Quadratische Zahlkörper, Klassengruppen und diskreter Logarithmus

Gutachter:
Dr. Michael Hortmann
Prof. Dr. Jens Gamst

Diplomarbeit im Fachbereich Mathematik, Universität Bremen,
vorgelegt von Ralf Stein im Juli 1998.

Mein besonderer Dank gilt meinen Eltern Inge und Hans Stein, deren Unterstützung mir dieses Studium ermöglicht hat.

Inhaltsverzeichnis

Einleitung

Die gegenwärtigen Kryptosysteme nutzen in der Regel die Eigenschaften von sogenannten *Einweg-Funktionen* aus, und diese sind, anschaulich formuliert, Funktionen, die sich leicht berechnen lassen, deren Umkehrung aber besonders schwierig ist. Ein Beispiel hierfür ist die Multiplikation zweier Primzahlen, die Umkehrung ist bekannt als das Faktorisierungsproblem. H.W.Lenstra beschreibt dieses sehr bildhaft [Lens]:

> „Suppose, for example, that two 80-digit numbers p and q have been proven prime, this is easily within reach of the modern techniques (...). Suppose further, that the cleaning lady gives p and q by mistake to the garbage collector, but that the product pq is saved. How to recover p and q? It must be felt as a defeat for mathematics that, in these circumstances, the most promising approaches are searching the garbage dump and applying mnemo-hypnotic techniques."

Daneben gibt es noch eine weitere Einweg-Funktion, die in der Kryptographie häufig verwendet wird. Sei etwa G eine endliche Gruppe, in der es einfach ist, n-te Potenzen eines Gruppenelementes zu berechnen. Die Umkehrung, die Zahl $x \in \mathbb{Z}$ zu bestimmen, so daß für gegebene Elemente $a, b \in G$ gilt, $a^x = b$, ist für bestimmte Gruppen sehr schwierig und als das Diskrete-Logarithmus-Problem (DLP) bekannt.
Für das DLP ist es wichtig, die Gruppe sorgfältig auszuwählen. So ist zum Beispiel in der additiven Gruppe $(\mathbb{Z}/p\mathbb{Z})^+$ das Logarithmusproblem leicht zu lösen, in der multiplikativen Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$, für ausreichend großes p aber nicht.

Die Motivation zu dieser Arbeit waren mehrere Artikel von Johannes Buchmann und Hugh C. Williams aus den Jahren 1988–93, im besonderen [BuWi88] und [BuWi89]. In diesen stellten sie Schlüsselaustauschverfahren vor, die das DLP auf quadratischen Zahlkörpern ausnutzten. Das Verfahren selbst ist von der Art, wie es Diffie und Hellmann 1976 in [DiffHell] veröffentlichten, und prinzipiell auf jede endliche Menge G übertragbar, auf der eine assoziative Verknüpfung erklärt und die folgende Eigenschaften hat:

1. Die Elemente der Menge müssen eine eindeutige Darstellung haben. Dies ist unter Umständen nicht ganz einfach, wenn z.B. die Elemente von G Klassen sind.

2. Die Verknüpfung muß eindeutig beschreibbar, sowie leicht und schnell ausführbar sein.

3. Das DLP muß in G schwierig sein. Das bedeutet, daß zu einem Eingabewert, z. B. der Ordnung von G, mit einer Größe von n Dezimalstellen, die Anzahl der Rechenschritte, die man benötigt um das DLP zu lösen, nicht polinomial in der Eingabe sein darf.

Buchmann und Williams beschreiben in [BuWi88] ein Verfahren, das als endliche Gruppe die Idealklassengruppe von imaginärquadratischen Zahlkörpern verwendet. 1989 stellen sie in [BuWi89] das erste Diffie-Hellmann Verfahren vor, das nicht auf einer Gruppe basiert, sondern die endliche Menge von reduzierten Hauptidealen in einem reellquadratischen Zahlkörper verwendet, auf der eine assoziative Verknüpfung erklärt ist, die es einem erlaubt, fast wie in einer zyklischen Gruppe zu rechnen.

In dieser Arbeit habe ich die drei oben aufgezählten Kriterien für die in [BuWi88] verwendete Gruppe bzw. in [BuWi89] verwendete endliche Menge der reduzierten Hauptideale untersucht. Dazu war es sinnvoll, den Zusammenhang zwischen der Idealklassengruppe und der Formklassengruppe von binär-quadratischen Formen einer festen Diskriminante herauszuarbeiten, da sich diese Gruppen zu einer vorgegebenen Diskriminante bijektiv aufeinander abbilden lassen. Damit erhält man zwei Vorteile. Erstens kann man durch den Übergang zu den Nullstellen der binär-quadratischen Formen die Struktur auf der Idealklassengruppe im imaginr-quadratischen Fall und auf der Menge der reduzierten Hauptideale im reell-quadratischen Fall besonders gut verstehen, und zweitens ermöglicht es einem für die Algorithmen, die die explizite Arithmetik beschreiben, zwischen Idealen und Formen zu wählen, je nachdem, welche Darstellung geeigneter ist.

Meine Arbeit gliedert sich daher wie folgt: Zunächst wird knapp in die Theorie algebraischer Zahlkörper eingeführt, wobei die wichtigsten Begiffe hier zunächst allgemein bereitgestellt werden. Im zweiten Kapitel werden diese Begriffe eingeschränkt auf den quadratischen Zahlkörper, die Darstellung von Idealen beschrieben und die Bijektion zwischen Idealen und binär-quadratischen Formen erklärt. Hierbei ist die Reduziertheit der zentrale Begriff zur Beschreibung der Idealklassengruppe bzw. der Formklassengruppe. Um diesen zu veranschaulichen, wird die Bijektion zwischen den Idealen und Formen auf die Nullstellen der letzteren ausgedehnt.
In imaginärquadratischen Zahlkörper werden die Idealklassen eindeutig durch reduzierte Ideale repräsentiert, so daß eine Verknüpfung dieser Vertreter bereits die Arithmetik auf der Idealklassengruppe vollständig beschreibt. Auf diese Weise wird das erste der oben genannten Kriterien für die Idealklassengruppe im imaginärquadratischen Zahlkörper erfüllt.

In reellquadratischen Zahlkörper gibt es in der Regel mehr als ein reduziertes Ideal pro Klasse. Diese haben jedoch eine eindeutige Darstellung und bilden eine endliche Menge, auf der eine assoziative Verknüpfung erklärt werden kann, die im Abschnitt über den Distanzbegriff auf Idealen vorgestellt und analysiert wird. Es stellt sich heraus, daß diese dem zweiten Kriterium genügt.
Wie man aus beliebigen Idealen bzw. Formen reduzierte Elemente der gleichen Klasse erzeugen kann, ist also von maßgeblicher Bedeutung und wird deshalb im dritten Kapitel ausführlich beschrieben.
Anschließend werden im vierten Kapitel explizit die Verknüpfungen angegeben und ihre Komplexität untersucht. Sie erfüllen das zweite der obigen Kriterien, da sie eindeutig beschrieben werden und in dem Sinne schnell sind, als daß sie polynomial in der Größe der Eingabe sind. Im folgenden fünften Kapitel wird das DLP auf quadratischen Zahlkörpern behandelt und Verfahren zur Lösung desselben beschrieben. Es zeigt sich dort, daß es sowohl im reellen, als auch im imaginären Fall schwierig ist, so daß auch das dritte Kriterium der Eignung für ein Diffie-Hellmann Verfahren erfüllt ist. Ein konkretes Beispiel für die Realisierung zeigt das Ende von Kapitel vier.

1 Grundlagen zu algebraischen Zahlkörpern

Quadratische Zahlkörper sind ein Spezialfall von algebraischen Zahlkörpern. Daher führe ich die wichtigsten grundlegenden Begriffe zunächst allgemein ein, um einige im anschließenden Kapitel für den quadratischen Fall zu konkretisieren.
Da es sich in diesem Kapitel um bekannte Theorie handelt, werde ich auf Beweise verzichten. Diese sind in Standardwerken zur algebraischen Zahlentheorie zu finden.
Ich habe mich mit dieser Einführung an dem Buch von Neukirch [Neuk] orientiert.

Definition 1.1. Ein algebraischer Zahlkörper ist eine endliche Körpererweiterung $\mathbb{K}$ von $\mathbb{Q}$.

In dieser Körpererweiterung $\mathbb{K}$ ist ein Ring, $\mathcal{O}_{\mathbb{K}}$, besonders von Interesse. Betrachtet man $\mathbb{Z}$ als einen Ring in $\mathbb{Q}$, so ist $\mathcal{O}_{\mathbb{K}}$ eine Ringerweiterung von $\mathbb{Z}$ in $\mathbb{K}$. Die Elemente in diesem Ring haben eine Eigenschaft, die man etwas allgemeiner definieren kann, als es in diesem Zusammenhang nötig ist:

Definition 1.2. Sei $A \subseteq B$ eine Ringerweiterung. Ein Element $b \in B$ heißt *ganz* über A, wenn es Nullstelle eines normierten Polynoms $g \in A[X]$ ist.Die Menge $\overline{A} = \{b \in B \mid b \textit{ ganz über } A\}$ heißt *ganzer Abschluß* von A in B. Ist $A = \overline{A}$, so heißt A *ganzabgeschlossen* zu B.

Lemma 1.3. *Der ganze Abschluß von $\mathbb{Z}$ in $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}} = \{x \in \mathbb{K} | x \text{ ist ganz über } \mathbb{Z}\}$, bildet einen Ring. Er heißt der Ring der ganzen Zahlen in $\mathbb{K}$.*

Lemma 1.4. *Jedes Element $\xi \in \mathbb{K}$ ist von der Form $\xi = \frac{\alpha}{a}$, mit $\alpha \in \mathcal{O}_{\mathbb{K}}$ und $a \in \mathbb{Z}$.*

Definition 1.5. Ein System $\{\omega_1, \dots, \omega_n\}$ von Elementen $\omega_i \in \mathcal{O}_{\mathbb{K}}$ heißt *Ganzheitsbasis*, wenn sich jedes Element $\alpha \in \mathcal{O}_{\mathbb{K}}$ eindeutig darstellen läßt als

$$\alpha = a_1\omega_1 + \dots + a_n\omega_n \ , \ a_i \in \mathbb{Z} \, ,$$

d.h. wenn $\{\omega_1, \dots, \omega_n\}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_{\mathbb{K}}$ ist.

Es gibt zu $\mathcal{O}_{\mathbb{K}}$ immer eine Ganzheitsbasis, denn es gilt:

Satz 1.6. *Ist A ein Hauptidealring, $Q(A)$ sein Quotientenkörper, $\mathbb{K}/Q(A)$ eine separable Körpererweiterung und B der ganze Abschluß von A in $\mathbb{K}$, so ist jeder endlich erzeugte B-Untermodul $M \subseteq \mathbb{K}$, $M \neq 0$, frei vom Rang $n = [\mathbb{K} : Q(A)]$.*

$\mathcal{O}_{\mathbb{K}}$ ist also ein freier $\mathbb{Z}$-Modul von endlichem Rang. Also besitzt $\mathcal{O}_{\mathbb{K}}$ stets eine Ganzheitsbasis.

Jedes Element $x \in \mathbb{K}$ besitzt ein Minimalpolynom, d.h. ein normiertes Polynom $f \in \mathbb{Q}[X]$, mit $\mathrm{Grad}(f) \leq n$, mit $(x) = 0$. Ist $\mathrm{Grad}(f) = n$, für ein $x \in \mathbb{K}$, so gilt

$$\mathbb{K} \simeq \mathbb{Q}[X]/(f)\ .$$

Mit Lemma 1.4 läßt sich ein solches Element in $\mathcal{O}_{\mathbb{K}}$ wählen.

Sind $\sigma_i : \mathbb{K} \to \mathbb{C}\,, 1 \leq i \leq n$, $\sigma_i \in Hom_{\mathbb{Q}}(\mathbb{K}, \mathbb{C})$ die $\mathbb{K}$-Einbettungen nach $\mathbb{C}$, so sind $\sigma_i\theta$ die Nullstellen von f. Die Elemente $\sigma_j\theta$, $1 \leq j \leq n$, heißen die *Konjugierten* von θ.

Ein wichtiges Hilfsmittel für den Umgang mit algebraischen Zahlkörpern stellen die beiden nächsten Begriffe dar.

Definition 1.7. Sei $x \in \mathbb{K}$. Dann ist $T_x : \mathbb{K} \to \mathbb{K}$, $\alpha \mapsto \alpha x$ sei eine lineare Abbildung des n-dimensionalen $\mathbb{Q}$-Vektorraumes $\mathbb{K}$ in sich.
Die Spur der Transformation T_x heißt *Spur* von $x \in \mathbb{K}$, kurz

$$Tr_{\mathbb{K}/\mathbb{Q}}(x) := Tr(T_x).$$

Die Determinante von T_x heißt *Norm* von $x \in \mathbb{K}$, kurz

$$N_{\mathbb{K}/\mathbb{Q}}(x) := det(T_x).$$

Im folgenden schreibe ich lediglich $Tr(x)$ und $\mathcal{N}(x)$ statt $Tr_{\mathbb{K}/\mathbb{Q}}(x)$ und $N_{\mathbb{K}/\mathbb{Q}}(x)$.

Bemerkung. Da $T_{x+y} = T_x + T_y$ und $T_{xy} = T_x \circ T_y$ gilt, ist die Spur ein additiver und die Norm ein multiplikativer Homomorphismus von $\mathbb{K}$ nach $\mathbb{Q}$.

Der folgende, auch allgemein für separable Körpererweiterungen geltende Satz liefert eine weitere Definition der Spur und der Norm.

Satz 1.8. *Sei* $\mathbb{K} = \mathbb{Q}(\xi)$ *ein algebraischer Zahlkörper, und durchläuft* $\sigma : \mathbb{K} \to \mathbb{C}$ *die verschiedenen* $\mathbb{Q}$*-Einbettungen von* $\mathbb{K}$ *nach* $\mathbb{C}$*, so gilt*

$$\begin{aligned} (i) \quad Tr(x) &= \sum_{\sigma} \sigma x \\ (ii) \quad \mathcal{N}(x) &= \prod_{\sigma} \sigma x \, . \end{aligned}$$

Ist $\alpha_1, \ldots, \alpha_n$ eine beliebige $\mathbb{Q}$-Basis von $\mathbb{K}$, so heißt

$$d(\alpha_1, \ldots, \alpha_n) := det(\sigma_i \alpha_j)^2 \quad \in \mathbb{Q}$$

die Diskriminante dieser Basis. Mit Hilfe der Ganzheitsbasis erhält man hiermit nach dem Körpergrad die zweite wichtige Invariante von Zahlkörpern.

Definition 1.9. Ist $\Omega = \{\omega_1, \ldots, \omega_n\}$ eine Ganzheitsbasis von $\mathcal{O}_{\mathbb{K}}$, so ist

$$discr(\mathbb{K}) = d(\omega_1, \ldots, \omega_n)$$

die *Diskriminante* von $\mathbb{K}$.

An der Definition sieht man bereits, daß $discr(\mathbb{K})$ nicht von der Wahl der Ganzheitsbasis abhängt, da Ω eine $\mathbb{Z}$-Basis von $\mathcal{O}_{\mathbb{K}}$ ist. Eine Basiswechselmatrix hat dann ganzzahlige Einträge und ist invertierbar. Somit hat sie Determinante ± 1 und beeinflußt den Wert der Diskriminante nicht.

Ideale von $\mathcal{O}_{\mathbb{K}}$ sind als Untermoduln eines enlich erzeugten Moduls auch endlich erzeugt. Endlich erzeugte Untermoduln von $\mathbb{K}$ über $\mathcal{O}_{\mathbb{K}}$ spielen auf diesem Gebiet eine wichtige Rolle und haben daher einen eigenen Namen.

Definition 1.10. Ist $\mathrm{M} \subseteq \mathcal{O}_{\mathbb{K}}$ ein Ideal von $\mathcal{O}_{\mathbb{K}}$, so heißt M *ganzes Ideal* von $\mathbb{K}$.
Ein endlich erzeugter $\mathcal{O}_{\mathbb{K}}$-Untermodul $\mathrm{M} \neq 0$ von $\mathbb{K}$ heißt *gebrochenes Ideal* von $\mathbb{K}$.

Bemerkung. Ist $\mathfrak{A}$ ein gebrochenes Ideal, so existiert zu $\mathfrak{A}$ eine ganze Zahl m, so daß $(m)\mathfrak{A}$ ein ganzes Ideal ist. Ein möglicher Wert für m ist z.B. der Hauptnenner der Erzeugenden $\omega_i = \frac{\alpha_i}{q_i}$, mit $\alpha_i \in \mathcal{O}_{\mathbb{K}}$ und q_i aus $\mathbb{Z}$.

Die ganzen Ideale, also die Ideale von $\mathcal{O}_{\mathbb{K}}$, werden nun näher charakterisiert.

Satz 1.11. *$\mathcal{O}_{\mathbb{K}}$ ist ein Dedekindring, d.h. $\mathcal{O}_{\mathbb{K}}$ ist noethersch, ganzabgeschlossen und jedes Primideal $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{K}}$, $\mathfrak{p} \neq 0$ ist ein maximales Ideal.*

Man beachte, daß $\mathcal{O}_{\mathbb{K}}/\mathfrak{A}$ ein Quotient von freien $\mathbb{Z}$-Moduln desselben Ranges n ist. Darum ist der Index von $\mathcal{O}_{\mathbb{K}}$ über $\mathfrak{A}$ endlich.

Definition 1.12. Sei $\mathfrak{A} \subseteq \mathcal{O}_{\mathbb{K}}$ ein ganzes Ideal, so definiert $\mathcal{N}(\mathfrak{A}) = [\mathcal{O}_{\mathbb{K}} : \mathfrak{A}]$ die *Norm* des Ideals $\mathfrak{A}$.

Bemerkung. Ein Ideal, daß von über $\mathcal{O}_{\mathbb{K}}$ von einem Element erzeugt wird heißt *Hauptideal.* Ist $\mathfrak{A} = (\kappa)$ das von $\kappa \neq 0$ aus $\mathcal{O}_{\mathbb{K}}$ erzeugte Hauptideal, dann ist $\mathcal{N}(\mathfrak{A}) = |\mathcal{N}(\kappa)|$.

Nun werde ich die Verknüpfungen, sowie Teilbarkeitseigenschaften zwischen Idealen erklären.

Definition 1.13. Seien[1] $\mathfrak{A} = (a_1, \dots, a_r)$, $\mathfrak{B} = (b_1, \dots, b_s)$ gebrochene Ideale in $\mathbb{K}$,
dann sind *Summe* und *Produkt* gegeben durch:

$$\mathfrak{A} + \mathfrak{B} = \{\alpha + \beta | \alpha \in \mathfrak{A}, \beta \in \mathfrak{B}\} = (\{a_i + b_j\}_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}})$$

$$\mathfrak{A}\mathfrak{B} = \{\sum_{k=1}^{N} \alpha_k \beta_k | \alpha_k \in \mathfrak{A}, \beta_k \in \mathfrak{B}, N \in \mathbb{N}\} = (\{a_i b_j\}_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}}) .$$

Ferner gilt:

$$\mathfrak{B} \subseteq \mathfrak{A} \Leftrightarrow \mathfrak{A} | \mathfrak{B}$$

Satz 1.14. *Jedes Ideal $\mathfrak{A} \subsetneqq \mathcal{O}_{\mathbb{K}}$, $\mathfrak{A} \neq 0$ besitzt eine bis auf Reihenfolge eindeutige Darstellung der Form*

$$\mathfrak{A} = \prod_{i=1}^{m} \mathfrak{p}_i, \quad \mathfrak{p}_i \in \mathcal{O}_{\mathbb{K}} .$$

mit Primidealen $\mathfrak{p}_i$

[1] Sei R ein Ring, so bezeichne ich mit $(x_1, \dots, x_n) = x_1 R + \dots + x_n R$ den von $x_1, \dots, x_n$ erzeugten R-Modul. Ist $R = \mathbb{Z}$, so schreibe ich für den von $x_1, \dots, x_n$ erzeugten $\mathbb{Z}$-Modul $[x_1, \dots, x_n]$.

Satz 1.15. *Die gebrochenen Ideale bilden eine Gruppe bezüglich der Multiplikation.* $\mathcal{O}_{\mathbb{K}} = (1)$ *ist das Einselement, und das Inverse zu* $\mathfrak{A} \subset \mathbb{K}$ *ist* $\mathfrak{A}^{-1} = \{x \in \mathbb{K} \quad | \quad x \cdot \mathfrak{A} \subseteq \mathcal{O}_{\mathbb{K}}\}$.

Diese Gruppe heißt $\mathcal{J}_{\mathbb{K}}$. Die Menge der Hauptideale ist gegenüber der Multiplikation abgeschlossen und bildet daher eine Untergruppe von $\mathcal{J}_{\mathbb{K}}$. Diese Untergruppe heißt $\mathcal{P}_{\mathbb{K}}$

Definition 1.16. Die Faktorgruppe $\mathcal{C}l_{\mathbb{K}} = \mathcal{J}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}$ heißt *Idealklassengruppe.* Die Ordnung der Idealklassengruppe, $h_{\mathbb{K}} = Ord(\mathcal{C}l_{\mathbb{K}})$, heißt *Klassenzahl* von $\mathbb{K}$.

Es gilt, die Folge

$$1 \to {\mathcal{O}_{\mathbb{K}}}^* \to \mathbb{K}^* \to \mathcal{J}_{\mathbb{K}} \to \mathcal{C}l_{\mathbb{K}} \to 1$$

ist exakt.

Satz 1.17. *Die Klassenzahl von* $\mathbb{K}$, $h_{\mathbb{K}}$, *ist endlich.*

2 Quadratische Zahlkörper

Definition 2.1. Ein algebraischer Zahlkörper vom Grad 2 über $\mathbb{Q}$ heißt quadratischer Zahlkörper.

Nach vorigem Kapitel existiert ein über $\mathbb{Q}$ irreduzibles Polynom $f \in \mathbb{Z}[X]$ vom Grad 2, $f(X) = X^2 + aX + b$, so daß

$$\mathbb{K} \simeq \mathbb{Q}[X]/(f) .$$

Sind θ und das zu θ konjugierte $\overline{\theta}$ die Nullstellen von f, so ist $\theta = \frac{-a}{2} + \frac{\sqrt{a^2-4b}}{2}$ und $\overline{\theta} = \frac{-a}{2} - \frac{\sqrt{a^2-4b}}{2}$. Sei $d = a^2 - 4b \in \mathbb{Z}$, dann ist $\mathbb{K} = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$. Ohne Einschränkung ist d quadratfrei, und es folgt: $\mathbb{K}$ entsteht aus $\mathbb{Q}$ durch Adjunktion der Quadratwurzel einer quadratfreien ganzen Zahl.
Im folgenden sei $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ für eine gegebene quadratfreie ganze Zahl d.

Definition 2.2. Ist $d < 0$, so heißt $\mathbb{K}$ *imaginärquadratischer* Zahlkörper. Ist $d > 0$, so heißt $\mathbb{K}$ *reellquadratischer* Zahlkörper.

Die Elemente $x \in \mathbb{K}$ haben die Form $x = p + q\sqrt{d}, \quad p, q \in \mathbb{Q}$, das Konjugierte zu x die Form $\overline{x} = p - q\sqrt{d}$. Für die Norm und die Spur eines Elementes $x \in \mathbb{K}$ ergibt sich daraus,

$$Tr(x) = x + \overline{x} = 2p \quad \text{und} \quad \mathcal{N}(x) = x\overline{x} = p^2 - q^2 d$$

Eine explizite Ganzheitsbasis und damit auch die Körperdiskriminante erhält man durch den folgenden Satz:

Satz 2.3. *Sei $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ quadratfrei, und sei*

$$d_{\mathbb{K}} = \begin{cases} d & , d \equiv 1 \mod 4, \\ 4d & , d \equiv 2, 3 \mod 4, \end{cases} \tag{1}$$

dann ist $\{1, \eta\}$, $\eta = \frac{d_{\mathbb{K}} + \sqrt{d_{\mathbb{K}}}}{2}$ eine Ganzheitsbasis und $d_{\mathbb{K}}$ die Diskriminante von $\mathbb{K}$.

Beweis: Ich zeige zunächst, daß $\{1,\eta\}$ eine Ganzheitsbasis ist. Zu zeigen ist also:

$$x \in \mathbb{K} \text{ ganz} \Longleftrightarrow \text{Es existieren ganze Zahlen } a, b : x = a + b\eta.$$

„$\Longleftarrow$“:

Sei $x = a + b\eta$, $a, b \in \mathbb{Z}$,
dann ist $Tr(x) = 2a + bd_{\mathbb{K}}$ und $\mathcal{N}(x) = a^2 + abd_{\mathbb{K}} + \frac{b^2 d_{\mathbb{K}}}{4}(d_{\mathbb{K}} - 1)$. Es ist also $Tr(x) \in \mathbb{Z}$, und $\mathcal{N}(x)$ ist genau dann in $\mathbb{Z}$, wenn $\frac{b^2 d_{\mathbb{K}}}{4}(d_{\mathbb{K}} - 1) \in \mathbb{Z}$. Da $d_{\mathbb{K}} \equiv 0, 1 \mod 4$ ist, ist $\mathcal{N}(x) \in \mathbb{Z}$ erfüllt.
$\Rightarrow$ x ist ganz, da es der Ganzheitsgleichung $X^2 - Tr(x)X + \mathcal{N}(x) = 0$ genügt.

„$\Longrightarrow$“:

Sei $x \in \mathbb{K}$ ganz, so ist $x = p + q\sqrt{d}$, $p, q \in \mathbb{Q}$, und $X^2 - Tr(x)X + \mathcal{N}(x) = 0$ ist die Ganzheitsgleichung zu x. Aus $Tr(x), \mathcal{N}(x) \in \mathbb{Z}$ folgt:

$Tr(x) = 2p \quad \Rightarrow p = \frac{c}{2}$ für $c \in \mathbb{Z}$

$\mathcal{N}(x) = p^2 - q^2 d = \frac{c^2}{4} - q^2 d.$

$$\begin{aligned} &\text{Ist } d \equiv 1 \mod 4 \quad \Rightarrow \quad q = \frac{b}{2}, \qquad b \in \mathbb{Z} \text{ und } c \equiv b \mod 2\,. \\ &\text{Ist } d \equiv 2, 3 \mod 4 \quad \Rightarrow \quad c \equiv 0 \mod 2, \text{ und } q = \frac{b}{2} \text{ mit } b \equiv 0 \mod 2 \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{also } p, q \in \mathbb{Z}. \end{aligned}$$

Insgesamt ist:[2]
$x = \frac{c}{2} + \frac{b\sqrt{d}}{2}$, $c \equiv b\ (2)$, und ist $d \equiv 2, 3\ (4)$, so gilt $c \equiv b \equiv 0\ (2)$.
Mit $a = \frac{c - bd_{\mathbb{K}}}{2}$ ist $x = a + b\frac{d_{\mathbb{K}} + \sqrt{d_{\mathbb{K}}}}{2} \in \mathbb{Z} + \eta\mathbb{Z}$,

Schließlich ist die Diskriminante von $\mathbb{K}$

$discr(\mathbb{K}) = det^2(\sigma_i \eta^j) = det^2\binom{1\ \ \eta}{1\ \ \bar{\eta}} = (-\sqrt{d_{\mathbb{K}}})^2 = d_{\mathbb{K}}$

$\square$

Bemerkung. Es sei

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} = \frac{1+\sqrt{d_{\mathbb{K}}}}{2} & , d \equiv 1 \mod 4 \\ \sqrt{d} = \frac{\sqrt{d_{\mathbb{K}}}}{2} & , d \equiv 2, 3 \mod 4\,, \end{cases} \tag{2}$$

[2] $x \equiv y\ (z)$ bedeutet $x \equiv y \mod z$

dann ist $\{1,\omega\}$ ebenfalls eine Ganzheitsbasis, und es gilt

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\eta] = \mathbb{Z}[\omega]\,.$$

2.1 Ideale als $\mathbb{Z}$-Moduln

Die gebrochenen Ideale von $\mathbb{K}$ sind nach Satz 1.6 freie $\mathbb{Z}$-Moduln vom Rang 2. Da $\mathbb{K} = \mathbb{Q}(\omega)$ ist, hat ein gebrochenes Ideal $\mathfrak{A}$ eine Darstellung der Form $\mathfrak{A} = [q, \kappa]$, mit $q \in \mathbb{Q}$ und $\kappa \in \mathbb{K} \setminus \mathbb{Q}$.
Nach Definition 1.16 ist die Idealklassengruppe die Faktorgruppe $\mathcal{J}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}$. Die Bildung des Quotienten induziert daher folgende Äquivalenz:

Definition 2.4. Seien $\mathfrak{A}$ und $\mathfrak{B}$ gebrochene Ideale in $\mathbb{K}$, dann gilt $\mathfrak{A} \sim \mathfrak{B}$ genau dann, wenn es ein $x \in \mathbb{K}$ gibt, so daß $(x)\mathfrak{A} = \mathfrak{B}$.

Multipliziert man ein Ideal mit dem Hauptnenner der Erzeugenden des Ideals, so erhält man ein äquivalentes ganzes Ideal. Das bedeutet, daß es in jeder Klasse ganze Ideale gibt und es daher reicht, zur Betrachtung der Idealklassen sich auf ganze Ideale zu beschränken.

Satz 2.5. *Zu einem ganzen Ideal $\mathfrak{A} \subseteq \mathcal{O}_{\mathbb{K}}$ existieren $a, b, m \in \mathbb{Z}$, so daß*

$$\mathfrak{A} = [a, \kappa] = a\mathbb{Z} + \kappa\mathbb{Z}, \quad mit\ \kappa = \frac{-b + m\sqrt{d_{\mathbb{K}}}}{2}\ \ und\ a, m > 0\,.$$

In dieser Darstellung sind die Werte a und m eindeutig, b eindeutig modulo $2a$. Der Wert a ist gegeben durch $min\{\mathfrak{A} \cap \mathbb{N}\}$ und darüber hinaus gilt:

1. $m|a$, $m|b$ *und* $\frac{b}{m} \equiv d_{\mathbb{K}} \mod 2$.
2. $am|\mathcal{N}(\kappa)$ *und* $\mathcal{N}(\mathfrak{A}) = am$

Beweis: Sei $\mathfrak{A}_1 = \mathfrak{A} \cap \mathbb{Z}$. Ist $\mathfrak{A}$ nicht das Nullideal, so ist $\mathfrak{A}_1$ ein Ideal in $\mathbb{Z}$, also $\mathfrak{A}_1 = a\mathbb{Z}$ für eine eindeutige Zahl $a > 0$. Sei $\mathfrak{A}_2 = \{t \in \mathbb{Z} \mid \exists s \in \mathbb{Z} :\ s + t\omega \in \mathfrak{A}_2\}$, dann ist auch $\mathfrak{A}_2$ ein Ideal in $\mathbb{Z}$, also $\mathfrak{A}_2 = m\mathbb{Z}$ für eine eindeutige Zahl $m > 0$. Zu m existiert ein $n \in \mathbb{Z}$, so daß $(n + m\omega)\mathbb{Z}$ in $\mathfrak{A}$ liegt. Das heißt, $a\mathbb{Z} + (n + m\omega)\mathbb{Z} \subseteq \mathfrak{A}$.
Die umgekehrte Inklusion gilt ebenfalls, denn:
Sei $\xi = x + y\omega$ ein Element aus $\mathfrak{A}$, $x, y \in \mathbb{Z}$, so existiert eine ganze Zahl v, so daß $y = vm$. Dann ist $\xi - v(n + m\omega) \in \mathbb{Z}$, d.h. in $\mathfrak{A}_1$. Also gibt es eine ganze Zahl u, so daß $\xi - v(r + m\omega) = ua$, was bedeutet, daß $\mathfrak{A} \subseteq a\mathbb{Z} + (n + m\omega)\mathbb{Z}$.
Man setze $-b = 2n + m$ oder $-b = 2n$, je nachdem ob $d_{\mathbb{K}} \equiv 1\ (4)$ oder

$d_{\mathbb{K}} \equiv 0 \ (4)$ ist.

Zu 1.:
$\mathfrak{A}$ ist ein Ideal von $\mathcal{O}_{\mathbb{K}}$, das bedeutet, daß alle Elemente eine eindeutige Darstellung haben, zum einen als Linearkombination in a und κ, zum anderen als Linearkombination in 1 und ω. Man betrachte das Element $a\omega \in \mathfrak{A}$:

$$\exists x, y \in \mathbb{Z}: \ a\omega = xa + y\kappa = xa + yn + ym\omega$$
$$\Rightarrow \quad a = ym \quad \Rightarrow \quad m|a \text{ , und}$$
$$xa + yn = 0 \ \Leftrightarrow \ xym + yn = 0 \ \Leftrightarrow \ y(xm+n) = 0 \ \Leftrightarrow \ xm = -n$$
$$\Rightarrow \quad m|n \quad \Rightarrow \quad m|b \text{ und } \tfrac{b}{m} \equiv d_{\mathbb{K}} \mod 2 \text{ .}$$

Zu 2.:
Es ist $\mathfrak{A}$ ein Untermodul von $\mathcal{O}_{\mathbb{K}}$ frei von gleichem Rang. $\{1, \omega\}$ ist eine Basis von $\mathcal{O}_{\mathbb{K}}$, $\{a, \kappa\}$ eine von $\mathfrak{A}$. Die Matrix $M = \left(\begin{smallmatrix} a & 0 \\ n & m \end{smallmatrix}\right)$ beschreibt daher den Basiswechsel. Nach [HarHaw, Kap. 7] gilt: $\det M = [\mathcal{O}_{\mathbb{K}} : \mathfrak{A}]$, also $am = \mathcal{N}(\mathfrak{A})$. Da $\kappa \in \mathfrak{A}$, ist $(\kappa) \subseteq \mathfrak{A}$. Daraus folgt, daß $\mathfrak{A} \,|\, (\kappa)$ und damit $\mathcal{N}(\mathfrak{A}) \,|\, \mathcal{N}((\kappa))$. □

Es gilt auch die umgekehrte Aussage:

Lemma 2.6. *Sei $\mathfrak{M} = [a, \kappa]$, mit $\frac{-b+\sqrt{d_{\mathbb{K}}}}{2}$ und $a, b, m, d_{\mathbb{K}} \in \mathbb{Z}$, ein $\mathbb{Z}$-Modul frei vom Rang 2. Gilt*

1. *$m|a$, $m|b$ und $\frac{b}{m} \equiv d_{\mathbb{K}} \mod 2$ und*
2. *$am|\mathcal{N}(\kappa)$,*

dann ist $\mathfrak{M}$ ein ganzes Ideal in $\mathcal{O}_{\mathbb{K}}$.

