Verallgemeinerungen Euklidischer Algorithmen

Timo Hanke

Diplomarbeit
FU Berlin
Fachbereich Mathematik und Informatik
12. September 1996

Adresse des Autors:
Taylorstr. 4, 14195 Berlin
E-mail: hanke@math.fu-berlin.de

Inhaltsverzeichnis

Vorwort

Aus der Algebra ist der Begriff eines Euklidischen Ringes bekannt. Ein Euklidischer Ring ist ein Integritätsbereich R, für den eine sog. Euklidische Abbildung

$$\varphi\colon R \to \mathbb{N}_0$$

existiert, sodaß sich für je zwei Elemente $a, b \in R$ eine "Division mit Rest" der Form

$$a = qb + r$$

mit $q, r \in R$ durchführen läßt, bei der weiter

$$\varphi(r) < \varphi(b)$$

gilt. Auf dieser Eigenschaft der Euklidischen Abbildung basiert bekanntlich der Euklidische Algorithmus zur Berechnung des größten gemeinsamen Teilers zweier Elemente, der darin besteht, die "Division mit Rest" wiederholt durchzuführen bis der Rest 0 entsteht. Ein bekanntes nicht-triviales Beispiel für einen Euklidischen Ring ist der Gaußsche Zahlring $\mathbb{Z}[i]$.

In der Algebra beweist man nun recht einfach, daß jeder Euklidische Ring auch Hauptidealring ist. Keineswegs einfach ist es jedoch zu zeigen, daß die Umkehrung dieser Implikation nicht gilt. Dazu wird in der Regel auf die Algebraische Zahlentheorie verwiesen und als Gegenbeispiel z.B. der Ganzheitsring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-19})$ angeführt, der zwar Hauptidealring ist, aber nicht Euklidischer Ring.

Es ist nun aus verschiedenen Gründen naheliegend, die euklidische Bedingung abzuschwächen. Zum einen kann man abgeschwächte euklidische Bedingungen suchen, die immer noch die Hauptidealring-Eigenschaft implizieren. Diese wären dann beim Nachweis der Hauptidealring-Eigenschaft eines Integritätsbereiches hilfreich, da sie unter Umständen leichter nachzuweisen sind, als die gewöhnliche euklidische Bedingung. Zum anderen kann man euklidische Bedingungen suchen, mit deren Hilfe sich immer noch der Euklidische Algorithmus oder ein vergleichbarer Algorithmus durchführen läßt, um den größten gemeinsamen Teiler zweier Elemente zu berechnen. Ein weiterer Zusammenhang wird sich zwischen abgeschwächten euklidischen Bedingungen und der Idealklassengruppe und ihrer Erzeugendensysteme ergeben.

In dieser Arbeit sollen im wesentlichen zwei Ansätze für abgeschwächte euklidische Bedingungen untersucht werden. Dies ist zum einen das Konzept der "mehrstufigen Euklidischen Abbildung", das von Cooke in [6] eingeführt wurde und hier in Kapitel II behandelt wird. Die "einstufige Euklidische Abbildung" entspricht dabei der gewöhnlichen oben zitierten Euklidischen Abbildung. Es wird sich herausstellen, daß im Fall von Zahlringen, d.h. Ganzheitsringen Algebraischer Zahlkörper, alle "mehrstufigen" euklidischen Bedingungen noch die Hauptidealeigenschaft implizieren.

Der zweite Ansatz geht auf Lenstra zurück, der in [11] "Euklidische Ideale" eingeführt hat, wobei R selbst "Euklidisches Ideal" ist, genau dann wenn R Euklidischer Ring ist. Wesentliche Eigenschaft von "Euklidischen Idealen" ist, daß sie die Idealklassengruppe erzeugen. Dieser Ansatz wurde von Schulze in [16] auf Mengen von Idealen verallgemeinert, wodurch man zu dem Begriff des "Euklidischen Systemes" gelangt. Einelementige "Euklidische Systeme" entsprechen dabei genau den "Euklidischen Idealen" und die Eigenschaft, die Idealklassengruppe zu erzeugen, überträgt sich auch auf "Euklidische Systeme". Die beiden Konzepte "Euklidische Ideale" und "Euklidische Systeme" werden zusammen in Kapitel III behandelt.

Bei den Untersuchungen und bei der Illustration von Beispielen werden wir uns an einigen Stellen der geometrischen Methode der Minkowski-Theorie bedienen. Diese Methode wird auch bei dem in der Zahlentheorie üblichen elementaren Beweis der Tatsache, daß $\mathbb{Z}[i]$ Euklidischer Ring ist, verwendet. Dabei wird der Ring $\mathbb{Z}[i]$ bekanntlich als Gitter in der Gaußschen Zahlenebene aufgefaßt, wodurch sich die Aussage geometrisch beweisen läßt. Einige Teile der Minkowski-Theorie werden, zusammen mit anderen vorbereitenden Überlegungen, in Kapitel I kurz wiederholt.

KAPITEL I

Vorbereitungen

Diese Arbeit setzt die Grundlagen der Algebraischen Zahlentheorie auf idealtheoretischer Basis, wie sie z.B. in Borewics-Šafarevič [2] oder in Marcus [13] entwickelt werden, voraus. Dennoch sollen in diesem Kapitel zunächst einige Definitionen und Resultate der Algebraischen Zahlentheorie wiederholt werden, auf denen die nachfolgenden Ausführungen im wesentlichen beruhen. Der Kürze halber wird dabei gelegentlich auf die Ausführung von Beweisen verzichtet und an diesen Stellen auf die Standardliteratur verwiesen.

1.1. Grundlagen

Es sei im folgenden K ein Algebraischer Zahlkörper, d.h. eine endliche Körpererweiterung von $\mathbb{Q}$, vom Grade $[K:\mathbb{Q}] = n$. Da char $\mathbb{Q} = 0$ ist, ist $K/\mathbb{Q}$ stets separabel, d.h. nach dem Satz vom primitiven Element existiert ein algebraisches Element θ vom Grad n über $\mathbb{Q}$ mit $K = \mathbb{Q}(\theta)$. Weiter bezeichne R den Ganzheitsring von $K/\mathbb{Q}$. Dann ist K bekanntermaßen Quotientenkörper von R, insbesondere kann also $\theta \in R$ gewählt werden.

Unter einer Ganzheitsbasis von $K/\mathbb{Q}$ verstehen wir eine Basis des $\mathbb{Z}$-Moduls R, die dann zugleich Basis des $\mathbb{Q}$-Vektorraums K ist. Es folgt eine Betrachtung über die Form einer solchen Ganzheitsbasis.

SATZ 1.1.1. *Sei $\theta \in R$, sodaß $K = \mathbb{Q}(\theta)$. Dann existiert eine Ganzheitsbasis von $K/\mathbb{Q}$ der Form*

$$\left(1, \frac{f_1(\theta)}{d_1}, \ldots, \frac{f_{n-1}(\theta)}{d_{n-1}}\right) \tag{1}$$

wobei die f_i normierte Polynome über $\mathbb{Z}$ vom Grad i und die $d_i \in \mathbb{N}$ sind. Weiter gilt

$$d_1|d_2, \quad d_2|d_3, \quad \ldots, \quad d_{n-2}|d_{n-1}.$$

Beweis. siehe Marcus [13], Chapter 2, Theorem 13. □

Korollar 1.1.2. *Sei $\theta \in R$, sodaß $K = \mathbb{Q}(\theta)$. Dann ist*

$$\operatorname{disc}(\theta) = d^2 \operatorname{disc}(R)$$

für ein $d \in \mathbb{Z}$ und es gilt $R \subseteq \frac{\mathbb{Z}[\theta]}{d}$.

Beweis. Nach den Rechenregeln über Diskriminanten gilt für die d_i in (1)

$$\operatorname{disc}(\theta) = (d_1 d_2 \dots d_{n-1})^2 \operatorname{disc}(R). \tag{2}$$

Vgl. hierzu auch Marcus [13], Chapter 2, Exercise 40(a). Aus (2) folgt $d_i | d$ und damit $\frac{f_i(\theta)}{d_i} \in \frac{\mathbb{Z}[\theta]}{d}$ für alle $i = 1, \dots, n-1$. Da $(1, \frac{f_1(\theta)}{d_1}, \dots, \frac{f_{n-1}(\theta)}{d_{n-1}})$ Ganzheitsbasis von $K/\mathbb{Q}$ ist, folgt weiter $R \subseteq \frac{\mathbb{Z}[\theta]}{d}$. □

Es bezeichne I_K die Idealgruppe, d.h. die Gruppe der gebrochenen Ideale $\neq \{0\}$ des Dedekindringes R. Weiter sei H_K die Untergruppe der Hauptideale und $Cl_K = I_K/H_K$ die Idealklassengruppe.

Für ein $\mathfrak{c} \in I_K$ existiert nach der Definition eines gebrochenen Ideals stets ein $d \in R \backslash \{0\}$, sodaß $d\mathfrak{c}$ ein ganzes Ideal $\mathfrak{a}$ von R ist. Wir zeigen jetzt, daß man sogar $d \in \mathbb{N} \backslash \{0\}$ wählen kann.

Lemma 1.1.3. *Sei $\mathfrak{c} \in I_K$. Dann existieren ganze Ideale $\mathfrak{a}, \mathfrak{b} \in I_K$ und $a, b \in \mathbb{N} \backslash \{0\}$, sodaß $\mathfrak{c} = \frac{\mathfrak{a}}{a}$ und $\mathfrak{c} = \frac{b}{\mathfrak{b}}$.*

Beweis. Sei $d \in R \backslash \{0\}$, sodaß $d\mathfrak{c}$ ein ganzes Ideal von R ist. Wegen $d \neq 0$ ist $(d) \cap \mathbb{Z} \neq \{0\}$, d.h. es existiert $d' \in R$ mit $a := dd' \in \mathbb{N} \backslash \{0\}$. Damit ist auch $\mathfrak{a} := dd'\mathfrak{c} \in I_K$ ganz, und es gilt $\mathfrak{c} = \frac{\mathfrak{a}}{a}$.

Sei nun hiernach $\mathfrak{c}^{-1} = \frac{\mathfrak{b}}{b}$ mit $\mathfrak{b} \in I_K$ ganz und $b \in \mathbb{N} \backslash \{0\}$. Dann ist $\mathfrak{c} = \frac{1}{\mathfrak{c}^{-1}} = \frac{b}{\mathfrak{b}}$. □

Es bezeichne $N_{K/\mathbb{Q}} \colon K \to \mathbb{Q}$ die Normabbildung, d.h.

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

für $\alpha \in K$, wobei $\sigma_1, \sigma_2, \dots, \sigma_n$ die Einbettungen von $K/\mathbb{Q}$ in $\mathbb{C}$ sind. Für Ideale ist die Norm $\mathcal{N}_{K/\mathbb{Q}} \colon I_K \to \mathbb{Q}$ definiert durch

$$\mathcal{N}_{K/\mathbb{Q}}\left(\frac{\mathfrak{a}}{a}\right) := \frac{[R : \mathfrak{a}]}{|N(a)|} \quad \text{für } \mathfrak{a} \in I_K \text{ ganz und } a \in \mathbb{N},$$

wobei $[R : \mathfrak{a}]$ der Gruppenindex der entsprechenden additiven Gruppen ist. Bekanntermaßen gilt $\mathcal{N}_{K/\mathbb{Q}}((\alpha)) = |N(\alpha)|$ für $\alpha \in K$, und sowohl $N_{K/\mathbb{Q}}$ als auch $\mathcal{N}_{K/\mathbb{Q}}$ sind multiplikativ.

BEMERKUNG 1.1.4. *Sei* $\mathfrak{c} \in I_K$ *und* $\alpha \in \mathfrak{c}$. *Dann gibt es ein* $d \in \mathbb{N}$ *mit*

$$d\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{c}) = N_{K/\mathbb{Q}}(\alpha).$$

BEWEIS. Sei nach Lemma 1.1.3 $\mathfrak{c} = \frac{\mathfrak{a}}{a}$ mit $\mathfrak{a} \in I_K$ ganz und $a \in \mathbb{N}\backslash\{0\}$. Wegen $\alpha \in \mathfrak{c}$ ist also $(a\alpha) \subseteq \mathfrak{a}$, d.h. $\mathfrak{a}|(a\alpha)$. Da $\mathfrak{a}$ und $(a\alpha)$ ganze Ideale sind, folgt aufgrund der Multiplikativität der Idealnorm, daß es ein $d \in \mathbb{N}$ gibt mit

$$d\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) = \mathcal{N}_{K/\mathbb{Q}}((a\alpha)) = |N_{K/\mathbb{Q}}(a\alpha)| = |N_{K/\mathbb{Q}}(a)||N_{K/\mathbb{Q}}(\alpha)|.$$

Division durch $|N_{K/\mathbb{Q}}(a)|$ liefert dann

$$N_{K/\mathbb{Q}}(\alpha) = d\frac{\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})}{|N_{K/\mathbb{Q}}(a)|} = d\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{c}).$$

□

1.2. Geometrische Darstellung algebraischer Zahlen

In den folgenden Abschnitten sollen nun die für uns wichtigen Teile der Gitterpunkttheorie von Minkowski kurz dargestellt werden. Diese Theorie ist z.B. bei Borewics-Šafarevič [2], Kapitel II, §3, oder bei Marcus [13], Chapter 5, nachzulesen.

Sei K ein Algebraischer Zahlkörper vom Grad n, und sei r die Anzahl der reellen Einbettungen und s die Anzahl der Paare konjugiert komplexer Einbettungen von $K/\mathbb{Q}$ in $\mathbb{C}$. Dann ist bekanntlich $n = r+2s$. Wir betrachten den *Minkowski-Raum*

$$K_{\mathbb{R}} := \mathbb{R}^r \times \mathbb{C}^s,$$

den wir zunächst als direktes Produkt der Ringe $\mathbb{R}$ und $\mathbb{C}$ auffassen. Für ein beliebiges Element $x \in K_{\mathbb{R}}$ bezeichnen wir die $r+s$ Komponenten mit $x_1, x_2, \ldots, x_{r+s}$ und schreiben $x = (x_1, \ldots, x_{r+s})$.. Mit der komponentenweise erklärten Addition und Multiplikation wird $K_{\mathbb{R}}$ dann bekanntlich selbst kommutativer Ring mit der Eins $(1, 1, \ldots, 1)$. Es ist auch klar, daß $K_{\mathbb{R}}$ ein $\mathbb{R}$-Vektorraum wird, indem man die Multiplikation mit Elementen aus $\mathbb{R}$ komponentenweise erklärt, und offensichtlich bilden die n Vektoren

$$
(3) \qquad \begin{array}{ll}
(1,\dots,0, & 0,\dots,0)\ , \\
\vdots & \vdots \\
(0,\dots,1, & 0,\dots,0)\ , \\
(0,\dots,0, & 1,\dots,0)\ , \\
(0,\dots,0, & i,\dots,0)\ , \\
\vdots & \vdots \\
(0,\dots,0, & 0,\dots,1)\ , \\
(\underbrace{0,\dots,0}_{r}, & \underbrace{0,\dots,i}_{s})
\end{array}
$$

eine $\mathbb{R}$-Basis. $K_{\mathbb{R}}$ ist also ein $\mathbb{R}$-Vektorraum der Dimension $n = r + 2s$, und

$$v\colon K_{\mathbb{R}} \to \mathbb{R}^n, \quad x \mapsto (x_1,\dots,x_r, \operatorname{Re} x_{r+1}, \operatorname{Im} x_{r+1}, \dots, \operatorname{Re} x_{r+s}, \operatorname{Im} x_{r+s}).$$

ist offensichtlich ein $\mathbb{R}$-Vektorraum-Isomorphismus zwischen dem Minkowski-Raum $K_{\mathbb{R}}$ und $\mathbb{R}^n$.

Um zu einer geometrischen Interpretation der algebraischen Zahlen zu gelangen, soll der Algebraische Zahlkörper K in den Minkowski-Raum $K_{\mathbb{R}}$ bzw. in den dazu isomorphen Vektorraum $\mathbb{R}^n$ eingebettet werden. Es seien $\sigma_1, \sigma_2, \dots, \sigma_r$ die r reellen Einbettungen und $\sigma_{r+1}, \bar\sigma_{r+1}, \sigma_{r+2}, \bar\sigma_{r+2}, \dots, \sigma_{r+s}, \bar\sigma_{r+s}$ die s Paare konjugiert komplexer Einbettungen von $K/\mathbb{Q}$ in $\mathbb{C}$.

Definition 1.2.1. Die Abbildung $x\colon K \to K_{\mathbb{R}}$ sei definiert durch

$$x(\alpha) := (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \dots, \sigma_{r+s}(\alpha))$$

für $\alpha \in K$. Es heißt dann $v \circ x\colon K \to \mathbb{R}^n$,

$$\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re}\, \sigma_{r+1}(\alpha), \operatorname{Im}\, \sigma_{r+1}(\alpha), \dots, \operatorname{Re}\, \sigma_{r+s}(\alpha), \operatorname{Im}\, \sigma_{r+s}(\alpha))$$

die *geometrische Darstellung* von K und $(v \circ x)(\alpha)$ das *geometrische Bild* von $\alpha \in K$. [1]

Bemerkung 1.2.2. *Für $\alpha, \beta \in K$, $\lambda \in \mathbb{Q}$ gelten :*

(i) $x(\alpha + \beta) = x(\alpha) + x(\beta)$
(ii) $x(\alpha\beta) = x(\alpha)x(\beta)$
(iii) $x(\lambda\alpha) = \lambda x(\alpha)$

Beweis. Die Eigenschaften (i) bis (iii) prüft man leicht komponentenweise nach, da die Einbettungen σ_i von $K/\mathbb{Q}$ in $\mathbb{C}$ diese Eigenschaften haben. □

Bemerkung 1.2.3. *Die Abbildung $x\colon K \to K_{\mathbb{R}}$ ist ein injektiver, $\mathbb{Q}$-linearer Ringhomomorphismus.*

[1] vgl. Borewics-Šafarevič [2], Kapitel II, §3, Seite 115

Beweis. Wegen Bemerkung 1.2.2 ist x $\mathbb{Q}$-linearer Ringhomomorphismus. x ist auch injektiv, da alle Komponentenabbildungen als Einbettungen von $K/\mathbb{Q}$ in $\mathbb{C}$ injektiv sind. $\square$

Bemerkung 1.2.4. *Die geometrische Darstellung* $v \circ x\colon K \to \mathbb{R}^n$ *ist ein injektiver,* $\mathbb{Q}$*-linearer Gruppenhomomorphismus der additiven Gruppe* $(K,+)$ *in* $(\mathbb{R}^n,+)$.

Beweis. Es sind x und v injektive, $\mathbb{Q}$-lineare Gruppenhomomorphismen, also auch $v \circ x$, da v $\mathbb{R}$-Vektorraumisomorphismus ist. $\square$

Für einen fixierten Punkt $x \in K_\mathbb{R}$ sei m_x die Multiplikation mit x auf $K_\mathbb{R}$, d.h.

$$m_x\colon K_\mathbb{R} \to K_\mathbb{R}, \quad y \mapsto xy.$$

Dann ist m_x ein Vektorraum-Endomorphismus von $K_\mathbb{R}$ und die Matrix von m_x bzgl. der Basis (3) hat die Form

$$\begin{pmatrix} x_1 &&&&&&&& \\ & \ddots &&&&&&& \\ && x_r &&&&&& \\ &&& \operatorname{Re} x_{r+1} & -\operatorname{Im} x_{r+1} &&&& \\ &&& \operatorname{Im} x_{r+1} & \operatorname{Re} x_{r+1} &&&& \\ &&&&& \ddots &&& \\ &&&&&& \operatorname{Re} x_s & -\operatorname{Im} x_s \\ &&&&&& \operatorname{Im} x_s & \operatorname{Re} x_s \end{pmatrix}, \tag{4}$$

wobei alle nicht ausgeschriebenen Elemente der Matrix gleich Null sind.

Wir definieren eine Norm auf $K_\mathbb{R}$ durch

$$N_{K_\mathbb{R}}(x) := \det(m_x)$$

für $x \in K_\mathbb{R}$. Also ist $N_{K_\mathbb{R}}(x)$ gleich der Determinante der Matrix (4), d.h.

$$\begin{aligned} N_{K_\mathbb{R}}(x) &= x_1 \dots x_r((\operatorname{Re} x_{r+1})^2 + (\operatorname{Im} x_{r+1})^2) \dots ((\operatorname{Re} x_s)^2 + (\operatorname{Im} x_s)^2) \\ &= x_1 \dots x_r |x_{r+1}|^2 \dots |x_s|^2. \end{aligned} \tag{5}$$

Mittels des Vektorraum-Isomorphismus v können wir die Norm auch auf $\mathbb{R}^n$ übertragen :

$$N_{\mathbb{R}^n}(v(x)) := N_{K_\mathbb{R}}(x). \tag{6}$$

Bemerkung 1.2.5. *Es gelten :*

(i) $N_{K_\mathbb{R}}(xx') = N_{K_\mathbb{R}}(x) N_{K_\mathbb{R}}(x')$ *für alle* $x, x' \in K_\mathbb{R}$
(ii) $N_{K_\mathbb{R}}(tx) = t^n N_{K_\mathbb{R}}(x)$ *für alle* $x \in K_\mathbb{R}, t \in \mathbb{R}$
(iii) $N_{K_\mathbb{R}}(x(\alpha)) = N_{K/\mathbb{Q}}(\alpha)$ *für alle* $\alpha \in K$

Beweis. Die Eigenschaft (i) folgt aus der Multiplikativität der Determinantenabbildung. Zu (ii) und (iii) rechnet man unter Verwendung von (5) nach :

$$N_{K_{\mathbb{R}}}(tx) = \prod_{i=1}^{r} tx_i \prod_{i=r+1}^{r+s} |tx_i|^2 = (t^r \prod_{i=1}^{r} x_i)(t^{2s} \prod_{i=r+1}^{r+s} |x_i|^2) = t^n N_{K_{\mathbb{R}}}(x),$$

und

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha) &= \prod_{j=1}^{r} \sigma_j(\alpha) \prod_{j=r+1}^{r+s} \sigma_j(\alpha)\bar{\sigma}_j(\alpha) = \prod_{j=1}^{r} \sigma_j(\alpha) \prod_{j=r+1}^{r+s} |\sigma_j(\alpha)|^2 \\ &= \prod_{j=1}^{r} x(\alpha)_j \prod_{j=r+1}^{r+s} |x(\alpha)_j|^2 = N_{K_{\mathbb{R}}}(x(\alpha)). \end{aligned}$$

□

Aufgrund der Eigenschaft (iii) in Bemerkung 1.2.5 und (6) wollen wir im folgenden die Normen $N_{K/\mathbb{Q}}$, $N_{K_{\mathbb{R}}}$ und $N_{\mathbb{R}^n}$ nur noch kurz mit N bezeichnen. Ebenso bezeichnen wir die Idealnorm $\mathcal{N}_{K/\mathbb{Q}}$ kurz mit $\mathcal{N}$.

Bemerkung 1.2.6. *Sei $(y_1, y_2, \ldots, y_n)$ eine fest gewählte $\mathbb{R}$-Basis von $K_{\mathbb{R}}$. Dann gibt es ein homogenes Polynom $F \in \mathbb{R}[T_1, T_2, \ldots, T_n]$ mit*

$$N(\sum_{i=1}^{n} t_i y_i) = F(t_1, t_2, \ldots, t_n) \quad \textit{für alle } t_1, t_2, \ldots, t_n \in \mathbb{R}.$$

Beweis. Setze $x := \sum_{i=1}^{n} t_i y_i$. Dann gilt $x_j = \sum_{i=1}^{n} t_i y_{ij}$ für $j = 1, \ldots, r+s$. Damit ist nach (5)

$$\begin{aligned} N(x) &= \prod_{j=1}^{r} x_j \prod_{j=r+1}^{r+s} (\mathrm{Re}^2(x_j) + \mathrm{Im}^2(x_j)) \\ &= \prod_{j=1}^{r} (\sum_{i=1}^{n} t_i y_{ij}) \prod_{j=r+1}^{r+s} ((\sum_{i=1}^{n} t_i \,\mathrm{Re}(y_{ij}))^2 + (\sum_{i=1}^{n} t_i \,\mathrm{Im}(y_{ij}))^2) \\ &= \sum_{\substack{(e_i) \in \mathbb{N}^n, \\ \sum e_i = n}} c_{(e_i)} (\prod_{i=1}^{n} t_i^{e_i}) \end{aligned}$$

für geeignete $c_{(e_i)} \in \mathbb{R}$. Wählt man die $c_{(e_i)}$ als Koeffizienten von F, so ergibt sich die Behauptung. □

Korollar 1.2.7. *Die Normabbildung $N \colon K_{\mathbb{R}} \to \mathbb{R}$ ist stetig.*

Beweis. Das Polynom F in Bemerkung 1.2.6 ist stetig. □

SATZ 1.2.8. *Sind $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ linear unabhängig über $\mathbb{Q}$, so sind die geometrischen Bilder*

$$(v \circ x)(\alpha_1), (v \circ x)(\alpha_2), \dots, (v \circ x)(\alpha_n) \in \mathbb{R}^n$$

linear unabhängig über $\mathbb{R}$.

BEWEIS. siehe Borewics-Šafarevič [2], Kapitel II, §3, Seite 115ff. □

Damit ist klar

KOROLLAR 1.2.9. *Für eine Ganzheitsbasis $(\omega_1, \omega_2, \dots, \omega_n)$ von $K/\mathbb{Q}$ ist*

$$((v \circ x)(\omega_1), (v \circ x)(\omega_2), \dots, (v \circ x)(\omega_n))$$

eine $\mathbb{R}$-Basis von $\mathbb{R}^n$.

Wir identifizieren im folgenden $\alpha \in K$ mit dem geometrischen Bild $(v \circ x)(\alpha) \in \mathbb{R}^n$. Damit können wir also die Ganzheitsbasis Ω auch als $\mathbb{R}$-Basis von $\mathbb{R}^n$ auffassen.

Im folgenden wird uns das geometrische Bild von Idealen interessieren. Dazu führen wir den Begriff des Gitters ein.

1.3. Ganzzahlige Gitter in $\mathbb{Q}$- und $\mathbb{R}$-Vektorräumen

Sei in diesem Abschnitt $\mathbb{K}$ ein Körper mit $\mathbb{K} = \mathbb{Q}$ oder $\mathbb{K} = \mathbb{R}$ und V ein n-dimensionaler $\mathbb{K}$-Vektorraum, $n < \infty$.

DEFINITION 1.3.1. Seien $v_1, v_2, \dots, v_m \in V$ linear unabhängig und sei G der von $B := (v_1, v_2, \dots, v_m)$ erzeugte $\mathbb{Z}$-Modul.
Dann heißt G *Gitter* in V der Dimension m. Das m-Tupel $(v_1, v_2, \dots, v_m)$ heißt *Basis* von G und

$$D_G := D_G(B) := \{t_1 v_1 + t_2 v_2 + \dots + t_m v_m \mid t_i \in \mathbb{K}, 0 \le t_i < 1\}$$

die *Grundmasche von G bzgl. B*. Das Gitter G heißt *vollständig*, wenn die Dimension von G gleich n ist.

