Freie Universität Berlin
Fachbereich Mathematik und Informatik

Bachelorarbeit

Darstellung ganzer Zahlen durch ganzzahlige binäre quadratische Formen

bei

Prof. Dr. Volker Schulze

von

Mario Koddenbrock
Matrikelnr.: 4298300

20. Juli 2011

Inhaltsverzeichnis

Einleitung

Die ersten elementaren zahlentheoretischen Untersuchungen der Neuzeit gehen auf Pierre de Fermat (1607–1665) zurück. Aus seinen Briefen an Carcavi geht unter anderem sein Zwei-Quadrate-Satz hervor:

„Jede Primzahl, die ein Vielfaches von 4 um 1 übersteigt, besteht aus zwei Quadraten."

In heutiger Schreibweise entspricht dies, dass eine Primzahl $p \in \mathbb{N}$ genau dann eine Darstellung $p = x^2+y^2$ mit $x, y \in \mathbb{Z}$ besitzt, wenn $p \equiv 1 \pmod 4$ ist. Joseph-Louis Lagrange griff diese Sätze 1773 in seiner „Recherches d'arithmétique" auf und verallgemeinerte sie zur Theorie der binären quadratischen Formen. Er untersuchte die Zahlen, die sich durch eben diese Formen $ax^2 + bxy + cy^2$ darstellen lassen, und leitete daraus die von Fermat aufgestellten Sätze ab.
In dieser Arbeit geht es nun um binäre quadratischen Formen und insbesondere darum, welches Darstellungen eine ganze Zahl durch eine solche Form besitzt.
Das erste Kapitel wird hierzu erst einmal in die Theorie der binären quadratischen Formen einführen und elementare Aussagen zu diesen beweisen. Um jedoch genauer auf die Frage einzugehen, für welche ganzen Zahlen x und y die Zahl n eine Darstellung durch $ax^2 + bxy + cy^2$ besitzt, bedarf es einiger algebraischer Hilfsmittel, die im zweiten und dritten Kapitel eingeführt werden. Außerdem wird hier ein kurzer Einblick in die Theorie der Kettenbrüche gegeben, da diese bei der tatsächlichen Bestimmung der gesuchten Zahlen x und y sehr hilfreich ist.
Das vierte Kapitel beinhaltet die Hauptresultate dieser Arbeit. Mit Hilfe der eingeführten Hilfsmittel wird gezeigt, dass es zum obigen Problem äquivalent ist, bestimmte Elemente eines quadratischen Zahlkörpers zu finden. Gesucht werden dabei genau die Elemente, deren Norm $\frac{n}{a}$ ist.
Zum Abschluss werden im fünften Kapitel die gewonnenen Resultate angewandt.

Literaturhinweis: Die historischen Bemerkungen stammen aus [SO80] und [Rib09].

1 Binäre Quadratische Formen

1.1 Definition: Binäre Quadratische Formen und Diskriminanten

Ein Polynom der Form $f(x,y) = ax^2 + bxy + cy^2$ mit ganzzahligen Koeffizienten a, b, c heißt *ganzzahlige binäre quadratische Form*. Die *Diskriminante* einer solchen Form ist definiert durch $D := b^2 - 4ac$.

Dabei ist eine allgemeine Form ein Polynom, dessen Summanden alle den gleichen Grad haben. In diesem Fall der quadratischen Formen ist der Grad stets zwei. Da die hier betrachteten Polynome alle genau zwei Variablen haben, nennt man sie zudem binär. In der gesamten Arbeit werden nur binäre quadratische Formen betrachtet, weshalb diese im Folgenden der Einfachheit halber häufig auch nur mit *Form* bezeichnet werden.

Es wird nun untersucht, welche Werte eine solche Form für ganzzahlige x und y annehmen kann. Dafür ist folgende Unterscheidung sinnvoll:

1.2 Definition: Definitheit

Eine binäre quadratische Form f heißt *positiv definit*, falls für alle ganzzahligen von Null verschiedenen (x,y) gilt, dass $f(x,y) > 0$. Dementsprechend heißt f *negativ definit*, falls $f(x,y) < 0$. Falls f sowohl positive, als auch negative Werte annehmen kann, so heißt sie *indefinit*.

1.2.1 Bemerkungen

- f ist offenbar genau dann positiv definit, wenn $-f$ negativ definit ist.
- $f(x,y)$ zerfällt in $\mathbb{Q}[x]$ genau dann in Linearfaktoren, wenn $D = m^2$ ein Quadrat in $\mathbb{Q}$ ist. Falls $a = 0$, so ist $f(x,y) = (bx + cy)\,y$, falls $a \neq 0$, so ist $f(x,y) = \frac{1}{4a}(2ax + (b+m)\,y)(2ax + (b-m)\,y)$.

Der Fall, dass D ein Quadrat ist, ist jedoch für das Hauptresultat dieser Arbeit in Kapitel 4 uninteressant. Auch wenn es nur für wenige der folgenden Sätze benötigt wird, sei deshalb im Folgenden stets D kein Quadrat in $\mathbb{Q}$.

1.2.2 Satz

Eine binäre quadratische Form $f(x,y) = ax^2 + bxy + cy^2$ ist genau dann positiv definit, wenn a positiv und die Diskriminante negativ ist.

Beweis „⇒“ Da f positiv definit ist, muss es für alle $(x, y) \in \mathbb{Z}^2 \setminus \{0\}$ positive Werte annehmen. Also muss auch $f(1, 0) = a$ positiv sein. Hieraus erkennt man bei der Wahl $x = -b$ und $y = 2a$, dass D negativ sein muss.

$$f(-b, 2a) = ab^2 - 2ab^2 + 4a^2c = a\left(4ac - b^2\right) = a\,(-D)$$

„⇐“ Es ist sinnvoll $f\,(x, y)$ zunächst auf eine Form zu bringen, von der man leichter ablesen kann, wann f positiv ist. Dabei darf durch a dividiert werden, da es nach Voraussetzung positiv ist.

$$\begin{aligned} f(x, y) &= ax^2 + bxy + cy^2 \\ &= ax^2 + bxy + \frac{1}{4a}b^2y^2 + cy^2 - \frac{1}{4a}b^2y^2 \\ &= \frac{1}{4a}\left(4a^2x^2 + 4abxy + b^2y^2 + 4acy^2 - b^2y^2\right) \\ &= \frac{1}{4a}\left((2ax + by)^2 + \left(4ac - b^2\right)y^2\right) \\ &= \frac{1}{4a}\left((2ax + by)^2 + (-D)\,y^2\right) \end{aligned} \tag{1}$$

Nach Voraussetzung ist a positiv und D negativ und somit $f(x, y) \geq 0$. Falls aber $f(x, y) = 0$, so ist $-Dy^2 = 0$ und y war schon gleich 0. Damit folgt aus $2ax + by = 0$, dass auch $x = 0$.

□

1.2.3 Bemerkungen

- In Satz 1.2.2 kann anstelle von a positiv offenbar genauso gut c positiv bzw. a und c positiv gefordert werden.
- Analog zu Satz 1.2.2 ist die Form $f\,(x, y) = ax^2 + bxy + cy^2$ genau dann negativ definit, wenn a und die Diskriminante D negativ sind.
- Aufgrund dieser Äquivalenz gilt offenbar, dass eine Form definit ist, falls die Diskriminante negativ ist, und sie indefinit ist, falls die Diskriminante positiv ist.

1.2.4 Satz

Eine binäre quadratische Form f hat zu gegebenem ganzzahligem n nur endlich viele ganzzahlige x und y, sodass $f(x, y) = n$.

Beweis Da gefordert wurde, dass $D = b^2 - 4ac$ kein Quadrat ist, ist a und c von null verschieden. Das heißt, man kann die Umformung (1) von f aus dem Beweis von Satz 1.2.2 benutzen. Statt die obige Aussage zu zeigen, ist es dann einfacher, die folgende äquivalente Aussage zu zeigen. Es gibt nur endlich viele ganzzahlige x und y, die die Ungleichung $|f(x,y)| \leq |n|$ erfüllen. Die Endlichkeit dieser Menge kann dadurch gezeigt werden, dass zunächst Schranken für y und in einem zweiten Schritt Schranken für x gefunden werden.

$$\begin{aligned}
& |f(x,y)| \leq |n| \\
\overset{(1)}{\Longrightarrow}\ & \left|\frac{1}{4a}\left((2ax+by)^2 + (-D)\,y^2\right)\right| \leq |n| \\
\Longrightarrow\ & \left|\frac{1}{4a}\right| \left|\underbrace{(2ax+by)^2}_{\geq 0} + (-D)\,y^2\right| \leq |n| \\
\Longrightarrow\ & |D|\,y^2 \leq |4an| \\
\Longrightarrow\ & y^2 \leq \left|\frac{4an}{D}\right|
\end{aligned}$$

Offensichtlich kann es nur endlich viele solche ganzzahligen y geben. Analog geht man bei x vor, hier gilt $(\star)$ aufgrund der umgekehrten Dreiecksungleichung:

$$\begin{aligned}
& |f(x,y)| \leq |n| \\
\Longrightarrow\ & \left|(2ax+by)^2 + (-D)\,y^2\right| \leq |4an| \\
\overset{(\star)}{\Longrightarrow}\ & \left|(2ax+by)^2\right| - \left|(-D)\,y^2\right| \leq |4an| \\
\Longrightarrow\ & (2ax+by)^2 \leq 4an + |D|\,y^2 \\
\Longrightarrow\ & -\sqrt{4an+|D|\,y^2} \leq 2ax+by \leq \sqrt{4an+|D|\,y^2} \\
\Longrightarrow\ & -\frac{\sqrt{4an+|D|\,y^2}-by}{2a} \leq x \leq \frac{\sqrt{4an+|D|\,y^2}-by}{2a}
\end{aligned}$$

Die Menge aller x,y mit $|f(x,y)| \leq |n|$ ist also endlich. Hieraus folgt unmittelbar die Behauptung für $f(x,y) = n$. □

1.2.5 Bemerkung

- Mit Hilfe der Schranken aus dem Beweis von Satz 1.2.4 kann man alle Lösungen von $f(x,y) = n$ bei gegebenem $n \in \mathbb{Z}$ bestimmen.
- Außerdem ist es zu einer gegebenen Form $f(x,y) = ax^2 + bxy + cy^2$ nun möglich, in endlich vielen Schritten die betragsmäßig kleinste darstellbare Zahl $m \in \mathbb{N}$ zu finden. Denn nach 1.2.4 und mit $f(1,0) = a$, gibt es nur endlich viele x und y mit $|f(x,y)| \leq |a|$. So findet man durch einfaches Ausprobieren die vom Betrag her

kleinste Zahl m, die eine Darstellung durch f besitzt.
Desweiteren findet man auch die zugehörigen Werte u und v mit $ggT(u,v) = 1$, sodass $f(u,v) = m$. Sonst wäre nämlich $f\left(\frac{u}{ggT(u,v)}, \frac{v}{ggT(u,v)}\right) = \frac{m}{(ggT(u,v))^2}$ eine kleinere darstellbare Zahl.

Man kann sich nun Fragen, ob es unterschiedliche Formen gibt, die die gleichen Wertebereiche haben. Hierfür ist die Einführung der folgenden Äquivalenzrelation sinnvoll.

1.3 Definition: Äquivalenz von Formen

Zwei binäre quadratische Formen f und g heißen *äquivalent* ($f \sim g$), falls es eine Matrix $A_{f,g} \in M(2,2,\mathbb{Z})$ mit $\det(A_{f,g}) = \pm 1$ gibt, sodass gilt:

$$f\begin{pmatrix} x \\ y \end{pmatrix} = g\left(A_{f,g}\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

Das heißt, es gibt eine ganzzahlige Transformation mit det ± 1, die f in g überführt.

Dass $\sim$ wirklich eine Äquivalenzrelation auf der Menge der binären quadratischen Formen bildet, ist im Folgenden noch zu untersuchen.

1.3.1 Lemma

Eine Matrix $A \in M(2,2,\mathbb{Z})$ hat genau dann ein Inverses mit ganzzahligen Einträgen, wenn $\det(A) = \pm 1$.

Beweis „⇒“ Falls A ein ganzzahliges Inverses besitzt, so ist auch $\det(A)$ und $\det(A^{-1})$ ganzzahlig. Aus $\det(A)\det(A^{-1}) = 1$ folgt somit, dass $\det(A) = \pm 1$
„⇐“ Falls $\det(A) = \pm 1$, so ist $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ invertierbar und die inverse Matrix hat die Form $A^{-1} = \frac{1}{\det(A)}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Also ist A^{-1} wieder ganzzahlig. □

1.3.2 Nachweis der Äquivalenzrelation

1. $f \sim f$ für $A_{f,f} = E_2$ (Einheitsmatrix)
2. Aus $f \sim g$ folgt, dass $A_{f,g}$ mit $f\begin{pmatrix} x \\ y \end{pmatrix} = g\left(A_{f,g}\begin{pmatrix} x \\ y \end{pmatrix}\right)$ existiert. Mit Hilfe des obigen

Lemmas weiß man, dass $A_{f,g}^{-1} \in M(2,2,\mathbb{Z})$, und wegen

$$g\begin{pmatrix}x\\y\end{pmatrix} = g\left(A_{f,g}A_{f,g}^{-1}\begin{pmatrix}x\\y\end{pmatrix}\right) = f\left(A_{f,g}^{-1}\begin{pmatrix}x\\y\end{pmatrix}\right)$$

weiß man auch, dass $A_{g,f} = (A_{f,g})^{-1}$ und damit, dass $g \sim f$.

3. Wegen $f \sim g$ und $g \sim h$ weiß man, dass $A_{f,g}$ und $A_{g,h}$ existieren.
   Man wähle also $A_{f,h} := A_{g,h}A_{f,g}$. Dann ist $A_{f,h}$ wieder ganzzahlig, da $\det(A_{f,h}) = \det(A_{g,h})\det(A_{f,g}) = \pm 1$ und somit ist aufgrund von folgender Gleichung $f \sim h$.

$$f\begin{pmatrix}x\\y\end{pmatrix} = g\left(A_{f,g}\begin{pmatrix}x\\y\end{pmatrix}\right) = h\left(A_{g,h}A_{f,g}\begin{pmatrix}x\\y\end{pmatrix}\right)$$

Man hat also nun eine Äquivalenzrelation auf der Menge der binären quadratischen Formen. Folgende Bemerkungen machen deutlich, dass die lineare Transformation einer Substitution entspricht, die wieder rückgängig gemacht werden kann. Man kann also anstelle einer gegebenen Form genauso gut eine beliebige äquivalente Form betrachten.

1.3.3 Bemerkungen

- Es ist möglich jede binäre quadratische Form f durch eine symmetrische Matrix $F := \begin{pmatrix}a & \frac{b}{2}\\ \frac{b}{2} & d\end{pmatrix}$ zu beschreiben. Denn f hat folgende Form:

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{pmatrix}x & y\end{pmatrix}\begin{pmatrix}a & \frac{b}{2}\\ \frac{b}{2} & d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$$

  F heißt auch darstellende Matrix zu f.

- Wenn eine Form g zu obigem f mittels der Transformation A äquivalent ist, so gilt $G = A^T F A$ bzw.:

$$g\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x & y\end{pmatrix}A^T\begin{pmatrix}a & \frac{b}{2}\\ \frac{b}{2} & d\end{pmatrix}A\begin{pmatrix}x\\y\end{pmatrix}$$

- A entspricht also der Basiswechselmatrix, die F in G überführt. Die Lösungen von $f(x,y) = n$ stehen demnach in bijektiver Korrespondenz zu den Lösungen von $g(x,y) = n$. Äquivalente Formen nehmen also auch dieselben Werte an.

- Die Diskriminante D_f von f steht in engem Zusammenhang zur Determinante von F. Es gilt:

$$D_f = -4\ \det(F)$$

1.4 Beispiel

Bei dem Versuch die Gleichung $5x^2 + 26xy + 34y^2 = 2$ zu lösen, kann es nun hilfreich sein, eine äquivalente Form zu finden, deren Lösungen leichter zu bestimmen sind. Durch quadratische Ergänzung erhält man die äquivalente Gleichung $(2x + 5y)^2 + (x + 3y)^2 = 2$. Wenn man also als Transformationsmatrix $A := \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$ wählt, erhält man $f \sim g$ mit $f(x, y) = 5x^2 + 26xy + 34y^2$ und $g(x, y) = x^2 + y^2$. Offensichtlich hat $x^2 + y^2 = 2$ vier ganzzahlige Lösungen: $(\pm 1, \pm 1)$. Die Lösungen der eigentlichen Gleichung bekommt man nun durch Transformation mittels $A^{-1} = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}$.
Also $\pm A^{-1}(1, 1) = \pm(2, -1)$ bzw. $\pm A^{-1}(1, -1) = \pm(8, -3)$.

