universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Normeuklidische Ringe ganzer Zahlen in rein kubischen Zahlkörpern

Verfasser

Timo Wenzl

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag. rer. nat.)

Wien, 2013

Studienkennzahl lt. Studienblatt:	A 405
Studienrichtung lt. Studienblatt:	Diplomstudium Mathematik
Betreuerin / Betreuer:	ao. Univ.-Prof. Dr. Christoph Baxa

Einleitung. Die vorliegende Arbeit beschäftigt sich mit einer Problemstellung der algebraischen Zahlentheorie. Ziel der Arbeit ist es herauszufinden welche, unter allen Ringen ganzalgebraischer Zahlen in einem rein kubischen Zahlkörper, normeuklidisch sind. Es wird sich dabei herausstellen, dass man nur eine endliche Menge von Ringen betrachten muss. Ein sehr hilfreiches Argument dabei ist die Schranke von J.W.S. Cassels, die es erlaubt, die in Frage kommenden Ringe auf endlich viele einzuschränken. Es müssen nur mehr Ringe mit $d(K) < 420^2$ betrachtet werden, was die Suche erheblich einschränkt. Des weiteren können auch nur Ringe mit Klassenzahl 1 normeuklidisch sein. Schließlich bleiben 31 Ringe übrig, die man untersuchen muss. Das alle 31 Ringe auch tatsächlich Klassenzahl 1 haben, wird nur für einen Ring gezeigt und für den Rest aus der Literatur übernommen. Wie sich herausstellen wird, gibt es nur 3 Ringe die tatsächlich normeuklidisch sind, nämlich $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{5})$.
H.J. Godwin hat gezeigt, dass $\mathbb{Q}(\sqrt[3]{2})$ normeuklidisch ist. Die Tatsache, dass $\mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{10})$ normeuklidisch sind wurde von E.M. Taylor bewiesen.

Danksagung

Ich möchte mich an dieser Stelle bei Herrn Professor Baxa für die fachliche Betreuung dieser Arbeit bedanken.

Inhaltsverzeichnis

1. Rein kubische Zahlkörper

In diesem Kapitel folge ich dem Buch von Narciewicz [7].

Definition 1.1
Ein algebraischer Zahlkörper heißt kubisch, wenn $[K : \mathbb{Q}] = 3$.

Definition 1.2
Ein algebraischer Zahlkörper heißt rein kubisch, wenn es ein $n \in \mathbb{N} \setminus \{1\}$ gibt, mit der Eigenschaft, dass $p^3 \nmid n$ für alle Primzahlen p gilt, sodass $K = \mathbb{Q}(\sqrt[3]{n})$

Bemerkung 1.3
Wie in jedem algebraischen Zahlkörper gibt es auch in den rein kubischen Zahlkörpern eine Ganzheitsbasis.
Um diese darstellen und beweisen zu können braucht es aber ein wenig Vorarbeit.

Lemma 1.4
Sei L/K eine endliche Körpererweiterung und $v_1, \ldots, v_n \in L$, dann gilt:

(1) Wenn $i = 1, 2, \ldots, n$ und $u_i = \sum_{j=1}^{n} a_{ij} v_j$ mit $a_{ij} \in K$, dann

$$d_{L/K}(u_1, \ldots, u_n) = (det[a_{ij}])^2 d_{L/K}(v_1, \ldots, v_n).$$

(2) $d_{L/K}(v_1, \ldots, v_n) = 0$ genau dann wenn $v_1, \ldots, v_n$ linear abhängig über K ist.

(3) Falls $L = K(a)$ und $P \in K[x]$ ist das Minimalpolynom von a, dann

$$d_{L/K}(a) = (-1)^m det[c_{ij}] = (-1)^m N_{L/K}(P'(a))$$

mit $m = n(n-1)/2$ und die Elemente c_{ij} sind definiert durch

$$a^j P'(a) = \sum_{i=0}^{n-1} c_{ij} a^i \ (j = 0, 1, \ldots, n-1).$$

Beweis. (1) Ist eine Folgerung der Gleichung

$$det[F_j(u_i)] = det[a_{ij}] det[F_j(u_i)].$$

(2) Die Elemente $v_1,\ldots,v_n$ seien linear abhängig über K, dann gilt für passende $x_1,\ldots,x_n \in K$ (die nicht alle 0 sind),

$$\sum_{i=1}^{n} x_i F_j(v_i) = 0 \ (j = 1,2,\ldots,n)$$

woraus folgt, dass $d_{L/K}(v_1,\ldots,v_n) = 0$
Falls nun $d_{L/K}(v_1,\ldots,v_n)$ verschwinden sollte, dann besitzt das System

$$\sum_{i=1}^{n} x_i Tr_{L/K}(v_i v_j) = 0 \ (j = 1,2,\ldots,n)$$

eine Lösung $\neq 0$. Falls $v_1,\ldots,v_n$ ein linear unabhängiges System ist, ist $u = x_1v_1 + \ldots + x_nv_n$ mit $u \neq 0$ und $Tr_{L/K}(uv_i) = 0$ für $i = 1,2,\ldots,n$.
Daraus folgt, dass $Tr_{L/K}(uy) = 0$ für alle $y \in L$ gilt. Das ist aber nicht möglich, weil $y = 1/u$ gewählt werden kann, woraus man $n = Tr_{L/K}(1) = 0$ erhält.

(3) Es bezeichne $a_1 = a_1, a_2 \ldots a_n$ die Konjugierten von a über K und setze $b_i = P'(a_i)$. Alle diese Elemente liegen im fixen algebraischen Abschluß von L. Dann gilt

$$d_{L/K}(a) = \prod_{i<j}(a_i - a_j)^2 = (-1)^m \prod_{i=1}^{n} \prod_{i\neq j} (a_i - a_j)$$

$$= (-1)^m \prod_{i=1}^{n} P'(a_i) = (-1)^m b_1 \ldots b_n = (-1)^m N_{L/K}(P'(a))$$

Ferner gilt

$$b_1 \ldots b_n det[a_i^j] = det[a_i^j b_i] = det[\sum_{k=1}^{n} c_{kj} a_k^i]$$

$$= det[c_{kj}] det[a_j^k]$$

Nachdem nach (2) $det[a_i^k] \neq 0$ gilt, erhält man

$$b_1 \ldots b_n = det[c_{ij}],$$

und daher gilt

$$d_{L/K}(a) = (-1)^m det[c_{ij}].$$

□

Lemma 1.5
Seien $a_1, \ldots, a_n \in O_K$ linear unabhängig über $\mathbb{Q}$, dann ist

$$d_{K/\mathbb{Q}}(a_1, \ldots, a_n) = m^2 d(K)$$

wobei m der Index in O_K des $\mathbb{Z}$-Moduls M ist, der von den a_i erzeugt wird.

Beweis. Sei $\omega_1, \ldots, \omega_n$ eine Ganzheitsbasis von O_K und seien $b_1, \ldots, b_n \in M$ so gewählt, dass

$$b_i = \sum_{k=1}^{i} c_{ik}\omega_k \ (c_{ik} \in \mathbb{Z},\ i = 1, \ldots, n)$$

wobei c_{ii} positiv und so klein wie möglich ist. Die b_i bilden eine Menge von freien Erzeugern für M, und $\sum_{k=1}^{i} t_k\omega_k$, mit $t_k \in \mathbb{Z}$, liegt nur dann im M, wenn $c_{ii} \mid t_i$.
Das zeigt, dass die Zahlen

$$\sum_{i=1}^{j} a_i\omega_i \ (0 \le a_i < c_{jj}, j = 1, \ldots, n)$$

paarweise nicht kongruent mod M sind, und offensichtlich gibt es $c_{11} \ldots c_{nn}$ von diesen.
Nun muss man zeigen, dass diese Elemente alle Restklassen mod M repräsentieren.
Sei nun

$$\xi = \sum_{k=1}^{n} \lambda_k\omega_k \ (\lambda_k \in \mathbb{Z})$$

ein beliebiges Element von O_K, bezeichnet als μ_n, dem kleisten nichtnegativen Rest von λ_n mod c_{nn}. Nun setzt man $A_n = (\lambda_n - \mu_n)/c_{nn}$, dann ist

$$\xi = A_n b_n + \mu_n\omega_n + \sum_{k=1}^{n-1} (\lambda_k - A_n c_{nk})\omega_k.$$

Falls μ_{n-1} den kleinsten nichtnegative Rest von

$$\lambda_{n-1} - A_n c_{n,n-1} \bmod c_{n-1,n-1}$$

bezeichnet, setzt man

$$A_{n-1} = (\lambda_{n-1} - A_n c_{n,n-1} - \mu_{n-1})/c_{n-1,n-1}.$$

Dadurch ist

$$\xi = A_n b_n + A_{n-1} b_{n-1} + \mu_n \omega_n + \mu_{n-1}\omega_{n-1}$$
$$+ \sum_{k=1}^{n-2} (\lambda_k - A_n c_{n,k} - A_{n-1} c_{n-1,k})\omega_k.$$

Wendet man diese Prozedur fortlaufend an, so erhält man schließlich eine Gleichung der Form

$$\xi = \sum_{k=1}^{n} A_k b_k + \sum_{k=1}^{n} \mu_k \omega_k \ (0 \le \mu_k < c_{k,k}; \mu_k, A_k \in \mathbb{Z})$$

und dadurch ist

$$\xi \equiv \sum_{k=1}^{n} \mu_k \omega_k \pmod{M}$$

Dadurch sieht man, dass

$$d_{K/\mathbb{Q}}(a_1, \ldots, a_n) = d_{K/\mathbb{Q}}(b_1, \ldots, b_n) = (c_{11} \ldots c_{nn})^2 d(K).$$

nach Lemma 1.4(2) gilt. □

Lemma 1.6
Sei a ganzalgebraisch und $K = \mathbb{Q}(a)$ der von a erzeugte Körper. Erfüllt das Minimalpolynom von a über $\mathbb{Q}$ das Eisensteinkriterium bezüglich der Primzahl p, z.B. es hat die Form $X^n + a_{n-1}N^{n-1} + \ldots + a_0$ mit p teilt $a_0, \ldots a_{n-1}$, und $p^2 \nmid a_0$, dann ist der Index von a in K nicht durch p teilbar.

Beweis. Nach Annahme ist a^n/p ganz und überdies teilt p^2 nicht die Norm $N_{K/\mathbb{Q}}(a)$. Wenn p den Index von a teilt, dann existiert eine ganze Zahl $\psi \in R_K$ der Form

$$\psi = (b_0 + b_1 a + \ldots + b_{n-1} a^{n-1})/p \ (b_i \in \mathbb{Z})$$

wo aber nicht jedes b_i durch p teilbar ist. Sei nun j der kleinste Index für den den $p \nmid b_j$ gilt, dann ist die Zahl

$$\eta = (b_j a^j + \ldots + b_{n-1} a^{n-1})/p$$

$$= \psi - (b_0 + b_1 a + \ldots + b_{j-1} a^{j-1})/p$$

ganzalgebraisch und ebenso

$$\zeta = b_j a^{n-1}/p = \eta a^{n-j-1} - a^n (b_{j+1} + b_{j+2} a + \ldots + b_{n-1} a^{n-j-2})/p.$$

Daraus folgt

$$p^n N_{K/\mathbb{Q}}(\zeta) = N_{K/\mathbb{Q}}(p\zeta) = N_{K/\mathbb{Q}}(b_j a^{n-1}) = b_j^n N_{L/\mathbb{Q}}(a)^{n-1}$$

und das bedeutet, dass $p \mid b_j$, was aber ein Widerspruch zur Wahl von j ist. □

Satz 1.7
Sei $K = \mathbb{Q}(\theta)$ mit $\theta = \sqrt[3]{m}$ und $m = ab^2$, wobei ab quadratfrei ist dann unterscheidet man drei Fälle:

(1) Wenn $m \not\equiv \pm 1 \mod 9$, ist $d(K) = -27(ab)^2$ und die Zahlen $1, \theta, \theta^2/b$ bilden eine Ganzheitsbasis.
(2) Wenn $m \equiv 1 \pmod 9$, ist $d(K) = -3(ab)^2$ und die Zahlen $\theta, \theta^2/b, (1+\theta+\theta^2)/3$ bilden eine Ganzheitsbasis.
(3) Wenn $m \equiv -1 \pmod 9$, ist $d(K) = -3(ab)^2$, und die Zahlen $\theta, \theta^2/b, (1-\theta+\theta^2)/3$ bilden eine Ganzheitsbasis.

Beweis. Nach Lemma 1.4(3) erhält man $d_{K/\mathbb{Q}}(\theta) = 3^3 m^2$. Das Minimalpolynom von θ, $x^3 - m$, erfüllt das Eisensteinkriterium für jeden Primteiler von a. Wenn $3 \mid a$, dann erhält man $3^3 a^2 \mid d(K)$ und wenn $3 \nmid a$ dann erhält man $3a^2 \mid d(K)$. Die Zahl $\vartheta = \theta^2/b$ ist eine Wurzel von $x^3 - a^2 b$.Der letzte Audruck erfüllt das Eisensteinkriterium für alle Primzahlen, welche b teilen und daher $b^2 \mid d(K)$. Schließlich erhält man $d(K) = -3^N (ab)^2$, wobei $N = 3$, wenn $3 \mid n$ und ist 1 oder 3, wenn $3 \nmid n$

(1) Falls $m \not\equiv \pm 1 \pmod 9$, dann $m^3 \not\equiv m \pmod 9$ und daher ist $(x+m)^3 - m$ Eisenstein für $p = 3$, und die Diskriminante seiner Wurzel $\theta - m$ gleich $-3^3 m^2$.
Daher folgt aus Lemma 1.6, $d(K) = -3^3 (ab)^2$.

(2) Falls $m \equiv 1 \pmod 9$, ist $\phi = (1+\theta+\theta^2)/3$ ganzalgebraisch, weil sie Wurzel des Polynoms

$$x^3 - x^2 + \frac{1-m}{3}x - \frac{(m+1)^2}{27}$$

ist.Daher ist der Index von θ durch 3 teilbar. Nach Lemma1.5 gilt dann $d(K) = -3(ab)^2$.

(3) Falls $m \equiv -1 \pmod 9$ geht man ähnlich wie im vorigen Fall vor. Man betrachtet hier anstatt ϕ den Ausdruck $(1-\theta+\theta^2)/3$.
Die Ganzheitsbasis kann nun direkt, durch Berechnung der Diskriminante der relevanten Mengen verifiziert werden.

□

2. Cassels Schranke

In diesem Kapitel folge ich der Arbeiten von Cassels [2] und Mahler [6].

Bemerkung 2.1
Die Schranke von Cassels wird sich in späterer Folge als nützliche Bedingung, zur Einschränkung der Kandidaten, welche normeuklidisch sind, herausstellen.

Satz 2.2
Seien L_1, L_2, L_3 lineare Formen mit Determinante $\Delta \neq 0$ in x, y, z, wobei L_1 reell und $L_2 = \overline{L_3}$ ist. Dann existiert ein Punkt (x_0, y_0, z_0), sodass

$$\min_{(x,y,z)\equiv x_0,y_0,z_0 \pmod 1} |L_1, L_2, L_3| \geq \frac{|\Delta|}{420}.$$

Falls die Koeffizienten von L_1, L_2, L_3 einander entsprechende Zahlen in konjugierten kubischen Zahlkörper sind, dann können x_0, y_0, z_0 rational gewählt werden.
Man verwendet jetzt die Identität

$$L_1M_1 + L_2M_2 + L_3M_3 = \Delta(xu + yv + zw),$$

wobei M_1, M_2, M_3 die zu L_1, L_2, L_3 adjungierte Formen in den Variablen u, v, w sind. Daher ist $M_3 = \overline{M_2}, M_1$ ist reell und M_1, M_2, M_3 haben Determinante Δ^2.
Als Nächstes wird gezeigt, dass die adjungierten Darstellung immer $\neq 0$ sind.

Lemma 2.3
Falls $p > 0$, $q > 0$ und $pq^2 \geq |\Delta|^2 3^{-\frac{1}{2}}$, dann existieren ganzzahlige Werte für u, v, w, die nicht alle 0 sind, sodass

$$|M_1| \leq p,\ |M_2| = |M_3| \leq q$$

Bemerkung 2.4
Um das obige Lemma beweisen zu können, braucht es ein wenig Vorarbeit.
Bezeichne x_1, x_2, x_3 rechteckige Koordinaten in einem dreidimensionalen Raum, und K einen konvexen Körper mit Zentrum in $0 = (0, 0, 0)$. Ein Gitter λ,

$$x_h = \sum_{k=1}^{3} \alpha_{hk} u_k,\ (h = 1,2,3; u_1, u_2, u_3 = 0, \pm 1, \pm 2, \ldots),$$

mit Determinante

$$d(\lambda) = ||\alpha_{hk}|_{h,k=1,2,3}|,$$

heißt K-zulässig, falls 0 sein einziger innere Punkt von K ist. Sei $\Delta(K)$ die untere Schranke von $d(\lambda)$ über alle K-zulässigen Gitter, dann ist $\Delta(K) > 0$ und es gibt zumindest ein kritisches Gitter, das bedeutet ein K-zulässiges Gitter λ, sodass $d(\lambda) = \Delta(K)$.
Der Gitterpunktsatz von Minkowski kann wie folgt ausgedrückt werden:

$$\Delta(K) \geq \frac{1}{8} V,$$

wobei V das Volumen von K ist. Im allgemein erscheint das Symbol $>$ in der obigen Ungleichung. Es stellt sich die Frage nach den exakt Werten von $\Delta(K)$. Dieses Problem wurde von Minkowski für Würfel, Oktaeder und Kugel behandelt. Hier wird es für den Zylinder

$$K : x_1^2 + x_2^2 \leq 1,\ -1 \leq x_3 \leq 1.$$

gelöst, indem man zeigt, dass

$$\Delta(K) = \frac{1}{2}\sqrt{3}. \tag{1}$$

Die Tatsache, dass $\Delta(K) \leq \frac{1}{2}\sqrt{3}$, ist relativ klar, weil die folgenden Gitter mit Determinante $\frac{1}{2}\sqrt{3}$ K-zulässig sind:

(1) Die Gitter λ_1, abgleitet von dem speziellen Gitter

$$x_1 = u_1 + \frac{1}{2}u_2 + \alpha u_3,\ x_2 = \frac{1}{2}\sqrt{3}u_2 + \beta u_3,\ x_3 = u_3,\ (\alpha, \beta\ \textit{beliebig}).$$

durch beliebige Rotation um die x_3-Achse.

(2) Die Gitter λ_2, abgeleitet von dem speziellen Gitter

$$x_1 = u_1 + \frac{1}{2}u_2,\ x_2 = \frac{1}{2}\sqrt{3}u_2,\ x_3 = \alpha u_1 + \beta u_2 + u_3,\ (\alpha, \beta\ \textit{beliebig})$$

durch eine beliebige Rotation um die x_3-Achse.

Die Gitter λ_1, λ_2 sind die einzigen kritischen Gitter von K. Um Gleichung (1) zu zeigen, genügt es daher

$$\Delta(K) \geq \frac{1}{2}\sqrt{3}, \tag{2}$$

zu zeigen.
Um das zu beweisen, benötigt man die beiden folgenden Lemmata.