LEMMA 1.3.2. *Sei G ein vollständiges Gitter von V und D_G die Grundmasche von G bzgl. einer Basis. Dann gilt*

$$(D_G + g) \cap D_G = \emptyset \quad \textit{für alle } g \in G\backslash\{0\}.$$

BEWEIS. Wähle eine Basis $(v_1, v_2, \dots, v_n)$ von G. Es ist dann B auch $\mathbb{K}$-Basis von V, da $v_1, v_2, \dots, v_n$ linear unabhängig über $\mathbb{K}$ sind. Seien

$$v = t_1 v_1 + t_2 v_2 + \dots + t_n v_n \in D_G, \quad t_i \in \mathbb{K}, 0 \le \lambda < 1,$$

und

$$g = c_1 v_1 + c_2 v_2 + \dots + c_n v_n \in G\backslash\{0\}, \quad c_i \in \mathbb{Z}, c_{i_0} \neq 0.$$

Dann ist

$$v + g = t'_1 v_1 + \cdots + t'_{i_0} v_{i_0} + \ldots t'_n v_n$$

mit $t'_{i_0} = t_{i_0} + c_{i_0} \notin [0,1)$, d.h. $v + g \notin D_G$. $\square$

SATZ 1.3.3. *Sei G ein vollständiges Gitter von V und D_G die Grundmasche von G bzgl. einer Basis. Dann gibt es für jedes $v \in V$ genau ein $g \in G$, sodaß*

$$v + g \in D_G.$$

BEWEIS. Eindeutigkeit : Seien $g, g' \in G$ mit $v + g, v + g' \in D_G$. Dann ist $v + g' = (v + g) + (g' - g)$, und wegen $(g' - g) \in G$ folgt nach Lemma 1.3.2 $g' - g = 0$.

Existenz : Wähle eine Basis $(v_1, v_2, \ldots, v_n)$ von G. Seien

$$v = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n \in V, \quad t_i \in \mathbb{K},$$

und $t_i = c_i + t'_i$, $c_i \in \mathbb{Z}$, sodaß $0 \leq t'_i < 1$. Setze nun

$$g := -(c_1 v_1 + c_2 v_2 + \cdots + c_n v_n) \in G.$$

Dann ist

$$v + g = '_1 v_1 +'_2 v_2 + \cdots +'_n v_n \in D_G.$$

$\square$

KOROLLAR 1.3.4. *Sei G ein vollständiges Gitter von V und D_G die Grundmasche von G bzgl. einer Basis. Dann ist*

$$\bigcup_{g \in G} (D_G + g) = V \tag{7}$$

eine disjunkte Überdeckung von V.

BEWEIS. klar nach Satz 1.3.3. $\square$

Eine äquivalente Formulierung des Gitterbegriffs im Fall $\mathbb{K} = \mathbb{R}$ liefert der

SATZ 1.3.5. *Sei V ein $\mathbb{R}$-Vektorraum und U eine Untergruppe von $(V, +)$. Dann ist U ein Gitter von V genau dann, wenn in jeder Kugel*

$$U_r := \left\{ t_1 v_1 + t_2 v_2 + \cdots + t_n v_n \,\middle|\, t_1^2 + t_2^2 + \cdots + t_n^2 \leq r^2 \right\}, \quad r \in \mathbb{R},$$

nur endlich viele Elemente von U liegen, d.h. wenn U diskret ist.

BEWEIS. siehe Borewics-Šafarevič [2], Kapitel II, §3, Lemma 1 und 4. $\square$

1.4. Ideale als Gitter

Sei jetzt K ein algebraischer Zahlkörper vom Grad n und R sein Ganzheitsring. Wir fixieren im folgenden eine Ganzheitsbasis $\Omega = (\omega_1, \omega_2, \dots, \omega_n)$ von $K/\mathbb{Q}$. Bekanntlich ist K ein n-dimensionaler $\mathbb{Q}$-Vektorraum und Ω eine $\mathbb{Q}$-Basis von K. In Korollar 1.2.9 haben wir gesehen, daß Ω – sofern wir Ω mit dem geometrischen Bild $(v \circ x)(\Omega)$ identifizieren – auch $\mathbb{R}$-Basis von $\mathbb{R}^n$ ist.

Satz 1.4.1. *Sei $\mathfrak{c} \in I_K$ ein beliebiges Ideal und B eine $\mathbb{Z}$-Basis von $\mathfrak{c}$. Dann ist $\mathfrak{c}$ ein vollständiges Gitter im $\mathbb{Q}$-Vektorraum K mit der Basis B und $(v \circ x)(\mathfrak{c})$ ein vollständiges Gitter im $\mathbb{R}$-Vektorraum $\mathbb{R}^n$ mit der Basis $(v \circ x)(B)$.*

Beweis. Es ist $\mathfrak{c}$ ein $\mathbb{Z}$-Modul mit Basis B. Da $v \circ x$ $\mathbb{Q}$-linear ist, nach Bemerkung 1.2.4, ist auch $(v \circ x)(\mathfrak{c})$ $\mathbb{Z}$-Modul mit der Basis $(v \circ x)(B)$. □

Wir wollen $\mathfrak{c}$ im folgenden mit seinem geometrischen Bild $(v \circ x)(\mathfrak{c})$ und B mit $(v \circ x)(B)$ identifizieren und können dann $\mathfrak{c}$ auch als Gitter in $\mathbb{R}^n$ mit Basis B auffassen.

Definition 1.4.2. Sei $\mathfrak{c} \in I_K$ mit der $\mathbb{Z}$-Basis B. Es bezeichne dann

$$\Phi_\mathfrak{c}(B) := D_{(v \circ x)(\mathfrak{c})}((v \circ x)(B))$$

die Grundmasche [2] des mit $\mathfrak{c}$ identifizierten Gitters $(v \circ x)(\mathfrak{c})$ in $\mathbb{R}^n$.

Bemerkung 1.4.3. *Ist die $\mathbb{Z}$-Basis B eines Ideals $\mathfrak{c} \in I_K$ fest gewählt, so schreiben wir für $\Phi_\mathfrak{c}(B)$ auch kurz $\Phi_\mathfrak{c}$. Im Fall $\mathfrak{c} = R$ wählen wir speziell $B = \Omega$ und bezeichnen $\Phi_R(\Omega)$ einfach mit Φ.*

Bemerkung 1.4.4. *Sei $\mathfrak{c} \in I_K$ ein gebrochenes Ideal und*

$$D_\mathfrak{c} = \{\lambda_1\gamma_1 + \dots + \lambda_n\gamma_n \mid \lambda_i \in \mathbb{Q}, 0 \le \lambda_i < 1\}$$

die Grundmasche des Gitters $\mathfrak{c}$ im $\mathbb{Q}$-Vektorraum K bgzl. einer fixierten Basis $(\gamma_1, \dots, \gamma_n)$. Dann gilt

$$\Phi_\mathfrak{c} \cap (v \circ x)(K) = (v \circ x)(D_\mathfrak{c}).$$

Identifizieren wir K mit dem geometrischen Bild $(v \circ x)(K)$, so ist $\Phi_\mathfrak{c} \cap K$ also Grundmasche des Gitters $\mathfrak{c}$ in K.

Beweis. Nach Definition 1.4.2 ist

$$\Phi_\mathfrak{c} = \{t_1(v \circ x)(\gamma_1) + \dots + t_n(v \circ x)(\gamma_n) \mid t_i \in \mathbb{R}, 0 \le t_i < 1\},$$

und da $(\gamma_1, \dots, \gamma_n)$ $\mathbb{Q}$-Basis von K ist und $(v \circ x)$ nach Bemerkung 1.2.4 $\mathbb{Q}$-linear ist, gilt $t_1(v \circ x)(\gamma_1) + \dots + t_n(v \circ x)(\gamma_n) \in (v \circ x)(K)$ genau dann wenn $t_1, \dots, t_n \in \mathbb{Q}$. □

[2] wie sie in Definition 1.3.1 definiert wurde

An dieser Stelle wollen wir an das bekannte Beipiel des Gaußschen Zahlringes $\mathbb{Z}[i]$ erinnern, der sich bekanntlich in der Gaußschen Zahlebene $\mathbb{R}^2$ als das Gitter der Punkte mit ganzen Koordinaten anschauen läßt. Der in der elementaren Zahlentheorie übliche geometrische Beweis, daß $\mathbb{Z}[i]$ Euklidischer Ring ist, läuft dann darauf hinaus, daß die offenen Kreisscheiben vom Radius 1 um die Gitterpunkte die gesamte Gaußsche Zahlenebene überdecken. [3] Später werden wir dieses geometrische Beweisverfahren verallgemeinern und auf beliebige Zahlringe anwenden. Es wird dabei immer darauf ankommen, zu zeigen daß in einem Vektorraum V eine gewisse Teilmenge $E \subseteq V$ bereits den gesamten Vektorraum überdeckt. In dem Beispiel des Gaußschen Zahlringes $\mathbb{Z}[i]$ ist dann $V = \mathbb{R}^2$ die Gaußsche Zahlenebene, und die Menge E besteht aus den offenen Kreisscheiben vom Radius 1 um die Gitterpunkte.

Nach Korollar 1.3.4 überdecken die Translationen der Grundmasche Φ um Elemente aus R bereits den ganzen Vektorraum $\mathbb{R}^n$. Ist nun die Menge E invariant unter Translationen um Elemente aus R, so folgt daher aus $\Phi \subseteq E$ bereits $E = \mathbb{R}^n$, und die Überdeckung der beschränkten Menge Φ wird häufig leichter nachzuweisen sein als die Überdeckung des gesamten Vektorraums. Im folgenden sollen Hilfsmittel bereitgestellt werden, mit denen man sich beim Nachweis der Überdeckung von $\mathbb{R}^n$ auf noch kleinere Mengen als die Grundmasche Φ beschränken kann. Dazu werden wir die Überdeckungseigenschaft der Grundmasche aus Korollar 1.3.4 noch etwas verallgemeinern, und zwar dahingehend, daß neben der Translation um Elemente aus $\mathfrak{c}$ auch die Assoziiertenbildung zugelassen wird. Ein solches Gebiet, dessen Assoziierte und Translationen von Assoziierten den ganzen Vektorraum überdecken, werden wir *Überdeckungsgebiet* nennen, wie in der folgenden Definition 1.4.5 präziser formuliert wird.

Wir betrachten im folgenden stets die beiden Fälle $\mathbb{K} = \mathbb{Q}$, $V = K$ und $\mathbb{K} = \mathbb{R}$, $V = \mathbb{R}^n$. Es bezeichne R^* die Einheitengruppe des Ganzheitsrings R. Man beachte, daß in Abschnitt 1.2 auch für den Fall $\mathbb{K} = \mathbb{R}$, $V = \mathbb{R}^n$ eine Multiplikation auf ganz V definiert wurde.

DEFINITION 1.4.5. Sei $\mathfrak{c} \in I_K$. Erfüllt $\Psi \subseteq V$ die Bedingung

$$\bigcup_{u \in R^*, \gamma \in \mathfrak{c}} (u\Psi + \gamma) = V, \tag{8}$$

so heißt Ψ ein *V-Überdeckungsgebiet bzgl. $\mathfrak{c}$*.

SATZ 1.4.6. *Sei $\mathfrak{c} \in I_K$ und eine $\mathbb{Z}$-Basis B von $\mathfrak{c}$ fixiert. Sei $\Psi \subseteq V$ mit*

$$\bigcup_{u \in R^*, \gamma \in \mathfrak{c}} (u\Psi + \gamma) \supseteq \Phi_{\mathfrak{c}}. \tag{9}$$

[3] vgl. dazu z.B. Koch, Piper [9], Satz 1.9, Seite 18

Dann ist Ψ ein V-Überdeckungsgebiet bzgl. $\mathfrak{c}$. Insbesondere ist also die Grundmasche $\Phi_\mathfrak{c}$ auch V-Überdeckungsgebiet bzgl. $\mathfrak{c}$.

BEWEIS. Aus (9) folgt nach Korollar 1.3.4

$$\bigcup_{u \in R^*, \gamma \in \mathfrak{c}} (u\Psi + \gamma) \supseteq \bigcup_{\gamma \in \mathfrak{c}} (\Phi_\mathfrak{c} + \gamma) = V.$$

□

BEMERKUNG 1.4.7. *Sei $\mathfrak{c} \in I_K$ und $\Psi \subseteq \mathbb{R}^n$ ein $\mathbb{R}^n$-Überdeckungsgebiet bzgl $\mathfrak{c}$. Dann ist $\Psi \cap K$ ein K-Überdeckungsgebiet bzgl. $\mathfrak{c}$.*

BEWEIS. Wegen $uK + \gamma = K$ für alle $u \in R^*$, $\gamma \in R$ ist

$$\bigcup_{u \in R^*, \gamma \in \mathfrak{c}} (u(\Psi \cap K) + \gamma) = \bigcup_{u \in R^*, \gamma \in \mathfrak{c}} (u\Psi + \gamma) \cap K = \mathbb{R}^n \cap K = K.$$

□

Mit dieser Verallgemeinerung der Überdeckungseigenschaft nach Definition 1.4.5 müssen wir nun allerdings auch die oben angedeutete Invarianz-Eigenschaft der Teilmenge $E \subseteq V$ entsprechend verschärfen. Wir werden dazu ein $E \subseteq V$, das unter Assoziiertenbildung und Translationen invariant ist, *Fixgebiet* nennen, wie in der folgenden Definition präziser formuliert wird.

DEFINITION 1.4.8. Sei $\mathfrak{c} \in I_K$. Hat $E \subseteq V$ die Eigenschaften

(i) $E = E + \gamma$ für alle $\gamma \in \mathfrak{c}$
(ii) $E = uE$ für alle $u \in R^*$

so heißt E ein *Fixgebiet* bzgl. $\mathfrak{c}$.

BEMERKUNG 1.4.9. *Da die Translation um $\gamma \in R$ und die Multiplikation mit $u \in R^*$ invertierbar sind, reicht es in Definition* 1.4.8 *aus, jeweils die Inklusion "$\supseteq$" zu fordern.*

Wir kommen nun zu der wichtigen Eigenschaft von Fixgebieten im Zusammenang mit entsprechenden Überdeckungsgebieten.

SATZ 1.4.10. *Sei $\mathfrak{c} \in I_K$ und $E \subseteq V$ ein Fixgebiet bzgl. $\mathfrak{c}$. Ist $E \supseteq \Psi$ für ein V-Überdeckungsgebiet Ψ bzgl. $\mathfrak{c}$, so gilt schon $E = V$.*

BEWEIS. Sei $x \in V$. Da Ψ V-Überdeckungsgebiet bzgl. $\mathfrak{c}$ ist, gibt es $x' \in \Psi, u \in R^*, \gamma \in \mathfrak{c}$, sodaß

$$x = ux' + \gamma.$$

Nach Voraussetzung ist $x' \in E$, und da E Fixgebiet bzgl. $\mathfrak{c}$ ist, folgt auch $x \in E$. □

BEMERKUNG 1.4.11. *Sei $\mathfrak{c} \in I_K$. Dann gelten :*

(i) *Ist $E \subseteq \mathbb{R}^n$ ein Fixgebiet bzgl. $\mathfrak{c}$, so auch $E \cap K$.*
(ii) *Ist $(E_i)_{i\in I}$, $E_i \subseteq \mathbb{R}^n$, eine Familie von Fixgebieten bzgl. $\mathfrak{c}$, so ist auch $E := \bigcup_{i\in I} E_i$ Fixgebiet bzgl. $\mathfrak{c}$.*

BEWEIS. Prüfe jeweils die Eigenschaften (i) und (ii) aus Definition 1.4.8 nach.
(i) Wegen $K + \gamma = K$ für alle $\gamma \in \mathfrak{c}$ ist $(E \cap K) + \gamma = E \cap K$, und wegen $uK = K$ für alle $u \in R^*$ ist $u(E \cap K) = E \cap K$.
(ii) Für $\gamma \in \mathfrak{c}$ ist $E = \bigcup_{i\in I}(E_i + \gamma) = (\bigcup_{i\in I} E_i) + \gamma = E + \gamma$, und für $u \in R^*$ ist $E = \bigcup_{i\in I}(uE_i) = u(\bigcup_{i\in I} E_i) = uE$.

□

Wir definieren das Volumen $\operatorname{Vol} U$ einer Teilmenge $U \subseteq \mathbb{R}^n$ als deren Lebesgue-Maß. Das Volumen der Grundmaschen eines Gitters $\mathfrak{a}$ hängt dann nach der Gitterpunkttheorie von Minkowski wie folgt mit der Idealnorm von $\mathfrak{a}$ zusammen.

SATZ 1.4.12. *Sei $\mathfrak{a} \in I_K$ ein gebrochenes Ideal,* $\operatorname{disc}(K/\mathbb{Q})$ *die Diskriminante von K und s die Anzahl der Paare konjugiert-komplexer Einbettungen. Dann gilt für jede Grundmasche $\Phi_{\mathfrak{a}}$ von $\mathfrak{a}$:*

$$\operatorname{Vol} \Phi_{\mathfrak{a}} = \frac{1}{2^s}\mathcal{N}(\mathfrak{a})\sqrt{|\operatorname{disc}(K/\mathbb{Q})|}\ .$$

BEWEIS. siehe Marcus [13], Chapter 5, Theorem 36, Seite 134ff. □

Wir wollen nun für ein beliebiges Ideal mit gegebener $\mathbb{Z}$-Basis ein Beispiel für ein Überdeckungsgebiet bzgl. $\mathfrak{c}$ angeben, daß das halbe Volumen der Grundmasche $\Phi_{\mathfrak{c}}$ hat.

BEISPIEL 1.4.13. Sei $\mathfrak{c} \in I_K$ mit der $\mathbb{Z}$-Basis $(\gamma_1, \gamma_2, \dots, \gamma_n)$. Es ist dann

$$\Psi_{\mathfrak{c}} := \left\{ t_1\gamma_1 + \cdots + t_n\gamma_n \;\middle|\; t_i \in \mathbb{R}, 0 \le t_1 \le \frac{1}{2}, 0 \le t_i < 1 \quad \text{für } i = 2, \dots, n \right\}$$

ein $\mathbb{R}^n$-Überdeckungsgebiet bzgl. $\mathfrak{c}$. Nach Bemerkung 1.4.7 ist dann auch

$$\Psi_{\mathfrak{c}} \cap K = \left\{ t_1\gamma_1 + \cdots + t_n\gamma_n \;\middle|\; t_i \in \mathbb{Q}, 0 \le t_1 \le \frac{1}{2}, 0 \le t_i < 1 \quad \text{für } i = 2, \dots, n \right\}$$

ein K-Überdeckungsgebiet bzgl. $\mathfrak{c}$.

BEWEIS. Wir zeigen Bedingung (9) aus Satz 1.4.6. Sei dazu

$$x = t_1\gamma_1 + t_2\gamma_2 + \cdots + t_n\gamma_n \in \Phi_{\mathfrak{c}},$$

d.h. $t_i \in \mathbb{R}$, $0 \le t_i < 1$. Zu zeigen ist, daß es $u \in R^*$, $\delta \in \mathfrak{c}$ gibt, sodaß $u(x+\delta) \in \Psi_{\mathfrak{c}}$ gilt. Ist $t_1 \le \frac{1}{2}$, so ist schon $x \in \Psi_{\mathfrak{c}}$. Sei also o.B.d.A. $t_1 > \frac{1}{2}$. Dann ist aber

$$-(x - (\gamma_1 + \cdots + \gamma_n)) = (1 - t_1)\gamma_1 + \cdots + (1 - t_n)\gamma_n \in \Psi_{\mathfrak{c}},$$

denn $0 \leq 1 - t_1 < \frac{1}{2}$. Da $-1 \in R^*$ und $\gamma_1 + \cdots + \gamma_n \in \mathfrak{c}$ ist die Behauptung gezeigt. $\square$

Ein weiteres wichtiges Ergebnis der Gitterpunkttheorie von Minkowski ist der

SATZ 1.4.14. *Sei $\mathfrak{a}$ ganzes Ideal von K . Dann existiert ein $\alpha \in \mathfrak{a}$, $a \neq 0$ mit*

$$|N(\alpha)| \leq M_K \mathcal{N}(\mathfrak{a}),$$

wobei $M_K := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K/\mathbb{Q})|}$ die Minkowski-Schranke *von K ist. Bekanntlich folgt hieraus, daß jede Idealklasse aus Cl_K ein ganzes Ideal $\mathfrak{a}$ enthält mit $\mathcal{N}(\mathfrak{a}) \leq M_K$.*

BEWEIS. siehe Marcus [13], Chapter 5, Theorem 37, Seite 135. $\square$

KAPITEL II

k-stufig Euklidische Ringe und Zahlkörper

2.1. k-stufig Euklidische Ringe

Es sei in diesem Abschnitt R ein beliebiger Integritätsbereich mit Eins und $\varphi\colon R \to \mathbb{N}_0$ eine Abbildung mit $\varphi(a) = 0 \Leftrightarrow a = 0$. Später in Abschnitt 2.3 werden wir für R wieder speziell den Ganzheitsring eines Algebraischen Zahlkörpers betrachten.

Aus der Algebra ist die folgende Definition bekannt

DEFINITION 2.1.1. Es heißt R *Euklidisch* bzgl. φ und φ eine *Euklidische Abbildung* auf R, falls es für alle $a, b \in R, b \neq 0$, ein $q \in R$ gibt, sodaß

$$a = qb + r \quad \text{und} \quad \varphi(r) < \varphi(b). \tag{10}$$

R heißt *Euklidisch*, falls eine Euklidische Abbildung auf R existiert.

In einem Euklidischen Integritätsbereich erhält man bekanntlich aus (10) iterativ eine Sequenz von Gleichungen der Form

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \end{aligned} \tag{11}$$

mit

$$\varphi(r_k) < \varphi(r_{k-1}) < \cdots < \varphi(b). \tag{12}$$

Dieses Iterationsverfahren nennt man den Euklidischen Algorithmus, der sich solange fortsetzen läßt bis $\varphi(r_k) = 0$ ist. Die Definition 2.1.1 wurde nun von Cooke in [6] dahingehend verallgemeinert, daß in einer Gleichungssqeuenz der Form (11) statt (12) nur $\varphi(r_k) < \varphi(b)$ gefordert wird, ohne Bedingungen an die $r_1, \ldots, r_{k-1}$ zu stellen. Diese Verallgemeinerung wollen wir nun gemäß Cooke [6] ausführen.

DEFINITION 2.1.2. Seien $a, b \in R$. Eine *k-stufige Divisionskette* $\mathcal{D}^{(k)}$ zu dem geordneten Paar (a, b) ist eine Sequenz von k Gleichungen der Form (11) mit $q_1, q_2, \ldots, q_k, r_1, r_2, \ldots, r_k \in R$. Die q_i heißen die *Quotienten* und die r_i die *Reste* von $\mathcal{D}^{(k)}$, r_k heißt der *terminale Rest*. Ist der terminale Rest $r_k = 0$, so heißt $\mathcal{D}^{(k)}$ *terminierend*.

BEMERKUNG 2.1.3. *Man beachte, daß eine Divisionskette schon eindeutig durch ihre Quotienten gegeben ist und auch zu jeder gegebenen Folge von Quotienen* $(q_1, q_2, \ldots, q_k)$ *eine Divisionskette existiert.*

BEMERKUNG 2.1.4. *Ist* $\mathcal{D}^{(k)}$ *eine k-stufige Divisionskette zu* (a, b) *und gilt* $d|b$ *in R, so ist* $\mathcal{D}^{(k)}$ *auch eine k-stufige Divisionskette zu* (a, d).

BEWEIS. Sei $b = dd'$, $d' \in R$. Schreibe die erste Gleichung von $\mathcal{D}^{(k)}$ als

$$a = (q_1 d')d + r_1.$$

□

DEFINITION 2.1.5. Sei $k \in \mathbb{N} \cup \{\infty\}$ und $\varphi\colon R \to \mathbb{N}_0$ eine Abbildung mit $\varphi(a) = 0 \Leftrightarrow a = 0$. Es heißt R *k-stufig Euklidisch* bzgl. φ und φ eine *k-stufig Euklidische Abbildung* auf R, falls es für alle $a, b \in R, b \neq 0$, ein $l \in \mathbb{N}, l \leq k$, und eine l-stufige Divisionskette $\mathcal{D}^{(l)}$ zu (a, b) gibt mit

$$\varphi(r_l) < \varphi(b).$$

R heißt *k-stufig Euklidisch*, falls eine k-stufig Euklidische Abbildung auf R existiert.

BEMERKUNG 2.1.6. *Nach Definition ist klar, daß ein k-stufig Euklidischer Ring,* $k \in \mathbb{N}$, *auch l-stufig Euklidisch für alle* $l \in \mathbb{N} \cup \{\infty\}, l \geq k$, *ist. Für* $k = 1$ *ergibt sich genau die übliche euklidische Bedingung aus Definition* 2.1.1.

Der folgende Satz aus [6] charakterisiert die ∞-stufig euklidischen Bedingung durch terminierende Divisionsketten.

SATZ 2.1.7 (COOKE). *R ist genau dann ∞-stufig Euklidisch, wenn es für alle* $a, b \in R, b \neq 0$, *eine terminierende Divisionskette zu* (a, b) *gibt. Insbesondere ist also die ∞-stufig euklidische Eigenschaft unabhängig von der Wahl der Abbildung* φ.

Beweis. $\Leftarrow$: Für alle $a, b \in R, b \neq 0$, existiere eine terminierende Divisionskette zu (a, b). Dann gilt für den terminalen Rest stets $\varphi(r_k) = 0 < \varphi(b)$, da $b \neq 0$. Also ist R ∞-stufig Euklidisch.

$\Rightarrow$: Sei R ∞-stufig Euklidisch und $a, b \in R, b \neq 0$. Eine terminierende Divisionskette zu (a, b) erhält man durch Iteration wie beim Euklidischen Algorithmus : Nach Definition 2.1.5 exisitiert ein $k \in \mathbb{N}$ und eine k-stufige Divisionskette $\mathcal{D}_0^{(k)}$ zu (a, b) mit $\varphi(r_k) < \varphi(b)$. Ist $r_k = 0$, so ist $\mathcal{D}_0^{(k)}$ schon terminierend. Sei also $r_k \neq 0$ und $\tilde{\mathcal{D}}^{(l)}$ eine nach Definition existierende Divisionskette zu (r_{k-1}, r_k), $l \in \mathbb{N}$. Bezeichnet man die Reste von $\tilde{\mathcal{D}}^{(l)}$ mit $r_{r+1}, r_{r+2}, \ldots, r_{r+l}$, so wird $\mathcal{D}_0^{(k)}$ zu einer $(r+l)$-stufigen Divisionskette $\mathcal{D}_1^{(r+l)}$ mit $\varphi(r_{k+l}) < \varphi(r_k)$ verlängert. Ist $r_{k+l} = 0$, so ist $\mathcal{D}_1^{(k+l)}$ terminierend; wenn nicht, fährt man mit dem Anfangspaar (r_{r+l-1}, r_{r+l}) fort und verlängert so analog $\mathcal{D}_1^{(k+l)}$ zu einer Divisionskette $\mathcal{D}_2$ mit einem terminalen Rest von kleinerem φ-Bild. Da $\mathbb{N}_0$ wohlgeordnet ist, kommt man so nach endlich vielen Anwendungen der ∞-stufig euklidischen Eigenschaft zu einer Divisionskette $\mathcal{D}_i^{(m)}$ zu (a, b) mit $\varphi(r_m) = 0$. Es folgt $r_m = 0$, und $\mathcal{D}_i^{(m)}$ ist terminierend. $\square$

Wie in Euklidischen Ringen läßt sich das folgende Lemma aus [6] beweisen.

Lemma 2.1.8 (Cooke). *In einem k-stufig Euklidischen Integritätsbereich R, $k \in \mathbb{N} \cup \{\infty\}$, existiert zu jedem Paar $a, b \in R$ ein $d \in R$ mit $(d) = (a, b)$, wobei (a, b) das von a, b erzeugte Ideal in R bezeichnet.*

Beweis. Seien $a, b \in R, b \neq 0$. Im Fall $b = 0$ wäre $(a, b) = (a)$. Nach Bemerkung 2.1.6 ist R ∞-stufig Euklidisch, und nach Satz 2.1.7 existiert ein $k \in \mathbb{N}$ und eine k-stufige terminierende Divisionskette $\mathcal{D}^{(k)}$ zu (a, b) :

$$
\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\ \vdots \\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \\
r_{k-2} &= q_k r_{k-1}.
\end{aligned}
\tag{13}
$$

Also ist

$$
\begin{aligned}
(r_{k-1}) &= (r_{k-2}, r_{k-1}) = (r_{k-2}, r_{k-3} - q_{k-1} r_{k-2}) \\
&= (r_{k-3}, r_{k-2}) = \cdots = (a, b).
\end{aligned}
$$

$\square$

BEMERKUNG 2.1.9. *Durch Auflösen der ersten* $k-1$ *Gleichungen von* (13) *nach* r_{k-1} *erhält man wie beim Euklidischen Algorithmus eine explizite Darstellung*

$$r_{k-1} = \lambda a + \mu b$$

mit $\lambda, \mu \in R$.

