb{Z} + f\mathcal{O}_K \subseteq \mathcal{O}$. Weiter ist $\mathbb{Z} + f\mathcal{O}_K = [1, fw_K]$, wie man unmittelbar aus der Darstellung von $\mathcal{O}_K$ in Abschntt 1.2 abliest. Da $[1, fw_K]$ offensichtlich Index f in $[1, w_K] = \mathcal{O}_K$ besitzt, gilt Gleichheit, also $O = \mathbb{Z} + f\mathcal{O}_K = [1, fw_K]$. □

Definition 1.3.3. Ist $\mathcal{O}$ eine Ordnung von K, so heißt der Index $f = [\mathcal{O}_K : \mathcal{O}]$ der **Führer** der Ordnung $\mathcal{O}$.

Lemma 1.3.4. *Ist $\mathcal{O}$ eine Ordnung des imaginär-quadratischen Zahlkörpers K, so gilt $\{\pm 1\} \subseteq \mathcal{O}^*$. Ist $\mathcal{O}^* \neq \{\pm 1\}$, so muss $\mathcal{O} = \mathcal{O}_K$ für $K = \mathbb{Q}(\sqrt{-1})$ oder $K = \mathbb{Q}(\sqrt{-3})$ sein.*

Beweis. Natürlich gilt $\mathcal{O}^* \subseteq \mathcal{O}_K^*$ und aus Lemma 1.3.2 ist ersichtlich, dass stets $\{\pm 1\} \subseteq \mathcal{O}^*$ gilt. Leichte Fallunterscheidungen zeigen die Behauptung. □

Definition und Bemerkung 1.3.5. Ist $x \mapsto \overline{x}$ der nichttriviale Automorphismus von K und eine Ordnung $\mathcal{O} = [\alpha, \beta]$ von K gegeben, so heißt

$$D := \left(\det \begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix}\right)^2$$

die **Diskriminante** von $\mathcal{O}$. Sie ist unanhängig von der gewählten Basis. Stellen wir $\mathcal{O} = [1, fw_K]$ wie oben dar, so ist $D = f^2 d_K$. Die Diskriminante erfüllt also ebenfalls $D \equiv 0, 1 \bmod 4$ und $K = \mathbb{Q}(\sqrt{D})$. Die Diskriminante D bestimmt die Ordnung $\mathcal{O}$ eindeutig, denn es ist $\mathcal{O} = [1, w_D]$ mit $w_D = \frac{D+\sqrt{D}}{2}$. Wir schreiben deshalb auch $\mathcal{O} = \mathcal{O}_D$.

Analog zum Fall der Maximalordnung betrachtet man Ideale $\mathfrak{a}$ von $\mathcal{O}$. Der Beweis von Kor. 1.0.3 überträgt sich auf $\mathcal{O}$-Ideale, sodass wir auch hier die **Norm** von $\mathfrak{a}$ als $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ definieren können.

Ebenfalls überträgt sich der Beweis von Lemma 1.2.3 leicht auf $\mathcal{O}$-Ideale. Der Begriff **primitives** $\mathcal{O}$-Ideal ist dann analog zu verstehen.

Ist $\mathfrak{a} \subset \mathcal{O}$ ein Ideal, so gilt stets

$$\mathcal{O} \subseteq \{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\}.$$

Tritt sogar Gleicheit ein, was nicht immer der Fall ist, so heißt $\mathfrak{a}$ ein **eigentliches** $\mathcal{O}$-Ideal.
Jedes Hauptideal von $\mathcal{O}$ ist eigentlich und alle Ideale der Maximalordnung $\mathcal{O}_K$ sind eigentlich. Die Definition erweitern man ohne Schwierigkeiten auf gebrochene $\mathcal{O}$-Ideale.

Es stellt sich nun in natürlicherweise die Frage nach der Invertierbarkeit von Idealen einer Ordnung $\mathcal{O}$. Da $\mathcal{O} = [1, fw_K]$ für $f > 1$ nicht ganz abgeschlossen in K ist, also kein Dedekind-Ring ist, können wir auch keine eindeutige Zerlegung von Idealen in Primideale erwarten. Welche gebrochenen $\mathcal{O}$-Ideale sind also invertierbar?

Lemma 1.3.6. *Sei $K = \mathbb{Q}(\tau)$ und $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ das Minimalpolynom von τ und gelte ggT(a,b,c)=1. Dann ist $[1, \tau]$ ein gebrochenes eigentliches Ideal der Ordnung $[1, a\tau]$ von K.*

Beweis. Zunächst ist wegen $af(\tau) = 0$ $a\tau$ algebraisch ganz und deshalb $\mathcal{O} = [1, a\tau]$ eine Ordnung von K. Weiter ist $[1, \tau] = \frac{1}{a}[a, a\tau]$ ein gebrochenes $\mathcal{O}$-Ideal.
Ist $\beta \in K$ und gilt $\beta[1, \tau] \subseteq [1, \tau]$, so existieren also $m, n \in \mathbb{Z}$ mit $\beta = \beta \cdot 1 = m + n\tau$. Weiter ist auch $\beta\tau \in [1, \tau]$, also

$$\begin{aligned} \beta\tau &= m\tau + n\tau^2 = m\tau + \tfrac{n}{a}(-b\tau - c) \\ &= \tfrac{-cn}{a} + \left(\tfrac{-bn}{a} + m\right)\tau. \end{aligned}$$

Da $ggT(a, b, c) = 1$ ist, gilt $\beta\tau \in [1, \tau]$ genau dann, wenn n von a geteilt wird. Also ist $\beta = m \cdot 1 + t \cdot a\tau$ in $[1, a\tau]$ für ein $t \in \mathbb{Z}$. □

Proposition 1.3.7. *Sei $\mathcal{O}$ eine Ordnung von K und $\mathfrak{a}$ ein gebrochenes $\mathcal{O}$-Ideal. Es ist $\mathfrak{a}$ genau dann invertierbar, wenn $\mathfrak{a}$ eigentlich ist.*

Beweis. Sei zunächst $\mathfrak{a}$ invertierbar, d. h. es existiert ein gebrochenes $\mathcal{O}$-Ideal $\mathfrak{b}$ mit $\mathfrak{ab} = \mathcal{O}$. Ist

dann $\beta \in K$ mit $\beta\mathfrak{a} \subseteq \mathfrak{a}$, so gilt

$$\beta\mathcal{O} = \beta(\mathfrak{a}\mathfrak{b}) = (\beta\mathfrak{a})\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} = \mathcal{O},$$

und folglich ist $\mathfrak{a}$ eigentlich.

Sei andererseits $\mathfrak{a}$ als eigentlich vorausgesetzt. Wie in der Bemerkung nach Kor. 1.0.3 schließt man, dass $\mathfrak{a}$ ein $\mathbb{Z}$-Modul von Rang 2 ist, also eine Darstellung $\mathfrak{a} = [\alpha, \beta]$ mit α, $\beta \in K$ existiert. Das heißt $\mathfrak{a} = \alpha[1, \tau]$ mit $\tau = \beta/\alpha \in K - \mathbb{Q}$. Ist $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ das Minimalpolynom von τ, $ggT(a, b, c) = 1$, so sagt Lemma 1.3.6, dass $[1, \tau]$ ein gebrochenes eigentliches Ideal von $[1, a\tau]$ ist. Ist $\beta \in K$ mit $\beta\mathfrak{a} \subseteq \mathfrak{a}$, so folgt durch Multiplikation mit α^{-1} dann wegen $\beta[1, \tau] \subseteq [1, \tau]$, dass $\beta \in [1, a\tau]$ liegt. Da offensichtlich $[1, a\tau]\mathfrak{a} \subseteq \mathfrak{a}$ gilt, ist deshalb $\mathcal{O} = [1, a\tau]$.
Bezeichne $x \mapsto \overline{x}$ den nichttrivialen Automorphismus von K, so ist $\overline{\tau}$ die zweite Nullstelle von $f(x)$. Nach Lemma 1.3.6 ist dann $\overline{\mathfrak{a}} = \overline{\alpha}[1, \overline{\tau}]$ ein gebrochenes Ideal von $\overline{\mathcal{O}} = \mathcal{O}$ (benutze die Darstellung $\mathcal{O} = [1, fw_K]$).
Wir behaupten

$$\mathfrak{a}\overline{\mathfrak{a}} = \frac{N_{K/\mathbb{Q}}(\alpha)}{a}\mathcal{O}.$$

Es ist nämlich zunächst

$$a\mathfrak{a}\overline{\mathfrak{a}} = a\alpha\overline{\alpha}[1, \tau][1, \overline{\tau}] = N_{K/\mathbb{Q}}(\alpha)[a, a\tau, a\overline{\tau}, a\tau\overline{\tau}].$$

Da $\tau + \overline{\tau} = -b/a$ und $\tau\overline{\tau} = c/a$ ist, erhält man unter Benutzung von $ggT(a, b, c) = 1$

$$a\mathfrak{a}\overline{\mathfrak{a}} = N_{K/\mathbb{Q}}(\alpha)[a, a\tau, -b, c] = N_{K/\mathbb{Q}}(\alpha)\mathcal{O}.$$

□

Definition und Bemerkung 1.3.8. Bezeichnet $I(\mathcal{O})$ die Menge der gebrochenen eigentlichen $\mathcal{O}$-Ideale, so bilden diese nach Prop. 1.3.7 eine Gruppe. In $I(\mathcal{O})$ liegt die Untergruppe $P(\mathcal{O})$ der gebrochenen eigentlichen $\mathcal{O}$-Hauptideale. Der Quotient

$$\mathcal{C}(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$$

heißt die **Idealklassengruppe zur Ordnung** $\mathcal{O}$. Der Beweis von Prop. 1.3.7 zeigt dann gerade, dass das Inverse einer Idealklasse seine konjugierte Idealklasse ist. Dies gilt insbesondere für die Idealklassen von $\mathcal{C}(\mathcal{O}_K)$.

Die Norm von $\mathcal{O}$-Idealen verhält sich ebenso wie die Norm für Elemente aus K multiplikativ und es besteht ein enger Zusammenhang zwischen beiden. Genaueres sagt das folgende

Lemma 1.3.9. *Sei $\mathcal{O}$ eine Ordnung des imaginär-quadratischen Zahlkörpers K, so gilt:*

(i) $N(\alpha\mathcal{O}) = N_{K/\mathbb{Q}}(\alpha)$ *für* $\alpha \in \mathcal{O}$, $\alpha \neq 0$.

(ii) $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ *für eigentliche $\mathcal{O}$-Ideale* $\mathfrak{a}$ *und* $\mathfrak{b}$.

(iii) $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$ *für eigentliche $\mathcal{O}$-Ideale* $\mathfrak{a}$.

Beweis. (i) Sei $A \in M_2(\mathbb{Z})$ die Darstellungsmatrix des $\mathbb{Z}$-Modul-Endomorphismus $m_\alpha : \mathcal{O} \to \mathcal{O}$, $x \mapsto \alpha x$. Da $\alpha \neq 0$ und $\mathcal{O}$ nullteilerfrei ist, muss m_α injektiv, also $det(A) \neq 0$ sein. Es ist nach Definition der Norm $N_{K/\mathbb{Q}}(\alpha) = |det(A)|$. Da $\alpha\mathcal{O} = A\mathcal{O}$ ist, gibt uns Lemma A.0.2 $N(\alpha\mathcal{O}) = |det(A)|$ und die Behauptung ist gezeigt.

Sei $\alpha \in \mathcal{O}$ von Null verschieden und $\mathfrak{a}$ ein eigentliches $\mathcal{O}$-Ideal. Wegen $\alpha\mathfrak{a} \subseteq \alpha\mathcal{O} \subseteq \mathcal{O}$ ist dann

$$0 \to \alpha\mathcal{O}/\alpha\mathfrak{a} \to \mathcal{O}/\alpha\mathfrak{a} \to \mathcal{O}/\alpha\mathcal{O} \to 0$$

eine exakte Sequenz und folglich $|\mathcal{O}/\alpha\mathfrak{a}| = |\mathcal{O}/\alpha\mathcal{O}| \cdot |\alpha\mathcal{O}/\alpha\mathfrak{a}|$. Multiplikation mit α induziert einen Isomorphismus $\mathcal{O}/\mathfrak{a} \simeq \alpha\mathcal{O}/\alpha\mathfrak{a}$, so dass wir in diesem Spezialfall

$$N(\alpha\mathfrak{a}) = |\mathcal{O}/\alpha\mathfrak{a}| = |\mathcal{O}/\alpha\mathcal{O}| \cdot |\alpha\mathcal{O}/\alpha\mathfrak{a}| = N_{K/\mathbb{Q}}(\alpha) \cdot |\mathcal{O}/\mathfrak{a}| = N_{K/\mathbb{Q}}(\alpha)N(\mathfrak{a})$$

erhalten.
Schreiben wir $\mathfrak{a} = \alpha[1, \tau]$, so muss nach Lemma 1.3.6 $\mathcal{O} = [1, a\tau]$ für ein $a \in \mathbb{N}$ sein. Da $[a, a\tau]$ Index a in $[1, a\tau]$ besitzt, ist $N(a[1, \tau]) = a$.
Weiter ist $a \cdot \mathfrak{a} = \alpha a[1, \tau]$ und deshalb folgt aus

$$N(a\mathfrak{a}) = N(\alpha a[1, \tau]) = N_{K/\mathbb{Q}}(\alpha)N([a, a\tau]) = N_{K/\mathbb{Q}}(\alpha)a$$

und

$$N(a\mathfrak{a}) = N_{K/\mathbb{Q}}(a)N(\mathfrak{a}) = a^2N(\mathfrak{a})$$

schließlich

$$N(\mathfrak{a}) = \frac{N_{K/\mathbb{Q}}(\alpha)}{a}. \tag{1.3.1}$$

(iii) Ist $\mathfrak{a}$ ein eigentliches $\mathcal{O}$-Ideal, so gilt einerseits mit obigen Bezeichnungen $N(\mathfrak{a}) = \frac{N_{K/\mathbb{Q}}(\alpha)}{a}$. Andererseits wurde im Beweis zu Prop. 1.3.7 gezeigt, dass $\mathfrak{a}\overline{\mathfrak{a}} = \frac{N_{K/\mathbb{Q}}(\alpha)}{a}$ ist.

(ii) Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei eigentliche $\mathcal{O}$-Ideale, so gilt nach (iii)

$$N(\mathfrak{ab})\mathcal{O} = \mathfrak{ab} \cdot \overline{\mathfrak{ab}} = \mathfrak{a}\overline{\mathfrak{a}} \cdot \mathfrak{b}\overline{\mathfrak{b}} = N(\mathfrak{a})\mathcal{O} \cdot N(\mathfrak{b})\mathcal{O} = N(\mathfrak{a})N(\mathfrak{b})\mathcal{O}$$

und folglich muss $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ sein. □

1.4 Quadratische Formen

Es besteht eine bemerkenswerte Beziehung zwischen Idealen von imaginär-quadratischen Zahlkörpern und quadratischen Formen. Diese Beziehung gibt uns letztlich eine Möglichkeit zur Hand, die Idealklassen zu konstruieren

Definition 1.4.1. Es heißt $f(x, y) = ax^2 + bxy + cy^2$ mit a, b, $c \in \mathbb{Z}$ eine **quadratische Form**. Ist $ggT(a, b, c) = 1$, so heißt f **primitiv**.
Eine Zahl $m \in \mathbb{Z}$ wird von f **repräsentiert**, wenn es x, $y \in \mathbb{Z}$ mit $f(x, y) = m$ gibt. Sind zudem x, y teilerfremd, so wird m von f **eigentlich repräsentiert**.

Man definiert folgende **Äuivalenzrelation** zwischen quadratischen Formen.

$$f(x, y) \sim g(x, y) \quad \Longleftrightarrow \quad \exists \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}) : f(x, y) = g(px + qy, rx + sy)$$

Wird $m \in \mathbb{Z}$ von $f(x, y)$ (eigentlich) repräsentiert, so auch von jedem $g(x, y) \sim f(x, y)$. Ist $f(x, y)$ primitiv, so auch jedes $g(x, y) \sim f(x, y)$.

Definition 1.4.2. Es gelte $f(x, y) = g(px+qy, rx+sy)$ für $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$ und zwei quadratische Formen $f(x, y)$, $g(x, y)$. Dann heißt f **eigentlich äquivalent** zu g, wenn $det \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$=1 ist. Dagegen heißt f **uneigentlich äquivalent** zu g, wenn $det \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$=-1 ist.

Lemma 1.4.3. *Eine quadratische Form $f(x,y)$ repräsentiert genau dann $m \in \mathbb{Z}$ eigentlich, wenn f eigentlich äquivalent zu $mx^2+bxy+cy^2$ mit geeigneten b, $c \in \mathbb{Z}$ ist.*

Beweis. Es gelte zunächst $f(p,q) = m$ und $ggT(p,q) = 1$. Dann existieren Zahlen r, $s \in \mathbb{Z}$ mit $ps - qr = 1$ und es gilt

$$f(px+ry, qx+sy) = f(p,q)x^2 + (\dots)xy + f(r,s)y^2 = mx^2+bxy+cy^2,$$

für geeignete b, $c \in \mathbb{Z}$.
Ist andererseits $f(x,y)$ eigentlich äquivalent zu $g(x,y) = mx^2+bxy+cy^2$, so wird m eigentlich von g repräsentiert. Nach obiger Bemerkung wird m dann auch von f eigentlich repräsentiert. □

Definition 1.4.4. Die **Diskriminante** der quadratischen Form $f(x,y) = ax^2+bxy+cy^2$ ist $D := b^2 - 4ac$.

Bemerkung. Ist D bzw. D' die Diskriminante der Form $f(x,y)$ bzw. $g(x,y)$ und gilt $f(x,y) = g(px+qy, rx+sy)$ mit p, q, r, $s \in \mathbb{Z}$, so ist $D = (ps-qr)^2 D'$. Sind also f und g äquivalent, so besitzen sie die selbe Diskriminante.

Definition und Bemerkung 1.4.5. Für die quadratische Form $f(x,y) = ax^2+bxy+cy^2$ mit Diskriminante D ist $4af(x,y) = (2ax+by)^2 - Dy^2$.
Ist $D > 0$, so repräsentiert f positive *und* negative Zahlen und heißt **indefinit**.
Ist $D < 0$, so repräsentiert f nur positive *oder* nur negative Zahlen und heißt **positiv** oder **negativ definit**.

Ist f positiv definit, so folgt aus der Defintion, dass $a > 0$ und $c > 0$ gelten muss.
Da für die Diskriminante $D \equiv b^2 \bmod 4$ gilt, ist

$$D \equiv 0 \bmod 4 \Leftrightarrow 2|b \qquad \text{und} \qquad D \equiv 1 \bmod 4 \Leftrightarrow 2\not|b.$$

Lemma 1.4.6. *Seien D, $m \in \mathbb{Z}$, es gelte $D \equiv 0, 1 \bmod 4$ und $2\not|m$, sowie $ggT(m,D) = 1$. Dann ist*

$$\left(\frac{D}{m}\right) = +1 \qquad \Longleftrightarrow \qquad \textit{Es existiert eine primitive Form f(x,y) mit Diskriminante D, die m eigentlich repräsentiert.}$$

Beweis. Ist $f(x,y)$ eine m repräsentierende Form, so können wir nach Lemma 1.4.3 $f(x,y) = mx^2+bxy+cy^2$ annehmen. Dann ist die Diskriminante $D = b^2 - 4cm$, also $D \equiv b^2 \bmod m$.
Sei nun $D \equiv b^2 \bmod m$ für ein $b \in \mathbb{Z}$. Da m ungerade ist, können wir $D \equiv b \bmod 2$ annehmen, nachdem wir evtl. b durch $b+m$ ersetzt haben. Da $D \equiv 0, 1 \bmod 4$ ist, muss dann $D \equiv b^2 \bmod 4m$ gelten. Das heißt aber $D = b^2 - 4cm$ für ein $c \in \mathbb{Z}$, und $f(x,y) = mx^2+bxy+cy^2$ ist eine Form mit Diskriminante D, die m eigentlich repräsentiert. f ist außerdem primitiv, da $ggT(m,D) = 1$ gilt. □

Definition 1.4.7. Eine primitive positiv definite quadratische Form $f(x,y) = ax^2+bxy+cy^2$ heißt **reduziert**, wenn $|b| \le a \le c$ und $b \ge 0$ falls $|b| = a$ oder $c = a$ gilt.

Theorem 1.4.8. *Jede positiv definite quadratische Form ist eigentlich äquivalent zu genau einer reduzierten Form.*

Beweis. Sei eine pos.-def. quadr. Form gegeben, und $f(x,y) = ax^2+bxy+cy^2$ zu dieser eigentlich äquivalent mit der Eigenschaft, dass $|b|$ minimal ist.

Es ist
$$g(x,y) = f(x \pm y, y) = ax^2 + (\pm 2a + b)xy + c'y^2$$
zu f(x,y) eigentlich äquivalent. Angenommen es ist $a < |b|$. Da f ist pos.-def. ist, gilt $0 < a$. Dann ist $|\pm 2a + b| < |b|$ für $|b| = \pm b$, im Widerspruch zur Minimalität von $|b|$. Also gilt $|b| \leq a$.
Da $f(x,y)$ auch eigentlich äquivalent zu $f(x, \pm x + y)$ ist, folgt analog $|b| \leq c$. Gilt $a > c$, so vertausche die äußeren Koeffizienten mittels $(x,y) \mapsto (-y,x)$. Dann gilt für $f(x,y)$ also $|b| \leq a \leq c$. Ist $b \geq 0$, so ist die Form bereits reduziert. Gilt $b < 0$ und $a = -b$, so können wir mittels $(x,y) \mapsto (x+y,y)$ dann $f(x,y) = ax^2 - axy + cy^2$ annehmen. Gilt $b < 0$ und $a = c$, so können wir $f(x,y) = ax^2 - bxy + ay^2$ wegen $(x,y) \mapsto (-y,x)$ annehmen.

Für die Eindeutigkeit wird auf [3, Thm 2.8] verwiesen. □

Bemerkung 1.4.9. Ist $ax^2 + bxy + cy^2$ eine reduzierte quadratische Form mit Diskriminante $D < 0$, so ist $b^2 \leq a^2$ und $a \leq c$, also $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$ bzw. $a \leq \sqrt{\frac{-D}{3}}$.

Zu vorgegebener negativer Diskriminante D gibt es also wegen $|b| \leq a \leq \sqrt{\frac{-D}{3}}$ nur endlich viele a und b aus $\mathbb{Z}$ und c ist durch die Gleichung $D = b^2 - 4ac$ eindeutig bestimmt.
Mit anderen Worten: es gibt zu vorgegebener negativer Diskriminante nur endlich viele reduzierte Formen! Nach Thm. 1.4.8 ist die Anzahl der Äquivalenzklassen von eigentlich äquivalenten Formen also auch endlich. Wir fassen zusammen.

Theorem 1.4.10. *Sei $D < 0$ vorgegeben. Die Anzahl $h(D)$ von (eigentlichen Äquivalenz-) Klassen primitiver positiv definiter Formen mit Diskriminante D ist endlich. Sie ist gleich der Anzahl der reduzierten Formen mit Diskriminante D.*

Es zeigt sich, dass die Menge $\mathcal{C}(D)$, der eigentlichen Äquivalenzklassen von primitiven positiv definiten Formen zu vorgegebener Diskriminante D, eine Gruppe bildet, die **Formklassengruppe**.

Theorem 1.4.11. *Sei $\mathcal{O}$ eine Ordnung mit Diskriminante D eines imaginär-quadratischen Zahlkörpers K. Es gilt:*

(i) Ist $f(x,y) = ax^2 + bxy + cy^2$ eine primitive positiv definite quadratische Form mit Diskriminante D, so ist $[a, (-b + \sqrt{D})/2]$ ein eigentliches $\mathcal{O}$-Ideal.

(ii) Die Abbildung $f(x,y) \mapsto [a, (-b+\sqrt{D})/2]$ induziert einen Isomorphismus zwischen der Form- und Idealklassengruppe. Insbesondere besitzen beide Gruppen die gleiche Ordnung.

(iii) Es wird $m \in \mathbb{N}$ genau dann von der Form $f(x,y) \in \mathcal{C}(D)$ repräsentiert, wenn m die Norm $N(\mathfrak{a})$ eines Ideals $\mathfrak{a}$ aus der zu $f(x,y)$ gehörenden Idealklasse ist.

Beweis. (i) Sei $f(x,y) = ax^2 + bxy + cy^2$ eine primitive positiv definite quadratische Form mit Diskriminante $D < 0$.
Die Nullstellen von $f(x,1) = ax^2 + bx + c$ sind komplex, und die eindeutige Nullstelle τ in der oberen Halbebene $\mathfrak{H} := \{z \in \mathbb{C} | Im(z) > 0\}$ von $f(x,1)$ heißt *die* Nullstelle von $f(x,y)$. Da f positiv definit ist, also $a > 0$ gilt, ist $\tau = \frac{-b+\sqrt{D}}{2a} \in K$.
Wir können deshalb
$$[a, (-b + \sqrt{D})/2] = [a, a\tau] = a[1, \tau]$$
schreiben. Nach Lemma 1.3.6 ist $a[1,\tau]$ ein eigentliches Ideal der Ordnung $[1, a\tau]$.
Ist f der Führer von $\mathcal{O}$, also $D = f^2 \cdot d_K$, so ist
$$a\tau = \frac{-b + f\sqrt{d_K}}{2} = -\frac{b + fd_K}{2} + f\frac{d_K + \sqrt{d_K}}{2} = -\frac{b + fd_K}{2} + fw_K.$$
Aus $f^2 d_K = D = b^2 - 4ac$ folgt
$$b \equiv 1 \bmod 2 \Leftrightarrow D \equiv 1 \bmod 2 \Leftrightarrow f,\ d_K \equiv 1 \bmod 2 \Leftrightarrow fd_K \equiv 1 \bmod 2,$$

mit der Konsequenz, dass $-(b+fd_K)/2$ in $\mathbb{Z}$ liegt. Es ist deshalb $[1, a\tau] = [1, fw_K] = \mathcal{O}$ und $a[1,\tau]$ ein eigentliches $\mathcal{O}$-Ideal.

(ii) Sind $f(x,y)$ und $g(x,y)$ quadratische Formen mit Diskriminante D und den Nullstellen τ bzw. τ', so sind äquivalent:

$$\begin{array}{c} f(x,y) \text{ ist eigentlich äquivalent zu } g(x,y) \\ \Leftrightarrow \\ \exists \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL(2,\mathbb{Z}) : \ \tau' = \frac{p\tau+q}{r\tau+s} \\ \Leftrightarrow \\ \exists \lambda \in K^* : \ [1,\tau] = \lambda[1,\tau']. \end{array} \tag{1.4.1}$$

Ist nämlich $f(x,y) = g(px+qy, rx+sy)$ mit $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$, so folgt $f(\tau,1) = g(p\tau+q, r\tau+s) = (r\tau+s)^2 g(\frac{p\tau+q}{r\tau+s}, 1) = 0$. Ebenfalls verifiziert man, dass $\mathrm{Im}(\frac{p\tau+q}{r\tau+s}) > 0$ ist. Aus der Eindeutigkeit von τ' folgt deshalb $\tau' = \frac{p\tau+q}{r\tau+s}$.

Ist andererseits $\tau' = \frac{p\tau+q}{r\tau+s}$, so haben $f(x,y)$ und $g(px+qy, rx+sy)$ die gleiche Nullstelle τ. Die quadratischen Polynome $f(x,1)$ und $g(px+q, rx+s)$ besitzen die gemeinsame komplexe Nullstelle τ und haben folglich auch die zweite (zu τ konjugierte) Nullstelle $\overline{\tau}$ gemeinsam. Deshalb stimmen $f(x,y)$ und $g(px+qy, rx+sy)$ bis auf einen konstanten Faktor γ überein.
Der Faktor kann zunächst nur $\gamma = \pm 1$ sein, denn beide Formen sind primitiv. Da beide Formen positiv definit sind (also einen positiven Leitkoeffizienten besitzen), muss $\gamma = 1$ sein. Mit anderen Worten sind $f(x,y)$ und $g(px+qy, rx+sy)$ eigentlich äquivalent.

Ist $\tau' = \frac{p\tau+q}{r\tau+s}$, so definiere $\lambda = r\tau + s \in K^*$. Dann ist

$$\lambda[1,\tau'] = [r\tau+s, p\tau+q] = [1,\tau],$$

denn wegen $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$ gilt $s(p\tau+q) - q(r\tau+s) = \tau$ und $p(r\tau+s) - r(p\tau+q) = 1$.

Gilt abschließend $[1,\tau] = \lambda[1,\tau']$ für ein $\lambda \in K^*$, also $[1,\tau] = [\lambda, \lambda\tau']$, so ist

$$\lambda\tau' = p\tau + q \qquad \text{und} \qquad \lambda = r\tau + s \qquad \text{mit} \qquad \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL(2,\mathbb{Z}).$$

Also ist $\tau' = \frac{\lambda\tau'}{\lambda} = \frac{p\tau+q}{r\tau+s}$. Da $\mathrm{Im}(\tau') = det\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) |r\tau+s|^{-2} \mathrm{Im}(\tau) > 0$ gilt, muss also $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ in $SL(2,\mathbb{Z})$ liegen.

Die obigen Äquivalenzen zeigen, dass die Abbildung $f(x,y) \mapsto a[1,\tau]$ injektiv ist. Bleibt also die Sujektivität zu zeigen.
Ist ein gebrochenes $\mathcal{O}$-Ideal $\mathfrak{a} = [\alpha,\beta]$ mit $\alpha, \beta \in K$ gegeben, so sei o. B. d. A. $\tau = \alpha/\beta \in \mathfrak{H}$. Sei weiter ax^2+bx+c das Minimalpolynom von τ über $\mathbb{Z}$ und $ggT(a,b,c) = 1$ sowie $a > 0$ angenommen. Da $\tau \notin \mathbb{R}$ ist, ist die Diskriminante $b^2 - 4ac < 0$. Weil $a > 0$ gilt, ist dann $g(x,y) = ax^2 + bxy + cy^2$ eine primitive positiv definite quadratische Form mit Diskriminante

$$\begin{aligned} b^2 - 4ac &= a^2(\tau+\overline{\tau}) - a^2 4\tau\overline{\tau} = a^2(\tau^2 - 2\tau\overline{\tau} + \overline{\tau}^2) \\ &= det \begin{pmatrix} 1 & a\tau \\ 1 & a\overline{\tau} \end{pmatrix}^2 = discr([1, a\tau]) = D. \end{aligned}$$

Es wird $g(x,y)$ nach (i) auf das eigentliche $\mathcal{O}$-Ideal $a[1,\tau]$ abgebildet, welches in der Idealklasse von $\alpha[1,\tau] = [\alpha,\beta] = \mathfrak{a}$ liegt.
Dies zeigt die Mengen-Bijektion zwischen $\mathcal{C}(D)$ und $\mathcal{C}(\mathcal{O})$. Da wir die Gruppenstruktur auf $\mathcal{C}(D)$ nicht benutzen werden, verweisen wir für den Rest des Beweises auf [3, Thm 7.7].

(iii) Wird m von $f(x,y)$ repräsentiert, so ist $m = d^2 a$, wobei a von $f(x,y)$ eigentlich dargestellt wird. Sei o. B. d. A. deshalb $f(x,y) = ax^2 + bxy + cy^2$ und $f(x,y)$ wird auf $\mathfrak{a} = a[1,\tau]$ abgebildet. Wie im Beweis zu Lemma 1.3.9 gezeigt wurde, ist dann $N(\mathfrak{a}) = a$, also $N(d\mathfrak{a}) = d^2 a = m$ für das in der gleichen Idealklasse wie $\mathfrak{a}$ liegende Ideal $d\mathfrak{a}$.

Sei andererseits $N(\mathfrak{a}) = m$. Dann ist $\mathfrak{a} = \alpha[1, \tau]$, $Im(\tau) > 0$ und $a\tau^2 + b\tau + c = 0$, $ggT(a, b, c) = 1$ und $a > 0$ für geeignete $a, b, c \in \mathbb{Z}$. Die Form $f(x, y) = ax^2 + bxy + cy^2$ wird auf die Idealklasse von $\mathfrak{a}$ abgebildet. Nach (1.3.1) ist $m = N(\mathfrak{a}) = \frac{N_{K/\mathbb{Q}}(\alpha)}{a}$.
Außerdem ist $\alpha[1, \tau] = \mathfrak{a} \subset \mathcal{O} = [1, a\tau]$, also $\alpha = p + qa\tau$ und $\alpha\tau = r + sa\tau$ für $p, q, r, s \in \mathbb{Z}$. Aus $(p + qa\tau)\tau = r + sa\tau$ und $a\tau^2 = -b\tau - c$ folgt $p = as + bq$. Einsetzen liefert

$$m = \frac{N_{K/\mathbb{Q}}(\alpha)}{a} = \frac{p^2 - bpq + acq^2}{a} = \cdots = f(s, q),$$

womit alles gezeigt ist. □

Beispiel 1.4.12. (i) Wir wollen ein Repräsentantensystem der Idealklassen von $\mathcal{O}_K$ für $K = \mathbb{Q}(\sqrt{-1})$ bestimmen. Es ist $-1 \equiv 3 \bmod 4$ und nach Abschnitt 1.2 deshalb $d_K = -4$. Nach Thm. 1.4.11 besteht ein Isomorphismus zwischen der Formklassengruppe und der Idealklassengruppe und die Formklassengruppe kann nach Thm. 1.4.8 durch reduzierte quadratische Formen mit Diskriminante d_K repräsentiert werden.
Wir bestimmen also alle reduzierten quadratischen Formen mit Diskriminante d_K und bilden diese mit Thm. 1.4.11 auf die Idealklassen ab.
Nach Definition 1.4.7 muss für reduzierte Formen $f(x, y) = ax^2 + bxy + cy^2$ mit Diskriminante -4 zunächst $b^2 - 4ac = -4$ und

$$|b| \leq a \leq c \text{ und } b \geq 0 \text{ falls } |b| = a \text{ oder } c = a$$

gelten. In Bem. 1.4.9 haben wir gesehen, dass hier $a \leq \sqrt{\frac{4}{3}} \sim 1,2$ sein muss. Ist $a = 0$, so muss auch $b = 0$ sein und dies macht $b^2 - 4ac = -4$ unmöglich. Also kommt einzig $a = 1$ in Betracht. Dann muss $b \in \{\pm 1, 0\}$ sein. Es ist $b = \pm 1$ wegen $5 = b^2 - d_K = 4ac$ unmöglich. Wir finden deshalb mit Diskriminante -4 als einzige reduzierte Form $f(x, y) = 1 \cdot x^2 + 0 \cdot xy + 1 \cdot y^2$. Diese gibt das Ideal

$$\left[1, \frac{\sqrt{-4}}{2}\right] = [1, i] = \mathbb{Z}[i].$$

Die Idealklassengruppe von $\mathbb{Z}[i]$ besteht also aus nur einer Idealklasse und $\mathbb{Z}[i]$ ist folglich ein Hauptidealring.

(ii) Eine analoge Betrachtung des Ganzheitsringes $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ von $\mathbb{Q}(\sqrt{-3})$ zeigt, dass auch dieser ein Hauptidealring ist.

(iii) Wir wollen die Idealklassen von $\mathcal{O}_K$ für $K = \mathbb{Q}(\sqrt{-31})$ bestimmen. Es muss dann $a \leq \sqrt{\frac{31}{3}} \sim 3,2$ gelten. Aus $-31 = b^2 - 4ac$ folgt zunächst, dass b ungerade sein muss.

- Für $a = 3$ ist $-31 = b^2 - 12c$, insbesondere gilt $12|(b^2 + 31)$. Aus $b = \pm 1, \pm 3$ folgt $12|32, 40$, ein Widerspruch.
- Für $a = 2$ ist $-31 = b^2 - 8c$, insbesondere gilt $8|(b^2 + 31)$. Wir finden die Lösungen $b = \pm 1$ und $c = 4$.
- Für $a = 1$ ist $-31 = b^2 - 4c$, insbesondere gilt $4|(b^2 + 31)$. Wir finden die möglichen Lösugen $b = \pm 1$ und $c = 8$. Da dann $|b| = a$ gilt, muss $b > 0$ sein. Wir erhalten also die Lösung $b = 1$ und $c = 8$.

Die Klassengruppe von $\mathbb{Q}(\sqrt{-31})$ ist daher

$$\mathcal{C}(\mathcal{O}_K) = \left\{ \left[2, \frac{-1 + \sqrt{-31}}{2}\right], \left[2, \frac{1 + \sqrt{-31}}{2}\right], \left[1, \frac{-1 + \sqrt{-31}}{2}\right] \right\}.$$

(iv) Analog bestimmen wir die Klassengruppe von $K = \mathbb{Q}(\sqrt{-51})$ und finden

$$\mathcal{C}(\mathcal{O}_K) = \left\{ \left[3, \frac{-3 + \sqrt{-51}}{2}\right], \left[1, \frac{-1 + \sqrt{-51}}{2}\right] \right\}.$$

Korollar 1.4.13. *Sei $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers K. Zu beliebigem $M \in \mathbb{N}$ existiert in jeder Idealklasse $[\mathfrak{a}]$ von $C(\mathcal{O})$ ein eigentliches $\mathcal{O}$-Ideal mit zu M teilerfremder Norm.*

Beweis. Ist $f(x,y) = ax^2 + bxy + cy^2$ eine beliebige primitive pos.-def. Form und $p \in \mathbb{Z}$ prim, so ist zumindest einer der drei Werte $f(1,0) = a$, $f(0,1) = c$, $f(1,1) = a+b+c$ zu p teilerfremd. Ist nun $M = p_1^{e_1} \cdots p_r^{e_r}$ mit verschiedenen Primzahlen $p_i \in \mathbb{Z}$, so existieren also Paare $(x_i, y_i) \in \mathbb{Z}^2$ mit $p_i \nmid f(x_i, y_i)$. Der chinesische Restsatz liefert $(x,y) \in \mathbb{Z}^2$ mit

$$x \equiv x_i \bmod p_i^{e_i} \quad \text{und} \quad y \equiv y_i \bmod p_i^{e_i}.$$

Dann ist $f(x,y) \equiv f(x_i, y_i) \bmod p_i^{e_i}$ und es folgt $ggT(f(x,y), M) = 1$.
Ist $f(x,y)$ die primitive pos.-def. Form, welche auf die Idealklasse $[\mathfrak{a}]$ abbildet, so repräsentiert $f(x,y)$ nach dem eben Bewiesenen eine zu M teilerfremde Zahl k . Nach Thm. 1.4.11.(iii) gibt es dann in $[\mathfrak{a}]$ ein Ideal mit Norm k. □

1.5 Die Beziehung zwischen $\mathcal{C}(\mathcal{O})$ und $\mathcal{C}(\mathcal{O}_K)$

Wir wollen eine Beziehung zwischen $\mathcal{O}$-Idealen und $\mathcal{O}_K$-Idealen herleiten. Es zeigt sich, dass dies nicht im Allgemeinen gelingt, sondern nur für eine Teilmenge von $\mathcal{O}$-Idealen.

Definition 1.5.1. Sei K ein quadratischer Zahlkörper, $\mathcal{O}$ eine Ordnung von K und $f \in \mathbb{Z}$. Ein $\mathcal{O}$-Ideal $\mathfrak{a} \neq 0$ heißt zu f **teilerfremd** (oder prim), wenn $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$ gilt.

Lemma 1.5.2. *Sei $\mathcal{O}$ eine Ordnung des Zahlkörpers K zum Führer f.*

(i) Ein $\mathcal{O}$-Ideal $\mathfrak{a}$ ist genau dann zu f teilerfremd, wenn seine Norm $N(\mathfrak{a})$ teilerfremd zu f ist.

(ii) Jedes zu f teilerfremde $\mathcal{O}$-Ideal ist eigentlich.

