§ 1 Kriterien für die Existenz des Euklidischen Algorithmus

Im Folgenden sei K algebraischer Zahlkörper und R der Ring ganzer Zahlen in K. Um zu entscheiden, ob R normeuklidisch ist oder nicht, hat man verschiedene Kriterien entwickelt, von denen wir einige beschreiben wollen. Dazu sei P ein Primideal in R; wir nennen ein Polynom

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$$

eisensteinsch bezüglich P, wenn $a_i \in P$ für $0 \le i \le n-1$ und $a_0 \in P \setminus P^2$ ist (man beachte, daß f normiert sein muß!). Das Eisensteinsche Irreduzibilitätskriterium besagt dann, daß solche Polynome über K(x) irreduzibel sind.

Wir wollen nun folgende Situation betrachten: es sei L/K eine endliche Körpererweiterung vom Grade (L:K) =n, S der Ring der ganzen Zahlen in L und Q ein Primideal in S über P:

$$\begin{array}{ccccc} L & \supset & S & \supset & Q \\ | & & | & & | \\ K & \supset & R & \supset & P \\ | & & | & & | \\ \mathbf{Q} & \supset & \mathbf{Z} & \supset & (p) \end{array}$$

Das Primideal P heißt rein verzweigt in L/K, wenn $PS = Q^n$ gilt. Bekanntlich ist ein Primideal P in L/K genau dann rein verzweigt, wenn die Erweiterung von der Wurzel eines bezüglich P eisensteinschen Polynoms erzeugt wird; der Vollständigkeit halber wollen wir die Beweise hier geben.

(1.1) Sei $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in R[x]$ eisensteinsch bezüglich P und α eine Wurzel von f; ist dann $L = K(\alpha)$, so gilt $(L:K) = n = \deg f$, und P ist rein verzweigt in L/K.

Bew.: f ist wegen des Eisensteinschen Irreduzibilitätskriteriums irreduzibel, folglich gilt (L:K) = n. Außerdem können wir $a_i S = PA_i$ schreiben für gewisse ganze Ideale A_i in S, wobei noch $A_0 \equiv 0 \bmod P$ gilt. Wegen $f(\alpha) = 0$ gilt $\alpha^n = -(a_{n-1}\alpha^{n-1} + \ldots + a_0) \in PS$. Sei nun Q irgendein Primideal in S über P; dann ist $\alpha^n \in Q$, also sogar $\alpha \in Q$, weil Q prim ist, und damit $a^n \in Q^n$. Schreibt man $\alpha^n S = (PS)B$ für ein ganzes Ideal B in S, so folgt $Q^n \mid \alpha^n S = (PS)B$. Wenn wir noch zeigen können, daß Q+B=S ist, haben wir $Q_n \mid PS$ und damit $Q_n = PS$.

Wir nehmen daher an, es sei $Q \mid B$; dann folgt aber $a_0 \in Q(PS)$ wegen $\alpha^n = -(a_{n-1}\alpha^{n-2} + \ldots + a_1)\alpha - a_0 \in Q(PS)$. Wegen $a_0 \in R$ und $Q \cap R = P$ impliziert dies aber $a_0 \in P^2$ im Widerspruch zur Voraussetzung.

(1.2) Sei P in L/K rein verzweigt, $\pi \in S$ und f das Hauptpolynom von π. Ist dann $\pi \in Q$ und $f(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_o \in R[x]$, dann gilt $a_i \in P$ für alle $0 \le i \le n-1$. Ist außerdem $\pi \in Q \setminus Q^2$, so ist f sogar eisensteinsch bezüglich P und damit gleich dem Minimalpolynom von π.

Bew.: Wegen $f(\pi)=0$ ist $a_o \equiv 0 \bmod \pi$, also $a_o \in Q \cap R = P$. Betrachtet man die Gleichung $f(\pi) = 0 \bmod Q^2$, so erhält man entsprechend $a_1 \equiv 0 \bmod P$ usw. Ist schließlich $\pi \in Q \setminus Q^2$ und wäre $a_o \in P^2$, so folgte $\pi^n \equiv 0 \bmod \pi P$ im Widerspruch zu $PS = Q^n$. Also ist f eisensteinsch bezüglich P.

Die Bedeutung rein verzweigter Primideale für diesen Paragraphen beruht auf

(1.3) Ist P rein verzweigt in L/K, dann gibt es zu jedem $\alpha \in S$ ein $a \in R$ mit $\alpha \equiv a \bmod Q$, und es gilt $N_{L/K}(\alpha) \equiv a^n \bmod P$.

Bew.: Sei $\alpha \in S$; wegen $S/Q \cong R/P$ (P ist rein verzweigt, und insbesondere hat Q den Trägheitsgrad 1 über P) existiert ein $a \in R$ mit $\alpha \equiv a \bmod Q$. Damit ist $\alpha - a \in Q$, und das Hauptpolynom von $\alpha - a$ hat nach (1.2) die Gestalt $Hp(\alpha - a; K)(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_o$ mit $a_i \in P$ für $0 \le i \le n-1$; also ist α Nullstelle von $(x-a)^n + a_{n-1}(x-a)^{n-1} + \ldots + a_o$, und wir sehen

$$N_{L/K}(\alpha) = a^n - a_{n-1} a^{n-1} + \ldots + (-1)^n a_o \equiv a^n \bmod P.$$

Alle bekannten Kriterien für die Existenz eines EA, die auf rein verzweigten Primidealen beruhen, lassen sich auf das folgende zurückführen:

(1.4) Sei B Produkt von paarweise verschiedenen, in L/K rein verzweigten Primidealen, $BS = C^n$, und C ein Hauptideal in S. Gibt es dann ein $x \in R$ mit $x^n \equiv e \bmod B$ für ein $e \in R$, und existiert kein $r \in R$ mit den Eigenschaften a), b) und c), dann ist $M(L) \ge k$.

a) $r \equiv e \bmod B$

b) $r = N_{L/K}(\alpha)$ für ein $\alpha \in S$

c) $|N_{K/\mathbf{Q}}(r)| < k \cdot \|B\|$.

Bew.: Wir nehmen an, es sei $M(L) < k$; wegen $C = (c)$ für ein $c \in S$ gibt es dann ein $q \in S$ mit $|N_{L/\mathbf{Q}}(x - qc)| < k \cdot |N_{L/\mathbf{Q}}(c)|$. Setzt man $\alpha = x - qc$, so wird $\alpha \equiv x \bmod C$ und $|N_{L/\mathbf{Q}}(\alpha)| < k \cdot \|C\|$. Mit $r = N_{L/K}(\alpha)$ wird jetzt

a) $r = N_{L/K}(\alpha) \equiv x^n \equiv e \bmod B$; nach (1.3) ist diese Kongruenz nämlich für jeden Primteiler P von B richtig. Da diese P nach Voraussetzung paarweise verschieden sind, ergibt sich die Behauptung aus dem chinesischen Restsatz.

b) $r = N_{L/K}(\alpha)$ gilt nach Konstruktion.

c) $|N_{K/\mathbf{Q}}(r)| = |N_{K/\mathbf{Q}}(N_{L/K}(\alpha))| = |N_{L/\mathbf{Q}}(\alpha)| < k\|C\| = k\|B\|$, denn für Primideale Q in S über P mit relativem Trägheitsgrad 1 ist $\|Q\|=\|P\|$, sodaß $\|C\|=\|B\|$ aus der Multiplikativität der Idealnorm folgt.

Da es nach Voraussetzung aber kein $r\in R$ mit den Eigenschaften a), b), c) gibt, muß $M(L)\geq k$ sein.

Wir wollen ausdrücklich bemerken, daß L auch dann nicht normeuklidisch ist, wenn wir in (1.4) nur k=1 wählen können: dann ist nämlich $M(N_{L/\mathbf{Q}};x,c) = 1$, d.h. es gibt kein $q\in R$ mit $|N_{L/\mathbf{Q}}(x-qc)| < |N_{L/\mathbf{Q}}(c)|$.

Bisher war (1.4) nur im Fall $K=\mathbf{Q}$, k=1 bekannt; um dieses Kriterium anwenden zu können, mußte $L/\mathbf{Q}$ also rein verzweigte Primideale enthalten. Die hier gegebene Version läßt sich dagegen auch dann anwenden, wenn es einen Zwischenkörper K mit $\mathbf{Q} \subset K \subset L$ gibt, sodaß L/K rein verzweigte Ideale besitzt (ein typisches Beispiel hierfür sind z.B. die Dirichlet'schen Zahlkörper, das sind quadratische Erweiterungen von $\mathbf{Q}(i)$, $i^2=-1$).

Die (bisher notwendige) Bedingung, daß $L/\mathbf{Q}$ rein verzweigte Primideale enthalten muß, hat letztendlich dazu geführt, daß über den Euklidischen Algorithmus in reinen Zahlkörpern (Cioffari 1979, Egami 1979, 1984) oder in zyklischen Zahlkörpern (Heilbronn 1950, 1951, Egami 1984) viel mehr bekannt ist als in Körpern, die keine rein verzweigten Primideale enthalten. Im Spezialfall $K=\mathbf{Q}$ wird aus (1.4)

(1.5) Sei $(L:\mathbf{Q})=n$, $f\in\mathbb{N}$ ein Produkt von in $L/\mathbf{Q}$ rein verzweigten, paarweise verschiedenen rationalen Primzahlen und $fS=C^n$ für ein Hauptideal C in S. Ist dann a ein n-ter Potenzrest mod f und sind alle $r\in\mathbf{Z}$ mit $a\equiv r \bmod f$ und $|r|<k\cdot f$ keine Normen aus S, dann ist M(L)>k. Darüberhinaus ist L nicht normeuklidisch, falls $k\geq 1$ gilt.

Bew.: (1.4) mit $K=\mathbf{Q}$, $B=(f)$, $e=a$ und $R=\mathbf{Z}$.

Für k=1 schließlich erhält man aus (1.5) das bisher bereits bekannte Kriterium (Egami 1979):

(1.6) Sei $(L:\mathbf{Q})=n$, $f\in\mathbb{N}$ Produkt von rein verzweigten, paarweise verschiedenen rationalen Primzahlen; gibt es dann $a,b\in\mathbb{N}$ mit $f=a+b$, sodaß a ein n-ter Potenzrest mod f ist und weder a noch -b Normen aus S sind, dann ist L nicht normeuklidisch.

Bew.: (1.5) mit k=1; man beachte, daß a und -b die einzigen $r\in\mathbf{Z}$ sind mit $r \equiv a \bmod f$ und $|r|< f$. Wir demonstrieren die Anwendung von (1.5) an einigen einfachen Beispielen:

1. $L=\mathbf{Q}(\sqrt{7})$, $f=14$, $a=9$; dann ist a quadratischer Rest mod 14, und die $r\in\mathbf{Z}$ mit $r\equiv a \bmod f$ sind $r = \ldots -19, -5, 9, 23, \ldots$ usw. Wählen wir nun $k=9/14$, so erfüllt nur $r=-5$ die Bedingung $|r| < k\cdot f = 9$; nun gibt es aber kein $\alpha\in S$ mit $N_{L/\mathbf{Q}}(\alpha)=-5$, denn das Primideal (5) bleibt beim Übergang von $\mathbf{Z}$ nach S träge wegen $(28/5)=-1$ (Legendre-Symbol). Also ist $M(L)\geq 9/14$. Um auch ein $z\in L$ zu finden mit $M(z)=9/14$ (wir haben hier statt $M(N_{L/\mathbf{Q}};z)$ einfach $M(z)$ geschrieben), müssen wir zuerst ein Hauptideal C mit Norm $f=14$ finden: ein solches ist z.B. $C = (7-3\sqrt{7})$. Dann brauchen wir noch ein $x\in\mathbf{Z}$ mit $x^2 \equiv a = 9 \bmod 14$, z.B. $x=3$, und wir haben $z=x/c = -(21+9\sqrt{7})/14$; wegen $M(z)=M(z-y)$ für jedes $y\in R$ brauchen wir z nur mod R anzugeben, d.h. wir haben jetzt $z \equiv (7+5\sqrt{7})/14 \bmod R$.

2. $L=\mathbf{Q}(\sqrt{10})$: um $M(L)\geq 3/2$ zu zeigen, verwenden wir $f=10$ und $a=5$; tatsächlich ist a wegen $5^2 \equiv 5 \bmod 10$ quadratischer Rest mod f. Die einzigen $r\in\mathbf{Z}$ mit $|r|<k\cdot f$ und $r\equiv 5 \bmod 10$ sind $r=\pm 5$; weil jedoch das Primideal über (5) kein Hauptideal in S ist, gibt es in S keine Elemente der Norm 5, und wir haben $M(L)\geq 3/2$.

3. $L=\mathbf{Q}(\sqrt{15})$: wir behaupten $M(L)\geq 7/5$ und verwenden dazu $f=15$, $a=6$. Damit wird $r\in\{-9, 6\}$. Weil nun das Primideal über (3) Hauptideal ist, sind alle Elemente der Norm 9 von der Form $3u^k$, wo $u=4+\sqrt{15}$ die FE von L ist. Wegen $N_{L/\mathbf{Q}}(u)=+1$ ist aber $N_{L/\mathbf{Q}}(3u^k)=+9$, d.h. es gibt in S kein α mit $N_{L/\mathbf{Q}}(\alpha)=-9$. Analog wird jedes Ideal der Norm 6 von einem Element der Form $\beta=(3+\sqrt{15})u$ erzeugt, und wegen $N_{L/\mathbf{Q}}(\beta)=-6$ gibt es in S keine Elemente der Norm +6. Dies war zu zeigen.

