Verallgemeinerte Euklidische Algorithmen

Preprint der FU Berlin Nr. A-3/95

Volker Schulze

1. Es sei K ein algebraischer Zahlkörper und R der Ring der ganzen Zahlen von K.Bekanntlich heißt R norm-euklidischer Ring (bzw. K norm-euklidischer Zahlkörper), wenn für alle $a, b \in R$ mit $b \neq 0$ und $b \nmid a$ stets ein $\lambda \in R$ existiert mit $0 <\mid N(a - \lambda * b) \mid<\mid N(b) \mid$. Dabei bezeichne N die Absolutnorm.Wegen der Multiplikativität von N ist hierzu gleichwertig,daß zu jedem $\alpha \in K \backslash R$ ein $\lambda \in R$ existiert mit $0 <\mid N(\alpha - \lambda) \mid< 1$. Viele euklidische Zahlkörper wurden gefunden durch die von Lenstra [5] eingeführte Methode der Ausnahmeeinheiten (s.[7],[8]).Es liegt nahe, die euklidische Bedingung abzuschwächen.So hat Cooke in [2],[3] sogenannte mehrstufige euklidische Algorithmen eingeführt,deren Existenz leichter nachzuweisen ist,aber trotzdem Klassenzahl $h = 1$ zur Folge hat und Lenstra [6] euklidische Ideale,die von van der Linden [9] näher untersucht wurden.In der vorliegenden Arbeit werden Abschwächungen der euklidischen Bedingung betrachtet,aus denen die oben erwähnten Ansätze als Spezialfälle hervorgehen.

Es sei $\mathfrak{c}$ ein (gebrochenes) Ideal von K und $\alpha \in K \setminus \mathfrak{c}$.Dann wird α euklidischer Punkt von $\mathfrak{c}$ genannt,wenn ein $c \in \mathfrak{c}$ existiert mit $\mid N(\alpha - c) \mid< N(\mathfrak{c})$.Die Menge $E_\mathfrak{c}$ aller euklidischen Punkte von $\mathfrak{c}$ wird als euklidische Menge von $\mathfrak{c}$ bezeichnet.Offenbar gilt $E_\mathfrak{c} + c = E_\mathfrak{c}$ für alle $c \in \mathfrak{c}$.Ist M eine Menge von (gebrochenen) Idealen von K,so heißt $E_M := \bigcup_{\mathfrak{c} \in M} E_\mathfrak{c}$ euklidische Menge von M.Offenbar ist R norm-euklidischer Ring genau dann,wenn $E_R \cup R = K$ ist.Ein (gebrochenes) Ideal $\mathfrak{c}$ mit $E_\mathfrak{c} \cup \mathfrak{c} = K$ heißt euklidisches Ideal und erzeugt nach Lenstra die Idealklassengruppe von K.Dies ergibt sich aus

Lemma 1 (Lenstra [6]):Sei $\mathfrak{a}$ ein ganzes Ideal und $\mathfrak{c}$ ein beliebiges Ideal von K.Dann ist

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

gleichwertig damit,daß ein $d \in K$ und ein ganzes Ideal $\mathfrak{b}$ von R existiert mit

$$N(\mathfrak{b}) < N(\mathfrak{a}) \qquad \text{und} \qquad \mathfrak{b} * \mathfrak{c} = (d) * \mathfrak{a}.$$

Die obige Aussage von Lenstra über euklidische Ideale wird verallgemeinert auf Mengen von Idealen.

Satz 1 (a)Sei M eine Menge von (gebrochenen) Idealen von K und $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c}$.Ferner sei P die Menge aller Primideale $\mathfrak{p}$ von K mit $\frac{\mathfrak{m}}{\mathfrak{p}} \cap E_M = \phi$.Dann ist $P \cup M$ ein Erzeugenden-System für die Idealklassengruppe $C(K)$ von K.
(b)Sei $[K : \mathbb{Q}] = n, s$ die Anzahl der Paare konjugiert-komplexer Einbettungen von K in $\mathbb{C}$ und $M(K) = \frac{n!}{n^n}(\frac{4}{\pi})^s \sqrt{\mid diskrK \mid}$. Ferner sei $\mathfrak{c}$ ein beliebiges Ideal $\neq (0)$ von K.Für jedes ganze Ideal $\mathfrak{a}$ mit $N(\mathfrak{a}) > M(K)$ gilt dann $\frac{\mathfrak{c}}{\mathfrak{a}} \cap E_\mathfrak{c} \neq \phi$.

Beweis: (a)Sei $\mathfrak{q}$ ein ganzes Ideal mit minimaler Norm,deren Idealklasse nicht von $P \cup M$ erzeugt wird.Dann ist $\mathfrak{q}$ Primideal und $\mathfrak{q} \notin P$,also $\frac{\mathfrak{m}}{\mathfrak{q}} \cap E_M \neq \phi$. Für ein geeignetes $\mathfrak{c} \in M$ gilt dann

$\frac{\mathfrak{c}}{\mathfrak{q}} \cap E_{\mathfrak{c}} \neq \phi$ und nach Lemma 1 existiert ein $d \in K$ und ein ganzes Ideal $\mathfrak{b}$ von R mit $N(\mathfrak{b}) < N(\mathfrak{q})$ und $\mathfrak{b} * \mathfrak{c} = (d) * \mathfrak{q}$. Wegen der Minimalität der Norm von $\mathfrak{q}$ wird die Idealklasse $[\mathfrak{b}]$ erzeugt von $P \cup M$.Dies ein Widerspruch.

(b)Nach der Gitterpunkttheorie von Minkowski enthält $\frac{\mathfrak{c}}{\mathfrak{a}}$ ein Element α mit

$$\mid N(\alpha) \mid \leq M(K) * N(\frac{\mathfrak{c}}{\mathfrak{a}}) < N(\mathfrak{c}).$$

Es folgt $\alpha \in E_{\mathfrak{c}}$,da $E_{\mathfrak{c}}$ trivialerweise alle Elemente aus K mit Normbetrag $< N(\mathfrak{c})$ enthält.

Natürlich ist die Aussage von Satz 1(a) nur sinnvoll für $\mathfrak{m} \neq (0)$.Teil (b) besagt,daß in Teil (a) nur Primideale $\mathfrak{p}$ mit Norm $\mathfrak{p} \leq M(K)$ berücksichtigt werden müssen.Dies ist natürlich auch klar aufgrund der bekannten Aussage,daß in jeder Idealklasse ein ganzes Ideal mit Norm $\leq M(K)$ liegt (was wiederum für $\mathfrak{c} = (1)$ aus Satz 1(b) und Lemma 1 folgt).

2. In diesem Abschnitt wird ein Spezialfall von Satz 1 betrachtet. Nach Definition gilt stets $E_M \cap \mathfrak{m} = \phi$.Untersucht werden Mengen M von Idealen von K mit $E_M \cup \mathfrak{m} = K$ und $\mathfrak{m} \neq (0)$.In diesem Fall wird M euklidisches System (von Idealen von K) genannt.
Offenbar ist $\mathfrak{a}$ euklidisches Ideal im Sinne von Lenstra [6] genau dann,wenn $\{\mathfrak{a}\}$ euklidisches System ist und R norm-euklidischer Ring genau dann,wenn $\{(1)\}$ euklidisches System ist.
Aus Satz 1(a) ergibt sich unmittelbar

Satz 2 Ist M euklidisches System,so erzeugt M die Idealklassengruppe $C(K)$.

