§ 6 Bizyklische biquadratische Zahlkörper

Seien m und n quadratfreie ganze Zahlen und $K = \mathbb{Q}(\sqrt{m},\sqrt{n})$. Dann ist $K/\mathbb{Q}$ galoische Erweiterung von $\mathbb{Q}$ vom Grad 4 mit abelscher Galoisgruppe $G = \mathrm{Gal}(K/\mathbb{Q}) = V_4$ (Kleinsche Vierergruppe). K enthält genau drei nichttriviale Zwischenkörper, nämlich $k_1 = \mathbb{Q}(\sqrt{m})$, $k_2 = \mathbb{Q}(\sqrt{n})$, und $k_3 = \mathbb{Q}(\sqrt{mn})$. Ist $l = (m,n)$, so schreiben wir $m = lm'$, $n = ln'$ und haben $k_3 = \mathbb{Q}(\sqrt{m'n'})$ mit quadratfreiem $m'n'$. Jedes $\alpha \in K$ können wir in der Form $\alpha = r+s\sqrt{m}+t\sqrt{n}+u\sqrt{mn}$, $r,s,t,u \in \mathbb{Q}$ darstellen; bezeichnet man die Relativnorm von K nach k_i mit N_i, so findet man leicht

$$N_1(\alpha) = a+b\sqrt{m};\quad N_2(\alpha) = c+d\sqrt{n};\quad N_3(\alpha) = e+f\sqrt{mn} \quad \text{mit}$$
$$a = r^2+ms^2-nt^2-mnu^2,\quad b = 2(rs-ntu),$$
$$c = r^2-ms^2+nt^2-mnu^2,\quad d = 2(rt-msu),$$
$$e = r^2-ms^2-nt^2+mnu^2,\quad f = 2(ru-st).$$

Die Normschachtelungsformel liefert dann sofort

$$N_{K/\mathbb{Q}}(\alpha) = a^2-mb^2 = c^2-nd^2 = e^2-mnf^2.$$

Bezeichnet man mit T_i die Relativspur von K nach k_i, so ist ein $\alpha \in K$ genau dann ganz, wenn $N_i(\alpha)$ und $T_i(\alpha)$ für ein $i \in \{1,2,3\}$ ganz sind. Nach einer etwas langwierigen, aber elementaren Rechnung (sh. z.B. Williams (1970)) ergibt sich dann: $\alpha = (r+s\sqrt{m}+t\sqrt{n}+u\sqrt{m'n'})/g \in K$ ist genau dann ganz, wenn die r, s, t, u, $g \in \mathbb{Z}$ den Bedingungen (x) genügen:

m	n	g	(x)
1	1	4	$r \equiv s \equiv t \equiv u \bmod 2$, $r+s+t+lu \equiv 0 \bmod 4$
1	2	2	$r \equiv s \bmod 2$, $t \equiv u \bmod 2$
1	3	2	$r \equiv u \bmod 2$, $s \equiv t \bmod 2$
2	3	2	$r \equiv t \equiv 0 \bmod 2$, $s \equiv u \bmod 2$

Dabei sind m und n nur mod 4 angegeben; man macht sich schnell klar, daß wegen $\mathbb{Q}(\sqrt{m},\sqrt{n}) = \mathbb{Q}(\sqrt{m},\sqrt{mn}) = \mathbb{Q}(\sqrt{n},\sqrt{m})$ usw. alle möglichen Fälle aufgeführt sind.

Setzt man $d = \mathrm{disc}\, K$, $d_i = \mathrm{disc}\, k_i$ $(i = 1,2,3)$, so rechnet man leicht nach, daß in jedem Fall die Beziehung $d = d_1d_2d_3$ gilt (ein Beweis, der ohne Kenntnis der Ganzheitsbasis auskommt, verläuft via der "Führer - Diskriminanten - Formel"). Das Zerlegungsgesetz in K lautet dann

$(p) = P_1P_2P_3P_4$, falls $(d_1/p) = (d_2/p) = (d_3/p) = +1$ ist;

$(p) = P_1P_2$, falls $(d_1/p) = (d_2/p) = +1$, $(d_3/p) = -1$ ist;

$(p) = P_1^2P_2^2$, falls $p|d_1$, $p|d_2$ und $(d_3/p) = +1$ ist;

$(p) = P^2$, falls $p|d_1$, $p|d_2$ und $(d_3/p) = -1$ ist

$(p) = P^4$, falls $p=2$, $2|d_1$, $2|d_2$, $2|d_3$ ist.

Hierbei bezeichnet (/p) das Kroneckersymbol, das für ungerade p mit dem Legendresymbol übereinstimmt und für p=2 und $d \equiv 1 \bmod 4$ durch $(d/2) = (2/d)$ definiert ist.

