Über relative Normgleichungen in algebraischen Zahlkörpern

vorgelegt von
Diplom-Mathematiker

Claus Fieker

aus Haan

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

Berlin 1997
D83

Promotionsausschuß

Vorsitzender:	Professor Dr. J. Becker
Berichter:	Professor Dr. M. E. Pohst
Berichter:	Professor Dr. G. M. Ziegler

Tag der wissenschaftlichen Aussprache: 29. April 1997

Inhaltsverzeichnis

Einleitung

Eine der ältesten Diophantischen Gleichungen ist die Normgleichung; für Zahlkörper $\mathcal{F}/\mathcal{E}/\mathbb{Q}$ sowie eine Zahl $\theta \in \mathcal{E} := \mathbb{Q}(\alpha)$ wird eine Zahl $x \in \mathcal{F} := \mathcal{E}(\beta)$ mit

$$N_{\mathcal{F}/\mathcal{E}}(x) = \theta$$

gesucht oder der Nachweis, daß es keine solche gibt. Anwendungen hiervon gibt es z.B. in der Algebren Theorie ([1, Chapter 7] und [44, Lemmata 6.1, 6.2]).

In speziellen Situationen ist schon lange bekannt, daß obiges Problem in endlich vielen Schritten gelöst werden kann; z.B. führt dies für $\mathcal{F}$ reell quadratisch über $\mathbb{Q}$ auf Pell'sche Gleichungen, die schon Gauss behandelt hat.

Für (relativ-) Galois'sche Erweiterungen $\mathcal{F}/\mathcal{E}$ hat Siegel [48] Schranken für den Nenner und alle Koeffizienten einer Lösung angegeben und damit gezeigt, daß die Gleichung konstruktiv gelöst werden kann. Später hat Bartels [3] diese Ergebnisse auf beliebige Erweiterungen verallgemeinert. Mit anderen Methoden als Siegel hat Garbanati [25] für (absolut) Abel'sche Körper ebenfalls Schranken erhalten. Allen drei Arbeiten ist jedoch gemeinsam, daß die Schranken viel zu groß sind, um damit in der Praxis Lösungen zu finden.

Bei diesen drei Ansätzen wird zunächst der Nenner einer möglichen Lösung beschränkt. In einem zweiten Schritt werden dann (endlich viele) Normgleichungen in den ganzen algebraischen Zahlen gelöst. Der Spezialfall, Normgleichungen in Ordnungen — oder allgemeiner in Moduln — zu lösen, ist jedoch auch aus anderen Gründen von Interesse: Um Thue-Gleichungen zu lösen, sind wir an den Lösungen interessiert, die in der Gleichungsordnung $o_{\mathcal{E}}[\beta]$ über der Maximalordnung $o_{\mathcal{E}}$ von $\mathcal{E}$ liegen [5], genauer gesagt an einer Parametrisierung all dieser Lösungen. Für Hauptidealtests (im Falle $\mathcal{E} = \mathbb{Q}$) muß x ein Element des zu testenden Ideals sein [20, (1.7) Lemma]. Hier ist es ausreichend, „bis auf Vorzeichen“ zu lösen — $N_{\mathcal{F}/\mathcal{E}}(x) = -\theta$ ist auch zulässig; auch reicht es hier, eine Lösung zu finden.

Weitere Spezialfälle ergeben sich aus Einschränkungen an θ, i.allg. wird θ ganz algebraisch sein. Wenn θ eine Torsionseinheit ist, ist das Lösen der Normgleichung äquivalent zum Bestimmen der Relativ-Einheiten.

In dieser Arbeit ist der von Fincke im Rahmen seiner Dissertation entwickelte Algorithmus zum Lösen von Normgleichungen in Ordnungen absoluter Zahlkörper ($\mathcal{E} = \mathbb{Q}$, [20]) verallgemeinert, wobei die Arbeit von Jurk [31] fortgesetzt und erweitert wird. Ferner werden Methoden von Garbanati [24] verallgemeinert, um im Fall von relativ Galois'schen Körpern einen Algorithmus zu erhalten, der Normgleichungen in Körpern löst.

Nachdem im ersten Kapitel zunächst einige Notationen vereinbart werden, untersuchen wir im zweiten Kapitel die Wirkung der Normabbildung auf die Einheitengruppe. Die hier gewonnenen Ergebnisse werden einerseits für die Parametrisierung der Lösungsmenge benötigt und andererseits, um das Problem auf ein endliches zu reduzieren. Ferner wird dort eine für die Komplexität des Verfahrens wichtige Invariante, der relative Regulator, eingeführt.

Im dritten Kapitel wird die nötige Gittertheorie für Gitter über Zahlkörpern eingeführt, die benötigt wird, um das Ellipsoidverfahren entwickeln zu können. Speziell stellen wir eine Verallgemeinerung des LLL-Algorithmus zur Gitterreduktion und des Fincke-Pohst-Algorithmus zum Auszählen von Ellipsoiden vor.

Im vierten Kapitel werden dann die in den letzten beiden Kapiteln gewonnenen Ergebnisse dazu benutzt, das Ellipsoid-Verfahren zur Lösung von Normgleichungen auf Relativerweiterungen zu verallgemeinern. Für relativ Galois'sche Erweiterungen entwickeln wir dann ein Verfahren, um die Lösbarkeit im Körper zu entscheiden und ggf. eine Lösung zu finden. Zusätzlich geben wir dort ein Verfahren an, welches nicht auf dem Auszählalgorithmus beruht, um Normgleichungen mittels S-Einheiten zu lösen.

Zum Schluß geben wir einige Beispiele an, die sowohl die Mächtigkeit der vorgestellten Verfahren als auch deren Grenzen demonstrieren.

An dieser Stelle möchte ich mich bei Herrn Professor Dr. M. E. Pohst herzlich für die Betreuung während der Arbeit danken. Ferner bedanke ich mich bei Herrn Professor Dr. G. M. Ziegler für die Übernahme des Koreferats sowie bei Martin, Klaus und Jürgen für die Durchsicht einer vorläufigen Fassung dieser Arbeit. Schließlich möchte ich mich an dieser Stelle auch bei allen Mitgliedern der Kant-Gruppe bedanken, ohne deren Kooperation eine Arbeit wie diese nicht entstehen kann.

KAPITEL I

Grundlagen

Hier werden wir zunächst die (wichtigsten) in dieser Arbeit verwendeten Bezeichnungen festlegen und einige theoretische Vorbemerkungen machen.

1. Bezeichnungen

Wir wollen Normgleichungen in Relativerweiterungen algebraischer Zahlkörper untersuchen, dazu betrachten wir die folgende Situation (alle angegebenen Eigenschaften können z.B. in [10, 35, 42, 46] nachgelesen werden).

$$\begin{array}{c} \mathcal{F} = \mathcal{E}(\beta) \\ \Big| \; n \\ \mathcal{E} = \mathbb{Q}(\alpha) \\ \Big| \; m \\ \mathbb{Q} \end{array}$$

Es sei $f \in \mathbb{Z}[t]$ ein normiertes, irreduzibles Polynom vom Grad m und α eine Nullstelle hiervon in einem geeigneten Erweiterungskörper. Dann ist $\mathcal{E} := \mathbb{Q}(\alpha)$ ein algebraischer Zahlkörper vom Grad m über $\mathbb{Q}$. Den Ring der ganzen Zahlen von $\mathcal{E}$ bezeichnen wir mit $o_{\mathcal{E}}$. Ferner sei nun $g \in o_{\mathcal{E}}[t]$ normiert, irreduzibel vom Grad n und β eine Nullstelle von g in einem passenden Erweiterungskörper, dann setzen wir $\mathcal{F} := \mathcal{E}(\beta)$. Bezeichne $o_{\mathcal{F}}$ den Ring der ganzen Zahlen, $o_{\mathcal{E}}$ ist dann ein Dedekindring und freier $\mathbb{Z}$-Modul vom Rang m, $o_{\mathcal{F}}$ ist ebenfalls Dedekind'sch und ein $o_{\mathcal{E}}$-Modul von Rang n. Falls die Klassenzahl von $o_{\mathcal{E}}$ größer als 1 ist, ist $o_{\mathcal{F}}$ jedoch i.allg. nicht mehr frei über $o_{\mathcal{E}}$. Später werden wir Kriterien angeben, um entscheiden zu können, ob $o_{\mathcal{F}}$ frei über $o_{\mathcal{E}}$ ist. Analoges gilt auch für die (gebrochenen) Ideale von $\mathcal{E}$ und $\mathcal{F}$: Ideale $\mathfrak{a}$ von $\mathcal{E}$ sind frei vom Rang m über $\mathbb{Z}$, Ideale $\mathfrak{b}$ von $\mathcal{F}$ sind i.allg. nicht frei über $o_{\mathcal{E}}$. Hier, wie auch in der ganzen Arbeit, sind Ideale stets von $\{0\}$ verschieden.

$N_{\mathcal{F}/\mathcal{E}} : \mathcal{F} \to \mathcal{E} : x \mapsto N_{\mathcal{F}/\mathcal{E}}(x)$ sei die gewöhnliche Normabbildung, ebenfalls mit $N_{\mathcal{F}/\mathcal{E}}$ sei die Idealnorm bezeichnet. Es gilt dann

$$(N_{\mathcal{F}/\mathcal{E}}(x)) := N_{\mathcal{F}/\mathcal{E}}(x)o_{\mathcal{E}} = N_{\mathcal{F}/\mathcal{E}}(xo_{\mathcal{F}}) =: N_{\mathcal{F}/\mathcal{E}}((x)).$$

$N_{\mathcal{F}/\mathbb{Q}}$ und $N_{\mathcal{E}/\mathbb{Q}}$ seien die entsprechenden Normabbildungen nach $\mathbb{Q}$, es gilt $N_{\mathcal{F}/\mathbb{Q}} = N_{\mathcal{E}/\mathbb{Q}} \circ N_{\mathcal{F}/\mathcal{E}}$.

Seien nun $\alpha^{(1)}, \ldots, \alpha^{(r_1)} \in \mathbb{R}$ die reellen Nullstellen von f und $\alpha^{(r_1+1)} = \overline{\alpha^{(r_1+r_2+1)}}$, $\ldots, \alpha^{(r_1+r_2)} = \overline{\alpha^{(r_1+2r_2)}} \in \mathbb{C} \setminus \mathbb{R}$ die komplexen Nullstellen (r_1, $r_2 \in \mathbb{N}_0$ geeignet). Die Fortsetzungen der Abbildungen $(.)^{(i)} : \alpha \mapsto \alpha^{(i)}$ auf $\mathcal{E}$ liefern dann Einbettungen von $\mathcal{E}$ nach $\mathcal{E}^{(i)} := (\mathcal{E})^{(i)} \subset \mathbb{C}$ in die Konjugiertenkörper von $\mathcal{E}$. Nun setzen wir die Abbildungen noch auf den zugehörigen Polynomring $\mathcal{E}[t]$ fort, indem wir sie auf den Koeffizienten operieren lassen. Die Nullstellen der Polynome $g^{(i)} \in \mathcal{E}^{(i)}[t]$ seien $\beta^{(i,j)}$ mit $1 \leq j \leq n$. Da $g^{(i)} \in \mathbb{R}[t]$ für $1 \leq i \leq r_1$ gilt, können wir $\beta^{(i,j)} \in \mathbb{R}$ für $1 \leq j \leq s_i$ und $\beta^{(i,j)} = \overline{\beta^{(i,j+t_i)}} \in \mathbb{C}$ mit $n = s_i + 2t_i$, $s_i < j \leq s_i + t_i$ annehmen (s_i, $t_i \in \mathbb{N}_0$ geeignet). Wegen $f^{(i)} = \overline{f^{(i+r_2)}}$ können wir zusätzlich noch $\beta^{(i,j)} = \overline{\beta^{(i+r_2,j)}}$ für $r_1 < i \leq r_1 + r_2$ und $1 \leq j \leq n$ erreichen. Nach Jurk [31, Bemerkung 3.4] nennen wir $(s_i, t_i)_{1 \leq i \leq r_1}$ die relative Signatur von $\mathcal{F}/\mathcal{E}$.

In [49] ist ein Algorithmus angegeben, um ein Polynom $g_{\mathbb{Z}} \in \mathbb{Z}[t]$ mit $\mathcal{L} := \mathbb{Q}[t]/g_{\mathbb{Z}}\mathbb{Q}[t] \cong \mathcal{F}$ zu bestimmen, so daß wir $\mathcal{F}$ auch als einfache Erweiterung von $\mathbb{Q}$ zur Verfügung haben. Ferner liefert dieser Algorithmus auch Einbettungen von $\mathcal{E}$ nach $\mathcal{L}$, von $\mathcal{F}$ nach $\mathcal{L}$ und von $\mathcal{L}$ nach $\mathcal{F}$, so daß wir beide Darstellungen ($\mathcal{L}$ und $\mathcal{F}$) benutzen können, um bei Bedarf die geeignetere zu wählen.

Dieser Algorithmus, sowie Algorithmen für Operationen mit Ordnungen, Idealen, Zahlkörpern, algebraischen Zahlen und alle in dieser Arbeit vorgestellten und benutzten Algorithmen sind in KANT implementiert und können über KASH [32] aufgerufen werden.

2. Bewertungen und Primideale

Sei $V_{\mathbb{Q}} = V_{\mathbb{Q}}^{\text{fin.}} \dot{\cup} V_{\mathbb{Q}}^{\infty}$ die kanonische Menge exponentieller Bewertungen auf $\mathbb{Q}$, d.h., zu jeder Primzahl $p \in \mathbb{P}_{\mathbb{Q}}$ gibt es genau ein $v = v_p \in V_{\mathbb{Q}}^{\text{fin.}}$ mit $v_p(p) = 1$. Für jedes $V_{\mathbb{Q}}^{\text{fin.}} \ni v \neq v_p$ ist $v(p) = 0$, und es gilt $V_{\mathbb{Q}}^{\infty} = \{-\log|\cdot|\}$.

Für einen beliebigen Zahlkörper k sei $V_k^{\text{fin.}}$ die Menge der diskreten Bewertungen auf k, die eine Bewertung aus $V_{\mathbb{Q}}^{\text{fin.}}$ fortsetzen, d.h., für jedes $V \in V_k^{\text{fin.}}$ gibt es genau ein $v \in V_{\mathbb{Q}}^{\text{fin.}}$ mit $V|_{\mathbb{Q}} = v$. Analog sei V_k^{∞} die Menge der Bewertungen, die $V_{\mathbb{Q}}^{\infty}$ fortsetzen. Für jedes $v \in V_k^{\text{fin.}}$ definieren wir den folgenden p-adischen Betrag:

Sei $p \in \mathbb{P}_{\mathbb{Q}}$ diejenige Primzahl mit $v(p) \neq 0$, dann setzen wir $|\cdot|_v := p^{-v(\cdot)}$. Für $v \in V_k^\infty$ sei $|\cdot|_v := \exp(-v(\cdot))$, ferner sei $|0|_v := 0$ für jedes $v \in V_k$.

Sei nun $\mathcal{K}$ eine endliche Erweiterung von k. Aufgrund unserer Normierung besteht $V_{\mathcal{K}}$ ausschließlich aus Fortsetzungen von Elementen aus V_k. Wir schreiben $V|v$ falls $V \in V_{\mathcal{K}}$ eine Fortsetzung von $v \in V_k$ ist. In diesem Fall sei

$$n_{V|v} := n_{V,k} := [\overline{\mathcal{K}}^V : \overline{k}^v] = \frac{n_{V,\mathbb{Q}}}{n_{v,\mathbb{Q}}},$$

wobei $\overline{\mathcal{K}}^V$ wie Vervollständigung von $\mathcal{K}$ bzgl. der von V induzierten Topologie ist und $\overline{k}^v$ die Vervollständigung von k bzgl. v. Es gilt der für diese Arbeit wichtige Zusammenhang zwischen den Beträgen, ihren Fortsetzungen und der Norm:

$$|N_{\mathcal{K}/k}(x)|_v = (\prod_{\substack{V \in V_{\mathcal{K}} \\ V|v}} |x|_V^{n_{V,\mathbb{Q}}})^{1/n_{v,\mathbb{Q}}} = \prod_{\substack{V \in V_{\mathcal{K}} \\ V|v}} |x|_V^{n_{V,k}}$$

oder (additiv geschrieben)

$$v(N_{\mathcal{K}/k}(x)) = \sum_{\substack{V \in V_{\mathcal{K}} \\ V|v}} n_{V,k} V(x) \tag{1-1}$$

für $x \in \mathcal{K}$ und $v \in V_k$.

Ferner gilt die Produktformel:

$$\prod_{v \in V_k} |x|_v^{n_{v,\mathbb{Q}}} = 1.$$

3. Matrizen

Da wir im nächsten Abschnitt viel mit Matrizen arbeiten werden, wollen wir einige Abkürzungen und Schreibweisen vereinbaren.

Sei R ein Ring. Für eine beliebige Matrix $M \in R^{n' \times m'}$ ist $M_{i,j}$ das j-te Element der i-ten Zeile, es gilt $M = (M_{i,j})_{\substack{1 \leq i \leq n' \\ 1 \leq j \leq m'}}$. $M^{tr} := (M'_{i,j})_{\substack{1 \leq i \leq m' \\ 1 \leq j \leq n'}}$ mit $M'_{i,j} = M_{j,i}$. Für ein Ringelement $r \in R$ sei $R^{n' \times n'} \ni r_{n'} := (r)_{\substack{1 \leq i \leq n' \\ 1 \leq j \leq n'}}$ die Matrix, bei der alle Einträge gleich r sind, für R unitär bezeichne $I_{n'} \in R^{n' \times n'}$ die Einheitsmatrix, d.h. $(I_{n'})_{i,j} = \delta_{i,j} := \begin{cases} 1 & i = j \\ 0 & \text{sonst.} \end{cases}$. Sei nun $N \in R^{n' \times m''}$ eine weitere Matrix. Mit $(M|N)$ bezeichnen wir die Matrix aus $\mathbb{R}^{n' \times (m'+m'')}$, deren Spalten durch Anhängen der

Spalten von N an die von M entstehen, $(M|N)_{i,j} = \begin{cases} M_{i,j} & j \leq m' \\ N_{i,j-m'} & \text{sonst.} \end{cases}$. Analog ist $\begin{pmatrix} M^{tr} \\ \hline N^{tr} \end{pmatrix} = (M|N)^{tr}$. Für Matrizen $M_i \in R^{n_i \times m_i}$ $(1 \leq i \leq o)$ ist

$$\operatorname{diag}(M_1, \ldots, M_o) := \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & M_o \end{pmatrix} \in R^{\sum_{i=1}^{o} n_i \times \sum_{i=1}^{o} m_i}.$$

KAPITEL II

Einheiten in Relativerweiterungen

Obwohl Relativerweiterungen schon länger untersucht werden, gibt es bisher kaum Ansätze, die besondere Struktur dieser Körper bei der Berechnung der Einheiten auszunutzen. Im Gegensatz zu z.B. der Berechnung der Maximalordnung oder der Galoisgruppe gibt es hier kaum Eigenschaften, die sich mit relativen Methoden untersuchen lassen. Die wesentliche Schwierigkeit liegt darin begründet, daß die Eigenschaft einer Zahl $x \in o_{\mathcal{F}}$, eine Einheit zu sein, nicht von der Struktur von $o_{\mathcal{F}}$ als $o_{\mathcal{E}}$-Modul oder $\mathbb{Z}$-Modul abhängt und, daß es im wesentlichen diese Strukturinformation ist, die wir zusätzlich benutzen wollen.

Für die Struktur der Einheitengruppe U_k in beliebigen Zahlkörpern k gilt zunächst einmal der Dirichlet'sche Einheitensatz:

Satz 2.1. *Sei k ein Zahlkörper. Dann gibt es Einheiten $\epsilon_i \in o_k$ $(1 \leq i \leq \#V_k^\infty - 1 =: r)$ und $\zeta \in o_k$ mit*

$$U_k = \langle \zeta \rangle \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle,$$

wobei das Produkt direkt ist und $\langle \epsilon_i \rangle$ unendliche zyklische Gruppen sind. Für die Gruppe der Torsionseinheiten TU_k von k gilt: $TU_k = \langle \zeta \rangle$.

Hieraus erhalten wir eine Darstellung von $U_{\mathcal{F}}$, die völlig unabhängig von der Struktur von $o_{\mathcal{F}}$ als $o_{\mathcal{E}}$-Modul ist. In diesem Kapitel werden wir eine andere Darstellung von $U_{\mathcal{F}}$ finden, die die zusätzliche Strukturinformation berücksichtigt. Speziell die Einheiten, deren Norm Torsionseinheiten sind, werden dort eine entscheidende Rolle spielen. Diese Einheiten sind auch für das Lösen von Normgleichungen wichtig.

Schon sehr früh hat sich Artin [2] mit Einheiten der Norm 1 in relativ-galoisschen Zahlkörpern beschäftigt. Er zeigte, daß ein maximales unabhängiges Einheitensystem im wesentlichen durch die Anwendung der Galois-Automorphismen auf eine kleine Menge von Einheiten aus $\mathcal{E}$ erhalten werden kann. In diesem Spezialfall erhält er so auch den nachfolgenden Satz 2.5.

Es gibt verschiedene Ansätze, die Einheitengruppe U_k — oder wenigstens eine Untergruppe $U \leq U_k$ von endlichem Index $(U_k : U)$ — dadurch zu erhalten, daß die Einheiten geeigneter Teilkörper entsprechend „geliftet“ werden. Für bestimmte Typen von Abel'schen Zahlkörpern hat z.B. Leopoldt [37, 38] ein maximales System unabhängiger Einheiten aus zyklischen Teilkörpern bestimmt. Für den Fall, daß $\mathcal{F}$ die Galois'sche Hülle eines nicht Abel'schen quartischen Körpers ist, hat Holzberg [27] gezeigt, daß eine Untergruppe von endlichem Index immer aus den Einheiten der Teilkörper erhalten werden kann. In diesem Fall gibt es auch Abschätzungen für den Index.

Für CM-Körper ist schon lange bekannt, daß die Einheitengruppe einfach aus der Einheitengruppe des maximalen reellen Teilkörpers konstruiert werden kann, da die Einheitenränge identisch sind. Weiter ist bekannt, daß der Index (im wesentlichen) maximal 2 ist [52, Theorem 4.12]. Im Fall von Kreisteilungskörpern gibt es auch Kriterien, um den Index zu bestimmen.

Hier werden wir genauer untersuchen, wie die Einheitengruppe von $\mathcal{F}$ von der von $\mathcal{E}$ beeinflußt wird. Die hier vorgestellten Ergebnisse sind von zentraler Bedeutung für das Lösen von Normgleichungen in Relativerweiterungen. Ähnliche Konstruktionen sind von Klebel [33] zum Lösen von bestimmten Einheitengleichungen benutzt worden. Es ist zu erwarten, daß mit Hilfe dieser Ergebnisse sich zumindest die Theorie zum Lösen von Thue-Gleichungen auf den relativen Fall übertragen läßt.

Der nachfolgend definierte relative Regulator unterscheidet sich von der in [14] gegebenen Definition dadurch, daß hier keine absoluten Invarianten von $\mathcal{F}/\mathbb{Q}$ in der Definition benutzt werden. In der hier gegebenen Definition 2.8 werden ausschließlich „relative Invarianten“ benutzt. In [4] wird eine Variante von Satz 2.9 als Definition verwendet.

1. Struktur der Einheitengruppe in Relativerweiterungen

Für das Lösen von Normgleichungen ist die Kenntnis der Einheiten aus $\mathcal{F}$, deren Normen bestimmte Eigenschaften haben, wichtig. Im folgenden werden wir daher die Operation der Normabbildung auf der Einheitengruppe untersuchen.

Für das ganze Kapitel fixieren wir eine endliche Menge $V_{\mathcal{E}}^{\infty} \subseteq S_{\mathcal{E}} \subset V_{\mathcal{E}}$ und setzen

$$S_{\mathcal{F}} := \{V \in V_{\mathcal{F}} \mid \exists v \in S_{\mathcal{E}} : V|v\}. \tag{2-1}$$

Für jedes $v \in V_{\mathcal{E}}$ sei

$$P_v := \{V \in V_{\mathcal{F}} \mid V|v\}.$$

Fixiere nun ein beliebiges $V_v \in P_v$ ($\forall v \in V_{\mathcal{E}}$) und setze

$$\dot{P}_v := P_v \setminus \{V_v\}, r_v := \#P_v. \tag{2-2}$$

Ferner seien $r_{\mathcal{E}} := \#S_{\mathcal{E}}$, $r_{\mathcal{F}} := \#S_{\mathcal{F}}$ und $\dot{S_{\mathcal{F}}} := \bigcup_{v \in S_{\mathcal{E}}} \dot{P}_v$.

DEFINITION 2.2. *Seien $S_{\mathcal{E}}$ und $S_{\mathcal{F}}$ wie oben gegeben. Dann nennen wir die Elemente von*

$$U_{\mathcal{E},S_{\mathcal{E}}} := \{x \in \mathcal{E} \mid \forall v \in V_{\mathcal{E}} \setminus S_{\mathcal{E}} : v(x) = 0\}$$

bzw.

$$U_{\mathcal{F},S_{\mathcal{F}}} := \{x \in \mathcal{F} \mid \forall V \in V_{\mathcal{F}} \setminus S_{\mathcal{F}} : V(x) = 0\}$$

die $S_{\mathcal{E}}$-Einheiten von $\mathcal{E}$ bzw. $S_{\mathcal{F}}$-Einheiten von $\mathcal{F}$.