SATZ 2.1.10. *In einem* k*-stufig Euklidischen Integritätsbereich* R, $k \in \mathbb{N} \cup \{\infty\}$, *ist jedes endlich erzeugte Ideal Hauptideal.*

BEWEIS. Induktion nach der Länge des Erzeugendensystems mit Lemma 2.1.8. □

KOROLLAR 2.1.11. *Jeder* k*-stufig Euklidische noethersche Integritätsbereich* R, $k \in \mathbb{N} \cup \{\infty\}$, *ist Hauptidealring.*

BEWEIS. Da in einem noetherschen Ring jedes Ideal endlich erzeugt ist, ist R nach Satz 2.1.10 Hauptidealring. □

Wie für Hauptidealringe beweist man

LEMMA 2.1.12. *In einem* k*-stufig Euklidischen Integritätsbereich* R, $k \in \mathbb{N} \cup \{\infty\}$, *ist jedes unzerlegbare Element auch prim.*

BEWEIS. [1] Sei $p \in R$ unzerlegbar. Zu zeigen ist $p|ab \Rightarrow p|a \vee p|b$. Seien also $a, b \in R$ mit $p|ab$, $p\nmid a$. Nach Lemma 2.1.8 gibt es ein $d \in R$ mit $(a, p) = (d)$. Sei $d' \in R$, sodaß $p = dd'$. Dann ist d' keine Einheit, denn sonst wäre $(d) = (p)$ im Widerspruch zu $p\nmid a$. Da p unzerlegbar ist, folgt, daß d Einheit ist, d.h. $(a, p) = (1)$. Es existieren also $\lambda, \mu \in R$, sodaß $1 = \lambda a + \mu p$. Damit ergibt sich $p|b$, denn $b = \lambda ab + \mu pb$ und $p|ab$. □

Mit Hilfe der dieses Lemmas läßt sich nun der folgende Satz aus [6] beweisen.

SATZ 2.1.13 (COOKE). *Sei* R k*-stufig Euklidisch für ein* $k \in \mathbb{N} \cup \{\infty\}$ *und jede Nicht-Einheit aus* $R \setminus \{0\}$ *lasse sich als Produkt von unzerlegbaren Elementen schreiben. Dann ist* R *ZPE-Ring.*

BEWEIS. Da nach Lemma 2.1.12 jedes unzerlegbare Element aus R auch prim ist, läßt sich also jede Nicht-Einheit in R als Produkt von Primelementen schreiben.

Wir zeigen nun noch die Eindeutigkeit dieser Darstellung. Sei

$$p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$$

für Primelemente $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s \in R$.

Wir beweisen durch Induktion über r, daß $r = s$ und $p_i = q_i$ gilt (bei geeigneter Numerierung). Sei r=1. Es gilt $p_1 | q_1 q_2 \ldots q_s$, und da p_1 Primelement ist, folgt $p_1 | q_i$ für ein i, also $p_1 = q_i$. Mit der Kürzungsregel ergibt sich sofort $s = 1$ und $p_1 = q_1$.

[1] Der Beweis wird analog zu dem in der Algebra üblichen Beweis dieses Lemmas für Hauptidealringe geführt. Er beruht auf Lemma 2.1.8.

Sei nun $r > 1$ und wie oben $p_1 = q_i$, etwa $i = 1$. Nach der Kürzungsregel folgt $p_2 p_3 \dots p_r = q_2 q_3 \dots q_s$, und die Behauptung ergibt sich nach Induktionsvoraussetzung. $\square$

2.2. Kettenbrüche

Sei in diesem Abschnitt wieder R ein beliebiger Integritätsbereich mit Eins. Wir führen nun Kettenbrüche im Quotientenkörper $Q(R)$ von R ein und zeigen dann die Zusammenhänge zwischen Kettenbrüchen und Divisionketten auf. Dabei halten wir uns im wesentlichen an die Ausführungen in Cooke [6], §3.

DEFINITION 2.2.1. Seien $k \in \mathbb{N}, q_1, q_2, \dots, q_k \in R\backslash\{0\}$. Dann ist $[q_1, q_2, \dots, q_l] := \frac{a_l}{b_l} \in K$ für $1 \leq l \leq k$ induktiv definiert durch

$$\begin{aligned} a_0 &:= 1, & b_0 &:= 0, \\ a_1 &:= q_1, & b_1 &:= 1, \\ a_i &:= q_i a_{i-1} + a_{i-2}, & b_i &:= q_i b_{i-1} + b_{i-2} \quad \text{für } i > 1. \end{aligned}$$

Es heißt $[q_1, q_2, \dots, q_k]$ *(endlicher) Kettenbruch* der Länge k. Die Menge aller Kettenbrüche der Länge $\leq k$, $k \in \mathbb{N} \cup \{\infty\}$, bezeichnen wir mit CF_k :

$$CF_k := \{[q_1, q_2, \dots, q_l] \mid l \leq k, q_1, q_2, \dots, q_l \in R\}.$$

Es gilt also $CF_k \subseteq CF_{k+1} \subseteq CF_\infty$ für alle $k \in \mathbb{N}$ und $CF_1 = R$.

BEMERKUNG 2.2.2. *Seien $k \in \mathbb{N}, q_1, q_2, \dots, q_k \in R\backslash\{0\}$. Definiere*

$$A_i := \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \quad \textit{für } i = 1, 2, \dots, k.$$

Dann ist

$$A_1 A_2 \dots A_k = \begin{pmatrix} a_k & a_{k-1} \\ b_k & b_{k-1} \end{pmatrix}. \tag{14}$$

BEWEIS. Induktion über k. Es ist $A_1 = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_1 & a_0 \\ b_1 & b_0 \end{pmatrix}$. Sei nun $k > 1$ und (14) für $k - 1$ bereits bewiesen. Dann ist

$$\begin{aligned} A_1 A_2 \dots A_k &= \begin{pmatrix} a_{k-1} & a_{k-2} \\ b_{k-1} & b_{k-2} \end{pmatrix} \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} q_k a_{k-1} + a_{k-2} & a_{k-1} \\ q_k b_{k-1} + b_{k-2} & b_{k-1} \end{pmatrix} \\ &= \begin{pmatrix} a_k & a_{k-1} \\ b_k & b_{k-1} \end{pmatrix}. \end{aligned}$$

Also gilt (14) für alle $k \in \mathbb{N}$. $\square$

BEMERKUNG 2.2.3. *Seien* $k \in \mathbb{N}, k > 1, q_1, q_2, \ldots, q_k \in R\backslash\{0\}$. *Dann gilt*

$$[q_1, q_2, \ldots, q_k] = q_1 + \frac{1}{[q_2, q_3, \ldots, q_k]}, \tag{15}$$

also durch Induktion :

$$[q_1, q_2, \ldots, q_k] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_k}}}$$

BEWEIS. Definiere A_i für $i = 1, 2, \ldots, k$ wie in Bemerkung 2.2.2. Sei $A_2 A_3 \ldots A_k = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, d.h. nach (14) $[q_2, q_3, \ldots, q_k] = \frac{a}{b}$. Dann ist

$$A_1 A_2 \ldots A_k = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} q_1 a + b & q_1 c + d \\ a & c \end{pmatrix},$$

also nach (14)

$$[q_1, q_2, \ldots, q_k] = \frac{q_1 a + b}{a} = q_1 + \frac{b}{a} = q_1 + \frac{1}{[q_2, q_3, \ldots, q_k]}.$$

□

Hiermit haben wir eine etwas bessere Vorstellung von Kettenbrüchen bekommen. Man beachte jedoch, daß sich im allgemeinen nicht jedes Element des Quotientenkörpers $Q(R)$ als Kettenbruch schreiben läßt.

LEMMA 2.2.4. *Seien* $a, b \in R$. *Sei* $[q_1, q_2, \ldots, q_k] = \frac{a_k}{b_k}$ *ein Kettenbruch mit* $\frac{a}{b} = \frac{a_k}{b_k}$. *Dann gilt* $b_k | b$.

BEWEIS. Wir beweisen zunächst durch Induktion über k :

$$a_k b_{k-1} - a_{k-1} b_k = (-1)^k \tag{16}$$

Für $k = 1$ ist nach Definiton 2.2.1

$$a_1 b_0 - a_0 b_1 = 0 - 1 = -1.$$

Sei nun (16) für k bereits bewiesen. Dann ist

$$\begin{aligned} a_{k+1} b_k - a_k b_{k+1} &= q_{k+1} a_k b_k + a_{k-1} b_k - a_k q_{k+1} b_k - a_k b_{k-1} \\ &= a_{k-1} b_k - a_k b_{k-1} = -(-1)^k = (-1)^{k+1} \end{aligned}$$

Also gilt (16) für alle $k \geq 1$. Durch Multiplikation mit b folgt aufgrund der Voraussetzung $ba_k = ab_k$

$$ab_k b_{k-1} - ba_{k-1} b_k = (-1)^k b,$$

also $b_k | b$, da b_k die linke Seite teilt. □

BEMERKUNG 2.2.5. *Einen allgemeinen Kettenbruch aus CF_∞ schreiben wir entweder als $[q_1, q_2, \ldots, q_k]$ oder einfach als Bruch $\frac{a}{b}$. Bei der Schreibweise als Bruch setzen wir voraus, daß der Kettenbruch zunächst durch $q_1, q_2, \ldots, q_k$ gegeben ist, und sich der Zähler a und der Nenner b daraus wie a_k und b_k in Definition 2.2.1 ergeben. Als Folge von Lemma 2.2.4 sind dann a und b bis auf Assoziierte eindeutig bestimmt.*

Für die Mengen CF_k stellt man nun leicht fest :

BEMERKUNG 2.2.6. *Sei $k \in \mathbb{N} \cup \{\infty\}$. Dann ist CF_k ein Fixgebiet von R.* [2]

BEWEIS. Seien $q_1, q_2, \ldots, q_l \in R \backslash \{0\}$, $l \leq k$. Es ist zu zeigen, daß für alle $c \in R$, $u \in R^*$ gilt :

$$[q_1, q_2, \ldots, q_l] + c, u[q_1, q_2, \ldots, q_l] \in CF_k.$$

Aus Bemerkung 2.2.3 folgt aber sofort $[q_1, q_2, \ldots, q_l] + c = [q_1 + c, q_2, \ldots, q_l] \in CF_k$. Wir zeigen nun durch Induktion nach l :

$$u[q_1, q_2, \ldots, q_l] = [uq_1, u^{-1}q_2, uq_3, \ldots, u^{(-1)^{l-1}} q_l] \in CF_l. \tag{17}$$

Für $l = 1$ ist $u[q_1] = uq_1 = [uq_1] \in CF_1$. Sei also $l \geq 1$ und (17) für l bereits bewiesen. Dann ist nach Bemerkung 2.2.3 und der Induktionsvoraussetzung

$$\begin{aligned} u[q_1, q_2, \ldots, q_l] &= u(q_1 + \frac{1}{[q_2, q_3, \ldots, q_l]}) = uq_1 + \frac{1}{u^{-1}[q_2, q_3, \ldots, q_l]} \\ &= uq_1 + \frac{1}{[u^{-1}q_2, uq_3, u^{-1}q_4, \ldots, u^{(-1)^{l-1}} q_l]} \\ &= [uq_1, u^{-1}q_2, uq_3, \ldots, u^{(-1)^{l-1}} q_l] \in CF_l. \end{aligned}$$

und CF_k ist K-Fixgebiet von R. □

Das folgende Lemma liefert den Zusammenhang zwischen Kettenbrüchen und den in Abschnitt 2.1 eingeführten Divisionsketten.

[2] siehe Definiton 1.4.8

LEMMA 2.2.7. *Seien* $a, b \in R$, $q_1, q_2, \ldots, q_k \in R\backslash\{0\}$, $\frac{a_k}{b_k} = [q_1, q_2, \ldots, q_k]$. *Sei* $\mathcal{D}^{(k)}$ *die Divisionskette zu* (a, b) *mit Quotienten* $q_1, q_2, \ldots, q_k$. *Dann gilt für den terminalen Rest* r_k *von* $\mathcal{D}^{(k)}$

$$\frac{a}{b} - \frac{a_k}{b_k} = (-1)^{k+1}\frac{r_k}{bb_k}.$$

BEWEIS. Wir beweisen durch Induktion über k :

$$ab_k - ba_k = (-1)^{k+1} r_k. \tag{18}$$

Die Behauptung ergibt sich dann durch Multiplikation mit $\frac{1}{bb_k}$. Für $k = 1$ ist nach Definiton 2.2.1

$$ab_1 - ba_1 = a - bq_1 = r_1.$$

Sei nun $k > 1$ und (18) für $k - 1$ bereits bewiesen. Dann ist

$$\begin{aligned}
ab_k - ba_k &= aq_k b_{k-1} + ab_{k-2} - bq_k a_{k-1} - ba_{k-2} \\
&= q_k(ab_{k-1} - ba_{k-1}) + (ab_{k-2} - ba_{k-2}) \\
&= q_k(-1)^k r_{k-1} + (-1)^{k-1} r_{k-2} \\
&= (-1)^{k-1}(-q_k r_{k-1} + q_k r_{k-1} + r_k) \\
&= (-1)^{k+1} r_k.
\end{aligned}$$

Also gilt (18) für alle $k \in \mathbb{N}$. $\square$

SATZ 2.2.8. *Sei* $Q(R)$ *der Quotientenkörper von* R. *Dann sind äquivalent :*

(i) R *ist* ∞*-stufig Euklidisch*
(ii) $\forall a, b \in R, b \neq 0 : \exists k \in \mathbb{N}, \mathcal{D}^{(k)}$ *terminierende Divisionskette zu* (a, b)
(iii) $Q(R) = CF_\infty$

BEWEIS. (i) $\Leftrightarrow$ (ii) nach Definition 2.1.5 und Satz 2.1.7.
(ii) $\Rightarrow$ (iii) : Sei $\alpha = \frac{a}{b} \in Q(R)$, $a, b \in R, b \neq 0$. Nach (ii) existiert ein $k \in \mathbb{N}$ und eine terminierende Divisionskette $\mathcal{D}^{(k)}$ zu (a, b). Für die Quotienten $q_1, q_2, \ldots, q_k$ von $\mathcal{D}^{(k)}$ gilt dann nach Lemma 2.2.7 $\frac{a}{b} = [q_1, q_2, \ldots, q_k] \in CF_k$ wegen $r_k = 0$.

(iii) $\Rightarrow$ (ii) : Seien $a, b \in R, b \neq 0$. Nach (iii) gibt es ein $k \in \mathbb{N}$ und einen Kettenbruch $[q_1, q_2, \ldots, q_k] \in CF_k$ mit $\frac{a}{b} = [q_1, q_2, \ldots, q_k]$. Weiter ist dann nach Lemma 2.2.7 der terminale Rest r_k der Divisionskette $\mathcal{D}^{(k)}$ zu (a, b) mit Quotienten $q_1, q_2, \ldots, q_k$ gleich Null, d.h. $\mathcal{D}^{(k)}$ ist terminierend. $\square$

2.3. k-stufig Euklidische Zahlkörper

Ist R der Ganzheitsring eines Algebraischen Zahlkörpers K, so wählt man für φ häufig den Betrag der auf R eingeschränkten Normabbildung $N\colon R \to \mathbb{Z}$. Dies ist möglich, da die Bedingung

$$|N(\alpha)| = 0 \Leftrightarrow \alpha = 0$$

sogar für alle $\alpha \in K$ erfüllt ist. So kommt man zu folgender

Definition 2.3.1. Sei K ein Algebraischer Zahlkörper und R sein Ganzheitsring. Dann heißt K *k-stufig Euklidisch* genau dann, wenn R k-stufig Euklidisch im Sinne von Definition 2.1.5 ist. Speziell heißt K *Norm-Euklidisch* bzw. *k-stufig Norm-Euklidisch*, falls R Euklidisch bzw. k-stufig Euklidisch bzgl. der Normbetragsabbildung $|\cdot| \circ N$ ist.

Wir wollen nun zunächst die Norm-Euklidische und die k-stufig norm-euklidischen Eigenschaften etwas anschaulicher charakterisieren. Für die norm-euklidische Eigenschaft ist dies ohne weitere Hilfsmittel möglich.

Satz 2.3.2. *Sei K ein Algebraischer Zahlkörper. Dann sind äquivalent :*

(i) *K ist Norm-Euklidisch*
(ii) $\forall a, b \in R, b \neq 0 : \exists q \in R : |N(a - qb)| < |N(b)|$
(iii) $\forall \alpha \in K : \exists \lambda \in R : |N(\alpha - \lambda)| < 1$

Beweis. (i) $\Leftrightarrow$ (ii) ist klar nach Definition 2.3.1 und 2.1.1.

(ii) $\Rightarrow$ (iii) : Sei $\alpha \in K$. Da K Quotientenkörper von R ist, gibt es $a, b \in R, b \neq 0$ mit $\alpha = \frac{a}{b}$. Dann existiert nach (ii) ein $q \in R$ mit $|N(a - qb)| < |N(b)|$. Multiplikation mit $\frac{1}{|N(b)|}$ ergibt wegen der Multiplikativität der Norm : $|N(\alpha - q)| < 1$.

(iii) $\Rightarrow$ (ii) : Seien $a, b \in R, b \neq 0$. Es ist $\frac{a}{b} \in K$ und nach (iii) existiert ein $q \in R$ mit $|N(\frac{a}{b} - q)| < 1$. Multiplikation mit $|N(b)|$ liefert $|N(a - qb)| < |N(b)|$. □

Um zu einem ähnlichen Satz auch für die k-stufig norm-euklidischen Eigenschaften für $k > 1$ zu gelangen, greifen wir auf die in Abschnitt 2.2 eingeführten Kettenbrüche zurück.

Lemma 2.3.3. *Seien $a, b \in R$. Dann existiert eine k-stufige Divisionskette zu (a, b) mit $|N(r_k)| < |N(b)|$ genau dann, wenn ein Kettenbruch $\frac{a_k}{b_k} \in CF_k$ existiert mit*

$$\left| N\left(\frac{a}{b} - \frac{a_k}{b_k}\right)\right| < \frac{1}{|N(b_k)|} \tag{19}$$

BEWEIS. "$\Rightarrow$" : Sei $\mathcal{D}^{(k)}$ eine k-stufige Divisionskette zu (a,b) mit Quotienten $q_1, q_2, \ldots, q_k$ und $|N(r_k)| < |N(b)|$. Dann gilt für den Kettenbruch $\frac{a_k}{b_k} = [q_1, q_2, \ldots, q_k]$ nach Lemma 2.2.7 :

$$\left|N\left(\frac{a}{b} - \frac{a_k}{b_k}\right)\right| = \left|N\left(\frac{r_k}{bb_k}\right)\right| = \frac{|N(r_k)|}{|N(b)||N(b_k)|} < \frac{1}{|N(b_k)|}.$$

"$\Leftarrow$" : Sei $\frac{a_k}{b_k} = [q_1, q_2, \ldots, q_k] \in CF_k$, sodaß (19) erfüllt ist. Sei $\mathcal{D}^{(k)}$ die Divisionskette zu (a,b) mit Quotienten $q_1, q_2, \ldots, q_k$. Nach Lemma 2.2.7 ist dann $|N(\frac{r_k}{bb_k})| < \frac{1}{|N(b_k)|}$ und Multiplikation mit $|N(bb_k)|$ ergibt $|N(r_k)| < |N(b)|$. $\square$

Mit dieser Vorbetrachtung ergibt sich nun die folgende Verallgemeinerung von Satz 2.3.2.

SATZ 2.3.4. *Sei K ein Algebraischer Zahlkörper, $k \in \mathbb{N} \cup \{\infty\}$. Dann sind äquivalent :*

(i) *K ist k-stufig Norm-Euklidisch*
(ii) $\forall a, b \in R, b \neq 0 : \exists l \leq k, \mathcal{D}^{(l)}$ *Divisionskette zu* (a,b) :

$$|N(r_l)| < |N(b)|$$

(iii) $\forall \alpha \in K : \exists \frac{a}{b} \in CF_k : |N(\alpha - \frac{a}{b})| < \frac{1}{|N(b)|}$

Für $k = 1$ ergibt sich Satz 2.3.2, denn $CF_1 = R$.

BEWEIS. (i) $\Leftrightarrow$ (ii) ist klar nach Definition 2.3.1 und 2.1.5.

(ii) $\Rightarrow$ (iii) : Sei $\alpha \in K$. Da K Quotientenkörper von R ist, gibt es $a, b \in R, b \neq 0$ mit $\alpha = \frac{a}{b}$. Dann existiert nach (ii) ein $l \leq k$ und eine Divisionskette $\mathcal{D}^{(l)}$ mit $|N(r_l)| < |N(b)|$. Nach Lemma 2.3.3 existiert dann weiter ein Kettenbruch $\frac{a_l}{b_l} \in CF_l \subseteq CF_k$ mit $|N(\alpha - \frac{a_l}{b_l})| < \frac{1}{|N(b_l)|}$.

(iii) $\Rightarrow$ (ii) : Seien $a, b \in R, b \neq 0$. Nach (iii) gibt es ein $l \leq k$ und einen Kettenbruch $\frac{a_l}{b_l} \in CF_k$ der Länge l mit $|N(\frac{a}{b} - \frac{a_l}{b_l})| < \frac{1}{|N(b_l)|}$. Weiter existiert dann nach Lemma 2.3.3 eine l-stufige Divisionskette $\mathcal{D}^{(l)}$ mit $|N(r_l)| < |N(b)|$. $\square$

Die Bedingung (iii) aus Satz 2.3.4 gibt Anlaß zu der folgenden Definition.

DEFINITION 2.3.5. Sei $\frac{a}{b} \in CF_\infty$. Dann heißt

$$E\left(\frac{a}{b}\right) := \left\{ x \in \mathbb{R}^n \,\middle|\, \left|N\left(x - \frac{a}{b}\right)\right| < \frac{1}{|N(b)|} \right\}$$

die *Euklidische Menge von $\frac{a}{b}$*. Weiter heißt für $k \in \mathbb{N} \cup \{\infty\}$

$$E_k := \bigcup_{\frac{a}{b} \in CF_k} E\left(\frac{a}{b}\right)$$

die *k-stufig Euklidische Menge* und E_1 auch einfach *Euklidische Menge*.

Man beachte, daß die Mengen $E(\frac{a}{b})$ nur für Kettenbrüche $\frac{a}{b} \in CF_\infty$ definiert wurden. Das liegt daran, daß für beliebige $\alpha \in K$ die Darstellung $\alpha = \frac{a}{b}$ als Bruch mit $a, b \in R$ nicht eindeutig ist, und damit $|N(b)|$ nicht eindeutig bestimmt ist. Definition 2.3.5 wäre also für beliebige $\alpha \in K$ nicht eindeutig. Bei Kettenbrüchen $\frac{a}{b}$ ist aber b nach Bemerkung 2.2.5 bis auf Assoziierte eindeutig bestimmt. Da Einheiten den Normbetrag 1 haben ist $|N(b)|$ also in diesem Fall eindeutig und $E(\frac{a}{b})$ läßt sich wie in Definition 2.3.5 definieren.

BEMERKUNG 2.3.6. *Aus Definiton* 2.3.5 *ergibt sich nun, daß* (iii) *aus Satz* 2.3.4 *äquivalent ist zu $K \subseteq E_k$. Also gilt*

$$K \quad k\text{-stufig Norm-Euklidisch} \quad \Leftrightarrow \quad K \subseteq E_k.$$

Analog zu Bemerkung 2.2.6 gilt für die Mengen E_k die

BEMERKUNG 2.3.7. *Sei $k \in \mathbb{N} \cup \{\infty\}$. Dann ist E_k ein Fixgebiet bzgl. R.*

BEWEIS. Sei $x \in E_k$, $|N(x - \frac{a}{b})| < \frac{1}{|N(b)|}$ mit $\frac{a}{b} \in CF_k$. Zu zeigen ist nach Bemerkung 1.4.9, daß für alle $c \in R$, $u \in R^*$ auch $x + c, ux \in E_k$ ist.

Für $x + c$ erhält man

$$\left|N\left((x+c) - \left(\frac{a}{b} + c\right)\right)\right| = \left|N\left(x - \frac{a}{b}\right)\right| < \frac{1}{|N(b)|},$$

und nach Bemerkung 2.2.6 ist $\frac{a}{b} + c \in CF_k$, also $x + c \in E(\frac{a_k}{b_k})$.

Für ux ist wegen $|N(u)| = 1$

$$\left|N\left(ux - u\frac{a}{b}\right)\right| = |N(u)| \left|N\left(x - \frac{a}{b}\right)\right| < \frac{1}{|N(b)|},$$

und nach Bemerkung 2.2.6 ist $u\frac{a}{b} \in CF_k$, also $ux \in E(\frac{ua}{b})$. □

Hieraus erhält man

BEMERKUNG 2.3.8. *Sei $k \in \mathbb{N} \cup \{\infty\}$ und $\Psi \subseteq K$ ein K-Überdeckungsgebiet bzgl. R* [3]. *Gilt*

$$\Psi \subseteq E_k, \tag{20}$$

so ist K bereits k-stufig Norm-Euklidisch.

BEWEIS. Da E_k Fixgebiet bzgl. R ist, folgt aus (20) nach Satz 1.4.10 schon $K \subseteq E_k$, d.h. K ist nach Bemerkung 2.3.6 k-stufig Norm-Euklidisch. □

BEMERKUNG 2.3.9. *Die $E_k(\frac{a}{b})$ und damit die E_k sind offen in $\mathbb{R}^n$.*

[3] siehe Definition 1.4.5

Beweis. Dies ist eine direkte Folge aus der Stetigkeit von N. (siehe Korollar 1.2.7). □

Für $k = \infty$ gilt jetzt sogar

Satz 2.3.10. *Gilt $\mathbb{R}^n = E_\infty$, so ist K schon k-stufig Norm-Euklidisch für ein $k \in \mathbb{N}$.*

Beweis. Sei $(\omega_1, \dots, \omega_n)$ eine Ganzheitsbasis von $K/\mathbb{Q}$. Aus $\mathbb{R}^n = E_\infty$ folgt dann insbesondere

$$\bar{\Phi} \subseteq E_\infty = \bigcup_{\frac{a}{b} \in CF_\infty} E\left(\frac{a}{b}\right).$$

für den topologischen Abschluß der Grundmasche Φ von R in $\mathbb{R}^n$. Die $E(\frac{a}{b})$ sind offen, und da $\bar{\Phi}$ abgeschlossen und beschränkt, also kompakt ist, existiert nach dem Satz von Heine-Borel eine endliche Teilüberdeckung

$$\bar{\Phi} \subseteq \bigcup_{\frac{a}{b} \in T} E\left(\frac{a}{b}\right)$$

mit endlichem $T \subseteq CF_\infty$. Da T endlich ist, ist schon $T \subseteq CF_k$ für ein $k \in \mathbb{N}$, also

$$\Phi \cap K \subseteq \bar{\Phi} \subseteq E_k.$$

Da $\Phi \cap K$ als Grundmasche von $\mathfrak{c}$ in K nach Satz 1.4.6 auch K-Überdeckungsgebiet bzgl. $\mathfrak{c}$ ist, folgt mit Bemerkung 2.3.8, daß K k-stufig Norm-Euklidisch ist. □

Bevor wir diesen Satz anwenden, beweisen wir noch das folgende auf Dirichlet zurückgehende Approximationslemma, das z.B. in Hardy-Wright [8] nachzulesen ist.