Die Frage,ob jeder Zahlkörper ein euklidisches System besitzt, bleibt ungeklärt.Von besonderem Interesse sind euklidische Systeme,welche nur Hauptideale enthalten.Existiert ein solches System,so ist nach Satz 2 die Klassenzahl $h = 1$.Auch die Umkehrung ist richtig. Allgemeiner gilt

Bemerkung 1 Sei $H = \{\frac{1}{(\mu)} \mid \mu \in R, \mu \neq 0\}$.Dann sind folgende Aussagen gleichwertig:

(a) H ist euklidisches System (d.h. $E_H \cup R = K$)

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

$$0 <\mid N(\mu * a - \lambda * b) \mid<\mid N(b) \mid \qquad (\text{bzw. } 0 <\mid N(\frac{a}{b} - \frac{\lambda}{\mu}) \mid< \frac{1}{\mid N(\mu) \mid}).$$

(c) R ist Hauptidealring.

Beweis: Die Gleichwertigkeit von (a) und (b) ergibt sich direkt aus der Definition von E_H.Die Äquivalenz von (b) und (c) ist bekannt als Dedekind-Hasse-Kriterium (s.Pollard [11]) und ergibt sich leicht wie folgt: Nach Satz 2 folgt (c) aus (a).Sei R Hauptidealring und $a, b \in R, b \neq 0$, $b \nmid a, (d) = (a, b)$.Dann existieren $\lambda, \mu \in R$ mit $\mu * a - \lambda * b = d$,und es gilt $\mid N(d) \mid<\mid N(b) \mid$.

Läßt man in Bemerkung 1(b) nur den Fall $\mu = 1$ zu,so erhält man die übliche euklidische Bedingung.Offenbar verallgemeinert die Bedingung (b) auch das Konzept des mehrstufigen euklidischen Algorithmus im Sinne von Cooke ([2],[3]),bei dem nur gewisse λ zugelassen werden.Ist $H' \subseteq H$ ein endliches euklidisches System,so genügt es in Bemerkung 1(b) nur endlich viele verschiedene $\mu \in R$ zuzulassen.Auf die Frage,wann ein endliches euklidisches Teilsystem existiert,wird am Ende dieses Abschnitts eingegangen.

Allgemein gilt für jeden Zahlkörper mit der Ganzheitsbasis $\omega_1, \cdots, \omega_n$ über $\mathbb{Q}$

Satz 3 E_H enthält $\{\lambda_1 * \omega_1 + \cdots + \lambda_n * \omega_n \mid 0 \leq \lambda_i < 1, \lambda_i \in \mathbb{Q}\}$ bis auf höchstens endlich viele Elemente.

Enthält E_H die Menge $\{\lambda_1 * \omega_1 + \cdots + \lambda_n * \omega_n \mid 0 \leq \lambda_i < 1, \lambda_i \in \mathbb{Q}\}$ bis auf n Elemente,so gilt $h \leq n+1$.

Diese Aussage ist ein Spezialfall von Proposition 24 von Cooke [3].Ein kurzer Beweis ergibt sich wie folgt: Für ein Element $\gamma = \frac{\alpha}{\beta} \notin R$ $(\alpha, \beta \in R)$ gilt $\gamma \notin E_H$ offenbar genau dann,wenn (α, β) nicht Hauptideal ist und β ein Element mit minimalem Normbetrag aus (α, β).Nach der Gitterpunkttheorie von Minkowski können α, β so gewählt werden,daß $N((\alpha, \beta)) \leq M(K)$ ist.Natürlich kann β durch jedes zu β assoziierte Element ersetzt werden.Andererseits liegen in jedem Ideal nur endlich viele paarweise nicht assoziierte Elemente mit minimalem Normbetrag.Bei geeigneter Darstellung der $\gamma \notin E_H$ kann man sich also beschränken auf endlich viele Werte von β.Da nur die Elemente einer Grundmasche von R betrachtet werden,kommen für jedes β auch nur endlich viele α in Frage. Ist $\mathfrak{a}$ nicht Hauptideal und $\beta \in \mathfrak{a}$ ein Element mit minimalem Normbetrag aus $\mathfrak{a}$,so existiert (nach dem chinesischen Restsatz) bekanntlich ein $\alpha \in \mathfrak{a}$ mit $\mathfrak{a} = (\alpha, \beta)$.Dann ist $\frac{\alpha}{\beta} \notin E_H$.Gilt $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$,so erzeugen (α, β) und (α', β') dieselbe Idealklasse.Zusammen folgt $h \leq n+1$.

Im folgenden werden Hilfsmittel zusammengestellt für die Suche nach endlichen euklidischen Systemen,die nur Hauptideale enthalten.

Satz 4 Sei $[K : \mathbb{Q}] = n$ und $\alpha, \beta \in R; \alpha * \beta \neq 0; N(\alpha) = \alpha * \alpha'; N(\beta) = \beta * \beta'$.Gilt

$$(1) \qquad \mid ggT(N(\alpha), N(\beta)) \mid < \sqrt[n]{\mid N(\beta) \mid}$$

oder im Fall $\beta \in \mathbb{Z}$ schwächer $\beta \nmid N(\alpha)$,
so liegt $\frac{\alpha}{\beta}$ in der euklidischen Menge eines Hauptideals,nämlich

$$\frac{\alpha}{\beta} \in E_{\frac{1}{(\lambda * \alpha')}} \qquad \text{für ein geeignetes} \qquad \lambda \in \mathbb{Z}.$$

Beweis: Es existieren $\lambda, \mu \in \mathbb{Z}$ mit $\lambda * N(\alpha) - \mu * N(\beta) = ggT(N(\alpha), N(\beta)) \neq 0$,woraus im Fall (1)

$$0 < \mid N(\frac{\alpha}{\beta} - \frac{\mu * \beta'}{\lambda * \alpha'}) \mid = \mid N(\frac{ggT(N(\alpha), N(\beta))}{\beta * \lambda * \alpha'}) \mid < \mid N(\frac{1}{\lambda * \alpha'}) \mid$$

folgt,insbesondere auch $\frac{\alpha}{\beta} \notin \frac{1}{(\lambda * \alpha')}$ und damit die Behauptung $\frac{\alpha}{\beta} \in E_{\frac{1}{(\lambda * \alpha')}}$.Im Fall $\beta \in \mathbb{Z}$ betrachte man analog die Gleichung $\lambda * N(\alpha) - \mu * \beta = ggT(N(\alpha), \beta)$ bzw. $\frac{\alpha}{\beta} - \frac{\mu}{\lambda * \alpha'} = \frac{ggT(N(\alpha), \beta)}{\beta * \lambda * \alpha'}$.