Beweis: Zu zeigen ist, daß $\mathfrak{M}\mathcal{O}_{\mathbb{K}} \subseteq \mathfrak{M}$ ist, also daß $a\omega \in \mathfrak{M}$ und $\kappa\omega \in \mathfrak{M}$. Hierzu sei $n = ym$, $a = vm$ und $-b = 2n + m$ bzw. $b = 2n$, je nachdem, ob $d_{\mathbb{K}} \equiv 1 \mod 2$ oder $d_{\mathbb{K}} \equiv 0 \mod 2$ mit ganzen Zahlen n, y und v.

$$a\omega = v\kappa - vn = -vmy + v\kappa = a(-y) + v\kappa \in \mathfrak{M}.$$

Ist $d_{\mathbb{K}} \equiv 0 \mod 2$, so ist $-b = 2n$ und $\omega = \frac{\sqrt{d_{\mathbb{K}}}}{2}$:

$$\begin{aligned} \kappa\omega &= \tfrac{2n+m\sqrt{d_{\mathbb{K}}}}{2}\tfrac{\sqrt{d_{\mathbb{K}}}}{2} = \tfrac{md_{\mathbb{K}}+2n\sqrt{d_{\mathbb{K}}}}{4} = \tfrac{md_{\mathbb{K}}}{4} + \tfrac{n\sqrt{d_{\mathbb{K}}}}{2} = y\omega + yn - yn + \tfrac{md_{\mathbb{K}}}{4} \\ &= y\kappa + \tfrac{md_{\mathbb{K}}-4my^2}{4} = y\kappa + \tfrac{d_{\mathbb{K}}-b^2}{4m} = y\kappa + \tfrac{\mathcal{N}(\kappa)}{m} \\ &= wa + y\kappa \in \mathfrak{M}, \text{ für ein } w \in \mathbb{Z}, \end{aligned}$$

Ist $d_{\mathbb{K}} \equiv 1 \mod 2$, so ist $-b = 2n+1$ und $\omega = \frac{1+\sqrt{d_{\mathbb{K}}}}{2}$:

$$\begin{aligned}
\kappa\omega &= \tfrac{2n+m+m\sqrt{d_{\mathbb{K}}}}{2}\tfrac{1+\sqrt{d_{\mathbb{K}}}}{2} = \tfrac{2n+m+md_{\mathbb{K}}+(2n+2m)\sqrt{d_{\mathbb{K}}}}{4} \\
&= \tfrac{2ym+2m+m(d_{\mathbb{K}}-1)}{4} + \tfrac{(ym+m)\sqrt{d_{\mathbb{K}}}}{2} = (y+1)m\omega + (y+1)n - (y+1)n + m\tfrac{(d_{\mathbb{K}}-1)}{4} \\
&= (y+1)\kappa + m((y+1)y + \tfrac{(d_{\mathbb{K}}-1)}{4}) = (y+1)\kappa + \tfrac{\mathcal{N}(\kappa)}{m} \\
&= wa + (y+1)\kappa \in \mathfrak{M}, \text{ für ein } w \in \mathbb{Z}.
\end{aligned}$$

□

Definition 2.7. Sei $\mathfrak{A}$ ein ganzes Ideal. Die Darstellung $\mathfrak{A} = [a, \kappa]$, gemäß Satz 2.5 heißt *kanonisch* für $\kappa = \frac{-b+m\sqrt{d_{\mathbb{K}}}}{2}$, falls

(i) für $d_{\mathbb{K}} < 0$ gilt: $-a < -b \leq a$,

(ii) für $d_{\mathbb{K}} > 0$ gilt: $0 < -b \leq 2a$.

Damit erhält man eine eindeutige Darstellung für ein Ideal.

Definition 2.8. Ein Ideal $\mathfrak{A} \subseteq \mathcal{O}_{\mathbb{K}}$ habe die kanonische Darstellung $\mathfrak{A} = [a, \kappa]$.

- $\mathfrak{A}$ heißt *primitiv*, wenn m=1 ist.
  Ist $m \neq 1$, so erhält man wegen $m|a$ und $m|b$: $\frac{1}{m}\mathfrak{A} \subseteq \mathcal{O}_{\mathbb{K}}$ ist zu $\mathfrak{A}$ äquivalent und primitiv.

- Sei $\overline{\kappa}$ zu κ konjugiert, so heißt $\overline{\mathfrak{A}} = [a, \overline{\kappa}]$ das zu $\mathfrak{A}$ *konjugierte* Ideal.

- Sei $\mathfrak{A}$ primitiv, so heißt $\mathfrak{A}$ *reduziert* für

  (i) $d_{\mathbb{K}} < 0$, wenn $a \leq c = \frac{b^2-d_{\mathbb{K}}}{4a}$ und $0 \leq -b \leq a$, falls $a = c$ bzw.

  (ii) $d_{\mathbb{K}} > 0$, wenn es kein Element $\alpha \in \mathfrak{A}$ gibt, so daß sowohl $|\alpha| < a$ als auch $|\overline{\alpha}| < a$ erfüllt ist.

Die Definition von Reduziertheit im reellquadratischen Zahlkörper läßt sich etwas anschaulicher formulieren.

Korollar 2.9. *Sei $\mathfrak{A} = [a, \kappa]$ primitiv und in kanonischer Darstellung gegeben, $d_{\mathbb{K}} > 0$. Dann gilt: $\mathfrak{A}$ ist genau dann reduziert, wenn es ein $\beta \in \mathfrak{A}$ gibt, so daß $\mathfrak{A} = [a, \beta]$ und $\beta > a$, $-a < \overline{\beta} < 0$.*

Beweis: Es sei $\mathfrak{A} = [a, \kappa]$ reduziert, mit $\kappa = \frac{-b+\sqrt{d_{\mathbb{K}}}}{2}$. Nun existieren unendlich viele Paare $(x, y) \in \mathbb{Z}^2 \setminus (0, 0)$ mit

$$|xa + y\overline{\kappa}| < a\,,$$

z.B. $x = \lfloor \frac{-y\overline{\kappa}}{a} \rfloor$ und $k = 1, 2, \ldots$. Sei für ein solches Paar (t, s) $\gamma = ta + s\kappa$. Dann ist die Menge $A = \{\alpha \in \mathfrak{A} \mid |\overline{\alpha}| < a$ und $|\alpha \leq \gamma\}$ endlich.
Denn:
Für α aus $\mathfrak{A}$ gilt: Ist $\alpha = xa + y\kappa$, so ist $\alpha = \overline{\alpha} + y\sqrt{d_{\mathbb{K}}}$. Ist außerdem $\alpha \in A$, dann ist auch $|\overline{\alpha}| < a$ und:

$$|\alpha| = |\overline{\alpha} + y\sqrt{d_{\mathbb{K}}}| \geq |y\sqrt{d_{\mathbb{K}}}| - a\,.$$

Da $\alpha \in A$, ist $|\alpha| \leq |\gamma|$. Es kann also nur endlich viele Werte $y \in \mathbb{Z}$ geben , die die obige Ungleichung erfüllen. Zu diesen Werte von y kann es nur endlich viele Werte x geben, so daß $|\overline{\alpha}| < a$ erfüllt ist.
Nun sei β das Minimum der positiven Elemente in A, also $\beta > 0$ und $|\overline{\beta}| < a$. Da $\mathfrak{A}$ reduziert ist und $|\overline{\beta}| < a$, ist $\beta > a$. Da $\beta - a \in \mathfrak{A}$ und $0 < \beta - a < \beta$, ist $|\overline{\beta} - a| > a > |\overline{\beta}|$, da $\beta > 0$ minimal gewählt ist. Aus $|\overline{\beta} - a| > |\overline{\beta}|$ folgt, daß $\overline{\beta}$ und a verschiedene Vorzeichen haben, also ist $\overline{\beta} < 0$.

Es bleibt zu zeigen, daß $\mathfrak{A}$ von a und β erzeugt wird:
Sei $\beta = pa + q\kappa\ , p, q \in \mathbb{Z}$.
Angenommen, $|q| > 1$ und $s \equiv p \mod |q|$, so daß $|s| \leq \frac{|q|}{2}$. Dann ist $\frac{\beta - sa}{q} = \kappa + xa \in \mathfrak{A}$ für $x \in \mathbb{Z}$. Sei $\mu = \left|\frac{\beta - sa}{q}\right| \in \mathfrak{A}$. So ist zum einen $\mu > 0$ und zum anderen gilt

$$|\overline{\mu}| = \left|\frac{\overline{\beta} - sa}{q}\right| \leq \left|\frac{\overline{\beta}}{q}\right| + \left|\frac{sa}{q}\right| < \frac{a}{2} + \frac{a}{2} = a\,.$$

Außerdem gilt

$$\mu \leq \left|\frac{\beta}{q}\right| + \left|\frac{sa}{q}\right| < \frac{\beta}{2} + \frac{a}{2} < \beta\,,$$

im Widerspruch zur Wahl von β. $\Rightarrow$ $|q| \leq 1$. Da natürlich $q \neq 0$, ist $q = \pm 1$, und damit gilt $\mathfrak{A} = [a, \beta]$, mit $\beta > a$ und $-a < \overline{\beta} < 0$.

Sei andererseits $\mathfrak{A} = [a, \beta]$, mit $\beta > a$ und $-a < \overline{\beta} < 0$ gegeben. Angenommen, $\mathfrak{A}$ sei nicht reduziert, dann existiert ein $\alpha \in \mathfrak{A}$, mit $|\alpha| < a$ und $|\overline{\alpha}| < a$ und der Darstellung $\alpha = xa + y\beta$. Dann gelten folgende zwei Ungleichungen:

$$|xa + y\beta| < a \;\text{ und }\; |xa + y\overline{\beta}| < a\,.$$

Ist $x = 0$ oder $xy > 0$, so ist die linke Ungleichung nicht erfüllt, ist $y = 0$ oder $xy < 0$, so ist die zweite Ungleichung nicht erfüllt. Also kann es ein solches α nicht geben. $\square$

An Definition 2.8 sieht man, daß in jeder Klasse primitive Ideale existieren. Es genügt daher, sich auf diese zu beschränken, um die Idealklassengruppe zu beschreiben. Da es in jeder Klasse in der Regel nicht nur ein primitives Ideal gibt, versucht man möglichst eindeutige Repräsentanten zu finden. Diese sind die reduzierten Ideale. Ist $d < 0$, so gibt es in jeder Klasse nur ein reduziertes Ideal. Ist $d > 0$, so ist die Anzahl der reduzierten Ideale endlich, und sie bilden unter Anwendung des Reduktionsverfahrens einen Zykel.
Den reduzierten Idealen sowie den Reduktionsverfahren widme ich mich in Kapitel 3. Zuvor beschreibe ich noch einige in diesem Zusammenhang hilfreiche Eigenschaften von quadratischen Irrationalzahlen und führe in die Theorie binär-quadratischer Formen ein. Man wird sehen, daß die letzteren auf eindeutige Weise mit den primitiven Idealen korrespondieren.

2.2 Quadratische Irrationalzahlen

Mit Definition 2.4 erhält man folgendes: Die Idealklasse eines in kanonischer Darstellung gegebenen Ideals $\mathfrak{A} = [a, \kappa]$ wird bereits vollständig durch die quadratische Irrationalzahl

$$\tau = \frac{\kappa}{a} \in \mathbb{C} \setminus \mathbb{Q}, \tag{3}$$

beschrieben, mit $a > 0$ und positivem Vorzeichen vor der Quadratwurzel in κ.
Denn ist $\mathfrak{A} \sim \mathfrak{B}$, so existiert $x \in \mathbb{K}$ mit $\mathfrak{B} = x\mathfrak{A} = [xa, x\kappa]$, und die Klasse von $\mathfrak{B}$ wird beschrieben durch $\tau' = \frac{x\kappa}{xa} = \frac{\kappa}{a} = \tau$. $\mathfrak{A}$ und $\mathfrak{B}$ liegen in derselben Klasse, und somit ist diese Klasse vollständig durch τ beschrieben.
Im weiteren verwende ich für eine solche Zahl den Begriff *zum Ideal* oder *zur Klasse des Ideals gehörende Irrationalzahl.*
Es stellt sich daher die Frage, inwieweit τ eindeutig ist. Es gilt für die Ideale $\mathfrak{B}$ der Klasse von $\mathfrak{A} = [a, \kappa]$, $\mathfrak{B} \sim [1, \tau]$. τ ist aber nicht eindeutig, denn es gilt das folgende Lemma.

Lemma 2.10. *Seien $\tau, \tau' \in \mathbb{C}$, so gilt*

$$[1, \tau] = [1, \tau'] \quad \Leftrightarrow \quad \tau' = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}$$

mit $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ und $\alpha\delta - \beta\gamma = \pm 1$.

Beweis: $[1,\tau]$ und $[1,\tau']$ seien zwei Basen desselben Moduls über $\mathbb{Z}$, dann existiert eine Matrix $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{Z})$, so daß $\binom{\tau'}{1} = \binom{\alpha\tau+\beta}{\gamma\tau+\delta}$.
Damit gilt $\tau' = \frac{\tau'}{1} = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$.

□

Bemerkung. Für die Möbiustransformation $\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$ schreibe ich im weiteren kurz $M\tau$, mit $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{Z})$. Vergleiche dazu auch Abschnitt 3.1.1.
Ist $\tau' = M\tau = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$, so erhält man für τ':

$$\begin{aligned} \tau' &= \frac{\alpha\tau+\beta}{\gamma\tau+\delta} = \frac{(\alpha\tau+\beta)(\gamma\overline{\tau}+\delta)}{\mathcal{N}(\gamma\tau+\delta)} \\ &= \frac{\alpha\gamma\mathcal{N}(\tau)+\beta\delta+\alpha\delta\tau+\beta\gamma\overline{\tau}+\beta\gamma\tau-\beta\gamma\tau}{\mathcal{N}(\gamma\tau+\delta)} \\ &= \frac{\beta\delta+\alpha\gamma\mathcal{N}(\tau)+\beta\gamma Tr(\tau)+(detM)\tau}{\mathcal{N}(\gamma\tau+\delta)} \end{aligned} \tag{4}$$

Sei τ die durch Gleichung (3) gegebene zu $\mathfrak{A} = [a,\kappa]$ mit $\kappa = \frac{-b+\sqrt{d_{\mathbb{K}}}}{2}$, gehörende Irrationalzahl.
Ist $d_{\mathbb{K}} < 0$, so gilt für τ:
$\tau \in \mathcal{H} = \{z \in \mathbb{C} \,|\, \Im(z) > 0\}$. [3] Die zu den in kanonischer Darstellung gegebenen Idealen gehörenden Irrationalzahlen liegen also in der oberen komplexen Halbebene. Beschreibt τ' ebenfalls die Klasse von $\mathfrak{A}$ vollständig, so ist nach Gleichung (4), $\Im(\tau') = \frac{(detM)}{\mathcal{N}(\gamma\tau+\delta)}$. Da $\mathcal{N}(x) \geq 0$, $\forall x \in \mathbb{Q}(\sqrt{d_{\mathbb{K}}})$ für $d_{\mathbb{K}} < 0$, erhält man :

$$\tau' \in \mathcal{H} \Leftrightarrow detM = 1$$

Ist $d_{\mathbb{K}} > 0$, so ist das Ideal $a'[1,\tau']$ genau dann in kanonischer Darstellung gegeben, wenn [4] $sign\big((\mathcal{N}(\gamma\tau+\delta)\big) = detM$.

Insgesamt erhält man:

Korollar 2.11. *Seien τ_1 und τ_2 quadratische Irrationalzahlen mit $\tau_i = \frac{-b_i+\sqrt{d_{\mathbb{K}}}}{2a_i}$, $a_i, b_i \in \mathbb{Z}$ und $4a_i | b_i^2 - d_{\mathbb{K}}$. τ_1 und τ_2 repräsentieren genau dann dieselbe Idealklasse, wenn $\tau_2 = M\tau_1$, mit $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{Z})$.*

[3] Mit $\Im(z)$ und $\Re(z)$ sei der Imaginärteil, bzw der Realteil der komplexen Zahl $z \in \mathbb{C}$ bezeichnet.

[4] $sign(x)$ bezeichne das Vorzeichen von $x \in \mathbb{R}$

Gilt zusätzlich $a_1, a_2 > 0$, so gilt:

- *für $d_{\mathbb{K}} < 0$: τ_1 und τ_2 repräsentieren genau dann dieselbe Idealklasse, wenn $M \in SL_2(\mathbb{Z})$.*
- *für $d_{\mathbb{K}} > 0$: τ_1 und τ_2 repräsentieren genau dann dieselbe Idealklasse, wenn $M \in GL_2(\mathbb{Z})$ und $sign\big((\mathcal{N}(\gamma\tau + \delta)\big) = det M$.*

Definition 2.12. Eine quadratische Irrationalzahl $\tau = \frac{-b+\sqrt{d}}{2a}$, mit $a > 0$ und $4a|b^2 - d$, heißt *primitiv*, wenn $ggT(a, b, \frac{b^2-d}{4a}) = 1$.
Zwei quadratische Irrationalzahlen $\tau, \tau' \in \mathcal{H}$ heißen *äquivalent*, wenn sie dieselbe Idealklasse repräsentieren.

2.3 Binär-quadratische Formen

Definition 2.13. Eine binär-quadratische Form f ist ein homogenes Polynom über $\mathbb{Z}$ in zwei Unbestimmten vom Grad 2, der Gestalt

$$f(X, Y) = aX^2 + bXY + cY^2, \in \mathbb{Z}[X, Y]$$

$d_f = b^2 - 4ac$ heißt *Diskriminante* der Form f. Gilt $d_f \equiv 1 \mod 4$ oder $d_f \equiv 0 \mod 4$ mit $\frac{d_f}{4} \equiv 2$ oder $3 \mod 4$, und enthalte d_f bzw. $\frac{d_f}{4}$ keinen quadratischen Teiler, so heißt d_f *fundamental*.

Der Einfachheit halber sei im folgenen f beschrieben durch $f = (a, b, c)$. Betrachtet man f als inhomogenes Polynom in $Z = \frac{X}{Y}$, so sind $\tau = \frac{-b+\sqrt{d_f}}{2a}$ und $\overline{\tau}$ die Nullstellen von f, als welche ich sie im weiteren auch bezeichnen werde. Außerdem schreibe ich meistens lediglich *Form*, da ich ausschließlich binär-quadratische Formen betrachte.
Es läßt sich $f : \mathbb{Z}^2 \to \mathbb{Z}$ eindeutig durch eine symmetrische Matrix $A_f \in M(2, \mathbb{Q})$ beschreiben:

$$f(x, y) = (x, y)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = {}^t v A_f v, \text{ für } v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$$

Bemerkung. Man beachte: $d_f = -4 \det A_f$.

Definition 2.14. Auf folgende Weise liefert $SL_2(\mathbb{Z})$ eine Äquivalenzrelation auf Formen:
f ist genau dann äquivalent zu g, wenn es eine Matrix $B = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ gibt, so daß

$$g(v) = g(x,y) = f(\alpha x + \beta y, \gamma x + \delta y) = f(Bv), \text{ mit } v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 .$$

Ich werde im weiteren die Schreibweise $f' = Mf$ benutzen, statt $f'(v) = f(Mv)$, da mich die Form f als Zahlentripel und nicht so sehr als Abbildung von $\mathbb{Z}^2$ nach $\mathbb{Z}$ interessiert. Die Koeffizienten von f' lassen sich dann aus M und f wie folgt bestimmen:

$$\begin{aligned} a' =& f(\alpha,\gamma) = a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' =& 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ c' =& f(\beta,\delta) = a\beta^2 + b\beta\delta + c\delta^2 \end{aligned}$$

Ist M Produkt zweier Matrizen $A, B \in SL_2(\mathbb{Z})$, also $M = AB$, so ist folgendes zu beachten:

$$f'(v) = f(ABv) = f(A(Bv)) = Af(Bv) = B(Af(v)) ,$$

also $Mf = (AB)f = B(Af)$.

Definition 2.15. Sei $f = (a,b,c)$, dann heißt f

(i) *positiv definit*, wenn A_f positiv definit ist,

(ii) *negativ definit*, wenn A_f negativ definit ist oder

(iii) *indefinit*, wenn A_f indefinit ist.

Korollar 2.16. *Ist* $\det A_f < 0$*, also* $d_f > 0$*, so ist* f *indefinit.*
Ist $\det A_f > 0$*, also* $d_f < 0$*, so hängt es vom Vorzeichen von* a *ab, ob* A_f *und damit auch* f *positiv definit ist oder negativ definit. Der erste Fall tritt ein, für* $a > 0$*, der zweite für* $a < 0$*.*

Bemerkung. 1. Im weiteren ist es nützlich, sich auf Formen (a,b,c) mit $a > 0$ zu beschränken. Hierzu identifiziere ich die Formen (a,b,c) und $(-a,b,-c)$ miteinander, was der Aktion von

$$J = \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right) \in SL_2(\mathbb{C})$$

auf (a,b,c) entspricht. Das heißt, von nun an gelte beispielsweise $(-1,2,3) = (1,2,-3)$.
Auf diese Weise reicht, es nur die Mengen der indefiniten und die der positiv definiten Formen zu betrachten, die unter der Aktion von $SL_2(\mathbb{Z}) \cup \{J\}$ abgeschlossen sind, da die Diskriminante invariant ist unter Äquivalenzumformungen und durch die Aktion von J die negativ definiten Formen mit den positiv definiten Formen identifiziert wurden.

2. Der Vollständigkeit halber erwähne ich noch die *irregulären* Formen. Das sind Formen $f = (a,b,c)$, die rationale Nullstellen, also eine Zerlegung $f(x,y) = (rx+sy)(tx+uy)$ mit rationalen Koeffizienten r, s, t und u haben.
An der Darstellung $4af(x,y) = (2ax+by)^2 - d_f y^2$ erkennt man leicht, daß f nur dann eine Zerlegung der obigen Gestalt besitzt, wenn d_f eine Quadratzahl ist. Im Zusammenhang mit der Idealklassengruppe treten aber nur Formen zu vorgegebener fundamentaler Diskriminante $d_f \neq 0$ auf, so daß die irregulären Formen in diesem Zusammenhang nicht weiter von Bedeutung sind.

Definition 2.17. Sei $f = (a,b,c)$ eine binär-quadratische Form.

- f heißt *primitiv*, wenn $ggT(a,b,c) = 1$.
- f heißt *reduziert*, wenn gilt
  - f ist eine positiv definite Form, und es gilt
    $$-a \leq b < a, \; 0 < a \leq c. \text{ Ist } a = c \Rightarrow b \leq 0$$
    .
  - f ist eine indefinite Form, und es gilt
    $$0 < \left| \sqrt{d_f} - 2|a| \right| < -b < \sqrt{d_f}$$

Bemerkung. Ist die Diskriminante von f quadratfrei, so ist f bereits primitiv. Die Reduziertheit erkläre ich nicht für negativ definite Formen, da ich diese mit den positiv definiten via J identifiziert habe. Es ließe sich aber aus dieser Definition auch eine Definition für negativ definite Formen ableiten. Denn sei (a,b,c) eine negativ definite Form, so ist diese reduziert, wenn die positiv definite Form $(-a,b,-c)$ reduziert ist.

Ist $d_f < 0$, sieht man mit $4ac = b^2 + |d_f|$ und $|b| \leq a \leq c$, daß es nur endlich viele reduzierte Formen geben kann. Denn die Werte a, b und c, so daß $f = (a, b, c)$ reduziert ist, sind durch die Ungleichung $3a^2 < |d_f|$ beschränkt. Ist $d_f > 0$, so sind a und b nach Definition beschränkt. Da c eindeutig von a, b und d_f abhängt, gibt es auch in diesem Fall nur endlich viele reduzierte Formen. Im Kapitel 3 wird man sehen, daß es in jeder Klasse mindestens eine reduzierte Form gibt. Daher ist die Anzahl der Klassen endlich, und sie entspricht im Fall $d_f < 0$ genau der Klassenzahl $h_{\mathbb{K}}$ von $\mathbb{K} = \mathbb{Q}(\sqrt{d_f})$. Im Fall $d_f > 0$ entspricht die Anzahl der Formen der Klassenzahl im engeren Sinn von $\mathbb{K} = \mathbb{Q}(\sqrt{d_f})$. Ich werde allerdings nur eine Teilmenge der Formenklassen betrachten, deren Ordnung auch für $d_f > 0$ genau der Klassenzahl entspricht.

2.4 Bijektionen zwischen Idealen, Formen und Irrationalzahlen

In diesem Abschnitt erkläre ich in Anlehnung an [Cohen, Kap.5.2] Abbildungen zwischen primitiven Idealen, Formen und primitiven Irrationalzahlen. Ich habe allerdings darauf verzichtet, im Gegensatz zu Cohen, diese Abbildungen möglichst allgemein zu definieren, sondern habe sie speziell für diesen Kontext formuliert.
Diese Abbildungen erhalten die auf den jeweiligen Mengen definierten Äquivalenzen, so daß man anschließend alle Aussagen über die Idealklassengruppe mit Hilfe von binärquadratischen Formen bzw. Irrationalzahlen beschreiben kann, da, wie bereits beschrieben, jede Idealklasse primitive Ideale enthält.

Sei im folgenden D eine ganze Zahl, die den Eigenschaften einer fundamentalen Diskriminante aus Definition 2.13 genügt. Für Idealklassen und Irrationalzahlen sei dann $d_{\mathbb{K}} = D$, also sei $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, und für binär-quadratische Formen sei $d_f = D$. Die drei Mengen seien dann wie folgt gegeben:

$$I := \{\mathfrak{A} \subseteq \mathcal{O}_{\mathbb{K}} \mid \mathfrak{A} = [a, \tfrac{-b+\sqrt{D}}{2}] \text{ ist primitives Ideal}\}$$
$$Q := \{\tau \in \mathbb{C} \setminus \mathbb{Q} \mid \tau = \frac{-b+\sqrt{D}}{2a},\ a > 0 \text{ und } 4a|(D-b^2)\}$$
$$F := \{f = (a, b, c) \mid f \text{ ist binär-quadratische Form mit } a > 0 \text{ und } D = b^2 - 4ac\}$$

Man erinnere sich, daß die Basis eines primitives Ideals abgesehen von b eindeutig ist, und der Wert b eindeutig ist modulo $2a$. Weiterhin ist die Primitivität der Elemente aus F und Q bereits dadurch gegeben, daß D eine fundamentale Diskriminante ist. Denn nimmt man das Gegenteil an, so erhält

man mit $D = b^2 - 4ac$ einen Widerspruch.
Nun zu den Abbildungen zwischen I, Q und F:

Definition 2.18.

$$\Psi_{FQ}: \quad F \to Q\,, \quad f = (a,b,c) \quad \mapsto \quad \frac{-b+\sqrt{D}}{2a}$$

$$\Psi_{QF}: \quad Q \to F\,, \quad \tau = \frac{-b+\sqrt{D}}{2a} \quad \mapsto \quad (a, b, \tfrac{b^2-D}{4a})$$

$$\Psi_{QI}: \quad Q \to I\,, \quad \tau = \frac{-b+\sqrt{D}}{2a} \quad \mapsto \quad a[1,\tau]$$

$$\Psi_{IQ}: \quad I \to Q\,, \quad \mathfrak{A} = [a, \frac{-b+\sqrt{D}}{2}] \text{ in kanonischer Darstellung} \quad \mapsto \quad \frac{-b+\sqrt{D}}{2a}$$

$$\Psi_{FI}: \quad F \to I\,, \quad f = (a,b,c) \quad \mapsto \quad \left[a, \frac{-b+\sqrt{D}}{2}\right]$$

$$\Psi_{IF}: \quad I \to F\,, \quad \mathfrak{A} = [a, \frac{-b+\sqrt{D}}{2}] \text{ in kanonischer Darstellung} \quad \mapsto \quad (a, b, \tfrac{b^2-D}{4a})$$

Die ersten beiden Abbildungen sind die Bijektionen zwischen binärquadratischen Formen und ihren Nullstellen mit positivem Irrationalteil. Die mittleren zwei sind ebenfalls bereits bekannt, denn es sind die Abbildungen zwischen primitiven Idealen in kanonischer Darstellung und den *zu ihnen gehörenden* Irrationalzahlen. Es stellt sich daher nur die Frage, ob die letzten zwei tatsächlich Abbildungen zwischen primitiven Formen und primitiven Idealen sind, also ob $\Psi_{IF}(\mathfrak{A})$ eine Form bzw. ob $\Psi_{FI}(f)$ ein Ideal ist. Die Primitivität ergibt sich jeweils aus der Konstruktion.
Um zu sehen, daß $\Psi_{IF}(\mathfrak{A})$ eine binär-quadratische Form zur Diskriminante D ist, genügt es, die Diskriminantengleichung $d_f = b^2 - 4ac$ für $d_f = D$ zu betrachten. Diese ist aber nach Konstruktion erfüllt.
Das Bild von Ψ_{FI} ist zunächst nur ein freier $\mathbb{Z}$-Modul vom Rang 2. Es gilt aber $b^2 \equiv b \equiv D \mod 2$ und $4a \mid b^2 - D$. Nach Lemma 2.6 ist dieser Modul dann ein ganzes Ideal.

Es ist klar, daß die Abbildungen Ψ_{IX} für $X = F, Q$ injektiv, aber nicht surjektiv sind, da zum Beispiel $(a, b+2a, a+b+c)$ eine primitive Form in F ist, jedoch nicht in $\Psi_{IF}(I)$ liegt, falls $[a, \frac{-b+\sqrt{D}}{2}]$ ein primitives Ideal in kanonischer Darstellung ist.

Andererseits sind die Abbildungen Ψ_{XI} für $X = F, Q$ zwar surjektiv, da die Ideale $[a, \frac{-b+\sqrt{D}}{2}]$ und $[a, \frac{-b+2a+\sqrt{D}}{2}]$ gleich sind, aber, wie man an dem Beispiel bereits sieht, nicht injektiv.
Dies ließe sich von vornherein vermeiden, indem man die Abbildungen etwas anders definiert. Dazu gebe ich zwei Varianten an:

1. Die Abbildungen Ψ_{IX} und Ψ_{XI} definiert man auf den Basen, statt auf den Idealen selbst. Das bedeutet, daß man I durch eine Teilmenge von $\mathbb{Z} \times (\mathcal{O}_{\mathbb{K}} \setminus \mathbb{Z})$ ersetzen müßte. Zwar wären die Abbildungen dann bijektiv, jedoch hätte man das Problem lediglich verschoben, da man letztendlich eine Beziehung zwischen Idealen und Formen erhalten möchte, es aber keine eindeutige Basis zu einem Ideal gibt.

2. Verändert man in der Eingabe von Ψ_{IX} den Wert von b um $2ma$ für $m \in \mathbb{Z}$, so entspricht dies der Aktion von $M = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$ auf dem Bild.
Die Menge $\Gamma_\infty = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right), n \in \mathbb{Z}\}$ ist eine Untergruppe von $SL_2(\mathbb{Z})$, so daß man die Quotientenmengen $\hat{F} = F/\Gamma_\infty$ und $\hat{Q} = Q/\Gamma_\infty$ bilden kann, wobei die Aktion von Γ_∞ auf F erklärt ist durch: $\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right) : (a, b, c) \mapsto (a, 2am + b, am^2 + bm + c)$, und als gebrochen lineare Abbildung auf Q durch: $\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right) : \tau \mapsto \tau + m$.
Hierdurch erhielte man mit Ψ_{IX} und Ψ_{XI} bijektive Abbildungen zwischen den Mengen $I, \hat{F}$ und $\hat{Q}$, also nur eine Beziehung zwischen Idealen und Klassen von Formen bzw. Irrationalzahlen.

Ich habe mich nicht für diese Varianten entschieden, da die gewählte Definition den Vorteil hat, daß man auf sehr einfache Weise zwischen primitiven Idealen, Formen und Irrationalzahlen hin- und herrechnen kann. Außerdem erübrigt sich dieses scheinbare Manko, wenn man die Abbildungen auf die jeweils erklärten Äquivalenzklassen ausdehnt, da $\Gamma_\infty \subset SL_2(\mathbb{Z})$ ist. Aus den obigen Überlegungen folgt dann, daß die in Definition 2.18 erklärten Abbildungen Bijektionen zwischen den Quotientenmengen $\mathcal{C}l_{\mathbb{K}}, F/SL_2(\mathbb{Z})$ und $Q/GL_2(\mathbb{Z})$ sind.
Es ist aber noch zu zeigen, daß die Äquivalenzen erhalten bleiben:

Satz 2.19. *Die in Definition 2.18 definierten Abbildungen erhalten die auf Idealen, Irrationalzahlen und Formen jeweils erklärten Äquivalenzen.*

Beweis:

1. Ich betrachte zunächst Ψ_{QI} und Ψ_{IQ}. Seien $\mathfrak{A}$ und $\mathfrak{A}'$ primitive Ideale. Sei $\tau = \Psi_{IQ}(\mathfrak{A})$ und $\tau' = \Psi_{IQ}(\mathfrak{A}')$. Dann gilt nach Abschnitt 2.2, daß

die Klasse von $\mathfrak{A}$ vollständig durch τ repräsentiert wird und die Klasse von $\mathfrak{A}'$ durch τ'. Nach Definition 2.12 gilt

$$\tau \sim \tau' \Longleftrightarrow \mathfrak{A} \sim \mathfrak{A}'.$$

2. Nun zu Ψ_{FQ} und Ψ_{QF}.
   Zu zeigen: Ist $f \sim f'$, so muß gelten

$$\Psi_{FQ}(f) = \tau \sim \tau' = \Psi_{FQ}(f') \,.$$

   Ist $f = (a,b,c)$, $f' = (a',b',c')$, so existiert eine Matrix M, so daß $f' = Mf$ und entweder $M \in SL_2(\mathbb{Z})$ oder $MJ \in SL_2(\mathbb{Z})$, mit $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ oder $M = \left(\begin{smallmatrix} -i\alpha & -i\beta \\ i\gamma & i\delta \end{smallmatrix}\right)$ und $J = \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right)$. Damit ist

$$A_{f'} = {}^tMA_fM = \begin{pmatrix} \pm(a\alpha^2 + b\alpha\gamma + c\gamma^2) & \frac{2a\alpha\beta + b(\alpha\delta+\beta\gamma)+2c\gamma\delta}{2} \\ \frac{2a\alpha\beta + b(\alpha\delta+\beta\gamma)+2c\gamma\delta}{2} & \pm(a\beta^2 + b\beta\delta + c\delta^2) \end{pmatrix},$$

   also $a' = \pm f(\alpha,\gamma)$ und $b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$.
   Daraus folgt, daß
   $\tau = \Psi_{FQ}(f) = \frac{-b+\sqrt{D}}{2a}$ und $\tau' = \Psi_{FQ}(f') = \frac{-(2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta)+\sqrt{D}}{2|f(\alpha,\gamma)|}$
   Nun gilt $\tau \sim \tau'$, wenn es eine Matrix $\tilde{M} = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ gibt, so daß $\tau' = \tilde{M}\tau$. $\tilde{M} \in SL_2(\mathbb{Z})$, falls $f(\alpha,\gamma) > 0$, bzw. $\tilde{M} \in GL_2(\mathbb{Z})$ und $sign\big(\mathcal{N}(t\tau + r)\big) = det\tilde{M}$, falls $f(\alpha,\gamma) < 0$.