Die bei Cohn (1978, p. 202) gegebene Tafel der höheren Verzweigungsgruppen für K enthält zwei Fehler; um diese zu korrigieren, übernehmen wir die dortige Notation und unterscheiden:

I. $(d_1/p) = (d_2/p) = (d_3/p) = +1$

II. $(d_1/p) = (d_2/p) = +1,\ (d_3/p) = -1$

III. $p \equiv 1 \bmod 2,\ p|d_1,\ p|d_2,\ (d_3/p) = +1$

IV. $p \equiv 1 \bmod 2,\ p|d_1,\ p|d_2,\ (d_3/p) = -1$

V. $p=2,\ d_1 \equiv d_2 \equiv 12 \bmod 16,\ d_3 \equiv 1 \bmod 8$

VI. $p=2,\ d_1 \equiv d_2 \equiv 12 \bmod 16,\ d_3 \equiv 5 \bmod 8$

VII. $p=2,\ d_1 \equiv d_2 \equiv 8 \bmod 16,\ d_3 \equiv 1 \bmod 8$

VIII. $p=2,\ d_1 \equiv d_2 \equiv 8 \bmod 16,\ d_3 \equiv 5 \bmod 8$

IX. $p=2,\ d_1 \equiv d_2 \equiv 8 \bmod 16,\ d_3 \equiv 12 \bmod 8$

Cohn gibt nun für die Fälle V. und VII. (bzw. VI. und VIII.) dieselben Untergruppenreihen; dies würde jedoch implizieren, daß d = disc K in den Fällen V. und VII. (bzw. VI. und VIII.) durch dieselbe Zweierpotenz teilbar wäre, was aber nicht der Fall ist (beachte $d = d_1d_2d_3$).

Die richtigen Untergruppenreihen gibt folgende Tafel:

Typ	Q	K_Z	K_T	K_1	K_2	K_3	K_4	K
I	Q	K	K	K	K	K	K	K
II	Q	k_3	K	K	K	K	K	K
III	Q	k_3	k_3	K	K	K	K	K
IV	Q	Q	k_3	K	K	K	K	K
V	Q	k_3	k_3	k_3	K	K	K	K
VI	Q	Q	k_3	k_3	K	K	K	K
VII	Q	k_3	k_3	k_3	k_3	K	K	K
VIII	Q	Q	k_3	k_3	k_3	K	K	K
IX	Q	Q	Q	Q	k_3	k_3	K	K

Seien ab jetzt m und n negativ; dann ist K totalimaginär, und seine Einheitengruppe hat Rang 1. Ist u die FE von k_3 (das ist der größte reelle Teilkörper von K), dann gibt es zwei Möglichkeiten :

1. u ist auch FE von K; wir setzen dann q(K)=1;
2. u ist nicht FE von K; dann gibt es eine Einheitswurzel $\zeta \in K$, sodaß $u = \zeta \cdot e^2$ wird. In diesem Fall ist e FE von K, und wir schreiben q(K)=2.

Die Konstante $q(K)$ heißt der ***Einheitenindex von K*** und läßt sich verhältnismäßig leicht bestimmen:

(a) K enthält $\mathbf{Q}(i)$: dann ist $q(K)=2$ genau dann, wenn das Ideal (2) in k_3 Quadrat eines Hauptideals ist: schreibt man $(2) = (\alpha)^2$, so ist $e=\frac{\alpha}{1+i}$ FE von K.
(b) K enthält $\mathbf{Q}(i)$ nicht: dann ist $q(K)=2$ genau dann, wenn das Ideal (m_1) in k_3 Quadrat eines Hauptideals ist: mit $(m_1) = (\alpha)^2$ wird $u = \alpha/\sqrt{m_1}$ FE von K.

Bem.: Teil (a) steht auch in Cohn (1978) als Teil von Theorem 19.8; jedoch fehlt dort die Bedingung, daß (2) zum Quadrat eines Haupt-Ideals wird, obwohl dies im Beweis verwendet wird.

Aus der analytischen Klassenzahlformel folgt nun recht leicht die elegante Beziehung $H = q(K)h_1h_2h_3$, wo H, h_1, h_2, h_3 jeweils die Klassenzahl von K, k_1, k_2, k_3 bedeutet und $K \neq \mathbf{Q}(\sqrt{-1},\sqrt{2})$ ist. Hieraus wiederum erhält man $h_3 | H$ für die Klassenzahl h_3 des reellquadratischen Teilkörpers (dies ist ein Spezialfall der allgemeineren Relation $h^+ | h$, die für CM-Körper K mit größtem reellem Teilkörper K^+ gilt; sh. dazu Washington 1982). Ist K euklidisch, so muß insbesondere $H=1$ und damit auch $h_3=1$ sein.

Beweise für diese und andere Ergebnisse finden sich bei Kuroda (1943, 1950), Kubota (1956), Wada (1966), Fröhlich (1983), sowie in dem klassischen Werk von Hasse (1985).