Für eine Untergruppe $A \leq U_{\mathcal{E},S_{\mathcal{E}}}$ definieren wir $U^A_{\mathcal{F},S_{\mathcal{F}}} := {N_{\mathcal{F}/\mathcal{E}}}^{-1}(A) \cap U_{\mathcal{F},S_{\mathcal{F}}}$.

BEMERKUNG 2.3. (1) *Für $S_{\mathcal{E}} = V^{\infty}_{\mathcal{E}}$ (und $S_{\mathcal{F}} = V^{\infty}_{\mathcal{F}}$) gilt $U_{\mathcal{E}} = U_{\mathcal{E},S_{\mathcal{E}}}$ und $U_{\mathcal{F}} = U_{\mathcal{F},S_{\mathcal{F}}}$.*

(2) *Es gilt der Dirichlet'sche Einheitensatz: $U_{\mathcal{E},S_{\mathcal{E}}} = \langle\zeta\rangle \times \langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_{r_{\mathcal{E}}-1}\rangle$* [35, V, §1], *wobei ζ eine geeignete Einheitswurzel ist (es gilt $TU_{\mathcal{E}} = TU_{\mathcal{E},S_{\mathcal{E}}} = \langle\zeta\rangle$) und $\epsilon_1, \ldots, \epsilon_{r_{\mathcal{E}}-1}$ Grundeinheiten sind (d.h., sie haben unendliche Ordnung, das Produkt ist direkt und sie erzeugen die ganze Gruppe).*

(3) *Nach (2-1) und (1-1) gelten $N_{\mathcal{F}/\mathcal{E}}(U_{\mathcal{F},S_{\mathcal{F}}}) \subseteq U_{\mathcal{E},S_{\mathcal{E}}}$ und $U_{\mathcal{E},S_{\mathcal{E}}} \subseteq U_{\mathcal{F},S_{\mathcal{F}}}$.*

(4) *Offenbar gilt $A \subseteq U^A_{\mathcal{F},S_{\mathcal{F}}}$, da $N_{\mathcal{F}/\mathcal{E}}(A) = A^n$ ist.*

Als nächstes wollen wir die Struktur von $U^A_{\mathcal{F},S_{\mathcal{F}}}$ bestimmen. Dazu benötigen wir folgendes Lemma:

LEMMA 2.4. *Für $A \leq TU_{\mathcal{E}}$ gilt: $U^A_{\mathcal{F},S_{\mathcal{F}}}/TU_{\mathcal{F}}$ ist frei vom Rang $r_{\mathcal{F}} - r_{\mathcal{E}}$.*

BEWEIS. Nach Bemerkung 2.3.(2) sind $U_{\mathcal{F},S_{\mathcal{F}}}/TU_{\mathcal{F}}$ und daher auch jede Untergruppe hiervon frei. Es bleibt daher noch die Dimensionsaussage zu zeigen: Da

$$\tilde{N}_{\mathcal{F}/\mathcal{E}} : U_{\mathcal{F},S_{\mathcal{F}}}/TU_{\mathcal{F}} \to U_{\mathcal{E},S_{\mathcal{E}}}/TU_{\mathcal{E}} : xTU_{\mathcal{F}} \mapsto N_{\mathcal{F}/\mathcal{E}}(x)TU_{\mathcal{E}}$$

ein Modulhomomorphismus ist, folgt aus dem Isomorphiesatz für freie $\mathbb{Z}$-Moduln und aus $N_{\mathcal{F}/\mathcal{E}}(x) = x^n$ für jedes $x \in \mathcal{E}$: ($\sim$ bezeichnet hier $\mathbb{Z}$-Modulisomorphien)

$$U_{\mathcal{E},S_{\mathcal{E}}}/_{TU_{\mathcal{E}}} \sim \text{Bild}\,\tilde{N}_{\mathcal{F}/\mathcal{E}} \sim {U_{\mathcal{F}}/TU_{\mathcal{F}}}/_{\text{Kern}\,\tilde{N}_{\mathcal{F}/\mathcal{E}}},$$

und daher $\operatorname{rg}\text{Kern}\,\tilde{N}_{\mathcal{F}/\mathcal{E}} = r_{\mathcal{F}} - r_{\mathcal{E}}$. Mit $TU^s_{\mathcal{E}} \subseteq A$ für ein geeignetes $s \in \mathbb{N}$ folgt dann die Behauptung. □

Satz 2.5. *Sei $U \leq U^A_{\mathcal{F},S_\mathcal{F}}$ eine Untergruppe von endlichem Index. Dann gibt es unabhängige Einheiten $\epsilon_i \in U$ $(1 \leq i \leq r_\mathcal{F} - r_\mathcal{E} + \operatorname{rg} A =: r)$ sowie eine Torsionseinheit ζ, so daß*

$$U = \langle \zeta \rangle \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle.$$

Seien $A \leq TU_\mathcal{E}$ beliebig, $U \leq U_{\mathcal{F},S_\mathcal{F}}$ von endlichem Index. Dann gibt es Einheiten $\epsilon_i \in U$ $(1 \leq i \leq r_\mathcal{F} - r_\mathcal{E})$, $\tilde{\epsilon}_i \in U$ $(1 \leq i \leq r_\mathcal{E} - 1)$ sowie eine Torsionseinheit ζ, so daß

$$U^A_{\mathcal{F},S_\mathcal{F}} \cap U = \langle \zeta \rangle \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_{r_\mathcal{F} - r_\mathcal{E}} \rangle$$

und

$$U_{\mathcal{F},S_\mathcal{F}} \cap U = (U^A_{\mathcal{F},S_\mathcal{F}} \cap U) \times \langle \tilde{\epsilon}_1 \rangle \times \cdots \times \langle \tilde{\epsilon}_{r_\mathcal{E}-1} \rangle$$

gelten.

Beweis. Direkte Konsequenz aus Bemerkung 2.3.(4) und Lemma 2.4. □

Für den Fall $\mathcal{E} = \mathbb{Q}$ und $A = \{\pm 1\} = TU_\mathbb{Q}$ erhalten wir wieder den Dirichlet'schen Einheitensatz als Spezialfall.

Im weiteren seien $A \leq TU_\mathcal{E}$ beliebig und $U \leq U_{\mathcal{F},S_\mathcal{F}}$, von endlichem Index fixiert.

Wir werden im folgenden einen Regulator für $U^A_{\mathcal{F},S_\mathcal{F}} \cap U$ erklären, der die klassische Definition erweitert. Dies ermöglicht uns dann, Abschätzungen für den Index $(U^{TU_\mathcal{E}}_{\mathcal{F},S_\mathcal{F}} : (U^{TU_\mathcal{E}}_{\mathcal{F},S_\mathcal{F}} \cap U))$ anzugeben, um $U^{TU_\mathcal{E}}_{\mathcal{F},S_\mathcal{F}}$ auszurechnen, ohne zunächst $U_{\mathcal{F},S_\mathcal{F}}$ zu bestimmen, was speziell im letzten Schritt (Aufstieg zu Fundamentaleinheiten) wegen der hohen Körpergrade sehr aufwendig ist [55]. Ferner wird dieser Regulator ein Maß für die Komplexität des später vorgestellten Algorithmus zum Lösen von Normgleichungen darstellen.

Seien nun

$$L_\mathcal{F} : U_{\mathcal{F},S_\mathcal{F}} \to \mathbb{R}^{S_\mathcal{F}} : \epsilon \mapsto (n_{V,\mathcal{E}} V(\epsilon))_{V \in S_\mathcal{F}}, \tag{2-3}$$

$$\dot{L}_\mathcal{F} : U_{\mathcal{F},S_\mathcal{F}} \to \mathbb{R}^{\dot{S_\mathcal{F}}} : \epsilon \mapsto (n_{V,\mathcal{E}} V(\epsilon))_{V \in \dot{S_\mathcal{F}}} \tag{2-4}$$

definiert. Nach [35, V, §1] ist $L_F(U_{\mathcal{F},S_\mathcal{F}})$ ein Gitter vom Rang $r_\mathcal{F} - 1$ im $\mathbb{R}^{S_\mathcal{F}}$; daher ist dann $L_\mathcal{F}(U^A_{\mathcal{F},S_\mathcal{F}})$ ein Gitter vom Rang $r_\mathcal{F} - r_\mathcal{E}$.

Lemma 2.6. (1) *Sei $B \in \mathbb{R}^{n' \times n'}$ mit $B_{i,j} = a + \delta_{i,j} b_i$, $a, b_i \in \mathbb{R}$. Dann gilt*

$$\det B = (\prod_{i=1}^{n'} b_i)(a \sum_{i=1}^{n'} \frac{1}{b_i} + 1).$$

(2) *Seien* $B \in \mathbb{R}^{n' \times n'}$, $C \in \mathbb{R}^{m' \times n'}$ *beliebig. Für* $B' := \begin{pmatrix} B \\ CB \end{pmatrix}$ *gelten dann* $B'^{tr} B' = B^{tr}(I_{n'} + C^{tr}C)B$ *und* $\det(B'^{tr}B') = \det^2 B \, \det(I_{n'} + C^{tr}C)$. *Speziell gilt für* $m' = 1$, *d.h.* $C = (c_1, \dots, c_{n'})$*:*

$$\det(I_{n'} + C^{tr}C) = 1 + \sum_{i=1}^{n'} c_i^2.$$

Beweis. (1): Siehe [46, 5.6 Exercise 1].

(2): Es gilt:

$$\begin{aligned} (B'^{tr}B')_{i,j} &= \sum_{l=1}^{n'+m'} B'_{l,i}B'_{l,j} = \sum_{l=1}^{n'} B_{l,i}B_{l,j} + \sum_{l=1}^{m'} (CB)_{l,i}(CB)_{l,j} \\ &= (B^{tr}B)_{i,j} + ((CB)^{tr}(CB))_{i,j} = (B^{tr}(I_{n'} + C^{tr}C)B)_{i,j} \end{aligned}$$

Da alle Matrizen quadratisch sind, folgt die Aussage über die Determinanten.

Sei nun $m' = 1$ und $D := \mathrm{diag}(c_1, \dots, c_{n'})$. Wir erhalten:

$$\begin{aligned} I_{n'} + C^{tr}C &= I_{n'} + ((1, \dots, 1)D)^{tr}(1, \dots, 1)D \\ &= D(D^{-2} + 1_{n'})D. \end{aligned}$$

Mit (1) angewendet auf $a = 1$, $b_i = c_i^{-2}$ folgt daher:

$$\begin{aligned} \det(I_{n'} + C^{tr}C) &= \det^2(D) \prod_{i=1}^{n'} c_i^{-2} (\sum_{i=1}^{n'} c_i^2 + 1) \\ &= \sum_{i=1}^{n'} c_i^2 + 1. \quad \square \end{aligned}$$

Wir fixieren nun ein maximales unabhängiges Einheitensystem $\epsilon_i \in U_{\mathcal{F},S_{\mathcal{F}}}^{TU_{\mathcal{E}}} \cap U$ $(1 \le i \le r_{\mathcal{F}} - r_{\mathcal{E}})$, $\tilde{\epsilon}_i \in U$ $(1 \le i \le r_{\mathcal{E}} - 1)$ und $\zeta \in TU_{\mathcal{F}}$ mit

$$U = \langle \zeta \rangle \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_{r_{\mathcal{F}} - r_{\mathcal{E}}} \rangle \times \langle \tilde{\epsilon}_1 \rangle \times \cdots \times \langle \tilde{\epsilon}_{r_{\mathcal{E}} - 1} \rangle.$$

Nach Satz 2.5 gibt es solche Einheiten. Definiere

$$\iota : U_{\mathcal{F},S_{\mathcal{F}}}^{TU_{\mathcal{E}}} \cap U \to \mathbb{Z}^{r_{\mathcal{F}} - r_{\mathcal{E}}} : \epsilon = \zeta \prod_{i=1}^{r_{\mathcal{F}} - r_{\mathcal{E}}} \epsilon_i^{n_i} \mapsto (n_i)_{1 \le i \le r_{\mathcal{F}} - r_{\mathcal{E}}},$$

sowie mit $\{v_1,\dots,v_{r_\mathcal{E}}\} = S_\mathcal{E}$, $\{V_1,\dots,V_{r_v-1}\} = \dot{P}_v$ eine Anordnung

$$\tau : S_\mathcal{F} \to \mathbb{N} : V \mapsto \begin{cases} \sum_{l=1}^{i-1}(r_{v_l}-1)+j-1 & \text{für } V = V_j \in \dot{P}_{v_i} \\ r_\mathcal{F} - r_\mathcal{E} + i & \text{für } V = V_{v_i} \text{ wie in (2-2)} \end{cases}.$$

Damit ist $\tau(S_\mathcal{F}) = [\![1, r_\mathcal{F}]\!]$ und $\tau(\dot{S_\mathcal{F}}) = [\![1, r_\mathcal{F} - r_\mathcal{E}]\!]$. Für $x \in \mathbb{R}^{S_\mathcal{F}}$ sei $\mathbb{R}^{r_\mathcal{F}} \ni \tau(x) := (x_{\tau(i)})_{1\le i\le r_\mathcal{F}}$. Mit

$$\mathcal{L} := \left(n_{\tau^{-1}(i),\mathcal{E}}\, \tau^{-1}(i)(\epsilon_j)\right)_{\substack{1\le i\le r_\mathcal{F}\\ 1\le j\le r_\mathcal{F}-r_\mathcal{E}}} \in \mathbb{R}^{r_\mathcal{F}\times(r_\mathcal{F}-r_\mathcal{E})}$$

und

$$\dot{\mathcal{L}} := \left(n_{\tau^{-1}(i),\mathcal{E}}\, \tau^{-1}(i)(\epsilon_j)\right)_{\substack{1\le i\le r_\mathcal{F}-r_\mathcal{E}\\ 1\le j\le r_\mathcal{F}-r_\mathcal{E}}} \in \mathbb{R}^{(r_\mathcal{F}-r_\mathcal{E})\times(r_\mathcal{F}-r_\mathcal{E})}$$

erhalten wir dann die beiden kommutativen Diagramme:

$$\begin{tikzcd} U^{TU_\mathcal{E}}_{\mathcal{F},S_\mathcal{F}} \cap U \arrow[r, "L_\mathcal{F}"] \arrow[d, "\iota"'] & \mathbb{R}^{S_\mathcal{F}} \arrow[d, "\tau"] \\ \mathbb{Z}^{r_\mathcal{F}-r_\mathcal{E}} \arrow[r, "\mathcal{L}"] & \mathbb{R}^{r_\mathcal{F}} \end{tikzcd} \quad \text{und} \quad \begin{tikzcd} U^{TU_\mathcal{E}}_{\mathcal{F},S_\mathcal{F}} \cap U \arrow[r, "\dot{L}_\mathcal{F}"] \arrow[d, "\iota"'] & \mathbb{R}^{\dot{S_\mathcal{F}}} \arrow[d, "\tau"] \\ \mathbb{Z}^{r_\mathcal{F}-r_\mathcal{E}} \arrow[r, "\dot{\mathcal{L}}"] & \mathbb{R}^{r_\mathcal{F}-r_\mathcal{E}} \end{tikzcd}.$$

Lemma 2.7. *Sei* $\Gamma := [0,1]^{r_\mathcal{F}-r_\mathcal{E}}$. *Dann gelten:*

(1) $\mathrm{vol}_{r_\mathcal{F}-r_\mathcal{E}}(\mathcal{L}\Gamma) = \sqrt{\prod_{v\in S_\mathcal{E}} r_v}\,\mathrm{vol}(\dot{\mathcal{L}}\Gamma)$
(2) $\mathrm{vol}(\dot{\mathcal{L}}\Gamma)$ *ist unabhängig von der Anordnung der Bewertungen und dem speziell gewählten Einheitensystem.*

Beweis. (1): Sei

$$\text{(2-5)} \qquad C := \begin{pmatrix} \overbrace{-1,\dots,-1}^{r_{v_1}-1} & \overbrace{0}^{r_{v_2}-1} & & \overbrace{}^{r_{v_{r_\mathcal{E}}}-1} \\ & -1,\dots,-1 & & 0 \\ 0 & & \cdots & \\ & 0 & & -1,\dots,-1 \end{pmatrix}.$$

Dann gilt:

$$C^{tr}C = \mathrm{diag}(1_{r_{v_1}-1},\dots,1_{r_{v_{r_\mathcal{E}}}-1}).$$

Nach Lemma 2.6.(1) und [23, §5 (67)] gilt dann:

$$\text{(2-6)} \qquad \det(I_{r_\mathcal{F}-r_\mathcal{E}} + C^{tr}C) = \prod_{v\in S_\mathcal{E}} r_v.$$

Aus (1-1) zusammen mit Definition 2.2 und Bemerkung 2.3.(3) folgt für jedes $v \in S_{\mathcal{E}}$ und jedes $\epsilon \in U_{\mathcal{F},S_{\mathcal{F}}}^{TU_{\mathcal{E}}}$:

$$\sum_{V \in P_v} n_{V,\mathcal{E}} V(\epsilon) = v(N_{\mathcal{F}/\mathcal{E}}(\epsilon)) = 0. \tag{2-7}$$

Aus $\mathcal{L} = \begin{pmatrix} \dot{\mathcal{L}} \\ \hline C\dot{\mathcal{L}} \end{pmatrix}$, (2-6) und Lemma 2.6.(2) erhalten wir daher

$$\det(\mathcal{L}^{tr}\mathcal{L}) = \det(\dot{\mathcal{L}}^{tr}\dot{\mathcal{L}}) \prod_{v \in S_{\mathcal{E}}} r_v.$$

Wegen $\mathrm{vol}^2_{r_{\mathcal{F}}-r_{\mathcal{E}}}(\mathcal{L}\Gamma) = \det(\mathcal{L}^{tr}\mathcal{L})$ [34, Appendix II] und $\mathrm{vol}^2(\dot{\mathcal{L}}\Gamma) = \det(\dot{\mathcal{L}}^{tr}\dot{\mathcal{L}}) = \det^2(\dot{\mathcal{L}})$ ist dann (1) bewiesen.

(2): Da die entsprechenden Transformationen unimodular bzw. unitär sind, folgt die Behauptung. □

Definition 2.8. *Wir nennen*

$$\mathrm{reg}_{\mathcal{F}/E}(U) := \mathrm{vol}(\dot{\mathcal{L}}\Gamma)$$

den ($S_{\mathcal{F}}$-)Regulator von U (bezüglich $\mathcal{F}/\mathcal{E}$).

Ferner sei $\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F}) := \mathrm{reg}_{\mathcal{F}/\mathcal{E}}(U_{\mathcal{F},S_{\mathcal{F}}}^{TU_{\mathcal{E}}})$.

Satz 2.9. *Es gilt:*

$$\mathrm{reg}_{\mathcal{F}/\mathbb{Q}}(U) = (\prod_{i=1}^{r_{\mathcal{E}}} n_{v_i,\mathbb{Q}}^{r_{v_i}-1}) \, \mathrm{reg}_{\mathcal{F}/\mathcal{E}}(U) \, \mathrm{reg}_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(U)).$$

Beweis. Setze $\tilde{\mathcal{L}} := (\mathcal{L} \mid \tau L_{\mathcal{F}}(\tilde{\epsilon}_1), \ldots, \tau L_{\mathcal{F}}(\tilde{\epsilon}_{r_{\mathcal{E}}-1}))$. Da $\mathrm{rg}\,\dot{\mathcal{L}} = r_{\mathcal{F}} - r_{\mathcal{E}}$ gilt, gibt es ein $S \in \mathrm{GL}(r_{\mathcal{F}} - 1, \mathbb{R})$ mit

$$\tilde{\mathcal{L}} = \left(\begin{array}{c|c} \mathcal{L} & \begin{array}{c} 0_{r_{\mathcal{F}}-r_{\mathcal{E}}} \\ \hline B \end{array} \end{array} \right) S,$$

wobei (wie in (2-7)) für jedes $v \in S_{\mathcal{E}}$

$$\sum_{V \in P_v} n_{V,\mathcal{E}} V(\epsilon_i) = v(N_{\mathcal{F}/\mathcal{E}}(\epsilon_i)) = 0$$

und

$$\sum_{V \in P_v} n_{V,\mathcal{E}} V(\tilde{\epsilon}_i) = v(N_{\mathcal{F}/\mathcal{E}}(\tilde{\epsilon}_i))$$

gelten und daher o.B.d.A. B von folgender Form ist:

$$B = (v_i(N_{\mathcal{F}/\mathcal{E}}(\tilde{\epsilon}_j)))_{\substack{1 \le i \le r_{\mathcal{E}} \\ 1 \le j \le r_{\mathcal{E}}-1}}.$$

Seien $\mathcal{L}'$, $\tilde{\mathcal{L}}'$ und B' durch Streichen der letzten Zeile von $\mathcal{L}$, $\tilde{\mathcal{L}}$ und B definiert. Dann gelten:

$$\tilde{\mathcal{L}}' = \left(\begin{array}{c|c} \mathcal{L}' & \begin{array}{c} 0 \\ \hline B' \end{array} \end{array} \right) S = \left(\begin{array}{c|c} \dot{\mathcal{L}} & 0 \\ \hline * & B' \end{array} \right) S.$$

Sei

$$D_1 := \operatorname{diag}(\frac{n_{\tau^{-1}(1),\mathbb{Q}}}{n_{\tau^{-1}(1),\mathcal{E}}}, \ldots, \frac{n_{\tau^{-1}(r_{\mathcal{F}}-1),\mathbb{Q}}}{n_{\tau^{-1}(r_{\mathcal{F}}-1),\mathcal{E}}}) \in \mathbb{R}^{r_{\mathcal{F}}-1 \times r_{\mathcal{F}}-1}$$

sowie

$$D_2 := \operatorname{diag}(n_{v_1,\mathbb{Q}}, \ldots, n_{v_{r_{\mathcal{E}}-1},\mathbb{Q}}) \in \mathbb{R}^{r_{\mathcal{E}}-1 \times r_{\mathcal{E}}-1}.$$

Dann sind definitionsgemäß

$$\det(D_2 B') = \operatorname{reg}_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(U))$$

und

$$\det(D_1 \tilde{\mathcal{L}}') = \operatorname{reg}_{\mathcal{F}/\mathbb{Q}}(U).$$

Daher folgt:

$$\begin{aligned}
\operatorname{reg}_{\mathcal{F}/\mathbb{Q}}(U) &= \det(D_1)\det(\tilde{\mathcal{L}}') \\
&= \det(D_1)\det(\dot{\mathcal{L}})\det(B') \\
&= \frac{\det(D_1)}{\det(D_2)} \operatorname{reg}_{\mathcal{F}/\mathcal{E}}(U) \operatorname{reg}_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(U)) \\
&= \prod_{i=1}^{r_{\mathcal{F}}-1} \frac{n_{\tau^{-1}(i),\mathbb{Q}}}{n_{\tau^{-1}(i),\mathcal{E}}} \prod_{i=1}^{r_{\mathcal{E}}-1} \frac{1}{n_{v_i,\mathbb{Q}}} \operatorname{reg}_{\mathcal{F}/\mathcal{E}}(U) \operatorname{reg}_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(U)),
\end{aligned}$$

und mit $\frac{n_{V,\mathbb{Q}}}{n_{V,\mathcal{E}}} = n_{v,\mathbb{Q}}$ für jedes $V|v$ können wir weiter schließen:

$$\begin{aligned}
&= \prod_{i=1}^{r_{\mathcal{E}}} n_{v_i,\mathbb{Q}}^{r_{v_i}-1} n_{v_{r_{\mathcal{E}}}} \frac{n_{\tau^{-1}(r_{\mathcal{F}}),\mathcal{E}}}{n_{\tau^{-1}(r_{\mathcal{F}}),\mathbb{Q}}} \operatorname{reg}_{\mathcal{F}/\mathcal{E}}(U) \operatorname{reg}_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(U)) \\
&= \prod_{i=1}^{r_{\mathcal{E}}} n_{v_i,\mathbb{Q}}^{r_{v_i}-1} \operatorname{reg}_{\mathcal{F}/\mathcal{E}}(U) \operatorname{reg}_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(U)). \quad \square
\end{aligned}$$

Bemerkung 2.10. (1) *Für $\mathcal{E} = \mathbb{Q}$ und $S_{\mathcal{E}} = V_{\mathcal{E}}^{\infty}$ erhalten wir wieder die alte Definition des Regulators, d.h., es gilt:*

$$\operatorname{reg}(U) = \operatorname{reg}_{\mathcal{F}/\mathbb{Q}}(U).$$

(2) *Für $S_{\mathcal{E}} = V_{\mathcal{E}}^{\infty}$ gilt*

$$\begin{aligned}
\operatorname{reg}(U) &= 2^{r_2(n-1)} \operatorname{reg}_{\mathcal{F}/\mathcal{E}}(U) \operatorname{reg}_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(U)) \\
&= 2^{r_2(n-1)} \operatorname{reg}_{\mathcal{F}/\mathcal{E}}(U)(U_{\mathcal{E}} : TU_{\mathcal{E}} N_{\mathcal{F}/\mathcal{E}}(U)) \operatorname{reg}(U_{\mathcal{E}}).
\end{aligned}$$

(3) *Bei der in* [14] *gegebenen Definition entfällt der Faktor* $2^{r_2(n-1)}$. *Die dort gegebene Definition unterscheidet sich von unserer in der Normierung der Funktion* $L_{\mathcal{F}}$ (2-3); *dort wird statt mit* $n_{V,\mathcal{E}}$ *mit* $n_{V,\mathbb{Q}}$ *multipliziert. Ferner wird dort nur der Fall* $S_{\mathcal{E}} = V_{\mathcal{E}}^{\infty}$ *betrachtet.*

2. Eine untere Regulatorabschätzung

In diesem Abschnitt seien $A := TU_{\mathcal{E}}$ und $S_{\mathcal{E}} := V_{\mathcal{E}}^{\infty}$. Wir wollen eine untere Abschätzung für $\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F})$ herleiten, die es uns ermöglicht, mit den in [55] dargestellten Methoden, ausgehend von einer Untergruppe von endlichem Index, zu der vollen Einheitengruppe „aufzusteigen“. Im Gegensatz zu unteren Schranken wie z.B. in [22, 14] werden wir keine a-priori-Schranken erhalten; dafür wird unsere i.allg. größer, d.h. schärfer, sein.