Lemma 2.3.11. *Sei $\epsilon > 0$, $t_1, t_2, \dots, t_k \in \mathbb{R}$. Dann existieren $d \in \mathbb{N}, c_1, \dots, c_k \in \mathbb{Z}$, sodaß*

$$\left| t_i - \frac{c_i}{d} \right| < \frac{\epsilon}{d} \quad \textit{für } i = 1, 2, \dots, k.$$

Beweis. Wähle $m \in \mathbb{N}$ mit $\frac{1}{m} < \epsilon$. Für $t \in \mathbb{R}$ bezeichne $[t] \in \mathbb{Z}$ die größte in t enthaltene ganze Zahl und (t) die Differenz $t - [t]$. Es gilt also $t = [t] + (t)$ mit $[t] \in \mathbb{Z}$ und $0 \leq (t) < 1$.

Wir betrachten nun die $m^k + 1$ Punkte in $\mathbb{R}^k$

$$((lt_1), (lt_2), \dots, (lt_k)) \quad , l = 0, 1, \dots, m^k. \tag{21}$$

Die Punkte (21) liegen im "Einheitswürfel"

$$\{(x_1, x_2, \dots, x_k) \mid 0 \leq x_i < 1 \quad \text{für } i = 1, 2, \dots, k \quad \}.$$

Teil man diesen Würfel durch Schnitte parallel zu den Seitenflächen im Abstand $\frac{1}{m}$ in m^k Teilwürfel auf, so folgt nach dem Schubfachprinzip, daß zwei der Punkte

(21) in demselben Teilwürfel liegen. Seien dies die zu $l_1, l_2 \leq m^k$ gehörigen Punkte, also

$$|(l_2 t_i) - (l_1 t_i)| < \frac{1}{m} < \epsilon \quad \text{für } i = 1, 2, \ldots, k.$$

Sei o.B.d.A. $l_1 < l_2$. Setze nun $d := l_2 - l_1 \in \mathbb{N}$ und $c_i := [l_2 t_i] - [l_1 t_i] \in \mathbb{Z}$ für $i = 1, 2, \ldots, k$. Dann gilt

$$dt_i - c_i = l_2 t_i - l_1 t_i - ([l_2 t_i] - [l_1 t_i]) = (l_2 t_i) - (l_1 t_i) \quad \text{für } i = 1, 2, \ldots, k.$$

Durch Multiplikation mit $\frac{1}{d}$ ergibt sich

$$\left| t_i - \frac{c_i}{d} \right| = \frac{|(l_2 t_i) - (l_1 t_i)|}{d} < \frac{\epsilon}{d} \quad \text{für } i = 1, 2, \ldots, k.$$

□

LEMMA 2.3.12. *Sei $x \in \mathbb{R}^n$. Dann existieren $c \in R$ und $d \in \mathbb{N}$, sodaß*

$$\left| N\left(x - \frac{c}{d}\right) \right| < \frac{1}{|N(d)|}.$$

BEWEIS. Sei $(\omega_1, \ldots, \omega_n)$ eine Ganzheitsbasis von $K/\mathbb{Q}$ und

$$x = \sum_{i=1}^{n} t_i \omega_i, t_i \in \mathbb{R}\ .$$

Nach Bemerkung 1.2.6 ist $N(\sum t_i \omega_i)$ ein Polynomausdruck in $t_1, t_2, \ldots, t_n$ über $\mathbb{R}$. Sei $\rho \in \mathbb{R}$ die Summe der Absolutbeträge der auftretenden Koeffizienten. Wähle nun $\epsilon > 0$, sodaß $\rho \epsilon^n < 1$. Nach Lemma 2.3.11 existieren dann $d \in \mathbb{N}, c_1, \ldots, c_n \in \mathbb{Z}$ mit

$$\left| t_i - \frac{c_i}{d} \right| < \frac{\epsilon}{d} \quad \text{für } i = 1, 2, \ldots, n.$$

Setze $\alpha := \frac{\sum c_i \omega_i}{d} \in K$. Dann ist nach Bemerkung 1.2.6

$$\begin{aligned} N(x - \alpha) &= N\left(\sum \left(t_i - \frac{c_i}{d}\right) \omega_i\right) \\ &= \sum_{\substack{(e_i) \in \mathbb{N}^n, \\ \sum e_i = n}} c_{(e_i)} \left(\prod_{i=1}^{n} \left(t_i - \frac{c_i}{d}\right)^{e_i}\right), \end{aligned}$$

also

$$\begin{aligned} |N(x-\alpha)| &= \sum_{\substack{(e_i)\in\mathbb{N}^n,\\ \sum e_i=n}} |c_{(e_i)}| \left(\prod_{i=1}^n \left|t_i - \frac{c_i}{d}\right|^{e_i}\right) \\ &< \sum_{\substack{(e_i)\in\mathbb{N}^n,\\ \sum e_i=n}} |c_{(e_i)}| \left(\frac{\epsilon}{d}\right)^n < \rho\frac{\epsilon^n}{d^n} < \frac{1}{d^n} = \frac{1}{|N(d)|}. \end{aligned}$$

□

Mit Hilfe dieser Lemmata können wir nun den folgenden Satz aus Cooke [6] beweisen.

SATZ 2.3.13 (COOKE). *Sei R ∞-stufig Euklidisch. Dann ist R schon k-stufig Norm-Euklidisch für ein $k \in \mathbb{N}$.*

BEWEIS. Wir zeigen $\mathbb{R}^n = E_\infty$, dann folgt die Behauptung nach Satz 2.3.10.
Sei also $(\omega_1, \dots, \omega_n)$ eine Ganzheitsbasis von $K/\mathbb{Q}$ und

$$x = \sum_{i=1}^n t_i\omega_i \in \mathbb{R}^n, \quad t_i \in \mathbb{R}, 0 \le t_i < 1.$$

Gesucht ist dann ein $\frac{a_k}{b_k} \in CF_k$ mit $|N(x - \frac{a_k}{b_k})| < \frac{1}{|N(b_k)|}$.

Nach Satz 2.2.8 ist $K = CF_\infty$, es gibt also nach Lemma 2.3.12 einen Kettenbruch $\frac{a_k}{b_k} = \frac{c}{d}$ mit

$$\left|N\left(x - \frac{a_k}{b_k}\right)\right| < \frac{1}{|N(d)|}.$$

Nach Lemma 2.2.4 gilt dann $b_k|d$, d.h. $|N(b_k)| \le |N(d)|$. Also

$$\left|N\left(x - \frac{a_k}{b_k}\right)\right| < \frac{1}{|N(b_k)|},$$

und damit $x \in E(\frac{a_k}{b_k})$. □

Die k-stufig euklidischen Eigenschaften, $k \in \mathbb{N} \cup \{\infty\}$, sind nach Bemerkung 2.1.6 schwächere Bedingungen als die klassische euklidische Eigenschaft. Wir wollen nun zeigen, daß jedoch im Falle von Zahlringen, d.h. Ganzheitsringen Algebraischer Zahlkörper, aus jeder k-stufig euklidischen Eigenschaft, $k \in \mathbb{N} \cup \{\infty\}$, immer noch die Hauptidealeigenschaft folgt. Man beachte, daß sich dieses Resultat nicht auf die norm-euklidischen Eigenschaften beschränkt, sondern für beliebige Euklidische Abbildungen gilt. Dies ist aber sofort klar, da die ∞-stufig euklidische Eigenschaft allgemeiner als jede k-stufig Euklidische mit $k \in \mathbb{N}$, und nach Satz 2.1.7 unabhängig von der gewählten Euklidischen Abbildung φ ist.

SATZ 2.3.14. *Jeder k-stufig Euklidische Algebraische Zahlkörper K, $k \in \mathbb{N} \cup \{\infty\}$, hat die Klassenzahl $h = 1$, d.h. der Ganzheitsring R ist Hauptidealring.*

1. BEWEIS. Wir beweisen durch Widerspruchsbeweis, daß sich in R jede Nicht-Einheit aus $R \backslash \{0\}$ als Produkt unzerlegbarer Elemente schreiben läßt. Die Behauptung folgt dann nach Satz 2.1.13 und der bekannten Tatsache, daß jeder Dedekindring, der ZPE-Ring ist, auch Hauptidealring ist.

Sei $a \in R \backslash \{0\}$ eine Nicht-Einheit mit $|N(a)|$ minimal, die sich nicht als Produkt unzerlegbarer Elemente schreiben läßt. Es ist a selbst zerlegbar, also $a = bc$ für Nicht-Einheiten $b, c \in R \backslash \{0\}$. Wegen α Einheit $\Leftrightarrow |N(\alpha)| = 1$ ist $|N(b)|, |N(c)| > 1$ und daher $|N(a)| = |N(b)||N(c)| > |N(b)|, |N(c)|$. Wegen der Minimalität von $|N(a)|$ lassen sich dann b, c als Produkt unzerlegbarer Elemente schreiben, also auch $a = bc$. Widerspruch. □

2. BEWEIS. Als Dedekindring ist R insbesondere noethersch und daher nach Korollar 2.1.11 Hauptidealring. □

Für Zahlringe liefert Definition 2.1.5 also Bedingungen, die in ihrer Schärfe zwischen euklidischer Bedingung und Hauptidealringeigenschaft liegen. Das folgende Beispiel 2.3.15 zeigt, daß die Hauptidealringeigenschaft echt schwächer ist als die k-stufig euklidische Eigenschaft für alle $k \in \mathbb{N} \cup \{\infty\}$, d.h. daß die Umkehrung von Satz 2.3.14 nicht allgemein gilt.

BEISPIEL 2.3.15. Der Ganzheitsring $\mathbb{Z}[\frac{1+\sqrt{19}}{2}]$ von $\mathbb{Q}(\sqrt{-19})$ ist zwar Hauptidealring, da $\mathbb{Q}(\sqrt{-19})$ – wie wir in Beispiel 3.4.1 sehen werden – die Klassenzahl 1 hat, aber nach Cohn [5] nicht k-stufig Euklidisch für alle $k \in \mathbb{N} \cup \{\infty\}$. Der Beweis dieser Aussage soll hier nicht ausgeführt werden.

Ist K jedoch nicht imaginär-quadratisch, d.h. besitzt R unendlich viele Einheiten, so gilt nach Cooke [4] sogar die Umkehrung von Satz 2.3.14.

SATZ 2.3.16 (COOKE). *Sei K ein Algebraischer Zahlkörper mit Klassenzahl 1, der nicht imaginär-quadratisch ist. Dann ist K ∞-stufig Euklidisch.*

BEWEIS. siehe Cooke [6] Introduction, Theorem 1, und §4, Proposition 14. □

Zusammen mit Satz 2.3.13 und Satz 2.3.14 ergibt sich hieraus

SATZ 2.3.17. *Sei K ein Algebraischer Zahlkörper, der nicht imaginär-quadratisch ist. Dann hat K genau dann die Klassenzahl 1, wenn K k-stufig Norm-Euklidisch für ein $k \in \mathbb{N}$ ist.*

[4] vgl. [6] Introduction, Theorem 1

2.4. Beispiele k-stufig Euklidischer Zahlkörper

Wir wollen in diesem Abschnitt zeigen, daß der reell-quadratische Zahlkörper $\mathbb{Q}(\sqrt{14})$ 2-stufig Norm-Euklidisch, jedoch nicht Norm-Euklidisch ist. Dies zeigt auch, daß die Einführung k-stufig Euklidischer Ringe eine echte Verallgemeinerung darstellt.

Beispiel 2.4.1. $K = \mathbb{Q}(\sqrt{14})$ ist nicht Norm-Euklidisch.

Beweis. Zunächst ist $(1, \sqrt{14})$ eine Ganzheitsbasis von $R = \mathbb{Z}[\sqrt{14}]$.
Wir zeigen $\frac{1+\sqrt{14}}{2} \notin E_1$, die Behauptung folgt dann nach Bemerkung 2.3.6.
Annahme : $\frac{1+\sqrt{14}}{2} \in E_1$. Dann existiert $c = a + b\sqrt{14} \in R = CF_1$, $a, b \in \mathbb{Z}$, mit

$$\left| N\left(\frac{1+\sqrt{14}}{2} - c\right)\right| < 1.$$

Es folgt durch Multiplikation mit $|N(2)| = 4$

$$|N(1+\sqrt{14}-2c)| = |(1-2a)^2 - 14(1-2b)^2| < 4.$$

Wegen $(1-2a)^2, (1-2b)^2 \equiv 1 \pmod 4$ ist $(1-2a)^2 - 14(1-2b)^2 \equiv 3 \pmod 4$, d.h. $(1-2a)^2 - 14(1-2b)^2 \in \{-1, 3\}$. Wegen $(1-2a)^2 - 14(1-2b)^2 \equiv (1-2a)^2 \equiv 0, 1, 2, 4 \pmod 7$ ist aber $(1-2a)^2 - 14(1-2b)^2 \in \{-3, 0, 1, 2\}$. Dies ist ein Widerspruch, also $\frac{1+\sqrt{14}}{2} \notin E_1$. □

Zur Vollständigkeit sei ohne Beweis bemerkt :

Beispiel 2.4.2. Die Norm-Euklidischen quadratischen Zahlkörper sind genau die $\mathbb{Q}(\sqrt{d})$ mit $d = -1, -2, -3, -7, -11$ und $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.
Ein Beweis für den imaginär-quadratischen Fall ist besonders einfach und steht bei Hardy-Wright [5]. Der reell-quadratische Fall ist dagegen erheblich schwieriger, siehe dazu Chatland, Davenport [3].

Beispiel 2.4.3. $K = \mathbb{Q}(\sqrt{14})$ ist 2-stufig Norm-Euklidisch.

Beweis. [6] Zunächst ist $(1, \sqrt{14})$ eine Ganzheitsbasis von $R = \mathbb{Z}[\sqrt{14}]$.
Wir wählen also nach Beispiel 1.4.13

$$\Psi := \left\{ \lambda_1 + \lambda_2\sqrt{14} \;\middle|\; \lambda_1, \lambda_2 \in \mathbb{Q}, 0 \le \lambda_1 \le \frac{1}{2}, 0 \le \lambda_2 < 1 \right\}$$

als K-Überdeckungsgebiet bzgl. $\mathfrak{c}$. Nach Bemerkung 2.3.8 ist zu zeigen : $\Psi \subseteq E_2$.

[5] siehe Hardy-Wright, [8], §14.7
[6] vgl. auch den Beweis von Cooke [6], §4, Proposition 9, Seite 145

Die Einbettungen der reell-quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$, $d > 1$, sind die beiden reellen Einbettungen

$$\sigma_1 = id \quad \text{und} \quad \sigma_2 : \lambda_1 + \lambda_2\sqrt{d} \mapsto \lambda_1 - \lambda_2\sqrt{d}.$$

Für ein beliebiges Element $\lambda_1 + \lambda_2\sqrt{14} \in K$ ist also die geometrische Darstellung [7]

$$(v \circ x)(\lambda_1 + \lambda_2\sqrt{14}) = \begin{pmatrix} \lambda_1 + \lambda_2\sqrt{14} \\ \lambda_1 - \lambda_2\sqrt{14} \end{pmatrix},$$

d.h. $\lambda_1 + \lambda_2\sqrt{14} \in K$ wird mit $\begin{pmatrix} \lambda_1 + \lambda_2\sqrt{14} \\ \lambda_1 - \lambda_2\sqrt{14} \end{pmatrix} \in \mathbb{R}^2$ identifiziert. Also ist

$$\Psi = \left\{ \lambda_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} \sqrt{14} \\ -\sqrt{14} \end{pmatrix} \middle| \ \lambda_1, \lambda_2 \in \mathbb{Q}, 0 \leq \lambda_1 \leq \frac{1}{2}, 0 \leq \lambda_2 < 1 \right\}.$$

Es ist nach Definition 2.2.1 $[-2, 4 - \sqrt{14}] = \frac{a_2}{b_2}$ mit $a_2 = (4 - \sqrt{14})(-2) + 1$, $b_2 = (4 - \sqrt{14})$, d.h.

$$\frac{a_2}{b_2} = \frac{(4 - \sqrt{14})(-2) + 1}{(4 - \sqrt{14})} = \frac{2(-2) + 4 + \sqrt{14}}{2} = \frac{\sqrt{14}}{2} \in CF_2.$$

Trivialerweise sind auch $1, 1 + \sqrt{14} \in CF_2$.

Wir zeigen nun, daß bereits gilt

$$\Psi \subseteq E(1) \cup E\left(\frac{\sqrt{14}}{2}\right) \cup E(1 + \sqrt{14}) \subseteq E_2. \tag{22}$$

Wegen $N(x) = x_1 x_2$ für $x = \binom{x_1}{x_2} \in \mathbb{R}^2$ nach (5) aus Abschnitt 1.2 und $N(b_2) = (4 - \sqrt{14})(4 + \sqrt{14}) = 2$ ist

$$\begin{aligned} E\left(\frac{\sqrt{14}}{2}\right) &= \left\{ x \in \mathbb{R}^2 \ \middle| \ \left| \left(x_1 - \frac{\sqrt{14}}{2}\right)\left(x_2 + \frac{\sqrt{14}}{2}\right) \right| < \frac{1}{2} \right\}, \\ E(1 + \sqrt{14}) &= \left\{ x \in \mathbb{R}^2 \ \middle| \ |(x_1 - (1 + \sqrt{14}))(x_2 - (1 - \sqrt{14}))| < 1 \right\}, \\ E(1) &= \left\{ x \in \mathbb{R}^2 \mid |(x_1 - 1)(x_2 - 1)| < 1 \right\}. \end{aligned}$$

Die Gültigkeit von (22) entnimmt man nun leicht der Abbildung II.1. Die Euklidischen Mengen $E(1)$ und $E(1+\sqrt{14})$ sind das Innere der mit durchgezogener Linie gezeichneten Hyperbelästepaare, $E(\frac{\sqrt{14}}{2})$ ist das Innere des mit gestrichelter Linie gezeichneten Hyperbelästepaares und Ψ ist grau unterlegt eingezeichnet. $\square$

Zur Vollständigkeit sei wieder ohne Beweis bemerkt :

[7] siehe Definition 1.2.1

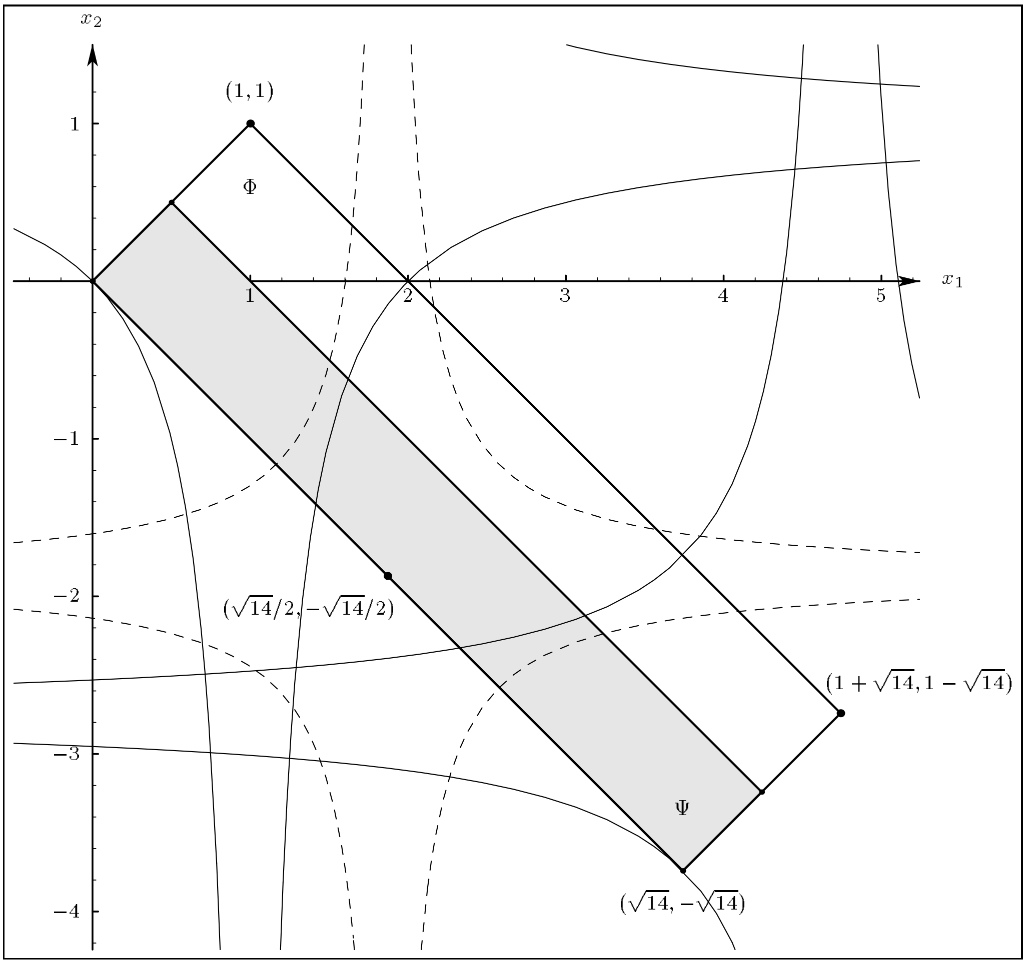

ABBILDUNG II.1. Der Zahlkörper $\mathbb{Q}(\sqrt{14})$

Beispiel 2.4.4. Die bekannten 2-stufig Norm-Euklidischen reell-quadratischen Zahlkörper sind nach [10] die $\mathbb{Q}(\sqrt{d})$ mit

$$d = 14, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 89, 93, 97, 101,$$
$$109, 113, 129, 133, 137, 149, 157, 161, 173, 177, 181, 193, 197, 201, 213, 253.$$

Es kann aber durchaus noch weitere solche Zahlkörper geben.

KAPITEL III

Euklidische Ideale und Euklidische Systeme

3.1. Euklidische Ideale

In diesem Abschnitt sollen Euklidische Ideale bzw. Euklidische Idealklassen eingeführt und untersucht werden. Wir halten uns dabei an die Definition von Lenstra aus [11].

DEFINITION 3.1.1. Sei $\mathfrak{c} \in I_K$ und $x \in \mathbb{R}^n \setminus \mathfrak{c}$. Dann heißt x *Euklidischer Punkt* von $\mathfrak{c}$, wenn ein $\gamma \in \mathfrak{c}$ existiert mit

$$|N(x-\gamma)| < \mathcal{N}(\mathfrak{c}).$$

Die Menge

$$E_{\mathfrak{c}} := \{x \in \mathbb{R}^n \mid x \notin \mathfrak{c}, \exists \gamma \in \mathfrak{c} : |N(x-\gamma)| < \mathcal{N}(\mathfrak{c})\}$$

aller Euklidischen Punkte von $\mathfrak{c}$ heißt *Euklidische Menge von* $\mathfrak{c}$. Für $\gamma \in \mathfrak{c}$ heißt

$$E_{\mathfrak{c}}(\gamma) := \{x \in \mathbb{R}^n \mid x \notin \mathfrak{c}, |N(x-\gamma)| < \mathcal{N}(\mathfrak{c})\}$$

Euklidische Menge von $\mathfrak{c}$ *um* γ.

DEFINITION 3.1.2. Sei $\mathfrak{c} \in I_K$. Gilt

$$E_{\mathfrak{c}} \cup \mathfrak{c} \supseteq K,$$

so heißt $\mathfrak{c}$ *Euklidisches Ideal.*

BEMERKUNG 3.1.3. *Sei* $\mathfrak{c} \in I_K$. *Es gilt*

$$E_{\mathfrak{c}} = \{x \in \mathbb{R}^n \mid \exists \gamma \in \mathfrak{c} : 0 < |N(x-\gamma)| < \mathcal{N}(\mathfrak{c})\}.$$

BEWEIS. "$\subseteq$" ist klar, denn aus $x \notin \mathfrak{c}$ folgt $N(x-\gamma)| \neq 0$ für alle $\gamma \in \mathfrak{c}$.
"$\supseteq$" : Zu zeigen ist : Aus $0 < |N(x-\gamma)| < \mathcal{N}(\mathfrak{c})$ folgt $x \notin \mathfrak{c}$. Dies ist aber klar, denn aus $x \in \mathfrak{c}$ folgt $x-\gamma \in \mathfrak{c}$, also existiert nach Bemerkung 1.1.4 ein $d \in \mathbb{N}$ mit $d\mathcal{N}(\mathfrak{c}) = N(x-\gamma)$, also ist $N(x-\gamma) = 0$ oder $|N(x-\gamma)| \geq \mathcal{N}(\mathfrak{c})$. $\square$

BEMERKUNG 3.1.4. *Sei* $\mathfrak{c} \in I_K$. *Dann sind die Mengen* $E_\mathfrak{c}$ *und* $E_\mathfrak{c} \cup \mathfrak{c}$ *offen.*

BEWEIS. Dies ist eine direkte Folge der Steigkeit der Norm (siehe Korollar 1.2.7). □

LEMMA 3.1.5. *Sei* $\mathfrak{c} \in I_K$ *und* $x \in \mathbb{R}^n \setminus \{0\}$ *beliebig. Aus* $|N(x)| < \mathcal{N}(\mathfrak{c})$ *folgt dann* $x \in E_\mathfrak{c}$.

BEWEIS. Es ist $0 < |N(x-0)| < \mathcal{N}(\mathfrak{c})$ und $0 \in \mathfrak{c}$. □

Für die Euklidische Menge $E_\mathfrak{c}$ stellt man nun fest :

BEMERKUNG 3.1.6. *Sei* $\mathfrak{c} \in I_K$. *Dann sind* $E_\mathfrak{c}$ *und* $E_\mathfrak{c} \cup \mathfrak{c}$ *Fixgebiete* [1] *bzgl.* $\mathfrak{c}$.

BEWEIS. Sei $x \in E_\mathfrak{c}$ und $\gamma \in \mathfrak{c}$, sodaß $0 < |N(x-\gamma)| < \mathcal{N}(\mathfrak{c})$. Nach Bemerkung 1.4.9 ist $x + \delta, ux \in E_\mathfrak{c}$ für alle $\delta \in R$, $u \in R^*$ zu zeigen, dann folgt, daß $E_\mathfrak{c}$ Fixgebiet bzgl. $\mathfrak{c}$ ist. Dies prüft man leicht nach :

(i) $0 < |N((x+\delta) - (\gamma+\delta)| = |N(x-\gamma)| < \mathcal{N}(\mathfrak{c})$ und $\gamma + \delta \in \mathfrak{c}$.
(ii) $0 < |N(ux - u\gamma)| = |N(u)||N(x-\gamma)| < 1 \cdot \mathcal{N}(\mathfrak{c})$ und $u\gamma \in \mathfrak{c}$.

Nun ist aber $\mathfrak{c}$ nach Definition eines Ideals trivialerweise Fixgebiet bzgl. $\mathfrak{c}$, also auch $E_\mathfrak{c} \cup \mathfrak{c}$ nach Bemerkung 1.4.11 (ii). □

BEMERKUNG 3.1.7. *Sei* $\mathfrak{c} \in I_K$ *und* $\Psi_\mathfrak{c} \subseteq K$ *ein* K*-Überdeckungsgebiet* [2] *bzgl.* $\mathfrak{c}$. *Gilt*

$$\Psi_\mathfrak{c} \subseteq E_\mathfrak{c} \cup \mathfrak{c}, \tag{23}$$

so ist $\mathfrak{c}$ *schon Euklidisches Ideal.*

BEWEIS. Da $E_\mathfrak{c} \cup \mathfrak{c}$ Fixgebiet bzgl. $\mathfrak{c}$ ist, folgt aus (23) nach Satz 1.4.10 schon $K \subseteq E_\mathfrak{c} \cup \mathfrak{c}$, d.h. $\mathfrak{c}$ ist Euklidisches Ideal. □

BEMERKUNG 3.1.8. *Sei* $\mathfrak{c} \in I_K$. *Dann gilt für alle* $\lambda \in K \setminus \{0\}$

$$\lambda E_\mathfrak{c} = E_{(\lambda)\mathfrak{c}}.$$

BEWEIS. Sei $x \in E_\mathfrak{c}$ und $\gamma \in \mathfrak{c}$, sodaß $0 < |N(x-\gamma)| < \mathcal{N}(\mathfrak{c})$. Dann ist

$$0 < |N(\lambda x - \lambda\gamma)| = |N(\lambda)||N(x - \lambda\gamma)| < \mathcal{N}((\lambda)\mathfrak{c})$$

und $\lambda\gamma \in (\lambda)\mathfrak{c}$, also $\lambda x \in E_{(\lambda)\mathfrak{c}}$. □

KOROLLAR 3.1.9. *Ist* $\mathfrak{c} \in I_K$ *Euklidisches Ideal, so sind auch alle Ideale aus* $[\mathfrak{c}]$ *Euklidisch.*

[1] siehe Definition 1.4.8
[2] siehe Definition 1.4.5

Beweis. Aus $E_\mathfrak{c} \cup \mathfrak{c} \supseteq K$ folgt nach Bemerkung 3.1.8

$$E_{(\alpha)\mathfrak{c}} \cup (\alpha)\mathfrak{c} = \alpha E_\mathfrak{c} \cup \alpha\mathfrak{c} = \alpha(E_\mathfrak{c} \cup \mathfrak{c}) \supseteq \alpha K = K$$

für alle $\alpha \in K$. $\square$

Für ein Ideal hängt also die Eigenschaft Euklidisch zu sein nur von seiner Idealklasse ab. Daher spricht man auch von *Euklidischen Idealklassen.*

wi wollen nun charakterisieren, wann die triviale Idealklasse $[R] = H_K$ Euklidisch ist.