Beweis. (i) Sei $m_f : \mathcal{O}/\mathfrak{a} \to \mathcal{O}/\mathfrak{a}$ die Multiplikation mit f, so gilt

$$\mathfrak{a} + f\mathcal{O} = \mathcal{O} \quad \Leftrightarrow \quad m_f \text{ ist surjektiv} \quad \Leftrightarrow \quad m_f \text{ ist ein Isomorphismus.}$$

Nach dem Struktursatz für abelsche Gruppen ist m_f genau dann ein Isomorphismus, wenn f teilerfremd zur Ordnung $N(\mathfrak{a})$ von $\mathcal{O}/\mathfrak{a}$ ist.
(ii) Ist $\mathfrak{a}$ ein zu f teilerfremdes $\mathcal{O}$-Ideal und $\beta \in K$ mit $\beta\mathfrak{a} \subseteq \mathfrak{a}$, so liegt zunächst β in $\mathcal{O}_K$. Deshalb ist

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathfrak{a} + \beta f\mathcal{O} \subseteq \mathfrak{a} + f\mathcal{O}_K \subseteq \mathcal{O},$$

also $\beta \in \mathcal{O}$, wie zu zeigen war. □

Die zu f teilerfremden $\mathcal{O}$-Ideale liegen folglich in $I(\mathcal{O})$. Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei solche Ideale, so ist mit $N(\mathfrak{a})$ und $N(\mathfrak{b})$ auch $N(\mathfrak{ab})$ teilerfremd zu f. Somit ist die Menge der zu f teilerfremden $\mathcal{O}$-Ideale abgeschlossen unter Multiplikation.
Die von ihr erzeugte Untergruppe der gebrochenen Ideale sei mit $I(\mathcal{O}, f)$ bezeichnet. In $I(\mathcal{O}, f)$ liegt in natürlicherweise die Untergruppe $P(\mathcal{O}, f)$, die von den zu f teilerfremden $\mathcal{O}$-Hauptidealen erzeugt wird.
Lemma 1.5.2 gilt natürlich auch im Fall der Maximalordnung $\mathcal{O}_K$. Abkürzend setzen wir hier $I_K(f) := I(\mathcal{O}_K, f)$ und $P_K(f) := P(\mathcal{O}_K, f)$.

Proposition 1.5.3. *Die Inklusion $I(\mathcal{O}, f) \subseteq I(\mathcal{O})$ induziert einen Isomorphismus*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I(\mathcal{O})/P(\mathcal{O}) = C(\mathcal{O}).$$

Beweis. Nach Kor. 1.4.13 ist die Abbildung $I(\mathcal{O},f) \to C(\mathcal{O})$ surjektiv, denn jede Idealklasse enthält zu f teilerfremde $\mathcal{O}$-Ideale. Der Kern der Abbildung ist $I(\mathcal{O},f) \cap P(\mathcal{O})$, und wir wollen $I(\mathcal{O},f) \cap P(\mathcal{O}) = P(\mathcal{O},f)$ zeigen. Ist $\mathfrak{a} \in P(\mathcal{O},f)$, so ist ersichtlich, dass $\mathfrak{a}$ in $I(\mathcal{O},f) \cap P(\mathcal{O})$ liegt. Ist andererseits ein Element aus $I(\mathcal{O},f) \cap P(\mathcal{O})$ gegeben, so besitzt dieses eine Darstellung $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$ mit $\alpha \in K$ und zu f teilerfremden $\mathcal{O}$-Idealen $\mathfrak{a}$ und $\mathfrak{b}$. Mit $m = N(\mathfrak{b}) = N(\overline{\mathfrak{b}})$ ist nach Lemma 1.3.9 $m\mathcal{O} = \mathfrak{b}\overline{\mathfrak{b}}$, also $m\mathfrak{b}^{-1} = \overline{\mathfrak{b}}$. Wegen

$$m\alpha\mathcal{O} = \mathfrak{a} \cdot m\mathfrak{b}^{-1} = \mathfrak{a}\overline{\mathfrak{b}} \subseteq \mathcal{O}$$

liegt $m\alpha\mathcal{O}$ in $P(\mathcal{O},f)$. Also liegt $\alpha\mathcal{O} = m\alpha\mathcal{O} \cdot (m\mathcal{O})^{-1}$ in $P(\mathcal{O},f)$. □

Proposition 1.5.4. *Sei $\mathcal{O}$ eine Ordnung zum Führer f des imaginär-quadratischen Zahlkörpers K.*

(i) Ist $\mathfrak{a}$ ein zu f teilerfremdes $\mathcal{O}_K$-Ideal, so ist $\mathfrak{a} \cap \mathcal{O}$ ein zu f teilerfremdes $\mathcal{O}$-Ideal gleicher Norm.

(ii) Ist $\mathfrak{a}$ ein zu f teilerfremdes $\mathcal{O}$-Ideal, so ist $\mathfrak{a}\mathcal{O}_K$ ein zu f teilerfremdes $\mathcal{O}_K$-Ideal gleicher Norm.

(iii) Die Abblidung $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induziert einen Isomorphismus $I_K(f) \xrightarrow{\sim} I(\mathcal{O},f)$ mit Umkehrabbildung $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.

Beweis. (i) Ist $\mathfrak{a}$ ein zu f teilerfremdes $\mathcal{O}_K$-Ideal, so ist $m_f : \mathcal{O}_K/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{a}$ nach Lemma 1.5.2 ein Isomorphismus. Per Definition ist $f\mathcal{O}_K \subseteq \mathcal{O}$, also gilt für das Bild $Im(m_f) = f \cdot (\mathcal{O}_K/\mathfrak{a}) = \mathcal{O}/\mathfrak{a} \cap \mathcal{O}$. Folglich ist

$$\mathcal{O}_K/\mathfrak{a} \simeq \mathcal{O}/\mathfrak{a} \cap \mathcal{O}.$$

(ii) Ist $\mathfrak{a}$ ein zu f teilerfremdes $\mathcal{O}$-Ideal, so ist per Definition auch $\mathfrak{a}\mathcal{O}_K$ zu f teilerfremd, denn es gilt

$$\mathfrak{a}\mathcal{O}_K + f\mathcal{O}_K = (\mathfrak{a} + f\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K.$$

Die Behauptung bzgl. der Norm wird im Folgenden mit bewiesen.

(iii) Es gilt

$$\begin{aligned} \mathfrak{a} &= \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} && \text{für jedes zu } f \text{ teilerfremde } \mathcal{O}\text{-Ideal } \mathfrak{a}, \\ (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K &= \mathfrak{a} && \text{für jedes zu } f \text{ teilerfremde } \mathcal{O}_K\text{-Ideal } \mathfrak{a}. \end{aligned} \tag{1.5.1}$$

Ist nämlich $\mathfrak{a}$ ein zu f teilerfremdes $\mathcal{O}$-Ideal, so gilt natürlich $\mathfrak{a} \subseteq \mathfrak{a}\mathcal{O}_K \cap \mathcal{O}$. Weiter ist

$$\begin{aligned} \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} &= (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\mathcal{O} = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{a} + f\mathcal{O}) \\ &= \mathfrak{a}(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) + f(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) \subseteq \mathfrak{a} + f(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) \\ &\subseteq \mathfrak{a} + \mathfrak{a} \cdot f\mathcal{O}_K \subseteq \mathfrak{a} + \mathfrak{a}\mathcal{O} = \mathfrak{a}. \end{aligned}$$

Bezeichnet $\mathfrak{a}$ ein zu f teilerfremdes $\mathcal{O}_K$-Ideal, so ist einerseits $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K \subseteq \mathfrak{a}$. Andererseits gilt wegen (i) zunächst

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + f\mathcal{O}) \subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + f\mathfrak{a}.$$

Da $f\mathfrak{a} \subseteq f\mathcal{O}_K \subseteq \mathcal{O}$ gilt, ist $f\mathfrak{a} \subseteq \mathfrak{a} \cap \mathcal{O} \subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$ und es folgt $\mathfrak{a} \subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$.

Die ausstehende Behauptung von (ii) lässt sich nun einfach zeigen. Es ist für ein zu f teilerfremdes $\mathcal{O}$-Ideal $\mathfrak{a}$ nach (ii) $\mathfrak{a}\mathcal{O}_K$ ein zu f teilerfremdes $\mathcal{O}_K$-Ideal und nach (i) ist $N(\mathfrak{a}\mathcal{O}_K) = N(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})$. Nach dem eben Bewiesenen ist $\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a}$, also $N(\mathfrak{a}\mathcal{O}_K) = N(\mathfrak{a})$.
Mit (1.5.1) erhalten wir eine Bijektion der Monoide der zu f teilerfremden $\mathcal{O}_K$- und $\mathcal{O}$-Ideale. Da $\mathfrak{a}\mathfrak{b}\mathcal{O}_K = \mathfrak{a}\mathcal{O}_K\mathfrak{b}\mathcal{O}_K$ für $\mathcal{O}$-Ideale $\mathfrak{a}$ und $\mathfrak{b}$ gilt, respektiert diese Bijektion die Multiplikation und lässt sich zu einem Gruppenisomorphismus $I_K(f) \xrightarrow{\sim} I(\mathcal{O},f)$ fortsetzen. □

Korollar 1.5.5. *Ist $\mathcal{O}$ eine Ordnung von K mit Führer f und $\mathfrak{a}$ ein zu f teilerfremdes $\mathcal{O}$-Ideal, so besitzt $\mathfrak{a}$ eine eindeutige Zerlegung in zu f teilerfremde $\mathcal{O}$-Primideale.*

Beweis. Es ist $\mathfrak{a} = \mathfrak{a}\mathcal{O}_K \cap \mathcal{O}$. Da $\mathfrak{a}\mathcal{O}_K = \prod_{i=1}^m \mathfrak{P}_i^{e_i}$ eine eindeutige Zerlegung von $\mathfrak{a}\mathcal{O}_K$ in $\mathcal{O}_K$-Primideale ist, erhalten wir mit $\mathfrak{p}_i = \mathfrak{P}_i \cap \mathcal{O}$ eine Zerlegung

$$\mathfrak{a} = \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \prod_{i=1}^m \mathfrak{P}_i^{e_i} \cap \mathcal{O} = \prod_{i=1}^m \mathfrak{p}_i^{e_i}$$

von $\mathfrak{a}$ in $\mathcal{O}$. Es ist $N(\mathfrak{p}_i)$ ein Teiler von $N(\mathfrak{a})$. Da $ggT(N(\mathfrak{a}), f) = 1$ ist, muss auch $ggT(N(\mathfrak{p}_i), f) = 1$, also $\mathfrak{p}_i$ zu f teilerfremd nach Lemma 1.5.2 sein. Außerdem gilt $\mathcal{O}/\mathfrak{p}_i \simeq \mathcal{O}_K/\mathfrak{P}_i$ und damit ist $\mathfrak{p}_i$ ein $\mathcal{O}$-Primideal. Wir haben also eine Zerlegung von $\mathfrak{a}$ in zu f teilerfremde $\mathcal{O}$-Primideale gewonnen. Gilt $\mathfrak{a} = \prod_{i=1}^m \mathfrak{p}_i^{e_i} = \prod_{j=1}^n \mathfrak{q}_i^{d_i}$, so folgt

$$\mathfrak{a}\mathcal{O}_K = \prod_{i=1}^m (\mathfrak{p}_i\mathcal{O}_K)^{e_i} = \prod_{j=1}^n (\mathfrak{q}_i\mathcal{O}_K)^{d_i}$$

in $\mathcal{O}_K$. Wegen der eindeutigen Zerlegung in Primideale in $\mathcal{O}_K$ gilt dann $m = n$ und o. B. d. A. $\mathfrak{p}_i\mathcal{O}_K = \mathfrak{q}_i\mathcal{O}_K$, $e_i = d_i$. Dann muss $\mathfrak{p}_i = \mathfrak{p}_i\mathcal{O}_K \cap \mathcal{O} = \mathfrak{q}_i\mathcal{O}_K \cap \mathcal{O} = \mathfrak{q}_i$ sein. □

Proposition 1.5.6. *Sei $\mathcal{O}$ eine Ordnung zum Führer f eines imaginär-quadratischen Zahlkörpers K. Es ist*

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f),$$

wobei $P_{K,\mathbb{Z}}(f)$ die Untergruppe von $I_K(f)$ bezeichnet, die von allen Hauptidealen $\alpha\mathcal{O}_K$ erzeugt wird, wobei $\alpha \in \mathcal{O}_K$ der Gleichung $\alpha \equiv a \bmod f\mathcal{O}_K$ mit einem zu f teilerfremden $a \in \mathbb{Z}$ genügt.

Beweis. Die erste Isomorphie ist nach Prop. 1.5.3 klar. Die Abbildung $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ induziert einen Isomorphismus $I(\mathcal{O}, f) \simeq I_K(f)$ nach Prop. 1.5.4. $P(\mathcal{O}, f)$ wird unter diesem Isomorphismus auf eine Untergruppe $\tilde{P} \subseteq I_K(f)$ abgebildet. Bleibt also $\tilde{P} = P_{K,\mathbb{Z}}(f)$ zu zeigen.
Für $\alpha \in \mathcal{O}_K$ gilt

$$\begin{aligned} &\alpha \equiv a \bmod f\mathcal{O}_K,\ a \in \mathbb{Z},\ \mathrm{ggT}(a, f) = 1 \\ &\quad\Longleftrightarrow\ \alpha \in \mathcal{O},\ \mathrm{ggT}(N(\alpha), f) = 1 \end{aligned} \tag{1.5.2}$$

Sei zunächst $\alpha \equiv a \bmod f\mathcal{O}_K$ für ein $a \in \mathbb{Z}$ mit $ggT(a, f) = 1$, so folgt $N_{K/\mathbb{Q}}(\alpha) \equiv a^2 \bmod f$.
Ist nämlich allgemein $\alpha \equiv \beta \bmod f\mathcal{O}_K$ für ein $\beta \in \mathcal{O}_K$, also $\alpha = \beta + f\gamma$ für ein $\gamma \in \mathcal{O}_K$, so ist $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta + f\gamma) = N_{K/\mathbb{Q}}(\beta) + f\,Tr_{K/\mathbb{Q}}(\beta\overline{\gamma}) + f^2 N_{K/\mathbb{Q}}(\gamma)$. Da mit α, β, γ auch das Element $\beta\overline{\gamma}$ im Ring $\mathcal{O}_K$ liegt, sind $N_{K/\mathbb{Q}}(\alpha)$, $N_{K/\mathbb{Q}}(\beta)$, $N_{K/\mathbb{Q}}(\gamma)$ und $Tr_{K/\mathbb{Q}}(\beta\overline{\gamma})$ in $\mathbb{Z}$ und es gilt $N_{K/\mathbb{Q}}(\alpha) \equiv N_{K/\mathbb{Q}}(\beta) \bmod f$.
Aus $ggT(a, f) = 1$ und $N_{K/\mathbb{Q}}(\alpha) \equiv a^2 \bmod f$ folgt deshalb $ggT(N_{K/\mathbb{Q}}(\alpha), f) = 1$. Da $\alpha = a + f\gamma$ für ein $\gamma \in \mathcal{O}_K$ ist und $f\mathcal{O}_K$ in $\mathcal{O}$ liegt, ist α in $\mathcal{O}$.

Sei andererseits $\alpha \in \mathcal{O} = [1, fw_K]$ und $N_{K/\mathbb{Q}}(\alpha)$ teilerfremd zu f. Wir können also $\alpha = a \cdot 1 + b \cdot fw_K$ für $a, b \in \mathbb{Z}$ schreiben, d. h. $\alpha \equiv a \bmod f\mathcal{O}_K$.
Nach dem oben Gezeigten ist dann $N_{K/\mathbb{Q}}(\alpha) \equiv a^2 \bmod f$. Da außerdem $ggT(a, f)$ ein Teiler von $ggT(a^2, f) = ggT(N_{K/\mathbb{Q}}(\alpha), f) = 1$ ist, müssen a und f teilerfremd sein.

Es wird $P(\mathcal{O}, f)$ von Idealen $\alpha\mathcal{O}$ erzeugt, wobei $\alpha \in \mathcal{O}$ und $N_{K/\mathbb{Q}}(\alpha)$ teilerfremd zu f ist. Also wird $\tilde{P}$ von den entsprechenden Idealen $\alpha\mathcal{O}_K$ erzeugt. (1.5.2) zeigt, dass deshalb $\tilde{P} = P_{K,\mathbb{Z}}(f)$ sein muss. □

2 Ringklassenkörper

2.1 Anwendung der Galois-Theorie

Definition 2.1.1. Ist eine galois'sche Erweiterung L/K von Zahlkörpern gegeben und $\mathfrak{P}$ ein Primideal von L, so heißt

$$D_{\mathfrak{P}} := \{\sigma \in Gal(L:K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

die **Zerlegungsgruppe** von $\mathfrak{P}$ und

$$I_{\mathfrak{P}} := \{\sigma \in Gal(L:K) : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \text{ für alle } \alpha \in \mathcal{O}_L\}$$

die **Restklassengruppe** von $\mathfrak{P}$.

Ist $\sigma \in I_{\mathfrak{P}}$, so folgt unmittelbar aus der Definition, dass $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$ gilt. Das gleiche gilt für $\sigma^{-1} \in I_{\mathfrak{P}}$, sodass man $\mathfrak{P} \subseteq \sigma(\mathfrak{P})$ und deshalb $\sigma(\mathfrak{P}) = \mathfrak{P}$ erhält. Mit anderen Worten ist $\sigma \in D_{\mathfrak{P}}$, und damit gilt $I_{\mathfrak{P}} \subseteq D_{\mathfrak{P}}$.

Jedes Element $\sigma \in Gal(L:K)$ ist ein Automorphismus von $\mathcal{O}_L$. Ist nämlich $\alpha \in \mathcal{O}_L$, d. h. es existiert ein $f(X) \in \mathbb{Z}[X]$ mit $f(\alpha) = 0$, so ist $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$ und damit $\sigma(\alpha) \in \mathcal{O}_L$. Also gilt zunächst $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$, und wie oben schließt man $\sigma(\mathcal{O}_L) = \mathcal{O}_L$.

Wählt man $\sigma \in D_{\mathfrak{P}}$, so induziert σ in natürlicher Weise einen Automorphismus $\overline{\sigma}$ von $\mathcal{O}_L/\mathfrak{P}$ mittels $\overline{\sigma}(\alpha + \mathfrak{P}) = \sigma(\alpha) + \sigma(\mathfrak{P}) = \sigma(\alpha) + \mathfrak{P}$ für $(\alpha + \mathfrak{P}) \in \mathcal{O}_L/\mathfrak{P}$. Da $\sigma|_{\mathcal{O}_K} = \mathrm{id}$ gilt, wirkt $\overline{\sigma}$ auf $\mathcal{O}_K/\mathfrak{p}$ als Identität, sodass $\overline{\sigma}$ ein Element von $\tilde{G} = Gal(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$ ist.

Die Abbildung $\sigma \mapsto \overline{\sigma}$ definiert also einen Homomorphismus $D_{\mathfrak{P}} \to \tilde{G}$. Ein Element $\sigma \in D_{\mathfrak{P}}$ liegt genau dann im Kern dieses Homomorphismus, wenn σ ein Element von $I_{\mathfrak{P}}$ ist, wie man unmittelbar aus der Definition abliest. Insbesondere ist $I_{\mathfrak{P}}$ deshalb ein Normalteiler von $D_{\mathfrak{P}}$.

Die Galois-Theorie gibt uns zu $I_{\mathfrak{P}}$ und $D_{\mathfrak{P}}$ die Zwischenkörper $L_{I_{\mathfrak{P}}}$ und $L_{D_{\mathfrak{P}}}$, den **Zerlegungs-** bzw. **Restklassenkörper**.
Allgemein bezeichne L_H den Fixkörper der Untergruppe $H \subseteq Gal(L/K)$. Ist $X \subseteq L$ eine Teilmenge, so sei $X_H = X \cap L_H$. Auf diese Weise erhalten wir zum Beispiel $L_{\{1\}} = L$, $L_{Gal(L/K)} = K$, den Ganzheitsring $(\mathcal{O}_L)_H$ von L_H, oder $\mathfrak{P}_H$, das eindeutige Primideal von L_H unter $\mathfrak{P}$.

Theorem 2.1.2. *Ist L/K eine galois'sche Erweiterung von Zahlkörpern, $[L:K] = n$, $\mathfrak{P}$ ein Primideal von $\mathcal{O}_L$, $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, $e = e_{\mathfrak{P}|\mathfrak{p}}$, $f = f_{\mathfrak{P}|\mathfrak{p}}$, $n = efr$, $D = D_{\mathfrak{P}}$ und $I = I_{\mathfrak{P}}$, so gilt:*

Körper-grad			*Verzweigungs-index*	*Restklassen-grad*
	L	$\mathfrak{P}$		
e	|	|	e	1
	L_I	$\mathfrak{P}_I$		
f	|	|	1	f
	L_D	$\mathfrak{P}_D$		
r	|	|	1	1
	K	$\mathfrak{p}$		

Beweis. Abkürzend setzen wir $G = Gal(L : K)$.
(i) Die Galois-Theorie gibt uns $[L_D : K] = [G : D]$. Ist $\sigma \in G$, so bildet jedes Element $\sigma \circ \psi$ der Linksnebenklasse σD das Ideal $\mathfrak{P}$ auf $\sigma(\mathfrak{P}) = \sigma \circ \psi(\mathfrak{P})$ ab. Es gilt also

$$\sigma D = \tau D \quad \Longleftrightarrow \quad \sigma(\mathfrak{P}) = \tau(\mathfrak{P}) \qquad \text{für alle } \sigma, \tau \in G,$$

und es besteht eine eineindeutige Beziehung zwischen Linksnebenklassen von D und $\mathcal{O}_L$-Primidealen über $\mathfrak{p}$, denn nach Theorem 1.1.2.(i) operiert G transitiv auf den $\mathcal{O}_L$-Primidealen über $\mathfrak{p}$. Da es r $\mathcal{O}_L$-Primideale über $\mathfrak{p}$ gibt, gilt

$$[L_D : K] = r.$$

(ii) L/L_D ist eine galois'sche Erweiterung mit Galois-Gruppe D. Theorem 1.1.2.(i) gibt uns erneut, dass $\sigma(\mathfrak{P})$ für $\sigma \in D$ alle $\mathcal{O}_L$-Primideale über $\mathfrak{P}_D$ durchläuft. Es ist aber $\sigma(\mathfrak{P}) = \mathfrak{P}$ für alle $\sigma \in D$ und somit $\mathfrak{P}$ das einzige $\mathcal{O}_L$-Primideal über $\mathfrak{P}_D$!
Aus $[L : L_D] \cdot [L_D : K] = ref$ folgt mit (i) deshalb

$$[L : L_D] = ef = e_{\mathfrak{P}|\mathfrak{P}_D} f_{\mathfrak{P}|\mathfrak{P}_D}.$$

Da andererseits $e_{\mathfrak{P}|\mathfrak{P}_D} \leq e$ und $f_{\mathfrak{P}|\mathfrak{P}_D} \leq f$ gelten muss, folgt $e_{\mathfrak{P}|\mathfrak{P}_D} = e$ und $f_{\mathfrak{P}|\mathfrak{P}_D} = f$ und deshalb

$$e_{\mathfrak{P}_D|\mathfrak{p}} = f_{\mathfrak{P}_D|\mathfrak{p}} = 1.$$

(iii) Sei $\overline{\theta} \in (\mathcal{O}_L)/\mathfrak{P}$ beliebig gewählt, so definiere für $\theta \in \overline{\theta}$

$$g(X) := \prod_{\sigma \in I} (X - \sigma(\theta)).$$

Es ist einerseits $g(X) \in \mathcal{O}_L[X]$. Andererseits ist L_I der Fixkörper von I, also $g(X) \in L_I[X]$. Deshalb liegt $g(X)$ in $(\mathcal{O}_L)_I[X]$. Entsteht $\overline{g}(X)$ durch Reduktion der Koeffizienten von g modulo $\mathfrak{P}$, so liegt $\overline{g}(X)$ sogar in $((\mathcal{O}_L)_I/\mathfrak{P}_I)[X]$. Nach Definition von I ist $\sigma(\theta) \equiv \theta \bmod \mathfrak{P}$ und folglich gilt stets $\sigma(\theta) \in \overline{\theta}$. Dies zeigt

$$\overline{g}(X) = \prod_{i=1}^{|I|} (X - \overline{\theta}).$$

Ist $\tau \in \check{G} = Gal(\mathcal{O}_L/\mathfrak{P} : (\mathcal{O}_L)_I/\mathfrak{P}_I)$, so ist $\tau(\overline{\theta})$ eine weitere Nullstelle von $\overline{g}(X)$. Da $\overline{\theta}$ und τ beliebig waren, muss $\check{G}$ trivial sein. Also ist $\mathcal{O}_L/\mathfrak{P}$ isomorph zu $(\mathcal{O}_L)_I/\mathfrak{P}_I$ und deshalb gilt

$$f_{\mathfrak{P}|\mathfrak{P}_I} = 1.$$

Da sich die Restklassengrade multiplikativ verhalten, folgt aus (ii) und (iii) unmittelbar

$$f_{\mathfrak{P}_I|\mathfrak{P}_D} = f.$$

(iv) Wegen $f_{\mathfrak{P}_I|\mathfrak{P}_D} = f$ muss $[L_I : L_D] \geq f$ sein. Andererseits ist I normal in D und D/I isomorph zu einer Untergruppe von $\tilde{G} = Gal(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$. Das führt wegen $[L : L_D] = |D|$ und $[L : L_I] = |I|$ zu $[L_I : L_D] = |D/I| \leq |\tilde{G}| = f$ und wir erhalten folglich

$$[L_I : L_D] = f.$$

Benutzen wir die erworbenen Kenntnisse, so folgen die ausstehenden Behauptungen

$$e_{\mathfrak{P}_I|\mathfrak{P}_D} = 1, \quad \text{und} \quad [L : L_I] = e \quad \text{und} \quad e_{\mathfrak{P}|\mathfrak{P}_I} = e.$$

□

Korollar 2.1.3. *Die Abbildung $\phi : D_{\mathfrak{P}} \longrightarrow \tilde{G}$ ist ein surjektiver Homomorphismus mit Kern $I_{\mathfrak{P}}$.*

Beweis. Es bleibt nur noch die Surjektivität zu zeigen. Da $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ eine Untergruppe von $\tilde{G}$ ist und $|\tilde{G}| = |D_{\mathfrak{P}}/I_{\mathfrak{P}}| = f$ nach oben Gezeigtem gilt, ist ϕ surjektiv. □

Korollar 2.1.4. *Ist die Zerlegungsgruppe D eine normale Untergruppe von $G = Gal(L:K)$, so zerfällt $\mathfrak{p}$ in r verschiedene Primideale in L_D.*
Ist die Restklassengruppe I ebenfalls normal in G, so bleiben alle Primideale von L_D über $\mathfrak{p}$ prim in L_I und tauchen als e-te Potenz in der Zerlegung von $\mathfrak{p}$ in L auf.

Beweis. Ist D normal in G, so ist nach der Galois-Theorie L_D normal über K. Nach Theorem 2.1.2 ist $e_{\mathfrak{P}_D|\mathfrak{P}} = f_{\mathfrak{P}_D|\mathfrak{P}} = 1$ und da L_D/K galois'sch ist, gilt dies somit für *alle* Primideale $\widetilde{\mathfrak{P}}_D$ von L_D über $\mathfrak{p}$. Da $[L_D : K] = r$ ist, muss es r über $\mathfrak{p}$ liegende Primideale von L_D geben.

Da es sowohl in L als auch in L_D genau r verschiedene Primideale über $\mathfrak{p}$ gibt, muss es auch r verschiedene in L_I geben. Folglich liegt jedes Primideal $\widetilde{\mathfrak{P}}_D$ von L_D über $\mathfrak{p}$ unter genau einem Primideal $\widetilde{\mathfrak{P}}_I$ von L_I.

Ist nun auch I normal in G, so ist L_I normal (und damit galois'sch) über K. Für jedes Primideal $\widetilde{\mathfrak{P}}_I$ von L_I über $\mathfrak{p}$ gilt dann nach Theorem 2.1.2

$$e_{\widetilde{\mathfrak{P}}_I|\mathfrak{p}} = e_{\mathfrak{P}_I|\mathfrak{p}} = 1, \qquad \text{also auch} \qquad e_{\widetilde{\mathfrak{P}}_I|\widetilde{\mathfrak{P}}_D} = 1.$$

D. h. $\widetilde{\mathfrak{P}}_D$ bleibt prim in L_I. Da $e = e_{\widetilde{\mathfrak{P}}|\mathfrak{p}} = e_{\widetilde{\mathfrak{P}}|\widetilde{\mathfrak{P}}_I}$ für beliebige $\mathcal{O}_L$-Primideale $\widetilde{\mathfrak{P}} \supseteq \mathfrak{p}$ ist, taucht jedes $\widetilde{\mathfrak{P}}_I$ in der Zerlegung von $\mathfrak{p}$ in L in einer e-ten Potenz auf. □

Wir gehen weiter von einer normalen (galois'schen) Zahlkörpererweiterung L/K aus und halten Primideale $\mathfrak{P}$ von $\mathcal{O}_L$ und $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ von $\mathcal{O}_K$ fest.

Wir betrachten nun einen Zwischenkörper $K \subseteq K' \subseteq L$. K' ist der Fixkörper einer Untergruppe $H \subseteq G = Gal(L:K)$, also $K' = L_H$. Der Ganzheitsring ist $\mathcal{O}_{K'} = (\mathcal{O}_L)_{K'}$ und $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_{K'}$ ist das eindeutige $\mathcal{O}_{K'}$-Primideal unter $\mathfrak{P}$.
L/K' ist ebenfalls normal, sodass die Zerlegung- und Restklassengruppen D' bzw. I' definiert sind. Es ist $D' = D \cap H$ und $I' = I \cap H$ unmittelbar aus der Definition abzulesen.
Die Galois-Theorie gibt uns

$$L_{D'} = L_{D \cap H} = L_D \cdot L_H = L_D K' \qquad \text{und ebenso} \qquad L_{I'} = L_I K'.$$

Theorem 2.1.5. *Mit den obigen Bezeichnungen gilt:*

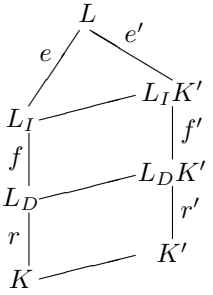
(i) L_D *ist der größte Zwischenkörper K', sodass $e_{\mathfrak{P}'|\mathfrak{p}} = f_{\mathfrak{P}'|\mathfrak{p}} = 1$ ist.*

(ii) L_D *ist der kleinste Zwischenkörper K', sodass $\mathfrak{P}$ das einzige $\mathcal{O}_L$-Primideal über $\mathfrak{P}'$ ist.*

(iii) L_I *ist der größte Zwischenkörper K', sodass $e_{\mathfrak{P}'|\mathfrak{p}} = 1$ ist.*

(iv) L_I *ist der kleinste Zwischenkörper K', sodass $\mathfrak{P}$ totalverzweigt über $\mathfrak{P}'$ ist (d. h. es gilt $e_{\mathfrak{P}|\mathfrak{P}'} = [L:K']$).*

Beweis. Nach Theorem 2.1.2 sind zunächst L_D und L_I Zwischenkörper mit diesen Eigenschaften. Es ergibt sich für einen Zwischenkörper $K \subseteq K' \subseteq L$ folgende Situation:



(i) Ist $K' = L_H$ ein Zwischenkörper mit Galois-Gruppe H und gilt $e_{\mathfrak{P}'|\mathfrak{p}} = f_{\mathfrak{P}'|\mathfrak{p}} = 1$, so folgt

$$f = f_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{P}'} = f' \qquad \text{und} \qquad e = e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{P}'} = e'.$$

Deshalb ist $[L : L_D] = [L : L_D K']$ und wegen $L_D \subseteq L_D K'$ muss $L_D = L_D K'$, also $K' \subseteq L_D$ gelten.

(ii) Sei $K' = L_H$ ein Zwischenkörper mit Galois-Gruppe H, sodass $\mathfrak{P}$ das einzige Primideal über $\mathfrak{P}'$ ist. Da jedes $\sigma \in H$ das Primideal $\mathfrak{P}$ auf das über $\mathfrak{P}'$ liegende Primideal $\sigma(\mathfrak{P})$ abbildet, muss $H \subseteq D$ sein. Die Galois-Theorie impliziert dann $L_D \subseteq L_H = K'$.

(iii) Ist $e_{\mathfrak{P}'|\mathfrak{p}} = 1$, so gilt $e = e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{P}'} = e'$ und wie bei (i) folgert man $K' \subseteq L_I$.

(iv) Ist $\mathfrak{P}$ totalverzweigt über $\mathfrak{P}'$, so gilt also $[L : L_I K'] = e' = [L : K']$. Erneut verwendet man die selben Argumente und schließt wegen $K' \subseteq L_I K'$ zunächst auf $K' = L_I K'$ und dann auf $L_I \subseteq K'$. □

Theorem 2.1.6. *Seien K, L, M Zahlkörper und gelte $K \subseteq L, M$. Für ein Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ gilt dann:*

(i) Ist $\mathfrak{p}$ unverzweigt in L und in M, so auch in LM.

(ii) Ist $\mathfrak{p}$ vollständig zerlegt in L und in M, so auch in LM.

Beweis. (i) Sei $\mathfrak{p}$ ein in L und M unverzweigtes $\mathcal{O}_K$-Primideal und $\mathfrak{P}'$ ein Primideal von LM über $\mathfrak{p}$. Bezeichne F die normale Hülle von LM über K und $\mathfrak{P}$ ein beliebiges Primideal von F über $\mathfrak{P}'$. Nach Voraussetzung sind $\mathfrak{P} \cap L$ und $\mathfrak{P} \cap M$ unverzweigt über $\mathfrak{p}$, d. h. $e_{\mathfrak{P}\cap L|\mathfrak{p}} = e_{\mathfrak{P}\cap M|\mathfrak{p}} = 1$. Theorem 2.1.5.(iii) gibt uns $L, M \subseteq F_I$. Also gilt auch $LM \subseteq F_I$ und erneut mit Theorem 2.1.5.(iii) schließt man, dass $\mathfrak{P} \cap LM = \mathfrak{P}'$ unverzweigt über $\mathfrak{p}$ ist.

(ii) Sei nun $\mathfrak{p}$ vollständig zerlegt in L und in M und $\mathfrak{P}'$ ein Primideal von LM über $\mathfrak{p}$, so ist $e_{\mathfrak{P}'|\mathfrak{p}} = f_{\mathfrak{P}'|\mathfrak{p}} = 1$ zu zeigen. Sei erneut F die normale Hülle von LM über K und $\mathfrak{P}$ ein Primideal von F über $\mathfrak{P}'$.
Nach Voraussetzung gilt

$$e_{\mathfrak{P}\cap L|\mathfrak{p}} = e_{\mathfrak{P}\cap M|\mathfrak{p}} = f_{\mathfrak{P}\cap L|\mathfrak{p}} = f_{\mathfrak{P}\cap M|\mathfrak{p}} = 1.$$

Nach Theorem 2.1.5.(i) muss deshalb $L, M \subseteq F_D$ gelten, also ist auch $LM \subseteq F_D$. Erneute Anwendung des Theorems 2.1.5.(i) liefert für $\mathfrak{P} \cap LM = \mathfrak{P}'$ die Behauptung. □

Korollar 2.1.7. *Seien $K \subseteq L$ Zahlkörper und $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Ist $\mathfrak{p}$ unverzweigt oder vollständig zerlegt in L, so auch in der normalen Hülle F von L über K.*

Beweis. Die normale Hülle F von LM über K besitzt die Darstellung

$$F = \prod_{\sigma \in Hom_K(L,\mathbb{C})} \sigma(L).$$

Die Zerlegung von $\mathfrak{p}$ in $\sigma(L)$ erhält man unmittelbar durch Anwenden von σ auf die Zerlegung von $\mathfrak{p}$ in L. Ist also $\mathfrak{p}$ unverzweigt oder vollständig zerlegt in L, so auch in jedem $\sigma(L)$. Mit Theorem 2.1.7 und der obigen Darstellung von F ist dann $\mathfrak{p}$ unverzweigt oder vollständig zerlegt in F. □

2.2 Die Artin-Abbildung

Lemma 2.2.1. *Sei $K \subseteq L$ eine galois'sche Erweiterung von Zahlkörpern und $\mathfrak{p} \subset \mathcal{O}_K$ ein in L unverzweigtes Primideal. Ist $\mathfrak{P} \subset \mathcal{O}_L$ ein Primideal über $\mathfrak{p}$, so existiert ein eindeutig bestimmtes Element $\sigma \in Gal(L:K)$, sodass gilt*

$$\forall \alpha \in \mathcal{O}_L : \ \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

Beweis. Bezeichne wie im letzten Abschnitt $D_\mathfrak{P}$ und $I_\mathfrak{P}$ die Zerlegungs- und Restklassengruppe von $\mathfrak{P}$. Jedes $\sigma \in D_\mathfrak{P}$ induziert einen Automorphismus $\overline{\sigma} \in \tilde{G} = Gal(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$. Nach Kor. 2.1.3 gibt uns die induzierte Abbildung einen Gruppenisomorphismus $D_\mathfrak{P}/I_\mathfrak{P} \simeq \tilde{G}$ und nach Theorem 2.1.2 ist $|D_\mathfrak{P}| = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$ und $|I_\mathfrak{P}| = e_{\mathfrak{P}|\mathfrak{p}}$. In unserer Situation ist $\mathfrak{p}$ unverzweigt, also gilt $e_{\mathfrak{P}|\mathfrak{p}} = 1$ und $D_\mathfrak{P} \simeq \tilde{G}$.
Es sind $\mathcal{O}_L/\mathfrak{P}$ und $\mathcal{O}_K/\mathfrak{p}$ endliche Körper. Ist $|\mathcal{O}_K/\mathfrak{p}| = q$, so wird bekanntermaßen $\tilde{G}$ vom Frobenius-Endomorphismus $x \mapsto x^q$ erzeugt. Folglich existiert ein eindeutiges Element $\sigma_0 \in D_\mathfrak{P}$, welches auf den Frobenius-Endomorphismus abgebildet wird. Es ist $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = q$, also

$$\sigma_0(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P} \qquad \text{für alle } \alpha \in \mathcal{O}_L.$$

Angenommen $\sigma_1 \in Gal(L:K)$ ist ein weiteres Element mit $\sigma_1(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$ für alle $\alpha \in \mathcal{O}_L$. Dann muss für $\alpha \in \mathfrak{P}$ gelten $\sigma_1(\alpha) \in \mathfrak{P}$. Es folgt $\sigma_1(\mathfrak{P}) = \mathfrak{P}$, d. h. σ_1 liegt in $D_\mathfrak{P}$. In $D_\mathfrak{P}$ ist σ_0 aber eindeutig, also gilt $\sigma_1 = \sigma_0$. □

Definition 2.2.2. Das eindeutige Element σ_0 aus Lemma 2.2.1 heißt **Artin-Symbol** und wird mit $\left(\frac{L/K}{\mathfrak{P}}\right)$ bezeichnet.

Korollar 2.2.3. *Sei L/K eine galois'sche Zahlkörpererweiterung, $\mathfrak{p} \subset \mathcal{O}_K$ ein unverzweigtes Primideal und $\mathfrak{P} \subset \mathcal{O}_L$ ein Primideal über $\mathfrak{p}$.*

(i) Für $\sigma \in Gal(L:K)$ gilt $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$.

(ii) $ord\left(\frac{L/K}{\mathfrak{P}}\right) = f_{\mathfrak{P}|\mathfrak{p}}$.

(iii) $\mathfrak{p}$ ist vollständig zerlegt $\quad \Leftrightarrow \quad \left(\frac{L/K}{\mathfrak{P}}\right) = id.$

Beweis. (i) Für beliebige $\sigma \in Gal(L:K)$ und $\alpha \in \mathcal{O}_L$ gilt $\left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}(\alpha) \equiv \sigma^{-1}(\alpha)^{N(\mathfrak{p})} \bmod \mathfrak{P}$, also

$$\sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \equiv \left(\frac{L/K}{\sigma(\mathfrak{P})}\right)(\alpha) \bmod \sigma(\mathfrak{P}).$$

Da das Artin-Symbol eindeutig ist, folgt die Behauptung.

(ii) Da $\mathfrak{p}$ unverzweigt ist, gilt $|D_\mathfrak{P}| = |\tilde{G}| = |\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}| = f_{\mathfrak{P}|\mathfrak{p}}$. Das Artin-Symbl wird auf einen Erzeuger von $\tilde{G}$ abgebildet und hat deshalb Ordnung $f_{\mathfrak{P}|\mathfrak{p}}$.

