§ 0 Einführung

Die Geschichte des Euklidischen Algorithmus ist, wie der Name Euklid schon vermuten läßt, recht lang: sie beginnt mit Euklids "Beweis", daß der Ring $\mathbb{Z}$ der ganzen rationalen Zahlen "euklidisch" ist (sh. dazu die Arbeiten von Hendy (1975), Knorr (1976) und Collison (1980).

Ist R ein Ring (darunter wollen wir hier nur einen kommutativen, nullteilerfreien Ring mit Eins verstehen), so nennen wir eine Funktion $f:R\to\mathbb{N}$ eine ***euklidische Funktion*** oder einen ***euklidischen Algorithmus*** (kurz EA) auf R, wenn gilt:

(E-1): $\forall a\in R: f(a)=0 \Leftrightarrow a=0$

(E-2): $\forall a\in R,\ b\in R\setminus\{0\}\ \exists c\in R: f(a-bc) < f(b)$.

Falls es ein solches f gibt, heißt R ***euklidisch bezüglich f.*** Ziel der Euklidschen Überlegungen war es, in $\mathbb{Z}$ den sogenannten "Fundamentalsatz der Arithmetik" zu zeigen: daß nämlich jede natürliche Zahl sich bis auf die Reihenfolge eindeutig als Produkt von Primzahlen schreiben läßt.

Zu Eulers Zeiten wurde dann erkannt, daß sich gewisse diophantische Gleichungen wie z.B. $y^2=x^3-2$ besonders einfach lösen lassen, wenn man stattdessen $x^3=(y+\sqrt{-2})(y-\sqrt{-2})$ schreibt und annimmt, daß der Ring $\mathbb{Z}[\sqrt{-2}]$ ein ZPE-Ring ist, d.h. daß in ihm gewissermaßen ein Analogon zum Fundamentalsatz der Arithmetik in $\mathbb{Z}$ gilt. Jedoch galt diese Annahme damals als selbstverständlich.

Erst Gauß, der für seine Theorie der biquadratischen Reste den Ring $\mathbb{Z}[i]$ studierte (wo $i^2=-1$ ist), sah die Notwendigkeit eines Beweises ein und zeigte dazu, daß $\mathbb{Z}[i]$ euklidisch bezüglich der Norm ist.

Danach versuchte man einerseits, die Theorie der quadratischen und biquadratischen Reste zu verallgemeinern auf p-te Potenzreste, andererseits wollte man Fermat's letzte Vermutung beweisen, wonach die diophantische Gleichung $x^p+y^p+z^p=0$ für prime $p\geq 3$ nur triviale Lösungen besitzt (das sind solche mit $xyz=0$).

Bevor aber Kummer seine Theorie der idealen Zahlen entwickelt hatte (die dann von Dedekind zur heutigen Idealtheorie ausgebaut wurde), mußte man für beide Aufgaben voraussetzen, daß die Ringe $\mathbb{Z}[\zeta_p]$, wo ζ_p eine primitive p-te Einheitswurzel ist, ZPE-Ringe sind. Für $p=3, 5, 7$ konnte man dies beweisen, indem man zeigte, daß die entsprechenden Ringe normeuklidisch sind (sh. Gauß (1876) und Kummer (1975)).

Einen genaueren Überblick über die Geschichte des euklidischen Algorithmus bis hin zu den neueren Ergebnissen von Weinberger und Lenstra findet man in dem sehr nett geschriebenen Artikel von Lenstra (1979); weitere historische Details stehen bei van der Linden (1984), sowie in der bereits etwas älteren Arbeit von Narkiewicz (1976).

Wir wollen nun wieder zu unserer Definition einer euklidischen Funktion zurückkehren; ist $f:R \to \mathbb{N}$ eine Funktion, die zwar (E-1), aber nicht notwendig (E-2) erfüllt, so setzen wir $M(f) := \inf \{x \in \mathbb{R}: \forall a,b \in R\setminus\{0\}\ \exists c \in R: f(a-bc) > x * f(b)\}$ und $M(f) = \infty$, falls es kein solches x gibt. Wir nennen M(f) das ***euklidische Minimum von R bezüglich f.*** Ist R ein Zahlring und f der Absolutbetrag der Norm, so schreiben wir auch M(R) statt M(f); ist K schließlich Zahlkörper und R der Ring aller ganzen Zahlen in K (also die Hauptordnung), so schreiben wir i.A. M(K) statt M(R) oder M(f). Ist $M(f) > 1$, so ist R euklidisch bezüglich f, während dies für $M(f) > 1$ nicht der Fall ist. Was alles passieren kann, wenn $M(f) = 1$ ist, sollen die folgenden Beispiele zeigen (die wir allerdings erst später werden rechtfertigen können):

1. R sei ein euklidischer Ring und f die "minimale euklidische Funktion" auf R (die wir gleich nachher kennenlernen werden); dann ist $M(f) = 1$ und R euklidisch bezüglich f.
2. Sei R der Ring ganzer Zahlen in dem kubischen Körper der Diskriminante $d = -199$, und f der Absolutbetrag der Norm; dann ist $M(f) = M(R) = M(K) = 1$, R hat Klassenzahl 1, aber f ist nicht euklidisch auf R (sh. Taylor 1976).
3. Sei R der Ring ganzer Zahlen in einem der Körper $K = \mathbb{Q}(\sqrt{65})$ (sh. z.B. Heinhold 1939), $K = \mathbb{Q}(\sqrt{-1}, \sqrt{15})$ oder $K = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$ (sh. dazu § 6); in diesen Fällen ist $M(K) = M(R) = 1$, aber K hat Klassenzahl 2, somit kann f nicht euklidisch sein auf R.
4. Sei $R = \mathbb{Z}[\sqrt{-3}]$ (sh. Cohn 1978), $R = \mathbb{Z}[\sqrt{5}]$ oder $R = \mathbb{Z}[\sqrt{13}]$ und f der Absolutbetrag der Norm; dann ist in allen drei Fällen $M(R) = 1$, obwohl R hier nicht einmal ganz abgeschlossen, geschweige denn ZPE-Ring oder gar euklidisch ist. Wir werden später in Zahlkörpern höheren Grades noch weitere Beispiele für ein solches Verhalten finden.

Diese Beispiele zeigen, daß man i.A. aus $M(f) = 1$ nicht folgern kann, daß R euklidisch (oder nicht euklidisch) bezüglich f ist.

Eine manchmal sogar exakte untere Schranke für das euklidische Minimum M(f) gibt das folgende Kriterium, das trotz seiner Einfachheit bisher nirgendwo explizit zu finden ist (nicht einmal in dem Falle, wo f der Absolutbetrag der Norm ist):

(0.1) Sei $b \in R\setminus\{0\}$ keine Einheit; dann ist $M(f) \geq 1/f(b)$.

Bew.: Da b keine Einheit ist, gibt es ein $a \in R$ mit $b \nmid a$, schreibt dann $a = bq + r$ für irgendwelche $q, r \in R$, so muß $r \neq 0$ sein. Wegen (E-1) ist also $f(r) \geq 1$ für jede Wahl von q und r, und damit $f(r)/f(b) \geq 1/f(b)$. Die Behauptung folgt nun nach Definition von M(f).

Ist K ein quadratischer Zahlkörper mit Diskriminante d, so gibt die untenstehende Tafel ein $b \in R$ mit minimaler Norm > 1 und die daraus resultierende Schranke für M(K):

d	b	M(K) ≥
-4	$1+i$	1/2
-3	$\sqrt{-3}$	1/3
5	2	1/4
8	$\sqrt{2}$	1/2
12	$1+\sqrt{3}$	1/2
13	$4+\sqrt{13}$	1/3
17	$(5+\sqrt{17})/2$	1/2

Wir werden in § 2 sehen, daß diese Schranken sogar exakt sind; weiter sind dies die einzigen quadratischen Körper, für welche die Schranke aus (0.1) exakt ist. Auffallend hierbei ist, daß man diese Körper auch noch durch $|d| \leq 4$ im komplexen, bzw. durch $d \leq 17$ im reellen Fall charakterisieren kann, d.h.: die Körper, für die die Schranke aus (0.1) exakt ist, sind gerade diejenigen mit minimaler Diskriminante! Ähnliche Beobachtungen werden wir später auch für Zahlkörper dritten und vierten Grades machen können.

