Beiträge zur Einheitenberechnung

vorgelegt von
Diplom-Mathematiker

Max Jüntgen

aus Hilden

Vom Fachbereich 3 Mathematik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
genehmigte Dissertation.

Berlin 1996
D83

Promotionsausschuß

Vorsitzender:	Professor Dr. J. Becker
Berichter:	Professor Dr. M. E. Pohst
Berichter:	Professor Dr. J. Buchmann

Tag der wissenschaftlichen Aussprache: 5. Dezember 1996

Inhaltsverzeichnis

KAPITEL I

Einleitung

1. Überblick

Gegenstand dieser Arbeit ist die Berechnung von Einheiten in algebraischen Zahlkörpern, die als endliche Erweiterungen über den rationalen Zahlen gegeben sind. Die Bestimmung der Einheitengruppe (des Regulators) eines algebraischen Zahlkörpers gehört neben der Berechnung der Klassengruppe (der Klassenzahl), der Maximalordnung (der Diskriminante) und der Galoisgruppe zu den wichtigsten Aufgaben der konstruktiven algebraischen Zahlentheorie. Hierbei interessiert man sich sowohl für theoretische Grundlagen der Strukturen dieser Größen als auch für die Entwicklung von Algorithmen zur expliziten Berechnung.

Während die Struktur der Einheitengruppe seit nunmehr rund 150 Jahren durch Dirichlet bekannt ist, entwickelte sich die Berechnung der Einheitengruppe durch algorithmische Verfahren in „natürlicher Weise“ mit dem Einheitenrang des Zahlkörpers. Der berühmteste Algorithmus ist hierbei wohl der Kettenbruchalgorithmus von Lagrange zur Berechnung der Grundeinheit einer reell–quadratischen Ordnung.

Durch zahlengeometrische Interpretationen des Kettenbruchverfahrens gelang es Minkowski [24] und Voronoi [39] ähnliche Verfahren für kubische Zahlkörper zu entwickeln. In Buchmann [4] konnten dann die Ideen von Voronoi auf beliebige Zahlkörper mit Einheitenrang 1 oder 2 ausgedehnt werden.

Die zwei zur Zeit bekanntesten Verfahren zur Berechnung von Einheitengruppen in Zahlkörpern mit beliebigem Einheitenrang sind die Algorithmen von Pohst [30] und Buchmann [5]. Ein guter Überblick über beide Verfahren ist in dem Buch von Pohst [31] enthalten, experimentelle Untersuchungen von Implementierungen dieser Algorithmen finden sich in Buchmann/Jüntgen/Pohst [8], Wildanger [41]. Beide Methoden verwenden im wesentlichen eine Form von Reduktionstheorie. Der Algorithmus von Buchmann ist in der Lage, Grundeinheiten zu berechnen und verwendet hierzu eine starke Reduktionsbedingung. Das Verfahren von Pohst liefert bei schwächerer Reduktionsbedingung basierend auf LLL-Reduktion nur ein System von maximal vielen unabhängigen Einheiten, die dann noch zur vollen Einheitengruppe erweitert werden müssen. In der Praxis erwies sich die zweite Methode als wesentlich effizienter.

Ein Ergebnis der Reduktionstheorie ist es, ein Erzeugendensystem für die Einheitengruppe eines Zahlkörpers anzugeben. Wir greifen diese Idee auf und werden mit geometrischen Mitteln ebenfalls Erzeugendensysteme finden. Anhand numerischer Beispiele werden wir unsere Ergebnisse mit denen der Reduktionstheorie vergleichen.

Eine weitere spezielle Situation der Einheitenberechnung ist gegeben, falls der betrachtete Zahlkörper über Teilkörper verfügt. Die ersten Ergebnisse auf diesem Gebiet wurden wie in vielen anderen Fällen für Kreisteilungskörper erzielt. Die Teilkörper sind hier einfach zu bestimmen, und man hat den Vorteil, daß der Einheitenrang des maximalen total reellen Teilkörpers mit dem des Kreisteilungskörpers übereinstimmt. Es konnte bewiesen werden, daß der erzeugte Index der Einheiten aus dem maximalen total reellen Teilkörper in der Einheitengruppe des Kreisteilungskörper höchstens 2 ist (siehe Washington[40]).

Dieses Thema erscheint umso brisanter, da es in jüngster Zeit effiziente Implementationen (siehe Klüners [19]) zur Berechnung der Teilkörper gibt. Umfangreiche Untersuchungen zu diesem Thema finden sich u.a. in Pohst [29], Leopoldt [21], Parry [27], Stender [37] und Kubota [20]. Oftmals geht man hier in die galoissche Hülle eines vorgegebenen Teilkörpers und betrachtet dessen Einheitengruppe. Dadurch gelingt es in vielen Fällen, die anderen Teilkörper explizit anzugeben und durch das Erzeugnis aller Einheiten aus den Teilkörpern ein maximal unabhängiges Einheitensystem in der galoisschen Hülle zu erhalten. Ein zweiter Effekt der galoisschen Erweiterung ist es, daß sich der Index des maximal unabhängigen Einheitensystems in der vollen Einheitengruppe abschätzen läßt. Hierbei benutzte man Methoden, die sich an die oben erwähnten Kreisteilungskörper anlehnen. Implementierungen dieser Ideen für quartische Zahlkörper finden sich in Holzberg [16].

Ein Ziel dieser Arbeit ist es, Situationen zu untersuchen, in denen man nicht ein maximales unabhängiges Einheitensystem durch Teilkörper erhält. Wir zeigen, daß die Untergruppe der (totalen) Relativeinheiten eine ausgezeichnete Rolle spielt. Die

Erzeuger der Relativeinheiten ergänzen die Einheiten eines Teilkörpers zu einem maximal unabhängigen Einheitensystem im Oberkörper. Leider bildet das so gebildete Einheitensystem i. allg. noch kein Grundeinheitensystem des Oberkörpers. Wir zeigen, daß nur Teiler des Relativgrades im Index zur vollen Einheitengruppe des Oberkörpers aufgehen können.

Eine besondere Frage ist, wie wir die Einheitengruppe in einem kleinsten gemeinsamen Oberkörper zweier vorgegebener Teilkörper berechnen können. Wir betrachten den kleinsten gemeinsamen Oberkörper eines reell–quadratischen und eines einfach reellen kubischen Zahlkörpers. Die (totale) Relativeinheitengruppe wird in dieser Situation von einem Element erzeugt. Für das Einheitensystem bestehend aus den beiden Grundeinheiten der Teilkörper und der Relativeinheit untersuchen wir den Index in der vollen Einheitengruppe. Dabei zeigt sich, daß mögliche Abweichungen zur vollen Einheitengruppe durch p-te Potenzen exakt angegeben werden können.

Im letzten Abschnitt dieser Arbeit beschäftigen wir uns mit einer parametrischen Familie von Zahlkörpern. Die Familie ist gegeben durch das parametrisierte Polynom

$$f_a(t) = t^4 - (a^2 + a + 1)t^2 + (a^2 + a)t + 1 \quad (a \in \mathbb{Z}^{\geq 3}).$$

Wir zeigen, daß eine Wurzel η des Polynoms eine total reelle Körpererweiterung vierten Grades über $\mathbb{Q}$ erzeugt. Dabei geben wir Abschätzungen der Nullstellen in Abhängigkeit des Parameters a an, so daß wir eine untere und obere Regulatorabschätzung bekommen. Der Zerfällungskörper des Polynoms hat Grad 24 über $\mathbb{Q}$. Diese Tatsache folgt aus der Betrachtung der Galoisgruppe von $f_a(t)$. Es zeigt sich durch Anwendung von Resolventen, daß die Galoisgruppe isomorph zur symmetrischen Gruppe auf 4 Elementen ist. In diesem Zusammenhang werden wir beweisen, daß die Resolvente stets irreduzibel und die Diskriminante von $f_a(t)$ kein Quadrat in $\mathbb{Z}$ für $a > 3$ ist. Für die drei Einheiten $\eta, \eta - 1$ und $\eta - a$ des Zahlkörpers werden wir beweisen, daß diese immer ein Grundeinheitensystem der Gleichungsordnung $\mathbb{Z}[\eta]$ bilden. Dabei verwenden wir folgende Strategie. Mittels Regulatorabschätzungen zeigen wir, daß der Index von $\eta, \eta - 1, \eta - a$ für $a > 100$ immer kleiner drei ist. Die verbleibenden Quadratwurzeln werden dann gesondert behandelt. Die nun verbleibenden Fälle für $3 \leq a \leq 100$ werden mittels Software [18] nachgerechnet. Für den Zerfällungskörper konstruieren wir ein erzeugendes Polynom mit Grad 24 in Abhängigkeit des Parameters a. Abschließend leiten wir ein allgemeines Konstruktionsprinzip für total reelle Zahlkörper beliebigen Grades größer vier ab.

2. Grundlagen und Notation

In dieser Arbeit verwenden wir folgende Bezeichnungen:

$\mathbb{N}$	Menge der natürlichen Zahlen
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{P}$	Menge der Primzahlen
$\mathbb{Q}$	Menge der rationalen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{C}$	Menge der komplexen Zahlen
$\Re z$	Realteil der komplexen Zahl z
$\Im z$	Imaginärteil der komplexen Zahl z
$\mathcal{F}$	Zahlkörper
$\mathcal{F}^{\times}$	Menge der invertierbaren Elemente in $\mathcal{F}$
$[\mathcal{F}:\mathbb{Q}]$	Körpergrad von $\mathcal{F}$ über $\mathbb{Q}$
$d_{\mathcal{F}}$	Diskriminante des Zahlkörpers $\mathcal{F}$
f	ein erzeugendes Polynom von $\mathcal{F}$
m_{α}	Minimalpolynom von α über $\mathbb{Q}$
d_f	Diskriminante des Polynoms f
r_1	Anzahl der reellen Nullstellen von f
r_2	halbe Anzahl der nichtreellen Nullstellen von f
(r_1, r_2)	Signatur des Zahlkörpers
$U_{\mathcal{F}}$	Einheitengruppe von $\mathcal{F}$
$r_{\mathcal{F}}$	Einheitenrang von $\mathcal{F}$
$TU_{\mathcal{F}}$	Untergruppe der Torsionseinheiten
$R_{\mathcal{F}}$	Regulator von $\mathcal{F}$
$< \varepsilon_1, \dots, \varepsilon_r >$	multiplikatives Erzeugnis der Elemente $\varepsilon_1, \dots, \varepsilon_r$
$\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$	Galoisgruppe von $\mathcal{F}$ über $\mathbb{Q}$
$o_{\mathcal{F}}$	Maximalordnung von $\mathcal{F}$
$\mathrm{C}ov(\mathcal{F}, \mathcal{K})$	kleinster gemeinsamer Oberkörper von $\mathcal{F}$ und $\mathcal{K}$
$\mathcal{O}$	Ordnung in einen Zahlkörper
$\omega^{(j)}$	die j-te Konjugierte von ω
$N_{\mathcal{E}/\mathcal{F}}(\omega)$	Norm von $\omega \in \mathcal{E}$ über $\mathcal{F}$
$T_{\mathcal{E}/\mathcal{F}}(\omega)$	Spur von $\omega \in \mathcal{E}$ über $\mathcal{F}$
$\lvert S\rvert$	Mächtigkeit der Menge S
C_4	zyklische Gruppe der Ordnung 4
V_4	Kleinsche Vierergruppe
S_n	symmetrische Gruppe mit n Elementen

Alle in dieser Arbeit benutzten Eigenschaften von algebraischen Zahlkörpern, algebraischen Zahlen und Idealen lassen sich in den Büchern von Pohst/Zassenhaus [34] und Pohst [31] nachlesen. Dies gilt insbesondere auch für Eigenschaften, die für die Arithmetik bei der Implementation von Algorithmen notwendig sind. Wir wollen an dieser Stelle nur die für diese Arbeit zentrale Aussage zitieren.

Wie bereits in der Einleitung erwähnt, ist der Dirichletsche Einheitensatz die Grundlage für unsere Untersuchungen. Die Struktur der Einheitengruppe eines algebraischen Zahlkörpers $\mathcal{F}$ wird dadurch wie folgt beschrieben:

$$U_{\mathcal{F}} =< \zeta > \times < \varepsilon_1 > \times \cdots \times < \varepsilon_{r_{\mathcal{F}}} >,$$

wobei ζ ein Erzeuger der Torsionseinheitengruppe mit endlicher Ordnung $w_{\mathcal{F}}$ ist, also eine primitive $w_{\mathcal{F}}$-te Einheitswurzel. Die Erzeuger $\varepsilon_1, \ldots, \varepsilon_{r_{\mathcal{F}}}$ des torsionsfreien Anteils von $U_{\mathcal{F}}$ bezeichnet man als Grundeinheiten von $\mathcal{F}$ oder auch als Basis von $U_{\mathcal{F}}$.

KAPITEL II

Geometrische Betrachtungen

In diesem Kapitel stellen wir einige grundlegende Eigenschaften von algebraischen Zahlen bzw. algebraischen Zahlkörpern zusammen, die wir zumeist aus geometrischen Betrachtungen herleiten. Die Ergebnisse können in [34] oder [31] nachgeschlagen werden. Wir erwähnen nur die für die Arbeit unmittelbar wichtigsten Grundlagen. Dazu fixieren wir einen Zahlkörper $\mathcal{F}$ über $\mathbb{Q}$ mit $[\mathcal{F} : \mathbb{Q}] = n$ und Signatur (r_1, r_2).

1. Gitter

Um geometrische Charakterisierungen von algebraischen Zahlen zu bekommen, bedarf es eines Zusammenhanges zwischen unserem Zahlkörper $\mathcal{F}$ und dem euklidischen Vektorraum $\mathbb{R}^n$. Dazu sei ω aus $\mathcal{F}$ mit den Konjugierten $\omega^{(1)}, \ldots, \omega^{(n)}$ gegeben. Wir ordnen die $n = r_1 + 2r_2$ Konjugierten von ω so an, daß $\omega^{(1)}, \ldots, \omega^{(r_1)}$ die reellen Konjugierten sind und für die restlichen gilt:

$$\omega^{(r_1+j)} = \overline{\omega^{(r_1+j+r_2)}} \qquad (j \in \{1, \ldots, r_2\}).$$

Dann betrachten wir die Abbildung

$$\begin{array}{cccl} \varphi\colon & \mathcal{F} & \to & \mathbb{R}^n : \\ & \omega & \mapsto & \Big(\omega^{(1)}, \ldots, \omega^{(r_1)}, \quad \Re\omega^{(r_1+1)}, \ldots, \Re\omega^{(r_1+r_2)}, \\ & & & \qquad , \Im\omega^{(r_1+1)}, \ldots, \Im\omega^{(r_1+r_2)}\Big)^{tr}, \end{array}$$

die unseren Zahlkörper in den euklidischen Vektorraum $\mathbb{R}^n$ überführt. Definieren wir nun noch eine Multiplikation auf dem $\mathbb{R}^n$, welche die Anordnung und Aufspaltung der komplexen Konjugierten beachtet, so erhalten wir die bekannte Aussage:

SATZ II.1. *Für die Abbildung φ gilt:*

(1) *φ ist ein additiver Monomorphismus.*
(2) *Für eine Ordnung $\mathcal{O}$ des Zahlkörpers $\mathcal{F}$ mit $\mathbb{Z}$-Basis $\omega_1, \ldots, \omega_n$ ist*

$$\varphi(\mathcal{O}) = \bigoplus_{i=1}^{n} \mathbb{Z}\varphi(\omega_i)$$

ein vollständiges Gitter im $\mathbb{R}^n$.

Beweis: Klar.

□

Für geometrische Betrachtungen erweist sich das Konjugiertengitter als ungeeignet, was in der Aufspaltung der komplexen Nullstellen begründet ist. Deshalb definieren wir eine zweite Abbildung

$$\begin{array}{cccl} \bar{\varphi}: & \mathcal{F}^{\times} & \to & \mathbb{R}^{r_1+r_2}: \\ & \omega & \mapsto & \left(|\omega^{(1)}|, \ldots, |\omega^{(r_1+r_2)}|\right)^t, \end{array}$$

indem wir die Beträge der komplexen Zahlen ausnutzen.

Zunächst scheint sich die Abbildung nachteilig auszuwirken, da die additive Struktur aufgrund des Absolutbetrages verloren geht. Das Bild einer Ordnung unter $\bar{\varphi}$ ist jetzt kein Gitter mehr, und natürlich ist mit $\bar{\varphi}(1) = \bar{\varphi}(-1)$ die Abbildung nicht mehr injektiv. Es wird sich jedoch im folgenden Satz zeigen, daß im Bild von $\bar{\varphi}$ sich die Einheitengruppe des Zahlkörpers in ausreichender Weise wiederfindet.

SATZ II.2. *Für die Abbildung $\bar{\varphi}$ gilt:*

(1) *Die Abbildung $\bar{\varphi}$ ist ein (multiplikativer) Gruppenhomomorphismus.*
(2) *Für eine Ordnung $\mathcal{O}$ des Zahlkörpers $\mathcal{F}$ ist $\bar{\varphi}(\mathcal{O})$ eine diskrete Menge im $\mathbb{R}^{r_1+r_2}$.*
(3) *Für die Abbildung $\bar{\varphi}_{|U_{\mathcal{F}}}$ gilt $\ker(\bar{\varphi}) = TU_{\mathcal{F}}$, und wir erhalten*

$$\bar{\varphi}(U_{\mathcal{F}}) \cong U_{\mathcal{F}}/TU_{\mathcal{F}}.$$

(4) *Für $\omega \in \mathcal{F}^{\times}$ gilt*

$$|N_{\mathcal{F}/\mathbb{Q}}(\omega)| = \left|\omega^{(1)}\right|^{c_1} \cdots \left|\omega^{(r_1+r_2)}\right|^{c_{r_1+r_2}}$$

mit $c_1 = \ldots = c_{r_1} = 1$ und $c_{r_1+1} = \ldots = c_{r_1+r_2} = 2$.

Beweis: Für den multiplikativen Gruppenhomomorphismus versehen wir den $\mathbb{R}^{r_1+r_2}$ noch mit punktweiser Multiplikation. Die Aussagen (1)–(4) lassen sich dann einfach nachrechnen.

□

Insbesondere Teil (3) des vorherigen Satzes zeigt, daß sich die Einheitengruppe modulo der Torsion in $\mathcal{F}$ wiederfindet. Dieses schmerzt aber in keinster Weise, da die Berechnung der Torsionseinheitenuntergruppe i. allg. kein Problem ist. Wir verweisen auf das Buch von Pohst [31], in dem sich ein effizienter Algorithmus zur Berechnung der Torsionseinheitenuntergruppe befindet. Desweiteren ist die Übertragung der multiplikativen Struktur nun wesentlich einfacher als bei der Konjugiertenabbildung φ. Neben dem Normbetrag benötigen wir noch ein zweites „Maß“ für algebraische Zahlen.

Definition II.3. *Für eine Zahl α in $\mathcal{F}$ definieren wir die* **Höhe** *von α durch*

$$H(\alpha) = \prod_{i=1}^{r_1+r_2} \max\{1, |\alpha^{(i)}|\}.$$

Wir erkennen unmittelbar, daß die Höhe jeder Torsionseinheit gleich 1 ist. Ebenfalls offensichtlich ist die Höhe einer ganzen algebraischen Zahl aus $\mathcal{F}$ größer oder gleich 1. Schränken wir die Höhe auf ganze algebraische Zahlen aus $\mathcal{F}$ ein, so stellt sich die Frage, ob ganze algebraische Zahlen, die keine Torsionseinheiten sind, nicht eine Höhe echt größer 1 haben. Das folgende Resultat beantwortet diese Frage.

Satz II.4. *Sei α in $\mathcal{F}$ eine ganze algebraische Zahl, die nicht Null ist. Falls für $n = [\mathcal{F} : \mathbb{Q}]$*

$$H(\alpha) \leq 1 + \frac{1}{52n \log 6n}$$

gilt, dann ist α eine Torsionseinheit.

Beweis: Siehe Blanskby/Montgomery [2].

□

Für ganze Zahlen in $\mathcal{F}^\times \setminus TU_\mathcal{F}$ gibt es somit eine **Mindesthöhe größer 1**, die nur vom Grad der Körpererweiterung $\mathcal{F}$ über $\mathbb{Q}$ abhängt. Von ähnlicher „Natur“ ist die folgende Aussage, da sich beide Resultate in der Diskretheit der zugrunde liegenden Punktmenge im $\mathbb{R}^{r_1+r_2}$ begründen.

Satz II.5. *In einen Zahlkörper $\mathcal{F}$ gibt es nur endlich viele ganze algebraische Zahlen mit beschränkter Höhe.*

Beweis: Siehe [34].

□

2. Reduktionstheorie

Wir werden kurz die von Buchmann [5] entwickelte Reduktionstheorie in einer leicht vereinfachten Form wiedergeben. Die wesentlichen Ideen dieser Theorie werden wir dann im nächsten Abschnitt für unsere Zwecke in neuer Form aufgreifen, um eine geometrische Charakterisierung der Einheitengruppe zu geben.

Definition II.6. *Eine ganze Zahl $\mu \neq 0$ in $\mathcal{F}$ heißt* **Minimum***, falls keine ganze Zahl $\beta \neq 0$ in $\mathcal{F}$ existiert mit*

$$|\beta^{(i)}| < |\mu^{(i)}| \quad (1 \leq i \leq r_1 + r_2).$$

Aus der Norm für ganze Elemente von $\mathcal{F}$ folgt, daß jede Einheit von $\mathcal{F}$ ein Minimum ist. Die Menge der Minima von $\mathcal{F}$ ist damit unendlich, jedoch ist zumindest die Absolutnorm eines Minimums beschränkt.

Lemma II.7. *Der Absolutbetrag der Norm eines Minimums ist beschränkt durch*

$$\mathrm{C}_{\mathcal{F}} = \left(\frac{2}{\pi}\right)^{r_2} |d_{\mathcal{F}}|^{1/2}.$$

Beweis: Siehe [5].

□

Damit ist die Anzahl paarweise nicht assoziierter Minima endlich. Die Idee, nicht assoziierte Elemente beschränkter Norm zur Einheitenberechnug zu nutzen, wird in vielen Algorithmen benutzt. In [33] findet man ein solches Verfahren inklusive einer Implementierung. Vorteilhaft bei der Reduktionstheorie ist, daß die Anzahl der nicht assoziierten Minima erheblich kleiner ist als die Anzahl der nicht assoziierten ganzen Elemente von $\mathcal{F}$, wobei die Norm in beiden Fällen durch $\mathrm{C}_{\mathcal{F}}$ beschränkt ist.

Definition II.8. *Ein Minimum μ von $\mathcal{F}$ heißt* **Nachbar** *eines Minimums ν von $\mathcal{F}$, wenn es in $\mathcal{F}$ keine ganze Zahl β gibt mit:*

(1) $|\beta^{(i)}| < \max\{|\mu^{(i)}|, |\nu^{(i)}|\} \qquad (1 \leq i \leq r_1 + r_2)$
und
(2) $|\mu| \leq |\nu|$. *(Dabei ist $|\varepsilon| := |\varepsilon^{(i)}|$ für einen festen Konjugiertenbetrag $i \in \{1, \ldots, r_1 + r_2\}$.)*

KOROLLAR II.9. *Die Anzahl der Nachbarn eines Minimums von $\mathcal{F}$ ist endlich.*

Beweis: Siehe [5].

□

DEFINITION II.10. *Eine Menge C von Minima in $\mathcal{F}$ heißt* **Zykel** *von Minima in $\mathcal{F}$, wenn gelten:*

(i) *die Elemente von C sind paarweise nicht assoziiert,*
(ii) *für jedes Element von C sind alle seine Nachbarn assoziiert zu Elementen aus C.*

DEFINITION II.11. *Es sei C ein Zykel in $\mathcal{F}$. Dann heißt*

$$U(C) := \{\varepsilon \in U_{\mathcal{F}} \quad | \quad \varepsilon = \frac{\mu}{\nu} \text{ mit } \mu \text{ in } C \text{ und } \nu \text{ Nachbar eines Elementes aus } C\}$$

die Menge der **Randeinheiten**.

Ein solcher Zykel läßt sich auch als Graph deuten. Die Elemente von C bilden die Knoten und die Kanten werden durch die Nachbarnrelation gebildet. In [17] wurden solche Graphen untersucht und dargestellt.

SATZ II.12. *Sei C ein Zykel von Minima in $\mathcal{F}$. Dann ist die Anzahl der Elemente in C und $U(C)$ endlich, und die Menge der Randeinheiten erzeugt die Einheitengruppe von $\mathcal{F}$.*

Beweis: Siehe [5].

□

Die Methode wurde von Jüntgen [17] implementiert und näher untersucht. Die Berechnung eines Zykels erwies sich algorithmisch als sehr schwierig und aufwendig. Zudem wußte man, daß die Zykellänge in der Größenordnung von $O(R_{\mathcal{F}})$ liegt, siehe Buchmann [6]. Dementsprechend ist die Anzahl der Randeinheiten groß. Bei wachsender Diskriminante (wachsendem Regulator) und damit steigender Zykellänge zeigte sich, daß die Anzahl der Randeinheiten unverhältnismäßig stark ansteigt gegenüber dem Einheitenrang des Zahlkörpers. Insbesondere erwies sich die Redundanz als erheblich, d.h., bei Berechnung der Randeinheiten durch Zykelelemente erhielt man die gleiche Einheit mehrfach. Verglichen mit anderen Verfahren erwies sich der Algorithmus als unzweckmäßig zur Berechnung von Grundeinheiten. Für spätere Vergleiche geben wir folgendes Beispiel.

$d_{\mathcal{F}}$	$R_{\mathcal{F}}$	$\lvert C\rvert$	$\lvert U(C)\rvert$
50225	12.550	19	172
50432	17.096	19	125
50437	12.869	16	106
50688	16.696	13	120
50688	27.779	28	248
50693	12.901	17	114
50725	10.136	9	109
50737	18.893	18	137
50908	25.996	30	238
51005	13.029	14	91
51125	9.493	10	104
51153	23.933	27	188
51181	13.386	12	84
51200	9.828	5	51
51264	30.609	28	217
51725	8.575	7	77
51776	9.416	7	43
51984	43.836	50	375
52025	16.761	23	207
52052	29.543	32	248
52176	16.822	18	125
52221	11.600	4	29
52225	14.235	19	181
52396	28.456	33	273
52400	14.172	20	172
52525	13.262	18	155
52592	11.074	13	81
52625	15.797	18	181
52816	19.651	23	184
53121	25.442	34	241
53312	30.741	35	275
53333	11.726	10	75
53361	13.103	16	124
53401	21.281	24	190
53568	20.463	21	184
53589	24.640	30	223
53824	15.355	13	133
53840	23.134	22	183
54225	13.859	22	193
54249	18.159	16	114
54332	47.150	62	457
54381	16.754	20	136
54725	7.236	10	79
54764	50.616	59	461
54848	11.959	13	118
54864	26.667	27	222
55025	16.561	20	189
55297	24.637	30	210
55377	24.434	25	193
55409	16.505	16	124
55552	18.520	18	138
55585	27.673	37	263
55600	11.748	16	135
55661	20.800	25	178
55665	21.693	25	194
55728	21.660	24	181
55872	14.287	12	98
55872	12.714	18	122
56025	15.296	15	118
56125	12.621	16	141
56137	24.467	25	202
56144	17.675	17	129
56333	18.230	19	138
56384	31.622	31	214
56592	37.751	42	316
56677	16.143	19	144
56749	15.700	21	156
56777	22.998	24	213
56896	12.504	12	80
57077	11.093	12	82
57600	17.204	22	182
57600	11.236	6	54
57600	14.795	24	183
57609	18.354	18	133
57909	24.926	31	204
58000	7.137	12	86
58025	17.341	20	195
58049	17.353	19	155
58217	22.737	24	181
58397	34.545	37	294
58469	12.519	13	97
58672	19.222	23	174
58896	31.493	28	242
59457	25.058	27	203
59468	49.597	59	427
59600	10.527	14	119
59648	21.718	20	168
59725	9.959	13	107
59749	16.524	16	107

TABELLE II.1. Tabelle über die Anzahl von Minima eines Zykels und die Anzahl der Randeinheiten für total reelle Körper vierten Grades mit $50000 < d_{\mathcal{F}} < 60000$.

Beispiel II.13. *Wir betrachten den total reellen Zahlkörper vierten Grades mit Diskriminante* $d_{\mathcal{F}} = 59468$. *In Jüntgen* [17] *berechneten wir einen Zykel mit* 59 *Elementen, und die Anzahl der Randeinheiten betrug* 427.

Andere typische Werte finden sich in Tabelle II.1.

Ferner bemerken wir, daß die Theorie nur eine unmittelbare Beschreibung des Erzeugendensystems für die Einheitengruppe gibt. Einerseits erzeugt die Menge der Randeinheiten die Einheitengruppe, andererseits ist jede Randeinheit über die sehr komplexen Eigenschaften eines Zykels charakterisiert. Wir werden im nächsten Abschnitt diesen Umstand beseitigen und wollen die Einheitengruppe eines Zahlkörpers mittels geometrischer Bedingungen auf Einheiten selbst beschreiben.

In [7] und [8] wurde versucht, die Berechnung von Nachbarn auf spezielle Nachbarn einzuschränken. Dabei konzentierte man sich auf Nachbarn, die einfach zu berechnen sind.

Definition II.14. *Ein Nachbar* μ *der* 1 *in* $\mathcal{F}$ *heißt* **Hauptnachbar** *in Richtung* $i \in \{1, \dots, r_1 + r_2\}$, *falls*

$$|\mu^{(i)}| > 1 \text{ und } |\mu^{(j)}| < 1 \text{ sonst } (j \in \{1, \dots, r_1 + r_2\} \setminus \{i\}).$$

Bemerkung II.15. *Aus dem Minkowskischen Gitterpunktsatz folgt die Existenz eines Hauptnachbarn für jedes* $i \in \{1, \dots, r_1 + r_2\}$, *was eine gezielte Berechnung ermöglicht.*

<u>Beweis:</u> Siehe [34] zur Konstruktion von Einheiten in Zahlkörpern.

□

Allerdings hat die Einschränkung auf Hauptnachbarn einen negativen Effekt. Die damit berechneten Einheiten erzeugen nur noch eine Untergruppe vom endlichen Index in der vollen Einheitengruppe von $\mathcal{F}$.