   Sei also $\tau' = \tilde{M}\tau$ für $\tilde{M} = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$:

$$\begin{aligned}
\tau' = \tilde{M}\tau &= \frac{r\tau + s}{t\tau + u} \\
&= \frac{(r\tau + s)(t\overline{\tau} + u)}{(t\tau + u)(t\overline{\tau} + u)} = \frac{us + tr\mathcal{N}(\tau) + stTr(\tau) + det\tilde{M}\tau}{\mathcal{N}(t\tau + u)} \\
&= \frac{4a^2(us + (\frac{b^2-D}{4a^2})tr + \frac{-b}{a}st + det\tilde{M}\frac{-b}{2a}) + det\tilde{M}\frac{\sqrt{D}}{2}}{4a^2u^2 + 4abut + (b^2 - D)t^2} \\
&= \frac{a(2us + 2ctr - 2bst - (ur - st)b) + det\tilde{M}\sqrt{D}}{2(au^2 + but + ct^2)} \\
&= \frac{(2aus - b(ru + st) + 2ctr) + det\tilde{M}\sqrt{D}}{2f(u,t)}
\end{aligned}$$

Ist $f(\alpha,\gamma) > 0$, so erhält man für $\tilde{M} = M^{-1} \in SL_2(\mathbb{Z})$: $\tau' = \frac{-b'+\sqrt{D}}{2a'}$.
Ist $f(\alpha,\gamma) < 0$, so erhält man für $\tilde{M} = \left(\begin{smallmatrix} \delta & -\beta \\ \gamma & -\alpha \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$: $\tau' = \frac{-b'+\sqrt{D}}{2|a'|}$,
denn es ist $\mathcal{N}(-\gamma\tau+\alpha) = \mathcal{N}(\gamma\tau-\alpha) = 2af(\alpha,\gamma)$.Das Vorzeichen von $\mathcal{N}(-\gamma\tau+\alpha)$ richtet sich also nach dem von $f(\alpha,\gamma)$.
Damit weiß man, daß auch Ψ_{QF} die Äquivalenz erhält.

Ergebnis: Sei $M \in SL_2(\mathbb{Z})$. Dann gilt für $\tau = \Psi_{FQ}(f)$ und $\tau' = \Psi_{FQ}(f')$:

$$f' = Mf \quad \Leftrightarrow \quad \tau' = M^{-1}\tau\,,$$
$$f' = (MJ)f \quad \Leftrightarrow \quad \tau' = \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)M^{-1}\right)\tau$$

3. Da $\Psi_{IF} = \Psi_{QF} \circ \Psi_{IQ}$ und $\Psi_{FI} = \Psi_{QI} \circ \Psi_{FQ}$, erhalten auch die Abbildungen Ψ_{IF} und Ψ_{FI} die auf I und F erklärten Äquivalenzen.

□

Außerdem haben die Abbildungen in Definition 2.18 die folgende wichtige Eigenschaft:

Lemma 2.20. *Reduzierte Ideale und reduzierte Formen werden durch Ψ_{FI} und Ψ_{IF} aufeinander abgebildet.*

Beweis: Für $D < 0$ ist nichts zu zeigen, da die Definitionen sich direkt entsprechen. Sei daher $D > 0$ und $\mathfrak{A} = [a,\beta]$, mit $\beta = \frac{-b+\sqrt{D}}{2}$, reduziert, also $a < \frac{-b+\sqrt{D}}{2}$ und $-a < \frac{-b-\sqrt{D}}{2} < 0$. So gilt sowohl $2a - \sqrt{D} < -b$, als auch $\sqrt{D} - 2a < -b < \sqrt{D}$,
also gilt $0 < \left|\sqrt{D} - 2a\right| < -b < \sqrt{D}$, das heißt $f = (a,b,c)$ ist reduziert.
Die Umkehrung ist damit klar. □

Im nächsten Kapitel werde ich unter anderem zeigen, daß es in jeder Klasse von Idealen mindestens ein reduziertes Ideal gibt. Da reduzierte Ideale den reduzierten Formen unter den äquivalenzerhaltenden Abbildungen Ψ_{FI} und Ψ_{IF} entsprechen, ist die Anzahl der Äquivalenzklassen von Formen in $F/SL_2(\mathbb{Z})$ gleich der Anzahl der Äquivalenzklassen von Idealen in $\mathcal{C}l_{\mathbb{K}}$, also gleich der Klassenzahl $h_{\mathbb{K}}$. Außerdem wird im vierten Kapitel eine Multiplikation auf I erklärt, so daß Ψ_{IF} eine Verknüpfung auf F induziert. Mit dieser bildet $F/SL_2(\mathbb{Z})$ eine Gruppe, und mit Ψ_{FI} und Ψ_{IF} erhält man Gruppenisomorphismen zwischen $F/SL_2(\mathbb{Z})$ und $\mathcal{C}l_{\mathbb{K}}$.

3 Reduktion von Idealen und Formen

In diesem Kapitel stelle ich Verfahren zur Berechnung reduzierter Ideale und reduzierter Formen vor. In imaginärquadratischen Zahlkörpern ist es das Ziel, zu einem gegebenen primitiven Ideal das dazu äquivalente eindeutig bestimmte reduzierte Ideal zu finden, entsprechend zu einer primitiven positiv definiten Form die reduzierte. Die Äquivalenz von Formen und quadratischen Irrationalzahlen, die die Idealklassen vollständig repräsentieren, habe ich mit Hilfe von Matrizen aus $SL_2(\mathbb{Z})$ definiert. Daher beschreibe ich diese im nächsten Abschnitt zunächst näher, ehe ich konkret das Reduktionsverfahren vorstelle.

In reellquadratischen Zahlkörpern nutze ich die Eigenschaft der Idealklasssen und indefiniten Formenklassen aus, daß sie durch reellquadratische Irrationalzahlen vollständig beschrieben werden. Letztere haben stets eine periodische Kettenbruchentwicklung, die in direktem Zusammenhang steht zu den reduzierten Idealen und reduzierten, indefiniten Formen einer Klasse. Aus diesem Grund leite ich den Abschnitt über das Reduktionsverfahren im reellquadratischem Zahlkörper mit einem Exkurs über Kettenbrüche ein.

3.1 Reduzieren im imaginärquadratischen Zahlkörper

3.1.1 Die Modulgruppe

Definition 3.1. Eine gebrochen lineare Abbildung der Zahlenkugel $\mathbb{C} \cup \{\infty\}$ auf sich, welche die Gestalt

$$\mu : z \longmapsto \frac{az+b}{cz+d} \text{ mit } a, b, c, d \in \mathbb{C} \text{ und } ad - bc \neq 0$$

hat, heißt *Möbiustransformation.*

Bemerkung. Eine rationale Funktion definiert genau dann eine bijektive Abbildung der Zahlenkugel auf sich, wenn sie eine Möbiustransformation ist. [vgl. Busam/Freitag].

Es läßt sich also den invertierbaren Matrizen $\pm M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{C})$ die Möbiustransformation μ, zuordnen. Die Möbiustransformationen bilden bezüglich der Komposition eine Gruppe, und es läßt sich leicht nachrechnen, daß

$$\begin{aligned} \varphi : GL_2(\mathbb{C})/(\pm E) &\longrightarrow \mathcal{M} \\ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto \mu\,,\ \left(\mu : z \longmapsto \frac{az+b}{cz+d}\right) \end{aligned} \tag{5}$$

ein Gruppenisomorphismus ist.

Definition 3.2. Eine Möbiustransformation μ heißt *unimodular*, wenn die Koeffizienten a,b,c und d ganzzahlig sind.

Die unimodularen Abbildungen bilden eine Untergruppe von $\mathcal{M}$, die via φ der Gruppe $GL_2(\mathbb{Z})/(\pm E)$ entspricht. Hiervon bilden die unimodularen Abbildungen eine Untergruppe, für deren Koeffizienten $ad - bc = +1$ gilt. Diese ist isomorph zu der Gruppe $SL_2(\mathbb{Z})/(\pm E) = PSL_2(\mathbb{Z})$.

Definition 3.3. Die Gruppe $\Gamma = PSL_2(\mathbb{Z})$ heißt *Modulgruppe.*

Satz 3.4. *$SL_2(\mathbb{Z})$ wird erzeugt von den Matrizen $S, T \in \Gamma$,*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ , \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} .$$

d.h. jedes $M \in SL_2(\mathbb{Z})$ besitzt eine Darstellung:

$$M = ST^{\nu_1}ST^{\nu_2} \cdot \ldots \cdot ST^{\nu_k}S \ , \ \textit{mit } \nu_i \in \mathbb{Z},\ 1 \leq i \leq k.$$

Beweis: Sei $M \in SL_2(\mathbb{Z})$, so hat eine der Matrizen M, SM, S^2M, oder S^3M die Gestalt

$$\begin{pmatrix} \alpha\ \beta \\ \gamma\ \delta \end{pmatrix} \text{ mit } \beta \geq |\delta| \geq 0$$

Ist $\delta \neq 0$, so existiert ein $n \in \mathbb{Z}$, so daß

$$T^n \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha + n\gamma & \beta + n\delta \\ \gamma & \delta \end{pmatrix}, \text{ mit } 0 \leq \beta + n\delta < |\delta| \, .$$

Dies läßt sich wiederholen, und man erhält wegen der Ganzzahligkeit der Matrizeneinträge nach endlich vielen Schritten und gegebenenfalls nach Multiplikation mit $S^2 = -E$ eine Matrix der Gestalt

$$\begin{pmatrix} \alpha'\ 0 \\ \gamma'\ \delta' \end{pmatrix}, \text{ mit } \alpha' = \delta' = +1 \, .$$

Nun multipliziere man mit $S^3T^{\gamma'}S$, und man erhält die Einheitsmatrix.

$$S^{\eta_k}T^{-\nu_k}S^{\eta_{k-1}}T^{-\nu_{k-1}}S^{\eta_{k-2}} \cdot \ldots \cdot S^{\eta_1}T^{-\nu_1}S^{-\eta_0}M = E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \nu_i, \eta_j \in \mathbb{Z}$$

Da S^2 mit allen Matrizen aus Γ kommutiert, erhält man insgesamt

$$\Rightarrow M = S^\eta T^{\nu_1} S \cdot \ldots \cdot S T^{\nu_k} S\,.$$

Da $Mz = -Mz$ und $S^2 = (ST)^3 = -E$, ist η eindeutig $\mod 2$. Ist $\eta \equiv 1 \mod 2$, so erhält man eine Darstellung wie in Satz 3.4.
Ist $\eta \equiv 0 \mod 2$, so läßt sich $S^\eta T^{\nu_1}$ schreiben als $(ST)^2 S T^{\nu_1+1}$, da $(ST)^3 = -E$.
$\square$

Bemerkung. S und T sind Automorphismen der oberen Halbebene. Geometrisch lassen sie sich folgendermaßen beschreiben:
S bewirkt eine Spiegelung an der Einheitskreislinie mit anschließender Spiegelung an der imaginären Achse.
$S : \tau \mapsto -\frac{1}{\tau} = -\frac{\overline{\tau}}{|\tau|^2}$.
T bewirkt eine Translation parallel zur reellen Achse um den Wert 1.
$T : \tau \mapsto \tau + 1$, entsprechend $T^n : \tau \mapsto \tau + n$.

Satz 3.5. *Zu jedem Punkt $\tau \in \mathcal{H}$ existiert genau eine Abbildung $M \in \Gamma$ mit*

$$M\tau \in \mathcal{F}_\Gamma = \Big\{ z \in \mathcal{H} \mid -\tfrac{1}{2} < \Re(z) \le \tfrac{1}{2}, |z| \ge 1 \textit{ und } \Re(z) \ge 0, \textit{ für } |z| = 1 \Big\}\,.$$

Korollar 3.6. *$\mathcal{F}_\Gamma$ ist ein* Fundamentalbereich *von Γ.*

Beweis zu Satz 3.5: Ich beweise zunächst die Existenz einer solchen Abbildung und anschließend die Eindeutigkeit.
(i) Existenz:
Es sei $M \in \Gamma$ und $\tau \in \mathcal{H}$, $\tau' = M\tau$. Aus dem Beweis zu Lemma 2.10 ist

$$\Im(\tau') = \frac{\Im(\tau)}{|\gamma\tau + \delta|^2} \tag{6}$$

bekannt.
Betrachtet man eine Folge von Paaren $(\gamma_i,\, \delta_i)_{i\in\mathbb{N}} \in \mathbb{Z}^2$, in der kein Paar doppelt vorkommt, so gilt $|\gamma_i\tau + \delta_i|^2 \xrightarrow{i\to\infty} \infty$.
Mit Gleichung (6) folgt, daß eine Matrix $M_0 \in \Gamma$ existiert, so daß für $\tau_0 = M_0\tau$ mit $-\frac{1}{2} < \Re(\tau_0) \le \frac{1}{2}$ gilt:

$$\Im(\tau_0) = \Im(M_0\tau) \ge \Im(M\tau)\,, \quad \forall M \in \Gamma\,.$$

Die Bedingung an den Realteil von τ_0 läßt sich immer erreichen, ohne den Imaginärteil zu ändern. Die Ungleichung gilt dann insbesondere auch für $M = SM_0 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) M_0$:

$$\Im(\tau_0) \geq \Im(M\tau) = \Im(SM_0\tau) = \Im(S\tau_0) = \frac{\Im(\tau_0)}{|\tau_0|^2} \text{ nach Gleichung (6),}$$

damit folgt, $|\tau_0| = |M_0\tau| \geq 1$. Ist $|\tau_0| = |M_0\tau| > 1$, so liegt bereits $M_0\tau$ in $\mathcal{F}_\Gamma$. Ist $|M_0\tau| = 1$ und $\Re(M_0\tau) < 0$, so liegt $SM_0\tau$ in $\mathcal{F}_\Gamma$, da S in diesem Fall lediglich eine Spiegelung an der imaginären Achse ist, weil $M_0\tau$ auf der Einheitskreislinie liegt.

(ii) Eindeutigkeit:
Seien $\tau, \tau' \in \mathcal{F}_\Gamma$ äquivalent, $\tau \neq \tau'$ und $M \in \Gamma$, so daß $\tau' = M\tau$. Dann sei oBdA $\Im(\tau') = \frac{\Im(\tau)}{|\gamma\tau+\delta|^2} \geq \Im(\tau)$. Also gilt $|\gamma\tau+\delta|^2 = \gamma^2\Im^2(\tau)+(\gamma\Re(\tau)+\delta)^2 \leq 1$. Da $\tau \in \mathcal{F}_\Gamma$, ist $\Im^2(\tau) \geq \frac{3}{4} \Rightarrow |\gamma| \leq 1$ und $|\delta| \leq 1$. Der Fall $\gamma = 0 = \delta$ existiert nicht, da $detM \neq 0$. Die drei übrigen betrachte ich getrennt.

- Sei $\gamma = 0 \quad \Rightarrow \quad \delta = \pm 1$ und $\alpha = \delta$. Also ist $\tau' = \tau + \beta$. Da $\tau \in \mathcal{F}_\Gamma$ ist $|\beta| < 1$, also $\beta = 0$ und $\tau = \tau'$. Widerspruch zur Annahme.

- Sei $\delta = 0$, also $\gamma = \pm 1$ und $\beta = -\gamma$. Damit ist $\tau' = \pm\alpha - \frac{1}{\tau}$ und $\Im(\tau') = \Im(-\frac{1}{\tau}) \leq \Im(\tau)$, aber nach Voraussetzung ist $\Im(\tau') \geq \Im(\tau)$ $\Rightarrow \Im(\tau') = \Im(\tau)$ und wegen Gleichung (6), $|\tau| = 1$. Da $\tau \in \mathcal{F}_\Gamma$, ist $0 \leq \Re(\tau) \leq \frac{1}{2} \Rightarrow |\alpha| \leq \frac{1}{2}$, also $\alpha = 0$. Also ist $M = \pm S$. S auf Punkte auf dem Einheitskreis angewandt, bewirkt aber lediglich eine Spiegelung an der imaginären Achse. Da aber auch $\tau \in \mathcal{F}_\Gamma$, ist auch $0 \leq \Re(\tau') \leq \frac{1}{2}$, und damit $i = \tau = \tau'$ im Widerspruch zur Annahme.

- Seien $|\gamma| = |\delta| = 1$. Ich nehme oBdA $\gamma = 1$ an.
$\Rightarrow \quad |\gamma\tau + \delta|^2 = \Im^2(\tau) + (\Re(\tau) \pm 1)^2$.
Da $\Im^2(\tau) \geq \frac{3}{4}$, muß $|\Re(\tau)| \geq \frac{1}{2}$ sein, wobei das Vorzeichen anders sein muß, als das von δ. Dies erfüllt nur ein einziger Punkt in $\mathcal{F}_\Gamma$, nämlich $-\overline{\rho} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, wenn ρ die dritte Einheitswurzel ist. Außerdem ist $\Im(\tau) = \Im(\tau')$. $-\overline{\rho}$ ist aber der einzige Punkt in $\mathcal{F}_\Gamma$ mit Imaginärteil gleich $\frac{\sqrt{3}}{2}$, also $\tau = \tau'$ und $M = \pm E$ im Widerspruch zu $\gamma = 1$. $\square$

Korollar 3.7. *In jeder Idealklasse existiert genau ein reduziertes Ideal.*

Beweis: Zu $\mathfrak{A}$ existiert eine eindeutige Zahl $\tau_0 \sim \tau = \Psi_{IQ}(\mathfrak{A})$, mit $\tau_0 \in \mathcal{F}_\Gamma$. τ_0 hat die eindeutige Darstellung $\frac{-b+\sqrt{D}}{2a}$, mit $a > 0$. Damit ist $\mathfrak{A}_0 = [a, \frac{-b+\sqrt{D}}{2}]$ reduziert. Ist $\mathfrak{B}$ äquivalent zu $\mathfrak{A}_0$ und $\tau_{\mathfrak{B}} = \Psi_{IQ}(\mathfrak{B}) \notin \mathcal{F}_\Gamma$, so ist $\mathfrak{B}$ nicht reduziert. Ist $\tau_{\mathfrak{B}} \in \mathcal{F}_\Gamma$, dann ist $\tau_{\mathfrak{B}} = \tau_0$. Damit haben $\mathfrak{A}_0$ und $\mathfrak{B}$ dieselbe kanonische Darstellung, also ist $\mathfrak{A}_0 = \mathfrak{B}$. $\square$

3.1.2 Das Reduktionsverfahren

Sei $\mathfrak{A} = [a, \kappa]$, mit $\kappa = \frac{-b+\sqrt{D}}{2}$, ein primitives Ideal in kanonischer Darstellung, D eine fundamentale Diskriminante, und seien f und τ die jeweiligen Bilder von $\mathfrak{A}$ in den Mengen F und Q unter den in Abschnitt 2.4 erklärten Abbildungen.
Es gilt, daß in diesem Fall $Q \subset \mathcal{H}$. Es existiert daher eine Matrix $M_0 \in \Gamma$, so daß $\tau_0 = M_0\tau \in \mathcal{F}_\Gamma$ mit $\tau_0 = \frac{\kappa_0}{a_0}$ und $a_0 > 0$, $\kappa_0 = \frac{-b_0+\sqrt{D}}{2}$.
Das entsprechende Ideal $\mathfrak{A}_0$ und die Form f_0 sind dann reduziert, da aus $-\frac{1}{2} < \Re(\tau_0) \leq \frac{1}{2}$ folgt, daß $-a_0 < -b_0 \leq a_0$, und mit $\mathcal{N}(\tau_0) = \frac{{b_0}^2-D}{4{a_0}^2} = \frac{c_0}{a_0} \geq 1$ folgt, daß $c_0 \geq a_0$ ist, und für $\mathcal{N}(\tau_0) = 1$, also $a = c$, gilt: $\Re(\tau_0) \geq 0$, also $0 \leq -b_0 \leq a$.

Diese Matrix M_0 hat nach Satz 3.4 eine Darstellung der Gestalt:
$M_0 = ST^{\nu_1}ST^{\nu_2} \cdot \ldots \cdot ST^{\nu_k}S$.
Die Konstruktion dieser Darstellung ist daher als Reduktionsverfahren zu verwenden. Man realisiert dies durch sukzessive Anwendung von S und T^n auf τ für geeignete $n \in \mathbb{Z}$:

Zu $\tau \in \mathcal{H}$ existiert ein $n_1 \in \mathbb{Z}$, so daß $\tau_1 = T^{n_1}\tau$ in $\mathcal{L} = \{z \in \mathbb{C} \mid -\frac{1}{2} < \Re(z) \leq \frac{1}{2}\}$ liegt.

Nun gibt es drei Fälle:

1. Ist $|\tau_1| > 1$, oder $|\tau_1| = 1$ und $\Re(\tau_1) \geq 0$, so liegt τ_1 in $\mathcal{F}_\Gamma$, und es ist $\tau_0 = \tau_1$.

2. Ist $|\tau_1| = 1$ und $\Re(\tau_1) < 0$, so liegt $S\tau_1 = T^0S\tau_1$ in $\mathcal{F}_\Gamma$, und es ist $\tau_0 = S\tau_1$.

3. Ist $|\tau_1| < 1$, so ist $\Im(S\tau_1) > \Im(\tau_1)$, und es existiert ein $n_2 \in \mathbb{Z}$, so daß $\tau_2 = T^{n_2}S\tau_1$ in $\mathcal{L}$ liegt.

Auf τ_2 wendet man nun dieselbe Fallunterscheidung an wie auf τ_1. Dabei bezeichne ich die Abbildung $T^n S$ als *Reduktionsschritt*. Dieser besteht aus:

1. einer Spiegelung am Einheitskreis sowie einer Spiegelung an der imaginären Achse, das heißt, $\Re(\tau) \mapsto \frac{-\Re(\tau)}{|\tau|^2}$ und $\Im(\tau) \mapsto \frac{\Im(\tau)}{|\tau|^2}$ und
2. einer Translation parallel zur reellen Achse in den Streifen $\mathcal{L}$, wobei der Imaginärteil natürlich unverändert bleibt.

Konkret bedeutet das für Ideale und Formen

Schritt 1:

$$\begin{aligned} \Psi_{QI} S \Psi_{IQ} : &\left[a, \tfrac{-b+\sqrt{D}}{2}\right] \longmapsto \left[c, \tfrac{b+\sqrt{D}}{2}\right], \; c = \tfrac{b^2-D}{4a} \\ -S = S^{-1} = \Psi_{QF} S \Psi_{FQ} : &\quad (a,b,c) \longmapsto (c,-b,a) \end{aligned}$$

Schritt 2:

$$\begin{aligned} \Psi_{QI} T^n \Psi_{IQ} : &\left[a, \tfrac{-b+\sqrt{D}}{2}\right] \longmapsto \left[a, \tfrac{2na-b+\sqrt{D}}{2}\right] \\ T^{-n} = \Psi_{QF} T^n \Psi_{FQ} : &\quad (a,b,c) \longmapsto (a, b-2an, c-bn+an^2) \end{aligned}$$

Nach dem Beweis zu Satz 2.19 bedeutet ein Reduktionsschritt für Formen die Anwendung von $(T^n S)^{-1} = -ST^{-n}$ in Γ. Ein Reduktionsschritt bewirkt also:

$$\begin{aligned} \Psi_{QI} T^n S \Psi_{IQ} : &\left[a, \tfrac{-b+\sqrt{D}}{2}\right] \longmapsto \left[c, \tfrac{b+2nc+\sqrt{D}}{2}\right] \\ -ST^{-n} = \begin{pmatrix} 0 & 1 \\ -1 & n \end{pmatrix} : &\quad (a,b,c) \longmapsto (c, -b-2nc, a+bn+cn^2) \end{aligned}$$

Aus Beweis zu Satz 3.5 folgt, daß dieses Verfahren nach endlich vielen Reduktionsschritten abbricht. Buchmann hat in [BuWi88] gezeigt, daß höchstens $2 + \lfloor \frac{1}{2} \log \frac{6a_0}{5 \cdot \sqrt{|D|}} \rfloor$ Schritte benötigt werden. Liegt a_0 also in der Größenordnung von $\sqrt{|D|}$, so benötigt man höchstens $O(\log \sqrt{|D|})$ Schritte.

Für die Translation T^n benötigt man ein geeignetes $n \in \mathbb{Z}$. Zu diesem Zweck betrachte man die folgende Ungleichung.

$$\begin{aligned} -\tfrac{1}{2} < x + n \leq \tfrac{1}{2} &\Leftrightarrow -x - \tfrac{1}{2} < n \leq -x + \tfrac{1}{2} \\ &\Rightarrow n = max\left\{ m \in \mathbb{Z} \mid m \leq -x + \tfrac{1}{2} \right\} \end{aligned}$$

Für $max\{m \in \mathbb{Z} | m \leq x\}$, verwende ich von nun an die folgende Schreibweise: floor(x) bzw. $\lfloor x \rfloor$. Analog für $min\{m \in \mathbb{Z} \mid m \geq x\}$, ceiling($x$) bzw. $\lceil x \rceil$.

Für die erste Translation, noch vor den eigentlichen Reduktionsschritten, setze man $\frac{-b}{2a}$ für x ein. Im Reduktionschritt wird $-b$ durch S zunächst auf b abgebildet, daher setze man im Reduktionsschritt $\frac{b}{2a}$ für x ein. Man erhält damit für den ersten Fall $n = \lfloor \frac{b}{2a} + \frac{1}{2} \rfloor$ und im zweiten Fall $n = \lfloor -\frac{b}{2a} + \frac{1}{2} \rfloor$

Die Ergebnisse des Reduktionsverfahrens lassen sich auf einfache Weise an Hand der folgenden Kriterien, die sich leicht aus den Eigenschaften von $\mathcal{F}_\Gamma$ ableiten lassen, auf ihre Reduziertheit hin überprüfen.

Lemma 3.8. *Sei* $\mathfrak{A} = [a, \kappa]$, $\kappa = \frac{-b+\sqrt{d_{\mathbb{K}}}}{2}$, *ein primitives Ideal in kanonischer Darstellung.*

(i) *Ist* $a < \frac{\sqrt{|d_{\mathbb{K}}|}}{2}$, *so ist* $\mathfrak{A}$ *reduziert.*

(ii) *Ist* $\mathfrak{A}$ *reduziert, so ist* $a \leq \sqrt{\frac{|d_{\mathbb{K}}|}{3}}$.

Beweis:

(i) Dies ist bereits anschaulich klar. Da $\mathfrak{A}$ in kanonischer Darstellung gegeben ist, liegt $\tau = \frac{\kappa}{a}$ in $\mathcal{L}$, und da $\Im(\tau) = \frac{\sqrt{|d_{\mathbb{K}}|}}{2a} > 1$ ist, liegt τ bereits in $\mathcal{F}_\Gamma$. Also ist $\mathfrak{A}$ reduziert.

(ii) $\mathfrak{A}$ ist reduziert, das heißt $|b| \leq a$ und $a \leq c = \frac{b^2 - d_{\mathbb{K}}}{4a}$.
Dann gilt $b^2 - d_{\mathbb{K}} = 4ac \geq 4a^2 \Rightarrow a^2 - d_{\mathbb{K}} \geq 4a^2 \Rightarrow a^2 \leq \frac{|d_{\mathbb{K}}|}{3}$.
Mit anderen Worten: $\Im(\tau) = \frac{\sqrt{|d_{\mathbb{K}}|}}{2a} \geq \frac{\sqrt{|d_{\mathbb{K}}|}}{2} \frac{\sqrt{3}}{\sqrt{|d_{\mathbb{K}}|}} = \frac{\sqrt{3}}{2}$. Dies ist aber bekannt, da $\tau \in \mathcal{F}_\Gamma$.

□

Ich gebe nun einen Algorithmus zur Reduktion von Idealen und Formen an.

Algorithmus: *REDUKTION1*

	Ideale	**Formen**
Eingabe	$a, \quad b, \quad D$	$a, \quad b, \quad c, \quad D$
	so daß $\mathfrak{A} = \left[a, \frac{-b+\sqrt{D}}{2}\right]$ primitives Ideal in $\mathcal{O}_{\mathbb{K}}$, $D = d_{\mathbb{K}}$	so daß $f = (a, b, c)$ primitive, positiv definite Form zur fundamentalen Diskriminante $D < 0$
Ausgabe	$a_0, \quad b_0$	$a_0, \quad b_0, \quad c_0$
	so daß $\mathfrak{A}_0 = \left[a_0, \frac{-b_0+\sqrt{D}}{2}\right]$ reduziert ist, und $\mathfrak{A}_0 \sim \mathfrak{A}$	so daß $f_0 = (a_0, b_0, c_0)$ reduziert ist, und $f_0 \sim f$
Programm		
(01)	$n \longleftarrow \left\lfloor \frac{b}{2a} + \frac{1}{2} \right\rfloor$	$n \longleftarrow \left\lfloor \frac{b}{2a} + \frac{1}{2} \right\rfloor$
(02)	$a_0 \longleftarrow 2a$	$a_0 \longleftarrow a$
(03)	$b_0 \longleftarrow b - a_0 n$	$b_0 \longleftarrow b - 2an$
(04)		$c_0 \longleftarrow c - bn + an^2$
(05)	$a_1 \longleftarrow \frac{b_0^2 - D}{a_0}$	
(06)	$n \longleftarrow \left\lfloor -\frac{b_0}{a_1} + \frac{1}{2} \right\rfloor$	
(07)	$b_1 \longleftarrow -a_1 n - b_0$	
(08)	solange $(a_1 < a_0) \vee (a_1 = a_0, b_0 > 0)$	solange $(c_0 < a_0) \vee (c_0 = a_0, b_0 > 0)$
(09)	Beginn der Schleife	Beginn der Schleife
(10)	$a_0 \longleftarrow a_1$	$a_1 \longleftarrow a_0$
(11)	$b_0 \longleftarrow b_1$	$b_1 \longleftarrow b_0$
(12)	$a_1 \longleftarrow \frac{b_0^2 - D}{a_0}$	$c_1 \longleftarrow c_0$
(13)	$n \longleftarrow \left\lfloor -\frac{b_0}{a_1} + \frac{1}{2} \right\rfloor$	$n \longleftarrow \left\lfloor -\frac{b_1}{2c_1} + \frac{1}{2} \right\rfloor$
(14)	$b_1 \longleftarrow -a_1 n - b_0$	$a_0 \longleftarrow c_1$
(15)	Ende der Schleife	$b_0 \longleftarrow -2c_1 n - b_1$
(16)		$c_0 \longleftarrow a_1 + b_1 n + c_1 n^2$
(17)		Ende der Schleife
(18)	$a_0 \longleftarrow \frac{a_0}{2}$	
(19)	Übergebe (a_0, b_0)	Übergebe (a_0, b_0, c_0)

Es sei $\tau = \frac{-b+\sqrt{D}}{2a} = \Psi_{IQ}(\mathfrak{A})$, $\tau_i = \frac{-b_i+\sqrt{D}}{2a_i} = \Psi_{IQ}([\frac{a_i}{2}, \frac{-b_i+\sqrt{D}}{2}])$, $i = 0, 1$, wobei a_i aus dem Algorithmus für Ideale stammt, welches sich vom a_i aus dem Algorithmus für Formen um den Faktor 2 unterscheidet.

In den Zeilen (01) – (04) wende ich zuerst T^n einmal auf τ an, für das geeignete $n \in \mathbb{Z}$, um τ in den Streifen $\mathcal{L}$ abzubilden.
In den Zeilen (05) – (07) berechne ich für das Ideal einen Reduktionsschritt, um überprüfen zu können, ob $\tau_0 = T^n\tau$ bereits in $\mathcal{F}_\Gamma$ liegt. Diesen Reduktionsschritt braucht man für die Form $f_0 = (a_0, b_0, c_0)$ nicht, da man mit c_0 die benötigte Information bereits besitzt, die man für die Abbruchbedingung in Zeile (08) benötigt. Diese spiegelt genau die Fallunterscheidung auf Seite 31 wieder. Ist diese nach Zeile (7) noch nicht erfüllt, beginnt man damit, die Schleife zu durchlaufen. Jeder Durchlauf entspricht dabei einem Reduktionsschritt.
Zunächst wird in der Schleife für Ideale $\mathfrak{A}_0 = \mathfrak{A}_1$ gesetzt, und entsprechend $f_1 = f_0$ bei den Formen, um sich die Werte vor dem Reduktionsschritt zu merken. Dies ist notwendig, da man bei den Idealen erst nach dem Reduktionsschritt sieht, ob es vorher schon reduziert war, so daß, wenn die Abbruchbedingung eintritt, $\mathfrak{A}_0$ reduziert ist, und nicht das neuberechnete Ideal $\mathfrak{A}_1$. Bei den Formen ist dies anders. Hier benötigt man zur Berechnung der neuen Werte alle alten, da man zur Berechnung des neuen Wertes von c die alten Werte von a und b, andererseits aber zur Berechnung der neuen Werte von a und b den alten Wert von c kennen muß. Aber auch hier ist, wenn die Abbruchbedingung erfüllt ist, f_0 reduziert.
Der Algorithmus für Formen hat den Vorteil, daß zur Berechnung der neuen Werte keine Division benötigt wird, wie in den Zeilen (05) und (12) bei den Idealen. Andererseits benötigt er ein wenig mehr Speicherplatz wegen der zusätzlichen Werte von c und c'.

Beispiel: Es sei $\mathbb{K} = \mathbb{Q}(\sqrt{-55})$.

