Euklidische Zahlkörper

Diplomarbeit
an der Universität Konstanz
im Fach Mathematik

von
Karin Halupczok

Konstanz,
den 24. März 1997

Inhaltsverzeichnis

Einleitung

Die Idee des euklidischen Algorithmus ist es, in Ringen eine Division mit Rest vorzunehmen: Ein Ring R hat einen euklidischen Algorithmus, falls es eine Funktion

$$\delta : R\backslash\{0\} \to \mathbb{N}$$

so gibt, daß

$$\forall\ x, z \in R\backslash\{0\} \quad \exists\ q, y \in R : \quad x = qz + y \ \text{ und } \ (\delta(y) < \delta(z) \ \text{ oder } \ y = 0).$$

Nun sind euklidische Integritätsbereiche Hauptidealbereiche und als solche faktoriell, d.h. in ihnen ist eine eindeutige Primfaktorzerlegung möglich. Aufgrund dieses Umstandes sind daher euklidische Ringe natürlich von Interesse.

In dieser Arbeit geht es lediglich um spezielle Ringe: Sei K ein algebraischer Zahlkörper, das ist eine endliche (algebraische) Erweiterung $K \subseteq \mathbb{C}$ von $\mathbb{Q}$. Und man sagt, ein solcher Zahlkörper K habe einen euklidischen Algorithmus, falls sein *Zahlring* $K \cap \mathbb{A}$ einen euklidischen Algorithmus hat; dabei bezeichnet $\mathbb{A}$ den Ring der ganz algebraischen Zahlen.

Ist K ein Zahlkörper vom Grad n über $\mathbb{Q}$, und sind $\sigma_1, \ldots, \sigma_n$ die Einbettungen von K über $\mathbb{Q}$ in $\mathbb{C}$, so ist

$$N(x) := \prod_{i=1}^{n} \sigma_i x$$

die Norm von $x \in K$, und $N : K \to \mathbb{Q}$ heißt Norm von K.

Hat K mit der Absolutnorm einen euklidischen Algorithmus, so heißt K normeuklidisch. Da dieser Sachverhalt in dieser Arbeit fast ausnahmslos vorkommt, wird hier dann auch abkürzend gesagt, K sei euklidisch.

Entsprechendes sagt man dann natürlich auch für den Zahlring von K. Wenn nichts ausdrücklich anderes gesagt wird, wird in dieser Arbeit unter »euklidisch« stets »normeuklidisch« verstanden.

Des weiteren wird noch oft die folgende Charakterisierung euklidischer Zahlkörper von Nutzen sein:

Satz: *Ein Zahlkörper K mit Zahlring R ist genau dann euklidisch, wenn*

$$\forall\ \zeta \in K \quad \exists\ \vartheta \in R: \quad |N(\zeta - \vartheta)| < 1.$$

Beweis:

Zunächst weiß man, daß K der Quotientenkörper von R ist. Ist nun einerseits K euklidisch, und $\zeta \in K$ beliebig, so ist etwa $\zeta = \frac{x}{z} \in K$ mit $x, z \in R\backslash\{0\}$. (Und falls $x = 0$, so ist $\zeta = 0$, und dann erfüllt $\vartheta = 0$ die zu zeigende Ungleichung.) Dann gibt es ein $\vartheta := q \in R$ und ein $y \in R$ mit $x = qz + y$, d.h. $\frac{x}{z} - q = \frac{y}{z}$ so, daß gilt: $y = 0$ (dann ist $|N(\zeta - \vartheta)| = 0 < 1$), oder $|N(y)| < |N(z)|$ (dann ist $|N(\zeta - \vartheta)| = |N(\frac{y}{z})| = \frac{|N(y)|}{|N(z)|} < 1$).

Seien nun umgekehrt $x, z \in R\backslash\{0\}$, und man setze $\zeta := \frac{x}{z} \in K$. Dann gibt es ein $q := \vartheta \in R$ mit $|N(\zeta - \vartheta)| < 1$. Sei $y := x - qz \in R$, dann ist also $x = qz + y$, und dabei $y = 0$ oder

$$|N(y)| = |N(x - qz)| = |N(\zeta - \vartheta)| \cdot |N(z)| < |N(z)|,$$

d.h. K ist dann euklidisch. $\square$

Daß euklidische Zahlkörper und ihre Theorie auch als Thema an sich hochinteressant sind, soll in dieser Arbeit deutlich werden. Eine zentrale Frage ist dabei die, ob es nun endlich oder unendlich viele euklidische Zahlkörper gibt.

Zwar kann man unendlich viele faktorielle Zahlkörper angeben, das sind also Zahlkörper mit faktoriellem Zahlring, jedoch sind bis heute nur etwas über 600 euklidische Zahlkörper bekannt, und obige Frage nach der Kardinalität der Menge aller euklidischen Zahlkörper bleibt ungeklärt.

Jedoch konnten im Verlauf dieses Jahrhunderts eine ganze Reihe von Teilresultaten in diesem Zusammenhang erzielt werden, von denen hier einige wichtige dargestellt werden sollen.

So beschäftigt sich Kapitel 1 mit dem Beweis des Satzes, daß es nur endlich viele euklidische quadratische Zahlkörper K, also vom Grad 2 über $\mathbb{Q}$, gibt. Dies wird für den imaginärquadratischen Fall ($K \not\subseteq \mathbb{R}$) und reellquadratischen Fall ($K \subseteq \mathbb{R}$) einzeln gezeigt, wobei der umfangreiche Beweis des schwierigen reellquadratischen Falls (nach H. Davenport [6]) einen Großteil der Arbeit ausmacht. Überraschenderweise ist dabei der Spezialfall $K = \mathbb{Q}(\sqrt{m})$ mit $m \equiv 2$ oder $3 \pmod 4$ sehr einfach zu handhaben.

Der vollständige Beweis erfolgt über den Satz (1.18) von H. Davenport mittels binärquadratische Formen: Anwendung von (1.18) auf die Normform

quadratischer Zahlkörper liefert das gewünschte Ergebnis über die Endlichkeit der Anzahl euklidischer reellquadratischer Zahlkörper.

Die beiden Teile zum Beweis von (1.18) verwenden das Hauptlemma (1.30), das die Existenz gewisser $\mathbb{Z}$-Folgen (dort Ketten genannt) regulärer äquivalenter Formen behauptet. Und auch zum Beweis dieses Hauptlemmas werden umfangreiche Überlegungen unternommen.

Doch man wird sehen, daß sich all diese Mühe lohnt: Der Satz von DAVENPORT liefert nämlich eine explizite obere Schranke für die Anzahl euklidischer reellquadratischer Zahlkörper, und darüberhinaus ist sogar eine Verallgemeinerung auf gewisse kubische und quartische Zahlkörper möglich. Dies wird hier aber nicht weiter besprochen; statt dessen werden zum Schluß noch einige euklidische reellquadratische Zahlkörper bestimmt und ein Beispiel für einen faktoriellen, aber nicht euklidischen reellquadratischen Zahlkörper genannt.

Das Kapitel 2 erläutert, wie H.W. LENSTRA in [14] mit Hilfe gewisser Methoden aus der Packungstheorie eine hinreichende Bedingung zur Bestimmung (allgemeiner) euklidischer Zahlkörper fand und diese erfolgreich einsetzen konnte. Mit seiner Arbeit [14] setzte er einen Meilenstein für die Theorie der euklidischen Zahlkörper: Zahlreiche neue euklidischen Zahlkörper konnten bis heute so bestimmt werden. Einige Beispiele werden auch hier gegeben, etwa die Kreisteilungskörper und ihre maximalen reellen Unterkörper.

Jedoch bleibt obige zentrale Frage nach der Anzahl euklidischer Zahlkörper mit diesen Methoden leider unbeantwortbar: Unter der Annahme bestimmter RIEMANN-Hypothesen ist die hinreichende Bedingung von H.W. LENSTRA nur für endlich viele Zahlkörper erfüllbar. Demnach besteht wenig Hoffnung, so unendlich viele euklidische Zahlkörper zu konstruieren.

Kapitel 1

Euklidische quadratische Zahlkörper

In diesem Kapitel wird der folgende Satz über euklidische quadratische Zahlkörper bewiesen:

(1.1) **Satz:** *Es gibt nur endlich viele euklidische quadratische Zahlkörper.*

Man unterscheidet dafür den Fall des imaginärquadratischen Zahlkörpers ($\not\subseteq \mathbb{R}$) von dem Fall des reellquadratischen ($\subseteq \mathbb{R}$). Der erste ist wesentlich einfacher zu handhaben und wird deswegen zuerst behandelt:

1.1 Euklidische imaginärquadratische Zahlkörper

Tatsächlich kann man hier sogar noch Aussagen über mögliche euklidische Algorithmen machen:

(1.2) **Satz:** *Es gibt genau fünf imaginärquadratische Zahlkörper, die einen euklidischen Algorithmus haben, nämlich* $\mathbb{Q}(\sqrt{m})$ *mit*

$$\boxed{m \in \{-1, -2, -3, -7, -11\}.}$$

Diese fünf Zahlkörper sind normeuklidisch.

Beweis:

Man betrachte $\mathbb{Q}(\sqrt{m})$ mit $m < 0$ quadratfrei.

- Ist $m \in \{-1, -2\}$ und $\zeta = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ beliebig, wobei $r, s \in \mathbb{Q}$, so setze man dazu $x, y \in \mathbb{Z}$ so, daß $|r - x| \leqslant \frac{1}{2}$ und $|s - y| \leqslant \frac{1}{2}$ sind.

  Dann gilt mit $\vartheta := x + y\sqrt{m} \in \mathbb{Z}[\sqrt{m}] = \mathbb{Q}(\sqrt{m}) \cap \mathbb{A}$:

$$|N(\zeta - \vartheta)| = |(r - x)^2 - m(s - y)^2| \leqslant \frac{1}{4} + \frac{|m|}{4} < 1.$$

- Ist nun $m \in \{-3, -7, -11\}$ und $\zeta = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ beliebig, wobei $r, s \in \mathbb{Q}$, so setze man dazu $y \in \mathbb{Z}$ so, daß $|2s - y| \leqslant \frac{1}{2}$ ist, sowie $x \in \mathbb{Z}$ so, daß $|r - x - \frac{1}{2}y| \leqslant \frac{1}{2}$ ist.

  Dann gilt mit $\vartheta := x + \frac{1}{2}(1 + \sqrt{m})y \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}] = \mathbb{Q}(\sqrt{m}) \cap \mathbb{A}$:

$$\begin{aligned} |N(\zeta - \vartheta)| &= \left| \left(r - x - \frac{1}{2}y\right)^2 - m\left(s - \frac{1}{2}y\right)^2 \right| \\ &\leqslant \frac{1}{4} + \frac{|m|}{16} \leqslant \frac{1}{4} + \frac{11}{16} = \frac{15}{16} < 1. \end{aligned}$$

Daher sind die angegebenen fünf Zahlkörper normeuklidisch.
Sei nun aber $m \notin \{-1, -2, -3, -7, -11\}$, also insbesondere $|m| > 4$.

Dann sind 1 und -1 die einzigen Einheiten in $\mathbb{Q}(\sqrt{m})$:
Ist $\varepsilon = a + b\sqrt{m}$ eine solche, so ist $N(\varepsilon) = a^2 + |m|b^2 = 1$. Und falls $b \neq 0$ gilt, folgt, da $2b \in \mathbb{Z}$, dann $4 = 4a^2 + 4|m|b^2 > 4$, so daß somit doch nur $b = 0$, also $\varepsilon = 1$ oder $\varepsilon = -1$ möglich ist.

Jede Nichteinheit $\neq 0$ des Zahlrings R von $\mathbb{Q}(\sqrt{m})$ hat die Norm > 3:

- Falls $m \equiv 2$ oder $3 \pmod 4$, ist $R = \mathbb{Z}[\sqrt{m}]$. Sei $x \in R$ eine Nichteinheit $\neq 0$, etwa $x = u + v\sqrt{m}$ mit $u, v \in \mathbb{Z}$.

  Ist $v \neq 0$, so gilt $|N(x)| = u^2 + v^2|m| \geqslant 5 > 3$, und ist $v = 0$, so gilt $|N(x)| = u^2 \geqslant 4 > 3$, da $|u| > 1$ wegen $x \notin \{\pm 1\}$.

- Falls $m \equiv 1 \pmod 4$, so ist ja

$$R = \left\{ \frac{1}{2}(u + v\sqrt{m});\ \ u, v \in \mathbb{Z},\ \ u \equiv v \pmod 2 \right\},$$

  und ferner $|m| \geqslant 15$. Sei $x \in R$ eine Nichteinheit $\neq 0$, etwa $x = \frac{1}{2}(u + v\sqrt{m})$ mit $u, v \in \mathbb{Z}$ und $u \equiv v \pmod 2$.

  Ist $v \neq 0$, so gilt $|N(x)| = \frac{1}{4}(u^2 + v^2|m|) \geqslant \frac{15}{4} > 3$, und ist $v = 0$, so ist u gerade und $x = \frac{u}{2} \in \mathbb{Z}$, also $u \notin \{0, \pm 2\}$, d.h. $|u| \geqslant 4$, und somit $|N(x)| = \frac{1}{4}u^2 \geqslant 4 > 3$.

Angenommen, $\delta : R\backslash\{0\} \to \mathbb{N}$ sei ein euklidischer Algorithmus von R. Man wähle $z \in R$ als Nichteinheit $\neq 0$ dann so, daß $\delta(z)$ minimal ist.

Sei weiter $x \in R$ beliebig, dann gibt es $q, y \in R$ so, daß $x = qz + y$ mit $\delta(y) < \delta(z)$ oder $y = 0$.

Falls $y = 0$, so ist $x \in Rz$, und ist $y \neq 0$, so ist y eine Einheit, also $y = 1$ oder $y = -1$. Daher gilt stets $x \equiv 1 \pmod{Rz}$ oder $x \equiv -1 \pmod{Rz}$ oder $x \equiv 0 \pmod{Rz}$.

Man hat also, daß $|N(z)| = |(R/Rz)| \leqslant 3$, nach obigem ist also z eine Einheit oder 0, im Widerspruch zur Wahl von z.

Dies zeigt, daß alle imaginärquadratischen Zahlkörper, außer den fünf in (1.2) genannten, keinen euklidischen Algorithmus haben. □

In der Zahlentheorie zeigt man auch den folgenden tiefliegenden

(1.3) **Satz:** *Es gibt genau neun faktorielle imaginärquadratische Zahlkörper, nämlich* $\mathbb{Q}(\sqrt{m})$ *mit*

$$\boxed{m \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.}$$

Dieses schwierige Ergebnis wurde 1967 von A. Baker[1] und H.M. Stark[22] erzielt.

Im Hinblick auf Satz (1.1) hätte dieser Satz für den imaginärquadratischen Fall natürlich gereicht. Mit Hilfe der obigen Überlegungen konnte jedoch auf einfache Weise explizit bestimmt werden, welche in dieser Liste faktorieller Zahlkörper tatsächlich auch euklidisch sind. Zusätzlich weiß man nun auch, daß alle anderen imaginärquadratischen Zahlkörper überhaupt keinen euklidischen Algorithmus besitzen.

1.2 Euklidische reellquadratische Zahlkörper

Alles Weitere in diesem Kapitel dient dem Beweis von folgendem

(1.4) **Satz:** *Es gibt nur endlich viele euklidische reellquadratische Zahlkörper.*

Dieser Satz (1.4) wurde von H. Heilbronn in [11] und H. Davenport in [6] mit unterschiedlichen Methoden bewiesen. Sein Beweis ist wesentlich schwieriger als der für den imaginärquadratischen Fall. Überraschenderweise läßt sich ein Spezialfall jedoch sehr leicht behandeln:

1.2.A Der Spezialfall $m \equiv 2$ oder $3 \pmod 4$

Folgender Satz und Beweis stammen aus dem Buch [10] von G.H. HARDY und E.M. WRIGHT:

(1.5) **Satz:** *Es gibt nur endlich viele euklidische reellquadratische Zahlkörper* $\mathbb{Q}(\sqrt{m})$ *mit* $m \equiv 2$ *oder* $3 \pmod 4$.

Beweis:

Man betrachte $\mathbb{Q}(\sqrt{m})$ mit $m > 1$ quadratfrei und $m \equiv 2$ oder $3 \pmod 4$. Angenommen, $\mathbb{Q}(\sqrt{m})$ sei euklidisch.

Seien $r := 0$ und $s := \frac{t}{m}$ mit $t \in \mathbb{Z}$, dann gibt es also ganze Zahlen x, y mit

$$\left| x^2 - m\left(y - \frac{t}{m}\right)^2 \right| < 1,$$
$$\text{also} \quad |(my - t)^2 - mx^2| < m.$$

Wegen $(my - t)^2 - mx^2 \equiv t^2 \pmod m$ ist mit $z := my - t \in \mathbb{Z}$ daher

$$z^2 - mx^2 \equiv t^2 \pmod m \quad \text{und} \quad |z^2 - mx^2| < m. \tag{1.6}$$

- Sei $m \equiv 3 \pmod 4$.

  Sei nun $t \in \mathbb{Z}$ ungerade mit $5m < t^2 < 6m$ gewählt, was für hinreichend großes $m > 1$ möglich ist.

  Nach (1.6) ist dann $z^2 - mx^2 \in \{t^2 - 5m, t^2 - 6m\}$, und somit

  $$t^2 - z^2 = m(5 - x^2) \quad \text{oder} \quad t^2 - z^2 = m(6 - x^2). \tag{1.7}$$

  Modulo 8 ist aber $t^2 \equiv 1$, sowie $z^2, x^2 \equiv 0, 1$ oder 4,
  und ferner $m \equiv 3$ oder 7. Also gilt $t^2 - z^2 \equiv 0, 1$ oder 5, sowie:

  $$5 - x^2 \equiv 1, 4 \text{ oder } 5, \quad \text{d.h.} \quad m(5 - x^2) \equiv 3, 4 \text{ oder } 7,$$
  $$\text{und} \quad 6 - x^2 \equiv 2, 5 \text{ oder } 6, \quad \text{d.h.} \quad m(6 - x^2) \equiv 2, 3, 6 \text{ oder } 7.$$

  Demnach sind die Gleichungen in (1.7) unmöglich.

- Sei $m \equiv 2 \pmod 4$.

  Sei nun $t \in \mathbb{Z}$ ungerade mit $2m < t^2 < 3m$ gewählt, was für hinreichend großes $m > 1$ möglich ist.

Nach (1.6) ist dann (wie oben)

$$t^2 - z^2 = m(2 - x^2) \quad \text{oder} \quad t^2 - z^2 = m(3 - x^2). \tag{1.8}$$

Modulo 8 ist aber $m \equiv 2$ oder 6, und somit

$$\begin{aligned} 2 - x^2 &\equiv 1, 2 \text{ oder } 6, \quad \text{d.h.} \quad m(2 - x^2) \equiv 2, 4 \text{ oder } 6, \\ \text{und} \quad 3 - x^2 &\equiv 2, 3 \text{ oder } 7, \quad \text{d.h.} \quad m(3 - x^2) \equiv 2, 4 \text{ oder } 6. \end{aligned}$$

Demnach sind auch die Gleichungen in (1.8) unmöglich. □

1.2.B Der allgemeine Fall: Der Satz von Davenport

Der erste Beweis des Satzes (1.4) stammt von H. Heilbronn in [11], in dem verschiedene, seinerzeit bekannte Methoden angewendet werden. H. Davenport fand in [6] einen anderen Beweis, der erste Abschätzungen über die Anzahl der euklidischen reellquadratischen Zahlkörper ermöglichte, so daß bald eine vollständige Liste sämtlicher euklidischer reelquadratischer Zahlkörper erstellt werden konnte. Dies gelang größtenteils H. Chatland in [4], der dort eine Zusammenstellung früherer Ergebnisse liefert und weitere Zahlkörper behandelt. Seine falsche Ankündigung von anderer Seite, daß $\mathbb{Q}(\sqrt{97})$ euklidisch sei, wurde von E.S. Barnes und H.P.F. Swinnerton-Dyer in [2] widerlegt. Übrigens hatte die Arbeit [6] von H. Davenport den Vorteil, daß diese verallgemeinerungsfähig auf Zahlkörper anderen Grades war: In den Arbeiten [8] und [9] konnte H. Davenport weiter zeigen, daß es in einer gewissen Klasse kubischer und quartischer Zahlkörper jeweils auch nur endlich viele euklidische gibt.

J.W.S. Cassels lieferte ferner in [3] mit anderen Methoden eine Verbesserung dieses Satzes von Davenport.

Im folgenden wird die Methode von Davenport, wie in [6] beschrieben, vorgestellt. Dazu ist ein Blick in die Theorie der binärquadratischen Formen nötig.

(1.9) **Definition:** *Eine binärquadratische Form F ist eine Funktion* $F : \mathbb{R}^2 \to \mathbb{R}$, $F(x, y) := ax^2 + bxy + cy^2$, *wo* $x, y \in \mathbb{R}$, *sowie* $a, b, c \in \mathbb{R}$ *fest.*

(1.10) **Definition:** *Die Determinante der Form* $F(x, y) = ax^2 + bxy + cy^2$ *ist* $\triangle := \det \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = ac - \frac{b^2}{4}$.

(1.11) **Definition:** *Die Diskriminante der Form* $F(x, y) = ax^2 + bxy + cy^2$ *ist* $\operatorname{disc}(F) := -4\triangle = b^2 - 4ac$.