Das folgende Kriterium enthält (1.4) als Spezialfall (für $m = 0,1$) und ließe sich noch weiter verallgemeinern; wir werden es jedoch nur in der vorgestellten einfacheren Version benutzen:

(1.7) Es sei P ein Primideal in R mit $PS=Q^n$, B ein Produkt von paarweise verschiedenen Primidealen mit $B+P=R$, und es sei $B'=P^mB$, sowie $B'S=Q^{mn}C^n$ für ein Hauptideal Q^mC. Ist dann $x^n \equiv e \bmod P$ für $x,e\in R$, und existiert ein $y\in S$ mit $y\equiv x \bmod QC$, sodaß es kein $r\in R$ gibt mit den Eigenschaften

a) $r \equiv e \bmod PB$

b) $r=N_{L/K}(\alpha)$ für ein $\alpha\in S$ mit $\alpha \equiv y \bmod Q^m C$

c) $|N_{K/\mathbf{Q}}(r)| < k\cdot\|B\|$

dann ist $M(L)\geq k$.

Bew.: Sei $M(L)<k$; dann gibt es ein $\alpha\in S$ mit $\alpha\equiv y \bmod Q^m C$ und $|N_{L/\mathbf{Q}}(\alpha)| < k\cdot\|Q^mC\|$, sowie ein $x\in R$ mit $y\equiv x \bmod QC$ (denn QC ist Produkt von paarweise verschiedenen, rein verzweigten Primidealen). Mit $r=N_{L/K}(\alpha)$ lassen sich nun wie in (1.4) die Eigenschaften a), b), c) nachweisen.

Der Schwierigkeit bei der Formulierung von (1.7) liegt die folgende Tatsache zugrunde: aus $\alpha \equiv a \bmod Q$ folgt zwar $N_{L/K}(\alpha) \equiv a^n \bmod P$, aber aus $\alpha \equiv a \bmod Q^m$ folgt eben i.A. nicht $N_{L/K}(\alpha) \equiv a^n \bmod P^m$, sondern wieder nur die schwächere Kongruenz mod P.

Wir geben einige Beispiele:

1. $L=\mathbf{Q}(\sqrt{14})$, $K=\mathbf{Q}$, $B' = (4) = (2)^2$, also $P=(2)$, $m=2$, $B=(1)$; weiter haben wir $Q = 2_1 = (4+\sqrt{14})$. Wir setzen nun $k=5/4$ und $y=1+\sqrt{14}$. Damit ist $y \equiv 1 \bmod Q$, also $x=e=1$, und wir müssen untersuchen, ob es ein $r \in \mathbf{Z}$ mit $|r|<5$ und $r \equiv 1 \bmod 2$ gibt, das Norm eines $\alpha \in S$ mit $\alpha \equiv 1+\sqrt{14} \bmod 2$ ist. Da (3) in L/K träge ist, gibt es keine Elemente der Norm 3, also kommt nur $r=1$ in Frage. Nun gibt es aber keine Einheit $\alpha \in S$ mit $\alpha \equiv 1+\sqrt{14} \bmod 2$, weil die FE $15+4\sqrt{14}$ bereits $\equiv 1 \bmod 2$ ist (damit ist jede Einheit $\equiv 1 \bmod 2$). Man vergleiche dieses Beispiel auch mit dem Beweis auf S. 11, daß $\frac{1}{2}(1+\sqrt{14})$ kein Kettenbruch der Länge 2 ist (insbesondere achte man auf die Rolle, die die FE in beiden Beweisen spielt).

2. $L=\mathbf{Q}(\sqrt{26})$, $K=\mathbf{Q}$, $B'=(4)$, $y=26$, $k=5/2$; hier ist zwar $Q=2_1=(2,\sqrt{26})$ kein Hauptideal, wohl aber $Q^2=(2)$. Nach (1.7) müssen wir die $r \in Z$ mit $r \equiv 0 \bmod 2$ und $|r|<10$ untersuchen. Wegen $y \in Q \setminus Q^2$ ist aber für alle $\alpha \equiv y \bmod Q$ auch $\alpha \in Q \setminus Q^2$, und man sieht leicht ein, daß dies $N_{L/\mathbf{Q}}(\alpha) \equiv 2 \bmod 4$ impliziert. Also brauchen wir nur die $r \equiv 2 \bmod 4$ zu betrachten. Weil es aber keine $\alpha \in S$ der Norm 2 (denn 2_1 ist kein Hauptideal) oder der Norm 6 gibt (da das Ideal (3) in L träge bleibt), folgt in der Tat $M(L) \geq 5/2$.

Es bleibt die Frage, wie man vorgehen soll, wenn die Kriterien (1.4) und (1.7) nichts bringen (z.B. wenn die von ihnen gelieferten Schranken nicht gut genug sind oder es gar keine rein verzweigten Primideale gibt). Dazu sei K ein Zahlkörper mit $M(K)=k$ und $I=(b)$ ein ganzes Ideal in R (also $b \in R$). Dann gibt es für alle $a \in R$ ein $q \in R$ mit $|N_{K/\mathbf{Q}}(a-qb)| < k \cdot \|I\|$ wegen $a-qb \equiv a \bmod I$ können wir dies auch so ausdrücken: jede Restklasse mod I enthält ein $r \in R$ mit $|N_{K/\mathbf{Q}}(r)| < k \cdot \|I\|$. Diese Überlegung führt uns auf die Definition

$$M(K,I) = \inf \{ x \in R: \forall\, a \in R\ \exists\, c \in I \text{ mit } |N_{K/\mathbf{Q}}(a-c)| < x \cdot \|I\| \},$$
$$= \inf \{ x \in R: \forall\, x \in I^{-1}\ \exists\, y \in R \text{ mit } |N_{K/\mathbf{Q}}(x-y)| < x \}.$$

Weil es zu jedem $x \in K$ ein Hauptideal I mit $x \in I^{-1}$ gibt, folgt sofort aus der Definition $M(K) = \sup \{M(K,I) : I \text{ ist Hauptideal in } R\}$.

Ein Hauptideal I mit $M(K,I)<1$ nennen wir ein ***euklidisches***, ein solches mit $M(K,I) > 1$ ein ***nicht euklidisches Ideal.***

In (1.4) und (1.7) haben wir nichts anderes gemacht, als $M(K,I)$ für rein verzweigte Hauptideale I nach unten abzuschätzen. Wir dürfen daher wegen $M(K) \geq M(K,I)$ für jedes Hauptideal I i.A. bessere Schranken für M(K) erwarten, wenn wir für I beliebige Hauptideale zulassen.

Betrachten wir beispielsweise $K = \mathbb{Q}(\sqrt{29})$; hier erzeugt $\alpha = \frac{1}{2}(3+\sqrt{29})$ ein Ideal I der Norm 5. Um M(K,I) zu bestimmen, stellen wir zuerst ein vollständiges Restsystem mod I auf; ein solches ist z.B. $\{ 0, \pm 1, \pm 2\}$. Jetzt suchen wir in jeder Restklasse mod I ein Element minimaler Norm > 1; in den Restklassen $0, \pm 1$ mod I sind dies die Elemente $0, \pm 1$ selbst (dies sind sozusagen die "uninteressanten" Restklassen). Um in der Restklasse 2 mod I ein Element minimaler Norm zu finden, müssen wir uns fragen, ob diese Restklasse eine Einheit enthält. Nun gilt aber für die FE $u = \frac{1}{2}(5+\sqrt{29})$ die Kongruenz $u \equiv 1$ mod I; da sich nach Dirichlet jede Einheit e in der Form $e = u^l$ für ein $l \in \mathbb{Z}$ schreiben läßt, ist also $e \equiv 1$ mod I für jede Einheit $e \in R$, und insbesondere gibt es keine Einheiten in den Restklassen 2 mod I.

Da es in R auch keine Elemente der Norm 2 oder 3 gibt (weil die Ideale (2) und (3) in R prim bleiben), kann die Restklasse 2 mod I nur Elemente der Norm ≥ 4 enthalten, und in der Tat ist $r=2$ ein solches Element. Damit haben wir $M(K,I) = 4/5$ gezeigt (dies ist etwas besser als die mit (1.5) erhaltene Schranke $M(K) \geq 23/29 = 0.7931\ldots$). Man beachte noch, daß in diesem Fall $I = (u-1)$ gilt, und daß diese Tatsache dafür gesorgt hat, daß $e \equiv 1$ mod I für jede Einheit $e \in R^\times$ ist.

Ganz analog läuft der Beweis von $M(K,I) = 16/9$ für $K = \mathbb{Q}(\sqrt{85})$ und $I = (u-1) = \frac{1}{2}(7+\sqrt{85})$; I hat Idealnorm 9, und $\{ 0, \pm 1, \pm 2, \pm 3, \pm 4\}$ ist vollständiges Restsystem mod I.

Es ist damit prinzipiell klar, wie man entsprechende Rechnungen in beliebigen Zahlkörpern für beliebige Hauptideale I durchführt: man wählt sich ein System von Grundeinheiten und bestimmt alle Restklassen mod I, die Einheiten enthalten (dazu läßt man einfach jede Grundeinheit die Potenzen von 1 bis $\Phi(I)$ durchlaufen und notiert sich die Restklassen, in denen die Produkte dieser Potenzen liegen). Dann sucht man sich ein Hauptideal $A=(a)$ minimaler Norm und fragt, in welchen Restklassen mod I die Elemente ae, $e \in R^\times$, liegen usw.

Allerdings werden die nötigen Rechnungen recht schnell umfangreich, wenn man ein I mit großer Norm zu betrachten hat (z.B. für $K = \mathbb{Q}(\sqrt{31})$ und $I=(u-1)$, $u = 1520 + 273\sqrt{31}$; hier ist $\|I\| = 3038$) oder wenn der Einheitenrang von K groß wird. Glücklicherweise läßt sich das obige Verfahren so modifizieren, daß es sich recht einfach programmieren läßt und damit von einem Rechner durchgeführt werden kann. Dazu sagen wir, die Punkte $x_1, \ldots, x_t \in K$ werden von einer Einheit $u \in R^\times$ (zyklisch) permutiert, wenn die folgenden Kongruenzen gelten: $x_1 u \equiv x_2 \bmod R$, $x_2 u \equiv x_3 \bmod R$, ..., $x_t u \equiv x_1 \bmod R$.

In diesem Falle gilt übrigens $M(K,x_1) = \ldots = M(K,x_t)$, wie man leicht aus den beiden Beobachtungen

1. für alle $y \in R$ ist $M(K,x) = M(K,x-y)$;
2. für alle Einheiten $u \in R^\times$ ist $M(K,x) = M(K,ux)$

folgert. Wir behaupten nun:

(1.8) Sei $R=D(m)$, $m\in\mathbb{N}$ quadratfrei, und sei $1\le u$ für eine Einheit u in R. Weiter seien Punkte $x_1,\dots,x_t$ gegeben, die von u permutiert werden. Ist dann $M(K,x_1)<k$, so gibt es ein $z=r+s\sqrt{m}\in K$ mit den Eigenschaften

a) $z \equiv x_j \bmod R$ für ein $j\in\{1,\dots,t\}$

b) $|N_{K/\mathbb{Q}}(z)| < k$

c) $|r|< \mu_1$, $|s|<\mu_2$ mit $\mu_1 = \frac{\sqrt{k}(\sqrt{u}+1/\sqrt{u})}{2}$ und $\mu_2 = \frac{\sqrt{k}(\sqrt{u}+1/\sqrt{u})}{2\sqrt{m}}$.

Dies ist im wesentlichen "Theorem B" von Barnes und Swinnerton-Dyer; deren Beweis ist jedoch völlig auf quadratische Zahlkörper zugeschnitten und läßt sich nicht verallgemeinern. Bevor wir aber einen Beweis für (1.8) geben, wollen wir uns klarmachen, was (1.8) im einfachsten Fall t=1 aussagt: Wir haben dann ein $x:=x_1$ gegeben mit $xu\equiv x \bmod R$; wenn wir dann $M(K,x)\ge k$ zeigen wollen, nehmen wir an, es sei $M(K,x)<k$. (1.8) garantiert dann die Existenz eines $z=r+s\sqrt{m}\in K$ mit den Eigenschaften

a) $z \equiv x \bmod R$, d.h. $z-x\in R$;

b) $|N_{K/\mathbb{Q}}(z)| < k$;

c) $|r|< \mu_1$, $|s|< \mu_2$.

Um $M(K,x)<k$ zum Widerspruch zu führen, müssen wir also nur zeigen, daß unter den endlich vielen $z\in K$, die den Bedingungen a) und c) genügen, keines mit $|N_{K/\mathbb{Q}}(z)|<k$ vorkommt.

Bew. von (1.8): Wegen $M(K,x_1)<k$ gibt es ein $y\in R$ mit $|N_{K/\mathbb{Q}}(x_1-y)| < k$; wir setzen nun $z_1=x_1-y$ und wählen $m\in\mathbb{Z}$ so, daß $\sqrt{k/u} \le |z_1u^m| < \sqrt{ku}$ wird (dies ist offenbar immer möglich). Jetzt behaupten wir, daß $z=z_1u^m$ den Bedingungen a), b), c) genügt:

a) $z = z_1u^m = x_1u^m - yu^m \equiv x_1u^m \equiv x_j \bmod R$, wobei j durch die Kongruenz $j \equiv 1+m \bmod t$ bestimmt ist.

b) $|N_{K/\mathbb{Q}}(z)| = |N_{K/\mathbb{Q}}(z_1)| = |N_{K/\mathbb{Q}}(x_1-y)| < k$.

c) Sei $z' = r-s\sqrt{m}$ die Konjugierte von z; dann haben wir

$|z'| = |zz'|/|z| = |N_{K/\mathbb{Q}}(z)|/|z| < k/|z| \le \sqrt{ku}$, also

$|2r| = |z+z'| \le |z|+|z'| < 2\sqrt{ku}$ und

$|2s\sqrt{m}| = |z-z'| \le |z|+|z'| < 2\sqrt{ku}$.

Diese Schranken lassen sich aber noch verbessern, wenn wir neben den Ungleichungen $|z|, |z'| < \sqrt{ku}$ auch die Ungleichung $|zz'| < k$ verwenden; die Behauptung folgt nämlich mit $a=\sqrt{ku}$ und $b=k$ aus

(1.9) Seien x, y, a, b positive reelle Zahlen; aus den Ungleichungen $x\le a$, $y\le a$, $xy \le b$ folgt dann $x+y \le a + \frac{b}{a}$.

Bew.: Es ist $0 \le (a-x)(a-y) = a^2-(x+y)a+xy \le a^2-(x+y)a+b$.