Lemma 2.5
Sei π ein flaches konvexes Polygon mit Fläche A und Winkeln nicht größer als 120^o, und $C_1, C_2, \ldots, C_s$ nicht-überlappende Kreise von Radius r, die in π enthalten sind, dann gilt

$$s \leq \frac{A}{r^2\sqrt{12}}.$$

Beweis. Siehe K. Mahler, B. Segre, *In the densest packing of circles*, Amer. Math. Monthly **51**, (1944), 261-270. □

Lemma 2.6
Sei n eine positive ganze Zahl und sei W der Würfel

$$|x_1| \leq n,\ |x_2| \leq n\ |x_3| \leq n.$$

Seien weiters $Z_1, Z_2, \ldots, Z_t$ nicht-überlappende kreisrunde Zylinder mit Radius $\frac{1}{2}$ und Höhe 1, die alle in W enthalten sind und mit ihren Achsen parallel zu der x_3-Achse liegen. Dann gilt

$$t \leq \frac{16}{\sqrt{3}}n^3$$

Beweis. Bezeichne x eine Zahl im Intervall $-n \leq x \leq n$. Die Fläche $x_3 = x$ schneidet die Zylinder $Z_1, Z_2, \ldots, Z_t$ in einer bestimmten Punktmenge $J(x)$ der Fläche $Q(x)$. Dann entspricht das Intergral $\int_{-n}^{n} Q(x)dx$ dem Gesamtvolumen der Zylinder $Z_1, Z_2, \ldots, Z_t$, und so ist

$$\int_{-n}^{n} Q(x)dx = \frac{1}{4}\pi t. \tag{3}$$

Nun gibt es höchstens $2t$ verschiedene Werte von x, für die die Fläche $x_3 = x$, entweder die Grundfläche oder die Deckfläche eines dieser Zylinder enthält.

Sei nun x keiner dieser Werte, dann besteht $J(x)$ aus einer endlichen Anzahl s von Kreisen mit Radius $\frac{1}{2}$: keine zwei dieser Kreise überlappen einander und alle liegen innerhalb des Quadrats

$$|x_1| \leq n,\ |x_2| \leq n,\ x_3 = x$$

mit Fläche $A = 4n^2$. Daher folgt nach Lemma 2.5

$$s \leq \frac{4n^2}{(\frac{1}{2})^2\sqrt{12}} = \frac{8}{\sqrt{3}}n^2.$$

Dann ist

$$Q(x) = \frac{1}{4}\pi s \leq \frac{2\pi}{\sqrt{3}}n^2,$$

und, nach Gleichung (3) ist

$$\frac{1}{4}\pi t = \int_{-n}^{n} Q(x)dx \leq \int_{-n}^{n} \frac{2\pi}{\sqrt{3}}n^2 dx = \frac{4\pi}{\sqrt{3}}n^3,$$

und daher

$$t \leq \frac{16}{\sqrt{3}}n^3.$$

Um Gleichung (2) zu beweisen, setzt man

$$F(x_1, x_2, x_3) = \max(|\sqrt{x_1^2 + x_2^2}|, |x_3|),$$

sodass der Zylinder K aus allen Punkten, die $F(x_1, x_2, x_3) \leq 1$ erfüllen, besteht. Es bezeichnet λ ein K-zulässiges Gitter. Dann liegt an jedem Punkt $X = (x_1^0, x_2^0, x_3^0)$ von λ ein Zylinder

$$Z(X):\ F(x_1 - x_1^0, x_2 - x_2^0, x_3 - x_3^0) \leq \frac{1}{2}$$

von halber Länge, Breite und Höhe von K seinem Zentrum in X und der Achse parallel zu der x_3-Achse. Nachdem λ K-zulässig und K konvex ist, überlappen keine zwei dieser Zylinder.
Sei n eine große positive ganze Zahl. Nachdem jedes Gitter-Parallelepiped das Volumen $d(\lambda)$ hat, enthält der Würfel

$$|x_1| \leq n - \frac{1}{2},\ |x_2| \leq n - \frac{1}{2},\ |x_3| \leq n - \frac{1}{2}$$

$$\frac{8n^3}{d(\lambda)} + O(n^2)$$

Punkte von λ. Schließlich liegen mindestens so viele Zylinder $Z(x)$ daher in dem Würfel

$$|x_1| \leq n, |x_2| \leq n, |x_3| \leq n.$$

Daher folgt aus Lemma 2.6

$$\frac{8n^3}{d(\lambda)} + O(n^2) \leq \frac{16}{\sqrt{3}} n^3,$$

wobei

$$d(\lambda) \geq \frac{1}{2}\sqrt{3} - o(1),$$

das heißt

$$d(\rho) \geq \frac{1}{2}\sqrt{3},\ \Delta(K) \geq \frac{1}{2}\sqrt{3}$$

□

Beweis. Der Beweis von Lemma 2.3 folgt nun aus den letzten beiden Lemmas und Bemerkung 2.4. □

Lemma 2.7
Sei $k > 1$. Es gibt eine unendliche Menge von Werten $\alpha_n, \beta_n, \gamma_n = \overline{\beta_n}$ von M_1, M_2, M_3, welche zu den ganzzahligen Werten u_n, v_n, w_n gehören, sodass

(1) $|\alpha_n \beta_n^2| \leq |\Delta|^2 3^{-\frac{1}{2}}$
(2) $k|\alpha_n| \leq |\alpha_{n-1}|$
(3) $|\beta_n^2||\alpha_{n-1}| \leq k|\Delta|^2 3^{-\frac{1}{2}}$
(4) $|\beta_n| \geq |\beta_{n-1}|$

Lemma 2.8
Falls $k > 2$, kann man (x_0, y_0, z_0) finden, sodass

$$||x_0 u_n + y_0 v_n + z_0 w_n|| \geq \frac{k-2}{2(k-1)}$$

für alle n gilt.

Beweis. Die Beweise der letzten beiden Lemmata sind ähnlich wie die die der Lemmata 2.12-2.14. □

Lemma 2.9
Angenommen $k > 2$, und

$$r = (\frac{k + k^{\frac{1}{2}}}{2})^{\frac{1}{3}},\ q = kr^{-2},$$

sodass

$$gr^2 = k,\ q + 2q^{-\frac{1}{2}} = 2r + r^{-2} = 2^{\frac{3}{2}} \frac{(1 + k^{\frac{1}{2}} + k)}{(k + k^{\frac{1}{2}})^{\frac{2}{3}}} = \lambda.$$

Falls $l, m, p > 0$, sodass

$$lm^2 \leq p^3,\ l \leq qp,\ m \leq rp,$$

dann ist

$$l + 2m \leq \lambda p.$$

Beweis. Offensichtlich, bzw nachrechnen. □

Seien nun $\xi, \eta, \zeta = \overline{\eta}$ Werte von L_1, L_2, L_3 für ein

$$(x, y, z) \equiv (x_0, y_0, z_0) \pmod 1$$

Wähle n so, dass

$$|\beta_n^2| \leq r^2 |\xi|^{\frac{2}{3}} |\eta|^{-\frac{2}{3}} (\frac{|\Delta|^2}{3^{\frac{1}{2}}})^{\frac{2}{3}} \leq ||\beta_{n+1}|^2.$$

Dann gilt nach Lemma 2.7, dass

$$|\alpha_n| \leq q |\xi|^{-\frac{2}{3}} |\eta|^{\frac{2}{3}} \left(\frac{|\Delta|^2}{3}\right)^{\frac{1}{3}}$$

Daher folgt aus Lemma 2.9, mit

$$l = |\xi \alpha_n|,\ m = |\eta \beta_n|$$

und

$$p = |\xi|^{\frac{1}{2}} |\eta|^{\frac{2}{3}} \left(\frac{|\Delta|^2}{3^{\frac{1}{2}}}\right)^{\frac{1}{3}},$$

dass

$$|\xi \alpha_n| + 2|\eta \beta_n| \leq \lambda |\xi|^{\frac{1}{3}} |\eta|^{\frac{2}{3}} \left(\frac{|\Delta|^2}{3^{\frac{1}{2}}}\right)^{\frac{1}{3}}.$$

Aber jetzt ist

$$|\Delta||xu_n + yv_n + zw_n| = |\xi \alpha_n + \eta \beta_n + \zeta \gamma_n| \leq |\xi \alpha_n| + 2|\eta \beta_n|,$$

und dadurch folgt aus Lemma 2.8

$$|\xi\eta^2| \geq 3^{\frac{1}{2}}\left\{\frac{k-2}{2(k-1)\lambda}\right\}^3|\Delta| = \frac{3^{\frac{1}{2}}}{2^5}\frac{(k-2)^3(k+k^{\frac{1}{3}})^2}{(k-1)^3(k+k^{\frac{1}{3}}+1)^3}|\Delta|.$$

Die Funktion auf der rechten Seite nimmt ihr Maximum in der Nähe der Stelle $k = 7$ an; Setzt man $k = (\frac{8}{3})^2$, dann erhält man, wie behauptet

$$|\xi\eta\zeta| = |\xi\eta^2| \geq |\frac{3^{\frac{5}{2}} \cdot 2^4 \cdot 23^3}{11 \cdot 5^3 \cdot 97^3}||\Delta| > \frac{|\Delta|}{420}.$$

Als nächstes wird der Fall behandelt, dass $M_1 = 0$, $M_2 = 0$, $M_3 = 0$ oder alle 0 sind. Das führt zu $f(x,y) = 0$ im binären Fall und kann analog behandelt werden.
Um dies zu zeigen, braucht es einiges an Vorarbeit.

Satz 2.10
Für fast alle Paare (x_0, y_0) gilt

$$\min|f(x,y)| = 0,\ (x,y) \equiv (x_0,y_0) \pmod 1$$

Wenn f kein Vielfaches des Produktes von zwei linearen Formen mit rationalen Koeffizienten ist.

Beweis. Um die Notwendigkeit der zweiten Bedingung zu zeigen muss man folgendes betrachten:
Sei $f(x,y) = ax^2 + bxy + cy^2$ eine indefinite Form. Dann existieren reelle Zahlenpaare (x_0, y_0), sodass

$$|f(x,y)| \geq \frac{\sqrt{b^2 - 4ac}}{48} \tag{4}$$

für alle $(x,y) \equiv (x_0,y_0) \pmod 1$. □

Lemma 2.11
Sei $\lambda_0, \lambda_1, \ldots, \lambda_n, \ldots$ eine endliche oder unendliche Menge reeller Zahlen mit

$$|\lambda_{n-1}| \geq k|\lambda_n| > 0$$

Seien $\mu_0, \mu_1, \ldots$ beliebig. Dann gibt es eine reelle Zahl ξ, sodass

$$||\lambda_n\xi + \mu_n|| \geq \frac{k-2}{2(k-1)},$$

für $n = 0, 1, 2 \ldots$.
Falls es nur eine endliche Zahl von λ_n gibt, gibt es ein Intervall jener Punkte, welche die geforderte Bedingung erfüllen.

Beweis. Mittels Induktion nach n zeigt man, dass es ein Intervall F_n der Länge $|F_n| \geq (k-1)^{-1}|\lambda_n|^{-1}$ gibt, sodass $F_n \subset F_{n-1}$ und

$$\|\lambda_v \xi + \mu_v\| \geq \frac{k-2}{2(k-1)}, \ (v = 0, 1, \ldots, n)$$

für alle $\xi \in F_n$ gilt. Nun nimmt man für F_o die Menge der $\xi = \lambda_0^{-1} x$,

$$\frac{1}{2} - \frac{1}{2(k-1)} - \mu_0 \leq x \leq \frac{1}{2} + \frac{1}{2(k-1)} - \mu_0,$$

welche die geforderte Eigenschaft erfüllt.
Wenn F_n existiert, ist die Menge R_n aller $\lambda_{n+1} x$, mit $x \in F_n$, ein Intervall der Länge von mindestens

$$|\lambda_{n+1}|(k-1)^{-1}|\lambda|^{-1} \geq 1 + \frac{1}{k-1}.$$

Daher enthält R_n ein Intervall L_n der Form

$$m + \frac{1}{2} - \frac{1}{2(k-1)} - \mu_{n+1} \leq x \leq m + \frac{1}{2} + \frac{1}{2(k-1)} - \mu_{n+1},$$

für eine gewisse ganze Zahlen m.
Nun definiert man F_{n+1} als die Menge aller $\lambda_{n+1}^{-1} x$, mit $x \in L_n$, und das Resultat folgt.
Falls es nur eine endliche Anzahl von λ_n gibt, kann man für ξ einen beliebigen Punkt nehmen, welcher im letzten F_n enthalten ist.
Falls es eine unendliche Anzahl an λ_n gibt, wird ξ von den Intervallen $F_0 \supset F_1 \supset F_2 \ldots$ bestimmt.
Sei nun $f(x, y) = (x + y\theta)(x + y\phi)$, mit $\theta \neq \phi$, und seien beide irrational. □

Lemma 2.12
Gegeben sei $M > 1$. Dann gibt es eine endliche Folge G_M von Paaren koprimen ganzer Zahlen (nicht beide 0) $(u_0, v_0), (u_1, v_1), \ldots, (u_N, v_N)$, sodass

(1) $|u_n - v_n\theta||u_n - v_n\phi| \leq |\theta - \phi|$

(2) $k|u_n - v_n\theta| \leq |u_{n-1} - v_{n-1}\theta|$
(3) $|u_n - v_n\phi||u_{n-1} - v_{n-1}\theta| \leq k|\theta - \phi|$
(4) $|u_0 - v_0\phi| \leq M^{-1}$, $|u_0 - v_0\theta| \geq M$
(5) $|u_N - v_N\phi| \geq M$, $|u_N - v_N\theta| \leq M^{-1}$
(6) $|u_n - v_n\phi| \geq u_{n-1} - v_{n-1}\phi|$ $(n \geq 1)$

Beweis. Nachdem ϕ irrational, und $\theta \neq \phi$ ist, gibt es u_0, v_0, welche Bedingung (1) und (4) erfüllen. Nun definiert man u_n, v_n induktiv, durch die Ungleichungen

$$|u_n - v_n\theta| \leq k^{-1}|u_{n-1} - v_{n-1}\theta|$$

und

$$|u_n - v_n\phi| \leq \frac{|\theta - \phi|k}{|v_{n-1} - v_{n-1}\theta|}$$

Dann existieren (u_n, v_n) nach Minkowskis Linearformensatz, welche (1),(2) und (3) erfüllen. Es wird jedesmal jene Lösung mit dem kleinsten $|u_n - v_n\phi|$ gewählt. Daraus folgt (4).
Nachdem θ irrational ist, muss man irgendwann (u_N, v_N) erreichen, für das (5) gilt. □

Nun betrachtet man die Bilinearform

$$F(x, y; u, v) = (x - y\theta)(u - v\phi) - (x - y\phi)(u - v\theta)$$

$$= (\theta - \phi)(xv - yu)$$

Lemma 2.13
Es gibt x_0, y_0, sodass

$$|F(x, y; u, v)| \geq |\theta - \phi|\frac{k-2}{2(k-1)} \tag{5}$$

für alle $(x, y) \equiv (x_0, y_0) \pmod 1$ und alle Paare $(u_n, v_n)(n = 0, 1, \ldots, N)$ gilt.

Beweis. Nach Lemma 2.12(2) und Lemma 2.11 mit

$$\lambda_{N-n} = \frac{u_n - v_n\theta}{\theta - \phi}, \mu_n = 0$$

kann man ein ζ finden, sodass

$$\|\frac{u_n - v_n\theta}{\theta - \phi}\zeta\| \geq \frac{2(k-1)}{k-2} \ (n = 0, 1, \ldots, N). \tag{6}$$

Man definiert x_0, y_0 durch die Gleichungen

$$x_0 - y_0\theta = 0,\ x_0 - y_0\phi = -\zeta \tag{7}$$

und so

$$F(x_0, y_0; u_n, v_n) = (u_n - v_n\theta)\zeta. \tag{8}$$

Falls $(x, y) \equiv (x_0, y_0) \pmod 1$, gilt

$$\begin{aligned} &F(x, y; u_n, v_n) - F(x_0, y_0; u_n, v_n) \\ &= (\theta - \phi)(v(x - x_0) - u(y - y_0)) = m(\theta - \phi) \end{aligned} \tag{9}$$

wobei m eine gewisse ganze Zahl ist. Das Resultat folgt aus den Gleichungen (6),(8) und (9). □

Lemma 2.14
Es gibt eine doppelt-unendliche Menge von Paaren ganzer Zahlen (u_n, v_n) mit $-\infty < n < \infty$, sodass (1-4) in Lemma 2.12 gelten und

$$\lim_{n\to\infty} |u_n - v_n\theta| = 0,\ \lim_{n\to\infty} |u_n - v_n\phi| = \infty,$$
$$\lim_{n\to-\infty} |u_n - v_n\theta| = \infty,\ \lim_{n\to-\infty} |u_n - v_n\phi| = 0,$$

und es gibt ein Paar (x_0, y_0), sodass Gleichung (5), für alle $(x, y) \equiv (x_0, y_0) \pmod 1$ und alle n gilt.