Hieraus wird auch deutlich, dass alle zu einer positiv definiten Form äquivalenten Formen auch positiv definit sein müssen. Denn die Darstellung einer negativen Zahl würde auch bei allen äquivalenten Formen eine transformierte Darstellung dieser Zahl liefern. Da solche Transformationen stets durch reguläre Matrizen dargestellt werden können, ist es auch nicht möglich, dass man durch Transformation eine nicht triviale Darstellung der 0 erhält.

Positive Definitheit ist also eine Eigenschaft, die mit einer Form ihrer ganzen Äquivalenzklasse zukommt. Der folgende Satz wird dies auch für den Wert der Diskriminante zeigen.

1.5 Satz: Invarianz der Diskriminante

Zwei äquivalente Formen haben stets gleiche Diskriminanten.

Beweis Seien f und g zwei äquivalente Formen mit darstellenden Matrizen F und G und den Diskriminanten D_f und D_g. Außerdem sei A die Transformationsmatrix mit $\det(A) = \pm 1$. Wegen Bemerkung 1.3.3 gilt dann:

$$\begin{aligned} D_g &= -4 \det(G) = -4 \det(A^T F A) \\ &= -4 \det(A^T) \det(F) \det(A) = (\pm 1)^2 (-4 \det(F)) \\ &= D_f \end{aligned}$$

□

Zusammenfassend stellt man also fest, dass es meistens nur wichtig ist, einen Repräsentanten aus jeder Äquivalenzklasse zu untersuchen. Hierfür ist es von Vorteil, sich ein geeignetes Repräsentantensystem zu überlegen. Folgende Definition ist hierfür sinnvoll:

1.6 Definition: Reduzierte Formen

Eine binäre quadratische Form $ax^2 + bxy + cy^2$ heißt *reduziert*, falls $|b| \leq |a| \leq |c|$.

1.6.1 Bemerkung

Für eine positiv definite Form $f(x, y) = ax^2 + bxy + cy^2$ gilt nach Satz 1.2.2, dass a und c positiv sind. Also ist f genau dann reduziert, wenn $|b| \leq a \leq c$.

1.6.2 Bemerkung

Im Folgenden wird man feststellen, dass zu jeder Form auch eine äquivalente reduzierte Form existiert. Diese reduzierte Form muss jedoch nicht eindeutig sein. Ein echtes Repräsentantensystem der Äquivalenzklassen stellen die reduzierten Formen nur für die definiten Formen und auch nur mit der stärkeren Bedingung $0 \leq b \leq a \leq c$ dar. Mit dieser zusätzlichen Bedingung, dass $b > 0$, ist dann die reduzierte Form eindeutig.

1.6.3 Satz

Zu jeder binären quadratischen Form existiert eine äquivalente reduzierte Form.

Beweis Sei $f(x, y) = Ax^2 + Bxy + Cy^2$ gegeben. Die Konstruktion von $\tilde{f}(x, y) = ax^2 + bxy + cy^2$ mit der Eigenschaft $|b| \leq |a| \leq |c|$ geschieht in mehreren Schritten.
Zuerst wird der führenden Koeffizienten von $\tilde{f}$ als die dem Betrag nach kleinste von f darstellbare Zahl gewählt. Dieses a kann man nach 1.2.5 genauso bestimmen, wie ganze Zahlen u und v mit $ggT(u, v) = 1$, sodass $f(u, v) = a$. Wegen $ggT(u, v) = 1$ gibt es ganze Zahlen α und β mit $\alpha u - \beta v = 1$. Diese Tatsache garantiert, dass $A := \begin{pmatrix} u & \beta \\ v & \alpha \end{pmatrix}$ eine ganzzahlige Transformation darstellt, die f in

$$\begin{aligned} g(x, y) &= A(ux + \beta y)^2 + B(ux + \beta y)(vx + \alpha y) + C(vx + \alpha y)^2 \\ &= \left(Au^2 + Buv + Cv^2\right) x^2 + \dots \\ &= ax^2 + \dots \end{aligned}$$

überführt. Es gilt also $f \sim g$, wobei g also führenden Koeffizienten a hat.

Von nun an kann man ohne Einschränkung davon ausgehen, dass f die Form $f(x, y) = ax^2 + Bxy + Cy^2$ hat. Um $\tilde{f}$ zu konstruieren, darf bei einer Transformation der führende Koeffizient von f nicht mehr verändert werden. Solch eine Transformation stellt $A := \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ für jedes ganzzahlige j dar. Nun kann das j so gewählt werden, dass bei der dabei

entstehenden Form

$$\begin{aligned} g(x,y) &= a(x+jy)^2 + B(x+jy)y + Cy^2 \\ &= ax^2 + (2aj+B)xy + \left(aj^2 + j + C\right)y^2 \end{aligned}$$

der 2. Koeffizient $2aj + B$ die gewünschte Bedingung $|2aj + B| \leq |a|$ erfüllt. Dies ist genau dann der Fall, wenn:

$$-\frac{B}{2a} - \frac{1}{2} \leq j \leq -\frac{B}{2a} + \frac{1}{2}$$

Für $j := \left[-\frac{B}{2a}\right]$ gilt also, dass $|2aj + B| \leq |a|$. Nun ist die Gleichung $|b| \leq |a|$ erfüllt. Nach Annahme ist a der betragsmäßig kleinste Wert, den f annimmt. Deshalb muss $|C| = |f(0,1)| \geq |a|$ sein. □

1.6.4 Satz

Für jede positiv definite Form $f(x,y) = ax^2+bxy+cy^2$ existiert eine eindeutige äquivalente Form $\tilde{f}(x,y) = ax^2 + bxy + cy^2$ mit $0 \leq b \leq a \leq c$.

Beweis Nach Satz 1.6.3 existiert zu f schon eine reduzierte Form $\tilde{f}$. Da die Transformation $A := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ aber offenbar $ax^2 + bxy + cy^2$ in $ax^2 - bxy + cy^2$ überführt, kann man ohne Einschränkung von $0 \leq b \leq a \leq c$ für $\tilde{f}$ ausgehen.

Nun bleibt noch die Eindeutigkeit zu zeigen. Das heißt, dass zwei äquivalente reduzierte Formen stets identisch sind. Seien hierzu $\tilde{f}(x,y) = ax^2 + bxy + cy^2$ und $\tilde{g}(x,y) = Ax^2 + Bxy + Cy^2$ zwei reduzierte Formen mit $b, B > 0$ und $T := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ die entsprechende Transformation. Es gilt dann:

$$0 \leq b \leq a \leq c \qquad 0 \leq B \leq A \leq C \qquad \alpha\delta - \beta\gamma = \pm 1$$

Wegen 1.5 weiß man außerdem, dass:

$$A = a\alpha^2 + b\alpha\gamma + c\gamma^2 \tag{2}$$

$$B = 2a\alpha\beta + b(\alpha\gamma + \beta\delta) + 2c\gamma\delta \tag{3}$$

$$C = a\beta^2 + b\beta\delta + c\delta^2 \tag{4}$$

$$D_{\tilde{f}} = D_{\tilde{g}} \tag{5}$$

Falls nun $\tilde{f} \neq \tilde{g}$, so gilt $a \neq A$ oder $c \neq C$. Andernfalls wäre $\tilde{f} = \tilde{g}$ aufgrund von:

$$b = \sqrt{D_{\tilde{f}} + 4ac} \overset{(5)}{=} \sqrt{D_{\tilde{g}} + 4AC} = B$$

- Falls $a \neq A$, so kann man ohne Einschränkung annehmen, dass $a > A$. Andernfalls tauscht man die Bezeichnungen von $\tilde{f}$ und $\tilde{g}$. Es ergibt sich dann, dass

$$\begin{aligned} A &\overset{(2)}{=} a\alpha^2 + b\alpha\gamma + c\gamma^2 \overbrace{\geq}^{b\geq 0} a\alpha^2 - b\,|\alpha\gamma| + c\gamma^2 \\ &\overbrace{\geq}^{a\leq c} a\alpha^2 - b\,|\alpha\gamma| + a\gamma^2 = a\left(\alpha^2 + \gamma^2\right) - b\,|\alpha\gamma| \\ &\geq 2a\,|\alpha\gamma| - b\,|\alpha\gamma| \qquad [\text{denn } \alpha^2 + \gamma^2 \geq \pm 2\alpha\gamma\ ] \\ &\underbrace{\geq}_{a\geq b} a\,|\alpha\gamma| \end{aligned} \tag{6}$$

  Aufgrund von $a \neq A$ muss nun also $|\alpha\gamma| < 1$ und damit $|\alpha\gamma| = 0$ sein. Da aber $\det(T) = \alpha\delta - \beta\gamma = \pm 1$, kann lediglich einer der beiden Faktoren gleich Null sein. Dann erhält man aber mit Hilfe der obigen Ungleichungskette

$$A = a\alpha^2 + \underbrace{b\alpha\gamma}_{=0} + c\gamma^2 \geq a\alpha^2 + a\gamma^2 \geq a$$

  einen Widerspruch zu $a > A$.

- Analog zu oben kann man von $c > C$ ausgehen, da sonst wegen $a = A$ die Koeffizienten einfach umbenannt werden könnten. Wegen (6) ist nun $|\alpha\gamma| \leq 1$.

  1. Fall: Es ist $|\alpha\gamma| = 1$. Dann ist auch $\gamma \neq 0$ und man bekommt einen Widerspruch zu $a = A$:

$$\begin{aligned} & c > C \geq A = a \\ \Longrightarrow\ & c\gamma^2 > a\gamma^2 \\ \Longrightarrow\ & a\alpha^2 + c\gamma^2 > a\alpha^2 + a\gamma^2 \\ \Longrightarrow\ & a\alpha^2 - b\,|\alpha\gamma| + c\gamma^2 > a\alpha^2 - b\,|\alpha\gamma| + a\gamma^2 \\ \overset{(6)}{\Longrightarrow}\ & A > a \end{aligned}$$

  2. Fall $|\alpha\gamma| = 0$. Dann ist wegen $\det(T) \neq 0$ wieder nur einer der beiden Faktoren gleich Null. Wenn $\alpha = 0$, so ist mit demselben Argument wie im 1. Fall $A > a$. Wenn

allerdings $\gamma = 0$, so ist wegen $\det(T) = \alpha\delta - \beta\gamma = \alpha\delta = \pm 1$:

$$B \overset{(5)}{=} 2a\alpha\beta + b\left(\underbrace{\alpha\delta}_{\pm 1} + \underbrace{\beta\gamma}_{=0}\right) + \underbrace{2c\gamma\delta}_{=0} = 2a\alpha\beta \pm b \quad .$$

Falls nun $B = 2a\alpha\beta + b$, so ist $b - B = -2a\alpha\beta$ und gleichzeitig $0 \leq B < b \leq a$. Dies ist ein Widerspruch, da $b - B$ sowohl ein Vielfaches von $2a$ ist, als auch die Ungleichung $0 < b - B \leq a$ erfüllen müsste.

Falls aber $B = 2a\alpha\beta - b$, so ist ganz analog $B + b = 2a\alpha\beta$ und $0 \leq B < b \leq a$. Hier bekommt man einen Widerspruch, da $B + b$ ein Vielfaches von $2a$ ist und gleichzeitig $0 < b + B < 2a$ erfüllt.
Somit muss gelten $b = B$ und die beiden Formen $\tilde{f}$ und $\tilde{g}$ stimmen überein.

1.6.5 Bemerkungen

- Der Beweis von 1.6.3 zeigt auch, wie man aus einer gegebenen positiv definiten Form die äquivalente reduzierte Form konstruieren kann.
- Falls f negativ definit ist, so ist $-f$ positiv definit und damit existiert ein eindeutiges $\tilde{f}$ mit $0 \leq -b \leq -a \leq -c$, sodass $-\tilde{f}$ zu f äquivalent ist.

1.7 Satz: Diskriminanten reduzierter Formen

Zu jeder beliebigen Diskriminante gibt es nur endlich viel reduzierte Formen.

Beweis Es ist zu zeigen, dass es nur endlich viele ganze Zahlen a, b und c gibt, die gleichzeitig die Bedingung der Reduziertheit $|b| \leq |a| \leq |c|$, als auch $b^2 - 4ac = D$ erfüllen. Ähnlich wie im Beweis von 1.2.4 kann man hier zunächst zeigen, dass a unabhängig von b und c beschränkt ist und anschließend, dass b unabhängig von c beschränkt ist. Dass dann auch die Menge aller dazu passender c beschränkt ist, ergibt sich, da D kein Quadrat ist und somit $a \neq 0$, aus: $D = b^2 - 4ac$ genau dann, wenn $\frac{b^2 - D}{4a} = c$. Die Beschränktheit von a ergibt sich aus folgender Bedingung:

$$|-D| = \left|4ac - b^2\right| \geq |4ac - |ac|| \geq 3\,|ac| \geq 3a^2 \quad \Longleftrightarrow \quad \sqrt{\frac{|D|}{3}} \geq a \geq 0$$

Da $|b| \leq |a|$ schon Voraussetzung war, ist hiermit gezeigt, dass nur endlich viele reduzierte Formen die Diskriminante D besitzen. □

1.7.1 Beispiel

Bestimmung aller positiv definiten Formen mit Diskriminante $0 < -D \leq 12$. Nach Satz 1.2.2 gilt $a > 0$ und aus dem Beweis 1.7 ist klar, dass:

$$2 = \sqrt{\frac{12}{3}} \geq \sqrt{\frac{|D|}{3}} \geq a \geq 1$$

Außerdem muss die Bedingung der Reduziertheit $0 \leq b \leq a \leq c$ erfüllt sein. Somit kann man alle möglichen Werte a, b und damit auch für c bestimmen.

$$\left\{ \begin{array}{c} a=1 \\ b=0 \end{array} \right\} \Rightarrow D = b^2 - 4ac = -4c \Rightarrow \left\{ \begin{array}{c} c=1 \\ D=-4 \end{array} \right\} \text{oder} \left\{ \begin{array}{c} c=2 \\ D=-8 \end{array} \right\} \text{oder} \left\{ \begin{array}{c} c=3 \\ D=-12 \end{array} \right\}$$

$$\left\{ \begin{array}{c} a=1 \\ b=1 \end{array} \right\} \Rightarrow D = 1-4c \qquad \Rightarrow \left\{ \begin{array}{c} c=1 \\ D=-3 \end{array} \right\} \text{oder} \left\{ \begin{array}{c} c=2 \\ D=-7 \end{array} \right\} \text{oder} \left\{ \begin{array}{c} c=3 \\ D=-11 \end{array} \right\}$$

$$\left\{ \begin{array}{c} a=2 \\ b=0,1 \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} D=1-8c \\ D=-8c \end{array} \right\} \Rightarrow c = 1 \Rightarrow \text{nicht reduziert.}$$

$$\left\{ \begin{array}{c} a=2 \\ b=2 \end{array} \right\} \Rightarrow D = 4-8c \qquad \Rightarrow \left\{ \begin{array}{c} c=2 \\ D=-12 \end{array} \right\}$$

Es ergibt sich daraus folgende Tabelle:

Diskriminante	Anzahl der Klassen	pos def Formen
-3	1	$x^2 + xy + y^2$
-4	1	$x^2 + y^2$
-7	1	$x^2 + xy + 2y^2$
-8	1	$x^2 + 2y^2$
-11	1	$x^2 + xy + 3y^2$
-12	2	$x^2 + 3y^2$ und $2x^2 + 2xy + 2y^2$

Nun sieht man noch einmal, dass die Form $5x^2 + 26xy + 34y^2$ aus dem Beispiel 1.4 schon allein aufgrund ihrer Diskriminante $D = 26^2 - 4 \cdot 5 \cdot 36 = -4$ äquivalent zu $x^2 + y^2$ sein muss.

1.7.2 Bemerkung

Es ist stets $D = b^2 - 4ac \equiv b^2 \equiv 0, 1 \pmod 4$.

- Falls $D \equiv 0 \pmod 4$, so hat $x^2 - \frac{D}{4}y^2$ die Diskriminate D
- Falls $D \equiv 1 \pmod 4$, so hat $x^2 + xy + \frac{1-D}{4}y^2$ die Diskriminate D

Die entsprechende Form heißt auch *Hauptform* der Diskriminante D.