(iii) Da wir $e_{\mathfrak{P}|\mathfrak{p}} = 1$ vorausgesetzt haben ($\mathfrak{p}$ ist unverzweigt), gilt folgende Äquivalenz:
$\mathfrak{p}$ ist vollst. zerlegt $\Leftrightarrow f_{\mathfrak{P}|\mathfrak{p}} = 1 \Leftrightarrow \left(\frac{L/K}{\mathfrak{P}}\right) = id.$ □

Ist L/K eine galois'sche Erweiterung mit abelscher Galois-Gruppe (man sagt dann auch L/K ist abelsch), so hängt das Artin-Symbol nur von $\mathfrak{p}$ und nicht von $\mathfrak{P}$ ab!
Sind nämlich $\mathfrak{P}$, $\mathfrak{P}'$ zwei $\mathcal{O}_L$-Primideale über $\mathfrak{p}$, so existiert ein $\sigma \in Gal(L:K)$ mit $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Mit diesem σ gilt

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right),$$

wobei beim letzten Gleichheitszeichen die Kommutativität ausgenutzt wurde.
Ist L/K eine abelsche Erweiterung, so schreibt man für das Artin-Symbol auch

$$\left(\frac{L/K}{\mathfrak{p}}\right).$$

Ist L/K eine unverzweigte abelsche Erweiterung (d.h. *alle* Primideale von K sind unverzweigt in L), so ist das Artin-Symbol für alle $\mathcal{O}_K$-Primideale definiert. Das Artin-Symbol lässt sich dann in kanonischer Weise auf alle gebrochenen $\mathcal{O}_K$-Ideale fortsetzen. Ist nämlich $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i} \in I_K$, $r_i \in \mathbb{Z}$ ein gebrochenes $\mathcal{O}_K$-Ideal, so definiert man

$$\left(\frac{L/K}{\mathfrak{a}}\right) := \prod_{i=1}^{r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}.$$

Die so definerte Abbildung

$$\left(\frac{L/K}{\cdot}\right) : \; I_K \to Gal(L:K)$$

heißt **Artin-Abbildung**.

2.3 Theorie der Ringklassenkörper

Beschäftigt man sich mit Bewertungen von Zahlkörpern K, so stellt sich heraus, dass die Primideale von $\mathcal{O}_K$ in Beziehung zu den nicht-archimedischen Bewertungen stehen, während bei archimedischen Bewertungen eine Korrespondenz zu den Einbettungen von K in $\mathbb{C}$ besteht. Primideale von $\mathcal{O}_K$ heißen deshalb oft auch **endliche Primstellen**, während Einbettungen von K in $\mathbb{C}$ auch **unendliche Primstellen** heißen. Eine Einbettung $\sigma : K \to \mathbb{R}$ heißt dann auch **reelle** unendliche Primstelle und ein Paar komplex-konjugierter Einbettungen $\sigma, \overline{\sigma} : K \to \mathbb{C}$ **komplexe** unendliche Nullstelle.
Ist eine Erweiterung $K \subseteq L$ gegeben, so heißt eine unendliche Primstelle σ von K **verzweigt** in L, wenn σ reell ist, aber eine komplexe Fortsetzung auf L besitzt.

Definition 2.3.1. Ist K ein Zahlkörper, so ist ein **Modulus** $\mathfrak{m}$ in K ein formales Produkt

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$$

über alle (endlichen und unendlichen) Primstellen $\mathfrak{p}$ von K. Die Exponenten erfüllen dabei

(i) $n_\mathfrak{p} \geq 0$, und nur endlich viele sind von Null verschieden.
(ii) $n_\mathfrak{p} = 0$, falls $\mathfrak{p}$ eine komplexe unendliche Primstelle ist.
(iii) $n_\mathfrak{p} \leq 1$, falls $\mathfrak{p}$ eine reelle unendliche Primstelle ist.

Ein Modulus $\mathfrak{m}$ kann daher als $\mathfrak{m}_0\mathfrak{m}_\infty$ geschrieben werden, wobei $\mathfrak{m}_0$ ein $\mathcal{O}_K$-Ideal und $\mathfrak{m}_\infty$ ein Produkt über verschiedene reelle unendliche Primstellen von K ist. Sind alle $n_\mathfrak{p} = 0$, so setzt man $\mathfrak{m} = 1$.
Im Falle eines imaginär-quadratischen Zahlkörpers ist ein Modulus schlicht ein Ideal des Ganzheitsringes.

Definition 2.3.2. Sei K ein Zahlkörper und $\mathfrak{m}$ ein Modulus.
Es bezeichne $I_K(\mathfrak{m})$ die Gruppe der gebrochenen $\mathcal{O}_K$-Ideale, die teilerfremd zu $\mathfrak{m}$ (d. h. zu $\mathfrak{m}_0$) sind.

Mit $P_{K,1}(\mathfrak{m})$ sei die Untergruppe von $I_K(\mathfrak{m})$ gemeint, die von allen Hauptidealen $\alpha\mathcal{O}_K$ erzeugt wird, mit $\alpha \in \mathcal{O}_K$ und

$$\alpha \equiv 1 \bmod \mathfrak{m}_0 \quad \text{sowie} \quad \sigma(\alpha) > 0 \text{ für reelle unendl. Primstellen } \sigma \text{ mit } \sigma|\mathfrak{m}_\infty.$$

Definition 2.3.3. Sei K ein Zahlkörper, $\mathfrak{m}$ ein Modulus von K und $H \subseteq I_K(\mathfrak{m})$ eine Untergruppe. H heißt **Kongruenz-Untergruppe** für $\mathfrak{m}$, wenn $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$ gilt. In diesem Fall heißt $I_K(\mathfrak{m})/H$ **allgemeine Idealklassengruppe** für $\mathfrak{m}$.

Beispiel. (i) Wir betrachten den Modulus $\mathfrak{m} = 1$. Dann ist $P_K = P_{K,1}(1)$ eine Kongruenz-Untergruppe und $C(\mathcal{O}_K) = I_K/P_K$ die zugehörige allgemeine Idealklassengruppe.

(ii) Sei $\mathcal{O}$ eine Ordnung mit Führer f eines imaginär-quadratischen Zahlkörpers K. Nach Prop. 1.5.6 ist $C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$. Setzen wir $\mathfrak{m} = f\mathcal{O}_K$, so ist nach Definition

$$P_{K,1}(f\mathcal{O}_K) \subseteq P_{K,\mathbb{Z}}(f) \subseteq I_K(f) = I_K(f\mathcal{O}_K),$$

also $C(\mathcal{O})$ eine allgemeine Idealklassengruppe.

Sei L/K eine abelsche Zahlkörpererweiterung und $\mathfrak{m}$ ein Modulus, welcher von allen in L verzweigten Primstellen von K geteilt wird (nach Prop. 1.1.3 sind dies nur endich viele). Ist $\mathfrak{p}$ ein Primideal, welches $\mathfrak{m}$ nicht teilt, so ist das Artin-Symbol $((L/K)/\mathfrak{p})$ in $Gal(L:K)$ definiert. Multiplikativ fortgesetzt gibt uns dies einen Homomorphismus

$$\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to Gal(L:K),\ \prod_{i=1}^{r} \mathfrak{p}_i^{r_i} \mapsto \prod_{i=1}^{r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i},$$

welcher Artin-Abbildung für L/K und $\mathfrak{m}$ heißt. (Ist die Körpererweiterung klar, so schreibt man auch kurz $\Phi_\mathfrak{m}$.)
Es folgen nun zunächst drei Theoreme ohne Beweis (siehe [7, Kapitel V, Theoreme 5.7, 12.7 und 9.16]).

Theorem 2.3.4 (Artins Reziprozitäts-Theorem)**.** *Sei $K \subseteq L$ eine abelsche Erweiterung von Zahlkörpern und $\mathfrak{m}$ ein Modulus, welcher von allen in L verzweigten Primstellen von K geteilt wird.*

(i) Die Artin-Abbildung $\Phi_\mathfrak{m}$ ist surjektiv.

(ii) Sind die Exponenten der endlichen Primstellen welche $\mathfrak{m}$ teilen genügend groß gewählt worden, so ist $Ker(\Phi_\mathfrak{m})$ eine Kongruenz-Untergruppe von $\mathfrak{m}$, d. h es gilt

$$P_{K,1}(\mathfrak{m}) \subseteq Ker(\Phi_\mathfrak{m}) \subseteq I_K(\mathfrak{m}).$$

Der Isomorphismus $I_K(\mathfrak{m})/Ker(\Phi_\mathfrak{m}) \simeq Gal(L:K)$ zeigt, dass $Gal(L:K)$ eine allgemeine Idealklassengruppe für den Modulus $\mathfrak{m}$ ist.

Der Modulus $\mathfrak{m}$ in Thm. 2.3.4 ist nicht eindeutig bestimmt. Ist nämlich $\mathfrak{n}$ ein weiterer Modulus, der von $\mathfrak{m}$ geteilt wird, so gilt

$$P_{K,1}(\mathfrak{m}) \subseteq Ker(\Phi_\mathfrak{m}) \quad \Rightarrow \quad P_{K,1}(\mathfrak{n}) \subseteq Ker(\Phi_\mathfrak{n}).$$

Da nämlich $\mathfrak{m}$ ein Teiler von $\mathfrak{n}$ ist, gilt $\mathfrak{n}_0 \subseteq \mathfrak{m}_0$ und für jedes $\sigma|\mathfrak{m}_\infty$ gilt $\sigma|\mathfrak{n}_\infty$. Ist dann $\alpha \in \mathcal{O}_K$ ein erzeugendes Element von $P_{K,1}(\mathfrak{n})$, so liegt α auch in $P_{K,1}(\mathfrak{m})$. Deshalb ist nach Voraussetzung $\Phi_\mathfrak{m}(\alpha) = \Phi_\mathfrak{n}(\alpha) = id$, das heißt α liegt in $Ker(\Phi_\mathfrak{n})$ und die Behauptung ist gezeigt. Dies hat zur Folge, dass in der obigen Situation

$$I_K(\mathfrak{m})/Ker(\Phi_\mathfrak{m}) \simeq Gal(L:K) \simeq I_K(\mathfrak{n})/Ker(\Phi_\mathfrak{n})$$

gilt. Ein Modulus ist jedoch vor allen anderen ausgezeichnet.

Theorem 2.3.5 (Führer-Theorem). *Sei L/K eine abelsche Erweiterung von Zahlkörpern. Es existiert ein Modulus $\mathfrak{f} = \mathfrak{f}(L/K)$, sodass gilt:*

(i) Jede unendliche oder endliche Primstelle von K ist genau dann in L verzweigt, wenn sie $\mathfrak{f}$ teilt.

(ii) Sei $\mathfrak{m}$ ein Modulus, welcher von allen in L verzweigten Primstellen von K geteilt wird. Dann ist $Ker(\Phi_{\mathfrak{m}})$ genau dann eine Kongruenz-Untergruppe für $\mathfrak{m}$, wenn $\mathfrak{f}$ ein Teiler von $\mathfrak{m}$ ist.

Der Modulus $\mathfrak{f}$ ist eindeutig durch L/K bestimmt und heißt der **Führer** der Erweiterung, wodurch sich auch der Name des Theorems erklärt.

Theorem 2.3.6 (Existenz-Theorem). *Sei $\mathfrak{m}$ ein Modulus von K, H eine Kongruenz-Untergruppe für $\mathfrak{m}$, d. h. es ist $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$.*

Dann existiert eine eindeutige abelsche Erweiterung L/K, sodass alle in L verzweigten Primstellen von K $\mathfrak{m}$ teilen. Ist weiter

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to Gal(L:K)$$

die Artin-Abbildung von L/K, so ist

$$H = Ker(\Phi_{\mathfrak{m}}).$$

Korollar 2.3.7. *Seien L und M abelsche Erweiterungen des Zahlkörpers K. Es gilt genau dann $L \subseteq M$, wenn ein Modulus $\mathfrak{m}$ existiert, der von allen Primstellen von K geteilt wird, die in L oder M verzweigten sind, und folgende Inklusionskette gilt:*

$$P_{K,1}(\mathfrak{m}) \subseteq Ker(\Phi_{M/K,\mathfrak{m}}) \subseteq Ker(\Phi_{L/K,\mathfrak{m}}).$$

Beweis. Sei zunächst $L \subseteq M$. Dann gibt es die natürliche Restriktion $\pi : Gal(M:K) \to Gal(L:K)$. Nach Thm. 2.3.5 existieren zu L und M die Führer $\mathfrak{f}_L$ und $\mathfrak{f}_M$. Setzen wir $\mathfrak{m} = \mathfrak{f}_L\mathfrak{f}_M$, so sind erneut nach Thm. 2.3.5 $Ker(\Phi_{L/K,\mathfrak{m}})$ und $Ker(\Phi_{M/K,\mathfrak{m}})$ Kongruenz-Untergruppen, d. h. insbesondere

$$P_{K,1}(\mathfrak{m}) \subseteq Ker(\Phi_{M/K,\mathfrak{m}}),\ Ker(\Phi_{L/K,\mathfrak{m}}).$$

Wir behaupten $\pi \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$. Es genügt dies für Primideale in $I_K(\mathfrak{m})$ zu zeigen, denn die Artin-Abbildung ist multiplikativ. Seien also $\mathfrak{p} \in I_K(\mathfrak{m})$ ein Primideal und $\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{Q} \subset \mathcal{O}_M$ Primideale mit $\mathfrak{p} \subseteq \mathfrak{P} \subseteq \mathfrak{Q}$. Es ist zu zeigen, dass für alle $\alpha \in \mathcal{O}_L$ gilt:

$$\left(\frac{M/K}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{Q} \quad \overset{!}{\equiv} \quad \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P} \equiv \left(\frac{L/K}{\mathfrak{p}}\right)(\alpha).$$

Ist also $\alpha \in \mathcal{O}_L$, so gilt per Definition, dass

$$\left(\frac{M/K}{\mathfrak{p}}\right)(\alpha) - \alpha^{N(\mathfrak{p})} \in \mathfrak{Q}$$

ist. Da L/K galois'sch ist, ist die Einschränkung von $((M/K)/\mathfrak{p})$ auf L ein Element von $\mathrm{Gal}(L:K)$. Also liegt $((M/K)/\mathfrak{p})(\alpha)$ in $\mathcal{O}_L$. Folglich ist auch

$$\left(\frac{M/K}{\mathfrak{p}}\right)(\alpha) - \alpha^{N(\mathfrak{p})} \in \mathcal{O}_L$$

und da $\mathfrak{Q} \cap \mathcal{O}_L = \mathfrak{P}$ ist, gilt die Behauptung.
Das impliziert, dass für ein Ideal $\mathfrak{a} \in I_K(\mathfrak{m})$, für welches $\Phi_{M/K,\mathfrak{m}}(\mathfrak{a}) = id$ gilt, auch $\Phi_{L/K,\mathfrak{m}}(\mathfrak{a}) = \pi \circ \Phi_{M/K,\mathfrak{m}}(\mathfrak{a}) = id$ ist. Also gilt

$$Ker(\Phi_{M/K,\mathfrak{m}}) \subseteq Ker(\Phi_{L/K,\mathfrak{m}}).$$

Gelte andererseits $P_{K,1}(\mathfrak{m}) \subseteq Ker(\Phi_{M/K,\mathfrak{m}}) \subseteq Ker(\Phi_{L/K,\mathfrak{m}})$ mit einem den Voraussetzungen nach gewählten Modulus $\mathfrak{m}$. Dann sind die Abbildungen $\Phi_{M/K,\mathfrak{m}}$ und $\Phi_{L/K,\mathfrak{m}}$ auf ganz $I_K(\mathfrak{m})$ definiert. Unter der Artin-Abbildung für M/K und $\mathfrak{m}$

$$\Phi_{M/K,\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(M:K)$$

wird $Ker(\Phi_{L/K,\mathfrak{m}})$ auf eine Untergruppe $H \subseteq Gal(M:K)$ abgebildet. Setzen wir $\tilde{L} = L_H$, also $K \subseteq \tilde{L} \subseteq M$, so ist $M/\tilde{L}$ abelsch mit $Gal(M:\tilde{L}) = H$.
Ebenfalls ist $\tilde{L}/K$ abelsch und wir wenden die schon bewiesene Richtung auf $K \subseteq \tilde{L} \subseteq M$ an. Dies gibt uns die Existenz eines Modulus $\tilde{\mathfrak{m}}$, der von allen in $\tilde{L}$ und M verzweigten Primidealen von K geteilt wird, so dass

$$P_{K,1}(\tilde{\mathfrak{m}}) \subseteq Ker(\Phi_{M/K,\tilde{\mathfrak{m}}}) \subseteq Ker(\Phi_{\tilde{L}/K,\tilde{\mathfrak{m}}})$$

gilt. Definieren wir $\mathfrak{n} := \tilde{\mathfrak{m}}\mathfrak{m}$, so folgt aus der Überlegung nach Thm. 2.3.4, dass auch $P_{K,1}(\mathfrak{n}) \subseteq Ker(\Phi_{M/K,\mathfrak{n}})$ gilt.
Ebenso folgt $Ker(\Phi_{M/K,\mathfrak{n}}) \subseteq Ker(\Phi_{\tilde{L}/K,\mathfrak{n}})$. Wäre dem nämlich nicht so, so existierte ein $\mathfrak{a} \in Ker(\Phi_{M/K,\mathfrak{n}}) \subseteq I_K(\mathfrak{n})$, also wegen $I_K(\mathfrak{n}) \subseteq I_K(\tilde{\mathfrak{m}})$ ein $\mathfrak{a} \in I_K(\tilde{\mathfrak{m}})$, mit $\mathfrak{a} \notin Ker(\Phi_{\tilde{L}/K,\mathfrak{n}})$. D. h. jedoch $Ker(\Phi_{M/K,\tilde{\mathfrak{m}}}) \not\subseteq Ker(\Phi_{\tilde{L}/K,\tilde{\mathfrak{m}}})$, Widerspruch! Mit anderen Worten gilt

$$P_{K,1}(\mathfrak{n}) \subseteq Ker(\Phi_{M/K,\mathfrak{n}}) \subseteq Ker(\Phi_{\tilde{L}/K,\mathfrak{n}}),$$

und die gleichen Überlegungen für K, L, M führen auf

$$P_{K,1}(\mathfrak{n}) \subseteq Ker(\Phi_{M/K,\mathfrak{n}}) \subseteq Ker(\Phi_{L/K,\mathfrak{n}}).$$

Es lässt sich also ein Modulus für beide Ketten angeben, so dass wir o. B. d. A. $\mathfrak{m} = \tilde{\mathfrak{m}}$ und damit

$$Ker(\Phi_{M/K,\mathfrak{m}}) \subseteq Ker(\Phi_{\tilde{L}/K,\mathfrak{m}}). \tag{2.3.1}$$

annehmen können. Es ist nach Definition $\Phi_{M/K,\mathfrak{m}}(Ker(\Phi_{L/K,\mathfrak{m}})) = H = Gal(M:\tilde{L})$. Unter Verwendung von $((M/K)/\cdot)|_{\tilde{L}} = ((\tilde{L}/K)/\cdot)$ folgt

$$\begin{aligned}
\Phi_{M/K,\mathfrak{m}}(Ker(\Phi_{\tilde{L}/K,\mathfrak{m}})) &= \left\{((M/K)/\mathfrak{a}) :\ \mathfrak{a} \in I_K(\mathfrak{m}),\ ((\tilde{L}/K)/\mathfrak{a}) = id\right\} \\
&= \left\{\sigma \in Gal(M:K) :\ \sigma = \Phi_{M/K,\mathfrak{m}}(\mathfrak{a}),\ \mathfrak{a} \in I_K(\mathfrak{m}),\ \sigma|_{\tilde{L}} = id\right\} \\
&= Gal(M:\tilde{L}).
\end{aligned}$$

Zusammenfassend gilt also

$$\Phi_{M/K,\mathfrak{m}}(Ker(\Phi_{L/K,\mathfrak{m}})) = H = Gal(M:\tilde{L}) = \Phi_{M/K,\mathfrak{m}}(Ker(\Phi_{\tilde{L}/K,\mathfrak{m}})).$$

Da $Ker(\Phi_{M/K,\mathfrak{m}})$ sowohl in $Ker(\Phi_{L/K,\mathfrak{m}})$ nach Voraussetzung als auch in $Ker(\Phi_{\tilde{L}/K,\mathfrak{m}})$ nach (2.3.1) liegt, folgt mit einem einfachen gruppentheoretischen Argument

$$Ker(\Phi_{L/K,\mathfrak{m}})) = Ker(\Phi_{\tilde{L}/K,\mathfrak{m}}).$$

Aus Theorem 2.3.6 folgt dann $L = \tilde{L} \subseteq M$. □

Das Existenz-Theorem offenbart eine interessante Beziehung zwischen allgemeinen Idealklassengruppen eines Zahlkörpers und abelschen Erweiterungen.

Ist K ein Zahlkörper und der Modulus $\mathfrak{m} = 1$ gegeben, so ist $P_K = P_{K,1}(\mathfrak{m})$. Nach Thm. 2.3.6 existiert eine unverzweigte (denn $\mathfrak{m} = 1$) abelsche Erweiterung H_K/K, und die Artin-Abbildung gibt uns die Isomorphie

$$C(\mathcal{O}_K) = I_K/P_K \xrightarrow{\sim} Gal(H_K:K).$$

Definition und Theorem 2.3.8. Der Körper H_K heißt **Hilbert Klassenkörper** von K. Der Hilbert Klassenkörper ist die maximale unverzweigte abelsche Erweiterung von K und als solche eindeutig.

Beweis. Es ist H_K eine unverzweigte abelsche Erweiterung von K.
Sei nun M eine weitere unverzweigte abelsche Erweiterung von K. Da M/K unverzweigt ist, muss nach Thm. 2.3.5 dann $\mathfrak{f}(M/K) = 1$ sein. Erneut nach Thm. 2.3.5 ist $Ker(\Phi_{M/K,1})$ eine Kongruenz-Untergruppe für den Modulus 1, insbesondere gilt

$$P_K \subseteq Ker(\Phi_{M/K,1}).$$

Nach Definition von H_K ist

$$P_K = Ker(\Phi_{H_K/K,1}) \subseteq Ker(\Phi_{M/K,1}),$$

und Kor. 2.3.7 gibt $M \subseteq H_K$. □

Korollar 2.3.9. *Sei H_K der Hilbert Klassenkörper des Zahlkörpers K und $\mathfrak{p}$ ein Primideal von K. Es gilt:*

$$\mathfrak{p} \text{ ist vollständig zerlegt in } H_K \quad \Leftrightarrow \quad \mathfrak{p} \text{ ist ein } \mathcal{O}_K\text{-Hauptideal.}$$

Beweis. Nach Kor. 2.2.3 ist $\mathfrak{p}$ genau dann vollständig zerlegt in H_K, wenn $((H_K/K)/\mathfrak{p}) = id$ gilt. Da $C(\mathcal{O}_K) \simeq Gal(H_K : K)$ ist, ist genau dann $((H_K/K)/\mathfrak{p}) = id$, wenn $\mathfrak{p}$ ein Hauptideal ist. □

Ist $\mathcal{O}$ eine Ordnung zum Führer f eines Zahlkörpers K, so ist $C(\mathcal{O})$ eine allgemeine Idealklassengruppe, denn es gilt $P_{K,1}(f) \subseteq P_{K,\mathbb{Z}}(f) \subseteq I_K(f)$.
Auch hier gibt uns das Existenz Theorem 2.3.6 eine abelsche Erweiterung $H_{\mathcal{O}}$, sodass alle in $H_{\mathcal{O}}$ verzweigten $\mathcal{O}_K$-Primideale $f\mathcal{O}_K$ teilen, und die Artin-Abbildung induziert einen Isomorphismus

$$C(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f) \simeq Gal(H_{\mathcal{O}} : K).$$

Definition 2.3.10. Der Körper $H_{\mathcal{O}}$ heißt **Ringklassenkörper** der Ordnung $\mathcal{O}$.

Lemma 2.3.11. *Sei $H_{\mathcal{O}}$ der Ringklassenkörper einer Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers K, so ist $H_{\mathcal{O}}$ galois'sch über $\mathbb{Q}$.*

Beweis. Sei $\mathfrak{m} := f\mathcal{O}_K$ und f der Führer von $\mathcal{O}$. τ bezeichne die komplexe Komjugation. Unmittelbar aus der Definition folgert man, dass $\tau(\mathfrak{m}) = \mathfrak{m}$ und $\tau(P_{K,\mathbb{Z}}(f)) = P_{K,\mathbb{Z}}(f)$ gilt. Außerdem ist mit $H_{\mathcal{O}}/K$ auch $\tau(H_{\mathcal{O}})/K$ abelsch (es gilt $\tau(K) = K$). Wir behaupten weiter

$$Ker(\Phi_{\tau(H_{\mathcal{O}})/K,\mathfrak{m}}) = \tau(Ker(\Phi_{H_{\mathcal{O}}/K,\mathfrak{m}})). \tag{2.3.2}$$

Es genügt hier die Gleichheit für Primideale der erzeugenden Mengen zu zeigen.
Unmittelbar aus der Definition folgert man, dass $\mathfrak{p}$ genau dann ein Primideal von K ist, wenn $\tau(\mathfrak{p})$ ein Primideal von K ist. Da $N(\mathfrak{p}) = N(\tau(\mathfrak{p}))$ ist, sieht man mit Lemma 1.5.2 ein, dass

$$\mathfrak{p} \in I_K(\mathfrak{m}) \qquad \Longleftrightarrow \qquad \tau(\mathfrak{p}) \in I_K(\mathfrak{m})$$

gilt. Die Zerlegungen von $\tau(\mathfrak{p})$ in $H_{\mathcal{O}}$ und von $\mathfrak{p}$ in $\tau(H_{\mathcal{O}})$ bedingen sich gegenseitig, d. h.

$$\tau(\mathfrak{p}) = \prod \mathfrak{P}_i \text{ in } H_{\mathcal{O}} \qquad \Longleftrightarrow \qquad \mathfrak{p} = \prod \tau(\mathfrak{P}_i) \text{ in } \tau(H_{\mathcal{O}}).$$

Deshalb gilt für ein beliebiges Primideal $\mathfrak{P}$ von $H_{\mathcal{O}}$ über $\tau(\mathfrak{p})$ (und damit auch für ein beliebiges Primideal $\tau(\mathfrak{P})$ von $\tau(H_{\mathcal{O}})$ über $\mathfrak{p}$) $f_{\tau(\mathfrak{P})|\mathfrak{p}} = 1 \Leftrightarrow f_{\mathfrak{P}|\tau(\mathfrak{p})} = 1$. Mit anderen Worten ist

$$\left(\frac{H_{\mathcal{O}}/K}{\tau(\mathfrak{p})}\right) = id \qquad \Longleftrightarrow \qquad \left(\frac{\tau(H_{\mathcal{O}})/K}{\mathfrak{p}}\right) = id.$$

Da $\tau = \tau^{-1}$ gilt, ist die Mengengleichheit (2.3.2) klar. Wir stellen deshalb fest, dass

$$Ker(\Phi_{H_\mathcal{O}/K,\mathfrak{m}}) = P_{K,\mathbb{Z}}(f) = \tau(P_{K,\mathbb{Z}}(f)) = \tau(Ker(\Phi_{H_\mathcal{O}/K,\mathfrak{m}})) = Ker(\Phi_{\tau(H_\mathcal{O})/K,\mathfrak{m}})$$

gilt und mit Korollar 2.3.7 folgert man $\tau(H_\mathcal{O}) = H_\mathcal{O}$. Es gilt

$$\tau(H_\mathcal{O}) = H_\mathcal{O} \qquad \Longleftrightarrow \qquad H_\mathcal{O}/\mathbb{Q} \text{ galois'sch.}$$

Ist nämlich $\sigma \in Hom_\mathbb{Q}(H_\mathcal{O}, \mathbb{C})$, so ist $\sigma|_K \in Gal(K : \mathbb{Q})$ und deshalb $\sigma|_K = id$ oder $\sigma|_K = \tau$. Im ersten Fall ist $\sigma \in Gal(H_\mathcal{O} : K)$ und damit $\sigma(H_\mathcal{O}) = H_\mathcal{O}$. Im zweiten Fall ist $\sigma \circ \tau \in Gal(H_\mathcal{O} : K)$ und deshalb ebenfalls $\sigma(H_\mathcal{O}) = \sigma \circ \tau \circ \tau(H_\mathcal{O}) = \sigma \circ \tau(H_\mathcal{O}) = H_\mathcal{O}$. Folglich ist $H_\mathcal{O}/\mathbb{Q}$ normal und damit galois'sch, wir sind am Ziel! □

Für den Fall eines imaginär-quadratischen Zahlkörpers K erhalten wir folgende Spezialisierung von Korollar 2.3.9.

Theorem 2.3.12. *Sei $\mathcal{O}$ eine Ordnung mit Diskriminante D des imaginär-quadratischen Zahlkörpers K und bezeichne $H_\mathcal{O}$ den Ringklassenkörper zu $\mathcal{O}$. Ist p eine ungerade Primzahl und $p \nmid D$, so gilt:*

$$\begin{aligned} &p \textit{ zerfällt in zwei verschiedene } \mathcal{O}\textit{-Hauptideale} \\ \Leftrightarrow\quad &p \textit{ ist vollständig zerlegt in } H_\mathcal{O}. \end{aligned}$$

Beweis. Bezeichnet f den Führer von $\mathcal{O}$, so ist $\mathcal{O} = [1, fw_K]$ und $D = f^2 d_K$. Da p nicht $f^2 d_K$ teilt, ist p zu f teilerfremd. Außerdem ist p nach Prop. 1.2.2 unverzweigt in $\mathcal{O}_K$. Wir beweisen:

$$\begin{aligned} &p \text{ zerfällt in zwei verschiedene } \mathcal{O}\text{-Hauptideale} \\ \overset{(1)}{\Leftrightarrow}\quad &p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ und } \mathfrak{p} = \alpha\mathcal{O}_K,\ \alpha \in \mathcal{O} \\ \overset{(2)}{\Leftrightarrow}\quad &p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ und } \mathfrak{p} \in P_{K,\mathbb{Z}}(f) \\ \overset{(3)}{\Leftrightarrow}\quad &p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ und } \left(\frac{H_\mathcal{O}/K}{\mathfrak{p}}\right) = id \\ \overset{(4)}{\Leftrightarrow}\quad &p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}} \text{ und } \mathfrak{p} \text{ zerfällt vollständig in } H_\mathcal{O} \\ \overset{(5)}{\Leftrightarrow}\quad &p \text{ zerfällt vollständig in } H_\mathcal{O}. \end{aligned}$$

(1) Für $\alpha \in \mathcal{O}$ gilt

$$p\mathcal{O} = \mathfrak{q}\bar{\mathfrak{q}},\ \mathfrak{q} \neq \bar{\mathfrak{q}},\ \mathfrak{q} = \alpha\mathcal{O} \quad \Leftrightarrow \quad p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}},\ \mathfrak{p} = \alpha\mathcal{O}_K.$$

Proposition 1.5.4 gibt nämlich $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}$ und $\mathfrak{p} = \mathfrak{q}\mathcal{O}_K$. Ist $\mathfrak{q} \neq \bar{\mathfrak{q}}$, so muss auch $\mathfrak{p} \neq \bar{\mathfrak{p}}$ sein, denn p ist unverzweigt in $\mathcal{O}_K$. Andererseits gibt $\mathfrak{p} \neq \bar{\mathfrak{p}}$ sofort $\mathfrak{q} \neq \bar{\mathfrak{q}}$.

(2) Aus $N(\mathfrak{p}) = p$ und $p \nmid f$ folgt $\mathrm{ggT}(N(\mathfrak{p}), f) = 1$. Nach (1.5.2) gilt dann für $\alpha \in \mathcal{O}_K$

$$\begin{aligned} &\alpha \equiv a \bmod f\mathcal{O}_K,\ a \in \mathbb{Z},\ \mathrm{ggT}(a, f) = 1 \\ \Leftrightarrow\quad &\alpha \in \mathcal{O},\ \mathrm{ggT}(N(\alpha), f) = 1. \end{aligned}$$

Da $\mathfrak{p}$ die Darstellung $\mathfrak{p} = \alpha\mathcal{O}_K$ besitzt, ist alles klar.

(3) Die Artin-Abbildung gibt uns die Isomorphie

$$I_K(f)/P_{K,\mathbb{Z}}(f) \simeq Gal(H_\mathcal{O}/K).$$

(4) Da $H_\mathcal{O}/K$ abelsch ist, ist $\left(\frac{H_\mathcal{O}/K}{\mathfrak{p}}\right) = \left(\frac{H_\mathcal{O}/K}{\mathfrak{P}}\right)$ für über $\mathfrak{p}$ liegende $\mathcal{O}_{H_\mathcal{O}}$-Primideale $\mathfrak{P}$. Das Kor. 2.2.3 gibt dann

$$\left(\frac{H_\mathcal{O}/K}{\mathfrak{p}}\right) = id \quad \Leftrightarrow \quad \mathfrak{p} \text{ ist vollständig zerlegt in } H_\mathcal{O}.$$

(5) Nach Lemma 2.3.11 ist $H_{\mathcal{O}}/\mathbb{Q}$ galois'sch und folglich gilt

$$\begin{aligned} & e_{\mathfrak{P}|p} = f_{\mathfrak{P}|p} = 1 \text{ für } \textit{ein } \mathcal{O}_{H_{\mathcal{O}}} - \text{Primideal über } p \\ \Longleftrightarrow\ & e_{\mathfrak{P}|p} = f_{\mathfrak{P}|p} = 1 \text{ für } \textit{alle } \mathcal{O}_{H_{\mathcal{O}}} - \text{Primideale über } p. \end{aligned}$$

Da $\mathfrak{p}$ in $H_{\mathcal{O}}$ vollständig zerlegt ist, gilt die Behauptung.

□

2.4 Cebotarevs Dichte-Theorem

Definition 2.4.1. Sei K ein Zahlkörper und P die **Menge der endlichen Primstellen** von K. Für eine Teilmenge $S \subseteq P$ heißt

$$\delta(S) := \lim_{t \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-t}}{-\log(t-1)}$$

Dirichlet-Dichte von S, falls der Grenzwert existiert.

Um Ringklassenkörper explizit konstruieren zu können, benötigen wir Aussagen über die Dirichlet-Dichte aus der analytischen Zahlentheorie, die wir hier ohne Beweis angeben (siehe [3, §8.B]).

Theorem 2.4.2. *Die Dirichlet Dichte besitzt folgende Eigenschaften:*

(i) $\delta(P) = 1$

(ii) *Ist* $S \subseteq T$ *und existieren* $\delta(S)$ *und* $\delta(T)$*, so ist* $\delta(S) \leq \delta(T)$.

(iii) *Existiert* $\delta(S)$*, so ist* $0 \leq \delta(S) \leq 1$.

(iv) *Existieren* $\delta(S)$ *und* $\delta(T)$ *und gilt* $S \cap T = \emptyset$*, so ist* $\delta(S \cup T) = \delta(S) + \delta(T)$.

(v) *Ist* S *endlich, so ist* $\delta(S) = 0$.

(vi) *Existieren* $\delta(S)$ *und* $\delta(T)$ *und stimmen* S *und* T *bis auf endlich viele Ausnahmen überein, so gilt* $\delta(S) = \delta(T)$.

Ist L/K eine (möglicherweise nicht abelsche aber) galois'sche Erweiterung von Zahlkörpern und $\mathfrak{p}$ ein in L unverzweigtes Primideal von K, so geben veschiedene über $\mathfrak{p}$ liegende Primideale $\mathfrak{P}_1$, $\mathfrak{P}_2$ von L eventuell verschiedene Artin-Symbole $((L/K)/\mathfrak{P}_1)$, $((L/K)/\mathfrak{P}_2)$.
Da L/K galois'sch ist, existiert ein $\sigma \in Gal(L:K)$, sodass $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$ gilt. Nach Kor. 2.2.3 ist dann

$$\left(\frac{L/K}{\mathfrak{P}_2}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P}_1)}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}_1}\right) \sigma^{-1}.$$

Das heißt, die Artin Symbole sind konjugiert zueinander. Andererseits ist für jedes Primideal $\mathfrak{P} \subset \mathcal{O}_L$ über $\mathfrak{p}$ und $\sigma \in Gal(L:K)$ dann $\sigma(\mathfrak{P})$ ein $\mathcal{O}_L$-Primideal über $\mathfrak{p}$ und $((L/K)/\sigma(\mathfrak{P})) = \sigma \circ ((L/K)/\mathfrak{P}) \circ \sigma^{-1}$. Die Menge

$$\left\{ \left(\frac{L/K}{\mathfrak{P}}\right) : \ \mathfrak{P} \subset \mathcal{O}_L \text{ ein Primideal über } \mathfrak{p} \right\}$$

ist also eine volle Konjugationsklasse von $Gal(L:K)$. Für ein Primideal $\mathfrak{p} \subset \mathcal{O}_K$ definieren wir deshalb

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \left\{ \left(\frac{L/K}{\mathfrak{P}}\right) : \ \mathfrak{P} \subset \mathcal{O}_L \text{ ein Primideal über } \mathfrak{p} \right\}.$$

Theorem 2.4.3 (Cebotarevs Dichte-Theorem). *Sei L/K eine galois'sche Zahlkörpererweiterung und $<\sigma>$ sei die Konjugationsklasse des Elements $\sigma \in Gal(L:K)$. Die Menge*

$$S := \{\mathfrak{p} \subset \mathcal{O}_K \text{ Primideal} : \mathfrak{p} \text{ ist unverzweigt in } L \text{ und } ((L/K)/\mathfrak{p}) = <\sigma>\}$$

besitzt die Dirichtlet-Dichte

$$\delta(S) = \frac{|<\sigma>|}{|Gal(L:K)|} = \frac{|<\sigma>|}{[L:K]}.$$

Aus den Eigenschaften von δ folgt hier sofort, dass S nicht endlich sein kann.

Korollar 2.4.4. *Sei L/K abelsch und $\mathfrak{m}$ ein Modulus, welcher von allen in L verzweigten Primstellen von K geteilt wird. Ist $\sigma \in Gal(L:K)$ ein beliebiges Element und*

$$S := \{\mathfrak{p} \subset \mathcal{O}_K \text{ Primideal: } \mathfrak{p} \nmid \mathfrak{m},\ ((L/K)/\mathfrak{p}) = \sigma\},$$

so gilt $\delta(S) = \frac{1}{[L:K]}$, und S ist deshalb nicht endlich.

Beweis. Da L/K abelsch ist, ist $<\sigma> = \{\sigma\}$. □

Dies zeigt, dass die Artin-Abbildung $I_K(\mathfrak{m}) \to Gal(L:K)$ surjektiv in einem sehr strengen Sinn ist: Das Urbild eines Elements ist eine unendliche Menge und besitzt positive Dirichlet-Dichte.

Ist L/K galois'sch, so sagt Thm. 2.4.3 angewandt auf $\sigma = id$ aus, dass die Primideale $\mathfrak{p}$ von K mit $((L/K)/\mathfrak{p}) = id$ die Dichte $1/[L:K]$ besitzen. Nach Kor. 2.2.3 gilt aber

$$\left(\frac{L/K}{\mathfrak{p}}\right) = id \quad \Leftrightarrow \quad \mathfrak{p} \text{ ist vollständig zerlegt in } L.$$

Im weiteren Verlauf wird sich zeigen, dass die in L vollständig zerlegten Primideale $\mathfrak{p}$ von K die Erweiterung L/K eindeutig charakterisieren.

Definition 2.4.5. Sind S und T zwei Mengen, so schreiben wir $S \dot{\subseteq} T$, wenn eine endliche Menge Ω existiert, sodass $S \subseteq (T \cup \Omega)$ ist.
Entsprechend ist genau dann $S \doteq T$, wenn $S \dot{\subseteq} T$ und $T \dot{\subseteq} S$ gilt.
Weiter definieren wir

$$S_{L/K} := \{\mathfrak{p} \subset \mathcal{O}_K \text{ Primideal: } \mathfrak{p} \text{ zerfällt vollständig in } L\}.$$

Proposition 2.4.6. *Es seien L, und M endliche Erweiterungen von K.*

(i) Ist M/K galois'sch, so gilt: $L \subseteq M \quad \Leftrightarrow \quad S_{M/K} \dot{\subseteq} S_{L/K}$.

(ii) Ist L/K galois'sch, so gilt: $L \subseteq M \quad \Leftrightarrow \quad \tilde{S}_{M/K} \dot{\subseteq} S_{L/K}$,
wobei

$$\tilde{S}_{M/K} := \left\{\mathfrak{p} \subset \mathcal{O}_K \text{ Primideal: } \begin{array}{l}\mathfrak{p} \text{ ist unverzweigt in } M \text{ und } f_{\mathfrak{P}|\mathfrak{p}} = 1 \\ \text{für ein Primideal } \mathfrak{P} \text{ von } M \text{ über } \mathfrak{p}\end{array}\right\}.$$

Beweis. (ii) Sei zunächst $L \subseteq M$. Weiter sei $\mathfrak{p}$ ein in M unverzweigtes $\mathcal{O}_K$-Primideal und es gelte $f_{\mathfrak{P}|\mathfrak{p}} = 1$ für ein über $\mathfrak{p}$ liegendes Primideal $\mathfrak{P}$ von M.
Bezeichnet $\mathfrak{P}' = \mathfrak{P} \cap L$, so muss auch $f_{\mathfrak{P}'|\mathfrak{p}} = 1$ gelten. Da L/K galois'sch ist, gilt dies dann für jedes über $\mathfrak{p}$ liegende Primideal von L. Außerdem ist $\mathfrak{p}$ in L unverzweigt, denn $\mathfrak{p}$ ist in M unverzweigt.
Folglich ist $\mathfrak{p}$ in L vollständig zerlegt, d. h. $\mathfrak{p}$ ist in $S_{L/K}$.