Beispiel II.16. *Wir betrachten einen total reellen Zahlkörper* $\mathbb{Q}(\rho)$ *sechsten Grades. Für* ρ *gilt*

$$\rho^6 + \rho^5 + 8\rho^4 + 8\rho^3 - 6\rho^2 - 6\rho + 1 = 0.$$

Dann liefert die Berechnug von Einheiten mittels Hauptnachbarn sechs Einheiten $\varepsilon_i \in \mathbb{Q}(\rho)$ *mit*

$$|{\varepsilon_i}^{(i)}| > 1 \quad (1 \leq i \leq 6)$$

und

$$|{\varepsilon_i}^{(j)}| < 1 \quad (1 \leq j \leq 6, j \neq i).$$

Für den Index dieser Einheiten in der vollen Einheitengruppe von $\mathbb{Q}(\rho)$ gilt:

$$[U_{\mathbb{Q}(\rho)} :< \varepsilon_1, \dots, \varepsilon_6 >] = 434.$$

Das Beispiel lehrt, daß die Einschränkung auf Hauptnachbarn einen großen Index zur Folge haben kann. In [8] wurden dann noch Nachbarn zugelassen, die zwei Konjugiertenbeträge größer 1 hatten. Dabei konnten wesentlich bessere Resultate erzielt werden. Wir werden im nächsten Abschnitt die Idee solcher „Freiheitsgrade" präzisieren.

3. Einheiten dicht an 1

Vom konstruktiven Standpunkt sind geometrische Charakterisierungen interessant, die eine endliche Menge zur Erzeugung der Einheitengruppe ergeben. Eine solche erste, wenn auch einfache, Aussage findet sich z.B. in Borevič/Šafarevič [9]. Dort gibt man eine Kugel im Logarithmenraum der Einheiten an, die eine Basis enthält. Der Radius der Kugel hängt dabei im wesentlichen von der Diskriminante des Körpers ab. Allerdings ist die Abschätzung für praktische Anwendungen völlig unbrauchbar.

In diesem Abschnitt werden wir eine Charakterisierung der Grundeinheit in einem reell–quadratischen Zahlkörper auf Zahlkörper höheren Grades erweitern. Wir beachten, daß der Dirichletsche Einheitensatz eine rein gruppentheoretische Beschreibung der Einheitengruppe ist. Neben der Eigenschaft, die Einheitengruppe des Zahlkörpers zu erzeugen, läßt sich *die Grundeinheit* ε eines reell–quadratischen Zahlkörpers auch geometrisch beschreiben. Beachten wir, daß mit ε auch ε^{-1}, $-\varepsilon^{-1}$ und $-\varepsilon$ Grundeinheiten sind, so können wir o.B.d.A. $\varepsilon > 0$ und $|\varepsilon^{(1)}| > 1$ annehmen. Unter allen diesen Einheiten ist nun ε dadurch charakterisiert, daß keine weitere Einheit η mit $\eta > 0$ und $|\varepsilon^{(1)}| > |\eta^{(1)}| > 1$ existiert. Geometrisch bedeutet dies, daß der erste Konjugiertenbetrag der Grundeinheit „dichter an 1" liegt als der aller anderen nicht trivialen Einheiten. Damit läßt sich die Grundeinheit in einem reell–quadratischen Zahlkörper *eindeutig* normieren.

Die eindeutige Normierung für ein Grundeinheitensystem $\varepsilon_1, \dots \varepsilon_{r_\mathcal{F}}$ eines beliebigen Zahlkörpers scheint sehr problematisch zu sein. Dazu beachten wir, daß jede unimodulare Transformation die Grundeinheiten $\varepsilon_1, \dots, \varepsilon_{r_\mathcal{F}}$ wieder in Grundeinheiten überführt.

Zunächst übertragen wir die geometrische Charakterisierung einer reell–quadratischen Grundeinheit auf Einheiten in beliebigen Zahlkörpern. Dazu definieren wir uns ein

Analogon zur Minimalitätsbedingung des ersten Konjugiertenbetrags der normierten Grundeinheit in Zahlkörpern höheren Grades.

DEFINITION II.17. *Eine Einheit $\varepsilon \in \mathcal{F}$ heißt* **dicht an 1**, *genau dann wenn keine Einheit $\eta \in \mathcal{F}$ existiert mit*

$$|\eta^{(i)}| < \max\{1, |\varepsilon^{(i)}|\} \quad (1 \leq i \leq r_1 + r_2).$$

Setze $S = \{\varepsilon \in U_{\mathcal{F}} | \quad \varepsilon$ ist dicht an 1 $\}$.

Mit der obigen Definition stellen wir noch keine expliziten Bedingungen an die Konjugiertenbeträge einer Einheit. Die Eigenschaft, dicht an 1 zu liegen, hängt nur von der Nichtexistenz einer Einheit bzgl. der Maximalitätsbedingung ab. Damit wir später Teilmengen von S auszeichen können, schränken wir mit der nächsten Definition die Anzahl der Konjugiertenbeträge einer Einheit größer 1 ein.

DEFINITION II.18. *Sei ε eine Einheit in $\mathcal{F}$. Dann nennen wir*

$$d(\varepsilon) := \left|\left\{|\varepsilon^{(i)}| > 1 | 1 \leq i \leq r_1 + r_2\right\}\right|$$

den **Freiheitsgrad** *von ε.*

Ferner setzen wir für $1 \leq i \leq r_1 + r_2$

$$S(i) = \{\varepsilon \in \mathcal{F} \quad | \quad \varepsilon \text{ ist dicht an } 1 \text{ und } d(\varepsilon) \leq i\},$$

und für die Menge S gilt $S = S(r_1 + r_2 - 1)$.

BEMERKUNG II.19. *Zunächst besitzen die Konjugiertenbeträge einer Einheit als Vektor im $\mathbb{R}^{r_1+r_2}$ natürlich $r_1 + r_2$ Freiheitsgrade. Da aber der Normbetrag einer Einheit gleich 1 ist, reduziert sich die Anzahl der Freiheitsgrade zu $r_1 + r_2 - 1$. Das Gitter der Einheiten bildet bei der entsprechenden Logarithmenabbildung (*[34]*) eine diskrete Teilmenge einer Hyperebene im Logarithmenraum.*

Die Eigenschaft dicht an 1 zu sein, verträgt sich mit der Verknüpfung der Einheitengruppe, d.h. der Inversenbildung.

SATZ II.20. *Sei $\varepsilon \in \mathcal{F}$ eine Einheit dicht an 1. Dann ist ε^{-1} ebenfalls dicht an 1.*

Beweis: Angenommen ε^{-1} läge nicht dicht an 1. Dann existiert eine Einheit $\eta \in U_{\mathcal{F}}$ mit

$$|\eta^{(i)}| < \max\{1, \frac{1}{|\varepsilon^{(i)}|}\} \quad (1 \leq i \leq r_1 + r_2).$$

Damit gilt

$$|\varepsilon^{(i)}||\eta^{(i)}| < |\varepsilon^{(i)}| \max\{1, \frac{1}{|\varepsilon^{(i)}|}\} \quad (1 \leq i \leq r_1 + r_2)$$

bzw.

$$|\varepsilon^{(i)}||\eta^{(i)}| < \max\{|\varepsilon^{(i)}|, 1\} \quad (1 \leq i \leq r_1 + r_2).$$

Damit existiert jedoch die Einheit $\varepsilon\eta \notin TU_{\mathcal{F}}$ mit

$$|(\varepsilon\eta)^{(i)}| < \max\{1, |\varepsilon^{(i)}|\} \quad (1 \leq i \leq r_1 + r_2).$$

Dies steht im Widerspruch zu ε dicht an 1.

□

Mit dem Freiheitsgrad messen wir nur die Anzahl von Konjugiertenbeträgen größer 1. Sprechen wir im folgenden von einer Verteilung auf den Konjugiertenbeträgen einer Einheit, so meinen wir eine explizite Vorschrift, welche Konjugiertenbeträge größer 1 sein sollen.

Zunächst beweisen wir, daß die Galoisgruppe von $\mathcal{F}/\mathbb{Q}$ in gewisser Weise invariant auf der Menge der Einheiten dicht an 1 operiert.

Satz II.21. *Die Elemente der Automorphismengruppe* $\mathrm{Aut}(\mathcal{F}/\mathbb{Q})$ *operieren auf der Menge* S*. Seien* $\sigma \in \mathrm{Aut}(\mathcal{F}/\mathbb{Q})$ *und* ε *eine Einheit in* $\mathcal{F}$*, die dicht an* 1 *liegt. Dann liegt* $\sigma(\varepsilon)$ *dicht an* 1.

Beweis: Sei ε in $\mathcal{F}$ dicht an 1. Nehmen wir an, daß $\sigma(\varepsilon)$ nicht dicht an 1 in $\mathcal{F}$ läge. Dann existiert eine Einheit η in $\mathcal{F}$ mit

$$|\eta^{(i)}| < \max\{1, |\sigma(\varepsilon)^{(i)}|\} \quad (1 \leq i \leq r_1 + r_2).$$

Dann folgt mit Anwendung von σ^{-1}

$$|\sigma^{-1}(\eta)^{(i)}| < \max\{1, |\varepsilon^{(i)}|\} \quad (1 \leq i \leq r_1 + r_2),$$

im Widerspruch zu ε dicht an 1.

□

Folgerung II.22. *Die Elemente der Automorphismengruppe* $\mathrm{Aut}(\mathcal{F}/\mathbb{Q})$ *operieren auf jeder der Mengen* $S(i)$ *für* $1 \leq i \leq r_1 + r_2$ *im Sinne von Satz* II.21.

Im reell–quadratischen Fall hat die Grundeinheit aufgrund der Minimalitätsbedingung an den ersten Konjugiertenbetrag die Eigenschaft, daß keine Wurzel von ihr im Zahlkörper liegt. Wir beweisen, daß Einheiten dicht an 1 die analoge Eigenschaft besitzen.

SATZ II.23. *Sei ε eine nicht triviale Einheit in $\mathcal{F}$, die dicht an* 1 *liegt. Dann liegt $\sqrt[p]{\varepsilon}$ nicht in $\mathcal{F}$ für alle Primzahlen p.*

<u>Beweis:</u> Aus der Annahme, $\sqrt[p]{\varepsilon}$ liegt in $\mathcal{F}$, und der Multiplikativität der Konjugiertenbeträge folgt sofort der Widerspruch zu ε dicht an 1.

□

SATZ II.24. *In $\mathcal{F}$ existieren nur endlich viele Einheiten dicht an* 1.

<u>Beweis:</u> In [34] wird bewiesen, daß die Menge S Einheiten $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2}$ mit der Eigenschaft

$$|{\varepsilon_i}^{(j)}| \begin{cases} > & 1 \quad \text{falls } i = j \\ < & 1 \quad \text{falls } i \neq j \end{cases} \quad (1 \leq i, j \leq r_1 + r_2).$$

enthält. Damit bekommen wir Schranken $B_i = |{\varepsilon_i}^{(i)}| \quad (1 \leq i \leq r_1 + r_2)$, so daß der i-te Konjugiertenbetrag jeder Einheit dicht an 1 durch B_i beschränkt ist für $1 \leq i \leq r_1 + r_2$. Es gibt jedoch nur endlich viele Einheiten mit beschränkten Konjugiertenbeträgen. Folglich auch nur endlich viele Einheiten dicht an 1.

□

FOLGERUNG II.25. *Die Menge S enthält ein maximales unabhängiges System von Einheiten.*

<u>Beweis:</u> Wähle $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1=r_{\mathcal{F}}}$ wie in Satz II.24 und verwende Lemma (2.12) in [34, Seite 332].

□

Für die Menge S gelten folgende Eigenschaften. Sie ist endlich und damit vom konstruktiven Standpunkt von großem Interesse. Sie enthält bis auf Torsionseinheiten nur ausgezeichnete Einheiten, die keine p-ten Wurzeln in $\mathcal{F}$ haben. In den beiden folgenden Sätzen werden wir jedoch die herausragende Eigenschaft von S beweisen, daß S die Einheitengruppe von $\mathcal{F}$ erzeugt.

SATZ II.26. *Die Menge S enthält alle Torsionseinheiten.*

<u>Beweis:</u> Es sei ε eine Torsionseinheit in $\mathcal{F}$, dann gilt $|\varepsilon^{(i)}| = 1$ für $1 \leq i \leq r_1 + r_2$. Da aber keine Einheit in $\mathcal{F}$ existiert deren Konjugiertenbeträge alle echt kleiner 1 sind, folgt die Behauptung.

□

SATZ II.27. *Die Menge S erzeugt die Einheitengruppe von $\mathcal{F}$.*

Beweis: Sei η eine beliebige Einheit in $\mathcal{F}$ und $S = \{\varepsilon_1, \ldots, \varepsilon_u\}$. Ziel ist es, die Höhe von η durch Multiplikation mit geeigneten Elementen aus S echt zu verkleinern. Nach endlich vielen Schritten erhalten wir dann eine Einheit aus S.

Falls η bereits in S enthalten ist, so ist nichts zu zeigen. Für $\eta \notin S$ existiert eine Einheit $\varepsilon \in S$ mit $|\varepsilon^{(i)}| < \max\{1, |\eta^{(i)}|\}$ für $1 \leq i \leq r_1 + r_2$. Die Konjugierten von ε und η seien o.B.d.A. wie folgt sortiert

(i) $1 \leq |\varepsilon^{(i)}| < |\eta^{(i)}|$ für $1 \leq i \leq j$ und $|\varepsilon^{(i)}| < 1$ für $i > j$,
(ii) $|\varepsilon^{(i)}| < 1 \leq |\eta^{(i)}|$ für $j+1 \leq i \leq k$ und $|\eta^{(i)}| < 1$ für $i > k$,
(iii) $|\varepsilon^{(i)}| \leq |\eta^{(i)}| < 1$ für $k+1 \leq i \leq l$,
(iv) $|\eta^{(i)}| < |\varepsilon^{(i)}| < 1$ für $i > l$.

Wir unterteilen den Beweis in zwei Schritte:

(1) Reduktion der Einheit η.
Für ε spalten wir das Produkt über $r_1 + r_2$-viele Konjugiertenbeträge wie folgt auf:
$$\prod_{i=1}^{r_1+r_2} |\varepsilon^{(i)}| = \prod_{i=1}^{l} |\varepsilon^{(i)}| \prod_{i=l+1}^{r_1+r_2} |\varepsilon^{(i)}|.$$
Dabei bemerken wir, daß der Fall (iv) stets für mindestens einen Index erfüllt ist. Dies gilt aufgrund von $\eta \notin S$ und der Wahl von $\varepsilon \in S$.
Es muß folglich mindestens ein Konjugiertenbetrag von η kleiner als der von ε sein. Damit gelten
$$\prod_{i=l+1}^{r_1+r_2} |\varepsilon^{(i)}| < 1 \text{ und } \prod_{i=1}^{l} |\varepsilon^{(i)}| > 1.$$
Nach der Wahl von k und l gilt $\prod_{i=k+1}^{l} |\eta^{(i)}| < 1$, und wir erhalten die Beziehung
$$\prod_{i=k+1}^{l} |\eta^{(i)}| < \prod_{i=1}^{l} |\varepsilon^{(i)}|$$
bzw.
$$\prod_{i=k+1}^{l} |\eta^{(i)}| \prod_{i=1}^{l} |\varepsilon^{(i)}|^{-1} < 1.$$
Multiplizieren wir beide Seiten mit $H(\eta)$, so ergibt sich
$$\prod_{i=k+1}^{l} |\eta^{(i)}| \prod_{i=1}^{l} |\varepsilon^{(i)}|^{-1} \prod_{i=1}^{k} |\eta^{(i)}| < \prod_{i=1}^{k} |\eta^{(i)}| = H(\eta).$$

Die linke Seite der Ungleichung läßt sich schreiben in der Form

$$\underbrace{\prod_{i=1}^{j} \frac{|\eta^{(i)}|}{|\varepsilon^{(i)}|} \prod_{i=j+1}^{k} \frac{|\eta^{(i)}|}{|\varepsilon^{(i)}|} \prod_{i=k+1}^{l} \frac{|\eta^{(i)}|}{|\varepsilon^{(i)}|}}_{H(\frac{\eta}{\varepsilon})} < H(\eta).$$

(2) Iteration der Reduktion.
Falls $\frac{\eta}{\varepsilon}$ nicht in S liegt, setzen wir $\eta \leftarrow \frac{\eta}{\varepsilon}$ und führen Schritt (1) erneut aus.
Da die Höhe der Einheit im Reduktionsschritt immer echt kleiner wird, erhalten nach s ($s \in \mathbb{N}$) vielen Schritten

$$\frac{\eta}{\tilde{\varepsilon}_1 \cdots \tilde{\varepsilon}_s} \in S$$

mit Einheiten $\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_s \in S$ und damit

$$\eta \in < \varepsilon_1, \ldots, \varepsilon_u > .$$

Beachte dazu, daß es nach Satz II.5 höchstens endlich viele Einheiten in $\mathcal{F}$ mit beschränkter Höhe gibt und somit der Reduktionsschritt (1) höchstens endlich oft durchgeführt wird.

Das Verfahren liefert somit einer Darstellung von η in den Einheiten $\varepsilon_1, \ldots, \varepsilon_u$.
□

Bemerkung II.28. *Mittels Satz* II.27 *ergeben sich noch folgende Aussagen:*

(1) *Satz* II.27 *liefert einen neuen Beweis dafür, daß die Einheitengruppe eines algebraischen Zahlkörpers endlich erzeugt ist.*
(2) *Für reell–quadratische Zahlkörper mit Grundeinheit ε besteht die Menge S aus den Elementen*

$$1, -1, \varepsilon, -\varepsilon, \frac{1}{\varepsilon}, -\frac{1}{\varepsilon}.$$

Damit haben wir nachvollzogen, daß reell–quadratische Zahlkörper den Einheitenrang 1 *besitzen.*
(3) *Für Zahlkörper mit Einheitenrang* 2 *können wir mit Hilfe von Berwick* [1] *beweisen, daß S wie im Fall des Einheitenrangs* 1 *ein System von Grundeinheiten enthält.*
(4) *Bei einem Einheitenrang größer als* 2 *bleibt die Frage offen, ob die Menge S immer ein Grundeinheitensystem enthält.*

Folgerung II.29. *Betrachten wir die aufsteigende Kette*

$$S(1) \subseteq S(2) \subseteq \cdots \subseteq S = S(r_1 + r_2 - 1),$$

so enthält jedes $S(i)$ $(1 \leq i \leq r_1 + r_2 - 1)$ *ein maximal unabhängiges Einheitensystem und alle Torsionseinheiten.*

Beweis: Klar.

□

Nachdem wir zeigen konnten, daß S endlich ist und die Einheitengruppe von $\mathcal{F}$ erzeugt, fragen wir uns nach der Mächtigkeit von S. Wir treffen einige Vorbereitungen, um uns ein Bild über die Anzahl der Elemente in S zu machen.

Im reell–quadratischen Falle gilt stets für eine Einheit, daß ein Konjugiertenbetrag größer gleich 1 und der andere kleiner gleich 1 ist. In Zahlkörpern von höherem Grad hat man bezüglich der Verteilung der Konjugiertenbeträge wesentlich mehr Freiheit.

Satz II.30. *Sei* $\{1, \ldots, r_1 + r_2\} = M \dot{\cup} \overline{M}$, *wo* $M, \overline{M}$ *beide nicht leer. Dann existiert in einem Zahlkörper* $\mathcal{F}$ *eine Einheit* ε *mit*

$$\begin{array}{lcll} |\varepsilon^{(i)}| & > & 1 \quad \textit{für} & i \in M \qquad \textit{und} \\ |\varepsilon^{(i)}| & < & 1 \quad \textit{für} & i \in \overline{M}. \end{array}$$

Beweis: Siehe Brunotte/Halter–Koch [3].

□

Der Satz gibt die Existenz einer Einheit für jede mögliche Verteilung auf den Konjugierten. Im folgenden spezialisieren wir dieses Problem, ob es zu jeder Verteilung auch Einheiten dicht an 1 gibt.

Satz II.31. *Sei* $\mathcal{F}$ *ein Zahlkörper mit* $r_1 + r_2 \geq 3$. *Dann existieren in* $\mathcal{F}$ *Einheiten mit Freiheitsgrad* 2, *die dicht an* 1 *liegen.*

Beweis: O.B.d.A. beweisen wir, daß in $\mathcal{F}$ eine Einheit η dicht an 1 existiert mit

$$|\eta^{(1)}| > 1, |\eta^{(2)}| > 1, |\eta^{(i)}| < 1 \text{ für } 3 \leq i \leq r_1 + r_2.$$

Seien $\varepsilon_1, \varepsilon_2$ nach Satz II.24 Einheiten in $\mathcal{F}$, die dicht an 1 liegen, mit

$$|{\varepsilon_1}^{(1)}| > 1, \quad |{\varepsilon_1}^{(i)}| < 1 \quad (1 \leq i \leq r_1 + r_2, i \neq 1),$$

$$|{\varepsilon_2}^{(2)}| > 1, \quad |{\varepsilon_2}^{(i)}| < 1 \quad (1 \leq i \leq r_1 + r_2, i \neq 2).$$

Dann betrachten wir das Produkt $\varepsilon_1\varepsilon_2$ und bemerken

$$|{\varepsilon_1}^{(i)}||{\varepsilon_2}^{(i)}| < 1 \text{ für } 3 \leq i \leq r_1 + r_2.$$

Wir unterscheiden drei Fälle:

(a) $|{\varepsilon_1}^{(1)}||{\varepsilon_2}^{(1)}| > 1$ und $|{\varepsilon_1}^{(2)}||{\varepsilon_2}^{(2)}| < 1$.
Dann gelten

$$1 < |{\varepsilon_1}^{(1)}||{\varepsilon_2}^{(1)}| < |{\varepsilon_1}^{(1)}| \text{ wegen } |{\varepsilon_2}^{(1)}| < 1 \text{ und}$$

$$|{\varepsilon_1}^{(i)}||{\varepsilon_2}^{(i)}| < 1 \text{ für } 2 \leq i \leq r_1 + r_2.$$

Damit existiert $\eta = \varepsilon_1\varepsilon_2$ in $U_{\mathcal{F}}$ mit

$$|\eta^{(i)}| < \max\{1, |{\varepsilon_1}^{(i)}|\} \quad (1 \leq i \leq r_1 + r_2),$$

im Widerspruch zu ε_1 dicht an 1.

(b) $|{\varepsilon_1}^{(1)}||{\varepsilon_2}^{(1)}| < 1$ und $|{\varepsilon_1}^{(2)}||{\varepsilon_2}^{(2)}| > 1$.
Analog wie in Teil (a).

(c) $|{\varepsilon_1}^{(1)}||{\varepsilon_2}^{(1)}| \geq 1$ und $|{\varepsilon_1}^{(2)}||{\varepsilon_2}^{(2)}| \geq 1$.
Durch $|{\varepsilon_1}^{(i)}||{\varepsilon_2}^{(i)}| < 1$ für $3 \leq i \leq r_1 + r_2$ ist ausgeschlossen, daß für $i = 1$ und $i = 2$ simultan Gleichheit gilt. Dann liegt entweder $\varepsilon_1\varepsilon_2$ selbst dicht an 1 oder es existiert eine Einheit η in $\mathcal{F}$ mit

$$1 < |\eta^{(i_0)}| < |{\varepsilon_1}^{(i_0)}||{\varepsilon_2}^{(i_0)}|$$

für mindestens ein i_0 in $\{1, 2\}$. Ist dies nur für einen Index, etwa $i_0 = 1$, erfüllt, so folgt

$$1 < |\eta^{(1)}| < |{\varepsilon_1}^{(1)}||{\varepsilon_2}^{(1)}| < |{\varepsilon_1}^{(1)}|$$

und wegen $|\eta^{(2)}| < 1$ wieder der Widerspruch zu ε_1 dicht an 1. Damit muß η die Eigenschaft haben:

$$|\eta^{(1)}| > 1, |\eta^{(2)}| > 1, |\eta^{(i)}| < 1 \text{ für } 3 \leq i \leq r_1 + r_2.$$

Da nur endlich viele Einheiten in $\mathcal{F}$ mit dieser Eigenschaft existieren, existiert auch eine Einheit dicht an 1 mit den ersten beiden Konjugiertenbeträgen größer 1 und den restlichen kleiner 1.

□

Wir beweisen durch geschickte Wahl zweier Einheiten dicht an 1, daß diese immer zu einem Grundeinheitensystem eines total reellen Zahlkörpers erweitert werden können.

Satz II.32. *Sei ε_1 eine Dirichlet-Einheit dicht an 1 in dem total reellen Zahlkörper $\mathcal{F}$ mit*

$$|\varepsilon^{(1)}| > 1,\ |\varepsilon^{(i)}| < 1 \quad (2 \leq i \leq r_1 + r_2).$$

Sei ε_{12} eine Einheit in $\mathcal{F}$ mit

$$|{\varepsilon_{12}}^{(1)}| > 1, |{\varepsilon_{12}}^{(2)}| > 1, |{\varepsilon_{12}}^{(i)}| < 1 \quad (3 \leq i \leq r_1 + r_2).$$

Ferner existiere in $\mathcal{F}$ keine Einheit α mit

$$|\alpha^{(1)}| > 1, 1 < |\alpha^{(2)}| < |{\varepsilon_{12}}^{(2)}|, |\alpha^{(i)}| < 1 \quad (3 \leq i \leq r_1 + r_2).$$

Dann ist ε_{12} dicht an 1 in $\mathcal{F}$ und $\varepsilon_1, \varepsilon_{12}$ lassen sich zu einem Grundeinheitensystem von $\mathcal{F}$ erweitern.

Beweis: Nach Satz II.31 existieren Einheiten in $\mathcal{F}$ mit Freiheitsgrad 2, die dicht an 1 liegen. Unter allen denen mit den ersten beiden Konjuguertenbeträgen größer 1 ist ε_{12} nach Voraussetzung diejenige mit dem kleinsten zweiten Konjugiertenbetrag.

Daß wir $\varepsilon_1, \varepsilon_{12}$ zu einem Grundeinheitensystem erweitern können, ist äquivalent damit, daß

$$\beta^p = \pm \varepsilon_1^m \varepsilon_{12}$$

mit $p \in \mathbb{P}$ und $0 \leq m < p$ keine Lösung in $\mathcal{F}$ besitzt. Ferner gilt $1 < |{\varepsilon_{12}}^{(1)}| < |{\varepsilon_1}^{(1)}|$, da ε_{12} dicht an 1 liegt.

Nehmen wir an, die obige Gleichung hätte eine Lösung. Dann gilt

$$1 < |\beta^{(1)}| = \sqrt[p]{|{\varepsilon_1}^{(1)}|^m |{\varepsilon_{12}}^{(1)}|} < |{\varepsilon_1}^{(1)}|.$$

Ist $|\beta^{(2)}| < 1$, so folgt

$$|\beta^{(i)}| < \max\{1, |{\varepsilon_1}^{(i)}|\} \ \ (1 \leq i \leq r_1 + r_2)$$

im Widerspruch zu ε_1 dicht an 1.

Für $|\beta^{(2)}| > 1$ folgt der Widerspruch zur Minimalität von ε_{12} im zweiten Konjugiertenbetrag.

Für $|\beta^{(2)}| = 1$ folgt $\beta = \pm 1$, da $\mathcal{F}$ total reell ist. Dies bedeutet $\varepsilon_1 \in < \varepsilon_{12} >$, was aufgrund der Verteilung der Konjugiertenbeträge nicht möglich ist.

$\square$

BEMERKUNG II.33. *Die Idee von Satz* II.32 *ist, ein Grundeinheitensystem rekursiv aufzubauen. Im nächsten Schritt müßte dann eine Einheit* ε_{123} *in Abhängigkeit von* ε_1 *und* ε_{12} *konstruiert werden, so daß sich* $\varepsilon_1, \varepsilon_{12}$ *und* ε_{123} *weiterhin zu einem Grundeinheitensystem erweitern lassen. Dazu müßten Potenzprodukte der Form*

$$\alpha^p = {\varepsilon_1}^l {\varepsilon_{12}}^m \varepsilon_{123}$$

mit $0 \leq m, l < p$ *analysiert werden. Im Gegensatz zum Beweis von* II.32 *kann* α *jetzt jede Verteilung auf den ersten drei Konjugiertenbeträgen annehmen. Insbesondere erhalten wir damit Einheiten, die bzgl. der Eigenschaft dicht an* 1 *nicht mehr mit den drei Einheiten* $\varepsilon_1, \varepsilon_{12}$ *und* ε_{123} *vergleichbar sind.*

FOLGERUNG II.34. *Sei* $\mathcal{F}$ *ein Zahlkörper mit* $r_1 + r_2 \geq 3$. *Dann gilt für die aufsteigende Kette*

$$S(1) \subset S(2) \subseteq \cdots \subseteq S = S(r_1 + r_2 - 1).$$

Beweis: Der Satz II.31 liefert die echte Inklusion am Anfang der Kette. □

Ein offenes Problem bleibt weiterhin, ob die obige Kette stets überall echt aufsteigend ist.

Nach diesen Vorbereitungen geben wir folgende untere Abschätzung für die Mächtigkeit von S.

SATZ II.35. *In einem total reellen Zahlkörper* $\mathcal{F}$ *mit* $r_{\mathcal{F}} \geq 1$ *gilt*

$$|S| \geq 2\left(2r_{\mathcal{F}} + \frac{r_{\mathcal{F}}(r_{\mathcal{F}}+1)}{2} + 1\right).$$

Beweis: In $\mathcal{F}$ existieren zunächst genau $2r_1$ viele Einheiten dicht an 1 mit Freiheitsgrad $d(\varepsilon) = 1$. Da ε^{-1} ebenfalls dicht an 1 liegt, existieren mindestens $2r_1$ viele Einheiten dicht an 1 mit $d(\varepsilon) = r_1 - 1$.

Ist andererseits ε eine Einheit dicht an 1 mit $d(\varepsilon) = r_1 - 1$, so gilt $d(\varepsilon^{-1}) = r_1 - d(\varepsilon) = 1$. Folglich existieren wie im Fall $d(\varepsilon) = 1$ genau $2r_1$ viele Einheiten dicht an 1 mit $d(\varepsilon) = r_1 - 1$.

