§ 5 Reine Zahlkörper von Zweierpotenzgrad

Wir beginnen mit rein biquadratischen Zahlkörpern und verwenden dazu folgende Notation:

$m = ab^2c^3$ mit $(a,b) = b,c) = (c,a) = 1$, a,b,c quadratfrei,

$K_1 = \mathbf{Q}(\sqrt[4]{m})$, $K_2 = \mathbf{Q}((1+i)\sqrt[4]{m}) = \mathbf{Q}(\sqrt[4]{-4m})$, $K_3 = \mathbf{Q}(i,\sqrt{ac})$,

$k_1 = \mathbf{Q}(\sqrt{ac})$, $k_2 = \mathbf{Q}(\sqrt{-ac})$, $k_3 = \mathbf{Q}(i)$, $L = K_1(i) = K_2(i) = \mathbf{Q}(i,\sqrt[4]{m})$.

Zuerst wollen wir uns fragen, wann das Polynom $f(x) = x^4 - m$ über $\mathbf{Q}$ irreduzibel ist; da nach Voraussetzung m keine 4. Potenz ist, hat f keine Nullstellen in $\mathbf{Q}$, sodaß f höchstens in das Produkt zweier quadratischer Faktoren zerfallen kann. Setzt man

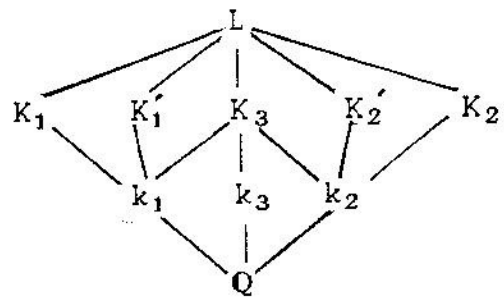
$f(x) = (x^2+rx+s)(x^2+tx+u)$ für $r,s,t,u \in \mathbf{Z}$, so folgt

(a) $r=t=0$, $s=-u$, also $m=s^2$: m ist Quadrat in $\mathbf{Z}$; oder

(b) $s=u$, $r=-t$, $r=2s$, $r^4=4s^2=-4m$: $-4m$ ist 4. Potenz in $\mathbf{Z}$.

Also ist f genau dann zerlegbar über $\mathbf{Q}$, wenn $ac=1$ oder $ac=-1$, $b \equiv 0 \bmod 2$ gilt. Diese beiden Fälle wollen wir in Zukunft ausschließen.

Damit entsteht K_1 durch Adjunktion einer Wurzel α des Polynoms f; die andern Wurzeln von f sind $-\alpha$ und $\pm i\alpha$. Falls $K_1/\mathbf{Q}$ galoisch ist, muß $i \in K_1$ sein. Dann zerfällt f über $\mathbf{Q}(i)$ in das Produkt zweier quadratischer Polynome mit Koeffizienten aus $\mathbf{Z}[i]$, und ein Koeffizientenvergleich liefert $m=-b$ für ein $b \in \mathbf{Z}$. Tatsächlich ist dann $f(x) = (x^2+ib)(x^2-ib)$, sowie $K_1=\mathbf{Q}(i,\sqrt{2b})$. Ist also $\pm m$ kein Quadrat in $\mathbf{Z}$, dann ist f irreduzibel, L der Zerfällungskörper von f und $(L:K_j) = 2$ für $j=1,2,3$. Als Galois- Gruppe von f bzw. $L/\mathbf{Q}$ entpuppt sich die Diedergruppe $D_4 = \{1, s, s^2, s^3, t, ts, ts^2, ts^3\}$ mit den Automorphismen $s : i \to i$, $\alpha \to i\alpha$ und $t : i \to -i$, $\alpha \to \alpha$. D_4 hat die folgenden Untergruppen: $G_1 = \{1, t\}$, $G_1' = s^{-1}G_1 s = \{1, ts^2\}$, $G_2 = \{1, ts\}$, $G_2' = s^{-1}G_2 s = \{1, ts^3\}$, $G_3 = \{1, s^2\}$, $= Z(D4)$ (Z bezeichnet das Zentrum): $g_1 = \{1, s^2, t, ts^2\}$; $g_2 = \{1, s^2, ts, ts^3\}$, $g_3 = \{1, s, s^2, s^3\}$. Dabei ist K_j Fixkörper von G_j, k_j Fixkörper von g_j, jeweils für $j=1, 2, 3$. Weiter ist $K_1' = \mathbf{Q}(i\sqrt[4]{m})$ der Fixkörper von G_1' und $K_2' = \mathbf{Q}(i\sqrt[4]{-4m}) = \mathbf{Q}((1-i)\sqrt[4]{m})$ derjenige von G_2'. Wir haben also das folgende Körperdiagramm:



Hilbert'sche Untergruppenreihe

p		e	f	g	K_1	K_2	Z	T	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8
$p \equiv 1 \bmod 4$:	$(\frac{m}{p}) = +1$, $(\frac{m}{p})_4 = +1$	1	1	8	(1,1,1,1)	(1,1,1,1)	1	1	1	1	1	1	1	1	1	1
	$(\frac{m}{p}) = +1$, $(\frac{m}{p})_4 = -1$	1	2	4	(2,2)	(2,2)	G_3	1	1	1	1	1	1	1	1	1
	$(\frac{m}{p}) = -1$	1	4	2	(4)	(4)	g_3	1	1	1	1	1	1	1	1	:
	$(\frac{ac}{p}) = +1$, p|b	2	1	4	$(1^2,1^2)$	$(1^2,1^2)$	G_3	G_3	1	1	1	1	1	1	1	:
	$(\frac{ac}{p}) = -1$, p|b	2	2	2	(2^2)	(2^2)	g_3	G_3	1	1	1	1	1	1	:	:
	p|ac	4	1	2	(1^4)	(1^4)	g_3	g_3	1	1	1	1	1	1	:	:
$p \equiv 3 \bmod 4$:	$(\frac{m}{p}) = +1$	1	2	4	(1,1,2)	(2,2)	G_1	1	1	1	1	1	1	:	:	:
	$(\frac{m}{p}) = -1$	1	2	4	(2,2)	(1,1,2)	G_2	1	1	1	1	1	1	:		
	$(\frac{ac}{p}) = +1$, p|b	2	2	2	$(1^2,1^2)$	(2^2)	g_1	G_3	1	1	1	1	:	:		
	$(\frac{ac}{p}) = -1$, p|b	2	2	2	(1^2)	$(1^2,1^2)$	g_2	G_3	1	1	1	:	:			
	p|ac	4	1	2	(1^4)	(1^4)	G	g_3	1	1	1	:	:			
p = 2 :	$m \equiv 1 \bmod 16$	2	1	4	$(1,1,1^2)$	$(1^2,1^2)$	G_1	G_1	G_1	1	1	1	:			
	$m \equiv 9 \bmod 16$	2	2	2	$(2,1^2)$	$(1^2,1^2)$	g_1	G_1	G_1	1	1	1	:			
	$\frac{m}{4} \equiv -1 \bmod 16$, 2|b	2	1	4	$(1^2,1^2)$	$(1,1,1^2)$	G_2	G_2	G_2	1	1	1	1			
	$\frac{m}{4} \equiv -9 \bmod 16$, 2|b	2	2	2	$(1^2,1^2)$	$(2,1^2)$	g_2	G_2	G_2	1	1	1	1			
	$ac \equiv 1 \bmod 8$, 2|b	4	1	2	$(1^2,1^2)$	(1^4)	g_1	g_1	g_1	G_3	G_3	1	1			
	$ac \equiv 5 \bmod 8$, 2+b	4	2	1	(1^2)	(1^4)	G	g_1	g_1	1	1	1	1			
	2|b	4	2	1	(1^2)	(1^4)	G	g_1	g_1	G_3	G_3	1	1	:	:	:
	$ac \equiv 7 \bmod 8$, 2+b	4	1	2	(1^4)	$(1^2,1^2)$	g_2	g_2	g_2	G_3	G_3	1	1	1	1	:
	$ac \equiv 3 \bmod 8$, 2+b	4	2	1	(1^4)	(2^2)	G	g_2	g_2	G_3	G_3	1	1	1	1	:
	2|b	4	2	1	(1^4)	(2^2)	G	g_2	g_2	1	1	1	1	1	1	1
	2|ac	8	1	1	(1^4)	(1^4)	G	G	G	g_3	g_3	G_3	G_3	G_3	G_3	1

Ganzheitsbasis von $\mathbf{Q}(\sqrt[4]{m})$

m	disc K_1	disc L	GHB	Bemerkun
2|ac	$2^8a^3b^2c^3$	$2^{18}a^6b^4c^6$	$\{1, \alpha_1, \alpha_2, \alpha_3\}$ -	
$ac \equiv 3 \bmod 4$, 2+b	$2^8a^3b^2c^3$	$2^{18}a^6b^4c^6$	$\{1, \alpha_1, \alpha_2, \alpha_3\}$ -	
$ac \equiv 3 \bmod 8$, 2|b	$2^4a^3b^2c^3$	$2^8a^6b^4c^6$	$\{1, \alpha_1, \beta_2, \beta_3\}$ $\beta_2 = (1 + \alpha_1 + \alpha_2)/2$,	
$ac \equiv 7 \bmod 8$, 2|b	$2^2a^3b^2c^3$	$2^4a^6b^4c^6$	$\{1, \alpha_1, \beta_2, \beta_3\}$ $\beta_2 = (1 + \alpha_1 + \alpha_2)/2$,	
$ac \equiv 1 \bmod 8$, 2+b	$2^2a^3b^2c^3$	$2^8a^6b^4c^6$	$\{1, \alpha_1, \beta_2, \beta_3\}$ $\beta_2 = (1 + \alpha_2)/2$,	
$ac \equiv 5 \bmod 8$, 2+b	$2^4a^3b^2c^3$	$2^{12}a^6b^4c^6$	$\{1, \alpha_1, \beta_2, \beta_3\}$ $\beta_2 = (1 + \alpha_2)/2$,	
$ac \equiv 1 \bmod 4$, 2|b	$2^4a^3b^2c^3$	$2^{12}a^6b^4c^6$	$\{1, \alpha_1, \beta_2, \beta_3\}$ $\beta_2 = (1 + \alpha_2)/2$,	