Lemma 2.11. *Die Abbildung:*

$$q : U_{\mathcal{F}}^{TU_{\mathcal{E}}} \to \mathbb{R}_{\geq 0} : \epsilon \mapsto \sum_{i=1}^{m}\sum_{j=1}^{n} |\log(|\epsilon^{(i,j)}|)|^2$$

ist eine positiv definite quadratische Form mit Determinante

$$d_q = 2^{r_2(n-1)-\sum_{i=1}^{r_1} t_i}\ n^{r_1+r_2}\,\mathrm{reg}^2_{\mathcal{F}/\mathcal{E}}(\mathcal{F}).$$

Beweis. Sei $\epsilon_1, \ldots, \epsilon_{r_{\mathcal{F}}-r_{\mathcal{E}}}$ ein unabhängiges Erzeugendensystem für $U_{\mathcal{F}}^{TU_{\mathcal{E}}}$. Dann gilt für $x \in U_{\mathcal{F}}^{TU_{\mathcal{E}}}$ mit $x = \zeta^{\mu_0}\prod_{i=1}^{r_{\mathcal{F}}-r_{\mathcal{E}}} \epsilon_i^{\mu_i}$:

$$\begin{aligned}
q(x) &= q(\prod_{l=1}^{r_{\mathcal{F}}-r_{\mathcal{E}}} \epsilon_l^{\mu_l}) \\
&= \sum_{i=1}^{m}\sum_{j=1}^{n}(\sum_{l=1}^{r_{\mathcal{F}}-r_{\mathcal{E}}} \mu_l \log|\epsilon_l^{(i,j)}|)^2 \\
&= \sum_{k,l=1}^{r_{\mathcal{F}}-r_{\mathcal{E}}} \mu_k\mu_l(\sum_{i=1}^{m}\sum_{j=1}^{n}\log|\epsilon_k^{(i,j)}|\log|\epsilon_l^{(i,j)}|) \\
&= (\mu_l)^{tr}_{1\leq l\leq r_{\mathcal{F}}-r_{\mathcal{E}}} \\
&\qquad\qquad (\log|\epsilon_k^{(i,j)}|)^{tr}_{\substack{1\leq i\leq m, 1\leq j\leq n\\ 1\leq k\leq r_{\mathcal{F}}-r_{\mathcal{E}}}} \\
&\qquad\qquad (\log|\epsilon_k^{(i,j)}|)_{\substack{1\leq i\leq m, 1\leq j\leq n\\ 1\leq k\leq r_{\mathcal{F}}-r_{\mathcal{E}}}} \\
&\quad\ (\mu_l)_{1\leq l\leq r_{\mathcal{F}}-r_{\mathcal{E}}} \\
&=: (\mu_l)^{tr}_{1\leq l\leq r_{\mathcal{F}}-r_{\mathcal{E}}} \quad {B'}^{tr} B' \quad (\mu_l)_{1\leq l\leq r_{\mathcal{F}}-r_{\mathcal{E}}}.
\end{aligned}$$

Da $q(x)$ als Summe nicht negativer Zahlen nicht negativ ist, haben wir q als positivsemidefinit nachgewiesen. Da $q(x) = 0$ äquivalent zu $x \in TU_{\mathcal{F}}$ ist, ist der erste Teil der Aussage gezeigt.

Weil definitionsgemäß
$$\det(B'^{tr} B') = d_q$$
gilt, müssen wir nun $\det B'^{tr} B'$ berechnen. Um die Lemmata 2.6.(1) und 2.6.(2) anwenden zu können, benötigen wir zunächst einige Hilfsmatrizen: Für $1 \leq i \leq r_1$ betrachten wir die folgenden Matrizen:

$$B_i' := \begin{pmatrix} \log|\epsilon_1^{(i,1)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,1)}| \\ \vdots & & \vdots \\ \log|\epsilon_1^{(i,s_i+t_i)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,s_i+t_i)}| \\ \log|\epsilon_1^{(i,s_i+2t_i)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,s_i+2t_i)}| \\ \log|\epsilon_1^{(i,s_i+t_i+1)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,s_i+t_i+1)}| \\ \vdots & & \vdots \\ \log|\epsilon_1^{(i,s_i+2t_i-1)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,s_i+2t_i-1)}| \end{pmatrix} =: \left(\begin{array}{ccc} & B_i & \\ \hline \log|\epsilon_1^{(i,s_i+t_i)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,s_i+t_i)}| \\ \log|\epsilon_1^{(i,s_i+2t_i)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,s_i+2t_i)}| \\ \log|\epsilon_1^{(i,s_i+t_i+1)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,s_i+t_i+1)}| \\ \vdots & & \vdots \\ \log|\epsilon_1^{(i,s_i+2t_i-1)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,s_i+2t_i-1)}| \end{array}\right)$$

und

$$C_i := \begin{cases} \left(\begin{array}{ccc|ccc} \multicolumn{3}{c}{\overbrace{\hphantom{-1/2 \ \dots \ -1/2}}^{s_i}} & \multicolumn{3}{c}{\overbrace{\hphantom{-1 \ \dots \ -1}}^{t_i-1}} \\ -1/2 & \dots & -1/2 & -1 & \dots & -1 \\ -1/2 & \dots & -1/2 & -1 & \dots & -1 \\ \hline & 0 & & & I_{t_i-1} & \end{array}\right) & t_i > 0 \\ \left(\underbrace{-1 \ \dots \ -1}_{n-1} \right) & t_i = 0 \end{cases} .$$

Für $r_1 < i \leq r_1 + r_2$ definieren wir analog:

$$B_i' := \begin{pmatrix} \log|\epsilon_1^{(i,1)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,1)}| \\ \vdots & & \vdots \\ \log|\epsilon_1^{(i,n)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,n)}| \end{pmatrix} =: \left(\begin{array}{ccc} & B_i & \\ \hline \log|\epsilon_1^{(i,n)}| & \dots & \log|\epsilon_{r_\mathcal{F}-r_\mathcal{E}}^{(i,n)}| \end{array}\right)$$

und

$$C_i := \left(\overbrace{-1 \ \dots \ -1}^{n-1} \right).$$

Damit gilt für $1 \leq i \leq r_1 + r_2$:

$$B_i' = \left(\frac{B_i}{C_i B_i} \right)$$

und

$$B' = S' \begin{pmatrix} B'_1 \\ \vdots \\ B'_{r_1+r_2} \\ B'_{r_1+1} \\ \vdots \\ B'_{r_1+r_2} \end{pmatrix} = S \begin{pmatrix} B_1 \\ \vdots \\ B_{r_1+r_2} \\ C_1 B_1 \\ \vdots \\ C_{r_1+r_2} B_{r_1+r_2} \\ B_{r_1+1} \\ \vdots \\ B_{r_1+r_2} \\ C_{r_1+1} B_{r_1+1} \\ \vdots \\ C_{r_1+r_2} B_{r_1+r_2} \end{pmatrix},$$

wobei S', S die notwendigen Zeilenvertauschungen darstellen und deswegen unitär sind. Schließlich seien noch

$$B := \begin{pmatrix} B_1 \\ \vdots \\ B_{r_1+r_2} \end{pmatrix} \text{ und } C := \begin{pmatrix} C_1 & 0 & & \ldots & & & 0 \\ 0 & C_2 & 0 & & \ldots & & 0 \\ & & \ddots & & & & \\ 0 & \ldots & 0 & C_{r_1+1} & 0 & \ldots & 0 \\ & & & & \ddots & & \\ 0 & & & \ldots & & 0 & C_{r_1+r_2} \\ 0 & \ldots & 0 & I_{n-1} & 0 & \ldots & 0 \\ & & & & \ddots & & \\ 0 & & & \ldots & & 0 & I_{n-1} \\ 0 & \ldots & 0 & C_{r_1+1} & 0 & \ldots & 0 \\ & & & & \ddots & & \\ 0 & & & \ldots & & 0 & C_{r_1+r_2} \end{pmatrix}.$$

Damit folgt

$$B' = S \begin{pmatrix} B \\ \hline CB \end{pmatrix}.$$

Nach Lemma 2.6.(2) gilt $\det(B'^{tr} B') = \det^2(B) \det(I + C^{tr} C)$. Offensichtlich haben wir

$$\prod_{i=1}^{r_1} 2^{\max(0, t_i - 1)} \det(B) = \mathrm{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F})$$

und (mit [23, §5 (67)])

$$\det(I + C^{tr} C) = \prod_{i=1}^{r_1} (I_{s_i + t_1 - 1} + C_i^{tr} C_i) \prod_{i=r_1+1}^{r_1+r_2} (I_{n-1} + 2 C_i^{tr} C_i + I_{n-1}).$$

Es verbleibt also nur noch $\det(I_{s_i+t_i-1} + C_i^{tr} C_i)$ bzw. $\det(2I_{n-1} + 2C_i^{tr} C_i)$ zu bestimmen. Für $1 \leq r_1, t_i = 0$ folgt aus Lemma 2.6.(2):

$$\det(I_{s_i+t_i-1} + c_i^{tr} c_i) = \sum_{l=1}^{n-1} (c_i)_l^2 + 1 = n.$$

Mir Lemma 2.6.(1) folgt:

$$\det(2I + 2c_i^{tr} c_i) = 2^{n-1}(\sum_{l=1}^{n-1} 1 + 1) = 2^{n-1} n.$$

Schließlich sei $1 \leq i \leq r_1$ und $t_i > 0$. Mit

$$D := \operatorname{diag}(\overbrace{\frac{1}{2}, \ldots, \frac{1}{2}}^{s_i}, \overbrace{1, \ldots, 1}^{t_i - 1})$$

und

$$\tilde{C}_i = \left(\begin{array}{c|c} -1 \quad \ldots & -1 \\ \hline 0 & I_{t_i-1} \end{array} \right)$$

folgt dann

$$\begin{aligned} \det(I_{s_i+t_i-1} + C_i^{tr} c) &= \det{}^2(D) \det(D^{-2} + \tilde{C}_i^{tr} \tilde{C}_i) \\ &= \left(\frac{1}{4}\right)^{s_i} 4^{s_i} 2^{t_i - 1} (2 \sum_{l=1}^{s_i} \frac{1}{4} + 2 \sum_{l=s_i+1}^{s_i+t_i-1} \frac{1}{2} + 1) \\ &= 2^{t_i} (\frac{s_i}{4} + \frac{t_i - 1}{2} + \frac{1}{2}) \\ &= 2^{t_i} \frac{n}{4} \end{aligned}$$

aus

$$\tilde{C}_i^{tr} \tilde{C}_i = \operatorname{diag}(\overbrace{0, \ldots, 0}^{s_i}, \overbrace{1, \ldots, 1}^{t_i - 1}) + 2_{s_i+t_i-1}.$$

Insgesamt gilt

$$\begin{aligned} d_q &= \prod_{i=1}^{r_1} 4^{-\max(0, t_i - 1)} \operatorname{reg}^2_{\mathcal{F}/\mathcal{E}}(\mathcal{F}) \prod_{\substack{i=1 \\ t_i = 0}}^{r_1} n \prod_{\substack{i=1 \\ t_i > 0}}^{r_1} 2^{t_i - 2}\, n \prod_{i=r_1+1}^{r_1+r_2} 2^{n-1}\, n \\ &= 2^{-\sum_{i=1}^{r_1} t_i}\, n^{r_1}\, 2^{(n-1) r_2}\, n^{r_2}\, \operatorname{reg}^2_{\mathcal{F}/\mathcal{E}}(\mathcal{F}) \\ &= 2^{r_2(n-1) - \sum_{i=1}^{r_1} t_i}\, n^{r_1 + r_2}\, \operatorname{reg}^2_{\mathcal{F}/\mathcal{E}}(\mathcal{F}) \end{aligned}$$

und die Behauptung folgt. $\square$

LEMMA 2.12. *Für*

$$h_1 : \mathbb{R}_{\geq 0} \to \mathbb{R} : x \mapsto \cosh(\sqrt{x}) - 1,$$

$x,\ y \in \mathbb{R}_{\geq 0},\ \lambda \geq 1$ *gelten:*

(1) $h_1(x+y) \geq h_1(x) + h_1(y)$,
(2) $h_1(\lambda x) \geq \lambda h_1(x)$,
(3) h_1 *ist streng monoton wachsend.*

BEWEIS. (1): Es gilt $\cosh(x) = \sum_{k=0}^{\infty} \frac{x^{2k}}{(2k)!}$ und daher:

$$\begin{aligned} h_1(x+y) &= \sum_{k=1}^{\infty} \frac{1}{(2k)!}(x+y)^k \\ &\geq \sum_{k=1}^{\infty} \frac{1}{(2k)!}(x^k + y^k) \\ &= h_1(x) + h_1(y). \end{aligned}$$

(2): Da $\lambda \leq \lambda^k$ gilt, folgt die Behauptung wie in (1).

(3): Da sowohl $\cosh(\cdot)$ als auch $\sqrt{\cdot}$ streng monoton wachsend sind, folgt die Aussage unmittelbar. □

LEMMA 2.13. *Seien* $n' \in \mathbb{N}$, $n' \leq K \in \mathbb{R}$ *und*

$$h_2 : \mathbb{R}^{n'} \to \mathbb{R} : x = (x_1, \dots, x_{n'}) \mapsto \sum_{i=1}^{n'} x_i^2$$

gegeben. Für das Minimum M *von* h_2 *unter den Nebenbedingungen*

(1) $\sum_{i=1}^{n'} e^{2x_i} \geq K$,
(2) $\sum_{i=1}^{n'} e^{-2x_i} \geq K$

gilt:

$$M \geq \frac{1}{4} \operatorname{arcosh}^2(K - n' + 1).$$

BEWEIS. Durch Addition der Bedingungen (1) und (2) erhalten wir ($\cosh(x) = \frac{1}{2}(e^x + e^{-x})$):

(3) $\sum_{i=1}^{n'} \cosh(2x_i) \geq K$.

Nach Lemma 2.12.(3) reicht es, das Minimum von $\cosh(\sqrt{4h_2})$ abzuschätzen. Mit Lemma 2.12.(1) gilt:

$$\begin{aligned}\cosh\sqrt{4h_2(x)}-1 &= \cosh(\sqrt{\sum_{i=1}^{n'}(2x_i)^2})-1\\ &\geq \sum_{i=1}^{n'}(\cosh(|2x_i|)-1)\\ &= \sum_{i=1}^{n'}(\cosh(2x_i)-1)\geq K-n',\end{aligned}$$

woraus die Behauptung dann unmittelbar folgt. □

LEMMA 2.14. *Sei $U \leq U_{\mathcal{F}}$ eine Untergruppe von endlichem Index mit $U_{\mathcal{E}} < U$. Dann gilt:*

$$(U_{\mathcal{E}} : TU_{\mathcal{E}}N_{\mathcal{F}/\mathcal{E}}(U_{\mathcal{F}}))|(U_{\mathcal{E}} : TU_{\mathcal{E}}N_{\mathcal{F}/\mathcal{E}}(U))|n^{r_1+r_2}.$$

BEWEIS. Unmittelbare Folge aus $N_{\mathcal{F}/\mathcal{E}}(U_{\mathcal{E}}) = U_{\mathcal{E}}^n$ und dem Satz von Lagrange [40, Satz 1.7.7.]. □

Analog [55, Kapitel 2] erhalten wir nun aus Lemma 2.11 und Lemma 2.13 eine untere Schranke für $\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F})$: Seien $r := \sum_{i=1}^{r_1}(s_i+t_i)+r_2n-1$, $M_1,\dots,M_r$ die sukzessiven Minima von q und γ_r^r die r-te Hermitesche Konstante. Dann gilt:

$$\sqrt{\frac{2^{\sum_{i=1}^{r_1} t_i - r_2(n-1)}\prod_{i=1}^r M_i}{n^{r_1+r_2}\gamma_r^r}} \leq \mathrm{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F}). \tag{2-8}$$

Nun können wir mit Hilfe einer modifizierten Version von [55, Algorithmus 2.7] eine untere Regulatorschranke bestimmen. Dort werden — mittels des Auszähl-Algorithmus 3.6 — die sukzessiven Minima teilweise bestimmt und gleichzeitig eine untere Schranke für die fehlenden Minima ermittelt. Alternativ hierzu können wir auch den ungeänderten Algorithmus verwenden, um eine Schranke für $\mathrm{reg}_{\mathcal{F}}(\mathcal{F})$ zu erhalten. Nachdem wir die n-maximale Obergruppe (d.h. p-maximal für jedes $p \in \mathbb{P}_{\mathbb{Q}}$ mit $p|n$) von $U_{\mathcal{E}}$ in $U_{\mathcal{F}}$ bestimmt haben, können wir mit Hilfe von Satz 2.9 eine untere Schranke erhalten.

In der Praxis sollten beide Schranken parallel berechnet werden, was einfach zu implementieren ist, da die Hauptarbeit im Auszählen und Testen einer großen Menge von algebraischen Zahlen liegt.

BEMERKUNG 2.15. *In* [45] *wird das Minimum von* $\mathbb{R}^{n'} \ni x \mapsto \sum_{i=1}^{n'} x_i^2$ *zusätzlich zu den in* Lemma 2.13 *gegebenen Nebenbedingungen noch unter*

$$\sum_{i=1}^{n'} x_i = 0$$

abgeschätzt. Die dort angegebene untere Schranke erfordert i.allg. noch das Lösen mehrerer algebraischer Gleichungssysteme. Für den Fall $n' = 5$ *ist die Schranke explizit, es gilt*

$$h_2 \geq \frac{1}{2} \operatorname{arcosh}^2\left(\frac{K-5+2}{2}\right).$$

Wegen $\operatorname{arcosh}'(x) \to 0$ *für* $x \to \infty$ *gilt*

$$\frac{\operatorname{arcosh}^2(\frac{K-n+2}{2})}{\operatorname{arcosh}^2(K-n+1)} \to 1,$$

d.h., unsere Regulatorschranke ist für große K *etwa halb so groß wie die in* [45]. *Im Gegensatz zu der in* [45] *ist unsere Schranke jedoch explizit gegeben.*

3. Konstruktion von Einheiten

Hier wollen wir kurz darauf eingehen, wie die in den letzten Abschnitten vorgestellten Ergebnisse für praktische Berechnungen genutzt werden können. Zunächst benötigen wir jedoch noch ein

LEMMA 2.16. (1) *Für jedes* $x \in o_{\mathcal{F}}$ *gilt:* $\frac{N_{\mathcal{F}/\mathcal{E}}(x)}{x} \in o_{\mathcal{F}}$.
(2) *Seien* $c > 0$ *und*

$$M_c := \{x \in o_{\mathcal{F}} \mid \forall v \in V_{\mathcal{E}}^{\infty} : v(N_{\mathcal{F}/\mathcal{E}}(x)) \leq c\}.$$

Dann enthält M_c *nur endlich viele bezüglich* $U_{\mathcal{F}}^1$ *nicht assoziierte Elemente.*

BEWEIS. (1): Konsequenz aus (1-1).

(2): Analog [46, 5 (2.3)]: Setze

$$\tilde{M}_c := \{x \in o_{\mathcal{E}} \mid \forall v \in V_{\mathcal{E}}^{\infty} : v(x) \leq c\}.$$

Dann ist offensichtlich $\#\tilde{M}_c < \infty$, und es reicht zu zeigen, daß für jedes $\mu \in \tilde{M}_c$ die Menge $N_\mu := \{x \in o_{\mathcal{F}} \mid \forall v \in V_{\mathcal{E}}^{\infty} : N_{\mathcal{F}/\mathcal{E}}(x) = \mu\}$ nur endlich viele nicht assoziierte Elemente enthält. Wir fixieren ein $\mu \in \tilde{M}_c$ und setze $T := o_{\mathcal{F}}/(\mu)$. Wir zeigen nun, daß $\alpha/\beta \in U_{\mathcal{F}}^1$ aus $\alpha \equiv \beta \mod \mu$ folgt. Seien dazu $\alpha \equiv \beta \mod \mu$ beliebig aus N_μ gegeben und $\gamma \in o_{\mathcal{F}}$ mit $\alpha - \beta = \gamma\mu$. Dann gilt: $\frac{\alpha}{\beta} = 1 + \gamma\frac{\mu}{\beta} \in o_{\mathcal{F}}$

nach (1). Analog folgt $\frac{\beta}{\alpha} \in o_{\mathcal{F}}$. Wegen $N_{\mathcal{F}/\mathcal{E}}(\alpha) = N_{\mathcal{F}/\mathcal{E}}(\beta)$ folgt dann $\frac{\alpha}{\beta} \in U^1_{\mathcal{F}}$, mit $\#T = N_{\mathcal{F}/\mathbb{Q}}(\mu) = N_{\mathcal{E}/\mathbb{Q}}(\mu)^n < \infty$ was die Behauptung impliziert. $\square$

Mit Hilfe dieses Lemmas ist es möglich, die in [55, Kapitel 3] vorgestellten Methoden — unter Zuhilfenahme der im nächsten Kapitel vorgestellten Ideen — auch in Relativerweiterungen zu benutzen. Jedoch sind diese „relativen Methoden“ viel aufwendiger als die entsprechenden „absoluten“. Daher lohnen sie sich nur, wenn die relative Struktur eine wesentliche Rolle spielt. Es scheint sinnvoll zu sein, zuerst ein maximales unabhängiges Einheitensystem (d.h. $U \leq U_{\mathcal{F}}$ mit endlichem Index) in dem entsprechenden absoluten Zahlkörper auszurechnen.

Sei nun $U \leq U_{\mathcal{F}}$ mit endlichem Index gegeben, ferner sei $r_{\mathcal{E}} - 1$ der Einheitenrang von $\mathcal{E}$ und $r_{\mathcal{F}} - 1$ der von $\mathcal{F}$. Wir fixieren in $U_{\mathcal{E}}/TU_{\mathcal{E}}$ ein unabhängiges Erzeugendensystem $\epsilon_1, \ldots, \epsilon_{r_{\mathcal{E}}-1}$ und definieren einen $\mathbb{Z}$-Modulisomorphismus

$$\iota_{\mathcal{E}} : U_{\mathcal{E}}/TU_{\mathcal{E}} \to \mathbb{Z}^{r_{\mathcal{E}}-1} : \epsilon = \prod_{i=1}^{r_{\mathcal{E}}-1} \epsilon_i^{n_i} \mapsto (n_i)_{i=1}^{r_{\mathcal{E}}-1}.$$

Analog definieren wir $\iota_{\mathcal{F}} : U/TU_{\mathcal{F}} \to \mathbb{Z}^{r_{\mathcal{F}}-1}$ für ein beliebiges festes System von unabhängigen Erzeugern von $U/TU_{\mathcal{F}}$. Ferner sei $\mathcal{N} \in \mathbb{Z}^{r_{\mathcal{E}}-1 \times r_{\mathcal{F}}-1} \cong \mathrm{Hom}(\mathbb{Z}^{r_{\mathcal{F}}-1}, \mathbb{Z}^{r_{\mathcal{E}}-1})$ so gewählt, daß das folgende Diagramm kommutativ ist:

$$\begin{array}{ccc} U/TU_{\mathcal{F}} & \xrightarrow{N_{\mathcal{F}/\mathcal{E}}} & U_{\mathcal{E}}/TU_{\mathcal{E}} \\ {\scriptstyle \iota_{\mathcal{F}}}\Big\downarrow & & \Big\downarrow{\scriptstyle \iota_{\mathcal{E}}} \\ \mathbb{Z}^{r_{\mathcal{F}}-1} & \xrightarrow{\mathcal{N}} & \mathbb{Z}^{r_{\mathcal{E}}-1} \end{array}.$$

Wenn wir nun die spaltenreduzierte Hermite-Normalform HNF($\mathcal{N}$) ausrechnen, erhalten wir eine Basis von $\mathbb{Z}^{r_{\mathcal{F}}-1}$ und ein System von Einheiten wie in Satz 2.5. Die Matrix $\mathcal{N}$ kann dadurch erhalten werden, daß wir die Normen der Erzeuger von U als Potenzprodukt der ϵ_i $(1 \leq i \leq r_{\mathcal{E}} - 1)$ darstellen. Diese Methode läßt sich natürlich auch anwenden, wenn $S_{\mathcal{E}} \supset V_{\mathcal{E}}^{\infty}$ gilt.

Als letzter Schritt in der Berechnung der Einheitengruppe bleibt noch der Aufstieg zu den Fundamentaleinheiten bzw. der Nachweis, daß $(U_{\mathcal{F}} : U) = 1$ gilt. O.B.d.A. nehmen wir von nun $U_{\mathcal{E}} \leq U$ an (ggf. müssen wir U entsprechend erweitern). Mit [55, Algorithmus 4.10] vergrößern wir nun U so, daß U p-maximal für $p|n$ wird. Mit obigem Algorithmus berechnen wir $U_{\mathcal{F}}^{TU_{\mathcal{E}}} \cap U$. Wie im letzten Abschnitt erklärt, können wir nun $U_{\mathcal{F}}^{TU_{\mathcal{E}}}$ bestimmen. Ein Vorteil dieser Methode ist, daß bei den erforderlichen Wurzeltests [55, Algorithmus 4.20] nicht alle Erzeuger von U berücksichtigt werden müssen, sondern „nur“ die von $U_{\mathcal{F}}^{TU_{\mathcal{E}}} \cap U$.