Gelte nun $\tilde{S}_{M/K} \dot{\subseteq} S_{L/K}$. Bezeichne N die normale Hülle von LM über K. Dann ist N/K galois'sch und $L, M \subseteq N$. Bekanntermaßen gilt

$$L \subseteq M \quad \Leftrightarrow \quad Gal(N:M) \subseteq Gal(N:L).$$

Sei deshalb $\sigma \in Gal(N:M)$. Nach Thm. 2.4.3 existiert ein in N unverzweigtes Primideal $\mathfrak{p}$ von K mit $((N/K)/\mathfrak{p}) = <\sigma>$. Also existiert ein Primideal $\mathfrak{P}$ von N über $\mathfrak{p}$ mit $((N/K)/\mathfrak{P}) = \sigma$.
Wir behaupten $\mathfrak{p} \in \tilde{S}_{M/K}$. Sei $\mathfrak{P}' := \mathfrak{P} \cap \mathcal{O}_M$, so gilt für beliebige $\alpha \in \mathcal{O}_M$

$$\alpha \equiv \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}',$$

denn $\sigma|_M = id$ und $\sigma = ((N/K)/\mathfrak{P})$. Deshalb ist $|\mathcal{O}_M/\mathfrak{P}'| = N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ und folglich $f_{\mathfrak{P}'|\mathfrak{p}} = 1$. D. h. $\mathfrak{p}$ liegt wie behauptet in $\tilde{S}_{M/K}$.
Nach Theorem 2.4.3 existieren unendlich viele solcher Primideale $\mathfrak{p}$ und da $\tilde{S}_{M/K} \subseteq S_{L/K}$ bis auf endlich viele Ausnahmen gilt, können wir $\mathfrak{p}$ in $S_{L/K}$ annehmen. $\mathfrak{p}$ ist also vollständig zerlegt in L und nach Korollar 2.2.3 ist $((L/K)/\mathfrak{p}) = \{id\}$. Im Beweis zu Kor. 2.3.7 wurde gezeigt, dass

$$\left(\frac{N/K}{\mathfrak{P}}\right)\Big|_L = \left(\frac{L/K}{\mathfrak{p}}\right)$$

gilt. Fasser wir zusammen, so ist $\sigma|_L = ((N/K)/\mathfrak{P})|_L = ((L/K)/\mathfrak{p}) = id$, also $\sigma \in Gal(N:L)$.

(i) Sei $L \subseteq M$ und $\mathfrak{p} \in S_{M/K}$. Dann ist $\mathfrak{p}$ auch vollständig zerlegt in L, also in $S_{L/K}$.
Gilt andererseits $S_{M/K} \dot{\subseteq} S_{L/K}$, so sei N die normale Hülle von L über K. Für Primideale $\mathfrak{p}$ von K gilt nach Kor. 2.1.7

$$\mathfrak{p} \text{ ist vollst. zerlegt in L} \quad \Leftrightarrow \quad \mathfrak{p} \text{ ist vollst. zerlegt in N.}$$

Also ist $S_{L/K} = S_{N/K}$. Da M/K galois'sch ist, gilt $\tilde{S}_{M/K} = S_{M/K}$. Die Voraussetzung ist deshalb äquivalent zu $\tilde{S}_{M/K} \dot{\subseteq} S_{N/K}$, und Teil (ii) gibt uns $L \subseteq N \subseteq M$. □

Aus Prop. 2.4.6 (i) folgt unmittelbar das

Theorem 2.4.7. *Seien M und L endliche galois'sche Erweiterungen von K, so gilt:*

(i) $L \subseteq M \quad \Longleftrightarrow \quad S_{M/K} \dot{\subseteq} S_{L/K}.$

(ii) $L = M \quad \Longleftrightarrow \quad S_{M/K} \doteq S_{L/K}.$

Korollar 2.4.8. *Sind $\mathcal{O}_1$ und $\mathcal{O}_2$ Ordnungen eines imaginär-quadratischen Zahlkörpers K mit Ringklassenkörpern L_1 ud L_2, so gilt*

$$\mathcal{O}_1 \subseteq \mathcal{O}_2 \quad \Longrightarrow \quad L_2 \subseteq L_1.$$

Beweis. Es bezeichne f_1 bzw. f_2 den Führer von $\mathcal{O}_1$ bzw. $\mathcal{O}_2$. Einfache Teilbarkeitsüberlegungen zeigen, dass genau dann f_2 ein Teiler von f_1 ist, wenn $\mathcal{O}_1 \subseteq \mathcal{O}_2$ gilt. Nach Thm. 2.4.7 zeigen wir deshalb die äquivalente Behauptung

$$f_2 | f_1 \quad \Longrightarrow \quad S_{L_1/K} \dot{\subseteq} S_{L_2/K}.$$

Sei $\mathfrak{p} \in S_{L_1/K}$ ein beliebiges $\mathcal{O}_K$-Primideal. $\mathfrak{p}$ ist vollständig zerlegt in L_1 und deshalb nach Definition von L_1 teilerfremd zu f_1. Also liegt $\mathfrak{p}$ in $I_K(f_1)$, und aus der Isomorphie $I_K(f_1)/P_{K,\mathbb{Z}}(f_1) \simeq Gal(L_1 : K)$ und Kor. 2.2.3 folgt $\mathfrak{p} \in P_{K,\mathbb{Z}}(f_1)$. Da f_1 von f_2 geteilt wird, liegt $\mathfrak{p}$ sogar in $P_{K,\mathbb{Z}}(f_2)$. Die Isomorphie $I_K(f_2)/P_{K,\mathbb{Z}}(f_2) \simeq Gal(L_2 : K)$ sagt uns dann, dass $\mathfrak{p}$ in L_2 vollständig zerlegt ist, also in $S_{L_2/K}$ liegt. □

3 Komplexe Multiplikation

3.1 Elliptische Funktionen

Definition 3.1.1. Ein **Gitter** ist eine additive Untergruppe L von $\mathbb{C}$, welche von zwei über $\mathbb{R}$ linear unabhängigen Zahlen $\omega_1, \omega_2 \in \mathbb{C}$ erzeugt wird. Wir schreiben $L = [\omega_1, \omega_2]$.

Definition 3.1.2. Eine **elliptische Funktion** von L ist eine Funktion $f(z)$, welche bis auf isolierte Singularitäten auf ganz $\mathbb{C}$ definiert ist, und folgende Bedingungen erfüllt:

- $f(z)$ ist meromorph auf $\mathbb{C}$.
- $f(z+\omega) = f(z)$ für alle $\omega \in L$.

Eine elliptische Funktion ist also eine doppelt-periodische, meromorphe Funktion. Eine entscheidende Rolle spielt die **Weierstrass $\wp$-Funktion** eines Gitters L. Sie ist definiert als

$$\wp(z; L) := \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{z^2} \right).$$

Besteht Klarheit über das zugrunde liegende Gitter, so schreibt man auch kurz $\wp(z)$ anstelle von $\wp(z; L)$. Es gilt das

Theorem 3.1.3. *Sei $\wp(z)$ die Weierstrass $\wp$-Funktion zum Gitter L.*

(i) $\wp(z)$ ist eine elliptische Funktion zum Gitter L. Die Singularitäten von $\wp(z)$ sind doppelte Polstellen in den Gitterpunkten von L.

(ii) $\wp(z)$ erfüllt die Differenzialgleichung

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

wobei g_2, g_3 die folgenden von L abhängigen Konstanten sind:

$$g_2 = g_2(L) := 60 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^4} \qquad \text{und} \qquad g_3 = g_3(L) := 140 \sum_{\omega \in L - \{0\}} \frac{1}{\omega^6}.$$

(iii) $\wp(z)$ genügt dem Additionsgesetz

$$\wp(z+w) \;=\; -\wp(z) - \wp(w) + \frac{1}{4} \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2,$$

für alle $z, w \in \mathbb{C}$ mit $z, w, z+w \notin L$.

Beweis. Siehe [4, Kap. V]. □

Lemma 3.1.4. *Für ein Gitter L und $z, w \notin L$ gilt genau dann $\wp(z) = \wp(w)$, wenn $z \equiv \pm w \bmod L$ ist.*

Beweis. Siehe [4, Satz V.2.10]. □

Die Funktion $\wp(z)$ ist nicht nur ein Beispiel für eine elliptische Funktion, sie ist der Grundbaustein aller elliptischen Funktionen.

Theorem 3.1.5 (Struktursatz)**.** *Die Menge aller elliptischen Funktionen zum Gitter L bildet einen Körper $K(L)$. Jedes $f(z) \in K(L)$ hat die Form*

$$f(z) = R(\wp(z)) + \wp'(z)S(\wp(z)),$$

wobei $R(x)$ und $S(x)$ rationale Funktionen mit komplexen Koeffizienten sind. Ist $f(z)$ eine gerade elliptische Funktion, so hat $f(z)$ die Form $P(\wp(z))$ mit einer rationalen Funktion $P(x) \in \mathbb{C}(x)$.

Beweis. Siehe [4, Thm. V.3.3]. □

Definition 3.1.6. Zwei Gitter L und L' heißen **linear äquivalent**, wenn ein $\lambda \in \mathbb{C} - \{0\}$ mit $L' = \lambda L$ existiert.

Ist $f(z)$ eine elliptische Funktion zum Gitter L, so ist $f(\lambda z)$ eine elliptische Funktion zum Gitter λL. Für die $\wp$-Funktion erhält man $\wp(\lambda z; \lambda L) = \lambda^{-2}\wp(z; L)$. Wir wollen daher Gitter bis auf lineare Äquivalenz näher charakterisieren.

Definition 3.1.7. Sei ein Gitter L mit zugehörigen Konstanten $g_2(L)$, $g_3(L)$ gegeben. Es heißt dann

$$\Delta_L := g_2(L)^3 - 27g_3(L)^2$$

die **Gitterdiskriminante** von L. Die Diskriminante eines Gitters L ist stets von Null verschieden. Weiter wird durch

$$j(L) := 12^3 \frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2} = 1728\frac{g_2(L)^3}{\Delta_L}$$

die **j-Invariante** des Gitters L definiert.

Theorem 3.1.8. *Sind L und L' Gitter in $\mathbb{C}$, so ist genau dann $j(L) = j(L')$, wenn L und L' linear äquivalent sind.*

Beweis. Siehe [4, Thm. VI.2.9]. □

Die j-Invariante wird im späteren Verlauf nicht nur als Gitterinvariante gesehen, sondern auch als Funktion. Wir bezeichnen mit $\mathfrak{H} = \{\tau \in \mathbb{C} : \ Im(\tau) > 0\}$ die obere komplexe Halbebene. Ist $\tau \in \mathfrak{H}$, so erhält man das Gitter $[1, \tau]$. Dadurch motiviert definieren wir

$$j : \mathfrak{H} \to \mathbb{C},\ \tau \mapsto j(\tau) := j([1, \tau]).$$

3.2 Komplexe Multiplikation

Sei $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers K und $\mathfrak{a}$ ein eigentliches gebrochenes $\mathcal{O}$-Ideal. Da $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul von Rang 2 ist, gibt es $\omega_1, \omega_2 \in K$, sodass $\mathfrak{a}$ die Darstellung $\mathfrak{a} = [\omega_1, \omega_2]$ besitzt. Dann ist $\tau = \omega_1/\omega_2 \in K$. Da K ein imaginär-quadratischer Zahlkörper ist, liegt τ nicht in $\mathbb{R}$. ω_1, ω_2 sind also über $\mathbb{R}$ linear unabhängig. M. a. W. ist $\mathfrak{a} = [\omega_1, \omega_2]$ ein Gitter. Sei andererseits $L = [\omega_1, \omega_2] \subset K$ ein Gitter in einem imaginär-quadratischen Zahlkörper K. Da ω_1, ω_2 linear unabhängig über $\mathbb{R}$ sind, ist $\tau := \omega_2/\omega_1 \in \mathbb{C} - \mathbb{R}$ und $L = \omega_1[1, \tau]$. Es muss dann $K = \mathbb{Q}(\tau)$ sein. Mit Lemma 1.3.6 folgt, dass $[1, \tau]$ ein eigentliches gebrochenes Ideal einer Ordnung von K ist. Dann muss das selbe auch für $L = \omega_1[1, \tau]$ gelten.

Definition 3.2.1. Unter einem **zyklischen Untergitter** $L' \subseteq L$ verstehen wir ein Untergitter L'von L, sodass die additive Gruppe L/L' zyklisch ist.

Lemma 3.2.2. *Sei $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers und $\mathfrak{b}$ ein eigentliches gebrochenes $\mathcal{O}$-Ideal.*
Ist $\mathfrak{a}$ ein eigentliches $\mathcal{O}$-Ideal, so ist $\mathfrak{ab}$ ein Untergitter von $\mathfrak{b}$ mit Index $N(\mathfrak{a})$. Es ist $\mathfrak{ab}$ genau dann ein zyklisches Untergitter von $\mathfrak{b}$, wenn $\mathfrak{a}$ ein primitives Ideal ist.

Beweis. Multipliziere wenn nötig mit dem Hauptnenner und nehme o. B. d. A. $\mathfrak{b} \subseteq \mathcal{O}$ an. Es ist

$$0 \to \mathfrak{b}/\mathfrak{ab} \to \mathcal{O}/\mathfrak{ab} \to \mathcal{O}/\mathfrak{b} \to 0$$

eine exakte Sequenz. Deshalb gilt $[\mathfrak{b} : \mathfrak{ab}]N(\mathfrak{b}) = N(\mathfrak{ab})$, also $[\mathfrak{b} : \mathfrak{ab}] = N(\mathfrak{a})$.

Ist $\mathfrak{b}/\mathfrak{ab}$ nicht zyklisch, so existiert nach Lemma A.0.5 ein $\mathfrak{ab} \subseteq \mathfrak{b}' \subseteq \mathfrak{b}$, sodass $\mathfrak{b}'/\mathfrak{ab} \simeq (\mathbb{Z}/d\mathbb{Z})^2$ ist für ein $d > 1$. Folglich ist $d\mathfrak{b}' = \mathfrak{ab}$, also $\mathfrak{a} = d\mathfrak{b}'\mathfrak{b}^{-1}$. Da $\mathfrak{b}' \subseteq \mathfrak{b}$ gilt, ist $\mathfrak{a}' = \mathfrak{b}'\mathfrak{b}^{-1} \subseteq \mathcal{O}$ ein eigentliches $\mathcal{O}$-Ideal. M. a. W. ist $\mathfrak{a} = d\mathfrak{a}'$ nicht primitiv.
Ist $\mathfrak{a}$ nicht primitiv, so existiert ein $d > 1$ und ein eigentliches $\mathcal{O}$-Ideal $\mathfrak{a}'$, so dass $\mathfrak{a} = d\mathfrak{a}'$ gilt. Dann ist

$$\mathfrak{a}'\mathfrak{b}/\mathfrak{ab} = \mathfrak{a}'\mathfrak{b}/d\mathfrak{a}'\mathfrak{b} \simeq (\mathbb{Z}/d\mathbb{Z})^2$$

eine Untergruppe von $\mathfrak{a}/\mathfrak{ab}$, also $\mathfrak{a}/\mathfrak{ab}$ nicht zyklisch nach Lemma A.0.5. □

Korollar 3.2.3. *Sei $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers, $\mathfrak{b}$ ein eigentliches gebrochenes $\mathcal{O}$-Ideal und $\alpha \in \mathcal{O}$.*
$\alpha\mathfrak{b}$ ist ein Untergitter von $\mathfrak{b}$ mit Index $N_{K/\mathbb{Q}}(\alpha)$ und $\alpha\mathfrak{b}$ ist genau dann ein zyklisches Untergitter, wenn α primitiv ist.

Beweis. $\mathcal{O}$-Hauptideale sind stets eigentlich und (α) genau dann ein primitives Ideal, wenn α ein primitives Element ist. □

Die Übertragbarkeit der Begriffe *Gitter* und *eigentliches gebrochenes Ideal* lässt einen ersten Zusammenhang zwischen elliptischen Funktionen und imaginär-quadratischen Zahlkörpern erkennen. Insbesondere können wir aber die j-Invariante $j(\mathfrak{a})$ für Ideale $\mathfrak{a}$ definieren.

Theorem 3.2.4. *Sei L ein Gitter und $\wp(z)$ die $\wp$-Funktion zum Gitter L. Für $\alpha \in \mathbb{C} - \mathbb{Z}$ sind äquivalent:*

(i) $\wp(\alpha z)$ ist eine rationale Funktion in $\wp(z)$.
(ii) $\alpha L \subseteq L$.
(iii) Es existiert eine Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers K, sodass α in $\mathcal{O}$ liegt und L ist linear äquivalent zu einem eigentlichen gebrochenen $\mathcal{O}$-Ideal.

Sind diese Bedingungen erfüllt, so kann $\wp(\alpha z)$ in der Form $\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$ geschrieben werden. Hierbei sind $A(x)$ und $B(x)$ teilerfremde Polynome und es gilt

$$deg(A(x)) = deg(B(x)) + 1 = [L : \alpha L] = N_{K/\mathbb{Q}}(\alpha).$$

Beweis. (i)⇒(ii): Ist $\wp(\alpha z)$ eine rationale Funktion in $\wp(z)$, so gilt

$$B(\wp(z))\wp(\alpha z) = A(\wp(z))$$

für Polynome $A(x), B(x)$. Da $\wp(z)$ und $\wp(\alpha z)$ einen doppelten Pol im Nullpunkt besitzen, muss $deg(A(x)) = deg(B(x)) + 1$ gelten.
Ist $\omega \in L$, so folgt aus obiger Gleichung und der Gradbetrachtung, dass $\wp(\alpha z)$ einen Pol in ω, also

$\wp(z)$ einen Pol in $\alpha\omega$ besitzt. Da die Pole von $\wp(z)$ exakt die Gitterpunkte von L sind, ist $\alpha\omega \in L$. Also gilt $\alpha L \subset L$.
(ii)⇒(i): Ist $\alpha L \subset L$, so sind die Polstellen von $\wp(\alpha z)$ in L enthalten. Da mit $\wp(z)$ auch $\wp(\alpha z)$ eine gerade Funktion ist, lässt sich $\wp(\alpha z)$ nach dem Struktursatz 3.1.5 als rationale Funktion in $\wp(z)$ darstellen.
(ii)⇒(iii): Wir gehen o. B. d. A. von dem (linear äquivalenten) Gitter $L = [1, \tau]$ mit einem $\tau \in \mathbb{C}-\mathbb{R}$ aus. Die Voraussetzung $\alpha L \subset L$ bedeutet dann, dass

$$\alpha = a + b\tau \quad \text{und} \quad \alpha\tau = c + d\tau,$$

für a, b, c, d aus $\mathbb{Z}$ gilt. Dies gibt die Gleichung $b\tau^2 + (a-d)\tau - c = 0$. Da τ nicht in $\mathbb{R}$ liegt, ist $b \neq 0$ und $K = \mathbb{Q}(\tau)$ ein imaginär-quadratischer Zahlkörper. Nach Lemma 1.3.6 ist dann L ein eigentliches gebrochenes Ideal der Ordnung $\mathcal{O} = [1, b\tau]$ von K.
(iii)⇒(ii): Klar.

Gelten die Bedingungen (i)-(iii), so ist $\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$ und für die Grade der Polynome $A(x)$ und $B(x)$ gilt $deg(A(x)) = deg(B(x)) + 1$.

Wir behaupten: $deg(A(x)) = [L : \alpha L]$.

Ist ein $z \in \mathbb{C}$ mit $2z \notin \frac{1}{\alpha}L$ fest gewählt, so betrachten wir das Polynom $F(x) = A(x) - \wp(\alpha z)B(x)$. Dieses besitzt den gleichen Grad wie $A(x)$. Es kann z nach den Lemmata A.0.3 und A.0.4 so gewählt werden, dass $F(x)$ keine mehrfachen Nullstellen besitzt.
Betrachte weiter die additiven Gruppen $L \subseteq \frac{1}{\alpha}L$ und wähle ein Repräsentantensystem der Nebenklassen $\{w_i\}$.
Sind nicht alle $\wp(z + w_i)$ verschieden, so gilt $\wp(z + w_i) = \wp(z + w_j)$ für $i \neq j$. Nach Lemma 3.1.4 ist deshalb $z + w_i \equiv \pm(z + w_j) \bmod L$. Im Fall des positiven Vorzeichens folgt $w_i \equiv w_j \bmod L$, also $w_i + L = w_j + L$ und $i = j$. Im Fall des negativen Vorzeichens folgt $2z \equiv -(w_i + w_j) \bmod L$, also $2z \in L$. Widerspruch! Also müssen alle $\wp(z + w_i)$ verschieden sein.
Da w_i in $\frac{1}{\alpha}L$ liegt, ist $\alpha(z + w_i) \equiv \alpha z \bmod L$. Folglich gilt $\wp(\alpha z) = \wp(\alpha(z + w_i))$ und $z + w_i$ ist eine Nullstelle von $F(x)$. Ist eine beliebige Nullstelle $u \in \mathbb{C}$ von $F(x)$ gegeben, so muss $B(u) \neq 0$ sein, denn $A(x)$ und $B(x)$ sind teilerfremd. Nach Lemma A.0.4 existiert ein $w \in \mathbb{C}$ mit $\wp(w) = u$. Dann ist

$$\wp(\alpha z) = \frac{A(u)}{B(u)} = \frac{A(\wp(w))}{B(\wp(w))} = \wp(\alpha w),$$

also gilt nach Lemma 3.1.4 $\alpha w \equiv \pm\alpha z \bmod L$. Da $\wp(z)$ eine gerade Funktion ist, gelte o. B. d. A. $\alpha w \equiv \alpha z \bmod L$, also $w \equiv z \bmod \frac{1}{\alpha}L$. Es existiert also ein $d \in \frac{1}{\alpha}L$ mit $w = z + d$ und d besitzt eine Darstellung $d = w_i + l$ für ein $l \in L$. Deshalb ist $w \equiv z + w_i \bmod L$ und $u = \wp(w) = \wp(z + w_i)$.
Die Nebenklassen $\{w_i\}$ stehen also in eineindeutiger Beziehung zu Nullstellen von $F(x)$, d. h. ihre Anzahl ist gleich dem Grad von $A(x)$. Mit Kor. 3.2.3 folgt nun die Behauptung

$$deg(A(x)) = [L : \alpha L] = N_{K/\mathbb{Q}}(\alpha).$$

□

Definition und Bemerkung 3.2.5. Besitzt ein Gitter L Multiplikation mit einem Element $\alpha \in \mathbb{C} - \mathbb{Z}$, so mit einer ganzen Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers. Alle Elemente aus $\mathcal{O} - \mathbb{Z}$ liegen dann in $\mathbb{C} - \mathbb{R}$. Wir sagen dann auch, dass L **komplexe Multiplikation** besitzt.

Korollar 3.2.6. *Ist $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers K, so besteht eine eineindeutige Beziehung zwischen den Idealklassen von $C(\mathcal{O})$ und Äquivalenzklassen von Gittern mit $\mathcal{O}$ als Ring der komplexen Multiplikation.*

Beweis. Zunächst ist klar, das jedes eigentliche gebrochene $\mathcal{O}$-Ideal als Gitter aufgefasst werden kann, welches mit $\mathcal{O}$ komplexe Multiplikation besitzt. Ist L ein beliebiges Gitter mit kom-

plexer Multiplikation mit $\mathcal{O}$, so ist dieses nach Thm. 3.2.4 linear äquivalent zu einem eigentlichen gebrochenen $\mathcal{O}$-Ideal. Außerdem sind zwei eigentliche gebrochende $\mathcal{O}$-Ideale $\mathfrak{a}$ und $\mathfrak{a}'$ genau dann als Gitter linear äquivalent, wenn sie in der selben Idealklasse liegen. Gilt nämlich $\mathfrak{a} = [w_1, w_2] \sim \mathfrak{a}' = [v_1, v_2]$ als Gitter mit $w_i, v_i \in K$, so existiert ein $\lambda \in \mathbb{C}^*$ mit $\lambda\mathfrak{a} = \mathfrak{a}'$. Insbesondere gilt dann $\lambda = \lambda\frac{w_1}{w_1} = \frac{rv_1+sv_2}{w_1} \in K$ mit geeigneten $r, s \in \mathbb{Z}$, denn λw_1 liegt in $\mathfrak{a}'$. Das heißt aber, dass $\mathfrak{a} \sim \mathfrak{a}'$ als Ideal ist, also beide in der selben Idealklasse liegen. □

3.3 Die j-Funktion und die Modulgleichung

Wir stellen einige benötigte Kenntnisse aus der Funktionentheorie zusammen.

Definition 3.3.1. In Abschnitt 3.1 wurde die j-Funktion definiert. Ebenso erklärt man die Funktionen

$$\begin{aligned} g_2 :\ \mathfrak{H} \to \mathbb{C}, &\qquad \tau \mapsto g_2([1,\tau]),\\ g_3 :\ \mathfrak{H} \to \mathbb{C}, &\qquad \tau \mapsto g_3([1,\tau]),\\ \Delta :\ \mathfrak{H} \to \mathbb{C}, &\qquad \tau \mapsto \Delta([1,\tau]). \end{aligned}$$

Für ein $\tau \in \mathfrak{H}$ definiert man außerdem die Aktion eines Elementes $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$ auf τ durch $\gamma\tau := \frac{a\tau+b}{c\tau+d}$. Es heißen dann τ und $\gamma\tau$ $SL(2,\mathbb{Z})$-**äquivalent**.

Theorem 3.3.2. *(i) j, g_2, g_3 und Δ sind holomorphe Funktionen auf $\mathfrak{H}$.*
(ii) $j :\ \mathfrak{H} \to \mathbb{C}$ ist surjektiv.

Beweis. Siehe [4, Satz V.8.3] und [3, Thm. 11.2]. □

Korollar 3.3.3. *Sind $g_2, g_3 \in \mathbb{C}$ beliebige Zahlen mit $g_2^3 - 27g_3^2 \neq 0$, so existiert ein Gitter L, so dass $g_2(L) = g_2$ und $g_3(L) = g_3$ gilt.*

Beweis. Siehe [3, Kor. 11.7]. □

Definition 3.3.4. Wir definieren die folgende Untergruppe von $SL(2,\mathbb{Z})$:

$$\Gamma_0(m) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) :\ c \equiv 0 \bmod m \right\}.$$

Außerdem bezeichne

$$C(m) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} :\ ad = m,\ a > 0,\ 0 \leq b < d,\ \mathrm{ggT}(a,b,d) = 1 \right\}.$$

Für das Element $\sigma_0 = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C(m)$ und $\tau \in \mathfrak{H}$ gilt $\sigma_0\tau = m\tau$ und $\Gamma_0(m) = (\sigma_0^{-1}SL(2,\mathbb{Z})\sigma_0) \cap SL(2,\mathbb{Z})$. Weiter besteht die folgende Verbindung zwischen $C(m)$ und $\Gamma_0(m)$.

Lemma 3.3.5. *Für $\sigma \in C(m)$ ist die Menge*

$$(\sigma_0^{-1}SL(2,\mathbb{Z})\sigma) \cap SL(2,\mathbb{Z})$$

eine Rechtsnebenklasse von $\Gamma_0(m)$ in $SL(2,\mathbb{Z})$. Dadurch ist eine eineindeutige Beziehung zwischen $C(m)$ und Rechtsnebenklassen von $\Gamma_0(m)$ in $SL(2,\mathbb{Z})$ gegeben.

Beweis. Siehe [3, Übung 11.8]. □

Ist $\gamma_1, \ldots, \gamma_{|C(m)|}$ ein Vertretersystem der Rechtsnebenklassen von $\Gamma_0(m)$ in $SL(2,\mathbb{Z})$, so definieren wir das Polynom

$$\Phi_m(X,\tau) := \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau)).$$

Es zeigt sich, dass $\Phi_m(X,\tau)$ als Modulfunktion für $SL(2,\mathbb{Z})$ ein Polynom in X und $j(\tau)$ ist und eine Darstellung

$$\Phi_m(X, j(\tau)) = \prod_{\sigma \in C(m)} (X - j(\sigma\tau)) \tag{3.3.1}$$

besitzt (vgl. [3, §11.B]). Die Gleichung $\Phi_m(X,Y) = 0$ heißt **Modulgleichung**.

Theorem 3.3.6. *Sei m eine natürliche Zahl.*

(i) $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$.

(ii) $\Phi_m(X,Y)$ *ist ein irreduzibles Polynom in* X.

(iii) Ist m kein Quadrat, so ist $\Phi_m(X,Y)$ ein Polynom mit Grad > 1 und Leitkoeffizient ± 1.

(iv) Kronecker Kongruenz*: Ist $m = p$ prim, so ist* $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \bmod p\mathbb{Z}[X,Y]$.

Beweis. Siehe [3, Thm 11.18]. □

Lemma 3.3.7. *Ist $\tau \in \mathfrak{H}$, so betrachte das Gitter $L = [1,\tau]$.*

(i) Ist $L' \subseteq [1,\tau]$ ein zyklisches Untergitter mit Index m, so existiert ein eindeutiges $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(m)$, sodass $L' = d[1,\sigma\tau]$ gilt.

(ii) Ist $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(m)$, so ist $d[1,\sigma\tau]$ ein zyklisches Untergitter von L mit Index m.

Beweis. Für ein Untergitter L' von $[1,\tau]$ können wir $L' = [a\tau + b, c\tau + d]$ schreiben. Es ist dann nach Lemma A.0.2 $m = [L : L'] = |ad - bc|$ und nach Lemma A.0.6 gilt

$$L/L' \text{ zyklisch} \quad \Longleftrightarrow \quad ggT(a,b,c,d) = 1.$$

(i) Ist nun $L' \subseteq [1,\tau]$ zyklisch mit Index m, so ist nach Lemma A.0.7 $L' = [d, a\tau + b]$ und d die kleinste natürliche Zahl in L'. Sei o. B. d. A. $a > 0$, also $[L : L'] = det\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = ad = m$. Es ist $[d, a\tau + b] = [d, a\tau + (b + d)]$ und wir können $0 \le b < d$ annehmen. Weiter ist $\mathrm{ggT}(a,b,d) = 1$, also $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(m)$. Die Eindeutigkeit folgt mit Lemma A.0.8.

(ii) Ist andererseits $L' = d[1,\sigma\tau]$ mit $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(m)$, so ist $[L : L'] = |\det(\sigma)| = m$ und da $ggT(a,b,d) = 1$ gilt, ist L/L' zyklisch.

□

Theorem 3.3.8. *Sei m eine natürliche Zahl und $u, v \in \mathbb{C}$. Es ist genau dann $\Phi_m(u,v) = 0$, wenn ein Gitter L und ein zyklisches Untergitter $L' \subseteq L$ mit Index $[L : L'] = m$ existiert, sodass $u = j(L')$ und $v = j(L)$ gilt.*

Beweis. Seien zunächst $u, v \in \mathbb{C}$ mit der Eigenschaft $\Phi_m(u,v) = 0$ beliebig gewählt. Nach Thm. 3.3.2 ist die j-Funktion surjektiv, es existieren also $\tau, \tau' \in \mathfrak{H}$ mit $j(\tau) = v$ und $j(\tau') = u$. Da $\Phi_m(X, j(\tau))$ nach (3.3.1) die Nullstellen $j(\sigma\tau)$ für $\sigma \in C(m)$ besitzt, existiert ein $\sigma_0 \in C(m)$ mit $\sigma_0\tau = \tau'$. Setzen wir $L = [1,\tau]$ und $L' = d[1,\sigma\tau]$, so ist $j(L) = u$ und $j(L') = v$ und mit Lemma 3.3.7 folgt die Behauptung.

Ist andererseits $L' \subseteq L$ ein zyklisches Untergitter mit Index m, o. B. d. A. $L = [1, \tau]$, so existiert nach Lemma 3.3.7 ein $\sigma_0 \in C(m)$ mit $L' = d[1, \sigma\tau]$. Da $j(L) = j(\tau)$ und $j(L') = j(\sigma_0\tau)$ ist, folgt aus der Darstellung (3.3.1) die Behauptung. □

3.4 Komplexe Multiplikation und Ringklassenkörper

Theorem 3.4.1. *Sei $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers K und $\mathfrak{a}$ ein beliebiges eigentliches gebrochenes $\mathcal{O}$-Ideal.*
Die j-Invariante $j(\mathfrak{a})$ ist algebraisch ganz und $K(j(\mathfrak{a}))$ ist der Ringklassenkörper von $\mathcal{O}$.

Beweis. Sei $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers K und $\mathfrak{a}$ ein eigentliches gebrochenes $\mathcal{O}$-Ideal.
Ist $\alpha \in \mathcal{O}$ ein primitives Element, so ist nach Kor. 3.2.3 $\alpha\mathfrak{a}$ ein zyklisches Untergitter von $\mathfrak{a}$ mit Index $m = N_{K/\mathbb{Q}}(\alpha)$. Nach Thm. 3.3.8 ist dann

$$0 = \Phi_m(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = \Phi_m(j(\mathfrak{a}), j(\mathfrak{a})),$$

da $j(\alpha\mathfrak{a}) = j(\mathfrak{a})$ nach Thm. 3.1.8 gilt. Damit ist $j(\mathfrak{a})$ eine Nullstelle des Polynoms $\Phi_m(X, X)$ und insbesondere $j(\mathfrak{a})$ eine algebraische Zahl. Es ist $\Phi_m(X, X) \in \mathbb{Z}[X]$ nach Thm. 3.3.6. Ist $\alpha \in \mathcal{O}$ primitiv und $N_{K/\mathbb{Q}}(\alpha)$ kein Quadrat, so folgt erneut mit Thm. 3.3.6, dass der Leitkoeffizient von $\Phi_m(X, X)$ gleich ± 1 ist. Damit ist $j(\mathfrak{a})$ eine algebraisch ganze Zahl. Gesucht wird also ein primitives $\alpha \in \mathcal{O}$, sodass $N_{K/\mathbb{Q}}(\alpha)$ kein Quadrat ist.
Bezeichnet f den Führer von $\mathcal{O}$, ist also $\mathcal{O} = [1, fw_K]$ gemäß Abschnitt 1.3, so setze $\alpha := fw_K$. Wäre α nicht primitiv, besäße also eine Darstellung $\alpha = d\alpha'$ mit $d > 1$ und $\alpha' \in \mathcal{O}$, so gäbe es $x, y \in \mathbb{Z}$ mit $\alpha' = x + y\alpha = x + yd\alpha'$ im Widerspruch zu $d > 1$. Wir berechnen die Norm von α:

$$N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(fw_K) = f^2 \frac{d_K(d_K - 1)}{4}.$$

Aus der Definition von d_K folgt nun, dass $N_{K/\mathbb{Q}}(\alpha)$ kein Quadrat sein kann. Also ist $j(\mathfrak{a})$ eine algebraisch ganze Zahl.

Bleibt zu zeigen, dass $j(\mathfrak{a})$ den Ringklassenkörper $H_\mathcal{O}$ von $\mathcal{O}$ erzeugt. Sei D die Diskriminante von $\mathcal{O}$. Wie in Abschnitt 2.4 bezeichne $S_{H_\mathcal{O}/\mathbb{Q}}$ die Menge

$$S_{H_\mathcal{O}/\mathbb{Q}} = \{p \in \mathbb{Z} \text{ prim} : \ p \text{ ist vollst. zerlegt in } H_\mathcal{O}\}.$$

Wir behaupten

$$S_{H_\mathcal{O}/\mathbb{Q}} \doteq \{p \in \mathbb{Z} \text{ prim} : \ p = N_{K/\mathbb{Q}}(\alpha) \text{ für ein } \alpha \in \mathcal{O}\}. \tag{3.4.1}$$

Ist $D \equiv 0 \bmod 4$, so gilt wegen $D = f^2 d_K$ dann $4|f^2$ oder $4|d_K$. In beiden Fällen erhält man die Darstellung $\mathcal{O} = [1, fw_K] = \mathbb{Z}[\sqrt{-n}]$ mit $-n = (f^2/4)d_K \in \mathbb{Z}$.
Für $\alpha = x + y\sqrt{-n} \in \mathcal{O}$ ist dann $N_{K/\mathbb{Q}}(\alpha) = x^2 + ny^2$. In Thm 2.3.12 wurde gezeigt, dass bis auf endlich viele Ausnahmen für prime $p \in \mathbb{Z}$ gilt:

$$p \text{ ist vollständig zerlegt in } H_\mathcal{O} \quad \Longleftrightarrow \quad p = x^2 + ny^2 \text{ mit } x, y \in \mathbb{Z}.$$

Ist hingegen $D \equiv 1 \bmod 4$, so gilt wegen $D = f^2 d_K$ auch $d_K \equiv 1 \bmod 4$ und wir erhalten die Darstellung $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Für $\alpha = x + y\frac{1+\sqrt{D}}{2} \in \mathcal{O}$ gilt dann $N_{K/\mathbb{Q}}(\alpha) = x^2 + xy + y^2(\frac{1-D}{4})$ und in Thm. 2.3.12 wurde gezeigt, dass bis auf endlich viele Ausnahmen gilt:

$$p \text{ ist vollständig zerlegt in } H_\mathcal{O} \quad \Longleftrightarrow \quad p = x^2 + xy + y^2(\frac{1-D}{4}) \text{ mit } x, y \in \mathbb{Z}.$$

Damit gilt die Behauptung (3.4.1).

Wir setzen $M := K(j(\mathfrak{a}))$. Da $H_{\mathcal{O}}$ nach Lemma 2.3.11 galois'sch über $\mathbb{Q}$ ist, gilt nach Proposition 2.4.6

$$M \subseteq H_{\mathcal{O}} \qquad \Longleftrightarrow \qquad S_{H_{\mathcal{O}}/\mathbb{Q}} \dot{\subseteq} S_{M/\mathbb{Q}},$$

und wir beweisen die rechte Seite. Sei also $p \in S_{H_{\mathcal{O}}/\mathbb{Q}}$. Da nur endlich viele Primzahlen in M verzweigt sind, können wir p als in M unverzweigt voraussetzen. Nach (3.4.1) ist $p = N_{K/\mathbb{Q}}(\alpha)$ für ein $\alpha \in \mathcal{O}$. Dann ist $\alpha\mathfrak{a} \subseteq \mathfrak{a}$ ein Untergitter mit Index $N_{K/\mathbb{Q}}(\alpha) = p$, also zyklisch. Folglich ist

$$0 = \Phi_p(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = \Phi_p(j(\mathfrak{a}), j(\mathfrak{a}))$$

und die Kronecker Kongruenz (Thm. 3.3.6) gibt

$$0 = \Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) = -(j(\mathfrak{a})^p - j(\mathfrak{a}))^2 + p\,\beta, \qquad \text{für ein } \beta \in \mathcal{O}_M,$$

denn $\mathbb{Z}[j(\mathfrak{a})]$ liegt in $\mathcal{O}_M$, da $j(\mathfrak{a})$ algebraisch ganz ist. Ist weiter $\mathfrak{P}$ ein Primideal von $\mathcal{O}_M$ über p, so ist

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{P}. \tag{3.4.2}$$

Wir behaupten:

(i) $\mathcal{O}_K[j(\mathfrak{a})] \subseteq \mathcal{O}_M$ hat endlichen Index.

(ii) Gilt $p \nmid [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$, so folgt $\alpha^p \equiv \alpha \bmod \mathfrak{P}$ für alle $\alpha \in \mathcal{O}_M$.

Dazu:

(i) Es ist $\mathcal{O}_M$ ein freier $\mathbb{Z}$-Modul von Rang $[M : \mathbb{Q}]$. $j(\mathfrak{a})$ ist algebraisch ganz. Das Minimalpolynom $f(X)$ von $j(\mathfrak{a})$ liegt also in $\mathbb{Z}[X]$, besitzt den Grad $[M : \mathbb{Q}]$ und $\mathbb{Z}[j(\mathfrak{a})]$ ist dann offensichtlich ein freier $\mathbb{Z}$-Modul von Rang $[M : \mathbb{Q}]$. Da $\mathbb{Z}[j(\mathfrak{a})] \subseteq \mathcal{O}_K[j(\mathfrak{a})] \subseteq \mathcal{O}_M$ ist, muss auch $\mathcal{O}_K[j(\mathfrak{a})]$ ein freier $\mathbb{Z}$-Modul von Rang $[M : \mathbb{Q}]$ sein. Es folgt die Behauptung.