In ihrer Arbeit aus dem Jahre 1972/73 schreibt J. Sauvageot: "On sait quels corps quadratiques sont euclidiens. La question reste ouverte pour les corps biquadratiques. Elle devrait être bientôt (?) résolue pour ceux d'entre eux qui sont bicyclique imaginaires, ...". In der Tat gilt (den Ring ganzer Zahlen in $\mathbf{Q}(\sqrt{m},\sqrt{n})$ wollen wir zukünftig mit $D(m,n)$ bezeichnen):

(6.1) Sei m negativ; dann sind genau die folgenden Ringe D(m,n) normeuklidisch:
$D(-1,n)$ für $n = 2, 3, 5, 7$;
$D(-2,n)$ für $n = -3, 5$;
$D(-3,n)$ für $n = 2, 5, -7, -11, 17, -19$, und
$D(-7,5)$.

Für Körper $\mathbf{Q}(\sqrt{m}, \sqrt{n})$ mit $m \equiv n \equiv 1 \bmod 2$, $m < 0$, hat bereits J. Sauvageot eine Klassifikation versucht. Trotz eines Fehlers (im Falle $m \equiv n \equiv 1 \bmod 4$) haben sich ihre Vermutungen, die sie am Ende ihrer Arbeit äußert, bestätigt; sie schreibt dort: "... les seuls survivants de ces éliminatoires sont
$\mathbf{Q}(i\sqrt{3}, i\sqrt{7})$; $\mathbf{Q}(i\sqrt{3}, i\sqrt{11})$; $\mathbf{Q}(i\sqrt{3}, \sqrt{5})$ dont LAKEIN a montré qu'ils le sont.
$\mathbf{Q}(i\sqrt{3}, i\sqrt{19})$; $\mathbf{Q}(i\sqrt{3}, \sqrt{17})$ dont j'espère montrer qu'ils le sont.
$\mathbf{Q}(i\sqrt{3}, i\sqrt{43})$, que je crois non-euclidien et
$\mathbf{Q}(i\sqrt{7}, \sqrt{5})$ dont je ne sais rien.
Les mots "j'espère" et "je crois" sont conséquence d'explorations du problème sur ordinateurs que j'exposerai . . . si elles aboutissent."

Bevor wir (6.1) beweisen, geben wir eine Tafel für die ersten Minima gewisser $D(m,n)$ zusammen mit einer Menge C_1 von Punkten, an denen diese angenommen werden.

m	n	$M_1(L)$	C_1
-1	2	$\frac{1}{2}$	$(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0)$
	3	$\frac{1}{4}$	$(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{1}{4})$
	5	$\frac{5}{16}$	$(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{1}{4}), (\frac{1}{4}, \frac{1}{2}, \frac{1}{4}, 0), (\frac{1}{2}, \frac{1}{4}, 0, \frac{1}{4})$
	6	$\frac{5}{2}$	$(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0)$
	7	$\frac{1}{2}$	$(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{1}{4})$
	10	$\frac{5}{2}$	$(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0)$
	11	$\frac{5}{4}$	$(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{1}{4})$
	13	≥ 1	$(0, 0, \frac{2}{13}, \frac{3}{13})$
	14	$\frac{9}{2}$	$(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0)$
	15	1	$(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{1}{4})$
-2	-3	$\frac{1}{3}$	$(\frac{1}{2}, \frac{1}{2}, \frac{1}{6}, \frac{1}{6})$
	5	$\frac{11}{16}$	$(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{1}{4}), (\frac{1}{4}, \frac{1}{2}, \frac{1}{4}, 0), (\frac{1}{2}, \frac{1}{4}, 0, \frac{1}{4})$
	-7	$\frac{9}{8}$	$(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{1}{4})$, $M_2 \leq 0.999$
	-11	$\geq \frac{6323}{5808}$	$(0, 0, \frac{13}{66}, \frac{13}{66})$
-3	2	$\geq \frac{1}{4}$	$(0, 0, \frac{1}{2}, \frac{1}{2})$
	5	$\frac{1}{4}$	$(0, \frac{1}{4}, \frac{1}{4}, 0), (\frac{3}{8}, \frac{1}{8}, \frac{1}{8}, -\frac{1}{8}), (\frac{1}{2}, \frac{1}{4}, \frac{1}{4}, 0)$
	-7	$\frac{4}{9}$	$(\frac{1}{4}, \frac{1}{12}, \frac{1}{4}, -\frac{1}{12})$
	-11	< 0.46	
	13	1	$(\frac{1}{4}, \frac{1}{12}, \frac{1}{4}, \frac{1}{12})$
	17	$\frac{13}{16}$	$(0, \frac{1}{4}, \frac{1}{4}, 0), (\frac{3}{8}, \frac{1}{8}, \frac{1}{8}, -\frac{1}{8}), (\frac{1}{2}, \frac{1}{4}, \frac{1}{4}, 0)$
	-19	< 0.95	
-7	5	$\frac{9}{16}$	$(0, \frac{1}{4}, \frac{1}{4}, 0), (\frac{3}{8}, \frac{1}{8}, \frac{1}{8}, -\frac{1}{8}), (\frac{1}{2}, \frac{1}{4}, \frac{1}{4}, 0)$

Hierbei sind die Punkte unter C_1 bezüglich der Basis $\{1, \sqrt{m}, \sqrt{n}, \sqrt{mn}\}$ angegeben. Weiter erhält man alle Punkte, an denen $M(L)$ angenommen wird, durch Multiplikation mit -1 und Anwenden der drei nichttrivialen Automorphismen von L/Q. Man beachte auch, daß die Ringe $D(-1,15)$ und $D(-3,13)$ semieuklidisch sind; möglicherweise sind auch $D(-1,13)$ und $D(-1,17)$ semieuklidisch.