Allgemein gilt für Ideale in quadratischen Zahlkörpern: $4a \mid b^2 - d_{\mathbb{K}}$, also auch $b \equiv d_{\mathbb{K}} \mod 2$. Für ein reduziertes Ideal $\mathfrak{A}_0 = \left[a_0, \frac{-b_0+\sqrt{d_{\mathbb{K}}}}{2}\right]$, gilt zusätzlich $|b_0| \leq a_0$ und, nach Lemma 3.8, $a_0 < \sqrt{\frac{55}{3}} \approx 4,28$. Damit erhält man folgende Aussagen über reduzierte Ideale in $\mathcal{O}_{\mathbb{K}}$:
$a_0 \in \{1, 2, 3, 4\}$ und $b_0 \in \{\pm 1, \pm 3\}$.

$$\begin{aligned} \Rightarrow 4a_0 \mid 56 \quad &\text{für } b_0 = \pm 1, \text{ also } a_0 = 1 \text{ oder } 2 \\ 4a_0 \mid 64 \quad &\text{für } b_0 = \pm 3, \text{ also } a_0 = 4. \end{aligned}$$

Insgesamt:

$$\begin{aligned} \mathfrak{A}_1 &= \left[1, \tfrac{1+\sqrt{d_{\mathbb{K}}}}{2}\right] = \mathcal{O}_{\mathbb{K}} = \left[1, \tfrac{-1+\sqrt{d_{\mathbb{K}}}}{2}\right] = \overline{\mathfrak{A}}_1 \\ \mathfrak{A}_2 &= \left[2, \tfrac{-1+\sqrt{d_{\mathbb{K}}}}{2}\right] \\ \mathfrak{A}_3 &= \left[2, \tfrac{1+\sqrt{d_{\mathbb{K}}}}{2}\right] = \overline{\mathfrak{A}}_2 \neq \mathfrak{A}_2 \\ \mathfrak{A}_4 &= \left[4, \tfrac{3+\sqrt{d_{\mathbb{K}}}}{2}\right] \end{aligned}$$

$\overline{\mathfrak{A}}_4$ ist nicht reduziert, da $-b < 0$ und $a = c = 4$. Aber $\mathfrak{A}_4$ und $\overline{\mathfrak{A}}_4$ liegen in derselben Klasse, also $[\mathfrak{A}_4] = [\overline{\mathfrak{A}}_4]$. In so einem Fall spricht man von einer ambigen Klasse. Man beachte, daß etwa $[\mathfrak{A}_2]$ keine ambige Klasse ist, während die Einsklasse stets ambig ist.
Dies sind die einzigen reduzierten Ideale in $\mathcal{O}_{\mathbb{K}}$. Die Klassenzahl von $\mathbb{Q}(\sqrt{-55})$ ist also $h_{\mathbb{K}} = 4$.

Wähle ich nun ein beliebiges primitives Ideal, zum Beispiel $\mathfrak{A} = \left[a, \frac{-b+\sqrt{d_{\mathbb{K}}}}{2}\right]$ aus $\mathcal{O}_{\mathbb{K}}$ mit der dazugehörenden Form $f = (a, b, c)$, mit $c = \frac{b^2+55}{4a}$, und wende auf $\mathfrak{A}$ und f den Algorithmus *REDUKTION1* an, so muß das Ergebnis $\mathfrak{A}_0 = \left[a_0, \frac{-b_0+\sqrt{d_{\mathbb{K}}}}{2}\right]$ in $\{\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \mathfrak{A}_4\}$ liegen, und f_0 in $\{f_1, f_2, f_3, f_4\}$, mit $f_i = \Psi_{IF}(\mathfrak{A}_i)$, $i = 1, \ldots, 4$.

Sei also zum Beispiel $a = 526,\ b = 4529,\ c = 9749$ und $D = -55$:

(01) – (04)	$n = 4$ $a_0 = 1052,\ b_0 = 321$	$n = 4$ $a_0 = 526,\ b_0 = 321,\ c_0 = 49$
(05) – (07)	$n = -3$ $a_1 = 98,\ b_1 = -27$	
(08)	Da $a_1 < a_0 \longrightarrow$ Schleife	Da $c_0 < a_0 \longrightarrow$ Schleife
Schleife:		
	1. Durchgang: $a_0 = 98,\ b_0 = -27$ $n = 3,\ \mathfrak{A}_1 = (8, 3)$	1. Durchgang: $f_1 = f_0$, $n = -3,\ a_0 = 49,\ b_0 = -27,\ c_0 = 4$
(08)	$a_1 < a_0 \longrightarrow$	$c_0 < a_0 \longrightarrow$
	2. Durchgang: $a_0 = 8,\ b_0 = 3$ $n = 0,\ \mathfrak{A}_1 = (8, -3)$	2. Durchgang: $f_1 = f_0$, $n = 3,\ a_0 = 4,\ b_0 = 3,\ c_0 = 4$
(08)	$a_1 = a_0$, und $b_0 > 0 \longrightarrow$	$c_0 = a_0$, und $b_0 > 0 \longrightarrow$
	3. Durchgang: $a_0 = 8,\ b_0 = -3$ $n = 0,\ \mathfrak{A}_1 = (8, 3)$	3. Durchgang: $f_1 = f_0$, $n = 0,\ a_0 = 4,\ b_0 = -3,\ c_0 = 4$
(08)	$a_1 = a_0$, aber $b_0 \leq 0 \longrightarrow$ (18)	$c_0 = a_0$, aber $b_0 \leq 0 \longrightarrow$ (19)
(18)	$a_0 = 4$	
(19)	Ausgabe: $(4, -3)$	Ausgabe: $(4, -3, 4)$

Vergleicht man die Werte von a_0 und b_0 jeweils am Ende eines Schleifendurchlaufes mit der Fallunterscheidung auf Seite 31, so sieht man, daß nach Durchgang 1 der Fall 3 eintritt, nach Durchgang 2 der Fall 2.
Fall 2 besagt jedoch, daß das gerade gültige τ_0 auf dem nicht zu $\mathcal{F}_\Gamma$ gehörenden Abschnitt des Einheitskreises liegt. Man benötigt also nur noch eine Multiplikation mit S. Dies wird dadurch bestätigt, daß in Durchgang 3 $n = 0$ ist, und anschließend Fall 1 eintritt, was bedeutet, daß das Ideal $\mathfrak{A}_0$ bzw. die Form f_0 reduziert ist und die Schleife abbricht.

Es ist $\mathfrak{A}_0 = \mathfrak{A}_4$. Also ist $\mathfrak{A}_0$ reduziert, und

$$\mathfrak{A} = \left[526, \tfrac{-4529+\sqrt{-55}}{2}\right] \sim \left[4, \tfrac{3+\sqrt{-55}}{2}\right] = \mathfrak{A}_0\,.$$

3.2 Reduzieren im reellquadratischen Zahlkörper

Auch in reellquadratischen Zahlkörpern werde ich das Reduzieren von Idealen mit Hilfe der Repräsentanten $\tau \in \mathbb{R}$ erklären. Zur Reduktion wird das Kettenbruchverfahren verwendet, welches ich zunächst kurz vorstelle, da später einige Eigenschaften für die Arithmetik auf Idealen benötigt werden, die ich nicht als allgemein bekannt voraussetzen möchte. Es wird sich herausstellen, daß ein Schritt des Kettenbruchverfahrens, via Ψ_{FQ} und Ψ_{QF} auf Formen angewandt, der Matrix $-T^nS$ aus dem Reduktionsverfahren für $D < 0$ entspricht. In der Tat ließe sich sogar dieselbe Matrix wie im imaginärquadratischen Zahlkörper zur Reduktion verwenden, wie dies etwa Cohen in [Cohen] tut, jedoch ginge damit der direkte Zusammenhang zum Kettenbruchverfahren verloren.
Diese Einführung basiert in erster Linie auf [Forster, Kap.21], die Aussagen in Zusammenhang mit Lemma 3.16 sind an [WiWu] angelehnt.

3.2.1 Kettenbrüche

Kettenbrüche sind eine Form der Darstellung von reellen Zahlen, deren Konstruktion rekursiv definiert wird. Ist $x \in \mathbb{R}$, $\phi_0 = x$, dann erhält man mit den Rekursionsformeln

$$\begin{aligned} q_i &= \lfloor \phi_i \rfloor \quad \text{und} \\ \phi_{i+1} &= \tfrac{1}{\phi_i - q_i} \end{aligned} \tag{7}$$

eine Darstellung der Form

$$x = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots \cfrac{1}{q_n + \frac{1}{\phi_{n+1}}}}}.$$

Definition 3.9. Sei $x \in \mathbb{R}$. Dann heißt

$$x = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots \cfrac{1}{q_n + \frac{1}{\phi_{n+1}}}}},$$

kurz $x = (q_0, q_1, \ldots, q_n, \phi_{n+1})$, die *Kettenbruchentwicklung n-ter Stufe* von x. $C_n = \frac{u_n}{v_n} = (q_0, q_1, \ldots, q_n)$ heißt der n-te *Näherungsbruch* von x und ϕ_{n+1} der *Rest* der Kettenbruchentwicklung n-ter Stufe.

Bemerkung.

1. Es gilt für alle $\phi_i \neq 0$: $\phi_i > 1$, für $i \geq 1$. Dies folgt direkt aus der Gleichung (7), da $\phi_{i-1} - q_{i-1} = \phi_{i-1} - \lfloor \phi_{i-1} \rfloor < 1$.
2. Es gilt $\phi_i \neq 0$ für alle i, genau dann, wenn $x \notin \mathbb{Q}$. Mit anderen Worten, die Kettenbruchentwicklung von x bricht genau dann ab, wenn $x \in \mathbb{Q}$. Ist x eine rationale Zahl mit der gekürzten Darstellung $x = \frac{p}{q}$ mit ganzen Zahlen p und q, dann gilt:
$\frac{p}{q} = \frac{u_n}{v_n} = (q_0, \ldots, q_n)$, für ein $n \in \mathbb{N}$. Man vergleiche dazu Satz 21.1 in [Forster].

Definition 3.10. Die Kettenbruchentwicklung von $x \in \mathbb{R}$ heißt *periodisch*, wenn es $k, l \in \mathbb{N}$ gibt, so daß $q_{l+i} = q_i$ für alle $i \geq k$. Dann schreibe ich $x = (q_0, q_1, \ldots, q_{k-1}, \overline{q_k, \ldots, q_{k+l-1}})$.
Sind k und l minimal, so heißt $(q_0, q_1, \ldots, q_{k-1})$ *Vorperiode* und $(q_k, \ldots, q_{k+l-1})$ *Periode* der Kettenbruchentwicklung.

Lemma 3.11. *Sei $x = (q_0, q_1, \ldots, q_n, \frac{\eta}{\zeta})$, mit $\eta, \zeta \in \mathbb{R}$. Dann gilt $x = \frac{y}{z}$ mit den Zahlen $y, z \in \mathbb{R}$, die gegeben sind durch*

$$\begin{pmatrix} y \\ z \end{pmatrix} = A_0 A_1 \cdot \ldots \cdot A_n \begin{pmatrix} \eta \\ \zeta \end{pmatrix} \qquad \textit{und } A_i = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$$

Beweis: siehe [Forster, S. 193] □

Sei $C_n = (q_0, q_1, \ldots, q_n) \in \mathbb{Q}$, so hat C_n die gekürzte Darstellung $C_n = \frac{u_n}{v_n}$ mit teilerfremden Zahlen $u_n, v_n \in \mathbb{Z}$, die sich wie folgt berechnen lassen:

$$\begin{pmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{pmatrix} = A_0 A_1 \cdot \ldots \cdot A_n \qquad , \; A_i = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}.$$

Das bedeutet, daß die Zahlen rekursiv erklärt sind. Man setze $u_{-2} = 0$, $u_{-1} = 1$ und $v_{-2} = 1$, $v_{-1} = 0$, dann ist:

$$\begin{aligned} u_{n+1} &= u_n q_{n+1} + u_{n-1} \\ v_{n+1} &= v_n q_{n+1} + v_{n-1}\,. \end{aligned} \tag{8}$$

Da die Matrizen A_i Determinante -1 haben, gilt dies auch für die Determinante des Produktes:
$u_n v_{n-1} - v_n u_{n-1} = (-1)^{n+1}$. Hieraus kann man direkt erkennen, daß u_n und v_n teilerfremd sind.
Für spätere Abschätzungen ist die folgende Eigenschaft der v_n hilfreich: Ist F_n das n-te Element in der Fibonacci-Folge, dann gilt stets $v_n \geq F_n$, da

$v_{-1} = 0$ und $q_i \geq 1$, für alle $i > 0$.

Ersetzt man in Lemma 3.11 y durch x und z durch 1, dann ist für $x = (q_0, q_1, \dots, q_n, \phi_{n+1})$ und $\phi_0 = x$:

$$\begin{aligned} \begin{pmatrix} x \\ 1 \end{pmatrix} &= A_0 A_1 \cdot \ldots \cdot A_n \begin{pmatrix} \phi_{n+1} \\ 1 \end{pmatrix} = \begin{pmatrix} u_n & u_{n-1} \\ v_n & v_{n-1} \end{pmatrix} \begin{pmatrix} \phi_{n+1} \\ 1 \end{pmatrix} \\ \Rightarrow x = \phi_0 &= \tfrac{u_n \phi_{n+1} + u_{n-1}}{v_n \phi_{n+1} + v_{n-1}} && (9) \\ \Rightarrow \phi_n &= \tfrac{u_{n-2} - \phi_0 v_{n-2}}{\phi_0 v_{n-1} - u_{n-1}} && (10) \end{aligned}$$

Mit Gleichung (9) erhält man

$$x - \tfrac{u_n}{v_n} = \tfrac{(-1)^n}{v_n (v_n \phi_{n+1} + v_{n-1})},$$

und mit Teil 1 der obigen Bemerkung folgt:

$$\left| x - \tfrac{u_n}{v_n} \right| \leq \tfrac{1}{v_n v_{n+1}} \leq \tfrac{1}{v_n^2}$$

Das heißt, daß $C_n = \frac{u_n}{v_n}$ für wachsendes $n \in \mathbb{N}$ eine zunehmend gute Näherung von x ist.

Satz 3.12. *Eine reelle Zahl x hat genau dann eine periodische Kettenbruchentwicklung, wenn x eine quadratische Irrationalzahl ist. Die Kettenbruchentwicklung ist reinperiodisch, d.h. die Länge der Vorperiode ist Null, genau dann, wenn $1 < x$ und $-1 < \overline{x} < 0$.*

Beweis: siehe [Forster, S. 196ff.] □

Unter Berücksichtigung der Abbildungen aus Abschnitt 2.4, ist die folgende Definition sinnvoll:

Definition 3.13. Eine quadratische Irrationalzahl x heißt reduziert, wenn $1 < x$ und $-1 < \overline{x} < 0$ gilt, also x eine reinperiodischer Kettenbruchentwicklung hat.

Auf diese Weise entsprechen sich die reduzierten Ideale in I und die reduzierten Irrationalzahlen in Q.

Definition 3.14. Die Abbildung $\rho : \phi_n \mapsto \phi_{n+1}$ heißt *Schritt der Kettenbruchentwicklung.* Ist $q_n = \lfloor \phi_n \rfloor$, dann ist ρ nach Gleichung (7) die gebrochen lineare Transformation mit der Matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & -q_n \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$.

Lemma 3.15. *Sei $\phi \in Q$ eine quadratische Irrationalzahl, sei also $\phi = \frac{-b+\sqrt{D}}{2a}$ und $\phi = (q_0, q_1, \ldots, q_{n-1}, \phi_n)$ die Kettenbruchentwicklung $(n-1)$-ter Stufe. Sei $\phi = \phi_0$ und $P_0 = -b$, $Q_0 = 2a$ sowie $q_i = \lfloor \phi_i \rfloor$.*
Dann ist $\phi_{n+1} = \frac{P_{n+1}+\sqrt{D}}{Q_{n+1}}$, mit

$$\begin{aligned} P_{n+1} &= q_n Q_n - P_n \\ Q_{n+1} &= \frac{D-P_{n+1}^2}{Q_n} \end{aligned}$$

der Rest der Kettenbruchentwicklung n-ter Stufe von ϕ.

Beweis: Zu zeigen ist, daß $\phi_{n+1} = \frac{P_{n+1}+\sqrt{D}}{Q_{n+1}}$, falls $\phi_n = \frac{P_n+\sqrt{D}}{Q_n}$ ist.
Nach Gleichung (7) ist

$$\phi_{n+1} = \frac{1}{\phi_n - q_n} = \frac{Q_n}{P_n+\sqrt{D}-q_n Q_n} = \frac{Q_n}{-P_{n+1}+\sqrt{D}} = \frac{P_{n+1}+\sqrt{D}}{Q_{n+1}}\,.$$

□

Das folgende Lemma beschreibt die Eigenschaften einer Größe, die im Abschnitt über die Distanzen von Idealen in Kapitel 4 von zentraler Bedeutung ist.

Lemma 3.16. *Sei $\psi_n = \frac{1}{\phi_n} = \frac{-P_n+\sqrt{D}}{Q_{n-1}}$, so sei*

$$\theta_0 = 1 \qquad \text{und} \qquad \theta_k = \prod_{i=1}^{k} \psi_i \quad , \text{ für } k > 1.$$

Dann hat θ_k folgende Eigenschaften:

(i) $\mathcal{N}(\theta_k) = (-1)^k \frac{Q_k}{Q_0}$

(ii) $\theta_k = (-1)^k \left(u_{k-1} - \phi v_{k-1}\right)$, *mit* $\phi = \phi_0$

Beweis: (i)

$$\mathcal{N}(\theta_k) = \prod_{i=1}^{k} \mathcal{N}(\psi_i) \text{ mit } \mathcal{N}(\psi_i) = \frac{P_i^2 - D}{Q_{i-1}^2} = -\frac{Q_i}{Q_{i-1}}$$

$\Rightarrow \quad \mathcal{N}(\theta_k) = \frac{-Q_1}{Q_0} \cdot \frac{-Q_2}{Q_1} \cdot \ldots \cdot \frac{-Q_k}{Q_{k-1}} = (-1)^k \frac{Q_k}{Q_0}$

(ii) nach Gleichung (10) ist $\psi_i = \frac{1}{\phi_i} = \frac{\phi v_{i-1} - u_{i-1}}{u_{i-2} - \phi v_{i-2}}$. Ist $\phi = \phi_0 = \frac{P_0+\sqrt{D}}{Q_0}$, so ergibt Induktion über k:

$k = 1$: $\theta_1 = \psi_1 = \frac{\phi v_0 - u_0}{u_{-1} - \phi v_{-1}} = \frac{\phi v_0 - u_0}{1} = (-1)^1 \big(u_0 - \phi v_0\big)$

$k > 1$: Sei $\theta_{k-1} = (-1)^{k-1}\big(u_{k-2} - \phi v_{k-2}\big)$. Dann ist

$$\begin{aligned}\theta_k &= \theta_{k-1}\psi_k = (-1)^{k-1}\big(u_{k-2} - \phi v_{k-2}\big)\frac{\phi v_{n-1} - u_{n-1}}{u_{n-2} - \phi v_{n-2}} \\ &= \quad (-1)^k \big(u_{k-1} - \phi v_{k-1}\big).\end{aligned}$$

□

Setzt man $G_n := Q_0 u_n - P_0 v_n$, so erhält man für θ_n die Darstellung

$$\theta_n = (-1)^n \frac{G_{n-1} - v_{n-1}\sqrt{D}}{Q_0} \;.$$

Die folgende Darstellung der G_n ist besser geeignet, wenn man die Kettenbruchentwicklung (n+1)-ter Stufe von ϕ_0 berechnet, da die Werte P_{n+1} und Q_{n+1} sowieso berechnet werden, zusäzlich aber nur die Werte v_i, für $i \leq n+1$, benötigt werden, und auf die der u_i verzichtet werden kann:

$$G_n = P_{n+1} v_n + Q_{n+1} v_{n-1} \tag{11}$$

Denn:
Es ist $\phi_{n+1} = \frac{P_{n+1}+\sqrt{D}}{Q_{n+1}}$ der Rest der Kettenbruchentwicklung n-ter Stufe von $\phi = \phi_0 = \frac{P_0+\sqrt{D}}{Q_0}$. Mit Gleichung (10) gilt:

$$\begin{aligned}\phi_{n+1} \;=\; \frac{P_{n+1}+\sqrt{D}}{Q_{n+1}} &= \frac{u_{n-1} - \phi v_{n-1}}{v_n \phi - u_n} \\ &= \frac{u_{n-1}Q_0 - v_{n-1}(P_0+\sqrt{D})}{Q_0} \frac{Q_0}{u_n Q_0 - v_n (P_0+\sqrt{D})} \\ &= \frac{u_{n-1}Q_0 - v_{n-1}(P_0+\sqrt{D})}{u_n Q_0 - v_n (P_0+\sqrt{D})}\end{aligned}$$

$$\begin{aligned}&\Leftrightarrow (P_{n+1} + \sqrt{D})(-G_n + v_n\sqrt{D}) \;=\; Q_{n+1}(u_{n-1}Q_0 - v_{n-1}P_0 + v_{n-1}\sqrt{D}) \\ &\Leftrightarrow -P_{n+1}G_n + v_n D - G_n\sqrt{D} + v_n P_{n+1}\sqrt{D} \;=\; Q_{n+1}G_{n-1} - v_{n-1}Q_{n+1}\sqrt{D}\end{aligned}$$

Vergleicht man die Irrationalteile, erhält man

$$G_n = v_n P_{n+1} + v_{n-1} Q_{n+1} \;.$$

3.2.2 Das Reduktionsverfahren

Es sei $\mathfrak{A} = \left[a, \frac{-b+\sqrt{D}}{2}\right]$ ein primitives Ideal in kanonischer Darstellung, f und τ die entsprechenden Elemente in F und Q.
Entwickelt man τ in einen Kettenbruch, so wird dieser nach endlich vielen, z.B nach k Schritten periodisch. Sei ϕ_k der Rest dieser Kettenbruchentwicklung, wie in Definition 3.9, so ist ϕ_k sowie $\mathfrak{A}_k$, das entsprechende Ideal in I, reduziert. Das bedeutet, daß das Kettenbruchverfahren geeignet ist, aus einem primitiven Ideal ein reduziertes Ideal zu gewinnen. Außerdem erhält man mit diesem Verfahren eine endliche Anzahl, etwa l, weiterer reduzierter Ideale, wenn l die Länge der Periode ist.
In diesem Abschnitt werde ich zeigen, daß das Kettenbruchverfahren (KBV) auf Idealen bzw. Formen eine Äquivalenzumformung ist, in dem Sinne, daß Bild und Urbild zueinander äquivalent sind für die jeweilige in Kapitel 2 erklärte Äquivalenz. Es ist daher als Reduktionsverfahren geeignet, da die reduzierten Ideale, die man erhält, in der gleichen Klasse liegen wie das Ausgangsideal. Damit die auf den Mengen I, Q und F definierten Äquivalenzen erhalten bleiben, wird es nötig sein, das KBV auf nicht reduzierten Irrationalzahlen leicht zu modifizieren. Zudem werde ich die Länge der Vorperiode untersuchen und das KBV in den Werten q_i verändern, wie dies auch Henri Cohen in [Cohen] getan hat, um die Reduktion deutlich zu beschleunigen. Das wichtigste Ergebnis wird sein, daß die Kettenbruchentwicklung eines primitiven Ideals alle reduzierten Ideale der Klasse erzeugt.

Zuerst beschreibe ich einige Eigenschaften von reduzierten Idealen/Formen. Nach Lemma 2.20 ist $\mathfrak{A}$ genau dann reduziert, wenn

$$|\sqrt{D} - 2a| < -b < \sqrt{D}, \qquad \text{für } a > 0\,.$$

Ist $\mathfrak{A}$ reduziert, so gilt also zum einen $0 < a < \sqrt{D}$ und $|b| < \sqrt{D}$ sowie zum anderen

1. $|a| + |c| < \sqrt{D}$, also auch $|c| < \sqrt{D}$. Denn man betrachte:

$$|a| + |c| - \sqrt{D} = \tfrac{D-4|a|\sqrt{D}+4a^2-b^2}{4|a|} = \tfrac{(\sqrt{D}-2|a|)^2-b^2}{4|a|} < 0\,.$$

   Die letzte Ungleichung gilt, da $\mathfrak{A}$ als reduziert vorausgesetzt wurde.

2. $\left|\sqrt{D} - 2|c|\right| < -b < \sqrt{D}$. Denn sei $\epsilon = \pm 1$, so betrachte

$$|b| - \epsilon(2|c| - \sqrt{D}) = \tfrac{1}{2|a|}\underbrace{\left(\sqrt{D} + \epsilon|b|\right)}_{>0}\underbrace{\left(|b| + \epsilon(2|a| - \sqrt{D})\right)}_{>0} > 0.$$

Da a und c in 2. eine symmetrische Funktion haben, erhält man folgende Aussage, die ich für Formen formuliere, da der Wert c beim Ideal nicht explizit auftaucht.

Korollar 3.17. *Eine Form (a, b, c) ist genau dann reduziert, wenn*

$$\left|\sqrt{D} - 2|c|\right| < -b < \sqrt{D}.$$

Nun werde ich zeigen, daß das Kettenbruchverfahren Ideale äquivalent umformt, also als Reduktionsverfahren geeignet ist. Dieselbe Aussage erhält man für Formen mit Hilfe von Ψ_{IF}.

Lemma 3.18. *Sei ρ die Abbildung, die einen Schritt im Kettenbruchverfahren beschreibt, $\mathfrak{A} = \left[\frac{Q_0}{2}, \frac{P_0+\sqrt{D}}{2}\right]$, $\tau = \Psi_{IQ}(\mathfrak{A})$ und $\phi_i = \rho^i \tau = \frac{P_i+\sqrt{D}}{Q_i}$ sowie $\mathfrak{A}_i = \Psi_{QI}(\phi_i)$, dann ist*

$$\mathfrak{A}_i = (-\overline{\psi}_i)\mathfrak{A}_{i-1}\ ,$$

mit $\psi_i = \phi_i^{-1}$, wie in Lemma 3.16.

Beweis:

$$\begin{aligned}
(-\overline{\psi_i})\mathfrak{A}_{i-1} &= \left(\tfrac{P_i+\sqrt{D}}{Q_{i-1}}\right)\left[\tfrac{Q_{i-1}}{2}, \tfrac{P_{i-1}+\sqrt{D}}{2}\right] = \left(\tfrac{P_i+\sqrt{D}}{Q_{i-1}}\right)\left[\tfrac{Q_{i-1}}{2}, \tfrac{q_{i-1}Q_{i-1}-P_i+\sqrt{D}}{2}\right] \\
&= \left[\tfrac{P_i+\sqrt{D}}{2}, \tfrac{D-P_i^2}{2Q_{i-1}} + q_{i-1}\tfrac{P_i+\sqrt{D}}{2}\right] = \left[\tfrac{Q_i}{2}, \tfrac{P_i+\sqrt{D}}{2}\right] \\
&= \mathfrak{A}_i
\end{aligned}$$

□

Im folgenden werde ich das Verhalten von Formen unter dem KBV genau untersuchen, um Aussagen über die Länge der Vorperiode machen zu können. Ausserdem wird man das KBV etwas verändern müssen, damit die Abbildung ρ ein Automorphismus der Mengen I, Q und F ist. Den Reduktionsalgorithmus werde ich sowohl für Formen als auch für Ideale angeben, da diese sich wie bereits in Algorithmus *REDUKTION1* leicht unterscheiden.

Lemma 3.19. *Sei ρ die Abbildung, die einen Schritt im Kettenbruchverfahren beschreibt, und sei $f = (a, b, c)$ mit $0 < a < \sqrt{D}$, $|b| < \sqrt{D}$. So gilt für $\rho f = f' = (a', b', c')$*

1. f und f' sind in F zueinander äquivalent.

2. $a' > 0$

3. f' ist reduziert

Beweis: Sei $\tau = \Psi_{FQ}(f) = \frac{-b+\sqrt{D}}{2a} \in Q$. Dann ist $\rho\tau = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -q \end{smallmatrix}\right)\tau = \frac{1}{\tau - q}$, mit $q = \lfloor \tau \rfloor$. Damit ist, nach Beweis zu Satz 2.19:

$$\rho f = \left(\begin{smallmatrix} -iq & -i \\ -i & 0 \end{smallmatrix}\right) f = \Big(\left(\begin{smallmatrix} q & 1 \\ -1 & 0 \end{smallmatrix}\right) J\Big) f = J\Big(\left(\begin{smallmatrix} q & -1 \\ 1 & 0 \end{smallmatrix}\right) f\Big) \Rightarrow f \sim f'.$$

Die Äquivalenz ist damit erhalten, wenn $f' \in F$, d.h., wenn $a' > 0$.
Ist $\rho f = f' = (a', b', c')$, dann sind

$$\begin{aligned} a' &= -(aq^2 + bq + c) \\ b' &= -b - 2aq \\ c' &= -a \end{aligned}$$

und $\frac{-b+\sqrt{D}}{2a} - 1 < q < \frac{-b+\sqrt{D}}{2a} \Leftrightarrow \sqrt{D} - 2a < b + 2aq < \sqrt{D}$.

Nun sind zwei Fälle zu unterscheiden:

1. $0 < a < \frac{\sqrt{D}}{2}$:

$$\sqrt{D} - 2a = |\sqrt{D} - 2a| = \big|\sqrt{D} - 2|c'|\big| < -b' < \sqrt{D}$$

2. $\frac{\sqrt{D}}{2} < a < \sqrt{D}$: $1 < \frac{-b+\sqrt{D}}{2a} < 2 \Rightarrow q = 1$

$$\Rightarrow -b' = b + 2a > 2a - \sqrt{D} = \big|\sqrt{D} - 2|c'|\big| > 0$$

Also ist f' reduziert. Da $|b'| < \sqrt{D}$ und $D = b'^2 - 4a'c'$, müssen a' und c' verschiedene Vorzeichen haben. Da $a > 0$ und $c' = -a \Rightarrow a' > 0$.

$\square$

Verzichtet man im vorigen Lemma auf die Einschränkungen für b, so benötigt man höchstens eine weitere Anwendung von ρ, um eine reduzierte Form zu erhalten, da b in das Intervall $[\sqrt{D} - 2a, \sqrt{D}]$ abgebildet wird. Ich fasse dies in einem Korollar zusammen.

Korollar 3.20. *Ist $f = (a, b, c)$, mit $a < \sqrt{D}$ und $|b| > \sqrt{D}$, so gilt für $f' = \rho f = (a', b', c')$, $a' < \sqrt{D}$ und $|b'| < \sqrt{D}$. Dann ist $\rho f'$ reduziert.*

Für eine gegebene Form $f = (a,b,c)$ mit $a < \sqrt{D}$ und $\tau = \Psi_{FQ}(f)$ stellt die Kettenbruchentwicklung also ein Reduktionsverfahren dar. Ist $a > \sqrt{D}$, so kann unter Umständen trotzdem $b' > \sqrt{D}$ sein. Dann haben a und a' unterschiedliche Vorzeichen. Dies ist für die Äquivalenz der Ideale einer Klasse nicht weiter von Bedeutung, verletzt jedoch die auf Q und F. Um auch diese zu erhalten, nehme man statt ρ die Abbildung
$R : \tau \mapsto -(\rho\tau) = \frac{-b'+\sqrt{D}}{|a'|} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -q \end{smallmatrix}\right)\tau$, mit $R = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -q \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.
Hierdurch ändern sich die Rekursionsformeln für Q_n, u_n und v_n wie folgt:

$$\begin{aligned} Q_{n+1} &= \tfrac{|D-P_{n+1}^2|}{Q_n} \\ u_{n+1} &= -q_{n+1}u_n - u_{n-1} \\ v_{n+1} &= -q_{n+1}v_n - v_{n-1} \end{aligned}$$

Diese Änderungen ergeben sich aus den Einträgen von R^{-1}, zusammen mit der Aussage von Lemma 3.11. Denn es ist $\phi_n = R^{-1}\phi_{n+1}$, mit $R^{-1} = \left(\begin{smallmatrix} -q_n & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Zur Implementation der Reduktion eines primitiven Ideals bzw. einer primitiven Form läßt sich auf die Verwendung von R statt ρ wegen Lemma 3.18 verzichten.

Sei $f = (a,b,c)$ eine beliebige primitive Form. Ist $a > \sqrt{D}$, so muß das KBV den Wert von a in jedem Schritt verkleinern, unabhängig davon, ob man R oder ρ als Abbildung verwendet. Die Länge der Vorperiode hängt davon ab, um wieviel der Wert von a sich pro Schritt der Kettenbruchentwicklung verringert. Deshalb betrachte man die folgende Ungleichung:
Sei τ' entweder $R\tau$ oder $\rho\tau$, und $a > \sqrt{D}$. Angenommen, b' ist bereits kleiner als $\sqrt{D}$, dann ist auch $a' < \sqrt{D}$. Ist $b' > \sqrt{D}$, so gilt $|b'| < 2a - \sqrt{D}$ und

$$a' = \tfrac{b'^2 - D}{4a} \leq \tfrac{(2a-\sqrt{D})^2 - D}{4a} = \tfrac{4a^2 - 4a\sqrt{D}}{4a} = a - \sqrt{D}\,.$$

Zusammen mit Korollar 3.20 erhält man somit nach höchstens $2 + \frac{a}{\lfloor\sqrt{D}\rfloor}$ Anwendungen von ρ oder R ein reduziertes Ideal bzw. eine reduzierte Form.

Theoretisch ist dieses Verfahren für große Werte von a nicht schnell genug. Aus diesem Grund wähle man eine Modifikation des Kettenbruchverfahrens, wie u.a. bei [Cohen]. Ändert man den Wert von q in der Matrix R ein wenig, so erhält man ein wesentlich schnelleres Reduktionsverfahren. Da der Wert von q die Determinante von R nicht beeinflußt, hat diese Modifikation auch keinen Einfluß auf die äquivalenzerhaltende Eigenschaft der Abbildung R auf den Mengen I, Q und F.
Falls $a, |b| > \sqrt{D}$, nehme man die Abbildung R, jedoch mit $q = \lfloor \frac{1}{2} + \frac{b}{2a} \rfloor$,

statt $q = \lfloor \tau \rceil$. Dann liegt b' zwischen $-a$ und a, und es gilt für a':

$$a' = \tfrac{|b'^2 - D|}{4a} \leq \tfrac{a^2+D}{4a} \leq \tfrac{2a^2}{4a} = \tfrac{a}{2}.$$

Damit erhält man:

Korollar 3.21. *Sei $f \in F$. Dann erhält man nach k Schritten des modifizierten Verfahrens, für ein $k \leq 2 + log\left(\frac{a}{\sqrt{D}}\right)$, eine zu f äquivalente reduzierte Form.*

Die Verbesserung des modifizierten Verfahrens gegenüber dem ersten verdeutlicht das nächste Beispiel. Dabei gibt die Zahl über dem Pfeil den Wert von q in der entsprechenden Übergangsmatrix an. Solange $|b| > \sqrt{D}$ ist, wird R angewandt, sonst ρ.

