EUKLIDISCHE RINGE

Diplomarbeit
von
Franz Lemmermeyer *betreut von Fr. Prof. S. Böge*

Universität Heidelberg
Fakultät für Mathematik
August 1989

EUKLIDISCHE RINGE

Überblick:

Zum besseren Verständnis der Arbeit sei im folgenden kurz beschrieben, was einen in den nächsten Paragraphen erwartet: Ausgangspunkt aller Überlegungen war das Kriterium (1.15) von Lenstra (1974, 1975, 1977), wonach ein Zahlkörper mit einer hinreichend langen "Ausnahmefolge " normeuklidisch ist. Etwa zur gleichen Zeit (nämlich in den Jahren 1975 bis 1977) hat Cooke den Begriff eines k-stufig normeuklidischen Zahlkörpers eingeführt. Dies legte die Frage nahe, ob sich das Lenstra-Kriterium so modifizieren läßt, daß man damit auch k-stufig normeuklidische Ringe finden kann. Tatsächlich gelingt dies recht einfach (sh. (1.16)). Das hierzu notwendige Studium von Kettenbrüchen der Länge $\leq k$ mit Koeffizienten aus dem betrachteten Ring führt auf Mengen, die denen ähneln, die Motzkin (1949) eingeführt hat, und die wir im § 0 vorstellen.

Damit hat man nun ein Kriterium, mit dem man (beispielsweise) 2-stufig normeuklidische Zahlkörper vom Grad 2, 3, 4, 5, usw. finden kann, und dies wirft die Frage auf, ob diese Körper nicht vielleicht schon (1-stufig) normeuklidisch sind. Das allgemeinste Kriterium, mit dessen Hilfe man zeigen konnte, daß ein gegebener Zahlring nicht normeuklidisch ist, war (1.6); den Nachteil dieses Kriteriums beschreibt van der Linden (1985) so: "If we generalize the methods for higher degree number fields it turns out that the arithmetical methods are applicable for extensions of $\mathbb{Q}$ in which at least one prime is totally ramified...". Eine genaue Analyse des Beweises von (1.6) zeigt jedoch, daß sich dieses Kriterium zumindest etwas verallgemeinern läßt (sh. (1.4)), dieweil es nämlich manchmal genügt, daß $K/\mathbb{Q}$ einen Zwischenkörper k enthält, sodaß es in K/k rein verzweigte Ideale gibt. Daß diese Verallgemeinerung tatsächlich von Nutzen ist, zeigt sich u.A. in § 6, wo wir alle normeuklidischen Zahlkörper der Form $\mathbb{Q}(\sqrt{m},\sqrt{n})$ mit $m,n \in \mathbb{Z}$, $m < 0$ finden. Weiter kann man mit (1.4) ggf. nicht nur die Existenz eines EA ausschließen, sondern sogar Abschätzungen für das euklidische Minimum von K geben.

Ein (von van der Linden mit dem Attribut "geometrisch" belegtes) Kriterium, einen reellquadratischen Zahlkörper als nicht normeuklidisch nachzuweisen, ist (1.8). In der hier vorgestellten Form stammt es von Barnes und Swinnerton-Dyer (1952), jedoch läßt es sich mehr oder weniger explizit bereits bei Redei (1941) und Inkeri (1950) finden. Zaghafte Verallgemeinerungen auf den kubischen Fall mit Einheitenrang 1 findet man bei Taylor (1976) und bei Cioffari (1979); van der Linden schreibt hierzu (in Fortsetzung von oben): "... and the geometrical methods apply for fields with $* S_\infty \leq 2$" (damit sind Zahlkörper mit Einheitenrang 1 gemeint). In der Tat läßt sich (1.8) jedoch ganz einfach auf beliebige Zahlkörper mit unendlicher Einheitengruppe verallgemeinern (sh. (1.12)); es ist bemerkenswert, daß die dabei benutzten Ungleichungen (wie z.B. (1.9), oder die entsprechende kubische in § 4) von Cassels benutzt wurden, um die Schranken für $|\mathrm{disc}\, K|$ zu verbessern, oberhalb derer

es keine quadratischen (r=2, s=0), kubischen (r=1, s=1) und biquadratischen (r=0, s =2) Körpern mit Euklidischem Algorithmus mehr gibt. Dies ist eigentlich ein mehr als deutlicher Hinweis darauf, daß sich auch das Casselsche Ergebnis auf Zahlkörper beliebigen Grades verallgemeinern läßt. Ein erster Schritt in diese Richtung wäre eine Verallgemeinerung von (2.12).