1.8 Vermutung von Gauss

Es sei $h(D)$ die Anzahl der Äquivalenzklassen von positiv definiten Formen mit Determinante $-D$, dann gilt:

$$\lim_{D\to-\infty} h(D) = \infty$$

Das bedeutet, es gibt nur endlich viele negative Diskriminanten mit Klassenzahl 1. Harold Stark [Sta67] bewies, dass dies genau $D = -3,-4,-7,-8,-11,-19,-43,-67$ und -163 sind. Die obige Aussage wurde 1934 von Hans Heilbronn [HL34] bewiesen und bereits von Gauss vermutet.

1.9 Satz: Eigentliche Darstellbarkeit ganzer Zahlen

Es sei f eine positiv definite quadratische Form mit Diskriminante D und Klassenzahl $h(D) = 1$. Für eine beliebige natürliche Zahl n gilt:

$$f \text{ stellt } n \text{ eigentlich dar } \iff x^2 \equiv D \pmod{4n} \text{ ist lösbar}$$

Hierbei bedeutet eine *eigentliche Darstellung* von n durch f, dass es teilerfremde Zahlen $x, y \in \mathbb{Z}$ gibt, sodass $f(x, y) = n$.

Beweis „⇒“ Da f n eigentlich darstellt, kann man analog zu dem Beweis von 1.6.2 eine zu f äquivalente Form konstruieren, deren führender Koeffizient n ist. Sei dies $g(x, y) = nx^2 + mxy + ly^2$. Dann gilt aufgrund von 1.5, dass $D = m^2 - 4nl$. Hieraus folgt direkt, dass $m^2 \equiv D \pmod{4n}$.

„⇐“ Da ein $m \in \mathbb{Z}$ existiert, sodass $m^2 \equiv D \pmod{4n}$, kann man m^2 folgendermaßen schreiben: $m^2 = D + 4nl$ mit $l \in \mathbb{Z}$. Dann ist $g(x, y) = nx^2 + mxy + ly^2$ eine Form mit Diskriminante $D_g = m^2 - 4nl = D$. Da $h(d) = 1$, ist g zu allen Formen mit gleicher Diskriminante äquivalent. Somit stellt f die gleichen Zahlen wie g dar. Da $g(1, 0) = n$, wird n von g eigentlich dargestellt. Sei $A_{g,f} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Dann ist $f(a, c) = n$. Diese Darstellung ist eine eigentliche, da aufgrund von $\det(A_{g,f}) = ad - bc = \pm 1$ gilt, dass $ggT(a, c) = 1$. □

1.9.1 Bemerkungen

- Eine Primzahl kann nur eigentlich dargestellt werden, denn $ggT(x, y)^2$ ist stets ein Teiler der dargestellten Zahl.
- Falls $2 \nmid n$ ist die Lösbarkeit von $x^2 \equiv D \pmod{4n}$ gleichwertig mit der Lösbarkeit von $x^2 \equiv D \pmod{n}$. Denn nach Bemerkung 1.7.2 ist stets $D \equiv 0, 1 \pmod 4$.

1.10 Beispiele

(*i*) Falls $D = -11$, so ist nach 1.8 $h(D) = 1$. Aber $x^2 \equiv -11 \pmod{4n}$ ist nicht lösbar für $n = 2$. Da 2 eine Primzahl ist, lässt sie sich nur eigentlich darstellen. Also lässt sich 2 überhaupt nicht durch eine positiv definite Form mit Diskriminante -11 darstellen.

(*ii*) $f(x, y) = x^2 + 2y^2$ hat Diskriminante $D = -8$. Also ist $D \equiv 0 \pmod 4$. f stellt die Primzahl p genau dann dar, wenn $x^2 \equiv -8 \pmod p$. Es sei denn $2|p$, also $p = 2$. Dann besitzt p aber die Darstellung $(0, 1)$. Also ist $p = 2$ oder -8 ist quadratischer Rest modulo p. Mit Hilfe des Legendre Symbols bedeutet dies: $\left(\frac{-8}{p}\right) = 1$ Aufgrund der Multiplikativität des Legendre Symbols gilt:

$$1 = \left(\frac{-8}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right)^2 = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$$

Es ist $p = 2$ oder $p \equiv 1, 3 \pmod 8$, denn für das Legendresymbol gilt:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ falls } p \equiv 1 \pmod 4 \\ -1 \text{ falls } p \equiv 3 \pmod 4. \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \text{ falls } p \equiv 1 \text{ oder } 7 \pmod 8 \\ -1 \text{ falls } p \equiv 3 \text{ oder } 5 \pmod 8. \end{cases}$$

(*iii*) Aus dem Beweis von 1.9 wird auch klar, dass $x^2 + 3y^2$ die Primzahl p höchstens dann darstellt, wenn $p \neq 2$ und $p \equiv 1 \pmod 3$. $x^2 + 3y^2$ hat zwar Diskriminante $D = -12$ und $h(-12) \neq 1$, aber für den ersten Teil des Beweises ist $h(D) = 1$ nicht notwendig. Es gilt also: Falls $p \neq 2$ durch f dargestellt wird, dann nach 1.9.1 nur eigentlich. Es folgt also, dass $\left(\frac{-12}{p}\right) = \left(\frac{p}{3}\right) = 1$ und somit $p \equiv 1 \pmod 3$. Tatsächlich ist es so, dass p genau dann darstellbar ist, wenn $p \equiv 1 \pmod 6$. (vgl. [But99])

(*iv*) Analog zu (*iii*) kann man sich fragen, welche Primzahlen p von einer der beiden Formen $x^2 + 3y^2$ oder $2x^2 + 2xy + 2y^2$ dargestellt werden. Offenbar sind beide Formen positiv definit (vgl. Satz 1.2.2), reduziert und haben Diskriminante -12. Demnach können sie nicht äquivalent sein. Außerdem ist $h(-12) = 2$. Also repräsentieren die beiden Formen alle Formen mit Diskriminante -12 und der Satz 1.9 kann in abgewandelter Form angewandt werden. Es gilt, dass $x^2 + 3y^2$ oder $2x^2 + 2xy + 2y^2$ die Primzahl p genau dann darstellt, wenn $p \neq 2$ und $p \equiv 1 \pmod 3$.

Literaturhinweis: Dieses Kapitel richtet sich im Wesentlichen nach [NZ76a]. In Auszügen auch [Zag81] und [Sch94].

2 Ordnungen und ganze Zahlen

2.1 Definition: Ganzheit

Es seien $R \subseteq R'$ Integritätsbereiche mit 1.
Ein Element $b \in R'$ heißt *ganz über* R, wenn ein normiertes Polynom $f \in R[x]$ existiert, sodass $f(b) = 0$. $f(b) = 0$ heißt *Ganzheitsgleichung* für b über R.

Das heißt, b ist Nullstelle eines normierten Polynoms mit Koeffizienten in R.

2.1.1 Bemerkung

$\alpha \in \mathbb{Q}$ ist ganz über $\mathbb{Z}$ genau dann, wenn $\alpha \in \mathbb{Z}$.

Beweis „⇒“ Es sei $\alpha = \frac{a}{b} \in \mathbb{Q}$ ganz über $\mathbb{Z}$ und $ggT(a,b) = 1$. Dann genügt $\frac{a}{b}$ der Gleichung:

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \ldots + c_1\frac{a}{b} + c_0 = 0$$
$$a^n + c_{n-1}a^{n-1}b + \ldots + c_1ab^{n-1} + c_0b^n = 0$$
$$b\left(c_{n-1}a^{n-1} + \ldots + c_1ab^{n-2} + c_0b^{n-1}\right) = -a^n$$

Also ist b ein Teiler von a^n und wegen $ggT(a,b) = 1$ auch ein Teiler von a. Hieraus folgt wieder wegen $ggT(a,b) = 1$, dass $b = \pm 1$ und somit $\alpha \in \mathbb{Z}$.
„⇐“ Wenn $\alpha \in \mathbb{Z}$, so ist es Nullstelle von $x - \alpha \in \mathbb{Z}[x]$ und somit ganz über $\mathbb{Z}$.

□

2.1.2 Bemerkung

Aus dem zweiten Teil des obigen Beweises wird auch klar, dass bei allen Integritätsbereichen $R \subseteq R'$ die Elemente aus R immer auch ganz über R sind.

2.1.3 Bemerkung

Sei R ein Unterring von R' und $b \in R'$.

- R' kann stets als R-Modul aufgefasst werden. Die skalare Multiplikation ist dabei die Multiplikation in R'.
- $R[b]$ ist der kleinste Unterring von R', der R und b enthält.

2.1.4 Satz

Es seien $R \subseteq R'$ Integritätsbereiche mit 1 und $b \in R'$. Folgende Aussagen sind dann äquivalent:

(*i*) b ist ganz über R.

(*ii*) $R[b]$ ist ein endlich erzeugter R-Modul.

(*iii*) $R[b]$ ist in einem Unterring S von R' enthalten, welcher endlich erzeugter R-Modul ist.

Beweis

(*i*) $\Rightarrow$ (*ii*) Für $i = 0, \ldots, n-1$ existieren $a_i \in R$, sodass:

$$b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0 \tag{7}$$

Es sei M der von $\{1, b, b^2, \ldots, b^{n-1}\}$ (endlich) erzeugte R-Untermodul von R'. Da $R[b]$ von den b^i für $i \geq 0$ erzeugt wird, reicht es zu zeigen, dass jedes dieser erzeugenden Elemente in M liegt. Für $i = 0, \ldots, n-1$ ist dies nach Definition klar. Aufgrund von (7) ist auch $b^n \in M$. Außerdem gilt folglich aber auch:

$$b^{n+j} = -a_{n-1}b^{n+j-1} - a_{n-2}b^{n+j-2} - \ldots - a_0 b^j$$

Das heißt mit $b^n \in M$ ist auch $b^{n+1} \in M$ und somit liegen nach Induktion über $j \in \mathbb{N}$ alle b^{n+j} in M. Offensichtlich ist damit $R[b] = M$ und somit endlich erzeugt.

(*ii*) $\Rightarrow$ (*iii*) Ist offensichtlich, wenn $S = R[b]$ gewählt wird.

(*iii*) $\Rightarrow$ (*i*) Es sei $\{s_1, \ldots, s_n\}$ eine endliche Basis von S als R-Modul. Da auch $b \in S$, ist $bs_i \in S$ für alle $i = 1 \ldots n$. Also können wir diese Elemente wieder als Linearkombination der erzeugenden s_i schreiben:

$$bs_i = \sum_{j=1}^{n} a_{i,j} s_j \qquad \text{f.a. } i = 1, \ldots, n \text{ mit } a_{i,j} \in R \text{ und } 1 \leq i, j \leq n$$

Daraus folgt, dass

$$0 = \left(\sum_{j=1}^{n} a_{i,j} s_j \right) - bs_i = \sum_{j=1}^{n} \left(a_{i,j} - \delta_{i,j} b \right) s_j \qquad \text{für } i = 1 \ldots n \text{ und } \delta_{i,j} = \begin{cases} 0 & \text{für } j \neq i \\ 1 & \text{für } i = j \end{cases}$$

Als Matrix geschrieben bedeutet das, dass:

$$\begin{pmatrix} a_{1,1}-b & a_{1,2} & a_{1,3} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2}-b & a_{2,3} & & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3}-b & & \vdots \\ & & & \ddots & a_{n-1,n} \\ a_{n,1} & a_{n,2} & \dots & a_{n,n-1} & a_{n,n}-b \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{n-1} \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$$

oder kürzer geschrieben $(A - bE_n)\, s = 0$. Da s eine Basis von S, also insbesondere $s \neq 0$, muss demnach $det\,(A - bE_n) = 0$ sein. $det\,(A - bE_n)$ ist gerade das charakteristische Polynom $p_A\,(b)$ von A. Der führende Koeffizient von p_A ist jedoch immer $(-1)^n$ und alle anderen Koeffizienten bilden sich aus den $a_{i,j} \in R$. Somit ist $p_A\,(b) = 0$ die Ganzheitsgleichung für b über R. □

2.1.5 Satz

Es seien $b_1, b_2, \dots, b_n \in R'$ ganz über R. Dann ist $R\,[b_1, b_2, \dots, b_n]$ ein endlich erzeugter R-Modul.

Beweis mittels vollständiger Induktion nach n.
Aus (2.1.4) weiß man, dass $R\,[b_1]$ endlich erzeugt ist. Sei nun $\{a_1, \dots, a_m\}$ ein Erzeugendensystem von $R\,[b_1, b_2, \dots, b_{n-1}]$. Da b_n ganz über R ist, ist es auch ganz über $R\,[b_1, b_2, \dots, b_{n-1}]$. $R\,[b_1, b_2, \dots, b_{n-1}]\,[b_n]$ ist dann über $R\,[b_1, b_2, \dots, b_{n-1}]$ erzeugt durch $1, b_n, \dots, b_n^k$ für ein geeignetes $k \in \mathbb{N}$. $R\,[b_1, b_2, \dots, b_{n-1}, b_n]$ wird dann von $a_i b_n^j$ erzeugt mit $i = 1, \dots, m$ und $j = 0, \dots k$. □

2.2 Definition: Ganze Hülle

Es sei $R \subseteq R'$ Integritätsbereich mit 1.
$M := \{b \in R' \mid b$ ganz über $R\ \}$ heißt *ganze Hülle* von R in R'.

2.2.1 Bemerkung

M ist ein Unterring von R'.

Beweis Seien $a, b \in M$. Dann sind $a - b$ und $ab \in R\,[a, b]$, also nach 2.1.5 in einem endlichen R-Modul enthalten. Nach Satz 2.1.4 sind sie also ganz und M ein Unterring von R' □

2.3 Definition: Ganz Abgeschlossen

Sei R ein Integritätsbereich mit 1 und $K = Q(R)$ der Quotientenkörper von R.
Dann heißt R *ganz abgeschlossen*, falls die ganze Hülle von R in K gleich R ist.

2.3.1 Satz

Jeder *ZPE*-Ring ist ganz abgeschlossen.

Beweis Der Satz 2.1.1 ist ein Spezialfall dieses Satzes mit $R = \mathbb{Z}$. Der Beweis geht allerdings vollkommen analog, da nur benutzt wurde, dass $\mathbb{Z}$ ein *ZPE*-Ring ist. □

2.3.2 Bemerkung

Für jede quadratische Körpererweiterung K von $\mathbb{Q}$ existiert ein quadratfreies d, sodass $K = \mathbb{Q}\left(\sqrt{d}\right)$ ist.
Denn da $[K : \mathbb{Q}] = 2$, ist für $\alpha \in K \setminus \mathbb{Q}$ das Minimalpolynom $\mathfrak{Irr}(\alpha, \mathbb{Q}) = x^2 + ax + b \in \mathbb{Q}[x]$. Also ist $\alpha = \frac{-a \pm \sqrt{a^2-4b}}{2}$ und $K = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{a^2-4b}\right)$. Jedes Quadrat in der Primfaktorzerlegung von $a^2 - 4b$ kann nun noch aus der Wurzel gezogen werden, und man erhält $K = \mathbb{Q}\left(\sqrt{d}\right)$ mit quadratfreiem d.

2.3.3 Satz

Sei $0, 1 \neq d \in \mathbb{Z}$ quadratfrei.

(*i*) Die ganze Hülle R von $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{d}\right)$ ist

$$R = \begin{cases} \left\{ \frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\} & \text{falls } d \equiv 1 \pmod 4 \\ \left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \right\} & \text{falls } d \equiv 2, 3 \pmod 4 \end{cases}$$

(*ii*) Es sei $\omega := \begin{cases} \frac{1+\sqrt{d}}{2} & \text{falls } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{falls } d \equiv 2, 3 \pmod 4 \end{cases}$

Dann ist $\{1, \omega\}$ eine $\mathbb{Z}$-Basis von R.

2.3.4 Hilfssatz

Es sei $\mathbb{Q} \subseteq K$ eine Körpererweiterung und $\alpha \in K$. Dann ist α genau dann ganz über $\mathbb{Z}$, wenn $\mathfrak{Irr}(\alpha, \mathbb{Q})$ Koeffizienten in $\mathbb{Z}$ besitzt.