Beispiel: Sei $D = 33$, $a = 9934$ und $b = -8999$, also $c = 2038$.
Das Verfahren vor der Modifikation:

$$\begin{aligned}
(9934, -8999, 2038) &\xrightarrow{0} (2038, 8999, 9934) \xrightarrow{-3} (1279, 3229, 2038) \xrightarrow{-2} \\
(696, 1887, 1279) &\xrightarrow{-2} (289, 897, 696) \xrightarrow{-2} (58, 259, 289) \xrightarrow{-3} \\
(34, 89, 58) &\xrightarrow{-2} (16, 47, 34) \xrightarrow{-2} (4, 17, 16) \xrightarrow{-2} \\
(2, -1, 4) &\xrightarrow{1} (3, -3, 2)\,.
\end{aligned}$$

Es ist zu beachten, daß $(2, -1, 4)$, noch nicht reduziert ist, da $|\sqrt{33} - 4| > 1 = -b$. Insgesamt wurden zehn Reduktionsschritte benötigt.

Das Verfahren nach der Modifikation:

$$\begin{aligned}
(9934, -8999, 2038) &\xrightarrow{0} (2038, 8999, 9934) \xrightarrow{-2} (88, -874, 2038) \xrightarrow{5} \\
(3, -33, 88) &\xrightarrow{6} (2, -3, -3)\,.
\end{aligned}$$

Es wurden nun nur vier Schritte benötigt. Zwar erhält man ein anderes Element aus F, aber nach den Vorüberlegung gilt:

$$(3, -3, 2) \sim (2, -3, -3)\,,\ \text{denn: } (3, -3, 2) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)(2, -3, -3)\,.$$

Nun beschreibe ich das modifizierte Verfahren explizit, und werde es von nun an als Reduktionsverfahren verwenden. Die erste Schleife des Algorithmus beschreibt das modifizierte Kettenbruchverfahren, welches R oder ρ verwendet,

so daß die Äquivalenz auf Q erhalten bleibt. Sie dient dazu, den Wert von a zu verkleinern, bis $a < \sqrt(D)$ ist.
Die zweite Schleife dient nur dazu, die eventuell nötigen zwei Schritte des gewöhnlichen Kettenbruchverfahrens auszuführen, so daß man ein reduziertes Ideal bzw. eine reduzierte Form erhält.

Algorithmus: *REDUKTION2*

	Ideale	Formen
Eingabe	a, b und D	a, b, c und D
	so daß $\mathfrak{A} = \left[a, \frac{-b+\sqrt{D}}{2}\right]$, primitive, und $D = d_{\mathbb{K}}$	so daß $f = (a, b, c)$ primitiv, und $d_f = D > 0$
Ausgabe	$a_0, \quad b_0$	$a_0, \quad b_0, \quad c_0$
	so daß $\mathfrak{A}_0 = \left[a_0, \frac{-b_0+\sqrt{D}}{2}\right]$ reduziert ist, und $\mathfrak{A}_0 \sim \mathfrak{A}$	so daß $f_0 = (a_0, b_0, c_0)$ reduziert ist, und $f_0 \sim f$
Programm		
(01)	$d \longleftarrow \lfloor\sqrt{D}\rfloor$	$d \longleftarrow \lfloor\sqrt{D}\rfloor$
(02)	$Q_0 \longleftarrow 2a$	$a_0 \longleftarrow a$
(03)	$P_0 \longleftarrow -b$	$b_0 \longleftarrow b$
(04)		$c_0 \longleftarrow c$
(05)	solange ($Q_0 > 2d$ und $\|P_0\| > d$)	solange ($a_0 > d$ und $\|b_0\| > d$)
(06)	Beginn der Schleife	Beginn der Schleife
(07)	$q \longleftarrow \left\lfloor \frac{1}{2} - \frac{P_0}{Q_0} \right\rfloor$	$q \longleftarrow \left\lfloor \frac{1}{2} - \frac{b_0}{2a_0} \right\rfloor$
(08)	$P_0 \longleftarrow qQ_0 - P_0$	$(a_1, b_1, c_1) \longleftarrow (a_0, b_0, c_0)$
(09)	$Q_0 \longleftarrow \frac{\|P_0^2 - D\|}{Q_0}$	$a_0 \longleftarrow a_1 q^2 + b_1 q + c_1$
(10)	Ende der Schleife	$b_0 \longleftarrow -2qa_1 - b_1$
(11)		$c_0 \longleftarrow a_1$
(12)		Ende der Schleife
(13)	wiederhole, bis $\|\sqrt{D} - Q_0\| < P_0 < \sqrt{D}$	wiederhole, bis $\|\sqrt{D} - 2a_0\| < -b_0 < \sqrt{D}$
(14)	Beginn der Schleife	Beginn der Schleife
(15)	$q \longleftarrow \left\lfloor \frac{P_0+d}{Q_0} \right\rfloor$	$q \longleftarrow \left\lfloor \frac{-b_0+d}{2a_0} \right\rfloor$
(16)	$P_0 \longleftarrow qQ_0 - P_0$	$(a_1, b_1, c_1) \longleftarrow (a_0, b_0, c_0)$
(17)	$Q_0 \longleftarrow \frac{D-P_0^2\|}{Q_0}$	$a_0 \longleftarrow -a_1 q^2 - b_1 q - c$
(18)	Ende der Schleife	$b_0 \longleftarrow -2qa_1 - b_1$
(19)		$c_0 \longleftarrow -a_1$
(20)		Ende der Schleife
(23)	Übergebe $(\frac{Q_0}{2}, -P_0)$	Übergebe (a_0, b_0, c_0)

Sei $\mathfrak{A}$ reduziert und f und τ die entsprechenden Elemente in F und Q, dann hat τ eine reinperiodische Kettenbruchentwicklung, $\tau = (\overline{q_0, q_2, \ldots, q_{l-1}})$ und $\tau_i = (\overline{q_i, \ldots, q_{l-1}, q_1, \ldots, q_{i-1}})$, für $\tau_i = \rho^i \tau$.
Ist also $l \in \mathbb{N}$ die Länge der Periode der Kettenbruchentwicklung von τ, so ist $\rho^l \tau = \tau$, also auch $\rho^l f = f$ und $\rho^l \mathfrak{A} = \mathfrak{A}$. Mit anderen Worten, durch iteriertes Anwenden von ρ erhält man einen Zyklus von reduzierten Formen/Idealen einer Klasse. Im folgenden werde ich zeigen, daß man auf diese Weise bereits alle reduzierten Elemente einer Klasse erhält. Dazu benötige ich zunächst ein Lemma.

Lemma 3.22. *Seien $\mathfrak{A}_1$ und $\mathfrak{A}_2$ Ideale in $\mathcal{O}_{\mathbb{K}}$ und $\mathfrak{A}_1 \sim \mathfrak{A}_2$. Sei $a_i = \mathcal{N}(\mathfrak{A}_i)$, für $i = 1, 2$, dann existiert ein $\gamma \in \mathfrak{A}_1$, so daß*

$$(\gamma)\mathfrak{A}_2 = (a_2)\mathfrak{A}_1 \qquad \textit{und} \qquad 0 < \gamma < a_1 \, .$$

Beweis: Da $\mathfrak{A}_1 \sim \mathfrak{A}_2$, existieren $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ mit $(\beta)\mathfrak{A}_2 = (\alpha)\mathfrak{A}_1$. Das bedeutet, es existiert ein $\lambda \in \mathfrak{A}_1$, so daß

$$a_2|\beta| = |\alpha|\lambda \, .$$

Sei $u > 0$ eine von 1 verschiedene Einheit in $\mathcal{O}_{\mathbb{K}}$, dann existiert ein $m \in \mathbb{Z}$ mit $u^m\lambda < a_1$. Sei $\gamma = u^m\lambda$ und $\mathfrak{A}_3 = (\gamma)\mathfrak{A}_2 = (\lambda)\mathfrak{A}_2$, dann ist

$$\begin{aligned} & (\alpha)(a_2)\mathfrak{A}_1 = (a_2)(\beta)\mathfrak{A}_2 = (\alpha)(\lambda)\mathfrak{A}_2 = (\alpha)\mathfrak{A}_3 \\ \Longrightarrow \qquad & (a_2)\mathfrak{A}_1 = \mathfrak{A}_3 = (\gamma)\mathfrak{A}_2 \end{aligned}$$

□

Die Bedeutung der Größe θ_n mit $\theta_n = \prod_{i=1}^k \psi_i = \prod_{i=1}^k \frac{1}{\phi_i}$, die im Lemma 3.16 eingeführt wurde, wird mit dem folgenden Satz klar.

Satz 3.23. *Sei $\mathfrak{A} = \mathfrak{A}_0 = \left[a, \frac{-b+\sqrt{D}}{2}\right]$, $P = P_0 = -b$ und $Q = Q_0 = 2a$. Werden P_i und Q_i erzeugt vom gewöhnlichen Kettenbruchverfahren, so gilt für $\mathfrak{A}_n = \rho^n\mathfrak{A} = \left[\frac{Q_n}{2}, \frac{P_n+\sqrt{D}}{2}\right]$:*

$$(Q_0\theta_n)\mathfrak{A}_n = (Q_n)\mathfrak{A} \, ,$$

für θ_n wie in Lemma 3.16.

Beweis: Sei $\phi_n = \Psi_{IQ}(\mathfrak{A}_n) = \frac{P_n+\sqrt{D}}{Q_n}$ und $\phi = \phi_0$, dann gilt

$$\begin{pmatrix} \theta_n \\ \theta_{n+1} \end{pmatrix} = M \begin{pmatrix} 1 \\ \phi \end{pmatrix}, \qquad \text{mit } M = (-1)^{n+1} \begin{pmatrix} -u_{n-1} & v_{n-1} \\ u_n & -v_n \end{pmatrix}$$

und $det M = (-1)^{2n+1} = -1$, also $M \in GL_2(\mathbb{Z})$.

$\Rightarrow \qquad [\theta_n, \theta_{n+1}] = [1, \phi]$,

und mit $\psi_{n+1} = \frac{1}{\phi_{n+1}} = \frac{\sqrt{D}-P_{n+1}}{Q_n}$, ist

$$\begin{aligned} & (\theta_n)[1, \psi_{n+1}] = [\theta_n, \theta_{n+1}] = [1, \phi] \\ \Rightarrow \quad & (Q_0\theta_n)\mathfrak{A}_n = (Q_0\theta_n)\left[\tfrac{Q_n}{2}, \tfrac{P_n+\sqrt{D}}{2}\right] = (Q_0\theta_n)\left[\tfrac{Q_n}{2}, \tfrac{-P_{n+1}+\sqrt{D}}{2}\right] \\ & \qquad = \left(\tfrac{Q_n Q_0}{2}\theta_n\right)[1, \psi_{n+1}] = \left(Q_n \tfrac{Q_0}{2}\right)[1, \phi] = (Q_n)\mathfrak{A} \end{aligned}$$

□

Damit stehen nun die Hilfsmittel bereit, die man benötigt, um die folgende bereits angekündigte Aussage beweisen zu können.

Satz 3.24. *Seien $\mathfrak{A} = \mathfrak{A}_0$ und $\mathfrak{B}$ reduzierte Ideale, $\rho^i\mathfrak{A} = \mathfrak{A}_i$, $a_i = \mathcal{N}(\mathfrak{A}_i)$ und $c = \mathcal{N}(\mathfrak{B})$. Sind $\mathfrak{A}$ und $\mathfrak{B}$ äquivalent und $\gamma \in \mathfrak{A}$ mit $0 < \gamma < a_0$, so daß*

$$(\gamma)\mathfrak{B} = (c)\mathfrak{A}\,,$$

dann existiert ein $n \geq 1$, so daß $\mathfrak{B} = \mathfrak{A}_n = \rho^n\mathfrak{A}$.

Beweis: Zunächst einmal existiert nach Lemma 3.22 ein solches γ.
Sei $\phi = \Psi_{IQ}(\mathfrak{A}) = \phi_0$ und $\phi_i = \rho^i\phi$. Da ϕ reduziert ist, sind es auch alle ϕ_i. Also gilt für alle $i:\ \phi_i > 1$ und damit sowohl $\theta_k > 0$, als auch $\theta_k > \theta_{k+1}$ für alle k. Außerdem gilt $-1 < \overline{\phi}_i < 0$, für alle i. Also haben $\overline{\theta}_k$ und $\overline{\theta}_{k+1} = \frac{\overline{\theta}_k}{\overline{\phi}_{k+1}}$ verschiedene Vorzeichen.
Des weiteren gibt es keine Schranke $\epsilon > 0$, so daß $\theta_k > \epsilon$, $\forall k$, da

$$0 < \frac{\theta_k}{v_{k-1}} = \left|\frac{u_{k-1}}{v_{k-1}} - \phi\right| < \frac{1}{v_k v_{k-1}}$$

$\Rightarrow\ \theta_k < \frac{1}{v_k}$ für alle k, während $v_k \xrightarrow{k\to\infty} \infty$.

Angenommen $\frac{\gamma}{a_0} \neq \theta_k$, $\forall k$. $\Rightarrow$ $\exists n \in \mathbb{N}:$ $\theta_{n+1} < \frac{\gamma}{a_0} < \theta_n$.
Nach vorigem Satz ist $a_0[\theta_n, \theta_{n+1}] = \mathfrak{A}$, für alle n. Da $\gamma \in \mathfrak{A}$, existieren also $x, y \in \mathbb{Z}$:

$$\frac{\gamma}{a_0} = x\theta_n + y\theta_{n+1}$$

Da $\gamma > \theta_{n+1}a_0$, muß auch $|\overline{\gamma}| < |\overline{\theta}_{n+1}|a_0$ gelten. Denn, angenommen, es sei $|\overline{\gamma}| > |\overline{\theta}_{n+1}|a_0$, und sei $\lambda = a_0\theta_{n+1}$, dann ist $\lambda \in \mathfrak{A}$ und $c\lambda = \gamma\delta$ für ein $\delta \neq 0$ aus $\mathfrak{B}$. Dann gilt für δ:

$$|\delta| = c\left|\frac{\lambda}{\gamma}\right| < c \quad \text{und} \quad |\overline{\delta}| = c\left|\frac{\overline{\lambda}}{\overline{\gamma}}\right| < c\,.$$

Dies steht aber im Widerspruch dazu, daß $\mathfrak{B}$ reduziert ist.

Also gilt $\gamma < \theta_n a_0$ und $|\overline{\gamma}| < |\overline{\theta}_{n+1}|a_0$

$$\Rightarrow \ |x\theta_n + y\theta_{n+1}| < \theta_n \quad \text{und} \quad |x\overline{\theta}_n + y\overline{\theta}_{n+1}| < \overline{\theta}_{n+1}.$$

Da $\overline{\theta}_n$ und $\overline{\theta}_{n+1}$ verschiedene Vorzeichen haben, können nicht beide Ungleichungen gleichzeitig gelten.
Also existiert ein $n \in \mathbb{N}$, so daß $\theta_n = \frac{\gamma}{a_0}$. Daraus folgt

$$\begin{aligned}
(\gamma)\mathfrak{B} \ &= \ (a_0\theta_n)\mathfrak{B} \ = \ (c)\mathfrak{A} \\
\Rightarrow \quad & |\mathcal{N}(\gamma)|\mathcal{N}(\mathfrak{B}) \ = \ c^2\mathcal{N}(\mathfrak{A}) \\
\Leftrightarrow \quad & a_0 a_n c \ = \ c^2 a_0 \ \Leftrightarrow \ c = a_n\,, \qquad \text{da } |\mathcal{N}(\theta_n)| = \tfrac{a_n}{a_0}\,.
\end{aligned}$$

Also ist $(a_0\theta_n)\mathfrak{B} = (a_n)\mathfrak{A}$. Nach Satz 3.23 gilt aber $(a_n)\mathfrak{A} = (a_0\theta_n)\mathfrak{A}_n$, $\forall n$.
$\Rightarrow$ $\mathfrak{B} = \mathfrak{A}_n$ für ein $n \in \mathbb{N}$, und $\gamma = \theta_n a_0$.

$\square$

Fazit: Die reduzierten Ideale einer Klasse bilden also unter Anwendung des Kettenbruchalgorithmus einen Zykel der Länge l. Die unter Ψ_{IQ} zu den reduzierten Idealen gehörenden Irrationalzahlen haben alle eine reinperiodische Kettenbruchentwicklung derselben Länge l. Außerdem dient das Reduktionsverfahren der Erzeugung aller zu einem primitiven Ideal äquivalenten reduzierten Ideale.

Beispiel:
1. Ich greife zuerst das Beispiel von vorher wieder auf, und gebe diesmal den gesamten Zykel der reduzierten Formen an. Auf den Pfeilen stehen wieder die Werte von q im Reduktionsverfahren, d.h. in R für nicht reduzierte Formen

und anschließend in der Abbildung ρ.

$$\begin{aligned}(9934,-8999,2038) &\xrightarrow{0} (2038,8999,9934) \xrightarrow{-2} (88,-874,2038) \xrightarrow{5} \\ (3,-33,88) &\xrightarrow{6} (2,-3,-3) \xrightarrow{2} (1,-5,-2) \xrightarrow{5} (2,-5,-1) \xrightarrow{2} \\ (3,-3,-2) &\xrightarrow{1} (2,-3,-3) \xrightarrow{2} (1,-5,-2) \xrightarrow{5} \dots\end{aligned}$$

Es gibt also nur vier reduzierte Formen in der Klasse von $(9934,-8999,2058)$. Außerdem läßt sich dem Beispiel direkt entnehmen, daß $\Psi_{FQ}\big((1,-5,-2)\big) = \frac{5+\sqrt{33}}{2} = \tau_0$ die Kettenbruchentwicklung $\tau_0 = (5,2,1,2,\tau_0) = (\overline{5,2,1,2})$ hat. Außerdem ist $\Psi_{QI}(\tau_0) = \mathcal{O}_{\mathbb{K}}$. Das heißt, daß $\Psi_{FI}\big((9934,-8999,2058)\big)$ in der Klasse der Hauptideale liegt. Vergleicht man die obigen reduzierten Formen mit der Bedingung für Reduziertheit, so stellt sich heraus, daß es keine weiteren Paare (b,c), geben kann, die die Ungleichung $\big|\sqrt{33}-2|c|\big| < -b < \sqrt{33}$ erfüllen. Das bedeutet, daß es nur diesen Zykel reduzierter Ideale in $\mathcal{O}_{\mathbb{K}}$ gibt. Also ist die Klassenzahl 1.

2. Nun betrachte ich einen Körper mit Klassenzahl größer als eins. Es sei $\mathbb{K} = \mathbb{Q}(\sqrt{257})$, dann ist $h_{\mathbb{K}} = 3$. Das heißt, daß es drei Zykel reduzierter Formen geben muß.
Mit den Bedingungen an reduzierte Formen läßt sich zunächst eine Liste aller möglichen reduzierten Formen erstellen. Wendet man auf diese dann das Kettenbruchverfahren an, so werden diese in ihre Zykel sortiert. Damit eine Form reduziert ist, muß gelten:

- $b \equiv D \mod 2$
- $a, |b| < \sqrt{D}$, und
- $|\sqrt{D} - 2a| < -b < \sqrt{D}$

Es ist $\sqrt{257} \approx 16,01$. Nun lassen sich zu jedem Wert von b alle Werte von a bestimmen, die die obigen Bedingungen erfüllen und für die gilt: $4a \mid b^2 - D$:

$$\begin{array}{ll} b=-1 \ : \ a \in \{8\} & b=\ \ -9 \ : \ a \in \{4,11\} \\ b=-3 \ : \ a \in \{\} & b=-11 \ : \ a \in \{\} \\ b=-5 \ : \ a \in \{\} & b=-13 \ : \ a \in \{2,11\} \\ b=-7 \ : \ a \in \{\} & b=-15 \ : \ a \in \{1,2,4,8\} \end{array}$$

Es gibt also neun reduzierte Formen. Die Zykel erhält man nun, indem man auf eine Form den Kettenbruchalgorithmus solange anwendet, bis man wieder die Ausgangsform erhält. Anschließend nimmt man eine Form, die in diesem Zykel nicht vorkommt, und wendet auf diese den Kettenbruchalgorithmus an, usw. .

Ich beginne mit der Einsklasse, also der Hauptidealklasse, wenn man die Idealklassengruppe betrachtet, und gebe jeweils den Wert q der Übergangsmatrix ρ an. Die drei Zykel lauten dann:

$$\begin{array}{l}
(1,-15,-8) \xrightarrow{15} (8,-15,-1) \xrightarrow{1} (8,-1,-8) \xrightarrow{1} (1,-15,-8) \\
(2,-13,-11) \xrightarrow{7} (4,-15,-2) \xrightarrow{3} (11,-9,-4) \xrightarrow{1} (2,-13,-11) \\
(2,-15,-4) \xrightarrow{7} (11,-13,-2) \xrightarrow{1} (4,-9,-11) \xrightarrow{3} (2,-15,-4)
\end{array}$$

Die Nullstellen mit positiven Irrationalteil der jeweils ersten Form in einem Zykel und ihre Kettenbruchentwicklung lauten dann:

$$\begin{aligned}
\tfrac{15+\sqrt{257}}{2} &= (\overline{15,1,1}) \\
\tfrac{13+\sqrt{257}}{4} &= (\overline{7,3,1}) \\
\tfrac{15+\sqrt{257}}{4} &= (\overline{7,1,3})
\end{aligned}$$

4 Arithmetik in der Klassengruppe

In diesem Kapitel stelle ich zunächst die explizite Multiplikation zweier primitiver Ideale dar. Diese läßt sich auf reduzierte Ideale einschränken. Damit erhält man zunächst eine eindeutige Multiplikation auf $\mathcal{C}l_{\mathbb{K}}$ für einen imaginärquadratischen Zahlkörper $\mathbb{K}$, da die reduzierten Ideale ein eindeutiges Repräsentantensystem der Klassen bilden. Mit Hilfe der Multiplikation läßt sich das Quadrat eines Ideals bestimmen, welches ein schnelles Potenzieren via binärem Shiften ermöglicht. Dies benötigt man unter anderem, um mit $\mathcal{C}l_{\mathbb{K}}$ ein Diffie-Hellmann Schlüsselaustauschverfahren wie in [BuWi88] zu verwirklichen.
Im reellquadratischen Zahlkörper ist die Situation eine andere. Zum einen bilden die reduzierten Ideale kein eindeutiges Repräsentantensystem der Klassen, zum anderen ist bei geeigneter Wahl der Diskriminante, z.B. D prim, die Klassenzahl nach [CoLe84a] und [CoLe84b] meistens eins. Das bedeutet, daß es dann ohnehin nur die Klasse der Hauptideale gibt. Wie bereits beschrieben, bilden die reduzierten Ideale unter Anwendung des gewöhnlichen Kettenbruchverfahrens einen endlichen Zykel. Auf diesem Zykel hat Daniel Shanks in [Shanks] einen Distanzbegriff eingeführt, der es einem ermöglicht, auf diesem Zykel fast wie in einer zyklischen Gruppe zu rechnen. Diesen Distanzbegriff stelle ich im zweiten Abschnitt dieses Kapitels vor und beschreibe im dritten eine Anwendung dieser zwei Arithmetiken: Die Realisierung des Diffie-Hellmann Verfahrens in quadratischen Zahlkörpern nach J. Buchmann und H.C. Williams.

4.1 Multiplikation

Die Definitionen in diesem Abschnitt sind unabhängig vom Vorzeichen der Diskriminante, das heißt, sie gelten sowohl für imaginär- als auch reellquadratische Zahlkörper.

Allgemein gilt für Ideale $\mathfrak{A}$ und $\mathfrak{B}$ eines algebraischen Zahlkörpers, daß das Produkt der Ideale erzeugt wird von den Produkten der Erzeugenden.
Sind $\mathfrak{A}$ und $\mathfrak{B}$ ganze Ideale in einem quadratischen Zahlkörper, so sind $\mathfrak{A} = [\omega_1, \omega_2]$ und $\mathfrak{B} = [\omega_3, \omega_4]$ $\mathbb{Z}$-Moduln vom Rang 2. So auch $\mathfrak{A}\mathfrak{B}$, da $\mathfrak{A}\mathfrak{B}$ wieder ein ganzes Ideal ist. Es existieren also $\omega_5 \in \mathbb{N}$, $\omega_6 \in \mathcal{O}_{\mathbb{K}}$:

$$\mathfrak{A}\mathfrak{B} = [\omega_1\omega_3, \omega_1\omega_4, \omega_2\omega_3, \omega_2\omega_4] = [\omega_5, \omega_6] \, .$$

Eine Basis des Produktes läßt sich für primitive Ideale wie folgt bestimmen.

Satz 4.1. *Seien* $\mathfrak{A}_1 = \left[a_1, \frac{-b_1+\sqrt{D}}{2}\right]$ *und* $\mathfrak{A}_2 = \left[a_2, \frac{-b_2+\sqrt{D}}{2}\right]$ *primitive Ideale in kanonischer Darstellung.*
Dann ist $\mathfrak{A}_1\mathfrak{A}_2 = (t)\mathfrak{A}_3$ *für ein* $t \in \mathbb{N}$ *und ein primitives Ideal* $\mathfrak{A}_3 = \left[a_3, \frac{-b_3+\sqrt{D}}{2}\right]$.
Es ist

$$\begin{aligned} t &= ggT\left(a_1, a_2, \tfrac{-b_1-b_2}{2}\right) \\ &= \alpha a_1 + \beta a_2 - \gamma\left(\tfrac{b_1+b_2}{2}\right), \qquad \alpha, \beta, \gamma \in \mathbb{Z} \textit{ eindeutig gegeben} \\ &\qquad\qquad \textit{durch den erweiterten Euklidischen Algorithmus} \\ a_3 &= \tfrac{a_1 a_2}{t^2} \\ b_3 &= \frac{\alpha a_1 b_2 + \beta a_2 b_1 - \gamma\left(\frac{b_1 b_2 + D}{2}\right)}{t} = b_2 + \tfrac{1}{t}\left(\beta a_2 (b_1 - b_2) - \gamma \tfrac{D - b_2^2}{2}\right). \end{aligned}$$

Beweis: Das Produkt ist ein ganzes Ideal und hat nach Lemma 2.5 eine Darstellung der Gestalt $\mathfrak{A}_1\mathfrak{A}_2 = \left[a, \frac{-b+t\sqrt{D}}{2}\right]$, mit $\mathcal{N}(\mathfrak{A}_1\mathfrak{A}_2) = a_1 a_2 = at$ und $t|a$, $t|b$.
Also existieren a_3 und b_3, so daß $\mathfrak{A}_1\mathfrak{A}_2 = (t)\left[a_3, \frac{-b_3+\sqrt{D}}{2}\right] = (t)\mathfrak{A}_3$, für ein primitives Ideal $\mathfrak{A}_3$. Aus der Betrachtung der Normen ergibt sich $a_3 = \frac{a_1 a_2}{t^2}$.

Es bleiben die Gleichungen für t und b_3 zu zeigen.

$$\mathfrak{A}_1\mathfrak{A}_2 = \left[a_1, \tfrac{-b_1+\sqrt{D}}{2}\right]\left[a_2, \tfrac{-b_2+\sqrt{D}}{2}\right] = \left[a, \tfrac{-b+t\sqrt{D}}{2}\right]$$
$$\Leftrightarrow (a_1 a_2)\mathbb{Z} + a_1 \tfrac{-b_2+\sqrt{D}}{2}\mathbb{Z} + a_2 \tfrac{-b_1+\sqrt{D}}{2}\mathbb{Z} + \tfrac{(-b_1+\sqrt{D})(-b_2+\sqrt{D})}{4}\mathbb{Z} = a\mathbb{Z} + \tfrac{-b+t\sqrt{D}}{2}\mathbb{Z}$$

Koeffizientenvergleich liefert:

1. $a_1\sqrt{D}\mathbb{Z} + a_2\sqrt{D}\mathbb{Z} + \frac{-b_1-b_2}{2}\sqrt{D}\mathbb{Z} = t\sqrt{D}\mathbb{Z}$
   $\Rightarrow \quad t = ggT\left(a_1, a_2, \frac{-b_1-b_2}{2}\right)$. Mit Hilfe des erweiterten Euklidischen Algorithmus lassen sich eindeutig bestimmte Koeffizienten $\alpha, \beta, \gamma \in \mathbb{Z}$ bestimmen, so daß
   $t = \alpha a_1 + \beta a_2 + \gamma\left(\frac{-b_1-b_2}{2}\right)$.

2. Setzt man in Gleichung (4.1) die Koeffizienten von $(a_1 a_2)$ auf der linken Seite und von a auf der rechten Seite gleich Null, so erhält man mit 1.
   $\alpha a_1 \frac{-b_2+\sqrt{D}}{2} + \beta a_2 \frac{-b_1+\sqrt{D}}{2} + \gamma \frac{(-b_1+\sqrt{D})(-b_2+\sqrt{D})}{4} = \frac{-b+t\sqrt{D}}{2}$
   $\Rightarrow tb_3 = b = \alpha a_1 b_2 + \beta a_2 b_1 - \gamma\left(\frac{b_1 b_2 + D}{2}\right) = tb_2 + \beta a_2 (b_1 - b_2) - \gamma \frac{D - b_2}{2}$
   $t|b$, da $\mathfrak{A}_1\mathfrak{A}_2$ ein Ideal ist, und man erhält die gewünschte Darstellung für b_3.

$\square$

Beispiel:

1. Sei $\mathfrak{A}_1 = \left[1, \frac{1+\sqrt{-55}}{2}\right]$, $\mathfrak{A}_2 = \left[4, \frac{3+\sqrt{-55}}{2}\right]$. Dann ist:

$$\begin{aligned} t &= \mathrm{ggT}(1, 2, \tfrac{4}{2}) = 1 = 1a_1 + 0a_2 + 0\tfrac{-b_1-b_2}{2} \\ a_3 &= \tfrac{1\cdot 4}{1} = 4 \\ b_3 &= b_2 = -3\,,\ \text{da } \beta = \gamma = 0 \end{aligned}$$

   Also ist $\mathfrak{A}_1\mathfrak{A}_2 = \left[4, \frac{3+\sqrt{-55}}{2}\right] = \mathfrak{A}_2$. Dies bestätigt, daß $\mathcal{O}_{\mathbb{K}}$ das neutrale Element der Multiplikation ist.

2. Sei $\mathfrak{A}_1 = \left[2, \frac{1+\sqrt{-55}}{2}\right]$, $\mathfrak{A}_2 = \left[2, \frac{-1+\sqrt{-55}}{2}\right]$. Dann ist:

$$\begin{aligned} t &= \mathrm{ggT}(2, 2, \tfrac{0}{2}) = 2 = 1a_1 + 0a_2 + 0\tfrac{-b_1-b_2}{2} \\ a_3 &= \tfrac{2\cdot 2}{2^2} = 1 \\ b_3 &= b_2 = 1\,,\ \text{da } \beta = \gamma = 0 \end{aligned}$$

   Also ist $\mathfrak{A}_1\mathfrak{A}_2 = (2)\left[1, \frac{-1+\sqrt{-55}}{2}\right] = (2)\mathcal{O}_{\mathbb{K}} = (2)$. Das konjugierte Ideal ist, wie man an diesem Beispiel gut sehen kann, das Inverse Element der Multiplikation auf den Idealklassen, da in dem Fall stets $t = a_1 = a_2$ und deswegen $a_3 = 1$ gilt. Das bedeutet, daß das Ergebnis stets das Hauptideal (t) ist, das in der Einsklasse liegt.

3. Schließlich ein nicht triviales Beispiel:
   Sei $\mathfrak{A}_1 = \left[270, \frac{-82+\sqrt{-3515156}}{2}\right]$,$\mathfrak{A}_2 = \left[1707, \frac{-322+\sqrt{-3515156}}{2}\right]$. Dann ist:

$$\begin{aligned} t &= \mathrm{ggT}(270, 1707, \tfrac{404}{2}) = 1 = -13132\cdot 270 + 2077\cdot 1707 - 1\cdot\tfrac{-404}{2} \\ a_3 &= \tfrac{270\cdot 1707}{1} = 460890 \\ b_3 &= -322 + 2077\cdot 1707(-82+322) - \tfrac{-3515156-103684}{2} = 852714458 \end{aligned}$$

   Also ist $\mathfrak{A}_1\mathfrak{A}_2 = \left[460890, \frac{-852714458+\sqrt{-3515156}}{2}\right]$. Das reduzierte Ideal in dieser Klasse läßt sich mit *REDUKTION1* berechnen:
   $\mathfrak{A}_1\mathfrak{A}_2 \sim \left[850, \frac{-538+\sqrt{-3515156}}{2}\right]$.

Korollar 4.2. *Seien $f_1 = (a_1, b_1, c_1)$, $f_2 = (a_2, b_2, c_2) \in F$ und die Bezeichnungen wie in Satz 4.1. So ist mit $f_1f_2 := f_3 = \Psi_{IF}(\mathfrak{A}_3)$ eine Multiplikation auf F definiert.*

F bildet, bezüglich der oben beschriebenen Verknüpfung, eine abelsche Gruppe. Die Form $(1, b, \frac{b^2-D}{4})$, für ein $b \equiv D \mod 2$, heißt Einsform und ist das neutrale Element der Multiplikation. Sei $f = (a, b, c)$, dann ist $f^{-1} = (a, -b, c)$ die zu f inverse Form, da $ggT(a, a, \frac{b-b}{2}) = a$, also $a_3 = 1$ ist. Verändert man die Eingabe durch die Aktion eines Elementes aus $SL_2(\mathbb{Z})$, so verändert sich auch das Ergebnis um ein Element aus $SL_2(\mathbb{Z})$, d.h. die zwei Ergebnisse f_3 und f_3' sind zueinander äquivalent. Denn: Variiert man die Formen f_1 und f_2, entspricht dies der Multiplikation von $\mathfrak{A}_1\mathfrak{A}_2$ mit einem Hauptideal (γ). Aber es ist $\mathfrak{A}_1\mathfrak{A}_2(\gamma) = (t)(\gamma)\mathfrak{A}_3 = (t')\mathfrak{A}'_3 \sim (t)\mathfrak{A}_3$, also auch $f_3' \sim f_3$.
Erklärt man dann die Multiplikation auf $F/SL_2(\mathbb{Z})$ repräsentantenweise, so erhält man eine endliche abelsche Gruppe. Das neutrale Element dieser Gruppe ist die Klasse der Einsform, kurz *Einsklasse*, das inverse Element ist die Klasse der inversen Form.
Via Ψ_{FI} wird die inverse Formklasse auf die Klasse des konjugierten Ideals abgebildet. Daß dies in der Tat das Inverse in $\mathcal{C}l_{\mathbb{K}}$ ist, läßt sich an Hand von $\mathfrak{A}\overline{\mathfrak{A}} = (\mathcal{N}(\mathfrak{A}))$ gut sehen, da $(\mathcal{N}(\mathfrak{A}))$ ein Hauptideal ist und daher in der Einsklasse liegt.