Die Galoisgruppe D_4 ist 1987 von C.E. van der Ploeg untersucht worden; dessen Arbeit enthält jedoch einige Fehler: so ist es z.B. nicht richtig, daß jeder nichtnormale Zahlkörper 4. Grades einen quadratischen Zahlkörper enthält, oder daß als Galoisgruppen von Polynomen 4. Grades nur Z_4, V_4 oder D_4 in Frage kommen (es fehlen A_4 und S_4; Zahlkörper 4. Grades, deren Galoisabschluß diese Gruppen als Galoisgruppen besitzt, haben z.B. keine quadratischen Zahlkörper); außerdem fehlt in den dort aufgeführten Körperdiagrammen der Körper, den wir mit k_3 bezeichnet haben.

Um nun eine GHB, die Diskriminante und das Zerlegungsgesetz von $Q(\sqrt[4]{m})$ zu finden, gehen wir wie folgt vor: wir stellen die Hilbertsche Untergruppenreihe für alle Primideale P in L auf, lesen daraus das Zerlegungsgesetz in L, K_1, K_2 ab, bestimmen die Beiträge der einzelnen P zur Differente, und errechnen schließlich die Diskriminante und die Ganzheitsbasis von K_1. Die Ergebnisse dieser Rechnungen sind in den oben stehenden Tafeln festgehalten; dabei bedeuten

$p \in \mathbb{N}$ eine rationale Primzahl
P ein Primideal in L über (p)
Z = Z(P|p) die Zerlegungsgruppe
T = T(P|p) die Trägheitsgruppe
$V_j = V_j(P|p)$ die j-te Verzweigungsgruppe, $V_o = T$
e = e(P|p) der Verzweigungsindex
f = f(P|p) der Trägheitsgrad
$\alpha_1 = \alpha = \sqrt[4]{m}$, $m = ab^2c^3$, $\alpha_2 = \sqrt{ac}$, $\alpha_3 = \sqrt[4]{a^3b^2c}$
(/p) das Legendre-Symbol
$(/p)_4$ das biquadratische Restsymbol (falls (/p) = +1 ist).

Weiter bedeutet z.B. (1,1,2), daß (p) in dem entsprechenden Körper in das Produkt dreier Primideale zerfällt, von denen eines den Trägheitsgrad 2, die beiden andern Trägheitsgrad 1 besitzen, d.h. $(p) = P_1P_2P_3$, $\|P_1\| = \|P_2\| = p$, $\|P_3\| = p^2$. Entsprechend soll dann $(1, 1, 1^2)$ die Zerlegung $(p) = P_1P_2P_3^2$ symbolisieren usw.

Eine GHB für $Q(\sqrt[4]{m})$ ist erstmals von Ljunggren (1936) angegeben worden, allerdings ohne Beweis. Auf einem anderen Weg als dem hier beschriebenen hat Funakura (1984) eine GHB für $Q(\sqrt[4]{m})$ errechnet. Die Parität der Klassenzahlen von K_1, K_2 und L hat Parry (1975a) bestimmt; die in seinem Beweis verwendeten Zerlegungen des Ideals (2) in den Zwischenkörpern von L/Q sind in den beiden Fällen $m \equiv 1 \bmod 8$ und $\frac{m}{4} \equiv -1 \bmod 8$ nicht richtig, weil diese - wie ein Vergleich mit unserer Tabelle zeigt - von den Restklassen mod 16 abhängen. Man kann sich aber leicht davon überzeugen, daß dieser Fehler Parry's Resultate nicht beeinflußt; diese lauten:

1. Sei $K = \mathbb{Q}(\sqrt[4]{m})$, $m \in \mathbb{N}$; dann ist h(K) genau dann ungerade, wenn m die folgende Gestalt hat:
   $m = 2, 2p^2$ $(p \equiv 3 \bmod 8)$, $m = p$ $(p \equiv \pm 3 \bmod 8)$, $m = 4p$ $(p \equiv \pm 3,7 \bmod 8)$, $m = 2p$ $(p \equiv 3 \bmod 8)$, $m = 8p$ $(p \equiv 3 \bmod 8)$;