(1.12) **Bemerkung:** *Eine binärquadratische Form F der Determinante $\triangle \neq 0$ ist positiv definit, falls $a > 0$ und $\triangle > 0$, negativ definit, falls $a < 0$ und $\triangle > 0$, sowie indefinit, falls $\triangle < 0$.*

(1.13) **Definition:** *Ein Gitter Γ (im $\mathbb{R}^2$) ist eine von zwei linear unabhängigen Vektoren $u, v \in \mathbb{R}^2$ erzeugte abelsche Gruppe $\mathbb{Z}u + \mathbb{Z}v$.*

(1.14) **Definition:** *Für eine binärquadratische Form F und ein Gitter Γ heißt*

$$\mu(F, \Gamma, z) := \inf\{|F(x - z)|;\ \ x \in \Gamma\}$$

das inhomogene Minimum von F bezüglich Γ und $z \in \mathbb{R}^2$.

Für einen quadratischen Zahlkörper $\mathbb{Q}(\sqrt{m})$ mit $m \in \mathbb{Z}$ quadratfrei ist $\mathbb{Q}(\sqrt{m}) \cap \mathbb{A} = \{x + \omega y;\ \ x, y \in \mathbb{Z}\}$, wobei

$$\omega := \begin{cases} \sqrt{m}, & \text{falls} \quad m \equiv 2, 3 \pmod 4 \\ \frac{1}{2}(1 + \sqrt{m}), & \text{falls} \quad m \equiv 1 \pmod 4 \end{cases}$$

Dabei lassen sich ebenso auch die Elemente von $\mathbb{Q}(\sqrt{m})$ schreiben als $x + \omega y$ mit $x, y \in \mathbb{Q}$.

Bezeichnet N die Norm von $\mathbb{Q}(\sqrt{m})$, und ist $x + \omega y \in \mathbb{Q}(\sqrt{m})$, so ist für $m \equiv 2, 3 \pmod 4$ also

$$N(x + \omega y) = x^2 - my^2,$$

und für $m \equiv 1 \pmod 4$ ist dann

$$N(x + \omega y) = \left(x + \frac{1}{2}y\right)^2 - m\frac{y^2}{4} = x^2 + xy + \frac{1}{4}y^2(1 - m).$$

Dabei seien nun auch $x, y \in \mathbb{R}$ möglich, und man bekommt die folgende quadratische Form:

(1.15) **Definition:** *Die Normform von $\mathbb{Q}(\sqrt{m})$ ist die binärquadratische Form N_m mit $N_m(x, y) := N(x + \omega y)$* für $x, y \in \mathbb{R}$.

(1.16) **Bemerkung:** *Die Normform N_m ist indefinit für $m > 1$.*

Beweis: Man hat, daß $\triangle = -m < 0$, falls $m \equiv 2, 3 \pmod 4$, und $\triangle = \frac{1}{4}(1 - m) - \frac{1}{4} = -\frac{m}{4} < 0$, falls $m \equiv 1 \pmod 4$. $\square$

(1.17) **Satz:** $\mathbb{Q}(\sqrt{m})$ *ist genau dann euklidisch, wenn*

$$\forall z \in \mathbb{Q}^2 : \quad \mu(N_m, \mathbb{Z}^2, z) < 1.$$

Beweis: $\mathbb{Q}(\sqrt{m})$ ist euklidisch genau dann, wenn

$$\forall \zeta \in \mathbb{Q}(\sqrt{m}) \ \exists \vartheta \in \mathbb{Q}(\sqrt{m}) \cap \mathbb{A} : \quad |N(\zeta - \vartheta)| < 1.$$

Schreibt man $\zeta = \zeta_1 + \omega\zeta_2 \in \mathbb{Q}(\sqrt{m})$ mit $\zeta_1, \zeta_2 \in \mathbb{Q}$, und $z = (\zeta_1, \zeta_2)$, sowie $\vartheta = \vartheta_1 + \omega\vartheta_2 \in \mathbb{Q}(\sqrt{m}) \cap \mathbb{A}$ mit $\vartheta_1, \vartheta_2 \in \mathbb{Z}$, und $t = (\vartheta_1, \vartheta_2)$, so läßt sich obige Aussage notieren als

$$\forall z \in \mathbb{Q}^2 \ \exists t \in \mathbb{Z}^2 : \quad |N_m(z - t)| < 1.$$

Dies ist äquivalent zu

$$\forall z \in \mathbb{Q}^2 : \quad \mu(N_m, \mathbb{Z}^2, z) = \inf\{|N_m(t - z)|; \ t \in \mathbb{Z}^2\} < 1. \quad \square$$

Jetzt kann der Satz von DAVENPORT formuliert werden:

(1.18) **Der Satz von Davenport:** *Es gibt eine Konstante $\kappa > 0$ so, daß für alle indefiniten binärquadratischen Formen $F(x, y) = ax^2 + bxy + cy^2$, mit $a, b, c \in \mathbb{R}$ und $d := \mathrm{disc}(F) > 0$ und mit*

$$\forall (x, y) \in \mathbb{Z}^2 \backslash 0 : \quad F(x, y) \neq 0$$

gilt:

(1) $\exists \xi, \eta \in \mathbb{R} \ \forall x, y \in \mathbb{Z} : \quad |F(x + \xi, y + \eta)| > \kappa^2\sqrt{d}$,

(2) *Sind $a, b, c \in \mathbb{Z}$, so sind $\xi, \eta \in \mathbb{Q}$ wählbar.*

Dieser Satz, der im nächsten Paragraphen bewiesen wird, liefert zusammen mit Satz (1.17) das gewünschte Resultat:

(1.19) **Korollar:** *Satz* (1.4), *also:*
Es gibt nur endlich viele euklidische reellquadratische Zahlkörper.

Beweis: Sei $\kappa > 0$ die Konstante aus Satz (1.18). Weiter sei $m > \kappa^{-4}$, und m quadratfrei. Man betrachte dann den Zahlkörper $\mathbb{Q}(\sqrt{m})$.

Sei nun dazu $F := N_m$, dies ist eine indefinite binärquadratische Form mit ganzzahligen Koeffizienten nach Bemerkung (1.16), und es ist

$$\forall (x, y) \in \mathbb{Z}^2 \backslash 0 : \quad F(x, y) \neq 0,$$

da eben $F = N_m$ die Normform, und die Norm multiplikativ ist.

Weiter ist

$$d = \mathrm{disc}(F) = -4\triangle = \begin{cases} 0 - 4 \cdot (-m) = 4m, & \text{falls } m \equiv 2,3 \pmod 4, \\ 1 - 4 \cdot \frac{1}{4}(1-m) = m, & \text{falls } m \equiv 1 \pmod 4, \end{cases}$$

also $d \geqslant m > \kappa^{-4}$. Somit folgt aus **(1)** und **(2)** von Satz (1.18):

$$\exists (\xi, \eta) \in \mathbb{Q}^2 \ \forall (x,y) \in \mathbb{Z}^2 : \quad |N_m(x+\xi, y+\eta)| > \kappa^2 \sqrt{d}.$$

Ist nun $\mathbb{Q}(\sqrt{m})$ euklidisch, so folgt mit Satz (1.17):

$$\kappa^2 \sqrt{d} \leqslant \inf\{|N_m(x+\xi, y+\eta)|; \ (x,y) \in \mathbb{Z}^2\} = \mu(N_m, \mathbb{Z}^2, (\xi,\eta)) < 1,$$

also $d < \kappa^{-4}$, im Widerspruch zu obigem. $\square$

Die Konstante $\kappa > 0$ liefert eine obere Schranke für die Anzahl euklidischer reellquadratischer Zahlkörper: Für $m > \kappa^{-4}$ ist $\mathbb{Q}(\sqrt{m})$ nicht euklidisch, d.h. κ^{-4} ist eine Abschätzung nach oben für diese Anzahl.

Man wird noch sehen, daß diese Konstante im Beweis des Satzes von DAVENPORT bestimmt werden kann. Dieser Satz liefert also noch mehr als nur obigen Satz (1.4) über die Endlichkeit der Anzahl der euklidischen reellquadratischen Zahlkörper.

1.3 Der Beweis des Satzes von Davenport

Für den Beweis des Satzes (1.18) werden einige vorbereitende Dinge über binärquadratische Formen benötigt, diese werden in diesem Abschnitt als erstes erläutert. Ferner ist ab jetzt unter einer Kette stets eine $\mathbb{Z}$-Folge zu verstehen, also eine Abbildung $A : \mathbb{Z} \to M$, wo hier M irgendeine Menge ist. Es wird dafür dann $(m_i)_{i \in \mathbb{Z}}$ geschrieben, wobei $m_i := A(i)$ für $i \in \mathbb{Z}$ ist.

(1.20) **Definition:** *Eine indefinite nichtausgeartete binärquadratische Form F mit*

$$\forall (x,y) \in \mathbb{Z}^2 \backslash 0 : \quad F(x,y) \neq 0$$

heiße im Folgenden dieses Kapitels brauchbar.

(1.21) **Bemerkung:** *Für eine brauchbare Form $F(x,y) = ax^2 + bxy + cy^2$ gilt $ac \neq 0$.*

Beweis: Sonst wäre $F(1,0) = a = 0$ bzw. $F(0,1) = c = 0$, also F nicht brauchbar. $\square$

(1.22) **Satz:** *Eine brauchbare Form* $F(x,y) = ax^2 + bxy + cy^2$ *läßt sich als*

$$F(x,y) = \sqrt{d}(\alpha x + \beta y)(\gamma x + \delta y)$$

schreiben, wobei $d = \operatorname{disc}(F) = b^2 - 4ac > 0$ *gilt, und* $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ *mit* $\alpha\delta - \beta\gamma = 1$ *sind.*

Beweis: Zunächst ist die 0 durch F nichttrivial darstellbar:

Denn ist $ax^2 + bxy + cy^2 = 0$ in $x, y \in \mathbb{R}$ nichttrivial lösbar, so gilt dies genau dann, wenn $t^2 + \frac{b}{a}t + \frac{c}{a}$ in $t \in \mathbb{R}$ nichttrivial lösbar ist. (Denn es gilt ja, daß $ac \neq 0$ nach (1.21); für die eine Richtung setze man $t := \frac{x}{y}$, wobei $xy \neq 0$ sein muß.)

Dies ist aber so, die beiden Lösungen davon sind $r := \frac{1}{2a}(-b + \sqrt{d})$, sowie $s := \frac{1}{2a}(-b - \sqrt{d})$. Damit ist dann

$$\begin{aligned} F(x,y) = ax^2 + bxy + cy^2 &= a(x - ry)(x - sy) \\ &= \sqrt{d}(ax - ary)\left(\frac{1}{\sqrt{d}}x - \frac{s}{\sqrt{d}}y\right). \end{aligned}$$

Mit $\alpha := a$, $\beta := -ar$, $\gamma := \frac{1}{\sqrt{d}}$, $\delta := -\frac{s}{\sqrt{d}}$ folgt das gewünschte Resultat mit

$$\alpha\delta - \beta\gamma = -\frac{as}{\sqrt{d}} + \frac{ar}{\sqrt{d}} = \frac{a}{\sqrt{d}} \cdot \frac{\sqrt{d}}{a} = 1. \quad \square$$

(1.23) **Bemerkung:** *Es sind* $\frac{\alpha}{\beta}$ *und* $\frac{\gamma}{\delta}$ *irrational.*

Beweis: Sonst wäre etwa $\frac{\alpha}{\beta} = \frac{p}{q}$ mit $p, q \in \mathbb{Z}, q \neq 0$, also $F(q, -p) = 0$, im Widerspruch zur Brauchbarkeit von F. $\square$

(1.24) **Definition:** *Zwei binärquadratische Formen* F_1 *und* F_2 *heißen äquivalent, falls es* $p, q, r, s \in \mathbb{Z}$ *mit* $ps - qr = 1$ *so gibt, daß* $F_1(x,y) = F_2(x', y')$ *mit*

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

für alle $x, y, x', y' \in \mathbb{R}$ *gilt. Eine solche Transformation* $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathbb{Z}^2$ *der Koordinaten heißt ganzzahlig unimodular.*

(1.25) **Bemerkung:** *Zwei äquivalente Formen haben dieselbe Determinante.*

(1.26) **Bemerkung:** *Die in* (1.24) *definierte Äquivalenz ist eine Äquivalenzrelation auf der Menge der binärquadratischen Formen, bzw. der*

(i) *brauchbaren,*

(ii) *positiv definiten,*

(iii) *negativ definiten,*

(iv) *indefiniten*

binärquadratischen Formen.

(1.27) **Bemerkung:** *Seien die brauchbaren Formen*

$$F_1(x,y) = \sqrt{d}(\alpha_1 x + \beta_1 y)(\gamma_1 x + \delta_1 y)$$

und

$$F_2(x,y) = \sqrt{d}(\alpha_2 x + \beta_2 y)(\gamma_2 x + \delta_2 y)$$

gemäß(1.22) *notiert. Gibt es dann* $p,q,r,s \in \mathbb{Z}$ *mit* $ps - qr = 1$, *und gilt*

$$\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \begin{pmatrix}p & r\\ q & s\end{pmatrix}\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}$$
$$\textit{sowie}\quad \begin{pmatrix}\gamma_2\\ \delta_2\end{pmatrix} = \begin{pmatrix}p & r\\ q & s\end{pmatrix}\begin{pmatrix}\gamma_1\\ \delta_2\end{pmatrix},$$

so sind F_1 *und* F_2 *äquivalent vermöge* $\begin{pmatrix}p & q\\ r & s\end{pmatrix}$.

Beweis: Es gilt

$$\begin{aligned} F_1(x,y) &= \sqrt{d}(\alpha_1 x + \beta_1 y)(\gamma_1 x + \delta_1 y)\\ &= \sqrt{d}(\alpha_1(px'+qy') + \beta_1(rx'+sy'))(\gamma_1(px'+qy') + \beta_1(rx'+sy'))\\ &= \sqrt{d}(\alpha_2 x' + \beta_2 y')(\gamma_2 x' + \delta_2 y') = F_2(x',y'). \quad \square \end{aligned}$$

(1.28) **Definition:** *Eine Kette* $(F_n)_{n\in\mathbb{Z}}$ *zu* F *äquivalenter brauchbarer Formen mit*

$$F_n(x,y) = \sqrt{d}(\alpha_n x + \beta_n y)(\gamma_n x + \delta_n y) \ \textit{für}\ n \in \mathbb{Z}$$

heißt <u>regulär</u>, *falls mit* $\vartheta, C, B \in \mathbb{R}_{>0}$, $C > 1$, *und* $\vartheta < 1$ *für alle* $n \in \mathbb{Z}$ *gilt:*

$$(1.29)\qquad \begin{cases} |\alpha_{n+1}| < \frac{1}{C}|\alpha_n|,\\ |\gamma_{n+1}| > C|\gamma_n|,\\ |\alpha_n\gamma_n| \leqslant \vartheta < 1,\\ |\alpha_n\gamma_{n+1}| < B^2, \end{cases}$$

Für den Beweis des Satzes von DAVENPORT ist die Existenz solcher regulärer Ketten brauchbarer Formen von entscheidender Wichtigkeit, daher wird diese Tatsache nun formuliert im

(1.30) **Hauptlemma:** *Zu einer brauchbaren Form F gibt es eine reguläre Kette $(F_n)_{n\in\mathbb{Z}}$ zu F äquivalenter brauchbarer Formen mit Transformationen* $\begin{pmatrix} p_n & q_n \\ r_n & s_n \end{pmatrix}$, *wobei* $p_n s_n - r_n q_n = 1$, *so wie in* (1.27), *d.h.*

$$\begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} = \begin{pmatrix} p_n & r_n \\ q_n & s_n \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$
$$\textit{und} \quad \begin{pmatrix} \gamma_n \\ \delta_n \end{pmatrix} = \begin{pmatrix} p_n & r_n \\ q_n & s_n \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix}.$$

Der Beweis von (1.30) wird im Unterabschnitt 1.3.3 geführt, also bis dahin zurückgestellt. Dort wird sich dann auch ergeben, daß ϑ und B als $\vartheta = \frac{1}{\sqrt{3}}$ und $B = 4 \cdot (\frac{4}{3})^{\frac{5}{4}} C^2$ gegeben sind, und daß $C > 1$ beliebig wählbar ist.

1.3.1 Beweis von Teil (1)

Seien also Formen F_n für $n \in \mathbb{Z}$ gemäß des Hauptlemmas (1.30) gegeben. Und da F_0 und F äquivalent sind, genügt es, für **(1)** zu zeigen, daß es reelle Zahlen λ_0 und μ_0 so gibt, daß für alle $x, y \in \mathbb{Z}$ gilt:

$$|(\alpha_0 x + \beta_0 y + \lambda_0)(\gamma_0 x + \delta_0 y + \mu_0)| > \kappa^2,$$

für irgendein $\kappa > 0$. Denn es ist ja

$$\begin{aligned} |(\alpha_0 x + \beta_0 y + \lambda_0)(\gamma_0 x + \delta_0 y + \mu_0)| &= |F_0(x + \xi, y + \eta)| \cdot \frac{1}{\sqrt{d}} \\ &= |F(x' + \xi', y' + \eta')| \cdot \frac{1}{\sqrt{d}}, \end{aligned}$$

wobei ξ, η das Gleichungssystem

$$\begin{cases} \alpha_0 \xi + \beta_0 \eta = \lambda_0 \\ \gamma_0 \xi + \delta_0 \eta = \mu_0 \end{cases}$$

lösen, und es gilt

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p_0 & q_0 \\ r_0 & s_0 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$
$$\text{und} \quad \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \begin{pmatrix} p_0 & q_0 \\ r_0 & s_0 \end{pmatrix} \begin{pmatrix} \xi' \\ \eta' \end{pmatrix}.$$

Es wird nun gezeigt, daß folgende reelle Zahlen λ_0 und μ_0 dies erfüllen: Man setzt

$$\lambda_0 := v_0\alpha_0 + v_1\alpha_1 + v_2\alpha_2 + \cdots = \sum_{n=0}^{\infty} v_n\alpha_n$$

$$\text{und} \quad -\mu_0 := v_{-1}\gamma_{-1} + v_{-2}\gamma_{-2} + \cdots = \sum_{n=-\infty}^{-1} v_n\gamma_n,$$

wobei $v_n := \lfloor \vartheta|\alpha_n\gamma_n|^{-1} \rfloor \in \mathbb{Z}$ für $n \in \mathbb{Z}$ sei; dabei bezeichnet $\lfloor\ \rfloor$ die Gaußklammer.

Dadurch sind λ_0 und μ_0 *wohldefiniert*: Zunächst ist $\alpha_n\gamma_n \neq 0$, da ja $\sqrt{d}\alpha_n\gamma_n = F_n(1,0) \neq 0$ für brauchbares F_n ist. Weiter ist

$$\frac{1}{2}\vartheta < v_n|\alpha_n\gamma_n| \leqslant \vartheta < 1, \tag{1.31}$$

da $\frac{1}{2} < \frac{\lfloor z \rfloor}{z}$ für $z \geqslant 1$ gilt, wobei hier $z := \vartheta|\alpha_n\gamma_n|^{-1} \geqslant 1$ ist, aufgrund der Regularität der Kette $(F_n)_{n\in\mathbb{Z}}$, vgl. (1.29).

Also ist $v_n|\alpha_n| \leqslant \frac{\vartheta}{|\gamma_n|}$ und $v_n|\gamma_n| < \frac{\vartheta}{|\alpha_n|}$.

Wegen $|\frac{\alpha_{n+1}}{\alpha_n}| < \frac{1}{C} < 1$ und $|\frac{\gamma_n}{\gamma_{n+1}}| < \frac{1}{C} < 1$ sind nach dem Quotientenkriterium die Reihen

$$\sum_{n=0}^{\infty} \frac{\vartheta}{|\gamma_n|} \qquad \text{und} \qquad \sum_{n=-\infty}^{-1} \frac{\vartheta}{|\alpha_n|}$$

absolut konvergent, und daher nach dem Majorantenkriterium auch die beiden Reihen, die λ_0 und μ_0 definieren.

Im folgenden wird die Annahme, λ_0 und μ_0 würden obige Bedingung nicht erfüllen, auf einen Widerspruch geführt:

Es sei also angenommen, daß es $x, y \in \mathbb{Z}$ gibt mit

$$|(\alpha_0 x + \beta_0 y + \lambda_0)(\gamma_0 x + \delta_0 y + \mu_0)| \leqslant \kappa^2.$$

Die Kette $(|\gamma_n|)_{n\in\mathbb{Z}}$ ist streng monoton wachsend mit $|\gamma_n|@ >> n \to \infty > \infty$ und $|\gamma_n|@ >> n \to -\infty > 0$ wegen der Regularität (1.29).