Beweis Falls $\mathfrak{Irr}(\alpha, \mathbb{Q})$ ganzzahlige Koeffizienten besitzt, ist α auch Nullstelle eines Normierten Polynoms in $\mathbb{Z}[x]$ und somit ganz über $\mathbb{Z}$.
Falls α ganz über $\mathbb{Z}$, gibt es ein normiertes Polynom $f \in \mathbb{Z}[x]$, sodass $f(\alpha) = 0$. Jede der Nullstelle $\alpha_1, \ldots, \alpha_k$ von $\mathfrak{Irr}(\alpha, \mathbb{Q})$ ist als Nullstelle von $f(x)$ ganz über $\mathbb{Z}$. Die Koeffizienten des Minimalpolynoms sind alle in $\mathbb{Q}$, da aber $\mathfrak{Irr}(\alpha, \mathbb{Q})(x) = (x - \alpha_1) \ldots (x - \alpha_k)$, sind sie ganz über $\mathbb{Z}$. Nach 2.1.1 ist $\mathbb{Z}$ ganz abgeschlossen in $\mathbb{Q}$ und somit $\mathfrak{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$. □

Beweis von 2.3.3 Zu (i) sei

$$R' = \begin{cases} \left\{ \frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\} & \text{falls } d \equiv 1 \pmod 4 \\ \left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \right\} & \text{falls } d \equiv 2, 3 \pmod 4 \end{cases}$$

Dann ist zu zeigen, dass $R \subseteq R'$ und $R \supseteq R'$

„$\subseteq$“ Sei $\alpha \in R \subseteq \mathbb{Q}\left(\sqrt{d}\right)$. Dann hat es die Form $\alpha = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$.
Falls $b = 0$, ist a ganz über $\mathbb{Z}$ und nach 2.1.1 ist $a \in \mathbb{Z}$.
Falls $b \neq 0$, ist α Nullstelle des Polynoms $p(x) := (x - \alpha)(x - \overline{\alpha}) \in \mathbb{Q}[x]$. Hierbei ist $\overline{\alpha} := a - b\sqrt{d}$ das konjugierte Element zu α. $p(x)$ ist irreduziebel über $\mathbb{Q}$, da α,$\overline{\alpha} \notin \mathbb{Q}$ die Nullstellen sind. Somit ist $p(x)$ auch das Minimalpolynom von α. Denn α kann nicht Nullstelle eines linearen Polynoms sein. Nach 2.3.4 hat $p(x)$ also ganzzahlige Koeffizienten.

$$\begin{aligned} p(x) &= (x - \alpha)(x - \overline{\alpha}) \\ &= x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} \\ &= x^2 - 2ax + a^2 - db^2 \end{aligned}$$

$-2a$ und $a^2 - db^2$ sind demnach ganzzahlig.
Falls $a \in \mathbb{Z}$, so ist $db^2 \in \mathbb{Z}$ und da d quadratfrei ist, damit auch $b \in \mathbb{Z}$.
Falls nicht, ist $2a = a' \in \mathbb{Z}$ mit a' ungerade und somit $a = \frac{a'}{2}$. Dann ist $4a^2 = a'^2 \in \mathbb{Z}$ und somit muss gelten $4db^2 \in \mathbb{Z}$ und $db^2 \notin \mathbb{Z}$. Wir können b als gekürzten Bruch $\frac{b'}{q}$ schreiben mit $q > 1$ und erhalten aufgrund von $4d\frac{b'^2}{q^2} \in \mathbb{Z}$ und d quadratfrei, dass $q^2|4$ uns somit $q = 2$.
Man erhält also $a = \frac{a'}{2}$ und $b = \frac{b'}{2}$. Wegen $a^2 - b^2 d \in \mathbb{Z}$ gilt also:

$$\begin{aligned} 4a^2 - 4b^2 d &\equiv 0 && \pmod 4 \\ a'^2 - b'^2 d &\equiv 0 && \pmod 4 \\ (\pm 1) - (\pm 1)\, d &\equiv 0 && \pmod 4 \end{aligned}$$

Somit muss in diesem Fall $d \equiv 1 \pmod 4$ sein. Außerdem kann $d \equiv 0 \pmod 4$ nicht sein, da d quadratfrei ist. Der erste Fall tritt also ein, wenn $d \equiv 2, 3 \pmod 4$. Also ist $\alpha \in R'$.

„$\supseteq$“ Es sei nun $\alpha = a + b\sqrt{d} \in R'$ mit $a, b \in \mathbb{Z}$. Dann ist α Nullstelle von $p(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$.
Falls allerdings $\alpha = \frac{a+b\sqrt{d}}{2} \in R'$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \pmod 2$, so ist es Nullstelle von $p(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - ax + \frac{1}{4}(a^2 - db^2) \in \mathbb{Z}[x]$. Denn aufgrund von

$$\begin{aligned} a &\equiv b && \pmod 2 \\ a^2 &\equiv b^2 && \pmod 4 \\ a^2 - b^2 &\equiv 0 && \pmod 4 \\ a^2 - b^2 d &\equiv 0 && \pmod 4 \qquad \text{denn } d \equiv 1 \pmod 4 \end{aligned}$$

ist $\frac{a^2 - db^2}{4} \in \mathbb{Z}$.

(ii) folgt nach (i), da im ersten Fall $a \equiv b \pmod 2$ und somit $a = b + 2n$ mit $n \in \mathbb{Z}$, also $\frac{a+b\sqrt{d}}{2} = \frac{b+b\sqrt{d}}{2} + \frac{2n}{2} = b \cdot \frac{1+\sqrt{d}}{2} + n \cdot 1$ ist. Im zweiten Fall ist $a + b\sqrt{d}$ schon eine Linearkombination der Basiselemente. □

2.4 Definition: Ganze Zahlen

Es sei $\mathbb{Q} \subseteq K$ eine Körpererweiterung.
Die ganze Hülle R von $\mathbb{Z}$ in K heißt *Ring der ganzen Zahlen* von K. Die Elemente von R heißen *ganze Zahlen* von K.

2.5 Definition: Ordnungen

Sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung und R der Ring der ganzen Zahlen von K.
$\mathcal{O}$ heißt *Ordnung* von K, falls gilt:

(i) $\mathcal{O}$ ist ein Integritätsbereich mit 1.

(ii) $\mathcal{O} \subseteq R$

(iii) Für den Quotientenkörper von $\mathcal{O}$ gilt: $Q(\mathcal{O}) = K$

2.5.1 Satz

Es sei $\mathbb{Q} \subseteq K$ eine algebraische Körpererweiterung und R der Ring der ganzen Zahlen von K. Dann existiert für alle $\alpha \in K$ ein $a \in \mathbb{Z}$ so dass $a\alpha \in R$

Beweis Es sei also $\alpha \in K$. Dann ist es algebraisch und somit Nullstelle eines ohne Einschränkung normierten Polynoms $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Q}[x]$
Es sei $a \in \mathbb{Z}$ das kleinste gemeinsame Vielfache aller Nenner der a_i. Dann ist $a^n f \in \mathbb{Z}[x]$ mit $a\alpha$ als Nullstelle. Denn $a^n f(\alpha) = (a\alpha)^n + a a_{n-1}(a\alpha)^{n-1} + \ldots + a^{n-1}a_1(a\alpha) + a^n a_0 = 0$.
Somit ist $a\alpha \in R$. □

2.5.2 Satz

Es sei $\mathbb{Q} \subseteq K$ eine algebraische Körpererweiterung. Dann ist der Ring der ganzen Zahlen R eine Ordnung von K.

Beweis Die Bedingung (i) ist klar. Es ist also noch zu zeigen, dass $Q(R) = K$. Aber aufgrund von 2.5.1 existiert für alle $\alpha \in K$ ein $a \in R$ und ein $n \in \mathbb{Z} \subseteq R$, sodass $n\alpha = a \in R$ und somit $\alpha = \frac{a}{n} \in Q(R)$. □

2.5.3 Satz

Sei $0, 1 \neq d \in \mathbb{Z}$ quadratfrei. Wie in 2.3.3 sei $\{1, \omega\}$ eine $\mathbb{Z}$-Basis des Ringes R der ganzen Zahlen von $\mathbb{Q}\left(\sqrt{d}\right)$. Dann haben alle Ordnungen von K die Form:

$$\mathcal{O}_f := \{a + bf\omega \mid a, b \in \mathbb{Z}\} \qquad \text{für ein } f \in \mathbb{N}$$

Beweis Dass $\mathcal{O}_f$ wirklich eine Ordnung ist, sieht man analog zum Beweis von Satz 2.5.2. Sei also $\mathcal{O} \subseteq K$ eine beliebige Ordnung. Alle Elemente aus $\mathcal{O}$ haben die Form $\alpha = a + b\omega$ mit $a, b \in \mathbb{Z}$. Falls stets $b = 0$ gilt, ist $\mathcal{O} = \mathbb{Z}$ und somit $f = 0$. Sonst wähle man ein Element mit minimalem positivem b aus. Dies existiert, da mit α auch $-\alpha$ in $\mathcal{O}$ ist. Sei dieses Element nun $n + f\omega$. Für beliebiges $a + b\omega \in \mathcal{O}$ ist auch $b\omega \in \mathcal{O}$. Sei nun $b = mf + r$ mit $0 \leq r < f$. Dann ist wegen der Minimalität von f und $r\omega = (b - mf)\omega \in \mathcal{O}$ $r = 0$ und somit $f|b$. Es lässt sich also jedes Element aus $\mathcal{O}$ in der Form $a + bf\omega$ mit $a, b \in \mathbb{Z}$ darstellen. Demnach ist $\mathcal{O} = \mathcal{O}_f$. □

Literaturhinweis: Im Wesentlichen nach [Sch94]. In Auszügen auch [KP76], [Bc66] und [Sam71].

3 Einheiten in Ordnungen quadratischer Zahlkörper

3.1 Definition: Quadratische Zahlkörper

Ein *quadratischer Zahlkörper* ist eine Körpererweiterung K von $\mathbb{Q}$ mit Erweiterungsgrad zwei. Also $[K : \mathbb{Q}] = 2$.

Alle quadratischen Zahlkörper haben dann die Form $\mathbb{Q}\left(\sqrt{d}\right)$ für ein quadratfreies $d \in \mathbb{Z}$. Nach 2.5.3 haben alle Ordnungen dieser Zahlkörper die Form

$$\mathcal{O}_f := \{a + bf\omega \mid a, b \in \mathbb{Z}\} \quad \text{für ein} \quad f \in \mathbb{N} \quad \text{und} \quad \omega := \begin{cases} \frac{1+\sqrt{d}}{2} & \text{falls } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{falls } d \equiv 2, 3 \pmod 4 \end{cases}$$

3.2 Definition: Norm und Einheiten

$\varepsilon \in \mathcal{O}_f$ heißt *Einheit* in $\mathcal{O}_f$, falls es ein multiplikatives Inverses in $\mathcal{O}_f$ besitzt.
Für $\alpha = a + b\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right)$ ist $N(\alpha) := \alpha \cdot \overline{\alpha} = a^2 - b^2 d$ die *Norm* von α.

3.2.1 Satz

ε ist genau dann eine Einheit, wenn $N(\varepsilon) = \pm 1$.

Beweis Nach Definition ist die Norm multiplikativ und damit $1 = N(1) = N(\varepsilon\varepsilon^{-1}) = N(\varepsilon)\, N(\varepsilon^{-1})$. Also ist $N(\varepsilon) = \pm 1$. Falls $N(\varepsilon) = \pm 1$, ist $\varepsilon \cdot \overline{\varepsilon} = \pm 1$ und somit ist $\pm\varepsilon$ ein Inverses von ε.

Zur Bestimmung aller Einheiten $\mathcal{O}_f^*$ von $\mathcal{O}_f$ ist es nützlich, reelle und imaginäre Zahlkörper zu unterscheiden; das heißt die beiden Fälle $d > 0$ und $d < 0$.

3.3 Satz: Einheiten imaginärer Zahlkörper

Falls $d < 0$ quadratfrei ist, so ist die Einheitengruppe $\mathcal{O}_f^*$ von $\mathcal{O}_f$ gerade $\{\pm 1\}$.
Ausnahme ist lediglich $\mathcal{O}_1^*$ in den Fällen $d = -1$ bzw. $d = -3$. In diesen Fällen besteht $\mathcal{O}_1^*$ aus den vierten bzw. sechsten Einheitswurzeln.

Beweis Es sei $\varepsilon \in \mathcal{O}_f^*$. Dann ist $N(\varepsilon) = \pm 1$.
Es sei zunächst $d \equiv 1 \pmod 4$ und somit $\omega = \frac{1+\sqrt{d}}{2}$. ε lässt sich nun auf die Form $\varepsilon = \frac{a+bf\sqrt{d}}{2}$ mit $a, b \in \mathbb{Z}$ bringen. Es gilt dann:

$$N(\varepsilon) = \frac{a + bf\sqrt{d}}{2} \cdot \frac{a - bf\sqrt{d}}{2} = \frac{a^2 - b^2 f^2 d}{4} = \frac{a^2 + b^2 f^2 |d|}{4} = \pm 1$$

Falls $b = 0$, so ist $a = \pm 2$ und man erhält unabhängig von d die Einheiten $\varepsilon = \pm 1$.
Sei $b \neq 0$. Dann ist, falls $a = \pm 1$, $b^2 f^2 |d| = 3$ und somit $d = -3$, $f = 1$ und $b = \pm 1$.
$a = 0$ kann nicht sein, da wegen $a \equiv b \pmod 2$ sonst $b = \pm 2$ wäre und damit $d = -1 \not\equiv 1 \pmod 4$.
Für $d = -3$ erhält man also die Einheitengruppe $\mathcal{O}_1^* = \left\{\pm 1, \frac{1\pm\sqrt{-3}}{2}, -\frac{1\pm\sqrt{-3}}{2}\right\}$.

Falls nun $d \equiv 2, 3 \pmod 4$, so ist $\omega = \sqrt{d}$. Sei $\varepsilon = a + bf\sqrt{d} \in \mathcal{O}_f$ eine Einheit. Man erhält dann:

$$N(\varepsilon) = a^2 + b^2 f^2 |d| = \pm 1$$

Falls $b = 0$, so ist analog zu oben $\varepsilon = \pm 1$. Andernfalls muss $a = 0$ sein und $d = -1$, $f = 1$ und $b = \pm 1$. Für $d = -1$ erhält man also die Einheitengruppe $\mathcal{O}_1^* = \{\pm 1, \pm i\}$ Für alle anderen $d < 0$ ist damit $\mathcal{O}_f^* = \{\pm 1\}$. □

3.3.1 Bemerkung

Nach Satz 3.3 gibt es in imaginären quadratischen Zahlkörpern also stets nur endlich viele Einheiten. Da die Gleichung $N(\varepsilon) = \frac{a^2 - b^2 f^2 |d|}{4} = \pm 1$ unendlich viele Lösungen hat, ist die Bestimmung aller Einheiten im reellen Fall deutlich schwieriger. Im Folgenden wird man jedoch sehen, dass sich alle Einheiten bis auf Vorzeichen als Potenzen einer sogenannten Grundeinheit schreiben lassen. Um diese Grundeinheit zu bestimmen, ist es hilfreich, sich die Theorie der Kettenbrüche von Nutzen zu machen.

3.4 Kettenbrüche

Der folgende Abschnitt ist eine kurze Zusammenfassung der benötigten Resultate über Kettenbrüche. Ausführlichere Erläuterungen und Beweise sind zum Beispiel in [HW58] zu finden.

Für $a_1 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ mit $i = 2, \dots n$, ist der zugehörige *endliche Kettenbruch* $[a_1, a_2, a_3, \dots, a_n]$ folgendermaßen definiert

$$[a_1, a_2, a_3, \dots, a_n] := a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

Ein unendlicher Kettenbruch $[a_1, a_2, a_3, \dots]$ ist für $a_1 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ mit $i > 1$ als Grenzwert der endlichen Kettenbrüche $[a_1, a_2, a_3, \dots, a_n]$ definiert. Also

$$[a_1, a_2, a_3, \dots] := \lim_{n\to\infty} [a_1, a_2, a_3, \dots, a_n] \quad .$$

Tatsächlich existiert dieser Grenzwert immer. Die rationalen Zahlen werden dann genau von den endlichen Kettenbrüchen und die irrationalen Zahlen von den unendlichen Kettenbrüchen dargestellt. Unter den unendlichen Kettenbrüchen kann man noch zwischen den periodischen und den nicht periodischen Kettenbrüchen unterscheiden. Dabei sind *periodische Kettebrüche* solche, bei denen die Folge $(a_n)_{n\in\mathbb{N}}$ ab einem bestimmten Folgenglied periodisch wird. Genauer gesagt, falls ein $k \in \mathbb{N}_0$ und $l \in \mathbb{N}$ existiert, sodass $a_{k+l+i} = a_{k+i}$ für alle $i \in \mathbb{N}$ ist. Diese periodischen Kettenbrüche sind in dieser Arbeit von Interesse, da sie gerade alle quadratischen Irrationalzahlen darstellen.