Wir wollen uns nun etwas mit der allgemeinen Theorie euklidischer Ringe befassen. Die Inklusionen

$$\{\text{Euklidische Ringe}\} \subset \{\text{Hauptidealringe}\} \subset \{\text{ZPE-Ringe}\}$$

sind klassisch. Für die hier betrachteten Zahlringe läßt sich die letzte Inklusion sogar umkehren, d.h. hier ist jeder ZPE-Ring auch Hauptidealring. Das Beispiel $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ zeigt allerdings, daß die erste Inklusion echt ist: R ist nämlich Hauptidealring, aber nicht euklidisch, wie wir gleich sehen werden.

Dazu folgen wir einer Idee Motzkins (1949; sh. auch Samuel 1971) und versuchen, zu einem gegebenen Ring eine Funktion f so zu konstruieren, daß f euklidisch auf R wird. Wegen (E-1) kennen wir alle $a \in R$ mit $f(a)=0$ (nämlich $a=0$) und fragen uns, für welche $b \in R$ wir $f(b)=1$ setzen dürfen. Wegen (E-2) ist dies nur dann möglich, wenn für alle $a \in R$ ein $q \in R$ existiert mit $f(a-bq) < f(b) = 1$; dies geht nur für $f(a-bq)=0$, und wegen (E-1) muß $a-bq=0$ sein. Dies zeigt, daß ein $b \in R$ mit $f(b)=1$ jedes $a \in R$ teilen muß: b muß also Einheit in R sein. Ist andererseits b eine Einheit, so läßt sich (E-2) für jedes gegebene $a \in R$ mit $q=ab$ sicher erfüllen, und wir dürfen in der Tat $f(b)=1$ setzen.

Ist nun $f(b)=2$, so soll es zu jedem $a \in R$ ein $q \in R$ geben mit $f(a-bq)<2$; also ist $a-bq=0$ (im Falle $f(a-bq)=0$) oder gleich einer Einheit (falls $f(a-bq)=1$ ist), anders ausgedrückt: jedes $a \in R$ ist mod b entweder 0 oder einer Einheit kongruent. Indem wir so fortfahren, werden wir auf die folgenden Teilmengen E_i von R geführt:

$E_0 = \{0\}$, $E_1 = E_0 \cup R^\times$ und allgemein für alle $i \geq 1$

$E_i \setminus E_{i-1} = \{b \in R$: jede Restklasse mod b enthält ein Element aus $E_{i-1}\}$.

Schließlich setzen wir noch $E_\infty = \bigcup_{i=0}^{\infty} E_i$.

Damit gilt

(0.2) Ein Ring R ist genau dann euklidisch, wenn $R=E_\infty$ gilt.

Bew.: Sei $R=E_\infty$. Wir definieren durch $f_o(a)=\min\{i\in\mathbb{N}: a\in E_i\}$ eine Funktion $f_o: R\to\mathbb{N}$; Sind dann $a,b\in R\setminus\{0\}$ gegeben und ist z.B. $f_o(b)=i$, so ist $i\geq 1$ wegen $b\neq 0$, und nach Konstruktion von f_o ist $b\in E_1$. Also gibt es ein $r\in E_{i-1}$ mit $a\equiv r \bmod b$; setzt man $a=bq+r$, so ist $q\in R$ und $f_o(r)\leq i-1 < f_o(b)$. Also ist R euklidisch bezüglich f_o.

Sei andererseits R euklidisch bezüglich einer Funktion f. Wir behaupten, daß dann alle $a\in R$ mit $f(a)=i$ bereits in E_i enthalten sind. Für $i=0$ ist dies wegen (E-1) sicher richtig. Haben wir die Behauptung für alle $i<k$ gezeigt und ist $f(b)=k$, dann existieren zu jedem $a\in R$ Elemente $q,r\in R$ mit $a=bq+r$ und $f(r)<f(b)$. Nach Induktionsvoraussetzung ist $r\in E_{k-1}$, d.h. zu jedem $a\in R$ gibt es ein $r\in E_{k-1}$ mit $a\equiv bq+r\equiv r \bmod b$; dies impliziert aber $b\in E_k = E_{f(b)}$, und folglich ist $R\subset E_\infty \subset R$.

Wenn wir uns den zweiten Teil des Beweises anschauen, so bemerken wir, daß wir viel mehr gezeigt haben: ist nämlich R euklidisch bezüglich f und f_o die im ersten Teil des Beweises definierte Funktion, dann zeigt die Relation $b\in E_{f(b)}$, daß $f_o(b)\leq f(b)$ für alle $b\in R$ ist, denn $f_o(b)$ gibt ja den kleinsten Index i an, für den $b\in E_i$ ist. Wir werden daher auf folgende Definition geführt: ist R ein euklidischer Ring, dann heißt die Funktion $f_m: R\to\mathbb{N}$, die durch

$$f_m(a) = \min\{f(a): f \text{ ist euklidische Funktion auf } R\}$$

definiert wird, die ***minimale euklidische Funktion auf R.*** Diese Bezeichnung wird gerechtfertigt durch

(0.3) f_m ist eine euklidische Funktion auf R mit der Eigenschaft $f_m(a)\leq f(a)$ für alle $a\in R$ und alle euklidischen Funktionen f auf R. Insbesondere gilt $f_m=f_o$.

Bew.: Seien $a,b\in R\setminus\{0\}$ gegeben. Nach Definition von f_m gibt es eine euklidische Funktion f mit $f_m(b)=f(b)$. Damit existieren $q, r\in R$ mit $a=bq+r$ und $f(r)<f(b)$. Daraus ergibt sich $f_m(r)\leq f(r)<f(b)=f_m(b)$, und f_m ist in der Tat eine euklidische Funktion auf R.

Wegen $f_m(a)\leq f(a)$ für alle euklidischen Funktionen f auf R und $f_o(a)\leq f_m(a)$ wegen der Bemerkung nach (0.2) muß nun $f_m(a)=f_o(a)$ für alle $a\in R$ gelten.

Im Falle $R=\mathbb{Z}$ lassen sich die Mengen E_i ganz einfach beschreiben: man hat nämlich $E_o=\{0\}$, $E_1=\{0, -1, 1\}$, und $E_2\setminus E_1$ enthält diejenigen $a\in\mathbb{Z}$, die in jeder Restklasse mod a einen Vertreter aus E_1 haben; da E_1 nur drei Elemente enthält, muß $|a|\leq 3$ gelten, und in der Tat findet man $E_2=\{0, \pm 1, \pm 2, \pm 3\}$. Mittels vollständiger Induktion sieht man nun leicht ein, daß $E_i = \{a\in\mathbb{Z}: |a|\leq 2^i-1\}$ gilt. Insbesondere ergibt sich hieraus $\mathbb{Z}=E_\infty$, d.h. $\mathbb{Z}$ ist euklidisch.

Etwas komplizierter liegen die Dinge in imaginärquadratischen Zahlkörpern. Ist $m \neq -1, -3$, so enthält $D(m)$ (wir werden künftig den Ring ganzer Zahlen in $\mathbb{Q}(\sqrt{m})$ mit $D(m)$ bezeichnen) für $m<0$ bekanntlich nur die Einheiten $+1$ und -1; in diesen Fällen ist also $E_1 = \{0, +1, -1\}$. E_2 besteht nun aus allen $a \in D(m)$, für die jede Restklasse mod a eines der drei Elemente 0, 1 oder -1 enthält. Wegen $|R/aR| = N_{K/\mathbb{Q}}(a)$ ist dies offenbar nur dann möglich, wenn $N_{K/\mathbb{Q}}(a) \leq 3$ ist. Die einzigen imaginärquadratischen Ringe, die Elemente der Norm 2 oder 3 enthalten, sind aber $D(m)$ für $m=-1, -2, -3, -7, -11$; für alle andern $D(m)$ ist also $E_1 = E_2 = \ldots = E_\infty = \{0, 1, -1\}$, und wir haben

(0.4) Sei $m<0$ und $R=D(m)$; dann ist R genau für die Werte $m=-1, -2, -3, -7, -11$ euklidisch, und in diesen Fällen ist die Norm eine euklidische Funktion. Für alle andern Werte von m ist $E_1 = E_2 = \ldots = E_\infty = \{0, 1, -1\}$.