In § 2 beschreiben wir eine Methode zur Bestimmung euklidischer Minima; diese geht im wesentlichen auf Barnes und Swinnerton-Dyer zurück (1952; wichtige Beiträge hierzu wurden aber u.a. von Cassels und Inkeri geliefert). Die in § 2 gegebenen Beweise dieser Theoreme erscheinen mir wesentlich klarer und durchsichtiger als die originalen.

In §3 geben wir (fast) eine Klassifikation aller normeuklidischen reellquadratischen Zahlkörper mittels (1.4) und (1. 8); Vorbild sind die klassischen Beweise von Behrbohm, Redei, Erdös & Ko usw. Die hier erzielten Ergebnisse verwenden wir auch in § 5.

In § 4 untersuchen wir kubische Körper; zur Auffindung aller normeuklidischen Körper der Form $Q(\sqrt[3]{m})$ folgen wir der Arbeit Cioffaris (1979). Dann bestimmen wir die euklidischen Minima kubischer Körper mit kleiner Diskriminante, und schließlich verbessern wir eine von Smith (1976) erhaltene Schranke, wonach es keine kubischen zyklischen Körper mit Diskriminante d, $157^2 \le d \le 10^8$ gibt, indem wir dieses Ergebnis auf alle solchen Körper mit $157^2 \le d \le 2.5 \cdot 10^{11}$ ausweiten.

In § 5 zeigen wir, daß es nur endlich viele normeuklidische Zahlkörper der Form $Q(\sqrt[4]{m})$ gibt, und für $m<0$ bestimmen wir sie alle. Damit werden die diesbezüglichen Untersuchungen von Cioffari (1979) und Egami (1984) abgeschlossen.

In § 6 bestimmen wir, wie schon erwähnt, alle imaginären, bizyklischen biquadratischen Zahlkörper. Nachdem van der Linden 1983 alle zyklischen imaginären Zahlkörper 4. Grades gefunden hat (es gibt nur zwei: $Q(\zeta_5)$ und den Teilkörper 4. Grades von $Q(\zeta_{13})$), sind jetzt alle galoischen imaginären Körper 4. Grades mit EA bekannt. Es scheint, als ob das nächstschwierigere Problem die Körper sind, deren normaler Abschluß die Diedergruppe als Galoisgruppe besitzt.

In § 7 beschäftigen wir uns mit der Klassifikation der normeuklidischen Dirichletschen Zahlkörper. Wir werden dabei alle solchen finden, wenn die Relativdiskriminante durch $(1+i)$ teilbar ist. Die vollständige Lösung dieses Problems scheint nur noch eine Frage der (Rechen-) Zeit zu sein.

In § 8 machen wir einige Andeutungen, wie man die restlichen imaginären Zahlkörper 4. Grades behandeln kann, und in § 9 geben wir einen Ausblick auf die Untersuchungen von Körpern höheren Grades.

Nach dem bisher Gesagten ist es nicht verwunderlich, daß auch viele Fragen offen bleiben mußten. Einige dieser Probleme sollten sich mit den hier vorgestellten Methoden lösen lassen ("je n'ai pas le temps"), andere scheinen tiefer zu liegen. Jedenfalls sind in § 10 einige dieser Frage aufgelistet.

§ 11 schließlich enthält die Beschreibung eines Algorithmus, mit dem man den EA in einem gegebenen Zahlkörper nachweisen oder widerlegen kann (die Frage, ob dieser Algorithmus immer terminiert, also eine Antwort liefert, hängt eng mit gewissen - noch nicht bewiesenen - Vermutungen von Barnes und Swinnerton-Dyer, sowie von Lenstra zusammen (sh. dazu Lenstra 1979).