- Falls $\alpha_0 x + \beta_0 y + \lambda_0 \neq 0$ ist, gibt es daher also ein $m \in \mathbb{Z}$ mit

$$\frac{B\kappa}{|\gamma_{m+1}|} \leqslant |\alpha_0 x + \beta_0 y + \lambda_0| < \frac{B\kappa}{|\gamma_m|},$$

wobei $\kappa > 0$ vorerst noch beliebig sei. Dann ist mit (1.29):

$$|\gamma_0 x + \delta_0 y + \mu_0| \leqslant \frac{\kappa^2}{|\alpha_0 x + \beta_0 y + \lambda_0|} \leqslant \frac{\kappa^2 |\gamma_{m+1}|}{B\kappa} < \frac{\kappa^2 B^2}{B\kappa |\alpha_m|} = \frac{B\kappa}{|\alpha_m|},$$

also gelten die Ungleichungen

$$\begin{cases} |\alpha_0 x + \beta_0 y + \lambda_0| < \frac{B\kappa}{|\gamma_m|}, \\ |\gamma_0 x + \delta_0 y + \mu_0| < \frac{B\kappa}{|\alpha_m|}. \end{cases} \tag{1.32}$$

- Falls $\alpha_0 x + \beta_0 y + \lambda_0 = 0$, gilt aber auch (1.32) für ein geeignet großes $m > 1$, da nach (1.29) gilt: $\frac{1}{|\alpha_n|}@ >> n \to \infty > \infty$.

In jedem Falle gelten also die Ungleichungen (1.32).

Jetzt setzt man für $n \in \mathbb{Z}$

$$\lambda_n := v_n \alpha_n + v_{n+1}\alpha_{n+1} + \cdots = \sum_{r=n}^{\infty} v_r \alpha_r$$

$$\text{und} \quad -\mu_n := v_{n-1}\gamma_{n-1} + v_{n-2}\gamma_{n-2} + \cdots = \sum_{r=-\infty}^{n-1} v_r \gamma_r,$$

wobei diese Reihen nach obigem absolut konvergieren.

Außerdem gelten die Rekursionen (für $n \in \mathbb{Z}$):

$$\begin{aligned} \lambda_n &= v_n \alpha_n + \lambda_{n+1} \\ \text{und} \quad \mu_n &= v_n \gamma_n + \mu_{n+1}. \end{aligned}$$

Für obige $x, y \in \mathbb{Z}$ ist also für $n \in \mathbb{Z}$:

$$\begin{aligned} \alpha_n x + \beta_n y + \lambda_n &= \alpha_n (x + v_n) + \beta_n y + \lambda_{n+1} \\ &= \alpha_{n+1} x' + \beta_{n+1} y' + \lambda_{n+1}, \end{aligned}$$

wobei

$$\begin{pmatrix} x + v_n \\ y \end{pmatrix} = \begin{pmatrix} p_n & q_n \\ r_n & s_n \end{pmatrix}^{-1} \begin{pmatrix} p_{n+1} & q_{n+1} \\ r_{n+1} & s_{n+1} \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

ist, d.h. die ganzen Zahlen x' und y' entstehen mittels einer ganzzahligen unimodularen Transformation aus den ganzen Zahlen $x + v_n$ und y. Mit derselben ist ebenso für $n \in \mathbb{Z}$:

$$\gamma_n x + \delta_n y + \mu_n = \gamma_{n+1} x' + \delta_{n+1} y' + \mu_{n+1}.$$

Somit lassen sich rekursiv Ketten $(x_n)_{n\in\mathbb{Z}}$ und $(y_n)_{n\in\mathbb{Z}}$ ganzer Zahlen definieren mit

$$\begin{aligned} \alpha_0 x + \beta_0 y + \lambda_0 &= \alpha_n x_n + \beta_n y_n + \lambda_n \\ \text{und} \quad \gamma_0 x + \delta_0 y + \mu_0 &= \gamma_n x_n + \delta_n y_n + \mu_n. \end{aligned}$$

Wegen (1.32) gibt es insbesondere $x_m, y_m \in \mathbb{Z}$ mit

$$\begin{aligned} |\alpha_m x_m + \beta_m y_m + \lambda_m| &< \frac{B\kappa}{|\gamma_m|} \\ \text{und} \quad |\gamma_m x_m + \delta_m y_m + \mu_m| &< \frac{B\kappa}{|\alpha_m|}. \end{aligned}$$

Es folgt:

$$\begin{aligned} &|y_m - \lambda_m\gamma_m + \mu_m\alpha_m| \\ &\quad = |\alpha_m\gamma_m x_m - \alpha_m\gamma_m x_m + (\alpha_m\delta_m - \gamma_m\beta_m)y_m - \lambda_m\gamma_m + \alpha_m\mu_m| \\ &\quad = |-\gamma_m(\alpha_m x_m + \beta_m y_m + \lambda_m) + \alpha_m(\gamma_m x_m + \delta_m y_m + \mu_m)| \\ &\quad < 2B\kappa. \end{aligned} \tag{1.33}$$

Nach Definition von λ_m und μ_m ist nun

$$\lambda_m\gamma_m - \mu_m\alpha_m = v_m\alpha_m\gamma_m + \sum_{r=m+1}^{\infty} v_r\alpha_r\gamma_m + \sum_{r=-\infty}^{m-1} v_r\gamma_r\alpha_m,$$

also wegen (1.31) und (1.29) ist dann

$$|\lambda_m\gamma_m - \mu_m\alpha_m - v_m\alpha_m\gamma_m| \leqslant \vartheta \sum_{r=m+1}^{\infty} \left|\frac{\gamma_m}{\gamma_r}\right| + \vartheta \sum_{r=-\infty}^{m-1} \left|\frac{\alpha_m}{\alpha_r}\right| < \frac{2\vartheta}{C-1}.$$

Mit (1.31) folgt daraus

$$\frac{1}{2}\vartheta - \frac{2\vartheta}{C-1} < \lambda_m\gamma_m - \mu_m\alpha_m < \vartheta + \frac{2\vartheta}{C-1}. \tag{1.34}$$

Hat man nun $C > 1$ und $\kappa > 0$ so gewählt, daß

$$0 < 2B\kappa < \min\left\{\frac{1}{2}\vartheta - \frac{2\vartheta}{C-1}, 1 - \vartheta - \frac{2\vartheta}{C-1}\right\} < 1 \tag{1.35}$$

ist, was für großes $C > 1$ und kleines $\kappa > 0$ bei $B = 4 \cdot (\frac{4}{3})^{\frac{5}{4}} C^2$ sicher möglich ist, so erhält man folgendermaßen einen Widerspruch:

Aus (1.33) und (1.35) folgt $|y_m - (\lambda_m \gamma_m - \mu_m \alpha_m)| < 2B\kappa < 1$, und aus (1.34) und (1.35) folgt

$$0 < \frac{1}{2}\vartheta - \frac{2\vartheta}{C-1} < \lambda_m \gamma_m - \mu_m \alpha_m < \vartheta + \frac{2\vartheta}{C-1} < 1.$$

Da nun $y_m \in \mathbb{Z}$ ist, ist beides nur für $y_m = 0$ oder $y_m = 1$ möglich.

- Falls $y_m = 0$, ist nach (1.33) dann aber

$$\lambda_m \gamma_m - \mu_m \alpha_m < 2B\kappa < \frac{1}{2}\vartheta - \frac{2\vartheta}{C-1},$$

  im Widerspruch zu (1.34).

- Falls $y_m \neq 0$, ist nach (1.33) dann aber

$$1 - \lambda_m \gamma_m - \mu_m \alpha_m < 2B\kappa < 1 - \vartheta - \frac{2\vartheta}{C-1},$$

  also

$$\lambda_m \gamma_m - \mu_m \alpha_m > \vartheta + \frac{2\vartheta}{C-1},$$

  im Widerspruch zu (1.34).

Damit ist der Beweis von Teil **(1)** erbracht. □

Mittels (1.35) ist natürlich eine explizite Bestimmung von $\kappa > 0$ möglich, allerdings sind diese Werte für κ mit (1.35) sehr klein. Im Hinblick auf (1.19) sind aber eher möglichst große $\kappa > 0$ von Interesse.

1.3.2 Beweis von Teil (2)

Sei nun also $F(x, y) = ax^2 + bxy + cy^2$ brauchbar mit $a, b, c \in \mathbb{Z}$, und seien

$$F_n(x, y) = \sqrt{d}(\alpha_n x + \beta_n y)(\gamma_n x + \delta_n y) = a_n x^2 + b_n xy + c_n y^2$$

für $n \in \mathbb{Z}$ dazu äquivalente reguläre brauchbare Formen gemäß des Hauptlemmas (1.30). Dabei sind dann auch $a_n, b_n, c_n \in \mathbb{Z}$.

Denn es ist

$$\begin{aligned} a_n &= \alpha_n\gamma_n\sqrt{d} \\ &= \sqrt{d}(p_n^2\alpha\gamma + p_nr_n(\alpha\delta+\beta\gamma) + r_n^2\beta\delta) \in \mathbb{Z}, \\ \text{und}\quad b_n &= \sqrt{d}(\alpha_n\delta_n + \beta_n\gamma_n) \\ &= \sqrt{d}(2p_nq_n\alpha\gamma + 2r_ns_n\beta\delta + (p_ns_n + r_nq_n)(\alpha\delta+\beta\gamma)) \in \mathbb{Z}, \\ \text{sowie}\quad c_n &= \beta_n\delta_n\sqrt{d} \\ &= \sqrt{d}(q_n^2\alpha\gamma + q_ns_n(\alpha\delta+\beta\gamma) + s_n^2\beta\delta) \in \mathbb{Z}. \end{aligned}$$

Ferner kann man ohne Einschränkung annehmen, daß für alle $n \in \mathbb{Z}$ gilt: $|b_n| \leqslant |a_n|$.

Denn sonst transformiere F_n mittels $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ für ein $h \in \mathbb{Z}$ in die Form

$$F_n'(x,y) = a_n'x^2 + b_n'xy + c_n'y^2 = \sqrt{d}(\alpha_n'x + \beta_n'y)(\gamma_n'x + \delta_n'y)$$

mit

$$\begin{pmatrix} \alpha_n' \\ \beta_n' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ h & 1 \end{pmatrix}\begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix}$$

und

$$\begin{pmatrix} \gamma_n' \\ \delta_n' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ h & 1 \end{pmatrix}\begin{pmatrix} \gamma_n \\ \delta_n \end{pmatrix},$$

d.h. $\alpha_n' = \alpha_n$, $\gamma_n' = \gamma_n$, $\beta_n' = h\alpha_n + \beta_n$, und $\delta_n' = h\gamma_n + \delta_n$. Es ist also $a_n' = a_n$ und $b_n' = 2a_nh + b_n$. Ist nun $h \in \mathbb{Z}$ so gewählt, daß

$$-\frac{1}{2} - \frac{b_n}{2a_n} \leqslant h \leqslant \frac{1}{2} - \frac{b_n}{2a_n} \quad\Leftrightarrow\quad |2a_nh + b_n| \leqslant |a_n|,$$

dann ist also $|b_n'| \leqslant |a_n'|$. (Dies ist möglich, da $\frac{1}{2} - \frac{b_n}{2a_n} + \frac{1}{2} + \frac{b_n}{2a_n} = 1$ ist.) Nun ersetze man F_n durch F_n'. Die Regularität (1.29) bleibt dabei erhalten wegen $\alpha_n' = \alpha_n$ und $\gamma_n' = \gamma_n$.

Somit ist nach (1.29) dann $|b_n| \leqslant |a_n| = |\alpha_n\gamma_n|\sqrt{d} \leqslant \vartheta\sqrt{d}$ beschränkt, und auch $|c_n|$ wegen $d = b_n^2 - 4a_nc_n$, denn es ist

$$|c_n| = \frac{|b_n^2 - d|}{4|a_n|} \leqslant \frac{b_n^2}{4|a_n|} + \frac{d}{4|a_n|} \leqslant (\vartheta^2 d + d),$$

weil $a_n \in \mathbb{Z}$ und $a_n \neq 0$ ist.

Da die a_n, b_n und c_n ganze Zahlen sind, gibt es für diese also nur endlich viele Möglichkeiten. Deswegen gibt es $j, g \in \mathbb{Z}$ mit $g > 0$ so, daß für alle $x, y \in \mathbb{R}$ gilt: $F_j(x,y) = F_{j+g}(x,y)$. Denn eine Form F_j muß dann ja wieder als eine Form F_{j+g} in der Kette auftauchen.

Insbesondere gilt also für alle $x, y \in \mathbb{R}$:

$$(\alpha_j x + \beta_j y)(\gamma_j x + \delta_j y) = (\alpha_{j+g} x + \beta_{j+g} y)(\gamma_{j+g} x + \delta_{j+g} y).$$

Da aber

$$\begin{aligned} \alpha_j\delta_j - \beta_j\gamma_j = 1 = \alpha_{j+g}\delta_{j+g} - \beta_{j+g}\gamma_{j+g}, \\ \alpha_j\gamma_j = \alpha_{j+g}\gamma_{j+g}, \\ \beta_j\delta_j = \beta_{j+g}\delta_{j+g} \end{aligned}$$

gilt, folgt mit $\omega := \frac{\alpha_j}{\alpha_{j+g}}$, also $\omega > 1$ nach (1.29), dann:

$$\begin{aligned} & \alpha_j = \omega\alpha_{j+g}, && \beta_j = \omega\beta_{j+g}, \\ \text{und} \quad & \gamma_j = \omega^{-1}\gamma_{j+g}, && \delta_j = \omega^{-1}\delta_{j+g}. \end{aligned}$$

Denn es ist

$$1 + 2\beta_j\gamma_j = \alpha_j\delta_j + \beta_j\gamma_j = \alpha_{j+g}\delta_{j+g} + \beta_{j+g}\gamma_{j+g} = 1 + 2\beta_{j+g}\gamma_{j+g},$$

also $\frac{\beta_{j+g}}{\beta_j} = \frac{\gamma_j}{\gamma_{j+g}} = \frac{\alpha_{j+g}}{\alpha_j} = \omega^{-1}$, und damit $\beta_{j+g}\omega = \beta_j$ und $\gamma_{j+g}\omega^{-1} = \gamma_j$. Ferner ist $\omega^{-1} = \frac{\beta_{j+g}}{\beta_j} = \frac{\delta_j}{\delta_{j+g}}$, also auch $\delta_{j+g}\omega^{-1} = \delta_j$.

Somit definiert man für $n < j$ oder $n > j + g$ die Zahlen $a_n, b_n, c_n \in \mathbb{Z}$ und $\alpha_n, \beta_n, \gamma_n, \delta_n \in \mathbb{R}$ neu aus den vorhandenen Werten für $j \leqslant n \leqslant j + g$ vermöge den Rekursionen

$$\begin{aligned} & a_{n+g} = a_n, && b_{n+g} = b_n, && c_{n+g} = c_n, \\ & \alpha_n = \omega\alpha_{n+g}, && \beta_n = \omega\beta_{n+g}, && \gamma_n = \omega^{-1}\gamma_{n+g}, \quad \delta_n = \omega^{-1}\delta_{n+g}. \end{aligned}$$

Damit erreicht man, daß diese Gleichungen für alle $n \in \mathbb{Z}$ gelten, und man erhält somit eine periodische Kette $(F_n)_{n\in\mathbb{Z}}$ der Periode g. Dabei bleibt die Regularität (1.29) erhalten, da diese bereits im Bereich für $j \leqslant n \leqslant j + g$ gegolten hat.

Daher sind wie im Unterabschnitt 1.3.1 die Reihen für λ_0 und μ_0 absolut konvergent, und insbesondere ist $v_n = \lfloor \vartheta |\alpha_n\gamma_n|^{-1} \rfloor$ auch periodisch mit der

Periode g, so daß gilt:

$$(1.36)\qquad \begin{cases} \lambda_0 = (\alpha_0 v_0 + \alpha_1 v_1 + \cdots + \alpha_{g-1} v_{g-1})(1 + \omega^{-1} + \omega^{-2} + \dots) \\ \quad = (\alpha_0 v_0 + \alpha_1 v_1 + \cdots + \alpha_{g-1} v_{g-1}) \dfrac{1}{1-\omega^{-1}}, \\ \mu_0 = -(\gamma_{-1} v_{-1} + \gamma_{-2} v_{-2} + \cdots + \gamma_{-g} v_{-g})(1 + \omega^{-1} + \omega^{-2} + \dots) \\ \quad = (\gamma_{g-1} v_{g-1} + \cdots + \gamma_0 v_0) \dfrac{\omega^{-1}}{\omega^{-1} - 1} \\ \quad = (\gamma_0 v_0 + \gamma_1 v_1 + \cdots + \gamma_{g-1} v_{g-1}) \dfrac{1}{1-\omega}. \end{cases}$$

Nun betrachte man eine der Formen F_n, etwa F_0, und es ist für alle $x, y \in \mathbb{R}$:

$$F_0(x,y) = (\alpha_0 x + \beta_0 y)(\gamma_0 x + \delta_0 y)$$

mit $\alpha_0, \beta_0, \gamma_0, \delta_0 \in \mathbb{R}$.

Ist nun D der quadratfreie Anteil von d, so sind $\frac{\beta_0}{\alpha_0}$ und $\frac{\delta_0}{\gamma_0} \in \mathbb{Q}(\sqrt{D})$. Denn es ist $\alpha_0\delta_0 - \beta_0\gamma_0 = 1$, also $\frac{\delta_0}{\gamma_0} - \frac{\beta_0}{\alpha_0} = \frac{1}{\alpha_0\gamma_0} = \frac{\sqrt{d}}{a_0} \in \mathbb{Q}(\sqrt{D})$, sowie $\sqrt{d}(\alpha_0\delta_0 + \beta_0\gamma_0) = b_0 \in \mathbb{Z}$, also $\frac{\delta_0}{\gamma_0} + \frac{\beta_0}{\alpha_0} = \frac{b_0}{\alpha_0\gamma_0\sqrt{d}} = \frac{b_0}{a_0} \in \mathbb{Q}$.

Setzt man $r + s\sqrt{D} = \frac{\beta_0}{\alpha_0}$ und $r' + s'\sqrt{D} = \frac{\delta_0}{\gamma_0}$ mit $r, s, r', s' \in \mathbb{Q}$, so ist für alle $x, y \in \mathbb{Z}$:

$$\begin{aligned} F_0(x,y) &= \alpha_0\gamma_0\sqrt{d}\left(x + \frac{\beta_0}{\alpha_0}y\right)\left(x + \frac{\delta_0}{\gamma_0}y\right) \\ &= a_0\left((x+ry) + sy\sqrt{D}\right)\left((x+r'y) + s'y\sqrt{D}\right) \\ &= a_0((x+ry)(x+r'y) + Dss'y^2 + ((x+ry)s'y + (x+r'y)sy)\sqrt{D}) \end{aligned}$$

ganzzahlig, und so ist also $(x+ry)s'y + (x+r'y)sy = 0$ für alle ganzen Zahlen x und y, insbesondere ist daher $rs' = -r's$ und $s' + rs' = -s - r's$, also $s' = -s$ und $r = r'$. Dies zeigt, daß $\frac{\beta_0}{\alpha_0}$ und $\frac{\delta_0}{\gamma_0}$ in $\mathbb{Q}(\sqrt{D})$ Konjugierte sind.

Daher ist auch $\frac{\alpha_n}{\alpha_0} = p'_n + r'_n\frac{\beta_0}{\alpha_0}$ konjugiert zu $p'_n + r'_n\frac{\delta_0}{\gamma_0} = \frac{\gamma_n}{\gamma_0}$ in $\mathbb{Q}(\sqrt{D})$ für alle $n \in \mathbb{Z}$, mit der ganzzahligen unimodularen Transformation $\begin{pmatrix} p'_n & q'_n \\ r'_n & s'_n \end{pmatrix}$ für F_n und F_0.

Insbesondere ist also $\omega = \frac{\alpha_0}{\alpha_g}$ konjugiert zu $\frac{\gamma_0}{\gamma_g} = \omega^{-1}$ in $\mathbb{Q}(\sqrt{D})$.

Und aus den Formeln (1.36) für λ_0 und μ_0 folgt nun, daß auch $\rho := \frac{\lambda_0}{\alpha_0}$ und $\rho' := \frac{\mu_0}{\gamma_0}$ in $\mathbb{Q}(\sqrt{D})$ konjugiert zueinander sind.

Nun ist zu zeigen, daß ξ_0 und η_0, mit

$$\begin{aligned} \lambda_0 &= \alpha_0\xi_0 + \beta_0\eta_0 \\ \text{und} \quad \mu_0 &= \gamma_0\xi_0 + \delta_0\eta_0, \end{aligned}$$

rational sind, man vergleiche dazu auch den Anfang des Unterabschnitts 1.3.1.

Aus diesen beiden Gleichungen folgt wegen $\alpha_0\delta_0 - \gamma_0\beta_0 = 1$:

$$\xi_0 = \delta_0\lambda_0 - \beta_0\mu_0 = \beta_0\delta_0\left(\rho\frac{\alpha_0}{\beta_0} - \rho'\frac{\gamma_0}{\delta_0}\right) = \frac{c_0}{\sqrt{d}}\left(\rho\frac{\alpha_0}{\beta_0} - \rho'\frac{\gamma_0}{\delta_0}\right)$$

und

$$\eta_0 = -\gamma_0\lambda_0 + \alpha_0\mu_0 = \alpha_0\gamma_0\left(\rho - \rho'\right) = \frac{a_0}{\sqrt{d}}\left(\rho' - \rho\right).$$

Die Klammerterme sind dabei Differenzen konjugierter Zahlen in $\mathbb{Q}(\sqrt{D})$ und somit rationale Vielfache von $\sqrt{D}$ bzw. $\sqrt{d}$. Dies zeigt, daß die Zahlen ξ_0 und η_0 rational sind.