Beweis. Man bemerke zuerst, dass es für ein gegebenes $L > 0$, nur eine endliche Anzahl an Paaren $(u_{n-1}, v_{n-1}), (u_n, v_n)$ ganzer Zahlen geben kann mit

$$|u_n - v_n\theta| \le L < |u_{n-1} - v_{n-1}\theta|,$$

die auch (1-3) von Lemma 2.12 erfüllen. Es gibt nur eine endliche Anzahl an Möglichkeiten für (u_n, v_n), da $|u_n - v_n\theta| \le k|\theta - \phi|L^{-1}$ nach 2.12(3).
Aber $|u_n - v_n\phi| \neq 0$ nach Vorausstzung und so folgt wieder nach 2.12(3),

$$L \le |u_{n-1} - v_{n-1}\theta| \le k|\theta - \phi||u_n - v_n\phi|^{-1}.$$

Daher gibt es, nach 2.12(1) mit $n-1$ anstatt n, nur eine endliche Anzahl an Möglichkeiten für (u_{n-1}, v_{n-1}). Genauer gesagt gibt es, für gegebene (u_n, v_n) nur eine endliche Anzahl an Möglichkeiten für (u_{n+1}, v_{n+1}) und (u_{n-1}, v_{n-1})

Nach 2.12(4) und 2.12(5) und weil $M > 1$, gibt es für jedes G_M eine eindeutiges N_1, sodass

$$|u_{N_1} - v_{N_1}\theta| \leq 1 < |u_{N_{1-1}} - v_{N_{1-1}}\theta|.$$

Sei G'_M eine Folge von (u'_n, v'_n) definiert durch

$$(u'_n, v'_n) = (u_{n-N_1}, v_{n-N_1}) \; für \; -N_1 \leq n \leq +N_2 = N - N_1.$$

Dann gilt (1-4) aus Lemma 2.12 für (u'_n, v'_n) anstatt (u_n, v_n) und

$$|u'_0 - v'_0\theta| \leq 1 < |u'_{-1} - v'_{-1}\theta|, \; |u_{N_2} - v_{v_{N_2}}\theta| \leq M^{-1}, \; |u_{-N_1} - v_{-N_1}\theta| \geq M.$$

Nun konstruiert man G durch ein Diagonalverfahren. Es gilt, dass es nur eine endliche Anzahl an Möglichkeiten für (u'_0, v'_0) und (u'_{-1}, v'_{-1}) gibt; und so muss mindestens eine der Möglichkeiten auftreten für beliebig großes M. Man fixiert ein solches mögliches Paar $(\overline{u_0}, \overline{v_0})$, $(\overline{u_{-1}}, \overline{v_{-1}})$ und betrachet nun nur diese G'_M, in denen diese aufreten.
Es gibt nun nur eine endliche Anzahl an Möglichkeiten für (u'_1, v'_1) und (u'_{-2}, v'_{-2}) und wieder nimmt eine Möglichkeit, welche für beliebig große M auftritt, nämlich $(\overline{u_1}, \overline{v_1})$, $(\overline{u_{-2}}, \overline{v_{-2}})$.
Dieser Prozess kann fortgeführt werden. Dann erfüllt $(\overline{u_n}, \overline{v_n})$ (1-4) aus Lemma 2.12, und auch

$$\lim_{n\to\infty} |\overline{u_n} - \overline{v_n}\theta| = 0, \; \lim_{n\to-\infty} |\overline{u_n} - \overline{v_n}| = \infty,$$

nach 2.12(2). Nach 2.12(1) folgt daraus

$$\lim_{n\to\infty} |\overline{u_n} - \overline{v_n}\phi| = \infty, \; \lim_{n\to-\infty} |\overline{u_n} - \overline{v_n}\phi| = 0,$$

weil θ und ϕ nach Voraussetzung irrational sind. Daher erfüllt die Folge $(\overline{u_n}, \overline{v_n})$ die von G geforderten Eigenschaften.
Umgekehrt, für ein gegebenes G ist es trivial ein G_M, für ein beliebiges M zu finden, indem man einen passenden Abschnitt der unendlichen Reihe nimmt und unnummeriert. Man kann annehmen, dass G_M von dieser Art ist. Zu jedem solchen G_M, mit $(M = 2, 3, 4, \ldots)$ gibt es ein zugehöriges $(x_0^{(M)}, y_0^{(M)})$, nach dem vorletzte Lemma, wobei man annehmen kann, dass $0 \leq x_0^{(M)} \leq 1$, $0 \leq y_0^{(M)} \leq 1$. Diese haben einen Grenzwert (x_0, y_0), der die geforderten Eigenschaften besitzt. □

Lemma 2.15
Seien l, m, n, p positive Zahlen und

$$lm \leq p^3,\ l \leq qp,\ m \leq qp.$$

Dann gilt

$$l + m \leq (q + \frac{1}{q})p.$$

Beweis. Folgt aus dem nächsten Lemma. □

Lemma 2.16
Sind $x, y, q > 0,\ xy \leq 1,\ x \leq q$ und $y \leq q$, dann gilt $x + y \leq q + \frac{1}{q}$.

Beweis. Die Funktion $f\colon (0,\infty) \to \mathbb{R},\ f(x) = x + \frac{1}{x}$ hat die Ableitung

$$f'(x) = 1 - \frac{1}{x^2} \begin{cases} < 0 & für\ 0 < x < 1, \\ = 0 & für\ x = 1, \\ > 0 & für\ x > 1. \end{cases}$$

Daher ist f streng monoton fallend auf $(0, 1]$ und streng monoton wachsend auf $[1, +\infty)$. Insbesondere besitzt f ein globales Minimum bei 1 und daher $x + \frac{1}{x} > 2$ für alle $x \geq 0$.
1.Fall:$x \geq 1$. Dann gilt $x + y \leq x + \frac{1}{x} \leq q + \frac{1}{q},\ da\ 1 \leq x \leq q$.
2.Fall:$y \geq 1$. Dann gilt $x + y \leq y + \frac{1}{y} \leq q + \frac{1}{q},\ da\ 1 \leq y \leq q$.
3.Fall:$x < 1$ und $y < 1$. Dann gilt $x + y \leq 2 \leq q + \frac{1}{q}$.

□

Bemerkung 2.17
Der Beweis von Lemma 2.15 folgt nun indem man $x = \frac{l}{p}$ und $y = \frac{m}{p}$ setzt.

Bemerkung 2.18
Daraus folgt nun auch Gleichung (4). Nimmt man x_0, y_0, wie im Lemma 2.14 und sei $x \equiv x_0,\ y \equiv y_0$.
Angenommen $x - y\theta = 0$, dann hat man

$$\lim_{n \to -\infty} |F(x, y; u_n, v_n)| = \lim_{n \to -\infty} |(u_n - v_n\theta)(x - y\phi)| = 0.$$

Das ist ein Widerspruch zur Annahme. Ähnlich führt auch $x - y\phi = 0$ zu einem Widerspruch, sodass

$$x - y\theta \neq 0,\ x - y\phi \neq 0,$$

und daher

$$f(x,y) \neq 0.$$

Nun wählt man (u_n, v_n), so wie bei 2.12(4), sodass

$$(u_n - v_n\phi)^2 \leq k|\theta - \phi||\frac{|x - y\phi|}{|x - y\theta|}| \leq (u_{n+1} + v_{n+1}\phi)^2$$

und daher folgt nach 2.12(3)

$$(u_n - v_n\phi)^2 \leq \frac{k^2(\theta - \phi)^2}{(u_{n+1} - v_{n+1}\phi)^2} \leq k|\theta - \phi|\frac{|x - y\theta|}{|x - y\phi|}.$$

Nun wendet man Lemma 2.15 mit

$$l = |u_n - v_n\phi||x - y\theta|,\ m = |u_n - v_n\theta||x - y\phi|,$$

$$p^2 = |\theta - \phi||f(x,y)|,\ q^2 = k$$

an, erhält man

$$|F(x,y;u_n,v_n)| \leq (k^{\frac{1}{2}} + k^{-\frac{1}{2}})|\theta - \phi|^{\frac{1}{2}}|f(x,y)|^{\frac{1}{2}}.$$

Daher folgt nach dem Lemma 2.13

$$|f(x,y)| \geq |\theta - \phi|\Big(\frac{k-2}{2(k-1)}\frac{1}{k^{\frac{1}{2}} + k^{-\frac{1}{2}}}\Big)^2$$

Die Funktion $g(k) = \frac{k(k-2)^2}{4(k^2-1)^2}$ hat ein Maximum für $k > 2$ nahe $k = 5 \cdot 5$ und

$$g(5 \cdot 5) = \frac{539}{25,578} > \frac{1}{48},$$

was Gleichung (4) beweist, wenn θ und ϕ irrational sind. Nun sei θ rational, ϕ aber nicht. Dann führt der Prozess von Lemma 2.12 zu einer unendlichen Menge (u_n, v_n), mit $-\infty < n \leq N$, und u_N, v_N ist die Lösung in koprimen ganzen Zahlen von $u_N - v_N\theta = 0$.

Man nehme nun eine Lösung κ von

$$||(u_N - v_N\phi)\kappa|| \geq \frac{k-2}{2(k-1)}.$$

Nun kann man nach dem Lemma 2.12 ein ξ finden, sodass

$$\|(u_n - v_n\theta)\xi - (u_n - v_n\phi)\kappa\| \geq \frac{k-2}{2(k-1)},\ -\infty < n \leq N$$

Dann erfüllt die Lösung x_0, y_0 von

$$x_0 - y_0\phi = \xi(\theta - \phi),\ x_0 - y_0\theta = \kappa(\theta - \phi)$$

die Gleichung

$$\|\frac{F(x_0, y_0; u_n, v_n)}{\theta - \phi}\| \geq \frac{k-2}{2(k-1)}$$

für alle n. Wie zuvor ist $x - y\theta \neq 0,\ x - y\phi \neq 0$ für $(x, y) \equiv (x_0, y_0)$. Falls

$$\kappa|\theta - \phi|\frac{|x - y\phi|}{|x - y\theta|} \geq (u_N - v_N\phi)^2$$

gelten die selben Argumente wie bevor. Falls nicht, hat man

$$|F(x, y; u_N, v_N)| = |(x - y\theta)(u_N - v_N\phi)| \leq k^{\frac{1}{2}}|\theta - \phi|^{\frac{1}{2}}|f(x, y)|^{\frac{1}{2}}$$

und nach Lemma 2.14 ist

$$|f(x, y)| \geq |\theta - \phi|\Big(\frac{k-2}{2(k-1)}k^{-\frac{1}{2}}\Big)^2,$$

was eine stärkere Bedingung ist, als die Ungleichung, welche man im allgemeinen Fall erhält. Daher stimmt der letzte Satz auch hier; Da man $\kappa = (x_N - y_N\theta)(\theta - \phi)^{-1}$ in einem Intervall beliebig wählen kann gibt es überabzählbar viele mögliche Werte von (x_0, y_0).
Falls θ und ϕ beide rational sind, kann man ähnliche Argumente verwenden. Es gibt dann nur eine endliche Kette von (u_n, v_n): Daher liegt $(x - y\theta)(\theta - \phi) = \kappa$ in einem Intervall und ebenso ξ, nach dem letzten Satz von Lemma 2.11.
Insbesondere können θ und ϕ rational gewählt werden, sodass x_0 und y_0 rational sind.
Dies beweist aber auch, dass die Bedingung in Satz 2.10 eine notwendige Bedingung ist.

Bemerkung 2.19
Nachdem man nun die Notwendigkeit der Bedingung bewiesen

hat, kann man daher ohne Verlust der Allgemeinheit voraussetzen, dass ϕ irrational ist. Man muss beweisen, dass

$$\min|(x-y\theta)(x-y\phi)| = 0,\ (x,y) \equiv (x_0,y_0) \pmod 1$$

für fast alle Punkte (x_0, y_0).

Lemma 2.20
Es gibt eine Konstante κ mit folgender Eigenschaft:
Seien θ und ϕ gegebene reelle Zahlen mit $\theta \neq \phi$, ϕ irrational. Dann gibt es für ein $\epsilon > 0$ und koprime ganze Zahlen m_0, n_0 mit

$$|m_0 - n_0\phi| < \epsilon,$$

$$|\theta - \phi| \leq |m_0 - n_0\theta||m_0 - n_0\phi| \leq \kappa|\theta - \phi|.$$

Beweis. Übersetzt in die Gittertheorie, ist dieses Lemma äquivalent zu der Tatsache, dass es in jedem Gitter mit Determinante 1, mit einem Punkt im Ursprung, aber keinen anderen Punkt auf der y-Achse, primitive Punkte gibt, sodass

$$1 \leq |xy| \leq \kappa$$

und x beliebig klein. Man zeigt nun, dass $\kappa = 2 - 5^{\frac{1}{2}}$. Es gibt bestimmte primitive Gitterpunkte (p,q) mit q beliebig groß, sodass $|pq| \leq 1$, und ohne Verlust der Allgemeinheit kann man voraussetzten, dass $q > 0$. Dann existieren Gitterpunkte auf $qx - py = 1$ und sind primitiv. Eine hinreichende Bedingung dafür, dass ein Punkt, auf dieser Gerade enthalten ist und die obere Gleichung erfüllt, ist

$$x_1 = \frac{1 + (1 + 4qp)^{\frac{1}{2}}}{2q} \leq x \leq \frac{1 + (1 + 4qp\kappa)^{\frac{1}{2}}}{2q} = x_2.$$

Falls $p > 0$, implizieren die Bedingungen von Lemma 2.20, dass $x_2 - x_1 \geq p$, und so es gibt einen Gitterpunkt (x_0, y_0) auf der Gerade mit $x_1 \leq x_0 \leq x_2$. Nachdem q beliebig groß sein kann, können x_2 und x_0 beliebig klein werden. Falls $p < 0$, betrachtet man die Gitterpunkte auf $qx - py = -1$ und verwendet das selbe Argument. □

Korollar 2.21
Es gibt eine Transformation

$$x = t_{11}x' + t_{12}y',\ y = t_{21}x' + t_{22}y',$$

wobei $t_{11}, t_{12}, t_{21}, t_{22}$ ganzzahlig sind und

$$t_{11}t_{22} - t_{21}t_{12} = 1$$

und Zahlen A, B, θ', ϕ', sodass

$$(x' - y'\theta') = A(x - y\theta),$$

$$(x' - y'\phi') = B(x - y\phi),$$

$$|B|^{-1} < \epsilon,\ |\theta - \phi| \leq |AB|^{-1} \leq \kappa|\theta - \phi|.$$

Beweis. Setze $t_{11} = m_0,\ t_{21} = n_0$ und wähle t_{12} und t_{22} so, dass sie eine unimodulare Determinante bilden. □

Lemma 2.22
Es gibt zwei Funktionen $\eta_1 > 0, \eta_2 > 0$ für die Variablen Ω_1, Ω_2 mit folgenden Eigeschaften:
Seien $\theta, \phi, t, d, D, x_0, y_0$ gegeben, sodass

$$0 < \Omega_1^{-1} \leq |\theta - \phi| \leq \Omega_2,\ 0 < t < 1,\ 0 < d < 1,\ D > \eta_1$$

Bezeichnet nun $F(t)$ die Menge aller (x, y), sodass

$$\min|(\xi - \eta\theta)(\xi - \eta\phi)| < t$$

$$(\xi, \eta) \equiv (x, y) \pmod 1$$

und B bezeichne das Parallelogramm

$$|(x - y\theta) - (x_0 - y_0\theta)| \leq d$$

$$|(x - y\phi) - (x_0 - y_0\phi)| \leq D.$$

So ist

$$|F(t) \bigcap B| \geq \eta_2 t|B|,$$

wobei $|B|$ die Fläche von B bezeichnet.

Beweis. Eine positive Konstante, die nur von Ω_1 und , Ω_2 abhängt, wird mit η mit einem Suffix bezeichnet. Nun macht man eine Transformation

$$x = x_0 + \lambda\theta + \mu\phi,\ y = y_0 + \lambda + \mu \tag{10}$$

zu den Variablen λ und μ. Dann ist B durch folgende Ungleichungen definiert

$$|\lambda| \leq \frac{D}{|\theta-\phi|} = D^*,\ |\mu| \leq \frac{d}{|\theta-\phi|} = d^*.$$

Man setzt nun

$$\eta_3 = [\Omega_1] + 1$$

und man kann annehmen, dass

$$D > 10\Omega_2\eta_3 = \eta_1,$$

sodass

$$D^* > 10\eta_3. \tag{11}$$

Nun definiert man ganze Zahlen $n_1, n_2, \ldots, n_s$ durch

$$n_1 = [y_0 - D^* + \eta_3] + 1,\ n_j = n_{j-1} + 2\eta_3,$$

wobei

$$s = \Big[\frac{D^*}{4\eta_3}\Big] > \eta_4 D^*$$

nach (11). Daher ist

$$y_0 - D^* + \eta_3 \leq n_1 < n_s \leq y_0 + D^* - \eta_3.$$

Nun definiert man ganze Zahlen m_j ($j = 1, 2, \ldots, s$), sodass

$$|m_j - x_0 - (n_j - y_0)\theta| \leq \frac{1}{2} \tag{12}$$

und λ_j und μ_j nach der obigen Gleichung (11). Dann gilt

$$|\mu_j| \leq \frac{1}{2|\theta-\phi|}$$

nach (12) und daher

$$|\lambda_j - (n_j - x_0)| \leq \frac{1}{2|\theta-\phi|}.$$

Daher ist

$$\lambda_j - \lambda_{j-1} \geq 2\eta_3 - \frac{1}{|\theta-\phi|} \geq 2\eta - \Omega_1 > \Omega_1, \tag{13}$$

und ebenso

$$\lambda_1 > -D^* + \frac{1}{2}\Omega_1,\ \lambda_s < D^* - \frac{1}{2}\Omega_1. \tag{14}$$

Nun bezeichne G_j ($j = 1, 2, \ldots, s$) die Menge aller (x, y) für die

$$|\lambda - \lambda_j| \leq \frac{t}{2|\theta - \phi|} < \frac{1}{2}\Omega_1,\ |\mu| \leq d^*$$

gilt.
Dann folgt aus (13) und (14), dass die G_i disjunkt und in B enthalten sind.
Weiters hat jedes G_i Fläche $4|\theta-\phi|\frac{t}{2|\theta-\phi|}d^* = 2td^*$, weil $|\frac{\partial(x,y)}{\partial(\lambda,\mu)}| = |\theta - \phi|$.
Daher ist die Gesamtfläche von $\bigcup G_j$ genau $s \cdot 2td^* \geq 2t\eta_4 D^* d^* > n_2 t|B|$. Das Lemma ist daher bewiesen, wenn man zeigen kann, dass

$$G_i \subset F(t).$$

Ist aber $(x, y) \in G_i$, dann hat man

$$|(x - m_j - (y - n_j)\theta)(x - m_j - (y - n_j)\phi)| = (\theta - \phi)^2 |\lambda - \lambda_j||\mu - \mu_j|$$

$$\leq (\theta - \phi)^2 \frac{t}{2|\theta - \phi|}(|\mu| + |\mu_j|) < t,$$

wie verlangt, nachdem

$$|\mu| + |\mu_j| \leq d^* + \frac{1}{2|\theta - \phi|} \leq \frac{d + \frac{1}{2}}{|\theta - \phi|} \leq \frac{3}{2}\frac{1}{|\theta - \phi|}.$$

□

Lemma 2.23
Sei $F(t)$ wie in Lemma 2.22 und sei U ein Parallelogramm

$$|(x - y\theta) - (x_0 - y_0\theta)| \leq u,\ |(x - y\phi) - (x_0 - y_0\phi)| \leq v.$$

Dann gibt es eine Konstante η_7, die nur von θ und ϕ abhängt, sodass

$$|F(t) \bigcap U| \geq \eta_7 t|U|.$$

Beweis. Man macht eine Substitution vom selben Typ, wie in Lemma 2.20. Bezeichne $'$ eine Größe die zu $(x' - y'\theta')(x' - y'\phi')$ in Beziehung steht. Dann hat man

$$(\theta' - \phi')^2 = A^2 B^2 (\theta - \phi)^2$$

und so

$$0 < \kappa^{-1} = \Omega_1^{-1} \leq |\theta' - \phi'| \leq \Omega_2 = 1.$$

Weiters ist

$$(x' - y'\theta')(x' - y'\phi') = AB(x - y\theta)(x - y\phi),$$

und so wird $F(t)$ zu $F'(t)$ transponiert, wobei $t' = |AB|t$. Schließlich wird U in das Parallelogramm B' transformiert, welches durch

$$|x' - y'\theta'| \leq u|A|,\ |x' - y'\phi'| \leq v|B|$$

definiert ist, wobei $u|A|$ beliebig klein und $v|B|$ beliebig groß sein kann. Somit ist

$$\frac{|F'(t) \bigcap U|}{|U|} = \frac{|F'(t') \bigcap B'|}{|B'|} \geq \eta_2 t' \geq \eta_7 t.$$

□

Korollar 2.24
Fast alle Punkte sind in $F(t)$.

Falls nicht gäbe es einen Punkt, in dem die Dichte von $F(t)$ gleich 0 ist. Das widerspricht Lemma 2.23.
Nun ist der Beweis des Satzes abgeschlossen weil

$$F(t_1) \supset F(t_2),$$

falls $t_1 > t_2$. Sei $F = \lim_{t \to 0} F(t)$. Dann folgt aus einem vorigen Korollar, dass fast alle Punkte in F sind, was zu zeigen war.
Der Fall, dass x_0, y_0, z_0 rational werden, wenn L_1, L_2, L_3 konjugiert sind, läuft wie im quadratischen Fall, im nächsten Satz bewiesen wird.

Satz 2.25
Falls a, b und c rational sind, dann können x_0 und y_0 auch rational gewählt werden.