Wenn wir statt $U_{\mathcal{F}}^{TU_{\varepsilon}}$, $U_{\mathcal{F}}^{TU_{\varepsilon}} \cap o$ für eine beliebige Ordnung $o \subseteq o_{\mathcal{F}}$ bestimmen wollen oder an einem Vertretersystem für $U_{\mathcal{F}}^{TU_{\varepsilon}} / U_{\mathcal{F}}^{TU_{\varepsilon}} \cap o$ interessiert sind, so können wir beides mit [55, Algorithmus 4.22] erhalten.

KAPITEL III

Gitter über Zahlkörpern

Für das Lösen von Normgleichungen (wie auch für die algorithmische Behandlung zahlreicher anderer zahlentheoretischer Probleme) sind $\mathbb{Z}$-Gitter, d.h. diskrete additive Untergruppen des $\mathbb{R}^n$, von großer Bedeutung. Vermöge der Minkowskiabbildung [46, 6 (2.6)]

$$\varphi : \mathcal{E} \to \mathbb{R}^m : x \mapsto \begin{pmatrix} x^{(1)} \\ \vdots \\ x^{(r_1)} \\ \sqrt{2}\,\mathrm{Re}(x^{(r_1+1)}) \\ \vdots \\ \sqrt{2}\,\mathrm{Re}(x^{(r_1+r_2)}) \\ \sqrt{2}\,\mathrm{Im}(x^{(r_1+1)}) \\ \vdots \\ \sqrt{2}\,\mathrm{Im}(x^{(r_1+r_2)}) \end{pmatrix}$$

wird der $\mathbb{Z}$-Modul $o_{\mathcal{E}}$ isomorph zu einem Gitter im $\mathbb{R}^m$ vom Rang m.

Auf $\mathcal{E}$ betrachten wir die von

$$\mathrm{T}_2 : \mathcal{E} \to \mathbb{R}_{\geq 0} : x \mapsto \sum_{i=1}^{m} |x^{(i)}|^2$$

induzierte Metrik und auf $\Lambda := \varphi(o_{\mathcal{E}})$ die von dem Skalarprodukt des $\mathbb{R}^m$ induzierte euklidische. Vermöge dieser Abbildung φ kann die von Minkowski begründete „Geometrie der Zahlen“ [41] auf Zahlkörper angewendet werden.

Speziell für das Lösen von Normgleichungen ist es wichtig, daß es sehr effiziente Methoden gibt, um alle $x \in \Lambda$ mit $x^{tr}x \leq c$ $(0 < c \in \mathbb{R})$ zu bestimmen [20, (2.15) Algorithmus].

Im folgenden werden wir nun die Gitterdefinition so verallgemeinern, daß auch Relativordnungen kanonisch mit Gittern identifiziert werden können. Obwohl es verschiedene theoretische Ansätze in der Literatur gibt, Gitter über anderen Strukturen als $\mathbb{Z}$ zu betrachten [8, 11, 17, 29, 39, 47, 54] und geometrische Methoden auf Relativerweiterungen zu übertragen [6], gibt es bisher kaum algorithmische Betrachtungen. Jurk [31] hat in seiner Dissertation eine erste Variante für einen Auszählalgorithmus für Gitter über Zahlkörpern gegeben.

Für diese neuen Gitter werden wir dann geeignete Auszähl- und Reduktionsalgorithmen entwickeln. Teile dieses Kapitels sind bereits in den ANTS-II Proceedings [19] erschienen.

1. Gitter über $\mathbb{Z}$

Wir geben hier einen kurzen Überblick über später verwendete Eigenschaften und Algorithmen für Gitter über $\mathbb{Z}$.

Definition 3.1. *Ein $\mathbb{Z}$-Gitter Λ ist eine diskrete additive Untergruppe des $\mathbb{R}^{n'}$.*

Im weiteren werden wir noch zusätzlich $[\Lambda]_{\mathbb{R}} = \mathbb{R}^{n'}$ fordern, d.h., $\mathbb{Z}$-Gitter sollen vollen Rang haben. Dann gilt der folgende

Satz 3.2. *Sei Λ ein $\mathbb{Z}$-Gitter. Dann gibt es $\alpha_i \in \Lambda$ $(1 \leq i \leq n')$ so, daß $\Lambda = \sum_{i=1}^{n'} \mathbb{Z}\alpha_i$ gilt. Die Elemente $\alpha_1, \dots, \alpha_{n'}$ bilden eine Gitterbasis für Λ.*

Sei nun B ein Skalarprodukt auf dem $\mathbb{R}^{n'}$, $Q(x) := B(x,x)$ die zugehörige quadratische Form. Wenn wir nun eine Gitterbasis $\alpha_1, \dots, \alpha_{n'}$ fixieren, gibt es eine positiv definite Matrix $G \in \mathbb{R}^{n' \times n'}$ mit $B(x,y) = (x_1, \dots, x_{n'})^{tr} G (y_1, \dots, y_{n'})$ $(x = \sum_{i=1}^{n'} x_i\alpha_i,\ y = \sum_{i=1}^{n'} y_i\alpha_i)$, G heißt die Gram-Matrix zu der Gitterbasis α_i $(1 \leq i \leq n')$. $d_{\mathbb{Z}}(\Lambda) := \sqrt{\det(G)}$ ist die Gitterdiskriminante von Λ, sie hängt nicht von der Wahl der speziellen Basis ab.

Seien $\beta_1, \dots, \beta_{n'} \in \Lambda$ linear unabhängig, dann gilt

$$\prod_{i=1}^{n'} Q(\beta_i) \geq d_{\mathbb{Z}}^2(\Lambda).$$

Definition 3.3. *Die Zahlen*

$$M_i := \inf\{\lambda \in \mathbb{R}_{>0} \mid \exists x_1, \dots, x_i \in \Lambda\ \mathbb{Z}\text{-lin. unabh. mit } Q(x_j) \leq \lambda \quad (1 \leq j \leq i)\}$$

$(1 \leq i \leq n')$ heißen die sukzessiven Minima von Λ.

Für die Minima von Λ gilt der folgende

SATZ 3.4. *Seien M_i $(1 \leq i \leq n')$ die sukzessiven Minima von Λ. Dann gilt*

$$\prod_{i=1}^{n'} M_i \leq \gamma_{n'}^{n'} d_{\mathbb{Z}}^2(\Lambda).$$

Wenn wir Berechnungen in einem Gitter anstellen, sind wir normalerweise daran interessiert, eine Gitterbasis aus möglichst kurzen Vektoren (bzgl. Q) zu erhalten. I.allg. ist es nicht möglich, eine Basis aus Vektoren α_i mit $Q(\alpha_i) = M_i$ $(1 \leq i \leq n')$ zu erhalten [46, 3 (3.21)], und es ist sehr aufwendig, eine minimale Basis zu konstruieren. Es gibt jedoch einen in der Praxis sehr schnellen Algorithmus [36, Seite 521] der eine Basis aus „kurzen" Vektoren errechnet, wobei „kurz" heißt: $Q(\alpha_i) \leq 2^{n'} M_i$ $(1 \leq i \leq n')$. Meist ist die so erhaltene Basis jedoch viel besser als diese Abschätzung vermuten läßt, oft gilt sogar $Q(\alpha_i) = M_i$ für $i = 1, 2$.

ALGORITHMUS 3.5 (LLL-ALGORITHMUS).

(Input): *Ein Gitter $\Lambda = \sum_{i=1}^{n'} \mathbb{Z}\alpha_i$.*

(Output): *Eine LLL-reduzierte Basis β_i $(1 \leq i \leq n')$*

(Initialisierung): *Setze $\beta_i \leftarrow \alpha_i$ $(1 \leq i \leq n')$ und berechne für $(1 \leq i \leq n')$ vermöge*

$$\mu_{i,j} \leftarrow B(\beta_i, \beta_j^*) \ (1 \leq j < i)$$

$$\beta_i^* \leftarrow \beta_i - \sum_{j=1}^{i-1} \frac{\mu_{i,j}}{B_j} \beta_j^*, \ B_i \leftarrow B(\beta_i^*, \beta_i^*)$$

die zugehörige Orthogonalbasis.

Setze $k \leftarrow 2$.

(Reduktion): *Für $1 \leq i \leq k$ setze $x \leftarrow \lfloor \mu_{k,i} \rceil$, $\beta_k \leftarrow \beta_k - x\beta_i$ und ändere die $\mu_{k,j}$ $(1 \leq j \leq i)$ entsprechend.*

(LLL-Bedingung): *Falls*

$$B_k + \mu_{k,k-1}^2 B_{k-1} \leq \frac{3}{4} B_{k-1}$$

ist:

(Tausch): *Vertausche β_k und β_{k-1} und ändere die $\mu_{j,l}$ ($j \in \{k-1, k\}, 1 \leq l < j$) und B_j ($j \in \{k-1, k\}$) entsprechend.*

Setze $k \leftarrow \max\{k-1, 2\}$ und gehe nach (Reduktion).

sonst: Setze $k \leftarrow k+1$. Falls $k \leq n'$ ist, gehe nach (Reduktion), *andernfalls terminiere.*

Am Ende dieses Algorithmus gilt:

$$\mu_{i,j}^2 \leq \frac{1}{4} \text{ für } 1 \leq j < i \leq n' \tag{3-1}$$

und

$$Q(\beta_i^*) + \mu_{i,i-1} Q(\beta_{i-1}^*) \geq \frac{3}{4} Q(\beta_{i-1}^*) \tag{3-2}$$

$(2 \leq i \leq n')$.

Die Menge $E := \{x \in \mathbb{R}^{n'} \mid Q(x) \leq c\}$ für ein $c > 0$ ist ein Ellipsoid mit dem Volumen $\operatorname{vol} E = C_{n'} c^{n'} d_{\mathbb{Z}}(\Lambda)$, wobei $C_{n'}$ das Volumen der n'-dimensionalen Einheitskugel ist. Die Menge der Gitterpunkte von E, d.h. $E \cap \Lambda$, kann mit dem Auszählalgorithmus von Fincke und Pohst [20, 21] effektiv bestimmt werden.

Algorithmus 3.6 (Auszählen).

(Input): *Ein Gitter $\Lambda = \sum_{i=1}^{n'} \mathbb{Z}\alpha_i$, eine Grammatrix G und ein $c \in \mathbb{R}_{>0}$.*

(Output): *Alle $x \in \Lambda$ mit $Q(x) \leq c$.*

(Reduktion): *Berechne eine reduzierte Basis $\tilde{\alpha}_i$ ($1 \leq i \leq n'$) für Λ, transformiere G entsprechend.*

(Initialisierung): *Berechne $q_{i,j} \in \mathbb{R}$ mit*

$$Q(x) = Q(x_1, \ldots x_{n'}) = \sum_{i=1}^{n'} q_{i,i}(x_i + \sum_{j=i+1}^{n'} q_{i,j} x_j)^2$$

mittels einer modifizierten Cholesky-Zerlegung von G [20, (2.5) Algorithmus].

Setze $i \leftarrow n'$, $T_i \leftarrow c$ und $M_i = 0$.

(Schleife): *Für alle $x_i \in \mathbb{Z}$ mit $|x_i - M_i| \leq \sqrt{\frac{T_i}{q_{i,i}}}$ führe den folgenden Schritt aus:*

Falls $i = 1$ *ist, gebe* $x = \sum_{j=1}^{n'} x_j \tilde{\alpha}_j$ *aus, andernfalls setze* $i \leftarrow i-1$, $M_i \leftarrow \sum_{j=i}^{n'} q_{i,j} x_j$, $T_i \leftarrow T_{i+1} - q_{i+1,i+1}|x_{i+1} + M_{i+1}|^2$ *und gehe zu* (Schleife).

Falls $i < n'$ *ist, setze* $i \leftarrow i+1$ *und gehe nach* (Schleife), *andernfalls terminiere.*

Fincke hat in [20, 2.15, 5.3] verschiedene Verfahren und Reduktionskriterien für den Schritt (Reduktion) implementiert und verglichen. Als optimal (im Sinne von kurzer Laufzeit) hat sich der LLL-Algorithmus 3.5, angewendet auf die duale Basis, herausgestellt.

Für weitere Anwendungen notieren wir noch die folgende Definition: Ein Simplex $S \subseteq \mathbb{R}^{n'}$ ist eine Menge, die durch endlich viele lineare Ungleichungen definiert wird, d.h. sei $A \in \mathbb{R}^{n' \times k}$ eine Matrix, und $b \in \mathbb{R}^k$ ein Vektor, dann ist

$$S := \{x \in \mathbb{R}^{n'} \mid \forall 1 \leq j \leq k : \sum_{i=1}^{n'} a_{i,j} x_i \leq b_j\}$$

ein Simplex. Später werden nur beschränkte Simplizes interessieren.

2. Gitter über $o_{\mathcal{E}}$

Wenn wir statt $\mathbb{Z}$ als Koeffizientenbereich eine Ordnung $o \subset \mathcal{E}$ zulassen wollen, entsteht das Problem, daß $o = o^{(1)}$ aufgefaßt als Teilmenge von $\mathcal{E}^{(1)} \subset \mathbb{C}$ nicht mehr diskret ist.

Im folgenden werden wir uns o und $\mathcal{E}$ daher immer als Teilmenge von $\mathcal{E} \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} =: K$ vorstellen. O.B.d.A. sei $(x \otimes 1)_i = x^{(i)}$ für $(1 \leq i \leq r_1 + r_2)$. Auf K werden alle Operationen $(+, -, \cdot, /, \overline{(\,\cdot\,)})$ komponentenweise durchgeführt. Ferner definieren wir die beiden folgenden Funktionen:

$$\tau : K \to \mathbb{R} : x = (x_1, \ldots, x_{r_1+r_2}) \mapsto \sum_{i=1}^{r_1} x_i + 2\sum_{i=1}^{r_2} \mathrm{Re}(x_{r_1+i})$$

und

$$\eta : K \to \mathbb{R} : x \mapsto \prod_{i=1}^{r_1} |x_i| \prod_{i=r_1+1}^{r_1+r_2} |x_i|^2.$$

Damit ist $\varphi(o) = \Lambda$ isometrisch zu $o \otimes 1$ mit der von $x \mapsto \tau(\overline{x \otimes 1} \cdot x \otimes 1)$ induzierten Metrik.

Wir schreiben $K \ni x > 0$, falls $x_i > 0$ $(1 \leq i \leq r_1 + r_2)$ gilt.

Für η und τ besteht die Ungleichung zwischen geometrischem und arithmetischem Mittel: Sei $0 < x \in K$, dann gilt:

$$\sqrt[m]{\eta(x)} \leq \frac{\tau(x)}{m}. \tag{3-3}$$

DEFINITION 3.7. *Sei $G = (g_{k,l})_{\substack{1\leq k\leq n'\\ 1\leq l\leq m'}} \in K^{n'\times m'}$ eine Matrix. Wir definieren*

$$G^* := (g^*_{k,l})_{\substack{1\leq k\leq n'\\ 1\leq l\leq m'}} := \begin{cases} ((g_{l,k})_i)_{\substack{1\leq l\leq m'\\ 1\leq k\leq n'}} & 1 \leq i \leq r_1 \\ \overline{((g_{l,k})_i)}_{\substack{1\leq l\leq m'\\ 1\leq k\leq n'}} & r_1+1 \leq i \leq r_1+r_2 \end{cases}.$$

G heißt symmetrisch, wenn $G = G^*$ gilt. Die Matrix $G \in K^{n'\times n'}$ heißt positiv definit, wenn für jedes $x \in K^{n'} \setminus \{0\}$

$$x^*Gx > 0$$

gilt.

Für Matrizen $G \in K^{n'\times n'}$ gilt eine Verallgemeinerung des Minkowski'schen Linearformensatzes [29]:

SATZ 3.8. *Sei $G \in K^{n'\times n'}$. Dann gibt es ein $0 \neq x \in o_{\mathcal{E}}^{n'}$ so, daß*

$$|G(x\otimes 1)| \leq \sqrt[n'm]{\eta\circ\det(G)}\,\sqrt[2m]{|d_{\mathcal{E}}|}$$

gilt.

Jede symmetrische, positiv definite Matrix $G \in K^{n'\times n'}$ definiert eine anti-hermite'sche und eine quadratische Form auf $K^{n'}$ mittels:

$$B := B_G : K^{n'} \times K^{n'} \to K : (x,y) \mapsto x^*Gy$$

und

$$Q := Q_G : K^{n'} \to \mathbb{R}_{\geq 0}^{r_1+r_2} \subset K : x \mapsto B(x,x).$$

Für $x, y \in \mathcal{E}^{n'}$ setzen wir zur Abkürzung $B(x,y) := B(x\otimes 1, y\otimes 1)$ und $Q(x) := Q(x\otimes 1)$.

Nun sind wir in der Lage, Gitter über $\mathcal{E}$ zu definieren:

DEFINITION 3.9. *Sei $o \subset \mathcal{E}$ eine Ordnung. Ein o-Modul $\Lambda \subset \mathcal{E}^{n'}$ mit $[\Lambda]_{\mathcal{E}} = \mathcal{E}^{n'}$ zusammen mit einer symmetrischen, positiv definiten Matrix $G \in K^{n'\times n'}$ heißt Gitter vom Rang n' über o (kurz: Gitter), wenn Λ in der von $\tau\circ Q_G$ induzierten Metrik diskret ist.*

BEISPIEL 3.10. (1) *Das wichtigste Beispiel für Gitter ist $o_{\mathcal{F}}$ zusammen mit der (gewichteten) relativen* $\mathrm{T}_2^{\mathcal{F}/\mathcal{E}}$*-Norm*

$$\mathrm{T}_2^{\mathcal{F}/\mathcal{E}} : \mathcal{F} \to \mathbb{R}_{\geq 0}^{r_1+r_2} : x \mapsto (\sum_{j=1}^{n} w_{i,j}|x^{(i,j)}|^2)_{1\leq i\leq r_1+r_2}$$

(mit $w_{i,j} > 0$). In [31, Abschnitt 3.1] *hat Jurk nachgewiesen, daß* $\mathrm{T}_2^{\mathcal{F}/\mathcal{E}}$ *eine positiv definite quadratische Form ist, mit der $o_{\mathcal{F}}$ zu einem $o_{\mathcal{E}}$-Gitter wird.*

(2) *Jedes Ideal $\mathfrak{b} \subset \mathcal{F}$ bildet zusammen mit* $\mathrm{T}_2^{\mathcal{F}/\mathcal{E}}$ *ein $o_{\mathcal{E}}$-Gitter.*

Wie im Fall von $\mathbb{Z}$-Gittern liefert die Parallelogrammgleichung die Äquivalenz von positiv definiten quadratischen Formen und positiv definiten symmetrischen Bilinearformen.

Für Gitter über der Maximalordnung $o_{\mathcal{E}}$ gibt es die folgende Darstellung:

SATZ 3.11. *Sei Λ ein Gitter vom Rang n' über $o_{\mathcal{E}}$ mit quadratischer Form Q. Dann existieren (gebrochene) Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n'}$ von $o_{\mathcal{E}}$, $\alpha_1, \ldots, \alpha_{n'} \in \mathcal{E}^{n'}$ sowie $G \in K^{n' \times n'}$ so, daß*

$$\Lambda = \sum_{i=1}^{n'} \mathfrak{a}_i \alpha_i \text{ und } Q = Q_G$$

gelten.

BEWEIS. [43, 81:3] oder [47, Theorem 1]. □

Analog zu [13] nennen wir $(\mathfrak{a}_i, \alpha_i)_{i\leq i\leq n'}$ eine Pseudobasis für Λ.

BEMERKUNG 3.12. (1) *Jedes Gitter über o ist in kanonischer Weise ein Gitter über $\mathbb{Z}$ vom Rang mn' mit $\tau \circ Q_G$ als quadratischer Form.*

(2) *Unsere Definition für Gitter ist identisch mit der in* [54] *gegebenen. Sie unterscheidet sich jedoch von der in* [47]*, da unsere Gitter nicht notwendig frei sind, wie wir später sehen werden.*

(3) *In* [47] *zeigen Rogers und Swinnerton-Dyer sogar eine stärkere Aussage als die in* Satz 3.11 *angegebene. Sie zeigen, daß jedes Gitter eine „fast freie" Darstellung hat, d.h., es ist möglich $\mathfrak{a}_1 = \ldots = \mathfrak{a}_{n'-1} = o_{\mathcal{E}}$ zu wählen. Wir werden später nochmals hierauf eingehen.*

(4) *I.allg. können wir entweder die Ideale als ganze Ideale wählen oder fordern, daß $\alpha_i \in \Lambda$ $(1 \leq i \leq n')$ gilt.*

(5) *Für jede Pseudobasis $(\mathfrak{a}_i, \alpha_i)_{1\leq i\leq n'}$ bildet die Menge $\{\alpha_i \mid 1 \leq i \leq n'\}$ eine Basis des $\mathcal{E}^{n'}$.*

(6) *Es gibt effiziente Algorithmen, die aus einem $o_{\mathcal{E}}$-Erzeugendensystem eine Pseudobasis ausrechnen* [7, 13, 28].

Im folgenden werden wir uns ausschließlich mit Gittern über der Maximalordnung beschäftigen. Die meisten Ergebnisse gelten jedoch für jedes Gitter (jeden o-Modul), mit einer Pseudobasis.

Über das Transformationsverhalten der Pseudobasen gibt der folgende Satz ([43, 81:7,81:8]) Auskunft:

SATZ 3.13. *Seien $(\mathfrak{a}_i, \alpha_i)_{1\le i\le n'}$ und $(\mathfrak{b}_i, \beta_i)_{1\le i\le n'}$ Pseudobasen für die Gitter Λ und Λ'. Für die Transformationsmatrix $T = (t_{l,k})_{\substack{1\le l\le n'\\ 1\le k\le n'}} \in \mathrm{GL}(n', \mathcal{E})$ mit $\alpha_i T = \beta_i$ $(1 \le i \le n')$ gilt:*

$$t_{l,k} \in \mathfrak{a}_l \mathfrak{b}_k^{-1} \iff \Lambda' \subseteq \Lambda.$$

Für $\Lambda' \subseteq \Lambda$ gilt zusätzlich:

$$\prod_{i=1}^{n'} \mathfrak{a}_i = \det(T) \prod_{i=1}^{n'} \mathfrak{b}_i \iff \Lambda' = \Lambda.$$

DEFINITION 3.14. *Seien Λ ein Gitter und $(\mathfrak{a}_i, \alpha_i)_{1\le i\le n'}$ eine Pseudobasis. Die nach* Satz 3.13 *eindeutig bestimmte Idealklasse $\prod_{i=1}^{n'} \mathfrak{a}_i$ heißt die Steinitzklasse* $\mathrm{St}(\Lambda)$ *von Λ.*

Im folgenden werden wir einige Eigenschaften der Pseudobasen auflisten, die wir später benötigen werden:

LEMMA 3.15. *Sei Λ ein Gitter. Dann gelten:*

(1) *Sei $(\mathfrak{a}_i, \alpha_i)_{1\le i\le n'}$ eine Pseudobasis für Λ sowie $x = \sum_{i=1}^{n'} \mu_i\alpha_i$ ein beliebiger Vektor des $\mathcal{E}^{n'}$. Setze*

$$\mathfrak{a}_{x,\Lambda} := \{\mu \in \mathcal{E} \mid \mu x \in \Lambda\}.$$

Dann ist $\mathfrak{a}_{x,\Lambda}$ ein Ideal, und es gilt:

$$\mathfrak{a}_{x,\Lambda} = \bigcap_{\substack{1\le i\le n'\\ \mu_i\ne 0}} \frac{\mathfrak{a}_i}{\mu_i}.$$

$\mathfrak{a}_{x,\Lambda}$ heißt das Koeffizientenideal zu x in Λ.

(2) *Sei $\beta_1, \dots, \beta_{n'}$ eine Basis des $\mathcal{E}^{n'}$. Dann gibt es eine hierzu adaptierte Pseudobasis $(\mathfrak{a}_i, \alpha_i)_{1\le i\le n'}$, d.h. $\alpha_i \in [\beta_1, \dots, \beta_i]_{\mathcal{E}}$.*

BEWEIS. [43, 81:4,81:3] $\square$

Die in einer Pseudobasis auftretenden Ideale sind in (fast) keiner Weise eindeutig, wie der nächste Satz zeigt:

LEMMA 3.16. (1) *Seien* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *Ideale von* $o_{\mathcal{E}}$. *Dann gibt es* $\alpha, \beta \in \mathcal{E}$ *so, daß* $\mathfrak{c} = \alpha\mathfrak{a} + \beta\mathfrak{b}$ *gilt.*

(2) *Sei* $\Lambda = \mathfrak{b}_1\beta_1 + \mathfrak{b}_2\beta_2 \subset \mathcal{E}^n$ *mit Idealen* $\mathfrak{a}$, $\mathfrak{b} \subset \mathcal{E}$ *und* β_1, $\beta_2 \in \mathcal{E}^{n'}$. *Ferner seien Ideale* $\mathfrak{a}_1$ *und* $\mathfrak{a}_2 \subset \mathcal{E}$ *mit* $\mathrm{cl}(\mathfrak{a}_1\mathfrak{a}_2) = \mathrm{cl}(\mathfrak{b}_1\mathfrak{b}_2)$ *gegeben. Dann gibt es* α_1 *und* $\alpha_2 \in \mathcal{E}^n$ *so, daß* $\Lambda = \mathfrak{a}_1\alpha_1 + \mathfrak{a}_2\alpha_2$ *gilt.*

BEWEIS. (1): Konsequenz aus dem schwachem Approximationssatz [43, 22:5].