Insbesondere sind also die Hauptidealringe $D(m)$ mit $m = -19, -43, -67, -163$ nicht normeuklidisch. Daß $D(m)$ für die oben angegebenen Werte von m normeuklidisch ist, stammt von Gauß ($m=-1, -3$), bzw. von Dedekind (1893) und Dickson (1927). Die beiden letzteren haben auch bemerkt, daß es keine andern normeuklidischen $D(m)$ mit $m<0$ gibt. Die weitergehende Aussage (0.4) dagegen stammt von Motzkin (1949) und unabhängig davon von Dubois und Steger (1958). Narkiewicz schreibt (1967, p. 175), daß Dubois und Steger darüberhinaus gezeigt hätten, daß jede euklidische Funktion f auf $D(m)$, $m<0$, mit der Norm übereinstimmen muß, was aber weder historisch (die beiden haben das nicht behauptet) noch mathematisch wahr ist (denn für $m = -1, -2, -3, -7, -11$ ist ja auch die minimale euklidische Funktion ein euklidischer Algorithmus auf $D(m)$, und dieser unterscheidet sich von der Norm). Weitere Beweise von (0.4) haben Stewart und Tall (1974) ih ihrem Lehrbuch "Algebraic number theory" und Chastro Chadid (1984) gegeben. Schließlich hat Campoli (1988) noch einmal gezeigt, daß $D(-19)$ zwar Hauptidealring, aber nicht euklidisch ist. Allen Beweisen gemeinsam ist die Konstruktion einer Nichteinheit der Norm ≤ 3 in einem euklidischen $D(m)$.

Für die Ringe $D(-1)$ und $D(-3)$ hat Lenstra (1974) die Mengen E_i explizit bestimmt; ansonsten kennt man nur einige elementare Eigenschaften der E_i:

(0.5) Sei R ein Zahlring; dann gilt

i) Ist $a \in E_\infty$, dann ist jeder Teiler des Ideals aR ein Hauptideal.

ii) Ist $a = p_1 p_2 \ldots p_m$ die Primzerlegung von $a \in R$, dann liegt a nicht in E_m.

iii) Für alle $i \in \mathbb{N}$ ist $E_i \neq R$.

iv) Es gilt $E_i R^\times = E_i$ d.h. mit $a \in E_i$ und $u \in R^\times$ ist auch $au \in E_i$.

v) Ist $K/\mathbb{Q}$ galoisch, dann ist $E_i^\sigma = E_i$ für alle $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Bew.: i) Sei $a \in E_i$; ist dann P ein Primideal in R, welches (a) teilt, dann gibt es ein $p_o \in R$ mit $P = (a, p_o)$ (denn jedes Ideal in einem Zahlkörper wird von maximal zwei Elementen erzeugt, wobei man $a \in P$ beliebig vorgeben darf; sh. z.B. Cohn 1978). Wegen $a \in E_i$ existiert nun ein $p_1 \in E_{i-1}$ mit $p_o \equiv p_1 \mod a$. Damit ist $P = (a, p_o) = (a, p_1)$. Ersetzt man in obigem Gedankengang $a \in E_i$ durch $p_1 \in E_{i-1}$, so folgt $P = (p_1, p_2)$ für ein $p_2 \in E_{i-2}$ usw. Schließlich erhalten wir $P = (p_{i-2}, p_{i-1})$ für ein $p_{i-1} \in E_1$ (möglicherweise tritt dies auch schon früher ein). Da P prim ist, kann p_{i-1} keine Einheit sein. Folglich ist $p_{i-1} = 0$ und $P = (p_{i-2})$ ein Hauptideal.

ii) Die Behauptung ist richtig für $m = 0, 1$; sei sie nun bewiesen für alle $i \in \mathbb{N}$ mit $i < k$ und sei $a \in E_k$. Wir nehmen an, es sei die Anzahl m der Faktoren von a größergleich k und wählen einen Primfaktor p von a. Dann ist $a/p \equiv e \mod a$ für ein $e \in E_{k-1}$, und es ist $e \neq 0$ (sonst wäre $a|a$). Nun gilt aber $e \equiv 0 \mod (a/p)$, d.h. $e \in E_{k-1}$ hat k-1 Primfaktoren, und dies widerspricht der Induktionsvoraussetzung.

iii) folgt sofort aus ii), wenn man beachtet, daß es in R unendlich viele Primideale gibt (nämlich mindestens eines über jeder rationalen Primzahl).

iv) folgt ebenfalls sofort, und zwar wegen $R/(a) \cong R/(au)$.

v) Die Behauptung ist richtig für j=0. Gilt sie für $j = k-1$ und ist $a \in E_k$ dann gibt es zu jedem $b \in R$ ein $c \in E_{k-1}$ mit $b \equiv c \mod a$. Also ist $b^\sigma \equiv c^\sigma \mod a^\sigma$, und nach Induktionsvoraussetzung ist $c^\sigma \in E_{k-1}$. Da mit b auch b^σ ganz R durchläuft, folgt $a^\sigma \in E_k$ und damit die Behauptung.

Damit sind wir in der Lage, $M(f_o)$ für die minimale euklidische Funktion f_o zu bestimmen. Da R euklidisch bezüglich f_o ist, gilt sicher $M(f_o) \leq 1$. Sei nun ein $b \in E_k \setminus E_{k-1}$ gegeben. Dann existiert ein $a \in R$ mit $a \equiv r \mod b$, sodaß $r \in E_{k-1} \setminus E_{k-2}$ gilt. Damit ist $a = bq + r$ und $f_o(r)/f_o(b) = (k-1)/k$; wegen (0.6,iii) dürfen wir k beliebig groß werden lassen, und dies zeigt $M(f_o) \geq 1$.

Man wird sich nun fragen, ob es Zahlringe gibt, die zwar bezüglich f_o, nicht aber bezüglich der Norm euklidisch sind. Bis heute ist kein einziger solcher Zahlring bekannt. Es wäre allerdings etwas voreilig, daraus auf irgendeine mathématische Wahrheit schließen zu wollen: falls nämlich gewisse Riemannsche Vermutungen richtig sind, ist jeder Zahlring mit Klassenzahl 1 und unendlicher Einheitengruppe euklidisch bezüglich f_o; dieses Resultat stammt von Weinberger (1971) und beruht auf einer Verallgemeinerung von Hooleys "Beweis" der Artinschen Vermutung über Primitivwurzeln (Hooley hatte diese Vermutung 1967 unter Annahme der Riemannschen Vermutung bewiesen). Für einen Beweis dieser Aussage verweisen wir auf Weinberger (1971) und Lenstra (1974), für Näheres über die Artinsche Vermutung auf Gupta, Murty, Murty (1987), Murty (1987) und Narkiewicz (1988). Hier wollen wir nur kurz andeuten, was die minimale euklidische Funktion mit Primitivwurzeln zu tun hat.

Dazu sei $a \in R$ prim; ist dann die Einheit $u \in R^\times$ eine Primitivwurzel mod a, dann gilt $a \in E_2$, weil die Potenzen von u zusammen mit 0 ein vollständiges Restsystem mod a bilden und als Einheiten in E_1 liegen. Ist u Primitivwurzel für "viele" $a \in R$, so wird E_2 "groß" und man hat gute Chancen, $R = E_\infty$ nachzuweisen. In der Tat hat Weinberger gezeigt, daß man bereits an E_3 ablesen kann, ob $R = E_\infty$ ist oder nicht.