Beweis. Angenommen $f(x, y)$ hat rationale Koeffizienten. Falls θ und ϕ beide rational sind, gilt Satz 2.25, nach Bemerkung 2.18.
Falls nicht, sind θ und ϕ konjugierte Zahlen in einem quadratischen Zahlkörper, wovon nun ausgegangen wird.
Man bemerke, dass, nachdem $N(u_n - v_n\theta) = f(u_n, v_n)$ beschränkt

ist, es eine Einheit ϵ des Körpers geben muss, und m_0, n_0 mit $m_0 > n_0$, sodass

$$(u_{m_0} - v_{m_0}\theta) = \epsilon(u_{n_0} - v_{n_0}\theta).$$

Setzt man $m_0 - n_0 = N$ und definiert eine neue Folge durch

$$u_n^* - v_n^*\theta = u_n - v_n\theta \ (n_0 \leq n \leq m_0),$$

und

$$u_{n+N}^* - v_{n+N}^*\theta = \epsilon(u_n^* - v_n^*\theta) \ (-\infty < n < \infty),$$

diese Folge erfüllt alle Bedingungen von Lemma 2.13 und Lemma 2.14. Man kann daher voraussetzen, dass es eine Einheit ϵ des Körpers, und eine ganze Zahl N gibt, sodass

$$u_{n+N} - v_{n+N}\theta = \epsilon(u_n - v_n\theta),$$

$$u_{n+N} - v_{n+N}\phi = \overline{\epsilon}(u_n - v_n\phi)$$

($\overline{\epsilon}$ ist Konjugierte von ϵ). Nimmt man $2N$ anstatt N und daher auch ϵ^2 anstatt ϵ, dann hat man $\overline{\epsilon} = (\epsilon)^{-1}$ $(\epsilon > 0)$. Weiters, nachdem $u_n - v_n\theta \to 0$ für $n \to 0$, hat man

$$0 < \epsilon < 1.$$

Um nun Satz 2.25 zu zeigen, muss man nur die Existenz der rationalen Zahlen x_0, y_0 zeigen, sodass

$$\|\frac{u_n - v_n\theta)(x_0 - y_0\phi) - (u_n - v_n\phi)(x_0 + y_0\theta)}{\theta - \phi}\| \geq \frac{k-2}{2(k-1)} - e,$$

für alle n gilt, wobei e eine beliebig kleine gegebene positive Zahl ist.
Nach Lemma 2.11 gibt es eine reelle Zahl ξ, sodass

$$\|\frac{u_n - v_n\theta}{\theta - \phi}\xi\| \geq \frac{k-2}{2(k-1)} \ (n \leq 0).$$

Setze

$$\lambda_n = \frac{u_{-n} - v_{-}n\theta}{\theta - \phi},$$

sodass $\lambda_{n+N} = \epsilon^{-1}\lambda_n$. Man kann nun jedes λ_n $(0 \leq n < N)$ in folgender Form darstellen

$$\lambda_n = \frac{a_n + b_n\epsilon}{c}$$

wobei a_n, b_n und c ganzzahlig sind. Daher ist

$$\|\epsilon^{-m}(a_n + b_n\epsilon)\zeta\| \geq \frac{k-2}{2(k-1)}, \tag{15}$$
$$0 \leq m < \infty,\ 0 \leq n < N, c\zeta = \xi.$$

Die Zahl ζ kann in der Form

$$\zeta = z_0 + z_1\epsilon + z_2\epsilon^2 + \ldots, \tag{16}$$

geschreiben werden, wobei $z_0, z_1, \ldots$ ganzzahlig sind und $0 \leq z_j < \epsilon^{-1}, (j \neq 0)$. Nun ist die Behauptung, dass der Bruchteil von $\epsilon^{-m}(a_n + b_n\epsilon)\zeta$ der selbe ist wie der von

$$p_{mn} = (a_n + b_n\epsilon)\zeta_m - (a_n - b_n\epsilon^{-1})\eta_m,$$

wobei (mit der Konvention $z_j = 0$, für $j < 0$),

$$\zeta_m = \sum_{j=0}^{\infty} z_{j+m}\epsilon^j,\ \eta_m = \sum_{-\infty}^{-1} z_{j+m}\epsilon^{-j}.$$

Allerdings

$$\epsilon^{-m}\zeta = \zeta_m + \sum_{-\infty}^{-1} z_{j+m}\epsilon^{-i}$$

und

$$(a_n + b_n\epsilon)\sum_{-\infty}^{-1} z_{j+m}\epsilon^j + (a_n + b_n\epsilon^{-1})\eta_m$$

$$= (a_n + b_n\epsilon)\sum_{-m}^{-1} z_{j+m}\epsilon^j + (a_n + b_n\epsilon^{-1})\sum_{-m}^{-1} z_{j+m}\epsilon^{-j}.$$

Das ist ganzzahlig, nachdem a_n und b_n ganzzahlig sind und ϵ und ϵ^{-1} konjugiert ganzalgebraisch sind.
Nachdem die z_j beschränkt sind, kann man ganze Zahlen P, Q und R, mit beliebiger Größe, finden, sodass $P < P + 2Q < P + R + 2Q$ und $z_{P+Q} = z_{P+R+q}$ für $0 \leq q \leq 2Q$. Nun definiert man eine neue Folge z_n^* durch

$$z_n^* = z_n$$

falls $P \leq n \leq P + R + 2Q$

$$z_n^* = z_{n+R}\ (\forall n)$$

und setzt

$$\zeta_m^* = \sum_0^\infty z_{j+m}^* \epsilon^j,\ \eta_m^* = \sum_{-\infty}^{-1} z_{j+m}^* \epsilon^j,$$

$$\zeta^* = \zeta_0^*,\ \eta^* = \eta_0^*,$$

$$\sigma_{mn} = \epsilon^{-m}(a_n + b_n\epsilon)\zeta^* - \epsilon^m(a_n + b_n\epsilon^{-1})\eta^*$$

für $-\infty < m < +\infty$ $(0 \le n < N)$. Anschließend beweist man , dass

$$\|\sigma_{mn}\| \ge \frac{k-2}{2(k-1)} - e$$

für alle m,n gilt, wobei e eine positive Konstante ist, die nur von $\lambda_0, \lambda_1, \ldots, \lambda_{N-1}, \zeta, \epsilon, Q$ abhängt und gegen 0 strebt, wenn $Q \to \infty$. Nach dem Argument von oben, ist der Bruchteil von σ_{mn} derselbe wie der von

$$p_{mn}^* = (a_n + b_n\epsilon)\zeta_m^* - (a_n + b_n\epsilon^{-1})\eta_m^*.$$

Nun ist p_{mn}^* in m mod R periodisch, weil z_m^* periodisch ist und ebenso ζ_m^* und η_m^*. Daher muss man nur zeigen, dass

$$\|p_{mn}^*\| \ge \frac{k-2}{2(k-1)} - e,$$

für

$$P + Q \le m \le P + R + Q.$$

Dann aber ist $\|p_{mn}\| \ge \frac{k-2}{2(k-1)}$ nach (15), und

$$|p_{mn} - p_{mn}^*| \le |a_n + b_n\epsilon||\zeta_m^* - \zeta_m| + |a_n + b_n\epsilon^{-1}||\eta_m^* - \eta_m|,$$

wobei

$$|\zeta_m^* - \zeta_m| = |\sum_{j=0}^\infty (z_{j+m}^* - z_{j+m})\epsilon^j| = |\sum_Q^\infty (z_{j+m}^* - z_{j+m})\epsilon^j|$$

$$\le \epsilon^{-1} \sum_Q^\infty \epsilon^j = \frac{\epsilon^{Q-1}}{1-\epsilon},$$

und

$$|\eta_m^* - \eta_m| \le \frac{\epsilon^{Q-1}}{1-\epsilon} + \epsilon|z_0|,$$

Nachdem beide gegen 0 streben, wenn $Q \to \infty$, beweist dies das Resultat.
Nun definiert man x_0, y_0 durch

$$x_0 + y_0\phi = c\zeta^*,\ x_0 + y_0\theta = -c\eta^*.$$

Dann hat man für alle n und passende m_1, n_1

$$\|\frac{(u_n - v_n\theta)(x_0 - y_0\phi) - (u_n - v_n\phi)(x_0 - y_0\theta)}{\theta - \phi}\| = \|\sigma_{m_1 n_1}\| \geq \frac{k-2}{2(k-1)} - e,$$

wie verlangt. Weiters ist

$$\zeta^* = (z_0^* + z_1^*\epsilon + \ldots + z_{R-1}\epsilon^{R-1})(1 + \epsilon^R + \epsilon^{2R} + \ldots) = \frac{z_0^* + \ldots z_{R-1}^*\epsilon^{R-1}}{1 - \epsilon^R}$$

$$\eta^* = \frac{z_{-1}^* + \ldots + z_{-R}\epsilon^R}{1 - \epsilon^R} = -\frac{z_0^* + \ldots + z_{R-1}^*\epsilon^{-R+1}}{1 - \epsilon^{-R}}.$$

Demnach sind ζ^* und $-\eta^*$ konjugierte algebraische Zahlen, weil ϵ und ϵ^{-1} solche sind, daher sind x_0 und y_0 rational, wie behauptet. □

3. Normeuklidische Ringe

In diesem Kapitel folge ich der Arbeit von Cioffari [3].

Bemerkung 3.1
Das nächste Ziel ist zu zeigen, dass $\mathbb{Q}(\sqrt[3]{n})$ für nur gewisse n normeuklidisch ist.

Definition 3.2
Ein algebraischer Zahlkörper ist normeuklidisch, wenn sein Ganzheitsring O_K folgende Eigenschaft erfüllt:

- Für $a, b \in O_K$ mit $b \neq 0$ $\exists p, r \in O_K$, sodass $a = bp + r$ mit $r = 0$ oder $|N(r)| < |N(b)|$.

Bemerkung 3.3
Jeder rein kubische Zahlkörper hat eine reelle Einbettung und ein Paar komplex konjugierter Einbettungen und daher eine Fundamentaleinheit sowie eine negative Diskriminate.

Bemerkung 3.4
Man kann zeigen, dass ein rein kubischer Zahlkörper mit Diskriminante $-D > 420^2 = 176400$ nicht reinkubisch sein kann.

Satz 3.5 (Cassels)
Sei K ein reinkubischer Zahlkörper. Dann ist K nicht reinkubisch für $D < -(420)^2 = -176400$

Beweis. Folgt aus Satz 2.2. □

Bemerkung 3.6
Einige Notationen, welche ab jetzt verwendet werden:

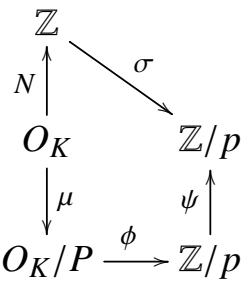
- ϵ: Fundamentaleinheit von $\mathbb{Q}(\sqrt[3]{d})$
- $\theta = (\sqrt[3]{d})$
- (b): Das Ideal bO_K mit $b \in \mathbb{Q}(\sqrt[3]{d})$
- $N(b)$: Die Norm von $b \in \mathbb{Q}(\sqrt[3]{d})$
- $N(P)$: Die Norm von P, wobei P Ideal in $\mathbb{Q}(\sqrt[3]{d})$ ist
- $\overline{b}(c)$: Restklasse von b mod c, mit $b, c \in O_K$

Bemerkung 3.7
$\mathrm{N}(a + b\sqrt[3]{d} + c\sqrt[3]{d^2}) = a^3 + b^3 d + c^3 d^2 - 3abcd$

Bemerkung 3.8
Man erarbeitet jetzt ein Kriterium um zu bestimmen wann ein algebraischer Zahlkörper K Klassenzahl $h(K) = 1$ hat. Dieses Kriterium ist notwendig für die euklidische Eigenschaft.

Definition 3.9
Unter einer verzweigten Primzahl versteht man eine Primzahl, welche sich in, sich wiederholenden Primideale faktorisieren lässt.

Satz 3.10
Sei K ein Körper vom Grad einer ungeraden Primzahl q. Sei p ein Primzahl, die total verzweigt in K ist, und $p \not\equiv 1 \pmod{q}$ und $(p) = P^q$ die Primidealzerlegungen von (P). Sei $u \in O_K$, der Ganzheitsring von K.
Dann gilt $u \equiv b \pmod{P}$, wobei b die eindeutige ganze Zahl in $\{0, 1, \ldots, p-1\}$ ist, sodass $b^q \equiv N(u) \pmod{p}$.



Beweis. In diesem Diagramm sind σ und μ kanonische Abbildungen. N ist die Normabbildung. ϕ ist die Abbildung, die jeder Klasse in O_K/P eine eindeutige ganze Zahl mod p zuordnet, die zu dieser Klasse gehört. ψ ist die Abbildung, die jedem Element seine q-te Potenz zuordnet.
Alle Abbildungen sind multiplikative Homomorphismen und ϕ und ψ sind Isomorphismen.
Um die Kommutativität dieses Diagramms zu zeigen sei $u \equiv c \pmod{P}$, mit $c \in \{0, 1, \ldots, p-1\}$. Somit ist $u - c \in P$, und so folgt nach dem Eisensteinkriterium, dass das charakteristische Polynom von $u - c$ die Form

$$x^q + d_{q-1}x^{q-1} + \ldots + d_1 x + d_0 \; mit \; p \mid d_i \forall i$$

hat. Daher ist u Nullstelle des Polynoms

$$(x-c)^q + d_{q-1}(x-c)^{q-1} + \ldots + d_1(x-c) + d_0,$$

und so gilt $N(u) \equiv c^q \pmod{p}$. □

Bemerkung 3.11
Der folgende Satz wird später dazu verwendet um zu zeigen, dass bestimmte Körper nicht euklidisch sind.

Satz 3.12
Sei $K = \mathbb{Q}(\sqrt[q]{r})$, wobei q eine ungerade Primzahl ist und r frei von q-ten Potenzen. Falls r durch eine Primzahl kongruent zu 1 mod q teilbar ist, dann $q \mid h(K)$.

Beweis. Folgt aus Satz 3.10. □

Satz 3.13
Sei K ein Körper vom Primzahlgrad q mit r Fundamentaleinheiten. Sind mindestens r+2 Primzahlen total verzweigt in K, dann $q \mid h(K)$

Beweis. Seien $\epsilon_1, \ldots, \epsilon_r$ die Fundamentaleinheiten und seien $p_1, \ldots, p_{r+2}$ total verzweigte Primzahlen und sei $(p_i) = P_i^q$ deren Primidealfaktorisierung. Falls q total verzweigt, sei $p_1 = q$
Angenommen: $h = 1$
Dann folgt $\forall i\ \exists b \in O_K$, sodass $(b_i) = P_i$ und

$$b_i^q = p_i \epsilon_1^{k_{i1}} \ldots \epsilon_r^{k_{ir}}\ i = 1, \ldots, r+2,\ k_{ij} \in \mathbb{Z}.$$

Man kann folgern, dass es gewisse ganze Zahlen s gibt, die durch keine q-te Potenz, und durch einige p_i teilbar sind, aber nicht durch p_{r+2}, eine q-te Potenz in K sind. Daraus folgt $K = \mathbb{Q}(\sqrt[q]{s})$
Das ist ein Widerspruch und daher ist $h \neq 1$. Daraus kann man folgern, dass $q \mid h$ □

Bemerkung 3.14
Es gibt insgesamt 42 Körper, die unter Cassels Schranke fallen und nicht durch die beiden vorigen Sätze ausgeschlossen werden.

Bemerkung 3.15
Von diesen 42 Körpern haben die folgenden 31 Körper Klassenzahl 1: $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{3}), \mathbb{Q}(\sqrt[3]{5}), \mathbb{Q}(\sqrt[3]{6}), \mathbb{Q}(\sqrt[3]{10})$, $\mathbb{Q}(\sqrt[3]{12}), \mathbb{Q}(\sqrt[3]{17}), \mathbb{Q}(\sqrt[3]{23}), \mathbb{Q}(\sqrt[3]{29}), \mathbb{Q}(\sqrt[3]{33}), \mathbb{Q}(\sqrt[3]{41}), \mathbb{Q}(\sqrt[3]{44})$, $\mathbb{Q}(\sqrt[3]{45}), \mathbb{Q}(\sqrt[3]{46}), \mathbb{Q}(\sqrt[3]{53}), \mathbb{Q}(\sqrt[3]{55}), \mathbb{Q}(\sqrt[3]{59}), \mathbb{Q}(\sqrt[3]{69}), \mathbb{Q}(\sqrt[3]{71})$, $\mathbb{Q}(\sqrt[3]{82}), \mathbb{Q}(\sqrt[3]{99}), \mathbb{Q}(\sqrt[3]{107}), \mathbb{Q}(\sqrt[3]{116}), \mathbb{Q}(\sqrt[3]{145}), \mathbb{Q}(\sqrt[3]{179})$, $\mathbb{Q}(\sqrt[3]{188}), \mathbb{Q}(\sqrt[3]{197}), \mathbb{Q}(\sqrt[3]{226}), \mathbb{Q}(\sqrt[3]{332}), \mathbb{Q}(\sqrt[3]{404})$ und $\mathbb{Q}(\sqrt[3]{575})$.

Bemerkung 3.16
Sei $\mathbb{Q}(\sqrt[3]{d})$, dann hat d immer eine der folgenden Darstellungen

- $d = p$ mit p Primzahl,
- $d = p_1 p_2$ mit p_1 und p_2 Primzahlen
- $d = p_1 p_2^2$ mit $p_1 > p_2$

Bemerkung 3.17
Jede Primzahl welche d teilt ist total verzweigt. Die Diskriminante zeigt, dass $(3) = P^3$, wenn $d \not\equiv \pm 1 \pmod 9$ und $(3) = P_1^2 P_2$, wenn $d \equiv \pm 1 \pmod 9$
Alle anderen Primzahlen sind unverzweigt. Für den Fall $p \equiv 2 \pmod 3$ verwendet man das Lemma von Hensel.

4. Eigenschaften der in Frage kommenden Ringe

In diesem Kapitel folge ich den Büchern von Alaca & Williams [1] und Narciewicz [7] .

Bemerkung 4.1
In diesem Kapitel werden Diskriminante und Ganzheitsbasis aller in Frage kommender Ringe bestimmt. Zusätzlich wird explizit gezeigt, dass $\mathbb{Q}(\sqrt[3]{2})$ Klassenzahl 1 hat.

Satz 4.2
Sei $K = \mathbb{Q}(\sqrt[3]{2})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{2})) = -108$ und $(1, \sqrt[3]{2}, \sqrt[3]{4})$ Ganzheitsbasis.

Beweis. $2 \not\equiv \pm 1 \pmod 9$ und $2 = 1^2 \cdot 2$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{2})) = -27 \cdot 1^2 \cdot 2^2 = -108$

$\rightarrow (1, \sqrt[3]{2}, \sqrt[3]{4})$ ist Ganzheitsbasis. □

Satz 4.3
Sei $K = \mathbb{Q}(\sqrt[3]{3})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{3})) = -243$ und $(1, \sqrt[3]{3}, \sqrt[3]{9})$ Ganzheitsbasis.