Offenbar sind für beliebige Kettenbrüche und $a \in \mathbb{Z}$ folgende Umformungen möglich:

$$[a_1, a_2, a_3, \ldots] = a_1 + \frac{1}{[a_2, a_3, a_4, \ldots]}$$
$$a + [a_1, a_2, a_3, \ldots] = [a + a_1, a_2, a_3, \ldots]$$

Für die folgendermaßen rekursiv definierten Folgen p_n und q_n heißt $\frac{p_n}{q_n}$ der *n-te Näherungsbruch* von $\alpha = [a_1, a_n, \ldots]$.

$$p_{-1} := 0 \qquad p_0 := 1 \qquad p_n := p_{n-1}a_n + p_{n-2}$$
$$q_{-1} := 1 \qquad q_0 := 0 \qquad q_n := q_{n-1}a_n + q_{n-2}$$

Man kann mittels Induktion leicht sehen, dass $\frac{p_n}{q_n} = [a_1, a_2, a_3, \ldots, a_n]$ ist. Das heißt, dass $\lim\limits_{n\to\infty} \frac{p_n}{q_n} = [a_1, a_2, a_3, \ldots]$. Außerdem gilt $p_n q_{n-1} - p_{n-1}q_n = (-1)^{n+1}$.

Für ein $\alpha \in \mathbb{R}$ sei $[a_1, a_2, \ldots]$ die zugehörige Kettenbruchentwicklung. Dann heißt $\alpha_n := [a_n, a_{n+1}, \ldots]$ die *n-te Restzahl* von α. Es gilt dann, dass

$$\alpha_1 = \alpha \qquad \alpha_{n+1} = \frac{1}{\alpha_n - a_n} \qquad \text{und} \qquad a_n = \lfloor \alpha_n \rfloor \qquad \text{falls} \qquad \alpha_n \neq a_n \ .$$

Eine andere Darstellungsweise dieser Rekursion ist in Matrizenform. Hierzu definiert man

$$A_n := \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{und} \qquad P_n := A_1 A_2 \ldots A_n$$

Dann hat nach der Rekursionsformel für die Näherungsbrüche P_n die Form:

$$P_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \qquad \text{mit} \qquad \det(P_n) = (-1)^{n+1}$$

Analog zur Äquivalenz von Brüchen sei $\sim \subseteq \mathbb{R}^2 \times \mathbb{R}^2$ folgende Äquivalenzrelation:

$$\begin{pmatrix} a \\ b \end{pmatrix} \sim \begin{pmatrix} c \\ d \end{pmatrix} \quad \Longleftrightarrow \quad ad = bc$$

Mit den obigen Definitionen ergibt sich also:

$$\begin{pmatrix} \alpha_n \\ 1 \end{pmatrix} \sim A_n \begin{pmatrix} \alpha_{n+1} \\ 1 \end{pmatrix} = \begin{pmatrix} a_n \alpha_{n+1} + 1 \\ \alpha_{n+1} \end{pmatrix} \qquad \Longleftrightarrow \qquad \alpha_n = a_n + \frac{1}{\alpha_{n+1}}$$

somit gilt: $\begin{pmatrix} \alpha \\ 1 \end{pmatrix} \sim P_n \begin{pmatrix} \alpha_{n+1} \\ 1 \end{pmatrix}$.

Die Kettenbrüche werden als Hilfsmittel im Beweis von Satz 3.6 wieder verwendet. Zunächst noch weitere hilfreiche Definitionen.

3.5 Definitionen: Reduziertheit, Diskriminanten und Grundeinheiten

Sei $\alpha = a + b\,\omega, \varepsilon_0 \in \mathbb{Q}\left(\sqrt{d}\right)$ mit $a, b \in \mathbb{Z}$.

(*i*) α heißt *quadratische Irrationalzahl*, falls $\alpha \notin \mathbb{Q}$

(*ii*) $\overline{\alpha} := a - b\,\omega$ heißt *konjugiertes Element* zu α.

(*iii*) α heißt *reduziert*, falls $\alpha > 1$ und $-1 < \overline{\alpha} < 0$.

(*iv*) Sei $\mathfrak{Irr}\,(\alpha, \mathbb{Q})\,(x) = ax^2 + bx + c$. Dann heißt $D_\alpha = b^2 - 4ac$ *Diskriminante* von α.

(*v*) ε_0 heißt *Grundeinheit* von $\mathbb{Q}\left(\sqrt{d}\right)$, falls $\varepsilon_0 > 1$ und $\pm\varepsilon_0^n$ mit $n \in \mathbb{Z}$ alle Einheiten von $\mathbb{Q}\left(\sqrt{d}\right)$ sind

Man wird sehen, dass in reell quadratischen Zahlkörpern eine solche Grundeinheit immer existiert und zudem eindeutig bestimmt werden kann.

3.5.1 Bemerkung

$\alpha \in \mathbb{Q}\left(\sqrt{d}\right)$ ist genau dann reduziert, wenn der Kettenbruch zu α rein periodisch ist. Dabei heißt $\alpha = [a_1, a_2, \ldots]$ *rein periodisch*, falls ein $l \in \mathbb{N}$ existiert, sodass $a_{l+i} = a_i$ für alle $i \in \mathbb{N}$ ist. Falls l minimal ist mit dieser Eigenschaft, heißt l die *minimale Periodenlänge*.

3.5.2 Bemerkung

Für ω aus 2.3.3 gilt, dass

$$D := D_\omega = \begin{cases} d & \text{falls } d \equiv 1 \pmod 4 \\ 4d & \text{falls } d \equiv 2,3 \pmod 4 \end{cases}$$

Beweis

$$\mathfrak{Irr}\left(\omega, \mathbb{Q}\right)(x) = \begin{cases} x^2 + x + \frac{1-d}{4} & \text{falls } d \equiv 1 \pmod 4 \\ x^2 - d & \text{falls } d \equiv 2,3 \pmod 4 \end{cases}$$

□

3.5.3 Bemerkung

1. $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(\sqrt{D}\right)$
2. Ein Element $\alpha \in \mathbb{Q}\left(\sqrt{d}\right)$ ist genau dann in $\mathcal{O}_f$, wenn $\alpha = \frac{a+bf\sqrt{D}}{2}$ für $a, b \in \mathbb{Z}$ mit $a \equiv bfD \pmod 2$.

Beweis

1. Falls $d \equiv 1 \pmod 4$, ist die Behauptung nach 3.5.2 klar. Sonst ist $D = 4d$ und somit $2\sqrt{d} = \sqrt{D}$. Also ist $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(\sqrt{D}\right)$.
2. „⇒“ Sei $\alpha \in O_f$. Dann hat α nach 2.5.3 die Form $\alpha = a + bf\omega$ mit $a, b \in \mathbb{Z}$.
   1. Fall: $d \equiv 1 \pmod 4$. Dann ist $\omega = \frac{1+\sqrt{d}}{2}$ und somit:

$$\alpha = \frac{2a}{2} + \frac{bf + bf\sqrt{d}}{2} = \frac{2a + bf}{2} + \frac{bf\sqrt{d}}{2} = \frac{2a + bf}{2} + \frac{bf\sqrt{D}}{2}$$

   und $2a + bf \equiv bfD \pmod 2$. Denn $D \equiv 1 \pmod 2$ und $2a \equiv 0 \pmod 2$
   2. Fall: $d \equiv 2,3 \pmod 4$. Dann ist $\omega = \sqrt{d}$ und somit:

$$\alpha = \frac{2a}{2} + \frac{2bf\sqrt{d}}{2} = \frac{2a}{2} + \frac{bf\sqrt{4d}}{2} = \frac{2a}{2} + \frac{bf\sqrt{D}}{2}$$

   und $2a \equiv bfD \pmod 2$. Denn $D \equiv 2a \equiv 0 \pmod 2$.

   „⇐“ Sei $\alpha = \frac{a+bf\sqrt{D}}{2}$ mit $a \equiv bD \pmod 2$.
   1. Fall: $d \equiv 1 \pmod 4$. Dann ist $\omega = \frac{1+\sqrt{d}}{2}$ und somit:

$$\alpha = \frac{a}{2} + \frac{bf\sqrt{D}}{2} = \frac{a - bf}{2} + \frac{bf + bf\sqrt{D}}{2} = \frac{a - bf}{2} + \frac{bf\left(1 + \sqrt{d}\right)}{2} = \frac{a - bf}{2} + bf\omega$$

Also ist $\alpha \in O_f$, denn $a \equiv bf \pmod 2$ wegen $d \equiv 1 \pmod 2$

2. Fall: $d \equiv 2,3 \pmod 4$. Dann ist $\omega = \sqrt{d}$ und somit:

$$\alpha = \frac{a}{2} + \frac{bf\sqrt{D}}{2} = \frac{a}{2} + \frac{2bf\sqrt{d}}{2} = \frac{a}{2} + bf\omega$$

Also ist $\alpha \in O_f$, denn $a \equiv bfD \equiv 4bfd \equiv 0 \pmod 2$.

□

Im Folgenden soll $\mathbb{Q}\left(\sqrt{d}\right)$ stets ein reell quadratischer Zahlkörper sein. Das heißt $d \neq 0, 1$ ist positiv und quadratfrei.

3.6 Satz: Einheiten reeller Zahlkörper

Es sei $\mathcal{O}_f$ eine Ordnung von $\mathbb{Q}\left(\sqrt{d}\right)$. $\alpha \in \mathbb{Q}\left(\sqrt{d}\right)$ sei reduziert mit Diskriminante $D_\alpha = f^2 D$ und $[\overline{a_1, a_2, \ldots, a_k}]$ die Kettenbruchentwicklung von α mit minimaler Periodenlänge $k \in \mathbb{N}$. Dann ist $\varepsilon_0 := q_k\alpha + q_{k-1}$ die Grundeinheit von $\mathcal{O}_f$. Das heißt:

$$\mathcal{O}_f^* = \{\pm\varepsilon_0^n \mid n \in \mathbb{Z}\}$$

Zur besseren Übersicht wird der Beweis dieses Satzes in vier Teile geteilt.

Lemma 1

Es sei $\mathcal{O}_f$ eine Ordnung von $\mathbb{Q}\left(\sqrt{d}\right)$. Dann ist $\alpha := \frac{1}{f\omega - \lfloor f\omega \rfloor}$ als erste Restzahl von $f\omega$ reduziert.

Beweis Es gilt:

$$-1 < \overline{\alpha} < 0 \quad \Longleftrightarrow \quad -\frac{1}{\overline{\alpha}} > 1$$

Da $d \in \mathbb{N}$ mit $d \neq 0, 1$ ist, ist $\sqrt{d} > 1$ und damit auch

$$\omega := \begin{cases} \frac{1+\sqrt{d}}{2} > 1 & \text{falls } d \equiv 1 \pmod 4 \\ \sqrt{d} > 1 & \text{falls } d \equiv 2,3 \pmod 4 \end{cases}$$

Da $\sqrt{d} \notin \mathbb{N}$, ist auch ω und $f\omega \notin \mathbb{N}$ und somit $0 < f\omega - \lfloor f\omega \rfloor < 1$. Damit gilt $\alpha > 1$. Für $\overline{\alpha}$ gilt dann:

$$\begin{aligned} -\frac{1}{\overline{\alpha}} &= \overline{\lfloor f\omega \rfloor - f\omega} = \lfloor f\omega \rfloor - f\overline{\omega} \\ &\geq f\lfloor \omega \rfloor - f\overline{\omega} > f\lfloor \omega \rfloor \geq f \geq 1 \end{aligned}$$

□

Lemma 2

Für eine quadratische Irrationalzahl $\alpha \in \mathbb{Q}\left(\sqrt{d}\right)$ mit Diskriminante D hat auch jede Restzahl α_n die Diskriminante D.

Beweis Sei $a, b, c \in \mathbb{Z}$ mit $D = b^2 - 4ac$, sodass $a\alpha^2 + b\alpha + c = 0$ gilt. Dann ist:

$$\alpha = a_1 + \frac{1}{\alpha_2}$$

also auch:

$$a\left(a_1 + \frac{1}{\alpha_2}\right)^2 + b\left(a_1 + \frac{1}{\alpha_2}\right) + c = 0$$

und somit:

$$\left(aa_1^2 + ba_1 + c\right)\alpha_2^2 + \left(b + 2aa_1\right)\alpha_2 + a = 0$$

Berechnet man nun hier die Determinante von α_2, so ergibt dies:

$$\left(b + 2aa_1\right)^2 - 4a\left(aa_1^2 + ba_1 + c\right) = b^2 - 4ac = D$$

Analog kann man so induktiv $D_\alpha = D_{\alpha_n}$ zeigen. □

Lemma 3

Unter den Voraussetzungen von 3.6 ist $\varepsilon_0 := q_k\alpha + q_{k-1}$ eine Einheit in $\mathcal{O}_f$.
Außerdem ist $\varepsilon_0 > 1$.

Beweis Da α reduziert ist, ist nach 3.5.1 die Kettenbruchentwicklung rein periodisch. Somit ist $\alpha = \alpha_1 = \alpha_{k+1}$. Nach 3.4 gilt

$$\begin{pmatrix}\alpha\\1\end{pmatrix} \sim P_n \begin{pmatrix}\alpha_{n+1}\\1\end{pmatrix} = P_n \begin{pmatrix}\alpha\\1\end{pmatrix}$$

Mit $\varepsilon_0 := q_k\alpha + q_{k-1}$ ergibt sich dann:

$$\varepsilon_0 \begin{pmatrix}\alpha\\1\end{pmatrix} = \begin{pmatrix}\alpha\left(q_k\alpha + q_{k-1}\right)\\q_k\alpha + q_{k-1}\end{pmatrix} = \begin{pmatrix}p_k\alpha + p_{k-1}\\q_k\alpha + q_{k-1}\end{pmatrix} = \begin{pmatrix}p_n & p_{n-1}\\q_n & q_{n-1}\end{pmatrix}\begin{pmatrix}\alpha\\1\end{pmatrix} = P_n\begin{pmatrix}\alpha\\1\end{pmatrix}$$

$$\text{Hierbei wird} \quad \alpha = \frac{p_k\alpha_k + p_{k-1}}{q_k\alpha_k + q_{k-1}} = \frac{p_k\alpha + p_{k-1}}{q_k\alpha + q_{k-1}} \text{ verwendet}$$

Also ist $(P_k - \varepsilon_0 E)\begin{pmatrix}\alpha\\1\end{pmatrix} = 0$ und somit auch

$$\det(P_k - \varepsilon_0 E) = \varepsilon_0^2 - Spur(P_k)\,\varepsilon_0 + \det(P_k) = 0 \tag{8}$$

Da $\alpha \notin \mathbb{Q}$, ist auch $\varepsilon_0 \notin \mathbb{Q}$ und somit $\mathfrak{Irr}(\varepsilon_0, \mathbb{Q})(x) = x^2 + (\varepsilon_0 + \overline{\varepsilon_0})\,x + \varepsilon_0\overline{\varepsilon_0}$. Da aber das Polynom aus (8) auch normiert ist, Grad 2 und ε_0 als Nullstelle hat, muss es mit $\mathfrak{Irr}(\varepsilon_0, \mathbb{Q})$ übereinstimmen.
Wegen $\det(P_k) = (-1)^{k+1}$ ist also $N(\varepsilon_0) = \varepsilon_0\overline{\varepsilon_0} = \pm 1$. Nach 3.2.1 ist ε_0 somit eine Einheit. Außerdem hat $\mathfrak{Irr}(\varepsilon_0, \mathbb{Q})$ damit ganzzahlige Koeffizienten und nach Hilfssatz 2.3.4 ist damit ε_0 ganz, also $\varepsilon_0 \in \mathcal{O}$. Nun bleibt zu zeigen, dass $\varepsilon_0 \in \mathcal{O}_f$.

$$\text{Aus} \quad \alpha = \frac{p_k\alpha + p_{k-1}}{q_k\alpha + q_{k-1}} \quad \text{folgt} \quad q_k\alpha^2 + (q_{k-1} - p_k)\,\alpha - p_{k-1} = 0\ .$$

Dies nach α aufgelöst ergibt:

$$\alpha = \frac{p_k - q_{k-1} \pm \sqrt{(p_k - q_{k-1})^2 + 4q_kp_{k-1}}}{2q_k}$$