Wir bemerken noch, daß die Voraussetzung $u > 1$ durch $u \neq 1$ ersetzt werden darf; man muß dann nur in (1.8.c) u durch $|u|$ ersetzen. Im Falle $N_{K/\mathbb{Q}}(u)=+1$ erhalten wir übrigens die von Barnes und Swinnerton-Dyer angegebenen Schranken zurück: setzt man $u=a+b\sqrt{m}$, so ist $1/u = a-b\sqrt{m}$ und damit $(\sqrt{u} + 1/\sqrt{u})^2 = u + 1/u + 2 = 2a+2$, und wir finden $2=\sqrt{k(a+1)/2m}$.

Beispiel: $K = \mathbb{Q}(\sqrt{19})$; sei $x = 20\sqrt{19}/57$ und $u=170+39\sqrt{19}$ die FE von K. Wir haben dann $xu = 260+60\sqrt{19} - x \equiv -x \bmod R$, sodaß wir (1.8) an sich mit $t=2$, $x_1=x$ und $x_2=-x$ anwenden müßten. Wenn wir aber statt u die Einheit $u'=-u$ nehmen, haben wir $xu' \equiv x \bmod R$, sodaß die Wahl von u' die Rechenzeit halbiert.

Wir zeigen nun, daß $M(K) \geq M(K,x)=170/171$ gilt; die eine Ungleichung $M(K,x) \leq 170/171$ folgt dabei aus der Beobachtung

$$M(K,x) \leq |N_{K/\mathbb{Q}}(x-3-\sqrt{19})| = 170/171.$$

Wir brauchen daher nur noch $M(K,x) \geq k = 170/171$ zu zeigen, und dies machen wir mit (1.8): wäre nämlich $M(K,x)<k$, so gäbe es ein $z \in K$ mit $z \equiv x \bmod R$, das den Bedingungen a), b), c) genügt. Wegen $a=170$ erhalten wir die Schranke $|s| < 2.12..$, für $z=r+s\sqrt{19}$. Damit kommen für s nur vier Werte in Frage, nämlich $s = i + 20/57$, $i \in \{-2, -1, 0, 1\}$:

$i=-2$: $|N_{K/\mathbb{Q}}(z)|$ wird minimal für $r= \pm 7$ mit $|N_{K/\mathbb{Q}}(z)|= 457/171$;
$i=-1$: $|N_{K/\mathbb{Q}}(z)|$ wird minimal für $r= \pm 3$ mit $|N_{K/\mathbb{Q}}(z)| = 170/171$;
$i= 0$: $|N_{K/\mathbb{Q}}(z)|$ wird minimal für $r= \pm 1$ mit $|N_{K/\mathbb{Q}}(z)|= 229/171$;
$i=+1$: $|N_{K/\mathbb{Q}}(z)|$ wird minimal für $r= \pm 6$ mit $|N_{K/\mathbb{Q}}(z)|= 227/171$;

nach (1.8) ist damit $M(K,x)=170/171$, und in der Tat werden wir in § 2 sehen, daß sogar $M(K) = M(K,x) = 170/171$ gilt. Hätten wir nur die Schranke $|s| < \sqrt{ku}$ verwendet, so hätten wir acht Werte für s betrachten müssen.

Bevor wir (1.8) auf beliebige Zahlkörper mit Einheitenrang > 1 verallgemeinern, wollen wir uns am kubischen Fall klar machen, welche Schwierigkeiten dabei auftreten. Wir zeigen daher zuerst

(1.10) Sei K kubischer Zahlkörper mit Einheitenrang 1, u eine Einheit mit $1<|u|$, und $x_1, \ldots, x_t \in K$ seien Punkte, die von u permutiert werden. Weiter sei $\{\alpha_1, \alpha_2, \alpha_3\}$ eine $\mathbb{Q}$-Basis von K. Ist dann $M(K,x_1)<k$, so gibt es ein $z \in K$, $z = r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3$, mit den Eigenschaften

a) $z \equiv x_j \bmod R$ für ein $j \in \{1,\ldots,t\}$;
b) $|N_{K/\mathbb{Q}}(z)| < k$;
c) $|r_i| < \mu_i$ für $i=1, 2, 3$, wobei die μ_i positive reelle Zahlen sind, die von den x_j unabhängig sind.

Bem.: Die Schranken μ_i werden sich aus dem Beweis ergeben und lassen sich explizit bestimmen. Die Schranken, die wir speziell in rein kubischen Körpern erhalten werden, sind weitaus besser als diejenigen, die Cioffari (1979) in den Fällen $K=\mathbb{Q}(\sqrt[3]{m})$, $m=12, 17, 44$, erhalten hat. Ähnlich wie im quadratischen Fall lassen sich die hier erreichten Schranken noch einmal verbessern; wir werden dies in § 4 tun.

Bew.: OBdA dürfen wir annehmen, daß K reell ist (denn da K Einheitenrang 1 hat, muß $r=s=1$ sein, wo r die Anzahl der reellen Einbettungen von K in $\mathbb{C}$ angibt). Damit dürfen wir die Bedingung $1<|u|$ durch $1<u$ ersetzen.
Nun ist nach Voraussetzung $M(K,x_1)<k$, folglich existiert ein $y\in\mathbb{R}$ mit $|N_{K/\mathbb{Q}}(x_1-y)|<k$; wir setzen $z_1=x_1-y$ und wählen ein $m\in\mathbb{N}$ so, daß

$$\sqrt[3]{k/u^2} \le |z_1u^m| < \sqrt[3]{ku}$$

wird. Mit $z=z_1u^m$ sind dann die Bedingungen a) und b) erfüllt, sodaß wir uns nur noch um c) zu kümmern brauchen. Wir bezeichnen nun die beiden Konjugierten von z mit z' und z''; da die beiden Körper K' und K'' konjugiert-komplex sind, gilt $|z'|=|z''|$, also $|N_{K/\mathbb{Q}}(z)| = |zz'z''| = |z||z'|^2$ und damit $|z'|^2 = |N_{K/\mathbb{Q}}(z)|/|z| < k/|z| \le \sqrt[3]{ku}^2$.
Wir betrachten nun zuerst den etwas einfacheren Spezialfall des reinen kubischen Zahlkörpers $K=\mathbb{Q}(\vartheta)$ für $\vartheta^3=m$, $m\in\mathbb{N}$; hier wählen wir die Basis $\{1, \vartheta, \vartheta^2\}$ und finden $z' = r_1+ r_2\rho\vartheta+r_3\rho^2\vartheta^2$, $z'' = r_1 +r_2\rho^2\vartheta +r_3\rho\vartheta^2$, wo ρ eine primitive dritte Einheitswurzel ist. Jetzt können wir ganz wie im quadratischen Fall schließen:

$|3r_1| = |T_{K/\mathbb{Q}}(z)| = |z+z'+z''| \le |z|+|z'|+|z''| < 3\sqrt[3]{ku}$,
$|3r_2\vartheta| = |z+\rho^2z'+\rho z''| \le |z|+|z'|+|z''| < 3\sqrt[3]{ku}$,
$|3r_3\vartheta^2| = |z+\rho z'+\rho^2z''| \le |z|+|z'|+|z''| < 3\sqrt[3]{ku}$,

und damit haben wir (1.8) in diesem Spezialfall bewiesen mit den Schranken $\mu_1=\sqrt[3]{ku}$, $\mu_2=\sqrt[3]{ku/m}$, $\mu_3=\sqrt[3]{ku/m^2}$. Da wir im allgemeinen Fall die Konjugierten von z nicht explizit angeben können, müssen wir hier einen etwas anderen Weg einschlagen:
Sei dazu $\{\beta_1,\beta_2,\beta_3\}$ die zu $\{\alpha_1,\alpha_2,\alpha_3\}$ duale Basis, die bekanntlich durch $T_{K/\mathbb{Q}}(\alpha_i\beta_j) = \delta_{ij}$ (Kroneckerdelta) definiert ist. Damit wird

$$T_{K/\mathbb{Q}}(z\beta_j) = \sum_{i=1}^{3} r_i T_{K/\mathbb{Q}}(\alpha_i\beta_j) = r_j, \text{ also}$$

$$|r_j| = |T_{K/\mathbb{Q}}(z\beta_j)| = |z\beta_j+ z'\beta_j' + z''\beta_j''| \le |z\beta_j|+|z'\beta_j'|+|z''\beta_j''| \le \sqrt[3]{ku}\,(|\beta_j|+2|\beta_j'|).$$

Daher müssen wir nur noch angeben, wie wir die β_j aus den α_i bestimmen können. Dazu betrachten wir die $n\times n$-Matrix $A=(T_{K/\mathbb{Q}}(\alpha_i\alpha_j))$; wir wissen, daß dann $\det A = \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ ist. Sei $B=(b_{ij})$ die Umkehrmatrix von A; dann ist $\beta_i = b_{i1}\alpha_1 + \ldots + b_{in}\alpha_n$ (sh. z.B. Cohn (1978) oder Marcus (1977)).

Da wir uns in § 6 ausführlich mit Dirichlet'schen Zahlkörpern beschäftigen werden, sei auch dieser Fall noch explizit ausgeführt. Sei dazu $L = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ ein imaginärer, bizyklischer, biquadratischer Zahlkörper (d.h. $m,n \in \mathbf{Z}$, $m<0$). Wir wählen die $\mathbf{Q}$-Basis $\alpha_1=1$, $\alpha_2=\sqrt{m}$, $\alpha_3=\sqrt{n}$, $\alpha_4=\sqrt{mn}$ und nehmen an, es sei $N_{L/\mathbf{Q}}(x_1-y)<k$ für ein $x_1 = r_1\alpha_1 + r_2\alpha_2 + r_3\alpha_3 + r_4\alpha_4 \in L$, ein $y \in R$ und ein $k \in \mathbb{R}$. Da REinheitenrang 1 hat, gibt es eine Fundamentaleinheit u, die wir so wählen können, daß $|u|>1$ ist. Mit $z_1=x_1-y$ finden wir dann ein $m \in \mathbf{Z}$ mit

$$\sqrt[4]{k}/\sqrt{|u|} \le |z_1| < \sqrt[4]{k}\cdot\sqrt{|u|} = \delta.$$

Sei nun $\mathrm{Gal}(L/\mathbf{Q}) = \{1, \sigma, \tau, \sigma\tau\}$, und oBdA sei σ der Automorphismus der komplexen Konjugation (damit ist dann $|z| = |z^\sigma|$; sind z.B. m und n beide negativ, so kann man σ auch durch σ: $\sqrt{m} \mapsto -\sqrt{m}$, $\sqrt{n} \mapsto -\sqrt{n}$ charakterisieren). Nun ist $N_{L/\mathbf{Q}}(x) = x\cdot x^\sigma\cdot x^\tau\cdot x^{\sigma\tau} = |x|^2|x^\tau|^2$, also auch $|x^\tau|^2 \le N_{L/\mathbf{Q}}(x)/|x|^2 < \delta$.

Wir setzen jetzt τ: $\sqrt{m} \mapsto \sqrt{m}$, $\sqrt{n} \mapsto -\sqrt{n}$ und erhalten

$4\cdot|r_1| = |z + z^\sigma + z^\tau + z^{\sigma\tau}| \le |z| + |z^\sigma| + |z^\tau| + |z^{\sigma\tau}| = 2\cdot(|z| + |z^\tau|) < 4\delta$, sowie

$4\cdot|r_2|\cdot\sqrt{|m|} = |z - z^\sigma + z^\tau - z^{\sigma\tau}| \le 2\cdot(|z| + |z^\tau|) < 4\delta$,

$4\cdot|r_3|\cdot\sqrt{|n|} = |z - z^\sigma - z^\tau + z^{\sigma\tau}| \le 2\cdot(|z| + |z^\tau|) < 4\delta$,

$4\cdot|r_4|\cdot\sqrt{|mn|} = |z + z^\sigma - z^\tau - z^{\sigma\tau}| \le 2\cdot(|z| + |z^\tau|) < 4\delta$.

Benutzt man auch (1.9), so kann man wie im reellquadratischen Fall den Faktor $\sqrt{|u|}$ in δ ersetzen durch $(\sqrt{|u|} + 1/\sqrt{|u|})/2$, und wir haben

(1.11) Sei $L=\mathbf{Q}(\sqrt{m},\sqrt{n})$ ein imaginärer, bizyklischer Zahlkörper, u eine Einheit in R mit $|u|>1$, und $x_1, \ldots, x_t \in L$ seien Punkte, die von u permutiert werden. Ist dann $M(L,x_1) < k$, so gibt es ein $z = r_1 + r_2\sqrt{m} + r_3\sqrt{n} + r_4\sqrt{mn} \in L$ mit den Eigenschaften

a) $z \equiv x_j \bmod R$ für ein $j \in \{1, \ldots, t\}$;

b) $|N_{L/\mathbf{Q}}(z)| < k$;

c) $|r_i| < \mu_i$ für $1 \le i \le 4$ und mit $\mu_1 = \lambda$, $\mu_2 = \lambda/\sqrt{|m|}$, $\mu_3 = \lambda/\sqrt{|n|}$, $\mu_4 = \lambda/\sqrt{|mn|}$, wobei $\lambda = \sqrt[4]{k}\cdot(\sqrt{|u|} + 1/\sqrt{|u|})$ gesetzt wurde.

Es ist eine merkwürdige Tatsache, daß man (1.11) auch einsetzen kann, um $M(K,x)$ für ein reellquadratisches abzuschätzen: ist nämlich $e>1$ die FE von K und $N_{K/\mathbf{Q}}(e) = +1$, so gibt es einen imaginären, bizyklischen Zahlkörper $L=K(\sqrt{m})$, $m<0$, indem $-e = u^2$ zum Quadrat wird für eine Einheit u in S (dem Ring der ganzen Zahlen in L; sh. hierzu § 6 und die dort angegebene Literatur). Anstatt dann $|N_{K/\mathbf{Q}}(x-y)| < k$ für ein $x \in K$ mit $xe \equiv x \bmod R$ und $y \in R$ zu untersuchen, betrachtet man $N_{L/\mathbf{Q}}(x-y) < k^2$ und $N_{L/\mathbf{Q}}(xu-y) < k^2$. Wir werden in § 2 ein Beispiel geben, das zeigt, daß man mit dieser Idee eine Menge Arbeit sparen kann.