An dieser Stelle sei noch eine Liste der Körper angegeben, von denen bisher nicht bekannt war, ob sie normeuklidisch sind oder nicht:

n=3, r=3, s=0: disc K= 2021, 2024, 2057, 2101, 2213;

n=4, r=0, s=2: $Q(\sqrt{-2}, \sqrt{5})$, $Q(\sqrt{-3}, \sqrt{17})$, $Q(\sqrt{-3}, \sqrt{-19})$, $Q(\sqrt{-7}, \sqrt{5})$,
$Q(\sqrt{5+2i})$, $Q(\sqrt{1+6i})$, $Q(\sqrt{7+2i})$, $Q(\sqrt{7+4i})$, $Q(\sqrt{1+8i})$,
$Q(\sqrt{3+8i})$, $Q(\sqrt{5+8i})$, $Q(\sqrt{9+4i})$, $Q(\sqrt{7+8i})$, $Q(\sqrt{11+4i})$, $Q(\sqrt[4]{12})$;

n=4, r=2, s=1: $Q(\sqrt[4]{2})$, $Q(\sqrt[4]{5})$;

n=4, r=4, s=0: $Q(\sqrt{3}, \sqrt{5})$, $Q(\sqrt{3}, \sqrt{7})$, $Q(\sqrt{5}, \sqrt{13})$, $Q(\sqrt{5}, \sqrt{17})$.

Zweifellos lassen sich mit den vorgestellten Methoden noch viele weitere normeuklidische Zahlkörper 3. und 4. (oder auch höheren) Grades finden.

Weiter sind mir neben den 14 von Cooke gefundenen reellquadratischen, 2-stufig normeuklidischen Körpern noch die folgenden bekannt:

$Q(\sqrt{m})$ für m = 47, 59, 62, 67, 71, 109, 149, 157, 161, 173, 193, 201, 213,
sowie die kubischen Körper mit Diskriminante d = - 199, -351.

NOTATION

$\mathbb{N}$	die natürlichen Zahlen
$\mathbb{Z}$	die ganzen, rationalen Zahlen
$\mathbb{Q}$	die rationalen Zahlen
$\mathbb{R}$	die reellen Zahlen
$\mathbb{C}$	die komplexen Zahlen
$\mathbb{F}_q$	der endliche Körper mit q Elementen
K	ein algebraischer Zahlkörper
R	ein nullteilerfreier, kommutativer Ring mit 1
O_K	der Ring ganzer Zahlen in K
Φ_K	die Eulersche Phi-Funktion in K
$\|I\|$	die Absolutnorm eines Ideals I
$T_{K/\mathbb{Q}}(\alpha)$	die Spur eines Elements $\alpha \in K$
$N_{K/\mathbb{Q}}(\alpha)$	die Norm eines Elements $\alpha \in K$
disc K	die Diskriminante einer Körpererweiterung
diff K	die Differente einer Körpererweiterung
(K:Q)	der Grad einer Körpererweiterung
Gal(K/Q)	die Galoisgruppe
Z(P|p)	die Zerlegungsgruppe
T(P|p)	die Trägheitsgruppe
V_i(P|p)	die Verzweigungsgruppen
Cl(K)	die Idealklassengruppe
h(K)=#Cl(K)	die Klassenzahl
$\|\ \|_i$	die normierten Bewertungen von K (sh. S. 29 und 48)
D(m)	der Ring ganzer Zahlen in $\mathbb{Q}(\sqrt{m})$
D(m,n)	der Ring ganzer Zahlen in $\mathbb{Q}(\sqrt{m},\sqrt{n})$
QRG	quadratisches Reziprozitätsgesetz
FE	Fundamentaleinheit
GHB	Ganzheitsbasis
PERS	primes Einheitenrestsystem (S. 36)
E_i	sh. S. 3
E_i'	sh. S. 10
F_i	sh. S. 12
B_i	sh. S. 66
M_1	erstes euklidisches Minimum (sh. S. 2)
M_2,...	zweites euklidisches Minimum, ...(sh. S. 17)
M^1, M^2,...	sh. S. 8
$C_1, C_2, \ldots$	sh. S. 17
$M_{r,s}$	die Minkowski-Schranke (sh. S. 33)
μ_k	die Lenstra-Konstanten (sh. S. 36)
λ_k	sh. S. 36
$\mathcal{M}_K$	die "Generalmensur", sh. S. 38
$\underline{K}$	sh. S. 48

INDEX