Ist K ein algebraischer Zahlkörper und $\alpha, \beta \in R$ mit $\beta \neq 0, \frac{\alpha}{\beta} \in K \setminus R$,so existiert ein $\gamma \in R$ mit $\frac{\alpha}{\beta} \in E_{\frac{1}{(\gamma)}}$ offenbar genau dann,wenn ein $\delta \in (\alpha, \beta)$ existiert mit $\mid N(\delta) \mid < \mid N(\beta) \mid$.Natürlich ist dies lediglich ein notwendiges und hinreichendes Kriterium für die Existenz eines solchen γ.Im folgenden wird unter gewissen Voraussetzungen ein Verfahren für die Konstruktion eines solchen γ angegeben.
Seien $\alpha, \alpha' \in R$ mit $\alpha' \neq 0$ und $\frac{\alpha}{\alpha'} \in K \setminus R$.Weiter sei der Nenner α' zerlegt in der Form $\alpha' = \beta * \beta'$ mit $\beta, \beta' \in R$ derart,daß $1 \in (\alpha, \beta)$ und β nicht Einheit ist,aber (in R) Teiler einer Primzahl $p \in \mathbb{Z}$. Sind die Primidealteiler von (α') sämtlich Hauptideale, so besitzt α' stets eine solche Zerlegung;insbesondere ist dies natürlich stets der Fall,wenn K die Klassenzahl 1 hat.Gilt $\frac{\alpha}{\beta} \in E_{\frac{1}{(\gamma)}}$ für ein $\gamma \in R$, so folgt sofort $\frac{\alpha}{\beta * \beta'} \in E_{\frac{1}{(\gamma * \beta')}}$.Es genügt also,die Konstruktion von γ für den Fall $\beta' = 1$,also für $\frac{\alpha}{\beta}$ durchzuführen (Die Existenz von γ ist klar aufgrund der Voraussetzungen).
Sei nun der algebraische Zahlkörper $K = \mathbb{Q}(\theta)$ mit $\theta \in R$ gegeben durch $h(x) := Irr(\theta, \mathbb{Q})$, und sei $diskr(\theta) = d^2 * diskrR$, also $R \subseteq \frac{\mathbb{Z}[\theta]}{d}$.Ferner seien α, β gegeben in der Form

$$\alpha = \frac{f(\theta)}{d}, \beta = \frac{g(\theta)}{d} \qquad \text{mit} \qquad f(x), g(x) \in \mathbb{Z}[x].$$

Unter der Voraussetzung $p \nmid d$ liefert nun das folgende Verfahren ein $\gamma \in R$ mit $\frac{\alpha}{\beta} \in E_{\frac{1}{(\gamma)}}$.
Für jedes $r(x) \in \mathbb{Z}(x)$ bezeichne $\overline{r}(x) \in \mathbb{Z}_p[x]$ das zugehörige Polynom mit mod p reduzierten Koeffizienten.Die Konstruktion von γ beruht nun darauf,daß

$$ggT(\overline{f}(x), \overline{g}(x), \overline{h}(x)) = \overline{1}$$

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

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

also existiert auch ein Polynom $r_3(x) \in \mathbb{Z}[x]$ mit

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

und wegen $p \nmid d$ folgt die Behauptung.
Mittels des euklidischen Algorithmus in $\mathbb{Z}_p[x]$ lassen sich also Polynome $\lambda_i(x) \in \mathbb{Z}[x]$ $(i = 1, \cdots, 4)$ berechnen mit

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

Es folgt

$$(d * \lambda_1(\theta)) * \alpha + (d * \lambda_2(\theta) + \frac{p}{\beta} * \lambda_4(\theta)) * \beta = 1.$$

Da β nicht Einheit ist,muß $\lambda_1(\theta) \neq 0$ sein,und es kann $\gamma = d * \lambda_1(\theta)$ gewählt werden.
Bei quadratischen Zahlkörpern kann bekanntlich θ stets so gewählt werden,daß $d = 1$ ist.Für quadratische Zahlkörper mit Klassenzahl 1 ist die obige Konstruktion also stets für alle Elemente aus $K \setminus R$ durchführbar.Die Polynome $f(x), g(x)$ können in diesem Fall von Grad < 2 gewählt werden.
Hat man eine Darstellung,bei der $\beta = p$ Primzahl ist,so kann man auch Satz 4 anwenden,da wegen der Voraussetzung $1 \in (\alpha, \beta)$ dann $p \nmid N(\alpha)$ ist.

Wie bei der Suche nach euklidischen Zahlkörpern liefert auch bei der Suche nach euklidischen Systemen (zumindest bei kleinen Körpergraden) die folgende geometrische Interpretation im Sinne von Minkowski ein wesentliches Hilfsmittel.Der algebraische Zahlkörper K besitze r reelle Einbettungen $\sigma_1, ..., \sigma_r$ und s Paare konjugiert-komplexer Einbettungen $\sigma_{r+1}, \overline{\sigma_{r+1}}, ..., \sigma_{r+s}, \overline{\sigma_{r+s}}$.Für jedes $a \in K$ wird in der üblichen Weise das geometrische Bild definiert durch

$$g(a) := (\sigma_1(a), \cdots, \sigma_r(a), Re\sigma_{r+1}(a), Im\sigma_{r+1}(a), \cdots) \in \mathbb{R}^n$$

und für jedes $\alpha = (\alpha_1, \cdots, \alpha_r, \beta_{r+1}, \beta'_{r+1}, \cdots \beta_{r+s}, \beta'_{r+s}) \in \mathbb{R}^n$ die Norm durch

$$N(\alpha) = \prod_{i=1}^{r} \alpha_i * \prod_{j=r+1}^{r+s} (\beta_j^2 + \beta_j'^2),$$

so daß $N(g(a)) = N(a)$ gilt für alle $a \in K$.Sei M eine Menge von Idealen von K und $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c} \neq (0)$.Mit M ist natürlich auch $M \cup \{\mathfrak{m}\}$ euklidisches System. Sei deshalb o.B.d.A. $\mathfrak{m} \in M$.Ist $m_1, \cdots, m_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{m}$,so ist $g(m_1), \cdots, g(m_n)$ eine $\mathbb{Z}$-Basis des Gitters $g(\mathfrak{m})$.
Nun ist M euklidisches System genau dann,wenn

$$\{q_1 g(m_1) + \cdots + q_n g(m_n) \mid 0 \leq q_i < 1, q_i \in \mathbb{Q}\} \setminus \{0\}$$

enthalten ist in

$$\bigcup_{\mathfrak{c}\in M}\{\beta\in\mathbb{R}^n \mid \beta\notin g(\mathfrak{c}), \exists c\in\mathfrak{c} \text{ mit } \mid N(\beta-g(c))\mid < N(\mathfrak{c})\}.$$

Gilt die Inklusion sogar für

$$\{q_1 g(m_1)+\cdots+q_n g(m_n) \mid 0\le q_i<1, q_i\in\mathbb{R}\}\setminus\{0\},$$

so besitzt M eine endliche Teilmenge,welche euklidisches System ist. Denn die kompakte Teilmenge

$$\{q_1 g(m_1)+\cdots+q_n g(m_n) \mid 0\le q_i\le 1, q_i\in\mathbb{R}\}$$

des $\mathbb{R}^n$ wird überdeckt von den offenen Mengen

$$\{\beta\in\mathbb{R}^n \mid \beta\notin g(\mathfrak{c}), \exists c\in\mathfrak{c} \text{ mit } \mid N(\beta-g(c))\mid < N(\mathfrak{c})\} \qquad (\mathfrak{c}\in M\setminus\{\mathfrak{m}\})$$

und

$$\{\beta\in\mathbb{R}^n \mid \exists c\in\mathfrak{m} \text{ mit } \mid N(\beta-g(c))\mid < N(\mathfrak{m})\}.$$

Nach dem Satz von Heine-Borel existiert eine endliche Teilüberdeckung, die wiederum ein endliches euklidisches Teilsystem von M liefert.