Um (6.1) zu beweisen, gehen wir wie folgt vor: wir betrachten eine Restklasse α mod 2 in $D(m,n)$. Ist σ derjenige Automorphismus von $\mathbb{Q}(\sqrt{m},\sqrt{n})$, der genau $\mathbb{Q}(\sqrt{m})$ elementweise fest läßt, so ist $N_1(\beta) = \beta\beta^\sigma$. Aus $\beta \equiv \alpha$ mod 2 folgt nun aber $\beta^\sigma \equiv \alpha^\sigma$ mod 2 (wegen $(2)^\sigma = (2)$), also $N_1(\alpha) \equiv N_1(\beta)$ mod 2 für alle $\alpha \equiv \beta$ mod 2. Entsprechendes gilt natürlich auch für die beiden andern Relativnormen N_2 und N_3.

Diese Beobachtung wird es uns ermöglichen, in den beiden imaginärquadratischen Teilkörpern von $\mathbb{Q}(\sqrt{m},\sqrt{n})$ die Existenz ganzer Zahlen mit kleiner Norm nachzuweisen. Hat man z.B. gezeigt, daß $D(m)$, m negativ, ein Element der Norm 2 enthält, so folgt leicht $m \in \{-1, -2, -7\}$ (man braucht ja nur die Lösbarkeit der diophantischen Gleichung $x^2 - my^2 = 2$ für $m \equiv 2,3$ mod 4, bzw. von $x^2 - my^2 = 8$, $x \equiv y$ mod 2, für $m \equiv 1$ mod 4 zu untersuchen).

Den Beweis von (6.1) unterteilen wir in zwei Fälle:

I. Es existiert ein Ideal der Norm 2 in $D(m,n)$.
Da $D(m,n)$ euklidisch ist, ist dieses Ideal Hauptideal, und Relativnormbildung zeigt, daß beide imaginärquadratischen Teilkörper Elemente der Norm 2 enthalten. Also sind zwei der drei Körper $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$ in $\mathbb{Q}(\sqrt{m},\sqrt{n})$ enthalten, und es verbleiben die Möglichkeiten $D(-1,2)$, $D(-1,7)$ und $D(-2,-7)$. Die obige Tabelle zeigt, daß hiervon genau die Ringe $D(-1,2)$ und $D(-1,7)$ normeuklidisch sind.

II. Es existiert kein Ideal der Norm 2 in $D(m,n)$.
Dann kommen nur folgende Möglichkeiten in Betracht:
a) $m \equiv 2, 3$ mod 4, $n \equiv 5$ mod 8
b) $m \equiv 1$ mod 8, $n \equiv 5$ mod 8
Wir betrachten zuerst den Fall a) und unterscheiden, ob $n > 0$ ist oder nicht:

a1) $m \equiv 2, 3$ mod 4, $n \equiv 5$ mod 8, $-m, n \in \mathbb{N}$.
Hier verzweigt (2) in beiden imaginärquadratischen Teilkörpern $\mathbb{Q}(\sqrt{m})$ und $\mathbb{Q}(\sqrt{mn})$; wären die Primideale über (2) in beiden Körpern keine Hauptideale, so könnte nach der Klassenzahlformel nicht $H=1$ sein. Also enthält mindestens einer der beiden imaginärquadratischen Körper ein Element der Norm 2, und wegen $m \equiv 2, 3$ mod 4 ist $m \in \{-1, -2\}$. Ist $D(-1,n)$ normeuklidisch, so gibt es ein $\alpha \in D(-1,n)$ mit $\alpha \equiv (1+\sqrt{-n})/(1+i)$ mod 2 und $N_{K/\mathbb{Q}}(\alpha) < 16 = N_{K/\mathbb{Q}}(2)$. Bezeichnet N_2 die Norm von K nach $\mathbb{Q}(\sqrt{-n})$, so findet man $N_2(\alpha) \equiv \sqrt{-n}$ mod 2. Also enthält $k_2 = \mathbb{Q}(\sqrt{-n})$ ein Element $\beta = N_2(\alpha) \equiv \sqrt{-n}$ mod 2 mit $N(\beta) < 16$ (N steht hier natürlich für die Norm von k_2 nach $\mathbb{Q}$). Wegen $N(\beta) \geq N(\sqrt{-n}) = n$ muß also $n < 16$ sein, und wegen $n \equiv 5$ mod 8 bleiben nur die beiden Möglichkeiten $n=5$ und $n=13$.
Daß $D(-1,13)$ nicht normeuklidisch ist, entnimmt man entweder obiger Tafel oder man verwendet (1.4) mit $L = \mathbb{Q}(\sqrt{-13})$, $K = \mathbb{Q}(\sqrt{-1})$, $B = (3+2i)$, $x=2$ und $e=4$. Wir brauchen dann nur noch zu zeigen, daß es kein $r \in \mathbb{Z}[i]$ gibt mit $N(r) < 13$ und $r \equiv 4$ mod $3+2i$, sodaß r Norm aus $D(-1,13)$ ist. Die beiden ersten Bedingungen werden aber nur von $r = 1-2i$ und $r = -1+i$ erfüllt; wegen $(\frac{13}{2}) = (\frac{13}{5}) = -1$ bleiben aber beide r in L prim.