Aus den r_1 vielen Konjugiertenbeträgen einer Einheit können wir

$$2\binom{r_1}{2} = r_1(r_1 - 1)$$

$d_{\mathcal{F}}$	$\lvert S\rvert$	$d_{\mathcal{F}}$	$\lvert S\rvert$	$d_{\mathcal{F}}$	$\lvert S\rvert$	$d_{\mathcal{F}}$	$\lvert S\rvert$	$d_{\mathcal{F}}$	$\lvert S\rvert$
725	34	2777	34	5125	50	7225	30	8525	82
1125	38	3600	42	5225	58	7232	46	8725	66
1600	58	3981	46	5725	74	7488	58	8768	42
1957	46	4205	50	5744	46	7537	46	8789	54
2000	54	4225	82	6125	70	7600	82	8957	58
2048	62	4352	38	6224	34	7625	54	9225	54
2225	50	4400	58	6809	42	8000	38	9248	30
2304	70	4525	58	7053	50	8069	30	9301	46
2525	50	4752	30	7056	42	8112	30	9792	38
2624	34	4913	74	7168	46	8468	38	9909	38

TABELLE II.2. Tabelle über die Anzahl von Einheiten dicht an 1 im Sinne von Definition II.17 für die ersten 50 total reellen Körper vierten Grades.

viele Kandidaten für Einheiten dicht an 1 mit $d(\varepsilon) = 2$ auswählen. Daher ergibt sich

$$\begin{aligned} |S| &\geq \left(\underbrace{(r_1 - 1)}_{d(\varepsilon)=1} + \underbrace{(r_1 - 1)}_{d(\varepsilon)=r_1-1} + \underbrace{\frac{r_1(r_1-1)}{2}}_{d(\varepsilon)=2} \right) \underbrace{2}_{\text{Torsion}} + \underbrace{2}_{\text{Torsionseinheiten}} \\ &= 2\left(2r_{\mathcal{F}} + \frac{r_{\mathcal{F}}(r_{\mathcal{F}}+1)}{2} + 1\right). \end{aligned}$$

□

Damit ist die Anzahl der Elemente von S in jedem Falle groß gegenüber dem Einheitenrang. Die Menge S scheint somit nicht geeignet zu sein. Das folgende Beispiel zeigt, daß $S(1)$ ebenfalls keine geeignete Wahl ist.

BEMERKUNG II.36. *In Beispiel* II.16 *wurde mittels Hauptnachbarn ein maximal unabhängiges Einheitensystem für einen total reellen Zahlkörper sechsten Grades berechnet. In diesem Falle bilden die sechs dort berechneten Einheiten, zusammen mit ihren Inversen und den Torsionseinheiten, die Menge* $S(1)$. *Damit erzeugt die Menge* $S(1)$ *i. allg. nicht die volle Einheitengruppe eines Zahlkörpers.*

Damit stellt sich die Frage, ob ein $S(i)$ mit $1 < i < r_1 + r_2 - 1$ bereits die volle Einheitengruppe erzeugt.

Satz II.37. *Die Menge der Einheiten dicht an* 1 *mit Freiheitsgrad kleiner gleich* $\left\lceil\frac{r_1+r_2}{2}\right\rceil$ *erzeugt die Einheitengruppe von* $\mathcal{F}$.

<u>Beweis:</u> Der Beweis verläuft annähernd analog wie der Beweis von Satz II.27. Wir skizzieren nur die wesentlichen Modifikationen.

Sei η eine Einheit in $\mathcal{F}$ mit

$$\eta \notin S\left(\left\lceil\frac{r_1+r_2}{2}\right\rceil\right).$$

Falls $d(\eta) > \left\lceil\frac{r_1+r_2}{2}\right\rceil$ ersetzen wir η durch η^{-1}. Dann existiert ein

$$\varepsilon \in S\left(\left\lceil\frac{r_1+r_2}{2}\right\rceil\right)$$

mit

$$|\varepsilon^{(i)}| < \max\{1, |\eta^{(i)}|\} \qquad 1 \leq i \leq r_1+r_2$$

weil $d(\eta) \leq \left\lceil\frac{r_1+r_2}{2}\right\rceil$.

(1) Reduktion der Einheit η
Der Schritt verläuft völlig analog wie in Satz II.27.

(2) Falls $\frac{\eta}{\varepsilon}$ nicht in $S\left(\left\lceil\frac{r_1+r_2}{2}\right\rceil\right)$ entscheide:
Falls $d\left(\frac{\eta}{\varepsilon}\right) > \left\lceil\frac{r_1+r_2}{2}\right\rceil$ ersetzen wir $\frac{\eta}{\varepsilon}$ durch $\frac{\varepsilon}{\eta}$.
Führe Schritt (1) erneut aus.
Da die Höhe der Einheit im Reduktionsschritt immer kleiner wird, erhalten nach endlich vielen Schritten $s+v$

$$\eta^{\pm}\frac{\hat{\varepsilon}_1\cdots\hat{\varepsilon}_v}{\tilde{\varepsilon}_1\cdots\tilde{\varepsilon}_s} \in S\left(\left\lceil\frac{r_1+r_2}{2}\right\rceil\right)$$

und damit

$$\eta \in < \varepsilon_1, \ldots, \varepsilon_u > .$$

□

Im allgemeinen kennen wir die Mächtigkeit der Mengen S bzw. $S(i)$ $(1 \leq i \leq r_1+r_2-1)$ nicht. Für spezielle Situationen erhalten wir jedoch Zusammenhänge.

$d_{\mathcal{F}}$	$\|S(2)\|$	$d_{\mathcal{F}}$	$\|S(2)\|$	$d_{\mathcal{F}}$	$\|S(2)\|$	$d_{\mathcal{F}}$	$\|S(2)\|$	$d_{\mathcal{F}}$	$\|S(2)\|$
725	26	2777	26	5125	42	7225	22	8525	74
1125	30	3600	34	5225	50	7232	38	8725	58
1600	50	3981	38	5725	66	7488	50	8768	34
1957	38	4205	42	5744	38	7537	38	8789	46
2000	46	4225	74	6125	62	7600	74	8957	50
2048	54	4352	30	6224	26	7625	46	9225	46
2225	42	4400	50	6809	34	8000	30	9248	22
2304	62	4525	50	7053	42	8069	22	9301	38
2525	42	4752	22	7056	34	8112	22	9792	30
2624	26	4913	62	7168	38	8468	30	9909	30

Tabelle II.3. Tabelle über die Anzahl von Einheiten dicht an 1 mit Freiheitsgrad kleiner gleich 2 für die ersten 50 total reellen Körper vierten Grades.

Satz II.38. *In einem total reellen Zahlkörper $\mathcal{F}$ gilt*

$$|S(r_1-2)| = |S| - 2(r_{\mathcal{F}}+1).$$

<u>Beweis:</u> Nach Satz II.35 gibt es genau $2r_1$ viele Einheiten dicht an 1 mit $d(\varepsilon) = r_1 - 1$. Wir erhalten

$$\begin{aligned} |(S(r_1-2)| &= |S| - 2 \underbrace{r_1}_{d(\varepsilon)=r_1-1} \\ &= |S| - 2(r_{\mathcal{F}}+1). \end{aligned}$$

□

Bemerkung II.39. *Falls $\mathcal{F}$ total reell vierten Grades ist, ergibt sich*

$$|S(2)| = |S| - 8.$$

Dieses Ergebnis bestätigt sich in den Tabellen II.2 *und* II.3

Bei unseren bisherigen Betrachtungen haben wir den Freiheitsgrad der Einheiten dicht an 1 beschränkt. Dabei haben wir die Positionen der Konjugiertenbeträge größer 1 stets variabel gehalten. Neben dieser Beschränkung von Freiheitsgraden kann man noch andere Bedingungen an die Konjugiertenbeträge geben. Dazu wählen wir *einen festen* Konjugiertenbetrag $|\varepsilon| := |\varepsilon^{(i)}|$ für ein $i \in \{1, \dots, r_1+r_2\}$.

Definition II.40. *Setze* $S_{|\cdot|} = \{\varepsilon \in \mathcal{F} \quad | \quad \varepsilon$ *ist dicht an* 1 *mit* $|\varepsilon| \leq 1$ $\}$.

SATZ II.41. *Die Menge der Einheiten in $S_{|.|}$ erzeugt die volle Einheitengruppe von $\mathcal{F}$.*

Beweis: Der Beweis verläuft annähernd analog wie der Beweis von Satz II.27. Wir skizzieren nur die wesentlichen Modifikationen.

Sei η eine nicht triviale Einheit in $\mathcal{F}$ mit

$$\eta \notin S_{|.|}.$$

Falls $|\eta| > 1$ ersetzen wir η durch η^{-1}. Dann existiert ein

$$\varepsilon \in S_{|.|}$$

mit

$$|\varepsilon^{(i)}| < \max\{1, |\eta^{(i)}|\} \qquad 1 \leq i \leq r_1 + r_2.$$

(1) Reduktion der Einheit η
Der Schritt verläuft völlig analog wie in Satz II.27.

(2) Falls $\frac{\eta}{\varepsilon}$ nicht in $S_{|.|}$ entscheide:
Falls $\left|\frac{\eta}{\varepsilon}\right|$ ersetzen wir $\frac{\eta}{\varepsilon}$ durch $\frac{\varepsilon}{\eta}$.
Führe Schritt (1) erneut aus.
Da die Höhe der Einheit im Reduktionsschritt immer kleiner wird, erhalten nach endlich vielen Schritten $s + v$

$$\eta^{\pm}\frac{\hat{\varepsilon}_1 \cdots \hat{\varepsilon}_v}{\tilde{\varepsilon}_1 \cdots \tilde{\varepsilon}_s} \in S_{|.|}$$

und damit

$$\eta \in < \varepsilon_1, \ldots, \varepsilon_u > .$$

$\square$

Zunächst bemerken wir, daß stets $S_{|.|} \subset S$ gilt. Damit haben wir im Vergleich zu S eine kleinere Menge von Einheiten charakterisiert, die die Einheitengruppe von $\mathcal{F}$ erzeugt. Dieses Ergebnis läßt sich quantitativ fassen, wie der folgende Satz zeigt.

SATZ II.42. *Es sei $\mathcal{F}$ eine total reelle Körpererweiterung über $\mathbb{Q}$. Dann gilt der Zusammenhang:*

$$2\left|S_{|.|}\right| - 2 = |S|$$

Beweis: Es sei $\varepsilon \in S_{|.|}$. Dann ist ε dicht an 1 und nach Satz II.20 ist ε^{-1} ebenfalls dicht an 1. Daher verdoppeln wir die Anzahl der Einheiten in $S_{|.|}$. Da ± 1 dicht an 1 und zu sich selbst invers sind, dürfen diese beiden Einheiten nicht doppelt gezählt werden.

Sei umgekehrt $\varepsilon \in S$ eine Einheit, die dicht an 1 ist. Falls ε eine Torsionseinheit ist, folgt $\varepsilon \in S_{|.|}$. Falls ε keine Torsionseinheit ist, gilt entweder $|\varepsilon| > 1$ oder $|\varepsilon| < 1$. Damit liegt genau eine der beiden Einheiten ε oder ε^{-1} in $S_{|.|}$.

□

Wir vergleichen unsere gewonnenen Erkenntnisse mit der Reduktionstheorie von Buchmann exemplarisch an einem Beispiel, siehe auch II.13.

Beispiel II.43. (a) *Für den total reellen Körper vierten Grades mit Diskriminante* 59468 *bestimmten wir* $|S(2)|$ *und* $\left|S_{|.|}\right|$. *Wir erhalten folgende Tabelle:*

Menge	$U(C)$	$\|S(2)\|$	$\left\|S_{\|.\|}\right\|$	$\|S\|$
$\|Menge\|$	434	36	22	42

Die Tabelle spiegelt den typschen Fall wieder. Während die Anzahl der Randeinheiten bei steigender Diskriminante wächst, bleiben die Mächtigkeiten der Mengen $S(2), S_{|.|}$ *und* S *moderat klein. Nicht klein gegenüber dem Einheitenrang des Zahlkörpers, aber klein gegenüber der Anzahl der Randeinheiten.*

(b) *In der Tabelle* II.4 *geben wir die Anzahl der Elemente für kleinere Diskriminanten an.*
Der Vergleich der Tabellen II.1 *und* II.5 *ergibt dann einen klaren Eindruck. Die Anzahl der Randeinheiten wächst, während die Anzahl der Einheiten dicht an* 1 *stets klein bleibt.*

$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$	$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$	$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$	$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$	$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$
725	18	2777	18	5125	26	7225	16	8525	42
1125	20	3600	22	5225	30	7232	24	8725	34
1600	30	3981	24	5725	38	7488	30	8768	22
1957	24	4205	26	5744	24	7537	24	8789	28
2000	28	4225	42	6125	36	7600	42	8957	30
2048	32	4352	20	6224	18	7625	28	9225	28
2225	26	4400	30	6809	22	8000	20	9248	16
2304	36	4525	30	7053	26	8069	16	9301	24
2525	26	4752	16	7056	22	8112	16	9792	20
2624	18	4913	38	7168	24	8468	20	9909	20

Tabelle II.4. Tabelle über die Anzahl von Einheiten dicht an 1 in $S_{|\cdot|}$ für die ersten 50 total reellen Körper vierten Grades.

$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$	$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$	$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$	$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$	$d_{\mathcal{F}}$	$S_{\lvert\cdot\rvert}$
50225	30	52025	30	53824	38	55665	36	57600	26
50432	16	52052	20	53840	20	55728	30	57609	32
50437	24	52176	20	54225	42	55872	22	57909	22
50688	36	52221	24	54249	40	55872	26	58000	42
50688	24	52225	42	54332	18	56025	30	58025	38
50693	24	52396	16	54381	24	56125	38	58049	24
50725	38	52400	26	54725	50	56137	22	58217	26
50737	20	52525	38	54764	24	56144	22	58397	18
50908	18	52592	18	54848	22	56333	16	58469	24
51005	22	52625	54	54864	28	56384	26	58672	20
51125	42	52816	18	55025	38	56592	22	58896	22
51153	32	53121	18	55297	18	56677	26	59457	26
51181	22	53312	26	55377	20	56749	24	59468	22
51200	40	53333	24	55409	26	56777	30	59600	46
51264	20	53361	32	55552	28	56896	26	59648	28
51725	26	53401	20	55585	16	57077	20	59725	38
51776	26	53568	20	55600	38	57600	36	59749	24
51984	34	53589	20	55661	22	57600	22		

Tabelle II.5. Tabelle über die Anzahl von Einheiten dicht an 1 in $S_{|\cdot|}$ für total reelle Körper vierten Grades mit $50000 < d_{\mathcal{F}} < 60000$.

KAPITEL III

Relativeinheiten

Spricht man von Einheiten eines Zahlkörpers $\mathcal{M}$, so meint man i. allg. dessen ganze Elemente mit Norm ± 1 über $\mathbb{Q}$. Für einen Zwischenkörper $\mathcal{L}$ mit $\mathbb{Q} \subset \mathcal{L} \subset M$ läßt sich auch die Norm der Elemente von $\mathcal{M}$ bzgl. $\mathcal{L}$ betrachten. In diesem Fall sprechen wir von der Relativnorm der Elemente von $\mathcal{M}$ bzgl $\mathcal{L}$, siehe auch [14]. Im folgenden Diagramm stellen wir die Situation dar.

$$
\begin{array}{ccc}
\gamma & \in & \mathcal{M} \\
 & & \Big| \\
 & & \mathcal{L} \\
 & & \Big| \\
 & & \mathbb{Q}
\end{array}
\left.\begin{array}{c} \\ \\ \end{array}\right\rangle N_{\mathcal{M}/\mathcal{L}}(\gamma)
\qquad\qquad
\begin{array}{ccc}
\gamma & \in & U_{\mathcal{M}} \\
 & & \Big| \\
TU_{\mathcal{L}} & \subseteq & U_{\mathcal{L}} \\
 & & \Big| \\
 & & \{\pm 1\}
\end{array}
\left.\begin{array}{c} \\ \\ \end{array}\right\rangle N_{\mathcal{M}/\mathcal{L}}(\gamma)
$$

Betrachtungen für besondere Fälle finden sich in [22] und [26]. Über $\mathbb{Q}$ ist die Norm einer Einheit aus $\mathcal{M}$ stets ± 1, also eine Torsionseinheit. Betrachtet man die Norm über dem Zwischenkörper $\mathcal{L} \subset \mathcal{M}$, so muß nicht jede Norm eine Torsionseinheit sein. Diese neue Situation führt zur folgenden Definition. (Sprechen wir im folgenden von Körpererweiterungen, so meinen wir stets Zahlkörper.)

Definition III.1. *Es sei $\mathcal{M}/\mathbb{Q}$ eine Körpererweiterung und $\mathcal{L}$ ein echter Zwischenkörper ($\mathbb{Q} \subset \mathcal{L} \subset \mathcal{M}$) von $\mathcal{M}$.*
Dann nennen wir $\gamma \in U_{\mathcal{M}}$ eine **Relativeinheit** *(bzgl. $\mathcal{L}$), falls $N_{\mathcal{M}/\mathcal{L}}(\gamma) \in TU_{\mathcal{L}}$ gilt. Wir nennen $\gamma \in U_{\mathcal{M}}$ eine* **totale Relativeinheit**, *falls $N_{\mathcal{M}/\mathcal{L}}(\gamma) \in TU_{\mathcal{L}}$ für alle Zwischenkörper $\mathcal{L}$ von $\mathcal{M}$ gilt.*

Bemerkung III.2. *Die Menge aller Relativeinheiten bzgl. eines Teilkörpers bildet eine Untergruppe in der Gruppe der Einheiten. Ebenfalls bildet die Menge aller totalen Relativeinheiten eine Untergruppe. Beides ergibt sich sofort aus der Multiplikativität der Norm.*

Für die Betrachtung von Relativeinheiten geben wir folgende Motivation.

Die Menge der Relativeinheiten spielt eine besondere Rolle beim Lösen von Normgleichungen. Wir betrachten die Normgleichung

$$N_{\mathcal{M}/\mathcal{L}}(\gamma) = \beta \in \mathcal{L}.$$

Mit jeder Lösung $\gamma \in \mathcal{M}$ ist auch das Element $\varepsilon\gamma \quad (\varepsilon \in U_{\mathcal{M}})$ eine Lösung, falls $N_{\mathcal{M}/\mathcal{L}}(\varepsilon) = 1$ gilt.

Wir wollen Strukturaussagen über die Menge der (totalen) Relativeinheiten gewinnen und führen dazu folgende Bezeichnung ein.

Definition III.3. *Die Untergruppe der Relativeinheiten (bzgl. $\mathcal{L}$) einer Körpererweiterung $\mathcal{M}/\mathbb{Q}$ bezeichnen wir mit $RU_{\mathcal{M}/\mathcal{L}}$. Die Untergruppe der totalen Relativeinheiten mit $RU_{\mathcal{M}}$.*

Satz III.4. *Für eine Körpererweiterung $\mathcal{M}/\mathbb{Q}$ gilt:*

$$RU_{\mathcal{M}} = \bigcap_{\mathbb{Q}\subset\mathcal{L}\subset\mathcal{M}} RU_{\mathcal{M}/\mathcal{L}}.$$

(Durchschnitt über alle echten Zwischenkörper von $\mathcal{M}$.)

<u>Beweis:</u> Klar.

□

Für eine Körpererweiterung $\mathcal{M}/\mathbb{Q}$ ist das Bild einer Einheit unter der Norm $N_{\mathcal{M}/\mathbb{Q}}$ stets eine Torsionseinheit. Damit gilt $RU_{\mathcal{M}/\mathbb{Q}} = U_{\mathcal{M}}$. Dies muß bzgl. der Relativnorm eines echten Zwischenkörpers $\mathcal{L}$ von $\mathcal{M}$ nicht gelten. Wir werden im folgenden diese Situation näher beschreiben.

Satz III.5. *Es sei $\mathcal{M}/\mathbb{Q}$ eine Körpererweiterung und $\mathcal{L}$ ein echter Zwischenkörper. Es sei ζ eine Torsionseinheit in $\mathcal{M}$. Dann ist $N_{\mathcal{M}/\mathcal{L}}(\zeta)$ eine Torsionseinheit in $\mathcal{L}$.*

<u>Beweis:</u> Für $\zeta = \pm 1$ ist nichts zu zeigen. Sei daher $\zeta \neq \pm 1$ und $k \in \mathbb{N}^{>1}$ mit $\zeta^k = \zeta$. Für $\xi := N_{\mathcal{M}/\mathcal{L}}(\zeta)$ erhalten wir dann die Gleichungskette:

$$\xi = N_{\mathcal{M}/\mathcal{L}}(\zeta) = N_{\mathcal{M}/\mathcal{L}}(\zeta^k) = N_{\mathcal{M}/\mathcal{L}}(\zeta)^k = \xi^k.$$

Mit $\xi = \xi^k$ für $k > 1$ folgt dann die Behauptung.

$\square$

Der folgende Satz zeigt auf, wann die Untergruppe $RU_{\mathcal{M}/\mathcal{L}}$ nicht trivial ist.

SATZ III.6. *Es sei $\mathcal{M}/\mathbb{Q}$ eine Körpererweiterung und $\mathcal{L}$ ein echter Zwischenkörper mit $r_{\mathcal{M}} > r_{\mathcal{L}}, n = [\mathcal{M} : \mathcal{L}]$. Dann ist $RU_{\mathcal{M}/\mathcal{L}}$ nicht trivial (besteht nicht nur aus Torsionselementen).*

<u>Beweis:</u> Es sei ζ_0 ein Erzeuger von $TU_{\mathcal{L}}$ und definiere $l := r_{\mathcal{L}}$. Ferner bilde $\varepsilon_1, \ldots, \varepsilon_l$ ein Grundeinheitensystem von $\mathcal{L}$.

Dann existiert eine nicht triviale Einheit γ in $\mathcal{M}$ mit

$$\gamma \notin < \varepsilon_1, \ldots, \varepsilon_l >, \quad \gamma \neq \zeta_0^{u_0} \sqrt[p]{\varepsilon_1^{u_1} \cdots \varepsilon_l^{u_l}} \quad \forall p \in \mathbb{P} \text{ und } u_0, \ldots, u_l \in \mathbb{Z}.$$

Für die Norm gilt die Darstellung

$$N_{\mathcal{M}/\mathcal{L}}(\gamma) = {\zeta_0}^{m_0} {\varepsilon_1}^{m_1} \ldots {\varepsilon_l}^{m_l}.$$

mit $m_0, \ldots, m_l \in \mathbb{Z}$. Die Einheit γ existiert, weil wir $r_{\mathcal{M}} > r_{\mathcal{L}}$ vorausgesetzt haben. Dann gilt für

$$\gamma_0 = \gamma^n {\varepsilon_1}^{-m_1} \ldots {\varepsilon_l}^{-m_l}$$

$$N_{\mathcal{M}/\mathcal{L}}(\gamma_0) = N_{\mathcal{M}/\mathcal{L}}(\gamma^n {\varepsilon_1}^{-m_1} \ldots {\varepsilon_l}^{-m_l}) = {\zeta_0}^{n m_0}.$$

Aufgrund der Wahl von γ ist γ_0 keine Torsionseinheit und somit ist $RU_{\mathcal{M}/\mathcal{L}}$ nicht trivial.

$\square$

Der Beweis von Satz III.6 ist konstruktiv. Er liefert ein Verfahren um eine gegebene nicht triviale Einheit, die nicht im Zwischenkörper liegt oder keine p-te Wurzel in den Einheiten des Zwischenkörpers ist, zu einer Relativeinheit zu modifizieren.

Bislang haben wir aufgezeigt, wann die Relativeinheitengruppe eines Zahlkörpers bzgl. eines festen Zwischenkörpers nicht trivial ist. Dies ist stets der Fall, falls der Einheitenrang des Zahlkörpers größer als der des Zwischenkörpers ist. Wir verallgemeinern jetzt diese Problemstellung auf die totale Relativeinheitengruppe eines Zahlkörpers. Im folgenden werden wir Kriterien für die Existenz von nicht trivialen totalen Relativeinheiten angeben.

SATZ III.7. *Es seien $\mathcal{L}, \mathcal{K}$ zwei Körpererweiterungen mit $[\mathcal{L} : \mathbb{Q}] = p$ und $[\mathcal{K} : \mathbb{Q}] = q$, $p, q \in \mathbb{P}$ mit $p \neq q$. Ferner sei $\mathcal{M} = Cov(\mathcal{L}, \mathcal{K})$ und $r_{\mathcal{M}} > r_{\mathcal{L}} + r_{\mathcal{K}}$. Dann ist $RU_{\mathcal{M}}$ nicht trivial.*

<u>Beweis:</u>

Wir haben die Situation:
$$\begin{array}{ccccc} & & & \mathcal{M} & \\ & \mathcal{L} & & & \\ p & & & \mathcal{K} & \\ & & & q & \\ & \mathbb{Q} & & & \end{array}$$

Es sind $\mathcal{L}, \mathcal{K}$ die beiden einzigen echten Zwischenkörper von $\mathcal{M}$, aufgrund der verschiedenen Primzahlen p und q. Definiere $l := r_{\mathcal{L}}$, und $\varepsilon_1, \ldots, \varepsilon_l$ sei ein Grundeinheitensystem von $\mathcal{L}$. Es sei $m_{\varepsilon_i} \in \mathbb{Z}[t]$ das Minimalpolynom von ε_i. Dann ist m_{ε_i} ebenfalls irreduzibel über $o_{\mathcal{K}}[t]$. Damit gilt

$$N_{\mathcal{M}/\mathcal{K}}(\varepsilon_i) \in TU_{\mathcal{K}} \quad (1 \leq i \leq l).$$

Für $k := r_{\mathcal{K}}$ sei $\eta_1, \ldots, \eta_k$ ein Grundeinheitensystem von $\mathcal{K}$, und wir erhalten analog

$$N_{\mathcal{M}/\mathcal{L}}(\eta_i) \in TU_{\mathcal{L}} \quad (1 \leq i \leq k).$$

Sei ζ_0 der Erzeuger von $TU_{\mathcal{L}}$ und ζ_1 der Erzeuger von $TU_{\mathcal{K}}$. Dann existiert eine Einheit γ in $\mathcal{M}$ mit

$$\gamma \notin < \zeta_0, \zeta_1, \eta_1, \ldots, \eta_k, \varepsilon_1, \ldots, \varepsilon_l >,$$

$$\gamma \neq \zeta_0^{s_0} \zeta_1^{t_0} \sqrt[p]{\varepsilon_1^{s_1} \cdots \varepsilon_l^{s_l} \eta_1^{t_1} \cdots \eta_k^{t_k}}, \quad \forall p \in \mathbb{P} \text{ und } s_0, \ldots, s_l, t_0, \ldots, t_k \in \mathbb{Z}.$$

Für die Normen über den Teilkörpern nehmen wir folgende Dartellung an:

$$N_{\mathcal{M}/\mathcal{L}}(\gamma) = {\zeta_0}^{u_0} {\varepsilon_1}^{u_1} \ldots {\varepsilon_l}^{u_l} \text{ bzw. } N_{\mathcal{M}/\mathcal{K}}(\gamma) = {\zeta_1}^{v_0} {\eta_1}^{v_1} \ldots {\eta_k}^{v_k}.$$

Gemäß Satz III.6 gilt für

$$\gamma_0 = \gamma^p {\varepsilon_1}^{-u_1} \ldots {\varepsilon_l}^{-u_l}$$

$$N_{\mathcal{M}/\mathcal{L}}(\gamma_0) = \zeta_0^{pu_0}.$$

Dann folgt für $\gamma_1 = \gamma_0^q {\eta_1}^{-v_1} \ldots {\eta_k}^{-v_k}$

$$N_{\mathcal{M}/\mathcal{L}}(\gamma_1) = \pm \zeta_0^{pu_0 q} \text{ und } N_{\mathcal{M}/\mathcal{K}}(\gamma_1) = \pm \zeta_1^{qv_0 p}.$$

$\square$

Bis zum gegenwärtigen Zeitpunkt haben wir gezeigt, in welchen Situationen die Untergruppe der (totalen) Relativeinheiten nicht trivial ist. Im folgenden werden wir Aussagen über die Anzahl der Erzeuger dieser Untergruppe machen.

Satz III.8. *Es seien $\mathcal{L}, \mathcal{K}$ zwei Körpererweiterungen mit $[\mathcal{L} : \mathbb{Q}] = p$ und $[\mathcal{K} : \mathbb{Q}] = q$, $p, q \in \mathbb{P}$ mit $p \neq q$. Ferner sei $\mathcal{M} = Cov(\mathcal{L}, \mathcal{K})$ und $r_{\mathcal{M}} > r_{\mathcal{L}} + r_{\mathcal{K}}$. Dann existieren in $RU_{\mathcal{M}}$ genau $r_{\mathcal{M}} - r_{\mathcal{L}} - r_{\mathcal{K}}$ viele unabhängige Einheiten.*

Beweis: Für $l := r_{\mathcal{L}}$ sei $\varepsilon_1, \ldots, \varepsilon_l$ ein Grundeinheitensystem von L, für $k := r_{\mathcal{K}}$ sei $\eta_1, \ldots, \eta_k$ ein Grundeinheitensystem von K. Sei ζ_0 der Erzeuger von $TU_{\mathcal{L}}$ und ζ_1 der Erzeuger von $TU_{\mathcal{K}}$. Dann existieren nach dem Einheitensatz von Dirichlet weitere $r_{\mathcal{M}} - r_{\mathcal{L}} - r_{\mathcal{K}} =: j$ viele unabhängige Einheiten $\gamma_1, \ldots, \gamma_j$ in $\mathcal{M}$. Wieder können wir für jedes $\gamma \in \{\gamma_1, \ldots, \gamma_j\}$ annehmen:

$$\gamma \neq \zeta_0^{s_0} \zeta_1^{t_0} \sqrt[p]{\varepsilon_1^{s_1} \cdots \varepsilon_l^{s_l} \eta_1^{t_1} \cdots \eta_k^{t_k}}, \quad \forall p \in \mathbb{P} \text{ und } s_0, \ldots, s_l, t_0, \ldots, t_k \in \mathbb{Z}.$$

Jede der Einheiten $\gamma_i \quad (1 \leq i \leq j)$ kann gemäß Satz III.6 zu einer Einheit $\beta_i \in RU_{\mathcal{M}} (1 \leq i \leq j)$ modifiziert werden. Für $\beta_i (1 \leq i \leq j)$ wählen wir die Darstellung:

$$\beta_i = \gamma_i^{pq} \zeta_0^{u_{o,i}} \zeta_1^{v_{0,i}} \varepsilon_1^{u_{1,i}} \cdots \varepsilon_l^{u_{l,i}} \eta_1^{v_{1,i}} \cdots \eta_k^{u_{k,i}}$$

mit $u_{0,i}, \ldots, u_{l,i}, v_{0,i}, \ldots, v_{k,i} \in \mathbb{Z}, 1 \leq i \leq j$.