Wir kommen damit zum allgemeinen Fall:

(1.12) Sei K ein Zahlkörper mit $(K:\mathbb{Q})=n=r+2s$, $\{u_1,\dots,u_l\}$ ein System von $l=r+s-1$ unabhängigen Einheiten, $\{\alpha_1,\dots,\alpha_n\}$ eine $\mathbb{Q}$-Basis von K und $x_1,\dots,x_t$ Elemente von K, die von den u_i irgendwie permutiert werden. Ist dann $M(K,x_1)<k$, dann gibt es ein $z\in K$ mit $z=\sum r_j\alpha_j$ und den Eigenschaften

a) $z \equiv x_i \mod R$ für ein $i\in\{1,\dots,t\}$

b) $|N_{K/\mathbb{Q}}(z)| < k$

c) $|r_j| < \mu_j$ für $j=1,\dots,n$, wo die μ_j positive reelle Zahlen sind, die nur von k, der Wahl der α_j und der u_i, nicht aber von den Punkten x_i abhängen.

Bevor wir dies beweisen, führen wir noch einige Bezeichnungen ein. Dazu denken wir uns die $n=r+2s$ Einbettungen von K in $\mathbb{C}$ folgendermaßen angeordnet: $\tau_1, \dots, \tau_r, \tau_{r+1}, \overline{\tau_{r+1}}, \dots, \tau_{r+s}, \overline{\tau_{r+s}}$, wo $\tau_1, \dots, \tau_r$ die reellen, $\tau_{r+1}, \overline{\tau_{r+1}}, \dots, \tau_{r+s}, \overline{\tau_{r+s}}$ die Paare konjugiert-komplexer Einbettungen bezeichnen. Ist $|\ |$ der gewöhnliche Absolutbetrag auf $\mathbb{R}$ (bzw. $\mathbb{C}$), so sind durch

$$|x|_i = \begin{cases} |\tau_i(x)| & \text{für } 1 \leq i \leq r \\ |\tau_i(x)|^2 & \text{für } r+1 \leq i \leq r+s \end{cases}$$

alle $r+s$ verschiedenen archimedischen Bewertungen von K definiert. Damit ist $|N_{K/\mathbb{Q}}(x)| = |x|_1 \cdot \dots |x|_{r+s}$. Wir behaupten nun

(1.13) Es seien $l=r+s-1$ unabhängige Einheiten $u_1,\dots,u_l$ gegeben, und es sei $x_i = |\log |u_1|_i| + \dots + |\log |u_l|_i|$ für $i=1,\dots,l$; weiter sei $k_i=\exp(x_i)$. Sind dann c_i $(1 \leq i \leq l)$ irgendwelche positiven reellen Zahlen, dann gibt es zu jedem $z_1 \in K\setminus\{0\}$ eine Einheit $u\in R^\times$ mit $c_i \leq |z_1 u|_i < c_i k_i$ für $i=1,\dots,l$.

Bew.: Wir definieren eine Abbildung $\Lambda : K\setminus\{0\} \to \mathbb{R}$ durch

$$\Lambda(x) = \begin{pmatrix} \log |x|_1 \\ \dots \\ \log |x|_l \end{pmatrix};$$

Λ hängt natürlich davon ab, welche der $r+s=l+1$ Bewertungen von K wir hier auswählen. Wir behaupten nun, daß die l Vektoren $v_1 = \Lambda(u_1), \dots, v_l = \Lambda(u_l)$ im $\mathbb{R}^l$ unabhängig sind. Dazu nehmen wir an, es sei $\sum a_i v_i = 0$ für gewisse $a_i \in \mathbb{Z}$. Indem wir diese Gleichung koordinatenweise betrachten, folgt

$$\sum_{i=1}^{l} a_i \cdot \log |u_i|_j = 0 \quad \text{für alle } j \text{ mit } 1 \leq j \leq l;$$

addiert man diese l Gleichungen auf und beachtet

$$\sum_{i=1}^{l} \log |u_i|_j = 0 \qquad \text{(wegen } |N_{K/\mathbb{Q}}(u_i)|=1\text{)},$$

so folgt $\sum_{i=1}^{l} a_i \cdot \log |u_i|_j = 0$ auch für $j=r+s$. Dann ist aber $\prod_{i=1}^{l} u_i^{a_i} = 1$,

und da die u_i unabhängig sind, folgt $a_i = 0$ für alle i ($1 \leq i \leq l$). Also sind die Vektoren $v_1, \ldots, v_l$ in der Tat linear unabhängig. Nun können wir einen beliebigen Vektor im $\mathbb{R}^l$ durch Verschieben um geeignete ganzzahlige Vielfache der v_i in den Fundamentalbereich

$$F = \{\sum b_i v_i : 0 \leq |b_i| \leq \tfrac{1}{2}\}$$

bringen. Für ein $w = (w_1, \ldots, w_l)^t \in F$ gilt nun

$$w_i = \sum_{j=1}^{l} b_i \cdot \log |u_j|_i = 0,$$

also $0 \leq |w_i| \leq x_i/2$.
Indem wir

$$w = \begin{pmatrix} \log |z_1|_1 - \log c_1 - x_1/2 \\ \log |z_1|_1 - \log c_1 - x_1/2 \end{pmatrix}$$

setzen und $a_i \in \mathbb{Z}$ so finden, daß $w - \sum a_i v_i \in F$ wird, erhalten wir die Existenz einer Einheit $u = \prod u_i^{a_i}$ mit

$$\log c_1 \leq \log |z_1 u|_1 < \log c_1 + x_1$$

$$\ldots$$

$$\log c_l \leq \log |z_1 u|_l < \log c_l + x_l.$$

Daraus folgt aber sofort unsere Behauptung.

Bew. von 1.13.: Wegen $M(K, x_1) < k$ existiert ein $y \in R$ mit $|N_{K/\mathbf{Q}}(x_1 - y)| < k$. Wir setzen $z_1 = x_1 - y$ und finden mit (1.12) eine Einheit u mit $\sqrt[n]{k} \leq |z_1 u|_i < x_i \sqrt[n]{k}$ für $i = 1, \ldots, l$. Mit $z = z_1 u$ sind a) und b) offenbar erfüllt, und um auch c) nachzuweisen, beachten wir

$$|z|_{l+1} = |N_{K/\mathbf{Q}}(z)| / \prod_{i=1}^{l} |z|_i < \sqrt[n]{k},$$

mit $x_{l+1} = 1$ also $|z|_i < x_i \cdot \sqrt[n]{k}$ für $i = 1, \ldots, l+1$.
Sei nun $\{\beta_1, \ldots, \beta_n\}$ die zu $\{\alpha_1, \ldots, \alpha_n\}$ duale Basis. Wie schon im kubischen Fall folgt nun auch hier

$$|r_j| = |T_{K/\mathbf{Q}}(z\beta_j)| \leq \sum_{\tau} |z^{\tau}||\beta_j^{\tau}| < \sqrt[n]{k} \cdot \left(\sum_{\tau} \lambda_{\tau} |\beta_j^{\tau}|\right) =: \mu_j .$$

Hierbei stimmen die λ_τ mit den x_i überein, falls τ reell ist ($i = 1, \ldots, r$), und nach geeigneter Umnumerierung mit $\sqrt{x_i}$, falls τ nicht reell ist ($i = r+1, \ldots, r+2s$). Diese lästige Umbenennung rührt von der Definition der $|\ |_i$ vor (1.13) her, wo bei nichtreellen Einbettungen das Quadrat des gewöhnlichen Betrages steht. Ich habe aber bisher nicht gesehen, wie sich dieser Mangel beheben läßt.

Zweifellos lassen sich die Abschätzungen, die wir im Verlauf des Beweises von (1.12) gemacht haben, noch verbessern. Wenn man daher (1.12) zur Bestimmung von M(K) benutzen will, wird man sich hierüber Gedanken machen müssen.

Nachstehend geben wir einige Tabellen, die zeigen sollen, wie man die Kriterien 1.5., 1.7. und 1.8. in reellquadratischen Zahlkörpern anwenden kann. Aus diesen Tabellen kann man bereits ersehen, daß die Ringe D(m) mit $m \leq 101$ höchstens für die Werte m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73 normeuklidisch sein können; in § 2 und § 3 werden wir zeigen, daß diese Ringe die einzigen normeuklidischen reellquadratischen Zahlkörper sind.

Anwendung von (1.5) auf quadratische Zahlkörper $\mathbf{Q}(\sqrt{m})$

m	f	a	k = M(x)	r
7	14	9	9/14	-5
10	10	5	3/2	5
11	22	3	19/22	3
13	13	4	4/13	-
15	15	6	7/5	6, -9
17	17	8	8/17	-
19	38	7	31/38	7
21	7	2	5/7	2
22	22	5	27/22	5, -17
23	46	31	77/46	-15, 31, -61
29	29	6	23/29	6
31	31	14	45/31	14, -17
33	11	5	6/11	5
35	35	15	17/7	15, -20, 50, -55
37	37	10	27/37	10
47	94	65	253/94	-29, 65, -123, 159, -217
51	102	19	287/102	(e=23): -185, -83, 19, 121, 223
53	53	15	68/53	15, -38
57	19	5	14/19	5
59	59	7	125/59	7, -52, 66, -111
69	23	2	25/23	2, -21
77	11	3	19/11	3, -8, 14
	11	5	16/11	5, -6
79	158	111	585/158	-47, 111, -205, 269, -363, 427, -521
83	166	33	631/166	33, -133, 199, -299, 365, -465, 531
85	85	19	151/85	19, -66, 104
87	58	53	169/58	-5, 53, -63, 111, -121
93	31	18	44/31	-13, 18
101	101	24	125/101	24, -77

Bem.: Ist $e^2 \equiv a \bmod f$ und $(c)^2 = (f)$ für ein $c \in R$, so setze man $x = e/c$; man erhält damit ein $x \in K$ mit $M(K,x)=k$.
Im Falle m=51 ist noch zu bemerken, daß 121 natürlich Norm aus S ist wegen $121 = N_{K/Q}(11)$; jedoch ist $11 \not\equiv e = 23 \bmod f$. Diese Schwierigkeit tritt hier auf, weil die Kongruenz $x^2 \equiv a \equiv 19 \bmod f$ vier verschiedene Lösungen hat, nämlich $x \equiv 11$ und und $x \equiv 23$.

Anwendung von (1.7) auf quadratische Zahlkörper $Q(\sqrt{m})$

m	B'	y	k=M(x)	r
6	4	$1+\sqrt{6}$	3/4	1
10	4	$\sqrt{10}$	3/2	2
14	4	$1+\sqrt{14}$	5/4	1, 3
15	4	$1+\sqrt{15}$	3/2	2
26	4	$\sqrt{26}$	5/2	2, 6
30	4	$\sqrt{30}$	3/2	2
	20	$1+\sqrt{30}$	29/20	-19, -9, 1, 11, 21
34	4	$1+\sqrt{34}$	9/4	1, 3, 5, 7
38	4	$1+\sqrt{38}$	11/4	1, 3, 5, 7, 11
39	4	$1+\sqrt{39}$	5/2	2, 6
42	4	$1+\sqrt{42}$	7/4	1, 3, 5
55	4	$\sqrt{55}$	9/4	1, 3, 5, 7
58	4	$\sqrt{58}$	3/2	2
62	4	$1+\sqrt{62}$	13/4	1, 3, 5, 7, 11, 13
66	4	$1+\sqrt{66}$	15/4	1, 3, 5, 7, 11, 13
74	4	$\sqrt{74}$	5/2	2, 6
78	4	$\sqrt{78}$	7/2	2, 6, 10
82	4	$\sqrt{82}$	9/2	2, 6, 10, 14
91	4	$1+\sqrt{91}$	5/2	2, 6
95	4	$1+\sqrt{95}$	7/2	2, 6, 10

Bem.: Ist $B'=(c)^2$ für ein $c \in R$, so ist $M(x) = k$ für $x=y/c$.

Anwendung von (1.8) auf quadratische Zahlkörper $\mathbf{Q}(\sqrt{m})$ (t=1)

m	x	M(x)	u
19	(0 , 20/57)	170/171	$170 + 39\sqrt{19}$
21	(2/5 , 1/5)	12/25	$(5 + \sqrt{21})/2$
22	(0 , 9/28)	443/392	$197 + 42\sqrt{22}$
29	(3/5 , 1/5)	4/5	$(5 + \sqrt{29})/2$
33	(1/2 , 2/11)	29/44	$23 + 4\sqrt{33}$
34	(1/2 , 6/17)	135/68	$35 + 6\sqrt{34}$
	(0 , 5/12)	137/72	$35 + 6\sqrt{34}$
35	(0 , 3/7)	17/7	$6 + \sqrt{35}$
38	(0 , 5/12)	173/72	$37 + 6\sqrt{38}$
39	(0 , 5/12)	107/48	$25 + 4\sqrt{39}$
41	(15/32 , 5/32)	23/32	$32 + 5\sqrt{41}$
42	(0 , 7/12)	41/24	$13 + 2\sqrt{42}$
43	(1/118 , 1/2)	11829/6962	$3482 + 531\sqrt{43}$
	(0 , 193/387)	5902/3483	$3482 + 531\sqrt{43}$
46	(1/2 , 311/1058)	76877/48668	$24335 + 3588\sqrt{46}$
53	(1/14 , 3/14)	9/7	$(7 + \sqrt{53})/2$
55	(1/2 , 19/44)	351/176	$89 + 12\sqrt{55}$
57	(0 , 15/76)	219/304	$151 + 20\sqrt{57}$
61	(1/78 , 17/78)	41/39	$(39 + 5\sqrt{61})/2$
62	(1/2 , 48/124)	367/124	$63 + 8\sqrt{62}$
	(0 , 7/16)	367/128	$63 + 8\sqrt{62}$
65	(1/4 , 1/4)	1	$8 + \sqrt{65}$
66	(0 , 7/16)	31/128	$65 + 8\sqrt{66}$
67	(1/2 , 7/18)	341/162	$48842 + 5967\sqrt{67}$
70	(1/2 , 6/25)	891/500	$251 + 30\sqrt{70}$
71	(0 , 216/497)	7393/3479	$3480 + 413\sqrt{71}$
73	(41 , 283)/2136	1541/2136	$1068 + 125\sqrt{73}$
85	(4/9 , 2/9)	16/9	$(9 + \sqrt{85})/2$
86	(0 , 133/473)	10030/5203	$10405 + 1122\sqrt{86}$
89	(3 , 159)/1000	1004/1000	$500 + 53\sqrt{89}$
94	(0 , 3661/14194)	4708623/2143294	$2143295 + 221064\sqrt{94}$
97	(1496,2587)/11208	3001/2802	$5604 + 569\sqrt{97}$
109	(17 , 82)/261	289/261	$261 + 25\sqrt{109}$
113	(3 , 219)/1552	967/776	$776 + 73\sqrt{113}$
137	(3 , 447)/3488	2177/1744	$1744 + 149\sqrt{137}$

t=2

m	x_1, x_2	$M(x_1)$
19	(0 , 173/494)	10579/12844
	(1/2 , -115/247)	
22	(1182 , 49644)/155236	175903/155236
	(-1182 , 49644)/155236	
58	(1/2 , 197/754)	27477/19604
	(1/2 , 276/754)	
61	(0 , 66/305)	1611/1525
	(0 , 67/305	
74	(1/2 , 19/43)	16255/7396
	(1/86 , 1/2)	
93	(0 , 44/279)	2198/1674
	(1/2 , 119/558)	

Für weitere Beispiele mit t=2 sh. § 2.