Ist $D(-2,n)$ normeuklidisch, so betrachten wir entsprechend die Restklasse $\alpha \equiv \sqrt{-2n} + (1+\sqrt{n})/2 \bmod 2$ und finden wie oben $\beta = N_2(\alpha) \equiv 1+\sqrt{-2n} \bmod 2$ und $N(\beta)<16$. Aus $n \equiv 5 \bmod 8$ und $1+2n<16$ folgt aber $n=5$.

a2) $m \equiv 2, 3 \bmod 4$, $n \equiv 5 \bmod 8$, $-m, -n \in \mathbb{N}$

Hier zeigt (1.4) mit $K = \mathbb{Q}(\sqrt{n})$, $L = K(\sqrt{m})$, $B = 2_1$ und $e = (1+\sqrt{n})/2$ (e ist quadratischer Rest mod 2_1 wegen $\Phi_K(2_1)=3$), daß $\mathbb{Q}(\sqrt{n})$ ein Element ungerader Norm < 4 enthält; also ist $n=-3$ oder $n=-11$.

Im Falle $n=-11$ muß außerdem noch $(1+\sqrt{-11})/2$ Norm aus $D(m,-11)$ sein, folglich enthält $D(m)$ ein Element der Norm 3, und dies impliziert $m = -2$.

Ist $D(m,-3)$ normeuklidisch, so betrachten wir die Restklasse $\alpha \equiv \rho+\sqrt{m} \bmod 2$, wo ρ primitive 3. Einheitswurzel ist. Damit ist $N_1(\alpha) \equiv m+1+\sqrt{m} \bmod 2$. Im Falle $m \equiv 2 \bmod 4$ enthält $\mathbb{Q}(\sqrt{m})$ also ein $\beta \equiv 1+\sqrt{m} \bmod 2$ mit $N(\beta)<16$, und dies liefert $m \in \{-2, -6, -10, -14\}$. Unter diesen $D(m,-3)$ haben nur $D(-2,-3)$ und $D(+2,-3) = D(-6,-3)$ Klassenzahl 1.

Entsprechend erhält man im Falle $m \equiv 3 \bmod 4$ nur die Möglichkeiten $m \in \{-1, -5, -13\}$, wobei aber nur $D(-1,-3)$ Klassenzahl 1 hat.

b) $m \equiv 1 \bmod 8$, $n \equiv 5 \bmod 8$.

Sei $\alpha \equiv (1+\sqrt{m})/2 \bmod 2$; dann ist $N_1(\alpha) \equiv (\pm 1+\sqrt{m})/2 \bmod 2$. Soll also die Restklasse $\alpha \bmod 2$ ein Element der Norm <16 enthalten, so enthält auch $D(m)$ ein solches; dies liefert $m<64$. Also enthält jeder der beiden imaginärquadratischen Zahlkörper ein Element der Norm < 64, und von den nun noch verbliebenen Ringen haben nur die folgenden Klassenzahl 1: $D(-3,5)$, $D(-3,-7)$, $D(-3,-11)$, $D(-3,17)$, $D(-3,-19)$, $D(-3,-43)$, $D(-7,5)$, $D(-7,-11)$, $D(-7,-19)$, $D(-7,-43)$ und $D(-11,-19)$. J. Sauvageot hat 1972/73 versucht, durch Betrachten der Restklasse mod 2 noch einige dieser Ringe auszuschließen, hat dabei jedoch einen Fehler gemacht. In der Tat kommen wir hier nur mit (1.4) (oder 1.12.) weiter:

m	n	x	K	B	r mod B	M(K)≥
-3	-43	$(1+\sqrt{-43})/2$	$\mathbb{Q}(\sqrt{-43})$	(3)	$\sqrt{-43}$	$13/9$
-7	-11	3	$\mathbb{Q}(\sqrt{-7})$	$2+\sqrt{-7}$	-2	$16/11$
-7	-19	2	$\mathbb{Q}(\sqrt{-19})$	$(3+\sqrt{-19})/2$	-3	1
-7	-43	$(3+\sqrt{-43})/2$	$\mathbb{Q}(\sqrt{-43})$	(7)	$(-3+3\sqrt{-43})/2$	$99/49$
-11	-19	4	$\mathbb{Q}(\sqrt{-19})$	$(5+\sqrt{-19})/2$	5	1

Damit ist (6.1) bewiesen.