Allerdings ist $p_k - q_{k-1} - \sqrt{(p_k - q_{k-1})^2 + 4q_kp_{k-1}} < 0$. Oben tritt also $+$ auf. Nach Voraussetzung ist $D_\alpha = f^2D$. Um unter der Wurzel wirklich f^2D stehen zu haben, muss man noch den größtmöglichen Faktor von $(p_k - q_{k-1})^2 + 4q_kp_{k-1}$ aus der Wurzel ziehen. Mit $t := ggT(p_{k-1}, q_k, q_{k-1} - p_k)$ ergibt sich dann:

$$\alpha = \frac{p_k - q_{k-1}}{2q_k} + \frac{t}{2q_k}\sqrt{f^2D}$$

Dies in die Definition von ε_0 eingesetzt ergibt:

$$\begin{aligned}\varepsilon_0 = q_k\alpha + q_{k-1} &= q_k\left(\frac{p_k - q_{k-1}}{2q_k} + \frac{tf}{2q_k}\sqrt{D}\right) + q_{k-1}\\ &= \frac{p_k + q_{k-1}}{2} + \frac{tf}{2}\sqrt{D}\end{aligned}$$

Falls $d \equiv 1 \pmod 4$, so ist $\omega = \frac{1+\sqrt{d}}{2}$ und $D = d$. ε_0 ist ganz und somit muss nach Satz 2.3.3 $p_k + q_{k-1} \equiv tf \pmod 2$ und somit auch $\frac{p_k+q_{k-1}-tf}{2} \in \mathbb{Z}$ gelten. Dann ist aber

$$\varepsilon_0 = \frac{p_k + q_{k-1}}{2} + \frac{tf}{2}\sqrt{d} = \frac{p_k + q_{k-1} - tf}{2} + tf\frac{1+\sqrt{d}}{2} \in \mathcal{O}_f$$

Falls $d \equiv 2,3 \pmod 4$, so ist $\omega = \sqrt{d}$ und $D = 4d$. Also:

$$\varepsilon_0 = \frac{p_k + q_{k-1}}{2} + \frac{tf}{2}\sqrt{D} = \frac{p_k + q_{k-1}}{2} + \frac{2tf}{2}\sqrt{d} = \frac{p_k + q_{k-1}}{2} + tf\sqrt{d} \in \mathcal{O}_f$$

Bleibt noch zu zeigen, dass $\varepsilon_0 > 0$. Da α jedoch reduziert ist, ist $\alpha > 1$ und für $k \geq 1$ ist $q_k \geq 1$ und $q_{k-1} \geq 0$. Also ist $\varepsilon_0 = q_k\alpha + q_{k-1} \geq \alpha > 1$. □

Lemma 4

Es sei $\mathcal{O}_f$ eine Ordnung von $\mathbb{Q}\left(\sqrt{d}\right)$ und $\varepsilon \in \mathcal{O}_f^*$ mit $\varepsilon > 1$. Dann gilt $\varepsilon = \varepsilon_0^n$ für ein $n \in \mathbb{N}$. Dabei sei ε_0 wie in 3.6 definiert.

Beweis Ziel ist es, einen Kettenbruch $[c_1, c_2, \ldots, c_s]$ zu finden, sodass die in 3.4 definierten zugehörigen Matrizen C_i folgendes erfüllen. $P := C_1C_2 \ldots C_s$ genügt der Gleichung

$$\varepsilon \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = P \begin{pmatrix} \alpha \\ 1 \end{pmatrix} \tag{9}$$

Denn dann gilt für $\alpha' := [c_1, \ldots, c_s, \alpha]$

$$\begin{pmatrix} \alpha' \\ 1 \end{pmatrix} \sim P \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \varepsilon \begin{pmatrix} \alpha \\ 1 \end{pmatrix} \sim \begin{pmatrix} \alpha \\ 1 \end{pmatrix}$$

Und somit folgt $\alpha' = \alpha$. Da k die Länge der minimalen Periode ist, ist damit $s = hk$ mit $h \in \mathbb{N}$. Also ist $P = A_1 \ldots A_k \; A_1 \ldots A_k \; \ldots \; A_1 \ldots A_k = P_k^h$. Somit gilt:

$$\varepsilon \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = P_k^h \begin{pmatrix} \alpha \\ 1 \end{pmatrix} \quad \text{und} \quad \varepsilon_0 \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = (q_{k+1}\alpha + q_k) \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = P_k \begin{pmatrix} \alpha \\ 1 \end{pmatrix}$$

Beim Potenzieren der rechten Gleichung mit h ergibt sich, dass $\varepsilon = \varepsilon_0^h$.
Außerdem gilt für ein P, das die Gleichung (9) erfüllt, dass $\det(P) = N(\varepsilon)$.
Dies ergibt sich aus dem Beweis von Lemma 3.

Sei nun $\varepsilon = \frac{u+vf\sqrt{D}}{2}$ mit $u \equiv vfD \pmod 2$ und $a, b, c \in \mathbb{Z}$ sodass

$$a\alpha^2 + b\alpha + c = 0 \tag{10}$$

Solche Zahlen a, b, c existieren, da α algebraisch vom Grad 2 ist. Ohne Einschränkung sei $a > 0$ und $ggT(a, b, c) = 1$. Da $\alpha \notin \mathbb{Q}$, ist auch $a\alpha \notin \mathbb{Q}$ und somit wegen (10)

$$\mathfrak{Irr}(a\alpha, \mathbb{Q})(x) = x^2 + bx + ac$$

Aber offensichtlich ist $\mathfrak{Irr}(a\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$ und damit ist nach 2.3.4 $a\alpha$ ganz. Aufgrund von (10) und $a\alpha > 0$ gilt:

$$a\alpha = \frac{b}{2} + \frac{f\sqrt{D}}{2} \tag{11}$$

Denn nach Voraussetzung war die Diskriminante $D_\alpha = f^2 D$. Nun ist $a\alpha$ aber ganz und somit $b \equiv fD \pmod 2$. Zusammen mit $u \equiv vfD \pmod 2$ ergibt dies $u \equiv vb \pmod 2$. Mit

$$p := \frac{u + bv}{2} \qquad p^* := cv \qquad q := av \qquad q^* := \frac{u - bv}{2}$$

ist $P := \begin{pmatrix} p & p^* \\ q & q^* \end{pmatrix}$ dann eine ganzzahlige Matrix. Insbesondere ist es aber die oben gesuchte Matrix P. Dazu ist zu überprüfen ob

$$\varepsilon \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = P \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} p & p^* \\ q & q^* \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{u+bv}{2} & cv \\ av & \frac{u-bv}{2} \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix}$$

In der ersten Komponente bedeutet dies:

$$\begin{aligned}
& \frac{u + bv}{2}\alpha + cv = \frac{u + vf\sqrt{D}}{2}\alpha \\
\iff \quad & c = \left(\frac{f\sqrt{D}}{2} - \frac{b}{2}\right)\alpha \\
\iff \quad & 4ac = 4a\alpha\left(\frac{f\sqrt{D}}{2} - \frac{b}{2}\right) \overset{(11)}{=} 2\left(b + f\sqrt{D}\right)\left(\frac{f\sqrt{D} - b}{2}\right) \\
\iff \quad & 4ac = f^2 D - b^2 \\
\iff \quad & Df^2 = b^2 + 4ac = D_\alpha
\end{aligned}$$

Und in der zweiten Komponente:

$$\begin{aligned}
& av\alpha + \frac{u + bv}{2} = \frac{u + vf\sqrt{D}}{2} \\
\iff \quad & a\alpha + \frac{u - bv}{2} = \frac{f\sqrt{D}}{2} \\
\iff \quad & a\alpha = \frac{b}{2} + \frac{f\sqrt{D}}{2}
\end{aligned}$$

Dies gilt wegen (11). Nun ist noch zu zeigen, dass P die Form $C_1 \dots C_s$ hat.
Hierfür braucht man zunächst folgende Abschätzungen: Wegen (11) gilt $\alpha = \frac{b+f\sqrt{D}}{2a}$.

Außerdem ist α reduziert und deshalb gilt

$$\begin{aligned} b + f\sqrt{D} &> 2a \\ 0 < f\sqrt{D} - b &< 2a \end{aligned} \tag{12}$$

Daraus folgt, dass:

$$b - 2a > -f\sqrt{D} \tag{13}$$

$$b + 2a > f\sqrt{D} \tag{14}$$

Außerdem ist (12) äquivalent zu $b - f\sqrt{D} > -2a$ mit $b < f\sqrt{D}$.
Also ist auch $2b = b + f\sqrt{D} + b - f\sqrt{D} > 2a - 2a = 0$. Zusammen ergibt sich:

$$0 < b < f\sqrt{D} \tag{15}$$

Da $\varepsilon > 1$, gilt:

$$q^* = \frac{u - vb}{2} \overset{(15)}{>} \frac{u - vf\sqrt{D}}{2} = \overline{\varepsilon} = \frac{N(\varepsilon)}{\varepsilon} > \begin{cases} 0 & \text{falls } N(\varepsilon) = 1 \\ -1 & \text{falls } N(\varepsilon) = -1 \end{cases}$$

$$q - q^* = \frac{u + (b + 2a)\, v}{2} \overset{(14)}{>} \frac{-u + vf\sqrt{D}}{2} = -\overline{\varepsilon} > \begin{cases} -1 & \text{falls } N(\varepsilon) = 1 \\ 0 & \text{falls } N(\varepsilon) = -1 \end{cases}$$

$$p - q = \frac{u - (b - 2a)\, v}{2} \overset{(13)}{>} \frac{u - vf\sqrt{D}}{2} = \overline{\varepsilon} > \begin{cases} 0 & \text{falls } N(\varepsilon) = 1 \\ -1 & \text{falls } N(\varepsilon) = -1 \end{cases}$$

Diese drei Gleichungen ergeben:

$$0 < q^* \leq q \quad \text{und} \quad \frac{p}{q} > 1 \quad \text{für } N(\varepsilon) = 1 \tag{16}$$

$$0 \leq q^* < q \quad \text{und} \quad \frac{p}{q} \geq 1 \quad \text{für } N(\varepsilon) = -1 \tag{17}$$

Nun werden $c_1, \ldots, c_s$ definiert. 1. Fall: $\frac{p}{q} = 1$. Dann ist $N(\varepsilon) = -1$. Man setze $c_0 = 1$ und $s = 0$. Dann ist $p = q = q^* = 1$, $q^* = 0$ und $N(\varepsilon) = \det(P) = -1$

2. Fall: $\frac{p}{q} > 1$. Sei $[b_1, \ldots, b_t]$ der endliche Kettenbruch zu $\frac{p}{q}$. Dann ist $[b_1, \ldots, b_t] = [b_1, \ldots, b_t - 1, 1]$. Denn:

$$[x, y] = x + \frac{1}{y} = x + \frac{1}{y - 1 + \frac{1}{1}} = [x, y - 1, 1]$$

Falls nun $N(\varepsilon) = (-1)^t$, so setze man $s = t$ und $c_i = b_i$ für $i = 1, \ldots, s$.

Falls nun $N(\varepsilon) = (-1)^{t+1}$, so setze man $s = t+1$ und $c_i = b_i$ für $i = 1, \ldots, s-1$, $c_s = b_s - 1$ und $c_{s+1} = 1$.
Dann gilt stets $N(\varepsilon) = (-1)^t$. Sei $\frac{p_i}{q_i}$ der zu $\frac{p}{q}$ gehörende i-te Näherungsbruch. Es gilt:

$$P_t = \begin{pmatrix} p_t & p_{t-1} \\ q_t & q_{t-1} \end{pmatrix} = C_0 \ldots C_t$$

Nun ist also $P_t = P$ zu zeigen.

Es ist $\frac{p}{q} = \frac{p_t}{q_t}$. Da beide Brüche gekürzt sind und wegen (16) und (17) p und q positiv sind, ist $p = p_t$ und $q = q_t$. Nun gilt:

$$\det(P) = pq^* - p^*q = (-1)^t$$

$$\det(P_t) = p_t q_{t-1} - p_{t-1} q_t = (-1)^t$$

Also ergibt sich:

$$\begin{aligned} & p_t q_{t-1} - p_{t-1} q_t = pq^* - p^*q \\ \Longrightarrow \quad & p(q_{t-1} - q^*) = q(p_{t-1} - q^*) \\ \Longrightarrow \quad & q \mid (q_{t-1} - q^*) \end{aligned} \tag{18}$$

Nun sind drei Fälle zu unterscheiden.

1. Fall: In (17) gilt $0 < q^* < q$. Dann gilt wegen $0 < q_{t-1} \leq q_t = q$, dass: $|q^* - q_{t-1}| \leq |q^* - q| \leq q - 1 < q$. Da aber $q \mid (q_{t-1} - q^*)$ gilt, ist $|q^* - q_{t-1}| = 0$ und somit $q^* = q_{t-1}$. Wegen (18) gilt dann auch $p^* = p_{t-1}$.

2. Fall: In (17) gilt $0 < q^* = q$. Dann ist $1 = N(\varepsilon) = pq - p^*q = (p - p^*)q$. Wegen (16) und (17) sind p und q positiv und deshalb $q = q^* = 1$. Damit aber auch $\frac{p}{q} = p = \lfloor p \rfloor$. Daraus ergibt sich $t = 1$ und $q_0 = 1 = q^*$. Damit gilt aber auch $p_{t-1} = p^* = 1$.

3. Fall: In (17) gilt $0 = q^* \leq q$. Dann ist $-1 = N(\varepsilon) = -p^*q$. Somit ist $q = 1$ und wieder $\frac{p}{q} = p = \lfloor p \rfloor$. Daraus ergibt sich $t = 1$ und $q_0 = 0$. Damit gilt aber auch $p_{t-1} = p^* = 1$.Insgesamt ist also $P_t = P$. Wie zu Beginn erklärt, folgt daraus, dass $\varepsilon = \varepsilon_0^h$ mit $h \in \mathbb{N}$. Aus 3.5.2 ergibt sich, dass die Diskriminante von $f\omega$ gleich $f^2 D$ ist. Da α gerade der erste Näherungsbruch von $f\omega$ ist, hat es nach Lemma 2 dieselbe Diskriminante und erfüllt damit alle Voraussetzungen von Satz 3.6. □

Beweis von 3.6 Zunächst braucht man Lemma 1, um die Existenz eines reduzierten Elements α nachzuweisen. Dieses α ist gerade der erste Näherungsbruch von $f\omega$. Aus 3.5.2 wird klar, dass $D_{f\omega} = f^2 D$. Da $f\omega$ eine quadratische Irrationalzahl ist, hat nach Lemma 2 auch α die Diskriminante $f^2 D$. Also erfüllt das in Lemma 1 definierte α alle Voraussetzungen von Satz 3.6. Nach Lemma 3 weiß man dann, dass $\varepsilon_0 \in \mathcal{O}_f^*$. Mit Lemma 4 gilt für jedes beliebige $\varepsilon \in \mathcal{O}_f^*$ mit $\varepsilon > 1$, dass $\varepsilon = \varepsilon_0^n$ für ein $n \in \mathbb{N}$ ist. Somit gilt für jedes beliebige $\varepsilon \in \mathcal{O}_f^*$, dass $\varepsilon = \pm\varepsilon_0^n$ mit $n \in \mathbb{Z}$.