Beweis. $3 \not\equiv \pm 1 \pmod 9$ und $3 = 1^2 \cdot 3$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{3})) = -27 \cdot 1^2 \cdot 3^2 = -243$

$\rightarrow (1, \sqrt[3]{3}, \sqrt[3]{9})$ ist Ganzheitsbasis. □

Satz 4.4
Sei $K = \mathbb{Q}(\sqrt[3]{5})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{5})) = -675$ und $(1, \sqrt[3]{5}, \sqrt[3]{25})$ Ganzheitsbasis.

Beweis. $5 \not\equiv \pm 1 \pmod 9$ und $5 = 1^2 \cdot 5$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{5})) = -27 \cdot 1^2 \cdot 5^2 = -675$

$\rightarrow (1, \sqrt[3]{5}, \sqrt[3]{25})$ ist Ganzheitsbasis. □

Satz 4.5
Sei $K = \mathbb{Q}(\sqrt[3]{6})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{6})) = -972$ und $(1, \sqrt[3]{6}, \sqrt[3]{36})$ Ganzheitsbasis.

Beweis. $6 \not\equiv \pm 1 \pmod 9$ und $6 = 1^2 \cdot 6$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{6})) = -27 \cdot 1^2 \cdot 6^2 = -972$

$\rightarrow (1, \sqrt[3]{6}, \sqrt[3]{36})$ ist Ganzheitsbasis. □

Satz 4.6
Sei $K = \mathbb{Q}(\sqrt[3]{10})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{10})) = -300$ und $(\sqrt[3]{10}, \sqrt[3]{100}, \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3})$ Ganzheitsbasis.

Beweis. $10 \equiv 1 \pmod 9$ und $10 = 1^2 \cdot 10$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{10})) = -3 \cdot 1^2 \cdot 10^2 = -300$

$\rightarrow (\sqrt[3]{10}, \sqrt[3]{100}, \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3})$ ist Ganzheitsbasis. □

Satz 4.7
Sei $K = \mathbb{Q}(\sqrt[3]{12})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{12})) = -972$ und $(1, \sqrt[3]{12}, \frac{\sqrt[3]{144}}{2})$ Ganzheitsbasis.

Beweis. $12 \not\equiv \pm 1 \pmod 9$ und $12 = 2^2 \cdot 3$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{12})) = -27 \cdot 2^2 \cdot 3^2 = -972$

$\rightarrow (1, \sqrt[3]{12}, \frac{\sqrt[3]{144}}{2})$ ist Ganzheitsbasis. □

Satz 4.8
Sei $K = \mathbb{Q}(\sqrt[3]{17})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{17})) = -867$ und $(\sqrt[3]{17}, \sqrt[3]{289}, \frac{1-\sqrt[3]{17}+\sqrt[3]{289}}{3})$ Ganzheitsbasis.

Beweis. $17 \equiv -1 \pmod 9$ und $17 = 1^2 \cdot 17$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{17})) = -3 \cdot 1^2 \cdot 17^2 = -867$

$\rightarrow (\sqrt[3]{17}, \sqrt[3]{289}, \frac{1-\sqrt[3]{17}+\sqrt[3]{289}}{3})$ ist Ganzheitsbasis. □

Satz 4.9
Sei $K = \mathbb{Q}(\sqrt[3]{23})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{23})) = -14283$ und $(1, \sqrt[3]{23}, \sqrt[3]{529})$ Ganzheitsbasis.

Beweis. $23 \not\equiv \pm 1 \pmod 9$ und $23 = 1^2 \cdot 23$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{23})) = -27 \cdot 1^2 \cdot 23^2 = -14283$

$\rightarrow (1, \sqrt[3]{23}, \sqrt[3]{529})$ ist Ganzheitsbasis. □

Satz 4.10
Sei $K = \mathbb{Q}(\sqrt[3]{29})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{29})) = -22707$ und $(1, \sqrt[3]{29}, \sqrt[3]{841})$ Ganzheitsbasis.

Beweis. $29 \not\equiv \pm 1 \pmod 9$ und $29 = 1^2 \cdot 29$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{29})) = -27 \cdot 1^2 \cdot 29^2 = -22707$

$\rightarrow (1, \sqrt[3]{29}, \sqrt[3]{841})$ ist Ganzheitsbasis. □

Satz 4.11
Sei $K = \mathbb{Q}(\sqrt[3]{33})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{33})) = -29403$ und $(1, \sqrt[3]{33}, \sqrt[3]{1089})$ Ganzheitsbasis.

Beweis. $33 \not\equiv \pm 1 \pmod 9$ und $33 = 1^2 \cdot 33$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{33})) = -27 \cdot 1^2 \cdot 33^2 = -29403$

$\rightarrow (1, \sqrt[3]{33}, \sqrt[3]{1089})$ ist Ganzheitsbasis. □

Satz 4.12
Sei $K = \mathbb{Q}(\sqrt[3]{41})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{41})) = -45387$ und $(1, \sqrt[3]{41}, \sqrt[3]{1681})$ Ganzheitsbasis.

Beweis. $41 \not\equiv \pm 1 \pmod 9$ und $41 = 1^2 \cdot 41$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{41})) = -27 \cdot 1^2 \cdot 41^2 = -45387$

$\rightarrow (1, \sqrt[3]{41}, \sqrt[3]{1681})$ ist Ganzheitsbasis. □

Satz 4.13
Sei $K = \mathbb{Q}(\sqrt[3]{44})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{44})) = -1452$ und $(\sqrt[3]{44}, \frac{\sqrt[3]{1936}}{2}, \frac{1-\sqrt[3]{44}+\sqrt[3]{1936}}{3})$ Ganzheitsbasis.

Beweis. $44 \equiv -1 \pmod 9$ und $44 = 2^2 \cdot 11$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{44})) = -3 \cdot 2^2 \cdot 11^2 = -1452$

$\rightarrow (\sqrt[3]{44}, \frac{\sqrt[3]{1936}}{2}, \frac{1-\sqrt[3]{44}+\sqrt[3]{1936}}{3})$ ist Ganzheitsbasis. □

Satz 4.14
Sei $K = \mathbb{Q}(\sqrt[3]{45})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{45})) = -6075$ und $(1, \sqrt[3]{45}, \frac{\sqrt[3]{2025}}{3})$ Ganzheitsbasis.

Beweis. $45 \not\equiv \pm 1 \pmod 9$ und $45 = 3^2 \cdot 5$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{45})) = -27 \cdot 3^2 \cdot 5^2 = -6075$

$\rightarrow (1, \sqrt[3]{45}, \frac{\sqrt[3]{2025}}{3})$ ist Ganzheitsbasis. □

Satz 4.15
Sei $K = \mathbb{Q}(\sqrt[3]{46})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{46})) = -6348$ und $(\sqrt[3]{46}, \sqrt[3]{2116}, \frac{1+\sqrt[3]{46}+\sqrt[3]{2116}}{3})$ Ganzheitsbasis.

Beweis. $46 \equiv 1 \pmod 9$ und $46 = 1^2 \cdot 46$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{46})) = -3 \cdot 1^2 \cdot 46^2 = -6348$

$\rightarrow (\sqrt[3]{46}, \sqrt[3]{2116}, \frac{1+\sqrt[3]{46}+\sqrt[3]{2116}}{3})$ ist Ganzheitsbasis. □

Satz 4.16
Sei $K = \mathbb{Q}(\sqrt[3]{53})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{53})) = -8427$ und $(\sqrt[3]{53}, \sqrt[3]{2809}, \frac{1-\sqrt[3]{53}+\sqrt[3]{2809}}{3})$ Ganzheitsbasis.

Beweis. $53 \equiv -1 \pmod 9$ und $53 = 1^2 \cdot 53$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{53})) = -3 \cdot 1^2 \cdot 53^2 = -8427$

$\rightarrow (\sqrt[3]{53}, \sqrt[3]{2809}, \frac{1-\sqrt[3]{53}+\sqrt[3]{2809}}{3})$ ist Ganzheitsbasis. □

Satz 4.17
Sei $K = \mathbb{Q}(\sqrt[3]{55})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{55})) = -9075$ und
$(\sqrt[3]{55}, \sqrt[3]{3025}, \frac{1+\sqrt[3]{55}+\sqrt[3]{3025}}{3})$ Ganzheitsbasis.

Beweis. $55 \equiv 1 \pmod 9$ und $55 = 1^2 \cdot 55$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{55})) = -3 \cdot 1^2 \cdot 55^2 = -9075$

$\rightarrow (\sqrt[3]{55}, \sqrt[3]{3025}, \frac{1+\sqrt[3]{55}+\sqrt[3]{3025}}{3})$ ist Ganzheitsbasis. □

Satz 4.18
Sei $K = \mathbb{Q}(\sqrt[3]{59})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{59})) = -93987$ und
$(1, \sqrt[3]{59}, \sqrt[3]{3481})$ Ganzheitsbasis.

Beweis. $59 \not\equiv \pm 1 \pmod 9$ und $59 = 1^2 \cdot 59$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{59})) = -27 \cdot 1^2 \cdot 59^2 = -93987$

$\rightarrow (1, \sqrt[3]{59}, \sqrt[3]{3481})$ ist Ganzheitsbasis. □

Satz 4.19
Sei $K = \mathbb{Q}(\sqrt[3]{69})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{69})) = -128547$ und
$(1, \sqrt[3]{69}, \sqrt[3]{4761})$ Ganzheitsbasis.

Beweis. $69 \not\equiv \pm 1 \pmod 9$ und $69 = 1^2 \cdot 69$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{69})) = -27 \cdot 1^2 \cdot 69^2 = -128547$

$\rightarrow (1, \sqrt[3]{69}, \sqrt[3]{4761})$ ist Ganzheitsbasis. □

Satz 4.20
Sei $K = \mathbb{Q}(\sqrt[3]{71})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{71})) = -15123$ und
$(\sqrt[3]{71}, \sqrt[3]{5041}, \frac{1-\sqrt[3]{71}+\sqrt[3]{5041}}{3})$ Ganzheitsbasis.

Beweis. $71 \equiv -1 \pmod 9$ und $71 = 1^2 \cdot 71$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{71})) = -3 \cdot 1^2 \cdot 71^2 = -15123$

$\rightarrow (\sqrt[3]{71}, \sqrt[3]{5041}, \frac{1-\sqrt[3]{71}+\sqrt[3]{5041}}{3})$ ist Ganzheitsbasis. □

Satz 4.21
Sei $K = \mathbb{Q}(\sqrt[3]{82})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{82})) = -20172$ und
$(\sqrt[3]{82}, \sqrt[3]{6724}, \frac{1+\sqrt[3]{82}+\sqrt[3]{6724}}{3})$ Ganzheitsbasis.

Beweis. $82 \equiv 1 \pmod 9$ und $82 = 1^2 \cdot 82$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{82})) = -3 \cdot 1^2 \cdot 82^2 = -20172$

$\rightarrow (\sqrt[3]{82}, \sqrt[3]{6724}, \frac{1+\sqrt[3]{82}+\sqrt[3]{6724}}{3})$ ist Ganzheitsbasis. □

Satz 4.22
Sei $K = \mathbb{Q}(\sqrt[3]{99})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{99})) = -3267$ und
$(1, \sqrt[3]{99}, \frac{\sqrt[3]{9801}}{3})$ Ganzheitsbasis.

Beweis. $99 \equiv \pm 1 \pmod 9$ und $99 = 3^2 \cdot 11$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{99})) = -3 \cdot 3^2 \cdot 11^2 = -3267$

$\rightarrow (1, \sqrt[3]{99}, \frac{\sqrt[3]{9801}}{3})$ ist Ganzheitsbasis. □

Satz 4.23
Sei $K = \mathbb{Q}(\sqrt[3]{107})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{107})) = -34347$ und
$(\sqrt[3]{107}, \sqrt[3]{11449}, \frac{1-\sqrt[3]{107}+\sqrt[3]{11449}}{3})$ Ganzheitsbasis.

Beweis. $107 \equiv -1 \pmod 9$ und $107 = 1^2 \cdot 107$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{107})) = -3 \cdot 1^2 \cdot 107^2 = -34347$

$\rightarrow (\sqrt[3]{107}, \sqrt[3]{11449}, \frac{1-\sqrt[3]{107}+\sqrt[3]{11449}}{3})$ ist Ganzheitsbasis. □

Satz 4.24
Sei $K = \mathbb{Q}(\sqrt[3]{116})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{116})) = -10092$ und
$(\sqrt[3]{116}, \frac{\sqrt[3]{13456}}{2}, \frac{1-\sqrt[3]{116}+\sqrt[3]{13456}}{3})$ Ganzheitsbasis.

Beweis. $116 \equiv -1 \pmod 9$ und $116 = 2^2 \cdot 29$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{116})) = -3 \cdot 2^2 \cdot 29^2 = -10092$

$\rightarrow (\sqrt[3]{116}, \frac{\sqrt[3]{13456}}{2}, \frac{1-\sqrt[3]{116}+\sqrt[3]{13456}}{3})$ ist Ganzheitsbasis. □

Satz 4.25
Sei $K = \mathbb{Q}(\sqrt[3]{145})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{145})) = -63075$ und $(\sqrt[3]{145}, \sqrt[3]{21025}, \frac{1+\sqrt[3]{145}+\sqrt[3]{21025}}{3})$ Ganzheitsbasis.

Beweis. $145 \equiv 1 \pmod 9$ und $145 = 1^2 \cdot 145$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{145})) = -3 \cdot 1^2 \cdot 145^2 = -63075$

$\rightarrow (\sqrt[3]{145}, \sqrt[3]{21025}, \frac{1+\sqrt[3]{145}+\sqrt[3]{21025}}{3})$ ist Ganzheitsbasis. □

Satz 4.26
Sei $K = \mathbb{Q}(\sqrt[3]{179})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{179})) = -96123$ und $(\sqrt[3]{179}, \sqrt[3]{32041}, \frac{1-\sqrt[3]{179}+\sqrt[3]{32041}}{3})$ Ganzheitsbasis.

Beweis. $179 \equiv -1 \pmod 9$ und $179 = 1^2 \cdot 179$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{179})) = -3 \cdot 1^2 \cdot 179^2 = -96123$

$\rightarrow (\sqrt[3]{179}, \sqrt[3]{32041}, \frac{1-\sqrt[3]{179}+\sqrt[3]{32041}}{3})$ ist Ganzheitsbasis. □

Satz 4.27
Sei $K = \mathbb{Q}(\sqrt[3]{188})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{188})) = -26508$ und $(\sqrt[3]{188}, \frac{\sqrt[3]{35344}}{2}, \frac{1-\sqrt[3]{188}+\sqrt[3]{35344}}{3})$ Ganzheitsbasis.

Beweis. $188 \equiv -1 \pmod 9$ und $188 = 2^2 \cdot 47$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{188})) = -3 \cdot 2^2 \cdot 47^2 = -26508$

$\rightarrow (\sqrt[3]{188}, \frac{\sqrt[3]{35344}}{2}, \frac{1-\sqrt[3]{188}+\sqrt[3]{35344}}{3})$ ist Ganzheitsbasis. □

Satz 4.28
Sei $K = \mathbb{Q}(\sqrt[3]{197})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{197})) = -116427$ und $(\sqrt[3]{197}, \sqrt[3]{38809}, \frac{1-\sqrt[3]{197}+\sqrt[3]{38809}}{3})$ ist Ganzheitsbasis.

Beweis. $197 \equiv -1 \pmod 9$ und $197 = 1^2 \cdot 197$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{197})) = -3 \cdot 1^2 \cdot 197^2 = -116427$

$\rightarrow (\sqrt[3]{197}, \sqrt[3]{38809}, \frac{1-\sqrt[3]{197}+\sqrt[3]{38809}}{3})$ ist Ganzheitsbasis. □

Satz 4.29
Sei $K = \mathbb{Q}(\sqrt[3]{226})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{226})) = -153228$ und $(\sqrt[3]{226}, \sqrt[3]{51076}, \frac{1+\sqrt[3]{226}+\sqrt[3]{51076}}{3})$ Ganzheitsbasis.

Beweis. $226 \equiv 1 \pmod 9$ und $226 = 1^2 \cdot 226$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{226})) = -3 \cdot 1^2 \cdot 226^2 = -153228$

$\rightarrow (\sqrt[3]{226}, \sqrt[3]{51076}, \frac{1+\sqrt[3]{226}+\sqrt[3]{51076}}{3})$ ist Ganzheitsbasis. □

Satz 4.30
Sei $K = \mathbb{Q}(\sqrt[3]{332})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{332})) = -82668$ und $(\sqrt[3]{332}, \frac{\sqrt[3]{110224}}{2}, \frac{1-\sqrt[3]{332}+\sqrt[3]{110224}}{3})$ Ganzheitsbasis.

Beweis. $332 \equiv -1 \pmod 9$ und $332 = 2^2 \cdot 83$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{332})) = -3 \cdot 2^2 \cdot 83^2 = -82668$

$\rightarrow (\sqrt[3]{332}, \frac{\sqrt[3]{110224}}{2}, \frac{1-\sqrt[3]{332}+\sqrt[3]{110224}}{3})$ ist Ganzheitsbasis. □

Satz 4.31
Sei $K = \mathbb{Q}(\sqrt[3]{404})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{404})) = -122412$ und $(\sqrt[3]{404}, \frac{\sqrt[3]{163216}}{2}, \frac{1-\sqrt[3]{404}+\sqrt[3]{163216}}{3})$ Ganzheitsbasis.

Beweis. $404 \equiv -1 \pmod 9$ und $404 = 2^2 \cdot 101$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{404})) = -3 \cdot 2^2 \cdot 101^2 = -122412$

$\rightarrow (\sqrt[3]{404}, \frac{\sqrt[3]{163216}}{2}, \frac{1-\sqrt[3]{404}+\sqrt[3]{163216}}{3})$ ist Ganzheitsbasis. □

Satz 4.32
Sei $K = (\mathbb{Q}\sqrt[3]{575})$. Dann ist $d(\mathbb{Q}(\sqrt[3]{575})) = -39625$ und $(\sqrt[3]{575}, \frac{\sqrt[3]{330625}}{5}, \frac{1-\sqrt[3]{575}+\sqrt[3]{330625}}{3})$ Ganzheitsbasis.

Beweis. $575 \equiv -1 \pmod 9$ und $575 = 5^2 \cdot 23$

$\rightarrow d(\mathbb{Q}(\sqrt[3]{575})) = -3 \cdot 5^2 \cdot 23^2 = -39625$

$\rightarrow (\sqrt[3]{575}, \frac{\sqrt[3]{330625}}{5}, \frac{1-\sqrt[3]{575}+\sqrt[3]{330625}}{3})$ ist Ganzheitsbasis. □

Bemerkung 4.33
Um die Klassenzahlen berechnen zu können benötigt man noch das Resultat des folgenden Satzes.