Jeder algebraische Zahlkörper mit Klassenzahl 1 besitzt ein endliches euklidisches System,welches nur Hauptideale der Form $\frac{1}{(\mu)}$ $(\mu\in R)$ enthält.Dies ergibt sich wie folgt.Sind $\omega_1,\cdots,\omega_m$ beliebige ganze Elemente aus K mit $m>M(K)$,so gilt für $M:=\{\frac{1}{(\omega_i-\omega_j)}\mid i\neq j\}$ stets

$$\bigcup_{\mathfrak{c}\in M} E_{\mathfrak{c}}\cup\bigcup_{\mathfrak{c}\in M}\mathfrak{c}=K. \tag{2}$$

Dies erhält man leicht mit Hilfe der von Lenstra [5] eingeführten Methode der Ausnahmefolgen zum Auffinden euklidischer Zahlkörper. Sei nun $\frac{a}{b}\in\mathfrak{c}\setminus R$ $(a,b\in R, a*b\neq 0)$ für ein $\mathfrak{c}\in M$.Dann existiert nach Bemerkung 1 ein $\mu\in R$ mit $\frac{a}{b}\in E_{\frac{1}{(\mu)}}$.Es folgt $\frac{a}{b}+\lambda\in E_{\frac{1}{(\mu)}}$ für alle $\lambda\in R$.Andererseits liegen nur endlich viele Elemente von $\mathfrak{c}$ in einer festen Grundmasche von R.Damit folgt die Behauptung.
Speziell läßt sich mit Hilfe des oben beschriebenen Konstruktionsverfahrens auf diese Weise für jeden quadratischen Zahlkörper mit Klassenzahl 1 ein endliches euklidisches System bestimmen,welches nur Hauptideale enthält.

3. Es folgen Beispiele für die Berechnung von endlichen euklidischen Systemen,welche nur Hauptideale enthalten.Neben Klassenzahl $h=1$ liefern diese gleichzeitig ein Verfahren zur Bestimmung des ggT zweier Elemente α,β,welches i.a. schneller ist als der euklidische Algorithmus bzgl. der Norm.

Zunächst wird der imaginär-quadratische Zahlkörper $\mathbb{Q}(\sqrt{-19})$ betrachtet,welcher die Klassenzahl $h=1$ besitzt,aber weder euklidisch ist (nach Motzkin [10]),noch k-stufig euklidisch im Sinne von Cooke [2].Mit Hilfe der geometrischen Methode läßt sich leicht zeigen,daß

$$H=\{\frac{1}{(\alpha)}\mid\alpha\in\{1,2,\frac{1-\sqrt{-19}}{2},\frac{3-\sqrt{-19}}{2}\}\}$$

ein endliches euklidisches System ist.Wegen

$$0,1,\frac{1+\sqrt{-19}}{2},\frac{3+\sqrt{-19}}{2}\in(1),\qquad N((1))=1;$$

$$\frac{1+\sqrt{-19}}{4},\frac{3+\sqrt{-19}}{4},\frac{5+\sqrt{-19}}{4}\in\frac{1}{(2)},\qquad N(\frac{1}{(2)})=\frac{1}{4};$$

$$\frac{1+\sqrt{-19}}{5}\in\frac{1}{(\frac{1-\sqrt{-19}}{2})},\qquad N(\frac{1}{(\frac{1-\sqrt{-19}}{2})})=\frac{1}{5};$$

$$\frac{9+3*\sqrt{-19}}{14}\in\frac{1}{(\frac{3-\sqrt{-19}}{2})},\qquad N(\frac{1}{(\frac{3-\sqrt{-19}}{2})}=\frac{1}{7}$$

genügt es zu zeigen,daß das Innere der Kreise mit den Mittelpunkten

$$(0,0),(1,0),(\frac{1}{2},\frac{\sqrt{19}}{2}),(\frac{3}{2},\frac{\sqrt{19}}{2})\qquad \text{(und dem Radius 1)},$$

$$(\frac{1}{4},\frac{\sqrt{19}}{4}),(\frac{3}{4},\frac{\sqrt{19}}{4}),(\frac{5}{4},\frac{\sqrt{19}}{4})\qquad \text{(und dem Radius } \frac{1}{2}),$$

$$(\frac{1}{5}),\frac{\sqrt{19}}{5})\qquad \text{(und dem Radius } \frac{1}{\sqrt{5}}),$$

$$(\frac{9}{14},\frac{3*\sqrt{19}}{14})\qquad \text{(und dem Radius } \frac{1}{\sqrt{7}})$$

ohne die jeweiligen Mittelpunkte den Bereich $\{q_1(1,0)+q_2(\frac{1}{2},\frac{\sqrt{19}}{2})\mid 0\le q_1<1, 0\le q_2<1\}\setminus\{0\}$ überdeckt.Dies läßt sich leicht überprüfen.Auf die Wahl von H kommt man sehr schnell.Die geometrische Situation (bzw. die Wahl von $\omega_1=0,\omega_2=1,\omega_3=2$ in Abschnitt 2) legt es nahe,zunächst $\alpha=1,2$ zu wählen.Damit ist die Grundmasche bis auf endlich viele Punkte überdeckt.Satz 4 führt dann auf die übrigen Werte von α.Es sei noch erwähnt,daß $\mathbb{Q}(\sqrt{-19})$ kein euklidisches System besitzt,welches nur Ideale der Form $\frac{1}{(a)}$ mit $a\in\mathbb{N}$ enthält,denn für ein beliebiges $a\in\mathbb{N}$ gilt $\frac{1+\sqrt{-19}}{4}\notin E_{\frac{1}{(a)}}$.Im Fall $2\mid a$ ist nämlich $\frac{1+\sqrt{-19}}{4}\in\frac{1}{(a)}$ und anderenfalls ist $N(\frac{1+\sqrt{-19}}{4}-\alpha)>\frac{19}{16*a^2}>\frac{1}{a^2}$ für alle $\alpha\in\frac{1}{(a)}$.
Wie man zeigt,daß $\mathbb{Q}(\sqrt{-19})$ dem Dedekind-Hasse-Kriterium genügt,steht bei Wilson [13].