2. Sei $K = \mathbb{Q}(\sqrt[4]{-m})$, $m \in \mathbb{N}$; dann ist h(K) genau dann ungerade, wenn m die folgende Gestalt hat:
   $m = 2$, p $(p \equiv 3 \bmod 8)$, $m = 4p$ $(p \equiv 3 \bmod 4)$

3. Sei $L = \mathbb{Q}(i, \sqrt[4]{m})$; dann ist h(L) genau dann ungerade, wenn m die folgende Gestalt hat:
   $m = 2$, p $(p \equiv 3 \bmod 8)$, $m = 4p$ $(p \equiv 3 \bmod 4)$;

hierbei bedeutet p immer eine rationale, positive Primzahl.

Berücksichtigt man diese Ergebnisse von Parry, so folgt aus Theorem B von Cioffari (1979): ist m kein Quadrat und $K = \mathbb{Q}(\sqrt[4]{-m})$ normeuklidisch, so ist $m \in \{2, 3, 7, 12, 44, 67\}$. Wir werden hier zeigen, daß genau die $\mathbb{Q}(\sqrt[4]{-m})$ mit $m = 2, 3, 7, 12$ normeuklidisch sind; dabei werden wir einen etwas anderen Weg einschlagen als Cioffari; dies wird es uns erlauben, auf das tiefliegende Ergebnis von Stark (nämlich die Bestimmung aller imaginärquadratischen Zahlkörper mit Klassenzahl 1) zu verzichten.

Der zweite Teil von Cioffaris Arbeit enthält nocheinmal zwei kleinere Druckfehler:

1. In Prop. 14 muß das erste K durch k ersetzt werden;
2. In der Bemerkung zu Prop. 16 schreibt Cioffari: "Cassels proved that K cannot be Euclidean if $D_{K/\mathbb{Q}} > 5300^2$; hence $\mathbb{Q}(\sqrt[4]{-163})$ and $\mathbb{Q}(\sqrt[4]{652})$ are not Euclidean."
   Dabei sollte es selbstverständlich $\mathbb{Q}(\sqrt[4]{-652})$ heißen. Zweitens hat van der Linden 1983 bemerkt, daß sich Cassels in seiner Arbeit verrechnet hat und die richtige Schranke $D_{K/\mathbb{Q}} > 15170^2$ lautet. Dies führt dazu, daß sich $\mathbb{Q}(\sqrt[4]{-163})$ mit Hilfe der Schranke von Cassels nicht mehr ausschließen läßt.

Im folgenden werden wir Körper der Form $K = \mathbb{Q}(\sqrt[k]{-m})$, $k = 2^l$, $l \geq 1$ betrachten; hier haben wir

(5.1) Sei $m \in \mathbb{Z}$ und $\pm m$ kein Quadrat; mit $K = \mathbb{Q}(\sqrt[k]{m})$ und $L = \mathbb{Q}(\sqrt[2k]{m})$ für ein $k \in \mathbb{N}$ gilt dann $h(K) | h(L)$.

Bevor wir (5.1) beweisen, erinnern wir an einige Tatsachen aus der Klassenkörpertheorie: ist K ein algebraischer Zahlkörper mit Klassenzahl h (im weiteren Sinne), dann existiert ein über K abelscher Körper L mit den Eigenschaften

(CF-1) L/K ist an allen Primstellen (einschließlich der unendlichen) unverzweigt;

(CF-2) Die Galoisgruppe Gal(L/K) ist isomorph zur Idealklassengruppe Cl(K); insbesondere ist (L:K) = h = |Cl(K)|.

L ist durch K eindeutig bestimmt, heißt der Hilbertklassenkörper von K und wird mit CF(K) bezeichnet. Ist umgekehrt L/K abelsch und überall unverzweigt, so gilt (L:K)|h(K).

Bew. von 5.1.: Wegen der Inklusion $K \subset L \cap CF(K) \subset L$ und (L:K)=2 ist entweder $K = L \cap CF(K)$ oder $L \subset CF(K)$; in letzterem Falle wäre aber L/K unverzweigt, und dies ist nicht der Fall: denn da m kein Quadrat ist, gibt es eine rationale Primzahl p, die in m ungerade oft aufgeht. Diese ist dann in L/Q und insbesondere auch in L/K rein verzweigt.
Also ist $L \cap CF(K) = K$, somit $L \cdot CF(K)/L$ eine abelsche, unverzweigte Erweiterung vom Grade $(L \cdot CF(K):L) = (CF(K):L \cap CF(K)) = (CF(K):K) = h(K)$, und dies zeigt h(K)|h(L).