Damit ist der Beweis von Teil **(2)** abgeschlossen. □

Die Arbeit, die jetzt noch zu leisten ist, ist der Beweis des Hauptlemmas (1.30) zur Existenz einer regulären Kette $(F_n)_{n\in\mathbb{Z}}$ zu F äquivalenter brauchbarer Formen. Dies geschieht im nächsten Unterabschnitt:

1.3.3 Beweis des Hauptlemmas

Zum Beweis des Hauptlemmas (1.30) werden zunächst einige Hilfslemmata und Lemmata formuliert und bewiesen:

1.3.3.A Hilfslemmata und Lemmata

Als erstes sind einige Hilfslemmata über positiv definite binärquadratische Formen notwendig:

(1.37) **Hilfslemma:** *Sei F eine positiv definite binärquadratische Form. Dann ist F äquivalent zu einer Form $F'(x,y) = A'x^2 + B'xy + C'y^2$ mit $|B'| \leqslant A'$.*

Beweis: Sei $F(x,y) = Ax^2 + Bxy + Cy^2$. Nach (1.12) ist dann $A = F(1,0) > 0$. Für ein $h \in \mathbb{Z}$ transformiere man F mittels $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ in die Form $F'(x,y) = A'x^2 + B'xy + C'y^2$ mit $A' = A,\ B' = 2Ah + B,\ C' =$

$C + Bh + Ah^2$. Hat man $h \in \mathbb{Z}$ nun so gewählt, daß $-\frac{1}{2} - \frac{B}{2A} \leqslant h \leqslant \frac{1}{2} - \frac{B}{2A}$, d.h. $|2Ah + B| \leqslant A$ ist, so ist also $|B'| \leqslant A'$. (Dieser Schluß wurde übrigens im Unterabschnitt 1.3.2 schon einmal verwendet.) $\square$

(1.38) **Hilfslemma:** *Sei F eine positiv definite binärquadratische Form. Dann existiert* $\min\{F(x,y);\ (x,y) \in \mathbb{Z}\backslash 0\}$.

Beweis: Man schreibe

$$F(x,y) = Ax^2 + Bxy + Cy^2 = A\left(x + \frac{B}{2A}y\right)^2 + \left(C - \frac{B^2}{4A}\right)y^2.$$

Nach (1.37) sei dabei ohne Einschränkung $|B| \leqslant A$. Weiter ist lediglich der Ausdruck $F'(x,y) = Ax^2 - |B|xy + Cy^2$ für $(x,y) \in \mathbb{N}^2$ auf Minimalität zu untersuchen:

Sei nun dazu $R > 1$ genügend groß, so, daß auch $R^2 > \frac{A}{C - \frac{B^2}{4A}}$. Für $y \geqslant R$ ist dann

$$F'(x,y) \geqslant \left(C - \frac{B^2}{4A}\right)y^2 \geqslant \left(C - \frac{B^2}{4A}\right)R^2 > A = F(1,0),$$

sowie, falls $y \leqslant R$ und $x \geqslant R$, gilt folgendes:

- Falls $A \neq |B|$, sei außerdem noch $R^2 > \frac{A}{A - |B|}$. Dann ist

$$\begin{aligned} F'(x,y) &\geqslant A\left(x - \frac{|B|}{2A}y\right)^2 = A|x|^2\left(1 - \frac{B}{2A}\left(\frac{y}{x}\right)\right)^2 \\ &\geqslant AR^2\left(1 - \frac{|B|}{A}\right) = R^2(A - |B|) > A = F(1,0). \end{aligned}$$

- Falls $A = |B|$, so ist

$$\begin{aligned} F'(x,y) &= Ax(x-y) + Cy^2 \geqslant Ax(x-R) + C \\ &\geqslant AR(\lceil R \rceil - R) + C \geqslant \frac{1}{2}AR + C > C = F(0,1), \end{aligned}$$

  wobei ohne Einschränkung R so groß sei, daß $\lceil R \rceil - R \geqslant \frac{1}{2}$ ist; dabei bezeichnet $\lceil\ \rceil$ die obere Gaußklammer.

F nimmt also seine kleinsten Werte in der endlichen Menge

$$\{(x,y) \in \mathbb{Z}^2;\ |x| \leqslant R \text{ und } |y| \leqslant R\}$$

an. Also existiert $\min\{F(x,y);\ (x,y) \in \mathbb{Z}\backslash 0\}$. $\square$

(1.39) **Definition:** *Eine positiv definite Form* $F(x,y) = Ax^2 + Bxy + Cy^2$ *heißt reduziert, falls* $|B| \leqslant A \leqslant C$ *gilt.*

(1.40) **Hilfslemma:** *Jede positiv definite binärquadratische Form ist äquivalent zu einer reduzierten Form.*

Beweis: Sei $F(x,y) = Ax^2+Bxy+Cy^2$ positiv definit. Weiter sei gemäß (1.38) dann $F(p,q) = \min\{F(x,y);\ (x,y) \in \mathbb{Z}^2\backslash 0\}$. Dabei sind $p, q \in \mathbb{Z}$ teilerfremd.

Denn sonst sei $p = ra$ und $q = sa$ mit $a > 1,\ r, s, a \in \mathbb{Z}$. Dann ist nämlich

$$F(p,q) = Ar^2a^2 + Brsa^2 + Cs^2a^2 = a^2F(r,s),$$

also $F(r,s) < F(p,q)$, im Widerspruch zur Minimalität von $F(p,q)$.

Daher existieren also ganze Zahlen u und v mit $pu - qv = 1$. Nun transformiere man F mittels $\begin{pmatrix} p & v \\ q & u \end{pmatrix}$ in die Form $F'(x,y) = A'x^2 + B'xy + C'y^2$, wobei $A' = Ap^2 + Bpq + Cq^2 = F(p,q)$ ist.

Nach (1.37) darf ferner $|B'| \leqslant A'$ angenommen werden, und weiter ist $A' \leqslant C'$ wegen der Minimaleigenschaft von A'. Also ist F' reduziert. $\square$

Nun werden diejenigen Lemmata formuliert und bewiesen, die in dieser Form für den Beweis Hauptlemmas verwendet werden:

(1.41) **Lemma:** *Ist* $F(x,y) = Ax^2 + Bxy + Cy^2$ *eine positiv definite Form mit* $B^2 - 4AC = -4$, *so ist* $\min\{F(x,y);\ (x,y) \in \mathbb{Z}^2\backslash 0\} \leqslant \sqrt{\frac{4}{3}}$.

Beweis: Nach (1.40) ist F äquivalent zu $F'(x,y) = A'x^2+B'xy+C'y^2$, die in (1.40) konstruierte Form mit $|B'| \leqslant A' \leqslant C'$, dabei bleibt $(B')^2 - 4A'C' = -4$ nach (1.25); das Minimum ist A' nach Konstruktion in (1.40). Somit gilt:

$$\begin{aligned} 4A'C' = (B')^2 + 4 \leqslant (A')^2 + 4, \quad \text{also} \\ -3(A')^2 + 4 = (A')^2 - 4(A')^2 + 4 \geqslant (A')^2 - 4A'C' + 4 \geqslant 0, \end{aligned}$$

und somit ist $A' \leqslant \sqrt{\frac{4}{3}}$. $\square$

(1.42) **Lemma:** *Für* $R > 0$ *sei*

$$Q_R(x,y) := R^2\,(\alpha x + \beta y)^2 + \frac{1}{R^2}\,(\gamma x + \delta y)^2\,,$$

wobei $\alpha, \beta, \gamma, \delta \in \mathbb{R}^\times,\ \frac{\alpha}{\beta}, \frac{\gamma}{\delta} \in \mathbb{R}\backslash\mathbb{Q}$ *und* $\alpha\delta - \beta\gamma = 1$ *sei. Dann ist* Q_R *positiv definit, und für* $R > 0$ *sei*

$$C_R := \min\{Q_R(x,y);\ (x,y) \in \mathbb{Z}^2\backslash 0\},$$

dies existiert, man vergleiche dazu auch (1.38)*. Dann gilt:*

(a) *Es ist*

$$\mathbb{R}_{>0} = \bigcup_{n\in\mathbb{Z}} [R_n, R_{n+1}]$$

mit einer Kette $(R_n)_{n\in\mathbb{Z}}$ *reeller Zahlen, und zwar mit* $R_m < R_n$ *für alle ganzen* $m < n$*, und es gilt*

$$\forall n \in \mathbb{Z}\ \exists x^n, y^n \in \mathbb{Z}\ \forall R \in [R_n, R_{n+1}] : \quad C_R = Q_R(x^n, y^n),$$

d.h. ist R *in einem Intervall* $[R_n, R_{n+1}]$*, so wird das Minimum* C_R *in immer demselben Punkt* $(x^n, y^n) \in \mathbb{Z}^2$ *angenommen. Dabei ist* $x^n > 0$ *wählbar.*

(b) *Für* $R > R_{n+1}$ *oder* $R < R_n$ *ist* $C_R \neq Q_R(x^n, y^n)$*, d.h. außerhalb von* $[R_n, R_{n+1}]$ *wird das Minimum* C_R *in einem anderen Punkt aus* $\mathbb{Z}^2$ *angenommen; dies gilt für beliebiges* $n \in \mathbb{Z}$*.*

(c) *Es gilt:*

$$\forall n \in \mathbb{Z} : \quad Q_{R_n}(x^n, y^n) = C_{R_n} = Q_{R_n}(x^{n-1}, y^{n-1}).$$

Bemerkung: Teil (c) folgt sofort aus Teil (a) mit $R := R_n$.

Beweis: Die Determinante der Form Q_R ist gleich der der Form

$$F_R(u, v) := R^2u^2 + \frac{1}{R^2}v^2$$

für $R > 0$, also $= 1 > 0$, aufgrund der linearen Transformation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit Determinante 1.

Und da F_R positiv definit ist, ist somit auch Q_R positiv definit. Nach (1.41) ist dann insbesondere $C_R \leqslant \sqrt{\frac{4}{3}}$.

Man betrachte nun das Gitter $\Gamma := \{(\alpha x + \beta y, \gamma x + \delta y);\ (x, y) \in \mathbb{Z}^2\}$, und $\Gamma^* := \Gamma\backslash 0$. Dabei hat Γ mit den beiden Koordinatenachsen in $\mathbb{Z}^2$ nur den Punkt 0 gemeinsam, da ja $\frac{\alpha}{\beta}$, $\frac{\gamma}{\delta}$ irrational sind.

Ferner sei $\bar{\Gamma} := \{(\alpha x+\beta y, \gamma x+\delta y);\ (x, y) \in \mathbb{N}\times\mathbb{Z}\}$. Für $R > 0$ betrachte man weiter die Form $F_R(u, v) := R^2u^2 + \frac{1}{R^2}v^2$, es ist also

$$C_R = \min\{F_R(u, v);\ (u, v) \in \Gamma^*\}.$$

Für ein $p \in \Gamma^*$ sei

$$M_p := \{R > 0;\ C_R = F_R(p)\}.$$

Und für zwei Gitterpunkte $p = (u, v),\ q = (r, s) \in \Gamma^*$ definiere man die Funktion $f_q^p : \mathbb{R}_{>0} \to \mathbb{R}$ vermöge

$$f_q^p(R) := R^2(u^2 - r^2) + \frac{1}{R^2}(v^2 - s^2) = F_R(p) - F_R(q).$$

Diese Funktion ist also stetig. Ferner hat f_q^p für $p \neq \pm q$ höchstens eine Nullstelle.

Es gilt:

$$0 = f_q^p(R) = R^2(u^2 - r^2) + \frac{1}{R^2}(v^2 - s^2) \ \Leftrightarrow\ R^4(u^2 - r^2) = s^2 - v^2.$$

- Dabei ist $u^2 = r^2 \Leftrightarrow (\alpha x + \beta y)^2 = (\alpha w + \beta z)^2$ mit $x, y, w, z \in \mathbb{Z}$, d.h. $u^2 = r^2 \Leftrightarrow \pm(\alpha x + \beta y) = \alpha w + \beta z \Leftrightarrow \alpha(\pm x - w) = \beta(z \mp y)$. Da nun $\frac{\alpha}{\beta}$ irrational ist, ist also $u^2 = r^2$ nur möglich, wenn $x = w$ und $y = z$, bzw. $x = -w$ und $y = -z$ sind. Dies widerspricht aber der Annahme, daß $p \neq \pm q$ ist.

- Ebenso unmöglich ist auch, daß $s^2 = v^2$ ist.

Daher schreibt sich obige Nullstellenbedingung als $R^4 = \frac{s^2 - v^2}{u^2 - r^2}$, die höchstens eine positive reelle Lösung für R hat.

Somit ist nach dem Zwischenwertsatz $\{R > 0;\ f_q^p(R) \leqslant 0\}$ ein in $\mathbb{R}_{>0}$ abgeschlossenes Intervall, und außerdem gilt:

$$F_R(p) \leqslant F_R(q) \Leftrightarrow f_q^p(R) \leqslant 0.$$

Somit gilt für ein $p \in \Gamma^*$:

$$\begin{aligned} M_p &= \{R > 0;\ C_R = F_R(p)\} = \{R > 0;\ \forall q \in \Gamma^* : F_R(p) \leqslant F_R(q)\} \\ &= \{R > 0;\ \forall q \in \Gamma^* : f_q^p(R) \leqslant 0\} = \bigcap_{q \in \Gamma^*} \{R > 0;\ f_q^p(R) \leqslant 0\}, \end{aligned}$$

d.h. M_p ist ein in $\mathbb{R}_{>0}$ abgeschlossenes Intervall.

Ferner ist, falls $M_p \neq \emptyset$, die Menge M_p ein Intervall endlicher Länge mit positiven Intervallgrenzen.

- Denn ist M_p nicht endlich, so existiert ein $R' > 0$ so, daß für alle $R \geqslant R'$ gilt:
$$R^2u^2 + \frac{1}{R^2}v^2 = F_R(p) = C_R \leqslant \sqrt{\frac{4}{3}},$$
wobei $p = (u, v) \in \Gamma^*$ ist, was aber wegen
$$R^2u^2 + \frac{1}{R^2}v^2 \geqslant R^2u^2@ >> R \to \infty > \infty, \text{ da } u \neq 0,$$
nicht sein kann.

- Ist $M_p = (0, R']$, so gilt für alle $0 < R \leqslant R'$:
$$R^2u^2 + \frac{1}{R^2}v^2 = F_R(p) = C_R \leqslant \sqrt{\frac{4}{3}},$$
wobei $p = (u, v) \in \Gamma^*$ ist, was aber wegen
$$R^2u^2 + \frac{1}{R^2}v^2 \geqslant \frac{1}{R^2}v^2@ >> R \to 0 > \infty, \text{ da } v \neq 0,$$
nicht sein kann.

Für Gitterpunkte $p, p' \in \Gamma^*$ mit $p \neq \pm p'$ ist weiter $|M_p \cap M_{p'}| \leqslant 1$. Denn sonst ist $I := M_p \cap M_{p'}$ ein in $\mathbb{R}$ abgeschlossenes Intervall positiver Länge, also ist für alle $q \in \Gamma^*$: $f_q^p(I) \leqslant 0$ und $f_q^{p'}(I) \leqslant 0$, insbesondere also $f_{p'}^p(I) \leqslant 0$ und $f_p^{p'} \leqslant 0$. Da nun $f_p^{p'} = -f_{p'}^p$, ist demnach $f_{p'}^p(I) = 0$, d.h. $f_{p'}^p$ hat unendlich viele positive Nullstellen, was nach obigem aber nur für $p = \pm p'$ möglich ist.

Es gilt nun:
$$\mathbb{R}_{>0} = \bigcup_{p \in \Gamma^*} M_p.$$
Denn »$\supseteq$« ist klar nach Definition der M_p, und »$\subseteq$«: Sei $R > 0$, dann gibt es wegen (1.38) ein $p \in \Gamma^*$ mit $C_R = F_R(p)$, d.h. es gilt $R \in M_p$.

Nun liegen in jedem Intervall $J = [\sigma, \tau]$ mit $\sigma, \tau \in \mathbb{R}_{>0}$ nur endlich viele der Intervalle M_p mit $p \in \Gamma^*$ und $|M_p| \geqslant 1$.

Denn sonst gibt es unendlich viele solche Intervalle M_p mit $\sigma \leqslant M_p \leqslant \tau$ zu unendlich vielen Gitterpunkten $p \in \Gamma^*$.

Für ein jedes solches p gilt dann $\forall R \in M_p : \ F_R(p) = C_R$, d.h. $p \in E_R \cap \Gamma$, wobei
$$E_R := \left\{ (u, v) \in \mathbb{R}^2; \ R^2u^2 + \frac{1}{R^2}v^2 = F_R(u, v) = C_R \right\}$$

eine Ellipse mit den Halbachsen $\frac{1}{R}\sqrt{C_R}$ und $R\sqrt{C_R}$ ist. Da $C_R \leqslant \sqrt{\frac{4}{3}}$ ist, liegt diese Ellipse ganz im Rechteck

$$W := \left\{ (u,v) \in \mathbb{R}^2;\ |u| \leqslant \frac{1}{\sigma}\sqrt[4]{\frac{4}{3}},\ |v| \leqslant \tau\sqrt[4]{\frac{4}{3}} \right\},$$

also $E_R \cap \Gamma \subseteq W \cap \Gamma$, d.h. es gibt unendlich viele Gitterpunkte p im beschränkten Gebiet W, Widerspruch.

Sei nun $\mathcal{P} := \{p \in \Gamma^*;\ |M_p| > 1,\ \text{und}\ p \in \bar{\Gamma}\}$. Damit ist wegen $M_p = M_{-p}$ und obigem gewährleistet, daß nur ein $p \in \mathcal{P}$ dieses Intervall M_p darstellt. Dann ist

$$\mathbb{R}_{>0} = \bigcup_{p\in\mathcal{P}} M_p.$$

»$\supseteq$«: Nach Definition von M_p. »$\subseteq$«: Sei $R > 0$ mit $R \in M_p$ und $p \in \bar{\Gamma}$. Weiter sei $M_p = \{R\}$, sonst ist $p \in \mathcal{P}$, und man ist fertig. Weiter sei $R \in J := [\sigma, \tau]$ mit $\sigma \neq R \neq \tau$. In J liegen insbesondere also nur endlich viele einpunktige Intervalle $M_{p'} \neq M_p$, etwa $M_{p_1}, \ldots, M_{p_m}$. Sei

$$\varepsilon := \min\{|s_i - R|;\ i \in \{1, \ldots, m\}\},$$

wobei $\{s_i\} = M_{p_i}$ für $i \in \{1, \ldots, m\}$ sei, es ist also $\varepsilon > 0$.

Daher liegt jedes $R + \frac{\varepsilon}{n}$ für $n \geqslant 2$ in einem Intervall M_q mit $|M_q| > 1$. Ab einem $n_0 \geqslant 2$ liegen die Punkte $R + \frac{\varepsilon}{n}$ mit $n \geqslant n_0$ dann alle indemselben Intervall M_q mit $|M_q| > 1$, da ja nur endlich viele Intervalle M_q ganz in J liegen. Dann aber ist auch $R \in M_q$, da M_q abgeschlossen ist.

Sei nun $\mathcal{M} := \{M_p;\ p \in \mathcal{P}\}$. Dann ist vermöge

$$M_p \lhd M_q \ :\Leftrightarrow\ M_p \leqslant M_q \ \text{oder}\ M_p = M_q$$

eine Ordnung auf $\mathcal{M}$ definiert.

Für ein $p \in \mathcal{P}$ sei nun $N(p)$ dasjenige $q \in \mathcal{P}$ mit $M_p \lhd M_q$ und so, daß $|M_p \cap M_q| = 1$. Dabei existiert q eindeutig, da die Intervalle $M_{p'}$ für $p' \in \mathcal{P}$ nach obigen $\mathbb{R}_{>0}$ ausschöpfen, in jedem Intervall mit positiven Intervallgrenzen nur endlich viele der $M_{p'}$ liegen können, und da sich je zwei in höchstens einem Punkt schneiden. Entsprechend sei $N^{-1}(p)$ dasjenige eindeutige $q \in \mathcal{P}$ mit $M_q \lhd M_p$ und so, daß $|M_p \cap M_q| = 1$. Weiter sei $N^0(p) := p$.

Dies liefert eine bijektive »Nachfolgerfunktion« $N : \mathcal{P} \to \mathcal{P}$ mit Inverser $N^{-1} : \mathcal{P} \to \mathcal{P}$. Weiter sei für $m > 0$ noch $N^{-m} := (N^{-1})^m$ definiert.

Für diese Abbildung gilt nun somit:

Es gibt für $p, q \in \mathcal{P}$ genau ein $m \in \mathbb{Z}$ mit $N^m(p) = q$. Denn sei J ein Intervall mit positiven Intervallgrenzen, das M_p und M_q ganz enthält, wobei ohne Einschränkung $p, q \in \mathcal{P}$ mit $M_p \triangleleft M_q$ seien. Darin liegen also nur endlich viele Intervalle $M_{p'}$ mit $p' \in \mathcal{P}$, etwa $M_{p_1}, \ldots, M_{p_{m-1}}$ seien alle Intervalle zwischen M_p und M_q mit $p_i \in \mathcal{P}$, d.h. $M_p \leqslant M_{p_i} \leqslant M_q$ für $i \in \{1, \ldots, m-1\}$. Dann aber ist $N^m(p) = q$, und dies kann nur für dieses eine $m \geqslant 1$ gelten. Analog geht diese Überlegung mit $M_q \triangleleft M_p$.