Nachdem wir uns bisher mit notwendigen Kriterien beschäftigt haben, wenden wir uns nun solchen zu, die die Existenz des EA garantieren.

1974 hat Lenstra eine Methode vorgestellt, mit der inzwischen (sh. z.B. Lenstra (1977), Leutbecher u. Martinet (1981, 1982), Leutbecher (1985, 1986), Leutbecher u. Niklasch (1987)) ca. 400 normeuklidische Zahlkörper gefunden wurden. Eine Modifikation dieses Kriteriums wird es uns erlauben, auf ähnliche Art und Weise auch k-stufig normeuklidische Zahlringe zu erhalten (diese wollen wir in Zukunft einfach k-euklidisch nennen).

Lenstras Methode basiert auf einer Idee von Hurwitz (1919): dieser hat gezeigt, daß es in einem Zahlkörper K eine nur von K abhängige natürliche Zahl $m \geq 2$ gibt, sodaß gilt:

für alle $x \in K$ gibt es ein $y \in R$ und ein $j \in \mathbb{N}$, $1 \leq j < m$ mit $|N_{K/\mathbb{Q}}(jx-y)| < 1$.

Man beachte, daß K genau dann normeuklidisch ist, wenn wir $m=2$ wählen dürfen. Lenstra hat dann bemerkt, daß es im Beweis dieser Aussage nicht darauf ankommt, daß die obigen j natürliche Zahlen sind, sondern daß etwas allgemeiner gilt:

(1.14) Sei K ein Zahlkörper, $(K:\mathbb{Q}) = n = r+2s$, und $d = |\mathrm{disc}\ K|$. Ist dann $m \in \mathbb{N}$, $m > M_{r,s} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{d}$ und sind $\vartheta_1, \ldots, \vartheta_n$ irgendwelche paarweise verschiedenen Elemente von K, dann gibt es für alle $x \in K$ ein $y \in R$ mit $|N_{K/\mathbb{Q}}((\vartheta_i-\vartheta_j)x - y)| < 1$ für gewisse $i,j \in \mathbb{N}$, $1 \leq i < j \leq m$.

Lenstras Idee war nun die folgende: wenn wir die $\vartheta_1, \ldots, \vartheta_m$ so wählen können, daß die Differenzen $\vartheta_i - \vartheta_j$ für $i<j$ lauter Einheiten in R sind, dann ist $x - y/(\vartheta_i-\vartheta_j) \in R$, und (1.14) besagt dann gerade, daß es für alle $x \in K$ ein $c \in R$ mit $|N_{K/\mathbb{Q}}(x-c)| < 1$ gibt: R wäre damit normeuklidisch.

Der Beweis von (1.14), den wir nun vorstellen wollen, stammt von Lenstra (1974) und hat große Ähnlichkeit mit dem klassischen Beweis für die Endlichkeit der Klassenzahl (1977 hat Lenstra einen weiteren Beweis in der Sprache der Packungstheorie gegeben). Einige der untenstehenden Aussagen werden wir daher als bekannt voraussetzen; für Beweise verweisen wir auf Marcus (1977) oder Cassels (1986).

Seien nun die Einbettungen $\tau_1, \ldots, \tau_n$ von K in $\mathbb{C}$ wie vor 1.12. angeordnet; wir definieren dann eine Einbettung von K in den $\mathbb{R}^n$ durch $\varphi : K \hookrightarrow \mathbb{R}^n$: $\alpha \mapsto \varphi(\alpha) = \big(\tau_1(\alpha), \ldots, \tau_r(\alpha), \operatorname{Re} \tau_{r+1}(\alpha), \operatorname{Im} \tau_{r+1}(\alpha), \ldots \operatorname{Re} \tau_{r+s}(\alpha), \operatorname{Im} \tau_{r+s}(\alpha)\big)$, wobei Re bzw. Im den Real-, bzw. Imaginärteil einer komplexen Zahl bezeichnen. Auf $\mathbb{R}^n$ definieren wir nun eine Norm für $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ durch $N(x) = x_1 \cdot \ldots \cdot x_r \cdot (x_{r+1}^2 + x_{r+2}^2) \cdot \ldots \cdot (x_{n-1}^2 + x_n^2)$. Damit wird $N_{K/\mathbb{Q}}(\alpha) = N(\varphi(\alpha))$ für alle $\alpha \in K$. Nun setzen wir

$$A = \Big\{ x \in \mathbb{R}^n : |x_1| + \ldots + |x_r| + 2\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + 2\sqrt{x_{n-1}^2 + x_n^2} < n \Big\} .$$

Bekanntlich ist A beschränkt und konvex, außerdem liefert die Ungleichung zwischen geometrischem und arithmetischem Mittel die Beziehung $|N(a)| < 1$ für alle $a \in A$. Mit $U = \frac{1}{2}A$ ist dann $u - v \in A$ für alle $u, v \in U$, sodaß für solche u, v $|N(u-v)| < 1$ gilt. Schließlich ist noch $\operatorname{vol}(A) = 2^r (\frac{\pi}{2})^s \frac{n^n}{n!}$ und $\operatorname{vol}(U) = 2^{-n} \cdot \operatorname{vol}(A)$, während die Fundamentalmasche F des Gitters $\Gamma_R := \varphi(R)$ im $\mathbb{R}^n$ das Volumen $\operatorname{vol}(F) = 2^{-s}\sqrt{d}$ besitzt.

Im folgenden wollen wir die $\alpha \in K$ mit ihren Bildern $\varphi(\alpha) \in \mathbb{R}^n$ identifizieren; da φ injektiv ist und $N_{K/\mathbb{Q}}(\alpha) = N(\varphi(\alpha))$ gilt, sollten deswegen keine Probleme auftreten.

Seien nun $\vartheta_1, \ldots, \vartheta_m \in K$ paarweise verschieden; dann können wir zu jedem Punkt z aus einer der Mengen $\vartheta_i x + U$ $(i = 1, \ldots, m)$ ein $y \in R$ finden, sodaß $z_o = z - y$ innerhalb der Fundamentalmasche F des Gitters R liegt. Nun ist aber das Gesamtvolumen der Mengen $\vartheta_i x + U$ gleich $m \cdot \operatorname{vol}(U) > M_{r,s} \cdot \operatorname{vol}(U) = 2^{-s}\sqrt{d} = \operatorname{vol}(F)$. Folglich gibt es Indizes i,j und Zahlen $y_1, y_2 \in R$, sodaß

$$\{\vartheta_i x + U - y_1\} \cap \{\vartheta_j x + U - y_2\} \neq \emptyset$$

ist und die Paare (i, y_1) und (j, y_2) verschieden sind. Damit haben wir $u, v \in U$ gefunden mit $\vartheta_i x + u - y_1 = \vartheta_j x + v - y_2$. Wäre $i = j$, so folgte $u - v = y_1 - y_2 \in R$; wegen $|N(u-v)| < 1$ muß dann $N(y_1 - y_2) = 0$ sein, und dies impliziert $y_1 = y_2$. Dies widerspricht aber der Tatsache, daß die Paare (i, y_1) und (j, y_2) verschieden sind. Daher ist $i \neq j$ und $(\vartheta_i - \vartheta_j)x - y = v - u$ für $y := y_1 - y_2$. Normbildung liefert nun $|N((\vartheta_i - \vartheta_j)x - y)| = |N(u-v)| < 1$ wie behauptet.

Wir haben bereits bemerkt, daß aus (1.14) folgt:

(1.15) Gibt es Zahlen $\vartheta_1, \ldots, \vartheta_m \in K$, deren Differenzen Einheiten in R sind, und ist $m > M_{r,s}$, dann ist R normeuklidisch.

Eine Folge $\vartheta_1, \ldots, \vartheta_m$ von Elementen aus K, deren Differenzen lauter Einheiten in R sind, nennen wir eine ***Ausnahmefolge*** ("exceptional sequences") Da es nur auf die Differenzen der ϑ_i ankommt, dürfen wir OBdA $\vartheta_1=0$ annehmen (damit sind alle $\vartheta_i \in R$).Weil weiter mit $\vartheta_i-\vartheta_j$ auch $(\vartheta_i-\vartheta_j)/\vartheta_2$ Einheit ist, ist mit $0, \vartheta_2, \ldots, \vartheta_m$ auch $0, 1, \vartheta_3/\vartheta_2, \ldots, \vartheta_m/\vartheta_2$ eine Ausnahmefolge. Also dürfen wir auch noch $\vartheta_2=1$ annehmen. Ein Beispiel für eine Ausnahmefolge der Länge p ist dann in $K=\mathbf{Q}(\zeta)$, wo $\zeta=\zeta_p$ eine primitive p-te Einheitswurzel bezeichnet: $0, 1, 1+\zeta, 1+\zeta+\zeta^2, \ldots, 1+\zeta+\zeta^2+\ldots+\zeta^{p-2}$; dies zeigt, daß der Ring $\mathbf{Z}[\zeta]$ normeuklidisch ist, falls $p > M_{r,s}$ gilt, und dies ist für $p = 3, 5, 7$ der Fall. Um ein zu (1.15) analoges Ergebnis auch für k-euklidische Ringe formulieren zu können, definieren wir: eine Folge $\vartheta_1, \ldots, \vartheta_m$ heiße ***k-Folge***, wenn die beiden folgenden Bedingungen erfüllt sind:

(F-1) es ist $\vartheta_i-\vartheta_j \in E_k' \setminus \{0\}$ für alle $1 \le i<j \le m$;

(F-2) jeder Teiler des Ideals $(\vartheta_i-\vartheta_j)$ ist Hauptideal.

Damit sind 1-Folgen und Ausnahmefolgen dasselbe, weil dann die Bedingung (F-2) automatisch erfüllt ist. Wir behaupten nun

(1.16) Gibt es in R eine k-Folge der Länge $m > M_{r,s}$, dann ist R k-euklidisch.

Bew.: Sei $x \in K$ gegeben; mit (1.14) finden wir ein $y \in R$ mit $|N((\vartheta_i-\vartheta_j)x-y)| < 1$, wobei $\vartheta_1, \ldots, \vartheta_m$ eine k-Folge der Länge m ist. Wegen (F-2) dürfen wir $y/(\vartheta_i-\vartheta_j) = a/b$ schreiben für gewisse $a,b \in R$ mit $(a,b)=1$ und $b \mid (\vartheta_i-\vartheta_j)$. Wegen (0.12) ist also $b \in k$, daher a/b nach (0.11) ein Kettenbruch der Länge $\le k$ mit Nenner ub für eine Einheit $u \in R^\times$, und schließlich

$$|N_{K/\mathbf{Q}}(x-\tfrac{a}{b})| < \frac{1}{N_{K/\mathbf{Q}}(\vartheta_i-\vartheta_j)} \le \frac{1}{N_{K/\mathbf{Q}}(b)} \cdot$$

mit (1.14). Nun zeigt (0.9), daß R wirklich k-euklidisch ist.

Man beachte, daß eine Folge $\vartheta_1, \ldots, \vartheta_m$ mit der Eigenschaft $\vartheta_i-\vartheta_j \in E_k$ schon eine k-Folge ist: wegen $E_k \subset E_k'$ ist nämlich (F-1) erfüllt, und (0.5.i) zeigt (F-2). Der Grund für die Einführung der Mengen E_k' liegt allein darin, daß diese Mengen i.A. echt größer als die entsprechenden E_k sind, was das Auffinden von (möglichst langen) k-Folgen natürlich erleichtert.

Ist I ein ganzes Ideal in R und gibt es ein primes Restsystem mod I, welches ganz aus Einheiten von R besteht, so sagen wir, I besitze ein primes Einheitenrestsystem (kurz: ein PERS). Insbesondere hat I ein PERS, wenn eine Einheit $u \in R$ existiert, die Primitivwurzel mod I ist. Dagegen gibt es selbst dann, wenn R Einheitenrang 1 hat, Ideale, die zwar ein PERS, aber keine Einheit als Primitivwurzel besitzen.