Im Falle k=2 stammt diese Aussage wohl von Chevalley (1931). Sei nun $m=qs^2$ für ein quadratfreies q>1: mit $L = Q(\sqrt[k]{-m})$, $k = 2^l$, ist $K = Q(\sqrt{-q})$ der quadratische Teilkörper von L. Soll L euklidisch sein, muß h(K)=1 sein wegen (5.1), und bekanntlich ist dies höchstens dann der Fall, wenn q=2 oder $q \equiv 3 \bmod 4$ prim ist. Ist aber $q \geq 19$ und h(K)=1, so müssen die Ideale (2) und (3) beim Übergang K/Q prim bleiben, weil es in K keine ganzen Zahlen der Norm 2 oder 3 geben kann. Nach dem Zerlegungsgesetz in quadratischen Zahlkörpern ist somit (-q/2) = (-q/3) = -1, nach dem QRG also (2/q) = (3/q) = -1. Weil (q) in L/Q rein verzweigt, können wir (1.6) anwenden mit f=q, a=6, b=q-6 und behaupten, daß a=6 ein 2^l-ter Potenzrest mod q ist. Wegen $q \equiv 3 \bmod 4$ und (a/q) = (2/q)(3/q) = +1 ist dies aber der Fall (es genügt ja, daß a quadratischer Rest mod q ist). Jetzt müssen wir nur noch zeigen, daß a und -b keine Normen aus S sind. Wegen $K \subset L$ und der Normschachtelungsformel brauchen wir dazu nur festzustellen, daß a und -b keine Normen aus D(-q) sind, und dies ist klar.

Nun gilt

(5.2) Sei $L = Q(\sqrt[k]{-m})$ mit $k = 2^l$, $l \geq 1$ und $m = qs^2$ für ein quadratfreies $q \in \mathbb{N}$, q>1. Dann ist L höchstens dann normeuklidisch, wenn $q \in \{2, 3, 7, 11\}$ ist. Ist sogar $k \geq 4$, so muß im Falle q = 11 auch $s \equiv \pm 2 \bmod 5$ gelten.

Zu beweisen ist nur noch die Aussage über q=11 für $k \geq 4$. Dazu setzen wir f=11, a=5, b=6 in (1.6); wegen $(\frac{5}{11}) = +1$ und $11 \equiv 3 \bmod 4$ ist 5 ein 2^l -ter Potenzrest mod 11. Ist dann $s \equiv \pm 1 \bmod 5$, dann gilt $(\frac{-m}{5})_4 = (\frac{-11}{5})_4 (\frac{s}{q}) = -1$, und nach dem Zerlegungsgesetz in $K = \mathbb{Q}(\sqrt[4]{-m})$ gibt es in K (und damit erst recht in L) keine Ideale der Norm 5. Weil L totalkomplex ist, ist auch -b = -6 keine Norm aus L und folglich L nicht normeuklidisch.

Aus (5.2) und den Ergebnissen von Parry folgt nun, daß $L = \mathbb{Q}(\sqrt[4]{-m})$ höchstens für $m \in \{2, 3, 7, 12, 44\}$ normeuklidisch sein kann. Tatsächlich gilt

(5.3) Sei $L = \mathbb{Q}(\sqrt[4]{-m})$, $m \in \mathbb{N}$ kein Quadrat und frei von 4. Potenzen; dann ist K genau für $m = 2, 3, 7, 12$ normeuklidisch.

Den Beweis, daß diese Körper normeuklidisch sind, erbringt man wie in den §§ 2, 3, 4 mit einem Computer (sh. § 11); für m=3 hat schon Lakein (1972) den EA nachgewiesen, für m = 2, 7 hat dies Cioffari (1979) getan. Es bleibt noch zu zeigen, daß $L = \mathbb{Q}(\sqrt[4]{-44})$ nicht normeuklidisch ist. Dazu verwenden wir (1.4) mit $K = \mathbb{Q}\sqrt{-11}$, B = (2) und $e = (1-\sqrt{-11})/2$ (wegen $\Phi_K(2) = 3$ sind in K alle Zahlen quadratische Reste mod 2). Um $M(L) \geq \frac{5}{4}$ zu zeigen, müssen wir die Elemente $r \in D(-11)$ betrachten, die $r \equiv e \bmod 2$ und $N_{K/\mathbb{Q}}(r) < \|B\| \, 5/4 = 5$ erfüllen. Das einzige solche r ist aber r = e, und es genügt zu zeigen, daß e keine Norm aus O_L ist. Bezeichnet [/] das quadratische Restsymbol in D(-11), so folgt dies sofort aus $[\sqrt{-44}/e] = [2\sqrt{-11}/e] = [-1/e] = (-1/3) = -1$ und dem Zerlegungsgesetz in relativquadratischen Zahlkörpern.