Wir kommen nun zur Definition von k-stufig euklidischen Ringen (sh. dazu die Arbeiten von Cooke (1976/1977), sowie Cooke und Weinberger (1975)). Seien dazu $a,b \in R\setminus\{0\}$; eine Folge von Gleichungen

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

wobei OBdA von zwei aufeinanderfolgenden q_i mindestens eines und außerdem q_k von 0 verschieden sind, heißt eine ***von (a,b) ausgehende Teilerkette der Länge k;*** ist $r_k = 0$, so nennt man sie ***abbrechend.*** Eine Abbildung $f: R \to \mathbb{N}$ heißt eine ***k-stufige euklidische Funktion auf R,*** wenn (E-1) erfüllt ist und es für alle $a,b \in R\setminus\{0\}$ eine von (a,b) ausgehende Teilerkette der Länge k gibt mit $f(r_k) < f(b)$. Gibt es ein solches f, dann heißt R ***k-stufig euklidisch bezüglich f.*** Schließlich nennen wir R ***quasi-euklidisch,*** wenn es für alle $a,b \in R\setminus\{0\}$ eine von (a,b) ausgehende, abbrechende Teilerkette gibt (man beachte, daß die Eigenschaft quasi-euklidisch nicht von irgendwelchen Funktionen abhängt). Statt quasi-euklidisch hat Cooke den Begriff ω-stufig euklidisch gewählt.

Wir zeigen zuerst, daß die in der Literatur auftauchenden Definitionen quasi-euklidischer Ringe (z.B. in Cooke (1976) , Bougaut (1976, 1980) oder Leutbecher (1977/78)) alle gleichbedeutend sind:

(0.6) Sei R ein Ring; dann sind äquivalent:

i) R ist quasi-euklidisch;

ii) für alle $a,b \in R\setminus\{0\}$ existiert ein $k \in \mathbb{N}$ und eine von (a,b) ausgehende, abbrechende Teilerkette; iii) es gibt eine Funktion $\Phi: R \times R \to \mathbb{N}$, sodaß für alle $a,b \in R\setminus\{0\}$ Zahlen $q,r \in R$ existieren mit $a = bq + r$ und $\Phi(b,r) < \Phi(a,b)$.

Bem.: Funktionen, wie sie in iii) beschrieben sind, nennen wir ***quasi-euklidische Funktionen auf R.***

Bew.: i) $\Rightarrow$ iii): wir definieren $\Phi: R \times R \to \mathbb{N}$ durch

$$\Phi(a,b) = \min \{k \in \mathbb{N}: \text{es gibt eine von } (a,b) \text{ ausgehende, k-stufige abbrechende Teilerkette}\}.$$

Man rechnet leicht nach, daß Φ eine quasi-euklidische Funktion ist.

iii) $\Rightarrow$ i) Seien $a,b \in R\setminus\{0\}$ gegeben. Dann existieren $q_1,r_1 \in R$ mit $a=bq_1+r_1$ und $\Phi(b,r_1) < \Phi(a,b)$. Ist $r_1 = 0$, so sind wir fertig; andernfalls gibt es zu b,r_1 Zahlen $q_2,r_2 \in R$ mit $b = q_2r_1 + r_2$ und $\Phi(r_1, r_2) < \Phi(b,r_1)$. Indem wir diesen Schritt genügend oft wiederholen, erhalten wir eine von (a,b) ausgehende, abbrechende Teilerkette.

i) $\Rightarrow$ ii) ist klar.

ii) $\Rightarrow$ i): Seien $a,b \in R\setminus\{0\}$ gegeben. Dann gibt es ein $k \in \mathbb{N}$ und eine von (a,b) ausgehende k-stufige Teilerkette mit $f(r_k) < f(b)$. Ist bereits $r_k = 0$, so sind wir fertig. Andernfalls wiederholen wir diesen Schritt mit dem Paar (r_{k-1},r_k) und erhalten eine von (r_{k-1},r_k) ausgehende Teilerkette der Länge 1 mit $f(r_{k-1}) < f(r_k)$ usw. Indem wir diese Teilerketten aneinanderhängen, bekommen wir eine von (a,b) ausgehende, abbrechende Teilerkette.

Die Implikation ii) $\Rightarrow$ i) zeigt, daß jeder k-stufig euklidische Ring auch quasi-euklidisch ist.

Betrachtet man eine von (a,b) ausgehende Teilerkette mit $r_{k-1} \neq 0$ und $r_k = 0$, so stellt man fest, daß $(a,b) = (r_{k-1})$ ist. Mittels vollständiger Induktion kann man dann folgern, daß in quasi-euklidischen Ringen jedes endlich erzeugte Ideal ein Hauptideal ist. Jedoch sind quasi-euklidische Ringe nicht notwendig Hauptidealringe, wie das folgende Beispiel belegt:
Sei A der Ring aller ganzen algebraischen Zahlen; jedes endlich erzeugte Ideal in A ist zwar Hauptideal, dennoch ist A bekanntlich kein Hauptidealring. Insbesondere kann A nicht euklidisch sein; dagegen ist A 2-stufig euklidisch bezüglich jeder Funktion, die (E-1) erfüllt: sind nämlich $a,b \in A$ teilerfremd (d.h. ist $(a,b)=A$), so gibt es nach Lenstra (1973) ein $q \in A$, sodaß $a-bq$ eine Einheit in A ist. Daher haben solche a,b eine abbrechende Teilerkette der Länge ≤ 2. Sind a und b aber nicht teilerfremd, so wähle man ein $d \in A$ mit $(d)=(a,b)$, setze dann $a'=a/d$, $b'=b/d$ und multipliziere die von (a',b') ausgehende, abbrechende Teilerkette der Länge 2 mit d.

Zur Untersuchung k-stufiger euklidischer Funktionen führen wir ein Analogon zu M(f) ein, indem wir definieren:

$$M^k(f) := \inf \{x \in \mathbb{R}: \text{ für alle } a,b \in R\setminus\{0\} \text{ existiert eine von } (a,b) \text{ ausgehende Teilerkette mit } f(r_k) < x \cdot f(b)\}.$$

Da die Bezeichnungen $M_2(f)$, $M_3(f)$ usw. für das zweite, dritte usw. Minimum von f schon fast klassisch sind, haben wir $M^k(f)$ oben indiziert. Wir haben damit die Ungleichungskette

$$M(f) = M^1(f) \geq M^2(f) \geq M^3(f) \geq \ldots \geq M^\infty(f) := \lim_{k\to\infty} M^k(f)$$

(dieser Grenzwert existiert, da die Folge $M^k(f)$ eine monoton fallende, durch 0 nach unten beschränkte Folge reeller Zahlen ist).

Zur Beschreibung k-stufiger Teilerketten in einem Ring R haben sich Kettenbrüche mit Koeffizienten aus R bewährt: ist eine Folge $q_1, \ldots, q_k \in R$ gegeben (wobei von zwei aufeinanderfolgenden q mindestens eines und außerdem noch q von 0 verschieden ist), so definiert man

$$[q_1] = q_1 = a_1/b_1 \qquad \text{mit } a_1=q_1,\ b_1=1$$
$$[q_1,q_2] = q_1 + 1/q_2 = a_2/b_2 \qquad \text{mit } a_2=q_1q_2+1,\ b_2=q_2,$$
$$\ldots$$
$$[q_1, \ldots, q_k] = a_k/b_k \qquad \text{mit } a_k=q_ka_{k-1}+a_{k-2},\ b_k=q_kb_{k-1}+b_{k-2}.$$

Man sieht dann leicht ein, daß $[q_1, \ldots, q_k] = [q_1, \ldots, q_{k-1} + 1/q_k]$ gilt, und daraus folgt durch vollständige Induktion

$$[q_1, \ldots, q_k] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}.$$

Diese letzte Identität wiederum impliziert sofort $[q_1, \ldots, q_k] = q_1 + 1/[q_2, \ldots, q_k]$ Nennt man a_k den Zähler und b_k den Nenner des Kettenbruchs, so hat man also

(0.7) Der Nenner von $[q_1, \ldots, q_k]$ ist gleich dem Zähler von $[q_2, \ldots, q_k]$.