Satz 4.34
Sei $K = \mathbb{Q}(\theta)$ ein algebraische Zahlkörper vom Grad n, sodass

$$O_K = \mathbb{Z} + \mathbb{Z}\theta + \ldots + \mathbb{Z}\theta^{n-1}.$$

Sei p eine Primzahl und sei f das Minimalpolynom von θ über $\mathbb{Q}$ in $Z[x]$. Sei $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $f \to \overline{f}$ die natürliche Abbildung wobei $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Sei

$$\overline{f}(x) = g_1(x)^{e_1} \ldots \; g_r(x)^{e_r},$$

wobei $g_1(x), \ldots, g_r(x)$ paarweise verschiedene normierte irreduzible Polynome in $\mathbb{Z}_p[x]$ und $e_1, \ldots, e_r$ positive ganze Zahlen sind. Für $i = 1, 2 \ldots, r$ seinen $f_i(x)$ normierte Polynome in $\mathbb{Z}[x]$, sodass $\overline{f}_i = g_i$. Sei

$$P_i = (p, f_i(\theta)),\ i = 1, 2, \ldots, r.$$

Dann sind $P_1, \ldots, P_r$ paarweise verschiedene Primideale von O_K mit

$$(p) = P_1^{e_1} \ldots P_r^{e_r}$$

und

$$N(P_i) = p^{deg\ f_i},\ i = 1, 2, \ldots, r.$$

Beweis. Für $i = 1, 2, \ldots, r$ sei θ_i eine Nullstelle von g_i in einem passenden Erweiterungskörper von $\mathbb{Z}_p$. Dieser Erweiterungskörper ist der endliche Körper $\mathbb{Z}_p[\theta_i] \simeq \mathbb{Z}_p[x]/(g_i(x))$. Sei $v_i \colon \mathbb{Z}[\theta] \to \mathbb{Z}_p[\theta_i]$ der surjektive Homomorphismus, gegeben durch

$$v_i(h(\theta)) = \overline{h}(\theta_i).$$

Dann ist

$$\mathbb{Z}[\theta]/ker\ v_i \simeq v_i(\mathbb{Z}[\theta]) = \mathbb{Z}_p[\theta_i]$$

ein Körper, sodass $ker\ v_i$ ein Primideal von $\mathbb{Z}[\theta] = O_K$ ist. Es gilt

$$v_i(p) = 0, v_i(f_i(\theta)) = \overline{f_i}(\theta_i) = g_i(\theta_i) = 0,$$

sodass

$$p \in ker\ v_i, f_i(\theta) \in ker\ v_i,$$

und daher

$$(p, f_i(\theta)) \subseteq ker\ v_i.$$

Falls $g(\theta) \in ker\ v_i$, ist

$$\overline{g}(\theta_i) = v_i(g(\theta)) = 0,$$

sodass $g_i(x) \mid \overline{g}(x)$ in $\mathbb{Z}_p[x]$. Daher

$$\overline{g}(x) = \overline{f_i}(x)\overline{h}(x),$$

für ein $\overline{h} \in \mathbb{Z}_p[x]$. Daher hat $(g - f_i h)(x) \in \mathbb{Z}[x]$ Koeffizienten, die durch p teilbar sind, sodass

$$\begin{aligned} g(\theta) &= (g(\theta) - f_i(\theta)h(\theta)) + f_i(\theta)h(\theta) \\ &\in (p, f_i(\theta)) \\ g &= (p, f_i(\theta)), \end{aligned}$$

was beweist, dass

$$ker\ v_i \subseteq (p, f_i(\theta)).$$

Man hat jetzt gezeigt, dass

$$P_i = (p, f_i(\theta)) = ker\ v_i,\ i = 1, 2, \ldots, r.$$

Daher ist jedes P_i $(i = 1, 2, \ldots, r)$ ein Primideal von O_K.
Als nächstes zeigt man, dass die Primideale P_i $(i = 1, 2, \ldots, r)$ verschieden sind. Angenommen $P_i = P_j$ für gewisse $i, j \in \{1, 2, \ldots, r\}$. Dann $(p, f_i(\theta)) = (p, f_j(\theta))$. Deshalb ist

$$f_j(\theta) = pg(\theta) + f_i(\theta)h(\theta)$$

für gewisse $g(x), h(x) \in \mathbb{Z}[x]$. Wendet man v_i an, erhält man

$$g_j(\theta_i) = \overline{f}_j(\theta_i) = \overline{f}_i(\theta_i)\overline{h}(\theta_i) = g_i(\theta_i)\overline{h}(\theta_i) = 0,$$

sodass $g_i(x) \mid g_j(x)$ in $\mathbb{Z}_p[x]$. Daher ist

$$g_j(x) = g_i(x) = g_i(x)l(x)$$

für ein $l(x) \in \mathbb{Z}_p[x]$. Nachdem $g_i(x)$ und $g_j(x)$ beide normierte Polynome sind, welche irreduzibel in $\mathbb{Z}_p[x]$ sind, hat man $l(x) =$

1, sodass $g_i(x) = g_j(x)$ und daher $i = j$. Anschließend zeigt man, dass

$$(p) = P_1^{e_1} \dots P_r^{e_r}.$$

Für alle Ideale A, B_1, B_2 gilt

$$(A + B_1)(A + B_2) \subseteq A + B_1 B_2,$$

sodass

$$\begin{aligned} P_1^{e_1} \dots P_r^{e_r} &= (p, f_1(\theta))^{e_1} \dots (p, f_r(\theta))^{e_r} \\ &= ((p) + (f_1(\theta)))^{e_1} \dots ((p) + (f_r(\theta)))^{e_r} \\ &\subseteq (p) + (f_1(\theta))^{e_1} \dots (f_r(\theta)))^{e_r} \\ &= (p) + (f_1(\theta)^{e_1} \dots f_r(\theta)^{e_r}) \\ &= (p) + (f(\theta)) \\ &= (p) \end{aligned}$$

sodass

$$(p) \mid P_1^{e_1} \dots P_r^{e_r}.$$

Nun ist $P_i = (p, f_i(\theta)) \supseteq (p)$, sodass

$$P_i \mid (p),\ i = 1, 2, \dots, r.$$

Daher ist

$$(p) = P_1^{k_1} \dots P_r^{k_r},$$

mit

$$k_i \in \{1, 2, \dots, e_i\},\ i = 1, 2, \dots, r. \tag{17}$$

Nun ist

$$O_K / P_i = \mathbb{Z}[\theta]/P_i = \mathbb{Z}[\theta]/ker\ v_i \simeq v_i(\mathbb{Z}[\theta]) = \mathbb{Z}_p[\theta_i],$$

sodass

$$N(P_i) = card(O_K/P_i) = card(\mathbb{Z}_p[\theta_i]) = p^{d_i},$$

wobei

$$d_i = deg\ g_i = deg \overline{f_i}.$$

Daher hat man

$$\begin{aligned} p^n = N((p)) &= N(P_1^{k_1} \dots P_r^{k_r}) \\ &= N(P_1)^{k_1} \dots N(P_r)^{k_r} \\ &= (p^{d_1})^{k_1} \dots (p^{d_r})^{k_r} \\ &= p^{d_1 k_1 + \dots + d_r k_r}, \end{aligned}$$

sodass

$$d_1k_1 + \ldots + d_rk_r = n. \tag{18}$$

Vergleicht man die Grade bei

$$\overline{f}(x) = \overline{f_1}(x)^{e_1} \ldots \overline{f_r}(x)^{e_r},$$

so erhält man

$$d_1e_1 + \ldots + d_re_r = n. \tag{19}$$

Aus (17), (18) und (19) kann man folgern, dass

$$k_i = e_i,\ i = 1, 2, \ldots, r,$$

sodass

$$(p) = P_1^{e_1} \ldots P_r^{e_r},$$

wie angenommen. Zuletzt erkennt man, dass

$$N(P_i) = p^{d_i} = p^{deg\overline{f_i}} = p^{deg\ f_i}\ , i = 1, 2, \ldots, r$$

und der Satz ist bewiesen. □

Satz 4.35
Sei $K = \mathbb{Q}(\sqrt[3]{2})$, dann ist $H(K) = 1$.

Beweis. Sei $\theta = \sqrt[3]{2}$. Dann ist $x^3 - 2$ das Minimalpolynom von θ über $\mathbb{Q}$. Diese Gleichung hat genau eine reelle Nullstelle θ und zwei nichtreelle Nullstellen, $\omega\theta$ und $\omega^2\theta$, wobei ω eine komplexe dritte Einheitswurzel ist. Daher ist

$$r = 1, s = 1.$$

Bereits in Satz 4.2 wurde gezeigt, dass $(1, \theta, \theta^2)$ eine Ganzheitsbasis für K und $d(K) = -108$ ist.
Die Minkowskischranke ist daher

$$M_K = (\frac{2}{\pi})^s \sqrt{|d(K)|} = \frac{2}{\pi}\sqrt{108} < \frac{2}{3} \cdot \frac{21}{2} = 7.$$

Daher sind die Primzahlen $p \leq M_K$ die Zahlen $p = 2, 3$ und 5. Es gilt

$$(2) = P^3,$$

wobei $P = (\theta)$ ein Hauptideal mit Norm 2 ist. Ebenso ist

$$(3) = Q^3,$$

wobei $Q = (\theta + 1)$ ein Hauptideal mit Norm 3 ist und zwar weil

$$Q^3 = (\theta+1)^3 = ((\theta+1)^3) = (\theta^3 + 3\theta^2 + 3\theta + 1)$$
$$= (3 + 3\theta + 3\theta^2) = (3(1 + \theta + \theta^2)) = (3),$$

nachdem $(1 + \theta + \theta^2)$ eine Einheit von O_K ist, weil

$$(1 + \theta + \theta^2)(-1 + \theta) = -1 + \theta^3 = 1.$$

Zuletzt erhält man für

$$x^3 - 2 = (x+2)(x^2 - 2x - 1) \pmod 5,$$

nach dem vorigen Satz

$$(5) = PQ,$$

wobei P und Q verschiedene Primideale sind mit

$$P = (5, 2 + \theta),\ N(P) = 5$$
$$Q = (5, -1 - 2\theta + \theta^2),\ N(Q) = 5^2.$$

Es ist

$$5 = 4 + 1 = \theta^6 + 1 = (\theta^2 + 1)(\theta^4 - \theta^2 + 1) = (\theta^2 + 1)(1 + 2\theta - \theta^2),$$

sodass $1 + 2\theta - \theta^2 \mid 5$ und daher

$$Q = (1 + 2\theta - \theta^2)$$

und

$$P = (5)Q^{-1} = (5)(1 + 2\theta - \theta^2)^{-1}$$
$$= (5)((1 + 2\theta - \theta^2)^{-1}) = (5)(1 + 2\theta - \theta^2)^{-1}$$
$$(\frac{5}{1 + 2\theta - \theta^2}) = (1 + \theta^2).$$

Nachdem alle Primfaktoren von 2, 3 und 5 Hauptideale sind, ist $H(\mathbb{Q}(\sqrt[3]{2}) = 1$. □

5. Kandidaten, die nicht normeuklidisch sind

In diesem Kapitel folge ich der Arbeit von Cioffari [3].

Bemerkung 5.1
Eine Möglichkeit, Ringe auszuschließen ist mittels total verzweigter Primzahlen, die im Folgenden auch angewendet wird.

Satz 5.2
Sei p eine total verzweigte Primzahl in Körper K, mit Grad q, wobei $q \neq 2$ eine Primzahl ist und $p \not\equiv 1 \pmod{q}$. Falls eine positive ganze Zahl $e < p$ existiert, sodass weder e noch $p - e$ Norm von O_K ist, dann ist K nicht normeuklidisch.

Beweis. Nachdem $p \not\equiv 1 \pmod{q}$, existiert ein eindeutiges $c \in \{0, 1, \ldots, p-1\}$, sodass $c^q \equiv e \pmod{p}$
Angenommen es existiert ein $u \in O_K$, sodass $u \equiv c \pmod{P}$ und $|N(u)| < N(P) = p$. Nach Satz 3.10 gilt $N(u) \equiv c^q \equiv e \pmod{p}$ und so ist entweder $N(u) = e$ oder $N(u) = -p + e$. Im letzten Fall ist $N(-u) = p - e$. Daher hat man einen Widerspruch.
Sei $b \in O_K$ ein Erzeuger von P, dann folgt

$$\forall r \equiv c(b),\ |N(r)| \geq |N(b)| = p$$

Daher ist K nicht euklidisch. □

Satz 5.3
Falls $d = 59, 71, 82, 107, 179, 197, 226, 332, 404$, dann ist $\mathbb{Q}(\sqrt[3]{d})$ nicht normeuklidisch.

Beweis. Für den Beweis des Satzes betrachtet man die Werte d, p, e und $p - e$ wie in Satz 5.2.
Sei
$d = 59$, dann sind $p = 59$, $e = 7$ und $p - e = 52$.
Sei
$d = 71$, dann sind $p = 71$, $e = 19$ und $p - e = 52$.
Sei
$d = 82$, dann sind $p = 41$, $e = 13$ und $p - e = 28$.
Sei
$d = 107$, dann sind $p = 107$, $e = 14$ und $p - e = 93$.
Sei

$d = 179$, dann sind $p = 179$, $e = 7$ und $p - e = 172$.
Sei
$d = 197$, dann sind $p = 197$, $e = 39$ und $p - e = 158$.
Sei
$d = 226$, dann sind $p = 113$, $e = 37$ und $p - e = 76$.
Sei
$d = 332$, dann sind $p = 83$, $e = 7$ und $p - e = 76$.
Sei
$d = 404$, dann sind $p = 101$, $e = 28$ und $p - e = 73$.

□

Satz 5.4
Seien p_1 und p_2 total verzweigte Primzahlen im kubischen Körper K, $p_1 \not\equiv 1 \pmod 3$ und $p_2 \not\equiv 1 \pmod 3$. Falls eine positive ganze Zahl e existiert mit $e < p_1 p_2$, sodass weder e noch $p_1 p_2 - e$ Normen von O_K sind, dann ist K nicht normeuklidisch.

Beweis. Sei $(p_1) = P_1^3$ und $(p_2) = P_2^3$, dann ist $R/P_1P_2 \backsim R/P_1$ x $R/P_2 \backsim \mathbb{Z}/p_1$ x $\mathbb{Z}/p_2$. Der Beweis folgt aus Satz 5.2. □

Satz 5.5
Falls $d = 23, 29, 33, 41, 46, 69, 116, 145, 188, 575$, ist $\mathbb{Q}(\sqrt[3]{d})$ nicht normeuklidisch.

Beweis. Sei
$d = 23$, dann ist $p_1 = 3$, $p_2 = 23$, $e = 13$ und $p_1 p_2 - e = 56$
Sei
$d = 29$, dann ist $p_1 = 3$, $p_2 = 29$, $e = 26$ und $p_1 p_2 - e = 61$
Sei
$d = 33$, dann ist $p_1 = 3$, $p_2 = 11$, $e = 7$ und $p_1 p_2 - e = 26$
Sei
$d = 41$, dann ist $p_1 = 3$, $p_2 = 41$, $e = 19$ und $p_1 p_2 - e = 104$
Sei
$d = 46$, dann ist $p_1 = 2$, $p_2 = 23$, $e = 7$ und $p_1 p_2 - e = 39$
Sei
$d = 69$, dann ist $p_1 = 3$, $p_2 = 23$, $e = 26$ und $p_1 p_2 - e = 43$
Sei

$d = 116$, dann ist $p_1 = 2$, $p_2 = 29$, $e = 21$ und $p_1 p_2 - e = 37$
Sei
$d = 145$, dann ist $p_1 = 5$, $p_2 = 29$, $e = 26$ und $p_1 p_2 - e = 119$
Sei
$d = 188$, dann ist $p_1 = 2$, $p_2 = 47$, $e = 37$ und $p_1 p_2 - e = 57$
Sei
$d = 575$, dann ist $p_1 = 5$, $p_2 = 23$, $e = 37$ und $p_1 p_2 - e = 78$
□

Satz 5.6
$\mathbb{Q}(\sqrt[3]{53})$ ist nicht normeuklidisch.

Beweis. Sei P das eindeutige Ideal mit Norm 53, und sei Q das eindeutige Ideal mit Norm 2. Sei $u \in O_K$, sodass $u \equiv 1 \pmod{Q}$ und $u \equiv -25 \pmod{P}$; dann ist $N(u) \equiv (-25)^3 \equiv -10 \pmod{53}$.
Angenommen $|N(u)| < 106$; dann ist $N(u) = -10$, $N(u) = 43$, $N(u) = -63$ oder $N(u) = 96$. 43 und -63 sind aber keine Normen von O_K, und jedes Element der Norm -10 oder 96 ist in Q. Daher $|N(u)| \geq 106$.
Sei $(b) = QP$. Wir haben bereits gezeigt, dass aus $a \equiv u \pmod{b}$ folgt, dass $|N(a)| \geq |N(b)| = 106$. Daher folgt, dass $\mathbb{Q}(\sqrt[3]{53})$ nicht normeuklidisch ist. □

Bemerkung 5.7
Eine weitere Möglichkeit, um Ringe auszuschließen funktioniert mittels Restklassen modulo 2.
Falls d ungerade ist, ist $\{0, 1, \theta, \theta^2, 1+\theta, 1+\theta^2, \theta+\theta^2, 1+\theta+\theta^2\}$ ist eine komplette Menge von Repräsentanten modulo 2. Elemente, die kongruent 1, θ oder θ^2 sind, haben ungerade Norm. Alle anderen Elemente haben gerade Norm.

Satz 5.8
Sei d wie in Bemerkung 3.16. Wenn $2 \nmid d$, $h = 1$ und falls es eine total verzweigte ungerade Primzahl p gibt mit $p \neq d$, dann ist $\epsilon \equiv 1 \pmod{2}$ (ϵ ist beliebig gewählt).

Beweis. Sei $(p) = P^3$. Nachdem $h = 1$, existiert ein $c \in O_K$, sodass $(c) = P$; c kann gewählt werden, sodass $c^3 = p\epsilon^n$, wobei

$n = 0$ oder $n = 1$ oder $n = -1$ ist. Nachdem $\mathbb{Q}(\sqrt[3]{d}) \neq \mathbb{Q}(\sqrt[3]{p})$, ist $n \neq 0$ und nach Wahl von ϵ kann man $n = 1$ voraussetzen.
Dann ist $c^3 = p\epsilon \equiv \epsilon \pmod 2$. Nachdem c ungerade Norm hat, ist $c \equiv 1 \pmod 2$ oder $c \equiv \theta \pmod 2$ oder $c \equiv \theta^2 \pmod 2$. In allen Fällen folgt, dass $\epsilon \equiv 1 \pmod 2$. Dann sind $-\epsilon, \epsilon^{-1}$ und $-\epsilon^{-1}$ alle kongruent 1 modulo 2. □

Bemerkung 5.9
Sei $p = 3$ oder eine Primzahl, welche durch d teilbar ist, dann ist Satz 5.10 anwendbar, wenn $d = 5, 45, 55$ oder 99 ist. Nachdem $\epsilon \equiv 1 \pmod 2$ gehören Elemente, die dasselbe Ideal erzeugen zur selben Restklasse modulo 2.

Satz 5.10
$\mathbb{Q}(\sqrt[3]{5})$ und $\mathbb{Q}(\sqrt[3]{45})$ sind nicht normeuklidisch.

Beweis. Man schreibt die Primfaktorzerlegung wie folgt:

$$2 = PP',\ N(P) = 2,\ N(P') = 4,\ (3) = Q^3,\ 5 = R^3$$

In beiden Körpern ist (7) Primideal. Daher gibt es 6 echte Ideale $\neq 0$ mit Norm kleiner 8: P, Q, P', P^2, R und QP.
In $\mathbb{Q}(\sqrt[3]{5})$ gehört keines der Ideale zu $\overline{\theta}(2)$; Daher folgt aus $a \equiv \theta(2)$, dass $|N(a)| \geq 8$, weshalb $\mathbb{Q}(\sqrt[3]{5})$ nicht normeuklidisch ist.
In $\mathbb{Q}(\sqrt[3]{45})$ gehört keines der sechs Ideale zu $\overline{1+\theta}(2)$, und so ist $\mathbb{Q}(\sqrt[3]{45})$ nicht normeuklidisch. □

Satz 5.11
$\mathbb{Q}(\sqrt[3]{55})$ und $\mathbb{Q}(\sqrt[3]{99})$ sind nicht normeuklidisch.