Wir geben einige einfache Beispiele:

1. $K = \mathbb{Q}(\sqrt{5})$: hier ist $\omega = (1+\sqrt{5})/2$ FE von R, und $0, 1, \omega, 1+\omega$ ist eine 1-Folge, da $1, \omega, 1+\omega, \omega-1$ Einheiten sind. Dagegen ist $0, 1, -1+\omega, \omega, 1+\omega$ keine 1-Folge, weil z.B. die Differenz $-2 = (\omega-1)-(\omega+1)$ keine Einheit ist. Allerdings haben wir hier eine 2-Folge, weil die Ideale $I_1=(2)$ und $I_2=(2+\omega)$ ein PERS besitzen: es ist $\{1, \omega, 1+\omega\}$ ein primes Restsystem mod I_1 und $\{1, \omega, \omega^2, \omega^3, \omega^4\}$ eines mod I_2 (in beiden Fällen ist ω Primitivwurzel).

2. $K=\mathbb{Q}(\sqrt{14})$: hier ist $0,1$ eine 1-Folge der Länge 2, und man sieht leicht ein, daß es keine längeren gibt; sind nämlich u und u-1 Einheiten in R, so sind sie (bis auf ein etwaiges Vorzeichen) Potenzen der FE $e = 15+4\sqrt{14}$. Nun ist aber $e \equiv 1 \bmod 2$, also müßten auch u und $u-1 \equiv 1 \bmod 2$ sein, was offenbar zum Widerspruch führt. Wir behaupten nun, daß $0, 1, 4+\sqrt{14}, 5+\sqrt{14}$ eine 2-Folge ist. Dazu müssen wir zeigen, daß die Ideale $I_1=(3+\sqrt{14})$, $I_2=(4+\sqrt{14})$ und $I_3=(5+\sqrt{14})$ ein PERS besitzen. In § 0 (S. 11) haben wir bereits gesehen, daß $3+\sqrt{14} \in E_2'$ ist, und daß e hier Primitivwurzel ist. Wegen $\|I_2\| = 2$ ist $\{1\}$ ein PERS von I_2; schließlich rechnet man noch nach, daß e auch mod I_3 eine Primitivwurzel ist. Da hier $M_{r,s} = 3,74...$ ist und wir eine 2-Folge der Länge 4 gefunden haben, können wir mit (1.16) folgern, daß $\mathbb{Q}(\sqrt{14})$ 2-euklidisch ist.

Im allgemeinen ist es recht mühsam, in einem gegeben Zahlkörper K eine k-Folge (oder gar eine 1-Folge) genügend großer Länge zu finden; bevor man mit der Suche nach k-Folgen beginnt, wird man daher wissen wollen, ob sich diese Mühe überhaupt lohnt, d.h. ob es in R k-Folgen der gewünschten Länge ($< M_{r,s}$) geben kann. Um diese Frage beantworten zu können, setzen wir

$\mu_k = \sup \{m \in \mathbb{N}$: es gibt eine k-Folge der Länge m in R$\}$ und

$\lambda_k = \inf \{\|I\|$: es gibt eine prime Restklasse mod I, die keinen Vertreter in E_k' hat$\}$.

Insbesondere ist $\lambda_1 = \min \{\|I\| \geq 2 : I$ ist ganzes Ideal in R$\}$, da die prime Restklasse 1 mod I keinen Vertreter in $E_k' = \{0\}$ hat (insbesondere ist $\lambda_1 \leq 2^n$, da man $I = (2)$ wählen kann), und $\lambda_2 = \inf \{\|I\| \geq 2$: I besitzt kein PERS in R$\}$. Mit diesen Bezeichnungen gilt dann

(1.17) Ist λ_k endlich, dann gilt $2 \leq \mu_1 \leq \mu_2 \leq \ldots \leq \mu_k \leq \lambda_k$.

Bew.: Da 0, 1 eine 1-Folge ist, gilt $\mu_1 \geq 2$; weiter ist jede k-Folge erst recht eine (k+1)-Folge, also $\mu_k \leq \mu_{k+1}$ für alle $k \in \mathbb{N}$. Also müssen wir nur noch $\mu_k \leq \lambda_k$ zeigen. Sei dazu I ein ganzes Ideal in R, das eine prime Restklasse mod I besitzt, welche keinen Vertreter in E_k' hat (ein solches existiert, da λ_k endlich ist). Ist dann $\vartheta_1, \ldots, \vartheta_m$ eine k-Folge, dann muß $\vartheta_i - \vartheta_j \not\equiv 0 \bmod I$ sein für alle $i \neq j$: ansonsten wäre nämlich I als Teiler des Ideals $(\vartheta_i - \vartheta_j)$ ein Hauptideal wegen (F-2), also $I=(b)$ für ein $b \in R$. Wegen $b \mid (\vartheta_i - \vartheta_j)$ und (0.12) ist nun $b \in E_k'$, während nach Voraussetzung das Ideal $I=(b)$ eine prime Rest klasse besitzt, welche keinen Vertreter in E' hat: Widerspruch! Also sind $\vartheta_1, \ldots, \vartheta_m$ paarweise inkongruent mod I und $m \leq \|I\|$. Dies aber impliziert $\mu_k \leq \lambda_k$.

Wir wollen die oben gegebenen Beispiele 1. und 2. von Seite 36 noch einmal im Lichte von (1.17) betrachten: in $\mathbf{Q}(\sqrt{5})$ ist $\lambda_1=4$, weil $I = (2)$ das Ideal mit minimaler Norm > 1 ist. Für jede 1-Folge $\vartheta_1,\ldots, \vartheta_4$ sind also die ϑ_i paarweise inkongruent mod 2, wie wir im Beweis von (1.17) gesehen haben, und für $0, 1, \omega, 1+\omega$ ist dies offenbar auch der Fall. Weiter können wir hier $\mu_1 = \lambda_1$ schließen.

In $K=\mathbf{Q}(\sqrt{14})$ dagegen ist $I_2=(4+\sqrt{14})$ ein Ideal der Norm 2, sodaß wir hier $\mu_1 = \lambda_1 = 2$ haben. Weiter ist $\lambda_2 =4$, da das Ideal $I=(2)$ kein PERS hat. Die angegebene 2-Folge der Länge 4 zeigt schließlich $\mu_2 = \lambda_2 = 4$.

Während es mir für $k \geq 3$ nicht gelungen ist zu zeigen, daß die λ_k endlich sind, gilt für k=2:

(1.18) Sei K ein Zahlkörper und q eine rationale Primzahl. Dann gibt es ein $a\in\mathbb{N}$, sodaß $I = (q^a)R$ kein PERS besitzt. Insbesondere ist $\lambda_2 \leq (q^a)^n$, wo $n=(K:\mathbf{Q})$ der Körpergrad ist.

Bew.: Sei N der normale Abschluß von $K/\mathbf{Q}$. Besitzt $I = (q^a)$ ein PERS, dann gibt es zu jedem $r\in\mathbf{Z}$ mit $q\nmid r$ eine Einheit $u\in R^\times$ mit $r \equiv u \bmod I$. Durchläuft σ die Einbettungen von K in $\mathbb{C}$, so folgt für jedes σ die Kongruenz $u^\sigma \equiv r \bmod I$ in $\mathbf{Z}_N$ (= der Ring der ganzen Zahlen in N), da $r^\sigma = r$ und $I^\sigma = I$ ist. Multiplikation über alle σ gibt dann $\pm 1 = N_{K/\mathbf{Q}}(u) = \prod u^\sigma \equiv r^n \bmod I$ in $\mathbf{Z}_N$. Wegen $1, r, q \in \mathbf{Z}$ gilt die Kongruenz $1 \equiv r^n \bmod q^a$ auch in $\mathbf{Z}$. Indem wir nun $r > 1$ und a so groß wählen, daß $q^a > r^n+1$ wird, erhalten wir den gewünschten Widerspruch.

Wir bemerken noch:

1. Ist $\vartheta_1, \ldots, \vartheta_m$ eine 1-Folge in K und $K \subset L$, dann ist $\vartheta_1, \ldots, \vartheta_m$ auch eine 1-Folge in L; für k-Folgen mit $k \geq 2$ gilt dies i.A. nicht mehr, weil die Norm der Ideale $(\vartheta_i - \vartheta_j)$ von L abhängt, falls $\vartheta_i - \vartheta_j$ keine Einheit ist.

2. Wie Lenstra (1977, p. 239) im Falle k=1 bereits bemerkt hat, kann man durch eine kleine Modifikation des Beweises von 1.13. eine obere Schranke für die euklidischen Minima $M^k(K)$ erhalten; es gilt nämlich unter der Voraussetzung von (1.16) $M^k(K) \leq M_{r,s} / \mu_k$.

3. Auch die Definition (1.17) von Lenstra (1977, p. 241) läßt sich auf k-Folgen mit $k>1$ verallgemeinern: man betrachtet hier Folgen $\vartheta_1, \ldots, \vartheta_m$, sodaß unter l+1 Folgengliedern mindestens zwei sind, deren Differenz in E'_k liegt (hierbei ist l eine natürliche Zahl; für l=1 erhält man die gewöhnlichen k-Folgen zurück). Bezeichnet man mit $\mu_{k,l}$ die maximale Länge solcher verallgemeinerter k-Folgen und ist $\mu_{k,l} > l \cdot M_{r,s}$, so kann man ähnlich wie in (1.16) schließen, daß K k-euklidisch ist.

4. Unter der Annahme der erweiterten Riemannschen Vermutung hat Lenstra gezeigt (1977, p. 242/243), daß man mit (1.15) nur endlich viele normeuklidische Zahlkörper finden kann; dabei wurde wesentlich die Ungleichung $\lambda_1 \leq 2^n$, $n=(K:\mathbb{Q})$, benutzt, die man direkt aus der Definition von λ_1 mit $I = (2)$ erhält. Die Abschätzung (1.18) für λ_2 läßt einen ähnlichen Schluß für k-euklidische Ringe mit $k \geq 2$ nicht zu.

Wenn wir zeigen wollen, daß ein Zahlkörper K normeuklidisch ist, müssen wir zu jedem $x \in K$ ein $y \in R$ mit $|N_{K/\mathbb{Q}}(x-y)|<1$ finden. Angenommen, wir kennen eine Funktion $\mathcal{M}_K : K \to \mathbb{R}$ mit der Eigenschaft $|N_{K/\mathbb{Q}}(x)| \leq \mathcal{M}_K(x)$ für alle $x \in K$, so genügt es offenbar, zu jedem $x \in K$ ein $y \in R$ mit $\mathcal{M}_K(x-y)<1$ zu finden. Wegen $N_{K/\mathbb{Q}}(x) = \prod \sigma(x)$, wo das Produkt über alle Einbettungen σ von K in $\mathbb{C}$ läuft, kommt z.B. $\mathcal{M}_K(x) = \mathcal{M}_{K/\mathbb{Q}}(x) = \frac{1}{n}(\sum|\sigma(x)|^2)$ als solche Funktion in Frage; in der Tat gilt

(1.19) Sei K ein Zahlkörper mit $(K:\mathbb{Q}) = n$; dann gilt für alle $x \in K$
$|N_{K/\mathbb{Q}}(x)| \leq \mathcal{M}_K(x)^{n/2}$.

Bew.: Aus der Ungleichung zwischen geometrischem und arithmetischem Mittel erhält man $|N_{K/\mathbb{Q}}(x)|^{2/n} = \{\prod |\sigma(x)|^2\}^{1/n} \leq (\sum |\sigma(x)|^2)/n = \mathcal{M}_K(x)$.

Die Funktion $\mathcal{M}_K$ ist für Kreisteilungskörper (abgesehen von dem Faktor 1/n) bereits von Gauß eingeführt (Werke II , S. 395) und von Cassels 1969 ausführlich untersucht worden. Lenstra ist es dann 1974 gelungen, mit Hilfe von $\mathcal{M}_K$ zu zeigen, daß die Kreisteilungskörper $\mathbb{Q}(\zeta_m)$ für m = 1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 20 normeuklidisch sind. Ojala hat 1977 auch $\mathbb{Q}(\zeta_{16})$ als normeuklidisch nachgewiesen und dabei (neben einem Computer) ebenfalls $\mathcal{M}_K$ benutzt.[1] Der Vorteil von $\mathcal{M}_K$ liegt darin, daß man $\mathcal{M}_K(x)$ i.A. viel einfacher berechnen kann als $N_{K/\mathbb{Q}}(x)$.

Während aber Norm und Spur in Körpertürmen transitiv sind, können wir dies für $\mathcal{M}_K$ nicht erwarten: für $x \in K$ ist nämlich nicht notwendig $\mathcal{M}_K(x) \in \mathbb{Q}$. Ist nämlich σ eine Einbettung von K in $\mathbb{C}$, so ist $|\sigma(x)|^2 = \sigma(x)\overline{\sigma(x)}$ eine Zahl aus dem größten reellen Teilkörper des normalen Abschlusses von $K/\mathbb{Q}$ (mit $\overline{}$ haben wir wie üblich die komplexe Konjugation bezeichnet). Etwas einfacher liegen die Dinge allerdings, wenn $K/\mathbb{Q}$ abelsch ist: dann ist die komplexe Konjugation ein Element der Galoisgruppe $Gal(K/\mathbb{Q})$ und daher mit jedem Automorphismus von $K/\mathbb{Q}$ vertauschbar. Damit folgt leicht $(\mathcal{M}_K(x)) = \mathcal{M}_K(x)$ für jedes $\sigma \in Gal(K/\mathbb{Q})$, und wir haben in der Tat $\mathcal{M}_K(x) \in \mathbb{Q}$ (wesentlich in diesem Beweis ist die Kommutativität von komplexer Konjugation und σ; deswegen gilt $\mathcal{M}_K(x) \in \mathbb{Q}$ sogar für alle CM-Körper, sh. Washington (1982)).

[1] Neulich hat R. McKenzie mit einem Computer gezeigt, daß auch $\mathbb{Q}(\zeta_{13})$ normeuklidisch ist; sh. dazu Leutbecher/Niklasch 1987.