(a) $\beta_1, \ldots, \beta_j$ sind unabhängig.
Nehmen wir an, es existieren $m_1, \ldots, m_j$ in $\mathbb{Z}$ nicht alle gleich Null mit

$$1 = \beta_1^{m_1} \cdots \beta_j^{m_j}.$$

Wir setzen die Darstellungen der β_i ein und erhalten:

$$\frac{1}{\gamma_1^{m_1 pq} \cdots \gamma_j^{m_j pq}} \zeta_0^{\sum_{i=1}^{j} m_i u_{0,i}} \zeta_1^{\sum_{i=1}^{j} m_i v_{0,i}} =$$

$$\varepsilon_1^{\sum_{i=1}^{j} m_i u_{1,i}} \cdots \varepsilon_l^{\sum_{i=1}^{j} m_i u_{l,i}} \eta_1^{\sum_{i=1}^{j} m_i v_{1,i}} \cdots \eta_k^{\sum_{i=1}^{j} m_i v_{k,i}}$$

Wegen $< \gamma_1, \ldots, \gamma_j, \zeta_0, \zeta_1 > \cap < \varepsilon_1, \ldots, \varepsilon_l, \eta_1, \ldots, \eta_k >= 1$ folgt, daß die rechte Seite gleich 1 ist. Damit folgt jedoch $\gamma_1, \ldots, \gamma_j$ linear abhängig, was ein Widerspruch ist.

(b) Es gibt höchstens j unabhängige Einheiten in $RU_{\mathcal{M}}$.
Wir nehmen an, es existiert eine weitere unabhängige Einheit β in $RU_{\mathcal{M}}$ von $\beta_1, \ldots, \beta_j$. Dann bilden $\beta, \beta_1, \ldots, \beta_j, \varepsilon_1, \ldots, \varepsilon_l, \eta_1, \ldots, \eta_k$ ein unabhängiges Einheitensystem von $\mathcal{M}$ mit $r_{\mathcal{M}} + 1$ Einheiten (Widerspruch).

Die Untergruppe wird in diesem Fall von $r_{\mathcal{M}} - r_{\mathcal{L}} - r_{\mathcal{K}}$ vielen unabhängigen Einheiten und einem Torsionselement erzeugt.

$\square$

Folgerung III.9. *Es sei $\mathcal{M}/\mathbb{Q}$ eine Körpererweiterung und $\mathcal{L}$ ein echter Zwischenkörper. Dann existieren in $RU_{\mathcal{M}/\mathcal{L}}$ genau $r_{\mathcal{M}} - r_{\mathcal{L}}$ viele unabhängige Einheiten.*

Beweis: Der Beweis kann analog zu dem Beweis von Satz III.8 geführt werden. Auf die Bedingung,daß der Grad von $\mathcal{L}/\mathbb{Q}$ eine Primzahl ist kann verzichtet werden. Die Forderung war nur aufgrund des zweiten Zwischenkörpers notwendig.

$\square$

Im allgemeinen sind wir nicht nur daran interessiert ob Einheiten in einem algebraischen Zahlkörper unabhängig sind, sondern auch an den Primteilern des Index zur vollen Einheitengruppe.

Definition III.10. *Es sei $\mathcal{M}$ ein algebraischer Zahlkörper über $\mathbb{Q}$ und $\varepsilon_1, \dots, \varepsilon_r$ seien unabhängige Einheiten in $\mathcal{M}$. Dann verstehen wir als* **Wurzelexponentenmenge** *von $\varepsilon_1, \dots, \varepsilon_r$ in $\mathcal{M}$:*

$$\mathrm{P}(\varepsilon_1, \dots, \varepsilon_r) := \{p \in \mathbb{P} \mid \quad \exists l_1, \dots, l_r \in \{0, \dots, p-1\} \text{ (nicht alle Null) und } \zeta \in TU_{\mathcal{M}} \text{ mit } \sqrt[p]{\zeta \varepsilon_1^{l_1} \cdots \varepsilon_r^{l_r}} \in \mathcal{M}\}$$

Bemerkung III.11.

(a) *$\varepsilon_1, \dots, \varepsilon_r$ aus $\mathcal{M}$ sind zu einem Grundeinheitensystem von $\mathcal{M}$ erweiterbar $\iff \mathrm{P} = \emptyset$.*
(b) *$\varepsilon_1, \dots, \varepsilon_r$ aus $\mathcal{M}$ bilden ein Grundeinheitensystem $\iff \mathrm{P} = \emptyset$ und $r = r_{\mathcal{M}}$.*

Beweis: Siehe etwa Pohst/Zassenhaus [34].

$\square$

Im folgenden studieren wir die Situation

$$\begin{array}{cl}
\mathcal{M} & \\
\Big| & \eta_1, \dots, \eta_k \text{ Basis von } RU_{\mathcal{M}/\mathcal{L}} \\
\mathcal{L} & \\
\Big| & \varepsilon_1, \dots, \varepsilon_l \text{ Grundeinheiten von } \mathcal{L} \\
\mathbb{Q} &
\end{array}$$

und beantworten die Frage, in wie weit wir die Einheitengruppe von $\mathcal{M}$ über $\mathbb{Q}$ bereits kennen.

Satz III.12. *Es sei $\mathcal{M}/\mathbb{Q}$ eine Körpererweiterung mit echtem Zwischenkörper $\mathcal{L}$. Ferner sei $\varepsilon_1, \ldots, \varepsilon_l$ ein Grundeinheitensystem von $\mathcal{L}$ und $RU_{\mathcal{M}/\mathcal{L}}$ sei nicht trivial mit Basis $\eta_1, \ldots, \eta_k$. Dann gilt*

(a) $\eta_1, \ldots, \eta_k, \varepsilon_1, \ldots, \varepsilon_l$ *bilden ein maximal unabhängiges Einheitensystem in* $\mathcal{M}$.
(b) $\mathrm{P}(\eta_1, \ldots, \eta_k, \varepsilon_1, \ldots, \varepsilon_l) \subseteq \{p \in \mathbb{P} \quad | \quad p \textit{ teilt } [\mathcal{M} : \mathcal{L}]\}$

Beweis:

(a) Da die $\eta_1, \ldots, \eta_k$ nach Voraussetzung eine Basis von $RU_{\mathcal{M}/\mathcal{L}}$ bilden folgt mit Satz III.9 $k + l = r_{\mathcal{M}}$.
(b) Wir nehmen an, es existieren $\alpha \in \mathcal{M}$, $\xi \in TU_{\mathcal{M}}$ und $p \in \mathbb{P}$ mit

$$\alpha^p = \xi \eta_1^{a_1} \cdots \eta_k^{a_k} \varepsilon_1^{b_1} \cdots \varepsilon_l^{b_l}, \quad a_i, b_j \in \{0, \ldots, p-1\} \quad (1 \leq i \leq k, 1 \leq j \leq l).$$

Dann folgt für einen Erzeuger $\zeta \in TU_{\mathcal{L}}$ und $n = [\mathcal{M} : \mathcal{L}]$, daß

$$N_{\mathcal{M}/\mathcal{L}}(\alpha^p) = N_{\mathcal{M}/\mathcal{L}}(\alpha)^p = \zeta^{b_0} \varepsilon_1^{b_1 n} \cdots \varepsilon_l^{b_l n}$$

gilt. Da $\varepsilon_1, \ldots, \varepsilon_l$ ein Grundeinheitensystem von $\mathcal{L}$ bilden und

$$b_j \in \{0, \ldots, p-1\} \quad (1 \leq j \leq l)$$

gilt, folgt p teilt n oder $b_j = 0$ für $(1 \leq j \leq l)$.
Im Fall $b_j = 0$ für $(1 \leq j \leq l)$ folgt

$$\sqrt[p]{\zeta} \sqrt[p]{\eta_1^{a_1} \cdots \eta_k^{a_k}} \in \mathcal{M}$$

im Widerspruch zu $\eta_1, \ldots, \eta_k$ Basis von $RU_{\mathcal{M}/\mathcal{L}}$, und damit p teilt n.

$\square$

KAPITEL IV

Erweiterungen vom Grad 6

1. Die Untergruppe der Relativeinheiten

In diesem Kapitel studieren wir Körper sechsten Grades, die einen reell–quadratischen Teilkörper und einen einfach reellen kubischen Teilkörper enthalten. Dabei werden wir die allgemeinen Ergebnisse aus dem vorherigen Kapitel anwenden. Wir fixieren folgendes Szenario:

$$\mathcal{E} = \mathrm{C}ov(\mathcal{F}, \mathcal{K})$$

reell–quadratisch $\mathcal{F}$ $\qquad\qquad$ $\mathcal{K}$ einfach reell kubisch

$$\mathbb{Q}$$

Wir nehmen an, daß

$$\begin{array}{rcll} \mathcal{F} & = & \mathbb{Q}(\sqrt{d}) & \text{mit } d \in \mathbb{N} \text{ quadratfrei und} \\ \mathcal{K} & = & \mathbb{Q}(\rho) & \text{mit } \rho^3 + a\rho + b = 0 \quad (a, b \in \mathbb{Z}) \end{array}$$

gilt. Dabei sei ε die Grundeinheit in $\mathcal{F}$ und η die Grundeinheit in $\mathcal{K}$. Wir sind interessiert an der Einheitengruppe von $\mathcal{E}$ und erhalten zunächst folgende Rangaussage.

Satz IV.1. *$\mathcal{E}$ kann über $\mathbb{Q}$ mit einem irreduziblen Polynom aus $\mathbb{Z}[t]$ erzeugt werden, welches 2 reelle und 4 nicht reelle Nullstellen hat. $\mathcal{E}$ hat somit Einheitenrang 3.*

Beweis: Wir können annehmen, daß $\mathcal{E} = \mathbb{Q}(\delta)$ mit $\delta = \sqrt{d} + \rho$ gilt. Aus den Konjugierten von δ folgt, daß das Minimalpolynom von δ über $\mathbb{Z}$ zwei reelle und vier nicht reelle Nullstellen hat. Die Signatur von $\mathcal{E}$ ist demnach $(2,2)$ und der Einheitenrang 3.

□

Satz IV.2. *Für das Minimalpolynom von $\delta = \sqrt{d} + \rho$ über $\mathbb{Z}[t]$ gilt*

$$m_\delta(t) = t^6 + (2\,a - 3\,d)\,t^4 + 2\,bt^3 + \left(3\,d^2 + a^2\right)t^2 + (2\,ab + 6\,db)\,t - da^2 - d^3 - 2\,d^2a + b^2.$$

Die Polynomdiskriminante von $m_\delta(t)$ ist

$$d_{m_\delta} = 64\,d^3\left(4\,a^3 + 27\,b^2\right)^2\left(4\,a^3 + 27\,b^2 + 36\,da^2 + 96\,d^2a + 64\,d^3\right)^2$$

Beweis: Per Nachrechnen.

□

Neben dem Einheitenrang sind wir daran interessiert, unabhängige Einheiten in $\mathcal{E}$ zu finden. Dabei beginnen wir mit den Einheiten der beiden Teilkörper.

Satz IV.3. *ε und η sind in $\mathcal{E}$ unabhängig.*

Beweis: Aus der Annahme, daß ε und η abhängig sind, folgt unmittelbar $\varepsilon \in \mathcal{K}$ bzw. $\eta \in \mathcal{F}$ und damit der Widerspruch.

□

Satz IV.4. *Das Element $\sqrt{\eta}$ liegt nicht in $\mathcal{E}$.*

Beweis: Zunächst bemerken wir, daß aufgrund $[\mathcal{E} : \mathcal{K}] = 2$ höchstens die 2-te Wurzel von η in $\mathcal{E}$ liegen kann.

Nehmen wir an, daß $\sqrt{\eta}$ in $\mathcal{E}$ sei. Dann können wir $\mathcal{E}$ in der Form $\mathcal{E} = \mathcal{K}(\sqrt{\eta})$ darstellen. Damit existiert eine Linearkombination der Form $\sqrt{d} = a + b\sqrt{\eta}$ mit $a, b \in \mathcal{K}$. Wegen $m_{\sqrt{d}}(t) = t^2 - d$ über $o_{\mathcal{K}}[t]$ folgt $T_{\mathcal{E}/\mathcal{K}}(\sqrt{d}) = 0$ und somit $a = 0$. Damit folgt $d = b^2\eta$ bzw. $b = \pm\sqrt{\dfrac{d}{\eta}} \notin \mathcal{K}$ im Widerspruch zum Ansatz.

□

BEISPIEL IV.5. *Wenn $\mathcal{K}$ keine reine Erweiterung ist, dann kann das Element $\sqrt[3]{\varepsilon}$ in $\mathcal{E}$ sein. Analog wie oben merken wir, daß aufgrund $[\mathcal{E} : \mathcal{F}] = 3$ höchstens die 3-te Wurzel von ε in $\mathcal{E}$ liegen kann.*
Wir betrachten den Körper $\mathcal{E}$, der erzeugt wird durch eine Wurzel δ des Polynoms

$$f(t) = t^6 - 2t^3 - 1 \textit{ mit } d_f = d_{\mathcal{E}} = 373248.$$

Dann enthält $\mathcal{E}$ die beiden Teilkörper

$$\begin{array}{llll} \mathcal{F} = \mathbb{Q}(\sqrt{d}) & \textit{mit} & \sqrt{d}^2 - 2 = 0 & \textit{und} \quad d_{\mathcal{F}} = 8 \\ \textit{sowie} & & & \\ \mathcal{K} = \mathbb{Q}(\rho) & \textit{mit} & \rho^3 + 3\rho + 2 = 0 & \textit{und} \quad d_{\mathcal{K}} = -216. \end{array}$$

In den beiden Körpern kennen wir die Grundeinheiten

$$\varepsilon = 1 + \sqrt{2} \in \mathcal{F} \textit{ und } \eta = \rho^2 + \rho + 1 \in \mathcal{K}.$$

Beachtet man jetzt

$$f(\sqrt[3]{\varepsilon}) = \varepsilon^2 - 2\varepsilon - 1 = 0,$$

so gilt $\sqrt[3]{\varepsilon} \in \mathcal{E}$. Damit ist $f(t)$ das Minimalpolynom von $\sqrt[3]{\varepsilon}$ über $\mathbb{Z}[t]$ und $\mathcal{E} = \mathbb{Q}(\sqrt[3]{\varepsilon})$.

SATZ IV.6. *Ist $\mathcal{K}$ rein kubisch der Form $\mathcal{K} = \mathbb{Q}(\sqrt[3]{k})$, dann liegt das Element $\sqrt[3]{\varepsilon}$ nicht in $\mathcal{E}$.*

Beweis: Siehe Stender [37]

□

SATZ IV.7. *Die totale Relativeinheitengruppe $RU_{\mathcal{E}}$ von $\mathcal{E}$ ist nicht trivial und es existiert ein erzeugendes Element.*

Beweis: Nach Satz III.8 ist die Gruppe $RU_{\mathcal{E}}$ nicht trivial und wird von einem Element erzeugt.

□

Sei γ in $\mathcal{E}$ ein Erzeuger von $RU_{\mathcal{E}}$. Dann bilden $\varepsilon, \eta, \gamma$ ein maximal unabhängiges Einheitensystem in $\mathcal{E}$. Im nächsten Satz beantworten wir die Frage, welche p-ten Potenzen dieses Einheitensystem noch enthalten kann.

Der Satz III.12 besagt, daß nur 2 und 3 als Teiler des Körpergrades $[\mathcal{E} : \mathbb{Q}]$ in Frage kommen. Unser Ansatz besteht nun darin, die möglichen Kandidaten in Form von Potenzprodukten explizit anzugeben.

SATZ IV.8. *Für das Einheitensystem $\varepsilon, \eta, \gamma$ können wir die möglichen Wurzelexponenten angeben durch:*

$$\mathrm{P}(\varepsilon, \eta, \gamma) \subseteq \{2, 3\}$$

<u>Beweis:</u> Wir wenden das in Pohst/Zassenhaus [34] vorgeschlagene Verfahren an. Dazu betrachten wir folgende Gleichungen:

(a)
$$\alpha^p = \varepsilon \text{ mit } p \in \mathbb{P}.$$
Nach IV.5 ist $\sqrt[p]{\varepsilon} \in \mathcal{E}$ nur für $p = 3$ möglich. Falls $\sqrt[3]{\varepsilon}$ in $\mathcal{E}$ existiert setzen wir $\varepsilon_0 = \sqrt[3]{\varepsilon}$. Sonst setzen wir $\varepsilon_0 = \varepsilon$.

(b)
$$\alpha^p = \varepsilon_0^l \eta \text{ mit } p \in \mathbb{P} \text{ und } l \in \{0, \ldots, p-1\}.$$
Dann folgt
$$N_{\mathcal{E}/\mathcal{F}}(\alpha)^p = \pm\varepsilon_0^{il} \text{ und } i = 1, 3.$$
Aufgrund $l \in \{0, \ldots, p-1\}$ folgt für $i = 1$, daß die Gleichung keine Lösung hat. Der Fall $i = 3$ impliziert $p = 3$, wieder aufgrund $l \in \{0, \ldots, p-1\}$. Ferner gilt $N_{\mathcal{E}/\mathcal{K}}(\alpha)^p = \eta^2$, was jedoch $p = 2$ impliziert. Folglich hat die Gleichung (b) keine Lösung.

(c)
$$\alpha^p = \varepsilon_0^l \eta^k \gamma \text{ mit } p \in \mathbb{P} \text{ und } l, k \in \{0, \ldots, p-1\}.$$
Da $< \gamma >$ als Erzeuger von $RU_{\mathcal{E}}$ keine p-te Potenz ist, folgt das mindestens einer der beiden Exponenten k, l ungleich Null ist.
Falls $l \neq 0$ ist, folgt
$$N_{\mathcal{E}/\mathcal{F}}(\alpha)^p = \pm\varepsilon_0^{il}.$$
Analog wie Fall (b) kann nur die Situation $i = 3$ und $p = 3$ eintreten. Wegen
$$N_{\mathcal{E}/\mathcal{K}}(\alpha)^p = \eta^{2k} \text{ und } k \in \{0, \ldots, p-1\},$$
folgt p teilt k und damit $k = 0$.
Im Fall $\varepsilon_0 = \sqrt[3]{\varepsilon}$ gilt
$$N_{\mathcal{E}/\mathcal{F}}(\sqrt[3]{\varepsilon_0\gamma}) = \sqrt[3]{\varepsilon} \text{ und } N_{\mathcal{E}/\mathcal{F}}(\sqrt[3]{\varepsilon_0^2\gamma}) = \sqrt[3]{\varepsilon^2}.$$
Damit erhalten wir
$$\sqrt[3]{\varepsilon_0\gamma} \notin \mathcal{E} \text{ und } \sqrt[3]{\varepsilon_0^2\gamma} \notin \mathcal{E}.$$
Im Fall $k \neq 0$ behandelt man analog. Es folgt $p = 2$ und es muß $l = 0$ gelten, ansonsten hat die Gleichung keine Lösung.

KOROLLAR IV.9. *Das Einheitensysten $\varepsilon, \eta, \gamma$ enthält höchstens die Wurzeln:*

$$\sqrt[3]{\varepsilon}, \sqrt[3]{\varepsilon\gamma}, \sqrt[3]{\varepsilon^2\gamma}, \sqrt{\eta\gamma}.$$

Beweis: Gemäß Satz IV.8.

□

BEMERKUNG IV.10. *Im Fall $\sqrt[3]{\varepsilon} \notin \mathcal{E}$ (insbesondere wenn $\mathcal{K}$ rein kubisch) folgt mittels* IV.8*, daß ε und η zu einem Grundeinheitensystem erweiterbar sind.*

SATZ IV.11. *Sei $\gamma \in U_{\mathcal{E}}$ keine Torsionseinheit und es gelte $\gamma \notin < \varepsilon, \eta >$ bzw. $\gamma \notin < \sqrt[3]{\varepsilon}, \eta >$ im Fall $\sqrt[3]{\varepsilon} \in \mathcal{E}$. Dann existieren Exponenten $m_1, m_2, m_3 \in \mathbb{Z}$ mit*

$$N_{\mathcal{E}/\mathcal{K}}(\gamma^{m_1}\varepsilon^{m_2}\eta^{m_3}) \in TU_{\mathcal{K}} \text{ und } N_{\mathcal{E}/\mathcal{F}}(\gamma^{m_1}\varepsilon^{m_2}\eta^{m_3}) \in TU_{\mathcal{F}}.$$

Beweis: Sei $N_{\mathcal{E}/\mathcal{K}}(\gamma) = \eta^{l_1}$ und $N_{\mathcal{E}/\mathcal{F}}(\gamma) = \varepsilon^{l_2}$. Setze $m_1 = 6$, $m_2 = -3l_2, m_3 = -2l_1$ und $\gamma_0 = \gamma^{m_1}\varepsilon^{m_2}\eta^{m_3}$, dann gilt

$$N_{\mathcal{E}/\mathcal{K}}(\gamma_0) = N_{\mathcal{E}/\mathcal{K}}(\gamma)^{m_1} N_{\mathcal{E}/\mathcal{K}}(\eta)^{2m_2} N_{\mathcal{E}/\mathcal{K}}(\varepsilon)^{3m_3} = \eta^{6l_2}\eta^{-6l_2}(\pm 1) = \pm 1$$

$$N_{\mathcal{E}/\mathcal{F}}(\gamma_0) = N_{\mathcal{E}/\mathcal{F}}(\gamma)^{m_1} N_{\mathcal{E}/\mathcal{F}}(\eta)^{2m_2} N_{\mathcal{E}/\mathcal{F}}(\varepsilon)^{3m_3} = \eta^{6l_1} \quad 1 \quad \eta^{-6l_1} = 1$$

Bemerkungen:

a) Falls $l_2 \equiv 0 \mod 2$ kann $m_2 = \dfrac{l_2}{2}$ gewählt werden.

b) Falls $l_1 \equiv 0 \mod 3$ kann $m_3 = \dfrac{l_1}{3}$ gewählt werden.

□

ALGORITHMUS 1. (Berechnung von γ.)

Eingabe: *Die Einheiten ε, η und den Körper $\mathcal{E}$.*

Ausgabe: *Erzeuger γ mit der Eigenschaft $< \gamma >= RU_{\mathcal{E}}$.*

(1) *Berechne $\gamma \in U_{\mathcal{E}} \backslash TU_{\mathcal{E}}$ und $\gamma \notin < \varepsilon, \eta >$ bzw. $\gamma \notin < \sqrt[3]{\varepsilon}, \eta >$ im Fall $\sqrt[3]{\varepsilon} \in \mathcal{E}$.*
(2) *Mittels $N_{\mathcal{E}/\mathcal{K}}(\gamma) = \eta^{l_1}$ und $N_{\mathcal{E}/\mathcal{F}}(\gamma) = \varepsilon^{l_2}$ setze $\beta = \gamma^6\eta^{-3l_1}\varepsilon^{-2l_2}$ gemäß Satz* IV.11.
(3) *Setze $x \leftarrow 1 + \dfrac{1}{312 \log 36}$*
(4) *Setze $B \leftarrow \dfrac{\log H(\gamma)}{\log x}$*
(5) *Für alle $p \in \mathbb{P}^{<B}$ setze $\beta \leftarrow \sqrt[p]{\beta}$ falls $\sqrt[p]{\beta} \in \mathcal{E}$.*
(6) *Setze $\gamma \leftarrow \beta$ und terminiere*

Die dritte unabhängige Einheit in Schritt 1 kann mit den gängigen Verfahren, wie etwa in Pohst [30], berechnet werden. Mittels den Bedingungen aus Satz IV.8 können wir dann in sehr einfacher Weise ein Grundeinheitensystem von $\mathcal{E}$ berechnen. Allerdings ist der Algrorithmus 1 in der Praxis äußerst ineffizient, aufgrund der in Schritt 3 verwendeten Abschätzung. Diese basiert auf der Abschätzung in Satz II.4 für die Mindesthöhe von algebraischen Zahlen.

Natürlich lassen sich auch andere Kriterien für die Höhe einer Einheit benutzen, siehe etwa das Kriterium von Pehtő und Mignotte [25]. Diese Kriterien gelten sehr allgemein und liefern oftmals schlechte Abschätzungen für Schritt 1. Im nächsten Abschnitt sehen wir, daß Relativeinheiten tiefgreifendere Eigenschaften haben. Eine präzisere Beschreibung läßt hoffen, den Schritt 1 effizienter zu gestalten bzw. ganz zu eleminieren.

2. Betrachtung der Konjugiertenbeträge des Erzeugers von $RU_{\mathcal{E}}$

Alle bisher entwickelten Eigenschaften des Erzeugers von $RU_{\mathcal{E}}$ waren von gruppentheoretischer Natur. Im folgenden greifen wir unsere Ideen der geometrischen Charakterisierung im Kapitel II auf. Dabei werden wir sehen, daß wir mit Hilfe der Relativnormen die Konjugiertenbeträge des Erzeugers beschreiben können.

Auf den Nullstellen $\rho_1, \dots, \rho_6$ eines erzeugenden Polynoms der Körpererweiterung $\mathcal{E}$ über $\mathbb{Q}$ wählen wir folgende Anordnung:

$$\begin{aligned} \rho^{(1)}, \rho^{(2)} &\in \mathbb{R} \\ \rho^{(3)}, \rho^{(4)}, \rho^{(5)}, \rho^{(6)} &\in \mathbb{C} \setminus \mathbb{R} \\ \rho^{(3)} &= \overline{\rho^{(5)}} \\ \rho^{(4)} &= \overline{\rho^{(6)}}. \end{aligned}$$

Die Komponenten des Konjugiertenvektors der Norm über $\mathcal{F}$ von ρ sind:

$$(\rho^{(1)}\rho^{(3)}\rho^{(5)}, \rho^{(2)}\rho^{(4)}\rho^{(6)})$$

und entsprechend für die Norm über $\mathcal{K}$:

$$(\rho^{(1)}\rho^{(2)}, \rho^{(3)}\rho^{(4)}, \rho^{(5)}\rho^{(6)}).$$

An dieser Stelle fragen wir uns, ob wir für einen Erzeuger von $RU_{\mathcal{E}}$ eine feste Verteilung auf den Konjugiertenbeträgen vorschreiben können.

Satz IV.12. *Es existiert ein Erzeuger γ von $RU_{\mathcal{E}}$ mit*

$$|\gamma^{(1)}| > 1, |\gamma^{(2)}| < 1, |\gamma^{(3)}| < 1, |\gamma^{(4)}| > 1, |\gamma^{(5)}| < 1, |\gamma^{(6)}| < 1.$$

Beweis: Aufgrund der Relativnormen gelten folgende Eigenschaft für die Konjugiertenbeträge von γ:

$$|\gamma^{(1)}\gamma^{(3)}\gamma^{(5)}| = 1 = |\gamma^{(1)}||\gamma^{(3)}|^2 \tag{1}$$

$$|\gamma^{(2)}\gamma^{(4)}\gamma^{(5)}| = 1 = |\gamma^{(2)}||\gamma^{(4)}|^2 \tag{2}$$

und

$$|\gamma^{(1)}\gamma^{(2)}| = 1 \tag{3}$$

$$|\gamma^{(3)}\gamma^{(4)}| = 1 \tag{4}$$

$$|\gamma^{(5)}\gamma^{(6)}| = 1 \tag{5}$$

Wegen $\gamma^{(1)} \in \mathbb{R}$ wählen wir nun o.B.d.A. $|\gamma^{(1)}| > 1$. Dann folgt $|\gamma^{(2)}| < 1$ und damit:

$$\begin{array}{rcccccrcl} & & & & & \Rightarrow & |\gamma^{(2)}| & < & 1 \\ \Rightarrow\ |\gamma^{(3)}\gamma^{(5)}| & = & |\gamma^{(3)}|^2 & < & 1 & \Rightarrow & |\gamma^{(3)}| & < & 1 \\ |\gamma^{(4)}\gamma^{(6)}| & = & |\gamma^{(4)}|^2 & > & 1 & \Rightarrow & |\gamma^{(4)}| & > & 1 \\ & & & & & \Rightarrow & |\gamma^{(5)}| & < & 1 \\ & & & & & \Rightarrow & |\gamma^{(6)}| & < & 1 \end{array}$$

□

Bemerkung IV.13. *Die in Satz* IV.12 *angegebene Verteilung für die Konjugiertenbeträge gilt nicht nur für einen Erzeuger von $RU_{\mathcal{E}}$. Jedes nicht triviale Element von $RU_{\mathcal{E}}$ oder sein Inverses genügt dieser Verteilung.*

Es stellt sich die Frage, ob der Erzeuger von $RU_{\mathcal{E}}$ nicht spezieller charakterisiert werden kann. Analog zur Grundeinheit im reell–quadratischen Fall können wir den Erzeuger von $RU_{\mathcal{E}}$ eindeutig festlegen.

Satz IV.14. *Die Zahl γ mit $<\gamma>= RU_{\mathcal{E}}$ kann durch:*

(a) $\gamma \in RU_{\mathcal{E}}$,
(b) $\gamma^{(1)} > 0$,
(c) $|\gamma^{(1)}| > 1$,
(d) *es existiert kein α in $RU_{\mathcal{E}}$ mit $0 < |\alpha^{(1)}| < |\gamma^{(1)}|$*

eindeutig beschrieben werden.

Beweis: Zunächst gilt mit (a) und (c) das γ eine nicht triviale Relativeinheit von $\mathcal{E}$ ist. Die Bedingung (d) garantiert, daß das Element γ keine p-te Potenz in $\mathcal{E}$ ist. Da nach Satz IV.7 $RU_{\mathcal{E}}$ von einem Element erzeugt wird folgt die Behauptung.

□

Der Erzeuger von $RU_{\mathcal{E}}$ läßt sich nicht nur eindeutig normieren sondern besitzt noch eine weitere besondere Eigenschaft. Im reell–quadratischen Fall ist mit dem ersten Konjugiertenbetrag auch der zweite Konjugiertenbetrag bekannt. Diese Eigenschaft läßt sich sogar auf alle Konjugiertenbeträge eines Erzeugers von $RU_{\mathcal{E}}$ verallgemeinern.