Als weiteres Beispiel wird der reell-quadratische Zahlkörper $\mathbb{Q}(\sqrt{83})$ betrachtet,welcher Klassenzahl $h=1$ besitzt,aber nicht norm-euklidisch ist und von dem unbekannt ist,ob er 2-stufig euklidisch ist (nach [4]).Gesucht wird ein endliches euklidisches System,welches nur Hauptideale enthält.Grundlage ist wieder die oben beschriebene geometrische Interpretation.Die Elemente aus $\mathbb{R}^2$ mit Normbetrag <1 liegen im Inneren der 4 Hyperbeläste mit der Gleichung $\mid\alpha_1*\alpha_2\mid=1$.Eine $\mathbb{Z}$-Basis des Gitters $g(R)$ ist $\{(1,1),(\sqrt{83},-\sqrt{83})\}$.
Nach (2) gilt für $m>M(K)$ und $\omega_i:=i-1$ $(i=0,\cdots,m)$ die Gleichung

$$\bigcup_{i=1}^{m}E_{\frac{1}{(i)}}\cup\frac{1}{(i)}=K.$$

Die untere Schranke für m läßt sich für quadratische Zahlkörper verbessern.Für $K = \mathbb{Q}(\sqrt{83})$ ergibt sich dies wie folgt.
Durch Betrachtung der Hyperbeläste mit den Mittelpunkten $(0,0),(1,1),(-1,-1),(2,2)$ sieht man, daß $E_{(1)} \cup (1)$ alle Elemente $a + b * \sqrt{83} \in \mathbb{Q}(\sqrt{83})$ enthält mit $0 \leq b \leq \sqrt{2}$.Man beachte $\sqrt{2}, \sqrt{5} \notin \mathbb{Q}(\sqrt{83})$.Entsprechend enthält für $n \in \mathbb{N}$ die Menge $E_{\frac{1}{(n)}} \cup \frac{1}{(n)}$ alle Elemente aus $\mathbb{Q}(\sqrt{83})$ mit

$$\frac{j * \sqrt{83} - \sqrt{2}}{n} \leq b \leq \frac{j * \sqrt{83} + \sqrt{2}}{n}, \qquad j \in \mathbb{N}.$$

Also ist

$$(3) \qquad \bigcup_{i=1}^{6} E_{\frac{1}{(i)}} \cup \frac{1}{(i)} = K.$$

Die Elemente $\frac{\alpha}{i} \in \bigcup_{i=1}^{6} \frac{1}{(i)} \setminus R$ liegen im Fall $\alpha \in \mathbb{Z}$ offenbar in $E_{(1)}$,und im Fall $\alpha \in R \setminus \mathbb{Z}$ erfüllen sie die Voraussetzung von Satz 4 bis auf die Elemente aus $\frac{1+\sqrt{83}}{2} + R$. Ferner gilt $\frac{1+\sqrt{83}}{2} + R \subseteq E_{(1)}$ wegen $\mid N(\frac{1+\sqrt{83}}{2} - 5) \mid = \frac{1}{2}$. Insgesamt erhält man auf einfache Weise ein endliches (aber relativ großes) euklidisches System,welches nur Hauptideale enthält. Durch geometrische Überlegungen im $\mathbb{R}^2$ läßt sich dieses euklidische System verkleinern zu

$$\{(1), \frac{1}{(2)}, \frac{1}{(3)}, \frac{1}{(4)}, \frac{1}{(5)}, \frac{1}{(6)}, \frac{1}{(9)}, \frac{1}{(\sqrt{83})}, \frac{1}{(1-\sqrt{83})}\}.$$

Als drittes Beispiel wird der kubische Körper K mit $diskrK = -199$ untersucht,welcher nach Taylor[12] nicht norm-euklidisch ist,aber Klassenzahl 1 besitzt.Er wird erzeugt von einer Nullstelle θ von $x^3 - x^2 + 4x - 1$ und besitzt $1, \theta, \theta^2$ als Ganzheitsbasis.Die Minkowskischranke $M(K)$ ist < 4;für ω_i $(i = 0, \cdots, 3)$ erhält man nach (2) also

$$\bigcup_{i=1}^{3} E_{\frac{1}{(i)}} \cup \frac{1}{(i)} = K.$$

Die Elemente $\frac{\alpha}{2}$ $(\alpha \in R, 2 \nmid \alpha)$ liegen in $E_{(1)}$,da jede von Null verschiedene Nebenklasse von (2) eine Einheit enthält,denn wegen $\theta \not\equiv 1 (mod\, 2)$ erzeugt die Einheit θ die multiplikative Gruppe des Körpers $R/2R$ der Ordnung 7.Auch die Elemente $\frac{\alpha}{3}$ $(\alpha \in R, 3 \nmid \alpha)$ liegen in $E_{(1)}$,da

$$\{(-1)^i * \alpha^j * \theta^k \mid 0 \leq i, j \leq 1; 0 \leq k \leq 3\} \cup \{(-1)^i * \beta * \alpha^j * \theta^k \mid o \leq i, j, k \leq 1\} \cup \{\gamma, -\gamma\}$$

ein vollständiges Restsystem der von Null verschiedenen Nebenklassen mod 3 ist,welches nur Elemente mit Normbetrag $< N(3)$ besitzt.Dabei sei $\alpha := -1 - \theta, \beta := 1 - \theta, \gamma := 4 + \theta^2$;man beachte $N(\alpha) = -7, N(\beta) = 3, N(\gamma) = 9$.Also ist $\{(1), \frac{1}{(2)}, \frac{1}{(3)}\}$ ein euklidisches System von K.

Durch den Nachweis der Existenz eines euklidischen Systems,welches nur Hauptideale enthält, läßt sich nach Satz 2 zeigen,daß der betreffende Zahlkörper die Klassenzahl $h = 1$ besitzt.Dies ist auch möglich mit Hilfe des folgenden Spezialfalls von Satz 1.

Satz 5 Es sei $M := \{\frac{1}{(a)} \mid a \in R, a \neq 0\}$ und für jede Primzahlpotenz $p^r \leq M(K)$ gelte

$$(4) \qquad \frac{R}{p^r} \setminus R \subseteq E_M.$$

Dann besitzt K die Klassenzahl $h = 1$.

Beweis: Sei $\mathfrak{p}$ Primideal mit $N(\mathfrak{p}) = p^r \le M(K)$.Für ein geeignetes Ideal $\mathfrak{p}'$ gilt $N(\mathfrak{p}) = \mathfrak{p} * \mathfrak{p}'$,also

$$R \subsetneq \frac{1}{\mathfrak{p}} = \frac{\mathfrak{p}'}{N(\mathfrak{p})} \subseteq \frac{R}{p^r}.$$

Es folgt $\frac{1}{\mathfrak{p}} \cap E_M \neq \phi$ und nach Satz 1 erzeugt M die Idealklassengruppe.

Man beachte,daß die Bedingung (4) häufig leicht nachzuweisen sein wird,da es genügt nur diejenigen Elemente von $\frac{R}{p^r} \setminus R$ zu betrachten,die in einer festen Grundmasche von R liegen,also eine endliche Menge.Nach Satz 4 kann man sich darüber hinaus beschränken auf diejenigen Elemente $\frac{\alpha}{p^r}$ $(\alpha \in R)$ mit $p^r \mid N(\alpha)$.
Eine einfache Anwendung erhält man im Fall $\mathbb{Q}(\sqrt{83})$(unter Verwendung von (3)).

4. In diesem Abschnitt werden euklidische Systeme von Zahlkörpern K mit Klassenzahl $h \neq 1$ betrachtet.

Satz 6 Sei M ein euklidisches System von K und $\mathfrak{a}$ ein ganzes Ideal von K mit minimaler Norm,welches nicht Hauptideal ist. Dann existiert ein $\mathfrak{c}' \in M$ mit $[\mathfrak{a}] = [\mathfrak{c}']$.