Man kann dies aber auch aus dem Zerlegungsgesetz in L folgern: es gilt nämlich $(3) = 3_1 3_2 3_3$ mit $\|3_1\| = \|3_2\| = 3$, $\|3_3\| = 9$; also bleibt genau eines der beiden Ideale $P_1 = (1+\sqrt{-11})/2$ und $P_2 = (e)$ beim Übergang nach L prim, und zwar ist dies P_2 wegen $P_1 O_L = 3_1 3_2$ für $3_1 = (3 - \sqrt[4]{-44} + \sqrt{-11})/2$ und $3_2 = (3 + \sqrt[4]{-44} + \sqrt{-11})/2$. Mit (1.4) folgt nun $M(L) \geq \frac{5}{4}$, und (5.3) ist bewiesen.

Jetzt wenden wir uns den Körpern $\mathbb{Q}(\sqrt[k]{m})$ mit $k=2^l$, $l \geq 1$, $m \in \mathbb{N}$ zu. Die einzigen bekannten Ergebnisse für $l \geq 2$, die den EA in diesen Körpern betreffen, stammen meines Wissens von Egami (1979), der unter Verwendung der Ergebnisse von Parry und tiefliegender Abschätzungen von Charaktersummen gezeigt hat:

die Anzahl der normeuklidischen Zahlkörper der Form $\mathbb{Q}(\sqrt[4]{m})$, wo m frei von 4. Potenzen und $m \neq 2p^2$ für prime $p \equiv 3 \bmod 8$ ist, ist endlich.

Wir werden nun zeigen, daß wir uns unter Beschränkung auf rein elementare Methoden erstens von der Einschränkung $m \neq 2p^2$ frei machen können, und daß wir zweitens diese endliche Liste von Körpern $\mathbb{Q}(\sqrt[4]{m})$, die möglicherweise normeuklidisch sind, sogar explizit angeben können.

(5.4) Sei $L = \mathbb{Q}(\sqrt[k]{2^m p})$ für $k=2^l$, $l \geq 1$, $m \equiv 1 \bmod 2$ und $p \equiv 3 \bmod 4$ prim. Dann ist L höchstens für $p=3$ normeuklidisch.

Bew.: Für $l=1$ wissen wir dies bereits aus § 3. Sei also $l \geq 2$; nach Parry dürfen wir dann $p \equiv 3 \bmod 8$, $p \geq 11$ annehmen. Nach (3.2) gibt es dann $a,b \in \mathbb{N}$ mit $2p=a+b$, $a \equiv 5 \bmod 8$ und $(\frac{a}{p}) = +1$. Wegen $p \equiv 3 \bmod 4$ und $a \equiv 1 \bmod 2$ ist a damit 2^l-ter Potenzrest mod 2p, sodaß wir (1.6) mit $f=2p$ anwenden können (denn die Ideale (2) und (p) sind in $L/\mathbb{Q}$ rein verzweigt). Mit $K=\mathbb{Q}(\sqrt{2p})$ sind aber a und $-b$ keine Normen aus O_K, wegen $K \subset L$ also erst recht keine Normen aus O_L. Also ist L dann nicht normeuklidisch.

Für $k=4$ bleiben also noch $L=\mathbb{Q}(\sqrt[4]{6})$ und $L=\mathbb{Q}(\sqrt[4]{24})$ zu untersuchen; beide Körper sind jedoch nicht normeuklidisch: dazu müssen wir nur zeigen, daß $M(L,I) = 9/8$ für das Ideal der Norm 8 für beide Körper L gilt. Ist aber $\alpha \equiv 1+\sqrt{6} \bmod I$ in O_L, so folgt schnell, daß $N_{L/K}(\alpha) \equiv 7+2\sqrt{6} \equiv 3 \bmod 4+2\sqrt{6}$ und $N_{L/\mathbb{Q}}(\alpha) \equiv 1 \bmod 8$ gilt, wobei $K = \mathbb{Q}(\sqrt{6})$ der quadratische Teilkörper von L ist. Die Kongruenz in O_K zeigt, daß α keine Einheit ist (denn die FE von O_K ist $= 5+2\sqrt{6} \equiv 1 \bmod 4+2\sqrt{6}$). Da (7) in K prim bleibt, ist also $|N_{L/\mathbb{Q}}(\alpha)| \geq 9$, und wegen $|N_{L/\mathbb{Q}}(3+\sqrt{6})| = 9$ folgt in der Tat $M(L,I) = 9/8$.

(5.5) Sei $L = \mathbb{Q}(\sqrt[k]{2^m p})$, $k=2^l$, $l \geq 2$, $m \equiv 0 \bmod 2$, $p \equiv 3 \bmod 8$ prim. Dann ist L höchstens für $p \leq 19$ normeuklidisch.