Direkt aus der Definition folgt für abelsche K (bzw. für CM-Körper K) die Beziehung $\mathcal{M}_K(x) = T_{K/\mathbf{Q}}(x\bar{x})/n$, ebenfalls wieder unter Beachtung der Vertauschbarkeit von σ mit den andern Automorphismen. Mit Hilfe dieser Beziehung hat Lenstra (1975) die beiden nächsten Ergebnisse für Kreisteilungskörper bewiesen und bemerkt, daß sie auch für CM-Körper gelten. Verzichtet man aber auf diese Formel, so erhält man etwas allgemeiner:

(1.20) Seien $K \subset L$ Zahlkörper mit $n = (L:K)$; dann gilt für alle $x \in L$ und alle $y \in K$ die Beziehung $\mathcal{M}_L(x) - \mathcal{M}_L(x-y) = \mathcal{M}_K(\frac{1}{n} T_{L/K}(x)) - \mathcal{M}_K(\frac{1}{n} T_{L/K}(x) - y)$.

Dies wird unser Ersatz für die fehlende Transitivität von $\mathcal{M}$ sein; mit (1.20) werden wir nämlich Aussagen über den EA in L machen können, sobald wir nur gewisse Eigenschaften von K gut genug kennen.

Bevor wir dies beweisen, erinnern wir an einige bekannte Tatsachen aus der Körpertheorie (sh. z.B. Marcus 1977): Sei $\mathbf{Q} \subset K \subset L \subset N$, N der normale Abschluß von $L/\mathbf{Q}$, $(K:\mathbf{Q})=k$, $(L:K)=n$, also $(L:\mathbf{Q}) = kn$. Dann gibt es k Einbettungen $\sigma_1, \ldots, \sigma_k$ von K in $\mathbb{C}$, sowie n Einbettungen $\tau_1, \ldots, \tau_n$ von L in $\mathbb{C}$, welche K elementweise fest lassen. Die σ_i und τ_j können wir zu Automorphismen von N fortsetzen (i.A. auf viele verschiedene Weisen), und wir wollen diese (ein für allemal gewählten) Fortsetzungen ebenfalls mit σ_i bzw. τ_j bezeichnen. Damit erhalten wir jede Einbettung ρ von L in $\mathbb{C}$ als Einschränkung der $(L:\mathbf{Q})$ Automorphismen $\sigma_i\tau_j$ von N auf L. Damit haben wir in (1.20)

$$(L:\mathbf{Q})(\mathcal{M}_L(x) - \mathcal{M}_L(x-y)) = \sum |x^\rho|^2 - \sum |(x-y)^\rho|^2$$

$$= \sum_\rho \{x^\rho \overline{x^\rho} - (x-y)^\rho \overline{(x-y)^\rho}\} = \sum_\rho (x^\rho \overline{y^\rho} + \overline{x^\rho} y^\rho - y^\rho \overline{y^\rho})$$

$$= \sum_{\sigma,\tau} \{\sigma\tau(x)\,\sigma\tau(y) + \sigma\tau(x)\,\sigma\tau(y) - \sigma\tau(y)\,\sigma\tau(y)\}.$$

Jetzt beachten wir $\sigma(y) = y$ (denn σ läßt K punktweise fest):

$$= \sum_{\sigma,\tau} \{\sigma\tau(x)\,\overline{\sigma(y)} + \overline{\sigma\tau(x)}\,\sigma(y) - \sigma(y)\overline{\sigma(y)}\}.$$

Indem wir die Summation über τ nach innen ziehen und $T_{L/K}(x) = \sum \tau(x)$ beachten, erhalten wir weiter

$$= \sum_\sigma \{\sigma(T_{L/K}(x))\overline{\sigma(y)} + \overline{\sigma(T_{L/K}(x))}\sigma(y) - n\cdot\sigma(y)\overline{\sigma(y)}$$

$$= n\cdot\{\sum_\sigma \sigma(\tfrac{1}{n} T_{L/K}(x))\ \overline{\sigma(\tfrac{1}{n} T_{L/K}(x))} - \sigma(\tfrac{1}{n} T_{L/K}(x) - y)\ \overline{\sigma(\tfrac{1}{n} T_{L/K}(x) - y)}\}$$

$$= (L:\mathbf{Q})\{\mathcal{M}_K(\tfrac{1}{n} T_{L/K}(x)) - \mathcal{M}_K(\tfrac{1}{n} T_{L/K}(x) - y)\} \quad \text{qued.}$$

Nun behaupten wir

(1.21) Sei $L = K(\zeta_m)$, wo ζ_m eine m-te Einheitswurzel ist. Dann gilt für alle $x \in L$ die Beziehung $(L:K)\mathcal{M}_L(x) = \frac{1}{m} \sum_{j=1}^{m} \mathcal{M}_K(T_{L/K}(x\zeta_m^j))$.

Für den Fall, daß K Kreisteilungskörper ist, stammt (1.21) in dieser Form von Lenstra (1975), geht aber im wesentlichen auf Cassels (1969) zurück.

Bew.: In den folgenden Rechnungen mögen τ und τ' alle (L:K) Einbettungen von L in $\mathbb{C}$ durchlaufen, die K elementweise fest lassen, σ dagegen die Einbettungen von K in $\mathbb{C}$. Dann ist

$$(K:\mathbf{Q})\sum_{j=1}^{m}\mathcal{M}_K(T_{L/K}(x\zeta_m^j)) = (K:\mathbf{Q})\sum_{j=1}^{m}\mathcal{M}_K(\sum_{\tau}\tau(x\zeta_m^j))$$

$$= \sum_{j=1}^{m}\sum_{\sigma}\sigma\Big(\sum\tau(x\zeta_m^j)\Big)\,\overline{\sigma\Big(\sum_{\sigma}\tau(x\zeta_m^j)\Big)}$$

$$= \sum_{\sigma}\sum_{\tau,\tau'}\sum_{j=1}^{m}\sigma\tau(x)\,\overline{\sigma\tau'(x)}\,\sigma\tau(\zeta_m^j)\,\overline{\sigma\tau'(\zeta_m^j)}\,,$$

wobei wir σ, τ, τ' wieder als Automorphismen von $N/\mathbf{Q}$ auffassen. Das Bild einer Einheitswurzel unter einem solchen Automorphismus ist wieder eine Einheitswurzel, und wir finden

$$\overline{\sigma\tau(\zeta_m^j)} = \sigma\tau(\zeta_m^j)^{-1} = \sigma\tau(\zeta_m^{-j}) \quad . \text{ Also ist}$$

$$(K:\mathbf{Q})\sum_{j=1}^{m}\mathcal{M}_K(T_{L/K}(x\zeta_m^j)) = \sum_{\sigma}\sum_{\tau,\tau'}\sum_{j=1}^{m}\sigma\tau(x)\,\overline{\sigma\tau'(x)}\,\Big(\sigma\tau(\zeta_m)\,\overline{\sigma\tau(\zeta_m)}\Big)^j \quad .$$

Jetzt setzen wir $\zeta_{\tau,\tau'} = \sigma\tau(\zeta_m)\,\overline{\sigma\tau(\zeta_m)}$ und finden
$\zeta_{\tau,\tau'} = 1 \Leftrightarrow \tau(\zeta_m) = \tau'(\zeta_m) \Leftrightarrow \tau = \tau'$, sowie

$$\sum_{j=1}^{m}\zeta_{\tau,\tau'}^j = \begin{cases} m\,, \text{ falls } \tau = \tau'; \\ 0 \quad \text{sonst} \end{cases} \quad .$$

Indem wir die Summation über j nach innen ziehen, folgt

$$(K:\mathbf{Q})\sum\mathcal{M}_K(T_{L/K}(x\zeta_m^j)) = m\cdot\sum_{\sigma}\sum_{\tau}\sigma\tau(x)\,\overline{\sigma\tau(x)} = m\cdot\sum_{\rho}x^{\rho}\overline{x^{\rho}}$$

$$= m\cdot(L:\mathbf{Q})\cdot\mathcal{M}_L(x).$$

Durch Division mit $m\cdot(K:\mathbf{Q})$ erhalten wir die Behauptung.

Lenstras Idee war nun, die Existenz des EA in $L=K(\zeta_m)$ auf Eigenschaften von K zurückzuführen. Dazu definiert man $F = F_K = \{x\in K: \mathcal{M}_K(x) \leq \mathcal{M}_K(x-y)$ für alle $y\in R\}$, sowie $c(K) = \sup\{\mathcal{M}_K(x): x\in F_K\}$. Direkt aus der Definition folgt dann, daß es zu jedem $x\in K$ ein $y\in R$ gibt mit $\mathcal{M}_K(x-y) \leq c(K)$. Wegen (1.19) ist R sicher dann normeuklidisch, wenn $c(K)<1$ ist. Tatsächlich genügt oft schon $c(K) \leq 1$, wie wir nun zeigen wollen.

(1.22) Sei K ein Zahlkörper, σ eine Einbettung von K in $\mathbb{C}$, und es gelte $|\sigma(x)| = |\sigma(x-u)| = 1$ für ein $x\in K$ und eine Einheitswurzel $u\in R$; dann ist $x\in R$.

Bew.: Wegen $x^\sigma\overline{x^\sigma} = 1$ und $u^\sigma\overline{u^\sigma} = 1$ gilt

$$1 = |\sigma(x-u)| = (x^\sigma-u^\sigma)\overline{(x^\sigma-u^\sigma)} = 2 - x^\sigma\overline{u^\sigma} - \overline{x^\sigma}u^\sigma$$

für $y = \sigma(-x/u)$ gilt also $y\overline{y} = 1$ und

$$y + \overline{y} = -x^\sigma/u^\sigma - \overline{x^\sigma/u^\sigma} = -(x^\sigma\overline{u^\sigma} + \overline{x^\sigma}u^\sigma)/u^\sigma\overline{u^\sigma} = -1.$$

Damit ist y Nullstelle von $x^2+x+1=0$, d.h. y ist eine dritte Einheitswurzel. Insbesondere ist y ganz, und dies impliziert, daß auch x/u und x ganz sind; dies war zu zeigen.

Ein reelles $c' \in \mathbb{R}$ heißt eine ***brauchbare Schranke*** ("usable bound" bei Lenstra) für K, wenn $c' \geq c(K)$ gilt und es für alle $x \in F_K$ mit $\mathcal{M}_K(x)=c'$ eine Einheitswurzel $u \in R$ gibt mit $\mathcal{M}_K(x-u)=c'$. Man beachte, daß jedes c' mit $c' > c(K)$ brauchbar ist.

(1.23) Ist $c'=1$ brauchbar für K, dann ist K normeuklidisch.

Bew.: Sei ein $x \in K$ gegeben; wir suchen ein $y \in R$ mit $|N_{K/\mathbb{Q}}(x-y)| < 1$. OBdA dürfen wir $x \in F_K$ annehmen; dann ist $\mathcal{M}_K(x) \leq 1$, wegen (1.19) also $|N_{K/\mathbb{Q}}(x)| \leq \mathcal{M}_K(x) \leq 1$. Also genügt $y=0$, falls nicht gerade $|N_{K/\mathbb{Q}}(x)| = 1$ ist. Tritt dies ein, so muß auch $\mathcal{M}_K(x) = 1$ sein, und da $c'=1$ eine brauchbare Schranke für K ist, gibt es eine Einheitswurzel $u \in R$ mit $\mathcal{M}_K(x) = \mathcal{M}_K(x-u) = 1$. Ist $|N_{K/\mathbb{Q}}(x-u)| < 1$, so können wir $y=u$ wählen; andernfalls haben wir $|N_{K/\mathbb{Q}}(x)| = |N_{K/\mathbb{Q}}(x-u)| = \mathcal{M}_K(x) = \mathcal{M}_K(x-u) = 1$. Aus der Gleichheit in (1.19) folgt dann $|\sigma(x)| = |\sigma(x-u)| = 1$ für alle Einbettungen σ, und nach (1.22) ist dann $x \in R$, sodaß hier $y=x$ genügt.

Zentrales Ergebnis ist nun

(1.24) Sei ζ_m eine m-te Einheitswurzel und $L = K(\zeta_m)$; dann gilt $c(L) \leq (L:K)\cdot c(K)$. Ist darüberhinaus c' eine brauchbare Schranke für K, dann ist $(L:K)\cdot c'$ eine solche für L.

Bew.: Sei $x \in F_L$; wir müssen zeigen, daß $\mathcal{M}_L(x) \leq (L:K)\cdot c(K)$ gilt. Wegen $x \in F_L$ ist für alle $y \in S$ und damit erst recht für alle $y \in R$ $\mathcal{M}_L(x-y) \geq \mathcal{M}_L(x)$. Also garantiert (1.20) $\frac{1}{n} T_{L/K}(x) \in F_K$ für $n = (L:K)$. Nun ist $|\sigma(\zeta_m)| = 1$ für jede Einbettung von K in $\mathbb{C}$ und jedes $j \in \mathbb{N}$; also ist $\mathcal{M}_L(x\zeta_m) = \mathcal{M}_L(x)$, und wie oben erhalten wir nun $\frac{1}{n} \cdot T_{L/K}(x\zeta_m) \in F_K$ für $j=1, \ldots, m$. Daher ist $\mathcal{M}_K(T_{L/K}(x\zeta_m)) = n^2 \cdot \mathcal{M}_K(\frac{1}{n} T_{L/K}(x\zeta_m)) \leq n^2 \cdot c(K)$. Mit (1.21) erhalten wir hieraus

$$mn \cdot \mathcal{M}_L(x) = \sum_{j=1}^{m} \mathcal{M}_K(T_{L/K}(x\zeta_m^j) \leq \sum_{j=1}^{m} n^2 \cdot c(K) = mn^2 \cdot c(K),$$

sodaß wir schließlich $\mathcal{M}_L(x) \leq n \cdot c(K)$ haben.

Sei nun c' eine brauchbare Schranke für K und $\mathcal{M}_L(x) = nc'$ für ein $x \in F_L$. Wegen $\mathcal{M}_L(x) \leq n \cdot c(K)$ und $c' \geq c(K)$ muß $c'=c(K)$ sein, und aus obigem Beweis folgt $\mathcal{M}_K(\frac{1}{n}T_{L/K}(x\zeta_m)) = c(K) = c'$ für alle $j \in \mathbb{Z}$. Indem wir $j=0$ wählen, sehen wir, daß $\alpha = \frac{1}{n}T_{L/K}(x)$ ein Element von F_K ist mit $\mathcal{M}_K(\alpha)=c'$. Da c' eine brauchbare Schranke für K ist, gibt es eine Einheitswurzel $u \in R$ mit $\mathcal{M}_K(\alpha - u) = c'$. Mit $y=u$ erhalten wir aus (1.20) $\mathcal{M}_L(x-u) = \mathcal{M}_L(x) = nc'$, und dies zeigt, daß nc' eine brauchbare Schranke für L ist.