(2): Zunächst können wir o.B.d.A. annehmen, daß $\mathrm{cl}(\mathfrak{b}_1) \neq \mathrm{cl}(\mathfrak{a}_1) \neq \mathrm{cl}(\mathfrak{b}_2)$ gilt, da andernfalls die Aussage trivial ist. Nach (1) gibt es $\mu_1, \mu_2 \in \mathcal{E}$ mit $\mathfrak{a}_1^{-1} = \mu_1\mathfrak{b}_1^{-1} + \mu_2\mathfrak{b}_2^{-1}$. Setze $\alpha_1 := \mu_1\beta_1 + \mu_2\beta_2$. Für das zugehörige Koeffizientenideal gilt dann nach Lemma 3.15.(1):

$$\mathfrak{a}_{\alpha_1,\Lambda} = \frac{\mathfrak{b}_1}{\mu_1} \cap \frac{\mathfrak{b}_2}{\mu_2} = (\mu_1\mathfrak{b}_1^{-1} + \mu_2\mathfrak{b}_2^{-1})^{-1} = (\mathfrak{a}_1^{-1})^{-1}.$$

Nun ergänzen wir $\{\alpha_1\}$ mit einem beliebigen $\mathcal{E}$-linear unabhängigen $\alpha_2' \in \mathcal{E}^n$ zu einer Basis von $\mathcal{E}\beta_1 + \mathcal{E}\beta_2$. Nach Lemma 3.15.(2) gibt es eine Pseudobasis $((\mathfrak{a}_1', \alpha_1'), (\mathfrak{a}_2', \alpha_2''))$. Wegen $\alpha_1' = \mu\alpha_1$ und der Eindeutigkeit der Darstellung gilt $\mathfrak{a}_1' = \mathfrak{a}_1/\mu$, womit

$$\mathrm{cl}(\mathfrak{a}_1\mathfrak{a}_2') = \mathrm{cl}(\mathfrak{a}_1'\mathfrak{a}_2') = \mathrm{cl}(\mathfrak{b}_1\mathfrak{b}_2) = \mathrm{cl}(\mathfrak{a}_1\mathfrak{a}_2)$$

und schließlich $\mathfrak{a}_2' = \mu'\mathfrak{a}_2$ folgen. Somit gilt $\Lambda = \mathfrak{a}_1\alpha_1 + \mathfrak{a}_2\alpha_2$ mit $\alpha_2 := \alpha_2''/\mu'$. □

SATZ 3.17. *Seien* Λ *ein Gitter über* $o_{\mathcal{E}}$ *und* $\mathfrak{a}_1, \dots, \mathfrak{a}_{n'}$ *Ideale von* $o_{\mathcal{E}}$ *mit*

$$\mathrm{cl}(\prod_{i=1}^{n'} \mathfrak{a}_i) = \mathrm{St}(\Lambda).$$

Dann gibt es eine Basis $\alpha_1, \dots, \alpha_{n'}$ *von* $\mathcal{E}^{n'}$ *so, daß* $(\mathfrak{a}_i, \alpha_i)_{1 \le i \le n'}$ *eine Pseudobasis von* Λ *ist.*

BEWEIS. Der Beweis verläuft analog [43, 81 C]:

Sei $(\mathfrak{b}_i, \beta_i)_{1 \le i \le n'}$ eine Pseudobasis. In einem ersten Schritt ändern wir die Ideale sukzessive zu einer fast freien Darstellung; in einem zweiten Schritt erhalten wir dann die gewünschte Darstellung:

$$
\begin{array}{rcl}
\Lambda & = & \mathfrak{b}_1\beta_1 + \cdots + \mathfrak{b}_{n'}\beta_{n'} \\
& \overset{3.16.(2)}{=} & o_{\mathcal{E}}\beta_1' + \mathfrak{b}_1\mathfrak{b}_2\beta_2' + \sum_{i=2}^{n'} \mathfrak{b}_i\beta_i \\
& = & \ldots \\
& = & \sum_{i=1}^{n'-1} o_{\mathcal{E}}\beta_i'' + \prod_{i=1}^{n'} \mathfrak{b}_i\beta_{n'}'' \\
& \overset{3.16.(2)}{=} & \sum_{i=1}^{n'-2} o_{\mathcal{E}}\beta_i'' + \prod_{i=1}^{n'} \mathfrak{b}_i\mathfrak{a}_{n'}^{-1}\beta_{n'-1}''' + \mathfrak{a}_{n'}\beta_{n'}''' \\
& = & \prod_{i=1}^{n'} \mathfrak{b}_i \prod_{i=1}^{n'-1} \mathfrak{a}_i^{-1}\beta_1''' + \sum_{i=2}^{n'} \mathfrak{a}_i\beta_i'''.
\end{array}
$$

Da $\mathrm{cl}(\prod_{i=1}^{n'} \mathfrak{b}_i) = \mathrm{cl}(\prod_{i=1}^{n'} \mathfrak{a}_i)$ gilt, gibt es ein $\mu \in \mathcal{E}$ mit:

$$
\Lambda \quad = \quad \mu\mathfrak{a}_1\beta_1''' + \sum_{i=2}^{n'} \mathfrak{a}_i\beta_i'''. \quad \square
$$

Da mit Hilfe von [13, Proposition 1.1.] Lemma 3.16.(1) konstruktiv bewiesen werden kann, haben wir einen Algorithmus, der eine beliebige Pseudobasis in eine Pseudobasis mit von uns vorgegebenen Idealen überführt. In der Praxis hat die fast freie Darstellung jedoch keine Vorteile gegenüber einer beliebigen Pseudobasis, da die Erzeuger i.allg. wesentlich schlechter konditioniert sind.

Der Satz zeigt außer der Existenz einer fast freien Darstellung auch noch, daß ein Gitter genau dann frei (über $o_{\mathcal{E}}$) ist, wenn $\mathrm{St}(\Lambda)$ trivial ist.

Definition 3.18. *Sei Λ ein Gitter mit zugehöriger Matrix $G \in K^{n' \times n'}$. Die Zahl*

$$
d(\Lambda) := \sqrt{\eta \circ \det(G)} \prod_{i=1}^{n'} N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{a}_i) |d_E|^{n'/2}
$$

heißt (Gitter-)Diskriminante von Λ.

Lemma 3.19. *Wenn wir Λ wie in* Bemerkung 3.12.(1) *als Gitter über $\mathbb{Z}$ auffassen, gilt $d_{\mathbb{Z}}(\Lambda) = d(\Lambda)$.*

Beweis. Mit Hilfe der Parallelogrammgleichung folgt zunächst $B_{\mathbb{Z}} = \tau \circ B$. Sei $\Lambda = \sum_{i=1}^{n'} \mathfrak{a}_i \alpha_i$, $\mathcal{E} \supset \mathfrak{a}_i = \sum_{j=1}^{m} a_j^i \mathbb{Z}$ und $a_j^i = \sum_{k=1}^{m} a_{j,k}^i \omega_k$ mit einer $\mathbb{Z}$-Basis $\omega_1, \dots, \omega_m$ für $o_{\mathcal{E}}$ und $a_{j,k}^i \in \mathbb{Q}$ $(1 \leq i \leq n',\ 1 \leq j,k \leq m)$. Eine $\mathbb{Z}$-Basis für Λ erhalten wir daher mit

$$\{a_j^i \alpha_i \mid 1 \leq i \leq n', 1 \leq j \leq m\}.$$

Bei geeigneter Anordnung der Basiselemente hat die ($\mathbb{Z}$-)Grammatrix daher die folgende Gestalt:

$$\begin{aligned} G_{\mathbb{Z}} &= \begin{pmatrix} \tau\circ B(a_1^1\alpha_1, a_1^1\alpha_1) & \cdots & \tau\circ B(a_m^1\alpha_1, a_1^1\alpha_1) & \tau\circ B(a_1^2\alpha_2, a_1^1\alpha_1) & \cdots & \tau\circ B(a_m^{n'}\alpha_{n'}, a_1^1\alpha_1) \\ \vdots & & \vdots & \vdots & & \vdots \\ \tau\circ B(a_1^1\alpha_1, a_m^1\alpha_1) & \cdots & \tau\circ B(a_m^1\alpha_1, a_m^1\alpha_1) & \tau\circ B(a_1^2\alpha_2, a_m^1\alpha_1) & \cdots & \tau\circ B(a_m^{n'}\alpha_{n'}, a_m^1\alpha_1) \\ \tau\circ B(a_1^1\alpha_1, a_1^2\alpha_2) & \cdots & \tau\circ B(a_m^1\alpha_1, a_1^2\alpha_2) & \tau\circ B(a_1^2\alpha_2, a_1^2\alpha_2) & \cdots & \tau\circ B(a_m^{n'}\alpha_{n'}, a_1^2\alpha_2) \\ \vdots & & \vdots & \vdots & & \vdots \\ \tau\circ B(a_1^1\alpha_1, a_m^{n'}\alpha_{n'}) & \cdots & \tau\circ B(a_m^1\alpha_1, a_m^{n'}\alpha_{n'}) & \tau\circ B(a_1^2\alpha_2, a_m^{n'}\alpha_{n'}) & \cdots & \tau\circ B(a_m^{n'}\alpha_{n'}, a_m^{n'}\alpha_{n'}) \end{pmatrix} \\ &= \begin{pmatrix} \tau(\overline{a}_1^1 a_1^1 G_{1,1}) & \cdots & \tau(\overline{a}_m^1 a_1^1 G_{1,1}) & \tau(\overline{a}_1^2 a_1^1 G_{2,1}) & \cdots & \tau(\overline{a}_m^{n'} a_1^1 G_{n',1}) \\ \vdots & & \vdots & \vdots & & \vdots \\ \tau(\overline{a}_1^1 a_m^1 G_{1,1}) & \cdots & \tau(\overline{a}_m^1 a_m^1 G_{1,1}) & \tau(\overline{a}_1^2 a_m^1 G_{2,1}) & \cdots & \tau(\overline{a}_m^{n'} a_m^1 G_{n',1}) \\ \tau(\overline{a}_1^1 a_1^2 G_{1,2}) & \cdots & \tau(\overline{a}_m^1 a_1^2 G_{1,2}) & \tau(\overline{a}_1^2 a_1^2 G_{2,2}) & \cdots & \tau(\overline{a}_m^{n'} a_1^2 G_{n',2}) \\ \vdots & & \vdots & \vdots & & \vdots \\ \tau(\overline{a}_1^1 a_m^{n'} G_{1,n'}) & \cdots & \tau(\overline{a}_m^1 a_m^{n'} G_{1,n'}) & \tau(\overline{a}_1^2 a_m^{n'} G_{2,n'}) & \cdots & \tau(\overline{a}_m^{n'} a_m^{n'} G_{n',n'}) \end{pmatrix}. \end{aligned}$$

Sei nun $A_1 \in K^{n' \times n'}$ beliebig mit $G = A_1^* A_1$. Dann gilt:

$$A_2 := \begin{pmatrix} (a_1^1(A_1)_{1,1})_1 & \cdots & (a_m^1(A_1)_{1,1})_1 & (a_1^2(A_1)_{1,2})_1 & \cdots & (a_m^{n'}(A_1)_{1,n'})_1 \\ \vdots & & \vdots & \vdots & & \vdots \\ (a_1^1(A_1)_{1,1})_{r_1+r_2} & \cdots & (a_m^1(A_1)_{1,1})_{r_1+r_2} & (a_1^2(A_1)_{1,2})_{r_1+r_2} & \cdots & (a_m^{n'}(A_1)_{1,n'})_{r_1+r_2} \\ (a_1^1(A_1)_{2,1})_{r_1+r_2} & \cdots & (a_m^1(A_1)_{2,1})_{r_1+r_2} & (a_1^2(A_1)_{2,2})_{r_1+r_2} & \cdots & (a_m^{n'}(A_1)_{2,n'})_{r_1+r_2} \\ \vdots & & \vdots & \vdots & & \vdots \\ (a_1^1(A_1)_{n',1})_{r_1+r_2} & \cdots & (a_m^1(A_1)_{n',1})_{r_1+r_2} & (a_1^2(A_1)_{n',2})_{r_1+r_2} & \cdots & (a_m^{n'}(A_1)_{n',n})_{r_1+r_2} \\ \overline{(a_1^1(A_1)_{1,1})}_{r_1+1} & \cdots & \overline{(a_m^1(A_1)_{1,1})}_{r_1+1} & \overline{(a_1^2(A_1)_{1,2})}_{r_1+1} & \cdots & \overline{(a_m^{n'}(A_1)_{1,n'})}_{r_1+1} \\ \vdots & & \vdots & \vdots & & \vdots \\ \overline{(a_1^1(A_1)_{n',1})}_{r_1+r_2} & \cdots & \overline{(a_m^1(A_1)_{n',1})}_{r_1+r_2} & \overline{(a_1^2(A_1)_{n',2})}_{r_1+r_2} & \cdots & \overline{(a_m^{n'}(A_1)_{n',n})}_{r_1+r_2} \end{pmatrix}$$

$$
= \begin{pmatrix}
(\omega_1(A_1)_{1,1})_1 & \cdots & (\omega_m(A_1)_{1,1})_1 & (\omega_1(A_1)_{1,2})_1 & \cdots & (\omega_m(A_1)_{1,n'})_1 \\
\vdots & & \vdots & \vdots & & \vdots \\
(\omega_1(A_1)_{1,1})_{r_1+r_2} & \cdots & (\omega_m(A_1)_{1,1})_{r_1+r_2} & (\omega_1(A_1)_{1,2})_{r_1+r_2} & \cdots & (\omega_m(A_1)_{1,n'})_{r_1+r_2} \\
(\omega_1(A_1)_{2,1})_{r_1+r_2} & \cdots & (\omega_m(A_1)_{2,1})_{r_1+r_2} & (\omega_1(A_1)_{2,2})_{r_1+r_2} & \cdots & (\omega_m(A_1)_{2,n'})_{r_1+r_2} \\
\vdots & & \vdots & \vdots & & \vdots \\
(\omega_1(A_1)_{n',1})_{r_1+r_2} & \cdots & (\omega_m(A_1)_{n',1})_{r_1+r_2} & (\omega_1(A_1)_{n',2})_{r_1+r_2} & \cdots & (\omega_m(A_1)_{n',n})_{r_1+r_2} \\
\overline{(\omega_1(A_1)_{1,1})}_{r_1+1} & \cdots & \overline{(\omega_m(A_1)_{1,1})}_{r_1+1} & \overline{(\omega_1(A_1)_{1,2})}_{r_1+1} & \cdots & \overline{(\omega_m(A_1)_{1,n'})}_{r_1+1} \\
\vdots & & \vdots & \vdots & & \vdots \\
\overline{(\omega_1(A_1)_{n',1})}_{r_1+r_2} & \cdots & \overline{(\omega_m(A_1)_{n',1})}_{r_1+r_2} & \overline{(\omega_1(A_1)_{n',2})}_{r_1+r_2} & \cdots & \overline{(\omega_m(A_1)_{n',n'})}_{r_1+r_2}
\end{pmatrix}
$$

$$
\begin{pmatrix}
a^1_{1,1} & \cdots & a^1_{m,1} & & & & \\
\vdots & & \vdots & & & & \\
a^1_{1,m} & \cdots & a^1_{m,m} & & & & \\
& & & \ddots & & & \\
& & & & a^{n'}_{1,1} & \cdots & a^{n'}_{m,1} \\
& & & & \vdots & & \vdots \\
& & & & a^{n'}_{1,m} & \cdots & a^{n'}_{m,m}
\end{pmatrix}
$$

$$
=: \quad A_3 A_4
$$

Analog [29, Seite 277] folgt nun: $\det(A_3) = \eta \circ \det(A_1)|d_{\mathcal{E}}|^{n'}$. Offenbar gilt $\det(A_4) = \prod_{i=1}^{n'} N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{a}_i)$. Aus $d_{\mathbb{Z}}(\Lambda) = \sqrt{\det(G_{\mathbb{Z}})}$ und $G_{\mathbb{Z}} = A_2^* A_2$ folgt nun die Behauptung. $\square$

Definition 3.20. *Seien Λ ein Gitter und $G \in K^{n' \times n'}$ die zugehörige Matrix. Die Zahlen*

$$
\lambda_i := \min\{\lambda \in \mathbb{R}_{>0} \mid \exists x_1, \ldots, x_i \in \Lambda \ \mathcal{E}\text{-lin. unabhängig} : \eta \circ Q_G(x_i) \leq \lambda\}
$$

($1 \leq i \leq n'$) heißen die sukzessiven Minima von Λ.

Es gilt der folgende Satz (vgl. [46, 3 (3.34),(3.37)], [39, Theorem 5, 6]):

Satz 3.21. *Sei Λ ein Gitter, $G \in K^{n \times n}$ die zugehörige Matrix und $\lambda_1 \leq \ldots \leq \lambda_{n'}$ die sukzessiven Minima. Dann gilt:*

$$
m^m \eta \circ \det(G) \prod_{i=1}^{n'} N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{a}_i) \leq (\prod_{i=1}^{n'} \lambda_i)^m \leq 2^{mn'} \frac{d_\Lambda}{d_{\mathcal{E}}^{n'}}.
$$

Beweis. Seien $x_1, \ldots, x_{n'} \in \Lambda$ unabhängig mit $\tau \circ Q(x_i) = \lambda_i$. Für das hiervon aufgespannte freie Teilgitter $\Lambda' = \sum_{i=1}^{n'} o_{\mathcal{E}} x_i$ von Λ gilt $d'_\Lambda \geq d_\Lambda$. Mit Hilfe der

Hadamard'schen Ungleichung $\det G_i \leq \prod_{j=1}^{n'} Q(x_j)_i$ folgt dann:

$$\eta \circ \det(G') \leq \eta \prod_{j=1}^{n'} Q'(x_j)_i \leq (\frac{1}{m} \prod_{j=1}^{n'} \tau \circ Q'(x_j))^m$$

und damit die behauptete untere Schranke.

Die obere Schranke folgt aus [39, Seite 19]. □

3. Auszählalgorithmen für $o_\mathcal{E}$-Gitter

Für $\mathbb{Z}$-Gitter sind zwei der wichtigsten Algorithmen die Bestimmung aller Punkte in einer Ellipse (Algorithmus 3.6) und LLL-Reduktion (Algorithmus 3.5) der Gitterbasis. Diese werden in diesem und dem nächsten Abschnitt auf Gitter über Zahlkörpern verallgemeinert.

Zunächst werden wir uns mit dem „Auszählen“ beschäftigen. Gegeben ist das folgende Problem: Sei Λ ein Gitter über $o_\mathcal{E}$, $Q = Q_G$ die zugehörige quadratische Form. Für ein beliebiges $c \in \mathbb{R}_{>0}^{r_1+r_2}$ bestimme alle $x \in \Lambda$ mit $Q(x) \leq c$. Im Falle von Gittern über $\mathbb{Z}$ wird dies i.allg. mit dem von Fincke [20] entwickelten Auszählalgorithmus 3.6 gelöst; für freie Gitter über Zahlkörpern hat Jurk [31] diesen Algorithmus übertragen. Um ihn angeben zu können, benötigen wir ein vorbereitendes Lemma:

LEMMA 3.22. *Sei $A \in \mathbb{R}^{n' \times n'}$ ($A \in \mathbb{C}^{n' \times n'}$) eine symmetrische (hermitesche) positiv definite Matrix. Dann existieren $0 < q_{i,i} \in \mathbb{R}$ ($1 \leq i \leq n'$) sowie $q_{i,j} \in \mathbb{R}$ ($q_{i,j} \in \mathbb{C}$) ($1 \leq i < j \leq n'$) so, daß für jedes $x \in \mathbb{R}^{n'}$ ($x \in \mathbb{C}^{n'}$)*

$$x^* A x = \sum_{i=1}^{n'} q_{i,i} |x_i + \sum_{j=i+1}^{n'} q_{i,j} x_j|^2$$

gilt.

BEWEIS. Für den reellen Fall siehe [20, (2.5) Algorithmus], für den komplexen: [31, Satz 3.6]. □

Der Beweis liefert in beiden Fällen einen elementaren Algorithmus, der die „quadratische Ergänzung“ durchführt. Wir erhalten so auch leicht eine Zerlegung von $A = R^* R$ als Produkt zweier Dreiecksmatrizen, die Cholesky-Zerlegung.

Nun können wir den Auszählalgorithmus formulieren:

ALGORITHMUS 3.23 (AUSZÄHLEN).

(Input): *Ein mittels einer Pseudobasis* $(\mathfrak{a}_i, \alpha_i)_{1 \le i \le n'}$ *gegebenes Gitter mit quadratischer Form* $Q = Q_G$ *sowie ein* $c \in \mathbb{R}_{>0}^{r_1+r_2}$.

(Output): *Alle* $x \in \Lambda$ *mit* $Q(x) \le c$.

(Quadratische Ergänzung): *Berechne* $q_{i,i} \in \mathbb{R}_{>0}^{r_1+r_2}$ *(*$1 \le i \le n'$*) und* $q_{i,j} \in K$ *(*$1 \le i < j \le n'$*) gemäß* Lemma 3.22.

(Initialisierung): *Setze* $i \leftarrow n'$, $T_i \leftarrow c$ *und* $M_i \leftarrow 0 \in K$.

(Auszählen eines Koeffizienten): *Setze*

$$K_i \leftarrow \{x \in \mathfrak{a}_i \mid |(x \otimes 1) - M_i| \le \sqrt{\frac{T_i}{q_{i,i}}}\}.$$

(Schleife): *Falls* $K_i \neq \emptyset$, *gehe zu* (Nächstes Element), *andernfalls setze* $i \leftarrow i+1$.

Falls $i = n'$ *ist, beende den Algorithmus, andernfalls setze* $i \leftarrow i+1$ *und gehe zu* (Schleife).

(Nächstes Element): *Wähle ein beliebiges* $x_i \in K_i$ *und entferne es aus* K_i.

Falls $i = 1$ *ist, gebe* $(x_1, \dots, x_{n'})$ *aus und gehe zu* (Schleife), *andernfalls setze* $i \leftarrow i-1$, $M_i \leftarrow \sum_{l=i+1}^{n'} q_{i,l}(x_l \otimes 1)$, $T_i \leftarrow T_{i+1} - q_{i+1,i+1}|(x_{i+1} \otimes 1) + M_{i+1}|^2$ *und gehe zu* (Auszählen eines Koeffizienten).

Die Korrektheit dieses Algorithmus folgt sofort aus Lemma 3.22. Der Algorithmus kann auf dieselbe Art beschleunigt werden wie im absoluten Fall: Da die gesuchte Menge, eingebettet in den $K^{n'}$, symmetrisch zu allen Achsen liegt, kann der Algorithmus so geändert werden, daß nur die Hälfte der Punkte tatsächlich ausgezählt wird. Im Unterschied zum absoluten Auszählen müssen dann jedoch die Mengen K_i richtig angeordnet werden. Ebenfalls wie beim absoluten Verfahren können die Werte $Q(x)$ leicht mitberechnet werden, es gilt $Q(x_1, \dots, x_{n'}) = c - T_1 + q_{1,1}|(x_1 \otimes 1) + M_1|^2$.

Es bleibt noch zu zeigen, wie der Schritt (Auszählen eines Koeffizienten) effektiv algorithmisch zu lösen ist. Da $\mathfrak{a}_i \otimes 1$ in kanonischer Weise ein Gitter ist, können wir zwei Methoden sofort angeben: Wir können, wie von Jurk vorgeschlagen, mittels dualer Gitterbasen die Koeffizienten beschränken, was bedeutet, statt K_i einen genügend großen achsenparallelen Quader auszuzählen. Oder wir können K_i in eine um M_i zentrierte Ellipse einbetten. Es besteht jedoch, wie wir zeigen werden, die Möglichkeit, K_i direkt auszuzählen, oder einen genügend großen Simplex zu betrachten.

Bevor wir nun fortfahren, die einzelnen Methoden detailliert darzustellen, fixieren wir zunächst einmal das Problem. Wir machen dies in einem etwas allgemeineren Rahmen als für Algorithmus 3.23.(Auszählen eines Koeffizienten) benötigt. Seien $v_i \in K$ $(1 \leq i \leq m)$ $\mathbb{R}$-linear unabhängig, $c \in \mathbb{R}_{>0}^{r_1+r_2}$ und $M \in \mathbb{C}^{r_1+r_2}$ gegeben. Gesucht sind nun alle $x \in \mathbb{Z}^m$ mit

$$|\sum_{i=1}^{m} x_i v_i + M| \leq c. \tag{3-4}$$

Ferner sei $\{v_i^* \in K \mid 1 \leq i \leq m\}$ die zu $\{v_i \mid 1 \leq i \leq m\}$ duale Basis, d.h.

$$b(v_i^*, v_j) := \sum_{l=1}^{r_1} v_{i,l}^* v_{j,l} + \sum_{l=1}^{r_2} v_{i,r_1+l}^* \overline{v}_{j,r_1+l} = \delta_{i,j}.$$

Wir definieren $\tilde{M} := (\operatorname{Re} M_1, \ldots, \operatorname{Re} M_{r_1}, M_{r_1+1}, \ldots, M_{r_1+r_2}) \in K$, $m_i := b(\tilde{M}, v_i^*)$ $(1 \leq i \leq m)$ sowie

$$\tilde{c} := (\sqrt{c_1^2 + \operatorname{Im}^2 M_1}, \ldots, \sqrt{c_{r_1}^2 + \operatorname{Im}^2 M_{r_1}}, c_{r_1+1}, \ldots, c_{r_1+r_2}).$$

Damit ist (3-4) äquivalent zu

$$|\sum_{i=1}^{m} (x_i + m_i) v_i| \leq \tilde{c}. \tag{3-5}$$

3.1. Duale Basis. Wegen $b(\sum_{i=1}^m x_i v_i, v_j^*) = x_j$ gilt für jede Lösung x von (3-5) und jedes $1 \leq j \leq m$:

$$\begin{aligned}
|x_j + m_j|^2 &= |b(\sum_{i=1}^{m}(x_i + m_i)v_i, v_j^*)|^2 \\
&\overset{\text{Cauchy-Schwarz}}{\leq} |b(\sum_{i=1}^{m}(x_i + m_i)v_i, \sum_{i=1}^{m}(x_i + m_i)v_i)||b(v_j^*, v_j^*)| \\
&\leq \tau(\tilde{c}^2)|b(v_j^*, v_j^*)|.
\end{aligned}$$

Daher reicht es, die Menge

$$\bigtimes_{i=1}^{m} [\![-\sqrt{\tau(\tilde{c}^2)|b(v_j^*, v_j^*)|} - m_j, \sqrt{\tau(\tilde{c}^2)|b(v_j^*, v_j^*)|} - m_j]\!]$$

auszuzählen.