Bemerkung 3.1.10. *Aus Definition* 2.3.5 *und Definition* 3.1.1 *ergibt sich wegen* $CF_1 = R$ *sofort*

$$E_1 = E_R \cup R.$$

Satz 3.1.11. *Es ist K genau dann Norm-Euklidisch, wenn $E_R \cup R \supseteq K$, d.h. wenn $[R]$ Euklidische Idealklasse ist.*

Beweis. klar nach Bemerkung 2.3.6 und Bemerkung 3.1.10. $\square$

Van der Linden zeigt in [12], daß in einigen Fällen nichttriviale Euklidische Idealklassen exisitieren, diese Fälle jedoch offenbar äußerst selten sind. Die einzigen quadratischen Zahlkörper, die eine nicht-triviale Euklidische Idealklasse besitzen, sind die $\mathbb{Q}(\sqrt{d})$ mit $d = -15, -5, 10, 15, 85$. In allen diesen Fällen ist die Klassenzahl $h = 2$. Das Beispiel $\mathbb{Q}(\sqrt{-15})$ aus [12] soll hier ausgeführt werden.

Beispiel 3.1.12. Sei $K = \mathbb{Q}(\sqrt{-15})$. Dann ist $(1, \omega)$ mit $\omega = \frac{1+\sqrt{-15}}{2}$ Ganzheitsbasis von R. Wir betrachten das ganze Ideal $\mathfrak{a} := (2, \omega)$, das von 2 und ω in R erzeugt wird.

Zunächst wird gezeigt, daß $(2, \omega)$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ ist. Sei dazu $\alpha = \lambda_1 2 + \lambda_2\omega$ ein beliebiges Element aus $\mathfrak{a}$ mit $\lambda_1, \lambda_2 \in R$. Da $(1, \omega)$ Ganzheitsbasis von R ist, gibt es $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, sodaß $\lambda_1 = a_1 + b_1\omega, \lambda_2 = a_2 + b_2\omega$. Es ist $\omega^2 = \frac{1+2\sqrt{-15}-15}{4} = \frac{-7+\sqrt{-15}}{2} = \omega - 4$, also

$$\begin{aligned} \alpha &= (a_1 + b_1\omega)2 + (a_2 + b_2\omega)\omega = 2a_1 + 2b_1\omega + a_2\omega + b_2(\omega - 4) \\ &= 2(a_1 - 2b_2) + \omega(2b_1 + a_2 + b_2) \in 2\,\mathbb{Z} + \omega\,\mathbb{Z}\,. \end{aligned}$$

Wegen

$$\begin{pmatrix} 2 \\ \omega \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \omega \end{pmatrix}$$

ist

$$\mathcal{N}(\mathfrak{a}) = \left| \det \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right| = 2.$$

Wir wählen nun nach Beispiel 1.4.13

$$\Psi_{\mathfrak{a}} := \left\{ \lambda_1 2 + \lambda_2 \omega \;\middle|\; \lambda_1, \lambda_2 \in \mathbb{Q}, 0 \leq \lambda_1 < 1, 0 \leq \lambda_2 \leq \frac{1}{2} \right\},$$

als K-Überdeckungsgebiet bzgl. $\mathfrak{a}$ und zeigen

$$\Psi_{\mathfrak{a}} \subseteq E_{\mathfrak{a}}(0) \cup E_{\mathfrak{a}}(2) \cup \mathfrak{a} \subseteq E_{\mathfrak{a}} \cup \mathfrak{a}, \tag{24}$$

dann ist $[\mathfrak{a}]$ nach Bemerkung 3.1.7 Euklidische Idealklasse. Gegenüber van der Linden, der in [12]

$$\Phi_{\mathfrak{a}} \subseteq E_{\mathfrak{a}}(0) \cup E_{\mathfrak{a}}(2) \cup E_{\mathfrak{a}}(\omega) \cup E_{\mathfrak{a}}(2+\omega) \cup \mathfrak{a} \tag{25}$$

zeigt, vereinfacht sich der Beweis hier durch Anwendung von Beispiel 1.4.13.

Die Einbettungen der imaginär-quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$, $d \leq 1$, sind die beiden konjugiert-komplexen Einbettungen $\sigma_1 = id$ und $\bar{\sigma}_1$. Für ein beliebiges Element $\alpha = \lambda_1 + \lambda_2\sqrt{-15} \in K$, $\lambda_1, \lambda_2 \in \mathbb{Q}$, ist also die geometrische Darstellung [3]

$$(v \circ x)(\alpha) = \begin{pmatrix} \operatorname{Re} \alpha \\ \operatorname{Im} \alpha \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2\sqrt{15} \end{pmatrix},$$

d.h. $\lambda_1 + \lambda_2\sqrt{-15} \in K$ wird mit $\left(\begin{smallmatrix} \lambda_1 \\ \lambda_2\sqrt{15} \end{smallmatrix}\right) \in \mathbb{R}^2$ identifiziert. Also ist

$$\Psi_{\mathfrak{a}} = \left\{ \begin{pmatrix} 2\lambda_1 + \frac{1}{2}\lambda_2 \\ \frac{1}{2}\sqrt{15}\lambda_2 \end{pmatrix} \;\middle|\; \lambda_1, \lambda_2 \in \mathbb{Q}, 0 \leq \lambda_1 < 1, 0 \leq \lambda_2 \leq \frac{1}{2} \right\}.$$

Wegen $N(x) = x_1^2 + x_2^2$ für $x = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \in \mathbb{R}^2$ nach (5) aus Abschnitt 1.2 ist

$$\begin{aligned}
E(0) &= \left\{ x \in \mathbb{R}^2 \;\middle|\; 0 < x_1^2 + x_2^2 < 2 \right\} \\
E(2) &= \left\{ x \in \mathbb{R}^2 \;\middle|\; 0 < (x_1 - 2)^2 + x_2^2 < 2 \right\} \\
E(\omega) &= \left\{ x \in \mathbb{R}^2 \;\middle|\; 0 < (x_1 - \frac{1}{2})^2 + (x_2 - \frac{\sqrt{15}}{2})^2 < 2 \right\} \\
E(\omega) &= \left\{ x \in \mathbb{R}^2 \;\middle|\; 0 < (x_1 - \frac{5}{2})^2 + (x_2 - \frac{\sqrt{15}}{2})^2 < 2 \right\}
\end{aligned}$$

Die Gültigkeit von (24) und (25) entnimmt man anschaulich leicht Abbildung III.2. Die Euklidischen Mengen sind darin das Innere der gezeichneten Kreise ohne die jeweiligen Mittelpunkte und $\Psi_{\mathfrak{a}}$ ist grau unterlegt eingezeichnet. Wir zeigen (24) jetzt auch auf algebraischem Wege.

---

[3] siehe Definition 1.2.1

Sei also $\alpha \in \Psi_{\mathfrak{a}} \backslash \mathfrak{a}$, $\alpha = \lambda_1 2 + \lambda_2 \frac{1+\sqrt{-15}}{2}$ mit $\lambda_1, \lambda_2 \in \mathbb{Q}$, $0 \leq \lambda_1 < 1, 0 \leq \lambda_2 \leq \frac{1}{2}$. Setze $c := 2$, falls $2\lambda_1 + \frac{1}{2}\lambda_2 > 1$, sonst $c := 0$. Dann ist $|2\lambda_1 - c + \frac{1}{2}\lambda_2| \leq 1$, also

$$\begin{aligned} |N(\alpha - c)| &= |N(2\lambda_1 - c + \frac{1}{2}\lambda_2 + \frac{\sqrt{-15}}{2}\lambda_2)| \\ &= |(2\lambda_1 - c + \frac{1}{2}\lambda_2)^2 - (\frac{\lambda_2\sqrt{-15}}{2})^2| \\ &= |(2\lambda_1 - c + \frac{1}{2}\lambda_2)^2 + \frac{15{\lambda_2}^2}{4}| \\ &\leq 1 + \frac{15}{16} < 2 = \mathcal{N}(\mathfrak{a}), \end{aligned}$$

also $\alpha \in E_{\mathfrak{a}}(0)$.

Wir zeigen jetzt noch, daß $[\mathfrak{a}]$ nicht die triviale Idealklasse, d.h. daß $\mathfrak{a}$ kein Hauptideal ist. Wegen $\mathcal{N}(\mathfrak{a}) = 2$ und $\mathcal{N}((\alpha)) = |N(\alpha)|$ für $\alpha \in K$ reicht es zu zeigen, daß kein Element $\gamma \in R$ existiert mit $|N(\gamma)| = 2$.

Annahme : Es gibt $a, b \in \mathbb{Z}$ mit

$$2 = N(a + b\omega) = \left(a + \frac{b}{2}\right)^2 + 15\left(\frac{b}{2}\right)^2 = a^2 + ab + 16\frac{b^2}{4} = a^2 + ab + 4b^2.$$

Betrachtet man b als konstant, so folgt

$$a = -\frac{b}{2} \pm \sqrt{\frac{b^2}{4} - 4b^2 + 2} = -\frac{b}{2} \pm \frac{\sqrt{-15b^2 + 8}}{2} \tag{26}$$

Wegen $a, b \in \mathbb{Z}$ muß dann $-15b^2 + 8 \geq 0$ gelten, d.h. $b^2 \leq \frac{8}{15} < 1$, also $b = 0$. Damit folgt $a^2 = 2$ im Widerspruch zu $a \in \mathbb{Z}$. Also ist $\mathfrak{a}$ nicht Hauptideal und $[\mathfrak{a}]$ eine nicht-triviale Euklidische Idealklasse.

Die eigentliche Bedeutung Euklidischer Idealklassen liegt nach Lenstra [11] darin, daß jede Euklidische Idealklasse die Idealklassengruppe Cl_K erzeugt. Existiert eine Euklidische Idealklasse, so ist Cl_K also insbesondere zyklisch. Um diese Aussage zu beweisen, brauchen wir das folgende aus [11] stammende Lemma.

LEMMA 3.1.13 (LENSTRA). *Sei $\mathfrak{a}$ ein ganzes Ideal, $\mathfrak{c}$ ein gebrochenes Ideal $\in I_K$. Dann sind äquivalent :*

(i) $\frac{\mathfrak{c}}{\mathfrak{a}} \cap E_{\mathfrak{c}} \neq \emptyset$

(ii) *Es gibt ein $\alpha \in K$ und ein ganzes Ideal $\mathfrak{b} \in I_K$ mit*

$$\mathcal{N}(\mathfrak{b}) < \mathcal{N}(\mathfrak{a}) \text{ und } \mathfrak{b}\mathfrak{c} = (\alpha)\mathfrak{a}$$

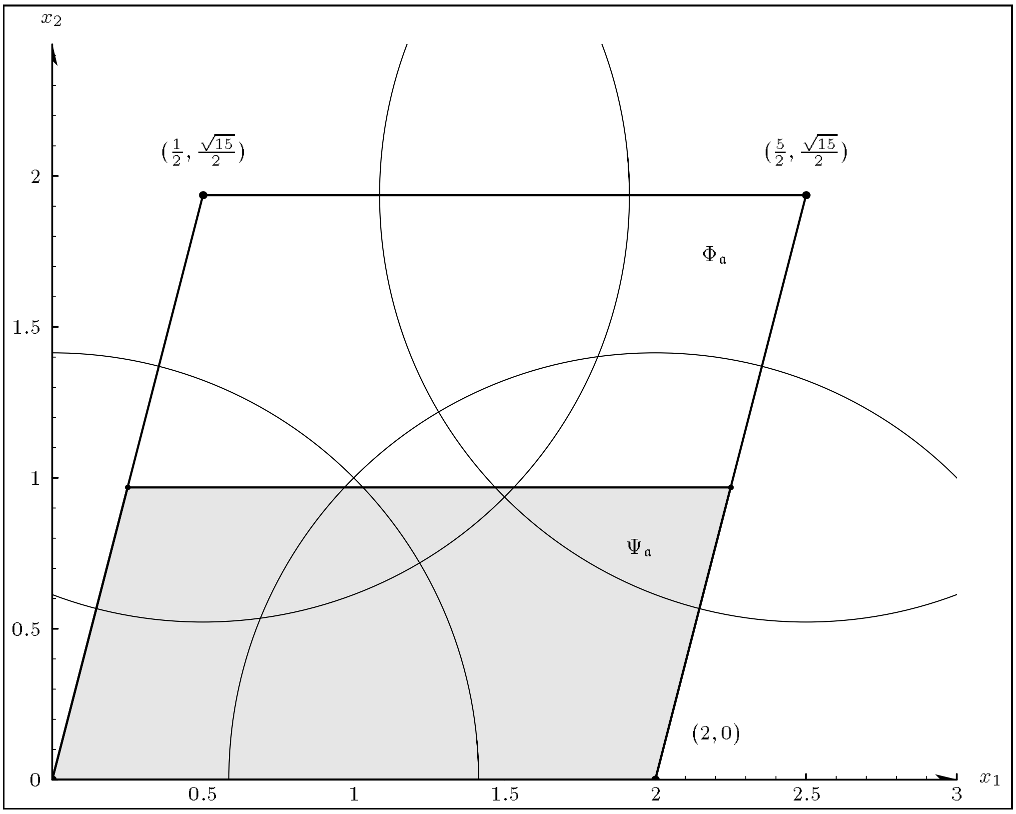

Abbildung III.2. Der Zahlkörper $\mathbb{Q}(\sqrt{-15})$

BEWEIS. (i) $\Rightarrow$ (ii) : Sei $\alpha' \in \frac{\mathfrak{c}}{\mathfrak{a}} \cap E_\mathfrak{c}$, dann gibt es ein $c \in \mathfrak{c}$ mit $|N(\alpha' - c)| < \mathcal{N}(\mathfrak{c})$. Setze nun $\alpha := \alpha' - c$ und $\mathfrak{b} := \frac{(\alpha)\mathfrak{a}}{\mathfrak{c}}$. Wegen $c \in \mathfrak{c} \subseteq \frac{\mathfrak{c}}{\mathfrak{a}}$ ist auch $\alpha' - c \in \frac{\mathfrak{c}}{\mathfrak{a}}$, d.h. $(\alpha) \subseteq \frac{\mathfrak{c}}{\mathfrak{a}}$. Also ist $\mathfrak{b} \subseteq R$, d.h $\mathfrak{b}$ ist ganz, und es gilt

$$(\alpha)\mathfrak{a} = \mathfrak{b}\mathfrak{c}.$$

Wegen $|N(\alpha)| < \mathcal{N}(\mathfrak{c})$ folgt weiter $\mathcal{N}(\mathfrak{b}) = \frac{|N(\alpha)|}{\mathcal{N}(\mathfrak{c})}\mathcal{N}(\mathfrak{a}) < \mathcal{N}(\mathfrak{a})$.

(ii) $\Rightarrow$ (i) : Wegen $(\alpha) = \mathfrak{b}\frac{\mathfrak{c}}{\mathfrak{a}} \subseteq \frac{\mathfrak{c}}{\mathfrak{a}}$ ist $\alpha \in \frac{\mathfrak{c}}{\mathfrak{a}}$. Weiter ist $|N(\alpha)| = \frac{\mathcal{N}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a})}\mathcal{N}(\mathfrak{c}) < \mathcal{N}(\mathfrak{c})$, d.h $\alpha \in E_\mathfrak{c}$ nach Lemma 3.1.5. Also ist $\frac{\mathfrak{c}}{\mathfrak{a}} \cap E_\mathfrak{c} \neq \emptyset$. $\square$

SATZ 3.1.14 (LENSTRA). *Sei* $[\mathfrak{c}]$ *Euklidische Idealklasse,* $\mathfrak{c} \in I_K$. *Dann wird die Idealklassengruppe* Cl_K *von* $[\mathfrak{c}]$ *erzeugt.*

BEWEIS. Annahme: Cl_K wird nicht von $[\mathfrak{c}]$ erzeugt. Sei also $\mathfrak{q} \in I_K$ ein ganzes Ideal von minimaler Norm, sodaß die Idealklasse $[\mathfrak{q}]$ nicht von $[\mathfrak{c}]$ erzeugt wird. Nach Satz 1.4.14 können wir $\mathcal{N}(\mathfrak{q}) \leq M_K$ annehmen.

Zunächst wird gezeigt, daß $\mathfrak{q}$ Primideal ist. Es gibt einen Primidealteiler von $\mathfrak{q}$ dessen Idealklasse nicht von $[\mathfrak{c}]$ erzeugt wird, denn würde $[\mathfrak{c}]$ die Idealklassen aller Primidealteiler von $\mathfrak{q}$ erzeugen, so auch $[\mathfrak{q}]$ selbst. Wegen der Minimalität von $\mathcal{N}(\mathfrak{q})$ ist also $\mathfrak{q}$ schon Primideal.

Da $\mathfrak{q}$ ganz ist, ist $\frac{\mathfrak{c}}{\mathfrak{q}} \supsetneq \mathfrak{c}$. Weil $[\mathfrak{c}]$ Euklidische Idealklasse ist, d.h. $E_\mathfrak{c} \cup \mathfrak{c} = K$, folgt also $\frac{\mathfrak{c}}{\mathfrak{q}} \cap E_\mathfrak{c} \neq \emptyset$. Nach Lemma 3.1.13 existiert dann ein $\alpha \in K$ und ein ganzes Ideal $\mathfrak{b} \in I_K$ mit $N(\mathfrak{b}) < N(\mathfrak{q})$ und $\mathfrak{b}\mathfrak{c} = (\alpha)\mathfrak{q}$. Wegen der Minimalität von $\mathcal{N}(\mathfrak{q})$ wird $[\mathfrak{b}]$ von $[\mathfrak{c}]$ erzeugt, also auch $[\mathfrak{b}\mathfrak{c}] = [\mathfrak{q}]$. Widerspruch. $\square$

3.2. Euklidische Systeme

Die obigen Betrachtungen Euklidischer Ideale werden nun nach Schulze [16] auf Mengen von Idealen verallgemeinert.

DEFINITION 3.2.1. Sei $M \subseteq I_K$ eine nichtleere Menge von gebrochenen Idealen. Dann heißt

$$E_M := \bigcup_{\mathfrak{c} \in M} E_\mathfrak{c}$$

Euklidische Menge von M.

DEFINITION 3.2.2. Sei $M \subseteq I_K$ eine nichtleere Menge von gebrochenen Idealen mit $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c} \neq (0)$. Gilt

$$E_M \cup \mathfrak{m} \supseteq K,$$

so heißt M *Euklidisches System.* Gilt

$$E_M \cup \bigcup_{\mathfrak{c} \in M} \mathfrak{c} \supseteq K,$$

so heißt M *schwach Euklidisches System.*

Daß diese Definitionen tatsächlich Verallgemeinerungen von Definition 3.1.1 sind, sieht man an

BEMERKUNG 3.2.3. *Es gelten :*

(i) *Für* $\mathfrak{c} \in I_K$ *ist* $[\mathfrak{c}]$ *Euklidische Idealklasse* $\Leftrightarrow \{\mathfrak{c}\}$ *Euklidisches System* $\Leftrightarrow \{\mathfrak{c}\}$ *schwach Euklidisches System.*

(ii) *Nach Satz* 3.1.11 *ist* K *Norm-Euklidisch* $\Leftrightarrow \{R\}$ *euklidsches System* $\Leftrightarrow \{R\}$ *schwach Euklidisches System.*

BEMERKUNG 3.2.4. *Sei* $M \subseteq I_K$ *nichtleer. Dann ist* E_M *ein Fixgebiet* [4] *bzgl.* $\mathfrak{m} := \bigcap_{\mathfrak{c}\in M} \mathfrak{c}$.

BEWEIS. Die $E_\mathfrak{c}$, $\mathfrak{c} \in M$, sind nach Bemerkung 3.1.6 Fixgebiete bzgl. $\mathfrak{c}$, also erst recht bzgl. $\mathfrak{m} \subseteq \mathfrak{c}$. Daher ist $E_M = \bigcup_{\mathfrak{c}\in M} E_\mathfrak{c}$ als Vereinigung von Fixgebieten bzgl. $\mathfrak{m}$ nach Bemerkung 1.4.11 (ii) selbst Fixgebiet bzgl. $\mathfrak{m}$. □

Mit Hilfe von Bemerkung 3.2.12 erhalten wir nun als Verallgemeinerung von Bemerkung 3.1.7 für Euklidische Systeme die

BEMERKUNG 3.2.5. *Sei* $M \subseteq I_K$ *nichtleer und* $\mathfrak{m} := \bigcap_{\mathfrak{c}\in M} \mathfrak{c} \neq (0)$. *Sei weiter* $\Psi_\mathfrak{m} \subseteq K$ *ein* K*-Überdeckungsgebiet* [5] *bzgl.* $\mathfrak{m}$. *Gilt*

$$\Psi_\mathfrak{m} \subseteq E_M \cup \mathfrak{m}, \tag{27}$$

bzw.

$$\Psi_\mathfrak{m} \subseteq E_M \cup \bigcup_{\mathfrak{c}\in M} \mathfrak{c}, \tag{28}$$

so ist M *schon Euklidisches System bzw. schwach Euklidisches System. Speziell ergibt sich für* $M = \{\mathfrak{c}\}$ *die Bemerkung* 3.1.7.

BEWEIS. Da $E_M \cup \mathfrak{m}$ und $E_M \cup \bigcup_{\mathfrak{c}\in M} \mathfrak{c}$ Fixgebiete bzgl. $\mathfrak{m}$ sind, folgt aus (27) bzw. (28) nach Satz 1.4.10 schon $K \subseteq E_M \cup \mathfrak{m}$ bzw. $K \subseteq E_M \cup \bigcup_{\mathfrak{c}\in M} \mathfrak{c}$, d.h. M ist Euklidisches System bzw. schwach Euklidisches System. □

Wir wollen nun wie in Schulze [16] zeigen, daß sich die Eigenschaft Euklidischer Ideale, die Idealklassengruppe Cl_K zu erzeugen [6], auch auf Euklidische Systeme übertragen läßt. Dadurch wird deutlich, daß Euklidische Systeme eine sinnvolle Verallgemeinerung der Euklidischen Ideale darstellen. Eine ähnliche Ausage für schwach Euklidische Systeme zu beweisen verschieben wir ans Ende dieses Abschnitts, da erst dann die notwedien Hilfsmittel bereitstehen werden. Wir sagen, daß eine Menge $M \subseteq I_K$ von Idealen die Idealklassengruppe erzeugt, wenn Cl_K

[4] siehe Definition 1.4.8
[5] siehe Definition 1.4.5
[6] wie in Satz 3.1.14 bewiesen

von der zugehörigen Menge der Äquivalenzklassen $\{[\mathfrak{c}] \mid \mathfrak{c} \in M\}$ erzeugt wird. In den folgenden Ausführungen wird wie in Abschnitt 3.1 entscheidend das Lemma 3.1.13 aus Lenstra [11] herangezogen.

LEMMA 3.2.6. *Sei $\mathfrak{c} \in I_K$ ein Ideal $\neq (0)$. Dann gilt für jedes ganze Ideal $\mathfrak{a} \in I_K$ mit $\mathcal{N}(\mathfrak{a}) > M_K$ (M_K die Minkowski-Schranke [7]) :*

$$\frac{\mathfrak{c}}{\mathfrak{a}} \cap E_{\mathfrak{c}} \neq \emptyset$$

.

BEWEIS. Nach Satz 1.4.14 der Gitterpunkttheorie enthält $\frac{\mathfrak{c}}{\mathfrak{a}}$ ein Element $\alpha \neq 0$ mit

$$|N(\alpha)| \leq M_K \mathcal{N}\left(\frac{\mathfrak{c}}{\mathfrak{a}}\right) < \mathcal{N}(\mathfrak{c}) ,$$

d.h. $\alpha \in E_{\mathfrak{c}}$ nach Lemma 3.1.5.. $\square$

SATZ 3.2.7 (SCHULZE). *Sei $M \subseteq I_K$ nichtleer und $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c} \neq (0)$. Setze*

$$P := \left\{ \mathfrak{p} \in I_K \;\middle|\; \mathfrak{p} \text{ Primideal}, N(\mathfrak{p}) \leq M_K, \frac{\mathfrak{m}}{\mathfrak{p}} \cap E_M = \emptyset \right\}.$$

Dann ist $P \cup M$ ein Erzeugendensystem der Idealklassengruppe Cl_K.

BEWEIS. Annahme: Cl_K wird nicht von $P \cup M$ erzeugt. Sei also $\mathfrak{q} \in I_K$ ein ganzes Ideal von minimaler Norm, sodaß die Idealklasse $[\mathfrak{q}]$ von $\mathfrak{q}$ nicht von $P \cup M$ erzeugt wird. Wegen Satz 1.4.14 können wir $\mathcal{N}(\mathfrak{q}) \leq M_K$ annehmen.

Zunächst ist $\mathfrak{q}$ Primideal. Es gibt einen Primidealteiler von $\mathfrak{q}$ dessen Idealklasse nicht von $P \cup M$ erzeugt wird, denn würde $P \cup M$ die Idealklassen aller Primidealteiler von $\mathfrak{q}$ erzeugen, so auch $[\mathfrak{q}]$ selbst. Wegen der Minimalität von $\mathcal{N}(\mathfrak{q})$ ist also $\mathfrak{q}$ schon Primideal.

Trivialerweise ist aber $\mathfrak{q} \notin P$, d.h. $\frac{\mathfrak{m}}{\mathfrak{q}} \cap E_M \neq \emptyset$. Also ist $\frac{\mathfrak{m}}{\mathfrak{p}} \cap E_{\mathfrak{c}} \neq \emptyset$ für ein $\mathfrak{c} \in M$, d.h. erst recht $\frac{\mathfrak{c}}{\mathfrak{p}} \cap E_{\mathfrak{c}} \neq \emptyset$. Nach dem Lemma 3.1.13 existiert dann ein $\alpha \in K$ und ein ganzes Ideal $\mathfrak{b} \in I_K$ mit $N(\mathfrak{b}) < N(\mathfrak{q})$ und $\mathfrak{b}\mathfrak{c} = (\alpha)\mathfrak{q}$. Wegen der Minimalität von $\mathcal{N}(\mathfrak{q})$ wird $[\mathfrak{b}]$ von $P \cup M$ erzeugt, wegen $\mathfrak{c} \in M$ also auch $[\mathfrak{b}\mathfrak{c}] = [\mathfrak{q}]$. Widerspruch. $\square$

KOROLLAR 3.2.8 (SCHULZE). *Sei $M \subseteq I_K$ nichtleer und $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c} \neq (0)$. Gilt für jede Primzahlpotenz $p^r \leq M_K$*

$$\frac{\mathfrak{m}}{p^r} \subseteq E_M \cup \mathfrak{m}, \tag{29}$$

so ist M Erzeugendensystem der Idealklassengruppe Cl_K.