Ein Teil der unter (6.1) aufgeführten Körper läßt sich leicht als normeuklidisch erkennen. Dazu beachten wir Folgendes: ist R ein Zahlring, $\alpha, \beta \in R$ und ist auch $(\alpha+\beta)/2$ ganz, so können wir $x\alpha + y\beta$ (mit $x,y \in \mathbb{Q}$) mod R so verschieben, daß $|x|,|y| \le \frac{1}{2}$ und $|x|+|y| \le \frac{1}{2}$ wird. Offensichtlich können wir ja $|x|,|y| \le \frac{1}{2}$ erreichen; ist dann z.B. $x+y \ge \frac{1}{2}$ (und damit $x,y \ge 0$), so setzen wir $x' = x - \frac{1}{2}$, $y' = y - \frac{1}{2}$ und haben $|x'|,|y'| \le \frac{1}{2}$ und $|x'|+|y'| \le \frac{1}{2}$.

Weiter beachten wir, daß K totalkomplex und somit $N_{K/\mathbb{Q}}(\alpha) \geq 0$ für alle $\alpha \in K$ ist. Um $|N_{K/\mathbb{Q}}(\alpha)| < 1$ zu zeigen, brauchen wir also nur $N_{K/\mathbb{Q}}(\alpha) < 1$ zu zeigen. Dies werden wir in der Regel dadurch tun, daß wir $N_{K/\mathbb{Q}}(\alpha) = X^2 - nY^2$ schreiben und dann $|X| < 1$ nachweisen; dann ist nämlich $N_{K/\mathbb{Q}}(\alpha) = X^2 - nY^2 \leq X^2 < 1$ (bessere Abschätzungen erhält man natürlich, wenn man auch $|Y| \geq c > 0$ für gewisse α zeigen kann, weil dann $N_{K/\mathbb{Q}}(\alpha) = X^2 - nY^2 \leq X^2 - nc^2$ ist).

Diese Überlegungen werden wir im Folgenden ständig benutzen; so wählen wir z.B. im Falle D(-1,2) die Basis $\{1, i, \sqrt{2}, \sqrt{-2}\}$, beachten, daß $(\sqrt{2}+\sqrt{-2})/2$ ganz ist, und verschieben $x+yi+z\sqrt{2}+w\sqrt{-2}$ mod R so, daß $|x|, |y|, |z|, |w| \leq \frac{1}{2}$ und $|z|+|w| \leq \frac{1}{2}$ wird. Die letzte Ungleichung liefert $z^2+w^2 \leq \frac{1}{4}$ und damit $x^2+y^2+2z^2+2w^2 \leq 1$ (wobei genau dann Gleichheit herrscht, wenn $|x| = |y| = \frac{1}{2}$ und $|z| = \frac{1}{2}$, $w = 0$ oder $z = 0$, $|w| = \frac{1}{2}$ ist).

Nun ist aber $N_{K/\mathbb{Q}}(x+yi+z\sqrt{2}+w\sqrt{-2}) = X^2-2Y^2$ mit $X = x^2+y^2+2z^2+2w^2$ und $Y = 2(xz+yw)$, folglich $N_{K/\mathbb{Q}}(x+yi+z\sqrt{2}+w\sqrt{-2}) \leq X^2 \leq 1$. Da Gleichheit höchstens in den beiden oben angegebenen Fällen eintreten kann, dort aber $|Y| = 2|xz| = \frac{1}{2}$ und somit $X^2-2Y^2 = \frac{1}{2}$ ist, haben wir in jedem Fall $N_{K/\mathbb{Q}}(x+yi+z\sqrt{2}+w\sqrt{-2}) < 1$ erreicht.

In D(-1,n), $n \in \{-3, 5\}$, gehen wir etwas anders vor: hier wählen wir die Basis $\{1, i, \sqrt{n}, \sqrt{-n}\}$ und beachten, daß $(1+\sqrt{n})/2$ und $(i+\sqrt{-n})/2$ ganz sind. Nun können wir $x+yi+z\sqrt{n}+w\sqrt{-n}$ mod R so verschieben, daß im Falle

$$n = -3: \quad x^2+3w^2 \leq \tfrac{1}{3}, \quad y^2+3z^2 \leq \tfrac{1}{3}$$
$$n = 5: \quad x^2+5z^2 \leq \tfrac{9}{20}, \quad y^2+5w^2 \leq \tfrac{9}{20}$$

wird (dies folgt aus dem Beweis von (0.21)). Jetzt folgt wieder

$$N_{K/\mathbb{Q}}(x+yi+z\sqrt{n}+w\sqrt{-n}) = X^2-|n|Y^2 \leq X^2 \quad \text{mit}$$
$$|X| = x^2+y^2+3z^2+3w^2 \leq \tfrac{2}{3} \quad \text{im Falle } D(-1,-3) \text{ und}$$
$$|X| = x^2+y^2+5z^2+5w^2 \leq \tfrac{9}{10} \quad \text{im Falle } D(-1,5).$$