Für $K=\mathbb{Q}$ ist $\mathcal{M}_{\mathbb{Q}}(x) = |x|^2$, $F_{\mathbb{Q}} = [-0.5, +0.5]$ und $c(\mathbb{Q}) = 1/4$; um zu zeigen, daß $c' = 1/4$ eine brauchbare Schranke für $\mathbb{Q}$ ist, müssen wir zu jedem $x \in F_{\mathbb{Q}}$ mit $\mathcal{M}_{\mathbb{Q}}(x) = 1/4$ eine Einheitswurzel $u \in \mathbb{Z}$ finden mit $\mathcal{M}_{\mathbb{Q}}(x-u) = 1/4$. Da aber c' auf $F_{\mathbb{Q}}$ nur in den Punkten 0.5 und -0.5 angenommen wird, genügt $u=\pm 1$.

Ist also ζ_m eine primitive m-te Einheitswurzel und $L=\mathbb{Q}(\zeta_m)$, so folgt aus (1.24), daß $c(L) \leq (L:\mathbb{Q})/4$ gilt und $(L:\mathbb{Q})/4$ eine brauchbare Schranke ist. Also sind alle Kreisteilungskörper $L=\mathbb{Q}(\zeta_m)$ mit $(L:\mathbb{Q}) \leq 4$ normeuklidisch: dies sind $\mathbb{Q}(\zeta_m)$ für $m = 3, 4, 5, 8, 12$. Für Kreisteilungskörper $K=\mathbb{Q}(\zeta_p)$, p ungerade Primzahl, hat Lenstra (1974) die Konstanten $c(K)$ auf elementare Weise bestimmt:

(1.25) Sei $K = \mathbb{Q}(\zeta_p)$, $p \equiv 1 \bmod 2$ prim; dann ist $c(K) = \frac{p+1}{12}$, und $c'=c(K)$ ist brauchbare Schranke für K.

Daraus folgt sofort, daß $\mathbb{Q}(\zeta_7)$ und $\mathbb{Q}(\zeta_{11})$ ebenfalls normeuklidisch sind; man erhält jedoch weiter für

$L = \mathbb{Q}(\zeta_9)$: $L = K(\zeta_9)$, $K = \mathbb{Q}(\zeta_3)$, $c(K) = 1/3$, also $c(L) \leq (L:K) \cdot c(K) = 1$;
$L = \mathbb{Q}(\zeta_{15}) = K(\zeta_3)$ für $K = \mathbb{Q}(\zeta_5)$, $c(K) = 1/2$, $c(L) \leq 2/2 = 1$;
$L = \mathbb{Q}(\zeta_{20}) = K(\zeta_4)$ für $K = \mathbb{Q}(\zeta_5)$, $c(K) = 1/2$, $c(L) \leq 2/2 = 1$.
Also sind auch $\mathbb{Q}(\zeta_9)$, $\mathbb{Q}(\zeta_{15})$ und $\mathbb{Q}(\zeta_{20})$ normeuklidisch.

Ist K imaginärquadratischer Zahlkörper, so gilt $\mathcal{M}_K(x) = N_{K/\mathbb{Q}}(x)$ und damit $c(K) = M(K)$; (0.18) zeigt, daß die einzigen imaginärquadratischen Körper mit $c(K) \leq 1/2$ die beiden Kreisteilungskörper $\mathbb{Q}(\zeta_3)$ und $\mathbb{Q}(\zeta_4)$ sind.

Ist dagegegen $K = \mathbb{Q}(\sqrt{m})$ reellquadratisch, so gilt für $x=a+b\sqrt{m}$
$\mathcal{M}_K(x) = ((a+b\sqrt{m})^2 + (a-b\sqrt{m})^2)/2 = a^2+mb^2$, und der Beweis von (0.18) zeigt

(1.26) Sei $K = \mathbb{Q}(\sqrt{m})$ reellquadratischer Zahlkörper; dann gilt

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

Für $K = \mathbb{Q}(\sqrt{5})$ ist also $c(K) = 9/20$, und (1.24) liefert die normeuklidischen Zahlkörper $\mathbb{Q}(\sqrt{5},\sqrt{-1})$, $\mathbb{Q}(\sqrt{5},\sqrt{-3})$ und $\mathbb{Q}(\zeta_5)$.

Um eine weitere Anwendung dieser Methode zu geben, betrachten wir eine quadratische Erweiterung von $K = \mathbb{Q}(\sqrt{-3})$: eine solche läßt sich in der Form $L = K(\sqrt{\mu})$ mit quadratfreiem $\mu \in D(-3)$ schreiben. Wir setzen $\mu = a+b\sqrt{-3}$, $\mu' = a-b\sqrt{-3}$, $\mu\mu' = a^2+3b^2 = p$, und finden für ein $x = r+s\rho+t\sqrt{\mu}+u\rho\sqrt{\mu} \in L$ ($\rho = (-1+\sqrt{-3})/2$) nach etwas Rechnung $\mathcal{M}_{L/\mathbb{Q}}(x) = r^2-rs+s^2+\sqrt{p}(t^2-tu+u^2)$.

Im Falle $\mu \equiv 1 \bmod 4$ ist nun $\beta = (1+\sqrt{\mu})/2$ ganz; indem wir x in der Form $x = e+f\rho+g\beta+h\rho\beta$ schreiben, erhalten wir in obiger Notation $r=e+g/2$, $s=f+h/2$, $t=g/2$, $u=h/2$, also $\mathcal{M}_{L/\mathbb{Q}}(x) = (e+g/2)^2-(e+g/2)(f+h/2)+(f+h/2)^2+\sqrt{p}(g^2-gh+h^2)/4$.

Nun wissen wir aber, daß $c(K) = 1/3$ ist; folglich können wir g und h mod $\mathbb{Z}$ so wählen, daß $g^2-gh+h^2 = \mathcal{M}_{K/\mathbb{Q}}(g+h\rho) \leq 1/3$ wird. Jetzt wählen wir $e+g/2$ und $f+h/2$ mod $\mathbb{Z}$ so, daß auch $(e+g/2)^2-(e+g/2)(f+h/2)+(f+h/2)^2 \leq 1/3$ wird, und haben damit gezeigt: Für alle $x \in L$ können wir ein $y \in S$ finden, sodaß $\mathcal{M}_{L/\mathbb{Q}}(x-y) \leq 1/3+\sqrt{p}/12 = (4+\sqrt{p})/12$ wird.

Insbesondere ist also $c(L) \leq (4+\sqrt{p})/12$, und L ist normeuklidisch, falls nur $\sqrt{p} \leq 8$ (und natürlich $\mu \equiv 1 \bmod 4$) ist. Damit erhalten wir die folgenden normeuklidischen Körper: $K(\sqrt{\mu})$ für $\mu = -1+2\sqrt{-3}$, $3+2\sqrt{-3}$, 5, $-5+2\sqrt{-3}$, -7, $-3+4\sqrt{-3}$, $7-2\sqrt{-3}$; die Diskriminanten dieser Körper sind übrigens $\operatorname{disc} K = 117$, 189, 225, 333, 441, 513, 549. Daß diese Körper normeuklidisch sind, hat schon Lakein (1972) bewiesen, allerdings mit einer völlig anderen Methode.

(1.27) Sei $L = \mathbb{Q}(\sqrt{a+b\sqrt{-3}})$, $p = a^2+3b^2$; dann ist $c(L) \leq (4+\sqrt{p})/12$.

Es sei noch bemerkt, daß für die Funktion $\mathcal{M}_K$ ein Analogon zu (1.14) existiert: setzt man nämlich $\mathcal{M}_K$ auf den $\mathbb{R}^n$ fort durch

$$\mathcal{M}(x) = (x_1^2+\ldots+x_r^2+2(x_{r+1}^2+x_{r+2}^2)+\ldots+2(x_{n-1}^2+x_n^2))/n$$

für ein $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ und setzt $U = \{x \in \mathbb{R}^n : \mathcal{M}(x) < 1/4\}$, so ist $\mathcal{M}(u-v) < 1$ für alle $u,v \in U$. Eine einfache Koordinatentrans formation und eine klassische Volumenberechnung (Volumen einer "Hyperkugel" im $\mathbb{R}^n$) zeigt dann $\operatorname{vol}(U) = 2^{-s}(\frac{\pi}{4})^{n/2}\Gamma(1+\frac{n}{2})$, wo Γ die Gammafunktion bezeichnet. Mit einem Packungsargument (sh. dazu Rogers (1964) und Lenstra (1977)) erhält man dann

(1.28) Sei K ein Zahlkörper mit $(K:\mathbb{Q}) = n$ und $\delta < 1$; dann gibt es für alle $x \in K$ ein $y \in R$ und eine Einheit $u \in R$ mit $\mathcal{M}_{K/\mathbb{Q}}(ux-y) < \delta$, wobei $\delta = \sigma_n \Gamma(1+\frac{n}{2})(\frac{4}{n\pi})^{n/2}\sqrt{|d|}/\mu_1$ ist.

Hierbei sind die σ_n die z.B. bei Lenstra (1977) angegebenen, nur von n abhängigen Größen, und μ_1 gibt (wie auf S. 33) die Länge einer maximalen 1-Folge in K an. Mit (1.19) folgt nun sofort

(1.29) Unter den Voraussetzungen von (1.27) gilt: für alle $x \in K$ gibt es ein $y \in R$ mit $|N_{K/\mathbb{Q}}(x-y)| < \delta^{n/2}$. Insbesondere ist K dann normeuklidisch.

Dies ist wie (1.14) ein Ergebnis, das auf Lenstra (1977) zurückgeht; die folgende Tabelle zeigt, daß (1.29) in den Fällen $n = 2$, $s = 1$; $4 \leqq n \leqq 7$, $s \geqq 2$; $n = 8$, $s \geqq 3$ bessere Schranken als (1.15) und (1.16) liefert:

n	$\sigma_n \Gamma(1+\frac{n}{2})/\pi^{n/2}$	$\sigma_n \Gamma(1+\frac{n}{2})(4/n\pi)^{n/2}$
1	0.5	1
2	$\sqrt{3}/6$	$\sqrt{3}/3$
3	0.18613	0.286566
4	0.13128	0.131280
5	0.09988	0.057175
6	0.08113	0.024039
7	0.06982	0.009848
8	0.06327	0.003955

Ersetzt man μ_1 in δ durch μ_k, so erhält man natürlich entsprechende Ergebnisse für k-euklidische Ringe. Da $\mathcal{M}_K$ nicht multiplikativ ist, erhält man aus (1.28) keine Schranken für c(K); geht man dagegen anders vor und setzt $F'(K) = \{x \in K: \mathcal{M}(x) \leqq \mathcal{M}(ux-y)$ für alle $u \in R^\times$ und alle $y \in R\}$, sowie $c'(K) = \sup\{\mathcal{M}(x): x \in F'\}$, so liefert (1.28) zwar Abschätzungen für $c'(K)$, jedoch hat man kein Ergebnis wie (1.20) oder (1.24) für die $c'(K)$ vorliegen.

Anmerkungen zu § 1

Die Existenz rein verzweigter Primideale läßt sich auch zum Auffinden von Faktoren der Klassenzahl verwenden; das bekannteste Ergebnis dieser Form ist wohl die Geschlechtertheorie von Gauß, der (in unserer Sprache) gezeigt hat, daß die Klassenzahl eines reell-quadratischen Zahlkörpers mit t verzweigten Primidealen durch 2^{t-2} bzw. 2^{t-1} teilbar ist, je nachdem die Norm der Grundeinheit +1 oder -1 ist. Für ähnliche Ergebnisse in Zahlkörpern höheren Grades sh. Ishida (1976).

Die Verwendung rein verzweigter Ideale im Sinne von (1.5) findet sich andeutungsweise bereits bei Behrbohm u. Redei (1936, p. 198); deren Methode ist dann von Erdös und Ko (1938) modifiziert und von Heilbronn (1938, 1950, 1951), Cioffari (1979) und Egami (1979) weiterentwickelt worden[1].

Die Betrachtung der Ideale $I = (u-1)$ für Einheiten u zur Abschätzung von M(K) hat erstmals Redei (1942) vorgeschlagen; er konnte damit z.B. zeigen, daß $\mathbf{Q}(\sqrt{61})$ und $\mathbf{Q}(\sqrt{109})$ nicht normeuklidisch sind.

[1] Beim letzten Abfassen der Arbeit habe ich bemerkt, daß sich zur Abschätzung von M(K) auch Ideale verwenden lassen, die nicht rein verzweigt sind; sh. dazu § 4.

Ist 0, 1, ϑ_2, ..., ϑ_m eine 1-Folge, so muß jedenfalls $\vartheta_i - 1$ für $i \geq 3$ eine Einheit sind. Einheiten u mit der Eigenschaft, daß auch u-1 Einheit ist, heißen ***Ausnahmeeinheiten*** (exceptional units). Ausnahmeeinheiten sind schon untersucht worden, bevor Lenstra ihre Bedeutung für die Existenz eines EA erkannt hat. Julia Robinson hat vermutet, daß es in einem algebraischen Zahlkörper nur endlich viele Ausnahmeeinheiten gibt; diese Vermutung haben dann S. Lang (1960), S. Chowla (1961) und T. Nagell (1964) unabhängig voneinander bewiesen. Nagell hat sich in einer Reihe von Arbeiten mit der Bestimmung aller Ausnahmeeinheiten in Zahlkörpern mit kleinem Einheitenrang befaßt.

Schließlich haben Chudnovsky u. Chudnovsky (1988) gezeigt, daß die Existenz "schneller" Algorithmen zur Multiplikation von Polynomen über $\mathbb{Z}$ von der Existenz von Zahlkörpern mit vielen Ausnahmeeinheiten abhängt.