(ii) Da p in $H_{\mathcal{O}}$ vollständig zerlegt ist, ist p auch in K vollständig zerlegt. Es ist $p \in \mathfrak{p} \subset \mathfrak{P}$ für ein $\mathcal{O}_K$-Primideal $\mathfrak{p}$ mit $N(\mathfrak{p}) = p$. Für alle $\alpha \in \mathcal{O}_K$ gilt dann $\alpha^p \equiv \alpha \bmod \mathfrak{p}$, also erst recht $\alpha^p \equiv \alpha \bmod \mathfrak{P}$. Aus der Kongruenz (3.4.2) folgt dann auch

$$\forall \alpha \in \mathcal{O}_K[j(\mathfrak{a})] : \ \alpha^p \equiv \alpha \bmod \mathfrak{P}.$$

Setzen wir $l = [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$, so gilt $l^p \equiv l \bmod p$ und auch $l^p \equiv l \bmod \mathfrak{P}$. Ist $\alpha \in \mathcal{O}_M$ beliebig gewählt, so folgt wegen $l\mathcal{O}_M \subseteq \mathcal{O}_K[j(\mathfrak{a})]$

$$l\alpha^p \equiv (l\alpha)^p \equiv l\alpha \bmod \mathfrak{P}.$$

Da $p \nmid l$ gilt, also $ggT(l, N(\mathfrak{P})) = 1$ ist, induziert die Multiplikation mit l einen Automorphismus von $\mathcal{O}_M/\mathfrak{P}$. Aus der Injektivität folgt dann wie behauptet

$$\alpha^p \equiv \alpha \bmod \mathfrak{P} \qquad \text{für alle } \alpha \in \mathcal{O}_M.$$

Da es auf endlich viele Primzahlen nicht ankommt, können wir $p \nmid [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$ annehmen. Aus (ii) folgt $|\mathcal{O}_M/\mathfrak{P}| = p$, also $f_{\mathfrak{P}|p} = 1$. Da $\mathfrak{P}$ als beliebiges $\mathcal{O}_M$-Primideal über p gewählt wurde, ist p vollständig zerlegt in M. Also gilt $S_{H_{\mathcal{O}}/\mathbb{Q}} \dot{\subseteq} S_{M/\mathbb{Q}}$, mit anderen Worten ist $M \subseteq H_{\mathcal{O}}$.

Diese Inklusion zeigt, dass der Ringklassenkörper $H_{\mathcal{O}}$ die j-Invariante eines jeden eigentlichen gebrochenen $\mathcal{O}$-Ideals enthält. Ist $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ ein vollständiges Vertretersystem von $C(\mathcal{O})$, so entspricht $j(\mathfrak{a})$ einem der Werte $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$. Nach Thm. 3.1.8 sind alle $j(\mathfrak{a}_i)$ verschieden. Deshalb ist

$$\Delta = \prod_{i<j} (j(\mathfrak{a}_i) - j(\mathfrak{a}_j)) \tag{3.4.3}$$

ein von Null verschiedenes Element aus $\mathcal{O}$.

Um die andere Inklusion $H_{\mathcal{O}} \subseteq M$ zu beweisen, benutzen wir Prop. 2.4.6:

$$H_{\mathcal{O}} \subseteq M \qquad \Longleftrightarrow \qquad \tilde{S}_{M/\mathbb{Q}} \dot{\subseteq} S_{H_{\mathcal{O}}/\mathbb{Q}}.$$

Sei $p \in \tilde{S}_{M/\mathbb{Q}}$ beliebig gewählt, so ist p unverzweigt in M und es existiert ein Primideal $\mathfrak{P} \subset \mathcal{O}_M$ mit $f_{\mathfrak{P}|p} = 1$. Deshalb ist p in K vollständig zerlegt und es existiert ein $\mathcal{O}_K$-Primideal $\mathfrak{p}$ über p mit Norm $N(\mathfrak{p}) = p$. Wir können p als teilerfremd zum Führer f voraussetzen (dies schließt nur endlich viele Primzahlen aus). Nach Prop. 1.5.4 ist dann $\mathfrak{p} \cap \mathcal{O}$ ein Primideal von $\mathcal{O}$ mit gleicher Norm $N(\mathfrak{p} \cap \mathcal{O}) = p$.
Wir suchen ein $\alpha \in \mathcal{O}$ sodass $\mathfrak{p} \cap \mathcal{O} = \alpha\mathcal{O}$ ein Hauptideal ist, also auch $N_{K/\mathbb{Q}}(\alpha) = p$ gilt. Infolge der Mengengleichheit (3.4.1) muss dann p in $S_{L/\mathbb{Q}}$ liegen.
Sei weiter vorausgesetzt, dass p nicht Δ teilt. Setzen wir $\mathfrak{a}' := (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$, so ist wegen $N(\mathfrak{p} \cap \mathcal{O}) = p$ nach Lemma 3.2.2 $\mathfrak{a}'$ ein zyklisches Untergitter von $\mathfrak{a}$. Folglich gilt $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$ und die Kronecker Kongruenz gibt

$$0 = \Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = (j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) + pQ(j(\mathfrak{a}'), j(\mathfrak{a}))$$

für ein Polynom $Q(X, Y) \in \mathbb{Z}[X, Y]$. Da $M \subseteq H_{\mathcal{O}}$ gilt, wählen wir ein $\mathcal{O}_{H_{\mathcal{O}}}$-Primideal $\tilde{\mathfrak{P}} \supseteq \mathfrak{P}$. Aus $j(\mathfrak{a}'), j(\mathfrak{a}) \in \mathcal{O}_M$ und $p \in \tilde{\mathfrak{P}}$ folgt $pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in \tilde{\mathfrak{P}}$ und es gilt

$$j(\mathfrak{a}')^p \equiv j(\mathfrak{a}) \bmod \tilde{\mathfrak{P}} \qquad \text{oder} \qquad j(\mathfrak{a})^p \equiv j(\mathfrak{a}') \bmod \tilde{\mathfrak{P}}. \tag{3.4.4}$$

Wir wissen außerdem $f_{\mathfrak{P}|p} = 1$. Deshalb ist $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{P}$ und wegen $\mathfrak{P} \subseteq \tilde{\mathfrak{P}}$ gilt dann

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \tilde{\mathfrak{P}}. \tag{3.4.5}$$

Aus (3.4.4) und (3.4.5) folgt nun

$$j(\mathfrak{a}) \equiv j(\mathfrak{a}') \bmod \tilde{\mathfrak{P}}.$$

Lägen $\mathfrak{a}$ und $\mathfrak{a}'$ in verschiedenen Idealklassen von $C(\mathcal{O})$, so wäre $j(\mathfrak{a}) - j(\mathfrak{a}')$ ein Faktor von Δ. Da p und Δ teilerfremd sind, würde gelten

$$\mathcal{O}_{H_{\mathcal{O}}} = p\mathcal{O}_{H_{\mathcal{O}}} + \Delta\mathcal{O}_{H_{\mathcal{O}}} \subseteq \tilde{\mathfrak{P}} + (j(\mathfrak{a}) - j(\mathfrak{a}'))\mathcal{O}_{H_{\mathcal{O}}} = \tilde{\mathfrak{P}}.$$

Widerspruch! Also liegen $\mathfrak{a}$ und $\mathfrak{a}'$ in der gleichen Idealklasse von $C(\mathcal{O})$ und $\mathfrak{p} \cap \mathcal{O}$ muss ein Hauptideal sein. Mit (3.4.1) liegt dann $p \in S_{H_{\mathcal{O}}/\mathbb{Q}}$. Es gilt also $\tilde{S}_{M/\mathbb{Q}} \subseteq S_{H_{\mathcal{O}}/\mathbb{Q}}$ und damit $M = H_{\mathcal{O}}$. □

Korollar 3.4.2. *Ist K ein imaginär-quadratischer Zahlkörper, so ist $K(j(\mathcal{O}_K))$ der Hilbert Klassenkörper.*

Lemma 3.4.3. *Ist $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers K, $[\mathfrak{a}]$ eine Idealklasse in $C(\mathcal{O})$ und $\mathfrak{a} \in [\mathfrak{a}]$ ein Vertreter, so gilt:*

$$j(\mathfrak{a}) \in \mathbb{R} \qquad \Longleftrightarrow \qquad [\mathfrak{a}]^2 = [\mathcal{O}] \in C(\mathcal{O}).$$

Beweis. Bezeichne $\overline{\mathfrak{a}}$ das komplex-konjugierte Ideal. Man rechnet nach, dass $j(\overline{\mathfrak{a}}) = \overline{j(\mathfrak{a})}$ ist. Nach Lemma 1.3.9 ist $[\mathfrak{a}][\overline{\mathfrak{a}}] = [\mathfrak{a}\overline{\mathfrak{a}}] = [N(\mathfrak{a})\mathcal{O}] = [\mathcal{O}]$. Mit Thm. 3.1.8 zusammen gilt deshalb

$$j(\mathfrak{a}) \in \mathbb{R} \;\Leftrightarrow\; j(\mathfrak{a}) = j(\overline{\mathfrak{a}}) \;\Leftrightarrow\; \mathfrak{a} \sim \overline{\mathfrak{a}} \;\Leftrightarrow\; [\mathfrak{a}] = [\overline{\mathfrak{a}}] \;\Leftrightarrow\; [\mathfrak{a}]^2 = [\mathfrak{a}][\overline{\mathfrak{a}}] = [\mathcal{O}].$$

□

Proposition 3.4.4. *Sei $\mathcal{O}$ eine Ordnung eines imaginär-quadratischen Zahlkörpers K und $\mathfrak{a}_i$, $i = 1, \ldots, h$, ein vollständiges Vertretersystem der Idealklassen von $C(\mathcal{O})$. Das Minimalpolynom von $j(\mathfrak{a}_i)$ ist*

$$H_{\mathcal{O}}(X) := \prod_{i=1}^{h} (X - j(\mathfrak{a}_i)) \in \mathbb{Z}[X].$$

*Die Gleichung $H_{\mathcal{O}}(X) = 0$ heißt die **Klassengleichung von** $\mathcal{O}$.*

Beweis. Nach Theorem 3.4.1 ist $K(j(\mathcal{O}))$ der Ringklassenkörper von $\mathcal{O}$. Deshalb ist $[K(j(\mathcal{O})) : K] = h$, und da $j(\mathcal{O})$ reell ist, gilt auch $[\mathbb{Q}(j(\mathcal{O})) : \mathbb{Q}] = h$. Das Minimalpolynom von $j(\mathcal{O})$ über $\mathbb{Q}$ besitzt also Grad h. Sei α eine Nullstelle des Minimalpolynoms und σ ein Automorphismus von $\mathbb{C}$, sodass $\sigma(j(\mathcal{O})) = \alpha$ gilt.
Sei $\wp(z; g_2, g_3)$ die $\wp$-Funktion zum Gitter $\mathcal{O}$ mit von $\mathcal{O}$ abhängigen Konstanten g_2, g_3. Diese besitzt nach Thm. 3.2.4 komplexe Multiplikation mit jedem $\gamma \in \mathcal{O}$ und $\wp(\gamma z; g_2, g_3)$ ist eine rationale Funktion in $\wp(z; g_2, g_3)$, also

$$\wp(\gamma z; g_2, g_3) = \frac{A(\wp(z; g_2, g_3))}{B(\wp(z; g_2, g_3))},$$

für teilerfremde Polynome $A(X)$, $B(X) \in \mathbb{C}[X]$. Wenden wir σ auf diese Gleichung an, so erhalten wir

$$\wp(\sigma(\gamma) z; \sigma(g_2), \sigma(g_3)) = \frac{A^\sigma(\wp(z; \sigma(g_2), \sigma(g_3)))}{B^\sigma(\wp(z; \sigma(g_2), \sigma(g_3))},$$

wobei $A^\sigma(X)$ bzw. $B^\sigma(X)$ aus $A(X)$ bzw. $B(X)$ durch Anwenden von σ auf die Koeffizienten hervorgeht. Aus $g_2^3 - 27g_3^2 \neq 0$ folgt $\sigma(g_2)^3 - 27\sigma(g_3)^2 \neq 0$ und nach Kor. 3.3.3 existiert ein Gitter $\mathfrak{a}$ mit $\sigma(g_2) = g_2(\mathfrak{a})$, $\sigma(g_3) = g_3(\mathfrak{a})$ und $j(\mathfrak{a}) = \sigma(j(\mathcal{O}))$. Das heißt, $\wp(z; \sigma(g_2), \sigma(g_3)) = \wp(z; g_2(\mathfrak{a}), g_3(\mathfrak{a}))$ ist die $\wp$-Funktion zum Gitter $\mathfrak{a}$. Diese besitzt komplexe Multiplikation mit dem Element $\sigma(\gamma) \in \mathbb{C} - \mathbb{Z}$, also mit einer ganzen Ordnung $\mathcal{O}'$. Nach Thm. 3.2.4 können wir o. B. d. A. $\mathfrak{a}$ als ein eigentliches gebrochenes $\mathcal{O}$-Ideal annehmen. Da $\gamma \in \mathcal{O}$ beliebig war, folgt $\sigma(\mathcal{O}) \subseteq \mathcal{O}'$. Es ist $\sigma|_K = id$ oder $\sigma|_K = \tau$, die komplexe Konjugation. Deshalb ist $\sigma(\mathcal{O}) = \mathcal{O}$ und wir erhalten $\mathcal{O} \subseteq \mathcal{O}'$. Die gleiche Argumentation mit $\wp(z; g_2(\mathfrak{a}), g_3(\mathfrak{a}))$ und σ^{-1} liefert $\mathcal{O}' \subseteq \mathcal{O}$ und wir schließen $\mathcal{O} = \mathcal{O}'$.
Zusammenfassend finden wir ein eigentliches gebrochenes $\mathcal{O}$-Ideal $\mathfrak{a}$ mit $\sigma(j(\mathcal{O})) = \alpha = j(\mathfrak{a})$. Jede Nullstelle des Minimalpolynoms ist also Nullstelle von $H_{\mathcal{O}}(X)$ und da beide Polynome normiert und von gleichem Grad sind, folgt Gleichheit. □

Beispiel 3.4.5. Wir wollen die Klassenpolynome $H_{d_K}(X)$ der Maximalordnungen aus Bsp. 1.4.12 bestimmen.
(i) Die Klassengruppe von $K = \mathbb{Q}(\sqrt{-1})$ ist $\mathcal{C}(\mathcal{O}_K) = \{[1, i]\}$. Aus $g_3([1, i]) = g_3(i[1, i]) = i^{-6} g_3([1, i]) = -g_3([1, i])$ folgt $g_3([1, i]) = 0$ und deshalb nach Definition $j([1, i]) = 1728$. Das Klassenpolynom ist

$$H_{-4}(X) = X - 1728.$$

(ii) Die Klassengruppe von $K = \mathbb{Q}(\sqrt{-3})$ ist $\mathcal{C}(\mathcal{O}_K) = \{[1, \omega]\}$ mit $\omega = \frac{-1+\sqrt{-3}}{2}$. Aus $g_2([1, \omega]) = g_2(\omega[1, \omega]) = \omega^{-4} g_2([1, \omega]) = \omega^2 g_2([1, \omega])$ folgt $g_2([1, \omega]) = 0$ und deshalb nach Definition $j([1, \omega]) = 0$. Das Klassenpolynom ist hier

$$H_{-3}(X) = X.$$

(iii) Die Klassengruppe von $K = \mathbb{Q}(\sqrt{-31})$ ist

$$\begin{aligned} \mathcal{C}(\mathcal{O}_K) &= \left\{[2, (-1 + \sqrt{-31})/2],\ [2, (1 + \sqrt{-31})/2],\ [1, (-1 + \sqrt{-31})/2]\right\} \\ &= \left\{[1, (-1 + \sqrt{-31})/4],\ [1, (1 + \sqrt{-31})/4],\ [1, (-1 + \sqrt{-31})/2]\right\}. \end{aligned}$$

Wir bestimmen die Werte der j-Funktion mit PARI:

$$\begin{array}{rcrcl} a_1 & := & j((-1 + \sqrt{-31})/4) & \sim & 743,455778122071940 1637 + 6253,062846903285088550 \cdot i \\ a_2 & := & j((1 + \sqrt{-31})/4) & \sim & 743,455778122071940 1637 - 6253,062846903285088550 \cdot i \\ a_3 & := & j((-1 + \sqrt{-31})/2) & \sim & -39492793,91155624414388 + 0 \cdot i \end{array}$$

Das Klassenpolynom ist dann

$$\begin{aligned} H_{-31}(X) &= X^3 - (a_1 + a_2 + a_3)X^2 + (a_1 a_2 + a_1 a_3 + a_2 a_3)X - a_1 a_2 a_3 \\ &= X^3 + 39491307 \cdot X^2 - 58682638134 \cdot X + 1566028350940383 \\ &= X^3 + 3^3 \cdot 53 \cdot 9199 \cdot X^2 - 2 \cdot 3^7 \cdot 29 \cdot 462629 \cdot X + (3^3 \cdot 11 \cdot 17 \cdot 23)^3. \end{aligned}$$

(iv) PARI gibt uns für $K = \mathbb{Q}(\sqrt{-51})$ das Klassenpolynom

$$\begin{aligned} H_{-51}(X) &= X^2 + 5541101568 \cdot X + 6262062317568 \\ &= X^2 + 2^{15} \cdot 3^3 \cdot 6263 \cdot X + (2^{11} \cdot 3^2)^3. \end{aligned}$$

Bemerkung 3.4.6. Ist $\mathfrak{a} \subseteq \mathcal{O}$ ein eigentliches gebrochenes Ideal der Ordnung $\mathcal{O}$ eines imaginärquadratischen Zahlkörpers K, so gilt

$$j(\mathfrak{a}) = 0 \iff \mathcal{O} = \mathbb{Z}[\omega],\ K = \mathbb{Q}(\sqrt{-3}).$$

Ist nämlich $j(\mathfrak{a}) = 0$, so ist nach Thm. 3.1.8 und Bsp. 3.4.5.(ii) $\mathfrak{a} = \lambda[1, \omega]$ für ein $\lambda \in \mathbb{C}$. Es gilt dann $\omega\mathfrak{a} = \omega\lambda[1, \omega] = \lambda[1, \omega] = \mathfrak{a}$. Deshalb liegt $\mathbb{Z}[\omega]$ in $\mathcal{O}$. Da $\mathbb{Z}[\omega]$ die Maximalordnung von $K = \mathbb{Q}(\sqrt{-3})$ ist, folgt $\mathcal{O} = \mathbb{Z}[\omega]$ und $K = \mathbb{Q}(\sqrt{-3})$. Ist andererseits $\mathcal{O} = \mathbb{Z}[\omega]$, so muss $\mathfrak{a}$ linear äquivalent zu $[1, \omega]$ sein, denn $\mathcal{O}$ ist ein Hauptidealring. Es folgt $j(\mathfrak{a}) = 0$ mit Thm. 3.1.8 und Bsp. 3.4.5.(ii).
Analog folgert man für ein eigentliches gebrochenes Ideal $\mathfrak{a} \subseteq \mathcal{O}$ der Ordnung $\mathcal{O}$ eines imaginärquadratischen Zahlkörpers K die Äquivalenz

$$j(\mathfrak{a}) = 1728 \iff \mathcal{O} = \mathbb{Z}[i],\ K = \mathbb{Q}(\sqrt{-1}).$$

4 Elliptische Kurven

Sei k ein Körper der Charakteristik $\neq 2, 3$, $L \supseteq k$ ein Erweiterungskörper und $\mathbb{P}^2(L)$ die projektive Ebene über L.

Definition 4.0.7. Eine **elliptische Kurve** E **über** k ist durch ein Paar $(a, b) \in k^2$ mit $\Delta_E := -16(4a^3 + 27b^2) \neq 0$ gegeben. Die Menge der L-rationalen Punkte auf E ist

$$E(L) := \{(X : Y : Z) \in \mathbb{P}^2(L) : Y^2Z = X^3 + aXZ^2 + bZ^3\}.$$

Es existiert genau ein Punkt auf E mit $Z = 0$, nämlich $(0 : 1 : 0)$. Er heißt der **Fernpunkt** von E und wird mit O_E bezeichnet.
Δ_E heißt **Diskriminante** von E und der Wert $j(E) := 1728 \cdot 4a^3/(4a^3+27b^2)$ heißt die **j-Invariante** von E.

Wechselt man mittels der Transformation $x = X/Z$, $y = Y/Z$ zu affinen Koordinaten, so ist die elliptische Kurve durch die Gleichung $y^2 = x^3 + ax + b$ gegeben. Die L-rationalen Punkte auf E sind dann

$$E(L) = \{(x, y) \in L^2 : \ y^2 = x^3 + ax + b\} \cup \{O_E\}.$$

Die definierende Gleichung von E heißt **kurze Weierstrass Normalform**.

Bemerkung. Auch über Körpern der Charakteristik 2 und 3 können elliptische Kurven definiert werden, allerdings sind dort die definierenden Gleichungen, Definition der j-Invariante, etc. komplizierter (vgl. [13]).

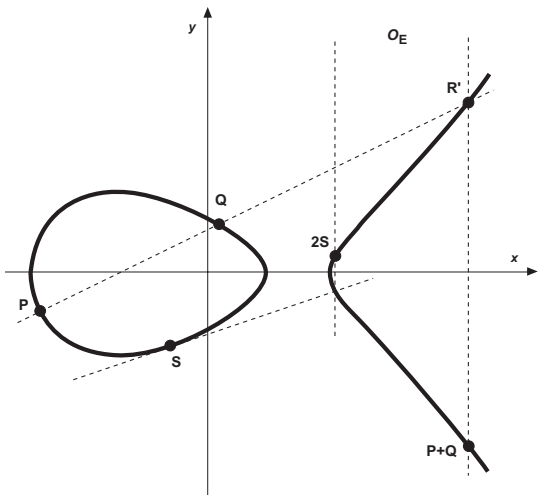
Proposition 4.0.8. *Ist k ein Körper der Charakteristik $\neq 2, 3$, so existiert zu jedem Element $j_0 \in k$ eine elliptische Kurve E über k mit j-Invariante $j(E) = j_0$.*

Beweis. Ist $j_0 = 0$, so ist $y^2 = x^3+1$ eine elliptische Kurve mit j-Invariante 0, denn $\Delta = -16 \cdot 27 \neq 0$. Ist $j_0 = 1728$, so ist $y^2 = x^3 + x$ eine elliptische Kurve mit j-Invariante 1728, denn $\Delta = -16 \cdot 4 \neq 0$. Sei nun $j_0 \neq 0, 1728$. Setzen wir $c := j_0/(1728 - j_0)$, so ist $y^2 = x^3 + 3cx + 2c$ eine elliptische Kurve. Es ist $\Delta = -16(4 \cdot 27c^3 + 27 \cdot 4c^2) = -1728c^2(c + 1)$. Da $char(k) \neq 2, 3$ gilt, ist $1728 \neq 0$ und damit $c \neq -1$. Außerdem ist wegen $j_0 \neq 0$ auch $c \neq 0$. Folglich gilt $\Delta \neq 0$. Die j-Invariante dieser Kurve ist j_0. □

Bekanntermaßen besitzt die Menge der L-rationalen Punkte von E eine abelsche Gruppenstruktur, die sich einfach geometrisch erklären lässt.

Sind P und Q zwei Punkte auf der elliptischen Kurve E, so zeigt sich, dass die Gerade duch P und Q die Kurve in genau einem weiteren Punkt R' schneidet (im Falle $P = Q$ wählt man die Tangente durch P). Wir wiederholen diesen Prozess ausgehend von den Punkten R' und O_E, finden den Punkt R und setzen $P + Q = R$.

Auf dem Bild sind zwei Beispiele für die Addition von $\mathbb{R}$-rationalen Punkten auf der elliptischen Kurve $y^2 = x^3 - 45x + 90$ zu sehen.



4.1 Endomorphismen

Definition 4.1.1. Sei E eine elliptische Kurve über einem beliebigen Körper K. Unter einem **Endomorphismus von E über K** verstehen wir einen durch K-rationale Funktionen über dem algebraischen Abschluss $\overline{K}$ von K gegebenen Homomorphismus $\alpha : E(\overline{K}) \to E(\overline{K})$. M. a. W. gilt:

(i) $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ für alle Punkte $P_1, P_2 \in E(\overline{K})$.

(ii) es existieren rationale Funktionen $R_1(X,Y), R_2(X,Y) \in \overline{K}(X,Y)$, so dass

$$\alpha(x,y) = (R_1(x,y), R_2(x,y))$$

für alle $(x,y) \in E(\overline{K})$ gilt.

Wie allgemein für Homomorphismen folgt $\alpha(O_E) = O_E$. Es existiert somit genau ein konstanter Endomorphismus. Dieser wird mit 0 bezeichnet und bildet alle Punkte P von E auf O_E ab.

Einige technische Bemerkungen sind notwendig, wenn die rationalen Funktionen in einem Punkt nicht definiert sind. Leichte Umformungen (siehe etwa [13, S. 46]) zeigen, dass sich ein Endomorphismus α als

$$\alpha(X,Y) = (r_1(X), r_2(X)Y)$$

mit rationalen Funktionen $r_1(X), r_2(X) \in \overline{K}(X)$ darstellen lässt. $r_1(X)$ besitzt eine eindeutige Darstellung als $r_1(X) = p(X)/q(X)$ mit teilerfremden Polynomen $p(X), q(X) \in \overline{K}[X]$.
Ist $q(x) = 0$ für einen Punkt $(x,y) \in E(\overline{K})$ so setzen wir $\alpha(x,y) = O_E$. Ist $q(x) \neq 0$, so folgt ([13, Übung 2.14]), dass auch $r_2(x)$ definiert ist.

Definition 4.1.2. Mit den Bezeichnungen von oben heißt

$$deg(\alpha) := Max\{deg(p(X)), deg(q(X))\}$$

der **Grad** von α. Ist $\alpha = 0$, so setzen wir $deg(\alpha) = 0$.
Der Endomorphismus α heißt **separabel**, wenn $\alpha \neq 0$ ist und für die Ableitung $r_1'(X) \neq 0$ gilt.

Proposition 4.1.3. *Ist $\alpha \neq 0$ ein separabler Endomorphismus einer elliptischen Kurve E, so gilt*

$$deg(\alpha) = \#Ker(\alpha).$$

Ist $\alpha \neq 0$ nicht separabel, so ist $deg(\alpha) > \#Ker(\alpha)$.

Beweis. Siehe [13, Prop. 2.20]. □

Bemerkung. Die Endomorphismen einer elliptischen Kurve E bilden in natürlicherweise einen Ring, den **Endomorphismenring** $\mathrm{End}(E)$. Da für alle $m \in \mathbb{Z}$ das m-fache eines Punktes P von E erklärt ist, haben wir stets die Inklusion $\mathbb{Z} \subseteq \mathrm{End}(E)$.

Ein bedeutendes Beispiel eines Endomorphismus ist der **Frobenius**-Endomorphismus ϕ_q. Ist E eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$, so ist ϕ_q gegeben durch

$$\phi_q(x,y) := (x^q, y^q) \qquad \text{für alle Punkte } (x,y) \in E(\overline{\mathbb{F}_q}).$$

Proposition 4.1.4. *Ist E eine elliptische Kurve über $\mathbb{F}_q$ mit $char(\mathbb{F}_q) = p$, so ist $1 - \phi_q$ ein separabler Endomorphismus von E.*

Beweis. Siehe [13, Prop. 2.28]. □

Definition 4.1.5. Es seien zwei elliptische Kurven E und E' über dem Körper k durch die Gleichungen $y^2 = x^3 + Ax + B$ und $y^2 = x^3 + A'x + B'$ gegeben. $L \supseteq k$ sei ein Erweiterungskörper. Unter einem **Isomorphismus von E nach E' über L** verstehen wir eine Abbildung

$$\varphi : E \to E',\ (x,y) \mapsto (c^2x, c^3y)$$

für ein Element $c \in L^*$.

Bemerkung. Ist in obiger Situation ein Isomorphismus durch $c \in L^*$ gegeben, so gilt $c^6y^2 = c^6x^3 + A'c^2x + B'$. Es folgt $y^2 = x^3 + A'c^{-4}x + B'c^{-6}$ und damit $A' = c^4A$, $B' = c^6B$.

Andererseits erhält man ausgehend von $A' = c^4A$, $B' = c^6B$ den obigen Isomorphismus $(x,y) \mapsto (c^2x, c^3y)$, so dass wir einen Isomorphismus von E nach E' mit einem Element $c \in L^*$ identifizieren können, für welches $A' = c^4A$, $B' = c^6B$ gilt.

Proposition 4.1.6. *Sind E und E' elliptische Kurven über einem Körper k, so gilt:*

(i) E und E' haben genau dann die gleiche j-Invariante, wenn sie isomorph über einer endlichen Erweiterung von k sind.

(ii) Ist k algebraisch abgeschlossen, so haben E und E' genau dann die gleiche j-Invariante, wenn sie isomorph über k sind.

Beweis. Die elliptischen Kurven E und E' mit j-Invarianten j und j' seien durch die Gleichungen $y^2 = x^3 + Ax + B$ und $y^2 = x^3 + A'x + B'$ über k gegeben.
(i) Gilt $E \simeq E'$, so folgt leicht $j = j'$. Ist $j = j'$, so folgt aus der Definition der j-Invarianten

$$A^3B'^2 = A'^3B^2. \tag{4.1.1}$$

Wir suchen ein $c \in k^*$ mit $A' = c^4A$, $B' = c^6B$ und unterscheiden verschiedene Fälle.

a) Es ist $A = 0$. Da $\Delta_E \neq 0$ ist, muss $B \neq 0$ sein und aus (4.1.1) folgt $A' = 0$. Eine sechste Wurzel c aus (B/B') in einem Erweiterungskörper von k erfüllt die Bedingungen.

b) Es ist $B = 0$. Wie oben folgt $A \neq 0$ und $B' = 0$. Hier wählt man c als vierte Wurzel aus (A/A').

c) Es ist $AB \neq 0$. Dann muss wegen $\Delta_{E'} \neq 0$ und (4.1.1) auch $A'B' \neq 0$ sein. Setze $c = \left(\frac{A}{A'}\right)^{1/4} = \left(\frac{B}{B'}\right)^{1/6}$.

Teil (ii) folgt nun sofort aus Teil (i). □

4.2 Elliptische Kurven über $\mathbb{C}$

Im Falle $k = \mathbb{C}$ gibt uns die Weierstrass $\wp$-Funktion elliptische Kurven. Ist nämlich $L \subset \mathbb{C}$ ein Gitter, so genügt die $\wp$-Funktion von L nach Thm. 3.1.3 der Differenzialgleichung

$$\left(\frac{\wp'(z)}{2}\right)^2 = \wp(z)^3 - \frac{g_2}{4}\wp(z) - \frac{g_3}{4}.$$

Setzen wir $a := -g_2/4$, $b := -g_3/4$, $y := \wp(z)'/2$ und $x := \wp(z)$, so erhalten wir wegen $\Delta_E = -16(4a^3 + 27b^2) = g_2^3 - 27g_3^2 = \Delta_L \neq 0$ eine elliptische Kurve E mit definierender Gleichung

$$y^2 = x^3 + ax + b$$

und j-Invariante $j(E) = j(L)$. Als Folgerung aus Korollar 3.3.3 erhalten wir direkt

Korollar 4.2.1. *Sei E eine elliptische Kurve über $\mathbb{C}$ mit definierender Gleichung*

$$y^2 = x^3 + a^x + b, \qquad a, b \in \mathbb{C}, \;\; -16(4a^3 + 27b^2) \neq 0.$$

Dann existiert ein Gitter L mit $a = -g_2(L)/4$ und $b = -g_3(L)/4$.

Wir können also elliptische Kurven E über $\mathbb{C}$ mit Gittern L identifizieren. Der Isomorphismus kann direkt angegeben werden.

Theorem 4.2.2. *Ist L ein Gitter und E die elliptische Kurve $y^2 = x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$ mit von L abhängigen Konstanten g_2, $g_3 \in \mathbb{C}$, so ist die Abbildung*

$$\begin{array}{rccc} \Phi: & \mathbb{C}/L & \longrightarrow & E(\mathbb{C}) \\ & z & \mapsto & (\wp(z), \wp(z)/2) \\ & 0 & \mapsto & O_E \end{array}$$

ein Gruppenisomorphismus.

Beweis. Siehe [13, Thm. 9.10]. □

Mittels Φ können wir die Addition zweier Punkte P, Q auf E wegen $P+Q = \Phi(\Phi^{-1}(P)+\Phi^{-1}(Q))$ erneut einfach beschreiben, denn die Addition auf $\mathbb{C}/L$ ist schlicht Addition modulo L. Allgemein ausgedrückt gibt uns Φ mittels $\varphi \mapsto \Phi^{-1} \circ \varphi \circ \Phi$ einen Isomorphismus der Endomorphismenringe $End(E) \xrightarrow{\sim} End(\mathbb{C}/L)$.

Bemerkung 4.2.3. Ist $\tilde{\varphi} = \Phi^{-1} \circ \varphi \circ \Phi$ ein beliebiger Endomorphismus von $End(\mathbb{C}/L)$ und wählen wir eine hinreichend kleine Umgebung U von $z = 0$, so erhalten wir eine analytische Abbildung von U nach $\mathbb{C}$ mit

$$\tilde{\varphi}(z_1 + z_2) \equiv \tilde{\varphi}(z_1) + \tilde{\varphi}(z_2) \bmod L \qquad \text{für} \qquad z_1, z_2 \in U.$$

Es ist $\tilde{\varphi}(0) \equiv 0 \bmod L$ und wir können daher o. B. d. A. $\tilde{\varphi}(0) = 0$ annehmen. Aus Stetigkeitsgründen ist $\tilde{\varphi}(z)$ nahe 0 für z nahe 0. Wählen wir U entsprechend klein, so gilt sogar

$$\tilde{\varphi}(z_1 + z_2) = \tilde{\varphi}(z_1) + \tilde{\varphi}(z_2) \qquad \text{für} \qquad z_1, z_2 \in U,$$

denn es steht außer 0 kein Element aus L zur Verfügung, um die Kongruenz zu erfüllen. Für $z \in U$ gilt deshalb

$$\tilde{\varphi}'(z) = \lim_{h\to 0} \frac{\tilde{\varphi}(z+h) - \tilde{\varphi}(z)}{h} = \lim_{h\to 0} \frac{\tilde{\varphi}(z) + \tilde{\varphi}(h) - \tilde{\varphi}(z)}{h} = \lim_{h\to 0} \frac{\tilde{\varphi}(h) - \tilde{\varphi}(0)}{h} = \tilde{\varphi}'(0).$$

Setzen wir $\alpha := \tilde{\varphi}'(0)$, so muss wegen $\tilde{\varphi}(0) = 0$ dann $\tilde{\varphi}(z) = \alpha z$ für beliebige $z \in U$ gelten. Ist $z \in \mathbb{C}$ beliebig, so existiert ein $n \in \mathbb{Z}$ mit $z/n \in U$ und es gilt

$$\tilde{\varphi}(z) \equiv n\tilde{\varphi}(z/n) = n\alpha/n = \alpha \bmod L.$$

Der Endomorphismus $\tilde{\varphi}$ ist also durch Multiplikation mit α bestimmt, und es gilt $\alpha L \subseteq L$. Andererseits gibt jedes $\alpha \in \mathbb{C}$ mit $\alpha L \subseteq L$ einen Endomorphismus von $\mathbb{C}/L$ in der beschriebenen Weise. Fassen wir zusammen, so gilt für eine elliptische Kurve E zum Gitter L

$$\{\alpha \in \mathbb{C} : \ \alpha L \subseteq L\} \simeq End(E).$$

Als Folgerung aus Theorem 3.2.4 erhalten wir deshalb eine Aussage über die Endomorphismenringe elliptischer Kurven über $\mathbb{C}$.

Theorem 4.2.4. *Ist E eine elliptische Kurve über $\mathbb{C}$, so gilt für den Endomorphismenring von E*

$$End(E) \simeq \mathbb{Z} \qquad oder \qquad End(E) \simeq \mathcal{O}$$

für eine Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers.

Definition 4.2.5. Eine elliptische Kurve E über einem Körper k besitzt **komplexe Multiplikation**, wenn $\mathbb{Z} \neq \mathrm{End}(E)$ gilt.

Als Folgerung aus Proposition 4.1.6 und Theorem 3.1.8 erhalten wir für elliptische Kurven über $\mathbb{C}$

Proposition 4.2.6. *Sind E und E' zwei elliptische Kurven zu den Gittern L und L', so sind äquivalent:*

(i) E und E' sind isomorph über $\mathbb{C}$.
(ii) L und L' sind linear äquivalent.
(iii) $j(E) = j(E')$.

4.3 Elliptische Kurven über endlichen Körpern

Die Menge der $\mathbb{F}_q$-rationalen Punkte einer elliptischen Kurve E über dem endlichen Körper $\mathbb{F}_q$ ist endlich. Ist E durch die Gleichung $y^2 = x^3 + Ax + B$ über $\mathbb{F}_q$ definiert, so können wir die Anzahl genau angeben. Es ist

$$|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right), \tag{4.3.1}$$

wobei der Summand als das verallgemeinerte Legendre-Symbol für $\mathbb{F}_q$ zu verstehen ist. Es muss deshalb $|E(\mathbb{F}_q)| \leq 2q + 1$ sein. Eine bessere Abschätzung liefert

Theorem 4.3.1 (Hasse)**.** *Sei p eine Primzahl, $q = p^n$ und E eine elliptische Kurve über $\mathbb{F}_q$, dann gilt*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Beweis. Siehe [13, Theorem 4.2]. □

Es gilt also $|E(\mathbb{F}_q)| = q + 1 - a$ für ein $|a| \leq 2\sqrt{q}$. In Abschnitt 4.1 wurde der Frobenius-Endomorphismus ϕ_q vorgestellt. Dieser steht in einer engen Beziehung zu elliptischen Kurven über endlichen Körpern, denn es gilt

$$(x, y) \in E(\mathbb{F}_q) \iff \phi_q(x, y) = (x, y) \iff (x, y) \in Ker(1 - \phi_q).$$

Die Zahl $a = (q + 1) - |E(\mathbb{F}_q)|$ ist eindeutig durch die Gleichung

$$\phi_q^2 - a\phi_q + q = 0$$

bestimmt, entspricht also der *Spur* des Frobenius (siehe [13, Thm. 4.10]).
Ist $a \neq \pm 2\sqrt{q}$, so ist $\phi_q \notin \mathbb{Z}$ und folglich $\mathbb{Z} \neq \mathbb{Z}[\phi_q] \subseteq End(E)$. Auch im Falle $a = \pm 2\sqrt{q}$ kann gezeigt werden, dass $\mathbb{Z} \neq End(E)$ gilt. Elliptische Kurven über endlichen Körpern besitzen also stets komplexe Multiplikation. Ohne Beweis (siehe [11, Theorem V.3.1]) zitieren wir

Definition und Theorem 4.3.2. Sei E eine elliptische Kurve über einem endlichen Körper $\mathbb{F}_q$, so gilt für den Endomorphismenring von E einer der folgenden Fälle:

(i) $End(E) \simeq \mathcal{O}$ für eine Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlköpers.

(ii) $End(E) \simeq \mathcal{M}$ für eine Ordnung $\mathcal{M}$ einer Quaternionenalgebra.

Im ersten Fall nennen wir E **ordinär**, im zweiten Fall **supersingulär**.

Es gibt ein einfaches Kriterium, um supersinguläre von ordinären Kurven zu unterscheiden.

Proposition 4.3.3. *Sei E eine elliptische Kurve über $\mathbb{F}_q$ für eine Primpotenz $q = p^f$ und E besitze $|E(\mathbb{F}_q)| = q + 1 - a$ Punkte. Es gilt*

$$E \text{ ist supersingulär} \iff a \equiv 0 \bmod p.$$

Beweis. Siehe [13, Prop. 4.29]. □

Für elliptische Kurven über Primkörpern $\mathbb{F}_p$, $p \geq 5$, vereinfacht sich dieses Kriterium, denn nach Theorem 4.3.1 kommt einzig $a = 0$ in Frage.

Korollar 4.3.4. *Sei $p \geq 5$ und E eine elliptische Kurve über $\mathbb{F}_p$, so gilt*

$$E \text{ ist supersingulär} \iff |E(\mathbb{F}_p)| = p + 1.$$

Da endliche Körper nicht algebraisch abgeschlossen sind, werden isomorphe elliptische Kurven über $\mathbb{F}_q$ nicht eindeutig durch ihre j-Invariante charakterisiert. Ohne Beweis zitieren wir die folgende Aussage ([3, Prop. 14.19]).