Ganz analog kann man nun zeigen, daß die Ringe D(-3,2), D(-3,-2), D(-3,5), und D(-3,-7) normeuklidisch sind. Daß D(-1,2) und D(-1,3) normeuklidisch sind, wußte schon Eisenstein (1850), dessen Beweis dem obigen recht ähnlich ist. Masley hat 1972 (in Unkenntnis der Eisensteinschen Arbeit) weitere Beweise hierfür gegeben, die jedoch weit komplizierter als die oben angegebenen sind. Lakein wies dann (ebenfalls 1972) nach, daß der EA auch in den Ringen D(-1,5), D(-1,7), D(-3,2), D(-3,-2), D(-3,5), D(-3,-7), und D(-3,-11) gilt. Dies läßt sich per Computer leicht nachprüfen; außerdem erhält man die neuen normeuklidischen Ringe D(-2,5), D(-3,17), D(-3,-19) und D(-7,5).

Schließlich kann man wie im reellquadratischen Fall die ersten Minima M(K) für eine ganze Klasse von Zahlkörpern angeben:

(6.2) <u>Sei</u> $m = n^2+1$, <u>$n \equiv 1$ mod 2</u>, $R = \mathbb{Z}[i, \sqrt{m}, (\sqrt{m}+\sqrt{-m})/2]$, <u>und f der Absolutbetrag der Norm. Dann ist</u> $M(f) = \frac{m}{4}$, <u>und dieses Minimum wird mod R nur in dem Punkt</u> $(1+i+\sqrt{m})/2$ <u>angenommen. Ist m quadratfrei, so ist</u> $M(f) = M(K)$.

Wir gehen vor wie in $\mathbb{Q}(\sqrt{m})$ (sh. § 2) und setzen $\vartheta = n+\sqrt{m}$. Damit ist $\{1, i, \vartheta, (1+i+\vartheta+i\vartheta)/2\}$ eine GHB, und mit $x = a+bi$, $y = c+di$ gilt $N_1(x+y\vartheta) = x^2+2nxy-y^2$, sowie $N_{K/\mathbb{Q}}(x+y\vartheta) = |x^2+2nxy-y^2|^2$ (hier fassen wir $x^2+2nxy-y^2$ als Element von $\mathbb{C}$ auf; $|\ |$ ist der gewöhnliche Betrag auf $\mathbb{C}$). Für jeden Ausnahmepunkt $z = x+y\vartheta$ gilt daher $\frac{m}{4} \le N_{K/\mathbb{Q}}(x+y\vartheta)$ und somit $\frac{n}{2} < |x^2+2nxy-y^2|$! Nun können wir z mod R so wählen, daß zuerst $|c|, |d| \le \frac{1}{2}$ und $|c|+|d| \le \frac{1}{2}$, und dann $|a|,|b| \le \frac{1}{2}$ wird. Damit ist dann $|x|^2 = a^2+b^2 \le \frac{1}{2}$ und $|y|^2 = c^2+d^2 \le \frac{1}{4}$, also $\frac{n}{2} \le |N_1(z)| = |x^2+2nxy-y^2| \le |x|^2+2n|xy|+|y|^2 \le n|x|+\frac{3}{4}$.

Dies impliziert $|x| \ge \frac{1}{2}-\frac{3}{4n}$ für jeden Ausnahmepunkt $z = x+y\vartheta$. Indem wir z mod R aber so wählen, daß zuerst $|a|, |b| \le \frac{1}{2}$, $|a|+|b| \le \frac{1}{2}$ und dann $|c|,|d| \le \frac{1}{2}$ wird, folgt entsprechend $|y| \ge \frac{1}{2}-\frac{3}{4n}$. Wenn wir den Fundamentalbereich F nun geeignet wählen, liegt jeder Ausnahmepunkt $z = x+y\vartheta$ in der durch die Ungleichungen $\left||x|-\frac{1}{2}\right| \le \frac{3}{4n}$, $\left||y|-\frac{1}{2}\right| \le \frac{3}{4n}$ definierten Menge.