Satz IV.15. *Sei γ der Erzeuger von $RU_{\mathcal{E}}$. Dann sind mit $|\gamma^{(1)}|$ alle weiteren Konjugiertenbeträge bekannt. Es gilt:*

$$|\gamma^{(1)}|, |\gamma^{(2)}| = \frac{1}{|\gamma^{(1)}|}, |\gamma^{(3)}| = \frac{1}{\sqrt{|\gamma^{(1)}|}}, |\gamma^{(4)}| = \sqrt{|\gamma^{(1)}|}, |\gamma^{(5)}| = \frac{1}{\sqrt{|\gamma^{(1)}|}}, |\gamma^{(6)}| = \sqrt{|\gamma^{(1)}|}.$$

Beweis: Wie bereits oben gesehen gilt:

$$1 = |\gamma^{(2)}\gamma^{(4)}\gamma^{(6)}| = |\frac{1}{\gamma^{(1)}}\gamma^{(4)}\gamma^{(6)}| = \frac{|\gamma^{(4)}|^2}{|\gamma^{(1)}|} \Rightarrow |\gamma^{(1)}| = |\gamma^{(4)}|^2.$$

Der Rest folgt analog.

□

Bemerkung IV.16. *Der Satz* IV.15 *gilt näturlich für jede Einheit von $RU_{\mathcal{E}}$. Damit sind die Elemente von $RU_{\mathcal{E}}$ von sehr spezieller Natur. Für ein solches Element reicht die Kenntnis eines Konjugiertenbetrages bereits aus, um alle anderen Konjugiertenbeträge zu kennen.*

Letztendlich sind wir an einem Algorithmus interessiert, der den Erzeuger von $RU_{\mathcal{E}}$ explizit ermittelt. Gegenstand dieser Untersuchung ist eine Verallgemeinerung des reell–quadratischen Kettenbruchverfahrens auf diesen speziellen Fall. Das Problem besteht darin, die Symmetriebedingung aus Satz IV.15 auf den sechs Konjugiertenbeträgen in einen mehrdimensionalen Kettenbruch zu überführen.

KAPITEL V

Eine parametrisierte Familie von Zahlkörpern

In diesem Kapitel werden wir eine Familie von total reellen Zahlkörpern vierten Grades betrachten. Die Zahlkörper sind durch ein parametrisiertes Polynom vierten Grades in $\mathbb{Z}[t]$ gegeben.

Gegenstand unserer Untersuchungen ist die Einheitengruppe der Gleichungsordnung des Zahlkörpers, die nach dem Dirichletschen Einheitensatz mittels dreier Grundeinheiten erzeugt werden kann. Ähnliche Betrachtungen sind bereits für quadratische Zahlkörper von Degert [11] und kubische Zahlkörper von Stender [38] gemacht worden.

Die Komplexität dieser Probleme scheint bei Grad 4 doch wesentlich größer zu werden, da nur wenige Untersuchungen darüber bekannt sind. Für Körper vierten Grades mit Galoisgruppe C_4 oder V_4, also galoisssche Erweiterungen über $\mathbb{Q}$, liegen bereits einige Ergebnisse vor. Jedoch gibt es kaum Resultate für nicht galoissche Erweiterungen. In jüngster Zeit gelang es A. Pethő [28] eine solche Familie in Zusammenhang mit Thuegleichungen zu untersuchen. Dabei konnten Grundeinheiten in der Gleichungsordnung in parametrisierter Form bestimmt werden.

Neben der Einheitengruppe der Gleichungsordnung werden wir auch die Galoisgruppe des definierenden Polynoms und die p-Maximalität der Gleichungsordnung betrachten. Die Untersuchungen zur Galoisgruppe führen uns zu folgendem Ergebnis. Die Galoisgruppe der betrachteten Körper (Polynome) wird isomorph zur S_4 sein.

1. Das parametrisierte Polynom

Ausgangspunkt unserer Betrachtungen bildet die Familie von Körpern vierten Grades, welche durch folgende Parametrisierung

$$f(t) = t^4 - (a^2 + a + 1)t^2 + (a^2 + a)t + 1 \in \mathbb{Z}[t], \quad a \in \mathbb{Z}$$

gegeben ist.

Zunächst beweisen wir einige grundlegende Eigenschaften des Polynoms.

SATZ V.1. *Für alle $a \in \mathbb{Z}$ ist das Polynom $f(t) \in \mathbb{Z}[t]$ irreduzibel in $\mathbb{Z}[t]$.*

Beweis: Als Linearfaktoren von $f(t)$ in $\mathbb{Z}[t]$ sind nur die beiden Polynome $(t-1)$ oder $(t+1)$ möglich. Wegen $f(1) = 1$ und $f(-1) = -2(a^2 + a) + 1 \neq 0$ für alle $a \in \mathbb{Z}$ kann $f(t)$ in $\mathbb{Z}[t]$ keine Linearfaktoren haben. Es bleibt zu überprüfen, ob $f(t)$ in $\mathbb{Z}[t]$ in zwei irreduzible, quadratische Faktoren zerfallen kann. Mit $p, q, u, v \in \mathbb{Z}$ verfolgen wir den Ansatz:

$$\begin{aligned} f(t) &= t^4 - (a^2 + a + 1)t^2 + (a^2 + a)t + 1 \\ &= (t^2 + pt + q)(t^2 + ut + v) \\ &= t^4 + (u + p)t^3 + (v + pu + q)t^2 + (pv + qu)t + qv. \end{aligned}$$

Durch Koeffizientenvergleich vor t^3 erhalten wir $u = -p$ und somit

$$f(t) = t^4 + (v - p^2 + q)t^2 + p(v - q)t + qv.$$

Durch Koeffizientenvergleich der konstanten Glieder auf beiden Seiten erhalten wir $qv = 1$ und damit folgt $q = v = 1$ oder $q = v = -1$.

Für die beiden Fälle ergibt sich:

- $q = v = 1$:
  Dann erhalten wir $p(1 - 1) = 0$ als Faktor vor t in $f(t)$, im Widerspruch zu $a^2 + a \neq 0$ für $a \in \mathbb{Z} \setminus \{-1, 0\}$.
- $q = v = -1$:
  Dann erhalten wir $p((-1) - (-1)) = 0$ als Faktor vor t in $f(t)$, im Widerspruch zu $a^2 + a \neq 0$ für $a \in \mathbb{Z} \setminus \{-1, 0\}$.

Es bleiben folglich nur die Fälle $a = -1$ oder $a = 0$, in denen $f(t)$ jeweils folgende Gestalt besitzt:

$$f(t) = t^4 - t^2 + 1.$$

Für die Parameter q, v diskutieren wir die verbleibenden Fälle:

- $q = v = 1$:
  Dann erhalten wir $1 - p^2 + 1 = -1$ als Faktor vor t^2 in $f(t)$ und damit $-p^2 = -3$ (Widerspruch).
- $q = v = -1$:
  Dann erhalten wir $-1 - p^2 - 1 = -1$ als Faktor vor t^2 in $f(t)$ und damit $-p^2 = 1$ (Widerspruch).

Somit ist $f(t)$ für alle $a \in \mathbb{Z}$ irreduzibel.

□

Damit erzeugt eine Wurzel des Polynoms $f(t)$ eine Erweiterung vierten Grades über $\mathbb{Q}$. Die Signatur dieser Erweiterung bestimmen wir durch Betrachtung von Vorzeichenwechsel.

Satz V.2. *Das Polynom $f(t) \in \mathbb{Z}[t]$ besitzt für $a \in \mathbb{Z}^{\geq 3}$ vier paarweise verschiedene reelle Nullstellen.*

Beweis: Wir werten das Polynom $f(t)$ an den Stellen $-a-2, -a, 0, 2, a+1$ aus und erhalten folgenden Ungleichungen:

$$\begin{array}{lclcl} f(-a-2) & = & 2\,a^3 + 12\,a^2 + 22\,a + 13 & > & 0, \\ f(-a) & = & -2\,a^3 - 2\,a^2 + 1 & < & 0, \\ f(0) & = & 1 & > & 0, \\ f(2) & = & 13 - 2\,a^2 - 2\,a & < & 0, \\ f(a+1) & = & 2\,a^3 + 4\,a^2 + 2\,a + 1 & > & 0. \end{array}$$

Für alle $a \in \mathbb{Z}^{\geq 0}$ sind bis auf die vierte Ungleichung alle weiteren stets erfüllt. Die Einschränkung $a \in \mathbb{Z}^{\geq 3}$ sorgt für $f(2) < 0$. Das Polynom besitzt somit im Intervall $[-(a+2), a+1]$ mindestens (und damit auch höchstens) vier Vorzeichenwechsel. Damit erhalten wir vier verschiedene reelle Nullstellen von $f(t)$.

□

In den beiden nächsten Sätzen diskutieren wir die weiteren Werte von a.

Bemerkung V.3.

(1) *Ersetzen wir $a = 2$ in $f(t)$, so erhalten wir*

$$f(t) = t^4 - 7t^2 + 6t + 1.$$

Das Polynom besitzt ebenfalls 4 reelle Nullstellen:

$$-2.983110855..., -.1429092782..., 1.251060047..., 1.874960086... \quad .$$

Allerdings läßt sich nachrechnen, daß die Galoisgruppe im Fall $a = 2$ isomorph zur Diedergruppe mit 8 Elementen ist. Wir werden später beweisen, daß die Galoisgruppe der Polynome für $a \geq 3$ stets isomorph zur symmetrischen Gruppe auf 4 Elementen ist.

(2) *Ersetzen wir $a = 1$ in $f(t)$, so erhalten wir*

$$f(t) = t^4 - 3t^2 + 2t + 1.$$

Das Polynom besitzt nur noch 2 reelle Nullstellen:

$$-1.940392664..., -.3365322739... \quad .$$

(3) *Ersetzen wir $a = 0$ in $f(t)$, so erhalten wir*

$$f(t) = t^4 - t^2 + 1,$$

und dieses Polynom besitzt keine reellen Nullstellen mehr.

Im folgenden Satz leiten wir eine Symmetriebedingung her, die es ermöglicht auch negative Werte von a einfach zu betrachten.

Satz V.4. *Wir betrachten $f(t)$ jetzt in der Form $f(t) = f(t, a)$, also als Polynom in zwei Variablen. Dann gilt:*

$$f(t, a) = f(t, -a - 1).$$

Beweis: Einfaches Substituieren von a durch $-a - 1$ in $f(t)$.

□

Für den Rest der Arbeit setzen wir $a \in \mathbb{Z}^{\geq 3}$ voraus, ohne dieses weiterhin explizit zu erwähnen.

Jede Wurzel des Polynoms $f(t) \in \mathbb{Z}[t]$ erzeugt somit eine total reelle Körpererweiterung über $\mathbb{Q}$. Nach dem Dirichletschen Einheitensatz ist der Rang der Einheitengruppe 3 und somit maximal für Erweiterungen vierten Grades.

Neben der Existenz von vier reellen Nullstellen werden wir im späteren Verlauf noch explizite Abschätzungen der Nullstellen von $f(t)$ benötigen. Im folgenden Satz leiten wir einfache Abschätzungen in Abhängigkeit des Parameters a her.

Satz V.5. *Es seien $\rho_1, \dots, \rho_4$ die vier reellen Nullstellen von $f(t)$. O.B.d.A. wählen wir die Anordnung $\rho_1 > \rho_2 > \rho_3 > \rho_4$. Dann gelten für $a \geq 6$ die folgenden*

Abschätzungen:

$$\begin{array}{rcccl} a-\dfrac{1}{a^3} & < & \rho_1 & < & a-\dfrac{1}{a^4}, \\ 1+\dfrac{1}{a^{2.1}} & < & \rho_2 & < & 1+\dfrac{1}{a^2}, \\ -\dfrac{1}{a^2} & < & \rho_3 & < & -\dfrac{1}{a^{2.1}}, \\ -a-1+\dfrac{1}{a^4} & < & \rho_4 & < & -a-1+\dfrac{1}{a^3}. \end{array}$$

Beweis: Wir werten das Polynom an den Stellen

$$a-\frac{1}{a^3},\quad a-\frac{1}{a^4},\quad 1+\frac{1}{a^{2.1}},\quad 1+\frac{1}{a^2},$$
$$-\frac{1}{a^2},\quad -\frac{1}{a^{2.1}},\quad -a-1+\frac{1}{a^4},\quad -a-1+\frac{1}{a^3}$$

aus und erhalten:

$$\begin{array}{lcl} f(a-\frac{1}{a^3}) & = & -\frac{a^{12}-5\,a^8+4\,a^4-1-a^{11}+a^7-a^{10}+a^6}{a^{12}}, \\ f(a-\frac{1}{a^4}) & = & \frac{-2\,a^{15}+5\,a^{10}-4\,a^5+1+a^{14}-a^9+a^{13}-a^8+a^{16}}{a^{16}}, \end{array}$$

$$\begin{array}{lcl} f(1+\frac{1}{a^{2.1}}) & = & 1-a^{-1/10}-a^{-\frac{11}{10}}+2a^{-\frac{21}{10}}-a^{-\frac{11}{5}}-a^{-\frac{16}{5}} \\ & & +5a^{-\frac{21}{5}}+4a^{-\frac{63}{10}}+a^{-\frac{42}{5}} \\ f(1+\frac{1}{a^2}) & = & -\frac{-a^6-5\,a^4-4\,a^2-1+a^7+a^5}{a^8}, \end{array}$$

$$\begin{array}{lcl} f(-\frac{1}{a^2}) & = & -\frac{-1+a^6+a^5+a^4+a^7}{a^8}, \\ f(-\frac{1}{a^{2.1}}) & = & \frac{a^{\frac{21}{10}}-a^{\frac{83}{10}}-a^{\frac{73}{10}}-a^{\frac{63}{10}}-a^{\frac{52}{5}}-a^{\frac{47}{5}}+a^{21/2}}{a^{21/2}} \end{array}$$

$$\begin{array}{lcl} f(-a-1+\frac{1}{a^4}) & = & \frac{a^{16}-7\,a^{13}-4\,a^4-7\,a^{14}+5\,a^{10}-2\,a^{15}-2\,a^{12}+5\,a^8+11\,a^9-4\,a^5+1}{a^{16}}, \\ f(-a-1+\frac{1}{a^3}) & = & -\frac{a^{12}+2\,a^9-11\,a^7-1+7\,a^{10}-5\,a^6+7\,a^{11}-5\,a^8+4\,a^4+4\,a^3}{a^{12}}. \end{array}$$

Für die Einschachtelung der Nullstelle ρ_1 zeigen wir

$$f(a-\frac{1}{a^3})<0<f(a-\frac{1}{a^4}).$$

Ersetzen wir die entsprechenden Funktionswerte, so ist zu zeigen

$$f\left(a-\frac{1}{a^3}\right) = -\frac{a^{12}-5\,a^8+4\,a^4-1-a^{11}+a^7-a^{10}+a^6}{a^{12}}$$
$$< 0 <$$
$$\frac{-2\,a^{15}+5\,a^{10}-4\,a^5+1+a^{14}-a^9+a^{13}-a^8+a^{16}}{a^{16}} = f\left(a-\frac{1}{a^4}\right).$$

Dies folgt, indem wir a durch $a+3$ substituieren:

$$-\frac{184210578a+423875862a^2+603553848a^3+594681449a^4+8254017a^9+1974a^{13}+32419354a^8+26205a^{12}}{(a+3)^{12}}$$
$$-\frac{429449463a^5+234797998a^6+240681a^{11}+98964061a^7+1619940a^{10}+92a^{14}+2a^{15}+37347803}{(a+3)^{12}}$$
$$< 0 <$$
$$\frac{123708a^{12}+116228682a+302703048a^2+18266540a^9+13273a^{13}+58797305a^8+467273633a^5+4467182a^{10}}{(a+3)^{16}}$$
$$+\frac{557521806a^4+a^{16}+991a^{14}+46a^{15}+20994229+491816088a^3+299375667a^6+850824a^{11}+149506050a^7}{(a+3)^{16}}.$$

Auf der linken und rechten Seite der Ungleichung befinden sich nur positive Summanden im Zähler. Der linke Bruch hat ein negatives Vorzeichen und der rechte Bruch ein positives Vorzeichen. Die Ungleichung gilt für $a \in \mathbb{Z}^{\geq 0}$, die ursprüngliche Ungleichung gilt folglich für $a \in \mathbb{Z}^{\geq 3}$.

Damit folgt:

$$\rho_1 \in]a-\frac{1}{a^3}, a-\frac{1}{a^4}[.$$

Für die Nullstelle ρ_3 müssen wir eine schärfere Ungleichung beweisen. Es ist zu zeigen, daß

$$f(-\frac{1}{a^2}) < 0 < f(-\frac{1}{a^{2.1}})$$

gilt. Während $f(-\frac{1}{a^2}) < 0$ klar ist, muß für die andere Ungleichung noch folgendes betrachtet werden. Es gilt

$$f(-\frac{1}{a^{2.1}}) = \frac{a^{\frac{21}{10}}-a^{\frac{83}{10}}-a^{\frac{73}{10}}-a^{\frac{63}{10}}-a^{\frac{52}{5}}-a^{\frac{47}{5}}+a^{21/2}}{a^{21/2}},$$

und für $a=6$ erhalten wir den Wert

$$f(-\frac{1}{6^{2.1}}) = 0.001528630438 > 0.$$

Für die Ableitung von $f(-\frac{1}{a^{2.1}})$ nach a gilt

$$\left(f(-\frac{1}{a^{2.1}})\right)' = \frac{0.1a^{\frac{83}{10}} + 1.1a^{\frac{73}{10}} + 2.2a^{\frac{31}{5}} + 3.2a^{\frac{26}{5}} + 4.2a^{\frac{21}{5}} - 8.4}{a^{\frac{47}{5}}}.$$

Für $a > 6$ ist die Ableitung stets positiv und damit gilt

$$f(-\frac{1}{a^{2.1}}) > 0.$$

Folglich gilt

$$\rho_3 \in]-\frac{1}{a^2}, -\frac{1}{a^{2.1}}[,$$

Für die weiteren Nullstellen ρ_2, ρ_4 können die obigen Ungleichungen analog nachvollzogen werden und wir bekommen:

$$\rho_2 \in]1 + \frac{1}{a^{2.1}}, 1 + \frac{1}{a^2}[,$$

$$\rho_4 \in]-a-1+\frac{1}{a^4}, -a-1+\frac{1}{a^3}[.$$

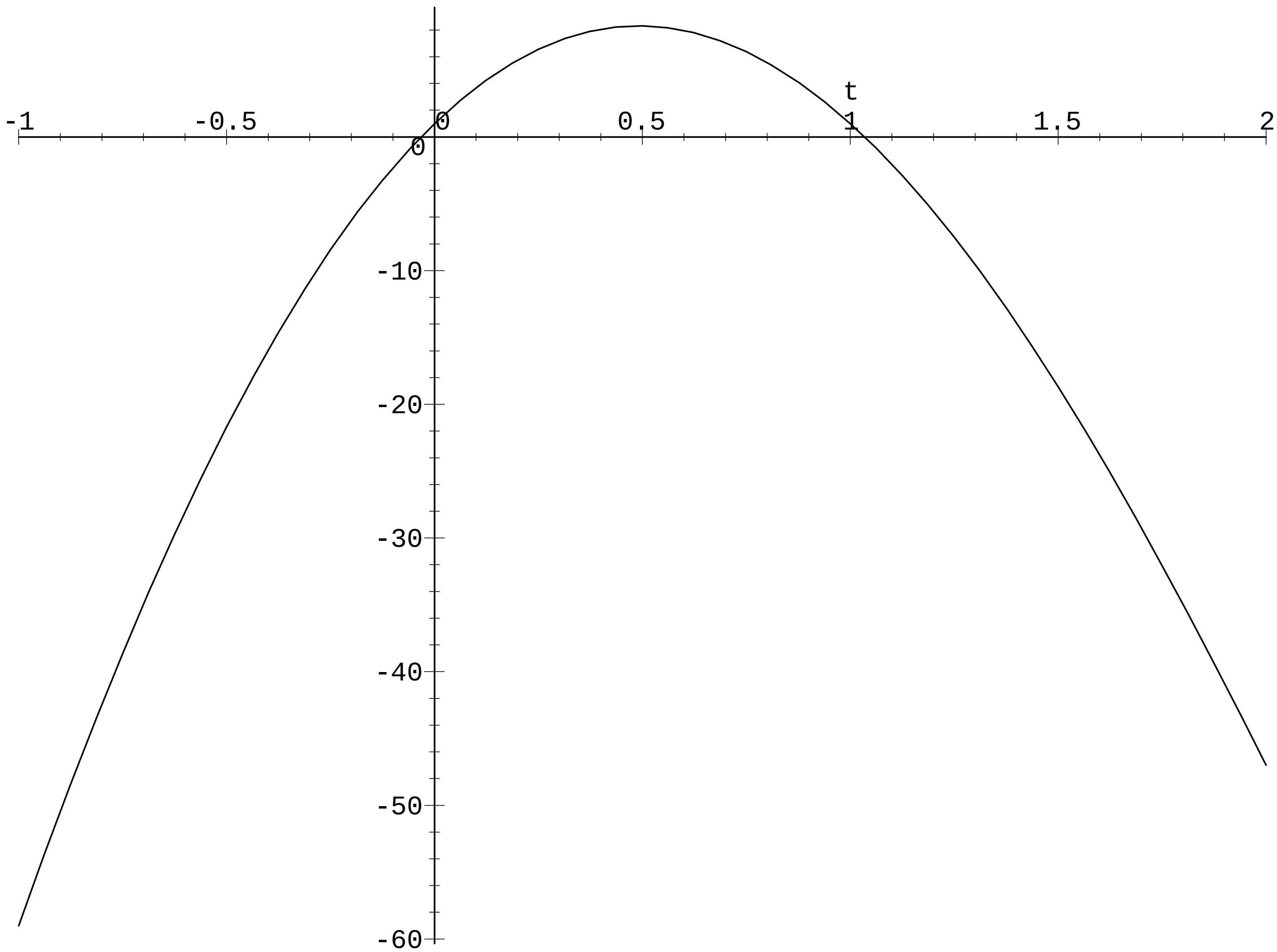
□

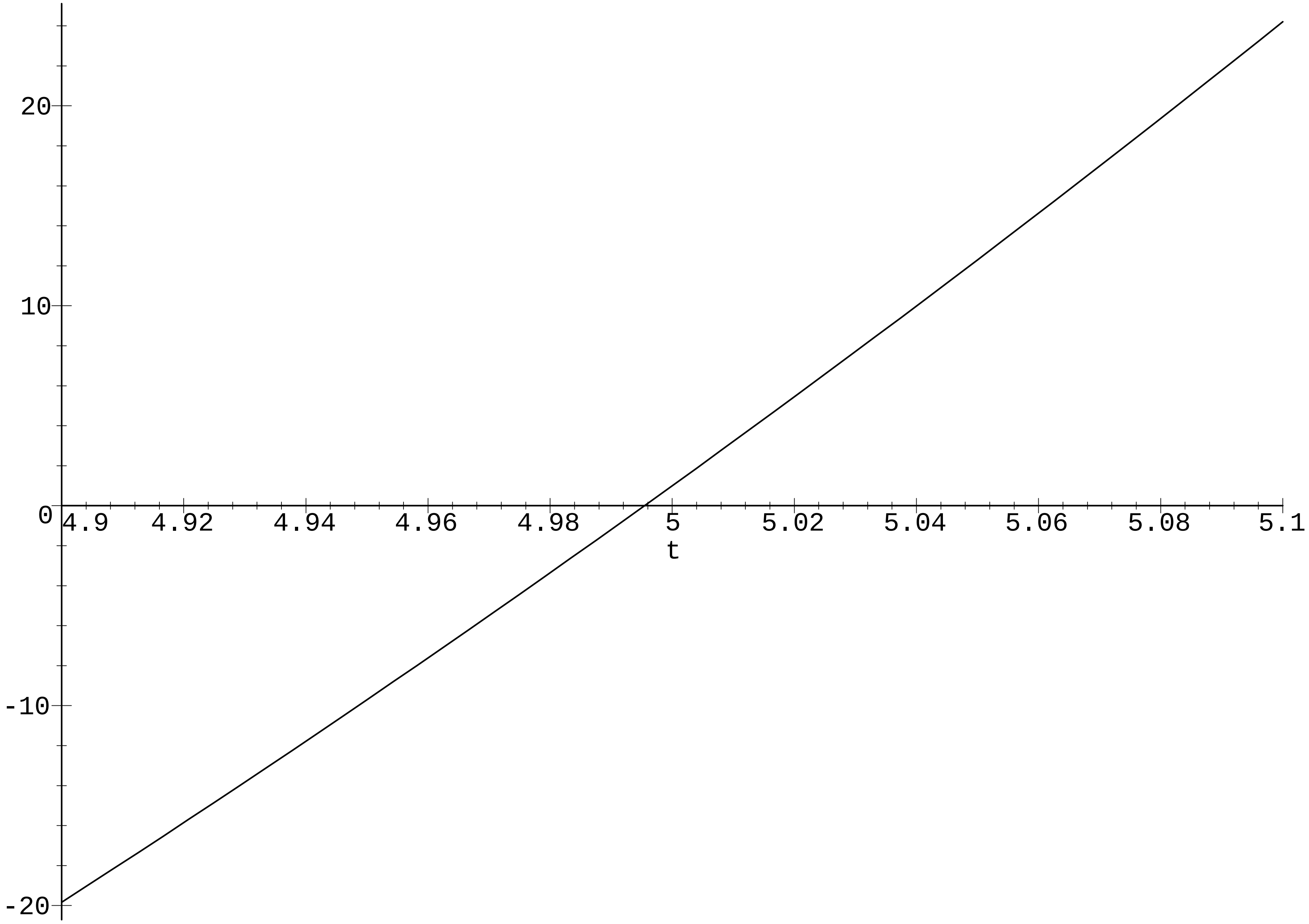
Bemerkung V.6. *Später benötigen wir folgende (grobe) Ungleichungskette für die Nullstellen:*

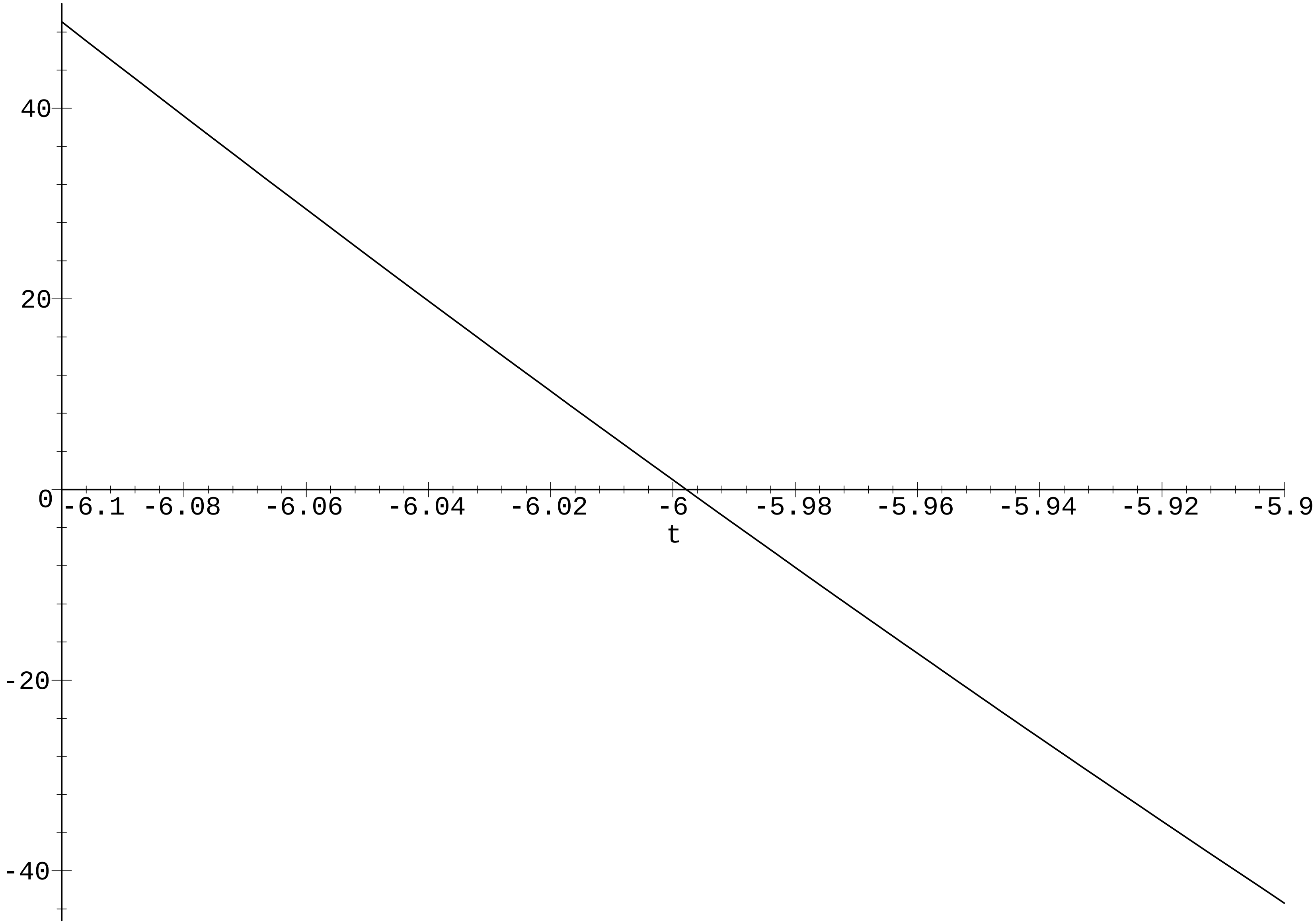
$$\rho_4 < -1 < \rho_3 < 0 < 1 < \rho_2 < 2 < \rho_1 < a.$$

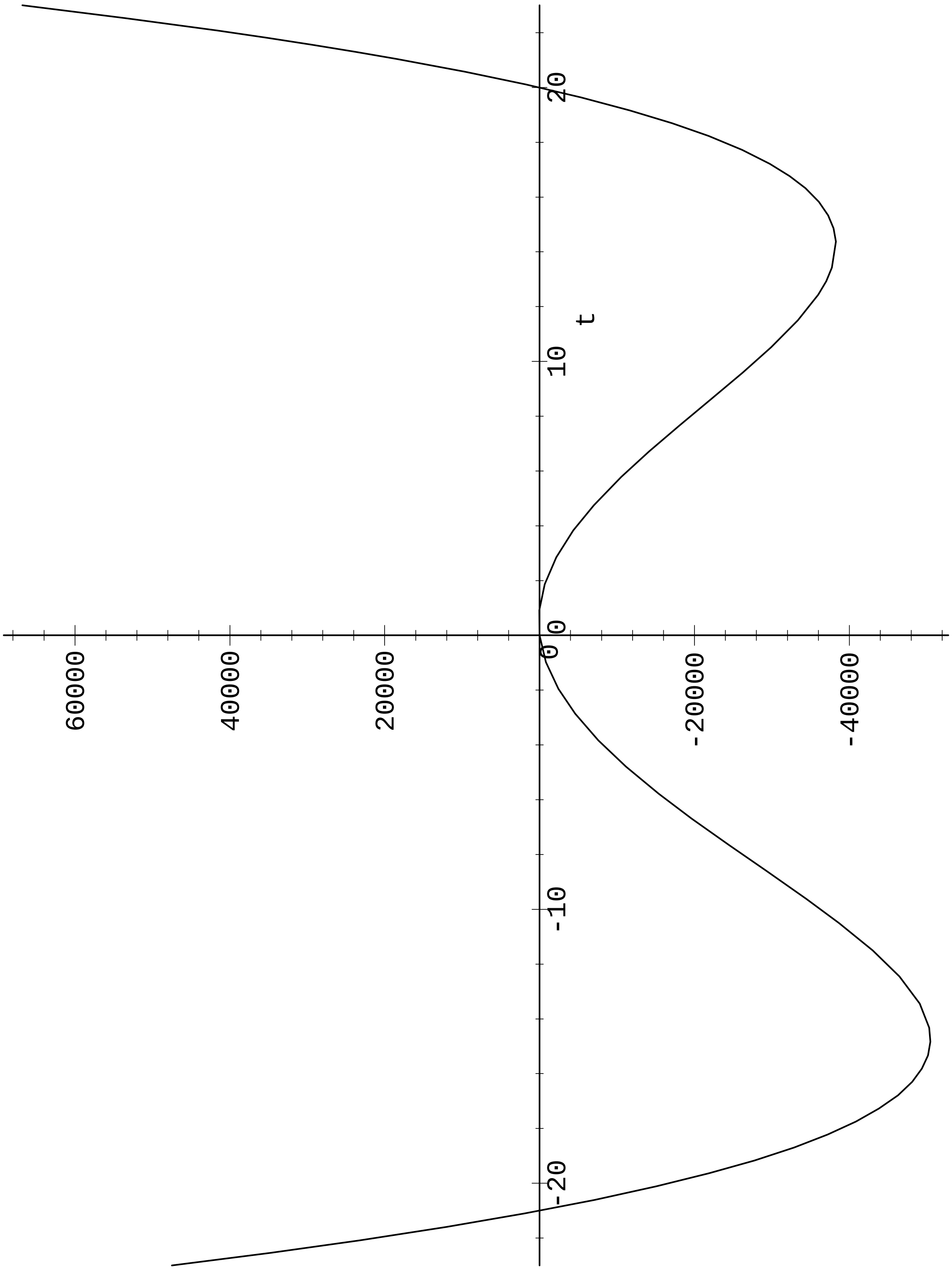
Auf den folgenden Seiten haben wir den Graphen für zwei Werte von a exemplarisch gezeichnet. Die graphische Darstellung spiegelt die Lage der Nullstellen aus Satz V.5 wieder.