Definition 4.3. Die Gruppe $F_D = F/SL_2(\mathbb{Z})$ heißt Formenklassegruppe.

Ψ_{IF} und Ψ_{FI} bilden die Gruppen F_D und $\mathcal{C}l_{\mathbb{K}}$ bijektiv aufeinander ab. Daher ist die Ordnung der Formenklassegruppe gleich der Klassenzahl.

Schränkt man die Multiplikation primitiver Ideale auf reduzierte Ideale ein und reduziert anschließend das Ergebnis wieder, so erhält man die gesuchte explizite Arithmetik auf der Idealklassengruppe imaginärquadratischer Zahlkörper. Dazu gebe ich die folgenden Algorithmen an, die lediglich für Ideale formuliert sind. Um sie für Formen zu beschreiben, muß man nur $D - b_2^2$, bzw $D - b'^2$ durch $4a_2c_2$, bzw. $4a'c'$ ersetzen und den Algorithmus *PRODUKT1/QUADRAT* um die Zeile ergänzen: $c_3 \longleftarrow \frac{{b_3}^2-D}{4a_3}$ bzw. $c' \longleftarrow \frac{b'^2-D}{4a'}$. Dadurch vergrößert sich die Eingabe und die Ausgabe ebenfalls um die jeweiligen Werte c. So ist in diesem Fall, im Gegensatz zur Implementation der Reduktion, die Idealdarstellung vorzuziehen.
Desweiteren wird eine Pozedur namens ggT3 verwendet, die den größten gemeinsamen Teiler t dreier Zahlen x, y und z sowie die Koeffizienten der Darstellung $t = \alpha x + \beta y + \gamma z$ berechnet. Diese läßt sich durch zweifache Anwendung des erweiterten Euklidischen Algorithmus verwirklichen, der u.a. als Algorithmus *gcd-coeff* in [Forster, Seite 30] und als Algorithmus *Euclid Extended* in [Cohen, Seite 16] beschrieben wird, denn:
Sei $t_1 = \alpha_1 x + \beta_1 y = ggT(x, y)$, dann ist

$t = \beta_2 t_1 + \gamma z = (\alpha_1\beta_2)x + (\beta_1\beta_2)y + \gamma z = ggT(t_1, z) = ggT(x, y, z)$, mit $\alpha = (\alpha_1\beta_2)$ und $\beta = (\beta_1\beta_2)$. Habe im folgenden also ggT3 das Tripel (x, y, z) als Eingabe und das Tripel (t, β, γ) als Ausgabe. Der Wert von α wird im weiteren nicht benötigt.
Die Funktion ggT habe als Eingabe das Zahlenpaar (x, y) und gibt das Tripel (t_1, α_1, β_1) wie oben, aus.

Algorithmus: *PRODUKT1/QUADRAT*

	Produkt auf $\mathcal{C}l_{\mathbb{K}}$ für $D < 0$	**Quadrat** auf $\mathcal{C}l_{\mathbb{K}}$ für $D < 0$
Eingabe	$a_1, b_1, a_2, b_2, D,$	a, b, D
	so daß $\mathfrak{A}_i = \left[a_i, \frac{-b_i+\sqrt{D}}{2}\right]$ reduzierte Ideale sind, für $i = 1, 2$	so daß $\mathfrak{A} = \left[a, \frac{-b+\sqrt{D}}{2}\right]$ reduziert ist
Ausgabe	a_3, b_3	a', b'
	so daß $\mathfrak{A}_3 = \left[a_3, \frac{-b_3+\sqrt{D}}{2}\right]$ reduziert ist, und $\mathfrak{A}_3 \sim \mathfrak{A}_1\mathfrak{A}_2$	so daß $\mathfrak{A}' = \left[a', \frac{-b'+\sqrt{D}}{2}\right]$ reduziert ist, und $\mathfrak{A}' \sim \mathfrak{A}^2$
Programm		
(01)	$(t, \beta, \gamma) \longleftarrow \text{ggT3}(a_1, a_2, \frac{-b_1-b_2}{2})$	$(t, \alpha, \beta) \longleftarrow \text{ggT}(a, -b)$
(02)	$a_3 \longleftarrow \frac{a_1 a_2}{t^2}$	$a' \longleftarrow \left(\frac{a}{t}\right)^2$
(03)	$b_3 \longleftarrow b_2 + \frac{2\beta a_2(b_1-b_2)-\gamma(D-b_2{}^2)}{2t}$	$b' \longleftarrow b + \frac{\beta}{t}\frac{b^2-D}{2}$
(04)	$(a_3, b_3) \longleftarrow$ *REDUKTION1*(a_3, b_3, D)	$(a', b') \longleftarrow$ *REDUKTION1*(a', b', D)
(05)	Übergebe (a_3, b_3)	Übergebe (a', b')

Für $D > 0$ bleibt die Multiplikation lediglich auf den einzelnen Idealen erklärt statt auf den Klassen. Außerdem wird nur in einer einzigen Klasse, z.B. der Hauptidealklasse, gerechnet. Mit Hilfe des im folgenden beschriebenen Distanzbegriffes läßt sich eine Art Multiplikation auf dem Zykel der reduzierten Ideale einer einzigen Klasse erklären.
Diese zwei Multiplikationen, auf $\mathcal{C}l_{\mathbb{K}}$ für $D < 0$ einerseits und auf den reduzierten Hauptidealen andererseits, eignen sich für schnelles Potenzieren via binärem Shiften, was für diese Theorie für verschiedene Anwendungen interessant macht. Eine beschreibe ich beispielhaft im dritten Abschnitt dieses Kapitels, nämlich die Realisierung eines Schlüsselaustauschverfahrens nach Diffie-Hellmann.

4.2 Der Distanzbegriff auf Idealen

In diesem Abschnitt werden nur reellquadratische Zahlkörper betrachtet. Hier bilden die reduzierten Ideale einer Klasse, wie bereits beschrieben, einen endlichen Zykel. Sei $I_R := \{\mathcal{O}_{\mathbb{K}} = \mathfrak{A}_0, \mathfrak{A}_1, \ldots, \mathfrak{A}_{l-1}\}$ der Zykel der reduzierten Hauptideale, so bilden die Erzeugenden die endliche Menge $\{1 = \overline{\theta}_0, \overline{\theta}_1, \ldots, \overline{\theta}_{l-1}\}$. Daniel Shanks erklärte in [Shanks] auf diesem Zykel die Distanz eines Ideals $\mathfrak{A}_n$ zu $\mathfrak{A}_0 = \mathcal{O}_{\mathbb{K}}$ als $\log|\overline{\theta}_n|$. Da die Menge der Erzeugenden diskret in $\mathbb{R}$ liegt, läßt sich zu jeder reellen Zahl x das *dichteste* reduzierte Ideal erklären, indem man das Ideal nimmt, das von $\overline{\theta}_n$ erzeugt wird für $n \in \mathbb{Z}$, so daß $\log|\overline{\theta}_n - x|$ minimal ist. Nennt man dieses $\mathfrak{A}(x)$, so läßt sich mit Hilfe der Addition reeller Zahlen eine Abbildung auf der Menge der reduzierten Hauptideale in sich erklären:

$$* : I_R \times I_R \longrightarrow I_R\,,\ (\mathfrak{A}(x), \mathfrak{A}(y)) \longmapsto \mathfrak{A}(x+y)$$

Kennt man jedoch nur die Zahlen x und y, ist es nicht in angemessener Zeit möglich, die Ideale $\mathfrak{A}(x)$, $\mathfrak{A}(y)$ und $\mathfrak{A}(x+y)$ zu berechnen.
Ziel ist es in diesem Abschnitt, zu beschreiben, wie $\mathfrak{A}(x) * \mathfrak{A}(y) = \mathfrak{A}(x+y)$ mit Kenntnis der Ideale $\mathfrak{A}(x)$ und $\mathfrak{A}(y)$ und Verwendung der Multiplikation von primitiven Idealen relativ schnell berechnet werden kann. Dafür werden zunächst die benötigten Begriffe bereitgestellt. Dabei habe ich den Distanzbegriff gewählt, wie er ursprünglich von Shanks vorgeschlagen wurde und von Wunderlich, Williams und Buchmann erweitert wurde, da dieser sich für eine Anwendung z.B. in einem Diffie-Hellmann Verfahren besser eignet, als der von Cohen in [Cohen, Seite 275] vorgeschlagende. Letzterer ist etwas aufwendiger zu berechnen, wodurch er für eine Implementierung schlechter geeignet ist.

Definition 4.4. Seien $\mathfrak{A}$ und $\mathfrak{B}$ äquivalente Ideale, so daß $\mathfrak{B} = (\gamma)\mathfrak{A}$ für ein $\gamma \in \mathbb{K}$, dann sei die *Distanz* des Ideals $\mathfrak{B}$ zu $\mathfrak{A}$ gegeben durch

$$d(\mathfrak{B}, \mathfrak{A}) := \log|\gamma|\,.$$

Man beachte für die Distanz folgendes:

1. $d(\mathfrak{B}, \mathfrak{A}) = -d(\mathfrak{A}, \mathfrak{B})$. Außerdem ist $d(\mathfrak{B}, \mathfrak{A}) = 0$ genau dann, wenn $\mathfrak{B} = \mathfrak{A}$.

2. Eine Dreiecksungleichung der Form $|d(\mathfrak{C}\mathfrak{B}, \mathfrak{A})| \leq |d(\mathfrak{C}, \mathfrak{A})| + |d(\mathfrak{B}, \mathfrak{A})|$ gilt nicht, da die Distanz nur jeweils auf einer Klasse definiert ist. Die Ungleichung ist daher nur für Hauptideale $\mathfrak{A} = (\alpha)$, $\mathfrak{B} = (\beta)\mathfrak{A}$ und $\mathfrak{C} = (\gamma)\mathfrak{A}$ sinnvoll. Aber auch hier gilt:

$|d(\mathfrak{C}\mathfrak{B}, \mathfrak{A})| = |\log|\alpha\beta\gamma||$. Dies ist im allgemeinen größer als $|\log|\beta\gamma|| = |d(\mathfrak{C}, \mathfrak{A})| + |d(\mathfrak{B}, \mathfrak{A})|$.
Dafür hat man aber für drei beliebige Ideale einer Klasse:
$|d(\mathfrak{C}, \mathfrak{A})| = |d(\mathfrak{C}, \mathfrak{B}) + d(\mathfrak{B}, \mathfrak{A})| \le |d(\mathfrak{C}, \mathfrak{B})| + |d(\mathfrak{B}, \mathfrak{A})|$. Dies ist leichter zu erkennen, wenn man die Gleichungen $\mathfrak{B} = (\gamma)\mathfrak{A}$ und $\mathfrak{C} = (\delta)\mathfrak{B}$ einsetzt.

Für die Distanz reduzierter Ideale lassen sich weitere Aussagen machen:
Seien $\mathfrak{A} = \mathfrak{A}_0$ und $\mathfrak{A}_n = \rho^n \mathfrak{A}_0$ zwei reduzierte zueinander äquivalente Ideale, dann ist nach Satz 3.23:

$$\overline{\theta}_n(Q_0\theta_n)\mathfrak{A}_n = \overline{\theta}_n(Q_n)\mathfrak{A}_0 \;\Leftrightarrow\; (Q_n)\mathfrak{A}_n = (\overline{\theta}_n Q_n)\mathfrak{A}_0 \;\Leftrightarrow\; \mathfrak{A}_n = (\overline{\theta}_n)\mathfrak{A}_0\,,$$

wenn die Werte Q_i wie in der Kettenbruchentwicklung, also $\mathcal{N}(\mathfrak{A}) = \frac{Q_0}{2}$ und $\mathcal{N}(\mathfrak{A}_n) = \frac{Q_n}{2}$ sind.
Die Distanz von $\mathfrak{A}_n$ zu $\mathfrak{A}$ ist also gegeben durch:

$$d(\mathfrak{A}_n, \mathfrak{A}_0) := \log|\overline{\theta}_n|\,.$$

Ist $n > 0$, so ist auch $d(\mathfrak{A}_n, \mathfrak{A}_0) > 0$. Denn ist $\mathfrak{A}_0$ reduziert, so auch alle $\mathfrak{A}_i$, und es gilt: $-1 < \overline{\Psi_{IQ}(\mathfrak{A}_i)} = \overline{\phi}_i < 0$ für alle $i \ge 0$. Also ist $|\overline{\theta}_n| = \prod_{i=1}^{n} \frac{1}{|\overline{\phi}_i|} \ge 1$.
Hieraus folgt, daß

$$d(\mathfrak{A}_n, \mathfrak{A}_m) = \begin{cases} \log\left(\prod_{i=m}^{n} |\overline{\psi_i}|\right) > 0 & , \text{ für } n > m \\ \log\left(\prod_{i=n}^{m} |\overline{\phi_i}|\right) < 0 & , \text{ für } m > n \end{cases}$$

für äquivalente reduzierte Ideale $\mathfrak{A}_m$ und $\mathfrak{A}_n$.
Die Distanz zwischen reduzierten Idealen eines Zykels ist jedoch nicht eindeutig, denn:

Satz 4.5. *Sei l die Länge der Periode in der Kettenbruchentwicklung von $\Psi_{IQ}(\mathfrak{A}_0)$, $\mathfrak{A}_0$ reduziert, dann ist $n = l$ die kleinste Zahl, so daß $\mathfrak{A}_n = \mathfrak{A}_0$, und es gilt:*
$|\overline{\theta}_l|$ ist die Grundeinheit in $\mathcal{O}_{\mathbb{K}}$.

Die Grundeinheit η ist die kleinste Einheit größer als eines. Der Dirichletsche Einheitensatz besagt, daß dann jede Einheit u in $\mathcal{O}_{\mathbb{K}}$ eine Darstellung der Form: $u = \pm\eta^n$ für ein $n \in \mathbb{Z}$ hat.
Das Berechnen der Grundeinheit in reellquadratischen Zahlkörpern ist eins der klassischen schwierigen Probleme in der Zahlentheorie. Shanks hat zur Berechnung derselben den Distanzbegriff eingeführt, um schneller den Zykel der reduzierten Ideale ohne Informationsverlust durchlaufen zu können.

Der Logarithmus der Grundeinheit heißt Regulator und wird im weiteren mit $\mathtt{R} := \log \eta$ bezeichnet.
Beweis zu Satz 4.5: Sei $u > 1$ eine Einheit in $\mathcal{O}_{\mathbb{K}}$, dann gilt $\mathfrak{A}_0 = u\mathfrak{A}_0$. Sei $\mathfrak{A}_{n-1}$ reduziert und $\mathfrak{A}_n = \mathfrak{A}_0$, so ist $n = xl$ und $\mathfrak{A}_n = u\mathfrak{A}_0 = (\overline{\theta}_n)\mathfrak{A}_0$.
Es ist $|\overline{\theta}_{j+1}| \geq |\overline{\theta}_j| \geq 1$ für alle $j > 0$. Deshalb ist $|\overline{\theta}_{l+1}|$ die kleinste Zahl größer als eins, die die Gleichung erfüllt. Damit ist u eine Potenz von $|\overline{\theta}_{l+1}|$. □

Korollar 4.6. *Die in Definition 4.4 definierte Distanz ist nur modulo Regulator,* $\mathtt{R} = \log|\overline{\theta}_l|$, *eindeutig.*

Nun läßt sich eine Distanz zwischen reellen Zahlen und Hauptidealen erklären. Hier orientiere ich mich an den Definitionen von Buchmann, Williams und Wunderlich in [BuWi89] und [WiWu].

Definition 4.7. Sei $\mathfrak{A} = (\alpha)$ und $x \in \mathbb{R}$. Dann sei die Distanz von $\mathfrak{A}$ zu x gegeben durch

$$d(\mathfrak{A}, x) := \log|\alpha| - x\,.$$

Da I_R endlich ist, läßt sich zu jedem $x \in \mathbb{R}_{>0}$ ein Ideal $\mathfrak{A}_n \in I_R$ bestimmen, so daß $|\log|\overline{\theta}_n| - x|$ minimal ist. Ein solches Ideal sei näher bezeichnet:

Definition 4.8. Sei $\mathfrak{A}_0 = \mathcal{O}_{\mathbb{K}}$, $\mathfrak{A}_n = (\overline{\theta}_n)\mathfrak{A}_0 = (\overline{\theta}_n)$ und $x \in \mathbb{R}_{>0}$. Dann sei die Distanz von $\mathfrak{A}_n$ zu x gegeben durch

$$d(\mathfrak{A}_n, x) := \log|\overline{\theta}_n| - x\,.$$

Sei $x \in \mathbb{R}_{>0}$ gegeben, so sei $\mathfrak{A}(x) := \mathfrak{A}_n$ das reduzierte Hauptideal, für daß $|\log|\overline{\theta}_n| - x|$ minimal ist.
Mit $\mathfrak{A}_-(x)$ sei das reduzierte Hauptideal $\mathfrak{A}$ bezeichnet, für das $d(\mathfrak{A}, x) < 0$ maximal ist, und mit $\mathfrak{A}_+(x)$ sei das reduzierte Hauptideal $\mathfrak{A}$ bezeichnet, für das $d(\mathfrak{A}, x) > 0$ minimal ist.

Ich werde im weiteren die Distanz $d(\mathfrak{A}(x), x)$ kurz mit $d(x)$ bezeichnen. Weiterhin sei zu beachten, daß $\mathfrak{A}(x) \in \{\mathfrak{A}_-(x), \mathfrak{A}_+(x)\}$, wobei $\mathfrak{A}_-(x)$ und $\mathfrak{A}_+(x)$ im Zykel der reduzierten Ideale nebeneinander stehen. Diese Eigenschaft sei ebenfalls näher gekennzeichnet.

Definition 4.9. Sei $(\mathfrak{A}_0, \mathfrak{A}_1, \dots, \mathfrak{A}_{l-1}, \mathfrak{A}_l = \mathfrak{A}_0)$ der Zykel der reduzierten Ideale einer Klasse.
Ein Ideal $\mathfrak{A}$ heißt *linker Nachbar* von $\mathfrak{A}_i$, wenn
$\mathfrak{A} = \mathfrak{A}_{i-1} = (-\overline{\phi}_i)\mathfrak{A}_i = (-\overline{\phi}_i\overline{\theta}_i)\mathfrak{A}_0 = \rho^{-1}\mathfrak{A}_i$.
$\mathfrak{A}$ heißt *rechter Nachbar* von $\mathfrak{A}_i$, wenn
$\mathfrak{A} = \mathfrak{A}_{i+1} = (-\overline{\psi}_{i+1})\mathfrak{A}_i = (\overline{\theta}_{i+1})\mathfrak{A}_1 = \rho\mathfrak{A}_i$.

An der Definition läßt sich die Distanz benachbarter Ideale direkt ablesen:

$$d(\mathfrak{A}_{i+1}, \mathfrak{A}_i) = \log|\overline{\psi}_{i+1}| \qquad \text{und} \qquad d(\mathfrak{A}_i, \mathfrak{A}_{i+1}) = \log|\overline{\phi}_{i+1}|$$

Das folgende Lemma beschreibt die Größenordnung der Distanz benachbarter Ideale.

Lemma 4.10. *Seien mit* $\mathfrak{A}_n = \left[\frac{Q_n}{2}, \frac{P_n+\sqrt{D}}{2}\right]$*, für* $n \geq 0$*, die reduzierten Ideale einer Klasse gegeben, so gilt für benachbarte Ideale* $\mathfrak{A}_{n-1}, \mathfrak{A}_n$ *und* $\mathfrak{A}_{n+1}$*:*

(i) $\log\left|1 + \frac{1}{\sqrt{D}}\right| < d(\mathfrak{A}_{n+1}, \mathfrak{A}_n) < \log\sqrt{D}$*, für* $n \geq 0$*,*

(ii) $\log 2 < d(\mathfrak{A}_{n+1}, \mathfrak{A}_{n-1})$*, für* $n \geq 1$*.*

Beweis: Es ist:

$$\begin{aligned} \mathfrak{A}_{n+1} &= (-\overline{\psi}_{n+1})\mathfrak{A}_n = (\overline{\psi}_{n+1}\overline{\psi}_n)\mathfrak{A}_{n-1} \\ \mathfrak{A}_{n-1} &= (-\overline{\phi}_n)\mathfrak{A}_n = (\overline{\phi}_n\overline{\phi}_{n+1})\mathfrak{A}_{n+1}\,. \end{aligned}$$

Da die Ideale reduziert sind, gilt für die Werte P_i, Q_i und q_i aus der Kettenbruchentwicklung, für alle $i \geq 0$, :
$0 < P_i < \sqrt{D}$, $2 \leq Q_i < 2\sqrt{D}$ und $q_i \geq 1$, sowie für $\phi_i = \Psi(\mathfrak{A}_i)$:
$1 < \phi_i$, $-1 < \overline{\phi}_i < 0$ und $\psi_i = \frac{1}{\phi_i}$.

zu (i) $\exp(d(\mathfrak{A}_{n+1}, \mathfrak{A}_n)) = |\overline{\psi}_{n+1}| = -\overline{\psi}_{n+1} = \frac{P_{n+1}+\sqrt{D}}{Q_n} < \frac{2\sqrt{D}}{Q_n} < \sqrt{D}$ und
$-\overline{\psi}_{n+1} = \frac{P_{n+1}+\sqrt{D}}{Q_n} = \frac{q_nQ_n-P_n+\sqrt{D}}{Q_n} = q_n + (-\overline{\phi}_n) = q_n + \frac{1}{-\overline{\psi}_n} > 1 + \frac{1}{\sqrt{D}}$.

zu (ii)

$$\begin{aligned} \exp(d(\mathfrak{A}_{n+1}, \mathfrak{A}_{n-1})) = |\overline{\psi}_{n+1}\overline{\psi}_n| &= \frac{P_n+\sqrt{D}}{Q_{n-1}}\frac{P_{n+1}+\sqrt{D}}{Q_n} = \frac{(P_n+\sqrt{D})(q_nQ_n-P_n+\sqrt{D})}{Q_nQ_{n-1}} \\ &= \frac{D-P_n^2}{Q_nQ_{n-1}} + q_nQ_n\frac{P_n+\sqrt{D}}{Q_nQ_{n-1}} = 1 + q_n\frac{q_{n-1}Q_{n-1}-P_{n-1}+\sqrt{D}}{Q_{n-1}} \\ &= 1 + q_nq_{n-1} + (-\overline{\phi}_{n-1}) > 1 + 1 + \frac{1}{\sqrt{D}} > 2 \end{aligned}$$

□

Die Nachbarn eines reduzierten Ideals lassen sich leicht mit den Rekursionsformeln für P_i und Q_i aus Lemma 3.15 bestimmen.
Hierzu gebe ich nun einen Algorithmus an.

Algorithmus: *NACHBAR*

	linker Nachbar	**rechter Nachbar**
Eingabe	P_i, Q_i und D	P_i, Q_i und D
	so daß $\mathfrak{A}_i = \left[\frac{Q_i}{2}, \frac{P_i+\sqrt{D}}{2}\right]$ ein reduziertes Ideal in $\mathcal{O}_{\mathbb{K}}$ ist, $D = d_{\mathbb{K}}$	so daß $\mathfrak{A}_i = \left[\frac{Q_i}{2}, \frac{P_i+\sqrt{D}}{2}\right]$ ein reduziertes Ideal in $\mathcal{O}_{\mathbb{K}}$ ist, $D = d_{\mathbb{K}}$
Ausgabe	$P_{i-1}, \quad Q_{i-1}, \quad \gamma$	$P_{i+1}, \quad Q_{i+1}, \quad \gamma$
	so daß $\mathfrak{A}_{i-1} = \left[\frac{Q_{i-1}}{2}, \frac{P_{i-1}+\sqrt{D}}{2}\right]$ der linke Nachbar von $\mathfrak{A}_i$ ist, und $\mathfrak{A}_{i-1} = (\gamma)\mathfrak{A}_i$	so daß $\mathfrak{A}_{i+1} = \left[\frac{Q_{i+1}}{2}, \frac{P_{i+1}+\sqrt{D}}{2}\right]$ der rechte Nachbar von $\mathfrak{A}_i$ ist, und $\mathfrak{A}_{i+1} = (\gamma)\mathfrak{A}_i$
Programm		
(01)	$Q_{i-1} \longleftarrow \frac{D-{P_i}^2}{Q_i}$	
(02)	$q_{i-1} \longleftarrow \left\lfloor \frac{P_i+\sqrt{D}}{Q_{i-1}} \right\rfloor$	$q_i \longleftarrow \left\lfloor \frac{P_i+\sqrt{D}}{Q_i} \right\rfloor$
(03)	$P_{i-1} \longleftarrow q_{i-1}Q_{i-1} - P_i$	$P_{i+1} \longleftarrow q_iQ_i - P_i$
(04)		$Q_{i+1} \longleftarrow \frac{D-{P_{i+1}}^2}{Q_i}$
(05)	$\gamma \longleftarrow \left\lvert \frac{-P_i+\sqrt{D}}{Q_i} \right\rvert$	$\gamma \longleftarrow \left\lvert \frac{P_{i+1}+\sqrt{D}}{Q_i} \right\rvert$
(06)	Übergebe $(P_{i-1}, Q_{i-1}, \gamma)$	Übergebe $(P_{i+1}, Q_{i+1}, \gamma)$

Mit den nun zur Verfügung stehenden Mitteln läßt sich $\mathfrak{A}(x)*\mathfrak{A}(y) = \mathfrak{A}(x+y)$ mit Hilfe der Idealmultiplikation berechnen, sofern $\mathfrak{A}(x)$, $\mathfrak{A}(y)$, $d(x)$ und $d(y)$ gegeben sind. Man beachte, daß dies keine echte Einschränkung ist, da dies die Werte sind, die man sich in einer Anwendung wie etwa dem Diffie-Hellmann Verfahren vorgibt. Als Ergebnis erhält man nicht nur $\mathfrak{A}(x+y)$, sondern auch $d(x+y)$:

Sei $\mathfrak{A}(x) = \mathfrak{A}_r = (\overline{\theta}_r)$ und $\mathfrak{A}(y) = \mathfrak{A}_s = (\overline{\theta}_s)$ für $r, s \in \mathbb{Z}$ und $\mathfrak{A}_0 = \mathcal{O}_{\mathbb{K}}$. Dann existiert ein primitives Ideal $\mathfrak{C}$ und eine ganze Zahl t, so daß

$$(t)\mathfrak{C} = \mathfrak{A}(x)\mathfrak{A}(y) = (\overline{\theta}_r\overline{\theta}_s)\,, \qquad \text{also}$$
$$d(\mathfrak{C}, x+y) = d(x) + d(y) - \log|t|\,.$$

Reduziert man $\mathfrak{C}$ und berechnet in jeder Schleife von *REDUKTION2* die Werte v_i, wie in Gleichung (8) bzw. wie auf Seite 46, so erhält man ein reduziertes Ideal $\mathfrak{C}_m = \mathfrak{A}_k$, für ein $k \in \mathbb{Z}$, wobei m die Anzahl der Reduktionsschritte angibt. Mit den Werten P_m und Q_m sowie der v_i aus dem Reduktionsverfahren läßt sich G_{m-1} und damit $\overline{\theta}_m$ berechnen, so daß $(\overline{\theta}_m)\mathfrak{C} = \mathfrak{C}_m = \mathfrak{A}_k$.
Hieraus berechne man die genaue Distanz von $\mathfrak{A}_k$ zu $x+y$:

$$d(\mathfrak{A}_k, x+y) = d(x) + d(y) + \log\left|\frac{\overline{\theta}_m}{t}\right|.$$

Das bedeutet, daß $\mathfrak{A}_k$ in der Regel nicht das gesuchte Ideal $\mathfrak{A}(x+y)$ ist. Die Werte $d(x)$ und $d(y)$ sind aber sehr klein, da etwa $|d(x)| < |d(\mathfrak{A}_+(x), \mathfrak{A}_-(x))|$. Aus Satz 4.11 wird folgen, daß auch $\delta = \log\left|\frac{\overline{\theta}_m}{t}\right|$ ausreichend klein ist, um mit wenigen, d.h. $O(\log D)$, Anwendungen des *NACHBAR* Algorithmus das gesuchte Ideal $\mathfrak{A}(x+y) = \mathfrak{A}_n$, für ein $n \in \mathbb{Z}$, zu berechnen. Ist $d(x) + d(y) + \delta < 0$, berechne man rechte Nachbarn, ist $d(x) + d(y) + \delta > 0$, linke Nachbarn.
Für die Multiplikation auf den reduzierten Hauptidealen im reellquadratischen Zahlkörper gebe ich nun einen Algorithmus an. In den Zeilen (01) bis (03) werden t und $\mathfrak{C}$ berechnet, in Zeile (04) $\mathfrak{C}_m = \mathfrak{A}_k$ und $\overline{\theta}_m$. Damit erhält man in Zeile (05) die Distanz $d(\mathfrak{A}_k, x+y)$.
Je nachdem, ob diese größer oder kleiner Null ist, werden solange die linken bzw. die rechten Nachbarn bestimmt, bis man die Ideale $\mathfrak{A}_-(x)$ und $\mathfrak{A}_+(x)$ erhält. In den Zeilen (13) und (22) werden die Distanzen dieser zwei Ideale zu $x+y$ miteinander verglichen und das dichtere übergeben.

Algorithmus: *PRODUKT2*

reduzierte Hauptideale

Eingabe

$a_1, b_1, a_2, b_2, d_1, d_2, D$, so daß

$\mathfrak{A}_i = \left[a_i, \frac{b_i+\sqrt{D}}{2}\right]$, $i = 1, 2$, und
$\mathfrak{A}_1 = \mathfrak{A}(x)$, $\mathfrak{A}_2 = \mathfrak{A}(y)$, $d_1 = d(x)$ und $d_2 = d(y)$,
für $x, y \in \mathbb{R}$

Ausgabe

a_3, b_3, d_3, so daß

$\mathfrak{A}_3 = \left[a_3, \frac{b_3+\sqrt{D}}{2}\right] = \mathfrak{A}(x+y)$,
und $d_3 = d(x+y)$

Programm

$(t, \beta, \gamma) \longleftarrow ggT3(a_1, a_2, \frac{-b_1-b_2}{2})$
$a_3 \longleftarrow \frac{a_1 a_2}{t^2}$
$b_3 \longleftarrow b_2 + \frac{2\beta a_2(b_1-b_2)-\gamma(D-b_2^2)}{2t}$
$(a_3, b_3, \overline{\theta}_m) \longleftarrow$ *REDUKTION2*(a_3, b_3, D)
$d_3 \longleftarrow d_1 + d_2 + \log|\frac{\overline{\theta}_m}{t}|$
falls $d_3 \leq 0$
  solange $d_3 \leq 0$, wiederhole
    Beginn der Schleife
    $(a_3', b_3', d_3') \longleftarrow (a_3, b_3, d_3)$
    $(a_3, b_3, \delta) \longleftarrow$ rechter*Nachbar*(a_3, b_3, D)
    $d_3 \longleftarrow d_3 + \log|\delta|$
    Ende der Schleife
  falls $|d_3'| < |d_3|$, dann übergebe (a_3', b_3', d_3')
  sonst übergebe (a_3, b_3, d_3)
falls $d_3 > 0$
  solange $d_3 > 0$, wiederhole
    Beginn der Schleife
    $(a_3', b_3', d_3') \longleftarrow (a_3, b_3, d_3)$
    $(a_3, b_3, \delta) \longleftarrow$ linker*Nachbar*(a_3, b_3, D)
    $d_3 \longleftarrow d_3 + \log|\delta|$
    Ende der Schleife
  falls $|d_3'| < |d_3|$, dann übergebe (a_3', b_3', d_3')
  sonst übergebe (a_3, b_3, d_3)

Ich gebe nun ein Beispiel für die „$*$“-Multiplikation an, wie sie z.B. in einem Diffie-Hellmann Verfahren verwendet werden kann, wodurch der Algorithmus *PRODUKT2* ebenfalls anschaulicher wird.

Beispiel: Sei $D = 421$. Dann ist der Zykel der Formen in der Einsklasse, mit anderen Worten der Zykel der Hauptideale beschrieben durch:

$f_0 = (1, -19, -15)$	$\xrightarrow{2} f_7 = (7, -15, -7)$
$\xrightarrow{19} f_1 = (15, -19, -1)$	$\xrightarrow{2} f_8 = (9, -13, -7)$
$\xrightarrow{1} f_2 = (5, -11, -15)$	$\xrightarrow{1} f_9 = (11, -5, -9)$
$\xrightarrow{3} f_3 = (3, -19, -5)$	$\xrightarrow{1} f_{10} = (3, -17, -11)$
$\xrightarrow{6} f_4 = (11, -17, -3)$	$\xrightarrow{6} f_{11} = (5, -19, -3)$
$\xrightarrow{1} f_5 = (9, -5, -11)$	$\xrightarrow{3} f_{12} = (15, -11, -5)$
$\xrightarrow{1} f_6 = (7, -13, -9)$	$\xrightarrow{1} f_{13} = (1, -19, -15)$

Die Form f_0 bzw. f_{13} ist also die Einsform. Ich betrachte das Produkt $\mathfrak{A}(x) * \mathfrak{A}(y)$, mit $x = \log|\overline{\theta}_1|$ und $y = \log|\overline{\theta}_3|$. Also $\mathfrak{A}_1 * \mathfrak{A}_3$, mit $d(x) = 0 = d(y)$.
Das Produkt der beiden primitiven Ideale wird im obigen Algorithmus in den Zeilen (01) bis (03) berechnet:
$\mathfrak{A}_1\mathfrak{A}_3 = (t)\mathfrak{C} = (1)\left[45, \frac{49+\sqrt{421}}{2}\right]$. $\mathfrak{C}$ entspricht der Form $(45, -49, 11)$. Diese ist noch nicht reduziert.
Es wird dann in Zeile (04) der Algorithmus *REDUKTION2* aufgerufen, den ich für die entsprechende Form beschreibe, und auf den sich die folgenden Zeilenangaben beziehen:
Der Algorithmus wird initialisiert mit den Werten $d = 20$, $a_0 = 45$, $b_0 = -49$ und $c_0 = 11$ sowie $v_{-2} = 1$ und $v_{-1} = 0$. Die Schleifenbedingung in Zeile (05) ist erfüllt, so daß die erste Schleife durchlaufen wird. Man erhält: $q_0 = -1$, $a_1 = 7$, $b_1 = -41$ und $c_1 = 45$ sowie $v_0 = -1$.