Sei jetzt wieder $|c|,|d| \le \frac{1}{2}$ und $|c|+|d| \le \frac{1}{2}$. Zusammen mit $|y| \ge \frac{1}{2}-\frac{3}{4n}$ folgt wegen $c^2+d^2 = |y|^2 \ge \frac{1}{4}-\frac{3}{4n}+(\frac{3}{4n})^2$ und $c^2 \le (\frac{1}{2}-|d|)^2$, daß

$\frac{1}{4}-\frac{3}{4n}+(\frac{3}{4n})^2 \le c^2+d^2 \le 2d^2-|d|+\frac{1}{4}$ gilt. Jetzt finden wir für $n \ge 7$

$$(|d|-\tfrac{1}{4})^2 \ge \tfrac{1}{16}-\tfrac{3}{8n}+\tfrac{9}{32}n^{-2} \ge (\tfrac{1}{4}-\tfrac{1}{n})^2,$$

und wenn wir berücksichtigen, daß $|x|$ und $|y|$ nahe bei $\frac{1}{2}$ liegen, können wir dies auch für $n \ge 5$ nachweisen. Also ist $|d| < \frac{1}{n}$, $\left||c|-\frac{1}{2}\right| < \frac{1}{n}$ oder $|c| < \frac{1}{n}$, $\left||d|-\frac{1}{2}\right| < \frac{1}{n}$. Ganz analog folgen die entsprechenden Ungleichungen für a und b. Damit bleiben die folgenden möglichen Ausnahmemengen ($\delta = \frac{1}{n}$):

$S_1 = (0, \frac{1}{2}, \frac{1}{2}, 0) + (-\delta,\delta)\times(-\delta,\delta)\times(-\delta,\delta)\times(-\delta,\delta)$ und

$S_2 = (\frac{1}{2}, 0, \frac{1}{2}, 0) + (-\delta,\delta)\times(-\delta,\delta)\times(-\delta,\delta)\times(-\delta,\delta)$ da z.B. S_1 und

$S_3 = (\frac{1}{2}, 0, 0, \frac{1}{2}) + (-\delta,\delta)\times(-\delta,\delta)\times(-\delta,\delta)\times(-\delta,\delta)$ mod R kongruent sind. Jetzt kann man leicht nachrechnen, daß S_2 keinen Ausnahmepunkt enthält und somit S_1 die einzige Ausnahmemenge ist.

Eine nochmalige Abschätzung der Norm auf S zeigt nun, daß man $\delta = \frac{1}{n}$ durch $\varepsilon = \frac{1}{3n}$ ersetzen darf. Dann beachtet man, daß ϑ eine Einheit ist und $(a+bi+c\vartheta+di\vartheta)\vartheta = c+di+(a+2nc)\vartheta+(b+2nd)i\vartheta$ gilt, und stellt fest, daß die Schranken die Anwendung von (2.3) erlauben. Also ist $z = (i+\vartheta)/2$ mod R der einzig mögliche Ausnahmepunkt, und wegen $N_{K/\mathbb{Q}}(z) = \frac{m}{4}$ folgt $M(K) \le \frac{m}{4}$.

Um M(K) nach unten abzuschätzen, gehen wir vor wie folgt: es sei z.B. $a \equiv d \equiv 0$, $b \equiv c \equiv \frac{1}{2}$ mod 1. Dann gelten mit $x=a+bi$, $y=c+di$ die Kongruenzen $2xy = 2(ac-bd)+2(ad+bc)i \equiv \frac{i}{2}$ mod $\mathbb{Z}[i]$ und $x^2-y^2 = a^2-b^2-c^2+d^2+2(ab-cd)i \equiv \frac{1}{2}$ mod $\mathbb{Z}[i]$. Also ist $|\mathrm{Re}(x^2+2nxy-y^2)| \ge \frac{1}{2}$ und $|\mathrm{Im}(x\ +2nxy-y\ )| \ge \frac{n}{2}$, folglich $N_{K/\mathbb{Q}}(z-a) \ge (1+n^2)/4 = \frac{m}{4}$ für alle $a \in R$. Damit sind alle Behauptungen bewiesen.

Anmerkungen zu § 6

1850: Eisenstein zeigt im Zuge seiner Untersuchungen über achte Potenzreste, daß D(-1,2) normeuklidisch ist und bemerkt, daß sich D(-1,3) ganz analog behandeln läßt.

1894: Hilbert schreibt eine Abhandlung über Dirichlet'sche Zahlkörper, in welcher er insbesondere das quadratische Reziprozitätsgesetz in diesen Körpern untersucht

1943: Kuroda beginnt, die Dirichlet'schen Zahlkörper zu studieren; diese Untersuchungen werden von Kubota (1956) und Wada (1966) fortgeführt.

1952: Hasse (1985) bestimmt alle imaginären bizyklischen Körper mit ungerader Klassenzahl.

1970: Williams veröffentlicht eine elementare Berechnung der GHB spezieller Dirichlet'scher Zahlkörper.

1972: Lakein bestimmt einige normeuklidische Dirichlet'sche Zahlkörper; unabhängig davon zeigt Masley, daß D(-1,2) und D(-1,3) normeuklidisch sind. Sauvageot gibt erstmals einige Dirichlet'sche Zahlkörper an, die zwar Klassenzahl 1 haben, aber nicht normeuklidisch sind.

1974: Brown und Parry bestimmen alle imaginären bizyklischen Zahlkörper mit Klassenzahl 1. Dies wurde durch die Lösung des "Klassenzahl-2"-Problems in imaginärquadratischen Körpern ermöglicht.