Jetzt definiere man die Funktion

$$\begin{aligned} f : \mathcal{M} &\to \mathbb{Z} \\ M_p &\mapsto m \quad \text{mit} \quad N^m(p_0) = p. \end{aligned}$$

Dies ist eine ordnungstreue Bijektion. Denn:

- f ist injektiv: Ist $f(M_p) = m = f(M_q)$, so ist $p = N^m(p_0) = q$, also $M_p = M_q$.
- f ist surjektiv: Für $m \in \mathbb{Z}$ setze man $p := N^m(p_0)$, dann ist $f(M_p) = m$.
- f ist ordnungstreu: Sei $M_p \triangleleft M_q$, dabei sei nun ohne Einschränkung $M_p \leqslant M_q$. Sei weiter $r := f(M_p)$, $s := f(M_q)$. Dann sei $m > 0$ mit $N^m(p) = q$. Daraus folgt, daß $N^m(N^r(p_0)) = N^s(p_0)$, also ist $m+r = s$, d.h. $r - s = -m < 0$, also $r < s$.

Sei nun R_n für $n \in \mathbb{Z}$ die linke Intervallgrenze von M_p mit $p = N^n(p_0)$, d.h. $n = f(M_p)$. Dann ist also $M_p = [R_n, R_{n+1}]$ aufgrund obiger Bijektion, und

$$\mathbb{R}_{>0} = \bigcup_{p \in \mathcal{P}} M_p = \bigcup_{n \in \mathbb{Z}} [R_n, R_{n+1}].$$

Dabei ist für alle $R \in [R_n, R_{n+1}]$: $C_R = F_R(p) = Q_R(x^n, y^n)$, wobei hier $p = N^n(p_0)$, und wo $p = (\alpha x^n + \beta y^n, \gamma x^n + \delta y^n)$ mit $x^n > 0$ sei. Es gilt also Teil (a).

Ist $R < R_n$ oder $R > R_{n+1}$, so ist $R \notin M_p$ mit $p = N^n(p_0)$, d.h. also $C_R \neq F_R(p) = Q_R(x^n, y^n)$, wo ebenso $p = (\alpha x^n + \beta y^n, \gamma x^n + \delta y^n)$ sei, aufgrund der Definition von M_p. Es gilt demnach auch (b). $\square$

(1.43) **Lemma:** *Sei $A > 1$ und $T : \mathbb{Z} \to \mathbb{R}_{>0}$ eine streng monoton wachsende Funktion mit $T(n)@ >> n \to -\infty > 0$ und $T(n)@ >> n \to +\infty > \infty$. Dann existiert eine Kette $(n_k)_{k \in \mathbb{Z}}$ mit $n_{k+1} > n_k$ sowie*

$$\forall k \in \mathbb{Z} : \quad AT(n_k) \leqslant T(n_{k+1}) < A^2 T(n_k + 1). \tag{1.44}$$

Bemerkung: Die beiden Ungleichungen (1.44) lassen sich auch durch

$$\forall k \in \mathbb{Z}: \quad \frac{1}{A^2} T(n_{k+1} - 1) < T(n_k) \leqslant \frac{1}{A} T(n_{k+1}). \tag{1.45}$$

ersetzen, ohne die Aussage der Behauptung zu verändern.

Beweis: Denn wendet man das Lemma in der Form (1.44) an auf die Funktion $U(m) := \frac{1}{T(-m)}$, die obige Voraussetzungen erfüllt, so gibt es eine Kette $(m_l)_{l \in \mathbb{Z}}$, streng monoton wachsend, mit

$$A \frac{1}{T(-m_l)} \leqslant \frac{1}{T(-m_{l+1})} < A^2 \frac{1}{T(-m_l - 1)}.$$

Setzt man nun $-n_{-k} := m_k$ für $k \in \mathbb{Z}$ (es ist dann auch $(-n_{-k})_{k \in \mathbb{Z}}$ streng monoton wachsend), so ist

$$A \frac{1}{T(n_{-k})} \leqslant \frac{1}{T(n_{-k-1})} < A^2 \frac{1}{T(n_{-k} - 1)},$$

d.h.

$$\frac{1}{A^2} T(n_{-k} - 1) < T(n_{-k-1}) \leqslant \frac{1}{A} T(n_{-k}).$$

Ersetzt man hier nun $-k$ durch $k + 1 \in \mathbb{Z}$, so hat man (1.45).

Ebenso kommt man von (1.45) wieder zurück zu den Ungleichungen (1.44). $\square$

Nun wird der **Beweis** für (1.43) in der Form (1.44) geführt:

- Fall 1: Sei $\forall n \in \mathbb{Z}: T(n+1) < AT(n)$.

  Sei $n_0 \in \mathbb{Z}$ beliebig, und definiere dazu $n_1, n_2, n_3, \ldots$ rekursiv vermöge der Bedingung

  $$\forall k \geqslant 0: \quad T(n_{k+1} - 1) < AT(n_k) \leqslant T(n_{k+1}).$$

  Denn dies ist möglich wegen $T(n+1) > T(n)$ für alle $n \in \mathbb{Z}$ und $T(n)@ >> n \to \infty > \infty$: Für ein $n_k \in \mathbb{Z}$ sei $n_{k+1} \in \mathbb{Z}$ dasjenige eindeutig bestimmte $m \in \mathbb{Z}$ mit $T(m-1) < AT(n_k) \leqslant T(m)$.

  Da nun $A > 1$, ist dann $n_{k+1} > n_k$ für $k \geqslant 0$, und $AT(n_k) \leqslant T(n_{k+1})$, die erste Ungleichung von (1.44). Ferner ist auch in diesem Fall 1:

  $$T(n_{k+1}) < AT(n_{k+1} - 1) < A^2 T(n_k) < A^2 T(n_k + 1),$$

die zweite Ungleichung von (1.44).

Nun definiere man noch $n_{-1}, n_{-2}, n_{-3}, \ldots$ rekursiv vermöge der Bedingung

$$T(n_k) \leqslant \frac{1}{A} T(n_{k+1}) < T(n_k + 1).$$

(Ähnlich wie oben, da $T(n)@ >> n \to -\infty > 0$.) Dann ist $n_{k+1} > n_k$ für $k \leqslant -1$, und es gilt

$$AT(n_k) \leqslant T(n_{k+1}) < AT(n_k + 1) < A^2 T(n_k + 1),$$

da $A > 1$.

- Fall 2: Sei $T(n+1) \geqslant AT(n)$ für gewisse $n \in \mathbb{Z}$, die nach oben beschränkt sind.

  Sei $n_0 \in \mathbb{Z}$ größer als die größte dieser Zahlen $n \in \mathbb{Z}$, so daß $\forall n \geqslant n_0 :\ T(n+1) < AT(n)$. Dann läßt sich auch hier der Beweis von Fall 1 führen, da dort diese Ungleichung lediglich für $n = n_{k+1} - 1 \geqslant n_k \geqslant n_0$ mit $k \geqslant 0$ angewandt wurde.

- Fall 3: Ansonsten sei $(g_r)_{r \in \mathbb{N}}$ eine streng monoton wachsende Folge ganzer Zahlen mit $T(g_r + 1) \geqslant AT(g_r)$ für alle $r \in \mathbb{N}$.

  Definiere nun $n_0^{(r)}, n_{-1}^{(r)}, n_{-2}^{(r)}, \ldots$ vermöge $n_0^{(r)} := g_r$, und für $k \leqslant -1$ werde $n_k^{(r)}$ definiert vermöge

  $$T\left(n_k^{(r)}\right) \leqslant \frac{1}{A} T\left(n_{k+1}^{(r)}\right) < T\left(n_k^{(r)} + 1\right),$$

  man vergleiche dazu den Fall 1. Sei ferner $\mathcal{N}^{(r)} := \left\{ n_0^{(r)}, n_{-1}^{(r)}, n_{-2}^{(r)}, \ldots \right\}$. Dann ist also

  $$AT\left(n_k^{(r)}\right) \leqslant T\left(n_{k+1}^{(r)}\right) < A^2 T\left(n_k^{(r)} + 1\right) \tag{1.46}$$

  für je zwei aufeinanderfolgende $n_k^{(r)}$ aus $\mathcal{N}^{(r)}$.

  Nun ist $\mathcal{N}^{(r)} \subseteq \mathcal{N}^{(r+1)}$.

  Denn man definiere nun ein $k \in \mathbb{Z},\ k \leqslant -1$, vermöge

  $$n_k^{(r+1)} \leqslant g_r < n_{k+1}^{(r+1)}.$$

  (Dies ist möglich wegen $n_0^{(r+1)} = g_{r+1} > g_r$ für alle $r \in \mathbb{N}$, da hier $\left(n_k^{(r+1)}\right)_{k \in \mathbb{Z}}$ eine streng monoton wachsende Kette ist. Insbesondere ist $k \leqslant -1$.)

Dann ist $\frac{1}{A}T\left(n_{k+1}^{(r+1)}\right) < T\left(n_k^{(r+1)}+1\right)$. Ferner ist aber

$$T\left(n_{k+1}^{(r+1)}\right) \geqslant T(g_r+1) \geqslant AT(g_r);$$

also ist $T(g_r) < T\left(n_k^{(r+1)}+1\right)$. Somit ist $g_r \leqslant n_k^{(r+1)}$, und daher sogar $g_r = n_k^{(r+1)}$. Und so ist $g_r \in \mathcal{N}^{(r+1)}$, und deswegen sind auch die $n_{-1}^{(r)}, n_{-2}^{(r)}, n_{-3}^{(r)}, \cdots \in \mathcal{N}^{(r+1)}$ aufgrund deren Konstruktion.

Man definiere nun $(n_k)_{k\in\mathbb{Z}}$ als Kette ganzer Zahlen vermöge

$$(n_k)_{k\in\mathbb{Z}} = \bigcup_{r\in\mathbb{N}} \mathcal{N}^{(r)}.$$

Dann sind zwei aufeinanderfolgende Glieder n_k und n_{k+1} auch in einem $\mathcal{N}^{(r)}$ aufeinanderfolgend für ein hinreichend großes $r \in \mathbb{N}$. Und für diese gilt ja (1.46), und das ist die Behauptung. $\square$

Damit sind nun alle für das Hauptlemma benötigten Hilfsmittel bereitgestellt.

1.3.3.B Der eigentliche Beweis des Hauptlemmas

Sei nun also

$$F(x,y) = \sqrt{d}(\alpha x+\beta y)(\gamma x+\delta y),$$

wo $\frac{\alpha}{\beta}, \frac{\gamma}{\delta} \in \mathbb{R}\backslash\mathbb{Q}$ und $\alpha\delta-\beta\gamma = 1$. Zum Parameter $R > 0$ betrachte man dann

$$Q_R(x,y) := R^2(\alpha x+\beta y)^2 + \frac{1}{R^2}(\gamma x+\delta y)^2.$$

Nach Lemma (1.42) ist Q_R positiv definit von der Determinante 1 für jedes $R > 0$, und man bekommt eine Zerlegung

$$\mathbb{R}_{>0} = \bigcup_{n\in\mathbb{Z}} [R_n, R_{n+1}]$$

von $\mathbb{R}_{>0}$ in abgeschlossene Intervalle, in denen die Form Q_R stets in ein und demselben Punkt ihr Minimum für $(x,y) \in \mathbb{Z}^2\backslash 0$ annimmt.

Für $n \in \mathbb{Z}$ sei (x^n, y^n) (in der dortigen Notation) dieser Punkt, und man setze nun

$$\begin{aligned} \alpha_n &:= \alpha x^n + \beta y^n \\ \text{und} \quad \gamma_n &:= \gamma x^n + \delta y^n. \end{aligned}$$

Die so definierten Ketten $(\alpha_n)_{n\in\mathbb{Z}}$ und $(\gamma_n)_{n\in\mathbb{Z}}$ werden zur Definition einer regulären Kette im Sinne des Hauptlemmas zu Hilfe genommen. Zunächst einmal gilt:

$$\forall n \in \mathbb{Z}: \quad |\alpha_{n+1}| < |\alpha_n| \text{ und } |\gamma_{n+1}| > |\gamma_n|. \tag{1.47}$$

Denn wegen Lemma (1.42), Teil (c), ist ja

$$Q_{R_{n+1}}(x^n, y^n) = Q_{R_{n+1}}(x^{n+1}, y^{n+1}),$$

also

$$R_{n+1}^2\alpha_n^2 + \frac{1}{R_{n+1}^2}\gamma_n^2 = R_{n+1}^2\alpha_{n+1}^2 + \frac{1}{R_{n+1}^2}\gamma_{n+1}^2,$$

woraus die Gleichung

$$\gamma_{n+1}^2 - \gamma_n^2 = R_{n+1}^4(\alpha_n^2 - \alpha_{n+1}^2) \tag{1.48}$$

folgt, für alle $n \in \mathbb{Z}$. Weiter gilt wegen Lemma (1.42), Teil (b), daß

$$Q_{R_{n+1}}(x^{n+1}, y^{n+1}) < Q_{R_{n+1}}(x^{n+2}, y^{n+2}),$$

also

$$R_{n+1}^2\alpha_{n+1}^2 + \frac{1}{R_{n+1}^2}\gamma_{n+1}^2 < R_{n+1}^2\alpha_{n+2}^2 + \frac{1}{R_{n+1}^2}\gamma_{n+2}^2,$$

und daher ist mit (1.48) dann

$$\begin{aligned}
\alpha_n^2 - \alpha_{n+2}^2 &< \frac{1}{R_{n+1}^4}(\gamma_{n+2}^2 - \gamma_n^2) \\
&= \frac{1}{R_{n+1}^4}(\gamma_{n+2}^2 - \gamma_{n+1}^2 + \gamma_{n+1}^2 - \gamma_n^2) \\
&= \frac{1}{R_{n+1}^4}(R_{n+2}^4(\alpha_{n+1}^2 - \alpha_{n+2}^2) + R_{n+1}^4(\alpha_n^2 - \alpha_{n+1}^2)) \\
&= \left(\frac{R_{n+2}}{R_{n+1}}\right)^4(\alpha_{n+1}^2 - \alpha_{n+2}^2) + (\alpha_n^2 - \alpha_{n+1}^2), \quad \text{also ist} \\
0 &< \left(\frac{R_{n+2}}{R_{n+1}}\right)^4(\alpha_{n+1}^2 - \alpha_{n+2}^2) + (\alpha_{n+2}^2 - \alpha_{n+1}^2) \\
&= (\alpha_{n+1}^2 - \alpha_{n+2}^2) \cdot \left(\left(\frac{R_{n+2}}{R_{n+1}}\right)^4 - 1\right),
\end{aligned}$$

wobei die letzte Klammer im letzten Term > 0 ist, und somit ist nun also $\alpha_{n+1}^2 > \alpha_{n+2}^2$, d.h. für alle $n \in \mathbb{Z}$ ist $|\alpha_{n+1}| < |\alpha_n|$. Die Gleichung (1.48) ergibt weiter auch, daß $|\gamma_{n+1}| > |\gamma_n|$ ist für alle $n \in \mathbb{Z}$. Und somit hat man gerade die beiden zu zeigenden Ungleichungen (1.47).

Da nun Lemma (1.41) auf die Form Q_R anwendbar ist, gilt für alle $n \in \mathbb{Z}$:

$$Q_{R_n}(x^{n-1}, y^{n-1}) = Q_{R_n}(x^n, y^n) \leqslant \sqrt{\frac{4}{3}},$$

also

$$R_n^2\alpha_{n-1}^2 + \frac{1}{R_n^2}\gamma_{n-1}^2 = R_n^2\alpha_n^2 + \frac{1}{R_n^2}\gamma_n^2 \leqslant \sqrt{\frac{4}{3}}, \tag{1.49}$$

und somit

$$|\alpha_n\gamma_n| = \sqrt{R_n^2\alpha_n^2\frac{1}{R_n^2}\gamma_n^2} \leqslant \frac{1}{2}\left(R_n^2\alpha_n^2 + \frac{1}{R_n^2}\gamma_n^2\right) \leqslant \frac{1}{\sqrt{3}} < 1, \tag{1.50}$$

für alle $n \in \mathbb{Z}$. Nun ist

$$\begin{aligned}\alpha_n\gamma_{n-1} - \alpha_{n-1}\gamma_n &\\ &= (\alpha x^n + \beta y^n)(\gamma x^{n-1} + \delta y^{n-1}) - (\alpha x^{n-1} + \beta y^{n-1})(\gamma x^n + \delta y^n)\\ &= (x^n y^{n-1} - y^n x^{n-1})(\alpha\delta - \beta\gamma) = x^n y^{n-1} - y^n x^{n-1} \in \mathbb{Z}\backslash 0,\end{aligned}$$

da man sonst für $\frac{x^n}{y^n} = \frac{x^{n-1}}{y^{n-1}}$, also $x^n = ax^{n-1}$ und $y^n = ay^{n-1}$ mit $a \in \mathbb{N}_{>1}$ dann

$$Q_{R_n}(x^{n-1}, y^{n-1}) \cdot a^2 = Q_{R_n}(x^n, y^n)$$

hätte. (Man beachte dabei: Es ist $x^n > 0$ für alle $n \in \mathbb{Z}$, man vergleiche dazu auch den Beweis von (1.42).)

Also ist

$$|\alpha_n\gamma_{n-1}| + |\alpha_{n-1}\gamma_n| \geqslant |\alpha_n\gamma_{n-1} - \alpha_{n-1}\gamma_n| \geqslant 1.$$

Wegen (1.47) folgt daraus $|\alpha_{n-1}\gamma_n| \geqslant \frac{1}{2}$, und daraus mit (1.49) dann

$$\begin{aligned}|\alpha_{n-1}| \geqslant \frac{1}{2}\frac{1}{|\gamma_n|} \geqslant \frac{1}{2}\sqrt[4]{\frac{3}{4}}\frac{1}{R_n} \quad \text{und}\\ |\gamma_n| \geqslant \frac{1}{2}\frac{1}{|\alpha_{n-1}|} \geqslant \frac{1}{2}\sqrt[4]{\frac{3}{4}}R_n,\end{aligned}$$

also gilt

$$\begin{cases}\frac{1}{2}\sqrt[4]{\frac{3}{4}}\frac{1}{R_n} \leqslant |\alpha_{n-1}| \leqslant \sqrt[4]{\frac{4}{3}}\frac{1}{R_n} \quad \text{und}\\ \frac{1}{2}\sqrt[4]{\frac{3}{4}}R_n \leqslant |\gamma_n| \leqslant \sqrt[4]{\frac{4}{3}}R_n.\end{cases} \tag{1.51}$$

Nun setze man für $n \in \mathbb{Z}$ weiter $p_n := x^n$ und $r_n := y^n$. Damit ist dann

$$\begin{aligned} \alpha_n &= p_n\alpha + r_n\beta \\ \text{und} \quad \gamma_n &= p_n\gamma + r_n\delta. \end{aligned}$$

Da p_n und r_n teilerfremd sind (man vergleiche dazu den Anfang des Beweises von (1.40)), so gibt es dazu $q_n, s_n \in \mathbb{Z}$ mit $p_n s_n - q_n r_n = 1$.

Dies liefert eine ganzzahlige unimodulare Transformation $\begin{pmatrix} p_n & r_n \\ q_n & s_n \end{pmatrix}$ vermöge (1.27): Mit

$$\begin{aligned} \beta_n &:= q_n\alpha + s_n\beta \\ \text{und} \quad \delta_n &:= q_n\gamma + s_n\delta \end{aligned}$$

ist dann die Form

$$F_n(x,y) := \sqrt{d}(\alpha_n x + \beta_n y)(\gamma_n x + \delta_n y)$$

somit äquivalent zu F für jedes $n \in \mathbb{Z}$, und daher auch brauchbar. Aus dieser Kette $(F_n)_{n\in\mathbb{Z}}$ zu F äquivalenter Formen wähle man nun nur noch eine gemäß (1.29) reguläre Teilkette aus:

Wegen (1.50) ist die dritte Ungleichung »$|\alpha_n\gamma_n| \leqslant \vartheta < 1$« von (1.29) mit $\vartheta := \frac{1}{\sqrt{3}} < 1$ automatisch erfüllt.

Zu zeigen ist noch die Existenz von $(n_k)_{k\in\mathbb{Z}}$ mit $n_k < n_{k+1}$ für alle $k \in \mathbb{Z}$ so, daß für ein $C > 1$ und $B = B(C) > 0$ gilt:

$$\begin{aligned} |\alpha_{n_{k+1}}| &\leqslant \frac{1}{C}|\alpha_{n_k}|, \\ |\gamma_{n_{k+1}}| &\geqslant C|\gamma_{n_k}|, \quad \text{und} \\ |\alpha_{n_k}\gamma_{n_{k+1}}| &< B^2. \end{aligned}$$

Im Zusammenhang mit (1.51) genügt es weiter, die Existenz einer streng monoton steigenden Kette $(n_k)_{k\in\mathbb{Z}}$ zu zeigen, die mit $R(m) := R_m$ und mit $A' := A^4$ für beliebiges $A > 1$ erfüllt:

$$\begin{aligned} R(n_{k+1}) &\geqslant AR(n_k), \\ R(n_{k+1}+1) &\geqslant AR(n_k+1), \quad \text{und} \\ R(n_{k+1}) &< A'R(n_k+1), \end{aligned}$$

für alle $k \in \mathbb{Z}$.