[7] siehe Satz 1.4.14

Beweis. Sei $\mathfrak{p}$ Primideal mit $\mathcal{N}(\mathfrak{p}) \leq M_K$. Zu zeigen ist $\frac{\mathfrak{m}}{\mathfrak{p}} \cap E_M \neq \emptyset$, dann ist in Satz 3.2.7 $P = \emptyset$, und M erzeugt schon Cl_K. Aus $p^r = \mathcal{N}(\mathfrak{p}) \in \mathfrak{p}$ folgt $\frac{1}{(p^r)} \supseteq \frac{1}{\mathfrak{p}}$, also gilt

$$\mathfrak{m} \subsetneq \frac{\mathfrak{m}}{\mathfrak{p}} \subseteq \frac{\mathfrak{m}}{p^r} \subseteq E_M \cup \mathfrak{m}.$$

Das bedeutet aber $\frac{\mathfrak{m}}{\mathfrak{p}} \cap E_M \neq \emptyset$. □

Bemerkung 3.2.9. *Wegen Bemerkung* 3.2.12 (i) *folgt in Korollar* 3.2.8 *aus*

$$\frac{\mathfrak{m}}{p^r} \cap \Phi_{\mathfrak{m}} \subseteq E_M \cup \mathfrak{m} \tag{30}$$

schon (29). *Dabei sei* $\Phi_{\mathfrak{m}}$ *die Grundmasche von* $\mathfrak{m}$. *Da* $\frac{\mathfrak{m}}{p^r} \cap \Phi_{\mathfrak{m}}$ *nach Satz* 1.3.5 *endlich ist, wird Bedingung* (30) *häufig leichter nachzuweisen sein als* (29).

Als oben angekündigte Verallgemeinerung von Satz 3.1.14 ergibt sich das

Korollar 3.2.10 (Schulze). *Ist M Euklidisches System, so erzeugt M die Idealklassengruppe Cl_K. Insbesondere erzeugt also jedes Euklidische Ideal die Idealklassengruppe.*

Beweis. Nach Definition 3.2.2 gilt $E_M \cup \mathfrak{m} \supseteq K$, wobei $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c}$, also ist (29) aus Korollar 3.2.8 erfüllt. □

Bemerkung 3.2.11. *Wählt man $M \subseteq H_K$, z.B. $M = \{R\}$, so folgt aus Satz 3.2.7 die aus der Gitterpunkttheorie bekannte Aussage*[8], *daß die Menge aller Primideale mit Norm $\leq M_K$ die Idealklassengruppe Cl_K erzeugen.*

Beweis. Die Menge aller Primideale mit Norm $\leq M_K$ umfaßt die Menge P aus Satz 3.2.7 und M ist in der trivialen Klasse enthalten. □

Wir wollen nun unter der Voraussetzung, daß ein (schwach) Euklidisches System existiert, einige Überlegungen dazu anstellen, wie sich dieses System auf eine möglichst einfache Form bringen läßt. Von besonderem Interesse ist es natürlich, ein endliches System anzugeben. Der Frage, ob überhaupt ein Euklidisches System existiert, werden wir uns erst danach widmen.

Bemerkung 3.2.12. *Sei $M \subseteq I_K$ nichtleer und für $\alpha \in K$ sei $\alpha M := \{(\alpha)\mathfrak{c} \mid \mathfrak{c} \in M\}$. Dann gilt*

$$\alpha E_M = E_{\alpha M}$$

für alle $\alpha \in K \backslash \{0\}$.

[8] Die Aussage ergibt sich unmittelbar aus Satz 1.4.14 der Gitterpunkttheorie

Beweis. Nach Bemerkung 3.1.8 ist

$$\alpha E_M = \bigcup_{\mathfrak{c}\in M} \alpha E_{\mathfrak{c}} = \bigcup_{\mathfrak{c}\in M} E_{(\alpha)\mathfrak{c}} = E_{\alpha M}.$$

□

Satz 3.2.13. *Sei M (schwach) Euklidisches System und $\alpha \in K$. Dann ist auch $M' := \alpha M$ (schwach) Euklidisches System.*

Insbesondere existieren (schwach) Euklidische Systeme M', M'' mit $\mathfrak{m}' := \bigcap_{\mathfrak{c}\in M'} \mathfrak{c} = \mathfrak{a}$ und $\mathfrak{m}'' = \bigcap_{\mathfrak{c}\in M''} \mathfrak{c} = \frac{1}{\mathfrak{b}}$ für ganze Ideale $\mathfrak{a}, \mathfrak{b} \in I_K$

Beweis. Nach Bemerkung 3.2.12 ist $E_{\alpha M} = \alpha E_M$. Damit folgt

$$E_{\alpha M} \cup \bigcap_{\mathfrak{c}\in M} (\alpha)\mathfrak{c} = \alpha(E_M \cup \bigcap_{\mathfrak{c}\in M} \mathfrak{c}) \supseteq \alpha K = K,$$

bzw.

$$E_{\alpha M} \cup \bigcup_{\mathfrak{c}\in M} (\alpha)\mathfrak{c} = \alpha(E_M \cup \bigcup_{\mathfrak{c}\in M} \mathfrak{c}) \supseteq \alpha K = K,$$

d.h. αM ist (schwach) Euklidisches System.

Sei nun nach Lemma 1.1.3 $\mathfrak{m} := \bigcap_{\mathfrak{c}\in M} \mathfrak{c} = \frac{\mathfrak{a}}{r} = \frac{s}{\mathfrak{b}}$ mit $\mathfrak{a}, \mathfrak{b} \in I_K$ ganz und $r, s \in \mathbb{Z}$. Dann sind also $M' := rM$ und $M'' := \frac{1}{s}M$ (schwach) Euklidische Systeme mit $\mathfrak{m}' = r\mathfrak{m} = \mathfrak{a}$ und $\mathfrak{m}'' = \frac{1}{s}\mathfrak{m} = \frac{1}{\mathfrak{b}}$. □

Satz 3.2.14. *Sei M endliches (schwach) Euklidisches System. Dann gibt es ein (schwach) Euklidisches System M' von gleicher Mächtigkeit aus reziproken ganzen Idealen, d.h.*

$$M' \subseteq \left\{ \frac{1}{\mathfrak{a}} \;\middle|\; \mathfrak{a} \in I_K \text{ ganz} \right\}.$$

Inbesondere ist dann $\mathfrak{m}' := \bigcap_{\mathfrak{c}\in M'} \mathfrak{c} \supseteq R$.

Beweis. Sei $M = \{\mathfrak{c}_1, \mathfrak{c}_2, \dots, \mathfrak{c}_m\}$, $m \in \mathbb{N}$, und nach Lemma 1.1.3

$$\mathfrak{c}_i = \frac{d_i}{\mathfrak{a}_i} \quad , \quad \mathfrak{a}_i \in I_K \text{ ganz}, \ d_i \in \mathbb{N} \text{ für } i = 1, 2, \dots, m.$$

Setze $d := \prod_{i=1}^m d_i$. Dann ist $M' := \frac{1}{d}M \subseteq \left\{ \frac{1}{\mathfrak{a}} \;\middle|\; \mathfrak{a} \in I_K \text{ ganz}\right\}$, und nach Satz 3.2.13 ist M' selbst (schwach) Euklidisches System. □

Bemerkung 3.2.15. *Ist M (schwach) Euklidisches System, $\mathfrak{m} := \bigcap_{\mathfrak{c}\in M} \mathfrak{c}$, so auch $M \cup \{\mathfrak{m}\}$. Wir können also stets $\mathfrak{m} \in M$ annehmen.*

Beweis. Ist M (schwach) Euklidisches System, so erst recht $M' := M \cup \mathfrak{m}$, denn $E_{M'} \subseteq E_M$ und

$$\mathfrak{m}' := \bigcap_{\mathfrak{c} \in M'} \mathfrak{c} = \mathfrak{m},$$

bzw.

$$\bigcup_{\mathfrak{c} \in M'} \mathfrak{c} = \bigcup_{\mathfrak{c} \in M} \mathfrak{c} \cup \mathfrak{m} \supseteq \bigcup_{\mathfrak{c} \in M} \mathfrak{c}.$$

□

In Satz 3.2.14 haben wir gesehen, daß sich ein endliches (schwach) Euklidisches System auf eine recht einfache Form bringen läßt. Der folgende Satz aus Schulze [17] stellt ein Kriterium für die Existenz eines endlichen (schwach) Euklidischen Systems dar.

Satz 3.2.16 (Schulze). *Sei $M \subseteq I_K$ nichtleer und $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c} \neq (0)$. Gilt*

$$\mathbb{R}^n \subseteq E_M \cup \mathfrak{m} \tag{31}$$

bzw.

$$\mathbb{R}^n \subseteq E_M \cup \bigcup_{\mathfrak{c} \in M} \mathfrak{c}, \tag{32}$$

so existiert ein endliches Euklidisches bzw. schwach Euklidisches System $M' \subseteq M$.

Beweis. Wir nehmen nach Bemerkung 3.2.15 $\mathfrak{m} \in M$ an. Aus (31) bzw. (32) folgt insbesondere

$$\bar{\Phi}_{\mathfrak{m}} \subseteq E_M \cup \mathfrak{m} = \bigcup_{\mathfrak{c} \in M} E_{\mathfrak{c}} \cup \mathfrak{m} = \bigcup_{\mathfrak{c} \in M} E_{\mathfrak{c}} \cup (E_{\mathfrak{m}} \cup \mathfrak{m})$$

bzw.

$$\bar{\Phi}_{\mathfrak{m}} \subseteq E_M \cup \bigcup_{\mathfrak{c} \in M} \mathfrak{c} = \bigcup_{\mathfrak{c} \in M} (E_{\mathfrak{c}} \cup \mathfrak{c})$$

für den topologischen Abschluß $\bar{\Phi}_{\mathfrak{m}}$ der Grundmasche $\Phi_{\mathfrak{m}}$ von $\mathfrak{m}$. Die $E_{\mathfrak{c}}$, $E_{\mathfrak{c}} \cup \mathfrak{c}$ und $E_{\mathfrak{m}} \cup \mathfrak{m}$ sind nach Bemerkung 3.1.4 offen, und da $\bar{\Phi}_{\mathfrak{m}}$ abgeschlossen und beschränkt, also kompakt ist, existiert nach dem Satz von Heine-Borel eine endliche Teilüberdeckung

$$\bar{\Phi}_{\mathfrak{m}} \subseteq \bigcup_{\mathfrak{c} \in M'} E_{\mathfrak{c}} \cup (E_{\mathfrak{m}} \cup \mathfrak{m})$$

bzw.

$$\bar{\Phi}_{\mathfrak{m}} \subseteq \bigcup_{\mathfrak{c} \in M'} (E_{\mathfrak{c}} \cup \mathfrak{c})$$

mit $M' \subseteq M$ endlich. Da auch $M' \cup \{\mathfrak{m}\}$ endlich ist, können wir $\mathfrak{m} \in M'$ annehmen. Es folgt also

$$\Phi_{\mathfrak{m}} \cap K \subseteq \bar{\Phi}_{\mathfrak{m}} \subseteq \bigcup_{\mathfrak{c} \in M'} E_{\mathfrak{c}} \cup \mathfrak{m} = E_{M'} \cup \mathfrak{m}$$

bzw.

$$\Phi_{\mathfrak{m}} \cap K \subseteq \bar{\Phi}_{\mathfrak{m}} \subseteq \bigcup_{\mathfrak{c} \in M'} (E_{\mathfrak{c}} \cup \mathfrak{c}) = E_{M'} \cup \bigcup_{\mathfrak{c} \in M'} \mathfrak{c}.$$

Da $\Phi_{\mathfrak{m}} \cap K$ als Grundmasche von $\mathfrak{m}$ in K nach Satz 1.4.6 auch K-Überdeckungsgebiet bzgl. $\mathfrak{m}$ ist, folgt mit Bemerkung 3.2.5, daß M' Euklidisches bzw. schwach Euklidisches System ist. □

DEFINITION 3.2.17. Wir definieren die Menge der *reziproken ganzen Hauptideale*

$$H^- := H_K^- := \left\{ \frac{1}{(\mu)} \,\middle|\, \mu \in R, \mu \neq 0 \right\},$$

und die Menge

$$Z^- := Z_K^- := \left\{ \frac{1}{(d)} \,\middle|\, d \in \mathbb{Z}, d \neq 0 \right\}.$$

BEMERKUNG 3.2.18. *Es gilt*

$$\bigcup_{d \in \mathbb{Z}} \frac{1}{(d)} = K \quad \textit{und} \quad \bigcap_{d \in \mathbb{Z}} \frac{1}{(d)} = R.$$

Damit folgt auch

$$\bigcup_{\mu \in R} \frac{1}{(\mu)} = K \quad \textit{und} \quad \bigcap_{\mu \in R} \frac{1}{(\mu)} = R.$$

Daß Z^- bzw. H^- Euklidisches System ist, bedeutet also nach Definition 3.2.2 gerade $K \subseteq E_{Z^-} \cup R$ bzw. $K \subseteq E_{H^-} \cup R$, und daß Z^- bzw. H^- schwach Euklidisches System ist, bedeutet gerade $K \subseteq E_{Z^-} \cup K$ bzw. $K \subseteq E_{H^-} \cup K$. Daher sind Z^- und H^- stets schwach Euklidische Systeme.

BEWEIS. Jedes $\alpha \in K$ läßt sich als $\alpha = \frac{\alpha'}{a}$ mit $\alpha' \in R$ und $a \in \mathbb{Z}$ schreiben, also gilt $K = \bigcup_{d \in \mathbb{Z}} \frac{1}{(d)}$.

Es ist klar $\bigcap_{d \in \mathbb{Z}} \frac{1}{(d)} \supseteq R$. Sei nun $\frac{a}{b} \in K \backslash R$, $a, b \in R$, $b \neq 0$, und seien o.B.d.A. a und b teilerfremd. Wähle $d \in \mathbb{Z}$, sodaß $b \nmid d$. Dann ist $\frac{a}{b} \notin \frac{1}{(d)} \supseteq \bigcap_{d \in \mathbb{Z}} \frac{1}{(d)}$, denn aus $\frac{a}{b} \in \frac{1}{(d)}$ folgt, da a, b teilerfremd sind, $d | b$. Also ist $\bigcap_{d \in \mathbb{Z}} \frac{1}{(d)} \subseteq R$ gezeigt. □

LEMMA 3.2.19. *Es gilt $\mathbb{R}^n \backslash K \subseteq E_{Z^-}$.*

BEWEIS. Sei $x \in \mathbb{R}^n \backslash K$. Das Approximationslemma 2.3.12 liefert dann Elemente $c \in R, d \in \mathbb{Z}$, sodaß

$$\left| N\left(x - \frac{c}{d}\right) \right| < \frac{1}{|N(d)|} = \mathcal{N}\left(\frac{1}{(d)}\right).$$

Nach Voraussetzung ist $x \notin \frac{1}{(d)}$, also folgt $x \in E_{\frac{1}{(d)}} \subseteq E_{Z^-}$. □

Satz 3.2.20. *Sei M ein (schwach) Euklidisches System. Dann existiert auch ein endliches (schwach) Euklidisches System $M' \subseteq M \cup Z^-$.*

Beweis. Setze $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c}$. Nach Lemma 1.1.3 gibt es ein $r \in \mathbb{Z}$, sodaß $r\mathfrak{m}$ ganzes Ideal von R ist, und nach Satz 3.2.13 ist dann auch rM (schwach) Euklidisches System, also insbesondere

$$K \subseteq E_{rM} \cup r\mathfrak{m}$$

bzw.

$$K \subseteq E_{rM} \cup K,$$

und mit Lemma 3.2.19 folgt

$$\mathbb{R}^n \subseteq E_{rM \cup Z^-} \cup r\mathfrak{m}$$

bzw.

$$\mathbb{R}^n \subseteq E_{rM \cup Z^-} \cup K.$$

Nun ist $\bigcap_{\mathfrak{c} \in rM \cup Z^-} \mathfrak{c} \supseteq r\mathfrak{m} \cap R = r\mathfrak{m}$ und nach Bemerkung 3.2.18 $\bigcup_{\mathfrak{c} \in rM \cup Z^-} \mathfrak{c} = K$. Nach Satz 3.2.16 existiert also ein endliches (schwach) Euklidisches System $M' \subseteq rM \cup Z^-$, und nach Satz 3.2.13 ist dann auch $\frac{1}{r}M'$ endliches (schwach) Euklidisches System mit $\frac{1}{r}M' \subseteq M \cup \frac{1}{r}Z^- \subseteq M \cup Z^-$. □

Wir können also nach diesem Satz von einem (schwach) Euklidischen System immer annehmen, daß es endlich ist, und dann nach Satz 3.2.14 sogar, daß es aus reziproken ganzen Idealen besteht.

Jetzt kommen wir zu der Frage, wann überhaupt ein (schwach) Euklidisches System existiert. Für ein schwach Euklidisches System ist dies sofort klar.

Bemerkung 3.2.21. *Für jeden Zahlkörper existiert ein endliches schwach Euklidisches System $\subseteq Z^-$.*

Beweis. klar nach Bemerkung 3.2.18 und Satz 3.2.20. □

Wir werden später in Satz 3.3.1 ein solches endliches schwach Euklidisches System nach einer Methode von Lenstra konstruieren.

Es ist jedoch nicht klar, ob für jeden Zahlkörper auch ein Euklidisches System existiert. Wir werden in Satz 3.2.24 sehen, daß dies aber zumindest der Fall ist, wenn die Klassenzahl $h = 1$ ist. Umgekehrt folgt aus der Existenz eines Euklidischen Systems, welches nur aus Hauptidealen besteht, sofort nach Korollar 3.2.10, daß die Klassenzahl $h = 1$ ist. Daher sind Euklidische Systeme aus Hauptidealen von besonderem Interesse.

Wir wollen nun charakterisieren, in welchen Zahlkörpern H^- Euklidisches System ist.

LEMMA 3.2.22. *Sei $\mu \in R$. Seien $a, b \in R$, $b \neq 0$ und $b \nmid a$, d.h. $\frac{a}{b} \in K \setminus R$. Dann sind äquivalent :*

(i) $\frac{a}{b} \in E_{\frac{1}{(\mu)}}$

(ii) *Es existiert ein $\lambda \in R$, sodaß $0 < |N(\mu a - \lambda b)| < |N(b)|$.*

(iii) *Die Nebenklasse $a\mu + (b)$ modulo b enthält ein Element $\neq 0$ mit Normbetrag $< |N(b)|$. Insbesondere ist dann $a\mu + (b)$ nicht die Nullklasse modulo b.*

BEWEIS. Nach Bemerkung 3.1.3 ist (i) äquivalent zu

$$\exists \lambda \in R : 0 < \left| N\left(\frac{a}{b} - \frac{\lambda}{\mu}\right)\right| < \frac{1}{|N(\mu)|}.$$

Durch Multiplikation mit $|N(b\mu)|$ ergibt sich hieraus (ii). Da der Ausdruck $a\mu - \lambda b$ aus (ii) für $\lambda \in R$ gerade ein allgemeines Element der Nebenklasse $a\mu + (b)$ darstellt, folgt auch die Äquivalenz von (ii) und (iii). □

LEMMA 3.2.23. *Seien $a, b \in R$, $b \neq 0$ und $b \nmid a$, d.h. $\frac{a}{b} \in K \setminus R$. Dann sind äquivalent :*

(i) $\frac{a}{b} \in E_{H^-}$

(ii) *Es existieren $\lambda, \mu \in R \setminus \{0\}$, sodaß*

$$0 < |N(\mu a - \lambda b)| < |N(b)|$$

(iii) *Es gibt $d \in (a, b)$, $d \neq 0$, sodaß $|N(d)| < |N(b)|$.*

BEWEIS. (i) $\Leftrightarrow$ (ii) :

(ii) $\Leftrightarrow$ (iii) : Der Ausdruck $\mu a - \lambda b$ in (ii) ist gerade ein allgemeines Element aus (a, b) und $d = 0 \Leftrightarrow N(d) = 0$. □

SATZ 3.2.24. *Folgende Aussagen sind äquivalent :*

(i) *H^- ist Euklidisches System*

(ii) *Es existiert ein endliches Euklidisches System $M \subseteq H^-$*

(iii) *Es existiert ein Euklidisches System aus Hauptidealen*

(iv) *R ist Hauptidealring.*

(v) *Für alle $a, b \in R$, $b \neq 0$, $b \nmid a$, existieren $\lambda, \mu \in R$ mit*

$$0 < |N(\mu a - \lambda b)| < |N(b)|.$$

BEWEIS. (i) $\Rightarrow$ (ii) : Satz 3.2.20

(ii) $\Rightarrow$ (iii) : klar.

(iii) $\Rightarrow$ (iv) : Korollar 3.2.10

(iv) $\Rightarrow$ (v) : Seien $a, b \in R, b \neq 0, b \nmid a$. Da R Hauptidealring ist, existieren $d, \lambda, \mu \in R$, $d \neq 0$, mit $(d) = (a, b)$ und $\mu a - \lambda b = d$. Wegen $b \nmid a$ ist $b \not\sim d$, also d echter Teiler von b in R. Aufgrund der Multiplikativität der Norm folgt dann $0 < |N(d)| < |N(b)|$.

(v) $\Rightarrow$ (i) : Wegen der Äquivalenz von (i) und (ii) in Lemma 3.2.23 folgt aus (v) $K \backslash R \subseteq E_{H^-}$, d.h. H^- ist Euklidisches System nach Bemerkung 3.2.18. $\square$

Die Äquivalenz von (iv) und (v) ist auch als Dedekind-Hasse-Kriterium [9] bekannt.

Läßt man in (v) von Satz 3.2.24 nur $\mu = 1$ zu, so erhält man genau die norm-euklidische Bedingung (vgl. Definition 2.1.1 für die Norm). Die Bedingung (v) ist also eine weitere Verallgemeinerung der norm-euklidischen Eigenschaft.

Daß H^- Euklidisches System ist bedeutet nach Bemerkung 3.2.18 genau $K \subseteq E_{H^-} \cup R$ und daraus folgt

$$\Phi \cap K \subseteq E_{H^-} \cup R \tag{33}$$

für die Grundmasche Φ des Gitters R in $\mathbb{R}^n$. Nach Bemerkung 3.2.5 folgt aus (33) schon, daß H^- Euklidisches System ist. Wegen $\Phi \cap R = \{0\}$ ist (33) auch äquivalent zu

$$(\Phi \cap K) \backslash \{0\} \subseteq E_{H^-},$$

d.h. daß E_{H^-} die Grundmasche $\Phi \cap K$ des Gitters R in K bis auf das Element 0 enthält. Allgemein gilt nun

SATZ 3.2.25. *Sei M endliches schwach Euklidisches System. Dann ist die Menge $(\Phi \cap K) \backslash E_M$ endlich.*

BEWEIS. Da M schwach Euklidisches System ist, gilt $K \subseteq E_M \cup \bigcup_{\mathfrak{c} \in M} \mathfrak{c}$, also

$$(\Phi \cap K) \backslash E_M = (K \backslash E_M) \cap \Phi \subseteq \Big(\bigcup_{\mathfrak{c} \in M} \mathfrak{c} \Big) \cap \Phi = \bigcup_{\mathfrak{c} \in M} (\mathfrak{c} \cap \Phi).$$

Die $\mathfrak{c} \cap \Phi$ sind nach Satz 1.3.5 der Gitterpunkttheorie endlich, da Φ als beschränkte Teilmenge von $\mathbb{R}^n$ offenbar in einer Kugel U_r enthalten ist und $\mathfrak{c}$ nach Satz 1.4.1 vollständiges Gitter in $\mathbb{R}^n$ ist. $\square$

KOROLLAR 3.2.26. *Es sind $(\Phi \backslash E_{Z^-}) \cap K$ und $(\Phi \backslash E_{H^-}) \cap K$ endlich.*

BEWEIS. Nach Bemerkung 3.2.21 existiert ein endliches schwach Euklidisches Teilsystem $M \subseteq Z^-$, und nach Satz 3.2.25 ist $(\Phi \backslash E_M) \cap K$ endlich. Wegen $E_{H^-} \supseteq E_{Z^-} \supseteq E_M$ folgt die Behauptung. $\square$

Wir wählen nun speziell $M = H^-$ und können dann Satz 3.2.25 wie folgt verschärfen.

SATZ 3.2.27 (SCHULZE). *E_{H^-} enthält $\Phi \cap K$ bis auf endlich viele Elemente. Sei etwa $|(\Phi \cap K) \backslash E_{H^-}| = n$, dann gilt für die Klassenzahl $h \leq n + 1$.*

---

[9] vgl. Pollard [15]

Beweis. In Korollar 3.2.26 wurde bereits gezeigt, daß $(\Phi \backslash E_{H^-}) \cap K$ endlich ist. Wir geben hier einen zweiten Beweis dieser Aussage, der nicht auf dem Satz von Heine-Borel beruht.

Dazu betrachten wir für alle $b \in R \backslash \{0\}$ die Mengen

$$F_b := \left\{ \frac{a}{b} \,\middle|\, a \in R, \frac{a}{b} \in \Phi \backslash E_{H^-} \right\},$$

die wegen $F_b \subseteq \frac{1}{(b)} \cap \Phi$ nach Satz 1.3.5 der Gitterpunkttheorie endlich sind, denn Φ ist als beschränkte Teilmenge von $\mathbb{R}^n$ in einer Kugel U_r enthalten. Weiter definieren wir für ganze Ideale $\mathfrak{a} \in I_K$ die Mengen

$$S_{\mathfrak{a}} := \{ b \in \mathfrak{a} \mid b \neq 0 \text{ von minimalem Normbetrag in } \mathfrak{a} \}.$$

Da es nur endlich viele ganze Ideale mit Norm $\leq M_K$ gibt, ist

$$S := \bigcup_{\substack{\mathfrak{a} \in I_K ganz, \\ \mathcal{N}(\mathfrak{a}) \leq M_K}} S_{\mathfrak{a}}$$

Vereinigung endlich vieler Mengen $S_{\mathfrak{a}}$.

Wir zeigen nun

$$(\Phi \cap K) \backslash E_{H^-} \subseteq F,$$

wobei $F := \bigcup_{b \in S} F_b$ gesetzt wird. Sei dazu $\alpha = \frac{a}{b} \in (\Phi \cap K) \backslash E_{H^-}$, $a, b \in R$, $b \neq 0$. Nach Satz 1.4.14 der Gitterpunkttheorie gibt es $\lambda \in K \backslash \{0\}$, sodaß $\mathfrak{a} := (\lambda)(a, b) = (\lambda a, \lambda b)$ ganz ist und $\mathcal{N}(\mathfrak{a}) \leq M_K$. Dann sind $\lambda a, \lambda b \in R$, $\lambda b \neq 0$, also $\alpha = \frac{\lambda a}{\lambda b} \in F_{\lambda b}$. Wegen der Äquivalenz von (i) und (iii) in Lemma 3.2.23 ist dann λb von minimalem Normbetrag in $\mathfrak{a}$, d.h. $\lambda b \in S_{\mathfrak{a}} \subseteq S$ und $\alpha = \frac{\lambda a}{\lambda b} \in F$ ist gezeigt.

Es bleibt zu zeigen, daß F endlich ist. In einem ganzen Ideal gibt es bis auf Assoziierte nur endlich viele Elemente einer vorgegebenen Norm, d.h. insbesondere bis auf Assoziierte nur endlich viele Elemente von minimalem Normbetrag. Also sind die Faktormengen $S_{\mathfrak{a}}/_{\sim}$ modulo der Assoziiertheitsrelation $\sim$ endlich. Damit ist auch $S/_{\sim}$ endlich.

Ist $b \sim b'$, so ergibt sich aus der Definiton der F_b sofort $F_b = F_{b'}$. Daher schreiben wir auch $F_{[b]}$ statt F_b, wobei $[b]$ die Äquivalenzklasse von b bzgl. $\sim$ bezeichnet. Dann gilt

$$F = \bigcup_{[b] \in S/_{\sim}} F_{[b]},$$

und F ist endlich, da $S/_{\sim}$ und die $F_{[b]}$ endlich sind.