(1) Auf der Seite 54 ist der Graph für $a = 5$ in grober Übersicht. Allerdings läßt sich die Lage der Nullstellen in dieser Übersicht nicht erkennen.
(2) Auf der Seite 55 ist der Graph für $a = 5$, so daß die Nullstellen in den Umgebungen von 0 und 1 besser sichtbar sind.
(3) Auf der Seite 56 ist der Graph für $a = 5$ in einer Umgebung von $t = 5$. Die Nullstelle liegt deutlich unterhalb von 5.
(4) Auf der Seite 57 ist der Graph für $a = 5$ in einer Umgebung von $t = -6$. Die Nullstelle liegt deutlich über -6.
(5) Auf der Seite 58 ist der Graph für $a = 20$ in grober Übersicht.


t
-1
-0.5
0
0.5
1
1.5
2
0
-10
-20
-30
-40
-50
-60


20
10
0
-10
-20
4.9
4.92
4.94
4.96
4.98
5
5.02
5.04
5.06
5.08
5.1
t


40
20
0
-20
-40
-6.1
-6.08
-6.06
-6.04
-6.02
-6
-5.98
-5.96
-5.94
-5.92
-5.9
t


20
10
t
0
-10
-20
60000
40000
20000
0
-20000
-40000

2. Zur Maximalordnung der Körper

Ab jetzt bezeichnen wir mit $\mathcal{F}$ den von einer Wurzel des Polynoms $f(t)$ erzeugten Zahlkörper. Die Bestimmung der Diskriminante von $\mathcal{F}$ bzw. einer Ganzheitsbasis setzt zunächst die Kenntnis der Polynomdiskriminante voraus.

SATZ V.7. *Die Polynomdiskriminante von $f(t)$ beträgt:*

$$d_f = 4\,a^{10}+20\,a^9+41\,a^8+44\,a^7-42\,a^6-196\,a^5-375\,a^4-412\,a^3-364\,a^2-192\,a+144.$$

Beweis: Dies rechnen wir leicht nach.

$\square$

BEMERKUNG V.8. *Die Polynomdiskriminante, als Polynom in $\mathbb{Z}[a]$, ist irreduzibel. Damit ist d_f nicht notwendig ein Quadrat in den ganzen Zahlen für alle a und somit S_4 als Galoisgruppe à priori nicht ausgeschlossen.*

Im folgenden untersuchen wir die p-Maximalität der Gleichungsordnung. Eine Vorhersage der Faktorisierung von d_f in den ganzen Zahlen scheint hoffnungslos. Wir analysierten die Faktorisierung der Diskriminante für $3 \leq a \leq 200$ und $1000 \leq a \leq 1050$. Dabei beobachteten wir, daß insbesondere die Primzahlen 2 und 3 eine spezielle Rolle spielen, wie wir den Tabellen auf den folgenden Seiten entnehmen.

a	Diskriminante von $f(t)$	Faktorisierung der Diskriminante
3	871632	2^4 3^2 6053
4	12343504	2^4 293 2633
5	96013584	2^4 3^2 71 9391
6	520527312	2^4 3^2 3614773
7	2200269712	2^4 131 1049747
8	7740258192	2^4 3^2 191 281423
9	23634227664	2^4 3^2 151 1086931
10	64474199824	2^4 227 617 28771
11	160442745552	2^4 3^2 1114185733
12	369888188112	2^4 3^2 491 5231503
13	799442670352	2^4 127 2027 194093
14	1634947836624	2^4 3^2 11353804421
15	3187417374864	2^4 3^2 22134842881
16	5959404341392	2^4 139 2679588283
17	10738468565712	2^4 3^2 74572698373
18	18725970020112	2^4 3^2 277 469463749
19	31711162354384	2^4 107 18522875207
20	52302541354704	2^4 3^2 691 525632551
21	84230630402832	2^4 3^2 131 4465152163
22	132738873602512	2^4 53 311473 502553
23	205082071619472	2^4 3^2 53 26871340621
24	311154849964944	2^4 3^2 2160797569201
25	464276008955344	2^4 29017250559709
26	682158283417872	2^4 3^2 2917 26513 61253
27	988097052898512	2^4 3^2 39371 174285263
28	1412415904180432	2^4 1143217 77217181
29	1994211671852304	2^4 3^2 53 1459 179092583
30	2783446683992784	2^4 3^2 53 10313 35363849
31	3843441433274512	2^4 83 11593 249647003
32	5253826793453712	2^4 3^2 17683 2063275931
33	7114021221814992	2^4 3^2 49402925151493
34	9547305144200464	2^4 596706571512529
35	12705571925283024	2^4 3^2 367 240417270763
36	16774842497260752	2^4 3^2 4289 37123 731639
37	21981638869668112	2^4 246523 5572917859
38	28600320386035152	2^4 3^2 22303 8905229611
39	36961495744193424	2^4 3^2 241 1065050015681
40	47461633470642064	2^4 101 16223 1810381723
41	60574003750064592	2^4 3^2 2312173 181929641
42	76861095273341712	2^4 3^2 457 147793 7902673
43	96988662095752912	2^4 6061791380984557
44	121741567406015184	2^4 3^2 353 352771 6789047
45	152041603610885904	2^4 3^2 1055844469520041
46	188967481253774032	2^4 173 617 110646027097
47	233777193023674512	2^4 3^2 1095989 1481267357
48	287932973487280272	2^4 3^2 197 1399 16091 450881
49	353129090206849744	2^4 22070568137928109
50	431322717603830544	2^4 3^2 25935449 115490449

a	Diskriminante von $f(t)$	Faktorisierung der Diskriminante
51	524768161307877072	2^4 3^2 83 43906305330311
52	636054717807266512	2^4 17939 2216033216063
53	768148472004329232	2^4 3^2 1439 3863 959615329
54	924438353792881104	2^4 3^2 163 193 3167 64435097
55	1108786794028291984	2^4 69299174626768249
56	1325585340269261712	2^4 3^2 127 23741 3053110139
57	1579815613448117712	2^4 3^2 467 2677 3433 2556259
58	1877116008188011792	2^4 13003 9022514074579
59	2223854561845293264	2^4 3^2 1583 2399 20959 194027
60	2627208440528086224	2^4 3^2 101 149 193 673 9333661
61	3095250514342215952	2^4 193453157146388497
62	3637043518957628112	2^4 3^2 25257246659427973
63	4262742326286839952	2^4 3^2 631 46913434652743
64	4983704873636270224	2^4 13313 22273 1050455561
65	5812612328146029264	2^4 3^2 71 233 3917 622932551
66	6763599091688427792	2^4 3^2 185543 253145837551
67	7852393280664597712	2^4 823 109097 5465997347
68	9096468345336725712	2^4 3^2 367277 171995303449
69	10515206524474995984	2^4 3^2 58393 1250531185777
70	12130074863197937104	2^4 73 127 263 450223 690611
71	13964814554956985232	2^4 3^2 54371 1783632430043
72	16045644402675226512	2^4 3^2 3877 5297 5425863917
73	18401479229110981072	2^4 659 1745208576357263
74	21064164102593654544	2^4 3^2 146278917379122601
75	24068725281386625744	2^4 3^2 53 73 467 92507083187
76	27453638818084376272	2^4 53 71 3347 136235409797
77	31261117804663114512	2^4 3^2 59951 3621142197223
78	35537419279090318032	2^4 3^2 15991 562631 27429893
79	40333171855773429904	2^4 223 11304140094106903
80	45703725184605911184	2^4 3^2 317386980448652161
81	51709522386964488912	2^4 3^2 83 6827 633723831253
82	58416496661739261712	2^4 53 591131 116534876599
83	65896493300352848592	2^4 3^2 53 8543 88853 11374739
84	74227718396760506064	2^4 3^2 83 6210485140291207
85	83495215586634609424	2^4 317 673 683 14143 2532241
86	93791372199338611152	2^4 3^2 24281 26824635460093
87	105216456256902068112	2^4 3^2 107 239 28571924886301
88	117879185806034084752	2^4 149 49445967200517653
89	131897332122272067024	2^4 3^2 915953695293556021
90	147398358379670536464	2^4 3^2 1023599710969934281
91	164520095435005430992	2^4 12547 819519085413871
92	183411456432317333712	2^4 3^2 1033 1233001616329981
93	204233191991756938512	2^4 3^2 223 449 4027 3517474837
94	227158687806142296784	2^4 229 4421 205847 68125363
95	252374806529404508304	2^4 3^2 30387661 57674818181
96	280082775903201036432	2^4 3^2 1217 1289 1239882169081
97	310499125131428258512	2^4 19406195320714266157
98	343856671577181721872	2^4 3^2 2221 542951 1980185003
99	380405559922908379344	2^4 3^2 223 12829 319819 2887237
100	420414356002084340944	2^4 509 51622587917741201

a	Diskriminante von $f(t)$	Faktorisierung der Diskriminante
101	464171197579748915472	2^4 3^2 1210042549 2663882437
102	511985004429645442512	2^4 3^2 1045807423 3399719051
103	564186750127576146832	2^4 129917 271416919132781
104	621130798053886498704	2^4 3^2 11351 380002494918391
105	683196304172768850384	2^4 3^2 975181 4865167367881
106	750788689232329956112	2^4 12547501 3739732164757
107	824341183107116885712	2^4 3^2 10499 545251123855127
108	904316444084055325392	2^4 3^2 163 103067 456811 818303
109	991208255973537838864	2^4 131 472904702277451259
110	1085543306009721852624	2^4 3^2 283 2861 9310657867067
111	1187883046587972446352	2^4 3^2 2791 14731 85229 2354137
112	1298825643972827988112	2^4 1811181959 44819683823
113	1419008017196891769552	2^4 3^2 127 77592301902717179
114	1549107970459674583824	2^4 3^2 83 129610773967509587
115	1689846422425646163664	2^4 145009 728336871515581
116	1841989735912612074192	2^4 3^2 433 63026869 468717409
117	2006352151555031549712	2^4 3^2 11228251 1240887922123
118	2183798329122045391312	2^4 18917 1469197 4910890493
119	2375246000266805917584	2^4 3^2 16494763890741707761
120	2581668736582207599504	2^4 3^2 91108711 196778715431
121	2804098836938321927632	2^4 1145173 153039040659049
122	3043630338178757770512	2^4 3^2 139 421 361187337324767
123	3301422153356813502672	2^4 3^2 131 223 784806172993001
124	3578701341797674024144	2^4 1721 34969871 3716469499
125	3876766515380048976144	2^4 3^2 8941 3011071433859661
126	4196991385539562494672	2^4 3^2 107 173 1621 971320802623
127	4540828455606904250512	2^4 13403279 21174055876583
128	4909812863206250815632	2^4 3^2 53 2033533 316355473697
129	5305566377553780087504	2^4 3^2 53 223 1531 2036166729469
130	5729801556612244109584	2^4 358112597288265256849
131	6184326069175551663312	2^4 3^2 432569 99282909347917
132	6671047187077155989712	2^4 3^2 193 76845173 3123615857
133	7191976452837759442192	2^4 692099 649471431547163
134	7749234528191450291664	2^4 3^2 83^2 229 34111800705001
135	8345056229054891815824	2^4 3^2 53 661 1291 2579 496834633
136	8981795752631604721552	2^4 53 71 149179440483517219
137	9661932102472735388112	2^4 3^2 94997599 706299437227
138	10388074717446998894352	2^4 3^2 131 193 8689 58211 5641169
139	11162969310705741820624	2^4 697685581919108863789
140	11989503924864299910864	2^4 3^2 127 35873599 18275112197
141	12870715209758044357392	2^4 3^2 101 151 10099 580314597857
142	13809794929270732245712	2^4 3623 301380187 790467857
143	14810096703874016084112	2^4 3^2 73^2 223 50047 1729285777
144	15875142995660238858384	2^4 3^2 279197857 394859938273
145	17008632342795959210704	2^4 1063039521424747450669
146	18214446850471030658832	2^4 3^2 126489214239382157353
147	19496659945567513762512	2^4 3^2 71 1906950307665054163
148	20859544402424245323472	2^4 73 197 98046511 924620687
149	22307580647226538588944	2^4 3^2 11527 13439208336482063
150	23845465348706257531344	2^4 3^2 151792519 1090920095779

a	Diskriminante von $f(t)$	Faktorisierung der Diskriminante
151	2547812030299541113872	2^4 239 557 11961738534567379
152	27210701620636464538512	2^4 3^2 131 443 1103 2952070423727
153	29048609223914778324432	2^4 3^2 201726452943852627253
154	30997496662842977196304	2^4 7499689 15024091 17193931
155	33063281258293633688784	2^4 3^2 139 1651842588843606799
156	35252154580945440610512	2^4 3^2 541 452507632226142953
157	37570593274879056573712	2^4 379 1949 3178901134171967
158	40025370234832054198992	2^4 3^2 345953 803444282790181
159	42623566146297895864464	2^4 3^2 1367 216530349032237543
160	45372581397831621499024	2^4 151 23291 806321839736429
161	48280148375104971436752	2^4 3^2 101 918962533 3612325901
162	51354344146435999268112	2^4 3^2 2113 168777751966779721
163	54603603549702869459152	2^4 25679 336527 394914700909
164	58036732690738496777424	2^4 3^2 83 4855817661541038887
165	61662922863491983778064	2^4 3^2 12401 575429 60008553989
166	65491764902434463280592	2^4 13005547421 314729951297
167	69533263977880969421712	2^4 3^2 83 233 24968710312595507
168	73797854845096358016912	2^4 3^2 18869 5601107 4849070431
169	78296417558252089119184	2^4 649261 7537070757970609
170	83040293660501886341904	2^4 3^2 21227 27166754886498683
171	88041302861647913230032	2^4 3^2 611397936539221619653
172	93311760215075171234512	2^4 283 38707 532402947672397
173	98864493805840341184272	2^4 3^2 100151351 6855214412063
174	104712862962012275073744	2^4 3^2 110932109 6555114348889
175	110870777001574812006544	2^4 80751107 85812118496387
176	117352714527418555773072	2^4 3^2 6110077147 133377924179
177	124173743283166726306512	2^4 3^2 977 193669159 4557348611
178	131349540582801197673232	2^4 1777 8761 86573 6090949517
179	138896414327278375825104	2^4 3^2 16087 59958875665339843
180	146831324621550664587984	2^4 3^2 631 8447 16223 11792155651
181	155171906005637932797712	2^4 53 182985738214195675469
182	163936490313624643637712	2^4 3^2 53 191 413417 272029230503
183	173144130174692153595792	2^4 3^2 127 9467636164407926159
184	182814623170532147557264	2^4 11425913948158259222329
185	192968536663726262902224	2^4 3^2 39236453 34153425703057
186	203627233311918683591952	2^4 3^2 4637 304955361033113309
187	214812897282852869628112	2^4 13309 1008776473076737873
188	226548561185590642463952	2^4 3^2 53 29684035794757683761
189	238858133733481587454224	2^4 3^2 53 4027 7771771859832191
190	251766428154703174765264	2^4 947 16616052544528984607
191	265299191366447154843792	2^4 3^2 19543 94271887407272551
192	279483133929085668077712	2^4 3^2 263 166393 44350887200047
193	294345960796911135189712	2^4 18396622549806945949357
194	309916402882307379699984	2^4 3^2 107 3037 6622980875243479
195	326224249450475590993104	2^4 3^2 6337 357495057083701093
196	343300381362107680641232	2^4 5039 4258042039121200643
197	361176805181671330186512	2^4 3^2 83 127 248621 930637 1028389
198	379886688169245590085072	2^4 3^2 484142123 5449023904031
199	399464394174123281478544	2^4 191 643 203288940388091693
200	419945520448676689401744	2^4 3^2 431 643 2473 4255181620589

a	Diskriminante von $f(t)$	Faktorisierung der Diskriminante
1000	40200410439578036245876358081 44	2^4 110854463 22665083429916820447 43
1001	40604025759403057862805279666 72	2^4 3^2 617 1667 27414847770183306573967
1002	41011284521401280343037699305 12	2^4 3^2 127 109451 20488842557178936645 49
1003	41422215931339127006074884236 32	2^4 241 10742275915803715509874191 97
1004	41836849399626934533536182955 04	2^4 3^2 2173447 29372701 455096547646703
1005	42255214542546810974513047815 84	2^4 3^2 617 6735173 7061287586432294221
1006	42677341183486626885948376153 12	2^4 28602967 93253746157449826109 71
1007	43103259354180164091548820297 12	2^4 3^2 144967 20513529121 10065563330839
1008	43532999295953446615968417301 92	2^4 3^2 7753 95507 906013 45062645152991
1009	43966591460977278424378467396 64	2^4 467 21701 22037 30713 40061893893727
1010	44404066513526012671061191278 24	2^4 3^2 229 9749 33721 409604061675987881
1011	44845455331242577234333465535 52	2^4 3^2 701 168673 2633858009298013525 21
1012	45290789006409781388922017881 12	2^4 28306743129006113368076261175 7
1013	45740098847227928540873004623 52	2^4 3^2 317639575327971725978284754 33
1014	46193416379098760024187037086 24	2^4 3^2 353 90874678114374331177579157
1015	46650773345915755032625616628 64	2^4 223 1599347 8175066645598655045 09
1016	47112201711360811834536724693 92	2^4 3^2 303762089039 107705365233381887
1017	47577733660207335493096140057 12	2^4 3^2 1699 66411727 98467703 2973783167
1018	48047401599629757389057065321 12	2^4 30029625999768598368160665825 7
1019	48521238160519511917943983863 84	2^4 3^2 73 193 2897 110467913 7473164962309
1020	48999276198807495808617482027 04	2^4 3^2 1718881 1979617852431946189306 1
1021	49481548796793035585275204508 32	2^4 223 283 20219 57667 4202860473420461
1022	49968089264479388770240308825 12	2^4 3^2 33149 13767031 76036046679903967
1023	50458931140915804500322892514 72	2^4 3^2 77093 213943 1314063119 1616762773
1024	50954108195546169305122029569 44	2^4 73 43625092633173090158494888 33
1025	51453654429564263871366415633 44	2^4 3^2 193 4909 30170663927 1250024499599
1026	51957604077275656693270329858 72	2^4 3^2 131 9371 17077 389819 4415245017551
1027	52465991607466260584908820185 12	2^4 83 2186689 29594921 61048585411591
1028	52978851724777578106791853324 32	2^4 3^2 7537 4881367819200976857391669
1029	53496219371088662035141786043 04	2^4 3^2 53 127 2908573 176582741 10746147227
1030	54018129726904817078852055607 84	2^4 53 797 151757665541 52666533313529
1031	54544618212753069125727599625 12	2^4 3^2 24889 15218854551082659543296 57
1032	55075720490584428376379344137 12	2^4 3^2 163 23464434428503931653195017 1
1033	55611472465182972801066288869 92	2^4 197 1102967 1599615731941345618063
1034	56151910285581778431849415124 64	2^4 3^2 305759 1784914259 71450526794701
1035	56697070346485723079641990110 24	2^4 3^2 223 31189 50527 2777491 40338118699
1036	57246989289701190143110986687 52	2^4 53 317 21295975421738732122757197
1037	57801704005572699253904424681 12	2^4 3^2 53 75735985332249343886143114 1
1038	58361251634426490580349614271 52	2^4 3^2 443 3020500523 30288618406884797
1039	58925669568021089689587688654 24	2^4 82007 44909024205266844362057 27
1040	59494995451004879946080597300 64	2^4 3^2 131 147555521 2137426472970157931
1041	60069267182380709502548037925 92	2^4 3^2 10513724519 3967649028778330547
1042	60648522916977560017663779817 12	2^4 9749 7981580797 4871371610350769
1043	61232801066929304313263618649 12	2^4 3^2 239 18189961 9781196088988535987
1044	61822140303160580262390948471 84	2^4 3^2 1314377 80120671 407677755841283
1045	62416579556879808278230785339 04	2^4 2369197 76109287 2163421569767971
1046	63016158021079379852859174220 32	2^4 3^2 86245452051053 507403228892201
1047	63620915152043044673762401545 12	2^4 3^2 83 151 41275667 167420971 510127133
1048	64230890670860523925259465122 72	2^4 12511 32087208591869416875779047
1049	64846124564949377461291966417 44	2^4 3^2 28351 15883753993820857157030 51
1050	65466657089584152615528132385 44	2^4 3^2 101 107 229 19717 13347311 69804339641

SATZ V.9. *Für die Primzahlen* $2, 3$ *und die Polynomdiskriminante* d_f *gelten die folgenden Aussagen:*

(i) *Für alle* $a \in \mathbb{Z}$ *teilt* 2^4 *die Polynomdiskriminante* d_f *und* 2^5 *teilt die Polynomdiskriminante nicht.*
(ii) *Falls* $a \equiv 0, 2 \mod 3$ *teilt* 3^2 *die Polynomdiskriminante* d_f *und* 3^3 *teilt die Polynomdiskriminante nicht.*
Falls $a \equiv 1 \mod 3$ *teilt* 3 *nicht die Polynomdiskriminante* d_f*.*

Beweis:

(i) Es gilt

$$d_f \equiv a^2 \left(4\,a^6 - 4\,a^5 + 13\,a^4 - 10\,a^3 + 13\,a^2 - 4\,a + 4\right)(a+1)^2 \mod 16.$$

Per Nachrechnen erhalten wir $d_f \equiv 0 \mod 16$ für alle möglichen Werte von a modulo 16. Ferner erhalten wir

$$d_f \equiv 4\,a^{10}+20\,a^9+9\,a^8+12\,a^7+22\,a^6+28\,a^5+9\,a^4+4\,a^3+20\,a^2+16 \mod 32.$$

Per Nachrechnen erhalten wir $d_f \not\equiv 0 \mod 32$ für alle möglichen Werte von a modulo 32.

(ii) Es gilt

$$d_f \equiv a\,(a+1)\left(4\,a^8 - 2\,a^7 + 7\,a^6 + a^5 + 2\,a^4 + 3\,a^2 - a + 6\right) \mod 9.$$

Im Fall $a \equiv 2, 3 \mod 3$ ist $d_f \equiv 0 \mod 9$. Im Fall $a \equiv 1 \mod 3$ erhalten wir per Austesten $d_f \not\equiv 0 \mod 9$. Ferner erhalten wir

$$\begin{aligned} d_f \;\equiv\;& 4\,a^{10} + 20\,a^9 + 14\,a^8 + 17\,a^7 + 12\,a^6 + 20\,a^5 \\ & +3\,a^4 + 20\,a^3 + 14\,a^2 + 24\,a + 9 \mod 27. \end{aligned}$$

Per Nachrechnen erhalten wir $d_f \not\equiv 0 \mod 27$ für alle möglichen Werte von a modulo 27.

□

Es sei ρ eine Nullstelle von $f(t)$. Wir studieren die p-maximalen Oberordnungen der Gleichungsordnung $\mathbb{Z}[\rho]$ für $p = 2$ und $p = 3$. Das folgende Kriterium ist bereits ausreichend, um die p-Maximalität der Gleichungsordnung zu erkennen.

SATZ V.10. *(Dedekind)*
Es sei $f(t) \equiv \prod_{i=1}^{n} f_i(t)^i \mod p\mathbb{Z}[t]$ *eine Kongruenzfaktorisierung von* $f(t)$ *in normierte Polynome* $f_i(t) \in \mathbb{Z}[t]$*, die zudem koprim und separabel modulo* $p\mathbb{Z}[t]$

sind. Es sei $h(t) := \frac{1}{p}\left(f(t) - \prod_{i=1}^{n} f_i(t)^i\right) \in \mathbb{Z}[t]$. *Dann ist die Gleichungsordnung* $\mathbb{Z}[\rho]$ *genau dann* p*-maximal, wenn* $\operatorname{ggT}\left(h(t), \prod_{i=2}^{n} f_i(t)\right) = 1$ *in* $\mathbb{F}_p[t]$ *gilt.*

Beweis: Siehe [34].

□

Satz V.11. *Die Gleichungsordnung* $\mathbb{Z}[\rho]$ *ist* 2*-maximal.*

Beweis: Es gilt

$$f(t) \equiv \left(t^2 + t + 1\right)^2 \mod 2\mathbb{Z}[t]$$

und

$$\begin{aligned} h(t) &:= \frac{1}{2}\left(-2t^3 - (a^2 + a + 4)t^2 + (a^2 + a - 2)t\right) \\ &= -t\left(t^2 + \left(\frac{a(a+1)}{2} + 2\right)t + \frac{a(a+1)}{2} - 1\right). \end{aligned}$$

Wir nehmen an, daß die Gleichungsordnung nicht 2-maximal sei. Dann muß nach dem Kriterium von Dedekind

$$g := \operatorname{ggT}\left(t^2 + \left(\frac{a(a+1)}{2} + 2\right)t + \frac{a(a+1)}{2} - 1, t^2 + t + 1\right) \neq 1$$

in $\mathbb{F}_2[t]$ gelten. Da $t^2 + t + 1$ irreduzibel in $\mathbb{F}_2[t]$ ist bedeutet dies $g = t^2 + t + 1$, was

$$\frac{a(a+1)}{2} \equiv 1 \mod 2 \qquad \text{und} \qquad \frac{a(a+1)}{2} \equiv 0 \mod 2$$

impliziert. Für $a \in \mathbb{Z}$ können beide Kongruenzen simultan nicht erfüllt sein. Die Gleichungsordnung ist somit 2-maximal.

□

Satz V.12. *Die Gleichungsordnung* $\mathbb{Z}[\rho]$ *ist* 3*-maximal.*

Beweis: Nach Satz V.9 müssen wir nur die Fälle $a \equiv 0, 2 \mod 3$ betrachten.

- Der Fall $a \equiv 0 \mod 3$.
  Es gilt
  $$f(t) \equiv \left(t^2 + 1\right)^2 \mod 3\mathbb{Z}[t]$$
  und
  $$h(t) := \frac{1}{3}\left(-(a^2 + a + 3)t^2 - (a^2 + a)t\right)$$

$$= \quad -\frac{1}{3}t\left((a^2+a+3)t+(a^2+a)\right).$$

Damit ist

$$\mathrm{ggT}\left(-\frac{1}{3}t\left((a^2+a+3)t+(a^2+a)\right), t^2+1\right) = 1$$

in $\mathbb{F}_3[t]$ stets erfüllt, da t^2+1 irreduzibel in $\mathbb{F}_3[t]$ ist und die linke Seite als Linearfaktor t enthält.

- Der Fall $a \equiv 2 \mod 3$.
  Es gilt hier ebenfalls
  $$f(t) \equiv \left(t^2+1\right)^2 \mod 3\mathbb{Z}[t],$$
  womit wir wie im ersten Fall vorgehen können.

Die Gleichungsordnung ist damit 3-maximal.

□

Nach den Aussagen in den beiden letzten Sätzen ist die Gleichungsordnung stets p-maximal für $p = 2$ und $p = 3$. In den Tabellen auf den vorherigen Seiten hatte die Polynomdiskriminante leider auch weitere quadratische Teiler. Für $a = 134$ und $a = 143$ ist dies der Fall und die Gleichungsordnung ist jeweils nicht maximal. In allen weiteren Fällen war die Berechnung der Körperdiskriminante bzw. einer Ganzheitsbasis von $\mathcal{F}$ bereits nach der Faktorisierung der Polynomdiskriminante abgeschlossen.