Bew.: Sei $p \geq 43$; nach (3.4) gibt es $a,b \in \mathbb{N}$ mit $p=a+b$, $a \equiv 2 \bmod 8$ und $(a/p) = +1$. Wegen $p \equiv 3 \bmod 4$ ist a damit k-ter Potenzrest mod p. Aus dem Beweis von (3.5) folgt, daß weder a noch $-b$ Normen aus O_K für $K = \mathbb{Q}(\sqrt{p})$ sind. Wegen $K \subset L$ ist daher L nicht normeuklidisch.

Im Falle $p=19$, $m \equiv 0 \bmod 4$, setzen wir $a=5$, $b=14$; dann ist $5 \equiv 3^4 \bmod 19$, und $(\frac{19}{5})_4 = -1$ zeigt, daß es in $\mathbb{Q}(\sqrt[4]{p})$ keine Ideale der Norm 5 gibt. Wegen $(\frac{19}{7}) = -1$ ist 14 nicht einmal Norm aus $\mathbb{Q}(\sqrt{19})$, und mit (1.6) folgt, daß L auch für $p=19$ nicht normeuklidisch sein kann. Man sieht nun leicht ein, daß auch $\mathbb{Q}(\sqrt[4]{11})$ nicht normeuklidisch ist: da es in $D(11)$ und damit erst recht in O_L keine Ideale der Norm 3 gibt, genügt es zu zeigen, daß die Grundeinheiten von L beide $\equiv 1 \bmod (3+\sqrt{11})$ sind, da das Ideal $I = (3+\sqrt{11})$ wegen $\Phi(I) = 2$ dann nicht euklidisch ist. Nun sind aber $u_1 = 10+3\sqrt{11}$ und $u_2 = 881+477\vartheta+264\vartheta^2+147\vartheta^3$ unabhängig, keine Quadrate und beide $\equiv 1 \bmod I$, sodaß die Behauptung folgt.

Ob $\mathbb{Q}(\sqrt[4]{3})$ normeuklidisch ist oder nicht, läßt sich wohl nicht so einfach entscheiden. Jedenfalls ist $M(L) \geq \frac{11}{12}$, wie man durch Betrachten des Ideals I der Norm 12 leicht feststellt.

Die Fälle $m \equiv 2 \bmod 4$, $p=11$ und $p=19$, lassen sich für $k \geq 4$ leicht entscheiden: man benutze einfach (1.6) mit $f = 11$, $a=5$, $b=6$ bzw. $f = 38$, $a=17$, $b=21$ und beachte $(\frac{44}{5})_4 = -1$, $(\frac{11}{3}) = -1$ resp. $(\frac{76}{17})_4 = -1$, $(\frac{19}{7}) = -1$.

(5.6) Sei $L = \mathbb{Q}(\sqrt[k]{p})$, $k=2^l$, $l \geq 2$, $p \equiv 5 \bmod 8$ prim. Dann ist L höchstens für die Werte $p = 5, 13, 37, 61$ normeuklidisch.

Bew.: Aus den Arbeiten von Behrbohm u. Redei (1936; ah. auch § 3) und Brauer (1940) folgt, daß für prime $p \equiv 5 \bmod 8$, $p > 109$, eine Darstellung $P = rs+tu$ existiert mit $r,s,t,u \in \mathbb{N}$, $(r,s) = (t,u) = 1$ und $(\frac{r}{p}) = (\frac{s}{p}) = (\frac{t}{p}) = -1$ (sh. 3.12.). Da -1 biquadratischer Nichtrest mod p ist, ist entweder rs oder tu biquadratischer Rest mod p (beachte $rs \equiv -tu \bmod p$). Sei also oBdA rs biquadratischer Rest mod p. Da weder $a=rs$, noch $-b=-tu$ Normen aus $\mathbb{Q}(\sqrt{p})$ sind, ist L nach (1.6) nicht normeuklidisch.

$p=29$: hier ist $24 \equiv 4^4 \bmod p$, $29 = 24 + 5$. Da (3) in $\mathbb{Q}(\sqrt{29})$ prim bleibt, ist 24 sicher keine Norm aus O_L. Weiter ist 5 keine Idealnorm wegen $(\frac{29}{5})_4 = -1$;

$p=53$: $53 = 15 + 38$, $8^4 \equiv 15 \bmod 53$;

$p=109$: $109 = 104 + 5$, $(\frac{104}{109})_4 = (\frac{-5}{109})_4) = +1$;

Im Falle $l=2$ können wir auch $p=37$ ausschließen: dazu beachten wir, daß das Ideal $I = (5-\sqrt{37})/2$ der Norm 3 in L prim bleibt wegen $[\sqrt{37}/I] = [5/I] = (\frac{5}{3}) = -1$. Dann setzen wir $B = (2)$, $e = (5-\sqrt{37})/2$, $k = \frac{7}{4}$ in (1.4) und betrachten alle $r \in O_K$, $K=\mathbb{Q}(\sqrt{37})$, mit $r \equiv e \bmod 2$ und $|N_{K/\mathbb{Q}}(r)| < 7$. Da $u = 6+\sqrt{37}$ die FE von K ist und $u \equiv 1 \bmod 2$ gilt, ist sicher $|N_{K/\mathbb{Q}}(r)| \in \{3, 5\}$, und weil (5) in K prim ist, muß sogar $|N_{K/\mathbb{Q}}(r)| = 3$ sein. Also ist $r = u^n e$ oder $r = u^n e'$ für $e' = (5+\sqrt{37})/2$. Letzteres widerspricht der Kongruenz $r \equiv e \bmod 2$, während die Möglichkeit $(r) = (e)$ daran scheitert, daß I in L prim bleibt.