3.2. Ellipse. Aus (3-5) folgt sofort

$$\sum_{i=1}^{r_1+r_2} |(\sum_{j=1}^{m}(x_j + m_j)v_j)_i|^2 \leq \sum_{i=1}^{r_1+r_2} \tilde{c}_i^2. \tag{3-6}$$

Da $\sum_{i=1}^{m} v_i\mathbb{Z}$ in kanonischer Weise ein Gitter vom Rang m über $\mathbb{Z}$ ist, entspricht dies dem Auszählen aller ganzen Punkte in einer Ellipse mit dem Mittelpunkt $\tilde{M}$, was mit dem Fincke-Pohst Verfahren ([46, 3.17c] oder [30, Algorithmus 11]) geschehen kann.

In der Praxis sollte jedoch statt (3-6)

$$\sum_{i=1}^{r_1+r_2} \frac{1}{\tilde{c}_i^2}|(\sum_{j=1}^{m}(x_j + m_j)v_j)_i|^2 \leq r_1 + r_2 \tag{3-7}$$

ausgezählt werden. Denn es hat sich gezeigt, daß (3-7) viel weniger „unzulässige“ Lösungen x für (3-4) liefert (d.h., x löst (3-7), aber nicht (3-4)) als (3-6), was sich auch geometrisch erklären läßt:

Da die Anzahl der Punkte, die (3-6) bzw. (3-7) erfüllen, im wesentlichen von den Volumina der betrachteten Ellipsen (und der Gitterdiskriminante) abhängt, wollen wir diese nun ausrechnen. Für das Volumen V_1 der durch (3-6) beschriebenen Ellipse ergibt sich:

$$V_1 = \frac{C_m 2^{r_2}}{d_{\mathcal{E}}}(\sum_{i=1}^{r_1+r_2} \tilde{c}_i)^{m/2}$$

und für (3-7)

$$V_2 = \frac{C_m 2^{r_2}}{d_{\mathcal{E}}}(r_1 + r_2)^{m/2} \prod_{i=1}^{r_1} \tilde{c}_i \prod_{i=r_1+1}^{r_1+r_2} \tilde{c}_i^2,$$

wo C_m das Volumen der m-dimensionalen Einheitskugel im $\mathbb{R}^m$ bezeichnet. Analog der Ungleichung zwischen dem arithmetischen und dem geometrischen Mittel folgt, daß V_2/V_1 beliebig klein werden kann, falls die $\tilde{c}_i$ verschieden sind.

3.3. Simplex. Für $1 \leq i \leq r_1$ ist (3-5) äquivalent zu den linearen Ungleichungen:

$$-\tilde{c}_i \leq \sum_{l=1}^{m}(x_l + m_l)(v_l)_i \leq \tilde{c}_i \tag{3-8}$$

bzw.

$$\pm \sum_{l=1}^{m} x_l(v_l)_i \leq \tilde{c}_i \mp \tilde{M}_i. \tag{3-9}$$

Für $r_1 + 1 \leq i \leq r_1 + r_2$ erhalten wir notwendige Bedingungen

$$\pm \sum_{l=1}^{m} x_l \operatorname{Re}(v_l)_i \leq \tilde{c}_i \mp \operatorname{Re} \tilde{M}_i \tag{3-10}$$

und

$$\pm \sum_{l=1}^{m} x_l \operatorname{Im}(v_l)_i \leq \tilde{c}_i \mp \operatorname{Im} \tilde{M}_i, \tag{3-11}$$

da $|\operatorname{Re} z| \leq |z|$ und $|\operatorname{Im} z| \leq |z|$ für jedes $z \in \mathbb{C}$ gilt.

Insgesamt sind daher alle Lösungen von (3-4) in dem durch die $2m$ Ungleichungen (3-9) bis (3-11) definierten Simplex enthalten. Sie können mit einer Variante des Fourier-Motzkin Eliminationsverfahrens [50] bestimmt werden.

Im folgenden werden wir eine solche Variante entwickeln, d.h., wir wollen alle $x \in \mathbb{Z}^m$ mit

$$Ax \leq b \tag{3-12}$$

für eine Matrix $A \in \mathbb{R}^{k \times m}$ und $b \in \mathbb{R}^k$ bestimmen oder feststellen, daß der Simplex unbeschränkt ist. Analog dem Gauß-Algorithmus werden wir dieses System zunächst in eine Dreiecksgestalt transformieren. Um Schwierigkeiten bei der Notation zu vermeiden, benötigen wir zunächst noch einige Bezeichnungen:

Bezeichnung 3.24. *Ein $x \in \mathbb{Z}^m$ mit $m \geq l$ erfüllt eine „lineare Bedingung a“ ($a \in \mathbb{R}^{l+1}$) genau dann, wenn*

$$\sum_{i=1}^{l} x_{m-l+i} a_i \leq a_{l+1}$$

gilt. Den Wert

$$\operatorname{bound}(a)(x) := \frac{1}{a_1}\left(a_{l+1} - \sum_{i=2}^{l} x_{m-l+i} a_i\right)$$

nennen wir die von a und x induzierte Schranke.

Für eine lineare Bedingung a nennen wir $\operatorname{lc}(a) := a_1$ den Leitkoeffizienten von a.

Der Sinn dieser Schreibweisen wird im folgenden Algorithmus unmittelbar klar:

Algorithmus 3.25 (Fourier-Motzkin Elimination).

(Input): *Eine Matrix $A \in \mathbb{R}^{k \times m}$ und ein Vektor $b \in \mathbb{R}^k$.*

(Output): *Ein endliches System* $B_i \subseteq \mathbb{R}^{m-i+2}$ *von linearen Bedingungen so, daß* $x = (x_1, \dots, x_m)^{tr} \in \mathbb{Z}^m$ *genau dann eine Lösung zu* (3-12) *ist, wenn* x *jedes* $a \in B_i$ *erfüllt* $(1 \leq i < m)$.

(Initialisierung): *Setze* $i \leftarrow 1$, $B_i \leftarrow \{(A_{i,1}, \dots, A_{i,m}, b_i) \mid 1 \leq i \leq k\}$ *und gebe* B_1 *aus.*

(Schleife): *Solange* $i < m - 1$ *ist, führe die folgenden Schritte durch*

(Trennen): *Setze*

$$\begin{aligned} P &\leftarrow \{a \in B_i \,|\, \mathrm{lc}(a) > 0\}, \\ M &\leftarrow \{a \in B_i \,|\, \mathrm{lc}(a) < 0\} \end{aligned}$$

und

$$N \leftarrow \{a \in B_i \,|\, \mathrm{lc}(a) = 0\}.$$

Falls P *oder* M *leer sind, gebe die Fehlermeldung „Simplex ist unbeschränkt“ aus und terminiere.*

Setze $i \leftarrow i + 1$ *und* $B_i \leftarrow \emptyset$.

(Kopieren): *Für jedes* $a \in N$ *füge in* B_i *die folgende Bedingung ein:*

$$(a_2, \dots, a_{m+2-i}).$$

(Kombinieren): *Für jedes Paar* $(a, \tilde{a}) \in P \times M$ *ergänze* B_i *um die folgende Bedingung:*

$$\frac{1}{\mathrm{lc}(a)}(a_2, \dots, a_{m+2-i}) - \frac{1}{\mathrm{lc}(\tilde{a})}(\tilde{a}_2, \dots, \tilde{a}_{m+2-i}).$$

Gebe B_i *aus.*

(Ende der Schleife): *Terminiere.*

Beweis. Zu beweisen ist nur die Korrektheit des Schritts (Kombinieren), da (Kopieren) die Lösungsmenge offensichtlich nicht ändert und wegen $A \cong B_1$ die Lösungsmenge des neuen Systems höchstens kleiner ist.

Seien daher o.B.d.A. $i = 1$, P, M wie in (Trennen), $(a, \tilde{a}) \in P \times M$ und ein $x \in \mathbb{Z}^m$, welches a und $\tilde{a}$ erfüllt, gegeben. Dann gelten

$$x_1 \leq \mathrm{bound}(a)(x) = \frac{1}{a_1}(a_{m+1} - \sum_{i=2}^{m} a_i x_i) \tag{3-13}$$

und

$$\frac{1}{\tilde{a}_1}(\tilde{a}_{m+1} - \sum_{i=2}^{m} \tilde{a}_i x_i) = \mathrm{bound}(\tilde{a})(x) \leq x_1, \tag{3-14}$$

da $\mathrm{lc}(\tilde{a}) < 0$ ist. Aus (3-13) und (3-14) folgt dann (als notwendige Bedingung):

$$\begin{aligned} & \mathrm{bound}(\tilde{a})(x) \leq x_1 \leq \mathrm{bound}(a)(x) \\ \iff \quad & \frac{1}{a_1}(\sum_{i=2}^{m} a_i x_i) - \frac{1}{\tilde{a}_1}(\sum_{i=2}^{m} \tilde{a}_i x_i) \leq \frac{a_{m+1}}{a_1} - \frac{\tilde{a}_{m+1}}{\tilde{a}_1} \quad \square \end{aligned}$$

Jetzt sind wir in der Lage, einen Algorithmus zum Lösen von (3-4) anzugeben:

ALGORITHMUS 3.26 (SIMPLEX-ENUMERATION).

(Input): *Eine Matrix* $A \in \mathbb{R}^{k \times m}$ *und ein Vektor* $b \in \mathbb{R}^k$.

(Output): *Alle* $x \in \mathbb{Z}^m$ *mit* $Ax \leq b$ *oder die Ausgabe „Simplex ist unbeschränkt“.*

(Initialisierung): *Berechne Mengen* $B_i \subset \mathbb{R}^{m+2-i}$ *mit* Algorithmus 3.25. *Setze* $i \leftarrow m$.

(Schranken): *Setze*

$$\max_i \leftarrow \lfloor \min\{\mathrm{bound}(a)(x) \mid a \in B_i \text{ und } \mathrm{lc}(a) > 0\} \rfloor,$$

$$\min_i \leftarrow \lceil \max\{\mathrm{bound}(a)(x) \mid a \in B_i \text{ und } \mathrm{lc}(a) < 0\} \rceil$$

und $x_i \leftarrow \min_i - 1$.

(Erhöhe x): *Setze* $x_i \leftarrow x_i + 1$. *Falls* $x_i \leq \max_i$ *ist, gehe nach* (Vermindere i).

(Erhöhe i): *Setze* $i \leftarrow i + 1$. *Falls* $i < m$ *ist, gehe nach* (Erhöhe x), *andernfalls terminiere.*

(Vermindere i): *Falls* $i = 1$ *ist, gebe* x *aus und gehe nach* (Erhöhe x).
Setze $i \leftarrow i - 1$ *und gehe nach* (Schranken).

Beweis. Da im i-ten Durchlauf von (Schranken) nur $x_{i+1}, \ldots, x_m$ benötigt werden, um die Schranken zu bestimmen, werden nur bereits definierte Komponenten zur Berechnung von $\mathrm{bound}(a)(x)$ benutzt. Im ersten Durchlauf ($i = m$) werden keine x-Komponenten benötigt.

Die Korrektheit folgt jetzt sofort aus der von Algorithmus 3.25. □

Bemerkung 3.27. (1) Algorithmus 3.26 *ist analog dem Algorithmus zum Auszählen von Ellipsoiden* 3.6.

(2) *Es ist bekannt, daß* Algorithmus 3.26 *in m doppelt exponentielle Laufzeit besitzt. Der Grund hierfür liegt zum einem darin, daß in einem Simplex exponentiell viele Punkte liegen können (z.B. $-1 \leq x_i \leq 1$ hat 3^m viele Lösungen); zum anderen liegt dies daran, daß im Schritt* (Kombinieren) *von* Algorithmus 3.25 *doppelt exponentiell viele Ungleichungen erzeugt werden. Für die Praxis ist daher* Algorithmus 3.26 *für $m > 7$ unbrauchbar, da der Speicherbedarf für die B_i in* Algorithmus 3.25 *zu stark wächst.*

Für total-reelle Körper $\mathcal{E}$ ist Algorithmus 3.26 in dem Sinne optimal zur Lösung von (3-4), daß tatsächlich nur Punkte gefunden werden, die (3-4) erfüllen. Für Körper mit gemischter Signatur (und total komplexe Körper) findet auch dieser Algorithmus zu viele Punkte, da der Übergang von (3-9) zu (3-10) bzw. (3-11) nur notwendige Bedingungen liefert und dort Informationen verloren gehen.

3.4. Mischformen. Als weitere Methode wollen wir noch eine Mischform aus Algorithmus 3.26 und 3.2 vorschlagen. Die Ursache für das relativ schlechte Laufzeitverhalten von 3.2 liegt im wesentlichen darin, daß viel zu viele Punkte betrachtet werden und erst sehr spät, d.h. zum Schluß, entschieden werden kann, ob ein Punkt (3-4) erfüllt oder nicht. Bei Algorithmus 3.26 werden viele „unzulässige“ Punkte schon früher entdeckt. Hier ist das Problem die stark wachsende Anzahl von Bedingungen. Als Kompromiß können wir Algorithmus 3.25 bis zu einer bestimmten Stufe $i_0 < m$ durchführen und die dann noch freien Variablen mit 3.2 beschränken.

4. Ein Reduktionsalgorithmus für $o_{\mathcal{E}}$-Gitter

Der wesentliche Unterschied zwischen Algorithmus 3.23 und dem Fincke-Pohst Algorithmus ist das Fehlen eines Reduktionsalgorithmus für die Pseudobasis des Gitters Λ, in dem ausgezählt werden soll. Im absoluten Fall ist die Wahl einer geeigneten Reduktionsmethode entscheidend für die Gesamtlaufzeit. Durch die Reduktion wird die Anzahl der zu durchlaufenden „toten Äste“, d.h. die Anzahl der x_i, die im Schritt Algorithmus 3.23.(Auszählen eines Koeffizienten) gefunden werden und sich nicht zu einer Lösung ergänzen lassen, stark reduziert. Im Anhang werden wir dazu einige Beispiele angeben, die dies unterstreichen werden.

Wir werden nun eine LLL-Variante für Gitter über Zahlkörpern entwickeln und ihren Einfluß auf das Auszählen numerisch untersuchen.

BEZEICHNUNG 3.28. *Sei* $\Lambda := \sum_{i=1}^{n'} \mathfrak{a}_i \alpha_i$ *mit einer symmetrischen, positiv definiten Matrix* $G \in K^{n' \times n'}$ *ein Gitter mit Pseudobasis* $(\mathfrak{a}_i, \alpha_i)_{1 \le i \le n'}$.

Induktiv definieren wir die zugehörige Orthogonal-Basis

$$\alpha_i^* := \alpha_i - \sum_{j=1}^{i-1} \mu_{i,j} \alpha_j^*,$$

$$B_i := Q_G(\alpha_i^*), \alpha_{i,j} := B_G(\alpha_i^*, \mathfrak{a}_j) \text{ und } \mu_{i,j} := \frac{\alpha_{i,j}}{B_i}$$

($1 \le i \le n'$, $1 \le j < i$*).*

Der LLL-Algorithmus versucht nun, die Ausgangsbasis zu verbessern, d.h. (für $\mathcal{E} = \mathbb{Q}$ und $\mathfrak{a}_i = \mathbb{Z}$)

$$\mu_{i,j} \le \frac{1}{2} \text{ für } 1 \le j < i \le n' \tag{3-15}$$

und

$$Q(\alpha_i^* + \mu_{i,i-1} \alpha_{i-1}^*) \ge \frac{3}{4} Q(\alpha_{i-1}^*) \tag{3-16}$$

zu erreichen. Die erste Bedingung (3-15) bewirkt, daß die reduzierte Basis annähernd orthogonal ist. Erreicht wird dies im Algorithmus dadurch, daß die $\mu_{i,j}$'s ganzzahlig approximiert werden.

Die andere Bedingung (3-16), die sog. Lovász-Bedingung, wird algorithmisch erreicht, indem die Basisvektoren, an denen sie nicht gilt, vertauscht werden. Mit dieser Bedingung wird versucht, die Diskriminanten bestimmter Teilgitter zu kontrollieren. Zusätzlich ist sie von Bedeutung, um die Endlichkeit des Algorithmus zu zeigen.

Wir werden nun zunächst die Variante für Gitter über beliebigen Ordnungen angeben und dann analysieren:

ALGORITHMUS 3.29 (rLLL).

(Input): *Ein Gitter* $\Lambda := \sum_{i=1}^{n'} \mathfrak{a}_i \alpha_i$ *mit einer symmetrischen, positiv definiten Matrix* $G \in K^{n' \times n'}$.

(Output): *Eine reduzierte Pseudobasis* $(\mathfrak{b}_i, \beta_i)$.

(Initialisierung): *Setzte* $\mathfrak{b}_i \leftarrow \mathfrak{a}_i$ *und* $\beta_i \leftarrow \alpha_i$. *Berechne die zu* $(\mathfrak{b}_i, \beta_i)$ *gehörige Orthogonalbasis* β_i^* *wie in* Bezeichnung 3.28.

Setze $k \leftarrow 2$.

(Reduktion): *Für* $1 \leq i < k$ *bestimme*

$x \in \mathfrak{a}_i\mathfrak{a}_k^{-1}$ *so, daß* $\tau((\overline{\mu_{k,i} - x})(\mu_{k,i} - x))$ *minimal wird.*

Ersetze β_k *durch* $\beta_k - x\beta_i$ *und ändere die* $\mu_{k,j}$ $(1 \leq j \leq i)$ *entsprechend.*

(rLLL-Bedingung): *Falls*

(3-17) $$\eta(B_k + |\mu_{k,k-1}|^2 B_{k-1}) N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{b}_k)^2 \leq \tfrac{3}{4}\eta(B_{k-1}) N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{b}_{k-1})^2$$

ist:

(Tausch): *Vertausche* β_k *und* β_{k-1} *sowie* $\mathfrak{b}_k$ *und* $\mathfrak{b}_{k-1}$.

Ändere die μ*'s und* B*'s entsprechend.*

Setze $k \leftarrow \max(k-1, 2)$ *und gehe nach* (Reduktion).

sonst: Setze $k \leftarrow k+1$. *Falls* $k \leq n'$ *ist, gehe nach* (Reduktion), *andernfalls terminiere.*

Beweis. Nach Satz 3.13 ändert die in (Reduktion) durchgeführte Transformation das Gitter nicht. Es bleibt daher noch die Endlichkeit des Algorithmus zu zeigen. Dies erfolgt analog [36, (1.23)]:

Sei $\Lambda_k := \sum_{i=1}^{k} \mathfrak{b}_i\beta_i$. Dann gilt $d^2(\Lambda_k) = \prod_{i=1}^{k} \eta \circ Q(\beta_i^*) N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{b}_i)^2$ (analog Lemma 3.19). Nach Satz 3.21 gibt es ein $0 \neq x \in \Lambda_k \subseteq \Lambda$ mit $\tau \circ Q(x) \leq \sqrt[mn']{\gamma_{mn'}^{mn'}} d_{\Lambda_k}$. Andererseits gilt $\tau \circ Q(x) \geq \lambda_1$ für das erste sukzessive Minimum von Λ. Da Λ_k bei jedem Durchlauf von (Tausch) um einen Faktor von mindestens 3/4 kleiner wird, kann dieser Schritt nur endlich oft durchgeführt werden. □

Offenbar liefert obiger Algorithmus eine Basis, die reduziert in dem folgenden Sinne ist:

(3-18) $$\mu_{i,j} \text{ ist } \tau \circ Q \text{ minimal in } \mu_{i,j} + \mathfrak{b}_i\mathfrak{b}_j^{-1}$$

$(1 \leq i \leq n'$, $1 \leq j < i)$ und

(3-19) $$\eta \circ Q(\beta_i^* + \mu_{i,i-1}\beta_{i-1}^*) \geq \frac{3}{4}\eta \circ Q(\beta_{i-1}^*)$$

$(2 \le i \le n')$. Im Unterschied zu (3-15) liefert (3-18) jedoch nicht genug Information, um eine Abschätzung für die Güte der reduzierten Basis zu erhalten. Der Beweis aus [36] läßt sich leider nicht verallgemeinern.

Ein weiterer Nachteil dieses Algorithmus ist, daß bei den Transformationen, die wir zulassen wollen, die Ideale nicht geändert werden. Wenn sie anfänglich „schlecht konditioniert" sind, wird der Algorithmus die Basis daher nicht allzu stark verbessern können. Wir werden verschiedene Ansätze vorstellen, um die Ideale zu ändern.

Entgegen allen Erwartungen hat sich das Finden von x in (Reduktion) in der Praxis als harmlos erwiesen. Schon in [19] haben wir vorgeschlagen, statt x als dichtestgelegenen Gitterpunkt auszuzählen [46, 3 (3.17)], was in [51] als NP-hart nachgewiesen worden ist, sich mit Approximationen zu begnügen, wie sie zum Beispiel durch den LLL-Algorithmus gefunden werden können. Beim Rechnen von umfangreichen Beispielen haben sich dabei zwei Effekte herausgestellt:

(1) Das Ausrechnen einer LLL-reduzierten Basis für $\mathfrak{a}_i\mathfrak{a}_j^{-1}$, was auch dem Auszählen vorangeht, ist für die betrachteten Beispiele ($\deg \mathcal{E} \le 12$) viel aufwendiger als das anschließende Auszählen.
(2) Der Algorithmus liefert i.allg. bessere Ergebnisse, wenn wir uns mit Approximationen begnügen. Die dichtestgelegenen Gitterpunkte waren bei fast allen Beispielen schlechter konditioniert als die Approximationen, d.h. sie führten in der Regel zu Basen aus längeren Vektoren.

Um die Ideale zu ändern haben wir im wesentlichen zwei Verfahren implementiert:

(1) Jedes 1-dimensionale Gitter $\mathfrak{b}_i\beta_i$ wird zu $\tilde{\mathfrak{b}}_i\tilde{\beta}_i$ reduziert, wobei $\tau \circ Q(\tilde{\beta}_i)$ das erste sukzessive Minimum in $\mathfrak{b}_i\beta_i$ darstellt. Erreicht wird dies durch LLL-Reduktion, bzw. Auszählen in dem $\mathbb{Z}$-Gitter $\mathfrak{b}_i\beta_i$ mit der quadratischen Form $x \mapsto \tau \circ Q(x\beta_i)$. Auch hier haben wir wieder die Wahl zwischen kurzen und kürzesten Elementen. Hier jedoch scheinen die kürzesten Elemente besser konditioniert zu sein als bei Algorithmus 3.29.(Reduktion).
(2) In dem Reduktionsschritt ändern wir beide Basiselemente. Dadurch haben wir die Möglichkeit, die Idealklassen zu ändern. Hier gibt es dann wieder zwei Möglichkeiten: Zum einen können wir in dem 2-dimensionalen Gitter $\mathfrak{b}_i\beta_i + \mathfrak{b}_l\beta_l$ ein kürzestes Element bestimmen (dies entspricht im wesentlichen einer Paarreduktion) und zu einer Basis ergänzen; zum anderen können wir versuchen, die Länge von β_i^* (und damit die Diskriminante von Λ_i) klein zu halten. Implementiert ist dies als Variation in Algorithmus 3.29.(Tausch), da es an dieser Stelle keine Rolle spielt, wenn wir β_k ändern. Solange wir garantieren, daß β_{k-1} oder β_{k-1}^* kürzer werden, terminiert der Algorithmus.

In beiden Fällen benötigen wir jedoch eine konstruktive Basisergänzung:

LEMMA 3.30. (1) *Seien Ideale* $\mathfrak{b}_1,\ \mathfrak{b}_2 \subset \mathcal{E}$, *sowie Elemente* $x_1, x_2 \in \mathcal{E}$ *gegeben. Die Kongruenzen*

$$x \equiv x_i \pmod{\mathfrak{b}_i}\ (i = 1, 2) \tag{3-20}$$

sind genau dann simultan lösbar, wenn

$$x_1 \equiv x_2 \pmod{\mathfrak{b}_1 + \mathfrak{b}_2}. \tag{3-21}$$

gilt. In diesem Fall können wir eine Lösung x *konstruktiv bestimmen, sie ist* $\pmod{\mathfrak{b}_1 \cap \mathfrak{b}_2}$ *eindeutig.*

(2) *Seien* $\Lambda = \alpha_1\mathfrak{a}_1 + \alpha_2\mathfrak{a}_2$ *sowie* $0 \neq \beta_1 \in \Lambda$. *Dann können wir konstruktiv ein* β_2 *sowie Ideale* $\mathfrak{b}_1, \mathfrak{b}_2$ *finden, so daß* $\Lambda = \beta_1\mathfrak{b}_1 + \beta_2\mathfrak{b}_2$ *gilt.*

BEWEIS. (1): Zunächst halten wir fest, daß (3-21) eine notwendige Bedingung ist: Angenommen x ist eine Lösung von (3-20). Dann gilt $x_1 - x_2 = x - x_2 - (x - x_1) \in \mathfrak{b}_1 + \mathfrak{b}_2$.