Proposition 4.3.5. *Seien E und E' elliptische Kurven über dem endlichen Körper $\mathbb{F}_q$. Ist E ordinär, so gilt*

$$E(\mathbb{F}_q) \simeq E'(\mathbb{F}_q) \iff j(E) = j(E') \text{ und } |E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|.$$

Die Gruppenordnung $|E(\mathbb{F}_q)|$ einer elliptischen Kurve E über $\mathbb{F}_q$ liegt im Hasse-Intervall. Welche Gruppenordnungen tatsächlich realisiert werden, spezifiziert Theorem 4.3.6, welches wir ebenfalls ohne Beweis ([13, Thm. 4.3]) hier angeben.

Theorem 4.3.6. *Sei $q = p^n$ eine Primpotenz und $N = q + 1 - a$. Es existiert genau dann eine elliptische Kurve E über $\mathbb{F}_q$ mit $|E(\mathbb{F}_q)| = N$ Punkten, wenn $|a| \leq 2\sqrt{q}$ gilt und eine der folgenden Bedingungen erfüllt ist:*

(i) $ggT(a, p) = 1$.
(ii) n *ist gerade und* $a = \pm 2\sqrt{q}$.
(iii) n *ist gerade,* $p \not\equiv 1 \bmod 3$ *und* $a = \pm\sqrt{q}$.
(iv) n *ist ungerade,* $p = 2$ *oder* $p = 3$ *und* $a = \pm p^{(n+1)/2}$.
(v) n *ist gerade,* $p \not\equiv 1 \bmod 4$ *und* $a = 0$.
(vi) n *ist ungerade und* $a = 0$.

Als Folgerung aus Thm. 4.3.6 halten wir fest, dass für jede Prizahl p und jede natürliche Zahl N im Hasse-Intervall von p eine elliptische Kurve E über $\mathbb{F}_p$ mit N Punkten existiert.

4.4 Twiste

Definition 4.4.1. Es seien E und E' elliptische Kurven über $\mathbb{F}_q$. E' heißt ein $\mathbb{F}_q$-**Twist** von E, wenn E und E' über einer endlichen Erweiterung $\mathbb{F}_{q^d}$ von $\mathbb{F}_q$ isomorph sind.

Bemerkung 4.4.2. Twiste haben nach Prop. 4.1.6 stets die gleiche j-Invariante!

Ist die elliptische Kurve E durch die Gleichung $y^2 = x^3 + Ax + B$ über $\mathbb{F}_q$ gegeben und $\beta \in \mathbb{F}_q^*$, so ist die elliptische Kurve E' mit der Gleichung $y^2 = x^3 + \beta^2 Ax + \beta^3 B$ ein $\mathbb{F}_q$-Twist von E.
Suchen wir nämlich $c = \sqrt{\beta} \in \mathbb{F}_{q^2}$, so ist durch $(A, B) \mapsto (c^4 A, c^6 B)$ ein Isomorphismus von E nach E' über $\mathbb{F}_{q^2}$ gegeben. Wir nennen hier E' einen **quadratischen** $\mathbb{F}_q$-**Twist** von E.

Ist die elliptische Kurve E durch die Gleichung $y^2 = x^3 + Ax$ über $\mathbb{F}_q$ gegeben und $\beta \in \mathbb{F}_q^*$, so ist die elliptische Kurve E' mit der Gleichung $y^2 = x^3 + \beta Ax$ ein $\mathbb{F}_q$-Twist von E.
Ein Element $c = \sqrt[4]{\beta} \in \mathbb{F}_{q^4}$ gibt uns hier die Isomorphie $E \simeq E'$ über $\mathbb{F}_{q^4}$. Es heißt dann E' auch ein **quartischer** $\mathbb{F}_q$-**Twist** von E.

Ist eine elliptische Kurve E durch die Gleichung $y^2 = x^3 + B$ über $\mathbb{F}_q$ gegeben und $\beta \in \mathbb{F}_q^*$, so ist die elliptische Kurve E' mit der Gleichung $y^2 = x^3 + \beta B$ ein $\mathbb{F}_q$-Twist von E.
Ein Element $c = \sqrt[6]{\beta} \in \mathbb{F}_{q^6}$ gibt uns hier die Isomorphie $E \simeq E'$ über $\mathbb{F}_{q^6}$. Es heißt dann E' auch ein **sextischer** $\mathbb{F}_q$-**Twist** von E.

Wir interessieren uns für die Anzahl $\mathbb{F}_q$-rationaler Punkte einer elliptischen Kurve im Verhältnis zu ihren Twisten. Dies wird im Folgenden näher beleuchtet.

Proposition 4.4.3. *Sei $E = (a, b)$ eine elliptische Kurve über $\mathbb{F}_q$, $char(\mathbb{F}_q) \geq 5$ und E' ein quadratischer $\mathbb{F}_q$-Twist von E zum* Nichtquadrat $\beta \in \mathbb{F}_q^*$, so gilt $|E(\mathbb{F}_q)| + |E'(\mathbb{F}_q)| = 2(q + 1)$.

Beweis. Nach (4.3.1) gilt

$$\begin{aligned} |E(\mathbb{F}_q)| + |E'(\mathbb{F}_q)| - 2(q+1) &= \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right) + \sum_{x \in \beta\mathbb{F}_q} \left(\frac{x^3 + \beta^2 Ax + \beta^3 B}{\mathbb{F}_q} \right) \\ &= \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right) + \left(\frac{\beta^3 (x^3 + Ax + B)}{\mathbb{F}_q} \right) = 0. \end{aligned}$$

□

Lemma 4.4.4. *Ist $p \equiv 1 \bmod 4$ eine Primzahl, so existiert ein eindeutig bestimmtes Element $\pi_0 \in \mathbb{Z}[i]$ mit $N_{K/\mathbb{Q}}(\pi_0) = p$ und $\pi_0 \equiv 1 \bmod (2+2i)$.*

Beweis. Es ist $\mathbb{Z}[i]$ der Ganzheitsring des Zahlkörpers $K = \mathbb{Q}(\sqrt{-1})$ mit Diskriminante $d_K = -4$ nach Abschnitt 1.2. Aus der Kongruenzbedingung und den quadratischen Reziprozitätsgesetzen folgt $(d_K/p) = (-4/p) = (-1)^{(p-1)/2}(4/p) = 1$, und p ist nach Prop. 1.2.2 in $\mathbb{Z}[i]$ vollständig zerlegt. Da $\mathbb{Z}[i]$ ein Hauptidealring ist, existiert also ein Element $\pi = A+Bi \in \mathbb{Z}[i]$ mit $p = \pi\overline{\pi} = N_{K/\mathbb{Q}}(\pi)$. Für jedes $\epsilon = r + si \in \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ gilt dann ebenfalls $N_{K/\mathbb{Q}}(\epsilon\pi) = p$. Es muss also $\pi_0 = \epsilon\pi$ und $\pi \equiv \epsilon^{-1} \bmod (2+2i)$ gelten, d. h. $A + Bi = (r - si) + 2(1+i)(\alpha + \beta i)$ für geeignete $\alpha, \beta \in \mathbb{Z}$. Dies führt auf

$$A = r + 2(\alpha - \beta) \qquad \text{und} \qquad B = -s + 2(\alpha + \beta) \tag{4.4.1}$$

und

$$A - B = r + s - 4\beta \equiv r + s \bmod 4. \tag{4.4.2}$$

Da $p = N_{K/\mathbb{Q}}(\pi) = A^2 + B^2$ ungerade ist, muss $A \equiv B + 1 \bmod 2$ gelten. Ist $A \equiv 0 \bmod 2$, so folgt mit (4.4.1) zunächst $r = 0$ und s ist durch (4.4.2) eindeutig bestimmt, denn $s \in \{-1, 0, 1\}$. Ist hingegen $B \equiv 0 \bmod 2$, so folgt mit (4.4.1) zunächst $s = 0$ und r ist durch (4.4.2) eindeutig bestimmt, denn $r \in \{-1, 0, 1\}$.
Wir sehen also, dass stets ein eindeutiges ϵ und damit ein eindeutiges π_0 der Behauptung entsprechend existiert. □

Es ist für $D \in \mathbb{F}_p^*$ die elliptische Kurve $y^2 = x^3 + Dx$ ein quartischer Twist von $y^2 = x^3 + x$. Über die Anzahl der Punkte gibt die folgende Proposition Auskunft (siehe [6, Prop. 18.3.4]).

Proposition 4.4.5. *Sei $p > 2$ prim, $D \in \mathbb{Z} - p\mathbb{Z}$ und betrachte die elliptische Kurve mit definierender Gleichung $y^2 = x^3 + Dx$ über $\mathbb{F}_p$. Ist $p \equiv 3 \bmod 4$, so ist die Kurve supersingulär. Ist $p \equiv 1 \bmod 4$, so ist $p = \pi_0\overline{\pi_0}$ für ein $\pi_0 \in \mathbb{Z}[i]$ mit $\pi_0 \equiv 1 \bmod 2 + 2i$ und die Kurve besitzt*

$$p + 1 - \overline{\left(\frac{-D}{\pi_0}\right)_4}\,\pi_0 - \left(\frac{-D}{\pi_0}\right)_4 \overline{\pi_0}$$

$\mathbb{F}_p$-rationale Punkte. Hierbei ist $(\frac{\alpha}{\pi_0})_4 \equiv \alpha^{\frac{p-1}{4}} \bmod \pi_0$ für $\alpha \in \mathbb{Z}[i]$ das quartische Potenzrestsymbol.

Lemma 4.4.6. *Ist $p \equiv 1 \bmod 3$ eine Primzahl, so existiert ein eindeutig bestimmtes Element $\pi_0 \in \mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{2}$, mit $N_{K/\mathbb{Q}}(\pi_0) = p$ und $\pi_0 \equiv 2 \bmod 3$.*

Beweis. Es ist $Z[\omega]$ der Ganzheitsring des Zahlkörpers $K = \mathbb{Q}(\sqrt{-3})$ mit Diskriminante $d_K = -3$ nach Abschnitt 1.2. Aus der Kongruenzbedingung und den quadratischen Reziprozitätsgesetzen folgt $(d_K/p) = (-3/p) = (-1)^{(p-1)/2}(3/p) = (-1)^{(p-1)/2}(-1)^{((p-1)/2)((3-1)/2)}(p/3) = (p/3) = (1/3) = 1$, und p ist nach Prop. 1.2.2 in $\mathbb{Z}[\omega]$ vollständig zerlegt. Da $\mathbb{Z}[\omega]$ ein Hauptidealring ist, existiert also ein Element $\pi = A + B\omega \in \mathbb{Z}[\omega]$ mit $p = \pi\overline{\pi} = N_{K/\mathbb{Q}}(\pi)$. Für jedes $\epsilon = r + s\omega$ in $\mathbb{Z}[\omega]^* = \{\pm 1, \pm\omega, \pm\omega^2\}$ gilt dann ebenfalls $N_{K/\mathbb{Q}}(\epsilon\pi) = p$. Es muss also $\pi_0 = \epsilon\pi$ und $\epsilon\pi \equiv 2 \bmod 3$ gelten, d. h. $(r + s\omega)(A + B\omega) \equiv 2 \bmod 3$. Dies führt unter Ausnutzung von $\omega^2 + \omega + 1 = 0$ auf

$$\begin{array}{ll} Ar - Bs & \equiv 2 \bmod 3 \\ Br + (A-B)s & \equiv 0 \bmod 3 \end{array} \qquad \text{bzw.} \qquad \begin{pmatrix} A & -B \\ B & A-B \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 0 \end{pmatrix} \bmod 3.$$

Die Determinante der rechten Matrix ist $A^2 - AB + B^2 = \cdots = N_{K/\mathbb{Q}}(\pi) = p \not\equiv 0 \bmod 3$ und das Gleichungssystem deshalb eindeutig lösbar:

$$\begin{array}{ll} r & \equiv B - A \bmod 3 \\ s & \equiv \quad B \bmod 3. \end{array} \tag{4.4.3}$$

Auch hier sehen wir, dass stets ein eindeutiges ϵ und damit ein eindeutiges π_0 der Behauptung entsprechend existiert. □

Es ist für $D \in \mathbb{F}_p^*$ die elliptische Kurve $y^2 = x^3 + D$ ein sextischer Twist von $y^2 = x^3 + 1$. Über die Anzahl der Punkte gibt die folgende Proposition Auskunft, welche wir ebenfalls zitieren (siehe [6, Prop. 18.3.4]).

Proposition 4.4.7. *Sei $p > 3$ prim, $D \in \mathbb{Z} - p\mathbb{Z}$ und betrachte die elliptische Kurve mit definierender Gleichung $y^2 = x^3 + D$ über $\mathbb{F}_p$. Ist $p \equiv 2 \bmod 3$, so ist die Kurve supersingulär. Ist $p \equiv 1 \bmod 3$, so ist $p = \pi_0\overline{\pi_0}$ für ein $\pi_0 \in \mathbb{Z}[\omega]$ mit $\pi_0 \equiv 2 \bmod 3$ und die Kurve besitzt*

$$p + 1 + \overline{\left(\frac{4D}{\pi_0}\right)_6}\,\pi_0 + \left(\frac{4D}{\pi_0}\right)_6 \overline{\pi_0}$$

$\mathbb{F}_p$-rationale Punkte. Hierbei ist $(\frac{\alpha}{\pi_0})_6 \equiv \alpha^{\frac{p-1}{6}} \bmod \pi_0$ für $\alpha \in \mathbb{Z}[\omega]$ das sextische Potenzrestsymbol.

4.5 Reduktion elliptischer Kurven

Sei E eine elliptische Kurve über $\mathbb{C}$, welche komplexe Multiplikation mit einer Ordnung $\mathcal{O}$ besitzt. E lässt sich mit einem Gitter L identifizieren, und L ist linear äquivalent zu einem eigentlichen gebrochenen $\mathcal{O}$-Ideal $\mathfrak{a}$. Die j-Invariante $j(E) = j(\mathfrak{a})$ von E liegt nach Theorem 3.4.1 im Ringklassenkörper $H_\mathcal{O}$. Mit Hilfe von Prop. 4.0.8 lässt sich deshalb eine elliptische Kurve über $H_\mathcal{O}$ aufstellen, welche die gleiche j-Invariante wie E besitzt. Diese ist dann nach Prop. 4.2.6 zu E isomorph. Wir können daher o. B. d. A. davon ausgehen, dass E selbst über $H_\mathcal{O}$ definiert ist. Sei E durch die Gleichung

$$y^2 = x^3 + ax + b \qquad \text{mit} \qquad a, b \in H_\mathcal{O}$$

gegeben. Da $H_\mathcal{O}$ der Quotientenkörper von $\mathcal{O}_{H_\mathcal{O}}$ ist, können wir a und b in der Form α_1/β_1 und α_2/β_2 mit $\alpha_i, \beta_i \in \mathcal{O}_{H_\mathcal{O}}$ schreiben, also

$$y^2 = x^3 + \alpha_1\beta_1^{-1}x + \alpha_2\beta_2^{-1}.$$

Sei $\mathfrak{P}$ ein Primideal von $\mathcal{O}_{H_\mathcal{O}}$ und $\beta_i \notin \mathfrak{P}$. Wir reduzieren die Koeffizienten modulo $\mathfrak{P}$ und erhalten die Gleichung

$$y^2 = x^3 + \tilde{\alpha}_1\tilde{\beta}_1^{-1}x + \tilde{\alpha}_2\tilde{\beta}_2^{-1}.$$

Die Koeffizienten liegen im endlichen Körper $\mathcal{O}_{H_\mathcal{O}}/\mathfrak{P} \simeq \mathbb{F}_q$. Ist $\Delta_E \notin \mathfrak{P}$, so ist $\Delta_E \not\equiv 0 \bmod \mathfrak{P}$ und deshalb

$$y^2 = x^3 + \tilde{a}x + \tilde{b}$$

eine elliptische Kurve $\tilde{E}$ über $\mathbb{F}_q$. Wir sagen in diesem Fall, dass E **gute Reduktion modulo $\mathfrak{P}$** besitzt und nennen $\tilde{E}$ die **Reduktion von E bei $\mathfrak{P}$**.

Bemerkung 4.5.1. Die Reduktion der elliptischen Kurve E wirkt sich in naheliegender Weise auf die j-Invariante und Diskriminante von E aus. Ist $\Delta_E = -16(4a^3 + 27b^2)$, so ist

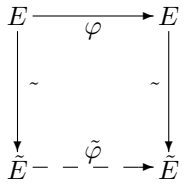
$$\Delta_{\tilde{E}} \equiv -16(4\tilde{a}^3 + 27\tilde{b}^2) \equiv \Delta_E \bmod \mathfrak{P}.$$

Analog verhält sich die j-Invariante $j(\tilde{E})$ von $\tilde{E}$. In Worten: Reduktion ist ein Homomorphismus und deshalb die j-Invariante / Diskriminante der reduzierten elliptischen Kurve $\tilde{E}$ gleich der reduzierten j-Invariante / Diskriminante der elliptischen Kurve E.

4.6 Reduktion von Endomorphismen

Um den Beweis des Theorems 4.6.3 anreißen zu können, werden zunächst einige Erkenntnisse zitiert (vgl. [12, Prop. II.4.4] und [8, Kap. 13.§4, Thm. 12]), die letztendlich alle auf Deuring und Hasse zurückgehen.

Der im vorigen Abschnitt beschriebene Reduktionsprozess zieht in natürlicherweise eine Reduktion des Endomorphismenringes nach sich. Sei E eine elliptische Kurve über einem Zahlkörper mit guter Reduktion, $\tilde{E}$ die reduzierte Kurve und ψ ein Endomorphismus von E. Dann induziert ψ einen Endomorphismus $\tilde{\psi}$ von $\tilde{E}$ mittels $\tilde{P} \mapsto \widetilde{\psi(P)}$ für Punkte $\tilde{P}$ von $\tilde{E}$.



Proposition 4.6.1. *Sei L ein Zahlkörper, $\mathfrak{P}$ ein maximales Ideal von L und E eine elliptische Kurve über L mit guter Reduktion bei $\mathfrak{P}$. $\tilde{E}$ bezeichne die reduzierte Kurve. Die natürliche Abbildung*

$$End(E) \to End(\tilde{E}), \quad \phi \mapsto \tilde{\phi}$$

ist injektiv und graderhaltend, d. h. $deg(\phi) = deg(\tilde{\phi})$.

Unter gewissen Umständen ist der soeben beschriebene Reduktionsprozess von Endomorphismen nicht nur injektiv, sondern sogar surjektiv.

Theorem 4.6.2. *Sei E eine elliptische Kurve über dem Zahlkörper L, mit $End(E) \simeq \mathcal{O}$, wobei $\mathcal{O}$ eine Ordnung des imaginär-quadratischen Zahlkörpers K ist. Sei $\mathfrak{P}$ ein Primideal von L über der Primzahl $p \in \mathbb{Z}$, so dass E gute Reduktion $\tilde{E}$ bei $\mathfrak{P}$ besitzt.*
Es ist $\tilde{E}$ genau dann supersingulär, wenn p in K nicht vollständig zerlegt ist.
Angenommen p ist vollständig zerlegt in K. Sei f der Führer von $\mathcal{O}$ und es gelte $p \nmid f$. Dann ist die Abbildung

$$\Phi : End(E) \to End(\tilde{E}), \quad \phi \mapsto \tilde{\phi}$$

surjektiv und damit ein Isomorphismus.

Das nun folgende Theorem stellt das Herzstück des Konstruktionsverfahrens für elliptische Kurven dar. Wir haben in den vorangegangenen Abschnitten gesehen, dass sowohl elliptische Kurven über $\mathbb{C}$ mit komplexer Multiplikation, als auch ordinäre elliptische Kurven über endlichen Körpern eine Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers K als Endomorphismenring besitzen.

Theorem 4.6.3 (Deuring)**.** *Sei K ein imaginär-quadratischer Zahlkörper, $\mathcal{O}$ eine Ordnung von K und $H_{\mathcal{O}}$ der Ringklassenkörper. $p \in \mathbb{Z}$ sei eine Primzahl, die in K vollständig zerlegt ist und $\mathfrak{P}$ ein Primideal von $H_{\mathcal{O}}$ über p mit Restklassengrad $f := f_{\mathfrak{P}|p}$ und $[\mathcal{O}_K : \mathcal{O}] \notin \mathfrak{P}$.*
Sei A eine elliptische Kurve über $H_{\mathcal{O}}$, welche komplexe Multiplikation mit $\mathcal{O}$ und gute Reduktion bei $\mathfrak{P}$ besitzt. $\tilde{A}$ bezeichne die reduzierte Kurve. Dann existiert ein Element $\pi \in \mathcal{O}/p\mathcal{O}$, welches den folgenden Gleichungen genügt

$$p^f = N_{K/\mathbb{Q}}(\pi) \qquad und \qquad \#\tilde{A}(\mathbb{F}_{p^f}) = N_{K/\mathbb{Q}}(1-\pi).$$

Zusatz: Jede (ordinäre) elliptische Kurve E über $\mathbb{F}_{p^f}$ mit Endomorphismenring $\mathcal{O}$ ist eine solche reduzierte Kurve.

Beweisskizze. Die elliptische Kurve A besitzt komplexe Multiplikation mit der Ordnung $\mathcal{O}$. Daher ist nach Thm. 3.2.4 $End(A) \simeq \mathcal{O}$. Da A gute Reduktion bei $\mathfrak{P}$ besitzt und p in K vollständig zerlegt ist, ist die reduzierte Kurve $\tilde{A}$ nach Theorem 4.6.2 ordinär. Außerdem ist

$$End(\tilde{A}) \simeq End(A),$$

denn p teilt nicht den Führer von $\mathcal{O}$. Somit gibt es ein Element $\pi \in \mathcal{O} \simeq End(A)$, dessen Reduktion der Frobenius $\phi_q \in End(\tilde{A})$ von $\tilde{A}$ ist.
Der Endomorphismus $(1-\pi) \in End(A)$ reduziert sich zu $(1-\phi_q) \in End(\tilde{A})$. Den Propositionen 4.1.3 und 4.1.4 zufolge gilt mit $q := p^f$

$$deg(\phi_q) = q \qquad \text{und} \qquad \#\tilde{A}(\mathbb{F}_q) = \#Ker(1-\phi_q) = deg(1-\phi_q).$$

Da die Reduktion nach Prop. 4.6.1 graderhaltend ist, gilt auch

$$deg(\pi) = q \qquad \text{und} \qquad \#\tilde{A}(\mathbb{F}_q) = deg(1-\pi).$$

Da $\tilde{A}$ ordinär ist, gilt nach Prop. 4.3.3 $a := q+1-\#\tilde{A}(\mathbb{F}_q) \not\equiv 0 \bmod p$. Insbesondere ist $a \neq \pm 2\sqrt{q}$ und $\pi \notin \mathbb{Z}$. In Theorem 3.2.4 wurde gezeigt, dass

$$deg(\pi) = N_{K/\mathbb{Q}}(\pi) \qquad \text{und} \qquad deg(1-\pi) = N_{K/\mathbb{Q}}(1-\pi)$$

gilt. Damit ist die erste Aussage klar.
Der Zusatz benutzt das sog. Lifting-Theorem von Deuring (vgl. [8, Kap. 13.§5, Thm. 14]). Dieses besagt, dass zu einer elliptischen Kurve E über einem endlichen Körper und *einem* Endomorphismus α_0 von E eine elliptische Kurve A mit guter Reduktion über einem Zahlkörper, sowie einem Endomorphismus α von A existiert, sodass für die Reduktionen $\tilde{A} \simeq E$ und $\tilde{\alpha} \simeq \alpha_0$ gilt. Bildlich gesprochen lassen sich eine elliptische Kurve und ein Endomorphismus ins Komplexe liften.
Starten wir mit einer ordinären elliptischen Kurve E über $\mathbb{F}_q$, so ist ihr Endomorphismenring eine Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers, d.h. ein $\mathbb{Z}$-Modul von Rang 2, besitzt also eine Darstellung $\mathcal{O} = [1, \alpha_0]$ für ein $\alpha_0 \in \mathbb{C}$. Liften wir den Endomorphismus α_0, so liften wir eine Basis von $\mathcal{O}$, denn die 1 liftet in trivialer Weise. Deshalb gilt $End(\tilde{A}) \simeq End(E)$ und sogar $End(A) \simeq End(E)$ nach Theorem 4.6.2, denn E ist ordinär. Folglich existiert in $End(A)$ ein zum Frobenius ϕ_q von E isomorphes Element π mit den gewünschten Eigenschaften. □

Ohne Beweis (vgl. [3, Thm. 13.21] bzw. [8, Kap. 13.§4, Thm. 13]) zitieren wir das folgende Theorem.

Theorem 4.6.4. *Seien $\mathcal{O}_1 \subset K_1$ und $\mathcal{O}_2 \subset K_2$ Ordnungen von imaginär-quadratischen Zahlkörpern, $\mathfrak{a}_1 \subseteq \mathcal{O}_1$ und $\mathfrak{a}_2 \subseteq \mathcal{O}_2$ eigentliche gebrochene Ideale. Sei L ein Zahlkörper, der $j(\mathfrak{a}_1)$ und $j(\mathfrak{a}_2)$ enthält und $\mathfrak{P}$ ein Primideal von L über der Primzahl $p \in \mathbb{Z}$. Ist $K_1 = K_2$, so teile p weder den Führer von $\mathcal{O}_1$ noch den Führer von $\mathcal{O}_2$.*
Ist $j(\mathfrak{a}_1) \neq j(\mathfrak{a}_2)$, so gilt

$$j(\mathfrak{a}_1) \equiv j(\mathfrak{a}_2) \bmod \mathfrak{P} \Longrightarrow \left\{ \begin{array}{c} p \text{ zerfällt weder in } K_1 \\ \text{noch in } K_2 \text{ vollständig.} \end{array} \right.$$

5 Konstruktionsverfahren

Das Konstruktionsverfahren stellt keine Bedingungen an die Charakteristik des verwendeten endlichen Körpers. Da wir die kurze Weierstrass Normalform für elliptische Kurven verwenden wollen, beschränken wir uns auf endliche Körper der Charakteristik ungleich 2 und 3.

5.1 Die Complex-Multiplication-Methode

Es sei eine Primpotenz $q = p^f$ für $p \geq 5$ und eine natürliche Zahl $N = q + 1 - a,\ |a| \leq 2\sqrt{q}$ vorgegeben. Wir setzen außerdem voraus, dass eine ordinäre elliptische Kurve E über $\mathbb{F}_q$ mit N Punkten existiert. N muss dann Proposition 4.3.3 und eine Bedingung von Theorem 4.3.6 erfüllen. Ist f=1, so ist dies gleichbedeutend mit $a \neq 0$.

Wir wollen eine Kurvengleichung für E bzw. eine Kurvengleichung einer zu E über $\mathbb{F}_q$ isomorphen elliptischen Kurve bestimmen.

Da E ordinär ist, ist der Endomorphismenring $End(E)$ nach Thm. 4.3.2 isomorph zu einer Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers K. Das Theorem 4.6.3 von Deuring sagt, dass E die Reduktion einer elliptischen Kurve A über dem Ringklassenkörper $H_{\mathcal{O}}$ von $\mathcal{O}$ ist. Die Primzahl p ist in K vollständig zerlegt, p teilt nicht den Führer $g := [\mathcal{O}_K : \mathcal{O}]$ von $\mathcal{O}$ und für ein über p liegendes Primideal $\mathfrak{P}$ von $H_{\mathcal{O}}$ gilt $f = f_{\mathfrak{P}|p}$. Der Endomorphismenring bleibt bei dieser Reduktion stabil, so dass $End(E) \simeq \mathcal{O} \simeq End(A)$ ist. Deshalb gibt es in $\mathcal{O}$ das Frobenius-Element $\pi_E \simeq \phi_q$ von E, welches die folgenden Normgleichungen erfüllt:

$$N_{K/\mathbb{Q}}(\pi_E) = p^f = q \qquad \text{und} \qquad N_{K/\mathbb{Q}}(1 - \pi_E) = 1 - Tr_{K/\mathbb{Q}}(\pi_E) + q = N. \tag{5.1.1}$$

Das gibt uns eine Möglichkeit zur Hand, K allein aus der Kenntnis von q und N zu gewinnen. Ist D die Diskriminante von $\mathcal{O}$, so besitzt π_E gemäß Abschnitt 1.3 eine Darstellung $\pi_E = \frac{\alpha+\beta\sqrt{D}}{2}$ mit $\alpha, \beta \in \mathbb{Z}$. Aus (5.1.1) folgt dann

$$4q = N_{K/\mathbb{Q}}(2\pi_E) = \alpha^2 - D\beta^2.$$

Es ist $\alpha = Tr_{K/\mathbb{Q}}(\pi_E)$ die Spur des Frobenius. Diese stimmt nach Abschnitt 4.3 also mit $a = q + 1 - N$ überein, wie wir auch sofort aus (5.1.1) ablesen.
Wir können daher $D\beta^2 = \alpha^2 - 4q = (q + 1 - N)^2 - 4q$ durch q und N ausdrücken und es ist

$$K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D\beta^2}) = \mathbb{Q}(\sqrt{(q+1-N)^2 - 4q}).$$

Da E ordinär ist, gilt nach Prop. 4.3.3 $\alpha \not\equiv 0 \bmod p$. Wir erhalten

$$(\beta g)^2 d_K \equiv \beta^2 D \equiv \alpha^2 - 4q \equiv \alpha^2 \not\equiv 0 \bmod p.$$

Insbesondere ist p kein Teiler von β, g oder d_K und $d_K \equiv (\frac{\alpha}{\beta g})^2 \bmod p$. Da also $\alpha, \beta \not\equiv 0 \bmod p$ sind, kann π_E kein Element von $p\mathcal{O}$ sein. Außerdem teilt p nicht den Führer $[\mathcal{O}_K : \mathcal{O}]$ von $\mathcal{O}$ und ist nach Prop. 1.2.2 in K vollständig zerlegt.

Ist $\mathfrak{p}$ ein Primideal von K über p und $\mathfrak{P}$ ein Primideal von $H_{\mathcal{O}}$ über p, so gilt deshalb $f_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|p} = f$. Korollar 2.2.3 zusammen mit der Tatsache, dass $H_{\mathcal{O}}/K$ abelsch ist, gibt uns

$$f = ord\left(\frac{H_{\mathcal{O}}/K}{\mathfrak{p}}\right).$$

Wegen der Korrespondenz $I_K(g)/P_{K,\mathbb{Z}}(g) \simeq Gal(H_{\mathcal{O}} : K)$ ist f folglich die kleinste Zahl, so dass $\mathfrak{p}^f$ ein Hauptideal ist. f ist also unter der Voraussetzung $p \nmid [\mathcal{O}_K : \mathcal{O}]$ durch $\mathfrak{p}$, d. h. durch p und K eindeutig bestimmt.

Für den Endomorphismenring $\mathcal{O} = \mathcal{O}_D$ von E gilt die Inklusion $\mathcal{O}_{\beta^2 D} \subseteq \mathcal{O} \subseteq \mathcal{O}_K$.

Bemerkung 5.1.1. Die Ordnung $\mathcal{O}$ können wir im Allgemeinen nicht genauer bestimmen. Allerdings ist dies kein Hindernis, denn wir können *jede* Ordnung $\mathcal{O}$ mit $\mathcal{O}_{\beta^2 D} \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ wählen, wie sich jetzt zeigt. Sei nämlich $\mathcal{O}$ eine beliebige solche Ordnung, so können wir π_E als Element von $\mathcal{O}$ auffassen. Es ist p vollständig zerlegt in K und da p nicht βg teilt, gilt $p \nmid [\mathcal{O}_K : \mathcal{O}]$. Können wir eine elliptische Kurve über dem Ringklassenkörper $H_{\mathcal{O}}$ finden, die $\mathcal{O}$ als Endomorphismenring und gute Reduktion bei einem Primideal $\mathfrak{P}$ von $\mathcal{O}_{H_{\mathcal{O}}}$ über p besitzt, so sagt das Theorem 4.6.3, dass die reduzierte Kurve ebenfalls die gesuchten Eigenschaften hat.
Wir gehen hier eine Hypothek ein und nehmen die Aussage von Lemma 5.1.2 vorweg, dass eine solche Kurve existiert. Deshalb können wir uns im Folgenden auf den Fall beschränken, dass $End(A) \simeq \mathcal{O}_K$ gilt und $H_{\mathcal{O}} = H_K$ der Hilbert Klassenkörper ist.

Wir wollen die elliptische Kurve A (bis auf Isomorphie über $\mathbb{C}$) näher bestimmen. Nach Prop. 4.2.6 genügt es daher, ihre j-Invariante zu bestimmen. Entsprechend Theorem 3.2.4 ist das zu A gehörende Gitter L linear äquivalent zu einem eigentlichen gebrochenen Ideal $\mathfrak{a}$ von $\mathcal{O}_K \simeq End(A)$. Die j-Invariante $j(A) = j(L) = j(\mathfrak{a})$ (vgl. Prop. 4.2.6) ist nach Theorem 3.4.1 algebraisch ganz und nach Prop. 3.4.4 eine Nullstelle des Klassenpolynoms

$$H_{\mathcal{O}_K}(X) := \prod_{[\mathfrak{a}] \in \mathcal{C}(\mathcal{O}_K)} (X - j(\mathfrak{a})) \quad \in \mathbb{Z}[X].$$

Bemerkung. Der Grad $h_{\mathcal{O}}$ des Klassenpolynoms zur Ordnung $\mathcal{O}$ entspricht dem Grad der Körpererweiterung $H_{\mathcal{O}}/K$, wo $H_{\mathcal{O}}$ den Ringklassenkörper von $\mathcal{O}$ bezeichnet. Mit Korollar 2.4.8 folgt deshalb für Ordnungen $\mathcal{O}_1$ und $\mathcal{O}_2$

$$\mathcal{O}_1 \subseteq \mathcal{O}_2 \qquad \Longrightarrow \qquad h_{\mathcal{O}_2} \leq h_{\mathcal{O}_1}.$$

Indem wir uns auf Maximalordnungen $\mathcal{O}_K$ als Endomorphismenring beschränken, wählen wir also ein Klassenpolynom kleinst möglichen Grades und verringern deshalb den Rechenaufwand.

Die elliptische Kurve A ist also durch *eine* Nullstelle $j(\mathfrak{a})$ von $H_{\mathcal{O}_K}(X)$ bestimmt. Es ist nun die Frage, *welche* Nullstelle uns eine elliptische Kurve A mit guter Reduktion bei $\mathfrak{P}$ und $End(A) \simeq \mathcal{O}_K$ liefert. Da jede Kurve, die wir durch den soeben beschriebenen Prozess erhalten, nach Bemerkung 4.2.3 und Theorem 3.2.4 den Endomorphismenring $\mathcal{O}_K$ besitzt, bleibt nur die Frage nach der Reduzierbarkeit zu klären.

Lemma 5.1.2. *Ist K ein imaginär-quadratische Zahlkörper, $\mathcal{O} \subset K$ eine Ordnung mit Ringklassenkörper $H_{\mathcal{O}}$, $p > 3$ eine Primzahl, die in K vollständig zerlegt ist und $\mathfrak{P} \subset \mathcal{O}_{H_{\mathcal{O}}}$ ein Primideal über p, sowie $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ ein vollständiges Vertretersystem der Idealklassen von $\mathcal{O}$, so existiert zu jedem $i = 1, \ldots, h$ eine elliptische Kurve A_i über $H_{\mathcal{O}}$ mit j-Invariante $j(\mathfrak{a}_i)$ und guter Reduktion bei $\mathfrak{P}$.*

Beweis. 1. Es sei $j(\mathfrak{a}_i) \neq 0, 1728$. Nach Bem. 3.4.6 ist dann $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. Nach Prop. 4.0.8 ist durch die Gleichung

$$y^2 = x^3 + \frac{3j(\mathfrak{a}_i)}{1728 - j(\mathfrak{a}_i)}x + \frac{2j(\mathfrak{a}_i)}{1728 - j(\mathfrak{a}_i)}$$

eine elliptische Kurve A_i mit $j(A_i) = j(\mathfrak{a}_i)$ über $H_{\mathcal{O}}$ gegeben. A_i besitzt genau dann gute Reduktion modulo $\mathfrak{P}$, wenn mit $c := j(\mathfrak{a}_i)/(1728 - j(\mathfrak{a}_i))$

$$1728 - j(\mathfrak{a}_i) \notin \mathfrak{P} \quad \text{und} \quad \Delta_{A_i} = -1728c^2(c+1) \notin \mathfrak{P}$$

ist.
Es ist $j([1,i]) = 1728 \neq j(\mathfrak{a}_i)$ und $[1,i]$ ein Ideal in $\mathbb{Q}(\sqrt{-1})$. Wäre $j(\mathfrak{a}_i) \equiv 1728 \bmod \mathfrak{P}$, so dürfte nach Theorem 4.6.4 p in K nicht vollständig zerlegt sein. Also ist $j(\mathfrak{a}_i) \not\equiv 1728 \bmod \mathfrak{P}$. Das selbe Argument angewandt auf $j([1, e^{2\pi i/3}]) = 0$ und das Ideal $[1, e^{2\pi i/3}]$ von $\mathbb{Q}(\sqrt{-3})$ liefert, dass $j(\mathfrak{a}_i) \not\equiv 0 \bmod \mathfrak{P}$ ist.

2. Es sei $j(\mathfrak{a}_i) = 0$ oder 1728. Dann sind nach Prop. 4.0.8 durch $y^2 = x^3 + 1$ oder $y^2 = x^3 + x$ elliptische Kurven A_i oder A_i' mit den entsprechenden j-Invarianten gegeben, die wegen

$$\Delta_{A_i} = -16 \cdot 27 \neq 0 \quad \text{oder} \quad \Delta_{A_i'} = -16 \cdot 4 \neq 0$$

offensichtlich gute Reduktion bei $\mathfrak{P}$ besitzen. □

Wir können also *jede* durch eine Nullstelle der Klassengleichung $H_{\mathcal{O}_K}(X) = 0$ gewonnene elliptische Kurve für den Reduktionsprozess verwenden!

Sei A, die durch eine beliebige Nullstelle $j(\mathfrak{a})$ von $H_{\mathcal{O}_K}(X)$ gewonnene elliptische Kurve, durch die Gleichung $y^2 = x^3 + ax + b$ gegeben. Da $j(\mathfrak{a}) \in \mathcal{O}_{H_K}$ ist, sind o. B. d. A. a, $b \in H_K$. Die modulo $\mathfrak{P}$ reduzierte Kurve $\tilde{A}$ besitzt dann die Gleichung

$$y^2 = x^3 + \tilde{a}x + \tilde{b}$$

über $\mathcal{O}_{H_K}/\mathfrak{P} \simeq \mathbb{F}_{p^f}$, denn nach Theorem 4.6.3 ist $f_{\mathfrak{P}|p} = f$.
Hier ist $\tilde{a} \equiv a \bmod \mathfrak{P}$ und $\tilde{b} \equiv b \bmod \mathfrak{P}$, und für die j-Invariante von $\tilde{A}$ gilt nach Bemerkung 4.5.1

$$j(\tilde{A}) \equiv j(A) \bmod \mathfrak{P}.$$

Da die Nullstellen von $H_{\mathcal{O}_K}(X)$ im Allgemeinen keine ganzen, sondern nur algebraisch ganze Zahlen sind, werden auch die Koeffizienten der definierenden Gleichung von A im Allgemeinen keine ganzen Zahlen sein. Der Reduktionsprozess der Kurvengleichung von A würde also die Kenntnis des über p liegenden Primideals $\mathfrak{P}$ von H_K voraussetzen.
Dies ist jedoch nicht notwendig, denn wir erhalten $j(\tilde{A})$ als Nullstelle von $H_{\mathcal{O}_K}(X) \bmod \mathfrak{P}$, das heißt als Nullstellen von

$$H_{\mathcal{O}_K}(X) \in \mathbb{F}_p[X]$$

in $\mathbb{F}_q \simeq \mathcal{O}_{H_K}/\mathfrak{P}$, denn $H_{\mathcal{O}_K}(X)$ besitzt ganzzahlige Koeffizienten.
Diese Erkenntnis ist konform mit der Aussage von Theorem 1.1.4, dass $H_{\mathcal{O}_K}(X) \bmod p$ (es ist p vollständig zerlegt in K) in irreduzible Faktoren vom Grad $f = f_{\mathfrak{P}|p}$, also über $\mathbb{F}_{p^f} = \mathbb{F}_q$ in Linearfaktoren zerfällt.