Nun ist die Bedingung in Zeile (05) nicht mehr erfüllt, da $a_1 < d$. Dafür ist aber die Bedingung in Zeile (13) noch erfüllt, so daß die zweite Schleife durchlaufen wird:
$q_1 = 1$, $a_2 = 7$, $b_2 = -15$ und $c_2 = -7$ sowie $v_1 = 4$. Diese Form ist reduziert, also bricht der Algorithmus ab.

Das bedeutet, daß $\mathfrak{C}_2 = \mathfrak{A}_7$ und $G_1 = 4 \cdot 15 - 1 \cdot 14 = 46$ also $\overline{\theta}_2 = \frac{46+4\cdot\sqrt{421}}{90}$

ist. Damit ergibt sich der Abstand

$$\begin{aligned} d(\mathfrak{A}_7, x+y) &= d(x) + d(y) + \log\left|\frac{\overline{\theta}_2}{t}\right| \\ &= \log|\overline{\theta}_2| \approx 0.35279182192872405806337287388l. \end{aligned}$$

Da dies größer Null ist, werden nun linke Nachbarn berechnet, sowie deren Abstand zu $x+y$:
$\mathfrak{A}_6 = \left[7, \frac{13+\sqrt{421}}{2}\right]$ und $\overline{\phi}_7 = \frac{15-\sqrt{421}}{14}$. Man erhält
$d(\mathfrak{A}_6, x+y) = d(\mathfrak{A}_7, x+y) + \log|\overline{\phi}_7| \approx -0.5781984694869888590264759850 28$. Daraus folgt, daß $\mathfrak{A}_6 = \mathfrak{A}_-(x+y)$ und $\mathfrak{A}_7 = \mathfrak{A}_+(x+y)$. Da $|d(\mathfrak{A}_7, x+y)| < |d(\mathfrak{A}_6, x+y)|$, ist $\mathfrak{A}_7$ das gesuchte Ideal.

Also diese Werte x und y gilt: $\mathfrak{A}_1 * \mathfrak{A}_3 = \mathfrak{A}_7$.

Der folgende Satz ist etwas allgemeiner gefaßt, als dies in diesem Zusammenhang nötig ist. Es erlaubt einem dafür, die Theorie auf jede beliebige Klasse auszudehnen, aber ich werde dies in dieser Arbeit nicht weiter verfolgen.
Der Satz gibt ein Maß dafür an, wie weit das zunächst berechnete reduzierte Ideal $\mathfrak{A}_k$ von $x+y$ entfernt ist. Das Ergebnis des Satzes liefert, daß $\mathfrak{A}(x)*\mathfrak{A}(y) = \mathfrak{A}(x+y)$ mit Hilfe der Idealmultiplikation und des *NACHBAR*-Algorithmus schnell berechnet werden kann. Um die verschiedenen Klassen besser unterscheiden zu können, sind die reduzierten Hauptideale mit $\mathfrak{A}_i$ und ihre Erzeugenden mit $\overline{\theta}_i$ bezeichnet. Die reduzierten Ideale einer zweiten, beliebigen Klasse heißen $\mathfrak{B}_j$. Diese werden durch das gewöhnliche KBV von einem reduzierten Ideal $\mathfrak{B}_0$ erzeugt, also $\mathfrak{B}_j = (\overline{\theta}'_j)\mathfrak{B}_0$. $\overline{\theta}'_j$ berechnet sich wie in Lemma 3.16, der Strich bei $\overline{\theta}'_j$ soll lediglich das Unterscheiden zwischen den beiden Klassen erleichtern. Die auftretenden Werte $\overline{\theta}''_k$ entstehen beim Reduzieren eines primitives Ideals mit dem modifizierten Kettenbruchverfahren. Sie unterscheiden sich daher von den $\overline{\theta}_i$ und $\overline{\theta}'_j$ in den Rekursionsformeln der v_n, die zur Berechnung der jeweiligen Werte benötigt werden, vgl. Seite 46.

Satz 4.11. *Seien $\mathfrak{A}_0 = \mathcal{O}_{\mathbb{K}} = (1)$, $\mathfrak{B}_0$ reduziert und $\mathfrak{A}_r = (\overline{\theta}_r)\mathfrak{A}_0 = (\overline{\theta}_r)$, $\mathfrak{B}_s = (\overline{\theta}'_s)\mathfrak{B}_0$, dann existiert ein $t \in \mathbb{Z}$ und ein primitives Ideal $\mathfrak{C} = \mathfrak{C}_0$:*

$$(t)\mathfrak{C} = \mathfrak{A}_r\mathfrak{B}_s\,.$$

Sei m minimal, so daß $\mathfrak{C}_m$ reduziert ist, dann existiert ein $k \in \mathbb{N}$, so daß $\mathfrak{C}_m = \mathfrak{B}_k$ und

$$d(\mathfrak{B}_k, \mathfrak{B}_0) = d(\mathfrak{A}_r, \mathfrak{A}_0) + d(\mathfrak{B}_s, \mathfrak{B}_0) + \delta\,,$$

mit $-\log D < \delta < \log(2\sqrt{D})$.

Beweis: Seien $d_r = d(\mathfrak{A}_r, \mathfrak{A}_0)$, $d_s = d(\mathfrak{B}_s, \mathfrak{B}_0)$ und $d_k = d(\mathfrak{B}_k, \mathfrak{B}_0)$.
Es gilt $\mathfrak{C}_m \sim \mathfrak{C}_0 \sim \mathfrak{A}_r\mathfrak{B}_s \sim \mathfrak{B}_s \sim \mathfrak{B}_0$, da $\mathfrak{A}_r$ ein Hauptideal ist.
Genauer: Mit $\mathfrak{C}_m = \overline{\theta}''_m\mathfrak{C}_0$ gilt, [5]

$$\begin{aligned} \mathfrak{B}_k = \mathfrak{C}_m = \left(\tfrac{\overline{\theta}_r\overline{\theta}'_s\overline{\theta}''_m}{t}\right)\mathfrak{B}_0 &= \overline{\theta}'_k\mathfrak{B}_0 \\ \Rightarrow d_k &= \log|\overline{\theta}_r| + \log|\overline{\theta}'_s| + \log\left|\tfrac{\overline{\theta}''_m}{t}\right| \\ &= d_r + d_s + \delta \end{aligned}$$

Zu zeigen bleibt: $-\log D < \delta = \log\left|\frac{\overline{\theta}''_m}{t}\right| < \log 2\sqrt{D}$.

Bezeichne ρ in diesem Fall einen Schritt im modifizierten KBV und sei $\mathfrak{C}_0 = \left[\frac{Q_0}{2}, \frac{P_0+\sqrt{D}}{2}\right]$ und $\rho^i\mathfrak{C}_0 = \mathfrak{C}_i = \left[\frac{Q_i}{2}, \frac{P_i+\sqrt{D}}{2}\right]$. Sei weiterhin m minimal, so daß $\mathfrak{C}_m$ reduziert ist.
Es existiert ein $k \leq \log\left|\frac{Q_0}{\sqrt{D}}\right|$, so daß $Q_k < 2\sqrt{D}$ und $Q_j > 2\sqrt{D}$ für alle $j < k$. Nach Korollar 3.20 ist $k \in \{m-2, m-1, m\}$.
$\mathfrak{A}_r$ und $\mathfrak{B}_s$ sind reduziert, daher sind $\mathcal{N}(\mathfrak{A}_r)$ und $\mathcal{N}(\mathfrak{B}_s)$ kleiner als $\sqrt{D}$. Also hat man
$t^2\frac{Q_0}{2} = \mathcal{N}(\mathfrak{A}_r)\mathcal{N}(\mathfrak{B}_s) < D$ und $1 \leq t < \sqrt{D}$.
Zudem gelten folgende Ungleichungen für $1 \leq i \leq k$:

(i) $2 \leq Q_i \leq \frac{Q_{i-1}}{2}$ und $|P_i| \leq \frac{Q_{i-1}}{2}$

(ii) $|\overline{\psi}''_i| = \left|\frac{-P_i-\sqrt{D}}{Q_{i-1}}\right| \leq \frac{|P_i|+\sqrt{D}}{Q_{i-1}} < \frac{1}{2} + \frac{1}{2} = 1$

(iii) $|\overline{\phi}''_i| = \frac{|P_i-\sqrt{D}|}{Q_i} \leq \frac{|P_i|+\sqrt{D}}{Q_{i-1}} < \frac{Q_{i-1}}{2Q_i} + \frac{Q_{i-1}}{2Q_i} = \frac{Q_{i-1}}{Q_i}$

$$\Rightarrow \frac{1}{D} < \frac{Q_k}{Q_0t^2} \leq \frac{Q_k}{Q_0t} \leq \frac{1}{t}\prod_{i=1}^{k}\left|\frac{1}{\overline{\phi}''_i}\right| = \frac{1}{t}|\overline{\theta}''_k| \leq |\overline{\theta}''_k| = \prod_{i=1}^{k}|\overline{\psi}''_i| < 1 < 2\sqrt{D} \quad (12)$$

Damit ist der Fall $k = m$ gezeigt.

[5]Es ist zu beachten, daß $\overline{\theta}''_m$ vom modifizierten KBV erzeugt wird, $\overline{\theta}_r$ und $\overline{\theta}'_s$ durch das gewöhnliche.

Sei nun $k = m - 1$: $\quad \overline{\theta}''_{k+1} = \overline{\theta}''_k \overline{\psi}''_{k+1}$, mit $\overline{\psi}''_{k+1} = \frac{-P_{k+1}-\sqrt{D}}{Q_k}$.
Da $2 \leq Q_k < 2\sqrt{D}$ und $\sqrt{D} \leq |\sqrt{D} - Q_k| < P_k + 1 < \sqrt{D}$, folgt mit Gleichung (12):

$$\tfrac{1}{Q_k} \leq |\overline{\psi}_{k+1}| < \sqrt{D} \;\Rightarrow\; \tfrac{1}{D} < \tfrac{1}{Q_0 t^2} \leq \tfrac{1}{t}|\overline{\theta}''_{k+1}| < \sqrt{D} < 2\sqrt{D}$$

Sei nun $k = m - 2$: $\quad \overline{\theta}''_{k+2} = \overline{\theta}''_k \overline{\psi}''_{k+1} \overline{\psi}''_{k+2}$.
Mit $P_{k+1} = q_{k+1}Q_{k+1} - P_{k+2}$ erhält man:

$$\begin{aligned}|\overline{\phi}''_{k+1}\overline{\phi}''_{k+2}| &= \tfrac{|(P_{k+1}-\sqrt{D})(P_{k+2}-\sqrt{D})|}{Q_{k+1}Q_{k+2}} = \tfrac{|P_{k+1}P_{k+2}+D-(P_{k+1}+P_{k+2})\sqrt{D}|}{Q_{k+1}Q_{k+2}}\\ &= \tfrac{|D-{P_{k+2}}^2+q_{k+1}Q_{k+1}(P_{k+2}-\sqrt{D})|}{Q_{k+1}Q_{k+2}} = \tfrac{|Q_{k+2}+q_{k+1}(P_{k+2}-\sqrt{D})|}{Q_{k+2}} \geq \tfrac{1}{Q_{k+2}} \geq \tfrac{1}{2\sqrt{D}}\end{aligned}$$

$$\begin{aligned}|\overline{\psi}''_{k+1}\overline{\psi}''_{k+2}| &= \tfrac{|(-P_{k+1}-\sqrt{D})(-P_{k+2}-\sqrt{D})|}{Q_k Q_{k+1}} = \tfrac{|D-{P_{k+1}}^2+q_{k+1}Q_{k+1}(P_{k+1}+\sqrt{D})|}{Q_{k+1}Q_{k+2}}\\ &= \tfrac{|Q_k+q_{k+1}(P_{k+1}+\sqrt{D})|}{Q_k} \geq \tfrac{1}{Q_k}\end{aligned}$$

(12)$\Rightarrow \frac{1}{D} < \frac{1}{Q_0 t^2} \leq \frac{1}{t}|\overline{\theta}''_{k+2}| \leq 2\sqrt{D}$
Also erhält man insgesamt: $-\log D < \delta = \log\left|\frac{\overline{\theta}''_m}{t}\right| < \log 2\sqrt{D}$. □

Das hier verwendete, modifizierte Reduktionsverfahren ist sogar etwas besser als das gewöhnliche KBV, das Buchmann und Williams zur Implementation eines Diffie-Hellmann Verfahrens verwendet haben, da Williams und Wunderlich in [WiWu] gezeigt haben, daß dann für δ lediglich die Abschätzung $0 < \delta < 8\log D$ gilt. Mit den Ergebnissen aus Lemma 4.10 benötigt man daher mit dem von mir verwendeten Reduktionsverfahren höchstens $2 + 2\log D$ Schritte des *NACHBAR*-Algorithmus, um aus einem reduzierten Ideal $\mathfrak{A}_k \sim \mathfrak{A}(x)\mathfrak{A}(y)$ das Ideal $\mathfrak{A}(x+y)$ zu berechnen. In der Praxis ist die Anzahl aber meistens kleiner, da die Distanz benachbarter Ideale meist deutlich über der unteren Schranke aus Lemma 4.10(i) liegt. Hierfür gebe ich einen Satz wieder, der in [WiWu] und [Shanks] „Lévy's Law" genannt wird:

Satz 4.12 (Lévy's Gesetz). *Sei ϕ eine Irrationalzahl mit der Kettenbruchentwicklung, $\phi = (q_0, q_1, \ldots, q_{k-1}, \phi_k)$. Dann gilt fast immer*

$$\lim_{k\to\infty} \sqrt[k]{\phi_1\phi_2 \cdot \ldots \cdot \phi_k} = e^{\lambda}, \qquad \textit{für } \lambda = \frac{\pi^2}{12\log 2} \approx 1,1866$$

Das bedeutet, daß benachbarte Ideale im Durchschnitt etwa die Distanz λ haben. Damit gilt also : $d_k \approx k$, $d_r \approx r$, $d_s \approx s$ und insgesamt $d_k \approx r+s \approx k$. Im oben beschriebenen Beispiel ist $k = 7$ und $r = 1$ und $s = 3$.

4.3 Komplexität und Anwendung

In diesem Abschnitt beschreibe ich erst die Komplexität der beschriebenen Arithmetik, um zu untersuchen, ob diese für Anwendungen auf einem Computer geeignet ist. Anschließend beschreibe ich beispielhaft eine solche Anwendung: Das bereits mehrfach erwähnte Diffie-Hellmann Verfahren.

Damit die gerade beschriebene Arithmetik kryptographisch genutzt werden kann, dürfen die einzelnen Rechnungen nicht zu aufwendig sein. Das bedeutet, daß die Anzahl der Rechenschritte höchstens polynomial im Logarithmus der Eingabe sein dürfen, also etwa bei Eingabe einer n-bit Zahl in der Größenordnung von $\mathrm{O}(\log n)$. Ist die Komplexität eines Algorithmus $\mathrm{O}(n)$, so spricht man von exponentieller Komplexität, und ein solcher Algorithmus wird als ungeeignet betrachtet.
Die folgende Tabelle beschreibt die von D. E. Knuth in [Knuth] angegebene Komplexität der grundlegenden Rechenschritte für Eingaben von n Bit Länge, bei Verwendung von Langzahlarithmetik:

Verknüpfung	Komplexität
Addition	$\mathrm{O}(n)$
Multiplikation	$\mathrm{O}(n \log n \log\log n)$
Division	$\mathrm{O}(n \log n \log\log n)$
Erw. Euklidischer Algor.	$\mathrm{O}(n^2 \log n \log\log n)$

Mit diesen Ergebnissen kann man die Komplxität der in dieser Arbeit entwickelten Algorithmen bestimmen, wobei beachtet werden sollte, daß diese nicht auf möglichst schnelle Laufzeit hin optimiert wurden, sondern den theoretischen Hintergrund veranschaulichen sollen.

Für negative Diskriminanten, also $D < 0$, sind *REDUKTION1* und *PRODUKT1* bzw. *QUADRAT* zu untersuchen. In den zwei letzteren ist abgesehen von der Reduktion die Division in den Zeilen (02) und (03) am aufwendigsten. Die Werte a, b und t sind durch $\sqrt{|D|}$, also t^2 durch $|D|$, beschränkt, da die eingegebenen Ideale als reduziert vorausgesetzt wurden. $|D|$ ist eine $\log |D|$-bit Zahl. Für das Multiplizieren zweier Ideale ohne Reduktion erhält man dann eine Komplexität von $\mathrm{O}(\log |D| \log\log |D| \log\log\log |D|)$.

Auch im Reduktionsalgorithmus ist die Division am aufwendigsten: In jedem Schleifendurchlauf wird in Zeile (13) der Wert n berechnet. Nach Seite 32 durchläuft man die Schleife $\mathrm{O}(\log\sqrt{|D|})$ Mal und erhält so für den Algorithmus *REDUKTION1* eine Komplexität von $\mathrm{O}(\log^2|D|\log\log|D|\log\log\log|D|)$. Somit ist dies auch der aufwendigste Rechenschritt in den zwei Multiplikationsalgorithmen, die deswegen von gleicher Komplexität sind.

Ist $D > 0$, so sind die die Algorithmen *REDUKTION2*, *PRODUKT2* und der *NACHBAR*-Algorithmus zu betrachten. Wieder ist das Berechnen des von Null verschieden Wertes q der Matrix T auf der Gegendiagonalen in Zeile (7) bzw. (15) am aufwendigsten. Für das verwendete modifizierte Kettenbruchverfahren benötigt man nach Korollar 3.21 $2 + log(\frac{a}{\sqrt{D}})$ Schleifendurchläufe. Der Wert a ist die Norm des primitives Ideals $\mathfrak{C}$, wenn $\mathfrak{A}_1\mathfrak{A}_2 = (t)\mathfrak{C}$, für zwei primitive Ideale $\mathfrak{A}_1$ und $\mathfrak{A}_2$. Das bedeutet, daß a beschränkt ist durch D, da die Normen reduzierter Ideale im reellquadratischen Zahlkörper beschränkt sind durch $\sqrt{D}$. Also hat auch *REDUKTION2* eine Komplexität von $\mathrm{O}(\log^2 D\log\log D\log\log\log D)$.
Der aufwendigste Rechenschritt im *NACHBAR*-Algorithmus ist wieder die Division von Werten, die alle durch $2\sqrt{D}$ beschränkt sind, ist also von Komplexität $\mathrm{O}(\log\sqrt{D}\log\log\sqrt{D}\log\log\log\sqrt{D})$.
PRODUKT2 ruft *REDUKTION2* einmal und nach Satz 4.11 *NACHBAR* höchstens $\log D$ mal auf. Das bedeutet, daß das Reduzieren und das Bestimmen der Nachbarn, bis man das gesuchte Ideal gefunden hat, ungefähr gleich aufwendig sind. Also ist die Multiplikation, wie im imaginärquadratischen Fall, von gleicher Komplexität wie das Reduzieren.
Zusammenfassend gebe ich die Algorithmen und deren Komplexität in einer Übersicht an:

Verknüpfung	Komplexität
REDUKTION1	$\mathrm{O}(\log^2\|D\|\log\log\|D\|\log\log\log\|D\|)$
PRODUKT1/QUADRAT	$\mathrm{O}(\log^2\|D\|\log\log\|D\|\log\log\log\|D\|)$
REDUKTION2	$\mathrm{O}(\log^2 D\log\log D\log\log\log D)$
NACHBAR	$\mathrm{O}(\log\sqrt{D}\log\log\sqrt{D}\log\log\log\sqrt{D})$
PRODUKT2	$\mathrm{O}(\log^2 D\log\log D\log\log\log D)$

Nun zur Anwendung:

Mit *PRODUKT1* und *PRODUKT2* gebe ich nun einen Algorithmus für schnelles Potenzieren auf der Idealklassengruppe für $D < 0$ bzw. auf dem Zykel der reduzierten Hauptideale für $D > 0$ an, mit dem ein Diffie-Hellmann Verfahren implementiert werden kann. Ist n der Exponent, so benötigt diese Variante des Potenzierens $2 \log n$ Multiplikationen, die hier durch die zwei Produkt-Algorithmen realisiert sind. Insgesamt erhält man für das Berechnen der n-ten Potenz in beiden Fällen eine Komplexität von $\mathrm{O}(\log n \log^2 |D| \log\log |D| \log\log\log |D|)$.
Die Zeilen, die nur für imaginärquadratische Zahlkörper gelten, sind mit *im* gekennzeichnet, analog die, die nur für reellquadratische Zahlkörper gelten, mit *re*. Wie ein solches Diffie-Hellmann Verfahren konkret aussieht veranschauliche ich anschließend an einem Beispiel.

Algorithmus: *POTENZIEREN*

Ideale

Eingabe $a, b, D, (n_0, n_1, \ldots, n_{k-1})$, für $D < 0$,
$a, b, d_x, D, (n_0, n_1, \ldots, n_{k-1})$, für $D > 0$,

so daß $\mathfrak{A} = \left[a, \frac{-b+\sqrt{D}}{2}\right]$ reduziert ist, $n = \sum_{i=0}^{k-1} n_i 2^i$,
und falls $D > 0$:
$\mathfrak{A} = \mathfrak{A}(x)$, $d_x = d(x)$, für ein $x \in \mathbb{R}$

Ausgabe a', b', sowie d_{nx} für $D > 0$

so daß $\mathfrak{A}' = \left[a', \frac{-b'+\sqrt{D}}{2}\right]$ reduziert ist, und für
$D < 0$: $\mathfrak{A}' \sim \mathfrak{A}^n$
$D > 0$: $\mathfrak{A}' = \mathfrak{A}(nx)$

Programm

(01)	$a' \longleftarrow 1$
(02)	$b' \longleftarrow D \mod 2$
(03re)	$d_{nx} \longleftarrow 1$
(04)	$i \longleftarrow k-1$
(05)	solange $i > 0$
(06)	Beginn der Schleife
(07im)	$(a', b') \longleftarrow QUADRAT(a', b', D)$
(07re)	$(a', b', d_{nx}) \longleftarrow PRODUKT2(a', b', a', b', d_{nx}, d_{nx}, D)$
(08)	falls $n_i = 1$, dann
(09im)	$(a', b', s) \longleftarrow PRODUKT(a', b', a, b, D)$
(09re)	$(a', b', s) \longleftarrow PRODUKT2(a', b', a, b, d_{nx}, d_x, D)$
(10)	$i \longleftarrow i-1$
(11)	Ende der Schleife
(12im)	Übergebe (a', b')
(12re)	Übergebe (a', b', d_{nx})

Nun zunächst ein Beispiel für ein Diffie-Hellmann Verfahren in der Idealklassengruppe eines imaginärquadratischen Zahlkörpers:

Seien `A` und `B` zwei Kommunikationspartner, die sich über einen öffentlichen Kanal, z.B. einer Telefonleitung, auf einen geheimen Schlüssel einigen wollen. Das Verfahren funktioniert wie folgt:

- $\mathtt{A}$ und $\mathtt{B}$ einigen sich öffentlich auf eine Diskriminante D, um die Idealklassengruppe des zugehörigen Zahlkörpers als Gruppe zu verwenden. Bei geeigneter Wahl, siehe dazu auch das nächste Kapitel, ist die Wahrscheinlichkeit sehr gering, in der Klassengruppe zufällig ein Element kleiner Ordnung zu wählen. $\mathtt{A}$ und $\mathtt{B}$ einigen sich beispielsweise auf $D = -4242424243$, dann ist die Klassenzahl $h_{\mathbb{K}} = 8661 = 3 \cdot 2887$ für $\mathbb{K} = \mathbb{Q}(\sqrt{D})$. Um also ein Element kleiner Ordnung zufällig zu wählen, müßte man in der 2887-elementigen Untergruppe genau das neutrale Element nehmen, bei einer offensichtlichen Wahrscheinlichkeit von 1/2887.
  Weiterhin einigen sich $\mathtt{A}$ und $\mathtt{B}$ zufällig auf ein zufälliges Ideal, z.B. $\mathfrak{A} = [18229, \frac{12511+\sqrt{-4242424243}}{2}]$. Dieses ist sogar ein Erzeugendes der Klassengruppe, da $\mathfrak{A}^3 = [30547, \frac{-3963+\sqrt{-4242424243}}{2}] \neq \mathcal{O}_{\mathbb{K}}$ und $\mathfrak{A}^{2887} = [9001, \frac{-2087+\sqrt{-4242424243}}{2}] \neq \mathcal{O}_{\mathbb{K}}$.

- Jetzt wählt $\mathtt{A}$ einen geheimen Exponenten, z.B. $a = 3576$, berechnet $\mathfrak{A}^a = [26111, \frac{-24557+\sqrt{-4242424243}}{2}]$ und schickt das Ergebnis an $\mathtt{B}$. Analog wählt $\mathtt{B}$ einen geheimen Exponenten, etwa $b = 45681$ und schickt $\mathtt{A}$ das Element $\mathfrak{A}^b = [25699, \frac{-5541+\sqrt{-4242424243}}{2}]$.

- Nun kann $\mathtt{A}$ $(\mathfrak{A}^b)^a$ und $\mathtt{B}$ $(\mathfrak{A}^a)^b$ berechnen.

- Es ist $\mathfrak{A}_s = (\mathfrak{A}^b)^a = (\mathfrak{A}^a)^b = [21467, \frac{12755+\sqrt{-4242424243}}{2}]$. Als Schlüssel ließe sich beispielsweise die Norm oder die Spur des Ideals $\mathfrak{A}_s$ verwenden.

Für einen sicheren Schlüssel müßte man allerdings die Diskriminante deutlich größer wählen, etwa mit zweihundert Dezimalstellen, da es dann nicht mehr möglich ist, in angemessener Zeit die Klassenzahl zu berechnen, wovon die Sicherheit des Verfahrens in erster Linie abhängt.
Für dieses Beispiel war es mir wichtig auch die Klassenzahl berechnen zu können, um die Struktur der Klassengruppe zu kennen. Das Programm, daß ich zu diesem Zweck im *aribas*-Code von Forster [Forster] geschrieben habe, ist jedoch nur für Diskriminanten bis zu einer Größe von zehn Dezimalstellen sinnvoll zu verwenden, was die Auswahl der Diskriminante in diesem Beispiel entsprechend einschränkte.

Beschreibung des Diffie-Hellmann Verfahrens für $D > 0$:

Meine Implementation der „$*$“-Multiplikation, ebenfalls in *aribas*, liefert leider zu $\mathfrak{A}(x)^n$ nicht genau das Ideal $\mathfrak{A}(nx)$, sondern in der Regel lediglich ein Ideal, das im Zykel *dicht* am eigentlichen Ergebnis liegt. Dies ist bedingt durch den Rundungsfehler, der beim Rechnen mit den Abständen auftritt. Zwar habe ich den von Scheidler, Buchmann und Williams in [SchBuWi] beschriebenen Algorithmus verwendet, in dem die Autoren eine Sicherheitskonstante eingeführt haben, um dieses Problem zu umgehen, jedoch waren die Ergebnisse letzten Endes unbefriedigend. Aus diesem Grund beschreibe ich an dieser Stelle lediglich das Verfahren, ohne ein konkretes Beispiel vorzustellen.

- `A` und `B` einigen sich öffentlich auf eine Diskriminante D, ein Hauptideal $\mathfrak{A}(x)$ und die Distanz $d(x)$ für eine reelle Zahl x. Letzteres läßt sich leicht realisieren, indem man das KBV auf das Einsideal zwei oder drei Mal anwendet. Dann ist z.B. $\mathfrak{A}(x) = \mathfrak{A}_2$. Weiterhin setzt man $d(x) = 0$, also $x = \overline{\theta}_2$. Man wählt sich also das Ideal aus und nicht die reelle Zahl x.

- Jetzt wählt `A` einen geheimen Exponenten a, berechnet mit *PRODUKT2* $\mathfrak{A}(ax)$ und $d(ax)$ und schickt beide Werte an `B`. Analog wählt `B` einen geheimen Exponenten b und schickt $\mathfrak{A}(bx)$ und $d(bx)$ an `A`.

- Nun kann `A` mit Hilfe von a und $d(bx)$ das Ideal $\mathfrak{A}(abx)$ und den Abstand $d(abx)$ berechnen und `B` mit Hilfe von b und $d(ax)$ das Ideal $\mathfrak{A}(bax)$ und den Abstand $d(bax)$. Hier treten in der Implementation die größten Schwierigkeiten auf, da die Abstände $d(ax)$ und $d(bx)$ lediglich gerundet übergeben werden können, so daß bei der zweiten Anwendung des Potenzier-Algorithmus bereits die Ausgangswerte nicht exakt sind. Rechnete man mit exakten Werten, so erhielten `A` und `B` die gleichen Ergebnisse, da „$*$“ assoziativ ist.

- Scheidler, Buchmann und Williams haben in [SchBuWi] beschrieben, wie man sich dennoch auf ein eindeutiges Ideal einigen kann, welches entweder $\mathfrak{A}(abx)$ oder $\mathfrak{A}_+(abx)$ ist. Dieses ist dann der geheime Schlüssel.

5 Das Diskrete Logarithmus Problem (DLP)

Dieses Kapitel gliedert sich in zwei Teile. Im ersten wird erst das DLP für die Idealklassengruppe in imaginärquadratischen Zahlkörpern einerseits und für die Menge der reduzierten Hauptideale in reellquadratischen Zahlkörpern andererseits erklärt und gezeigt, daß diese für große Diskriminanten nicht in angemessener Zeit zu lösen sind. Das bedeutet, daß z.B. die gerade beschriebenen Diffie-Hellmann Verfahren vom kryptographischen Standpunkt her sicher sind.
Im zweiten Teil stelle ich die zwei zur Zeit besten Verfahren zur Lösung des Diskreten Logarithmus Problems in der Idealklassengrupe für $D < 0$ vor. Das zweite ist das mächtigere und eignet sich für Diskriminanten bis zu $|D| \leq 10^{50}$. Mit einer Variation dieses Verfahrens ist es möglich, auch das DLP im reellquadratischen Fall für ähnlich große Diskriminanten zu lösen. Eine Beschreibung dessen ginge aber über den Rahmen dieser Arbeit hinaus, so daß ich hier auf die Beschreibungen des Verfahrens in [BuWi90] von Buchmann und Williams und [Cohen, Kap. 5] von Cohen verweise.

Verwendet man zur Multiplikation in $\mathcal{C}l_{\mathbb{K}}$ den Algorithmus *PRODUKT1*, so beschreibt die Multiplikation von reduzierten Idealen die Arithmetik auf den Klassen bereits vollständig. Deshalb unterscheide ich im weiteren im imaginärquadratischen Fall nicht mehr zwischen reduzierten Idealen und Idealklassen.
Dann lautet das DLP in der Idealklassengruppe eines imaginärquadratischen Zahlkörpers:
Sind $\mathfrak{A}$ und $\mathfrak{B}$ reduzierte Ideale in $\mathcal{O}_{\mathbb{K}}$, so daß $\mathfrak{A}^n = \mathfrak{B}$, dann bestimme n.

Das DLP auf dem Zykel der reduzierten Hauptideale eines reellquadratischen Zahlkörpers lautet:
Sind $\mathfrak{A}(x)$ und $d(x)$ gegeben, bestimme $\overline{\theta}_k$, so daß $\mathfrak{A}(x) = \mathfrak{A}_k = (\overline{\theta}_k)$.
Denn sind $\mathfrak{A}(x)$ und $d(x)$, sowie $\mathfrak{A}(nx)$ und $d(nx)$ gegeben, und ist man in der Lage, $\overline{\theta}_k$ und $\overline{\theta}_l$ zu berechnen, so daß $\mathfrak{A}(x) = (\overline{\theta}_k)$ und $\mathfrak{A}(nx) = (\overline{\theta}_l)$, dann erhält man den Wert n durch folgende Gleichungen:

$$d(x) = \log|\overline{\theta}_k| - x\ , \quad d(nx) = \log|\overline{\theta}_l| - nx \ \Rightarrow\ n = \frac{\log|\overline{\theta}_l| - d(nx)}{\log|\overline{\theta}_k| - d(x)}$$

Sei zunächst $D < 0$:

Das zufällig gewählte Ideal $\mathfrak{A}$, darf nicht von zu geringer Ordnung sein, da sonst der gesuchte Exponent n durch Ausprobieren leicht zu berechnen ist. Aus diesem Grund muß die Ordnung der Klassengruppe groß sein. Buchmann und Williams geben in [BuWi88] für $h_{\mathbb{K}}$ eine untere Schranke an:

$$|h_{\mathbb{K}}| > |D|^{\frac{1}{2}-\epsilon}$$

für alle $\epsilon > 0$, wenn $|D|$ ausreichend groß ist. Es ist also eine Gruppenordnung von etwa $\sqrt{|D|}$ zu erwarten. Damit auch die Elemente der Klassengruppe eine große Ordnung haben, muß man die Teiler von $h_{\mathbb{K}}$ untersuchen.