Dieses ε_0 ist eindeutig. Denn, falls es verschiedene ε_0 und ε_1 mit dieser Eigenschaft gibt, ist ohne Einschränkung $\varepsilon_0 < \varepsilon_1$. Da ε_0 eine Grundeinheit ist, müsste es aber wegen $1 < \varepsilon_0$ ein $n \in \mathbb{N}$ geben, sodass $\varepsilon_1^n = \varepsilon_0$. Dies kann jedoch wegen $\varepsilon_0 < \varepsilon_1$ nicht sein. Also ist ε_0 die eindeutig bestimmt Grundeinheit von $\mathcal{O}_f$ und $\mathcal{O}_f^* = \{\pm\varepsilon_0^n \mid n \in \mathbb{Z}\}$ □

3.7 Beispiele

Beispiel 1 Bestimmung der Einheiten $\mathcal{O}_3^*$ von $\mathbb{Q}\left(\sqrt{6}\right)$. Da $6 \equiv 2 \pmod 4$, ist $\omega = \sqrt{6}$ und $f\omega = 3\sqrt{6} = \sqrt{54}$. Also ist $\alpha = \frac{1}{\sqrt{54}-\lfloor\sqrt{54}\rfloor} = \frac{1}{\sqrt{54}-7}$.
Nun muss man die (rein periodische) Kettenbruchentwicklung von α berechnen. Dazu berechnet man den ganzen Teil $a_1 := \lfloor\alpha_1\rfloor$ und setzt $\alpha_2 = \frac{1}{\alpha_1 - \lfloor\alpha_1\rfloor}$. Dies wiederholt man, bis zum ersten Mal $\alpha_1 = \alpha_{k+1}$ für ein $k \in \mathbb{N}$ ist. Die minimale Periodenlänge ist dann k.

$$\begin{aligned}
\alpha_1 &= \frac{1}{\sqrt{54}-7} = \frac{\sqrt{54}+7}{5} = 2 + \frac{\sqrt{54}-3}{5} \\
\alpha_2 &= \frac{5}{\sqrt{54}-3} = \frac{\sqrt{54}+3}{9} = 1 + \frac{\sqrt{54}-6}{9} \\
\alpha_3 &= \frac{9}{\sqrt{54}-6} = \frac{\sqrt{54}+6}{2} = 6 + \frac{\sqrt{54}-6}{2} \\
\alpha_4 &= \frac{2}{\sqrt{54}-6} = \frac{\sqrt{54}+6}{9} = 1 + \frac{\sqrt{54}-3}{9} \\
\alpha_5 &= \frac{9}{\sqrt{54}-3} = \frac{\sqrt{54}+3}{5} = 2 + \frac{\sqrt{54}-7}{5} \\
\alpha_6 &= \frac{5}{\sqrt{54}-7} = \frac{\sqrt{54}+7}{1} = 14 + \frac{\sqrt{54}-7}{1}
\end{aligned}$$

Wie man sieht, wird der Kettenbruch hier periodisch mit $k = 6$, $\frac{1}{\sqrt{54}-7} = \overline{[2,1,6,1,2,14]}$ und nach 3.4: $q_1 = 1$, $q_2 = 1$, $q_3 = 7$, $q_4 = 8$, $q_5 = 23$ und $q_6 = 330$.
Die Grundeinheit von $\mathcal{O}_3^*$ ist, wie in Satz 3.6 bewiesen, also $\varepsilon_0 = 330\alpha + 23 = 485 + 198\sqrt{6}$ mit $N(\varepsilon_0) = 485^2 - 198^2 \cdot 6 = 1$.
Es ist also $\mathcal{O}_3^* = \left\{ \pm\left(485 + 198\sqrt{6}\right)^n \middle| \text{ mit } n \in \mathbb{Z} \right\}$. (vgl. [Bc66, Seite 152])

Beispiel 2 Bestimmung der Einheiten $\mathcal{O}_1^*$ von $\mathbb{Q}\left(\sqrt{5}\right)$.
Da $5 \equiv 1 \pmod 4$, ist $f\omega = \omega = \frac{1+\sqrt{5}}{2}$ (der goldene Schnitt).
Dann ist

$$\alpha = \frac{1}{\frac{1+\sqrt{5}}{2} - \left\lfloor \frac{1+\sqrt{5}}{2} \right\rfloor} = \frac{1}{\frac{1+\sqrt{5}}{2} - 1} = \frac{2}{\sqrt{5}-1} = \frac{1+\sqrt{5}}{2} \quad .$$

Der erste Näherungsbruch α von $f\omega$ ist also wieder $f\omega$. Außerdem ist $\left\lfloor \frac{1+\sqrt{5}}{2} \right\rfloor = 1$. Demnach muss $k = 1$ und $\frac{1+\sqrt{5}}{2} = [\overline{1}]$ sein.
Die Grundeinheit ist dann $\varepsilon_0 = q_1\alpha + q_0 = \frac{1+\sqrt{5}}{2}$ mit $N(\varepsilon_0) = -1$.

$$\mathcal{O}_1^* = \left\{ \pm \left(\frac{1+\sqrt{5}}{2} \right)^n \,\middle|\, \text{mit } n \in \mathbb{Z} \right\}$$

Literaturhinweis: Hauptsächlich nach [KP76]. In Auszügen auch [Bc66] und [NZ76b]. Die Kettenbruchtheorie ist nach [HW58].

4 Darstellung ganzer Zahlen durch ganzzahlige binäre quadratische Formen

Dieses Kapitel enthält nun das Hauptresultat dieser Arbeit, nämlich welche Lösungen $x, y \in \mathbb{Z}$ Gleichungen der Form $ax^2 + bxy + cy^2 = n$ mit $a, b, c \in \mathbb{Z}$ besitzen. Man wird jedoch sehen, dass es hierzu äquivalent ist, Elemente einer Ordnung mit einer vorgegebenen Norm zu bestimmen. Zunächst einmal kann man, um ganzzahlige Lösungen von $ax^2 + bxy + cy^2 = n$ zu finden, davon ausgehen, dass $t := ggT(a, b, c) = 1$. Denn sonst betrachtet man die äquivalente Gleichung $\frac{a}{t}x^2 + \frac{b}{t}xy + \frac{c}{t}y^2 = \frac{n}{t}$. Hierbei fällt schon auf, dass falls $ggT(a, b, c) \nmid n$, es keine Lösungen $x, y \in \mathbb{Z}$ geben kann. Um den Zusammenhang der Gleichung $ax^2 + bxy + cy^2 = n$ zu Gleichungen der Form $N(\gamma) = r$ herzustellen, ist es notwendig, solche binären quadratischen Formen zu faktorisieren. Dies ist in einem quadratischen Zahlkörpern folgendermaßen möglich:

$$f(x, y) = ax^2 + bxy + cy^2 = a(x - \alpha y)(x - \overline{\alpha} y)$$

α und $\overline{\alpha}$ sind nun Elemente des quadratischen Zahlkörpers $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$. Genauer gesagt, sind es die gegebenenfalls komplexen Nullstellen von

$$f(z) = az^2 + bz + c \quad . \tag{19}$$

Damit α wirklich eine quadratische Irrationalzahl ist, darf $D = b^2 - 4ac$ kein Quadrat in $\mathbb{Q}$ sein. Sonst ist nämlich $\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{D}}{2a} \in \mathbb{Q}$. Sei also, wie schon zu Anfang der Arbeit erwähnt, D kein Quadrat in $\mathbb{Q}$. Für die Norm von $(x - \alpha y)$ gilt dann:

$$N(x - \alpha y) = (x - \alpha y)(x - \overline{\alpha} y) \quad .$$

4.0.1 Bemerkung

Offenbar gilt
$$f(x, y) = n \quad \Longleftrightarrow \quad N(x - \alpha y) = \frac{n}{a} =: r \tag{20}$$

4.0.2 Satz

Mit den Bezeichnungen von oben sei $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{d}\right)$ ein quadratischer Zahlkörper, mit $d \in \mathbb{Z}$, $d \neq 0, 1$ und quadratfrei. $M := \{a + b\alpha \mid a, b \in \mathbb{Z}\}$

(*i*) M ist ein $\mathbb{Z}$-Modul über $\mathbb{Q}\left(\sqrt{d}\right)$.

(*ii*) $O(M) := \left\{\beta \in \mathbb{Q}\left(\sqrt{d}\right) \mid \beta M \subseteq M\right\}$ ist eine Ordnung von $\mathbb{Q}\left(\sqrt{d}\right)$.

(*iii*) $O(M) = O_a$.

Beweis

(*i*) trivial

(*iii*) Da $\{1, \alpha\}$ eine Basis von M ist, gilt für ein beliebiges $x + y\alpha \in \mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{d}\right)$:

$$(x + y\alpha) M \subseteq M \qquad \Longleftrightarrow \qquad x + y\alpha \in M \quad \text{und} \quad (x + y\alpha)\alpha \in M$$

Nach (19) ist $a\alpha^2 + b\alpha + c = 0$. Also ist

$$(x + y\alpha)\alpha = x\alpha - \frac{yc}{a} - \frac{yb\alpha}{a} = -\frac{-yc}{a} + \left(x - \frac{yb}{a}\right)\alpha$$

Demnach ist $(x + y\alpha) M \subseteq M$ genau dann, wenn $x, y \in \mathbb{Z}$ und $\frac{yc}{a}, \frac{yb}{a} \in \mathbb{Z}$. Da $ggT(a, b, c) = 1$, muss gelten $a \mid y$. Somit ist $O(M) = O_a$

(*ii*) $O(M)$ heißt Multiplikatorenring von M. Offensichtlich ist $1 \in O(M)$. Um also zu zeigen, dass $O(M)$ ein Integritätsbereich ist, reicht es zu zeigen, dass für beliebige $\alpha, \beta \in O(M)$ gilt, dass $(\alpha - \beta) \in O(M)$ und $\alpha\beta \in O(M)$. Da M selbst ein Integritätsbereich ist, gilt dies für $\xi \in M$ aufgrund von $(\alpha - \beta)\xi = \alpha\xi - \beta\xi \in M$ und $(\alpha\beta)\xi = \alpha(\beta\xi) \in M$. Sei $Q(O(M))$ der Quotientenkörper von $O(M)$. Um $Q(O(M)) = \mathbb{Q}\left(\sqrt{d}\right)$ zu zeigen, reicht es, die Inklusion „$\subseteq$“ zu zeigen, da „$\supseteq$“ offensichtlich ist. Sei hierzu $\frac{p}{q} + \frac{r}{s}\omega \in \mathbb{Q}\left(\sqrt{d}\right)$ mit $p, q, r, s \in \mathbb{Z}$ und $q, s \neq 0$ beliebig. Diese Darstellung existiert, da $\{1, \omega\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}\left(\sqrt{d}\right)$ ist. Aufgrund von (*iii*) ist $O(M) = O_a$. Also ist nach Satz 2.5.3 $aps + arq\,\omega \in O(M)$. Somit ist aber

$$\frac{p}{q} + \frac{r}{s}\omega = \frac{ps + rq\,\omega}{qs} = \frac{aps + arq\,\omega}{qsa} \in Q(O(M)) \quad .$$

Nun bleibt zu zeigen, dass $O(M)$ nur ganze Zahlen aus K enthält. Wegen der Gleichung $a\alpha^2 + b\alpha + c = 0$ ist auch $(a\alpha)^2 + b(a\alpha) + ac = 0$. Somit ist $a\alpha$ ganz und damit auch alle anderen Elemente $x + y\,a\alpha \in O(M)$.

□

4.1 Satz

Sei M wie in Satz 4.0.2 und $\mathbb{Q}\left(\sqrt{d}\right)$ ein imaginärer quadratischer Zahlkörper, also $d < 1$, d quadratfrei. Dann hat $N(\gamma) = r$ für festes $r \in \mathbb{Z}$ nur endlich viele Lösungen für $\gamma \in M$.

Beweis Da d negativ ist, gilt für $\gamma = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$, dass $N(\gamma) = a^2 - b^2 d = a^2 + b^2 |d|$. Es gibt also für negatives r kein γ, sodass $N(\gamma) = r$. Da es jedoch auch nur endlich viele positive Zahlen gibt, die in der Summe r ergeben, kann $N(\gamma) = r$ nur endlich viele Lösungen haben. □

4.1.1 Bemerkungen

- Da die Norm multiplikativ ist, ist, falls $N(\gamma) = r$, auch $N(\varepsilon\gamma) = N(\varepsilon)\,N(\gamma) = 1r = r$. Mit (20) heißt das, dass man durch Multiplikation mit einer Einheit auf der rechten Seite, eine weitere Lösung von $f(x,y) = n$ auf der linken Seite bekommt. Aus diesem Grund ist die Bestimmung aller Einheiten, wie in Kapitel 3 beschrieben, von großem Interesse.
- Falls $d < 0$, gibt es also nur endlich viele ganzzahlige Lösungen von $f(x,y) = n$.

4.2 Definition: Assoziierte Elemente

$\gamma_1, \gamma_2 \in M$ heißen *assoziiert*, falls ein $\varepsilon \in O(M)$ existiert, sodass $\gamma_1 = \varepsilon\gamma_2$.

4.2.1 Bemerkung

Falls γ_1 und γ_2 assoziiert sind, schreibt man auch $\gamma_1 \sim \gamma_2$. Da die Einheiten eine multiplikative Untergruppe von $O(M)$ bilden, ist $\sim \subseteq M \times M$ offenbar eine Äquivalenzrelation.

4.3 Satz

Sei M wie in Satz 4.0.2 und $\mathbb{Q}\left(\sqrt{d}\right)$ ein reell quadratischer Zahlkörper, also $d > 1$ und d quadratfrei. Dann hat

$$N(\gamma) = r \tag{21}$$

für festes $r \in \mathbb{Q}$ nur endlich viele nicht assoziierte Lösungen $\gamma \in M$.

Beweis Sei $\gamma \in M$ mit $N(\gamma) = r$ und ε_0 die Grundeinheit von $O(M)$. Ohne Einschränkung sei $\gamma > 0$, denn $N(\gamma) = N(-\gamma)$. Da $\varepsilon_0 > 1$, gibt es ein eindeutig bestimmtes $\nu \in \mathbb{Z}$, sodass:

$$\varepsilon_0^{\nu} \leq \gamma < \varepsilon_0^{\nu+1}$$

Also gilt:
$$1 \leq \varepsilon_0^{-\nu}\gamma < \varepsilon_0 \tag{22}$$

Sei $\gamma' := \varepsilon_0^{-\nu}\gamma$. Dann ist γ' eine zu γ assoziierte Lösung von (21). Das heißt, zu jeder Lösung γ von (21) gibt es aufgrund der Eindeutigkeit von ν genau eine assoziierte Lösung, die (22) erfüllt. Da $\gamma' \in M$ ist, lässt es sich eindeutig durch $\gamma' = x + y\alpha$ mit $x, y \in \mathbb{Z}$ schreiben. Das ergibt in (22):

$$1 \leq x + y\alpha < \varepsilon_0 \tag{23}$$

Wegen $N(\gamma') = (x + y\alpha)(x + y\overline{\alpha}) = r$, ist $|x + y\overline{\alpha}| \leq r$.
Das heißt, dass $-r \leq -x - y\overline{\alpha} \leq r$. Mit (23) addiert, ergibt dies:

$$\begin{aligned} & 1 - r \leq (\alpha - \overline{\alpha})\, y \leq r + \varepsilon_0 \\ \Longrightarrow \quad & \frac{1-r}{\alpha - \overline{\alpha}} \leq y \leq \frac{r + \varepsilon_0}{\alpha - \overline{\alpha}} \end{aligned} \tag{24}$$

Es erfüllen allerdings nur endlich viele ganzzahlige Paare (x, y) sowohl (24) als auch (23). Demnach gibt es auch nur endlich viele Einheiten, die (22) erfüllen, also zwischen 1 und ε_0 liegen. Da es zu jeder Lösung von (21) genau eine assoziierte Lösung gibt, die (22) erfüllt, kann es nur endlich viele paarweise nicht assoziierte Lösungen von (21) geben.

□

4.3.1 Bemerkung

Aus dem obigen Beweis wird klar, wie man alle nicht assoziierten Lösungen einer Form bestimmt. Zunächst sucht man alle y, die (24) erfüllen, dann alle dazu paasenden x, die (23) erfüllen. Zuletzt bleibt zu überprüfen, ob $x + y\alpha$ die Bedinung (21) erfüllt. Mit Kapitel 3 kann man dann alle Lösungen von (21) bestimmen. Nach (20) hat man somit auch alle Lösungen von $ax^2 + bxy + cy^2 = n$. Dazu einige Beispiele in folgendem Kapitel.

Literaturhinweis: Im wesentlichen nach [Sch]. In Auszügen auch [KP76].

5 Beispiele

5.1 Ganzzahlige Lösungen der Gleichung $\mathbf{x^2 - 2y^2 = 7}$

$x^2 - 2y^2 = \left(x - \sqrt{2}y\right)\left(x + \sqrt{2}y\right)$ also gilt nach 4.0.1:

$$x^2 - 2y^2 = 7 \quad \Longleftrightarrow \quad N\left(x - \sqrt{2}y\right) = 7 \tag{25}$$

Der zu betrachtende quadratische Zahlkörper ist also $\mathbb{Q}\left(\sqrt{2}\right)$ und somit ist $d = 2 \equiv 2 \pmod 4$ und $\omega = \sqrt{2}$. Zunächst bestimmt man die Grundeinheit ε_0. Hierzu muss man die Kettenbruchentwicklung von $\alpha = \frac{1}{\sqrt{2} - \lfloor\sqrt{2}\rfloor} = \frac{1}{\sqrt{2}-1} = 1 + \sqrt{2}$ bestimmen. Da $\sqrt{2} = [1, \overline{2}]$, ist $\alpha = 1 + \sqrt{2} = 1 + [1, \overline{2}] = [\overline{2}]$. Nach Satz 3.6 muss also $\varepsilon_0 = q_1\alpha + q_0 = 1 + \sqrt{2}$ sein. Für die Norm ergibt sich dann $N(\varepsilon_0) = \left(1 + \sqrt{2}\right)\left(1 - \sqrt{2}\right) = -1$.