Denn setzt man, wenn dies bewiesen ist, $C > 1$ so, daß $A = 2\sqrt{\frac{4}{3}}C > 1$, so ist nach (1.51) dann

$$|\gamma_{n_{k+1}}| \geqslant \frac{1}{2}\sqrt[4]{\frac{3}{4}}R(n_{k+1}) \geqslant \frac{1}{2}\sqrt[4]{\frac{3}{4}}AR(n_k) \geqslant \frac{1}{2}\sqrt[4]{\frac{3}{4}}A\sqrt[4]{\frac{3}{4}}|\gamma_{n_k}| = C|\gamma_{n_k}|,$$

$$|\alpha_{n_{k+1}}| \leqslant \sqrt[4]{\frac{4}{3}}R^{-1}(n_{k+1}+1) \leqslant \sqrt[4]{\frac{4}{3}}\frac{1}{A}R^{-1}(n_k+1)$$

$$\leqslant \frac{1}{A}\sqrt[4]{\frac{4}{3}}\cdot 2\sqrt[4]{\frac{4}{3}}|\alpha_{n_k}| = \frac{1}{C}|\alpha_{n_k}|,$$

und

$$|\alpha_{n_k}\gamma_{n_{k+1}}| \leqslant \sqrt{\frac{4}{3}}R^{-1}(n_k+1)R(n_{k+1})$$

$$< \sqrt{\frac{4}{3}}R^{-1}(n_{k+1})A'R(n_{k+1}) = A'\sqrt{\frac{4}{3}},$$

d.h. mit

$$B := \sqrt{A'}\sqrt[4]{\frac{4}{3}} = A^2\sqrt[4]{\frac{4}{3}} = 4\cdot\left(\frac{4}{3}\right)C^2\left(\frac{4}{3}\right)^{\frac{1}{4}} = 4\cdot\left(\frac{4}{3}\right)^{\frac{5}{4}}C^2$$

ist dann obiges erfüllt.

Um nun dies zu zeigen, wendet man das Lemma (1.43) in der Form (1.44) an auf die Funktion $T(m) := R(m)$ für $m \in \mathbb{Z}$, und man erhält so eine Kette $(m_j)_{j\in\mathbb{Z}}$ ganzer Zahlen mit $m_{j+1} > m_j$ für alle $j \in \mathbb{Z}$, und mit

$$AR(m_j) \leqslant R(m_{j+1}) < A^2R(m_j+1)$$

für ein $A > 1$ beliebig. Man definiere nun Ketten $(S(j))_{j\in\mathbb{Z}}$ und $(S_1(j))_{j\in\mathbb{Z}}$ vermöge $S(j) := R(m_j)$ und $S_1(j) := R(m_j+1)$, dann ist also

$$AS(j) \leqslant S(j+1) < A^2S_1(j).$$

Anwenden des Lemmas (1.43) in der Form (1.45) liefert dann noch eine Kette $(j_k)_{k\in\mathbb{Z}}$ ganzer Zahlen mit $j_{k+1} > j_k$ für alle $k \in \mathbb{Z}$. Nun ist

$$S(j_{k+1}) \geqslant S(j_k+1) \geqslant AS(j_k)$$

$$\text{und } S_1(j_{k+1}) \geqslant AS_1(j_k),$$

$$\text{sowie } S(j_{k+1}) < A^2S_1(j_{k+1}-1) < A^4S_1(j_k).$$

Setzt man nun $n_k := m_{j_k}$ für $k \in \mathbb{Z}$, dann ist nämlich $R(n_k) = S(j_k)$, $R(n_k+1) = S_1(j_k)$, und mit $A' := A^4$ ist wie gewünscht für alle $k \in \mathbb{Z}$ also

$$\begin{aligned} R(n_{k+1}) = S(j_{k+1}) &\geqslant AS(j_k) = AR(n_k), \\ R(n_{k+1}+1) = S_1(j_{k+1}) &\geqslant AS_1(j_k) = AR(n_k+1), \quad \text{und} \\ R(n_{k+1}) = S(j_{k+1}) &< A^4 S_1(j_k) = A'R(n_k+1). \end{aligned}$$

Damit ist dann das Hauptlemma und alles andere bewiesen. □ □

1.4 Ergebnisse

Der umfangreiche Beweis des Satzes von DAVENPORT macht deutlich, wie schwierig die Frage nach euklidischen reellquadratischen Körpern tatsächlich ist. Doch mit diesem Satz wurde viel erreicht: Es ist möglich, eine Konstante $\kappa > 0$ zu bestimmen, so daß $\mathbb{Q}(\sqrt{m})$ für alle $m > \kappa^{-4}$ nicht euklidisch ist.

In seiner ersten Arbeit [7] fand DAVENPORT selbst den Wert $\kappa^2 = \frac{1}{128}$. Mit anderen Mitteln bewies CASSELS in [3] den Satz von DAVENPORT erneut und verbesserte die Konstante κ zu $\kappa^2 = \frac{1}{51}$. Um eine Liste der euklidischen reellquadratischen Zahlkörper zu erstellen, war daher nur noch die Untersuchung der $\mathbb{Q}(\sqrt{m})$ mit $1 < m \leqslant 51^2 = 2601$ erforderlich. Dazu sei hier lediglich folgendes Teilresultat bewiesen: (Nach dem Buch [10] von G.H. HARDY und E.M. WRIGHT.)

(1.52) **Satz:** $\mathbb{Q}(\sqrt{m})$ *ist euklidisch für*

$$\boxed{m \in \{2,3,5,6,7,13,17,21,29\}.}$$

Beweis: Für $\zeta \in \mathbb{Q}(\sqrt{m})$, etwa $\zeta = r + s\sqrt{m}$ mit $r, s \in \mathbb{Q}$, und für $\vartheta \in \mathbb{Q}(\sqrt{m}) \cap \mathbb{A}$, etwa

$$\begin{cases} \vartheta = x + y\sqrt{m}, \ \text{wo } x, y \in \mathbb{Z}, & \text{falls } m \equiv 2,3 \pmod 4, \\ \vartheta = x + \frac{1}{2}(1+\sqrt{m})y, \ \text{wo } x, y \in \mathbb{Z}, & \text{falls } m \equiv 1 \pmod 4, \end{cases}$$

ist

$$|N(\zeta - \vartheta)| = \begin{cases} |(r-x)^2 - m(s-y)^2|, & \text{falls } m \equiv 2,3 \pmod 4, \\ |(r-x-\frac{1}{2}y)^2 - m(s-\frac{1}{2}y)^2|, & \text{falls } m \equiv 1 \pmod 4, \end{cases}$$

wie schon im Beweis zu Satz (1.2) zu sehen war. Schreibt man nun $\lambda := 0$, $n := m$ für $m \equiv 2,3 \pmod 4$, sowie $\lambda := \frac{1}{2}$, $n := \frac{1}{4}m$ für $m \equiv 1 \pmod 4$, und $2s$ statt s für $m \equiv 1 \pmod 4$, so läßt sich dies auch kurz schreiben als

$$|N(\zeta - \vartheta)| = |(r - x - \lambda y)^2 - n(s-y)^2|.$$

Angenommen, $\mathbb{Q}(\sqrt{m})$ sei nicht euklidisch. Dann ist

$$|(r-x-\lambda y)^2 - n(s-y)^2| \geqslant 1 \tag{1.53}$$

für gewisse $r, s \in \mathbb{Q}$ und alle $x, y \in \mathbb{Z}$.

Dabei darf man $0 \leqslant r \leqslant \frac{1}{2}$ und $0 \leqslant s \leqslant \frac{1}{2}$ annehmen.

- Falls $m \equiv 2, 3 \pmod 4$, ist $|(r-x)^2 - m(s-y)^2|$ die linke Seite von (1.53). Diese ändert sich nicht, wenn man r, x, s, y durch $\varepsilon_1 r + u, \varepsilon_1 x + u, \varepsilon_2 s + v, \varepsilon_2 y + v$ ersetzt, wobei $u, v \in \mathbb{Z}$, $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$. Dabei lassen sich $\varepsilon_1, \varepsilon_2, u, v$ so wählen, daß

$$0 \leqslant \varepsilon_1 r + u \leqslant \frac{1}{2} \quad \text{und}$$
$$0 \leqslant \varepsilon_2 s + v \leqslant \frac{1}{2}$$

  sind.

- Falls $m \equiv 1 \pmod 4$, ist $|(r - x - \frac{1}{2}y)^2 - \frac{1}{4}m(s-y))^2|$ die linke Seite von (1.53). Diese ändert sich nicht, wenn man r, x, s, y durch

$$\begin{array}{llllll}
(1.) & \varepsilon_1 r + u, & \varepsilon_1 x + u, & \varepsilon_1 s, & \varepsilon_1 y, & \\
(2.) & r, & x - v, & s + 2v, & y + 2v, & \\
(3.) & r, & x + y, & -s, & -y, & \text{oder} \\
(4.) & \frac{1}{2} - r, & -x, & 1 - s, & 1 - y &
\end{array}$$

  ersetzt, wobei $u, v \in \mathbb{Z}$ und $\varepsilon_1 \in \{\pm 1\}$. Mittels (1.) erreicht man $0 \leqslant r \leqslant \frac{1}{2}$, und mittels (2.) erreicht man dann $-1 \leqslant s \leqslant 1$, und falls nötig, liefert (3.) dann $0 \leqslant x \leqslant 1$. Falls nun $\frac{1}{2} \leqslant x \leqslant 1$ ist, liefert (4.) weiter $0 \leqslant s \leqslant \frac{1}{2}$, was ja erlaubt ist wegen $0 \leqslant \frac{1}{2} - r \leqslant \frac{1}{2}$.

Daher gibt es nun $r, s \in \mathbb{Q}$ so, daß immer eine der beiden Ungleichungen (für alle $x, y \in \mathbb{Z}$)

$$\begin{array}{ll}
[P(x,y)] & (r-x-\lambda y)^2 \geqslant 1 + n(s-y)^2 \\
[N(x,y)] & n(s-y)^2 \geqslant 1 + (r-x-\lambda y)^2
\end{array}$$

gültig ist. Insbesondere sind

$$\begin{array}{llll}
[P(0,0)] & r^2 \geqslant 1 + ns^2, & [N(0,0)] & ns^2 \geqslant 1 + r^2, \\
[P(1,0)] & (1-r)^2 \geqslant 1 + ns^2, & [N(1,0)] & ns^2 \geqslant 1 + (1-r)^2, \\
[P(-1,0)] & (1+r)^2 \geqslant 1 + ns^2, & [N(-1,0)] & ns^2 \geqslant 1 + (1+r)^2.
\end{array}$$

Mindestens eine dieser Ungleichungen eines jeden Paares ist für gewisse $r, s \in \mathbb{Q}$ mit $0 \leqslant r, s \leqslant \frac{1}{2}$ richtig. Für $r = 0 = s$ sind jedoch $[P(0,0)]$ und $[N(0,0)]$ falsch und dies daher ausgeschlossen. Da nun $0 \leqslant r, s \leqslant \frac{1}{2}$ und $(r,s) \neq (0,0)$, sind $[P(0,0)]$ und $[P(1,0)]$ falsch, also $[N(0,0)]$ und $[N(1,0)]$ richtig.

Wäre nun $[P(-1,0)]$ richtig, so würden $[N(1,0)]$ und $[P(-1,0)]$ liefern, daß $(1+r)^2 \geqslant 1+ns^2 \geqslant 2+(1-r)^2$, also $4r \geqslant 2$ sei. Wegen $0 \leqslant r \leqslant \frac{1}{2}$ wäre daher $r = \frac{1}{2}$, also $ns^2 = \frac{5}{4}$. Dies ist aber unmöglich:

Sei etwa $s = \frac{p}{q}$ mit $p, q \in \mathbb{Z}$ teilerfremd, wo $q \neq 0$.

- Für $m \equiv 2,3 \pmod 4$ ist dann $m = n$ und $4mp^2 = 5q^2$, also $p^2|5$, d.h. $p = 1$, und $q^2|4m$. Da nun aber m quadratfrei und $0 \leqslant s \leqslant \frac{1}{2}$, ist $q = 2$, $s = \frac{1}{2}$ und $m = 5 \equiv 1 \pmod 4$, Widerspruch.

- Für $m \equiv 1 \pmod 4$ ist dann $m = 4n$ und $mp^2 = 5q^2$, so daß $p = 1$, $q = 1$, und $s = 1$ folgt, im Widerspruch zu $0 \leqslant s \leqslant \frac{1}{2}$.

Also ist $[P(-1,0)]$ falsch und somit $[N(-1,0)]$ richtig. Das ergibt

$$ns^2 \geqslant 1 + (1+r)^2 \geqslant 2,$$

und mit $0 \leqslant s \leqslant \frac{1}{2}$ ist dann $n \geqslant 8$.

In allen Fällen, in denen $n < 8$ ist, ist dann aber $\mathbb{Q}(\sqrt{m})$ euklidisch, also für

$$m \in \{2,3,5,6,7,13,17,21,29\}. \quad \square$$

Mit der Arbeit [4] von H. Chatland und anderen, etwa der Arbeit [5] von H. Chatland und H. Davenport, war dann nach 1950 schon bald die vollständige Liste aller euklidischer reellquadratischer Zahlkörper bekannt:

(1.54) **Satz:** $\mathbb{Q}(\sqrt{m})$ *mit* $m > 1$ *quadratfrei ist euklidisch genau für*

$$\boxed{m \in \{2,3,5,6,7,13,17,21,29,33,37,41,57,73\}.}$$

Insbesondere sind diese reellquadratischen Zahlkörper auch faktoriell. Es gibt aber noch viel mehr faktorielle reellquadratische Zahlkörper, und man weiß bis heute nicht, ob es überhaupt endlich oder unendlich viele solcher Zahlkörper gibt. Ein Lösungsansatz zu diesem noch viel schwierigeren Problem ist längst noch nicht in Sicht. In diesem Zusammenhang sei hier lediglich das folgende Beispiel genannt:

(1.55) **Satz:** $\mathbb{Q}(\sqrt{14})$ *ist nicht euklidisch, aber faktoriell.*

Beweis:

Der Zahlring von $\mathbb{Q}(\sqrt{14})$ ist $\mathbb{Z}[\sqrt{14}]$. Wählt man nun im Zahlkörper ζ als $\zeta := \frac{1}{2}(1+\sqrt{14}) \in \mathbb{Q}(\sqrt{14})$, so ist für alle $\vartheta \in \mathbb{Z}[\sqrt{14}]$ dann $|N(\zeta - \vartheta)| > 1$.

Denn schreibt man $\zeta - \vartheta = \frac{1}{2}(a + b\sqrt{14})$ mit ungeraden $a, b \in \mathbb{Z}$, so ist $N(\zeta - \vartheta) = \frac{1}{4}(a^2 - 14b^2)$. Modulo $56 = 7 \cdot 8$ sind aber $1, 9, 25, 49$ alle Quadrate u^2 mit u ungerade, und daher ist $a^2 - 14b^2$ stets kongruent zu $-21, -13, -5$ oder 11 modulo 56, wie man durch Betrachten der ungeraden Quadrate modulo 7 und modulo 8 sieht. Aber dann ist nur $|N(\zeta - \vartheta)| = |\frac{1}{4}(a^2 - 14b^2)| > 1$ möglich.

Also ist $\mathbb{Q}(\sqrt{14})$ nicht euklidisch, dafür aber faktoriell:

Aus der Zahlentheorie ist bekannt, daß jede Klassengruppe der Idealklassengruppe ein ganzes Ideal mit Norm $< \lambda$ enthält, wo hier

$$\lambda = \left(\frac{4}{\pi}\right)^0 \cdot \frac{2!}{2^2}\sqrt{\left|\operatorname{disc}\left(\mathbb{Q}\left(\sqrt{14}\right)\right)\right|} = \sqrt{14} < 4$$

ist. Nun ist jedes Ideal mit Norm < 4 Produkt von Primidealen über 2 oder 3. Es ist dabei

$$\mathbb{Z}[\sqrt{14}] \cdot 2 = (2, \sqrt{14} - 14)^2 = (2, \sqrt{14})^2,$$

wo $(2, \sqrt{14}) = (4 + \sqrt{14})$ ein primes Hauptideal ist, da »$\supseteq$« klar ist und

$$N(4 + \sqrt{14}) = 16 - 14 = 2 = N(2, \sqrt{14})$$

gilt. Weiter ist $\mathbb{Z}[\sqrt{14}] \cdot 3$ prim, also insbesondere auch ein Hauptideal.

Daher ist die Klassenzahl von $\mathbb{Q}(\sqrt{14})$ gleich 1, also ist der Zahlkörper faktoriell. $\square$

Kapitel 2

Der Satz von Lenstra über euklidische Zahlkörper

In diesem Kapitel wird eine Methode von H.W. Lenstra der Arbeit [14] aus dem Jahre 1977 beschrieben, die eine hinreichende Bedingung für einen euklidischen Zahlkörper liefert. Dieser Satz von H.W. Lenstra wird in diesem letzten Kapitel behandelt. Damit konnte ein Großteil der heute über 600 bekannten (allgemeinen) euklidischen Zahlkörper bestimmt werden.

2.1 Hilfsmittel aus der Theorie der Packungen

Um den Satz von H.W. Lenstra über euklidische Zahlkörper verstehen zu können, sind zunächst einige Begriffe und Sätze aus der Theorie der Packungen nötig. Ihnen widmet sich im folgenden dieser Abschnitt.

(2.1) **Definition:** *Sei $(a_i)_{i\in\mathbb{N}}$ eine Folge von Punkten im $\mathbb{R}^n$, wobei $n \geqslant 2$ ist, und sei $U \subseteq \mathbb{R}^n$ beschränkt mit $\mu(U) > 0$, wobei μ das Lebesguemaß im $\mathbb{R}^n$ bezeichne.*

Dann heißt $\mathcal{U} := \{U + a_i;\ \ i \in \mathbb{N}\}$ ein System von U, und

$$C := \left\{ x \in \mathbb{R}^n;\ \ \forall j \in \{1, \ldots, n\} : c_j - \frac{1}{2}s \leqslant x_j \leqslant c_j + \frac{1}{2}s \right\}$$

heißt Würfel um $c = (c_1, \ldots, c_n) \in \mathbb{R}^n$ mit Kantenlänge $s(C) = s > 0$. Im folgenden seien Würfel stets achsenparallel in diesem Sinne, und $s(U)$ sei die Kantenlänge irgendeines festen Würfels, der U enthält.

Man setzt nun für einen Würfel C

$$\rho(\mathcal{U}, C) := \frac{1}{\mu(C)} \sum_{(U+a_i)\cap C\neq\emptyset} \mu(U + a_i)$$

sowie

$$\rho(\mathcal{U}) := \lim_{s\to\infty} \sup_{s(C)\geqslant s} \rho(\mathcal{U}, C).$$

$\rho(\mathcal{U})$ heißt obere Systemdichte von $\mathcal{U}$.

Ein System $\mathcal{U}$ von U heißt eine U-Packung, falls für alle $i, j \in \mathbb{N}$ mit $i \neq j$ gilt: $(U + a_i) \cap (U + a_j) = \emptyset$.

(2.2) **Lemma:** *Für eine U-Packung $\mathcal{U}$ gilt $\rho(\mathcal{U}) \leqslant 1$.*

Beweis: Sei C_0 ein fester Würfel mit $U \subseteq C_0$. Weiter sei C irgendein Würfel, und C' ein Würfel, der mit C konzentrisch liegt und die Kantenlänge $s(C') = s(C) + 2s(C_0)$ hat. Dann liegen die $U + a_i$, für die $(U + a_i) \cap C \neq \emptyset$ gilt, in C'.

Da die $U + a_i$ paarweise disjunkt sind, folgt

$$\sum_{(U+a_i)\cap C\neq\emptyset} \mu(U + a_i) \leqslant (s(C) + 2s(C_0))^n,$$

also ist

$$\rho(\mathcal{U}, C) \leqslant \left(1 + 2\frac{s(C_0)}{s(C)}\right)^n,$$

und somit

$$\rho(\mathcal{U}) \leqslant \lim_{s(C)\to\infty} \left(1 + 2\frac{s(C_0)}{s(C)}\right)^n = 1. \quad \square$$

(2.3) **Definition:**

$$\delta(U) := \sup_{\mathcal{U}\, U\text{-Packung}} \rho(\mathcal{U})$$

heißt Packungsdichte von U.

Es gilt, daß $\delta(U) \leqslant 1$ ist nach (3.2).

(2.4) **Definition:** *Sind $v_1, \ldots, v_n \in \mathbb{R}^n$ linear unabhängig, so heißt*

$$\Gamma := \{u_1v_1 + \cdots + u_nv_n;\ \ u_1, \ldots, u_n \in \mathbb{Z}\}$$

ein (volles) Gitter im $\mathbb{R}^n$. Man schreibt dann auch $\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ für Γ.

Der Fundamentalbereich von Γ *ist*

$$F_\Gamma := \{x \in \mathbb{R}^n;\ \ x = t_1v_1 + \cdots + t_nv_n \text{ mit } 0 \leqslant t_1, \ldots, t_n < 1 \text{ reell}\}.$$

Weiter bezeichnen nun im folgenden $e_1, \ldots, e_n \in \mathbb{R}^n$ *die Standardbasiselemente des* $\mathbb{R}^n$.