Beweis. Der Beweis ist ähnlich dem Beweis im vorigen Satz. □

Satz 5.12
$\mathbb{Q}(\sqrt[3]{6})$ ist nicht normeuklidisch.

Beweis. Die Fundamentaleinheit ϵ ist $1 - 6\theta + 3\theta^2$, und so ist $\epsilon \equiv 1 + \theta^2(2)$. Nachdem $O_K = \mathbb{Z}[\theta]$, ist die Menge$\{0, 1, \theta, \theta^2, 1 + \theta, 1 + \theta^2, \theta + \theta^2, 1 + \theta + \theta^2\}$ eine komplette Menge von Repräsentanten der Restklassen modulo 2.
Jedes Element mit Norm ± 2 hat die Form $\pm(2 - \theta)\epsilon^n$, mit $n \in \mathbb{Z}$,

und ist daher kongruent zu θ modulo 2.
Jedes Element mit Norm ± 6 hat die Form $\pm\theta\epsilon^n$, mit $n \in \mathbb{Z}$ ist daher ebenso kongruent θ modulo 2.
Angenommen $a \equiv \theta + \theta^2(2)$, $N(a) \equiv 2(4)$, und weil $|N(a)| \neq 2, 6$ folgt, dass $N(a) > N(2) = 8$. Daher ist $\mathbb{Q}(\sqrt[3]{6})$ nicht normeuklidisch. □

Bemerkung 5.13
Um zu zeigen, dass $\mathbb{Q}(\sqrt[3]{d})$, nicht normeuklidisch ist, für $d = 12, 17, 44$, benötigt man nun andere Techniken als bisher. Dazu verwendet man eine Charakterisierung euklidischer Ringe, welche folgendermaßen aussieht:

$$\forall x \in \mathbb{Q}(\sqrt[3]{d})\ \exists p \in R :\ |N(x+p)| < 1.$$

Falls $x_1, x_2 \in \mathbb{Q}(\sqrt[3]{d})$, und $x_1 - x_2 \in O_K$, dann sagt man $x_1 \equiv x_2 \pmod{O_K}$, oder x_1 ist ein O_K-Translat von x_2.
Um nun zu beweisen, dass $\mathbb{Q}(\sqrt[3]{d})$ nicht normeuklidisch ist, muss man ein passendes Element x finden und beweisen, dass es kein O_K-Translat von x gibt mit Absolutbetrag kleiner 1.
Der folgende Satz wird zeigen, dass es ausreichend ist endlich viele O_K-Translate von x zu testen.
Sei
$d = 12$, dann sind $\theta = \sqrt[3]{12}$, $\phi = \sqrt[3]{18}$, $a = 40$, $b = 6$ und $c = 7$.
Sei
$d = 17$, dann sind $\theta = \sqrt[3]{17}$, $\phi = \frac{1-\theta+\theta^2}{3}$, $a = 105$, $b = 17$ und $c = 15$.
Sei
$d = 44$, dann sind $\theta = \sqrt[3]{44}$, $\phi = \frac{-1+\theta+\theta^2/2}{3}$, $a = 230$, $b = 31$ und $c = 15$.

Satz 5.14
Seien d, θ, ϕ, a, b und c wie in obiger Bemerkung. Sei $x \in \mathbb{Q}(\sqrt[3]{d})$. Angenommen, es gilt

(1) $x\epsilon \equiv \pm x \pmod{O_K}$
(2) $\exists y \equiv x \pmod{O_K}$, sodass $|N(y)| < 1$.
Dann existiert $z = r + s\theta + t\phi$, $r, s, t \in \mathbb{Q}$, sodass
(3) $z \equiv \pm x \pmod{O_K}$

(4) $|N(z)| < 1$
(5) $|r| < a$, $|s| < b$, $|t| < c$

Beweis. $\{1, \theta, \phi\}$ ist eine $\mathbb{Z}$-Basis für O_K. Wir geben den Beweis für $d = 12$. Für $d = 17, 44$ verläuft er ähnlich.
Die Idee des Beweises ist, ein z zu finden, sodass $0,006 < |z| < 1$ und $|N(z)| < 1$ ist; die Grenzen für r, s und t folgen dann. Man identifiziert jedes $u \in O_K$ mit seiner reellen Einbettung. Es seien u' und u'' die Konjugierten von u, dh. für $u = \sqrt[3]{12}$, sind $u' = \sqrt[3]{12}\omega$ und $u'' = \sqrt[3]{12}\omega^2$, wobei $\omega = (-1 + \sqrt{3}i)/2$.
Nachdem $|\epsilon| > 0.006$, wobei ϵ die Fundamentaleinheit $1 + 3\sqrt[3]{12} - 3\sqrt[3]{18}$ ist, existiert ein n, sodass $0,006 < |y\epsilon^n| < 1$
Sei $z = y\epsilon^n$; dann ist $z \equiv \pm y \equiv \pm x \pmod{O_K}$, nach (1) und $|N(z)| = |N(y)| < 1$. Nachdem $N(z) = |z||z'||z''| = |z||z'|^2 < 1$ und $|z| > 0,006$, folgt, dass $|z'| < 14$. Daher ist $|z - z'| < 15$. Sind r, s und t die Koeffizienten von z, bezüglich der Basis $\{1, \theta, \phi\}$ hat man dann

$$|Re\ z - z'| = |\frac{3}{2}\sqrt[3]{12s} + \frac{3}{2}\sqrt[3]{18t}| < 15$$

$$|Im\ z - z'| = |-\frac{\sqrt{3}}{2}\sqrt[3]{12s} + \frac{\sqrt{3}}{2}\sqrt[3]{18t}| < 15$$

Durch Lösen der Ungleichungen folgt , dass $|s| < 6$ und $|t| < 7$.
Nachdem $|z| < 1$ folgt, dass $|r| < 40$ □

Satz 5.15
$\mathbb{Q}(\sqrt[3]{12}), \mathbb{Q}(\sqrt[3]{17})$ und $\mathbb{Q}(\sqrt[3]{44})$ sind nicht normeuklidisch.

Beweis. Für $d = 12$, ist

$$x = \frac{2}{3} + \frac{5}{6}\theta + \frac{4}{9}\phi.$$

Für $d = 17$, ist

$$x = -\frac{94}{257} + \frac{233}{514}\theta - \frac{19}{1028}\phi.$$

Für $d = 44$, ist

$$x = 12/c,\ mit\ c = 5 + 2\theta + \phi.$$

In jedem dieser Fälle wird mit Hilfe eines Computer gezeigt, dass kein O_K-Translat von x, in den Grenzen (5) in Satz 5.14,

Absolutbetrag kleiner 1 hat.
Daher hat, wieder nach Satz 5.14, kein O_K-Translat von x Absolutbetrag kleiner 1. □

6. Kandidaten, die normeuklidisch sind

In diesem Kapitel folge ich den Arbeiten von Cioffari [3], Godwin [4],[5] und Taylor [8].

Satz 6.1
$\mathbb{Q}(\sqrt[3]{2})$ ist normeuklidisch.

Satz 6.2
$\mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{10})$ sind normeuklidisch.

Bemerkung 6.3
Der Satz von Godwin zeigt, dass $\mathbb{Q}(\sqrt[3]{2})$ normeuklidisch ist. Die Tatsache, dass $\mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{10})$ normeuklidisch sind, wurde von M.Taylor bewiesen.

Bemerkung 6.4
Um zu zeigen, dass $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{10})$ normeuklidisch sind, benötigt man einen Computer. Man repräsentiert jeden Körper K durch die Korrespondenz

$$\sigma\colon\ x+y\theta+z\phi \to (x,y,z).$$

Für $d = 2,3$, wird der Ganzheitsring durch das Gitter der Punkte mit ganzzahligen Koordinaten repräsentiert.
Für $d = 10$, wird O_K durch die Vektoren $(1,0,0),(0,1,0)$ und $(1/3,1/3,1/3)$ das Gitter erzeugt und man muss die Vorgangsweise entsprechend modifizieren.
Für $d = 2,3$ definiert man den Fundamentalwürfel C als die Menge der Punkte (x,y,z) mit $0 \le x,y,z < 1$. Um zu beweisen, dass ein Körper euklidisch ist, muss man zeigen, dass jeder Punkt in C, ein O_K-Translat, mit $|N| < 1$ hat. Die Schwierigkeit ist die unendliche Anzahl von Punkten in C. Daher teilt man C in hinreichend kleine Würfel, von denen jeder ein O_K-Translat in dem Bereich hat, in dem $|N| < 1$ gilt.
Gegeben sei nun eine Menge von Punkten $S \subset \mathbb{R}^3$ und $\zeta \in O_K$, dann nennt man die Menge $\{(x,y,z)+\sigma(\zeta)|(x,y,z) \in S\}$ das Translat von S unter ζ. Das Programm teilt C in acht Würfel, durch Schnitte mit den Ebenen $x = y = z = 1/2$. Danach testet

man 1500 O_K-Translate eines gegebenen Würfels C': Falls eines dieser Translate vollständig im Bereich $|N| < 1$ liegt, dann sagt man C' ist bedeckt. Falls nicht gezeigt wird, dass C' bedeckt ist, wird C' wiederum in acht Würfel geteilt. Jeder dieser acht Würfel wird auf dieselbe Weise wieder getestet: Falls einer der 1500 O_K-Translate im Bereich $|N| < 1$ liegt, heißt der Würfel bedeckt; Andernfalls, wird er weiter geteilt. Wenn man schließlich erreicht hat, dass alle Würfel bedeckt sind, hat man bewiesen, dass jeder Punkt in C ein O_K-Translat hat mit $|N| < 1$: Daher ist der Körper euklidisch.
Die Zahl 1500 ist beliebig gewählt.
Die nun folgenden Sätze geben eine hinreichende Bedingung wann ein Würfel in einem Bereich $|N| < 1$ enthalten ist.
Um einfacher rechnen zu können setzt man $u = x$, $v = \sqrt[3]{d}y$ und $w = \sqrt[3]{d^2}z$.

Satz 6.5
Sei $\overline{N}(u,v,w) = u^3 + v^3 + w^3 - 3uvw$. Sei E ein Bereich in $\mathbb{R}^3$, begrenzt durch die Ebenen $u = a_1, u = a_2, v = b_1, v = b_2, w = c_1$ und $w = c_2$: Angenommen E liegt vollständig in einem Oktant in $\mathbb{R}^3$. Falls $|\overline{N}| < 1$ überall auf dem 1-Gerüst von E gilt, gilt $|\overline{N}| < 1$ überall in E.

Beweis. Sei S der Schnittpunkt von E mit einer Ebene, die parallel zu den Koordinatenebenen ist; Angenommen zB. S ist parallel zu der uv-Ebene. Um zu erreichen, dass $\overline{N}(u,v)$ ein Extremum im Inneren von S hat, ist es notwendig, dass $\delta\overline{N}/\delta u = \delta\overline{N}/\delta v = 0$.
Nachdem S komplett in einem Oktanten liegt, ist das nur möglich, wenn $u = v = w \neq 0$. In diesem Fall ist $\overline{N} = 0$. Nachdem dasselbe Argument angewendet werden kann, wenn S parallel zu irgendeiner Koordinatenebene ist, folgt daraus, dass $|\overline{N}|$ kein Maximum in S haben kann.
Es folgt, dass das Maximum von $|\overline{N}|$ auf E auf dem 1-Gerüst von E liegt. Der Satz folgt nun unmittelbar. □

Satz 6.6
Seien $\overline{N}$ und E wie im vorigen Satz. Angenommen $|\overline{N}| < 1$ an

allen acht Ecken von E und die folgenden Ausdrücke sind alle nicht negativ:

$$(a_1 - b_i c_j)(a_2 - b_i c_j),\ i, j = 1, 2$$

$$(b_1 - a_i c_j)(b_2 - a_i c_j),\ i, j = 1, 2$$

$$(c_1 - a_i b_j)(c_2 - a_i b_j),\ i, j = 1, 2$$

Dann ist $|\overline{N}| < 1$ überall in E.

Bemerkung 6.7
Die Bedingungen aus Satz 6.6 stellen sicher, dass auf jedem Teil des 1-Gerüsts, die zugehörige partielle Ableitung nicht 0 ist. Daher kann $\overline{N}$ ein lokales Maximum oder Minimum auf dem 1-Gerüst nur in den Ecken annehmen.
Daher folgt, dass $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{10})$ normeuklidisch sind.

Bemerkung 6.8
Nun ist das Ziel zu zeigen, dass $\mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{10})$ normeuklidisch sind.

Bemerkung 6.9
Für jedes Element α in einem algebraischen Zahlkörper K definiert man

$$M(\alpha, K) = \min_y |N(\alpha - y)|,$$

wobei das Minimum über alle ganzalgebraischen Zahlen y in K läuft, und N die Norm der algebraischen Zahl ist. Man definiert

$$M(K) = \max_\alpha M(K, \alpha)$$

$$M(K) = \max_\alpha \min_y |N(\alpha - y)|$$

wobei das Maximum über alle algebraische Zahlen $\alpha \in K$ läuft. Man nennt $M(K)$ das beschränke inhomogene Minimum des Körpers K.

Man beachte, dass es keinen euklidischen Algorithmus in einem algebraischen Zahlkörper gibt, wenn ganzalgebraische Zahlen β, ζ in K existieren, sodass $\beta \neq 0$ und für jede ganzalgebraische Zahl γ in K gilt, dass

$$|N(\zeta - \gamma\beta)| \geq |N(\beta)|, \tag{20}$$

wobei $|x|$ den Absolutbetrag von x bezeichnet.
Daher gilt

K hat einen euklidischen Algorithmus dann,

und nur dann wenn $M(K) < 1$.

Wenn man eine algebraisch ganze Zahl β finden kann, sodass zumindest eine der Restklassen modulo β keine algebraisch ganze Zahl von K, mit Absolutbetrages kleiner als $|N(\beta)|$ enthält, dann ist $M(K,\beta)$ zumindest 1 und K enthält keinen Euklidischen Algorithmus. Eine Methode, die auf dieser Tatsache beruht, kann für viele Körper angewandt werden, um zu beweisen, dass diese nicht normeuklidisch sind.
Diese Methode wird verwendet, um die Existenz eines Euklidischen Algorithmus zu beweisen und liefert für eine gegebenes K, ein M' mit einer der beiden folgenden Eigenschaften.

- Für jede algebraische Zahl $\alpha \in K$ existiert eine ganzalgebraische Zahl $\gamma \in K$, sodass

  $$|N(\alpha - \gamma)| \leq M'.$$

  Falls $M' < 1$, dann hat K eine euklidischen Algorithmus.
- Es existieren algebraische Zahlen $\beta_1, \ldots, \beta_n \in K$ welche inkongruent modulo 1 sind, und für jede algebraische Zahl $\alpha \in K$ welche inkongruent zu jedem der $\beta_1, \ldots, \beta_n$ modulo 1 ist, existiert eine algebraische Zahl $\gamma \in K$, sodass

  $$|N(\alpha - \gamma)| \leq M';$$

  und falls es eine Zahl $\beta \in K$ gibt, sodass

  $$M(K,\beta) > M',$$

  muss β kongruent zu einem der $\beta_1, \ldots, \beta_n$ modulo 1 sein.

Während man nach dem euklidischen Algorithmus sucht, wird $M = 0,99999$ gewählt sodass, ein euklidischer Algorithmus in K existiert, $M(K,\beta_i)$ für $i = 1,2,\ldots,n$ bestimmt werden kann. Falls für ein i, $M(K,\beta_i) \geq 1$, dann ist das beschränkte inhomogene Minimum auch bestimmt. Die Methode erlaubt den β's beliebige Werte beliebiger reeller Zahlen anzunehmen, obwohl diese in K sind. Daher war das beschränkte inhomogene Minimum das inhomogene Minimum der betrachteten Körper.
Eine Zahl $\frac{\alpha}{1-\epsilon^n}$, wobei α ein ganzalgebraische Zahl in K ist, n ist eine positive ganze Zahl und ϵ die Fundamentaleinheit des Körpers ist, und $0 < \epsilon < 1$, transformiert in sich selbst, wenn die Elemente von K durch

$$T : \gamma \to \frac{\gamma - \alpha}{\epsilon^n}$$

transformiert werden. Für eine beliebige ganzalgebraische Zahl γ in K und für jede ganze Zahl i gilt

$$N(\frac{\alpha}{1-\epsilon^n} - T^i(\gamma)) = N(\frac{\alpha}{1-\epsilon^n} - \gamma).$$

Ein Folge dieser Gleichung ist, dass es für eine beliebig gegebene reelle Zahl C, eine endliche Menge S von ganzalgebraischen Zahlen $\gamma \in K$ gibt, sodass für beliebiges ganzalgebraisches $\gamma_1 \in K$

$$|N(\frac{\alpha}{1-\epsilon^n} - \gamma_1)| \leq C$$

gilt. Ein $\gamma_2 \in S$ existiert, sodass

$$N(\frac{\alpha}{1-\epsilon^n} - \gamma_1) = N(\frac{\alpha}{1-\epsilon^n} - \gamma_2).$$

Somit hat man eine endliche Menge von ganzalgebraische Zahlen, unter denen man ein γ findet, sodass

$$M(K, \frac{\alpha}{1-\epsilon^n}) = |N(\frac{\alpha}{1-\epsilon^n} - \gamma_1)|$$

gilt.
Durch Ausdrücken von β in der Form $\frac{\alpha}{(1-\epsilon^n)}$, wobei α eine ganzalgebraische Zahl in K ist, ist es immer möglich $M(K,\beta)$ für

$i = 1, 2, \ldots, n$ zu bestimmen und dadurch die euklidische Eigenschaft des Körpers.

Bemerkung 6.10
Durch diese Methode wird bewiesen, dass $\mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{10})$ normeuklidisch sind.

Bemerkung 6.11
Ziel ist nun zu zeigen, dass $\mathbb{Q}(\sqrt[3]{2})$ normeuklidisch ist. Dazu müssen zuerst einige Lemmata bewiesen werden.

Bemerkung 6.12
Seien $m, n, p \in \mathbb{N}$. Dann bezeichnet man

$$\beta - n + ((\beta - n)^2 + \tau)^{-1}$$

mit

$$f_n(\beta, \tau) = f_n$$

und

$$\beta - (\beta^2 + \tau)^{-1}$$

mit

$$f_0(\beta, \tau) = f_0,$$

wobei $\beta, \tau \in \mathbb{R}$

Bemerkung 6.13
Sei $H = 8b - 3a^2$, $I = b^2 - 3ac + 12d$,
$J = 72bd + 9abc - 27c^3 - 27a^2d - 2b^3$, $\Delta = 4I^3 - J^2$
Dann hat die biquadratische Gleichung $x^4 - ax^3 + bx^2 - cx + d = 0$ zwei reelle Nullstellen falls $\Delta < 0$, und vier oder null reelle Wurzeln, wenn $\Delta > 0$: Sie hat 4 Nullstellen nur, wenn $H < 0$ und $16I - H^2 < 0$. Die doppelte Nullstelle tritt nur auf wenn $\Delta = 0$.