Im nächsten Schritt wird die Menge aller paarweise nicht assoziierter Lösungen von (25) bestimmt. Diese müssen sowohl (24) als auch (23) erfüllen.

$$1 \leq x + \sqrt{2}y < \varepsilon_0 = 1 + \sqrt{2} \tag{26}$$

$$\frac{1 - r}{\alpha - \overline{\alpha}} = \frac{-6}{2\sqrt{2}} < y < \frac{r + \varepsilon_0}{\alpha - \overline{\alpha}} = \frac{8 + \sqrt{2}}{2\sqrt{2}} \tag{27}$$

Also $-2 \leq y \leq 3$. Es sind bis auf Vorzeichen also vier Fälle zu unterscheiden:

$y = \pm 2$: Dann ist $x^2 = \pm 7 + 2 \cdot 4$, also $x = \pm 1$. Von $\pm 1 \pm 2\sqrt{2}$ erfüllt allerdings nur $\mu_1 := -1 + 2\sqrt{2}$ die Bedingung (26) und ist damit eine Lösung mit $N(\mu_1) = -7$.

$y = \pm 1$: Dann ist $x^2 = \pm 7 + 2 \cdot 1$, also $x = \pm 3$. Von $\pm 3 \pm \sqrt{2}$ erfüllt nur $\mu_2 := 3 - \sqrt{2}$ die Bedingung (26) und ist eine Lösung von $N(\mu_2) = 7$.

$y = 0$: $x^2 = \pm 7$ hat keine Lösungen.

$y = 3$: Dann ist $x^2 = \pm 7 + 2 \cdot 9$, also $x = \pm 5$. Von $\pm 5 + 3\sqrt{2}$ erfüllt allerdings keine die Bedingung (26).

Man erhält die beiden Lösungen μ_1 und μ_2, deren Norm unterschiedliche Vorzeichen haben. Da $N(\varepsilon_0) = -1$, ist $N(\varepsilon_0^n) = N(\varepsilon_0)^n = 1$ genau dann, wenn n gerade ist. Die Lösungen von $N(\mu) = 7$ sind also gerade:

$$\mu = \mu_1\varepsilon_0^{2k+1} = \left(-1 + 2\sqrt{2}\right)\left(1 + \sqrt{2}\right)^{2k+1} \quad \text{für } k \in \mathbb{Z}$$

$$\mu = \mu_2\varepsilon_0^{2k} = \left(3 - \sqrt{2}\right)\left(1 + \sqrt{2}\right)^{2k} \quad \text{für } k \in \mathbb{Z}$$

Also sind wegen (25) alle Lösungen von $x^2 - 2y^2 = 7$ die Folgen (x_n, y_n) und (x'_n, y'_n) mit:

$$x_n + y_n\sqrt{2} = \left(-1 + 2\sqrt{2}\right)\left(1 + \sqrt{2}\right)^{2n+1} \text{ für } n \in \mathbb{Z}$$
$$x'_n + y'_n\sqrt{2} = \left(3 - \sqrt{2}\right)\left(1 + \sqrt{2}\right)^{2n} \text{ für } n \in \mathbb{Z}$$

5.2 Ganzzahlige Lösungen der Gleichung $\mathbf{x^2 - 2y^2 = -7}$

Aus 5.4 wird klar, dass μ_1 und μ_2 von oben gerade mit Einheiten umgekehrten Vorzeichens multipliziert werden müssen, um Lösungen von $N(\gamma) = -7$ zu liefern. Die Folgen (x_n, y_n) und (x'_n, y'_n) mit

$$x_n + y_n\sqrt{2} = \left(-1 + 2\sqrt{2}\right)\left(1 + \sqrt{2}\right)^{2n} \text{ für } n \in \mathbb{Z}$$
$$x'_n + y'_n\sqrt{2} = \left(3 - \sqrt{2}\right)\left(1 + \sqrt{2}\right)^{2n+1} \text{ für } n \in \mathbb{Z}$$

sind also alle Lösungen von $x^2 - 2y^2 = -7$.

5.3 Ganzzahlige Lösungen der Gleichung $\mathbf{x^2 - 19y^2 = 5}$

Analog zu 5.4 muss man zunächst die Grundeinheit von $\mathbb{Q}\left(\sqrt{19}\right)$ bestimmen. Dies ist in diesem Fall nicht so einfach wie im obigen Beispiel. Deshalb muss man wie in 3.7 zunächst die Kettenbruchentwicklung von $\alpha = \frac{1}{\sqrt{19} - \lfloor\sqrt{19}\rfloor} = \frac{1}{\sqrt{19}-4}$ bestimmen.

$$\begin{aligned}
\alpha_1 &= \frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{3} = 2 + \frac{\sqrt{19}-2}{3} \\
\alpha_2 &= \frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5} = 1 + \frac{\sqrt{19}-3}{5} \\
\alpha_3 &= \frac{5}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{2} = 3 + \frac{\sqrt{19}-3}{2} \\
\alpha_4 &= \frac{2}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{5} = 1 + \frac{\sqrt{19}-2}{5} \\
\alpha_5 &= \frac{5}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{3} = 2 + \frac{\sqrt{19}-4}{3} \\
\alpha_6 &= \frac{3}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{1} = 8 + \frac{\sqrt{19}-4}{1}
\end{aligned}$$

Also ist $k = 6$, $\frac{1}{\sqrt{19}-4} = \overline{[2, 1, 3, 1, 2, 8]}$ und nach 3.4, ist $q_1 = 1$, $q_2 = 1$, $q_3 = 4$, $q_4 = 5$, $q_5 = 14$ und $q_6 = 117$. Die Grundeinheit ist, wie in Satz 3.6 bewiesen, also $\varepsilon_0 = 117\alpha + 14 = 170 + 39\sqrt{19}$ mit $N(\varepsilon_0) = 17^2 - 19 \cdot 39^2 = 1$. (vgl. [KP76, Seite 222])

Um die Menge aller paarweise nicht assoziierter Lösungen zu bestimmen, muss wieder (24) und (23) erfüllt sein.

$$1 \leq x + y\sqrt{19} < \varepsilon_0 = 170 + 39\sqrt{19} < 340 \tag{28}$$
$$\frac{1-r}{\alpha - \overline{\alpha}} = \frac{-12}{2\sqrt{19}} < y < \frac{r + \varepsilon_0}{\alpha - \overline{\alpha}} = \frac{525 + 117\sqrt{19}}{2\sqrt{19}}$$

Also $-1 \leq y \leq 118$. Für $y = 0$ gibt es offensichtlich keine Lösung. Da $N(\varepsilon_0) = 1$, muss man nur den Fall $x^2 = +5 + 19y^2$ betrachten. Für $y = \pm 1$ müsste $x^2 = 5 + 19$ sein. Also gibt es auch hier keine Lösung.

Es sind nun alle Quadratzahlen der Form $5 + 19y^2$ mit $y = 2, \ldots, 118$ gesucht. Dies sind genau $81 = 5 + 19 \cdot 2^2$ für $y = 2$ und $2304 = 5 + 19 \cdot 11^2$ für $y = 11$.
$x^2 = 81$ liefert $x = \pm 9$. Allerdings erfüllt nur $\left(9 + 2\sqrt{19}\right)$ die Bedingung (28).
$x^2 = 2304$ liefert $x = \pm 48$. Hier erfüllt $\left(48 + 11\sqrt{19}\right)$ die Bedingung (28).

Die Lösungen von $x^2 - 19y^2 = 5$ sind dann gerade die Folgen (x_n, y_n) und (x'_n, y'_n) mit:

$$x_n + y_n\sqrt{19} = \left(9 + 2\sqrt{19}\right)\left(170 + 39\sqrt{19}\right)^n \quad \text{für } n \in \mathbb{Z}$$
$$x'_n + y'_n\sqrt{19} = \left(48 + 11\sqrt{19}\right)\left(170 + 39\sqrt{19}\right)^n \quad \text{für } n \in \mathbb{Z}$$

5.4 Ganzzahlige Lösungen der Gleichung $\mathbf{x^2 - 2xy - 12y^2 = 3}$

Wie bisher wird zunächst die Nullstelle des Polynoms $z^2 - 2z - 12$ bestimmt, um die gegebene Form faktorisieren zu können. Diese Nullstelle ist $\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = 1 + \sqrt{13}$. Damit ergibt sich, dass $x^2 - 2xy - 12y^2 = \left(x - \left(1 + \sqrt{13}\right)y\right)\left(x + \left(1 - \sqrt{13}\right)y\right)$. Nach 4.0.1 gilt dann:

$$x^2 - 2xy - 12y^2 = 3 \quad \Longleftrightarrow \quad N\left(x - \left(1 + \sqrt{13}\right)y\right) = 3$$

Da der betrachtete quadratische Zahlkörper $\mathbb{Q}\left(\sqrt{13}\right)$ ist, ist $d = 13 \equiv 1 \pmod 4$. Also ist nach 2.3.3 $\omega = \frac{1+\sqrt{13}}{2}$. Wieder bestimmt man zunächst die Grundeinheit ε_0 mit Hilfe der Kettenbruchentwicklung von $\alpha = \frac{1}{\frac{1+\sqrt{13}}{2} - \left\lfloor \frac{1+\sqrt{13}}{2} \right\rfloor} = \frac{1}{\frac{1+\sqrt{13}}{2} - 2} = \frac{2}{\sqrt{13} - 3}$.

$$\alpha_1 = \frac{2}{\sqrt{13} - 3} = \frac{3 + \sqrt{13}}{2} = 3 + \frac{\sqrt{13} - 3}{2}$$

Der Kettenbruch ist also bereits hier periodisch und somit ist $k = 1$ und $\alpha = [\overline{3}]$. Demnach ist $\varepsilon_0 = q_1\alpha + q_0 = \alpha$. Für die Norm ergibt sich $N(\varepsilon_0) = \left(\frac{3+\sqrt{13}}{2}\right)\left(\frac{3-\sqrt{13}}{2}\right) = \frac{9-13}{4} = -1$.

Im nächsten Schritt wird die Menge aller paarweise nicht assoziierter Lösungen bestimmt. Diese müssen sowohl (24) als auch (23) erfüllen.

$$\begin{aligned} 1 \leq x + 1 + \sqrt{13}y < \varepsilon_0 = \frac{3+\sqrt{13}}{2} \\ \frac{1-r}{\alpha-\overline{\alpha}} = \frac{-2}{\sqrt{13}} < y < \frac{r+\varepsilon_0}{\alpha-\overline{\alpha}} = \frac{9+\sqrt{13}}{2\sqrt{13}} \end{aligned} \tag{29}$$

Also ist $0 \leq y \leq 1$.

$y = 0$: $x^2 = \pm 3$ hat keine Lösungen.

$y = 1$: Dann ist $x^2 - 2x - 12 = \pm 3$, also $x = 1 \pm 4$ oder $x = 1 \pm \sqrt{10} \notin \mathbb{Z}$. Von $1 \pm 4 + \frac{3+\sqrt{13}}{2}$ erfüllt nur $\mu := -3 + \frac{3+\sqrt{13}}{2} = \frac{-3+\sqrt{13}}{2}$ die Bedingung (29).

Man erhält also die Lösungen μ, deren Norm gleich 1 ist. Da $N(\varepsilon_0) = -1$, sind die Lösungen von $x^2 - 2xy - 12y^2 = 3$ die Folgenglieder der Folge (x_n, y_n) mit:

$$x_n + y_n\sqrt{13} = \left(\frac{-3+\sqrt{13}}{2}\right)\left(\frac{3+\sqrt{13}}{2}\right)^{2n} \quad \text{für } n \in \mathbb{Z}$$

Übersicht und Ergänzungen

Mit Hilfe der Resultate dieser Arbeit lassen sich also die ganzzahligen Lösungen von ganzzahligen binären quadratischen Formen bestimmen. Kurz zusammengefasst geht man hierbei, wie gesehen, folgendermaßen vor:

Seien $a, b, c, n \in \mathbb{Z}$ gegeben. Gesucht sind alle $x, y \in \mathbb{Z}$, sodass $f(x, y) = ax^2 + bxy + cy^2 = n$ ist.

1. Bestimmung von $\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Dann ist $f(x, y) = a(x - \alpha)(x - \overline{\alpha})$.

2. Bestimmung von d quadratfrei, sodass $\mathbb{Q}(\alpha) = \mathbb{Q}(d)$. Dementsprechend ist dann
$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{falls } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{falls } d \equiv 2, 3 \pmod 4 \end{cases}$$

3. Bestimmung der Grundeinheit ε_0 von $\mathbb{Q}(d)$ mit Hilfe der Kettenbruchtheorie.

4. Bestimmung der endlich vielen nicht assoziierten Lösungen $\{\mu_1, \ldots, \mu_k\}$ von $N(\mu_i) = \pm\frac{n}{a}$.

5. Die Lösungen von $ax^2 + bxy + cy^2 = n$ ergeben sich dann aus den Folgen (x_n^i, y_n^i) für $i = 1 \ldots k$ mit $\left(x_n^i + y_n^i\sqrt{d}\right) = \mu_i\, \varepsilon_0^n$.
Hierbei ist jedoch auf das Vorzeichen zu achten, sodass unter Umständen nur jedes ungerade oder gerade n eine Lösung liefert.

Die in dieser Arbeit gefundenen Resultate kann man natürlich verallgemeinern. So kann man Formen betrachten, die nicht nur binär oder auch höheren Grades sind. Für die zerlegbaren Formen n-ten Grades spielen dabei die Zahlkörper n-ten Grades eine entsprechende Rolle, wie die quadratischen Zahlkörper für die binären quadratischen Formen. Untersuchungen hierzu sind zum Beispiel in [Bc66] zu finden.

Bei der genaueren Untersuchung von Fragen wie zum Beispiel, wann eine Primzahl p durch eine gegebene binäre quadratische Form darstellbar ist, reicht die hier gegebene Einführung häufig nicht aus. Hier ist die sogenannte Klassenkörpertheorie zu erwähnen. Diese findet sich beispielsweise in [AT67].

Ein anschließendes Thema könnte außerdem die genauere Untersuchung der in Kapitel 1 erwähnten Klassenzahl sein. Eine Zusammenfassung zu diesem Thema ist zum Beispiel in [Rib09] zu finden.

Literatur

[AT67] Emil Artin and John Tate. *Class Field Theory*. American Mathematical Society, 1967.

[Bc66] Zenon Ivanovich Borewics and Igor' Rostislavovic Šafarevič. *Zahlentheorie*. Birkhäuser Verlag, Basel und Stuttgart, 1966.

[But99] John Butcher. Hardy's taxi, $x^2 + 3y^2 = p$ and Michael Lennon. *The New Zealand Mathematics Magazine*, 76, August 1999.

[HL34] Hans Arnold Heilbronn and Hubert Linfoot. On the imaginary quadratic corpora of class number one. *Quarterly Journal of Mathematics*, 5:293–301, 1934.

[HW58] Godfrey Harold Hardy and Edward Maitland Wright. *Zahlentheorie*. R. Oldenbourg, München, 1958.

[KP76] Helmut Koch and Herbert Pieper. *Zahlentheorie*. VEB Deutscher Verlag der Wissenschaft, 1976.

[NZ76a] Ivan Morton Niven and Herbert Samuel Zuckerman. *Einführung in die Zahlentheorie I*. B.I. Wissenschaftsverlag, 1976.

[NZ76b] Ivan Morton Niven and Herbert Samuel Zuckerman. *Einführung in die Zahlentheorie II*. B.I. Wissenschaftsverlag, 1976.

[Rib09] Paulo Ribenboim. *Meine Zahlen, meine Freunde*. Springer-Verlag, Berlin Heidelberg New York, 2009.

[Sam71] Pierre Samuel. *Algebraic Theory of Numbers*. Hermann, Paris, 1971.

[Sch] Volker Schulze. *Skript zum Seminar über Algebra und Zahlentheorie*.

[Sch94] Volker Schulze. *Skript zum Seminar über Zahlentheorie*, WS 1993/94.

[SO80] Winfried Scharlau and Hans Opolka. *Von Fermat bis Minkowski*. Springer-Verlag, Berlin Heidelberg New York, 1980.

[Sta67] Harold Mead Stark. There is no tenth complex quadratic field with class-number one. *Proceedings National Academy of Sciences*, 57:1–27, 1967.

[Zag81] Don Bernard Zagier. *Zetafunktion und quadratische Körper*. Springer-Verlag, Berlin Heidelberg New York, 1981.

Eidesstattliche Erklärung

Hiermit versichere ich an Eides statt, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind ausnahmslos als solche kenntlich gemacht.

Mario Koddenbrock, Berlin den 27. September 2011