(2.5) **Satz:** *Sei* $U \subseteq \mathbb{R}^n$ *beschränkt mit* $\mu(U) > 0$, T *eine nichtsinguläre affine Transformation des* $\mathbb{R}^n$, *und weiter* $a_1, \ldots, a_N \in \mathbb{R}^n$, *sowie* $(b_i)_{i\in\mathbb{N}}$ *eine Aufzählung der Elemente des (vollen) Gitters* $\Gamma := \mathbb{Z}se_1 + \cdots + \mathbb{Z}se_n$, *mit* $s > 0$. *Man betrachte dazu das System*

$$\mathcal{U} := \{U + a_i + b_j;\ \ i \in \{1, \ldots, N\},\ \ j \in \mathbb{N}\}$$

von U, *sowie*

$$T\mathcal{U} := \{T(U + a_i + b_j);\ \ i \in \{1, \ldots, N\},\ \ j \in \mathbb{N}\}.$$

Dann ist

$$\rho(T\mathcal{U}) = \rho(\mathcal{U}) = N\frac{\mu(U)}{\mu(C)},$$

wo $C = F_\Gamma$, *und somit* $\mu(C) = s^n$ *ist.*

Beweis:

Für den Beweis benötigt man zusätzlich noch den Begriff der unteren Systemdichte eines Systems $\mathcal{V} = \{V + c_i;\ \ i \in \mathbb{N}\}$ von $V \subseteq \mathbb{R}^n$ mit $\mu(V) > 0$: Es sei für einen Würfel D

$$\rho'(\mathcal{V}, D) := \frac{1}{\mu(D)} \sum_{(V+c_i)\subseteq D} \mu(V + c_i),$$

sowie

$$\rho'(\mathcal{V}) := \lim_{t\to\infty} \inf_{s(D)\geqslant t} \rho'(\mathcal{V}, D).$$

Klar ist natürlich, daß $\rho'(\mathcal{V}) \leqslant \rho(\mathcal{V})$ gilt.

Seien nun die $U + a_i$ ohne Einschränkung so, daß $(U + a_i) \cap C \neq \emptyset$ für $i \in \{1, \ldots, N\}$ ist. Dies ist erreichbar, da $\mathcal{U} = \mathcal{U} + b_j$ für alle $j \in \mathbb{N}$ gilt, und da Γ ein Gitter mit C als Fundamentalbereich ist.

Da T eine affine Transformation des $\mathbb{R}^n$ ist, ist

$$T\mathcal{U} = \{TU + T(a_i + b_j) - T0;\ \ i \in \{1, \ldots, N\},\ \ j \in \mathbb{N}\},$$

wobei $0 \in \mathbb{R}^n$ der Ursprung des $\mathbb{R}^n$ bezeichne.

(1) Sei G ein Würfel der Kantenlänge $s(G) > 2s(TC) + 2s(TU)$, ebenso G' und G'', konzentrisch mit G und

$$\begin{aligned} s(G') &= s(G) - 2s(TU), \\ \text{sowie } \ s(G'') &= s(G) - 2s(TU) - 2s(TC). \end{aligned}$$

Nun gilt, daß die $T(C+b_j)$ für $j \in \mathbb{N}$ den $\mathbb{R}^n$ überdecken, d.h. jeder Punkt von G'' liegt in einem $T(C + b_j) \subseteq G'$. Überdecken die $T(C + b_j) \subseteq G'$ ohne Einschränkung für $j \in \{1, \ldots, M\}$ den Würfel G'', so folgt:

$$M\mu(TC) = \sum_{j=1}^{M} \mu(T(C + b_j)) \geqslant \mu(G'') = (s(G) - 2s(TU) - 2s(TC))^n. \tag{2.6}$$

Wegen $(U + a_i) \cap C \neq \emptyset$ für $i \in \{1, \ldots, N\}$ hat für $j \in \{1, \ldots, M\}$ also $T(U + a_i + b_j)$ mit G' stets mindestens einen Punkt gemeinsam. Somit ist $T(U + a_i + b_j) \subseteq G$ für $i \in \{1, \ldots, N\}$ und $j \in \{1, \ldots, M\}$. Also gilt

$$\rho'(T\mathcal{U}, G) \geqslant \frac{1}{\mu(G)} \sum_{i=1}^{N} \sum_{j=1}^{M} \mu(T(U + a_i + b_j)) = NM \frac{\mu(TU)}{\mu(G)}.$$

Mit (2.6) folgt daraus:

$$\begin{aligned} \rho'(T\mathcal{U}, G) &\geqslant N \frac{\mu(TU)}{\mu(TC)} \left(1 - \frac{2s(TC)}{s(G)} - \frac{2s(TU)}{s(G)}\right)^n \\ &= N \frac{\mu(U)}{\mu(C)} \left(1 - \frac{2s(TC)}{s(G)} - \frac{2s(TU)}{s(G)}\right)^n, \end{aligned}$$

folglich ist

$$\rho'(T\mathcal{U}) = \lim_{s \to \infty} \inf_{s(G) \geqslant s} \rho'(T\mathcal{U}, G) \geqslant N \frac{\mu(U)}{\mu(C)}.$$

(2) Sei nun G ein Würfel, und G' bzw. G'' mit G konzentrische Würfel der Kantenlängen

$$\begin{aligned} s(G') &= s(G) + 2s(TU) \\ \text{und } \ s(G'') &= s(G) + 2s(TU) + 2s(TC). \end{aligned}$$

Sei weiter $\{1, \ldots, M\}$ die Menge der j, für die es ein $i \in \{1, \ldots, N\}$ gibt mit $T(U + a_i + b_j) \cap G \neq \emptyset$, also liegen alle diese $T(U + a_i + b_j)$ in G', und somit ist $T(C + b_j) \subseteq G''$ für $j \in \{1, \ldots, M\}$. Dies zeigt

$$M\mu(TC) = \sum_{j=1}^{M} \mu(T(C + b_j)) \leqslant \mu(G''),$$

da die $T(C+b_j)$ paarweise disjunkt sind, und daher folgt

$$\rho(T\mathcal{U},G)=\frac{1}{\mu(G)}\sum_{i=1}^{N}\sum_{j=1}^{M}\mu(T(U+a_i+b_j))=NM\frac{\mu(TU)}{\mu(G)}$$
$$\leqslant N\frac{\mu(TU)}{\mu(TC)}\cdot\frac{\mu(G'')}{\mu(G)}=N\frac{\mu(U)}{\mu(C)}\left(1+\frac{2s(TC)}{s(G)}+\frac{2s(TU)}{s(G)}\right)^n,$$

also ist

$$\rho(T\mathcal{U})=\lim_{s\to\infty}\sup_{s(G)\geqslant s}\rho(T\mathcal{U},G)\leqslant N\frac{\mu(U)}{\mu(C)}.$$

(3) Wegen $\rho'(T\mathcal{U})\leqslant\rho(T\mathcal{U})$ folgt aus (1) und (2) somit:

$$\rho'(T\mathcal{U})=N\frac{\mu(U)}{\mu(C)}=\rho(T\mathcal{U}),$$

und dies gilt insbesondere für $T=id_{\mathbb{R}^n}$. $\square$

(2.7) **Satz:** *Sei $U\subseteq\mathbb{R}^n$ beschränkt mit $\mu(U)>0$, sowie $\Gamma:=\mathbb{Z}g_1+\cdots+\mathbb{Z}g_n$ ein (volles) Gitter im $\mathbb{R}^n$, und ferner seien $a_1,\ldots,a_N\in\mathbb{R}^n$ sowie*

$$\mathcal{U}:=\{U+a_i+b_j;\ \ i\in\{1,\ldots,N\},\ \ j\in\mathbb{N}\},$$

wobei $(b_j)_{j\in\mathbb{N}}$ eine Aufzählung des Gitters Γ sei. Dann ist

$$\rho(\mathcal{U})=N\frac{\mu(U)}{\operatorname{vol}\Gamma},$$

wobei $\operatorname{vol}\Gamma=|\det(g_1,\ldots,g_n)|$ das Volumen des Fundamentalbereichs von Γ sei.

Beweis: Sei L die nichtsinguläre lineare Transformation des $\mathbb{R}^n$ definiert durch $L(e_i):=g_i$ für $i\in\{1,\ldots,n\}$, und sei C der Würfel

$$C:=\{x\in\mathbb{R}^n;\ \ 0\leqslant x\leqslant 1\ \text{ für }\ i\in\{1,\ldots,n\}\},$$

wo hier $(b'_j)_{j\in\mathbb{N}}$ eine Aufzählung des Gitters $\mathbb{Z}e_1+\cdots+\mathbb{Z}e_n$ sei. Dann ist also $(Lb'_j)_{j\in\mathbb{N}}\subseteq\Gamma$. Seien nun $a'_i:=L^{-1}a_i$ für $i\in\{1,\ldots,N\}$. Somit ist

$$\{L(L^{-1}U+a'_i+b'_j);\ \ i\in\{1,\ldots,N\},\ \ j\in\mathbb{N}\}=\mathcal{U}.$$

Satz (2.5), auf $L^{-1}U$ und L angewendet liefert dann, daß

$$\rho(\mathcal{U})=N\frac{\mu(L^{-1}U)}{\mu(C)}=N\frac{\mu(U)}{\mu(LC)}=N\frac{\mu(U)}{\operatorname{vol}\Gamma}.\quad\square$$

(2.8) **Definition:** *Sei S ein reguläres n-Simplex im $\mathbb{R}^n$ mit Seitenlänge 2, und bezeichnet $B(\varepsilon,1)$ die Kugel $\{x\in\mathbb{R}^n;\ \|x-\varepsilon\|_2<1\}$ in der 2-Norm um $\varepsilon\in\mathbb{R}^n$ vom Radius 1, so sei*

$$T := S\cap\left(\bigcup_{\varepsilon\,\text{Ecke von}\,S} B(\varepsilon,1)\right)\subseteq\mathbb{R}^n,$$

sowie $\sigma_n := \frac{\mu(T)}{\mu(S)} > 0$.

Es gilt der folgende tiefliegende Satz über die Packungsdichte einer Kugel (man vergleiche dazu auch das Buch [21] von C.A. Rogers):

(2.9) **Satz:** *Ist K eine Kugel (bezüglich der 2-Norm) im $\mathbb{R}^n$, so gilt die Ungleichung $\delta(K)\leqslant\sigma_n$.*

(2.10) **Bemerkung:** *Lediglich für $n=2$ ist die Gleichheit in (2.9) bekannt. Für Dimensionen $n\geqslant 3$ bleibt die Bestimmung der exakten Kugelpackungsdichte ein bis heute ungelöstes Problem.*

2.2 Euklidische Zahlkörper nach H.W. Lenstra

Sei K ein algebraischer Zahlkörper vom endlichen Grad n über $\mathbb{Q}$ und Diskriminante $\triangle$. Ist r die Anzahl der reellen Einbettungen von K in $\mathbb{C}$, und $2s$ die der imaginären, so ist

$$K_{\mathbb{R}} := K\otimes_{\mathbb{Q}}\mathbb{R}\cong\mathbb{R}^r\times\mathbb{C}^s$$

als $\mathbb{R}$-Algebrenisomorphie.

Identifiziert man $\mathbb{C}$ mit $\mathbb{R}^2$ vermöge der Abbildung $a+bi\mapsto(a+b,a-b)$, so ist $K_{\mathbb{R}}\cong\mathbb{R}^{r+2s}=\mathbb{R}^n$ als $\mathbb{R}$-Vektorraumisomorphie. Nun ist K in $K_{\mathbb{R}}$ einbettbar, und ist $R := K\cap\mathbb{A}$ der Zahlring von K, so ist R damit ein Gitter in $\mathbb{R}^n$ vom Rang n. Das Volumen der Grundmasche ist bei dieser Identifikation von $\mathbb{C}$ mit $\mathbb{R}^2$ dann $\mathrm{vol}(\mathbb{R}^n|\mathbb{R})=\sqrt{|\triangle|}$.

Man definiere nun die Normfunktion $N:\mathbb{R}^r\times\mathbb{C}^s\to\mathbb{R}$ vermöge

$$N(x) := \prod_{j=1}^{r}|x_j|\cdot\prod_{k=r+1}^{r+s}|x_k|^2$$

für $x=(x_1,\ldots,x_{r+s})\in\mathbb{R}^r\times\mathbb{C}^s$. Aufgrund obiger Identifikation hat man dann auch entsprechend $N:\mathbb{R}^n\to\mathbb{R}$. Die Einschränkung von N auf K ist

dabei der Absolutbetrag der Körpernorm $K \to \mathbb{Q}$. Sei nun

$$R^\times := \{x \in R;\ x \text{ Einheit in } R\},$$

sowie

$$M := \sup\{m \in \mathbb{N};\ \exists \omega_1, \ldots, \omega_m \in R\ \forall 1 \leqslant i < j \leqslant m : \omega_i - \omega_j \in R^\times\}.$$

M heißt LENSTRA-Konstante von K, und eine endliche Folge $\omega_1, \ldots, \omega_m \in R$ mit $\omega_i - \omega_j \in R^\times$ für alle $1 \leqslant i < j \leqslant m$ heißt eine Ausnahmefolge. Ein $x \in R^\times$ mit $1 - x \in R^\times$ heißt eine Ausnahmeeinheit.

(2.11) **Definition:** *Sei* $L := \min\{|R/I|;\ I \subsetneq R \text{ Ideal}\}$*, also die kleinste Idealnorm echter Ideale von* R*.*

(2.12) **Satz:** *Es gilt* $2 \leqslant M \leqslant L \leqslant 2^n$*. Insbesondere zeigt dies, daß nur endliches* M *möglich ist.*

Beweis: Die triviale Ausnahmefolge $0, 1$ zeigt $M \geqslant 2$, und $I := 2R$ zeigt, daß

$$L \leqslant |R/2R| = |N(2)| = 2^n.$$

Sei $\omega_1, \ldots, \omega_m$ eine Ausnahmefolge und $I \subsetneq R$ ein echtes Ideal. Dann enthält I keine der Einheiten $\omega_i - \omega_j$ für $1 \leqslant i < j \leqslant m$. Also sind die $\omega_1, \ldots, \omega_m$ paarweise inkongruent modulo I, und daher ist $m \leqslant |R/I|$, und somit dann auch $M \leqslant |R/I|$. Insbesondere folgt, daß $M \leqslant L$ ist. □

(2.13) **Satz von H.W. Lenstra:** *Mit obigen Bezeichnungen gilt:*
Ist $U \subseteq \mathbb{R}^n$ *beschränkt mit* $\mu(U) > 0$*, ist* $N(u - v) < 1$ *für alle* $u, v \in U$*, und ist*

$$M > \frac{\delta(U)}{\mu(U)}\sqrt{|\triangle|},$$

so ist K *euklidisch.*

Beweis: Zu zeigen ist: $\forall \zeta \in K\ \exists \vartheta \in R : N(\zeta - \vartheta) < 1$.

Sei dazu also $\zeta \in K$ gegeben. Ferner existiert eine Ausnahmefolge $\omega_1, \ldots, \omega_m \in R$ mit

$$m > \frac{\delta(U)}{\mu(U)}\sqrt{|\triangle|},\ \text{d.h. } \delta(U) < \frac{m\mu(U)}{\sqrt{|\triangle|}}.$$

Man betrachte das System

$$\mathcal{U} := \{U + \omega_i\zeta + \alpha;\ 1 \leqslant i \leqslant m, \alpha \in R\}$$

von U. Nach Satz (2.10) ist dann $\rho(\mathcal{U}) = m\frac{\mu(U)}{\sqrt{|\triangle|}}$, also $\rho(\mathcal{U}) > \delta(U)$.

Demnach ist $\mathcal{U}$ keine U-Packung, d.h. es gibt verschiedene $(i,\alpha),(j,\beta) \in \{1,\dots,m\} \times R$ mit

$$(U + \omega_i\zeta + \alpha) \cap (U + \omega_j\zeta + \beta) \neq \emptyset,$$

sei also etwa $u + \omega_i\zeta + \alpha = v + \omega_j\zeta + \beta$ für $u, v \in U$, also: $(\omega_j - \omega_i)\zeta = (u - v) - (\beta - \alpha)$.

Es folgt nun $i \neq j$: Denn wäre sonst $i = j$, so ist $u - v = \beta - \alpha$, also $N(\beta - \alpha) = N(u - v) < 1$, d.h. $\beta - \alpha = 0$, also $\alpha = \beta$, im Widerspruch zu $(i,\alpha) \neq (j,\beta)$.

Somit ist $\omega_j - \omega_i \in R^\times$, also $N(\omega_i - \omega_j) = 1$. Man setze $\vartheta := \frac{\alpha-\beta}{\omega_j-\omega_i} \in R$. Damit wird dann wie gewünscht

$$N(\zeta - \vartheta) = N\left(\frac{u-v}{\omega_j - \omega_i}\right) = N(u-v) < 1. \quad \square$$

(2.14) **Korollar:** *Ist*

$$M > \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\triangle|},$$

so ist K euklidisch.

Beweis: Sei

$$\mathcal{U} := \left\{ (x_1,\dots,x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s;\ \sum_{j=1}^{r} |x_j| + 2\sum_{k=r+1}^{r+s} |x_k| < \frac{n}{2} \right\},$$

dann ist U beschränkt und $\mu(U) = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s$, wie man in der Zahlentheorie sieht. Für $u, v \in U$ ist ferner (man beachte $n = r + 2s$)

$$\begin{aligned} N(u-v) &= \prod_{j=1}^{r} |u_j - v_j| \cdot \prod_{k=r+1}^{r+s} |u_k - v_k|^2 \\ &\leqslant \left(\frac{1}{r+2s} \left(\sum_{j=1}^{r} |u_j - v_j| + 2\sum_{k=r+1}^{r+s} |u_k - v_k| \right) \right)^{r+2s}, \end{aligned}$$

nach der Ungleichung vom geometrischen und arithmetischen Mittel,

$$\begin{aligned} &\leqslant \left(\frac{1}{r+2s} \left(\sum_{j=1}^{r} (|u_j| + |v_j|) + 2\sum_{k=r+1}^{r+s} (|u_k| + |v_k|) \right) \right)^{r+2s} \\ &< \left(\frac{1}{r+2s} \left(\frac{1}{2}(r+2s) + \frac{1}{2}(r+2s) \right) \right)^{r+2s} = 1^{r+2s} = 1. \end{aligned}$$

Nach (2.3) ist $\delta(U) \leqslant 1$, und somit ist

$$M > \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\triangle|} = \frac{\sqrt{|\triangle|}}{\mu(U)} \geqslant \frac{\delta(U)}{\mu(U)}\sqrt{|\triangle|}.$$

Nun liefert Satz (2.13) die Behauptung. □

(2.15) **Korollar:** *Ist*

$$M > \sigma_n \frac{\Gamma(1+\frac{n}{2})}{\pi^{\frac{n}{2}}}\left(\frac{4}{n}\right)^{\frac{n}{2}} \sqrt{|\triangle|},$$

so ist K euklidisch. Γ bezeichnet dabei die Γ-Funktion, und σ_n die Konstante aus (2.8).

Beweis: Sei

$$U := \left\{(x_1, \ldots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s;\ \sum_{j=1}^{r} x_j^2 + 2\sum_{k=r+1}^{r+s} |x_k|^2 < \frac{n}{4}\right\},$$

mit obiger Identifikation von $\mathbb{C}$ mit $\mathbb{R}^2$ ist dies eine n-dimensionale Kugel vom Radius $\frac{\sqrt{n}}{2}$ im $\mathbb{R}^n$, nämlich

$$U = \left\{(y_1, \ldots, y_n) \in \mathbb{R}^n;\ \sum_{j=1}^{n} y_j^2 < \frac{n}{4}\right\},$$

also

$$\mu(U) = \left(\frac{n}{4}\right)^{\frac{n}{2}} \frac{\pi^{\frac{n}{2}}}{\Gamma(1+\frac{n}{2})}.$$

Für $u, v \in U$ ist dann

$$N(u-v) = \prod_{j=1}^{n} |u_j - v_j| \leqslant \left(\frac{1}{n}\left(\sum_{j=1}^{n} |u_j - v_j|\right)\right)^n,$$

nach der Ungleichung vom geometrischen und arithmetischen Mittel,

$$\begin{aligned}
&\leqslant \left(\frac{1}{n}\left(\sum_{j=1}^{n} |u_j| + \sum_{k=1}^{n} |v_k|\right)\right)^n \\
&\leqslant \left(\frac{1}{n}\left(\sqrt{\sum_{j=1}^{n} u_j^2}\cdot\sqrt{n} + \sqrt{\sum_{j=1}^{n} v_j^2}\cdot\sqrt{n}\right)\right)^n \\
&< \left(\frac{1}{\sqrt{n}}\left(\frac{\sqrt{n}}{2} + \frac{\sqrt{n}}{2}\right)\right)^n = 1^n = 1.
\end{aligned}$$

Nach (2.9) ist weiter $\delta(U) \leqslant \sigma_n$, und somit gilt

$$M > \sigma_n \frac{\Gamma(1+\frac{n}{2})}{\pi^{\frac{n}{2}}} \left(\frac{4}{n}\right)^{\frac{n}{2}} \sqrt{|\triangle|} \geqslant \delta(U) \frac{\sqrt{|\triangle|}}{\mu(U)}.$$

Nun liefert Satz (2.13) die Behauptung. $\square$

(2.16) **Bemerkung:** *Für große n ist die rechte Seite der Formel in* (2.15) *kleiner als die in* (2.14)*, in diesem Fall also brauchbarer. Tatsächlich gilt unter der Annahme bestimmter Verallgemeinerter* RIEMANN*-Hypothesen, daß die Formel in* (2.15) *höchstens für endlich viele Zahlkörper erfüllbar sein kann, man vergleiche dazu die Arbeit* [14] *von* H.W. LENSTRA*. Daher besteht wenig Hoffnung, mit dieser Methode von* H.W. LENSTRA *unendlich viele euklidische Zahlkörper zu konstruieren.*

2.3 Anwendungsbeispiele und Ergebnisse

In diesem Abschnitt werden einige Beispiele für die Anwendung der Sätze des vorigen Abschnitts zusammengetragen.