Wir können also die j-Invariante $j(\tilde{A}) = \widetilde{j(A)}$ der gesuchten elliptischen Kurve bestimmen und dann die Kurvengleichung von $\tilde{A}$ gemäß Prop. 4.0.8 aufstellen. Damit haben wir jedoch wegen Prop. 4.3.5 noch keine elliptische Kurve gewonnen, die zu E über $\mathbb{F}_q$ isomorph ist, denn dies ist nur der Fall, wenn außerdem die Gruppenordnungen über $\mathbb{F}_q$ übereinstimmen, was uns ja maßgeblich interessiert.

Lassen wir den Konstruktionsprozess Revue passieren, so ist $\tilde{A}$ durch Reduktion einer elliptischen Kurve über H_K entstanden und $\tilde{A}$ besitzt *ein* Element π als Forbenius. Es muss jedoch nicht $\pi = \pi_E$ sein! Was wir sicher wissen ist, dass $N_{K/\mathbb{Q}}(\pi) = q$ gilt.

Lemma 5.1.3. *Sei $\mathcal{O}$ eine Ordung eines imaginär-quadratischen Zahlkörpers K und p^f eine Primpotenz, so dass p nicht $[\mathcal{O}_K : \mathcal{O}]$ teilt. p sei außerdem in K vollständig zerlegt. Sind π, $\pi_E \in \mathcal{O} - p\mathcal{O}$ mit $N_{K/\mathbb{Q}}(\pi) = p^f = N_{K/\mathbb{Q}}(\pi_E)$, so gilt*

$$\pi = \epsilon\pi_E \text{ oder } \pi = \epsilon\overline{\pi_E} \qquad \text{für ein} \qquad \epsilon \in \mathcal{O}^*.$$

$\overline{\pi_E}$ bezeichne das komplex Konjugierte von π_E.

Beweis. Seien π, $\pi_E \in \mathcal{O} - p\mathcal{O}$ wie oben gewählt, $N_{K/\mathbb{Q}}(\pi) = p^f = N_{K/\mathbb{Q}}(\pi_E)$. p ist nach Voraussetzung in die $\mathcal{O}$-Primideale $\mathfrak{q}$ und $\overline{\mathfrak{q}}$ zerlegt, $p = \mathfrak{q}\overline{\mathfrak{q}}$, denn die (vollständige) Zerlegung in $\mathcal{O}_K$ zieht die (vollständige) Zerlegung in $\mathcal{O}$ nach Prop. 1.5.4 nach sich. Es ist dann $(\pi)(\overline{\pi}) = \mathfrak{q}^f\overline{\mathfrak{q}}^f = (\pi_E)(\overline{\pi_E})$ die eindeutige Zerlegung von $(\pi)(\overline{\pi})$ und $(\pi_E)(\overline{\pi_E})$ in zum Führer teilerfremde $\mathcal{O}$-Primideale nach Kor. 1.5.5.
(π) besitzt ensprechend eine Zerlegung $(\pi) = \mathfrak{q}^s\overline{\mathfrak{q}}^t$ mit $s + t = f$, o. B. d. A. sei $s \geq t$. Dann ist $(\pi) = \mathfrak{q}^{s-t}(\mathfrak{q}\overline{\mathfrak{q}})^t = \mathfrak{q}^{s-t}p^t\mathcal{O}$, insbesondere also $\pi \in p^t\mathcal{O}$. Es folgt $t = 0$, denn $\pi \notin p\mathcal{O}$, und es ist $\mathfrak{q}^f = (\pi)$ ein Hauptideal. Ebenso folgert man für $\mathfrak{q}$, dass $(\pi_E) = \mathfrak{q}^f$ oder $(\overline{\pi_E}) = \mathfrak{q}^f$, also $(\pi) = (\pi_E)$ oder $(\pi) = (\overline{\pi_E})$ gilt. Damit ist alles klar. □

Für unsere reduzierte Kurve $\tilde{A}$ bedeutet Lemma 5.1.3, dass $\epsilon\pi_E$ oder $\epsilon\overline{\pi_E}$ für ein $\epsilon \in \mathcal{O}_K^*$ das Frobeniuselement von $\tilde{A}$ ist. Wir betrachten in Abhängigkeit der Einheitengruppe von $\mathcal{O}_K$ die verschiedenen Möglichkeiten für π[1]:

(i) Es ist $\mathcal{O}_K^* = \{\pm 1\}$ und deshalb $\pi \in \{\pm\pi_E, \pm\overline{\pi}_E\}$. Aus der Darstellung $\pi_E = \frac{\alpha+\beta\sqrt{D}}{2}$ folgt dann

$$\begin{aligned} Tr_{K/\mathbb{Q}}(\pi_E) = Tr_{K/\mathbb{Q}}(\overline{\pi_E}) &= \alpha, \\ Tr_{K/\mathbb{Q}}(-\pi_E) = Tr_{K/\mathbb{Q}}(-\overline{\pi_E}) &= -\alpha. \end{aligned}$$

Die erhaltene Kurve $\tilde{A}$ besitzt also eine Gruppenordnung $q + 1 - \alpha$ oder $q + 1 + \alpha$.

(ii) Es ist $\mathcal{O}_K^* = \{\pm 1, \pm i\}$ und deshalb $\pi \in \{\pm\pi_E, \pm i\pi_E, \pm\overline{\pi_E}, \pm i\overline{\pi_E}\}$. Lemma 1.3.4 zeigt, dass $\mathcal{O}_K = \mathbb{Z}[i]$ sein muss. Aus der spezialisierten Darstellung $\pi_E = \frac{\alpha}{2} + \beta i$ folgt dann

$$\begin{aligned} Tr_{K/\mathbb{Q}}(\pi_E) = Tr_{K/\mathbb{Q}}(\overline{\pi_E}) &= \alpha, \\ Tr_{K/\mathbb{Q}}(-\pi_E) = Tr_{K/\mathbb{Q}}(-\overline{\pi_E}) &= -\alpha, \\ Tr_{K/\mathbb{Q}}(i\pi_E) = Tr_{K/\mathbb{Q}}(i\overline{\pi_E}) &= -2\beta, \\ Tr_{K/\mathbb{Q}}(-i\pi_E) = Tr_{K/\mathbb{Q}}(-i\overline{\pi_E}) &= 2\beta. \end{aligned}$$

Die erhaltene Kurve $\tilde{A}$ besitzt also eine Gruppenordnung $q + 1 \pm \alpha$ oder $q + 1 \pm 2\beta$.

(iii) Es ist $\mathcal{O}_K^* = \{\pm 1, \pm\omega, \pm\omega^2\}$ für $\omega := (-1 + \sqrt{-3})/2$ und deshalb π oder $\overline{\pi}$ in $\{\pm\pi_E, \pm\omega\pi_E, \pm\omega^2\pi_E\}$. Lemma 1.3.4 zeigt, dass $\mathcal{O}_K = \mathbb{Z}[\omega]$ sein muss. Aus der spezialisierten Darstellung $\pi_E = \frac{\alpha+\beta\sqrt{-3}}{2}$ folgt dann

$$\begin{aligned} Tr_{K/\mathbb{Q}}(\pi_E) = Tr_{K/\mathbb{Q}}(\overline{\pi_E}) &= \alpha, \\ Tr_{K/\mathbb{Q}}(-\pi_E) = Tr_{K/\mathbb{Q}}(-\overline{\pi_E}) &= -\alpha, \\ Tr_{K/\mathbb{Q}}(\omega\pi_E) = Tr_{K/\mathbb{Q}}(\omega\overline{\pi_E}) &= \frac{-\alpha - 3\beta}{2}, \\ Tr_{K/\mathbb{Q}}(-\omega\pi_E) = Tr_{K/\mathbb{Q}}(-\omega\overline{\pi_E}) &= \frac{\alpha + 3\beta}{2}, \\ Tr_{K/\mathbb{Q}}(\omega^2\pi_E) = Tr_{K/\mathbb{Q}}(\omega^2\overline{\pi_E}) &= \frac{-\alpha + 3\beta}{2}, \\ Tr_{K/\mathbb{Q}}(-\omega^2\pi_E) = Tr_{K/\mathbb{Q}}(-\omega^2\overline{\pi_E}) &= \frac{\alpha - 3\beta}{2}. \end{aligned}$$

[1] Beschränken wir uns nicht auf Maximalordnungen $\mathcal{O}_K$ als Endomorphismenring, so folgt aus $\mathcal{O}^* \neq \{\pm 1\}$, dass $\mathcal{O} = \mathbb{Z}[i]$ oder $\mathcal{O} = \mathbb{Z}[\omega]$ sein muss. Unsere Fallbetrachtungen besitzen nach Lemma 1.3.4 also auch allgemeine Gültigkeit.

Die erhaltene Kurve $\tilde{A}$ besitzt also eine Gruppenordnung $q+1\pm\alpha$, $q+1\pm\frac{-\alpha-3\beta}{2}$ oder $q+1\pm\frac{-\alpha+3\beta}{2}$.

Wie sich nun zeigen wird, ist $\tilde{A}$ oder ein geeigneter Twist $\tilde{A}'$ von $\tilde{A}$ isomorph zu unserer gesuchten Kurve E. Wir unterscheiden anhand der j-Invarianten $j(\tilde{A})$, welche Twiste wir beachten müssen.

1) Ist $j(\tilde{A})\neq 0, 1728$, so ist auch $j(A)\neq 0, 1728$. Nach Bem. 3.4.6 muss deshalb $\mathcal{O}_K\neq\mathbb{Z}[i], \mathbb{Z}[\omega]$ sein und die Einheiten sind $\mathcal{O}_K^*=\{\pm 1\}$. Wir befinden uns also in Fall i) und die in Frage kommenden Gruppenordnungen für $\tilde{A}$ sind $p+1-\alpha$ und $p+1+\alpha$.
Ist die Gruppenordnung der gefundenen Kurve $\tilde{A}$ wie gewünscht $N=p+1-\alpha$, so haben wir unser Ziel erreicht. Besitzt die Kurve $\tilde{A}$ hingegen $N'=p+1+\alpha$ Punkte, dann besitzt ein quadratischer Twist $\tilde{A}'$ von $\tilde{A}$ nach Prop. 4.4.3 $N=p+1-\alpha$ Punkte. Es ist demnach $\tilde{A}$ oder $\tilde{A}'$ über $\mathbb{F}_q$ isomorph zu E. Indem wir für beliebige Punkte P auf $\tilde{A}$ und P' auf $\tilde{A}'$ das N-fache berechnen, können wir leicht feststellen, welcher Fall vorliegt.

In den verbleibenden beiden Fällen schlagen wir einen anderen Weg ein. Um diesen genauer erläutern zu können, benötigen wir das folgende Lemma.

Lemma 5.1.4. *Mit den Bezeichnungen aus dem Text gilt:*

(i) Es ist $\mathfrak{a}$ genau dann ein Hauptideal, wenn ein Element $\pi\in\mathfrak{a}$ mit $N_{K/\mathbb{Q}}(\pi)=N(\mathfrak{a})$ existiert.

(ii) Ist $\mathfrak{a}$ ein Hauptideal und $\pi_0\neq 0$ ein Element mininaler Norm in $\mathfrak{a}$, so ist $\mathfrak{a}=(\pi_0)$.

Beweis. (i) Ist $\mathfrak{a}=(\pi)$, so folgt mit Lemma 1.3.9 $N(\mathfrak{a})=N_{K/\mathbb{Q}}(\pi)$. Sei andererseits $\pi\in\mathfrak{a}$ ein Element mit gleicher Norm. Da $(\pi)\subseteq\mathfrak{a}$ gilt, folgt mit Kor. 1.0.6, dass $(\pi)=\mathfrak{b}\mathfrak{a}$ für ein $\mathcal{O}_K$-Ideal $\mathfrak{b}$ ist. Aus $N_{K/\mathbb{Q}}(\pi)=N(\mathfrak{a})N(\mathfrak{b})$ folgt $N(\mathfrak{b})=1$, also $\mathfrak{b}=\mathcal{O}_K$ und $(\pi)=\mathfrak{a}$.
(ii) Nach Voraussetzung ist $\mathfrak{a}=(\pi)$ ein Hauptideal und $N_{K/\mathbb{Q}}(\pi)=N(\mathfrak{a})$. Es ist dann $\pi_0=\zeta\pi$ das Element minimaler Norm und aus

$$N_{K/\mathbb{Q}}(\pi_0)=N_{K/\mathbb{Q}}(\zeta)N_{K/\mathbb{Q}}(\pi)\geq N_{K/\mathbb{Q}}(\zeta)N_{K/\mathbb{Q}}(\pi_0)=N_{K/\mathbb{Q}}(\zeta\pi_0)\geq N_{K/\mathbb{Q}}(\pi_0)$$

folgt $N_{K/\mathbb{Q}}(\zeta)=1$. Also ist $\zeta\in\mathcal{O}_K^*$ und $\mathfrak{a}=(\pi_0)$. □

2) Sei $j(\tilde{A})=1728$. Angenommen es ist $j(A)\neq 1728$. Da $j(\tilde{A})\equiv j(A) \bmod \mathfrak{P}$ nach Konstruktion und p in K vollständig zerlegt ist, erhalten wir mit Theorem 4.6.4 einen Widerspruch. Es muss also schon $j(A)=1728$ gelten und nach Bem. 3.4.6 deshalb $\mathcal{O}_K=\mathbb{Z}[i]$ sein. Die Einheiten sind $\mathcal{O}_K=\{\pm 1, \pm i\}$ und wir befinden uns in Fall ii).
Da $\mathbb{Z}[i]$ ein Hauptidealring ist, besteht die Klassengruppe aus nur einem Element, es gilt $K=H_K$ und insbesondere $f_{\mathfrak{P}|p}=1$, d. h. also $q=p$. Aus der Definition der j-Invarianten ist ersichtlich, dass wir eine Kurve der Gestalt $y^2=x^3+\tilde{a}x$ suchen.
Wir ermitteln zunächst den Frobenius π_E unserer Kurve, also das Element π_E mit $N_{K/\mathbb{Q}}(\pi_E)=p$ und $Tr_{K/\mathbb{Q}}(\pi_E)=p+1-N$. Mit Lemma 1.2.4 können wir die Zerlegung von p in $\mathbb{Z}[i]$ angeben. Es ist $p=\mathfrak{p}\overline{\mathfrak{p}}$, denn p ist vollständig zerlegt in K. Da $N(\mathfrak{p})=N(\overline{\mathfrak{p}})=p$ prim ist, ist $\mathfrak{p}$ ein primitives Ideal und besitzt deshalb die Darstellung $\mathfrak{p}=[p, i-r]$ mit einer Quadratwurzel ($r \bmod p$) von -1. Ein Erzeuger von $\mathfrak{p}$ ist nach Lemma 5.1.4 ein Element $\pi\in\mathfrak{p}$ mit minimaler Norm. Mit einem auf das Orthonormalisierungverfahren von Gram-Schmidt zurückgehenden Algorithmus kann ein Element minimaler Norm π in $\mathfrak{p}$ schnell berechnet werden (vgl. Bsp. 5.2.1 bzw. [17, Kapitel 4.2, S. 40]). π ist dann nach Lemma 5.1.3 zum Frobenius π_E assoziiert. Indem wir die Spur der vier zu π assoziierten Elemente berechnen, finden wir (bis auf komplexe Konjugation) den Frobenius $\pi_E=x+yi$ unserer Kurve.
Wir wollen Prop. 4.4.5 verwenden, um eine Kurve mit der gewünschten Anzahl an Punkten anzugeben. Dazu müssen wir das Element $\epsilon\in\mathbb{Z}[i]^*$ mit $\epsilon\pi_E=:\pi_0\equiv 1 \bmod (2+2i)$ kennen. Der Beweis von Lemma 4.4.4 ist konstruktiv, sodass wir $\epsilon=r+si$ ermitteln können.

Unmittelbar aus der Definition des quartischen Potenzrestes folgt, dass $(\frac{\alpha}{\pi_0})_4 = (\frac{\alpha}{\pi_E})_4$ für alle $\alpha \in \mathbb{Z}[i]$ gilt. Für ein $a \in \mathbb{Z} - p\mathbb{Z}$ besitzt die Kurve $y^2 = x^3 + \tilde{a}x$ nach Prop. 4.4.5 deshalb

$$p + 1 - \overline{\left(\frac{-a}{\pi_0}\right)}_4 \pi_0 - \left(\frac{-a}{\pi_0}\right)_4 \overline{\pi_0} = p + 1 - \overline{\left(\frac{-a}{\pi_E}\right)}_4 \epsilon\pi_E - \left(\frac{-a}{\pi_E}\right)_4 \overline{\epsilon\pi_E}$$

$\mathbb{F}_p$-rationale Punkte. Damit die gesuchte Kurve $N = p + 1 - \pi_E - \overline{\pi_E}$ Punkte besitzt, bestimmen wir a so, dass $\mathcal{A} := (-a)^{\frac{p-1}{4}} \equiv (\frac{-a}{\pi_E})_4 \equiv \epsilon \bmod \pi_E$ gilt. Dies ist äquivalent zu $\mathcal{A} - (r + si) = (u + vi)(x + yi)$ mit geeigneten u, $v \in \mathbb{Z}$, und führt auf

$$-s = xv + yu \tag{5.1.2}$$
$$\mathcal{A} = r + xu - yv. \tag{5.1.3}$$

Indem wir mit dem erweiterten Euklidischen Algorithmus (5.1.2) in u und v lösen und dann in (5.1.3) einsetzen, erhalten wir $\mathcal{A} \in \mathbb{Z}$. Wir wählen zufällige $a \in \mathbb{Z} - p\mathbb{Z}$ und testen, ob $(-a)^{\frac{p-1}{4}} \equiv \mathcal{A} \bmod p$ gilt. Ist dies der Fall, so gilt wegen $p = \pi_E\overline{\pi_E}$ auch $(-a)^{\frac{p-1}{4}} \equiv \mathcal{A} \bmod \pi_E$. Die Kurve $y^2 = x^3 + \tilde{a}x$ besitzt dann N $\mathbb{F}_q$-rationale Punkte und ist damit zu E isomorph.

3) Sei $j(\tilde{A}) = 0$. Analog schließen wir, dass $\mathcal{O}_K = \mathbb{Z}[\omega]$ sein muss. Die Einheiten sind $\mathcal{O}_K^* = \{\pm 1, \pm\omega, \pm\omega^2\}$ und wir befinden uns in Fall iii). Da $\mathbb{Z}[\omega]$ ein Hauptidealring ist, besteht die Klassengruppe aus nur einem Element, es gilt $K = H_K$ und insbesondere $f_{\mathfrak{P}|p} = 1$, d. h. also $q = p$. Aus der Definition der j-Invarianten ist hier ersichtlich, dass wir eine Kurve der Gestalt $y^2 = x^3 + \tilde{b}$ suchen.
Entsprechend den obigen Erläuterungen suchen wir zunächst den Frobenius $\pi_E = x + yi$ der Kurve. Wir wollen Prop. 4.4.7 verwenden, um eine Kurve mit der gewünschten Anzahl an Punkten anzugeben. Der Beweis von Lemma 4.4.6 ist konstruktiv, sodass wir zunächst das Element $\epsilon := r + s\omega \in \mathbb{Z}[\omega]^*$ mit $\pi_0 = \epsilon\pi_E \equiv 2 \bmod 3$ finden. Auch hier folgt aus der Definition des sextischen Potenzrestes, dass $(\frac{\alpha}{\pi_0})_6 = (\frac{\alpha}{\pi_E})_6$ für alle $\alpha \in \mathbb{Z}[\omega]$ gilt. Nach Prop. 4.4.7 besitzt für $b \in \mathbb{Z} - p\mathbb{Z}$ die durch $y^2 = x^3 + \tilde{b}$ gegebene elliptische Kurve

$$p + 1 + \overline{\left(\frac{4b}{\pi_0}\right)}_6 \pi_0 + \left(\frac{4D}{\pi_0}\right)_6 \overline{\pi_0} = p + 1 + \overline{\left(\frac{4b}{\pi_E}\right)}_6 \epsilon\pi_E + \left(\frac{4D}{\pi_E}\right)_6 \overline{\epsilon\pi_E}$$

$\mathbb{F}_q$-rationale Punkte. Damit die Kurve $N = p + 1 - \pi_E - \overline{\pi_E}$ Punkte besitzt, bestimmen wir b so, dass $\mathcal{C} := (4b)^{\frac{p-1}{6}} \equiv (\frac{4b}{\pi_E})_6 \equiv -\epsilon \bmod \pi_E$ gilt. Dies ist äquivalent zu $\mathcal{C} - (r + s\omega) = (u + v\omega)(x + y\omega)$ für geeignete u, $v \in \mathbb{Z}$, und führt auf

$$s = (x - y)v + yu \tag{5.1.4}$$
$$\mathcal{C} = -r + xu - yv. \tag{5.1.5}$$

Wir finden erneut mit dem erweiterten Euklidischen Algorithmus eine Lösung u und v von (5.1.4) und erhalten $\mathcal{C} \in \mathbb{Z}$ nach Einsetzen von u und v in (5.1.5). Wir wählen zufällige $c \in \mathbb{Z} - p\mathbb{Z}$, bis $c^{\frac{p-1}{6}} \equiv \mathcal{C} \bmod p$ gilt. Ist dies der Fall, so ermitteln wir $b \equiv 4^{-1}c \bmod p$. Wegen $p = \pi_E\overline{\pi_E}$ gilt auch $(4b)^{\frac{p-1}{6}} \equiv (c)^{\frac{p-1}{6}} \equiv \mathcal{C} \bmod \pi_E$. Die Kurve $y^2 = x^3 + \tilde{b}$ besitzt dann N $\mathbb{F}_q$-rationale Punkte und ist damit zu E isomorph.

Nachdem das Konstruktionverfahren nun detailiert dargestellt wurde, ist es Zeit für praktische Bespiele.

Beispiel 5.1.5. Wir wollen eine elliptische Kurve E mit $N = 19$ Punkten über $\mathbb{F}_q$, $q = p^2 = 25$, konstruieren.
Die Spur des Frobenius ist $a = q + 1 - N = 25 + 1 - 19 = 7$. Weil $ggT(a, p) = ggT(7, 5) = 1$ gilt, garantiert Thm. 4.3.6 die Existenz einer solchen Kurve, die nach Prop. 4.3.3 ordinär ist. Der Endomorphismenring ist eine Ordnung im Körper $K = \mathbb{Q}(\sqrt{D})$ mit $D = (q+1-N)^2 - 4q = -51$. D ist quadratfrei und ist deshalb die Diskriminante der Maximalordnung $\mathcal{O}_K$ von K, d.h. es ist $End(E) \simeq \mathcal{O}_K$. Das Klassenpolynom $H_{-51}(X)$ kennen wir aus Bsp. 3.4.5. Modulo 5 reduziert sich dies zu

$$H_{-51}(X) \equiv X^2 + 3X + 3 \bmod 5.$$

Über $\mathbb{F}_5$ ist $H_{-51}(X)$ irreduzibel und wir suchen eine Nullstelle in $\mathbb{F}_{25}$. Wir stellen

$$\mathbb{F}_{25} \simeq \mathbb{F}_5[X]/\left\langle X^2 + X + 2 \right\rangle \simeq \mathbb{F}_5[\alpha]$$

mit einer Nullstelle α von $f(X) = X^2 + X + 2$ dar. α besitzt Ordnung 24 in $\mathbb{F}_{25}^*$ und ist somit ein erzeugendes Element. In der folgenden Tabelle sind alle Elemente von $\mathbb{F}_{25}^*$ als Potenzen von α dargestellt. Für den späteren Gebrauch sind in der rechten Spalte alle Quadratwurzeln des Elements angegeben, falls diese existieren.

α-Potenz	mod $f(\alpha)$	Quadratwurzel
	0	0
α^0	1	α^0, α^{12}
α^6	2	α^3, α^{15}
α^{18}	3	α^9, α^{21}
α^{12}	4	α^6, α^{18}
α^1	α	
α^{17}	$\alpha + 1$	
α^{14}	$\alpha + 2$	α^7, α^{19}
α^{15}	$\alpha + 3$	
α^{10}	$\alpha + 4$	α^5, α^{17}
α^7	2α	
α^{21}	$2\alpha + 1$	
α^{23}	$2\alpha + 2$	
α^{16}	$2\alpha + 3$	α^8, α^{20}
α^{20}	$2\alpha + 4$	α^{10}, α^{22}
α^{19}	3α	
α^8	$3\alpha + 1$	α^4, α^{16}
α^4	$3\alpha + 2$	α^2, α^{14}
α^{11}	$3\alpha + 3$	
α^9	$3\alpha + 4$	
α^{13}	4α	
α^{22}	$4\alpha + 1$	α^{11}, α^{23}
α^3	$4\alpha + 2$	
α^2	$4\alpha + 3$	α, α^{13}
α^5	$4\alpha + 4$	

Es ist genau dann $X^2 + 3X + 3 \equiv 0 \bmod 5$, wenn $(X + 4)^2 \equiv 3 \bmod 5$ gilt, wie man ohne Schwierigkeiten sieht. Eine Nullstelle von $H_{-51}(X)$ in $\mathbb{F}_{25}$, welche wir als j-Invariante unserer gesuchten Kurve wählen, ist deshalb

$$j_0 \equiv 1 + \sqrt{3} \equiv 1 + \alpha^9 \equiv 3\alpha \equiv \alpha^{19} \bmod \alpha^2 + \alpha + 2.$$

Es ist $j_0 \not\equiv 0, 1728 \bmod \alpha^2 + \alpha + 2$ und wir stellen die Kurvengleichung mit Hilfe von Prop. 4.0.8 auf. Wir berechnen

$$1728 - j_0 \equiv 3 + 2\alpha \equiv \alpha^{16} \bmod \alpha^2 + \alpha + 2,$$

und finden $c \equiv \frac{j_0}{1728-j_0} \equiv \alpha^3 \bmod \alpha^2+\alpha+2$. Eine Kurvengleichung von $\tilde{A}$ ist dann durch $y^2 = x^3 + 3cx + 2c$, also durch

$$y^2 = x^3 + \alpha^{21}x + \alpha^9$$

gegeben. Wir bestimmen außerdem einen quadratischen Twist. Es ist α ein Nichtquadrat in $\mathbb{F}_{25}$. Ein quadratischer Twist $\tilde{A}'$ von $\tilde{A}$ ist dann durch

$$y^2 = x^3 + \alpha^{23}x + \alpha^{12}$$

gegeben. Wir bestimmen die Anzahl der Punkte von $\tilde{A}$ und $\tilde{A}'$, indem wir alle Körperelemente für x einsetzen:

Anzahl y	$x^3+\alpha^{21}x+\alpha^9$	x	$x^3+\alpha^{23}x+\alpha^{12}$	Anzahl y
	$3\alpha+4$	0	4	2
2	1	α^0	$2\alpha+2$	
2	$\alpha+2$	α^1	$4\alpha+2$	
2	3	α^2	$\alpha+1$	
2	$\alpha+4$	α^3	$2\alpha+1$	
2	$4\alpha+3$	α^4	4α	
	3α	α^5	$4\alpha+4$	
2	$2\alpha+4$	α^6	$4\alpha+1$	2
2	$3\alpha+2$	α^7	$2\alpha+2$	
2	$2\alpha+4$	α^8	2α	
2	$2\alpha+3$	α^9	$2\alpha+2$	
2	1	α^{10}	3α	
	$4\alpha+4$	α^{11}	$4\alpha+2$	
2	$\alpha+2$	α^{12}	$3\alpha+1$	2
2	1	α^{13}	$\alpha+1$	
	α	α^{14}	$4\alpha+2$	
2	4	α^{15}	$3\alpha+2$	2
	2α	α^{16}	$\alpha+3$	
	$3\alpha+3$	α^{17}	$\alpha+4$	2
	$4\alpha+4$	α^{18}	$\alpha+2$	2
2	$3\alpha+1$	α^{19}	$3\alpha+1$	2
	$4\alpha+4$	α^{20}	$3\alpha+3$	
	4α	α^{21}	$3\alpha+1$	2
2	$\alpha+2$	α^{22}	$2\alpha+3$	2
2	$2\alpha+4$	α^{23}	$\alpha+1$	
32	Summe			18

Zählen wir den Fernpunkt hinzu, so besitzt $\tilde{A}$ genau 33 $\mathbb{F}_{25}$-rationale Punkte, der Twist $\tilde{A}'$ hingegen 19 $\mathbb{F}_{25}$-rationale Punkte, und ist somit die von uns gesuchte Kurve $E \simeq \tilde{A}'$.

Da die Darstellung von endlichen Körpern $\mathbb{F}_{p^n}$ für $n > 1$ mühsam ist, beschränken wir uns in den folgenden Beispielen auf Primkörper.

Beispiel 5.1.6. (i) Wir wollen eine elliptische Kurve mit $N = 36$ Punkten über $\mathbb{F}_{37}$ konstruieren. Der Endomorphismenring ist eine Ordnung im Körper $K = \mathbb{Q}(\sqrt{D})$ mit

$$D = (p+1-N)^2 - 4p = -144 = (2\cdot 3)^2(-4).$$

Es muss deshalb $d_K = -4$ die Diskriminante von K und folglich $K = \mathbb{Q}(\sqrt{-1})$ sein. Wir wählen also die Maximalordnung $\mathcal{O}_K = \mathbb{Z}[i]$ von K als Endomorphismenring. Da dies ein Hauptidealring

ist, besitzt das Klassenpolynom Grad eins. Nach Bsp. 3.4.5.(i) ergibt sich dies zu

$$H_{-4}(X) = X - 1728.$$

Es ist also $1728 \equiv 26 \bmod 37$ die Nullstelle, welche wir als j-Invariante der gesuchten Kurve wählen. Da wir $\mathbb{Z}[i]$ als Endomorphismenring verwenden, müssen wir quartische Twiste betrachten.
Der Frobenius unserer Kurve ist $\pi_E = 1 + 6i$, denn es gilt

$$N_{K/\mathbb{Q}}(\pi_E) = (1+6i)(1-6i) = 37 = N \qquad \text{und} \qquad Tr_{K/\mathbb{Q}}(\pi_E) = (1+6i)+(1-6i) = 2 = p+1-N.$$

Entsprechend Lemma 4.4.4 suchen wir das eindeutig bestimmte Element π_0 mit $N_{K/\mathbb{Q}}(\pi_0) = 37$ und $\pi_0 \equiv 1 \bmod (2+2i)$, bzw. die Einheit $\epsilon := r + si \in \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ mit $\pi_0 = \epsilon \pi_E$.
Da $Im(\pi_E)$ gerade ist, folgt $s = 0$ und dann $r \equiv (1-6) \equiv -1 \bmod 4$. Es ist also $\epsilon = -1 + 0 \cdot i$ und deshalb $\pi_0 = -\pi_E = -1 - 6i$. Wir lösen die Gleichung

$$0 = 1 \cdot v + 6 \cdot u$$

in den Unbestimmten u und v. Das Lösungspaar $(u, v) = (0, 0)$ setzen wir in

$$\mathcal{A} = -1 + 1 \cdot u - 6 \cdot v$$

ein und erhalten $\mathcal{A} = -1 \equiv 36 \bmod 37$. Durch Ausprobieren finden wir, dass $(-9)^{\frac{37-1}{4}} \equiv 36 \bmod 37$ ist. Deshalb besitzt die durch

$$y^2 = x^3 + 9x$$

gegebene Kurve wie gewünscht über $\mathbb{F}_{37}$ 36 Punkte.

(ii) Wir wollen eine elliptische Kurve mit $N = 188$ Punkten über $\mathbb{F}_{173}$ konstruieren.
Es ist demnach $K = \mathbb{Q}(\sqrt{D})$ mit $D = (173 + 1 - 188)^2 - 4 \cdot 173 = 2^4 \cdot (-31)$. Da $-31 \equiv 1 \bmod 4$ und quadratfrei ist, gilt $d_K = -31$. Wir wählen wieder $\mathcal{O}_K$ als Endomorphismenring. Das Klassenpolynom ist uns aus Bsp. 3.4.5 bekannt:

$$H_{-31}(X) = X^3 + 39491307 * X^2 - 58682638134 * X + 1566028350940383$$

Über $\mathbb{F}_{173}$ zerfällt $H_{-31}(X)$ in Linearfaktoren:

$$H_{-31}(X) \equiv (X - 58)(X - 79)(X - 131) \bmod 173.$$

Wir wählen $j_0 = 58$ als j-Invariante unserer Kurve. Da $j_0 \not\equiv 0, 1728 \bmod 173$ ist, können wir eine Kurvengleichung mit Prop. 4.0.8 aufstellen. Gemäß den dortigen Bezeichnungen setzen wir $c \equiv j_0/(1728 - j_0) \equiv 58/1670 \equiv 74 \bmod 173$ Die Kurvengleichung von $\tilde{A}$ ist dann

$$y^2 \equiv x^3 + 3cx + 2c \equiv x^3 + 49x + 148 \bmod 173.$$

Es ist 2 ein Nichtquadrat modulo 173, denn nach dem quadratischen Reziprozitätsgesetz ist $\left(\frac{2}{173}\right) = (-1)^{(173^2-1)/8} = -1$. Ein quadratischer Twist $\tilde{A}'$ von $\tilde{A}$ ist deshalb durch

$$y^2 \equiv x^3 + 2^2 \cdot 49x + 2^3 \cdot 148 \equiv x^3 + 23x + 146 \bmod 173$$

gegeben. Wir finden zufällig die Punkte $P = [134, 81]$ auf $\tilde{A}$ und $Q = [93, 17]$ auf $\tilde{A}'$. Um die richtige Kurve auszuwählen, berechnen wir das N-fache von P und Q. Es ergibt sich

$$N \cdot P = [52, 135] \qquad \text{und} \qquad N \cdot Q = O_{\tilde{A}'}.$$

Deshalb besitzt der quadratische Twist $\tilde{A}'$ wie gewünscht 188 Punkte über $\mathbb{F}_{173}$.

(iii) Wir wollen eine Kurve mit $N = 2007$ Punkten konstruieren.
Wählen wir $p = \text{nextprime}(N + 1 - 2\sqrt{N}) = 1931$, so erhalten wir $D = (p+1-N)^2 - 4p = -2099$. Es ist 2099 prim und $-2099 \equiv 1 \bmod 4$, sodass $D = d_K$ die Diskriminante einer Maximalordnung sein muss, denn als Führer kommt nur $f = 1$ in Betracht. Es ist also $\mathcal{O}_D = \mathcal{O}_K$ der Ganzheitsring von $K = \mathbb{Q}(\sqrt{-2099})$. Ein vollständiges Vertretersystem der Ideaklassen von $\mathcal{O}_K$ ist nach Thm. 1.4.8 und Thm. 1.4.11 durch

$$\left\{ [a, (-b + \sqrt{d_K})/2] \;\middle|\; \text{mit } b^2 - 4ac = d_K,\ |b| \le a \le c \text{ und } b \ge 0 \text{ falls } |b| = a \text{ oder } c = a \right\}$$

gegeben. Wir finden für a, b, $c \in \mathbb{Z}$ die folgenden 19 möglichen Werte:

a	b	c
21	±1	25
21	±13	27
17	±3	31
15	±1	35
15	±11	37
9	±5	59
7	±1	75
5	±1	105
3	±1	175
1	1	525

Die Klassenzahl beträgt also 19, insbesondere besitzt das Klassenpolynom Grad 19. Es berechnet sich zu:

$$\begin{aligned} H_{-2099}(X) &= X^{19} + c_{63}X^{18} + c_{83}X^{17} + c_{104}X^{16} + c_{117}X^{15} + c_{129}X^{14} + c_{138}X^{13} \\ &+ c_{147}X^{12} + c_{154}X^{11} + c_{161}X^{10} + c_{165}X^9 + c_{169}X^8 + c_{173}X^7 \\ &+ c_{178}X^6 + c_{182}X^5 + c_{186}X^4 + c_{189}X^3 + c_{192}X^2 + c_{195}X^1 \\ &+ (2^{102} \cdot 11^9 \cdot 23^3 \cdot 29^2 \cdot 53^2 \cdot 89^2 \cdot 113 \cdot 131^2 \cdot 317 \cdot 383)^3 \end{aligned}$$

Hierbei bezeichnet c_i eine zusammengesetzte i-stellige Zahl. Dass das konstante Glied eine Dreierpotenz ist, ist übrigens nicht zufällig, sondern stets der Fall (siehe [3, § 12]). (Dies kann zur Überprüfung von Rundungsfehlern bei der Berechnung von $H_D(X)$ verwendet werden.) Modulo 1931 zerfällt $H_{-2099}(X)$ in Linearfaktoren:

$$\begin{aligned} H_{-2099}(X) \equiv\ & (X - 241) * (X - 368) * (X - 390) * (X - 416) * (X - 590) * (X - 643) * \\ & (X - 651) * (X - 840) * (X - 862) * (X - 961) * (X - 1091) * (X - 1317) * \\ & (X - 1384) * (X - 1461) * (X - 1467) * (X - 1506) * (X - 1524) * (X - 1538) * \\ & (X - 1851) \bmod 1931 \end{aligned}$$

Wir wählen die erste Nullstelle $j_0 \equiv 241 \bmod 1931$ als j-Invariante der gesuchten Kurve. Es ist $j_0 \not\equiv 0, 1728 \bmod 1931$ und wir müssen folglich nur quadratische Twiste betrachten.
Um die Kurvengleichung aufzustellen verwenden wir Prop. 4.0.8. Mit den dortigen Bezeichnungen setzen wir $c = j_0/(1728 - j_0) = 241/1487 \equiv 517 \bmod 1931$ Die Kurvengleichung von $\tilde{A}$ ist dann

$$y^2 \equiv x^3 + 3cx + 2c \equiv x^3 + 1551x + 1034 \bmod 1931.$$

Wir finden das Nichtquadrat (2 mod 1931), denn es ist nach dem quadratischen Reziprozitätsgesetzt $\left(\frac{2}{1931}\right) = (-1)^{(1931^2-1)/8} = -1$. Setzt man $a' = 1551 \cdot 2^2 \equiv 411 \bmod 1931$ und $b' = 1034 \cdot 2^3 \equiv 548 \bmod 1931$, so ist ein Twist $\tilde{A}'$ von $\tilde{A}$ durch die Gleichung $y^2 = x^3 + a'x + b'$, also durch

$$y^2 = x^3 + 411x + 548$$

gegeben.
Wir suchen zufällig Punkte auf den Kurven und finden $P = [1899, 362]$ auf $\tilde{A}$ und $Q = [850, 894]$ auf $\tilde{A}'$. Wir berechnen das N-fache und finden $N \cdot P = O_{\tilde{A}}$ und $N \cdot Q = [554, 1133] \neq O_{\tilde{A}'}$. Es ist also $\tilde{A}$ die gesuchte Kurve.

Wie aus dem letzten Beispiel ersichtlich ist, besitzt das Klassenpolynom für große Grade sehr große Koeffizienten. Dies stellt bei der computergestützten Berechnung ein Problem dar, denn es muss mit einer entsprechenden Genauigkeit gerechnet werden. Die Klassenzahl, welche mit dem Grad des Klassenpolynoms übereinstimmt, wird von der Diskriminante des Zahlkörpers K beeinflusst, wie man unmittelbar aus Bem. 1.4.9 abliest. Es ist daher zu erwarten, dass bei großer Diskriminante d_K, die Klassenzahl groß, und damit das Klassenpolynom schwer zu berechnen ist. Im folgenden Abschnitt 5.2 wird ein Weg vorgestellt, wie diesem Problem begegnet werden kann.

5.2 Konstruktion elliptischer Kurven bei freier Primkörperwahl

Im Folgenden wird das in dem Artikel "Constructing elliptic curves in almost polynomial time„ von R. Bröker und P. Stevenhagen [15] beschriebene Konstruktionsverfahren dargestellt.

Wollen wir mit der CM-Konstruktionsmethode zu vorgegebenem $p \geq 5$ und N eine elliptische Kurve E über dem endlichen Körper $\mathbb{F}_p$ mit $\#E(\mathbb{F}_p) = N$ Punkten konstruieren, so haben wir keinen Einfluss auf die Größe

$$\Delta := \Delta(p, N) = (p + 1 - N)^2 - 4p = (N + 1 - p)^2 - 4N.$$

Die wesentliche Arbeit besteht in der Aufstellung des Klassenpolynoms der Maximalordnung des Körpers $K = \mathbb{Q}(\sqrt{\Delta})$, dessen Grad mit der Klassenzahl h_K von K übereinstimmt. Annähernd gilt hier

$$h_K \approx |d_K|^{1/2}.$$

Der Zusammenhang zwischen Δ und d_K ist durch den Führer f der Ordnung $\mathcal{O}_\Delta$ gegeben. Es ist $\Delta = f^2 d_K$ und d_K enthält maximal einen quadratischen Faktor von 4. Da wir nach Bemerkung 5.1.1 $\mathcal{O}_K$ als Endomorphismenring wählen können, ist die Idee nun, bei vorgegebenem N eine Primzahl p zu finden, sodass

$$\Delta(p) = (N + 1 - p)^2 - 4N = f^2 \cdot d_K \qquad \text{mit } f, d_K \in \mathbb{Z}$$

für eine betraglich möglichst kleine Diskriminante $d_K < 0$ gilt. Analog versuchen wir die Gleichung

$$x^2 - f^2 d_K = 4N$$

für eine betraglich möglichst kleine Diskriminante $d_K < 0$ so zu lösen, sodass $p = N + 1 - x$ prim ist. Dies führt auf das folgende

Problem. Sei $N \geq 1$ fest gewählt. Suche ein $d \geq 1$ und ein algebraisch ganzes Element α in $K = \mathbb{Q}(\sqrt{-d})$, so dass gilt:

(i) $N_{K/\mathbb{Q}}(\alpha) = N$.