Lemma 6.14
$f_n = f_m$ hat keine reellen Nullstellen wenn $\tau > \tau_D$, hat zwei reelle Nullstellen, wenn $\tau < \tau_D$, und eine doppelte Nullstelle, wenn $\tau = \tau_D$, mit $D = (m + n)^2$ und τ_D ist die positive reelle Wurzel von

(21)
$$\tau^4 + \tau^3(\frac{1}{2}D + 4D^{-2}) + \tau^2(\frac{1}{16}D^2 + \frac{3}{2}D^{-1}) - \frac{3}{8}\tau - \frac{1}{16}D - \frac{27}{16}D^2 = 0.$$

Wenn es zwei Nullstellen gibt, ist die größere Nullstelle eine fallende Funktion von τ, und die kleinere Nullstelle ist eine wachsende Funktion von τ.

Beweis. Man schreibt $u = \beta - \frac{1}{2}(m+n)$ und $f_m = f_n$ wird

$$\phi(u) = u^4 + u^2(2\tau - \frac{1}{2}D) - 2u + (\tau + \frac{1}{4}D)^2 = 0.$$

Mit der Notation aus Bemerkung 6.13 hat man $16I - H^2 = 192\tau D$. Daher hat ϕ nicht mehr als zwei reelle Nullstellen. Für $\tau = 0$ ist $\phi(\sqrt{\frac{1}{4}D}) < 0$, sodass ϕ zwei reelle Nullstellen besitzt. Nachdem $\phi(u)$ eine wachsende Funktion von τ ist, gibt es nur einen Wert τ_D von τ mit den angegebenen Eigenschaften. Verwendet man nun die Bedingung, dass $\phi(u)$ zusammenfallende Nullstellen besitzt, erhält man die Gleichung im obigen Lemma.
Nachdem $\phi(u)$ eine wachsende Funktion von τ ist, folgt, dass die Nullstellen von ϕ in Abhängigkeit von τ monoton wachsen bzw. fallen wie angegeben. □

Lemma 6.15
$f_m = f_0$ $(m \geq 2)$ hat drei nichtnegative reelle Nullstellen falls

$$0 \leq \tau < \frac{1}{2}(-m^2 + 2m^{-1} + (\sqrt{m^4 + 4m^{-2}})),$$

hat vier reelle Nullstellen, falls

$$\frac{1}{2}(-m^2 + 2m^{-1} + (\sqrt{m^4 + 4m^{-2}})) \leq \tau < m^{-1} + m^{-4},$$

und hat keine reellen Nullstelle, wenn

$$m^{-1} + m^{-4} < \tau.$$

Die Gleichung $f_0 = f_1$ hat eine nichtnegative reelle Nullstelle falls $0 \leq \tau < \frac{1}{2}(1 + \sqrt{5})$. Sie hat zwei nichtnegative reelle Nullstelle falls $\frac{1}{2}(1 + \sqrt{5}) \leq \tau < \frac{7}{4}$ und 0 nichtnegative reelle Nullstellen falls $\frac{7}{4} < \tau$. In allen Fällen ist die größte Nullstelle stets eine fallende Funktion von τ, die nächstgrößere ist eine wachsende Funktion und alternierend so weiter.

Beweis. Setzt man $\beta - \frac{1}{2}m = u$, so erhält man

$$(u^2 + \tau - \frac{1}{4}m^2 - m^{-1})^2 = m + m^{-2} - m^2\tau.$$

Das Resultat des Lemmas folgt daraus auf elementare Weise. □

Lemma 6.16
Die simultanen Gleichungen $f_m = f_n = f_p$ bestimmen höchstens ein nichtnegatives Paar (β, τ) von Werten.

Beweis. Man hat

$$(\tau + (\beta - m)^2)(\tau + (\beta - n)^2) = 2\beta - (m + n)$$

und

$$(\tau + (\beta - m)^2)(\tau + (\beta - p)^2) = 2\beta - (m + p),$$

woraus sich ergibt, dass

$$(\tau + (\beta - m)^2)(2\beta - m - p) = 1$$

und so folgt

$$(2\beta - n - p)(2\beta - m - p)(2\beta - m - n) = 1. \tag{22}$$

Angenommen $m < n < p$. Dann beinhalten die Werte, die (22) erfüllen, einen Wert größer $\frac{1}{2}(n + p)$ und möglicherweise zwei Werte zwischen $\frac{1}{2}(m+n)$ und $\frac{1}{2}(m+p)$. Man beachte, dass durch die letzten zwei Werte, der Wert τ negativ wird. Man bezeichnet den Wert von τ, für den gilt $f_m = f_n = f_p$ und $\beta \geq 0$ mit τ_{mnp}. □

Lemma 6.17
Die simultanen Gleichungen $f_0 = f_n = f_m$ besstimmen höchstens ein nichtnegatives Paar von Werten (β, τ).

Beweis. Schreibt man v als $2\beta - m - n - \frac{2}{mn}$, so erhält man $\tau = -\beta^2 - v^{-1}$ und

$$(v + \frac{2}{mn})(v + m)(v + n) = 1. \tag{23}$$

Angenommen $m < n$. Dann enthalten die Werte, die (23) erfüllen, einen Wert größer $-2mn$ und möglicherweise 2 Werte zwischen $-n$ und $-m$. Falls v die Gleichung (23) erfüllt, dann ist

$$\tau = \frac{3}{4}v^2 + \frac{1}{2}v(m + n + \frac{2}{mn}) + (mn + 2m^{-1} + 2n^{-1}) - \frac{1}{4}(m + n + \frac{2}{mn})^2$$

wobei τ nicht positiv für $v = -m$ und $v = -n$ ist. Daher ergibt sich für Werte von v zwischen $-n$ und $-m$, die die obige Gleichung erfüllen, dass $\tau < 0$ und es gibt höchstens ein Paar (β, τ) mit $\beta \geq 0, \tau \geq 0$.
Wir bezeichnen den Wert von τ mit $f_0 = f_m = f_n$ und $\beta \geq 0$ mit τ_{0mn}.
Einige Werte sind:

$$\tau_{145} = 0,033336\ldots, \tau_{034} = 0,046846\ldots, \tau_{134} = 0,136153\ldots,$$

$$\tau_{023} = 0,185680\ldots, \tau_{123} = 0,316158\ldots, \tau_{012} = 0,554819\ldots,$$

$$\tau_1 = 0,640314\ldots, \tau_4 = 0,449901\ldots, \tau_9 = 0,382194\ldots .$$

Nun definiert man die Funktion $\Phi(\tau)$. Sei $C_{ij}(\tau)$ der gemeinsame Wert von f_i, f_j, für den größeren Wert von β und $c_{ij}(\tau)$ der gemeinsame Wert von f_i, f_j für den kleineren Wert von β. Dann ist

$$\Phi(\tau) = \begin{cases} c_{45}(\tau) & 0 \leq \tau \leq \tau_{145} \\ C_{14}(\tau) & \tau_{145} \leq \tau \leq \tau_{034} \\ c_{34}(\tau) & \tau_{034} \leq \tau \leq \tau_{134} \\ C_{13}(\tau) & \tau_{134} \leq \tau \leq \tau_{023} \\ c_{23}(\tau) & \tau_{023} \leq \tau \leq \tau_{123} \\ C_{12}(\tau) & \tau_{123} \leq \tau \leq \tau_{012} \\ C_{01}(\tau) & \tau_{012} \leq \tau \leq \frac{7}{4}. \end{cases}$$

In jedem der Fälle existiert der Wert von β nach Lemma 6.14 oder Lemma 6.15. □

Lemma 6.18
$\Phi(\tau) = \min_\beta \max_n f_n(\beta, \tau)$ in Abhängigkeit von $f_0(\beta, \tau) \geq f_n(\beta, \tau)$, für $n = 1, 2, \ldots$.

Beweis. Betrachtet das Intervall $0 \leq \tau \leq \tau_{145} = 0 \cdot 033336\ldots$. Die Bedingung $f_o \geq f_n$ kann geschrieben werden als $((\beta - n)^2 + \tau)^{-1} + (\beta^2 + \tau)^{-1} \leq n$ und ist nicht erfüllt, wenn $((\beta - n)^2 + \tau_{145}) + (\beta^2 + \tau_{145})^{-1} > n$. Daher muss, nachdem $n = 1$ ist, $\beta > 2,118$

sein. Verwendet man $n = 2$, dann muss $\beta > 2,709$ sein. Verwendet man $n = 3$, dann ist $\beta > 3,555$. Verwendet man $n = 4$, dann muss $\beta > 4,468$ sein. Als letztes muss für $n = 5$, der Wert $\beta < 4,590$ oder $\beta > 5,409$ sein. Für $4,468 \leq \beta \leq 4,590$ hat man $\partial f_5/\partial\beta > 1$ und so ist $f_5 \geq f_5(4,468, \tau_{145}) = 2,028\ldots$, während $f_n < 0$ für $n \geq 6$. Für die Werte von β für die man $f_4 = f_5$ hat, wenn $\tau = 0$ ist, $f_0 > f_4 = f_5 > f_1 > f_2 > f_3$ während, für $\tau = \tau_{145}$, hat man $f_0 > f_4 = f_5 = f_1 > f_2 > f_3$ Daher hat man für $0 \leq \tau \leq \tau_{145}$ und für diese Werte von β gilt $f_0 \geq f_4 = f_5 \geq f_1, f_2, f_3$, nach Lemma 6.16 und Lemma 6.17.
Nachdem

$$\frac{\partial f_4}{\partial \beta} < 1 - 2(0,468/((0,590)^2 + \tau_{145})^2 < 0$$

gilt $\min_\beta \max_n f_n = f_4 = f_5$. Nachdem f_4 und f_5 fallende Funktionen von β sind, ist $\min_\beta \max_n f_n$ nicht größer als der Wert für $\tau = 0$ welcher $4 \cdot 0774\ldots$ (für $\beta = 4,53101\ldots$) ist. Für $\beta \geq 5,409$ hat man $f_1 > 4,409$ und so muss man $\beta \geq 5,409$ nicht betrachten. Die restlichen Intervalle verhalten sich ähnlich. □

Lemma 6.19
Falls $(\beta - \alpha)^2 < \Phi^2(\tau)$, dann enthält die Menge aller x, für welche

$$|(x - \alpha)((x - \beta)^2 + \tau)| < 1,$$

gilt, ein vollständiges System von Restklassen modulo 1.

Beweis. Man zeigt, dass wenn die Menge der x nicht ein vollständiges System von Restklassen modulo 1 enthält, dann ist $(\beta - \alpha) \geq \Phi^2(\tau)$. Man ändert weder $(\beta - \alpha)^2$, noch τ wenn man eine Konstante zu x hinzufügt und darf daher annehmen, dass 0 die fehlende Restklasse ist. Nachdem man jede ganze Zahl zu x hinzufügen darf oder das Vorzeichen ändern kann, kann man annehmen, dass $0 < \alpha < 1$ und $\alpha \leq \beta$ gilt und man erhält daher

$$\alpha(\beta^2 + \tau) \geq 1$$

und

$$(n - \alpha)((\beta - n)^2 + \tau) \geq 1 \ , (n = 1, 2, \ldots).$$

Daher bekommt man

$$f_n(\beta,\tau) \leq (\beta-\alpha) \leq f_0(\beta,\tau)\ ,(n=1,2,\ldots)$$

Das ist, nach Lemma 6.18, genau dasselbe wie $(\beta-\alpha)^2 \geq \Phi^2(\tau)$, was das Lemma beweist. □

Bemerkung 6.20
Die Funktion Φ hat Unstetigkeitsstellen bei $\tau=\tau_{034}, \tau=\tau_{023}$ und $\tau=\tau_{012}$, während ihre Ableitung Unstetigkeitsstellen bei $\tau=\tau_{145}, \tau=\tau_{134}$ und $\tau=\tau_{123}$ hat. Im nächsten Lemma wird gezeigt, dass einige lineare Funktionen von τ untere Grenzen für Φ^2 sind.

Lemma 6.21
Sei p eine reelle Wurzel von $p^3=p+1$. So hat man für $0\leq\tau\leq\frac{7}{4}$

(1) $\Phi^2(\tau) \geq (2p+3)-\frac{1}{23}(72p^2+32p-45)\tau$,
(2) $\Phi^2(\tau) \geq \frac{1}{17}(p^2+22p+7)(\frac{7}{4}-\tau)$.

Gleicheit in (1) erhält man nur für $\tau=\tau_{123}$ und $\tau=\tau_{012}$. Bei (2) gilt Gleichheit nur wenn $\tau=\tau_{012}$ und $\tau=\frac{7}{4}$.

Beweis. Für jedes Intervall von τ für das Φ definiert ist, löst man die Gleichung $\Phi^2=A-B\tau$, wobei A und B wie in (1) und (2) definiert sind. Das Vorzeichen von $\Phi^2-A+B\tau$ wird durch die Nullstellen für verschiedene τ bestimmt. Damit ist das Lemma bewiesen. □

Lemma 6.22
Ellipsen kongruent zu $Ax^2+Bxy+Cy^2<K$ mit Achsen in die selben Richtungen und zentriert an den Punkten der des ganzen Gitters, überdecken die Ebene, wenn

$$\frac{AC(A+C-B)}{4AC-B^2} < K.$$

Beweis. Die Transformation $x_1=x+\frac{By}{2A}$, $y_1=\frac{y\sqrt{4AC-B^2}}{2A}$ bildet die Ellipsen in Kreise ab mit Radius $\sqrt{\frac{K}{A}}$, und das Gitter in das mit Basispunkten $P(1,0)$ und $Q(\frac{B}{2A},\frac{\sqrt{4AC-B^2}}{2A})$. Es genügt zu zeigen, dass die Kreise, die um 0, Q und P zentriert sind, das Dreick $0PQ$ überdecken. Der Umkreisradius von 0QP ist

$\sqrt{\frac{C(A+C-B)}{(4AC-B^2)}}$ und es genügt wenn der Radius des Kreises größer ist als dieser und das ist genau dann wenn

$$K > \frac{AC(A+C-B)}{AC-B^2}$$

Man beachte, dass das Dreieck $0PQ$ stumpfwinkelig ist außer wenn $0 \leq B \leq 2A$ und die Schranke für K ist unnötig groß. Die Schranke M in diesem Fall ist

$$M \leq \max\{\frac{AC_1(A+C_1-B_1)}{6(4AC_1-B_1^2)} - \frac{1}{8}, p_o\},$$

mit

$$B_1 = B - 2kA,\ C_1 = C - Bk - Ak^2,$$

k ist eine ganze Zahl und $p_0 = 0 \cdot 394120\ldots$. □

Bemerkung 6.23
Sei K ein kubische Körper mit negativer Diskriminante, die die Basis $1, \omega, \Omega$ hat und seien $1, \theta \pm i_\xi, \eta \pm iX$ Basen der konjugierten Körper. Dann und nur dann ist K euklidisch, wenn für jedes Tripel (x', y', z') rationaler Zahlen ein Tripel (x, y, z) existiert mit $(x, y, z) \equiv (x', y', z') \pmod 1$, sodass

$$|N(x + y\omega + z\Omega)| < 1. \tag{24}$$

Schreibt man $\alpha = -y\omega - z\Omega$, $\beta = -y\theta - z\eta$, $\tau = (y\xi - zX)^2$, dann bekommt man

$$N(x + y\omega + z\Omega) = (x - \alpha)((x - \beta)^2 + \tau)$$

und nach Lemma 6.19 folgt, dass (24) erfüllt ist, wenn

$$(\beta - \alpha)^2 < \Phi^2(\tau). \tag{25}$$

Nach dem Lemma 6.19 ist (25) erfüllt, wenn

$$(y(\omega - \theta) + z(\Omega - \eta))^2 < A - B(y\xi + zX)^2. \tag{26}$$

Das heißt $py^2 + qyz + rz^2 < 1$. Nach Lemma 6.22 kann man y und z wählen, wenn $pr(p + r - q) < 4pr - q^2$ (oder allgemeiner $p'r'(p' + r' - q') < 4p'r' - q'^2$, wobei $p'y^2 + q'yz + r'z^2$ eine äquivalente Form zu $py^2 + qyz + rz^2$) ist.

Wendet man nun Lemma 6.21 an, erhält man, dass $\mathbb{Q}(\sqrt[3]{2})$ normeuklidisch ist.

Zusammenfassung

Diese Diplomarbeit beschäftigt sich mit normeuklidischen Ringen ganzer Zahlen in rein kubischen
Zahlköpern.
In Kapitel 1 werden einige grundlegende Bedingungen und Definitionen in rein kubischen Zahlkörpern eingeführt.
Im Kapitel 2 wird eine Schranke entwickelt, sodass man nur mehr eine endliche Menge von Ringen betrachen muss auf der Suche nach normeuklidischen Ringen ganzer Zahlen in rein kubischen Zahlkörpern.
In Kapitel 3 werden einige Bemerkungen über rein kubische Zahlköper präsentiert und 2 Sätze die bei der Einschränkung möglicher Kandidaten helfen.
In Kapitel 4 werden Diskriminante und Ganzheitsbasis von noch in Frage kommender Ringe berechnet.Der algebraische Zahlkrper, fr den gezeigt wird, das er Klassenzahl 1 besitzt, ist derjenige, der sich durch Adjunktion der dritten Wurzel von 2 ergibt.
In Kapitel 5 werden von den möglichen Kandidaten fast alle auf verschiedenste Weise ausgeschlossen und sind daher nicht normeuklidisch.
In Kapitel 6 wird schließlich bewiesen, dass $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{3})$ und $\mathbb{Q}(\sqrt[3]{10})$ normeuklidisch sind.

Literaturverzeichnis

[1] S. Alaca & K.S. Williams *Introductory Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 2004.

[2] J. W. S. Cassels, *On the inhomogeneous minumum of binary quadratic ternary cubic and quaternary quartic forms*, Proc Cambridge Philos Soc., **48**, (1952), 72 – 86.

[3] V. Cioffari, *The Euclidean condition in pure cubic and complex quartic fields*, Math. Comp. **33** (1979), 389 – 398.

[4] H. J. Godwin, *On Euclid′s Algorithm in some cubic fields with signature one*, Quart. J. Math. (Oxford), **18** (1967), 333 – 338.

[5] H. J. Godwin, *On the inhomogeneous minima of totally real cubic norm − forms*, J. London Math. Soc. **40** (1965), 623 – 627.

[6] K. Mahler, *On lattice points in a cylinder*, Quart. J. Math., **17** (1946), 16 – 18.

[7] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, Berlin etc. 2004.

[8] E. M. Taylor, *Euclid′s algorithm in cubic fields with complex conjugates*, J. London Math. Soc. (2), **14**, (1976), 49 – 54.

Lebenslauf

PersönlicheDaten

- Name: Timo Wenzl
- Geburtstag: 25. August 1987
- Geburtsort: Wien
- Staatsbürgerschaft: Österreich

Ausbildung

- 1993-1998: Volksschule Kindemanngasse in 1170 Wien
- 1998-2002: Kooperative Mittelschule (Albertus Magnus Schule) in 1180 Wien
- 2002-2006: Bundesoberstufenrealgymnasium Hegelgasse 12 in 1010 Wien
- 23. Juni 2006: Matura mit gutem Erfolg bestanden
- WS 2006/07 : Beginn des Diplomstudiums Mathematik an der Universität Wien
- 27. Juni 2010: 1. Diplomprüfung bestanden