Sei nun $\mathfrak{c} := \mathfrak{b}_1 + \mathfrak{b}_2$ sowie $\tilde{\mathfrak{b}}_i := \mathfrak{b}_i\mathfrak{c}^{-1}$. Da $\tilde{\mathfrak{b}}_1$ und $\tilde{\mathfrak{b}}_2$ nun koprim sind, können wir konstruktiv Elemente $y_i \in \tilde{\mathfrak{b}}_i$ mit $y_1 + y_2 = 1$ finden [13, Proposition 1.1.]. $x := y_2x_1 + y_1x_2$ ist nun eine Lösung von (3-20):

$$x - x_1 = y_2x_1 + y_1x_2 - x_1 = (1 - y_1)x_1 + y_1x_2 - x_1 = y_1(x_2 - x_1) \in \tilde{\mathfrak{b}}_1\mathfrak{c} = \mathfrak{b}_1$$

(Analog für $\mathfrak{b}_2$).

(2): Sei nun $\beta_1 = u\alpha_1 + v\alpha_2 \in \Lambda$ beliebig, wobei o.B.d.A $uv \neq 0$ gilt. Wir setzen nun $\mathfrak{b}_1 := \frac{\mathfrak{a}_1}{u} \cap \frac{\mathfrak{a}_2}{v}$ und $\mathfrak{b}_2 := \frac{\mathfrak{a}_1\mathfrak{a}_2}{u\mathfrak{b}_1}$; gemäß Lemma 3.15.(1) gilt dann $\mathfrak{b}_1\beta_1 \subseteq \Lambda$.

Nach Lemma 3.15.(2) gibt es ein $\beta_2 = t\beta_1 + \alpha_2$ mit $\Lambda = \mathfrak{b}_1\beta_1 + \mathfrak{b}_2\beta_2$. Lemma 3.15.(1) liefert dann für die Ideale die folgenden Bedingungen:

$$\frac{\mathfrak{a}_1}{tu} \cap \frac{\mathfrak{a}_2}{tv + 1} = \mathfrak{b}_2 = \frac{\mathfrak{a}_1\mathfrak{a}_2}{u\mathfrak{b}_1},$$

was

$$u\mathfrak{b}_1 = (tu)\mathfrak{a}_2 + (tv + 1)\mathfrak{a}_1 \tag{3-22}$$

impliziert; im Falle von $tv + 1 = 0$ setzen wir $\frac{\mathfrak{a}_2}{tv+1} = \mathcal{E}$. Offenbar muß t daher die folgenden Kongruenzen lösen:

$$t \equiv 0 \pmod{\frac{\mathfrak{b}_1}{\mathfrak{a}_2}} \text{ und } t \equiv -\frac{1}{v} \pmod{\frac{u\mathfrak{b}_1}{v\mathfrak{a}_1}}. \tag{3-23}$$

Nach (1) können wir ein solches t finden. Mit Hilfe von Satz 3.13 folgt andererseits, daß jede Lösung von (3-23) eine Pseudobasis $(\mathfrak{b}_i, \beta_i)$ $(i = 1, 2)$ liefert. □

Weitere Varianten ergeben sich aus der Bedingung (3-17), die in keiner Weise eindeutig ist. Hier gibt es zunächst einmal die Variante, statt η die Funktion τ zu verwenden, um den Vergleich durchführen zu können: Tausche, falls

$$\tau(B_k + |\mu_{k,k-1}|^2 B_{k-1}) N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{b}_k)^{2/m} \leq \tfrac{3}{4}\tau(B_{k-1}) N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{b}_{k-1})^{2/m} \tag{3-24}$$

gilt. Hier folgt aus (3-3) die Existenz einer gegen 0 fallenden Majorante für $d(\Lambda_k)$. Da wir in Algorithmus 3.29 die Ideale nicht ändern, können wir den Test auch ohne die $N_{\mathcal{E}/\mathbb{Q}}(\mathfrak{b}_k)^2$ Faktoren durchführen. Cohen hat in [12] vorgeschlagen, statt der Norm das Minimum zu benutzen.

Bei dieser Variante bleibt jedoch, wie bei Algorithmus 3.29, als Hauptnachteil, daß die Ideale im Prinzip nicht berücksichtigt werden, und es daher nicht möglich ist, sie zu „verbessern“.

Analog zu [20, (2.15)] bietet es sich natürlich an, vor dem Auszählen nicht das Gitter selbst, sondern das duale Gitter zu reduzieren.

KAPITEL IV

Normgleichungen in Relativerweiterungen

1. Grundlagen

Die Bezeichnungen seien wie in Kapitel II, Abschnitt 1; ferner sei $A \leq TU_{\mathcal{E}}$.

SATZ 4.1. *Seien unabhängige Einheiten $\epsilon_i \in U^A_{\mathcal{F},S_{\mathcal{F}}}$ ($1 \leq i \leq r_{\mathcal{F}} - r_{\mathcal{E}}$) gegeben. Setze*

$$\Gamma := \{ \sum_{i=1}^{r_{\mathcal{F}}-r_{\mathcal{E}}} x_i L_{\mathcal{F}}(\epsilon_i) \mid x_i \in [-\frac{1}{2}, \frac{1}{2}]\}$$

und

$$\theta_0 := (\frac{n_{V,\mathcal{E}}}{n} V(\theta))_{V \in S_{\mathcal{F}}}.$$

Zu jedem $\alpha \in \mathcal{F}$ mit $N_{\mathcal{F}/\mathcal{E}}(\alpha) =: \theta$ gibt es dann ein $\tilde{\epsilon} \in U^A_{\mathcal{F},S_{\mathcal{F}}}$ so, daß $L_F(\tilde{\epsilon}\alpha) = \gamma + \theta_0$ mit $\gamma \in \Gamma$ gilt.

BEWEIS. Sei $\alpha \in \mathcal{F}$ mit $N_{\mathcal{F}/\mathcal{E}}(\alpha) = \theta$ gegeben. Wir definieren eine Abbildung

$$\mathcal{N} : \mathbb{R}^{S_{\mathcal{F}}} \mapsto \mathbb{R}^{S_{\mathcal{E}}} : x = (x_V)_{V \in S_{\mathcal{F}}} \mapsto (\sum_{V|v} x_V)_{v \in S_{\mathcal{E}}}.$$

Dann ist das Diagramm

$$\begin{tikzcd} \mathcal{F} \arrow[r, "N_{\mathcal{F}/\mathcal{E}}"] \arrow[d, "L_{\mathcal{F}}:=(n_{V,\mathcal{E}}|.|_V)_{V\in S_{\mathcal{F}}}"'] & \mathcal{E} \arrow[d, "(|.|_v)_{v\in S_{\mathcal{E}}}=:L_{\mathcal{E}}"] \\ \mathbb{R}^{S_{\mathcal{F}}} \arrow[r, "\mathcal{N}"] & \mathbb{R}^{S_{\mathcal{E}}} \end{tikzcd}$$

kommutativ. Wegen $N_{\mathcal{F}/\mathcal{E}}(\epsilon_i) \in A$ gilt $\mathcal{N} L_F(\epsilon_i) = 0$ mit (1-1). Wir definieren für $v \in S_{\mathcal{E}}$:

$$c_v := \left(\begin{cases} (\frac{n_{V,\mathcal{E}}}{n} \tilde{v}(\theta))_{V \in P_v} \in \mathbb{R}^{P_v} & \text{für } v = \tilde{v}, \\ 0 \in \mathbb{R}^{P_{\tilde{v}}} & \text{sonst.} \end{cases} \right)_{\tilde{v} \in S_{\mathcal{E}}} \in \mathbb{R}^{S_{\mathcal{F}}}.$$

Dann gilt

$$\mathcal{N}(c_v) = \left(\begin{cases} \sum_{V \in P_{\tilde{v}}} \frac{n_{V,\mathcal{E}}}{n} \tilde{v}(\theta) = \tilde{v}(\theta) & \text{für } v = \tilde{v}, \\ 0 & \text{sonst.} \end{cases} \right)_{\tilde{v} \in S_{\mathcal{E}}} \neq 0.$$

Offensichtlich bildet $\{L_{\mathcal{F}}(\epsilon_i) \mid 1 \leq i \leq r_{\mathcal{F}} - r_{\mathcal{E}}\} \cup \{c_v \mid v \in S_{\mathcal{E}}\}$ eine Basis des $\mathbb{R}^{S_{\mathcal{F}}}$. Daher gibt es $x_i,\ y_v \in \mathbb{R}$ $(1 \leq i \leq r_{\mathcal{F}} - r_{\mathcal{E}},\ v \in S_{\mathcal{E}})$ mit

$$L_{\mathcal{F}}(\alpha) = \sum_{i=1}^{r_{\mathcal{F}} - r_{\mathcal{E}}} x_i L_{\mathcal{F}}(\epsilon_i) + \sum_{v \in S_{\mathcal{E}}} y_v c_v.$$

Anwenden von $\mathcal{N}$ liefert:

$$\mathcal{N}(L_{\mathcal{F}}(\alpha)) = (y_v v(\theta))_{v \in S_{\mathcal{E}}}$$

und daher $y_v = 1$. Damit besitzt $\tilde{\epsilon} := \prod_{i=1}^{r_{\mathcal{F}} - r_{\mathcal{E}}} \epsilon_i^{-\lfloor x_i \rceil}$ nun alle gewünschten Eigenschaften. □

Bemerkung 4.2. *Sei* $S_{\mathcal{E}} = V_{\mathcal{E}}^{\infty}$ *und* $A = TU_{\mathcal{E}}$.

(1) *Es gilt* $\theta = N_{\mathcal{F}/\mathcal{E}}(\alpha) \equiv N_{\mathcal{F}/\mathcal{E}}(\tilde{\epsilon}\alpha) \mod TU_{\mathcal{E}}$.
(2) *Wegen*

$$\Gamma \subseteq \{ \sum_{i=1}^{r_{\mathcal{F}} - r_{\mathcal{E}}} x_i |L_{\mathcal{F}}(\epsilon_i)| \mid x_i \in [-\frac{1}{2}, \frac{1}{2}]\}$$

erhalten wir aus Satz 4.1 *sofort Schranken für die Konjugierten einer Lösungsmenge von* $|N_{\mathcal{F}/\mathcal{E}}(x)| = \theta$, *die für* $\mathcal{E} = \mathbb{Q}$ *denen in* [20, (6.3) Lemma] *entsprechen und sonst* [31, Lemma 4.1] *verbessern.*

Lemma 4.3. *Setze*

$$h : \mathbb{R}_{>1} \to]0,1[: x \mapsto \frac{x}{x-1} - \frac{1}{\log(x)}$$

und

$$g : [0,1] \times \mathbb{R}_{>1} \to \mathbb{R}_{>1} : (x,t) \mapsto (1-x)t^x + xt^{x-1}.$$

Für $\lambda > 1$ *und* $\gamma := g(h(\lambda), \lambda)$ *gilt dann*

$$\sup_{a \in [0,1]} g(a, \lambda) = \gamma. \tag{4-1}$$

Umgekehrt gibt es zu jedem $\gamma > 1$ *ein* $\lambda > 1$ *so, daß* (4-1) *gilt.*

Beweis. Um die Satzaussage auf die entsprechende Aussage in [20] zurückzuführen, benötigen wir eine Hilfsvariable. Für $K \geq 1$ beliebig fixiert, betrachten wir die folgende Bijektion:

$$\phi : \mathbb{R}_{>1} \to \mathbb{R}_{>0} : x \mapsto K(x^{n/2} - 1).$$

In [20, (6.23)] ist die Satzaussage für $\phi(\gamma)$ gezeigt. $\square$

Lemma 4.4. *Seien $\alpha \in \mathcal{F}$ mit $N_{\mathcal{F}/\mathcal{E}}(\alpha) =: \theta$ und $v \in V_{\mathcal{E}}$. Seien $|.|_1, \ldots, |.|_d$, die Fortsetzungen von $|.|_v$, $n_i := n_{V_i,\mathcal{E}}$, wobei o.B.d.A. $1 \leq n_1 \leq n_2 \leq \ldots \leq n_d$ gelte. Setze $I := \bigcup_{i=1}^d \{i\} \times [\![1, n_i]\!]$. Seien $\lambda,\ \gamma \in \mathbb{R}_{>1}$ so gewählt, daß (4-1) gilt. Dann gibt es ein $r = (r_{i,j})_{(i,j)\in I} \in \mathbb{Z}^I$ mit:*

(1) $n|\theta|_v^{2/n} \leq \sum_{(i,j)\in I} \lambda^{r_{i,j}} |\alpha|_i^2 \leq n\gamma|\theta|_v^{2/n}$.
(2) $\sum_{(i,j)\in I} r_{i,j} = 0$.
(3) *Für jedes $(i, j) \in I$ gilt $|r_{i,j} - \log_\lambda(|\alpha|_i^2 |\theta|_v^{-2/n})| < 1$.*
(4) *Sei $M := \{i \in [\![1, d]\!] \mid \#\{r_{i,j} | 1 \leq j \leq n_i\} > 1\}$. Dann gilt*

$$\#M \leq \begin{cases} 0 & n_1 = \ldots = n_d \\ 1 & \textit{sonst.} \end{cases}$$

Für $i \in M$ gibt es $j \in [\![1, n_i]\!]$ mit $r_{i,1} = \ldots = r_{i,j} = r_{i,j+1} + 1 = \ldots = r_{i,d} + 1$.

Beweis. Für $d = 1$ ist die Aussage trivial ($d = 1$ impliziert $|\alpha|_V = \sqrt[n]{|\theta|_v}$). Sei daher o.B.d.A. $d > 1$. Setze

$$\tau_i := \log_\lambda |\alpha|_i^2 |\theta|_v^{-2/n}. \tag{4-2}$$

Dann gilt

$$\sum_{i=1}^{d} n_i \tau_i = 0.$$

Für $2 \leq i \leq d$ und $1 \leq j \leq n_i$ setze $r_{i,j} := \lfloor \tau_i \rceil$, $e_{i,j} := \tau_{i,j} - r_{i,j} \in]-\frac{1}{2}, \frac{1}{2}]$, $\tilde{m} := \lfloor -\sum_{i=2}^d n_i r_{i,1} \rceil$ und $j_0 := \tilde{m} - n_1 \lfloor \tilde{m}/n_1 \rfloor$. Für $1 \leq j \leq j_0$ setze $r_{1,j} := \lfloor \tilde{m}/n_1 \rfloor + 1$, für $j_0 < j \leq n_1$ setze $r_{1,j} := \lfloor \tilde{m}/n_1 \rfloor$.

Nun gelten (2) und (4), da $n_1 | \tilde{m}$ für $n_1 = \ldots = n_d$ gilt. Schließlich seien $s := -\sum_{i=2}^d n_i e_{i,1} = -\sum_{i=2}^d \sum_{j=1}^{n_i} e_{i,j}$, $m := \lfloor s \rceil$, $\delta := s - m$, $e_{1,j} := \frac{\delta}{n_1} \in]-\frac{1}{2}, \frac{1}{2}]$.

Wir werden nun analog dem Beweis von [31, Satz 4.4] die $r_{i,j}$ sukzessiv so abändern, daß (1)–(5) gelten. Hier sei $(.) \mod n_1 : \mathbb{Z} \to [\![1, n_1]\!]$.

Solange $m > 0$ ist, führe die folgenden Schritte durch:

Bestimme ein $i \in [2, d]$ mit minimalem $e_{i,1}$. Hierfür gelten $-1 < e_{i,1} < 0$ und $r_{i,1} > \tau_i$.

Falls $e_{1,1} < e_{i,1}$:

Für $1 \leq h \leq \min(m, n_1)$ setze $e_{1,(h+j_0) \mod n_1} \leftarrow e_{1,(h+j_0) \mod n_1} + 1$.

Schließlich setze $m \leftarrow m - \min(m, n_1)$ und $j_0 \leftarrow (j_0 + \min(m, n_1)) \mod n_1$.

sonst:

Für $1 \leq h \leq \min(m, n_i)$ setze $e_{i,h} \leftarrow e_{i,h}+1$, $r_{i,h} \leftarrow r_{i,h}-1$ und $r_{1,(j_0+h) \mod n_1} \leftarrow r_{1,(j_0+h) \mod n_1} + 1$.

Schließlich setze noch $j_0 \leftarrow (j_0+\min(m, n_i)) \mod n_1$ und $m \leftarrow m-\min(m, n_i)$.

Falls $m < 0$ ist, verfahre analog.

Für die Menge M aus (4) gilt nun $\#M \leq 2$, wobei $\#M = 2$ höchstens dann gilt, wenn im letzten „sonst"-Schritt $\min(m, n_i) = m < n_i$ galt. In diesem Fall haben wir $M = \{1, i\}$ und müssen noch die folgenden Schritte durchführen, um $\#M \leq 1$ zu erhalten.

Finde j_1 so, daß $r_{i,1} = \ldots = r_{i,j_1} = r_{i,j_1+1} + 1 = \ldots = r_{i,n_i} + 1$ gilt.

Für $j_1 < j \leq n_i$ setze $r_{i,j} \leftarrow r_{i,j} + 1$, $e_{i,j} \leftarrow e_{i,j} - 1$, $r_{1,(j+j_0) \mod n_1} \leftarrow r_{1,(j+j_0) \mod n_1} - 1$ und $e_{1,(j_0-j) \mod n_1} \leftarrow e_{1,(j_0-j) \mod n_1} - 1$.

Schließlich setze noch $j_0 \leftarrow (j_0 - n_i + j) \mod n_1$, falls $j_0 = n_1$ gilt, setze $j_0 \leftarrow 0$.

Offenbar gelten nach wie vor (2) und (4). Bedingung (3) zeigen wir nun so: Es gilt $\sum_{j=1}^{n_1}(r_{1,j} - \tau_1) = -\sum_{i=2}^{d}\sum_{j=1}^{n_i}(r_{i,j} - \tau_i) = -\sum_{i=2}^{d}\sum_{j=1}^{n_i} e_{i,j} = m + \delta$. Wegen $m = 0$ folgt daher: $-1 < \sum_{i=2}^{d}\sum_{j=1}^{n_i} e_{i,j} < 1$ und $-1 < \sum_{j=1}^{n_1}(r_{1,j} - \tau_1) < 1$. Aus (4) folgt $\sum_{j=1}^{n_1}(r_{1,j} i \tau_i) = j_0 + n_1(r_{1,n_1} - \tau_1)$ und schließlich $-1 \leq -\frac{1+j_0}{n_1} < r_{1,n_1} - \tau_1 < \frac{1-j_0}{n_1} < 1$. Für $j_0 = 0$ ist damit (3) gezeigt. Sei also $j_0 > 0$. Dann gilt jedoch $r_{1,n_1} - \tau_1 < 0$, wegen $1 > r_{1,n_1} + 1 = r_{1,1}$ gilt (3) daher überall.

Um (1) zu erhalten, zeigen wir, daß r noch eine weitere Bedingung erfüllt:

(5) Für $a := \max_{i=2}^{d} e_{i,1}$, gelten $0 < a < 1$ und $e_{i,j} \in [a-1, a]$ für jedes $(i, j) \in I$.

Für $a := \max_{i=2}^d e_{i,1}$ und $i > 1$ gilt $e_{i,j} \in [a-1, a]$. Um nun noch $\tau_i - r_{1,j} \in [a-1, a]$ zu erhalten, müssen wir $r_{1,j}$ ggf. weiter abändern: Sei $e_{1,j} := \tau_1 - r_{1,j} \in]-1, 1[$ $(1 \leq j \leq n_1)$.

Falls $e_{1,1} > a \geq 0$ gilt: Finde i_0 mit $e_{i_0,1} = a$ und setze für $1 \leq h \leq j_0 \mod n_1$:

$r_{1,h} \leftarrow r_{1,h} - 1$, $e_{1,h} \leftarrow e_{1,h} - 1$, $r_{i,h} \leftarrow r_{i_0,h} + 1$ und $e_{i,h} \leftarrow e_{i_0,h} - 1$.

$j_0 \leftarrow 0$.

Für $e_{1,n_1} < a - 1 \leq 0$ verfahre analog: Finde i_0 mit $\min_{i=2}^d e_{i,1} = e_{i_0,1}$ und setze für $j_0 < h \leq n_1$

$r_{1,h} \leftarrow r_{1,h} - 1$, $e_{1,h} \leftarrow e_{1,h} + 1$, $r_{i,h} \leftarrow r_{i,h} + 1$ und $e_{i,h} \leftarrow e_{i,h} - 1$.

$j_0 \leftarrow 0$.

Da die letzten Änderungen die Eigenschaften (2)–(4) nicht beeinflussen, gelten sie nach wie vor. Damit folgt $a \in [0, 1]$ nun aus einer genaueren Analyse: Zu Beginn unserer Umformungen galt $e_{i,1} \in [-1/2, 1/2]$ für $2 \leq i \leq d$, d.h., für $a = 1/2$ und $2 \leq i$ galt (5). Da wir nur die jeweils Extremalen $e_{i,j}$'s geändert haben, gilt (5) für $2 \leq i$ immer noch. Für $i = 1$ haben wir es gerade nachgewiesen.

Es bleibt noch (1) zu zeigen. Da $|\theta|_v = \prod_{i=1}^d |\alpha|_i^{n_i}$ nach Voraussetzung und (1-1) gilt, folgt aus (2) und der Ungleichung zwischen geometrischem und arithmetischem Mittel:

$$|\theta|_v^{2/n} = (\prod_{i=1}^d |\alpha|_i^{2n_i})^{1/n} = (\prod_{i=1}^d \prod_{j=1}^{n_i} \lambda^{r_{i,j}} |\alpha|_i^2)^{1/n} \leq \frac{1}{n} \sum_{i=1}^d \sum_{j=1}^{n_i} \lambda^{r_{i,j}} |\alpha|_i^2.$$

Die andere Abschätzung erhalten wir aus:

$$\begin{aligned} \text{(4-3)} \quad \sum_{i=1}^d \sum_{j=1}^{n_i} \lambda^{r_{i,j}} |\alpha|_i^2 &\overset{(4\text{-}2)}{=} |\theta|_v^{2/n} \sum_{i=1}^d \sum_{j=1}^{n_i} \lambda^{e_{i,j}} \\ &= |\theta|_v^{2/n} \sum_{i=1}^d \sum_{j=1}^{n_i} \lambda^{(1-(a-e_{i,j}))a + (a-e_{i,j})(a-1)}. \end{aligned}$$

Da $x \mapsto \lambda^x$ konvex ist $(\lambda > 1)$, folgt:

$$\leq \quad |\theta|_v^{2/n} \sum_{i=1}^{d} \sum_{j=1}^{n_i} (1 - (a - e_{i,j}))\lambda^a + (a - e_{i,j})\lambda^{a-1}.$$

Mit $\sum_{(i,j)\in I} e_{i,j} = 0$ und (4-1) erhalten wir:

$$\leq \quad |\theta|_v^{2/n} \sum_{i=1}^{d} \sum_{j=1}^{n_i} \gamma \tag{4-4}$$

$$= \quad n\gamma|\theta|_v^{2/n}. \quad \square \tag{4-5}$$

BEMERKUNG 4.5. (1) *In* (4-3) *können wir trivialerweise* $e_{i,j} \in [-1, 1]$ *mit*

$$|\theta|_v^{2/n} \sum_{i=1}^{d} \sum_{j=1}^{n_i} \lambda \leq n\lambda|\theta|_v^{2/n}$$

abschätzen. Wegen $\gamma \leq \lambda$ *ist* Lemma 4.4.(1) *jedoch schärfer.*

(2) *Wenn wir auf* Lemma 4.4.(2) *verzichten, können wir immer* $\#M = 0$, $e_{i,j} \in [-\frac{1}{2}, \frac{1}{2}]$ *und* $\sum_{i=1}^{d} n_i \lambda^{r_{i,1}} |\alpha|_i^2 \leq n\sqrt{\lambda}|\theta|_v^{2/n}$ *erreichen, indem wir* $r_{i,j} := \lfloor \tau_i \rceil$ *setzen. In diesem Fall erhalten wir jedoch keine untere Abschätzung in* 4.4.(1)*, da wir hierfür* 4.4.(2) *benötigen. Zusätzlich ist dann die Anzahl der* $r \in \mathbb{Z}^I$ *die* 4.4.(3) *erfüllen viel größer.*

(3) *Analog* Beispiel 3.10.(1) *ist* Lemma 4.4.(1) *eine gewichtete quadratische Form auf dem* $o_{\mathcal{E}}$*-Gitter* $o_{\mathcal{F}}$.

(4) Satz 4.1 *zusammen mit* Lemma 4.4 *verallgemeinern die entsprechenden Resultate von* [20, (6.3) Satz] *und* [31, Satz 4.4].