(ii) $N_{K/\mathbb{Q}}(1 - \alpha) = N + 1 - Tr_{K/\mathbb{Q}}(\alpha)$ ist prim.

Sind α und d gefunden, so betrachten wir das Element $(1 - \alpha)$ als Frobenius der gesuchten elliptischen Kurve. Da $p = N_{K/\mathbb{Q}}(1 - \alpha) = (1 - \alpha)\overline{(1 - \alpha)}$ in das Produkt zweier Hauptideale zerfällt, ist p vollständig zerlegt in K. Nach Korollar 2.3.9 ist das Primideal $(1 - \alpha)$ im Hilbert Klassenkörper H_K vollständig zerlegt. Für ein über p liegendes Primideal $\mathfrak{P}$ von H_K gilt dann $f_{\mathfrak{P}|p} = 1$. Da wir nach Lemma 5.1.2 eine elliptische Kurve mit guter Reduktion bei $\mathfrak{P}$ und Endomorphismenring $\mathcal{O}_K$ finden können, garantiert uns das Theorem von Deuring 4.6.3 die Existenz einer elliptischen Kurve E über $\mathbb{F}_p$ mit N Punkten und $End(E) \simeq \mathcal{O}_K$. Diese kann mit Hilfe der im vorigen Abschnitt 5.1 beschriebenen CM-Methode konstruiert werden.

Definieren wir für beliebige Zahlen $n \in \mathbb{N}$ das Hasse-Intervall

$$\mathcal{H}_n := [n + 1 - 2\sqrt{n}, n + 1 + 2\sqrt{n}\,],$$

so gilt für die Zahlen p und N die Beziehung

$$N \in \mathcal{H}_p \quad \Longleftrightarrow \quad p \in \mathcal{H}_N.$$

Unser Ansatz setzt also voraus, dass zu beliebig vorgegebener Zahl N eine Primzahl p im Intervall $\mathcal{H}_N$ der Größe $4\sqrt{N}$ zu finden ist. Dies kann zwar aus theoretischer Sicht nicht garantiert werden, ist aber in der Praxis immer der Fall.

Der Algorithmus gliedert sich dann in folgende Schritte.

Für wachsende quadratfreie $d \in \mathbb{N}$:

(1) suche ein Ideal in $\mathbb{Q}(\sqrt{-d})$ mit Norm N.
(2) prüfe, ob dies ein Hauptideal ist und finde einen Erzeuger π.
(3) teste, ob $N_{K/\mathbb{Q}}(1-\pi)$ prim ist.

Ist ein Schritt nicht erfolgreich abzuschließen, so wähle das nächste d. Sind alle Bedingungen erfüllt, so konstruiere die elliptische Kurve mit der CM-Methode.

Dieses Verfahren liefert ein betraglich minimales d und ein $\alpha \in \mathcal{O}_K$ für $K = \mathbb{Q}(\sqrt{-d})$, mit denen eine elliptische Kurve mit N Punkten konstruiert werden kann. Wir erläutern die einzelnen Schritte näher.

(1) Wir suchen Ideale in $K = \mathbb{Q}(\sqrt{-d})$ mit Norm N und schreiben den Ganzheitsring $\mathcal{O}_K$ entsprechend Abschnitt 1.2 als $\mathbb{Z}[\omega]$, wobei $\omega = \omega_d$ eine Nullstelle von

$$f(X) = \begin{cases} X^2 - X + \frac{1+d}{4} & \text{für } -d \equiv 1 \bmod 4 \\ X^2 + d & \text{sonst} \end{cases}$$

ist. Jedes Ideal $\mathfrak{a}$ mit Norm N besitzt eine eindeutige Darstellung als $\mathfrak{a} = k \cdot \mathfrak{a}'$ mit $k \in \mathbb{N}$ und einem primitiven Ideal $\mathfrak{a}'$ von K (vgl. Bezeichnug 1.2.4). Wir suchen deshalb für alle $k \in \mathbb{N}$ mit $k^2 | N$ zunächst primitive Ideale $\mathfrak{a}'$ mit Norm $N_0 := N/k^2$. Ist ein solches primitives Ideal $\mathfrak{a}'$ gefunden, so setzen wir $\mathfrak{a} = k\mathfrak{a}'$ und haben ein Ideal mit Norm N gefunden.
Die Gestalt von primitiven Idealen mit Norm N_0 kann nach Lemma 1.2.5 explizit angegeben werden:

$$\mathfrak{a}' \text{ ist primitiv mit } N(\mathfrak{a}') = N_0 \quad \Longleftrightarrow \quad \begin{array}{c} \mathfrak{a}' = [N_0, \omega - r] \text{ für ein } r \in \mathbb{Z} \\ \text{mit } f(r) \equiv 0 \bmod N_0. \end{array}$$

Das Auffinden von primitiven Idealen läuft also auf das Lösen der quadratischen Gleichung $f(X) \equiv 0$ modulo allen Primteilern von N_0 hinaus. Mit Hilfe des chinesischen Restesatzes können die Lösungen dann zu Lösungen modulo N_0 angehoben werden.
Bei der Bestimmung von N_0 ist nach Lemma A.0.9 für Primzahlen $q \in \mathbb{N}$ zu beachten:

(a) Gilt $q | N_0$ und q ist prim in $\mathcal{O}_K$ (d. h. $\left(\frac{-d}{q}\right) = -1$), so besitzt $f(X) \equiv 0 \bmod N_0$ keine Lösungen.
(b) Gilt $q^2 | N_0$ und q ist verzweigt in $\mathcal{O}_K$ (d. h. $\left(\frac{-d}{q}\right) = 0$), so besitzt $f(X) \equiv 0 \bmod N_0$ keine Lösungen.

Wir ermitteln also für jeden Primteiler q von N, ob $(-d/q) = -1$ bzw. $(-d/q) = 0$ gilt. Ist dies der Fall, so wählen wir wenn möglich k so, dass q bzw. q^2 kein Teiler von $N_0 = N/k^2$ ist.

(2) Wir suchen einen Erzeuger π des in Schritt (1) gefundenen Ideals $\mathfrak{a}$, falls dieser existiert. Um einen Erzeuger von $\mathfrak{a}$ zu finden, suchen wir entsprechend Lemma 5.1.4 ein Element minimaler Norm in $\mathfrak{a}$ und testen, ob die Normen übereinstimmen. Ist dies der Fall, so ist $\mathfrak{a}$ ein Hauptideal, sonst nicht.
Das Auffinden eines Elements minimaler Norm kann mit einem auf das Orthonormalisierungsverfahren von Gram-Schmidt zurückgehenden Algorithmus gelöst werden (vgl. Bsp. 5.2.1 bzw. [17, Kapitel 4.2, S. 40]).
(3) Mit π sind auch alle zu π assoziierten Elemente $\zeta\pi$ mit $\zeta \in \mathcal{O}_K^*$ Erzeuger des Ideals $\mathfrak{a}$. Wir prüften also, ob $p = N_{K/\mathbb{Q}}(1-\zeta\pi)$ für ein $\zeta \in \mathcal{O}_K^*$ prim ist. Da dies im Allgemeinen nicht der Fall sein wird, prüfen wir zuerst mit Hilfe eines probabilistischen Primzahltests (etwa Miller-Rabin-Primzahltest). Besteht p diesen, kann mit einem deterministischen Primzahltest die Primalität nachgewiesen werden.

Wir stellen den Algorithmus in Pseudo-Code vor. Als Eingabe wird die faktorisierte Zahl $N = \prod_{i=1}^{n} p_i^{e_i}$ erwartet. Ausgegeben wird ein Lösungspaar (d, α) des Problems von Seite 64.

1. Setze $d \leftarrow 1$

2. Ist d nicht quadratfrei, so setze $d \leftarrow d+1$ und gehe zu Schritt 2. Ist d quadratfrei, so definiere $K = \mathbb{Q}(\sqrt{-d})$, ω_K und f_K.

3. Ermittle das Verzweigungsverhalten aller Primteiler p_i von N in $\mathbb{Z}[\omega]$. Setze $k_1 = 1$.

3a. Für jeden Primteiler p_i von N mit $\left(\frac{-d}{p_i}\right) = -1$ setze

$$k_1 \leftarrow k_1 p_i^{\lfloor e_i/2 \rfloor},$$

wenn e_i gerade ist. Ist e_i ungerade, so setze $d \leftarrow d+1$ und gehe zu Schritt 2.

3b. Für jeden Primteiler p_i von N mit $\left(\frac{-d}{p_i}\right) = 0$ setze

$$k_1 \leftarrow k_1 p_i^{\lfloor e_i/2 \rfloor}.$$

4. Setze $N_1 \leftarrow N/k_1^2$. Für jede Nullstelle $r \bmod N_1$ von f_K und jeden quadratischen Teiler k_2^2 von N_1:

4a. Setze $k \leftarrow k_1 k_2$ und $N_0 \leftarrow N/k^2 = N_1/k_2^2$. Suche einen Erzeuger von $[N_0, \omega - r] \subset \mathbb{Z}[\omega]$, falls dieser existiert.

4b. Ist ein Erzeuger π gefunden worden, teste für alle zu π assoziierten Elemente $\zeta\pi$ mit $\zeta \in \mathcal{O}_K^*$, ob $N_{K/\mathbb{Q}}(1 - k\zeta\pi)$ prim ist. Ist dies der Fall, so gib $(d, k\zeta\pi)$ zurück und terminiere.

5. Setze $d \leftarrow d+1$ und gehe zu Schritt 2.

Bemerkung. Die Wahl von k_1 in Schritt 3 wird entsprechend Lemma A.0.9 vorgenommen.
In Schritt 4 suchen wir die primitiven Ideale mit Norm N_0. Dazu wird nach den obigen Erläuterungen eine Lösung r von $f_K(X) \equiv 0 \bmod N_0$ benötigt. In Schritt 4 berechnet man *einmal* alle Lösungen von $f_K(X) \equiv 0 \bmod N_1$ und hat damit sofort alle Lösungen von $f_K(X) \equiv 0 \bmod N_0$ für *alle* N_0, denn $N_0 | N_1$.

Abschließend geben wir auch für die Konstruktion elliptischer Kurven bei freier Primkörperwahl Beispiele an.

Beispiel 5.2.1. (i) Wir haben in Bsp. 5.1.6 eine elliptische Kurve mit 2007 Punkten über $\mathbb{F}_{1931}$ konstruiert. Dabei mussten wir das Klassenpolynom $H_{-2099}(X)$ mit Grad 19 bestimmen. In diesem Beispiel wollen wir das Verfahren von Bröker und Stevenhagen verwenden, um eine Kurve mit $N = 2007 = 3^2 \cdot 223$ Punkten zu konstruieren.
Wir setzen im ersten Schritt $d = 1$. Es ist dann $K = \mathbb{Q}(\sqrt{-1})$ mit Diskriminante $d_K = -4$ und $\mathcal{O}_K = \mathbb{Z}[i]$. Die Primteiler von N sind 3 und 223 und wir ermitteln ihr Verzweigungsverhalten in $\mathbb{Z}[i]$. Nach dem quadratischen Reziprozitätsgesetzt gilt

$$\left(\frac{d_K}{223}\right) = \left(\frac{-d}{223}\right) = \left(\frac{-1}{223}\right) = (-1)^{\frac{223-1}{2}} = -1.$$

Nach Prop. 1.2.2 ist also 223 prim in $\mathbb{Z}[i]$. Da 223 mit einer ungeraden Potenz in N aufgeht, wählen wir das nächste d.
Auch für $d = 2$ ist $\left(\frac{-2}{223}\right) = -1$ und wir wählen $d = 3$. Es ist dann $K = \mathbb{Q}(\sqrt{-3})$ mit Diskriminante $d_K = -3$ und $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-3})/2]$. Hier ist

$$f_K(X) = X^2 - X + 1 \qquad \text{und} \qquad \omega_K = \frac{1+\sqrt{-3}}{2}.$$

Das Verzweigungsverhalten stellt kein Problem dar, denn es gilt

$$\left(\frac{-3}{3}\right) = 0 \qquad \text{und} \qquad \left(\frac{-3}{223}\right) = (-1)^{\frac{223-1}{2}} \left(\frac{3}{223}\right) = -(-1)^{\frac{223-1}{2}\frac{3-1}{2}} \left(\frac{1}{3}\right) = 1.$$

Wir setzen also $k_1 = 3$, $N_1 = N/k_1^2 = 223$ und folglich $k = 3$ und $N_0 = 223$, denn N_1 ist prim. Die Nullstellen von $f_K(X)$ mod 223 sind 486 und 630. Deshalb ist $\mathfrak{a} = [223, \omega_K - 486]$ ein primitives Ideal mit Norm 223. Wir testen, ob $\mathfrak{a}$ ein Hauptideal ist. Nach Lemma 5.1.4 suchen wir deshalb ein Element in $\mathfrak{a}$ mit minimaler Norm. Wie dies geschieht, wird hier beispielhaft vorgeführt.

Wir definieren die Basis $\mathcal{B} = \{1/2, \sqrt{d_K}/2\}$ von K und das Skalarprodukt

$$\langle u, v\rangle = \frac{u_1 v_1 - d_K u_2 v_2}{4} \qquad \text{für } u = [u_1, u_2]_{\mathcal{B}},\ v = [v_1, v_2]_{\mathcal{B}} \in K.$$

Die induzierte Norm gibt uns die Körpernorm zurück, d. h. $\langle \alpha, \alpha\rangle = N_{K/\mathbb{Q}}(\alpha)$ für $\alpha \in K$.

Um ein Element minimaler Norm in $\mathfrak{b} = [u, v]$ zu finden, gehen wir wie folgt vor:

I Berechne $\lambda = \frac{\langle u,v\rangle}{\langle v,v\rangle}$.

II Ziehe die ganzzahlige Projektion von u auf v von u ab, $u \leftarrow (u - \lfloor\lambda\rceil\, v)$.

III Falls $N_{K/\mathbb{Q}}(u) < N_{K/\mathbb{Q}}(v)$ gilt, tausche u und v und gehe zu I, sonst beende das Verfahren.

Als Resultat erhalten wir einen kürzesten Vektor v, d.h. ein Element minimaler Norm in $\mathfrak{b}$.

Bezüglich $\mathcal{B}$ stellen wir die erzeugenden Elemente $x = 223$ und $y = (1+\sqrt{-3})/2 - 486$ von $\mathfrak{a}$ dar. Es ist also $x = [446, 0]_{\mathcal{B}}$ und $y = [-971, 1]_{\mathcal{B}}$.

Wir berechnen:

$$\lambda = \frac{-446 \cdot 971 + 3 \cdot 0 \cdot 1}{971^2 + 3 \cdot 1^2} = -\frac{971}{2114}, \qquad \text{d. h.} \qquad \lfloor\lambda\rceil = 0 \qquad \text{und} \qquad x = [446, 0]_{\mathcal{B}}.$$

Da $N_{K/\mathbb{Q}}(x) = 49729 < 235711 = N_{K/\mathbb{Q}}(y)$ ist, vertauschen wir x und y und fahren fort:

$$\lambda = -\frac{971}{446}, \qquad \text{d. h.} \qquad \lfloor\lambda\rceil = -2 \qquad \text{und} \qquad x = [971, 1]_{\mathcal{B}} + 2\cdot[446, 0]_{\mathcal{B}} = [-79, 1]_{\mathcal{B}}.$$

Da $N_{K/\mathbb{Q}}(x) = 1561 < 49729 = N_{K/\mathbb{Q}}(y)$ ist, vertauschen wir x und y und fahren fort:

$$\lambda = -\frac{79}{14}, \qquad \text{d. h.} \qquad \lfloor \lambda \rceil = -6 \qquad \text{und} \qquad x = [446, 0]_{\mathcal{B}} + 6 \cdot [-79, 1]_{\mathcal{B}} = [-28, 6]_{\mathcal{B}}.$$

Da $N_{K/\mathbb{Q}}(x) = 223 < 1561 = N_{K/\mathbb{Q}}(y)$ ist, vertauschen wir x und y und fahren fort:

$$\lambda = -\frac{5}{2}, \qquad \text{d. h.} \qquad \lfloor \lambda \rceil = 3 \qquad \text{und} \qquad x = [-79, 1]_{\mathcal{B}} - 3 \cdot [-28, 6]_{\mathcal{B}} = [5, -17]_{\mathcal{B}}.$$

Es ist $N_{K/\mathbb{Q}}(x) = 223 \geq 223 = N_{K/\mathbb{Q}}(y)$ und wir haben mit $\pi = [-28, 6]_{\mathcal{B}} = -17 + 6\omega_K$ einen kürzesten Vektor gefunden.

Es ist $N_{K/\mathbb{Q}}(\pi) = 223$ und deshalb $\mathfrak{a}$ ein Hauptideal, was hier klar ist, denn $\mathbb{Z}[\omega_K]$ ist ein Hauptidealring.

Wir testen, ob $N_{K/\mathbb{Q}}(1 - k\zeta\pi)$ für eine Einheit ζ prim ist. Für $\zeta = \omega_K - 1 = \frac{-1+\sqrt{-3}}{2}$ haben wir Glück. Es ist

$$N_{K/\mathbb{Q}}(1 - k\zeta\pi) = N_{K/\mathbb{Q}}\left(1 - (33 - 51\omega_K)\right) = 1993$$

prim und wir haben das Lösungspaar $(-3,\ 33 - 51\omega_K)$ gefunden.

Wir konstruieren mit der CM-Methode eine elliptische Kurve mit N Punkten über $\mathbb{F}_{1993}$.
Der Endomorphismenring ist eine Ordnung im Körper $K = \mathbb{Q}(\sqrt{D})$ mit

$$D = (p + 1 - N)^2 - 4p = (1993 + 1 - 2007)^2 - 4 \cdot 1993 = -7803 = (3 \cdot 17)^2(-3).$$

Es muss deshalb $d_K = -3$ die Diskriminante von K und folglich $K = \mathbb{Q}(\sqrt{-3})$ sein, genau so, wie wir es entsprechend unserer Wahl von p erwarten. Wir wählen also die Maximalordnung $\mathcal{O}_K = \mathbb{Z}[\omega_K]$ von K als Endomorphismenring. Da dies ein Hauptidealring ist, besitzt das Klassenpolynom Grad eins. Nach Bsp. 3.4.5.(ii) ergibt sich dies zu

$$H_{-3}(X) = X.$$

(Man vergleiche dies mit $H_{-2099}(X)$ von Seite 62!)
Es ist also 0 die Nullstelle, welche wir als j-Invariante der gesuchten Kurve wählen. Da wir $\mathbb{Z}[\omega_K]$ als Endomorphismenring verwenden, müssen wir sextische Twiste betrachten.
Der Frobenius unserer Kurve ist $\pi_E = 1 - 33 + 51\omega_K = -32 + 51\omega_K$ nach Konstruktion. Wir setzen $\omega = \frac{-1+\sqrt{-3}}{2}$ und schreiben $\pi_E = 19 + 51\omega$. Wir suchen das eindeutig bestimmte Element π_0 mit $N_{K/\mathbb{Q}}(\pi_0) = 1993$ und $\pi_0 \equiv 2 \bmod 3$, bzw. die Einheit $\epsilon = r + s\omega \in \mathbb{Z}[\omega]^* = \{\pm 1, \pm\omega, \pm\omega^2\}$ mit $\pi_0 = \epsilon\pi_E$.
Nach Lemma 4.4.6 ist $s \equiv 51 \bmod 3$, also $s = 0$, und wegen $r \equiv 51 - 19 \bmod 3$ folgt $r = -1$, d. h. $\epsilon = -1$. Wir lösen die Gleichung

$$0 = (19 - 51)v + 51u$$

in den Unbestimmten u und v. Das Lösungspaar $(u, v) = (0, 0)$ setzen wir in

$$\mathcal{C} = 1 + 19u - 51v$$

ein und erhalten $\mathcal{C} = 1$. Für $c = 1$ gilt natürlich $c^{\frac{1993-1}{6}} \equiv \mathcal{C} \bmod 1993$ und wir ermitteln $b \equiv c \cdot 4^{-1} \equiv 1495 \bmod 1993$. Die durch

$$y^2 = x^3 + 1495$$

gegebene elliptische Kurve besitzt dann 2007 $\mathbb{F}_{1993}$-rationale Punkte.

(ii) Die vorangegangenen Beispiele wurden mit einem von mir geschriebenen PARI-Programm gefunden[2]. Da das Hauptaugenmerk meiner Diplomarbeit nicht auf der Implementierung, sondern auf dem theoretischen Hintergrund der Verfahren liegt, ist das Programm kaum optimiert. Abschließend wollen wir ein großes Beispiel geben, um die Leistungsfähigkeit des Verfahrens von Bröker und Stevenhagen zu demonstrieren. Wir wählen

$$\begin{aligned} N &= \text{nextprime}(2^{700}) \\ &= 526013590154837350724098988288012866555033980282317385949828090306873215429708082 \\ &\quad 211366653627758845122698296885617821771301943225018380386312781477065188084995522 \\ &\quad 367112844459819166375788432271727129325173578191 1, \end{aligned}$$

eine 211-stellige Primzahl. Für $d_K = -119995$ haben wir Glück und finden die (ebenfalls 211-stellige) Primzahl

$$\begin{aligned} p &= 526013590154837350724098988288012866555033980282317385949828090306873215429708082 \\ &\quad 211366653627758845122698754046429012160383398076986385019674327092791656662645630 \\ &\quad 220157964704648843376563840266235998298028671706 9. \end{aligned}$$

Die Klassenzahl von $K = \mathbb{Q}(\sqrt{-119995})$ ist 44 und das Klassenpolynom $H_{-119995}(X)$ hat bis zu 946-stellige Koefizienten. Wir ermitteln eine Lösung von $H_{-119995}(X) \equiv 0 \bmod p$ und finden letztendlich die Kurve

$$y^2 = x^3 + ax + b$$

mit

$$\begin{aligned} a &= 810581888054866270643970833541132174516711977134687435648982703322612019606714982 \\ &\quad 044967015907844131781804945634145571172810838565872029189661878349843091876756605 \\ &\quad 553824475212810568490797168996354022653670495095 \end{aligned}$$

und

$$\begin{aligned} b &= 404714519306882651858997381094750722671136785330524086343150907092756278260253053 \\ &\quad 610575570145695505533919499073229046185109654622382391959093676618517310566880 86 \\ &\quad 051702694148395326681709570477724760037559714747 76. \end{aligned}$$

Die Rechenzeit dieses Beispiels betrug auf einem PC mit einem 1,92 GHz AMD Athlon Prozessor akzeptable 8 Minuten und 56 Sekunden.

[2]Der Quellcode des PARI-Programms ist auf der Internetseite http://crypto.math.uni-bremen.de/Arbeiten/ der WE Algorithmische Zahlentheorie, Algebraische Geometrie und Kryptologie der Universität Bremen verfügbar.

A Einige theoretische Grundlagen

Theorem A.0.1. *Sei R ein Ring und $A \subseteq R$ ein Unterring, so sind für $x \in R$ äquivalent:*

(i) Es existieren $a_0, \ldots, a_{n-1} \in A$, sodass gilt

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

(ii) Der Ring $A[x]$ ist ein endlich erzeugter A-Modul.

(iii) Es existiert ein Unterring $B \subseteq R$, der A und x enthält und ein endlich erzeugter A-Modul ist.

Beweis. $(i) \Rightarrow (ii)$: Sei M der A-Untermodul von R, der von $1, x, \ldots, x^{n-1}$ erzeugt wird. Nach Voraussetzung ist $x^n \in M$ und rekursiv schließt man, dass x^k für $k \in \mathbb{N}_0$ in M liegt. Da $A[x]$ der A-Modul ist, welcher von den $(x^k)_{k\in\mathbb{N}_0}$ erzeugt wird, gilt $A[x] = M$ und (ii) ist gezeigt.

$(ii) \Rightarrow (iii)$: Wähle $B = A[x]$.

$(iii) \Rightarrow (i)$: Sei $(y_1, \ldots, y_n)$ ein endliches Erzeugendensystem des A-Moduls B, also ist $B = Ay_1 + \cdots + Ay_n$. Da B ein Unterring von R ist und x und y_i enthält, liegen auch die xy_i in B. Es existieren also Elemente $a_{ij} \in A$, sodass $xy_i = \sum_{j=1}^n a_{ij}y_j$ gilt. Dies impliziert

$$\sum_{j=1}^{n}(\delta_{ij}x - a_{ij})y_j = 0 \qquad \text{für } i = 1, \ldots, n.$$

Dies fassen wir als lineares Gleichungssystem auf und definieren die Matrix $M = (\delta_{ij}x - a_{ij})$. Multiplizieren wir mit der transponierten Matrix, so folgt $det(M)y_i = 0$ für alle i. Weiter folgt aus der Darstellung von B, dass auch $det(M)B = 0$ gilt, und da $1 \in B$ ist, folgt letztlich $det(M) = 0$. Entwickelt man andererseits die Determinante von M, so erhält man eine Gleichung $P(x) = 0$ mit einem normierten Polynom n-ten Grades über A. □

Lemma A.0.2. *Sei M ein freier $\mathbb{Z}$-Modul von Rang 2 und $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ eine Matrix mit ganzzahligen Einträgen und Determinante $ad - bc \neq 0$, so ist*

$$|M/AM| = |det(A)|.$$

Beweis. Wir können o. B. d. A. $M = \mathbb{Z}^2$ annehmen, schreiben $M = [e_1, e_2]$ und definieren $A' = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. Es ist dann $AA' = A'A = det(A)I$ und $AM = [ae_1 + be_2, ce_1 + de_2]$. Natürlich gilt $det(A)M = A' \cdot (AM) \subseteq AM$.
Betrachte weiter den durch $M \to AM$, $(x, y) \mapsto (ax + by, cx + dy)$ induzierten Modulhomomorphismus

$$M \to AM/det(A)M.$$

Wegen $det(A)M = A \cdot A'M$ ist der Kern gerade $A'M$ also

$$M/A'M \simeq AM/det(A)M.$$

Es ist deshalb $0 \to AM/det(A)M \to M/det(A)M \to M/AM \to 0$ eine exakte Sequenz. Folglich gilt

$$|M/AM| \cdot |M/A'M| = |M/det(A)M| = det(A)^2,$$

wobei beim letzten Gleicheitszeichen $M = \mathbb{Z}^2$ ausgenutzt wurde.
Durch $\theta = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ wir ein Isomorphismus $M \to M$ definiert. Da $\theta A \theta^{-1} = A'$ ist, gilt

$$M/AM \simeq \theta M/\theta AM \simeq \theta\theta^{-1}M/\theta A\theta^{-1}M = M/A'M.$$

Deshalb schließen wir $|M/AM| = |det(A)|$. □

Lemma A.0.3. *Sind $A(x)$, $B(x) \in \mathbb{C}[x]$ teilerfremde Polynome, so ist*

$$M = \{\lambda \in \mathbb{C} : \ A(x) - \lambda B(x) \text{ besitzt eine mehrfache Nullstelle}\}$$

endlich.

Beweis. Sei

$$N = \{\gamma \in \mathbb{C} : \text{ es ex. } \lambda \in M, \ \gamma \text{ ist mehrf. Nullst. von } A(x) - \lambda B(x)\}.$$

Für ein beliebiges $\lambda \in M$ existiert ein $\gamma \in N$, sodass gilt

$$A(\gamma) - \lambda B(\gamma) = 0 \quad \text{und} \quad A'(\gamma) - \lambda B'(\gamma) = 0.$$

Dann ist γ eine Nullstelle von $A(x)B'(x) - A'(x)B(x)$ und deshalb zunächst $|N|$ endlich.
Sei nun $\gamma \in N$ beliebig gewählt, so existiert ein $\lambda \in M$ und es ist $A(\gamma) = \lambda B(\gamma)$. Wäre γ eine Nullstelle von $A(x)$, so auch von $B(x)$ und die Polynome wären nicht teilerfremd.
Folglich sind für jedes $\gamma \in N$ die Werte $A(\gamma)$ und $B(\gamma)$ von Null verschieden und jedes $\lambda \in M$ besitzt eine Darstellung $\lambda = \frac{A(\gamma)}{B(\gamma)}$. Also ist auch $|M|$ endlich. □

Lemma A.0.4. *Ist ein Gitter L vorgegeben, so existiert zu jedem $u \in \mathbb{C}$ ein $w \in \mathbb{C}$ mit $\wp(w; L) = u$.*

Beweis. Zu vorgegebenem Gitter $L = [\omega_1, \omega_2]$ und $u \in \mathbb{C}$ definiere die elliptische Funktion $f(z) = \wp(z; L) - u$. Wähle ein $-1 < \delta < 0$, sodass $f(z)$ auf Γ, dem gegen den Uhrzeigersinn orientierten Rand der verschobenen Grundmasche $P = \{s\omega_1 + t\omega_2 : \ \delta \leq s, t \leq \delta + 1\}$, keine Null- und Polstellen besitzt. Die Funktionentheorie gibt die Beziehung

$$0 = \frac{1}{2\pi i} \int_\Gamma \frac{f(z)}{f'(z)} = \#\text{Nullstellen } - \#\text{Pole}.$$

Da $0 \in P$ ein Pol von $f(z)$ ist, existiert eine Nullstelle von $f(z)$ in P. Mit anderen Worten existiert ein $w \in P$ mit $\wp(w) = u$. □

Lemma A.0.5. *Ist G eine endliche abelsche Gruppe, so gilt:*

$$G \text{ ist nicht zyklisch} \iff \exists\, H \subseteq G \text{ Untergruppe, } H \simeq (\mathbb{Z}/d\mathbb{Z})^2 \text{ mit } d > 1.$$

Beweis. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen ist

$$G = \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}$$

mit Elementen $r_i \in \mathbb{Z}$, $r_i | r_{i+1}$ und $\prod r_i = m = |G|$. Um Trivialitäten auszuschließen, sei $|r_i| > 1$.

Sei G zunächst zyklisch. Da für $d > 1$ die Gruppen $(\mathbb{Z}/d\mathbb{Z})^2$ nicht zyklisch sind, können sie keine Untergruppen von G sein.
Ist G nicht zyklisch, so ist $G \not\simeq \mathbb{Z}/m\mathbb{Z}$, insbesondere also $n > 1$. G besitzt die Untergruppe $\mathbb{Z}/r_1\mathbb{Z} \times \mathbb{Z}/r_2\mathbb{Z}$. Da r_1 ein Teiler von r_2 ist, liegt $\mathbb{Z}/r_1\mathbb{Z}$ in $\mathbb{Z}/r_2\mathbb{Z}$. Also ist mit $d = |r_1|$ (es ist $d > 1$ nach Voraussetzung) dann

$$(\mathbb{Z}/d\mathbb{Z})^2 \subseteq \mathbb{Z}/r_1\mathbb{Z} \times \mathbb{Z}/r_2\mathbb{Z} \subseteq G.$$

□

Lemma A.0.6. *Sei $M = \mathbb{Z}^2$, $A = (a_{ij}) \in M_2(\mathbb{Z})$ mit $det(A) \neq 0$ und $d = ggT(a_{ij})$, so gilt*

$$M/AM \text{ nicht zyklisch} \qquad \Longleftrightarrow \qquad d > 1.$$

Beweis. Sei zunächst $d > 1$. Setze $A' = \frac{1}{d}A \in M_2(\mathbb{Z})$, also $A = dA'$ und betrachte die durch die Einbettung $A'M \hookrightarrow M$ induzierte Einbettung

$$(\mathbb{Z}/d\mathbb{Z})^2 \simeq A'M/dA'M = A'M/AM \subseteq M/AM.$$

Nach Lemma A.0.5 ist dann M/AM nicht zyklisch.

Ist nun M/AM als nicht zyklisch vorausgesetzt, so existiert eine Untergruppe

$$(\mathbb{Z}/f\mathbb{Z})^2 \simeq M'/AM \subseteq M/AM,$$

mit einem $f > 1$. Da $AM \subseteq M' \subseteq M$ gilt, gibt es ein $B \in M_2(\mathbb{Z}), \det(B) \neq 0$, mit $M' = BM$. Wegen obiger Isomorphie erhält man dann $fBM = AM$, also $fB = A$ und es muss deshalb $\mathrm{ggT}(a_{ij}) = d > 1$ sein. □

Lemma A.0.7. *Sei L' ein Untergitter von $L = [1, \tau]$ mit endlichem Index in L, $\tau \in \mathfrak{H}$. Ist $d \in \mathbb{N}$ die kleinste positive ganze Zahl in L', so besitzt L' die Darstellung $L' = [d, a\tau + b]$ mit $a, b \in \mathbb{Z}$.*

Beweis. Zunächst besitzt L' eine Darstellung $L' = [e_1, e_2]$ mit $e_1 = \alpha\tau + \beta$, $e_2 = \gamma\tau + \delta$ für geeignete $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Da d in L' liegt, existieren $u, v \in \mathbb{Z}$ mit $d = ue_1 + ve_2$. Wären u und v nicht teilerfremd, so könnte d nicht das kleinste positive ganzzahlige Element in L' sein. Folglich existieren $x, y \in \mathbb{Z}$ mit $ux + vy = 1$. Deshalb ist die Matrix $A = \left(\begin{smallmatrix} u & v \\ -y & x \end{smallmatrix}\right)$ in $SL(2, \mathbb{Z})$. Dann ist

$$L' = [e_1, e_2] = A[e_1, e_2] = [ue_1 + ve_2, xe_2 - ye_1] = [d, a\tau + b],$$

mit geeigneten $a, b \in \mathbb{Z}$. □

Lemma A.0.8. *Sind $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, $\sigma' = \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) \in C(m)$ und $\tau \in \mathfrak{H}$, so gilt:*

$$d[1, \sigma\tau] = d'[1, \sigma'\tau] \quad \Longrightarrow \quad \sigma = \sigma'.$$

Beweis. Aus $d[1, \sigma\tau] = d'[1, \sigma'\tau]$, also $[d, a\tau + b] = [d', a'\tau + b']$, folgt zunächst $d = d'$. Dann muss auch $a = \frac{m}{d} = \frac{m}{d'} = a'$ sein. Da $b - b' = (a\tau + b) - (a'\tau + b')$ in beiden Mengen liegt, muss $d|(b - b')$ gelten. Wegen $0 \leq b, b' < d$ folgt dann auch $b = b'$. □

Lemma A.0.9. *Es seien N_0 und $f(X)$ wie oben gewählt, $q \in \mathbb{N}$ eine Primzahl.*

(i) Gilt $q|N_0$ und q ist prim in $\mathcal{O}_K$ (d. h. $\left(\frac{-d}{q}\right) = -1$), so besitzt $f(X) \equiv 0 \bmod N_0$ keine Lösungen.

(ii) Gilt $q^2|N_0$ und q ist verzweigt in $\mathcal{O}_K$ (d. h. $\left(\frac{-d}{q}\right) = 0$), so besitzt $f(X) \equiv 0 \bmod N_0$ keine Lösungen.

Beweis. (i) Wir argumentieren per Widerspruch. Ist $\alpha \in \mathbb{Z}$ eine Nullstelle von $f(X) \bmod N_0$, so gilt auch $f(\alpha) \equiv 0 \bmod q$.
Ist $-d \not\equiv 1 \bmod 4$, so ist $f(X) = X^2 + d$, also $\alpha^2 \equiv -d \bmod q$. Deshalb ist $\left(\frac{-d}{q}\right) = 1$. Widerspruch!
Ist $-d \equiv 1 \bmod 4$, so gilt $f(\alpha) = (\alpha - \omega)(\alpha - \overline{\omega}) \equiv 0 \bmod q\mathcal{O}_K$. Da $q\mathcal{O}_K$ ein Primideal ist, gilt o. B. d. A. $\alpha \equiv \omega \bmod q\mathcal{O}_K$. Es ist $\omega = \frac{1+\sqrt{-d}}{2}$ und deshalb gilt $(2\alpha - 1)^2 \equiv -d \bmod q$, d. h. $\left(\frac{-d}{q}\right) = 1$. Widerspruch!

(ii) Sei auch hier $\alpha \in \mathbb{Z}$ eine Nullstelle von $f(X) \bmod N_0$, d. h. es gilt auch $f(\alpha) \equiv 0 \bmod q^2$.
Ist $-d \not\equiv 1 \bmod 4$, so ist $f(\alpha) = \alpha^2 + d \equiv \alpha^2 \equiv 0 \bmod q$. Es folgt aus $\alpha \equiv 0 \bmod q$, dass $\alpha^2 \equiv 0 \bmod q^2$ sein muss. Da d quadratfrei ist, gilt $d \not\equiv 0 \bmod q^2$, also $f(\alpha) = \alpha^2 + d \not\equiv 0 \bmod q^2$. Widerspruch!
Ist $-d \equiv 1 \bmod 4$, so folgt aus $q|d$ zunächst $q \neq 2$. Aus $f(\alpha) = \alpha^2 - \alpha + \frac{1+d}{4} \equiv 0 \bmod q^2$ folgt deshalb $4f(\alpha) \equiv (2\alpha - 1)^2 \equiv 0 \bmod q$ und schließlich $(2\alpha - 1)^2 \equiv 0 \bmod q^2$. Da d quadratfrei ist, also $d \not\equiv 0 \bmod q^2$ gilt, schließen wir auf $f(\alpha) \not\equiv 0 \bmod q^2$. Widerspruch! □

Literaturverzeichnis

[1] Siegfried Bosch. *Algebra.* Springer, 1999.

[2] Henri Cohen und Gerhard Frey. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Taylor & Francis Ltd, 1 edition, 2005.

[3] David A. Cox. *Primes of the Form $x^2 + ny^2$.* Wiley-Interscience, 1989.

[4] Eberhard Freitag und Rolf Busam. *Funktionentheorie 1.* Springer, 3 edition, 2000.

[5] Dale Husemöller. *Elliptic Curves.* Springer, 1987.

[6] Kenneth Ireland und Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer, 2 edition, 1998.

[7] Gerald J. Janusz. *Algebraic Number Fields.* Academic Press, 1973.

[8] Serge Lang. *Elliptic Functions.* Addison-Wesley, 1973.

[9] Daniel A. Marcus. *Number Fields.* Springer-Verlag, New York Inc., 1977.

[10] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, collection Méthodes, 1967.

[11] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.

[12] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer, 1994.

[13] Larry C. Washington. *Elliptic Curves. Number Theory and Cryptography.* Chapman and Hall (CRC), 2003.

[14] Harald Baier. *Efficient Algorithms for Generating Elliptic Curves over Finite Fields Suitable for Use in Cryptography.* PhD thesis, Technische Universität Darmstadt, 2002.

[15] Reinier Bröker und Peter Stevenhagen. Constructing elliptic curves in almost polynomial time. *ArXiv Mathematics e-prints*, November 2005.

[16] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abhandlungen des Mathematischen Seminars der Hansischen Universität*, 1941.

[17] Georg-Johann Lay. Konstruktion elliptischer Kurven mit gegebener Gruppenordnung über endlichen Primkörpern. Master's thesis, Universität Saarbrücken, 1994.

[18] Georg-Johann Lay und Horst G. Zimmer. Constructing elliptic curves with given group order over large finite fields. *LNCS*, 1994.

[19] H.W. Lenstra. Factoring integers with elliptic curves. *Report 86-18, Mathematisch Instituut, Universiteit van Amsterdam*, 1986.

[20] Francois Morain. Implementation of the atkin-goldwasser-kilian primality testing algorithm. Technical report, Institut National de Recherche en Informatique et Automatique, 1988.

[21] heise online. Rsa-640 geknackt. http://www.heise.de/newsticker/meldung/65957. Zugriff am 4. Juli 2007.

[22] Dr. Manfred Lochter. Ecc brainpool standard curves and curve generation. Technical report, ECC Brainpool, 2005.

[23] Harald Baier, Dennis Kügler und Marian Margraf. Elliptic curve cryptography based on iso 15946. Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2007.