3. Zur Galoisgruppe des Polynoms

Die Bestimmung der Galoisgruppe eines Polynoms erfolgt häufig über die Betrachtung von Resolventenpolynomen. Wir werden in diesem Abschnitt ebenfalls diesen Zugang wählen.

Definition V.13. *Es seien $\rho_1, \ldots, \rho_4$ die Nullstellen von $f(t)$. Dann setzen wir*

$$\begin{aligned} u &:= (\rho_1+\rho_2)(\rho_3+\rho_4), \\ v &:= (\rho_1+\rho_3)(\rho_2+\rho_4), \\ w &:= (\rho_1+\rho_4)(\rho_2+\rho_3) \end{aligned}$$

und definieren

$$g(t) := (t-u)(t-v)(t-w)$$

als kubische Resolvente von $f(t)$.

Satz V.14. *Die kubische Resolvente von $f(t)$ besitzt, als Polynom in $\mathbb{Z}[t]$, die Gestalt:*

$$g(t) = t^3 + 2(a^2+a+1)t^2 + \Big((a^2+a+1)^2 - 4\Big)\, t + (a^2+a)^2.$$

Beweis: Siehe [35].

□

Zwischen den Diskriminanten von $f(t)$ und $g(t)$ besteht folgender Zusammenhang, der zur Bestimmung der Galoisgruppe von $f(t)$ hilfreich sein kann.

Satz V.15. *Für die Diskriminante von $g(t)$ gilt:*

$$\begin{aligned} d_g &= 4\,a^{10} + 20\,a^9 + 41\,a^8 + 44\,a^7 - 42\,a^6 - 196\,a^5 - 375\,a^4 - 412\,a^3 - 364\,a^2 - 192\,a + 144 \\ &= d_f. \end{aligned}$$

Beweis: Dies rechnen wir leicht nach.

□

Zur Bestimmung der Galoisgruppe von $f(t)$ werden nun Eigenschaften der Resolvente $g(t)$ herangezogen. Ein erstes Resultat beschreibt die Faktorisierung der Resolvente über den ganzen Zahlen.

Satz V.16. *Die kubische Resolvente $g(t)$ ist irreduzibel über $\mathbb{Z}[t]$ für alle $a \in \mathbb{Z}^{\geq 3}$.*

Beweis: Für die Irreduzibilität von $g(t)$ in $\mathbb{Z}[t]$ genügt es zu zeigen, daß keine Nullstelle von $g(t)$ in $\mathbb{Z}$ liegt. Dazu werten wir das Polynom $g(t)$ an den Stellen

$$-1, \quad -2, \quad -a^2+1, \quad -a^2, \quad -a^2-2a-1, \quad -a^2-2a-2$$

aus. Für die entsprechenden Funktionswerte gilt damit:

$$\begin{array}{rcllr} g(-1) &=& 4 & > & 0, \\ g(-2) &=& -a^4-2a^3+3a^2+4a+6 & < & 0, \\ g(-a^2+1) &=& -2a(a+1)(a-2) & < & 0, \\ g(-a^2) &=& 4a^2 & > & 0, \\ g(-a^2-2a-1) &=& 4(a+1)^2 & > & 0, \\ g(-a^2-2a-2) &=& -2a^3-2a^2+2a+6 & < & 0. \end{array}$$

Die Resolvente $g(t)$ besitzt somit im Intervall $]-a^2-2a-2, -1[$ drei Vorzeichenwechsel und hat damit drei reelle Nullstellen. Für die drei reellen Nullstellen $\delta_1, \delta_2, \delta_3$ gilt ferner:

$$\delta_1 \in]-1, -2[, \quad \delta_2 \in]-a^2, -a^2+1[, \quad \delta_3 \in]-a^2-2a-1, -a^2-2a-2[.$$

Damit liegt keine der Nullstellen $\delta_i \in \mathbb{Z}(1 \leq i \leq 3)$ und $g(t)$ ist irreduzibel in $\mathbb{Z}[t]$.

□

Wir benötigen noch einen Zusammenhang zwischen der Galoisgruppe von $f(t)$ und der Galoisgruppe der zugehörigen Resolvente. Der folgende Satz gibt einen Zusammenhang zwischen der Galoisgruppe von $f(t)$ und der Ordnung der Galoisgruppe der Resolvente.

SATZ V.17. *Es sei $h(t) \in \mathbb{Z}[t]$ ein irreduzibles Polynom vierten Grades mit Galoisgruppe G und m die Ordnung der Galoisgruppe der Resolvente von $h(t)$. Dann gilt:*

(i) *Im Fall $m = 6$ ist $G \cong S_4$.*
(ii) *Im Fall $m = 3$ ist $G \cong A_4$.*

Beweis: Siehe Rotman [35].

□

Durch die Irreduzibilität der Resolvente von $f(t)$ kommen nunmehr nur noch zwei Galoisgruppen für $f(t)$ in Betracht.

SATZ V.18. *Die Galoisgruppe von $f(t)$ ist isomorph zur A_4 oder S_4.*

Beweis: Nach Satz V.16 ist die Resolvente von $f(t)$ irreduzibel. Damit ist die Ordnung der Galoisgruppe der Resolvente 3 oder 6. Nach Satz V.17 folgt dann, daß die Galoisgruppe von $f(t)$ isomorph zur A_4 oder S_4 ist.

□

Wir beachten das folgende Kriterium, um zwischen A_4 und S_4 zu unterscheiden.

SATZ V.19. *Es sei H die Galoisgruppe der Resolvente $g(t)$.*

(i) *Gilt $d_g > 0$ und $\sqrt{d_g} \in \mathbb{Q}$, so folgt $H \cong \mathbb{Z}_3$.*
(ii) *Gilt $d_g > 0$ und $\sqrt{d_g} \notin \mathbb{Q}$, so folgt $H \cong S_3$.*

Beweis: Siehe Rotman [35].

□

Das Problem hat sich reduziert auf die Entscheidung, ob die Diskriminante d_g ein Quadrat in $\mathbb{Z}$ ist oder nicht.

Im folgenden beweisen wir zunächst für hinreichend großes $a \in \mathbb{Z}$, daß die Diskriminante d_g stets kein Quadrat in $\mathbb{Z}$ ist. Die restlichen Fällen für a berechnen wir dann explizit, so daß sich folgendes Resultat ergibt.

Satz V.20. *Für $a \in \mathbb{Z}^{\geq 3}$ ist die Diskriminante von $f(t)$ bzw. die Diskriminante der Resolvente kein Quadrat in $\mathbb{Z}$.*

Beweis: Wir verfolgen den Ansatz, die Diskriminante als Quadrat eines Polynoms fünften Grades in $\mathbb{Z}[a]$ plus ein Restpolynom fünften Grades zu schreiben.

Seien folglich $u, p \in \mathbb{Z}[a]$ mit

$$d_f = u^2 + p$$

und

$$u = 2a^5 + ka^4 + la^3 + ma^2 + na + j$$

mit Unbekannten $k, l, m, n, j \in \mathbb{Z}$. Quadrieren wir u so ergibt sich

$$\begin{aligned} u^2 &= 4\,a^{10} + 4\,ka^9 + \left(4\,l + k^2\right) a^8 + (4\,m + 2\,kl)\,a^7 + \left(2\,km + 4\,n + l^2\right) a^6 \\ &+ (4\,j + 2\,lm + 2\,kn)\,a^5 + \left(2\,kj + m^2 + 2\,ln\right) a^4 + (2\,lj + 2\,mn)\,a^3 \\ &+ \left(n^2 + 2\,mj\right) a^2 + 2\,nja + j^2 \end{aligned}$$

Vergleichen wir die Koeffizienten sukzessive mit

$$\begin{aligned} d_f &= 4\,a^{10} + 20\,a^9 + 41\,a^8 + 44\,a^7 - 42\,a^6 \\ &- 196\,a^5 - 375\,a^4 - 412\,a^3 - 364\,a^2 - 192\,a + 144, \end{aligned}$$

so erhalten wir

$$u = 2a^5 + 5a^4 + 4a^3 + a^2 - 17a - 8.$$

Das Polynom p bestimmen wir aus dem Ansatz $d_f = u^2 + p$, indem wir u einsetzen, und wir erhalten:

$$p = -2a^5 - 160a^4 - 314a^3 - 637a^2 - 464a + 80.$$

Damit erhalten wir

$$d_f - u^2 = -2a^5 - 160a^4 - 314a^3 - 637a^2 - 464a + 80,$$

und dies ist für $a > 100$ sicherlich kleiner Null. Ferner erhalten wir

$$d_f - (u-1)^2 = 2a^5 - 150a^4 - 306a^3 - 635a^2 - 498a + 63,$$

und dies ist für $a > 100$ sicherlich größer Null. Damit liegt die Diskriminante zwischen zwei sukzessiven Quadraten

$$(u-1)^2 < d_f < u^2$$

und kann somit selbst kein Quadrat sein. Die restlichen Fälle für $3 \leq a \leq 100$ können wir der Tabelle auf Seite 60 entnehmen.

$\square$

Letztlich erhalten wir das einheitliche Resultat.

SATZ V.21. *Die Galoisgruppe ist für das Polynom*

$$f(t) = t^4 - (a^2 + a + 1)t^2 + (a^2 + a)t + 1 \quad (a \in \mathbb{Z}^{\geq 3})$$

stets isomorph zur symmetrischen Gruppe auf 4 *Elementen.*

Beweis: Konsequenz der Sätze V.19 und V.20.

$\square$

4. Zur Einheitengruppe der Gleichungsordnung

In diesem Abschnitt streben wir das Ziel an, die Einheitengruppe der Gleichungsordnung in parametrisierter Form anzugeben.

SATZ V.22. *Sei η eine Wurzel von $f(t)$. Dann ist η eine Einheit von $\mathcal{F}$.*

Beweis: Die Norm von η ist gleich dem konstanten Term von $f(t)$. Daher folgt $N(\eta) = 1$ und damit die Behauptung.

$\square$

Im folgenden betrachten wir $\mathcal{F} = \mathbb{Q}(\eta)$. Nach dem Dirichletschen Einheitensatz ist der Rang der Einheitegruppe von $\mathcal{F}$ gleich drei, d.h., wir benötigen noch zwei weitere unabhängige Einheiten für ein maximal unabhängiges Einheitensystem.

SATZ V.23. *Die Elemente $\eta - 1$ und $\eta - a$, welche beide in $\mathbb{Z}[\eta]$ liegen, sind ebenfalls Einheiten von $\mathcal{F}$. Ferner besitzt jedes dieser Elemente die Norm $+1$.*

Beweis: Zunächst zeigen wir, daß die jeweiligen Inversen der Elemente $\eta, \eta - 1, \eta - a$ wieder ganze Elemente in der Gleichungsordnung $Z[\eta]$ sind. Es gilt

$$\begin{aligned}
\eta^{-1} &= -(a^2 + a) + (a^2 + a + 1)\eta - \eta^3, \\
(\eta - 1)^{-1} &= (a^2 + a)\eta - \eta^2 - \eta^3, \\
(\eta - a)^{-1} &= (a + 1)\eta - a\eta^2 - \eta^3.
\end{aligned}$$

Die Inversen lassen sich durch $\eta\eta^{-1} = (\eta-1)(\eta-1)^{-1} = (\eta-a)(\eta-a)^{-1} = 1$ leicht nachrechnen. Um die Norm der Elemente zu berechnen, geben wir jeweils ihre Minimalpolynome in $\mathbb{Z}[t]$ an. Für diese gilt:

$$\begin{aligned}
m_\eta(t) &= t^4 - \left(a^2+a+1\right)t^2 + \left(a^2+a\right)t+1,\\
m_{\eta-1}(t) &= t^4 + 4\,t^3 + \left(-a^2+5-a\right)t^2 + \left(-a^2+2-a\right)t+1,\\
m_{\eta-a}(t) &= t^4 + 4\,at^3 + \left(5\,a^2-a-1\right)t^2 + \left(2\,a^3-a^2-a\right)t+1,
\end{aligned}$$

was sich durch $m_\eta(\eta) = m_{\eta-1}(\eta-1) = m_{\eta-a}(\eta-a) = 0$ nachrechnen läßt. Damit besitzen alle drei Einheiten eine positive Norm.

□

Somit kennen wir bereits drei verschiedene Einheiten in der Gleichungsordnung $\mathbb{Z}[\eta]$. Es bleibt zu zeigen, daß die drei Einheiten $\eta, \eta-1, \eta-a$ multiplikativ unabhängig sind.

Satz V.24. *Die Elemente $\eta, \eta-1, \eta-a$ bilden ein maximal unabhängiges Einheitensystem von $\mathbb{Z}[\eta]$.*

Beweis: Es seien die Konjugierten von η wie folgt angeordnet:

$$\eta^{(1)} < -1 < \eta^{(2)} < 0 < 1 < \eta^{(3)} < 2 < a-1 < \eta^{(4)} < a$$

Diese Anordnung kann gemäß Bemerkung V.6 so gewählt werden.

1. Schritt: Die beiden Einheiten η und $\eta-1$ sind unabhängig.
Angenommen es existieren $k, l \in \mathbb{Z}^{\neq 0}$ mit $(\eta-1)^k = \pm\eta^l$. O.B.d.A. nehmen wir $k>0$ an. Dann gilt im Falle von „+“:

- Wegen $1 < \eta^{(4)} - 1 < \eta^{(4)}$ folgt $l > 0$.
- Wegen $0 < \eta^{(3)} - 1 < 1 < \eta^{(3)}$ folgt $l < 0$.

Der Widerspruch im Fall des negativen Vorzeichen folgt analog. Damit sind η und $\eta-1$ unabhängig.

2. Schritt: Die drei Einheiten $\eta, \eta-1$ und $\eta-a$ sind unabhängig.
Angenommen es existieren $k, l, m \in \mathbb{Z}^{\neq 0}$ mit

$$(\eta-a)^k = \pm\eta^l(\eta-1)^m.$$

Die Fälle $l=0$ oder $m=0$ behandelt man analog dem ersten Schritt des Beweises.

O.B.d.A. sei $k > 0$. Dann gilt für die Konjugiertenbeträge von $(\eta - a)^k$:

$$|(\eta - a)^{(1)}|^k > 1, \quad |(\eta - a)^{(2)}|^k > 1, \quad |(\eta - a)^{(3)}|^k > 1, \quad |(\eta - a)^{(4)}|^k < 1.$$

- Falls $l > 0$ und $m > 0$, so erhalten wir für die vierte Konjugierte
$$\underbrace{\left|(\eta - a)^{(4)}\right|^k}_{<1} = \underbrace{\left|(\eta)^{(4)}\right|^l}_{>1} \underbrace{\left|(\eta - 1)^{(4)}\right|^m}_{>1}$$
und damit einen Widerspruch.
- Falls $l < 0$ und $m < 0$, so erhalten wir für die erste Konjugierte
$$\underbrace{\left|(\eta - a)^{(1)}\right|^k}_{>1} = \underbrace{\left|(\eta)^{(1)}\right|^l}_{<1} \underbrace{\left|(\eta - 1)^{(1)}\right|^m}_{<1}$$
und damit einen Widerspruch.
- Falls $l > 0$ und $m < 0$, so erhalten wir für die zweite Konjugierte
$$\underbrace{\left|(\eta - a)^{(2)}\right|^k}_{>1} = \underbrace{\left|(\eta)^{(2)}\right|^l}_{<1} \underbrace{\left|(\eta - 1)^{(2)}\right|^m}_{<1}$$
und damit einen Widerspruch.
- Falls $l < 0$ und $m > 0$, so erhalten wir für die dritte Konjugierte
$$\underbrace{\left|(\eta - a)^{(3)}\right|^k}_{>1} = \underbrace{\left|(\eta)^{(3)}\right|^l}_{<1} \underbrace{\left|(\eta - 1)^{(3)}\right|^m}_{<1}$$
und damit einen Widerspruch.

Damit kann keine Potenz von $\eta - a$ in $< \eta, \eta - 1 >$ liegen, und somit bilden diese drei Einheiten ein maximal unabhängiges System von Einheiten in $\mathcal{F}$.

□

Um eine untere Regulatorabschätzung anwenden zu können, notieren wir zunächst folgende Aussage.

Satz V.25. *Der Zahlkörper $\mathcal{F}$ ist primitiv.*

Beweis: Nach Satz V.18 ist Galoisgruppe von $f(t)$ isomorph zu A_4 oder S_4. Damit kann $\mathcal{F}$ nur $\mathbb{Q}$ als echten Teilkörper enthalten und ist somit primitiv.

□

SATZ V.26. *Es sei D die Diskriminante der Gleichungsordnung. Dann gilt für den Regulator R der Einheitengruppe*

$$R \geq \frac{\sqrt{64000}}{64000} \left(\log \left(\frac{D}{16} \right) \right)^3 .$$

Beweis: Nach [34] gilt für primitive Körper und $|D| > n^n$ die Schranke

$$R \geq \left[\left(\frac{3 \left(\log \left(\frac{|D|}{n^n} \right) \right)^2}{(n-1)n(n+1) - 6r_2} \right)^r \frac{2^{r_2}}{n \gamma_r^r} \right]^{\frac{1}{2}} ,$$

wobei γ_r^r die r-te Hermitsche Konstante bezeichnet.

Ersetzen wir $n = 4, r = 3, \gamma_3^3 = 2$, so ergibt sich

$$R \geq \left[\frac{1}{8} \left(\frac{\log \left(\frac{D}{256} \right)^2}{20} \right)^3 \right]^{\frac{1}{2}} .$$

Ebenfalls können wir nach [34] für total reelle Zahlkörper mit $n \leq 11$ die Schranke verbessern zu

$$R \geq \left[\frac{1}{8} \left(\frac{\log \left(\frac{D}{16} \right)^2}{20} \right)^3 \right]^{\frac{1}{2}} .$$

und erhalten damit

$$R \geq \frac{\sqrt{64000}}{64000} \left(\log \left(\frac{D}{16} \right) \right)^3 .$$

□

Um nun eine obere Regulatorabschätzung herzuleiten, betrachten wir folgende Aussage.

SATZ V.27. *Nach unseren bisherigen Betrachtungen können wie die Konjugierten von η wie folgt anordnen:*

$$\eta^{(1)} < -1 < \eta^{(2)} < 0 < 1 < \eta^{(3)} < 2 < \eta^{(4)} < a.$$

Dann gelten für die Vorzeichen und Konjugiertenbeträge folgende Aussagen:

$$\begin{aligned} \eta^{(1)} &< 0, \\ \eta^{(2)} &< 0, \\ \eta^{(3)} &> 0, \end{aligned}$$

$$\eta^{(4)} > 0,$$

$$\begin{aligned}\eta^{(1)}-1 &< 0,\\ \eta^{(2)}-1 &< 0,\\ \eta^{(3)}-1 &> 0,\\ \eta^{(4)}-1 &> 0,\end{aligned}$$

$$\begin{aligned}\eta^{(1)}-a &< 0,\\ \eta^{(2)}-a &< 0,\\ \eta^{(3)}-a &< 0,\\ \eta^{(4)}-a &< 0,\end{aligned}$$

$$\begin{array}{rcccl} a+1-\frac{1}{a^3} & < & \left|\eta^{(1)}\right| & < & a+1-\frac{1}{a^4},\\ \frac{1}{a^{2.1}} & < & \left|\eta^{(2)}\right| & < & \frac{1}{a^2},\\ 1+\frac{1}{a^{2.1}} & < & \left|\eta^{(3)}\right| & < & 1+\frac{1}{a^2},\\ a-\frac{1}{a^3} & < & \left|\eta^{(4)}\right| & < & a-\frac{1}{a^4},\end{array}$$

$$\begin{array}{rcccl} a+2-\frac{1}{a^3} & < & \left|\eta^{(1)}-1\right| & < & a+2-\frac{1}{a^4},\\ 1+\frac{1}{a^{2.1}} & < & \left|\eta^{(2)}-1\right| & < & 1+\frac{1}{a^2},\\ \frac{1}{a^{2.1}} & < & \left|\eta^{(3)}-1\right| & < & \frac{1}{a^2},\\ a-\frac{1}{a^3}-1 & < & \left|\eta^{(4)}-1\right| & < & a-1-\frac{1}{a^4},\end{array}$$

$$\begin{array}{rcccl} 2a+1-\frac{1}{a^3} & < & \left|\eta^{(1)}-a\right| & < & 2a+1-\frac{1}{a^4},\\ a+\frac{1}{a^{2.1}} & < & \left|\eta^{(2)}-a\right| & < & a+\frac{1}{a^2},\\ a-1-\frac{1}{a^2} & < & \left|\eta^{(3)}-a\right| & < & a-1-\frac{1}{a^{2.1}},\\ \frac{1}{a^4} & < & \left|\eta^{(4)}-a\right| & < & \frac{1}{a^3}.\end{array}$$

Beweis: Man verwende die Abschätzungen für die Nullstellen aus Satz V.5.

□

SATZ V.28. *Sei $a > 100$. Dann gilt für den Regulator R_η des Einheitensystem $\eta, \eta-1, \eta-a$:*

$$R_\eta \leq 8.63\,(\ln(a))^3 + 3.37\,(\ln(a))^2 + 0.0621\ln(a) + 0.01.$$

Beweis: Es gilt

$$R_\eta = \left| \begin{array}{ccc} \log\left|\eta^{(1)}\right| & \log\left|\eta^{(1)}-1\right| & \log\left|\eta^{(1)}-a\right| \\ \log\left|\eta^{(2)}\right| & \log\left|\eta^{(2)}-1\right| & \log\left|\eta^{(2)}-a\right| \\ \log\left|\eta^{(3)}\right| & \log\left|\eta^{(3)}-1\right| & \log\left|\eta^{(3)}-a\right| \end{array} \right|.$$

Wir berechnen die Determinante und erhalten:

$$\begin{aligned} R_\eta &= \log(\left|\eta^{(1)}\right|)\log(\left|\eta^{(2)}-1\right|)\log(\left|\eta^{(3)}-a\right|) \\ &- \log(\left|\eta^{(1)}\right|)\log(\left|\eta^{(2)}-a\right|)\log(\left|\eta^{(3)}-1\right|) \\ &- \log(\left|\eta^{(2)}\right|)\log(\left|\eta^{(1)}-1\right|)\log(\left|\eta^{(3)}-a\right|) \\ &+ \log(\left|\eta^{(2)}\right|)\log(\left|\eta^{(1)}-a\right|)\log(\left|\eta^{(3)}-1\right|) \\ &+ \log(\left|\eta^{(3)}\right|)\log(\left|\eta^{(1)}-1\right|)\log(\left|\eta^{(2)}-a\right|) \\ &- \log(\left|\eta^{(3)}\right|)\log(\left|\eta^{(1)}-a\right|)\log(\left|\eta^{(2)}-1\right|) \end{aligned}$$

Die Abschätzungen aus Satz V.5 werden ersetzt und wir erhalten eine obere Abschätzung der Form:

$$\begin{aligned} R_\eta &\leq \log(\left|a+1-a^{-4}\right|)\log(\left|1+a^{-2}\right|)\log(\left|a-1-a^{-3}\right|) \\ &- \log(\left|a+1-a^{-4}\right|)\log(\left|a+a^{-2}\right|)\log((|a|)^{-2.1}) \\ &- \log((|a|)^{-2.1})\log(\left|a+2-a^{-4}\right|)\log(\left|a-1-a^{-3}\right|) \\ &+ \left(\log((|a|)^{-2.1})\right)^2\log(\left|2\,a+1-a^{-4}\right|) \\ &+ \log(\left|1+a^{-2}\right|)\log(\left|a+2-a^{-4}\right|)\log(\left|a+a^{-2}\right|) \\ &- \left(\log(\left|1+a^{-3}\right|)\right)^2\log(\left|2\,a+1-a^{-3}\right|). \end{aligned}$$

Die sechs Summanden werden für $a > 100$ wie folgt abgeschätzt:

- Die drei Faktoren des ersten Summanden:

$$\begin{aligned} \log(a+1-a^{-4}) &= \log(a)+\log(1+a^{-1}-a^{-5}) \\ &\leq \log(a)+\log(1+a^{-1}) \\ &\leq \log(a)+a^{-1} \\ &\leq \log(a)+0.01, \\ \log((1+a^{-2}) &\leq \log(1+10^{-2}) \\ &\leq 0.01, \end{aligned}$$

$$\begin{aligned}\log(a-1-a^{-3}) &\leq \log(a)\log(1-a^{-1}-a^{-4}) \\ &\leq \ln(a)\end{aligned}$$

Der erste Summand läßt sich damit abschätzen durch:

$$10^{-2}\left(\log(a)^2+\log(a)\right).$$

- Die drei Faktoren des zweiten Summanden:

$$\begin{aligned}\log(a+1-a^{-4}) &\leq \log(a)+0.01, \\ \log(a+a^{-2}) &\leq \log(a)+\log(1+a^{-3}) \\ &\leq \log(a)+10^{-3}, \\ \log(a^{-2.1}) &= -2.1\log(a)\end{aligned}$$

Der zweite Summand läßt sich damit abschätzen durch:

$$2.1\log(a)^3+0.25\log(a)^2+10^{-4}\log(a).$$

- Die drei Faktoren des dritten Summanden:

$$\begin{aligned}\log(a^{-2.1}) &= -2.1\log(a), \\ \log(a+2-a^{-4}) &\leq \log 9a)+log(1+2a^{-1}-a^{-5}) \\ &\leq \log(a)+\log(1+2a^{-2}) \\ &\leq \log(a)+2\cdot 10^{-2}, \\ \log(a-1-a^{-3}) &\leq \ln(a).\end{aligned}$$

Der dritte Summand läßt sich damit abschätzen durch:

$$2.1\log(a)^3+4.2\cdot 10^{-2}\log(a).$$

- Die drei Faktoren des vierten Summanden:

$$\begin{aligned}\log(a^{-2.1})^2 &= 4.41\log(a), \\ \log(2a+1-a^{-4}) &\leq \log(a)+\log(2+a^{-1}-a^{-5}) \\ &\leq \log(a)+\log(2+a^{-1}) \\ &\leq \log(a)+0.7.\end{aligned}$$

Der vierte Summand läßt sich damit abschätzen durch:

$$4.41\log(a)^3+3.1\log(a)^2.$$

- Die drei Faktoren des fünften Summanden:

$$\begin{aligned}\log(1+a^{-2}) &\leq 10^{-2}, \\ \log(a+2-a^{-4}) &\leq \log(a)+2\cdot 10^{-2}, \\ \log(a+a^{-2}) &\leq \log(a)+10^{-3}.\end{aligned}$$

Der fünfte Summand läßt sich damit abschätzen durch:

$$10^{-2}(\log(a)^2 + \log(a) + 1).$$

- Der sechste Summand besitzt drei positve Faktoren und wird subtrahiert, daher vernachlässigen wir diesen.

Schließlich erhalten wir für $a > 100$:

$$\begin{aligned}
R_\eta &\leq 10^{-2}\left(\log(a)^2 + \log(a)\right) \\
&+ 2.1\log(a)^3 + 0.25\log(a)^2 + 10^{-4}\log(a) \\
&+ 2.1\log(a)^3 + 4.2\cdot 10^{-2}\log(a) \\
&+ 4.41\log(a)^3 + 3.1\log(a)^2 \\
&+ 10^{-2}(\log(a)^2 + \log(a) + 1) \\
&- 0 \\
&= 8.63\,(\ln(a))^3 + 3.37\,(\ln(a))^2 + 0.0621\ln(a) + 0.01.
\end{aligned}$$

□

Satz V.29. *Für $a > 100$ ist der Index des Einheitensystems $\eta, \eta - 1, \eta - a$ in der Einheitengruppe der Gleichungsordnung durch 3 beschränkt.*

Beweis: Wir ersetzen in der unteren Regulatorschranke aus Satz V.26 die Diskriminate und erhalten

$$\begin{aligned}
R &\geq \frac{\sqrt{64000}}{64000} \\
&\cdot \log\left(\frac{4\,a^{10} + 20\,a^9 + 41\,a^8 + 44\,a^7 - 42\,a^6 - 196\,a^5 - 375\,a^4 - 412\,a^3 - 364\,a^2 - 192\,a + 144}{16}\right)^3.
\end{aligned}$$

Für $a > 100$ können wir einfacher abschätzen durch

$$R \geq \frac{\sqrt{64000}}{64000}\log\left(\frac{1}{4}a^{10}\right)^3 =: R_u.$$

Setzen wir gemäß Satz V.28

$$R_o := 8.63\,(\ln(a))^3 + 3.37\,(\ln(a))^2 + 0.0621\ln(a) + 0.01$$

und bilden den Quotienten aus R_o und R_u, so erhalten wir

$$\frac{R_o}{R_u} = \frac{2183.236496\log(a)^3 + 852.5500571\log(a)^2 + 15.71019541\log(a) + 2.529822128}{1000\log(a)^3 - 415.8883083\log(a)^2 + 57.65436166\log(a) - 2.664197215}$$

Für $a = 100$ gilt $\frac{R_o}{R_u} = 2.596644070$. Wir beweisen noch, daß der Quotient monoton fallend für $a > 3$ ist. Dafür betrachten wir die Ableitung von $\frac{R_o}{R_u}$, wobei wir $x := \log(a)$ setzen:

$$\frac{1.23 \cdot 10^{21} x^2 + 8.81 \cdot 10^{21} x^3 - 7.42 \cdot 10^{22} x^4 - 9.75 \cdot 10^{19} x - 7508413552 \cdot 10^9}{(200000000000.0x^3 - 83177661660.0x^2 + 11530872330.0x - 532839443.0)^2}$$

Berechnet man die Nullstellen des Zählerpolynoms, so ergeben sich vier reelle Nullstellen:

$$-.09143525461, \quad -.06067636187, \quad .1386281358, \quad .1386307364.$$

Da der Leitterm des Zählerpolynoms $-7.42 \cdot 10^{22} x^4$ ist, ist die Ableitung somit für $x > 0.139$ monoton fallend. Zurücktransformiert bedeutet dies, daß die Funktion für $a > 3$ monoton fallend ist.

Der Quotient ist somit monoton fallend und für $a > 100$ stets kleiner drei, weil wir bereits

$$\frac{R_o}{R_u}(100) = 2.596644070$$

gesehen haben. Der Index ist damit für $a > 100$ durch drei abgeschätzt.