Mittels vollständiger Induktion folgt jetzt

(0.8). Sind $a,b \in R\setminus\{0\}$ und ist r_k der letzte Rest der von (a,b) ausgehenden Teilerkette mit den Quotienten $q_1, \ldots, q_k$, dann gilt

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

Ist f eine multiplikative Funktion, so kann man f multiplikativ von R nach K fortsetzen, und wegen (0.8) ist genau dann $f(r_k) < f(b)$, wenn $f(a/b - a_k/b_k) < 1$ gilt, damit erhält man

(0.9) Ein Ring R ist genau dann k-stufig normeuklidisch bezüglich einer multiplikativen Funktion f, wenn es zu jedem $a/b \in K$ einen Kettenbruch $[q_1, \ldots, q_l] = a_l/b_l$ der Länge $l \le k$ gibt, sodaß die Ungleichung

$$f\left(\frac{a}{b} - \frac{a_l}{b_l}\right) < f\left(\frac{1}{b_l}\right)$$

erfüllt ist.

Der Unterschied zum gewöhnlichen EA läßt sich also folgendermaßen in Worte fassen: in euklidischen Ringen läßt sich ein $x \in K$ so durch ein $y \in R$ approximieren, daß $f(x-y)<1$ wird; in einem k-stufig euklidischem Ring dagegen darf man y aus der R umfassenden Menge der Kettenbrüche der Länge $\leq k$ wählen, allerdings muß die Approximation "genauer" sein.

Nun ist es i.A. recht schwer, einen Kettenbruch (auch nur der Länge 2) als solchen zu erkennen; so ist z.B.

$$\frac{\sqrt{14}}{2} = -2 + \frac{1}{4-\sqrt{14}} = [-2, 4-\sqrt{14}]$$

ein Kettenbruch der Länge 2 mit Nenner $4-\sqrt{14}$, während $\frac{1+\sqrt{14}}{2}$ kein Kettenbruch der Länge 2 ist. Um dies zu beweisen, verwenden wir

(0.10) Ist a_k/b_k ein Kettenbruch und gilt $a/b = a_k/b_k$, dann ist $b_k | b$.

Bew.: Mittels vollständiger Induktion zeigt man $a_k b_{k-1} - a_{k-1} b_k = (-1)^{k-1}$. Multipliziert man diese Identität mit b, so folgt $ba_k b_{k-1} - ba_{k-1} b_k = (-1)^{k-1} b$. Wegen $ab_k = a_k b$ teilt b_k die linke und damit auch die rechter Seite der letzten Gleichung.

Wäre nun $(1+\sqrt{14})/2 = [q_1, q_2] = (1+q_1 q_2)/q_2$ ein Kettenbruch der Länge 2, so müßte $q_2 | 2$ gelten; da sich aber $(1+\sqrt{14})/2$ nicht mehr kürzen läßt, gilt auch $2 | q_2$. Folglich ist $q_2 = 2e$ für eine Einheit $e \in R^\times$. Nun ist aber $u = 15+4\sqrt{14}$ die FE von R, sodaß jede Einheit $\equiv 1 \bmod 2$ ist. Insbesondere ist $e \equiv 1 \bmod 2$, und es müßte $(1+\sqrt{14})e \equiv 1+\sqrt{14} \equiv 1 \equiv 1 + q_1 q_2 \bmod 2$ gelten, was offenbar falsch ist.

Um nun ein Kriterium herzuleiten, das es uns erlaubt, gewisse Zahlen als Kettenbrüche zu schreiben, führen wir die Mengen E'_j ein, die wie folgt definiert sind: $E'_0 = \{0\}$, und

$E'_j \setminus E'_{j-1} = \{a \in R$: jede prime Restklasse mod a hat einen Vertreter aus $E'_{j-1}\}$.

Man stellt dann fest, daß $E'_0 = E_0$, $E'_1 = E_1$, und $E'_j \subset E_j$ für $j \geq 2$ gilt, wobei die letzte Inklusion i.A. echt ist: für $D(-5)$ ist nämlich $E_1 = E_2 = \ldots = E_\infty = \{0,-1,+1\}$, während $E'_1 = E'_2 = \ldots = E'_\infty = \{0, \pm 1, \pm 1 \pm \sqrt{-5}\}$ gilt. Das bereits angekündigte Kriterium lautet nun

(0.11) Seien $a,b \in R \setminus \{0\}$, $b \in E'_k$, und $(a,b)=1$; dann ist a/b ein Kettenbruch der Länge $\leq k$ mit Nenner ub, wo $u \in R^\times$ eine Einheit in R ist.

Bew.: Ist k=1, so ist b eine Einheit und $a/b = q_1 \in R$ ein Kettenbruch der Länge 1 mit Nenner $1 = bu$, wo $u = 1/b$ Einheit in R ist.

Sei nun die Behauptung bewiesen für alle $j<k$ und $b \in E'_k$. Wegen $(a,b)=1$ liegt a in einer primen Restklasse mod b, folglich gibt es ein $e \in E'_{k-1}$ mit $a \equiv e \bmod b$, d.h. es existiert ein $q_1 \in R$ mit $a = q_1 b + e$. Jetzt sehen wir, daß $(b,e) = (b,a) = 1$ und $a/b = q_1 + e/b = q_1 + 1/(b/e)$ ist.

Nach Induktionsvoraussetzung ist nun b/e ein Kettenbruch der Länge $\leq k-1$, dessen Nenner (und damit auch dessen Zähler) mit e (bzw. mit b) bis auf einen Faktor $u \in R^\times$ übereinstimmt. Schreibt man $b/e = [q_2, \ldots, q_k]$, so ist $a/b = [q_1, \ldots, q_k]$, und (0.7) zeigt, daß a/b ein Kettenbruch der Länge $\leq k$ mit Nenner bu ist.

Als Beispiel zeigen wir, wie man (0.11) anwenden kann, um $(1+\sqrt{14})/2$ als Kettenbruch zu schreiben. Zuerst beachten wir $(1+\sqrt{14})/2 = -1 + (3+\sqrt{14})/2$ (damit haben wir die Norm des Nenners klein gemacht) und behaupten dann, daß $a = 3+\sqrt{14} \in E_2'$ ist. Dazu müssen wir zeigen, daß jede prime Restklasse mod a eine Einheit enthält. Dies sehen wir so ein: es gilt $u = 15+4\sqrt{14} \equiv 3 \bmod a$ (man beachte einfach $\sqrt{14} \equiv -3 \bmod a$), also ist $u^2 \equiv 4$, $u^3 \equiv 2$, $u^4 \equiv 1 \bmod a$. Wegen $|N_{K/\mathbb{Q}}(a)| = 5$ ist u damit Primitivwurzel mod a.

Insbesondere ist jetzt $2 \equiv -u \bmod a$, und wir erhalten

$$\frac{2}{a} = \frac{-u}{a} + 1 + \sqrt{14} = 1 + \sqrt{14} + \frac{1}{-a/u}.$$

Wegen $-a/u = 11 - 3\sqrt{14}$ haben wir $(1 + \sqrt{14})/2 = [-1, 1 + \sqrt{14}, 11 - 3\sqrt{14}]$, d.h. $(1 + \sqrt{14})/2$ ist ein Kettenbruch der Länge 2.

Wir beweisen nun eine wichtige Eigenschaft der Mengen E_j' (sh. § 1), die trivialer aussieht als sie ist, nämlich

(0.12) Ist $c \in E_k'$ und b|c für ein $b \in R$, dann ist auch $b \in E_k'$.

Bew.: Wir werden etwas mehr zeigen: sind B, C ganze Ideale in R (nicht notwendig Hauptideale) und ist B|C, dann gilt: hat jede prime Restklasse mod C einen Vertreter in E_k', dann gilt dasselbe für die primen Restklassen mod B. Indem wir Induktion über die Anzahl der Primidealteiler von CB^{-1} machen, dürfen wir C=BP für ein Primideal P annehmen.
Sei nun ein $r \in R$ gegeben mit $(r) + B = R$; wir suchen ein $e \in E_{k-1}'$ mit der Eigenschaft $r \equiv e \bmod B$. Dazu unterscheiden wir:

a) $B + P = R$: dann gibt es nach dem chinesischen Restsatz ein $s \in R$ das den Kongruenzen $s \equiv r \bmod B$ und $s \equiv 1 \bmod P$ genügt. Mit diesem s gilt dann $(s) + C = (s) + BP = R$, und weil jede prime Restklasse mod C nach Voraussetzung einen Repräsentanten $e \in E_{k-1}'$ hat, ist $s \equiv e \bmod C$, also erst recht $r \equiv s \equiv e \bmod B$.

b) $B \equiv 0 \bmod P$: dann ist auch $(r) + BP = R$, und wir finden sofort ein $e \in E_{k-1}'$ mit $r \equiv e \bmod C$, womit erst recht $r \equiv e \bmod B$ ist.