Beweis: Sei $\mathfrak{m} := \bigcap_{\mathfrak{c} \in M} \mathfrak{c}$.Da M euklidisches System ist,gilt $\frac{\mathfrak{m}}{\mathfrak{a}} \cap E_M \neq \phi$.Also existiert ein $\mathfrak{c}' \in M$ mit $\frac{\mathfrak{c}'}{\mathfrak{a}} \cap E_{\mathfrak{c}'} \neq \phi$ und nach Lemma 1 existiert ein ganzes Ideal $\mathfrak{b}$ mit $N(\mathfrak{b}) < N(\mathfrak{a})$ und $[\mathfrak{b}] * [\mathfrak{c}'] = [\mathfrak{a}]$.Wegen der Minimalität von $N(\mathfrak{a})$ ist $\mathfrak{b}$ Hauptideal.

Aus der Existenz eines euklidischen Ideals lassen sich nach van der Linden [9] Aussagen über die Klassenzahl herleiten.Allgemeiner gilt

Satz 7 Sei M ein euklidisches System von K,welches nur Elemente aus den zwei Idealklassen [1] und $[\mathfrak{c}]$ enthält.Dann gilt:

(i) Ist $[K : \mathbb{Q}]$ galoissch,so gilt $h \mid [K : \mathbb{Q}]$.

(ii)Sei $\alpha \in \mathfrak{c}$ mit minimalem Normbetrag und P die Anzahl aller Primzahlpotenzen p^r mit $1 < p^r \le \frac{|N(\alpha)|}{N(\mathfrak{c})}$, die als Norm eines ganzen Ideals auftreten.Dann ist $h \le 1 + P$.
Speziell gilt also $h \le \frac{|N(\alpha)|}{N(\mathfrak{c})}$ (Man beachte,daß nach der Gitterpunkttheorie von Minkowski stets $\frac{|N(\alpha)|}{N(\mathfrak{c})} \le M(K)$ ist).

(iii)Ist $[K : \mathbb{Q}]$ galoissch,so läßt sich (ii) verschärfen zu $h \le 1 + P'$,wobei P' die Anzahl aller Primzahlpotenzen p^r ist mit $1 < p^r \le \frac{|N(\alpha)|}{N(\mathfrak{c})}$, die als Norm eines ganzen Ideals auftreten,welches nicht Hauptideal ist.

Beweis: (i)Aus der Definition euklidischer Systeme folgt,daß für jedes $\sigma \in Gal(K : \mathbb{Q})$ mit M auch $\{\sigma(\mathfrak{c}) \mid \mathfrak{c} \in M\}$ euklidisches System ist.Sei $\mathfrak{a}$ ein ganzes Ideal mit minimaler Norm,welches kein Hauptideal ist.Aus Satz 6 folgt dann $[\mathfrak{c}] = [\mathfrak{a}] = [\sigma(\mathfrak{c})]$,also

$$[\mathfrak{c}]^{[K:\mathbb{Q}]} = \prod_{\sigma \in Gal(K:\mathbb{Q})} [\sigma(\mathfrak{c})] = [(N(\mathfrak{c}))] = [(1)],$$

und nach Satz 2 die Behauptung.

(ii)Sei $d \in K$ so gewählt,daß $(d) * \mathfrak{c}$ ganzes Ideal ist.Wegen $d * \alpha \in (d) * \mathfrak{c}$ existiert ein ganzes Ideal $\mathfrak{c}'$ mit $(d * \alpha) = (d) * \mathfrak{c} * \mathfrak{c}'$.Da $\mathfrak{c}$ nicht Hauptideal ist,ist auch $\mathfrak{c}'$ nicht Hauptideal.Ferner gilt

$N(\mathfrak{c}') = \frac{|N(\alpha)|}{N(\mathfrak{c})}$.Die Behauptung folgt,wenn ein $n \in \mathbb{N}$ existiert mit $n \le P$ und $[\mathfrak{c}'] = [\mathfrak{c}^n]$.Allgemeiner wird bewiesen: Für jedes ganze Ideal $\mathfrak{a}$,welches nicht Hauptideal ist,gilt $[\mathfrak{a}] = [\mathfrak{c}]^n$ für ein $n \in \mathbb{N}$ mit $n \le \sharp P(\mathfrak{a})$, wobei $P(\mathfrak{a})$ die Menge aller Primzahlpotenzen p^r bezeichnet mit $1 < p^r \le N(\mathfrak{a})$,die als Norm eines ganzen Ideals auftreten.
Der Beweis erfolgt durch vollständige Induktion nach $N(\mathfrak{a})$.Besitzt $\mathfrak{a}$ minimale Norm,so folgt die Behauptung,da $N(\mathfrak{a})$ Primzahlpotenz ist und nach Satz 6 gilt $[\mathfrak{a}] = [\mathfrak{c}]$.Ist $N(\mathfrak{a})$ Primzahlpotenz,so ergibt sich die Behauptung für $\mathfrak{a}$ daraus,daß nach Lemma 1 ein ganzes Ideal $\mathfrak{b}$ existiert mit $[\mathfrak{a}] = [\mathfrak{b}] * [\mathfrak{c}]$ oder $[\mathfrak{a}] = [\mathfrak{b}]$ und$P(\mathfrak{b}) \subsetneqq P(\mathfrak{a})$.Ist $N(\mathfrak{a})$ nicht Primzahlpotenz,so ist $\mathfrak{a}$ nicht Primideal und besitzt eine Zerlegung $\mathfrak{a} = \mathfrak{a}_1 * \mathfrak{a}_2$ in ein Produkt ganzer Ideale mit $N(\mathfrak{a}_i) < N(\mathfrak{a})$.Aus $[\mathfrak{a}_i] = [\mathfrak{c}]^{n_i}$ folgt $[\mathfrak{a}] = [\mathfrak{c}]^{n_1+n_2}$.Es genügt also $\sharp P(\mathfrak{a}) \ge \sharp P(\mathfrak{a}_1) + \sharp P(\mathfrak{a}_2)$ zu beweisen.Dies ist aber klar,denn ist p Primzahl und p^β maximale Potenz von p in $P(\mathfrak{a}_1)$ und $p^{\beta'} \in P(\mathfrak{a}_2)$,so gilt $p^{\beta+\beta'} \in P(\mathfrak{a}) \setminus P(\mathfrak{a}_1)$.