(5.7) Sei $L = \mathbb{Q}(\sqrt[k]{2^m p})$, $k=2^l$, $m \equiv 0 \bmod 2$, $p \equiv 5 \bmod 8$ prim. Dann ist L höchstens für $p = 5, 13, 29, 37, 61, 109$ normeuklidisch.

Bew.: wie (5.6).

Im Falle $k=4$ lassen sich die Körper $\mathbb{Q}(\sqrt[4]{4 \cdot 37})$ und $\mathbb{Q}(\sqrt[4]{4 \cdot 61})$ leicht ausschließen: im ersten Fall benutzt man den Zwischen- körper $K = \mathbb{Q}(\sqrt{37})$ und schließt genau wie oben im Falle $\mathbb{Q}(\sqrt[4]{37})$. Verwendung von (1.6) mit $f=61$, $a=56$ und $b=5$ erledigt den zweiten Fall.

Schließlich müssen wir noch den Fall behandeln, wo keine rationale Prinzahl außer $p=2$ in $L/\mathbb{Q}$ rein verzweigt, in dem sich also das Kriterium (1.6) nicht anwenden läßt. Überraschend einfach sieht man jedoch

(5.8) Sei $L = Q(\sqrt[4]{2p})$, $p \equiv 3 \bmod 8$ prim. Dann ist L nicht normeuklidisch.

Bew.: L hat zwei Fundamentaleinheiten, nämlich $u=1+\sqrt{2}$ und v; wir zeigen, daß $v \equiv 1 \bmod \sqrt{2}$ ist, und wegen $\Phi_L(I) = 2$ und $\|I\| = 4$ ist das Ideal $I = (\sqrt{2})$ nicht euklidisch (da es keine Elemente der Norm 3 gibt).
Da das Ideal (p) in L/K verzweigt, gibt es ein $\pi \in O_L$ mit $p = \pm \pi^2 u^m v^n$. Wäre $n \equiv 0 \bmod 2$, so folgte $\sqrt{\pm p} \in L$ oder $\sqrt{\pm up} \in L$, was aber nicht der Fall ist. Nun ist aber $p \equiv 1 \bmod 2$ und $u \equiv 1 \bmod \sqrt{2}$, sodaß sich $v^n \equiv 1 \bmod \sqrt{2}$ ergibt. Wegen $\Phi_L(I) = 2$ ist $v^2 \equiv 1 \bmod I$, und jetzt folgt sofort $v \equiv 1 \bmod I$.

Zusammenfassend können wir nun feststellen, daß $L = Q(\sqrt[4]{m})$ höchstens für die Werte m = 2, 3, 5, 12, 13, 20, 28, 37, 52, 61, 116, 436 normeuklidisch ist. Es ist anzunehmen, daß sich hierunter noch einige nicht normeuklidische Körper befinden. Weiter kann man mit Hilfe eines Computers bestätigen, daß die beiden Körper $Q(\sqrt[4]{2})$ und $Q(\sqrt[4]{5})$ normeuklidisch sind.

436: h=3

Anmerkungen zu § 5

1936 Ljunggren gibt Ganzheitsbasen und untersucht Einheiten rein biquadratischer Zahlkörper

1975 Parry gibt alle rein biquadratischen Zahlkörper mit ungerader Klassenzahl

1979 Egami zeigt, daß es nur endlich viele normeuklidische Körper der Form $Q(\sqrt[4]{m})$ gibt, falls nicht $m = 2p^2$, $p \equiv 3 \bmod 8$ prim ist. Der Fall $m = 2p^2$ bleibt unerledigt.
Cioffari zeigt $m \in \{2, 3, 7, 12, 44, 67\}$ oder $m = 2p^2$ für normeuklidische Körper $Q(\sqrt[4]{-m})$. Der Fall $m = 2p^2$ läßt sich aber mit den Ergebnissen von Parry (die Cioffari offenbar nicht bekannt waren) erledigen.

1980 Parry entwickelt eine Geschlechtertheorie für rein biquadratische Körper

1984 Funakura gibt eine GHB für rein biquadratische Körper

1987 Buchmann berechnet eine Grundeinheit von Ringen der Form $\mathbb{Z}[\sqrt[4]{-m}]$