Das war zu zeigen.

Als nächstes zeigen wir ein Analogon zu (0.1):

(0.13) Sei $b \in R \setminus E_2'$; dann ist $M^2(f) \geq 1/f(b)$.

Bew.: Sei $b \in R \setminus E_2'$. Dann gibt es ein $a \in R$ mit $(a,b) = 1$, sodaß a keiner Einheit kongruent mod b ist. Nun setzen wir $a = bq_1 + r_1$, $b = r_1q_2 + r_2$; wäre $r_2 = 0$, so folgt $r_1 | b$ und $r_1 | a$, also $r_1 | (a,b) = 1$. Damit wäre r_2 Einheit im Widerspruch zu $a \equiv r_1 \bmod b$ und der Wahl von a. Die Behauptung folgt nun wie in (0.1).

Auch (0.13) ist bestmöglich in dem Sinne, daß die angegebene Schranke manchmal exakt ist. So ist z.B. für $R = D(6)$ $M^2(f) = 1/4$, wenn f der Absolutbetrag der Norm ist, wobei die Ungleichung $M^2(f) \geq 1/4$ aus (0.13) folgt, weil $2 \in R\ E_2'$ ist.

Man bemerkt nun, daß man (0.1) und (0.13) in folgender Form aufschreiben kann: Sei $b \in R \setminus E_1'$; dann ist $M(f) \geq 1/f(b)$. Der Fall k=1 entspricht dabei (0.1), der Fall k = 2 dagegen (0.13). Ob diese Aussage allerdings auch für k = 3 gilt, ist zweifelhaft.

Ein weiterer interessanter Begriff zur Beschreibung k-stufig euklidischer Ringe stammt von Cooke und Weinberger (1975): Sei R ein Ring (hier also Integritätsbereich mit Eins) und K sein Quotientenkörper; existiert dann eine von (a,b) ausgehende Teilerkette der Länge $\leq k$ mit $f(r_k) < f(b)$ für $a,b \in R \setminus \{0\}$, so heißt K ***in x=a/b k-stufig euklidisch bezüglich f.*** Die Menge aller $x \in K$, in denen K k-stufig euklidisch bezüglich f ist, wollen wir mit F_k bezeichnen. Damit ist $F_1 \subset F_2 \subset \ldots \subset F_\infty = \bigcup_{j=1}^{\infty} F_j \subset K$.

Offenbar ist R genau dann k-stufig euklidisch bezüglich f, wenn bereits $F_k = K$ ist, und quasi-euklidisch, wenn $F_\infty = K$ ist. gibt es nun ein $k \in \mathbb{N}$ derart, daß $F_k = F_\infty$ ist (unabhängig davon, ob $F_\infty = K$ ist oder nicht), so nennt man das kleinste solche k die ***euklidische Tiefe von K bezüglich f.***

Cooke und Weinberger konnten 1975 folgende Aussagen beweisen:

(0.14) Sei R der Ring ganzer Zahlen in einem algebraischen Zahlkörper K mit Einheitenrang ≥ 1, und sei f der Absolutbetrag der Norm. Sind dann gewisse Riemannsche Vermutungen richtig, dann gibt es für alle $a,b \in R$ mit $(a,b)=1$ eine von (a,b) ausgehende, abbrechende Teilerkette der Länge $k \leq 5$. Hat K außerdem eine reelle Einbettung, so gibt es sogar solche der Länge $k \leq 3$.

Aus diesem Satz leiten sie dann folgende Korollare ab:

(0.15) Es ist $F_3 = F_\infty$: die euklidische Tiefe von K ist ≤ 5. Hat K eine reelle Einbettung, so ist bereits $F_3 = F_\infty$.

Bew.: Wir nehmen an, es gibt eine von (a,b) ausgehende, abbrechende Teilerkette der Länge k. Dann ist $(a,b) = (r_{k-1})$ ein Hauptideal, und indem wir $c = a/r_{k-1}$ und $d = b/r_{k-1}$ setzen, wird $(c,d) = 1$. Nach (0.14) gibt es dann eine von (c,d) ausgehende, abbrechende Teilerkette der Länge ≤ 5 (bzw. ≤ 3, falls K eine reelle Einbettung hat), und Multiplikation mit r_{k-1} liefert eine solche für (a,b).
Wir haben damit gezeigt, daß $x = a/b \in F_k$ sogar $x \in F_5$ (bzw. $x \in F_3$) impliziert, qued.

(0.16) Hat R Klassenzahl 1, dann ist R 4-stufig normeuklidisch; hat außerdem K eine reelle Einbettung, so ist R sogar 2-stufig normeuklidisch.

Bew.: Sei $x \in K$; wir dürfen $x = a/b$ mit $a,b \in R$, $(a,b)=1$ schreiben. Wir suchen eine von (a,b) ausgehende Teilerkette der Länge $l \leq 4$ mit $|N_{K/\mathbb{Q}}(r)| \leq |N_{K/\mathbb{Q}}(b)|$; für $|N_{K/\mathbb{Q}}(b)| = 1$ ist nichts zu zeigen. Ansonsten liefert (0.14) eine von (a,b) ausgehende, abbrechende Teilerkette der Länge $k \leq 5$; für diese ist r_{k-1} als Teiler von (a,b) eine Einheit, d.h. es existiert eine von (a,b) ausgehende Teilerkette der Länge 4 mit $1 = |N_{K/\mathbb{Q}}(r_{k-1})| \leq |N_{K/\mathbb{Q}}(b)|$. Entsprechend folgt die Behauptung, falls K eine reelle Einbettung besitzt.

Am Schluß ihrer Arbeit schreiben Cooke und Weinberger, daß man bei Berücksichtigung eines Theorems von Lenstra unter den Voraussetzungen von (0.14) eine von (a,b) ausgehende, abbrechende Teilerkette der Länge ≤ 4 erhält, falls R Klassenzahl 1 hat. Wie in (0.16) folgt dann, daß solche Ringe schon 3-euklidisch sind.

Wie es scheint, hat Cooke nicht bemerkt, daß man (0.15) ganz einfach verbessern kann; es gilt nämlich

(0.15') Die euklidische Tiefe ist ≤ 4; hat K eine reelle Einbettung, so gilt sogar $F_2 = F_\infty$.

Bew.: Im Beweis von (0.15) haben wir gesehen, daß sich $x = a/b$ als Kettenbruch a_k/b_k der Länge $k \leq 5$ schreiben läßt. Ist $b_k \in R^*$ eine Einheit, so ist a_k/b_k Kettenbruch der Länge 1 und somit nichts zu zeigen. Andernfalls ist wegen

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

$y = a_{k-1}/b_{k-1}$ ein Kettenbruch der Länge $k-1 \leq 4$, der x genügend genau approximiert, um $x \in F_4$ zu zeigen. Entsprechend folgt die Behauptung, wenn K eine reelle Einbettung besitzt.

Insbesondere haben also quadratische Zahlkörper euklidische Tiefe 2 (falls gewisse Riemannsche Vermutungen richtig sind). In § 2 werden wir z.B. sehen, daß die Körper $\mathbb{Q}(\sqrt{m})$ für m = 15, 26, 85 euklidische Tiefe 2 haben und daß hier $M^k(K) = 1$ für alle $k \geq 2$ gilt; dagegen hat $\mathbb{Q}(\sqrt{30})$ zwar ebenfalls euklidische Tiefe 2 , jedoch ist hier $M^k(K) = 3/2$ für alle $k \geq 2$.