(iii)In Verschärfung zu (ii) genügt es zu zeigen,daß für jedes ganze Ideal $\mathfrak{a}$,welches nicht Hauptideal ist,$[\mathfrak{a}] = [\mathfrak{c}]^n$ gilt für ein $n \in \mathbb{N}$ mit $n \le \sharp P'(\mathfrak{a})$,wobei $P'(\mathfrak{a})$ die Menge aller Primzahlpotenzen p^r bezeichnet mit $1 < p^r \le N(\mathfrak{a})$, die als Norm auftreten eines ganzen Ideals,welches nicht Hauptideal ist.Offenbar genügt es,Ideale $\mathfrak{a}$ zu betrachten,die kein ganzes Hauptideal $\neq (1)$ als Teiler besitzen.Zum Beweis werden ganze Ideale $\mathfrak{a} = \mathfrak{a}_0, \cdots, \mathfrak{a}_n = (1)$ konstruiert,welche keinen ganzen Hauptidealteiler $\neq (1)$ besitzen,mit

$$(5) \qquad [\mathfrak{a}_i] = [\mathfrak{c}] * [\mathfrak{a}_{i+1}], N(\mathfrak{a}_{i+1}) < N(\mathfrak{a}_i) \qquad \text{für} \qquad i = 0, \cdots, n-1$$

und

$$(6) \qquad s(\mathfrak{a}_i) + i \le \sharp P'(\mathfrak{a}) \qquad \text{für} \qquad i = 0 \cdots, n.$$

Dabei bezeichne $s(\mathfrak{a}_i)$ die Summe der Exponenten in der Primidealfaktorzerlegung von $\mathfrak{a}_i$.Dann folgt aus (5) die Gleichung $[\mathfrak{a}] = [\mathfrak{c}]^n$ und aus (6) für $i = n$ andererseits $n \le \sharp P'(\mathfrak{a})$,also die Behauptung.
Zunächst gilt (6) für $i = 0$,da $\mathfrak{a}$ mindestens $s(\mathfrak{a}_i)$ Teiler besitzt mit $s(\mathfrak{a}_i)$ verschiedenen Primzahlpotenznormen, und keiner der Teiler Hauptideal ist.Sei nun $\mathfrak{a}_i$ bereits konstruiert und $\mathfrak{p}_i$ ein Primidealfaktor von $\mathfrak{a}_i$ mit maximaler Norm.Nach Lemma 1 erhält man (eventuell durch mehrfache Anwendung) ein ganzes Ideal $\mathfrak{b}_i$ mit

$$[\mathfrak{p}_i] = [\mathfrak{c}] * [\mathfrak{b}_i], \qquad N(\mathfrak{b}_i) < N(\mathfrak{p}_i).$$

Setze

$$\mathfrak{a}'_{i+1} := \frac{\mathfrak{a}_i}{\mathfrak{p}_i} * \mathfrak{b}_i \qquad \text{und} \qquad \mathfrak{a}_{i+1} := \frac{\mathfrak{a}'_{i+1}}{(d_i)}$$

mit $d_i \in R$,so daß $\mathfrak{a}_{i+1}$ ganz ist,aber kein ganzes Hauptideal $\neq (1)$ als Teiler besitzt.Dann ist (5) erfüllt.Zu zeigen bleibt $s(\mathfrak{a}_{i+1}) + i + 1 \le \sharp P'(\mathfrak{a})$.$P'(\mathfrak{a})$ enthält mindestens $s(\mathfrak{a}_{i+1})$ Primzahlpotenzen,die als Norm von Teilern von $\mathfrak{a}_{i+1}$ auftreten.Da $K : \mathbb{Q}$ als galoissch vorausgesetzt wird,muß $N(\mathfrak{b}_i)$ zu $N(\mathfrak{p}_i)$ teilerfremd sein.Also tritt $\mathfrak{p}_i$ bei $\mathfrak{a}_i$ häufiger als Faktor auf als bei $\mathfrak{a}_{i+1}$.Also enthält $P'(\mathfrak{a})$ als weiteres Element q_i eine Potenz von $N(\mathfrak{p}_i)$,die als Norm eines Teilers von $\mathfrak{a}_i$ aber nicht von $\mathfrak{a}_{i+1}$ auftritt.Wegen der jeweils maximalen Wahl der Norm der $\mathfrak{p}_i$ enthält $P'(\mathfrak{a})$ entsprechend weitere Elemente $q_j (j = 0, \cdots, i-1)$,die Potenzen sind von $N(\mathfrak{p}_j)$ und als Norm eines Teilers von $\mathfrak{a}_j$ aber nicht von $\mathfrak{a}_{j+1}$ auftreten.Damit ist der Satz bewiesen.

Nach van der Linden [9] sind $\mathbb{Q}(\sqrt{-5})$ und $\mathbb{Q}(\sqrt{-15})$ die einzigen imaginär-quadratischen Zahlkörper,die ein euklidisches Ideal besitzen.Der Körper $\mathbb{Q}(\sqrt{-6})$ besitzt aber ein euklidisches System M,welches nur Elemente aus $[(1)]$ und einer weiteren Idealklasse enthält,nämlich

$$M = \{(1), \frac{1}{(2, \sqrt{-6})}, \frac{1}{(3, \sqrt{-6})}\}.$$

Zur Überdeckung einer Grundmasche betrachte man die Kreise um die Mittelpunkte $(0,0),(0,\sqrt{6}),(\sqrt{6},0),(\sqrt{6},\sqrt{6})$ (mit dem Radius 1);$(0,\frac{\sqrt{6}}{2}),(1,\frac{\sqrt{6}}{2})$ (mit dem Radius $\frac{1}{\sqrt{N(2,\sqrt{-6})}}=\frac{1}{\sqrt{2}}$); $(0,\frac{\sqrt{6}}{3}),(1,\frac{\sqrt{6}}{3})$ (mit dem Radius $\frac{1}{\sqrt{N(3,\sqrt{-6})}}=\frac{1}{\sqrt{3}}$).Nach Satz 7 erhält man die Klassenzahl $h=2$.

Aus Satz 7 folgt,daß ein quadratischer Zahklörper mit Klassenzahl $h>2$ kein euklidisches System besitzt,welches nur Ideale aus $[(1)]$ und einer weiteren Idealklasse enthält.Insbesondere gibt es Zahlkörper mit zyklischer Klassengruppe,die kein solches euklidisches System besitzen;z.B. $\mathbb{Q}(\sqrt{-14})$ und $\mathbb{Q}(\sqrt{-31})$ mit Klassenzahl 4 und 3.

5. Häufig ist es schwierig, ein euklidisches System zu finden; stets läßt sich aber eine endliche Menge M von Idealen angeben mit der schwächeren Bedingung (vergleiche Gleichung (2))

$$\bigcup_{\mathfrak{c}\in M} E_{\mathfrak{c}} \cup \bigcup_{\mathfrak{c}\in M} \mathfrak{c} = K. \tag{7}$$

Dann wird die Klassengruppe zwar nicht von M erzeugt,aber es gilt

Satz 8 Sei M eine Menge von Idealen von K,$\mathfrak{a}_1$ der ggT bzw. $\mathfrak{a}_2$ das kgV der Zähler der Elemente aus M,$\mathfrak{b}_1$ der ggT bzw. $\mathfrak{b}_2$ das kgV der Nenner der Elemente aus M und $\mathfrak{a}_2\neq(0),\mathfrak{b}_2\neq(0)$.Ferner gelte (7).
Dann liegt in jeder Idealklasse ein ganzes Ideal,welches Produkt von Idealen aus M und höchstens einem Teiler von $\frac{\mathfrak{a}_2*\mathfrak{b}_2}{\mathfrak{a}_1*\mathfrak{b}_1}$ mit Norm $\leq M(K)$ ist.