(2.17) **Beispiel:**

(a) Sei p eine ungerade Primzahl, und $L_p := \mathbb{Q}(\zeta)$, wo ζ eine primitive p-te Einheitswurzel bezeichne, der p-te Kreisteilungskörper. Dieser hat den Grad $p-1$ über $\mathbb{Q}$, und es ist $L = p$ die kleinste Idealnorm echter Ideale des Zahlrings R_p von L_p.

Nun ist für $j \in \{1, \ldots, p-1\}$ stets

$$N_{\mathbb{Q}}^{L_p}(\zeta^{-j} - \zeta^j) = N_{\mathbb{Q}}^{L_p}(1 - \zeta^{2j}) = p,$$

da

$$N_{\mathbb{Q}}^{L_p}(1-\omega) = \prod_{j=1}^{p-1}(1-\omega^j) = f(1) = p$$

für eine primitive p-te Einheitswurzel ω ist, wobei

$$f(X) = X^{p-1} + \cdots + X + 1$$

das Minimalpolynom von ω bzw. ζ über $\mathbb{Q}$ bezeichnet.

Die endliche Folge

$$\omega_p := 0 \text{ und } \omega_j := \frac{\zeta^j - 1}{\zeta - 1} \in R_p^\times$$

für $j \in \{1, \ldots, p-1\}$ (Zähler und Nenner haben die Norm p) liefert dann eine Ausnahmefolge, da für $1 \leqslant i < j \leqslant p$ gilt:

$$\omega_i - \omega_j = \frac{\zeta^i - \zeta^j}{\zeta - 1} \in R_p^\times$$

(Zähler und Nenner haben die Norm p).

Dies zeigt $M \geqslant p$, und mit (2.12) ist dann $M = p$. Weiter ist noch $\operatorname{disc} L_p = p^{p-2}$.

Berechnen der rechten Seite von (2.14) zeigt nun, daß diese $< p$ genau für $p = 3, 5, 7$ ist. Für diese Primzahlen ist demnach L_p euklidisch. Übrigens ist $L_3 = \mathbb{Q}(\sqrt{-3})$, und somit schon aus Kapitel 1 bekannt.

(b) Sei nun $m \in \mathbb{Z}_{\geqslant 1}$ und $\zeta := e^{\frac{2\pi i}{m}}$, sowie $L_m := \mathbb{Q}(\zeta)$ der m-te Kreisteilungskörper vom Grad $\varphi(m)$ über $\mathbb{Q}$, wo hier φ die EULERsche φ-Funktion bezeichnet. Für jede Primzahl p, die m teilt, ist dann $M \geqslant p$ nach Teil (a).

- Für $m = 12$ ist also $M \geqslant 3$, und $\operatorname{disc} L_{12} = 3^2 \cdot 2^4$, sowie $n := \varphi(12) = 4$ und $s = 2$.
  Die rechte Seite von (2.14) ist dann

  $$\frac{4!}{4^4} \left(\frac{4}{\pi}\right)^2 \sqrt{3^2 \cdot 3^4} < 1.83 < 2 < M,$$

  und daher ist L_{12} euklidisch.
- Für $m = 15$ ist also $M \geqslant 5$, und $\operatorname{disc} L_{15} = 3^4 \cdot 5^6$, sowie $n := \varphi(15) = 8$ und $s = 4$.
  Nach einer Tabelle von J. LEECH in seiner Arbeit [12] ist dann

  $$\sigma_8 \frac{\Gamma(5)}{\pi^4} \leqslant 0.06327,$$

  also ist

  $$\sigma_8 \frac{\Gamma(5)}{\pi^4} \left(\frac{4}{8}\right)^4 \sqrt{3^4 \cdot 5^6} \leqslant 4.45 < 5 \leqslant M,$$

  und daher ist nach (2.15) auch L_{15} euklidisch.

Allerdings lassen sich nicht alle euklidischen Kreisteilungskörper mit dieser Methode von H.W. LENSTRA bestimmen. Man kennt die folgenden:

(2.18) **Satz:** *L_m ist euklidisch für*

$$\boxed{m \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 16, 20, 24\}.}$$

Dabei entdeckte H.W. LENSTRA selbst die Kreisteilungskörper L_m, wo $m \in \{4, 8, 9, 11, 20\}$, mit anderen Mitteln, man vergleiche dazu auch seine frühere Arbeit [13].

Immerhin weiß man, daß es nur endlich viele euklidische Kreisteilungskörper gibt, aufgrund des folgenden tiefliegenden Umstandes:

(2.19) **Satz:** *L_m ist faktoriell genau für*

$$\boxed{\begin{aligned} m \in \{ \quad & 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, \\ & 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}. \end{aligned}}$$

Dieses Ergebnis wurde 1976 von J.M. MASLEY und H.L. MONTGOMERY erzielt, man vergleiche dazu auch [19].

Ein anderer Beweis dafür, daß es nur endlich viele euklidische Kreisteilungskörper gibt, außer über (2.19), bleibt bis heute unbekannt.

(2.20) **Beispiel:** (Nach dem Buch [16] von A. LEUTBECHER.)

Sei p eine ungerade Primzahl, und

$$K_p := \mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\vartheta),$$

wo ζ eine primitive p-te Einheitswurzel bezeichne, und $\vartheta = \zeta + \zeta^{-1}$ sei. K_p ist also der maximale reelle Teilkörper des p-ten Kreisteilungskörpers und hat den Grad $n := \frac{p-1}{2}$ über $\mathbb{Q}$. Sein Zahlring ist $S_p = K_p \cap \mathbb{A} = \mathbb{Z}[\vartheta]$. Die Diskriminante $\triangle$ von K_p hat den Betrag $p^{\frac{p-3}{2}}$.

Dies zeigt man folgendermaßen: Ist L_p der p-te Kreisteilungskörper, so hat L_p über K_p den Grad 2. Man findet ferner die beiden Ganzheitsbasen

$$\{1, \zeta, \zeta^{-1}, \zeta^2, \zeta^{-2}, \ldots, \zeta^{n-1}, \zeta^{-(n-1)}\}$$

und

$$\{1, \zeta, \vartheta, \vartheta\zeta, \vartheta^2, \vartheta^2\zeta, \ldots, \vartheta^{n-1}, \vartheta^{n-1}\zeta\}$$

von L_p über $\mathbb{Q}$, und die Ganzheitsbasis

$$\{1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}\}$$

von K_p über $\mathbb{Q}$, sowie die Ganzheitsbasis $\{1, \zeta\}$ von L_p über K_p. Nach dem Schachtelungssatz für Diskriminanten ist dann

$$(-1)^n p^{p-2} = \mathrm{disc}_{\mathbb{Q}}^{L_p}(\zeta) = \left(\mathrm{disc}_{\mathbb{Q}}^{K_p}(\vartheta)\right)^2 N_{\mathbb{Q}}^{K_p}\left(\mathrm{disc}_{K_p}^{L_p}(\zeta)\right),$$

wobei

$$\mathrm{disc}_{K_p}^{L_p}(\zeta) = \left(\det \begin{pmatrix} 1 & \zeta \\ 1 & \zeta^{-1} \end{pmatrix}\right)^2 = (\zeta^{-1} - \zeta)^2 = \zeta^2 + \zeta^{-2} - 2 \in K_p.$$

Dann ist

$$\begin{aligned} \left| N_{\mathbb{Q}}^{K_p} \left(\left(\zeta^{-1} - \zeta\right)^2 \right) \right| &= \left| \prod_{j=1}^{n} \left(\zeta^{-j} - \zeta^j\right)^2 \right| \\ &= \left| \prod_{j=1}^{p-1} \left(\zeta^j - \zeta^{-j}\right) \right| = \left| N_{\mathbb{Q}}^{L_p} \left(\zeta^{-1} - \zeta\right) \right| = p, \end{aligned}$$

man vergleiche oben. Also ist

$$|\triangle| = \left| \mathrm{disc}_{\mathbb{Q}}^{K_p}(\vartheta) \right| = \sqrt{\frac{p^{p-2}}{p}} = p^{\frac{p-3}{2}},$$

Man betrachte nun

$$\omega_j := \frac{\zeta^{j+1} - \zeta^{-j-1}}{\zeta^j - \zeta^{-j}} \in S_p^\times$$

für $j \in \{1, \ldots, p-1\}$ (Zähler und Nenner haben die Absolutnorm $\sqrt{p}$), diese bilden nun eine Ausnahmefolge der Länge $p-1$:

Denn für $i < j$ ist

$$\begin{aligned} \omega_i - \omega_j &= \frac{(\zeta^{i+1} - \zeta^{-i-1})(\zeta^j - \zeta^{-j}) - (\zeta^{j+1} - \zeta^{-j-1})(\zeta^i - \zeta^{-i})}{(\zeta^i - \zeta^{-i})(\zeta^j - \zeta^{-j})} \\ &= \frac{(\zeta - \zeta^{-1})(\zeta^{j-i} - \zeta^{i-j})}{(\zeta^i - \zeta^{-i})(\zeta^j - \zeta^{-j})} \in S_p^\times, \end{aligned}$$

da Zähler und Nenner die Absolutnorm p haben. Somit ist $M \geqslant p-1$. Berechnen der rechten Seite von (2.14) zeigt, daß diese $< p-1$ genau für $p = 3, 5, 7, 11, 13$ ist. Für diese Primzahlen ist demnach K_p euklidisch. Übrigens sind $K_3 = \mathbb{Q}$ und $K_5 = \mathbb{Q}(\sqrt{5})$, und somit schon aus Kapitel 1 bekannt.

Für die folgenden beiden Beispiele ist K ein Zahlkörper, der aus $\mathbb{Q}$ durch Adjunktion einer Wurzel x eines über $\mathbb{Q}$ irreduziblen Polynoms $f \in \mathbb{Z}[X]$ entsteht. Das Problem besteht dann darin, den Wert $\mathrm{disc}(x)$ zu bestimmen. Dazu zunächst

(2.21) **Definition:** *Die* Resultante *zweier Polynome* $f, g \in \mathbb{Z}[X]$*, etwa*

$$\begin{aligned} f &= a_0 X^n + \cdots + a_n \\ \textit{und} \quad g &= b_0 X^m + \cdots + b_m, \end{aligned}$$

ist

$$\operatorname{res}(f,g) := \det \underbrace{\left(\begin{array}{ccccccc} a_0 & a_1 & \ldots\ldots & a_n & & & \\ & a_0 & a_1 & \ldots\ldots & a_n & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & \ldots\ldots & a_n \\ b_0 & b_1 & \ldots\ldots & b_m & & & \\ & b_0 & b_1 & \ldots\ldots & b_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_0 & b_1 & \ldots\ldots & b_m \end{array} \right)}_{m+n} \begin{array}{l} \left.\vphantom{\begin{array}{c} a \\ a \\ a \\ a \\ a \end{array}}\right\} m \\ \left.\vphantom{\begin{array}{c} a \\ a \\ a \\ a \\ a \end{array}}\right\} n \end{array}.$$

Dafür gilt nun der

(2.22) **Satz:** *Es ist*

$$\operatorname{disc}(x) = (-1)^{\frac{n(n-1)}{2}} \operatorname{res}(f, f'),$$

falls $f \in \mathbb{Z}[X]$ *das Minimalpolynom von* x *vom Grad* n *ist.* f' *bezeichnet die formale Ableitung von* f*.*

Dies liefert dann eine Möglichkeit zur Berechnung der Diskriminanten von Zahlkörpern und wird in den folgenden Beispielen angewendet.

(2.23) **Beispiel:** Man betrachte $K = \mathbb{Q}(x)$, wo x Wurzel des über $\mathbb{Q}$ irreduziblen Polynoms

$$f(X) := X^5 - X^3 + X^2 + X - 1$$

ist. Es ist also 5 der Grad von K über $\mathbb{Q}$. Nach obigem Satz (2.22) ist dann

$$\operatorname{disc}(x) = \operatorname{res}(f, f') = \det \begin{pmatrix} 1 & 0 & -1 & 1 & 1 & -1 & & & \\ & 1 & 0 & -1 & 1 & 1 & -1 & & \\ & & 1 & 0 & -1 & 1 & 1 & -1 & \\ & & & 1 & 0 & -1 & 1 & 1 & -1 \\ 5 & 0 & -3 & 2 & 1 & & & & \\ & 5 & 0 & -3 & 2 & 1 & & & \\ & & 5 & 0 & -3 & 2 & 1 & & \\ & & & 5 & 0 & -3 & 2 & 1 & \\ & & & & 5 & 0 & -3 & 2 & 1 \end{pmatrix}$$

$$= 1609,$$

dies ist prim und insbesondere quadratfrei, d.h. $(1, x, x^2, x^3, x^4)$ ist eine Ganzheitsbasis von K, und somit ist $\operatorname{disc} K = \operatorname{disc}(x) = 1609$. Weiter ist $0, 1, x$ eine Ausnahmefolge von K, da x eine Ausnahmeeinheit ist:

Denn zum einen ist $x|(x^5 - x^3 + x^2 + x) = 1$, also ist $x \in K^\times$, und zum anderen ist $x^5 - x^2(x-1) + (x-1) = 0$, also $(x-1)^2(x+1) = x^5 \in K^\times$, also $x - 1 \in K^\times$.

Somit ist $M \geqslant 3$. Nach der Tabelle von J. Leech in seiner Arbeit [12] ist

$$\sigma_5 \frac{\Gamma(\frac{7}{2})}{\pi^{\frac{5}{2}}} \leqslant 0.09988,$$

also ist

$$\sigma_5 \frac{\Gamma(\frac{7}{2})}{\pi^{\frac{5}{2}}} \left(\frac{4}{5}\right)^{\frac{5}{2}} \sqrt{|\operatorname{disc} K|} \leqslant 2.294 < 3 \leqslant M.$$

Die Voraussetzung von Korollar (2.15) ist erfüllt, und demnach ist K euklidisch.

(2.24) **Beispiel:** Man betrachte $K = \mathbb{Q}(x)$, wo x Wurzel des über $\mathbb{Q}$ irreduziblen Polynoms

$$f(X) := X^3 - X - 1$$

ist. Es ist also 3 der Grad von K über $\mathbb{Q}$. Nach obigem Satz (2.22) ist dann

$$\operatorname{disc}(x) = -\operatorname{res}(f, f') = -\det \begin{pmatrix} 1 & 0 & -1 & -1 & \\ & 1 & 0 & -1 & -1 \\ 3 & 0 & -1 & & \\ & 3 & 0 & -1 & \\ & & 3 & 0 & -1 \end{pmatrix} = -23,$$

dies ist prim und insbesondere quadratfrei, d.h. $(1, x, x^2)$ ist eine Ganzheitsbasis von K, und es ist also $\operatorname{disc} K = \operatorname{disc}(x) = -23$. Somit ist

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)^2 \sqrt{|-23|} \leqslant 1.73 < 2 \leqslant M$$

erfüllt, und daher ist K nach Korollar (2.14) euklidisch.

(2.25) **Ergebnisse:** Mit seiner Arbeit [14] fand H.W. LENSTRA mit seiner neuen Methode so über 100 neue euklidische Zahlkörper und erhöhte damals die Anzahl bekannter euklidischer Zahlkörper auf 311. A. LEUTBECHER und J. MARTINET fanden 1982, siehe [17], weitere 114 euklidische Zahlkörper mittels expliziter Bestimmung von Ausnahmefolgen und LENSTRA-Konstanten. Weitere 37 fanden A. LEUTBECHER und G. NIKLASCH 1989 mit der Arbeit [18] durch Studium einer Gruppenoperation auf Cliquen von Ausnahmeeinheiten. Insgesamt sind heute über 600 euklidische Zahlkörper bekannt. In diesem Zusammenhang ist ferner noch die Arbeit [20] von G. NIKLASCH und R. QUÊME aus dem Jahr 1991 zu nennen, in der eine Verallgemeinerung obigen Satzes (2.13) von H.W. LENSTRA vorgenommen wird, so daß im Falle eines totalreellen Zahlkörpers Verbesserungen möglich waren. Auch damit wurden weitere neue euklidische Zahlkörper gefunden.

Die Frage, ob es endlich viele oder unendlich viele euklidische Zahlkörper gibt, bleibt aber weiterhin offen, man vergleiche dazu auch die Bemerkung (2.16).

Ferner ist es noch so, daß alle bekannten Zahlkörper, die einen euklidischen Algorithmus besitzen, tatsächlich auch normeuklidisch sind. Und es gibt unendlich viele faktorielle Zahlkörper, die nicht normeuklidisch sind. Insofern ist folgendes Ergebnis in [15] von H.W. LENSTRA sehr erstaunlich:

(2.26) **Satz:** *Ein faktorieller Zahlkörper mit unendlich vielen Einheiten hat unter der Annahme bestimmter Verallgemeinerter* RIEMANN*-Hypothesen einen euklidischen Algorithmus.*

Man vergleiche dies mit den imaginärquadratischen Zahlkörpern aus Abschnitt 1.1: Diese haben nur endlich viele Einheiten, und die Sätze (1.2) und (1.3) besagen, daß es unter diesen genau vier faktorielle gibt, die gar keinen euklidischen Algorithmus besitzen, nämlich $\mathbb{Q}(\sqrt{m})$ mit

$$m \in \{-19, -43, -67, -163\}.$$

Literaturverzeichnis

[1] A. Baker: *Linear forms in the logarithms of algebraic numbers.*
Mathematika 13 (1966), S. 204-216

[2] E.S. Barnes und H.P.F. Swinnerton-Dyer: *The inhomogeneous minima of binary quadratic forms (1).*
Acta Math. 87 (1952), S. 259-323

[3] J.W.S. Cassels: *The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms.*
Proc. Cambridge Philos. Soc. 48 (1952), S. 72-86 und S. 519-520

[4] H. Chatland: *On the Euclidean algorithm in quadratic number fields.*
Bulletin Amer. Math. Soc. 55 (1949), S. 948-953

[5] H. Chatland und H. Davenport: *Euclid's algorithm in real quadratic fields.*
Canad. J. of Math. 2 (1950), S. 289-296

[6] H. Davenport: *Indefinite binary quadratic forms.*
Quat. J. Math. Oxford (2),1 (1950), S. 54-62

[7] H. Davenport: *Indefinite binary quadratic forms and Euclid's algorithm in the real quadratic fields.*
Proc. Lond. math. Soc. (2),53 (1951), S. 65-82

[8] H. Davenport: *Euclid's algorithm in cubic fields of negative discriminant.*
Acta math. Stockh. 84 (1950), S. 159-178

[9] H. Davenport: *Euclid's algorithm in certain quartic fields.*
Trans. Amer. math. Soc. 68 (1950), S. 508-532

[10] G.H. Hardy und E.M.Wright: *An introduction to the theory of numbers.*
Fourth ed., Clarendon Press, Oxford 1962

[11] H. Heilbronn: *On Euclid's algorithm in real quadratic fields.*
Proc. Cambridge Phil. Soc. 34 (1938), S. 521-526

[12] J. Leech: *Notes on sphere packings.*
Canad. J. Math. 19 (1967), S. 251-267

[13] H.W. Lenstra, Jr.: *Euclid's algorithm in cyclotomic fields.*
J. London Math. Soc. 10 (1975), S. 457-465

[14] H.W. Lenstra, Jr.: *Euclidean number fields of large degree.*
Invent. Math. 38 (1977), S. 237-254

[15] H.W. Lenstra, Jr.: *On Artin's conjecture and Euclid's algorithm in global fields.*
Invent. Math. 42 (1977), S. 201-224

[16] A. Leutbecher: *Zahlentheorie: Eine Einführung in die Algebra.*
Springer-Verlag Berlin Heidelberg (1996)

[17] A. Leutbecher und J. Martinet: *Lenstra's constant and euclidean number fields.*
Journées Arithmétiques Metz (1981), Astérisque 94 (1982), S. 87-131

[18] A. Leutbecher und G. Niklasch: *On cliques of exceptional units and Lenstra's construction of euclidean fields.*
Journées Arithmétiques Ulm (1987), (E.Wirsing ed.) Lecture Notes in Math. 1380 (1989), Springer, Heidelberg et. al.

[19] J.M. Masley: *On cyclotomic fields euclidean for the norm map.*
Notices Amer. Math. Soc. 19 (1972), S. A-813 (abstract 700-A3)

[20] G. Niklasch und R. Quême: *An improvement of Lenstra's criterion for euclidean number fields: The totally real case.*
Acta Arithmetica 58.2 (1991), S. 157-168

[21] C.A. Rogers: *Packing and covering.*
Cambridge: Cambridge University Press (1964)

[22] H.M. Stark: *A complete determination of the complex quadratic fields of class-number one.*
Mich. Math. J. 14 (1967), S. 1-27