Schließlich wollen wir der Ähnlichkeit der Mengen E_k und E'_k eine Deutung geben: dazu nennen wir eine Abbildung $f: R \to \mathbb{N}$ semi-euklidisch auf R, wenn für alle $a,b \in R\setminus\{0\}$ gilt:

(E-1) $f(a) = 0 \Leftrightarrow a = 0$;

(E'-2) ist $(a,b) = 1$ so gibt es ein $q \in R$ mit $f(a-bq) < f(b)$.

Falls ein solches f existiert, heißt der Ring R semi-euklidisch. Wie für gewöhnlich euklidische Ringe gilt nun

(0.17) Ein Ring R ist genau dann semi-euklidisch, wenn $R = E_\infty$ gilt. In diesem Fall ist $f_o(a) = \min\{j \in \mathbb{N}: a \in E'_j\}$ eine semi-euklidische Funktion auf R, und diese stimmt mit der durch $f_m(a) = \min\{f(a): f$ ist semi-euklidische Funktion auf R$\}$ definierten minimalen semi-euklidischen Funktion überein.

Der Beweis verläuft exakt wie im euklidischen Fall.

(0.18) Sei f multiplikativ; dann sind äquivalent:

i) für alle $a,b \in R\setminus\{0\}$ mit $(a,b) = 1$ existiert ein $q \in R$ mit $f(a-bq) < f(b)$;

ii) für alle $a,b \in R\setminus\{0\}$ mit $(a,b) = d$ existiert ein $q \in R$ mit $f(a-bq) < f(b)$.

Bew.: Die Richtung ii) $\Rightarrow$ i) ist trivial; sei also i) richtig. Ist dann $(a,b) = (d)$ für ein $d \in R$, so setzen wir $a' = a/d$, $b' = b/d$, und finden wegen i) ein $q \in R$ mit $f(a'-qb') < f(b')$. Weil f multiplikativ ist, folgt dann $f(a-bq) < f(b)$ durch Multiplikation mit $f(d)$.

Als Korollar hiervon hat man sofort

(0.19) Ein Hauptidealring R ist genau dann semi-euklidisch bezüglich einer multiplikativen Funktion f, wenn R euklidisch bezüglich f ist.

Will man daher Zahlringe finden, die semi-euklidisch, aber nicht euklidisch bezüglich der Norm sind, so muß man unter Ringen mit Klassenzahl > 1 suchen. Eine elementare, aber etwas langwierige Rechnung zeigt

(0.20) Ist $R = D(m)$, $m \leq 0$ quadratfrei, dann ist R genau dann semi- euklidisch bezüglich einer Funktion f, wenn R schon euklidisch ist.

Als Beispiel betrachten wir D(-5): hier ist $E_1' = \{0, -1, +1\}$ und für alle $a \in E_2'$ muß $\Phi(a) \leq 2$ gelten (weil E_1' nur zwei von 0 verschiedene Elemente enthält). Also ist $N_{K/Q}(a) \in \{2, 3, 4, 6\}$ und wir sehen $a \in \{\pm 2, \pm 1 \pm \sqrt{-5}\}$; nun ist $\{-1, +1\}$ zwar ein primes Restsystem mod $(\pm 1 \pm \sqrt{-5})$, aber nicht mod 2, und wir haben $E_2' = \{0, \pm 1, \pm 1 \pm \sqrt{-5}\}$. Jetzt betrachtet man alle $a \in D(-5)$ mit $\Phi(a) \leq 6$ und findet $E_2' = E_3' = \ldots = E_\infty'$, und aus (0.14) folgt, daß D(-5) nicht semi-euklidisch ist.

Aus dem Beweis von (0.20) ergibt sich übrigens , daß im Ring D(-15) $E_2' \neq E_3' = E_4'$ gilt, während für alle andern D(m) bereits $E_2' = E_3'$ ist.

Schon der reellquadratische Fall zeigt, daß (0.20) für algebraische Zahlkörper nicht typisch ist. So zeigten beispiels- weise Johnson, Queen und Sevilla (1985), daß D(10) und D(65) semi-euklidische Ringe bezüglich der Norm mit Klassenzahl 2 sind. Wahrscheinlich sind dies sogar die einzigen reellquadratischen, bezüglich der Norm semi-euklidischen Ringe mit von 1 verschiedener Klassenzahl. Wir werden später sehen, daß auch die Ringe ganzer Zahlen in den biquadratischen Körpern $Q(\sqrt{-1}, \sqrt{15})$ und $Q(\sqrt{-3}, \sqrt{13})$ Klassenzahl 2 haben und semi-euklidisch sind.

In Analogie hierzu definieren wir k-stufig semi-euklidische Ringe durch die Forderung, daß es für alle $a,b \in R\setminus\{0\}$ mit (a,b) = 1 eine von (a,b) ausgehende Teilerkette der Länge $\leq k$ gibt mit $f(r_k) < f(b)$. Damit wäre auch klar, was man unter einem quasi- semi-euklidischen Ring zu verstehen hat; glücklicherweise existiert jedoch in der mathematischen Literatur bereits ein Begriff mit derselben Bedeutung: solche Ringe heißen GE_2-Ringe.

Zum Schluß dieses Paragraphen wollen wir zeigen, wie man die euklidischen Minima M(K) bestimmen kann, wenn K ein imaginärquadratischer Zahlkörper ist.

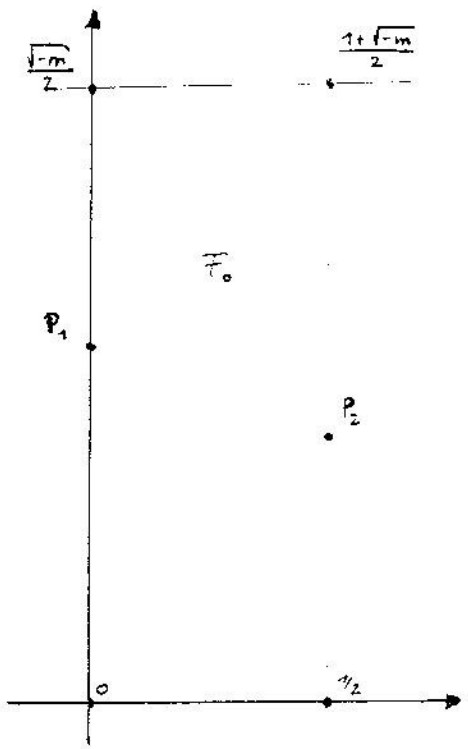
(0.21) Sei $R = D(m)$ imaginärquadratisch; dann gilt

$$M(K) = \begin{cases} \frac{1+|m|}{4}, & \text{falls } m \equiv 2, 3 \bmod 4 \\ \frac{(1+|m|)^2}{16|m|}, & \text{falls } m \equiv 1 \bmod 4. \end{cases}$$

Insbesondere haben wir für die euklidischen Ringe die folgende Tafel:

m	-1	-2	-3	-7	-11
M(K)	1/2	3/4	1/3	4/7	9/11

Bew.: Ist $m \equiv 2, 3 \bmod 4$, dann gibt es für alle $x \in K$ ein $y \in R$ mit $x-y = a+b\sqrt{m}$ und $|a|, |b| \leq 1/2$. Damit wird $N_{K/Q}(x-y) = a^2 - mb^2 \leq (1+|m|)/4$. Um auch $M(K) \geq (1+|m|)/4$ einzusehen, betrachten wir z.B. den Punkt $x = (1+\sqrt{m})/2$; für alle $y \in R$ mit $x-y = a+b\sqrt{m}$ ist dann offenbar $|a|, |b| \geq 1/2$, und es folgt $N_{K/Q}(x-y) \geq (1+|m|)/4$.