Beweis: Es gilt

$$\frac{\mathfrak{a}_2}{\mathfrak{b}_1} \subseteq \bigcap_{\mathfrak{c}\in M} \mathfrak{c} \subseteq \bigcup_{\mathfrak{c}\in M} \mathfrak{c} \subseteq \frac{\mathfrak{a}_1}{\mathfrak{b}_2}. \tag{8}$$

Sei $\mathfrak{a}$ ein ganzes Ideal mit $N(\mathfrak{a})\leq M(K)$ und $\mathfrak{a}\nmid\frac{\mathfrak{a}_2*\mathfrak{b}_2}{\mathfrak{a}_1*\mathfrak{b}_1}$.Dann folgt

$$\frac{\mathfrak{a}_2}{\mathfrak{b}_1*\mathfrak{a}} \not\subseteq \frac{\mathfrak{a}_1}{\mathfrak{b}_2},$$

wegen (8)

$$\frac{\mathfrak{a}_2}{\mathfrak{b}_1*\mathfrak{a}} \not\subseteq \bigcup_{\mathfrak{c}\in M} \mathfrak{c}$$

und wegen (7)

$$\frac{\mathfrak{a}_2}{\mathfrak{b}_1*\mathfrak{a}} \cap \bigcup_{\mathfrak{c}\in M} E_{\mathfrak{c}} \neq \phi.$$

Also existiert ein $\mathfrak{c}_1\in M$ mit

$$\frac{\mathfrak{a}_2}{\mathfrak{b}_1*\mathfrak{a}} \cap E_{\mathfrak{c}_1} \neq \phi.$$

Wegen (8) folgt

$$\frac{\mathfrak{c}_1}{\mathfrak{a}} \cap E_{\mathfrak{c}_1} \neq \phi$$

und nach Lemma 1 existiert ein ganzes Ideal $\mathfrak{b}$ mit $[\mathfrak{b}] * [\mathfrak{c}_1] = [\mathfrak{a}], N(\mathfrak{b}) < N(\mathfrak{a})$. Wiederholte Anwendung liefert die Behauptung.

Satz 9 Enthält M nur Ideale der Form $\frac{1}{(\mu)}$ $(\mu \in R)$ und ist (7) erfüllt,so liegt in jeder Idealklasse ein Teiler von (μ) für geeignetes $\frac{1}{(\mu)} \in M$.

Beweis: Sei $\mathfrak{a} = (\alpha, \beta)$ nicht Hauptideal und $\beta \in \mathfrak{a}$ mit minimalem Normbetrag.Dann gilt $\frac{\alpha}{\beta} \notin E_M$,wegen (7) also $\frac{\alpha}{\beta} = \frac{a}{\mu}$ für ein geeignetes $\frac{1}{(\mu)} \in M$, $a \in R$.Es folgt,daß $\mathfrak{a}$ und (a, μ) dieselbe Idealklasse erzeugen.

Als einfaches Beispiel eines Zahlkörpers mit $h \neq 1$ sieht man leicht,daß für $\mathbb{Q}(\sqrt{-6})$ die Menge $M = \{(1), \frac{1}{(2)}\}$ die Voraussetzung (7) erfüllt.
Enthält M nur ein Ideal,so liefert Satz 8 die Aussage von Lenstra [6],daß ein euklidisches Ideal die Idealklassengruppe erzeugt.

Sind $\omega_1, \cdots, \omega_m$ beliebige ganze Elemente aus K und ist $m > M(K)$,so erfüllt $M := \{\frac{1}{(\omega_i - \omega_j)} \mid i \neq j\}$ stets die Bedingung (7)(s. Abschnitt 2).Man erhält nach Satz 9,daß in jeder Idealklasse ein Teiler eines der Ideale $(\omega_i - \omega_j)$ liegt.(Dies ergibt sich auch direkt:Ist nämlich $\mathfrak{a}$ ein ganzes Ideal mit $N(\mathfrak{a}) \leq M(K)$,so existieren i, j mit $\omega_i - \omega_j \in \mathfrak{a}$,also $\mathfrak{a} \mid (\omega_i - \omega_j)$).
Ist für $i \neq j$ stets $\mid N(\omega_i - \omega_j) \mid = 1$,so heißt $\omega_1, \cdots, \omega_m$ Ausnahmefolge und K ist norm-euklidisch nach Lenstra [5].Auf diese Weise wurden viele euklidische Zahlkörper gefunden (s.[5],[7],[8]).Ist für $i \neq j$ stets $\mid N(\omega_i - \omega_j) \mid$ gleich 1 oder Primzahl, so besitzt K die Klassenzahl $h = 1$.Es ist naheliegend in diesem Fall von einer verallgemeinerten Ausnahmefolge zu sprechen.Offenbar genügt zum Nachweis von $h = 1$ sogar $m > M'$,wobei M' die größte Primzahlpotenz $\leq M(K)$ ist.Nichttriviale Beispiele verallgemeinerter Ausnahmefolgen gibt Blöhmer [1] an für $\mathbb{Q}(\alpha)$,wobei α Nullstelle eines der Polynome

$$x^8 + x^6 - 3x^5 + 3x^4 - 2x^3 + 3x^2 - 3x + 1,$$

$$x^4 - x^2 + (\zeta_3 - 1)x - 1 \qquad (\zeta_3 \text{ primitive dritte Einheitswurzel}),$$

$$x^8 - x^7 - x^6 + x^5 + 2x^4 - 2x^2 + 1$$

ist.Unbekannt ist,ob diese Körper norm-euklidisch sind.

Literatur

[1] *J.Blöhmer*;Euklidische Ringe;Diplomarbeit FU Berlin,1989

[2] *G.Cooke*;The weakening of the Euclidean property for integral domains and application to algebraic number theory (I);J.f.Math.,282 (1976),133-156

[3] *G.Cooke*;The weakening of the Euclidean property for integral domains and application to algebraic number theory (II);J.f.Math.,283 (1977),71-85

[4] *F.Lemmermeyer*;Euklidische Ringe;Diplomarbeit Heidelberg,1989

[5] *H.W.Lenstra jr.*;Euclidean number fields of large degree; Invent.Math.,38 (1977),237-254

[6] *H.W.Lenstra jr.*;Euclidean ideal classes;J.arithmetiques de Luminy; Asterisque,61 (1979),121-131

[7] *A.Leutbecher*;Euclidean number fields having a large Lenstra constant;Ann.Inst.Fourier,35 (1985), 83-106

[8] *A.Leutbecher;G.Niklasch*;On cliques of exeptional units and Lenstra's construction of Euclidean fields;Lecture Notes Bd.1380, Number Theory,Ulm 1987

[9] *F.J.van der Linden*;Euclidean rings with two infinite primes; Ph.D.thesis,Univ Amsterdam,May 1984

[10] *T.H.Motzkin*;The Euclidean Algorithmus;Bull.Amer.Math.Soc.,55 (1949),1142-1146

[11] *H.Pollard*;The Theory of Algebraic Numbers;Carus Monograph 9, MAA,Wiley,New York,1950

[12] *E.M. Taylor*;Euclid's algorithm in cubic fields with complex conjugates;J.London Math.Soc.(2),14 (1976),49-54

[13] *J.C.Wilson*;A principal ideal ring that is not a Euclidean ring; Math.Mag.,46 (1973),34-38

Prof.Dr.V.Schulze
Freie Universität Berlin
Fachbereich Mathematik
Institut f. Mathematik II
Arnimallee 3
D-14195 Berlin