Dazu sei zur Diskriminante D die Klassenzahl $h_{\mathbb{K}} = 2^r u$, mit $r \geq 0$ und u ungerade. Cohen und Lenstra haben in [CoLe84b] einige heuristische Ergebnisse über die Klassenzahl quadratischer Zahlkörper beschrieben. Danach beträgt die Wahrscheinlichkeit $97,7575\%$, daß der ungerade Anteil der Klassengruppe zyklisch ist.
Ist G eine zyklische Gruppe der Ordunung n, so ist bekannt, daß in jeder zyklischen Untergruppe von G der Ordnung d, $\varphi(d)$ Erzeugende[6] existieren. Damit die Idealklassengruppe möglichst viele Elemente großer Ordnung hat, ist es also wichtig, daß die Klassenzahl einen möglichst großen und sonst verhältnismäßig kleine Primteiler besitzt. Denn um dann zufällig ein Element kleiner Ordnung zu wählen, hieße, daß man in der zyklischen Untergruppe von der Ordnung des großen Primteilers p, das neutrale Element genommen hat. Die Wahrscheinlichkeit, daß das passiert, ist aber $\frac{1}{p}$.
In [Knuth, Seite 367 ff.] werden die durch die folgenden Gleichungen gegebenen heuristischen Funktionen untersucht, um Aussagen über die Größe von Primteilern beliebiger ganzer Zahlen machen zu können:

$$\begin{aligned} F(\alpha) &= \int_0^\alpha F\left(\tfrac{t}{1-t}\right)\tfrac{dt}{t}\ , \quad \text{für } 0 \leq \alpha \leq 1 \text{ und } F(\alpha) = 1 \text{ sonst.} \\ G(\beta) &= \int_0^\beta \left(G\left(\tfrac{t}{1-t}\right) - F\left(\tfrac{t}{1-t}\right)\right)\tfrac{dt}{t}\ , \quad \text{für } 0 \leq \beta \leq \tfrac{1}{2} \text{ und } G(\beta) = 1 \text{ für} \beta > \tfrac{1}{2}. \end{aligned}$$

Es ist $F(\alpha) = 1 - \int_\alpha^1 F\left(\frac{t}{1-t}\right)\frac{dt}{t} = 1 + \log\alpha$, für $\frac{1}{2} \leq \alpha < 1$, man vergleiche [Knuth].
Die Wahrscheinlichkeit, daß der größte Primteiler einer zufällig gewählten Zahl N zwischen 1 und einer Schranke x größer ist als x^α, beträgt für $x \to \infty$: $1 - F(\alpha) = \log\frac{1}{\alpha}$.
Die Wahrscheinlichkeit, daß der zweitgrößte Primteiler von N kleiner ist als x^β beträgt für $x \to \infty$: $G(\beta)$.
Das heißt zum Beispiel, wenn der ungerade Anteil u der Klassenzahl 100 Dezimalstellen besitzt, hat der größte Primteiler von u mit einer Wahrscheinlichkeit von $\frac{1}{2}$ mehr als 60 Dezimalstellen und mit gleicher Wahrscheinlichkeit der

[6] Mit $\varphi(x)$ ist die Eulersche Phi-Funktion gemeint.

zweitgrößte Primteiler weniger als 22 Dezimalstellen. Vergleiche dazu auch die Tabelle [Knuth, Seite 368].
Das bedeutet, daß die Wahrscheinlichkeit, ein Element kleiner Ordnung zufällig zu wählen, sehr klein ist, wenn die Klassenzahl erstens groß ist und zweitens nur einen kleinen geraden Anteil enthält.
Die Ordnung der 2-Sylow-Untergruppe von $\mathcal{C}l_{\mathbb{K}}$ kann man durch die Wahl von D beschränken.
Es ist bekannt, siehe u.a. [Nark], daß $2^{n-1}|h_{\mathbb{K}}$, falls D Produkt von n verschiedenen Primteilern ist, d.h. $r \geq n-1$. Bei geeigneter Wahl von D läßt sich für r eine obere Schranke angeben, vergleiche dazu u.a. [Nark]. So ist für $D \in \{-4, -8, -p \mid p \text{ prim}, p \equiv 3 \ (4)\}$ die Klassenzahl ungerade, also $r = 0$. Ist $D = -p_1 p_2$, für zwei ungerade Primzahlen p_1 und p_2, so daß $\left(\frac{p_2}{p_1}\right) \neq 1$, so gilt: $4 \nmid h_{\mathbb{K}}$.

Mit einer solchen Wahl von D ist die Wahrscheinlichkeit, zufällig ein Ideal kleiner Ordnung zu wählen, klein. Das bedeutet, daß das DLP dann nicht auf triviale Weise zu lösen ist.

Sei nun $D > 0$:

Ließe sich durch wiederholtes Anwenden des Nachbaralgorithmus schnell das Einsideal finden, wäre das DLP gelöst, da die Distanzen zwischen den Nachbarn mitberechnet werden. Deshalb ist es notwendig, daß die Länge des Zykels der reduzierten Hauptideale möglichst groß ist.
Sei l die Länge dieses Zykels und $\mathtt{R} = \log|\overline{\theta}_l|$ der Regulator, so geben Buchmann und Williams in [BuWi89] folgende untere Schranke für die Periodenlänge an:

$$l \geq \tfrac{1}{\log D}\mathtt{R}\,.$$

Es läßt sich aber auch eine obere Schranke für l herleiten: Nach Lemma 3.16 (ii) und Gleichung (8) ist $Q_0|\overline{\theta}_n| = G_{n-1} + v_{n-1}\sqrt{D}$. Sei F_n das n-teElement in der Fibonacci-Folge, so ist $F_n \leq v_n$, für alle n. Haben weiterhin die reduzierten Ideale des Hauptidealzykels die Form $\left[\frac{Q_n}{2}, \frac{P_n+\sqrt{D}}{2}\right]$, $P_n > 0$ und $Q_n \geq 2$, dann folgt aus Gleichung (11) $G_{n-1} \geq F_{n-1} + 2F_{n-2}$.
Damit erhält man:

$$\begin{aligned}
Q_0|\overline{\theta}_n| \;&\geq\; F_{n-1} + 2F_{n-2} + F_{n-1}\sqrt{D} \;=\; F_n + F_{n-2} + F_{n-1}\sqrt{D} \\
&=\; 2F_n + F_{n-1}(\sqrt{D}-1) \;=\; F_{n+1} + F_n + F_{n-1}(\sqrt{D}-2) \\
&>\; F_{n+2}\,, \qquad \text{für } D > 4\,.
\end{aligned}$$

Außerdem gilt $F_{n+2} > \tau^n$ für $\tau = \frac{1+\sqrt{5}}{2}$ und insgesamt $Q_0|\overline{\theta}_n| > \tau^n$.
Setzt man $n = l$ ein, so ist $|\overline{\theta}_l|$ die Grundeinheit und

$$\log Q_0 + \mathtt{R} > l \cdot \log \tau \,.$$

Mit dieser oberen Schranke für l hat man insgesamt:

$$\frac{1}{\log D}\mathtt{R} \leq l \leq \frac{\log Q_0 + \mathtt{R}}{\log \tau} \,.$$

Die Periodenlänge hängt also direkt von der Größe des Regulators ab. Für diesen geben Buchmann und Williams in [BuWi90], unter Annahme der Erweiterten Riemann Hypothese, die Grenzen

$$\mathtt{R} < \sqrt{D}(\log \sqrt{D} + 1) \qquad \text{und} \qquad h_{\mathbb{K}}\mathtt{R} \gg D^{\frac{1}{2}-\epsilon}$$

für beliebig kleines $\epsilon > 0$ an.
Damit ist bei kleiner Klassenzahl eine Periodenlänge $l \approx \sqrt{D}$ zu erwarten. Ist die Diskriminante eine Primzahl, so geben die heuristischen Ergebnisse von Cohen und Lenstra [CoLe84b] Wahrscheinlichkeiten an, daß die Klassenzahl einen bestimmten Wert annimmt. Diese sind $75,446\%$ für $h_{\mathbb{K}} = 1$, $12,574\%$ für $h_{\mathbb{K}} = 3$ und $3,377\%$ für $h_{\mathbb{K}} = 5$.
Für diese Diskriminanten ist das DLP also auch nicht auf triviale Weise zu lösen.

Es ist nun denkbar, daß es andere Verfahren gibt, mit denen die oben beschriebenen Diskreten Logarithmus Probleme schnell gelöst also Anwendungen wie das Diffie-Hellmann Verfahren attackiert werden können. Dies ist jedoch sehr unwahrscheinlich, denn man wäre dann in der Lage, schnell zu faktorisieren, wie man im folgenden Abschnitt sehen wird.

5.1 Bezug zum Faktorisierungsproblem

Buchmann und Williams haben in [BuWi88] und [BuWi90] gezeigt, daß man in der Lage ist, in polynomialer Zeit die Diskriminante zu faktorisieren, wenn man ein Verfahren findet, um eins dieser zwei DLP in polynomialer Zeit zu lösen.

Betrachte man wieder den imaginärquadratischen Fall zuerst. Sei $D = -pq$ bzw. $\frac{D}{4} = -pq$, mit $p, q > 1$, eine echte Zerlegung von D. Es teilt also 2 die Klassenzahl. Das bedeutet, es existiert eine Idealklasse der Ordnung 2.

Eine solche Klasse wird von einem *ambigen*[7] reduzierten Ideal $\mathfrak{A} = \left[a, \frac{-b+\sqrt{D}}{2}\right]$ repräsentiert. Nach [Forster, S. 264] gilt für ambige reduzierte Ideale:

1. $a = b \quad \Rightarrow \quad D = a(a - 4c)$,
2. $b = 0 \quad \Rightarrow \quad D = -4ac$ oder
3. $a = c \quad \Rightarrow \quad D = (b - 2a)(b + 2a)$,

und man erhält die jeweils angegebene, nach [Forster] echte Zerlegung von D.
Kann man das DLP lösen, so ist man in der Lage, die Ordnung eines Ideals, nämlich durch $\mathfrak{A}^x = (1)$, zu berechnen. Um dann ein ambiges reduziertes Ideal zu konstruieren, suche man ein Ideal $\mathfrak{B}$ mit gerader Ordnung m und berechne das reduzierte Ideal $\mathfrak{A} = \mathfrak{B}^{\frac{m}{2}}$. Diese Ideal $\mathfrak{A}$ ist dann ambig und gibt eine der oben angegebenen echten Zerlegungen von D.
Ein Ideal gerader Ordnung findet man schnell durch Probieren, da nach [BuWi88] jedes zweite Element der Klassengruppe von gerader Ordnung ist, wenn die Diskriminante nicht prim ist.

Für den Fall $D > 0$, sei $f : x \mapsto \mathfrak{A}(x)$. Eine Umkehrfunktion f^* von f, die zu einem Ideal $\mathfrak{A}$ die ganze Zahl x berechnet, so daß $|d(\mathfrak{A}, (1)) - x|$ minimal ist, wäre eine Lösung des DLP. Sei l, wie bisher, die Länge des Zykels der Hauptideale, $\mathtt{R} = \log|\overline{\theta}_l|$ der Regulator und haben die Hauptideale die Gestalt $\mathfrak{A}_i = \left[\frac{Q_i}{2}, \frac{P_i+\sqrt{D}}{2}\right]$ und sei $\mathcal{O}_{\mathbb{K}} = \mathfrak{A}_0$, so folgt aus [SteWi88b, Thm. 2.1], da $\mathfrak{A}_0$ ambig ist, daß $Q_{l-1} = Q_1$ und $P_l = P_1$. Das bedeutet, daß $\mathfrak{A}_{l-1} = \left[\frac{Q_1}{2}, \frac{P_2+\sqrt{D}}{2}\right]$ und $\psi_l = \frac{-P_1+\sqrt{D}}{Q_0}$.
Da $\mathfrak{A}_l = \mathfrak{A}_0 = \mathfrak{A}_{l-1}(-\overline{\psi}_l) = (\overline{\theta}_l)$, läßt sich eine Näherung R^* des Regulators $\mathtt{R}$berechnen:

$$R^* = f^*(\left[\tfrac{Q_1}{2}, \tfrac{P_2+\sqrt{D}}{2}\right]) + \log|\tfrac{P_1+\sqrt{D}}{Q_0}| \approx \mathtt{R}\,.$$

Berechnet man nun das Ideal $\mathfrak{B} = f(\frac{R^*}{2})$, so ist nach [BuWi90] in der Nähe von $\mathfrak{B}$ mit großer Wahrscheinlichkeit ein Ideal $\mathfrak{J}$ mit $\mathfrak{J}^2 = (\mathcal{N}(\mathfrak{J}))$ und $\mathcal{N}(\mathfrak{J})|D$. Wiederholt man dies für Diskriminanten pD mit kleinen Primzahlen p, so findet man nach [Schoof], unter der Annahme Varianten der Riemannschen Vermutung, nach nicht mehr als $O(\log^2 D)$ Versuchen einen echten Teiler von D.

[7]Ein Ideal $\mathfrak{A}$ heißt ambig, wenn $\mathfrak{A} \sim \overline{\mathfrak{A}}$

Nun werden die zwei Verfahren zur Lösung des DLP in imaginärquadratischen Zahlkörpern beschrieben. Das erste ist die sogenannte *Baby-step–Giant-step* Methode von Daniel Shanks, die u.a. in [Schoof] beschrieben wird.

5.2 Das Baby-step–Giant-step Verfahren

Sei $D < 0$, $\mathfrak{A}$ und $\mathfrak{B}$ reduzierte Ideale und $\mathfrak{A}^x = \mathfrak{B}$ für ein $x \in \mathbb{Z}$. Für eine Diskriminante von großem Absolutbetrag ist zu erwarten, daß $h_{\mathbb{K}} \approx \sqrt{|D|}$. Man setze daher $q = \lfloor \sqrt[4]{|D|} \rfloor$ und erhält für den gesuchten Exponenten x folgende Zerlegung:

$$x = qk - r\,, \qquad \text{für } 0 \leq r < q$$

sowie aus $\mathfrak{A}^x = \mathfrak{B}$ die Gleichung $\mathfrak{A}^{qk} = \mathfrak{B}\mathfrak{A}^r$.
Das Verfahren gliedert sich nun in zwei Schritte:

Erstens, der *Baby-step*: Man berechnet das Ideal $\mathfrak{A}^q$ und die Menge $\mathtt{B} = \{\mathfrak{B}\mathfrak{A}^r \mid 0 \leq r \leq q-1\}$. Gegebenenfalls sortiert man die Ideale nach der Norm, merkt sich aber zu jedem Ideal den Exponenten r.
Zweitens, der *Giant-step*: Man bildet sukzessive die Potenzen $\mathfrak{A}^{qk}$, für $k = 1, 2, \ldots$, und vergleicht diese mit den Elementen in $\mathtt{B}$.

Findet man einen Exponenten k_0, so daß $\mathfrak{A}^{qk_0} = \mathfrak{B}\mathfrak{A}^{r_0} \in \mathtt{B}$ für ein $r_0 < q$, so ist der gesuchte Wert $x = qk_0 - r_0$.
Da $h_{\mathbb{K}} \approx \sqrt{|D|}$, ist zu erwarten, daß k_0 von gleicher Größenordnung ist wie q. Das bedeutet, daß dieses Verfahren etwa $O(\sqrt[4]{|D|})$ Idealmultiplikationen und Reduktionen sowie für $\mathtt{B}$ ebensoviel Speicherplatz benötigt.
Es ist daher nur für Diskriminanten von relativ kleinem Absolutbetrag geeignet.

Vielversprechender ist eine Variante der *Index-Calculus* Methode von Hafner und McCurley, die u.a. von Buchmann und Düllmann [BuDü] implementiert wurde [BuDü] und von Komplexität $L(|D|, \frac{1}{2})$ ist, mit $L(x, \alpha) = (e^{\sqrt{\log x \log\log x}})^{\alpha + o(1)}$.

5.3 Eine Variante der Index-Calculus Methode

Dieses Verfahren läßt sich sowohl auf imaginär-, als auch auf reellquadratische Zahlkörper anwenden, ist aber im zweiten Fall um einige Ideen zu ergänzen. Ich beschreibe daher nur das Verfahren für den Fall $D < 0$.

Die Idee zu diesem Verfahren ist folgende:
Sei

$$\mathcal{C}l_{\mathbb{K}} = (\mathfrak{C}_1) \times (\mathfrak{C}_2) \times \ldots \times (\mathfrak{C}_l)\,, \quad l \geq 1$$

mit $\mathrm{ord}(\mathfrak{C}_i) = g_i \geq 1$, d.h. $h_{\mathbb{K}} = \prod g_i$.
Um das Diskrete Logarithmusproblem $\mathfrak{A}^x = \mathfrak{B}$ für zwei Ideale $\mathfrak{A}$ und $\mathfrak{B}$ zu lösen, bestimme man die Darstellungen

$$\mathfrak{A} = \prod_{i=1}^{l} \mathfrak{C}_i^{a_i} \quad \text{und } \mathfrak{B} = \prod_{i=1}^{l} \mathfrak{C}_i^{b_i} = \prod_{i=1}^{l} \mathfrak{C}_i^{x a_i} \tag{13}$$

und berechne, unter Verwendung des Chinesischen Restsatzes, den Wert x aus den Kongruenzen $x a_i \equiv b_i \mod g_i$.

Die Schwierigkeit besteht dann darin,

1. Erzeugende $\mathfrak{C}_i$ und deren Ordnung g_i zu finden und
2. die Darstellung von $\mathfrak{A}$ und $\mathfrak{B}$ als Produkt der $\mathfrak{C}_i$ zu bestimmen.

Zur Lösung des ersten Problems betrachte man erst ein Ergebnis aus der Zerlegungstheorie, siehe [Koch, Seite 183].

Lemma 5.1. *Sei D eine fundamentale Diskriminante und $p \in \mathbb{Z}$ prim, $p \neq 2$, falls $D \not\equiv 1$ (8).*
Es existieren genau dann Primdideale $\mathfrak{p}_1$ und $\mathfrak{p}_2$ in $\mathcal{O}_{\mathbb{K}}$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$, so daß $(p) = \mathfrak{p}_1\mathfrak{p}_2$, wenn $\left(\frac{D}{p}\right) = 1$.
Dabei gilt $\mathfrak{p}_2 = \overline{\mathfrak{p}}_1$ und $\mathcal{N}(\mathfrak{p}_i) = p$, für $i = 1, 2$.

Zu p mit $\left(\frac{D}{p}\right) = 1$ existieren Zahlen b_p, so daß $D \equiv b_p^2 \mod p$. Dann ist $[p, \frac{-b_p+\sqrt{D}}{2}]$ ein Primideal in $\mathcal{O}_{\mathbb{K}}$ von Norm p in kanonischer Darstellung.
Dies nutzen Buchmann und Williams in [BuWi90] aus, um mit dem folgenden Ergebnis von Lagarias, Montgomery und Odlyzko [LaMoOd] ein Erzeugendensystem der Idealklassengruppe zu gewinnen:
Unter der Annahme der Verallgemeinerten Riemannschen Vermutung existiert eine Konstante C, so daß für $P = \{p \text{ prim} \mid \left(\frac{D}{p}\right) = 1 \text{ und } p \leq C \log^2 |D|\}$ das System $B_P = \{\mathfrak{p} \mid \mathcal{N}(\mathfrak{p}) = p \in P\}$ die Klassengruppe erzeugt. Eric Bach hat bewiesen [Bach], daß $C = 6$ für die Mengen P und B_P eine geeignete

Konstante ist. In der Praxis reicht es aber, mit Werten für C zwischen $\frac{1}{2}$ und 2 zu arbeiten [Cohen], damit die Faktorbasis B_P die Idealklassengruppe erzeugt.
Sei $k = ordP$, dann erhält man einen surjektiven Gruppenhomomorphismus

$$\begin{aligned} \phi: \ \mathbb{Z}^k &\longrightarrow \mathcal{C}l_{\mathbb{K}} \\ x = (x_1, \ldots, x_k) &\longmapsto \prod_{i=1}^{k} \mathfrak{p}_i^{x_i} . \end{aligned}$$

Sei $L = Kern\phi$, dann gilt nach dem Homomorphiesatz

$$\mathbb{Z}^k / L \simeq \mathcal{C}l_{\mathbb{K}} \text{ und } [\mathbb{Z}^k : L] = h_{\mathbb{K}} .$$

B_P ist aber als Erzeugendensystem zu groß, um effizient Diskrete Logarithmen zu berechnen. Mit Hilfe einiger Begriffe und Aussagen aus der Modultheorie, die ich hier ohne Beweis angebe und die u.a. in [Cohen, S. 74 ff.] zu finden sind, läßt sich aus B_P ein minimales Erzeugendensystem gewinnen.

Definition 5.2. Sei $M = ((m_{ij}))$ eine $n \times n$-Matrix mit ganzzahligen Einträgen. M ist eine Matrix in *Smith Normal Form*, kurz SNF, wenn sie folgende Eigenschaften besitzt:

1. M ist eine Diagonalmatrix, d.h. $m_{ij} = 0$ genau dann, wenn $i \neq j$.

2. Alle Diagonalelemente sind ungleich Null, und es gilt: $m_{jj} | m_{ii}$ für alle $j \geq i$.

Satz 5.3. *Sei $A \in M(n, \mathbb{Z})$, mit $\det A \neq 0$, dann existiert eine eindeutig bestimmte Matrix B in SNF, kurz $B = SNF(A)$, und Matrizen $U, V \in GL_n(\mathbb{Z})$, so daß*

$$B = VAU .$$

Korollar 5.4. *Sei L ein freier $\mathbb{Z}$-Modul vom Rang n, L' ein Untermodul von L, von demselben Rang, dann existieren eindeutig bestimmte ganze Zahlen $d_1, \ldots, d_n$, so daß gilt:*

1. *$d_{i+1} | d_i$, für alle $i < n$.*

2. *Es existiert eine $\mathbb{Z}$-Basis $\{b_1, \ldots, b_n\}$ von L, so daß $\{d_1 b_1, \ldots, d_n b_n\}$ eine $\mathbb{Z}$-Basis von L' ist und*

3. $[L:L'] = \prod_{i=1}^{n} d_i$ *und*

$$L/L' \simeq \bigoplus_{1\le i\le n} \Big(\mathbb{Z}/d_i\mathbb{Z}\Big) \text{ \textit{als} } \mathbb{Z}\text{-\textit{Moduln}.}$$

Jetzt kann man Basen von Untergittern des Kerns L berechnen:
Dazu wähle man zufällige Exponenten $x = (x_1, \ldots, x_k) \in \mathbb{Z}^k$, so daß $\mathcal{N}(\mathfrak{I}) > \sqrt{\frac{|D|}{3}}$ für

$$\mathfrak{I} = \prod_{i=1}^{k} \mathfrak{p}_i^{x_i} .$$

Dann reduziere man $\mathfrak{I}$ und erhält $\mathfrak{I}' \sim \mathfrak{I}$, mit $\mathfrak{I}' \neq \mathfrak{I}$, wegen der Bedingung an die Norm.
Nun versucht man, auf $\mathcal{N}(\mathfrak{I}')$ über P, z.B. durch *trial division*, zu faktorisieren. Wenn dies gelingt, erhält man folgende Faktorisierung von $\mathfrak{I}$ über B_P:

$$\mathfrak{I}' = \prod_{i=1}^{k} \mathfrak{p}_i^{y_i} \quad \text{und} \quad \prod_{i=1}^{k} \mathfrak{p}_i^{x_i - y_i} \sim (1) .$$

Das bedeutet, daß $z = x - y = (x_1 - y_1, \ldots, x_k - y_k)$ im Kern von ϕ liegt. Diesen Vorgang wiederholt man, bis man k linear unabhängige Vektoren z_j, $1 \le j \le k$, gefunden hat. Diese Vektoren spannen ein Untergitter von $L = Kern\, \phi$ auf. Ist $h' = [\mathbb{Z}^k : L']$, so ist daher $h' = h_{\mathbb{K}}[\mathbb{Z}^k : L]$, also ist h' ein Vielfaches der Klassenzahl.
Unter Annahme der Verallgemeinerten Riemannschen Vermutung läßt sich mit der analytischen Formel zur Berechnung der Klassenzahl eine Näherung h_1 von $h_{\mathbb{K}}$, für die $h_{\mathbb{K}} \le h_1 < 2h_{\mathbb{K}}$ gilt, berechnen. Dies ist die Eigenschaft, die es einem überhaupt nur ermöglicht, ein Index-Calculus Verfahren auf dieses DLP anzuwenden, denn durch den Vergleich von h_1 und h' besitzt man ein Kriterium, ob das Untergitter L' bereits der gesuchte Kern L ist:

Sei $B = (z_j)$ die Matrix, deren Spalten von den Vektoren z_j gebildet werden. Dann ist nach Satz 5.3 und Korollar 5.4 $\det B = h'$. Ist $h' > h_1$, so berechne man ein anderes Untergitter, indem man einige der erzeugenden Vektoren z_j durch neuberechnete ersetzt. H. Cohen schlägt in [Cohen] eine Anzahl von fünf vor.

Sobald man ein Gitter L' findet mit $h' \le h_1$, berechne man die Matrizen $U, V \in GL_k(\mathbb{Z})$ und $S = SNF(B) = diag(g_1, \ldots, g_l, 1, \ldots, 1)$, so daß

$S = U^{-1}BV$.

Satz 5.4 besagt dann, daß

$$\mathcal{C}l_{\mathbb{K}} \simeq \bigoplus_{1 \leq i \leq l} \left(\mathbb{Z}/g_i\mathbb{Z} \right).$$

Sei $U = ((u_{ij}))$ und $U^{-1} = ((u'_{ij}))$, dann sind

$$\mathfrak{C}_i = \prod_{j=1}^{k} \mathfrak{p}_j^{u_{ij}}, \qquad 1 \leq i \leq l \tag{14}$$

Erzeugende der Klassengruppe, mit $ord(\mathfrak{C}_i) = g_i$ und

$$\mathcal{C}l_{\mathbb{K}} = (\mathfrak{C}_1) \times (\mathfrak{C}_2) \times \ldots \times (\mathfrak{C}_l), \quad l \geq 1.$$

Es ist zu beachten, daß die Ordnungen der zyklischen Untergruppe, die von den Idealen $\mathfrak{C}_i$ erzeugt werden, nicht unbedingt von Primpotenzordnung sind. Da sie von der SNF erzeugt werden, gilt vielmehr $g_j | g_i$, für $j > i$.

Um einen Überblick über das Verfahren zur Konstruktion der Klassengruppe zu gewinnen, fasse ich dieses nocheinmal schematisch zusammen.

1. Berechne h_1, so daß $h_{\mathbb{K}} \leq h_1 < 2h_{\mathbb{K}}$.

2. Bilde die Mengen P und B_P für eine geeignete Konstante C.

3. Berechne Elemente z_j im Kern von ϕ, durch Faktorisierung von reduzierten Idealen über B_P, wie oben beschrieben, bis k linear unabhängige Elemente gefunden sind.

4. Berechne $h' = \det B$, für $B = (z_j)$. Falls $h' > h_1$, streiche fünf der Vektoren und gehe zurück zu 3.

5. Ist $h' \leq h_1$, berechne U und S, so daß $S = SNF(B) = U^{-1}BV$.

6. Berechne $\mathfrak{C}_i = \prod_{j=1}^{k} \mathfrak{p}_j^{u_{ij}}$, für $1 \leq i \leq l$. Dann ist $\mathcal{C}l_{\mathbb{K}} = (\mathfrak{C}_1) \times \ldots \times (\mathfrak{C}_l)$, $ord(\mathfrak{C}_i) = g_i$ und $h_{\mathbb{K}} = \prod_{i=1}^{l} g_i$.

Es bleibt noch das Problem, die Darstellungen in (13) zu finden. Dazu benutze man wieder die Faktorbasis B_P. Man berechne für zufällige Exponenten

x die reduzierten Ideale $\mathfrak{A}' \sim \mathfrak{A} \prod_{i=1}^{k} \mathfrak{p}_i^{x_i}$, bis man eins findet, daß über B_P zerfällt, also $\mathfrak{A}' = \prod_{i=1}^{k} \mathfrak{p}_i^{w_i}$. Dann ist

$$\mathfrak{A} \sim \prod_{i=1}^{k} \mathfrak{p}_i^{w_i - x_i} \text{ und mit Gleichung (14) } \mathfrak{A} \sim \prod_{i=1}^{l} \mathfrak{C}_i^{a_i} \,.$$

Analog erhält man eine Darstellung für $\mathfrak{B}$.

Dieses Verfahren eignet sich, Diskrete Logarithmen in Klassengruppen zu berechnen, deren Diskriminante bis zu fünfzig Dezimalstellen besitzt. Das Aufwendigste dabei ist das Berechnen der Erzeugenden $\mathfrak{C}_i$ und deren Ordnungen g_i. Hat man dies einmal getan, ist man in der Lage, in dieser Klassengruppe beliebig viele Diskrete Logarithmen zu berechnen, da das Finden der Darstellungen (13) und das Lösen der Kongruenzen $xa_I \equiv b_i \mod b_i$, im Vergleich dazu relativ schnell geht. Zur Veranschaulichung gebe ich nun einige Ergebnisse von Buchmann aus [BuDü] wieder.

Seien die Bezeichnungen wie oben, die Werte g_i aber in umgekehrter Reihenfolge gegeben:

D	k	l	$h_{\mathbb{K}}$	$g_i,\ 1 \leq i \leq l$
$-4 \cdot 10^{24} - 4$	1404	3	1 154 987 161 920	2, 4, 144 373 395 240
$-4 \cdot 10^{34} - 4$	2609	4	189 652 590 177 168 096	2, 2, 2, 23 706 573 772 146 012
$-4 \cdot 2^{2^7} - 4$	3257	2	17 787 144 930 223 461 408	2, 8 893 572 465 111 730 704

Um einen Eindruck von der Komplexität der einzelnen Berechnungen zu erhalten, beschreibt die nächste Tabelle die Rechenzeiten, die Buchmann für die obigen Beispiele auf einer Sun 4/60 Sparc Station 1 in Sekunden benötigte.

t_1: Die Zeit zur Berechnung der $\mathfrak{C}_i$ und deren Ordnungen g_i.

t_2: Die Zeit zur Berechnung der Darstellungen (13).

t_3: Die Zeit zur Lösung der Kongruenzen $xa_i \equiv b_i \mod g_i$.

D	t_1	t_2	t_3
$4 \cdot 10^{24} + 4$	3418	9	< 1
$4 \cdot 10^{34} + 4$	123 404	47	< 1
$4 \cdot 2^{2^7} + 4$	511 978	114	< 1

Literatur

[Bach] BACH, ERIC: *Explicit bounds for primality testing and related problems.* Math. Comp., 55(191): S.355–380, 1990.

[Buch] BUCHMANN, JOHANNES: *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields.* Semin. Theor. Nombres, Paris/Fr. 1988-89, Prog. Math., 91: S.27–41, 1990.

[BuDü] BUCHMANN, JOHANNES und S. DÜLLMANN: *On the computation of discrete logarithms in class groups.* Crypto'90, Lecture Notes in Computer Science, 537: S.134–139, 1990.

[BuDüWi] BUCHMANN, JOHANNES, S. DÜLLMANN und H.C. WILLIAMS: *On the complexity and efficiency of a new key exchange system.* Advances in cryptology - EUROCRYPT'89, Proc. Workshop, Houthalen/Belg. 1989, Lect. Notes Comput. Sci., 434: S.597–616, 1993.

[BuWi88] BUCHMANN, JOHANNES und H.C. WILLIAMS: *A key exchange system based on imaginary quadratic fields.* Journal of Cryptology, 1: S.107–118, 1988.

[BuWi89] BUCHMANN, JOHANNES und H.C. WILLIAMS: *A key exchange system based on real quadratic fields.* Crypto'89, Lecture Notes in Computer Science, 435: S.335–343, 1989.

[BuWi90] BUCHMANN, JOHANNES und H.C. WILLIAMS: *Quadratic fields and cryptology.* London Math. Soc. Lecture Note Series, 154: S.9–25, 1990.

[Buell] BUELL, DUNCAN A.: *Binary Quodratic Forms.* Springer-Verlag, New York, 1989.

[Cohen] COHEN, HENRI: *A Course in Computational Number Theory.* Springer-Verlag, Berlin, 1993.

[CoLe84a] COHEN, HENRI und H.W. LENSTRA: *Heuristics on class groups.* Lecture Notes in Mathematics, 1052: S.26–36, 1984.

[CoLe84b] COHEN, HENRI und H.W. LENSTRA: *Heuristics on class groups of number fields.* Number Theory '83, Lecture Notes in Mathematics, 1068: S.33–62, 1984.

[Cohn] COHN, HENRY: *Advanced Number Theory.* Dover Publications Inc., New York, 1980.

[DiffHell] DIFFIE, W. und M. E. HELLMANN: *New directions in cryptography.* IEEE, Trans. Inf. Theory, 22(6): S.644–654, 1976.

[Elg85a] ELGAMAL, TAHER: *Public key cryptosystems and a signature scheme based on discrete logarithms.* IEEE, Trans. Inf. Theory, 31(4): S.469–472, 1985.

[Elg85b] ELGAMAL, TAHER: *Subexponential-time algorithm for computing* DL *over* $\mathrm{GF}(p^2)$. IEEE, Trans. Inf. Theory, 31(4), 1985.

[Forster] FORSTER, OTTO: *Algorithmische Zahlentheorie.* Vieweg-Verlag, 1996.

[HarHaw] HARTLEY, B. und T.O. HAWKES: *Rings, Modules and Linear Algebra.* Chapman and Hall, 1970.

[Knuth] KNUTH, DONALD E.: *The Art of Computer Programming,* Band 2. Addison-Wesley, Reading,MA, 1981.

[Koch] KOCH, HELMUT: *Einführung in die klassische Mathematik.* Akademie-Verlag, Berlin, 1986.

[LaMoOd] LAGARIAS, J.C., H.L. MONTGOMERY und A.M. ODLYZKO: *A bound for the least prime Ideal in the Chebotarev density theorem.* Invent. Math., 54: S.271–296, 1979.

[Lens] LENSTRA, H.W.: *Primality testing.* Computational Methods in Number Theory, Part 1, Math. Cent. Tracts, 154: S.55–77, 1982.

[Leutb] LEUTBECHER, ARMIN: *Zahlentheorie.* Springer-Verlag, New York, 1996.

[McCur] MCCURLEY, KEVIN S.: *The discrete logarithm problem.* Proc. Symposia Applied Mathematics, AMS, 42: S.49–74, 1984.

[Nark] NARKIEVICZ, WLADYSLAV: *Elementary and Analytic Theory of Algebraic Numbers.* 2nd ed., Springer-Verlag, Warszawa, 1990.

[Neuk] NEUKIRCH, JÜRGEN: *Algebraische Zahlentheorie.* Springer-Verlag, Berlin, 1992.

[PoZass] POHST, M. und H. ZASSENHAUS: *On unit computation in real quadratic fields.* EUROSAM'79, Intl. Symp. Marseille, Lecture Notes in Computer Science, 72: S.140–152, 1979.

[SchBuWi] SCHEIDLER, RENATE, J. BUCHMANN und H.C. WILLIAMS: *A key exchange protocol using real quadratic fields.* Journal of Cryptology, 7: S.171–199, 1994.

[Schoof] SCHOOF, R.J.: *Quadratic fields and factorization.* Computational Methods in Number Theory, Part 2, Math. Centrum Tracts, 155: S.235–286, 1982.

[Shanks] SHANKS, DANIEL: *The infrastructure of a real quadratic field and its applications.* Proc. 1972 Number Theory Conference, Boulder, Colorado: S.217–224, 1973.

[SteWi88a] STEPHENS, A.J. und H.C. WILLIAMS: *Computation of real quadratic fields with classnumber one.* Math. Comp, 51(184): S.809–824, 1988.

[SteWi88b] STEPHENS, A.J. und H.C. WILLIAMS: *Some computational results on a problem concerning powerful numbers.* Math. Comp, 50(182): S.619–632, 1988.

[WiWu] WILLIAMS, HUGH C. und M.C. WUNDERLICH: *On the parallel generation of the residues for the continued fraction factoring algorithm.* AMS Math. Comp., 48(177): S.405–423, 1987.