Im Falle $m \equiv 1 \bmod 4$ verwenden wir eine geometrische Methode: wir betten K via $a+b\sqrt{m} \longrightarrow (a,b\sqrt{|m|})$ in den $\mathbb{R}^2$ ein. Ist $\| \ \|$ die gewöhnliche euklidische Norm im $\mathbb{R}^2$, so stimmen $N_{K/\mathbb{Q}}$ und $\| \ \|^2$ überein in dem Sinne, daß $N_{K/\mathbb{Q}}(a+b\sqrt{m}) = \|(a,b\sqrt{|m|})\|$ ist. Um nun zu zeigen, daß es zu jedem $x \in K$ ein $y \in R$ gibt mit $N_{K/\mathbb{Q}}(x-y) < k$, dürfen wir uns auf diejenigen $x \in K$ mit $x = r+s\sqrt{m}$ und $|r|, |s| \leq 1/2$ beschränken, weil wir alle andern x durch Addition gewisser $y \in R$ erreichen können. Aus Symmetriegründen dürfen wir sogar $0 \leq r, s \leq 1/2$ annehmen. Wir setzen nun $k = (1+|m|)/4\sqrt{|m|}$ und behaupten, daß die Kreise um die Punkte 0 und $(1+\sqrt{m})$ (genauer um deren Bilder $(0, 0)$ und $(1/2, \sqrt{m}/2)$) mit Radius k ganz F_o bedecken, wo $F_o = \{x = r+s\sqrt{m}: 0 \leq r, s \leq 1/2\}$ ist. Dazu rechnen wir einfach nach, daß sich diese beiden Kreise in F_o genau in den Punkten $P_1 = (0 \ , (1+|m|)\sqrt{|m|}/4|m|)$ und $P_2 = (1/2 \ , (|m|-1)\sqrt{|m|}/4|m|$ schneiden . Bezeichnen wir die obige Einbettung mit φ , so gibt es also zu jedem $x \in K$ ein $y \in R$ mit $\|\varphi(x-y)\| \leq k$, d.h. mit $N_{K/\mathbb{Q}}(x-y) \leq k^2$ wie behauptet. Die Punkte P_1 und P_2 zeigen auch, daß diese Schranke bestmöglichst ist, womit wir alles bewiesen haben.

Zu (021) wollen wir noch einige Bemerkungen machen. Dazu sei $f: R \longrightarrow \mathbb{N}$ eine Funktion, die (E-1) erfüllt, $a,b \in R\setminus\{0\}$ und $M(f;a,b) = \inf \{f(a-bq)/f(b) : q \in R\}$; wir finden dann $M(f) = \sup \{M(f; a,b): a,b \in R\setminus\{0\}\}$. Ist f darüberhinaus multiplikativ, so dürfen wir einfacher $M(f;x) = \inf \{ f(x-q): q \in R\}$, $x = a/b$ schreiben. Sind nun $a,b \in R\setminus\{0\}$ und ist ein positives, reelles $\varepsilon > 0$ gegeben, so können wir, falls $M(f) < \infty$ ist, ein $q \in R$ finden mit $f(a-bq)/f(b) < M(f)+\varepsilon$. Dagegen ist es denkbar, daß wir kein $q \in R$ finden, sodaß $f(a-qb)/f(b) \leq M(f)$ wird (es könnte ja eine Folge $(q_n)_{n \in \mathbb{N}}$ geben mit $f(a-q_n b)/f(b) \longrightarrow M(f) + 0$ für $n \longrightarrow \infty$. Falls wir für alle $a,b \in R\setminus\{0\}$ die Ungleichung $f(a-qb)/f(b) \leq M(f)$ erfüllen können, so sagen wir, daß $M(f)$ ***erreicht*** wird. Wie das Beispiel der minimalen euklidischen Funktion zeigt, braucht es im Falle eines erreichten euklidischen Minimums $M(f)$ keine $a,b \in R$ zu geben mit $M(f;a,b) = M(f)$. Wie wir in (0.21) gesehen haben, ist dies aber in imaginärquadratischen Zahlkörpern der Fall, wenn man für f die Norm nimmt, nämlich für $P = (1+\sqrt{m})/2$, falls $m \equiv 2, 3 \bmod 4$ ist, und für die Punkte P_1 und P_2, falls $m \equiv 1 \bmod 4$ ist.

Wir setzen jetzt $C_1 = \{(a,b) \in R \times R: M(f; a,b) = M(f)\}$ und definieren $M_2(f) = \sup \{ M(f;a,b): (a,b) \in R \times R \setminus C_1 \}$. Ist $M_2(f) < M(f)$, so heißt $M(f)$ isoliert und $M_2(f)$ das ***zweite euklidische Minimum von R bezüglich f.*** Wie (0.21) zeigt, ist das euklidische Minimum bezüglich der Norm in imaginärquadratischen Zahlkörpern nicht isoliert. Dagegen haben Barnes und Swinnerton- Dyer vermutet, daß dies in Zahlkörpern mit Einheitenrang > 1 immer der Fall ist.

Man kann nun in dieser Art weitermachen und sich fragen, ob auch das zweite euklidische Minimum isoliert ist und dann dementsprechend $M_3(f)$ definieren usw. Wir werden sehen, daß es Zahlkörper gibt, die eine unendliche Kette $M_1(K)$, $M_2(K)$, ... von euklidischen Minima besitzen (wie z.B. $\mathbb{Q}(\sqrt{5})$), während in andern Zahlkörpern (wie $\mathbb{Q}(\sqrt{23})$) bereits $M_2(K)$ nicht isoliert ist. Schließlich kann man entsprechende Begriffsbildungen auch für die k-stufigen Minima $M_k(f)$ einführen.

ANMERKUNGEN ZU § 0

Wie wir schon eingangs erwähnten, war Gauß der erste , der einen algebraischen Zahlkörper $\neq \mathbb{Q}$ (nämlich $\mathbb{Q}(i)$) als normeuklidisch nachwies. Allerdings ist es nicht ganz richtig, daß er dies tat, um in $\mathbb{Z}[i]$ den Satz von der eindeutigen Primfaktorzerlegung zu beweisen. Dazu ging er nämlich wie folgt vor: in Art. 33 (sh. Werke II, theoria residuorum biquadraticum) benutzt er die Fermat'sche Erkenntnis, daß sich jedes prime $p \equiv 1 \bmod 4$ als Summe zweier Quadrate schreiben läßt, um zu zeigen, daß solche p in $\mathbb{Z}[i]$ zum Produkt zweier verschiedener Primfaktoren werden. Mit Hilfe dieser Tatsache führt er in Art. 37 die eindeutige Primfaktorzerlegung in $\mathbb{Z}[i]$ auf diejenige in $\mathbb{Z}$ zurück. Erst in Art. 46 beschreibt er dann den Euklidischen Algorithmus zur Bestimmung zweier Zahlen aus $\mathbb{Z}[i]$.

Den Vorschlag, in Zahlkörpern nach euklidischen Funktionen zu suchen, die vom Absolutbetrag der Norm verschieden sind, hat wohl als erster H. Hasse (1928) gemacht. Wie solche Funktionen aussehen könnten, haben Lenstra (1974) und Bedocchi (1985) beschrieben; wir werden in §10 auf deren Vorschläge zurück kommen. Der Begriff des Euklidischen Algorithmus, den wir ganz am Anfang dieses Paragraphen definiert haben, läßt sich noch verallgemeinern: so kann man in nichtkommutativen Ringen linkseuklidische (bzw. rechtseuklidische) Funktionen definieren und z.B. nach euklidischen Quaternionenalgebren fragen. Damit haben sich z.B. Dickson (1927) , Redei (1967) , Newman (1972), Brungs (1973) und Lenstra (1974, 1978) befaßt (sh. auch Felgner (1972)).

Weiter kann man statt Abbildungen $f:R \rightarrow \mathbb{N}$ Funktionen betrachten , die R in eine wohlgeordnete Gruppe W abbilden; Samuel (1971) hat gezeigt, daß die Forderung $W = \mathbb{N}$ in Ringen mit endlichen Restklassenkörpern keine Einschränkung ist in dem Sinne, daß ein Ring, der bezüglich einem $g: R \rightarrow W$ euklidisch ist, auch bezüglich einem geeigneten $f: R \rightarrow \mathbb{N}$ euklidisch ist. Dagegen hat Hiblot (1975) einen Ring konstruiert, für den beide Definitionen nicht äquivalent sind. Für eine gründliche Untersuchung solcher und ähnlicher Fragen verweisen wir auf Lenstra (1974) . Einen Zusammenhang der im Text nur kurz gestreiften GE_2- Ringe mit dem Euklidischen Algortihmus findet man bei Hurwitz (1932), P. Cohn (1966), Vaserstein(1972) und Cooke (1977).