$\square$

Für $a > 10^{30}$ impliziert die obere Abschätzung sofort $\frac{R_o}{R_u} < 2$. Die explizite Berechnung aller Fälle für $100 \leq a \leq 10^{30}$ mittels Software ist nicht in angemessener Zeit möglich. Um die Fälle $100 \leq a \leq 10^{30}$ betrachten zu können, benötigen wir den folgenden Satz.

Satz V.30. *Für mögliche Quadratwurzeln in $\eta, \eta - 1, \eta - a$ seien $m_1, m_2, m_3 \in \{0, 1\}$ (nicht alle Null). Dann besitzt die Gleichung*

$$\alpha^2 = \pm\eta^{m_1}(\eta - 1)^{m_2}(\eta - a)^{m_3}$$

keine Lösung $\alpha \in \mathbb{Z}[\eta]$.

Beweis: In den Fällen

$$\begin{aligned} \alpha^2 &= \pm\eta, \\ \alpha^2 &= \pm(\eta - 1), \\ \alpha^2 &= \pm\eta(\eta - a), \\ \alpha^2 &= \pm(\eta - 1)(\eta - a) \end{aligned}$$

besitzt jeweils die rechte Seite nach Satz V.27 mindestens eine negative Konjugierte und kann somit kein Quadrat sein. Für die restlichen Fälle

$$\begin{aligned}\alpha^2 &= \pm\eta - a,\\ \alpha^2 &= \pm\eta(\eta-1) = \pm(\eta^2-\eta),\\ \alpha^2 &= \pm\eta(\eta-1)(\eta-a) = \pm(\eta^3-(a+1)\eta^2+a\eta)\end{aligned}$$

treffen wir folgende Vorbereitung. Wir setzen

$$\alpha = m\eta^3 + p\eta^2 + q\eta + l$$

mit $m, p, q, l \in \mathbb{Z}$. Dann gilt

$$\alpha^2 = m^2\eta^6 + 2\,mp\eta^5 + \left(p^2 + 2\,mq\right)\eta^4 + (2\,pq + 2\,ml)\,\eta^3 + \left(2\,pl + q^2\right)\eta^2 + 2\,ql\eta + l^2$$

und durch Reduktion der η Potenzen erhalten wir

$$\begin{aligned}\alpha^2 \;=\; & \left(2\,lm - m^2\left(a^2+a\right) + 2\,mp\left(a^2+a\right) + 2\,qp + 2\,pm\right)\eta^3\\ & + \Big(p^2\left(a^2+a\right) + 2\,mq + m^2\left(a^2+a\right)^2 + 2\,m^2\left(a^2+a\right) + q^2 + p^2 - 2\,mp\left(a^2+a\right)\\ & + 2\,lp + 2\,mq\left(a^2+a\right)\Big)\eta^2\\ & + \Big(-m^2\left(a^2+a\right)^2 + 2\,lq - 2\,pm - p^2\left(a^2+a\right) - 2\,mq\left(a^2+a\right) - m^2\left(a^2+a\right)\Big)\eta\\ & - m^2 + l^2 - 2\,mq - m^2\left(a^2+a\right) - p^2\end{aligned}$$

Da $a(a+1) = a^2 + a \in \mathbb{Z}$ stets gerade ist, sind die Koeffizienten von α^2 vor den Potenzen von η^3 und η auch gerade. Damit können die Elemente

$$\begin{aligned}\alpha^2 &= \pm\eta - a,\\ \alpha^2 &= \pm\eta(\eta-1) = \pm(\eta^2-\eta),\\ \alpha^2 &= \pm\eta(\eta-1)(\eta-a) = \pm(\eta^3-(a+1)\eta^2+a\eta)\end{aligned}$$

keine Quadrate sein, da sie vor η oder η^3 ungerade Koeffizienten haben. Damit folgt die Behauptung.

□

Wir erhalten schließlich die folgende Aussage.

Satz V.31. *Für $a \geq 3$ bilden die Einheiten $\eta, \eta-1, \eta-a \in \mathbb{Z}[\eta]$ ein Grundeinheitensystem von $\mathbb{Z}[\eta]$, wobei jede der Einheiten eine positive Norm hat.*

Beweis: Die Fälle $a > 100$ wurden oben behandelt. Für $3 \leq a \leq 100$ wurde dies explizit mit KASH nachgerechnet.

Nach Satz V.23 besitzen alle drei Elemente eine positive Norm. Die Polynome $f(t)$ erzeugen somit eine besondere Klasse von Körpern. Die Gleichungsordnung besitzt in diesen Fällen ein ausgezeichnetes Grundeinheitensystem, indem jede der drei Grundeinheiten eine positive Norm hat.

□

5. Zum Zerfällungskörper des Polynoms

In diesem Abschnitt charakterisieren wir den Zerfällungskörper $\mathcal{L}$ unseres parametrisierten Polynoms

$$f(t) = t^4 - (a^2 + a + 1)t^2 + (a^2 + a)t + 1.$$

Nach den Betrachtungen über die Galoisgruppe hat der Zerfällungskörper den Grad 24. Ziel ist es, den Zerfällungskörper durch eine parametrisierte Gleichung anzugeben.

Es seien $\rho_1, \dots, \rho_4$ die vier verschiedenen Nullstellen von $f(t)$ in $\mathbb{R}$. Dann wählen wir das Element

$$\alpha := \rho_1 - \rho_2 + 2\rho_3 \in \mathcal{L}$$

als Kandidaten für ein primitives Element, um den Zerfällungskörper über $\mathbb{Q}$ zu erzeugen.

Per Konjugation von α bilden wir die 24 Elemente

$$\begin{array}{lll}
\alpha_1 := \rho_1 - \rho_2 + 2\rho_3, & \alpha_2 := \rho_2 - \rho_1 + 2\rho_3, & \alpha_3 := \rho_1 - \rho_3 + 2\rho_2, \\
\alpha_4 := \rho_3 - \rho_1 + 2\rho_2, & \alpha_5 := \rho_3 - \rho_2 + 2\rho_1, & \alpha_6 := \rho_2 - \rho_3 + 2\rho_1, \\
\alpha_7 := \rho_1 - \rho_2 + 2\rho_4, & \alpha_8 := \rho_2 - \rho_1 + 2\rho_4, & \alpha_9 := \rho_4 - \rho_2 + 2\rho_1, \\
\alpha_{10} := \rho_2 - \rho_4 + 2\rho_1, & \alpha_{11} := \rho_1 - \rho_4 + 2\rho_2, & \alpha_{12} := \rho_4 - \rho_1 + 2\rho_2, \\
\alpha_{13} := \rho_1 - \rho_4 + 2\rho_3, & \alpha_{14} := \rho_4 - \rho_1 + 2\rho_3, & \alpha_{15} := \rho_1 - \rho_3 + 2\rho_4, \\
\alpha_{16} := \rho_3 - \rho_1 + 2\rho_4, & \alpha_{17} := \rho_3 - \rho_4 + 2\rho_1, & \alpha_{18} := \rho_4 - \rho_3 + 2\rho_1, \\
\alpha_{19} := \rho_4 - \rho_2 + 2\rho_3, & \alpha_{20} := \rho_2 - \rho_4 + 2\rho_3, & \alpha_{21} := \rho_3 - \rho_2 + 2\rho_4, \\
\alpha_{22} := \rho_2 - \rho_3 + 2\rho_4, & \alpha_{23} := \rho_4 - \rho_3 + 2\rho_2, & \alpha_{24} := \rho_3 - \rho_4 + 2\rho_2.
\end{array}$$

Damit erhalten wir ein Polynom $h_\alpha(t) \in \mathbb{Z}[t]$ mit α als Nullstelle.

$$\begin{array}{rcl}
h_\alpha(t) & = & \prod_{i=1}^{24} (x - \alpha_i) \\
& = & x^{24} \\
& + & (-40\,a^2 - 40\,a - 40)x^{22} \\
& + & (684\,a^4 + 1368\,a^3 + 2052\,a^2 + 1368\,a + 604)x^{20} \\
& + & (-6600\,a^6 - 19800\,a^5 - 39260\,a^4 - 45520\,a^3 - 36540\,a^2 - 17080\,a - 3880)x^{18} \\
& + & (39990\,a^8 + 159960\,a^7 + 390628\,a^6 + 612024\,a^5 + 683826\,a^4 + 534232\,a^3 + 273940\,a^2 + 82168\,a + 8614)x^{16} \\
& + & (-160200\,a^{10} - 801000\,a^9 - 2300060\,a^8 - 4394240\,a^7 - 6083720\,a^6
\end{array}$$

$$
\begin{aligned}
& -6235520\,a^{5}-4551800\,a^{4}-2235680\,a^{3}-625740\,a^{2}-55080\,a-17800)x^{14}\\
+\quad & (435180\,a^{12}+2611080\,a^{11}+8509468\,a^{10}+18612440\,a^{9}+29696710\,a^{8}+35834080\,a^{7}\\
& +31638672\,a^{6}+18947104\,a^{5}+6058918\,a^{4}-518184\,a^{3}-484996\,a^{2}+367432\,a-371588)x^{12}\\
+\quad & (-809400\,a^{14}-5665800\,a^{13}-20307860\,a^{12}-48191760\,a^{11}-82972620\,a^{10}-108140200\,a^{9}-102683780\,a^{8}\\
& -60514880\,a^{7}-5518500\,a^{6}+28104280\,a^{5}+19688820\,a^{4}-4078800\,a^{3}-7576340\,a^{2}-1692520\,a+6425960)x^{10}\\
+\quad & (1027665\,a^{16}+8221320\,a^{15}+31439308\,a^{14}+76202056\,a^{13}+128935822\,a^{12}+157058264\,a^{11}+124716644\,a^{10}\\
& +20324168\,a^{9}-103298269\,a^{8}-157422328\,a^{7}-72187196\,a^{6}+90855064\,a^{5}\\
& +170477998\,a^{4}+124821096\,a^{3}-15755268\,a^{2}-54702936\,a+1083169)x^{8}\\
+\quad & (-874000\,a^{18}-7866000\,a^{17}-31182860\,a^{16}-71166880\,a^{15}-96032000\,a^{14}-50839600\,a^{13}+89797760\,a^{12}\\
& +279456320\,a^{11}+363124080\,a^{10}+148898200\,a^{9}-426125680\,a^{8}-1122767360\,a^{7}-1458369760\,a^{6}-1204877840\,a^{5}\\
& -348179440\,a^{4}+386921280\,a^{3}+385453700\,a^{2}+119853680\,a-91007760)x^{6}\\
+\quad & (475744\,a^{20}+4757440\,a^{19}+19036208\,a^{18}+35738832\,a^{17}+10148862\,a^{16}\\
& -114228048\,a^{15}-313884632\,a^{14}-436227152\,a^{13}-233730528\,a^{12}+526045464\,a^{11}+1759761076\,a^{10}+2858366488\,a^{9}\\
& +3241779504\,a^{8}+2945131536\,a^{7}+1759380280\,a^{6}-101334064\,a^{5}-1053875730\,a^{4}\\
& -688284528\,a^{3}+157752944\,a^{2}+316877760\,a+13807584)x^{4}\\
+\quad & (-149760\,a^{22}-1647360\,a^{21}-6489920\,a^{20}-7241600\,a^{19}+26176080\,a^{18}+113322000\,a^{17}+171274980\,a^{16}\\
& -5657760\,a^{15}-561305320\,a^{14}-1335883720\,a^{13}-1622854940\,a^{12}-245815600\,a^{11}+2990296580\,a^{10}\\
& +5988431480\,a^{9}+6079799400\,a^{8}+3212678400\,a^{7}-871977580\,a^{6}-4039372400\,a^{5}\\
& -3235818800\,a^{4}-254844800\,a^{3}+73717440\,a^{2}-381300480\,a+270846720)x^{2}\\
-\quad & 4540528\,a^{18}+258474969\,a^{16}+20736\,a^{24}+248832\,a^{23}-238553172\,a^{14}+942336\,a^{22}\\
& -126720\,a^{21}-1595658346\,a^{12}-10517024\,a^{20}-27288128\,a^{19}-294414100\,a^{10}+2259741512\,a^{9}+113498544\,a^{17}\\
& +5159832281\,a^{8}+6871004528\,a^{7}+200122632\,a^{15}+6636152272\,a^{6}+4969016768\,a^{5}-965895672\,a^{13}\\
& +2451793504\,a^{4}+368316672\,a^{3}-1562007416\,a^{11}-662738688\,a^{2}-525837312\,a+171714816
\end{aligned}
$$

Für die Diskriminante von $h_\alpha(t)$ gilt

$$
\begin{aligned}
d_{h_\alpha} \quad = \quad & (20064\,a-4520\,a^{9}+26116\,a^{5}+40648\,a^{2}+48184\,a^{3}+864\,a^{11}\\
& +43269\,a^{4}+680\,a^{10}+144\,a^{12}-7388\,a^{7}-11003\,a^{8}+9582\,a^{6}-13104)^{2}\\
\cdot\quad & a^{16}(a+1)^{16}\\
\cdot\quad & (3037500\,a^{10}+15187500\,a^{9}+15528375\,a^{8}-29011500\,a^{7}-83136150\,a^{6}-84080700\,a^{5}\\
& -51194025\,a^{4}-26475300\,a^{3}+4790700\,a^{2}+13406400\,a-13868176)^{4}\\
\cdot\quad & (-519475923412992\,a-279606481760\,a^{19}+6506955076584\,a^{17}-263694588696\,a^{15}-101815755767760\,a^{13}\\
& +463793947913288\,a^{9}+1424610979974560\,a^{5}+396208069560576-714982270117248\,a^{2}-225900142495104\,a^{3}\\
& -136357472894864\,a^{11}+513886530846640\,a^{4}+55641963468548\,a^{10}+10180442037825\,a^{16}+1552785650936\,a^{18}\\
& -267306216176\,a^{20}-38013742490652\,a^{14}-47399616000\,a^{21}+5229504000\,a^{22}+2488320000\,a^{23}+207360000\,a^{24}\\
& -157379603381530\,a^{12}+1636371232308104\,a^{7}+1053014480850401\,a^{8}+1823506890822616\,a^{6})^{4}\\
\cdot\quad & (419904\,a-383220\,a^{9}+1978276\,a^{5}-244944+1041228\,a^{2}+1438524\,a^{3}+31104\,a^{11}+1580959\,a^{4}\\
& -19620\,a^{10}+5184\,a^{12}+545332\,a^{7}-524033\,a^{8}+1946202\,a^{6})^{4}\\
\cdot\quad & (-132496+69372\,a^{2}+52416\,a-12609\,a^{4}+26604\,a^{3}-48294\,a^{6}-51516\,a^{5}+2079\,a^{8}-20844\,a^{7}+972\,a^{10}+4860\,a^{9})^{8}\\
\cdot\quad & (144-364\,a^{2}-192\,a-375\,a^{4}-412\,a^{3}-42\,a^{6}-196\,a^{5}+41\,a^{8}+44\,a^{7}+4\,a^{10}+20\,a^{9})^{12}
\end{aligned}
$$

Damit gilt der Zusammanhang

$$
\frac{d_{h_\alpha}}{(d_f)^{12}} \in \mathbb{Z},
$$

denn die 12-te Potenz der Polynomdiskriminate d_f ist der letzte Faktor.

6. Weitere Parametrisierungen

In diesem Abschnitt diskutieren wir die Motivation des Polynoms

$$f(t) = t^4 - (a^2 + a + 1)t^2 + (a^2 + a)t + 1$$

und geben Ideen für entsprechende Verallgemeinerungen an.

Für die Familie vierten Grades betrachten wir den Ansatz in Form der Gleichung

$$t(t-1)(t-a)(t-b) + 1 = 0,$$

mit $a, b \in \mathbb{Z}$ und t als Unbestimmte. Durch Ausmultiplizieren erhalten wir das Polynom

$$f_{a,b}(t) = t^4 - (b + a + 1)t^3 + (a + ab + b)t^2 - abt + 1.$$

Mittels des Parameters b eliminieren wir den Koeffizienten vor t^3. Wir setzen $b := -a - 1$ und erhalten unser Polynom

$$f(t) = t^4 - (a^2 + a + 1)t^2 + (a^2 + a)t + 1.$$

Durch den Ansatz besitzt $f(t)$ vier verschiedene reelle Nullstellen für $a > 3$ in kleinen Umgebungen von $-a - 1, 0, 1, a$.

Wegen $f(0) = 1$, ist eine Wurzel η eine Einheit in $\mathbb{Z}[\eta]$. Substituiert man t durch $t + 1$, so gilt

$$(t+1)t(t+1-a)(t+1+a+1) + 1 = 0.$$

Dann erkennen wir, daß $\eta - 1$ eine Einheit ist. Insgesamt erhalten wir durch dieses Verfahren die Einheiten $\eta, \eta - 1, \eta - a, \eta + a + 1$.

Diese Konstruktion läßt sich auch für Polynome höheren Grades durchführen. Wir betrachten die Familie

$$f_{n,a,b} = t(t-1)(t-2)(t-n+3)\cdots(t-a)(t-b) + 1.$$

Die Transformation $b = -a - \sum_{i=1}^{n-3} i = -a - \frac{(n-3)(n-2)}{2}$ läßt den Koeffizienten vor t^{n-1} verschwinden.

Es sei $n \in \mathbb{Z}^{\geq 4}$ und $a > |-n+3|$. Dann liegen die Nullstellen von $f_{n,a,b}$ in kleinen Umgebungen von $-a - -\frac{(n-3)(n-2)}{2}, 0, 1, 2, 3, -n+3, a$. $f_{n,a,b}$ bestitzt somit n reelle Nullstellen. Als Einheiten liefert das Polynom die Elemente:

$$\eta, \eta - 1, \eta - 2, \ldots, \eta - n + 3, \eta - a.$$

Für $5 \leq n \leq 9$ geben wir einen Überblick.

$$f_{5,a} = x^5 + \left(-7 - a^2 - 3\,a\right)x^3 + \left(6 + 3\,a^2 + 9\,a\right)x^2 + \left(-6\,a - 2\,a^2\right)x + 1,$$

$$\begin{aligned}
f_{6,a} &= x^6 + \left(-25 - a^2 - 6\,a\right) x^4 + \left(60 + 6\,a^2 + 36\,a\right) x^3 \\
&\quad + \left(-36 - 11\,a^2 - 66\,a\right) x^2 + \left(6\,a^2 + 36\,a\right) x + 1, \\
f_{7,a} &= x^7 + \left(-a^2 - 10\,a - 65\right) x^5 + \left(300 + 10\,a^2 + 100\,a\right) x^4 + \left(-476 - 35\,a^2 - 350\,a\right) x^3 \\
&\quad + \left(240 + 50\,a^2 + 500\,a\right) x^2 + \left(-24\,a^2 - 240\,a\right) x + 1, \\
f_{8,a} &= x^8 + \left(-140 - a^2 - 15\,a\right) x^6 + \left(1050 + 15\,a^2 + 225\,a\right) x^5 + \left(-3101 - 85\,a^2 - 1275\,a\right) x^4 \\
&\quad + \left(225\,a^2 + 3375\,a + 3990\right) x^3 + \left(-1800 - 274\,a^2 - 4110\,a\right) x^2 + \left(1800\,a + 120\,a^2\right) x + 1, \\
f_{9,a} &= x^9 + \left(-266 - a^2 - 21\,a\right) x^7 + \left(21\,a^2 + 441\,a + 2940\right) x^6 + \left(-175\,a^2 - 3675\,a - 13811\right) x^5 \\
&\quad + \left(32340 + 735\,a^2 + 15435\,a\right) x^4 + \left(-36324 - 1624\,a^2 - 34104\,a\right) x^3 \\
&\quad + \left(15120 + 1764\,a^2 + 37044\,a\right) x^2 + \left(-720\,a^2 - 15120\,a\right) x + 1.
\end{aligned}$$

Für $5 \leq n \leq 9$ und kleine Werte von a ($|-n+3| < a \leq |-n+3| + 10$) haben wir als Motivation einige Beispiele gerechnet. Die Polynome zeigen ein ähnliches Verhalten wie die diskutierte Familie. Die Galoisgruppe war jeweils S_n und die entsprechenden Einheiten bereits ein Grundeinheitensystem in der Gleichungsordnung.

Literaturverzeichnis

[1] W.E.H. Berwick, *Algebraic number fields with two independent units*, Proc. London Math. Soc. (2) **34** (1932), 360–378.

[2] P.E. Blanskby and H. Montgomery, *Algebraic integers near the unit circle*, Acta. Arith. **18** (1971), 355–369.

[3] H. Brunotte, F. Halter–Koch, *Grundeinheitensysteme algebraischer Zahlkörper mit vorgegebener Verteilung der Konjugiertenbeträge*, Arch. Math. **37** (1981), 512–513.

[4] J. Buchmann, *A generalization of Voronoi's unit algorithm I, II*, J. Number Theory **20** (1985), 177–209.

[5] J. Buchmann, *On the computation of units and class numbers by a generalization of Lagrange's algorithm*, J. Number Theory **26** (1987), 8–30.

[6] J. Buchmann, *On the period length of the generalized Lagrange algorithm*, J. Number Theory **26** (1987), 31–37.

[7] J. Buchmann, *The generalized Voronoi-algorithm in totally real algebraic number fields*, Eurocal 1985, 479–486.

[8] J. Buchmann, M. Jüntgen und M.E. Pohst, *A practical version of the generalized Lagrange algorithm*, Experimental Mathematics, Vol. **3**, 1994.

[9] S. I. Borevič and I. R. Šafarevič, *"Zahlentheorie"*, Birkhäuser, Basel 1966.

[10] T.W.Cusick, *Lower bounds for regulators*, in Number Theory, Noordwijkerhout 1983, Proceedings of the J. Arithmetiques, Lectture Notes in Math., vol. 1068, Springer New York, 1984.

[11] G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell quadratischer Zahlkörper*, Abh. Math. Sem. Hamburg, **22**, 1958, 92–97.

[12] V. Ennola, R. Turunen, *On Cyclic Cubic Fields*, Math. Comp., **45**, 585–589, 1985.

[13] V. Ennola, R. Turunen, *On Totally Real Cubic Fields*, Math. Comp., **44**, 495–518, 1985.

[14] C.Fieker, A.Jurk, M.E. Pohst, *On Solving Relative Norm Equations in Algebraic Number Fields*; to appear in Math. Comp..

[15] U. Fincke und M.E. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471.

[16] M. Holzberg, *"Zur Berechnung der Einheitengruppe der Galoisschen Hüllen von Zahlkörpern vierten Grades"*, Diplomarbeit, Düsseldorf 1991.

[17] M. Jüntgen, *"Berechnung von Einheiten in algebraischen Zahlkörpern mittels des verallgemeinerten Lagrangeschen Kettenbruchalgorithmus"*, Diplomarbeit, Düsseldorf 1990.

[18] KANT group: *KANT V4*; erscheint im J. Symb. Comput..

[19] J. Klüners, *"Über die Berechnung von Teilkörpern algebraischer Zahlkörper"*, Diplomarbeit, Berlin 1994.

[20] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65–85.

[21] H.W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Bayer Akad. Wiss. Math.–Nat., Nr. **2**, 1954.

[22] H.W. Leopoldt, *Über ein Fundamentalproblem der Theorie der Einheiten algebraischer Zahlkörper*, S. B. Bayer. Akad. Wiss. (1965),41 – 48.

[23] E.M.Matveev, *On Fundamental Units of certain Fields*, Russian Acad. Sci. Sb. Math., **76**, No. 2, 1993, 293–304.

[24] H. Minkowski, *Zur Theorie der Kettenbrüche*, Ges. Abh. I.

[25] M.Mignotte, A.Pethő, *Sur les carres dans certaines suites de Lucas (On squares in certain Lucas sequences)*, J. Theor. Nombres Bordx. **5, No. 2**, (1993), 333-341.

[26] Yoshitaka Odia, *On the Group of Units of an Abelian Extension of an Algebraic Number Field*, Proc. Japan Acad., **64** Ser A, 304–306, 1988.

[27] C.J. Parry, *A unit relationship for pure sixtic fields*, Arch. Math. **37** (1981), 210–221.

[28] A. Pethő, *Complete solutions to families of quartic Thue equations*, Math. Comp., **57** No. 196, 1991, 777-798.

[29] M.E. Pohst, *Berechnung unabhängiger Einheiten und Klassenzahlen in total reellen biquadratischen Zahlkörpern*, Computing **14** (1975), 67–78.

[30] M.E. Pohst, *On computing fundamental units*, J. Number Theory **47** (1994), 93–105.

[31] M.E. Pohst, *Computational Algebraic Number Theory*, DMV Seminar Bd. **21**, Birkhäuser Verlag 1993.

[32] M.E. Pohst, *In Memoriam (Hans Zassenhaus)*, J. Number Theory **47**, 1–19, 1994.

[33] M.E. Pohst, P. Weiler and H. Zassenhaus, *On effective computation of fundamental units I, II*, Math. Comp. **38** (1982), 275–328.

[34] M.E. Pohst and H. Zassenhaus, *"Algorithmic Algebraic Number Theory"*, Cambridge Univ. Press 1989.

[35] Joseph Rotman, *"Galois Theory"*, Springer Verlag 1990.

[36] R.Steiner, R. Rudman, *On an Algorithm of Billevich for Finding Units in Algebraic Number Fields*, Math. Comp., **30**, 598–609, 1976.

[37] H.-J. Stender, *Über die Einheitengruppe der reinen algebraischen Zahlkörper sechsten Grades* J. Reine Angew. Math. **290** (1977), 24-62.

[38] H.-J. Stender, *Über die Grundeinheit für spezielle undendliche Klassen reiner kubischer Zahlkörper.* Abh. Math. Sem. Hamburg, **33**, (1969), 203–215.

[39] G. Voronoi, *Eine Verallgemeinerung des Kettenbruchalgorithmus*, Dissertation Warschau, 1896.

[40] L. Washington, *"Introduction to cyclotomic fields"*, Springer, New York 1982.

[41] K. Wildanger, *"Über Grundeinheitenberechnung in algebraischen Zahlkörpern"*, Diplomarbeit, Düsseldorf 1993.

Zusammenfassung

In dieser Arbeit betrachten wir das Thema der Einheitenberechnug in algebraischen Zahlkörpern unter drei verschiedenen Aspekten.

Wir behandeln in unserem ersten Thema die Einheitenberechnung mit Hilfe der Geometrie der Zahlen. Der zentrale Gesichtspunkt ist die geometrische Beschreibung einer endlichen Menge, die die Einheitengruppe des Zahlkörpers erzeugt. Dazu führen wir den neuen Begriff der „Einheiten dicht an 1“ ein. Diese Definition charakterisiert eine endliche Menge von Einheiten und basiert auf geometrischen Minimalbedingungen an die Konjugiertenbeträge der Einheiten. Wir beweisen, daß die Einheiten dicht an 1 die Einheitengruppe des Zahlkörpers erzeugen. Numerische Betrachtungen liefern einen Vergleich zur Reduktionstheorie.

Die Untersuchung von Relativeinheiten eines algebraischen Körperturms $\mathbb{Q} \subset \mathcal{L} \subset \mathcal{M}$ bildet das zweite Thema dieser Arbeit. Wir zeigen, wie die Einheitengruppe von $\mathcal{L}$ mit Hilfe von Relativeinheiten zu einem maximal unabhängigen Einheitensystem in $\mathcal{M}$ erweitert werden kann. Für mögliche Teiler des Index des Einheitensystems in der vollen Einheitengruppe von $\mathcal{M}$ werden Abschätzungen angegeben. Der zweite Abschnitt diese Themas behandelt spezielle Erweiterungen vom Grad sechs über $\mathbb{Q}$. Dabei werden wir die beiden Grundeinheiten zweier Teilkörper durch eine Relativeinheit passend ergänzen. Hier gelingt es, mögliche p-te Wurzeln in der vollen Einheitengruppe genau anzugeben. Ferner übertragen wir in dieser Situation die geometrische Charakterisierung der Grundeinheit eines reell–quadratischen Zahlkörpers auf die Relativeinheit.

Die parametrische Darstellung einer Familie von Polynomen der Form

$$f_a(t) = t^4 - (a^2 + a + 1)t^2 + (a^2 + a)t + 1 \quad (a \in \mathbb{Z}^{\geq 3})$$

bildet die Grundlage für das dritte Thema dieser Arbeit. Eine Wurzel η des Polynoms $f_a(t)$ erzeugt einen total reellen Zahlkörper vierten Grades über $\mathbb{Q}$. Wir beweisen, daß die Galoisgruppe des Polynoms stets isomorph zur symmetrischen Gruppe auf vier Elementen ist. Die Berechnung der Einheitengruppe der Gleichungsordnung des Polynoms kann in diesem Fall sehr einfach behandelt werden. Es wird bewiesen, daß die Elemente $\eta, \eta - 1$ und $\eta - a$ ein Grundeinheitensystem der Gleichungsordnung bilden. Dabei wird das Resultat bis auf wenige Ausnahmen theoretisch bewiesen. Die restlichen Fälle werden mit Hilfe zahlentheoretischer Software nachgerechnet.

Ich danke Herrn Professor Dr. M.E. Pohst für die Betreuung dieser Arbeit und seine Gesprächsbereitschaft. Herrn Professor Dr. J. Buchmann danke ich für die Übernahme des Koreferates.

Mein besonderer Dank gilt meiner Frau und meinem Sohn. Beide gaben stets Kraft und Unterstützung in allen Lebenslagen.

Lebenslauf

Name:	Max Walter Jüntgen
geboren am:	15.04.1964 in Hilden, römisch–katholisch, verheiratet
Ehefrau:	Claudia Jüntgen, geb. Pohl, Kinderkrankenschwester
Kinder:	Philipp Jüntgen (7.9.1994)
Vater:	Max Willi Hermann Jüntgen, Fuhrunternehmer
Mutter:	Roswitha Jüntgen, geb. Theodor, Hausfrau
Schulbesuch:	1970 bis 1974: Augusta-Grundschule Hilden 1974 bis 1980: Fliedner-Realschule Hilden 1980 bis 1983: Dietrich-Bonhoeffer-Gymnasium Hilden
Studium:	seit WS 83/84 an der Universität Düsseldorf Mathematik mit Nebenfach Physik. Studienschwerpunkt Mathematik: Konstruktive Zahlentheorie. Studienschwerpunkt Physik: Theoretische Physik März 1991: Diplom in Mathematik
3/91 – 4/93:	wissenschaftlicher Mitarbeiter (DFG) an der Universität Düsseldorf
4/93 – 9/93:	wissenschaftlicher Mitarbeiter (DFG) an der TU Berlin
seit Oktober 1993	wissenschaftlicher Mitarbeiter an der TU Berlin