Zum Beweis der zweiten Aussage betrachten wir die Abbildung

$$(\Phi \cap K) \backslash E_{H^-} \to Cl_K \quad , \quad \frac{a}{b} \mapsto [(a, b)].$$

Sie ist wohldefiniert, denn aus $\frac{a}{b} = \frac{a'}{b'}$ folgt $a' = \lambda a, b' = \lambda b$ für ein $\lambda \in K\backslash\{0\}$, also $[(a', b')] = [(\lambda)(a, b)] = [(a, b)]$.

Wir zeigen, daß jede nichttriviale Idealklasse $[\mathfrak{a}]$, $\mathfrak{a}$ also kein Hauptideal, ein Urbild hat. Dann folgt die Behauptung $|Cl_K| \leq |\Phi\backslash E_{H^-}| + 1$.

Sei $b \in \mathfrak{a}$ von minimalem Normbetrag. Dann kann $a \in \mathfrak{a}$ so gewählt werden, daß $\mathfrak{a} = (a, b)$ [10]. Aufgrund der Äquivalenz von (i) und (iii) in Lemma 3.2.23 ist dann $\frac{a}{b} \notin E_{H^-}$. Nach Satz 1.3.3 existiert ein $d \in R$, sodaß $\frac{a}{b} + d = \frac{a+bd}{b} \in \Phi$ und da E_{H^-} nach Bemerkung 3.1.6 Fixgebiet bzgl R ist, ist auch $\frac{a+bd}{b} \notin E_{H^-}$. Wegen $\mathfrak{a} = (a + bd, b)$ ist also $\frac{a+bd}{b}$ Urbild von $[\mathfrak{a}]$. □

Für schwach Euklidische Systeme können wir nun eine ähnliche Aussage wie Korollar 3.2.10 beweisen.

Satz 3.2.28. *Sei M schwach Euklidisches System und $M \subseteq H^-$. Dann erzeugen alle Teiler der (μ) mit $\frac{1}{(\mu)} \in M$ die Idealklassengruppe.*

Beweis. Sei $\mathfrak{a}$ nicht Hauptideal. Zu zeigen ist, daß die Idealklasse $[\mathfrak{a}]$ einen Teiler von (μ) enthält für ein $\frac{1}{(\mu)} \in M$. Sei $\beta \in \mathfrak{a}$ mit minimalem Normbetrag und $\alpha \in \mathfrak{a}$ so gewählt, daß $\mathfrak{a} = (\alpha, \beta)$. Da $\mathfrak{a}$ nicht Hauptideal ist, teilt β nicht α und da β von minimalem Normbetrag in (α, β) ist, gilt nach Lemma 3.2.23 $\frac{\alpha}{\beta} \notin E_{H^-}$, also erst recht $\frac{\alpha}{\beta} \notin E_M$. Da M schwach Euklidisches System ist, gilt aber $K \subseteq E_M \cup \bigcup_{\frac{1}{(\mu)} \in M} \frac{1}{(\mu)}$, also folgt $\frac{\alpha}{\beta} = \frac{\lambda}{\mu}$ für geeignete $\frac{1}{(\mu)} \in M$ und $\lambda \in R$. Wie im Beweis von Satz 3.2.27 ergibt sich hieraus, daß $\mathfrak{a} = (\alpha, \beta)$ und (λ, μ) dieselbe Idealklasse erzeugen, und (λ, μ) ist Teiler von (μ). □

Eine weitere interessante Eigenschaft schwach Euklidischer Systeme liefert

Satz 3.2.29. *Sei $M = \left\{\frac{1}{(d_1)}, \frac{1}{(d_2)}, \ldots, \frac{1}{(d_m)}\right\}$, $m \in \mathbb{N}$, $d_i \in \mathbb{Z}\backslash\{0\}$, schwach Euklidisches System.* [11] *Sei weiter $R' \subseteq K$ ein Teilring mit $R' \supseteq \bigcup_{i=1}^{m} \frac{1}{(d_i)} \supsetneq R$.*

Dann ist R' Norm-Euklidisch.

Beweis. Für den Quotientenkörper von R' gilt $Q(R') = K$. Nach Satz 2.3.2 ist also zu zeigen :

$$\forall \alpha \in K : \exists \lambda \in R' : |N(\alpha - \lambda)| < 1.$$

Sei also $\alpha \in K$. Da M schwach Euklidisches System ist, gibt es $1 \leq i \leq m$ und $c \in R$, sodaß $|N(\alpha - \frac{c}{d_i})| < \frac{1}{\mathcal{N}((d_i))} \leq 1$. Wegen $\frac{c}{d_i} \in \frac{1}{(d_i)} \subseteq R'$ ist alles gezeigt. □

[10] siehe dazu Marcus [13], Chapter 3, Theorem 17, Seite 61

[11] Ein solches System existiert stets in Hauptidealringen nach Satz 3.2.24 und Satz 3.2.14.

Beispiel 3.2.30. Sei $M = \left\{\frac{1}{(d_1)}, \frac{1}{(d_2)}, \ldots, \frac{1}{(d_m)}\right\}$, $m \in \mathbb{N}$, schwach Euklidisches System. Sei weiter $a \in \bigcap_{i=1}^{m}(d_i)$. Dann ist die Lokalisierung

$$R_a := \left\{\frac{c}{a^k} \mid k \in \mathbb{N}_0, c \in R\right\} \subseteq K$$

Norm-Euklidisch.

Beweis. Zu zeigen ist

$$\bigcup_{i=1}^{m} \frac{1}{(d_i)} \subseteq R_a,$$

dann folgt die Behauptung nach Satz 3.2.29. Sei also $\alpha \in \frac{1}{(d_i)}$ für ein i. Dann ist $\alpha(d_i) \subseteq R$, also wegen $a \in (d_i)$ speziell $c := \alpha a \in R$, und es folgt $\alpha = \frac{c}{a} \in R_a$. $\square$

3.3. Konstruktionsverfahren Euklidischer Systeme

Zunächst wollen wir angeben, wie man auf allgemeine Weise ein endliches schwach Euklidisches System $\subseteq Z^-$ erhält.

Satz 3.3.1. *Sei $m > M_K$ und seien $\mu_1, \mu_2, \ldots, \mu_m \in R$ paarweise verschieden. Dann ist*

$$M := \left\{\frac{1}{(\mu_i - \mu_j)} \;\middle|\; i \neq j\right\}$$

schwach Euklidisches System.

Beweis. Sei $\frac{a}{b} \in K$, $a, b \in R$. Nach der Minkowski-Theorie [12] gibt es eine meßbare beschränkte Teilmenge $U \subseteq \mathbb{R}^n$ mit $\operatorname{Vol} U \cdot M_K = \operatorname{Vol} \Phi$ und

$$|N(u_1 - u_2)| < 1 \quad \text{für alle } u_1, u_2 \in U. \tag{34}$$

Wir betrachten nun für $i = 1, 2, \ldots, m$ die Mengen $U_i := \frac{a}{b}\mu_i + U$, die dann auch die Eigenschaft (34) erfüllen. Wegen der Translationsinvarianz des Lebesgue-Maßes gilt $\operatorname{Vol} U_i = \operatorname{Vol} U$ für $i = 1, 2, \ldots, m$.

Für festes i läßt sich nach Korollar 1.3.4 jedes Element aus U_i durch Translation um ein eindeutig bestimmtes Element aus R in die Grundmasche Φ verschieben. So entsteht die Menge der verschobenen Elemente

$$U_i' := \bigcup_{c \in R} ((U_i + c) \cap \Phi) \subseteq \Phi.$$

Da U_i beschränkt ist, ist $(U_i + c) \cap \Phi \neq \emptyset$ nur für endlich viele $c \in R$, d.h. U_i' ist in Wirklichkeit Vereinigung von endlich vielen Mengen $(U_i + c) \cap \Phi$. Die Mengen $U_i \cap (\Phi - c)$ für $c \in R$ sind als Durchschnitt zweier meßbarer Mengen selbst meßbar und aufgrund der Translationsinvarianz des Lebesgue-Maßes folgt $\operatorname{Vol}((U_i + c) \cap \Phi) =$

[12] vgl. Marcus [13], Chapter 5, Proof of Theorem 37, Seite 139

$\mathrm{Vol}\,(U_i \cap (\Phi - c))$. Insbesondere existiert also $\mathrm{Vol}\,((U_i + c) \cap \Phi)$ für alle $c \in R$ und damit auch $\mathrm{Vol}\,U_i'$.

Bei der Translation von U_i um Elemente aus R kann es zu keinen Überschneidungen kommen, d.h. $(U_i + c_1) \cap (U_i + c_2) = \emptyset$ für $c_1, c_2 \in R$ mit $c_1 \neq c_2$. Denn wäre $c_1 + u_1 = c_2 + u_2$ für $u_1, u_2 \in U_i$, so wäre $|N(u_1 - u_2)| = |N(c_2 - c_1)| \geq 1$ im Widerspruch zu (34). Es ist also

$$\mathrm{Vol}\,U_i' = \sum_{c \in R} \mathrm{Vol}\,((U_i + c) \cap \Phi) = \sum_{c \in R} \mathrm{Vol}\,(U_i \cap (\Phi - c)).$$

Da die Translationen von Φ um Elemente $c \in R$ nach Korollar 1.3.4 ganz $\mathbb{R}^n$ überdecken, gilt

$$\mathrm{Vol}\,U = \mathrm{Vol}\,U_i = \sum_{c \in R} \mathrm{Vol}\,(U_i \cap (\Phi - c)) = \mathrm{Vol}\,U_i',$$

d.h. das Volumen von U_i bleibt bei der Verschiebung in Φ erhalten.

Wegen $\sum_{i=1}^m \mathrm{Vol}\,U_i' > M_K \,\mathrm{Vol}\,U = \mathrm{Vol}\,\Phi$ existieren also $i \neq j$, sodaß sich U_i' und U_j' überschneiden. Es gibt also $u, u' \in U$, $c \in R$, sodaß

$$\frac{a}{b}\mu_i + u = \frac{a}{b}\mu_j + u' + c,$$

also

$$\frac{a}{b} - \frac{c}{\mu_i - \mu_j} = \frac{u' - u}{\mu_i - \mu_j}.$$

Wegen $|N(u' - u)| < 1$ ist $|N(\frac{u'-u}{\mu_i - \mu_j})| < \frac{1}{|N(\mu_i - \mu_j)|}$, d.h. $\frac{a}{b} \in E_{\frac{1}{(\mu_i - \mu_j)}} \cup \frac{1}{(\mu_i - \mu_j)}$. □

Es sei noch bemerkt, daß man mit Hilfe dieses Satzes ein endliches schwach Euklidisches System $M \subseteq Z^-$ erhält, indem man die $\mu_1, \mu_2, \ldots, \mu_m$ paarweise verschieden aus $\mathbb{Z}$ wählt.

Im folgenden sollen nun einige Hilfsmittel zusammengestellt werden, um Euklidische Systeme aus reziproken ganzen Hauptidealen zu konstruieren. Mit Hilfe des vorigen Satzes 3.3.1 können wir schon leicht ein endliches schwach Euklidisches System $M_0 \subseteq Z^-$ angeben, d.h.

$$K \subseteq \bigcup_{\frac{1}{(d)} \in M_0} E_{\frac{1}{(d)}} \cup \bigcup_{\frac{1}{(d)} \in M_0} \frac{1}{(d)}.$$

Dieses schwach Euklidische System M_0 können wir nun zu einem Euklidischen System $M \subseteq H^-$ erweitern, indem wir zu jedem der endlich vielen $d \in \mathbb{Z} \setminus \{0\}$ mit $\frac{1}{(d)} \in M_0$ ein endliches $M_d \subseteq H^-$ finden, sodaß

$$\frac{1}{(d)} \setminus R \subseteq E_{M_d}. \tag{35}$$

Dann folgt

$$K \subseteq \bigcup_{\frac{1}{d)} \in M_0} (E_{\frac{1}{(d)}} \cup E_{M_d}) \cup R,$$

und $M := M_0 \cup \bigcup_{\frac{1}{(d)} \in M_0} M_d$ ist endliches Euklidisches System.

LEMMA 3.3.2. *Seien $\alpha, \beta, \mu \in R$, $\beta \nmid \alpha$, mit $\frac{\alpha}{\beta} \in E_{\frac{1}{(\mu)}}$. Dann ist auch $\frac{\alpha'}{\beta} \in E_{\frac{1}{(\mu)}}$ für alle $\alpha' \equiv \alpha \pmod{\beta}$.*

BEWEIS. Sei $\lambda \in R$, sodaß $\alpha' = \alpha + \lambda\beta$. Dann ist $\frac{\alpha'}{\beta} = \frac{\alpha}{\beta} + \lambda \in E_{\frac{1}{(\mu)}}$, da $E_{\frac{1}{(\mu)}}$ nach Bemerkung 3.1.6 Fixgebiet bzgl. $\frac{1}{(\mu)}$, also erst recht bzgl. R ist. □

Um (35) nachzuweisen, reicht es also, für ein vollständiges Restsystem $0, \alpha_1, \dots, \alpha_l$ modulo d, $\alpha_i \not\equiv 0 \pmod{d}$,

$$\frac{\alpha_i}{d} \in E_{M_d} \quad \text{für } i = 1, 2, \dots, l$$

zu zeigen.

Insgesamt läßt sich die Konstruktion eines Euklidischen Systems $M \subseteq H^-$ also auf die Konstruktion eines $\mu \in R \backslash \{0\}$ mit $\frac{\alpha}{\beta} \in E_{\frac{1}{(\mu)}}$ für endlich viele Elemente $\frac{\alpha}{\beta} \in K \backslash R$ reduzieren. Nach Lemma 3.2.23 gibt es ein solches μ genau dann, wenn ein $\delta \in (\alpha, \beta)$, $\delta \neq 0$, mit $|N(\delta)| < |N(\beta)|$ existiert, und aus einer Darstellung $\delta = \mu\alpha + \lambda\beta$ mit $\lambda, \mu \in R$, $\mu \neq 0$, folgt nach Lemma 3.2.22 $\frac{\alpha}{\beta} \in E_{\frac{1}{(\mu)}}$. Im folgenden Satz aus Schulze [17] wird ein spezieller Ansatz für δ gewählt, sodaß sich μ in diesen Fällen mittels des Euklidischen Algorithmus in $\mathbb{Z}$ berechnen läßt.

SATZ 3.3.3 (SCHULZE). *Seien $\alpha, \beta \in R \backslash \{0\}$. Weiter seien $\alpha', \beta' \in R \backslash \{0\}$, sodaß*

$$a := \alpha\alpha', b := \beta\beta' \in \mathbb{Z} \backslash \{0\}.$$

(i) *Solche α', β' existieren stets (z.B. $a = N(\alpha), b = N(\beta)$).*
(ii) *Setze $\delta := \operatorname{ggT}(a, b)$. Mittels des Euklidischen Algorithmus in $\mathbb{Z}$ lassen sich $\lambda, \mu \in \mathbb{Z}$ konstruieren, sodaß $\delta = \mu a - \lambda b$. Gilt*

$$|\delta| < \sqrt[n]{|N(\beta)|}, \tag{36}$$

so ist $\mu \neq 0$ und $\frac{\alpha}{\beta} \in E_{\frac{1}{(\mu\alpha')}}$.

BEWEIS.

(i) Wegen $|N(\alpha)| = \mathcal{N}((\alpha)) \in (\alpha)$ existiert $\alpha' \in R \backslash \{0\}$, sodaß $\alpha\alpha' = N(\alpha) \in \mathbb{Z} \backslash \{0\}$. Analog ergibt sich β'.

(ii) Zunächst ist (36) wegen $\delta \in \mathbb{Z}$ äquivalent zu $|N(\delta)| < |N(\beta)|$. Hieraus folgt $b \nmid a$, denn sonst wäre $\delta = \pm b$ und $|N(\delta)| = |N(b)| \geq |N(\beta)|$. Damit ist auch $\mu \neq 0$, da sonst δ Vielfaches von b und damit $b|a$ wäre. Aus (36) folgt weiter

$$\left| N\left(\frac{\alpha}{\beta} - \frac{\lambda\beta'}{\mu\alpha'}\right)\right| = \left| N\left(\frac{a\mu - \lambda b}{\beta\mu\alpha'}\right)\right| = \left| N\left(\frac{\delta}{\beta\mu\alpha'}\right)\right| < \frac{1}{|N(\mu\alpha')|}.$$

Wegen $\delta \neq 0$ ist auch

$$0 < \left| N\left(\frac{\alpha}{\beta} - \frac{\lambda\beta'}{\mu\alpha'}\right)\right|,$$

also $\frac{\alpha}{\beta} \in E_{\frac{1}{(\mu\alpha')}}$.

□

Bemerkung 3.3.4. *Ist in Satz 3.3.3 $\beta \in \mathbb{Z}$, so folgt aus $\beta \nmid a$ bereits* (36).

Beweis. Man kann $b = \beta$ wählen, und $b \nmid a$ ist äquivalent zu $\mathrm{ggT}(a,b) \neq \pm b$, also wegen der Multiplikativität der Norm äquivalent zu $|N(\mathrm{ggT}(a,b))| < |N(b)|$. □

Eine weitere recht allgemeine Möglichkeit zur Konstruktion eines oben beschriebenen μ liefert der aus Schulze [17] stammende

Satz 3.3.5 (Schulze). *Sei $\frac{\alpha}{\alpha'} \in K \setminus R$, $\alpha, \alpha' \in R\setminus\{0\}$, eine reduzierte Darstellung, d.h. für alle Primelemente $\pi \in R$ mit $\pi|\alpha'$ gilt $\pi \nmid \alpha$. Weiter besitze der Nenner α' eine Zerlegung*

$$\alpha' = \beta\beta' \quad \textit{in } R \textit{ mit } \beta, \beta' \neq 0,\ \beta \textit{ keine Einheit,}$$

sodaß $1 \in (\alpha, \beta)$ und β Teiler einer Primzahl $p \in \mathbb{Z}$ ist.

(i) *Eine solche Zerlegung von α' existiert, falls α' einen Primfaktor $\pi \in R$ besitzt. Dies ist insbesondere der Fall, wenn die Klassenzahl $h = 1$ ist, da dann R ZPE-Ring ist.*
(ii) *Sei nun $K = \mathbb{Q}(\theta)$, $\theta \in R$, und $d \in \mathbb{Z}$, sodaß $\mathrm{disc}(\theta) = d^2 \,\mathrm{disc}\, R$. Gilt $p \nmid d$, so läßt sich ein $\mu \in R$ mit $\frac{\alpha}{\alpha'} \in E_{\frac{1}{(\mu)}}$ konstruieren.*

Beweis.

(i) Aus $\pi|\alpha'$ folgt $\pi \nmid \alpha$, da $\frac{\alpha}{\alpha'}$ nach Voraussetzung eine reduzierte Darstellung ist, d.h. $\alpha \notin (\pi)$. Weil (π) im Dedekindring R auch maximales Ideal ist, ist dann $1 \in (\alpha, \pi)$ und $\beta := \pi$ erfüllt die gewünschten Eigenschaften.
(ii) Wir konstruieren nun $\mu \in R$, sodaß $\frac{\alpha}{\beta} \in E_{\frac{1}{(\mu)}}$. Nach Bemerkung 3.1.8 folgt dann $\frac{\alpha}{\beta\beta'} \in E_{\frac{1}{(\mu\beta')}}$.

Es gilt nach Korollar 1.1.2 $R \subseteq \frac{\mathbb{Z}[\theta]}{d}$. Seien daher $f(x), g(x) \in \mathbb{Z}[x]$, sodaß

$$\alpha = \frac{f(\theta)}{d}, \quad \beta = \frac{g(\theta)}{d},$$

und weiter $h(x) := \operatorname{Irr}(\theta, \mathbb{Q})$. Für jedes $r(x) \in \mathbb{Z}[x]$ bezeichne $\overline{r}(x)$ das zugehörige Polynom mit $\mod p$ reduzierten Koeffizienten. Wir zeigen nun

$$\text{ggT}\,(\overline{f}(x), \overline{g}(x), \overline{h}(x)) = \overline{1} \quad \text{in } \mathbb{Z}_p[x]. \tag{37}$$

Wegen $1 \in (\alpha, \beta)$ existieren $r_1(x), r_2(x) \in \mathbb{Z}[x]$ mit

$$r_1(\theta)f(\theta) + r_2(\theta)g(\theta) = d^2,$$

d.h. $r_1(x)f(x) + r_2(x)g(x) - d^2 \in \mathbb{Z}[x]$ hat θ als Nullstelle und ist daher Vielfaches von $\operatorname{Irr}(\theta, \mathbb{Q})$. Also gibt es $r_3(x) \in \mathbb{Z}[x]$ mit

$$r_1(x)f(x) + r_2(x)g(x) + r_3(x)h(x) = d^2.$$

Wegen $p \nmid d$ ist $\overline{d} \neq \overline{0}$, also $\overline{d}$ im Körper $\mathbb{Z}_p$ invertierbar. Sei $d' \in \mathbb{Z}$, sodaß $\overline{d'} = \overline{d}^{-2} \neq \overline{0}$. Dann ist

$$\overline{d'r_1}(x)\overline{f}(x) + \overline{d'r_2}(x)\overline{g}(x) + \overline{d'r_3}(x)\overline{h}(x) = \overline{1}.$$

Damit ist (37) gezeigt.
Mittels des Euklidischen Algorithmus in $\mathbb{Z}_p[x]$ lassen sich also Polynome $\lambda_1(x), \lambda_2(x), \lambda_3(x), \lambda_4(x) \in \mathbb{Z}[x]$ bestimmen, sodaß

$$\lambda_1(x)f(x) + \lambda_2(x)g(x) + \lambda_3(x)h(x) = 1 + p\lambda_4(x),$$

also

$$(d\lambda_1(\theta))\,\alpha + \left(d\lambda_2(\theta) - \frac{p}{\beta}\lambda_4(\theta)\right)\beta = 1.$$

Wähle also $\mu := d\lambda_1(\theta)$, $\lambda := d\lambda_2(\theta) - \frac{p}{\beta}\lambda_4(\theta))$. Da β keine Einheit ist, folgt $\mu \neq 0$ und

$$0 < |N(\mu\alpha + \lambda\beta)| = 1 < |N(\beta)|,$$

d.h. $\frac{\alpha}{\beta} \in E_{\frac{1}{(\mu)}}$.

□

Bemerkung 3.3.6. *Bei Quadratischen Zahlkörpern kann in Satz* 3.3.5 *immer* $d = 1$ *gewählt werden, denn nach Satz* 1.1.1 *existiert eine Ganzheitsbasis der Form* $(1, \omega)$, *und damit ist* $\operatorname{disc}(\theta) = \operatorname{disc}(R)$. *Das bedeutet, daß sich für Quadratische Zahlkörper mit Klassenzahl* $h = 1$ *die Konstruktion für alle Elemente* $\frac{\alpha}{\alpha'} \in K \backslash R$ *durchführen läßt. Die Polynome* $f(x), g(x)$ *können zudem vom Grad* < 2 *gewählt werden.*

BEMERKUNG 3.3.7. *Hat man in Satz 3.3.5 eine Zerlegung, sodaß $\beta = p$ Primzahl ist, so läßt sich zur Konstruktion von μ auch Satz 3.3.3 anwenden.*

BEWEIS. Wir zeigen $p \nmid N(\alpha)$, dann sind nach Bemerkung 3.3.4 die Voraussetzungen von Satz 3.3.3 erfüllt.

Annahme: $p | N(\alpha)$. Sei $(\alpha) = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r$ die Primidealzerlegung von (α) in R, also

$$|N(\alpha)| = \mathcal{N}((\alpha)) = \mathcal{N}(\mathfrak{p}_1)\mathcal{N}(\mathfrak{p}_2)\dots\mathcal{N}(\mathfrak{p}_r).$$

Dann gilt $p | \mathcal{N}(\mathfrak{p}_i)$ für ein i. Es folgt $\mathfrak{p}_i \supseteq (p)$, also auch $\mathfrak{p}_i \supseteq (\alpha, p)$ im Widerspruch zur Voraussetzung $1 \in (\alpha, p)$. $\square$

Hat K die Klassenzahl $h = 1$, so existiert zu $\alpha, \beta \in R$ stets ein größter gemeinsamer Teiler $\mathrm{ggT}(\alpha, \beta)$, da R Hauptidealring ist. Dieser größte gemeinsame Teiler läßt sich mit Hilfe eines Euklidischen Systems $M \subseteq H^-$ berechnen.

BEMERKUNG 3.3.8. *Sei K Algebraischer Zahlkörper mit Klassenzahl $h = 1$ und $M \subseteq H^-$ Euklidisches System. Seien $\alpha, \beta \in R$ und o.B.d.A. $\alpha, \beta \neq 0$ und $|N(\alpha)| \geq |N(\beta)|$.*

Gilt $\beta | \alpha$, so ist $(\beta) = (\alpha, \beta)$. Sei also $\beta \nmid \alpha$. Weil M Euklidisches System ist, gibt es nach der Äquivalenz von (i) und (ii) in Lemma 3.2.22 Elemente $\lambda_1, \mu_1 \in R$ mit $\frac{1}{(\mu_i)} \in M$ und $0 < |N(\mu_1\alpha - \lambda_1\beta)| < |N(\beta)|$. Setzt man $\delta_1 := \mu_1\alpha - \lambda_1\beta$ so gilt

$$\mu_1\alpha = \lambda_1\beta + \delta_1, \quad 0 < |N(\delta_1)| < |N(\beta)|.$$

Wiederholte Anwendung von Lemma 3.2.22 liefert dann eine Sequenz von Gleichungen

$$\begin{aligned} \mu_1\alpha &= \lambda_1\beta + \delta_1, \\ \mu_2\alpha &= \lambda_2\delta_1 + \delta_2, \\ &\vdots \\ \mu_k\alpha &= \lambda_k\delta_{k-1} + \delta_k \end{aligned}$$

mit

$$0 < |N(\delta_k)| < \dots < |N(\delta_1)| < |N(\beta)|.$$

Dies läßt sich solange fortsetzen, bis $\delta_k | \alpha$ gilt. Da die $|N(\delta_i)|$ eine absteigende Kette in der wohlgeordneten Menge $\mathbb{N}$ bilden, wird $\delta_k | \alpha$ auch für ein endliches $k \in \mathbb{N}$ erreicht. Wegen $\delta_i \in (\alpha, \beta)$ und $\delta_i \neq 0$ für alle $i \in \{1, 2, \dots, k\}$, gilt also $(\alpha, \beta) = (\delta_k, \beta)$ mit $|N(\beta)| < |N(\alpha)|, |N(\delta_k)| < |N(\beta)|$. Ersetzt man nun α durch β und β durch δ_k, so hat man den Normbetrag der beiden erzeugenden Elemente α und β echt reduziert. Da $\mathbb{N}$ wohlgeordnet ist, liefert wiederholte Anwendung des gesamten Verfahrens also nach endlich vielen Schritten $\alpha', \beta' \in R$ mit $(\alpha, \beta) =$

(α', β') und $\beta'|\alpha'$ oder $|N(\beta')| = 0$. Im Fall $\beta'|\alpha'$ ist $(\alpha, \beta) = (\beta')$ und im Fall $|N(\beta)| = 0$ ist $\beta = 0$ und damit $(\alpha, \beta) = (\alpha')$.

3.4. Beispiele Euklidischer Systeme

In diesem Abschnitt sollen einige Beispiele für Euklidische Systeme quadratischer und kubischer Zahlkörper gegeben werden.

Zunächst betrachten wir das Beispiel des imaginär-quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{-19})$ aus Schulze [16]. In Beispiel 2.3.15 haben wir gesehen, daß $\mathbb{Q}(\sqrt{-19})$ nicht k-stufig Norm-Euklidisch ist. Nach Bemerkung 3.3.6 existiert aber sicher ein euklidisches System, und läßt sich wie folgt konstruieren.

Beispiel 3.4.1. Sei $K = \mathbb{Q}(\sqrt{d})$ mit $d = -19$. Dann ist

$$M = \left\{ \frac{1}{(\mu)} \,\middle|\, \mu = 1, 2, \frac{1-\sqrt{-19}}{2}, \frac{3-\sqrt{-19}}{2} \right\}$$

Euklidisches System. Da M nur aus Hauptidealen besteht, hat nach Satz 3.2.24 $\mathbb{Q}(\sqrt{-19})$ die Klassenzahl 1.

Beweis. R hat die Ganzheitsheitsbasis $(1, \omega)$ mit $\omega = \frac{1+\sqrt{-19}}{2}$, und die Diskriminante $\operatorname{disc}(K/\mathbb{Q}) = -19$. Als imaginär-quadratischer Zahlkörper hat K ein Paar komplex-konjugierter Einbettungen, d.h. $s = 1$. Also ist die Minkowski-Schranke

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K/\mathbb{Q})|} = \frac{2}{4}\left(\frac{4}{\pi}\right)^1 \sqrt{19} = \frac{2}{\pi}\sqrt{19} < 3.$$

Wählt man in Satz 3.3.1 $\mu_1 = 0, \mu_2 = 1, \mu_3 = 2$, so folgt, daß $M_0 := \left\{(1), \frac{1}{(2)}\right\}$ schwach Euklidisches System ist.

Es ist $0, 1, \omega, \omega + 1$ ein vollständiges Restsystem $\pmod 2$. Wegen $\frac{1}{2} \in E_{(1)}$ sind also noch geeignete $\mu_1, \mu_2 \in R$ gesucht mit $\frac{\omega}{2} \in E_{\frac{1}{(\mu_1)}}$ und $\frac{1+\omega}{2} \in E_{\frac{1}{(\mu_2)}}$, dann ist $M_0 \cup \left\{\frac{1}{(\mu_1)}, \frac{1}{(\mu_2)}\right\}$ Euklidisches System. Die μ_1, μ_2 berechnen wir nun mit Satz 3.3.3.

Es ist $\frac{\omega}{2} = \frac{1+\sqrt{-19}}{4}$. Sei also $\alpha = 1+\sqrt{-19}$, $\beta = 4$. Für $\alpha' := 1-\omega = \frac{1-\sqrt{-19}}{2} \in R$ ist $a := \alpha\alpha' = \frac{1+19}{2} = 10 \in \mathbb{Z}$. Also gilt $\beta \nmid a$ mit $\beta \in \mathbb{Z}$ und nach Bemerkung 3.3.4 sind die Voraussetzungen von Satz 3.3.3 erfüllt. Man kommt sofort auf die Darstellung $\operatorname{ggT}(a, b) = 2 = 1a - 2\beta$, d.h. $\frac{\alpha}{\beta} \in E_{\frac{1}{(\alpha')}} = E_{\frac{1}{(1-\omega)}}$.

Es ist $\frac{1+\omega}{2} = \frac{3+\sqrt{-19}}{4}$. Sei also $\alpha = 3+\sqrt{-19}$, $\beta = 4$. Für $\alpha' := 2 - \omega = \frac{3-\sqrt{-19}}{2} \in R$ ist $a := \alpha\alpha' = \frac{9+19}{2} = 14 \in \mathbb{Z}$. Also gilt $\beta \nmid a$ mit $\beta \in \mathbb{Z}$ und nach Bemerkung 3.3.4 sind die Voraussetzungen von Satz 3.3.3 erfüllt. Man kommt sofort auf die Darstellung $\operatorname{ggT}(a, b) = 2 = 1a - 3\beta$, d.h. $\frac{\alpha}{\beta} \in E_{\frac{1}{(\alpha')}} = E_{\frac{1}{(2-\omega)}}$.

Der Beweis läßt sich mit Hilfe von Abbildung III.3 auch geometrisch führen. Darin ist die Menge

$$\Psi := \left\{ \lambda_1 + \lambda_2\omega \;\middle|\; \lambda_1, \lambda_2 \in \mathbb{Q}, 0 \leq \lambda_1 < 1, 0 \leq \lambda_2 \leq \frac{1}{2} \right\},$$

die nach Beispiel 1.4.13 K-Überdeckungsgebiet bzgl. R ist, grau unterlegt eingezeichnet. Man sieht, daß gilt

$$\Psi \backslash \left\{0, \frac{\omega}{2}, \frac{1+\omega}{2}\right\} \subseteq E_R(0) \cup E_R(1) \cup E_{\frac{1}{(2)}}\left(\frac{\omega}{2}\right) \cup E_{\frac{1}{(2)}}\left(\frac{\omega+1}{2}\right),$$

d.h. $\left\{(1), \frac{1}{(2)}\right\}$ ist schwach euklidisches System. Wie in Beispiel 3.1.12 sind die Euklidischen Mengen das Innere der gezeichneten Kreise ohne die jeweiligen Mittelpunkte. Dabei sind die zu R gehörigen Euklidischen Mengen das Innere der mit durchgezogener Linie gezeichneten Kreise vom Radius $\sqrt{|N(1)|} = 1$, und die zu $\frac{1}{(2)}$ gehörigen Euklidischen Mengen das Innere der grob gestrichelt eingezeichneten Kreise vom Radius $\sqrt{|N(\frac{1}{2})|} = \frac{1}{2}$.

Weiter ist $\frac{1}{(1-\omega)} = \frac{\omega}{5} \in \frac{1}{(1-\omega)}$ und $\frac{3}{(2-\omega)} = \frac{9+3\sqrt{-19}}{14} \in \frac{1}{(2-\omega)}$, und man sieht leicht $\frac{\omega}{2} \in E_{\frac{1}{(1-\omega)}}(\frac{\omega}{5})$ und $\frac{1+\omega}{2} \in E_{\frac{1}{(2-\omega)}}(\frac{9+3\sqrt{-19}}{14})$.

Die zu $\frac{1}{(1-\omega)}$ und $\frac{1}{(2-\omega)}$ gehörigen Euklidischen Mengen sind dabei das Innere der fein gestrichelt eingezeichneten Kreise vom Radius $\sqrt{|N(\frac{1}{1-\omega})|} = \frac{1}{\sqrt{5}}$ bzw. $\sqrt{|N(\frac{1}{2-\omega})|} = \frac{1}{\sqrt{7}}$. $\square$

Wir zeigen nun noch, daß u.a. für $\mathbb{Q}(\sqrt{-19})$ kein Euklidisches System $M \subseteq Z^-$ existiert.

Bemerkung 3.4.2. *Sei K ein imaginär-quadratischer Zahlkörper, $K = \mathbb{Q}(\sqrt{d})$ mit $d < 0$, d quadratfrei. Dann besitzt K ein Euklidisches System $M \subseteq Z^-$ genau dann, wenn $d = -1, -2, -3, -7, -11$ ist (d.h. nach Beispiel 2.4.2 wenn K Norm-Euklidisch ist).*

Beweis. Wir nehmen an, es existiere ein Euklidisches System $M \subseteq Z^-$ und zeigen $d > -4$, falls $d \equiv 2, 3 \pmod 4$, bzw. $d > -15$, falls $d \equiv 1 \pmod 4$. Dann ist die Behauptung bewiesen.

1. Fall: $d \equiv 2, 3 \pmod 4$. Es ist $(1, \sqrt{d})$ Ganzheitsbasis von R, also $\alpha := \frac{\sqrt{d}}{2} \notin R$. Da $M \subseteq Z^-$ Euklidisches System ist, gibt es $c \in \mathbb{Z}$, $\lambda \in R$ mit $\frac{1}{(c)} \in M$ und

$$0 < \left| N\left(\frac{\sqrt{d}}{2} + \frac{\lambda}{c}\right) \right| = \left| N\left(\frac{c\sqrt{d} + 2\lambda}{2c}\right) \right| < \frac{1}{|N(c)|}.$$

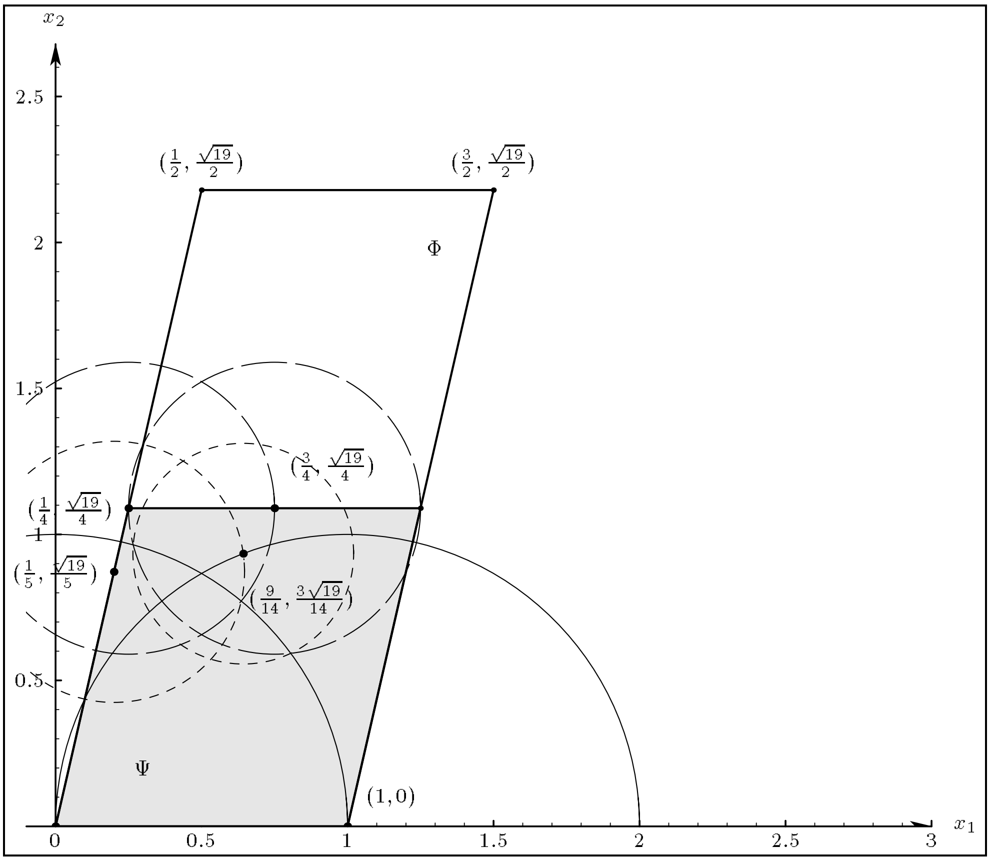

Abbildung III.3. Der Zahlkörper $\mathbb{Q}(\sqrt{-19})$

Sei $\lambda = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$. Dann folgt

$$0 < |N(c\sqrt{d} + 2\lambda)| = |4a^2 - d(2b+c)^2| < 4.$$

Wegen $d < 0$ ergibt sich $a = 0$ und damit $2b + c \neq 0$. Also ist $-d < \frac{4}{(2b+c)^2} \leq 4$.

2. Fall : $d \equiv 1 \pmod 4$. Dann ist $(1, \frac{1+\sqrt{d}}{2})$ Ganzheitsbasis von R, also $\alpha := \frac{1+\sqrt{d}}{4} \notin R$. Da $M \subseteq Z^-$ Euklidisches System ist, gibt es $c \in \mathbb{Z}$, $\lambda \in R$ mit $\frac{1}{(c)} \in M$ und

$$0 < \left| N\left(\frac{1+\sqrt{d}}{4} + \frac{\lambda}{c}\right)\right| = \left| N\left(\frac{c + c\sqrt{d} + 4\lambda}{4c}\right)\right| < \frac{1}{|N(c)|}.$$

Sei $\lambda = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$. Dann folgt

$$0 < |N(c\sqrt{d} + c + 4\lambda)| = |(4a+c)^2 - d(4b+c)^2| < 16. \tag{38}$$

Es ist $c \not\equiv 0 \pmod 4$, denn aus $c \equiv 0 \pmod 4$ folgt $(4a+c)^2 - d(4b+c)^2 \equiv 0 \pmod{16}$ im Widerspruch zu (38). Also sind $(4a+c)^2, (4b+c)^2 \geq 1$ und wegen $d < 0$ folgt daher aus (38) $-d < 15$. □

Jetzt wollen wir kubische Zahlkörper untersuchen und beginnen mit dem Beipiel des kubischen Zahlkörpers mit der Diskriminante -199 aus Schulze [16].

Beispiel 3.4.3. Der kubische Zahlkörper der Diskriminante -199, der von einer Nullstelle von $h(x) := x^3 + x^2 + 4x + 1$ erzeugt wird, ist nach Taylor [18] nicht Norm-Euklidisch, hat aber das Euklidische System

$$M = \left\{(1), \frac{1}{(2)}, \frac{1}{(3)}\right\},$$

also insbesondere die Klassenzahl 1.

Beweis. Wir rechnen zunächst nach, daß $K = \mathbb{Q}(\theta)$ für eine Nullstelle θ von $h(x)$ tatsächlich die Diskriminante -199 hat. Die formale Ableitung von $h(x)$ ist

$$h'(x) = 3x^2 + 2x + 4,$$

also ist nach den Rechenregeln für Diskriminanten

$$\operatorname{disc}(\theta) = (-1)^{\frac{n(n-1)}{2}} N(h'(\theta)) = (-1)^3 N(3\theta^2 + 2\theta + 4).$$

Wegen $\theta^3 = -\theta^2 - 4\theta - 1$ hat die Multiplikation mit $3\theta^2 + 2\theta + 4$ als lineare Abbildung im $\mathbb{Q}$-Vektorraum K bzgl. der Basis $(1, \theta, \theta^2)$ die Matrix $\begin{pmatrix} 4 & -3 & -1 \\ 2 & -8 & 1 \\ 3 & -1 & -7 \end{pmatrix}$, d.h. es ist

$$N(3\theta^2+2\theta+4) = \begin{vmatrix} 4 & -3 & -1 \\ 2 & -8 & 1 \\ 3 & -1 & -7 \end{vmatrix} = 199.$$

Da $\operatorname{disc}(\theta)$ quadratfrei ist, folgt schon $\operatorname{disc}(K/\mathbb{Q}) = \operatorname{disc}(\theta)$ und $(1,\theta,\theta^2)$ ist Ganzheitsbasis von R.

Seien $\theta_1 = \theta, \theta_2, \theta_3$ die Konjugierten zu θ. Bekanntlich [13] ist

$$\operatorname{disc}(\theta) = \begin{vmatrix} 1 & 1 & 1 \\ \theta_1 & \theta_2 & \theta_3 \\ \theta_1^2 & \theta_2^2 & \theta_3^2 \end{vmatrix}^2 = \prod_{1\le j<i\le 3} (\theta_i-\theta_j)^2.$$

Da $\operatorname{disc}(\theta)$ negativ ist, müssen also komplexe Konjugierte von θ auftreten, also hat K ein Paar komplex-konjugierter Einbettungen. Das bedeutet $s=1$, und die Minkowski-Schranke ist

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K/\mathbb{Q})|} = \frac{2}{9}\left(\frac{4}{\pi}\right)\sqrt{199} < 4.$$

Wählt man in Satz 3.3.1 $\mu_1 = 0, \mu_2 = 1, \mu_3 = 2, \mu_4 = 3$, so folgt, daß $M_0 := \left\{(1), \frac{1}{(2)}, \frac{1}{(3)}\right\}$ schwach Euklidisches System ist. Wir zeigen jetzt $\frac{1}{(2)}\backslash R \subseteq E_{(1)}$ und $\frac{1}{(3)}\backslash R \subseteq E_{(1)}$, dann ist M_0 sogar Euklidisches System.

Sei $\frac{\alpha}{2} \in \frac{1}{(2)}\backslash R$, d.h. $2\nmid\alpha$. Nach Lemma 3.2.22 bedeutet $\frac{\alpha}{2} \in E_{(1)}$ gerade, daß die Nebenklasse $\alpha+(2)$ ein Element mit Normbetrag $< |N(2)| = 8$ enthält. Zu zeigen ist also, daß jede von Null verschiedene Nebenklasse mod 2 ein Element mit Normbetrag $< |N(2)| = 8$ enthält. Da $h(x)$ mod 2 irreduzibel ist, ist (2) nach dem Satz von Dedekind über die Primidealzerlegung Primideal, d.h. $R/2R$ ist Körper der Ordnung $|N(2)| = 8$. Die multiplikative Gruppe von $R/2R$ ist zyklisch der Ordnung 7, und da 7 Primzahl ist wird sie von jeder von Null und Eins verschiedenen Restklasse erzeugt. Da $(1,\theta,\theta^2)$ Ganzheitsbasis von R ist, gilt $2\nmid\theta, \theta-1$, denn die Koeffizienten der Basiselemente von θ und $\theta-1$ sind nicht durch 2 teilbar. Also ist $\theta \not\equiv 0,1 \pmod 2$, d.h. $\theta+(2)$ erzeugt die multiplikative Gruppe von $R/2R$. Es ist aber θ Einheit, denn $\theta(-\theta^2-\theta-4) = 1$, d.h. in jeder Nebenklasse mod 2 liegt sogar eine Einheit, also ein Element mit Normbetrag $= 1$.

Um weiter $\frac{\alpha}{3} \in E_{(1)}$ zu zeigen, geben wir ein vollständiges Restsystem mod 3 aus Elementen mit Normbetrag < 27 an. Dazu betrachten wir einige Elemente mit möglichst kleinem Normbetrag, hier θ, $\alpha := \theta+1$, $\beta := \theta-1$ und $\gamma := \theta^2+4$

[13] vgl. Marcus [13], Chapter 2, Theorem 8, Seite 26

mit $N(\theta) = 1$, $N(\alpha) = 7, N(\beta) = -3$ und $N(\gamma) = 9$ und versuchen durch Produktbildung dieser Elemente ein vollständiges Restsystem mod 3 zu erlangen.

Element	mod 3 reduzierte Koeffizienten bzgl. $(1, \theta, \theta^2)$
1	$1, 0, 0$
θ	$0, 1, 0$
θ^2	$0, 0, 1$
θ^3	$2, 2, 2$
α	$1, 1, 0$
$\alpha\theta$	$0, 1, 1$
β	$2, 1, 0$
$\beta\theta$	$0, 2, 1$
$\beta\theta^2$	$2, 2, 1$
$\beta\theta^3$	$2, 1, 1$
γ	$1, 0, 1$
$\beta\alpha$	$2, 0, 1$
$\beta\alpha\theta$	$2, 1, 2$

Man prüft leicht nach, daß diese Elemente zusammen mit ihren Negativen und der 0 ein vollständiges Restsystem modulo 3 bilden und allesamt den Normbetrag < 27 haben. $\square$

Beispiel 3.4.4. Der kubische Zahlkörper der Diskriminante -307, der von einer Nullstelle von $h(x) := x^3 + x^2 + 3x - 2$ erzeugt wird, ist nach Taylor [18] nicht Norm-Euklidisch, hat aber das Euklidische System

$$M = \left\{(1), \frac{1}{(2)}, \frac{1}{(3)}, \frac{1}{(4)}, \frac{1}{(2\theta^2 + 5\theta + 7)}\right\},$$

also insbesondere die Klassenzahl 1.

Beweis. Sei θ eine Nullstelle von $h(x)$. Dann hat $K = \mathbb{Q}(\theta)$ die Diskriminante -307 und $(1, \theta, \theta^2)$ ist Ganzheitsbasis. Für die Minkowski-Schranke gilt

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K/\mathbb{Q})|} = \frac{2}{9} \left(\frac{4}{\pi}\right) \sqrt{307} < 5.$$

Wählt man in Satz 3.3.1 $\mu_i = i$ für $i = 1, 2, \ldots, 5$, so folgt, daß $M_0 := \left\{(1), \frac{1}{(2)}, \frac{1}{(3)}, \frac{1}{(4)}\right\}$ schwach Euklidisches System ist. Wir zeigen, daß für $M_1 := \left\{(1), \frac{1}{(2\theta^2+5\theta+7)}\right\}$ bereits $\frac{1}{(i)} \backslash R \subseteq E_{M_1}$ für $i = 2, 3, 4$ gilt.

Zunächst zeigen wir $\frac{1}{(3)} \backslash R \subseteq E_{(1)}$. Dazu schreiben wir uns die zunächst die Restklasen mod 3 (ohne die Nullklasse) hin und versuchen durch Probieren möglichst "einfache" Nebenklassenvertreter mit Normbetrag < 27 zu finden. Dabei kommt man z.B. auf die folgenden Elemente :

Element	Normbetrag	mod 3 reduzierte Koeffizienten bzgl. $(1, \theta, \theta^2)$
1	1	$1, 0, 0$
θ	2	$0, 1, 0$
$\theta + 1$	5	$1, 1, 0$
$\theta + 2$	12	$2, 1, 0$
θ^2	4	$0, 0, 1$
$\theta^2 + 1$	13	$1, 0, 1$
$\theta^2 + 2$	18	$2, 0, 1$
$\theta^2 + \theta$	10	$0, 1, 1$
$\theta^2 + \theta + 1$	12	$1, 1, 1$
$\theta^2 + \theta + 2$	8	$2, 1, 1$
$\theta^2 + 2\theta$	24	$0, 2, 1$
$\theta^2 + 2\theta + 1$	25	$1, 2, 1$
$\theta^2 + 2\theta + 2$	18	$2, 2, 1$

Man sieht sofort, daß diese Elemente zusammen mit ihren Negativen und der 0 ein vollständiges Restsystem modulo 3 bilden. Mit Lemma 3.2.22 folgt dann $\frac{1}{(3)}\backslash R \subseteq E_{(1)}$.

Wir zeigen nun $\frac{1}{(4)}\backslash R \subseteq E_{M_1}$, dann folgt auch $\frac{1}{(2)}\backslash R \subseteq E_{M_1}$.

Dazu gehen wir genauso vor wie oben, und versuchen durch Probieren ein vollständiges Restsystem modulo 4 aus Elementen mit Normbetrag < 64 zu finden. Dabei kommt man z.B. auf die folgenden Elemente :

Element	Normbetrag	mod 2 reduzierte Koeffizienten bzgl. $(1, \theta, \theta^2)$
1	1	$1, 0, 0$
2	8	$2, 0, 0$
θ	2	$0, 1, 0$
$\theta + 1$	5	$1, 1, 0$
$\theta + 2$	12	$2, 1, 0$
$\theta - 1$	3	$3, 1, 0$
2θ	16	$0, 2, 0$
$2\theta + 1$	1	$1, 2, 0$
$2\theta + 2$	40	$2, 2, 0$
θ^2	4	$0, 0, 1$
$\theta^2 + 1$	13	$1, 0, 1$
$\theta^2 + 2$	18	$2, 0, 1$
$\theta^2 - 1$	15	$3, 0, 1$
$\theta^2 + \theta - 4$	6	$0, 1, 1$
$\theta^2 + \theta$	10	$0, 1, 1$
$\theta^2 + \theta + 1$	12	$1, 1, 1$
$\theta^2 + \theta + 2$	8	$2, 1, 1$
$\theta^2 + \theta - 1$	4	$3, 1, 1$
$\theta^2 + 2\theta + 4$	4	$0, 2, 1$
$\theta^2 + 2\theta$	24	$0, 2, 1$
$\theta^2 + 2\theta + 1$	25	$1, 2, 1$
$\theta^2 + 2\theta + 2$	18	$2, 2, 1$
$\theta^2 + 2\theta - 1$	9	$3, 2, 1$
$\theta^2 - \theta$	6	$0, 3, 1$
$\theta^2 - \theta + 1$	16	$1, 3, 1$
$\theta^2 - \theta + 2$	36	$2, 3, 1$
$\theta^2 - \theta - 1$	36	$3, 3, 1$
$2\theta^2$	32	$0, 0, 2$
$2\theta^2 + 1$	37	$1, 0, 2$
$-2\theta^2 + \theta$	2	$0, 1, 2$
$2\theta^2 - 3\theta + 1$	3	$1, 1, 2$
$-2\theta^2 + 5\theta - 2$	16	$2, 1, 2$
$2\theta^2 + \theta - 1$	5	$3, 1, 2$
$2\theta^2 + 2\theta - 8$	48	$0, 2, 2$
$-2\theta^2 - 2\theta - 7$	31	$1, 2, 2$
$2\theta^2 + 2\theta + 6$	32	$2, 2, 2$

Bis auf die von $2\theta^2 + 2$ erzeugte Nebenklasse bilden diese Elemente zusammen mit ihren Negativen und der Null ein vollständiges Restsystem mod 4. Es liegt aber $\frac{2\theta^2+2}{4} = \frac{\theta^2+1}{2}$ in $E_{\frac{1}{(\mu)}}$ mit $\mu := 2\theta^2 + 5\theta + 7$, denn

$$0 < \left| N\left(\frac{\theta^2+1}{2} - \frac{6}{\mu}\right) \right| = \left| N\left(\frac{(\theta^2+1)\mu - 12}{2\mu}\right) \right| = \left| N\left(\frac{13-12}{2\mu}\right) \right| < \frac{1}{|N(\mu)|}.$$

Auf die Wahl von μ kommt man wie folgt mit Hilfe von Satz 3.3.3. Setze $\alpha := \theta^2 + 1$, $b := 2$. Dann ist $a := N(\alpha) = 13$ und $\operatorname{ggT}(a, b) = 1$. Setze $\alpha' := \frac{a}{\alpha} = 2\theta^2 + 5\theta + 7$. Aus der Darstellung $1 = 1a - 6b$ folgt nach Satz 3.3.3

$$\frac{\alpha}{b} \in E_{\frac{1}{(\alpha')}}.$$

Also folgt $\frac{1}{(4)} \backslash R \subseteq E_{M_1}$ und M ist euklidisches System. $\square$

Literaturverzeichnis

[1] J. Blöhmer, *Euklidische Ringe*, Diplomarbeit TU Berlin, 1989

[2] S.I. Borewics, J.R. Šafarevič, *Zahlentheorie*, Birkhäuser, Basel Stuttgart, 1966

[3] H. Chatland, H. Davenport, *Euclids algorithm in real quadratic fields*, Canad. J. Math. 2 (1950), 289-296

[4] D.A. Clark, *A quadratic field which is euclidean but not norm-euclidean*, Manuscripta math. 83 (1994), 389-398

[5] P.M. Cohn, *On the Structure of the* GL_2 *of a ring*, I.H.E.S. Publ. Math. 30 (1966), 365-413

[6] G. Cooke, *The weakening of the euclidean property for integral domains and applications to algebraic number fields I*, J. Reine Angew. Math. 282 (1976), 133-156

[7] G. Cooke, *The weakening of the euclidean property for integral domains and applications to algebraic number fields II*, J. Reine Angew. Math. 283 (1977), 71-85

[8] G.H.Hardy, E.M.Wright, *An introduction to the theory of numbers*, Oxford University Press, 1938

[9] H. Koch, H. Pieper, *Zahlentheorie*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1976

[10] F. Lemmermeyer, *Euclidean Number Fields*, Universität Heidelberg, 1995

[11] H.W. Lenstra jr., *Euclidean ideal classes*, Asterisque 61 (1979), 121-131 (Journées Arihmetiques de Luminy)

[12] F.J. van der Linden, *Euclidean number rings with two infinite primes*, Ph.D. thesis, Univ. Amsterdam, 1984

[13] D.A. Marcus, *Number Fields*, Springer, New York, 1977

[14] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin Heidelberg, 1992

[15] H. Pollard, *The theory of algebraic numbers*, Carus Monograph 9, MAA, Wiley, New York, 1950

[16] V. Schulze, *Verallgemeinerte Euklidische Algorithmen*, Arch. Math. 64 (1995), 313-315

[17] V. Schulze, *Verallgemeinerte Euklidische Algorithmen*, Preprint, FU Berlin 1995

[18] E.M. Taylor, *Euclid's Algorithm in cubic fields with complex conjugates*, J. London Math. Soc. (2) 14 (1976), 49-54