2. Nenner von nicht ganzen Lösungen

Im letzten Kapitel haben wir die Bestimmung von

$$\alpha \in o_{\mathcal{F}} : \quad N_{\mathcal{F}/\mathcal{E}}(\alpha) = \theta \tag{4-6}$$

für $\theta \in o_{\mathcal{E}}$ auf ein endliches Problem reduziert, und mit Satz 4.1 können wir Schranken für hinreichend viele Bewertungen einer möglichen Lösung erhalten. Im nächsten Abschnitt werden wir zeigen, wie diese Information effizient genutzt werden kann. Wenn wir jedoch statt (4-6)

$$\alpha \in \mathcal{F} : \quad N_{\mathcal{F}/\mathcal{E}}(\alpha) = \theta \tag{4-7}$$

lösen wollen, müssen wir Schranken für die auftretenden Nenner finden. Wir werden uns dabei auf den Fall $\mathcal{F}/\mathcal{E}$ Galois'sch beschränken. Die Schranken, die es im allgemeinen Fall gibt (siehe z. B. [3, Satz 2]) — und die mit den gleichen Methoden gewonnen werden können — sind für die praktische Lösung von Normgleichungen ungeeignet, da sie viel zu groß sind. Sie hängen i.allg. von der Minkowski-Schranke der Galois'schen Hülle von $\mathcal{F}$ ab. Im Fall einer Galois'schen Körpererweiterung werden wir den Beweis von [25, Theorem 1] genauer analysieren, um effektive Schranken zu erhalten:

LEMMA 4.6. *Seien $\mathcal{F}/\mathcal{E}$ Galois'sch und $\alpha \in \mathcal{F}$ mit $N_{\mathcal{F}/\mathcal{E}}(\alpha) = \theta \in o_{\mathcal{E}}$. Dann gibt es ein ganzes Ideal $\mathfrak{a} \subseteq o_{\mathcal{F}}$ mit $N_{\mathcal{F}/\mathcal{E}}(\mathfrak{a}) = N_{\mathcal{F}/\mathcal{E}}(\alpha)o_{\mathcal{E}}$.*

BEWEIS. Sei $(\alpha) = \prod_{\mathfrak{p}\in\mathbb{P}_{\mathcal{E}}} \prod_{\mathbb{P}_{\mathcal{F}}\ni\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(\alpha)}$. Dann gilt

$$\begin{aligned}(\theta) &= (N_{\mathcal{F}/\mathcal{E}}(\alpha)) = \prod_{\mathfrak{p}\in\mathbb{P}_{\mathcal{E}}} \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(\alpha)} \\ &= \prod_{\mathfrak{p}\in\mathbb{P}_{\mathcal{E}}} \mathfrak{p}^{e_{\mathfrak{p}} f_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(\alpha)}.\end{aligned}$$

(Mit $f_{\mathfrak{p}} := f_{\mathfrak{P}|\mathfrak{p}}$ und $e_{\mathfrak{p}} := e_{\mathfrak{P}|\mathfrak{p}}$ für ein beliebiges (und damit alle) $\mathfrak{P}|\mathfrak{p}$.) Da $\theta \in o_{\mathcal{E}}$ ist, folgt $\sum_{\mathbb{P}_{\mathcal{F}}\ni\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(\alpha) \geq 0$ für alle $\mathfrak{p} \in \mathbb{P}_{\mathcal{E}}$. Wir fixieren nun für jedes $\mathfrak{p} \in \mathbb{P}_{\mathcal{E}}$ ein $\mathfrak{P}_{\mathfrak{p}}|\mathfrak{p}$. Dann ist $\mathfrak{a} := \prod_{\mathfrak{p}\in\mathbb{P}_{\mathcal{E}}} \mathfrak{P}_{\mathfrak{p}}^{e_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(\alpha)}$ ein ganzes Ideal mit

$$N_{\mathcal{F}/\mathcal{E}}(\mathfrak{a}) = \prod_{\mathfrak{p}\in\mathbb{P}_{\mathcal{E}}} \mathfrak{p}^{e_{\mathfrak{p}} f_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(\alpha)} = (N_{\mathcal{F}/\mathcal{E}}(\alpha)). \quad \square$$

SATZ 4.7. *Seien $\mathcal{F}/\mathcal{E}$ Galois'sch und $M \subseteq \mathbb{P}_{\mathcal{F}}$ so gegeben, daß es zu jedem Ideal $\mathfrak{a}$ von $\mathcal{F}$ ein Ideal $\mathfrak{P} \in M$ mit $\mathrm{cl}(\mathfrak{a}) = \mathrm{cl}(\mathfrak{P})$ gibt. Ferner sei $\alpha \in \mathcal{F}$ mit $N_{\mathcal{F}/\mathcal{E}}(\alpha) =: \theta \in o_{\mathcal{E}}$ gegeben.*

Dann gibt es $c \in o_{\mathcal{E}}$ und $\beta \in \mathcal{F}$ mit

(1) *$\mathbb{P}_{\mathcal{E}} \ni \mathfrak{p}|(c)$ impliziert, die Existenz eines $\mathfrak{P} \in M$ mit $\mathfrak{p}|N_{\mathcal{F}/\mathcal{E}}(\mathfrak{P})$,*
(2) *$N_{\mathcal{F}/\mathcal{E}}(\beta) = \theta$,*
(3) *$c\beta \in o_{\mathcal{F}}$.*

BEWEIS. Sei $\mathrm{Gal}(\mathcal{F}/\mathcal{E}) = \{\sigma_1, \ldots, \sigma_n\}$.

Nach Lemma 4.6 gibt es ein Ideal $\mathfrak{a} \subseteq o_{\mathcal{F}}$ mit $N_{\mathcal{F}/\mathcal{E}}(\mathfrak{a}) = \theta$. Wegen $N_{\mathcal{F}/\mathcal{E}}(\frac{\mathfrak{a}}{\alpha}) = o_{\mathcal{E}}$ gibt es nach [24, Lemma 6] Ideale $\mathfrak{b}_i'$ $(1 \leq i \leq n)$ mit

$$\frac{\mathfrak{a}}{\alpha} = \prod_{i=1}^{n} \frac{\sigma_i \mathfrak{b}_i'}{\mathfrak{b}_i'}. \tag{4-8}$$

Nach Voraussetzung gibt es $\beta_i \in \mathcal{F}$ und $\mathfrak{b}_i \in M$ mit $\mathfrak{b}_i' = \beta_i \mathfrak{b}_i$ $(1 \leq i \leq n)$. Dann existieren $k_i \in \mathbb{N}$ sowie $\tilde{\beta}_i \in o_{\mathcal{E}}$ mit $N_{\mathcal{F}/\mathcal{E}}{}^{k_i}(\mathfrak{b}_i) = (\tilde{\beta}_i)$. Setzen wir nun

$$\beta := \alpha \prod_{i=1}^{n} \frac{\sigma_i \beta_i}{\beta_i}, \tag{4-9}$$

so erfüllt β (1) – (3):

Wegen $N_{\mathcal{F}/\mathcal{E}}(\sigma\beta_i) = N_{\mathcal{F}/\mathcal{E}}(\beta_i)$ folgt $N_{\mathcal{F}/\mathcal{E}}(\beta) = \theta$. Um nun Aussagen über den Nenner von β treffen zu können, schreiben wir (4-9) mit Hilfe von (4-8) um:

$$\begin{aligned}
(\beta) \quad &= \quad (\alpha) \prod_{i=1}^{n} \frac{\sigma_i \beta_i}{\beta_i} = \mathfrak{a} \prod_{i=1}^{n} \frac{\mathfrak{b}_i'}{\sigma_i \mathfrak{b}_i'} \frac{\sigma_i \beta_i}{\beta_i} \\
&= \quad \mathfrak{a} \prod_{i=1}^{n} \frac{\mathfrak{b}_i}{\sigma_i \mathfrak{b}_i} = \mathfrak{a} \prod_{i=1}^{n} \frac{\mathfrak{b}_i \prod_{\substack{j=1 \\ i \neq j}}^{n} \sigma_j \mathfrak{b}_i}{\prod_{j=1}^{n} \sigma_j \mathfrak{b}_i} \\
&\overset{[35,\, \text{I } \S 7]}{=} \quad \mathfrak{a} \prod_{i=1}^{n} \frac{\mathfrak{b}_i \prod_{\substack{j=1 \\ i \neq j}}^{n} \sigma_j \mathfrak{b}_i}{N_{\mathcal{F}/\mathcal{E}}(\mathfrak{b}_i)} \\
&= \quad \mathfrak{a} \prod_{i=1}^{n} \frac{\mathfrak{b}_i (\prod_{\substack{j=1 \\ i \neq j}}^{n} \sigma_j \mathfrak{b}_i) N_{\mathcal{F}/\mathcal{E}}{}^{k_i - 1}(\mathfrak{b}_i)}{N_{\mathcal{F}/\mathcal{E}}{}^{n_i}(\mathfrak{b}_i)} = \mathfrak{a} \prod_{i=1}^{n} \frac{\mathfrak{b}_i (\prod_{\substack{j=1 \\ i \neq j}}^{n} \sigma_j \mathfrak{b}_i) N_{\mathcal{F}/\mathcal{E}}{}^{k_i - 1}(\mathfrak{b}_i)}{\tilde{\beta}_i} \\
&=: \quad \frac{1}{c} \mathfrak{a} \prod_{i=1}^{n} \mathfrak{b}_i \Big(\prod_{\substack{j=1 \\ i \neq j}}^{n} \sigma_j \mathfrak{b}_i\Big) N_{\mathcal{F}/\mathcal{E}}{}^{k_i - 1}(\mathfrak{b}_i)
\end{aligned}$$

Da alle Ideale ganz sind, folgen (1) – (3) sofort. □

3. Lösen von Normgleichungen (in Relativerweiterungen)

In diesem Abschnitt werden wir die in den letzten Kapiteln gewonnenen Informationen zu einem vollständigen Algorithmus zum Lösen von Normgleichungen zusammensetzen.

Zunächst wollen wir eines der beiden folgenden Probleme betrachten: Für ein $\theta \in o_{\mathcal{E}}$ bestimme eine endliche Menge $L \subset o_{\mathcal{F}}$ so, daß für jedes $x \in o_{\mathcal{F}}$ mit

$$N_{\mathcal{F}/\mathcal{E}}(x) = \theta \tag{4-10}$$

bzw.

$$N_{\mathcal{F}/\mathcal{E}}(x) \equiv \theta \pmod{TU_{\mathcal{E}}} \tag{4-11}$$

ein $\tilde{x} \in L$ mit $N_{\mathcal{F}/\mathcal{E}}(\tilde{x}) = N_{\mathcal{F}/\mathcal{E}}(x)$ bzw. $N_{\mathcal{F}/\mathcal{E}}(\tilde{x}) = N_{\mathcal{F}/\mathcal{E}}(x) \pmod{TU_{\mathcal{E}}}$ und $\frac{x}{\tilde{x}} \in U_{\mathcal{F}}$ gilt, d.h., wir wollen (4-10) bzw. (4-11) bis auf Assoziierte vollständig lösen. Wir geben hier zunächst einen Algorithmus zum Lösen von (4-10) an, dazu fixieren wir folgende Situation: Sei $S_{\mathcal{E}} = V_{\mathcal{E}}^{\infty}$, $S_{\mathcal{F}} = V_{\mathcal{F}}^{\infty}$ und $u := r_{\mathcal{F}} - r_{\mathcal{E}}$. Wir definieren

$$I_1 := [\![1, r_1 + r_2]\!] \times [\![1, n]\!] \text{ und } I_2 := \bigcup_{i=1}^{r_1+r_2} \{i\} \times [\![1, s_i + t_i]\!],$$

wobei wir (um die Notation zu vereinfachen) $s_i := n$, $t_i := 0$ für $r_1 < i \leq r_1 + r_2$ setzen, $n_{i,j} := 2$ für $r_1 < i \leq r_1 + r_2$ und $s_i < j \leq s_i + t_i$. Für alle anderen $(i,j) \in I_1$ sei $n_{i,j} := 1$.

Für $c_i > 0$ $(1 \leq i \leq r_1 + r_2)$ seien

$$D_1(c) := \operatorname{diag}(\overbrace{c_1, \dots, c_1}^{n}, \dots, \overbrace{c_{r_1+r_2}, \dots, c_{r_1+r_2}}^{n})$$

und

$$D_2(c) := \operatorname{diag}(\overbrace{c_1, \dots, c_1}^{s_1+t_1}, \dots, \overbrace{c_{r_1+r_2}, \dots, c_{r_1+r_2}}^{s_{r_1+r_2}+t_{r_1+r_2}}).$$

Schließlich betrachten wir noch folgende Abbildungen:

$$L_1 : \mathcal{F} \to \mathbb{R}^{I_1} : x \mapsto (\log |x^{(i,j)}|)_{(i,j)\in I_1}$$

und

$$L_2 : \mathcal{F} \to \mathbb{R}^{I_2} : x \mapsto (n_{i,j} \log |x^{(i,j)}|)_{(i,j)\in I_2}.$$

Für ein $r > 0$ seien

$$B_r^2 := \{x \in \mathbb{R}^{n'} \mid \sum_{i=1}^{n'} x_i^2 \leq r^2\}$$

und

$$B_r^{\infty} := \{x \in \mathbb{R}^{n'} \mid \max_{i=1}^{n'} |x_i| \leq r\}.$$

Bei passender Anordnung der Bewertungen gilt dann $L_{\mathcal{F}} = -L_1$.

ALGORITHMUS 4.8 (LÖSEN VON EXAKTEN NORMGLEICHUNGEN).

(Input): *Zahlkörper $\mathcal{F}/\mathcal{E}$ und $\theta \in o_{\mathcal{E}}$.*

(Output): *Eine Menge L wie oben beschrieben.*

(Einheiten): *Bestimme ein maximales unabhängiges Einheitensystem $\epsilon_i \in U := U_{\mathcal{F}}^1$ $(1 \leq i \leq u)$.*

(Lambda): *Für $1 \leq i \leq r_1 + r_2$ wähle $\lambda_i > 1$ und bestimme γ_i hierzu so, daß* (4-1) *gilt.*

(Ceiling): *Seien*

$$\Gamma_j := \{\sum_{i=1}^{u} \mu_i L_j(\epsilon_i) \mid \mu_i \in [-\frac{1}{2}, \frac{1}{2}]\} \quad j \in \{1, 2\}$$

und

$$\begin{aligned} R \ &:= \ \{r \in \mathbb{Z}^{I_1} \cap (2D_1((\log^{-1}\lambda_i)_{1\le i\le r_1+r_2})\,(\Gamma_1 + \frac{1}{n}L_1(\theta)) + B_1^\infty) \mid \\ &\qquad r \textit{ erfüllt } \text{Lemma 4.4.(2) } \textit{und } (4)\}. \end{aligned}$$

Setze $L := \emptyset$.

Für jedes $r \in R$ *führe die folgenden Schritte durch:*

(Auszählen): *Bestimme*

$$X_r := \{\alpha \in o_{\mathcal{F}} \mid \sum_{j=1}^{n} \lambda_i^{r_{i,j}} |x^{(i,j)}|^2 \le n\gamma_i |\theta^{(i)}|^{2/n} \textit{ für } 1 \le i \le r_1 + r_2\}.$$

(Testen): *Setze* $L := L \cup \{\alpha \in X_r \mid N_{\mathcal{F}/\mathcal{E}}(\alpha) = \theta\} \mod U$.

Gib L *aus und terminiere.*

Beweis. Wir müssen zeigen, daß der Algorithmus „alle" Lösungen von (4-10) findet. Das Verfahren ist offensichtlich endlich. Sei α eine Lösung von (4-10). Nach Satz 4.1 gibt es dann eine Einheit $\epsilon \in U$ so, daß $L(\alpha\epsilon) \in \Gamma + \theta_0$ gilt, d.h., es gilt

$$L_2(\alpha\epsilon) \in \Gamma_2 + \frac{1}{n}L_2(\theta).$$

Hierfür folgt:

$$(n_{i,j} \log_{\lambda_i}(|\alpha^{(i,j)}\epsilon^{(i,j)}|^2 |\theta^{(i)}|^{-2/n})_{(i,j)\in I_2} \in 2D_2((\log^{-1}\lambda_i)_{1\le i\le r_1+r_2})\,(\Gamma_2 + \frac{1}{n}L_2(\theta)).$$

Nach Lemma 4.4 gibt es dann ein $r \in R$ so, daß $\alpha\epsilon \in X_r$ gilt. $\square$

Um (4-11) statt (4-10) zu lösen, muß lediglich im Schritt (Einheiten) $U_{\mathcal{F}}^{TU_{\mathcal{E}}}$ anstelle von $U_{\mathcal{F}}^1$ berechnet werden. Die Menge R aus (Ceiling) kann z.B. mit einer Variante von Algorithmus 3.26 erhalten werden. Nach Beispiel 3.10.(1) erhalten wir X_r aus (Auszählen) mit Hilfe von Algorithmus 3.23.

Es bleibt noch Schritt (Lambda) zu erläutern, d.h. Kriterien für die Wahl von λ anzugeben. In den nächsten beiden Lemmata werden wir den Einfluß von λ (und γ) auf die (zu erwartende) Laufzeit untersuchen:

Lemma 4.9. *Seien $\epsilon_i \in U$ $(1 \le i \le u)$ wie in* (Einheiten) *gegeben, $c_i > 0$ $(1 \le i \le r_1 + r_2)$ und*

$$\Gamma_j(c) := D_j(c)\Gamma_j \quad j \in \{1,2\}.$$

Dann gelten:

(1)
$$\mathrm{vol}_u(\Gamma_2(c)) = \prod_{i=1}^{r_1+r_2} c_i^{s_i+t_i-1}\, \mathrm{vol}_u(\Gamma_2)$$

und

$$\mathrm{vol}_u(\Gamma_2) = \prod_{i=1}^{r_1+r_2} (s_i + t_i)\, \mathrm{reg}_{\mathcal{F}/\mathcal{E}}(U).$$

(2) *Sei*

$$S_c := \#(\mathbb{Z}^{I_2} \cap D_2(c)(\Gamma_2 + \frac{1}{n}L_2(\theta)) + B_1^\infty).$$

Dann gibt es ein $\delta \in \mathbb{R}_{\geq 0}^{r_1+r_2}$, welches nur von Γ_2 abhängt, so daß für $\tilde{c} := \delta + c$

$$S_c \le \prod_{i=1}^{r_1+r_2} \tilde{c}_i^{s_i+t_i-1}\, \mathrm{reg}_{\mathcal{F}/\mathcal{E}}(U)(2\sqrt{n})^{r_1+r_2}$$

gilt.

(3)
$$\#R \le S_c \prod_{i=1}^{r_1}(t_i + 1)$$

für $c_i := 2\log^{-1}\lambda_i$.

Beweis. (1): Der Beweis von Lemma 2.7.(1) kann ungeändert übernommen werden, da dort nur $\sum_{j=1}^{s_i+t_i} \log|x^{(i,j)}| = 0$ $(1 \le i \le r_1 + r_2)$ ausgenutzt wurde.

(2): Sei $H := \{x \in \mathbb{R}^{I_2} \mid \sum_{j=1}^{s_i+t_i} n_{i,j}x_{i,j} = 0\}$. Dann gilt:

$$\begin{aligned} S_c &= \# \, \mathbb{Z}^{I_2} \cap (D_2(c)(\Gamma_2 + \frac{1}{n}L_2(\theta)) + B_1^\infty) \\ &\le \mathrm{vol}(D_2(c)(\Gamma_2 + \frac{1}{n}L_2(\theta)) + B_2^\infty) \\ &= \mathrm{vol}(D_2(c)\Gamma_2 + B_2^\infty) \\ &\le \mathrm{vol}_u(D_2(c)\Gamma_2 + H \cap B_2^\infty)\,\mathrm{diam}(B_2^\infty)^{r_1+r_2}. \end{aligned}$$

Da $\mathrm{vol}_u(\Gamma_2) > 0$ gilt und Γ_2 sowohl konvex als auch 0-symmetrisch ist, gibt es $\delta \in \mathbb{R}_{>0}^{r_1+r_2}$ so, daß $H \cap B_2^\infty \subseteq D_2(\delta)\Gamma_2$ gilt. Dann folgt:

$$\le \mathrm{vol}_u(D_2(c+\delta)\Gamma_2)\sqrt{2n}^{r_1+r_2}.$$

Nach (1) folgt dann:

$$= \prod_{i=1}^{r_1+r_2} \tilde{c}_i^{s_i+t_i-1} \operatorname{reg}_{\mathcal{F}/\mathcal{E}}(U) \sqrt{2n}^{r_1+r_2}.$$

(3): Sei $r \in R$ beliebig. Wir definieren $\tilde{r} := (n_{i,j} r_{i,j})_{(i,j)\in I_2} \in D_2(c)(\Gamma_2 + \frac{1}{n} L_2(\theta))$. Sei nun ein weiteres $s \in R$ mit $\tilde{s} = \tilde{r}$ gegeben. Wegen Lemma 4.4.(4) kann es hiervon höchstens $\prod_{i=1}^{r_1}(t_i+1)$ viele geben, daher folgt (3) aus (2). □

Lemma 4.10. *Die Voraussetzungen seien wie bei* Algorithmus 4.8.(Auszählen). *Ferner sei für beliebiges $r \in \mathbb{Z}^{I_2}$ mit $\sum_{j=1}^{s_i+t_i} n_{i,j} r_{i,j} = 0$ $(1 \le i \le r_1 + r_2)$:*

$$X_r((\lambda_i, \gamma_i)_{1\le i\le r_1+r_2}) := \{x \in \mathbb{C}^{I_2} \mid \sum_{i=1}^{s_i+t_i} n_{i,j} \lambda_i^{r_{i,j}} |x_{i,j}|^2 \le n\gamma_i |\theta^{(i)}|^{2/n} \text{ für } 1 \le i \le r_1 + r_2\}.$$

Dann gelten:

(1) *Seien λ_i, γ_i beliebig fixiert und r wie oben. Dann gilt:*

$$\# X_r \cap (o_{\mathcal{F}} \otimes 1) = \frac{\operatorname{vol}(B_1^2) n^{n/2} |N_{\mathcal{E}/\mathbb{Q}}(\theta)| \prod_{i=1}^{r_1+r_2} \gamma_i^{n/2}}{\sqrt{|d_{\mathcal{F}/\mathbb{Q}}|}} + O(|N_{\mathcal{E}/\mathbb{Q}}(\theta)|^{1-1/n})$$

für $N_{\mathcal{E}/\mathbb{Q}}(\theta) \to \infty$.

(2) *Sei nun θ fixiert. Im folgenden betrachten wir nur Paare (λ_i, γ_i), für die (4-1) gilt. In diesem Fall schreiben wir $\lambda_i = \lambda(\gamma_i)$, dann wächst $\# X_r((\lambda(\gamma_i), \gamma_i)_{1\le i\le r_1+r_2}) \cap (o_{\mathcal{F}} \otimes 1)$ mindestens so stark wie $(\prod_{i=1}^{r_1+r_2} \gamma_i^{n/2})$ für $\gamma_i \to \infty$.*

Beweis. Zunächst gilt:

$$\text{(4-12)} \qquad \operatorname{vol}(X_r((\lambda_i, \gamma_i)_{1\le i\le r_1+r_2})) = \operatorname{vol}(B_1^2) \prod_{i=1}^{r_1+r_2} \gamma_i^{n/2} |N_{\mathcal{F}/\mathbb{Q}}(\theta)| n^{n/2},$$

da $\sum_{j=1}^{n} r_{i,j} = 0$ für alle i gilt.

(1): Direkte Folge von [35, VI, §2].

(2): Mit [46, 3 (4.3)] und (4-12). □

Wenn wir nun davon ausgehen, daß die Gesamtlaufzeit T von Algorithmus 4.8 für ein festes θ im wesentlichen von der Anzahl der zu untersuchenden algebraischen Zahlen abhängt, erhalten wir aus Lemma 4.9.(3) zusammen mit Lemma 4.10.(2) für festes θ:

$$\text{(4-13)}\, T \sim \sum_{r\in R} \#X_r \cap (o_{\mathcal{F}} \otimes 1) \sim \#R\#X_r \cap (o_{\mathcal{F}} \otimes 1) \sim \prod_{i=1}^{r_1+r_2} \frac{\gamma_i^{n/2}}{\log^{s_i+t_i-1} \lambda_i},$$

d.h., wir müssen λ_i, γ_i so wählen, daß (4-13) minimal wird. Mit Lemma 4.3 können wir γ_i als Funktion von λ_i auffassen. Da die λ_i's für verschiedene $1 \leq i \leq r_1 + r_2$ offenbar unabhängig voneinander sind, erhalten wir $r_1 + r_2$ viele 1-dimensionale Minimierungsprobleme: Wir bestimmen λ_i so, daß

$$\text{(4-14)} \qquad \frac{g(h(\lambda_i), \lambda_i)^{n/2}}{\log^{s_i+t_i} \lambda_i}$$

minimal wird.

BEMERKUNG 4.11. (1) *Das Minimierungsproblem* (4-14) *ist identisch mit dem von Fincke in* [20, (9.6)] *betrachteten. Obige Überlegungen verallgemeinern daher direkt die von Fincke erhaltenen Ergebnisse.*

(2) *Für „kleine“ θ sind die so erhaltenen λ_i nicht optimal. Hier ist das Problem, daß das Initialisieren eines neuen Auszählprozesses (*Algorithmus 3.23*) verhältnismäßig aufwendig ist. Hier sollten größere Werte für λ_i benutzt werden, um die Anzahl der quadratischen Formen klein zu halten.*

(3) *δ in* Lemma 4.9.(2) *kann — bei fixem Körpergrad mn — unabhängig von Γ_2 gewählt werden, da es eine nur von mn abhängige Schranke für das erste sukzessive Minimum im Einheitengitter gibt.*

Seien nun λ_i und γ_i fixiert. Nach Lemma 4.9.(2), Lemma 4.10.(1) und Bemerkung 4.11.(3) gilt für die Anzahl P_{rel} der von Algorithmus 4.8 zu betrachtenden Punkte:

$$\text{(4-15)} \qquad P_{\text{rel}} = O(n^{(m+n)/2} |N_{\mathcal{E}/\mathbb{Q}}(\theta)| \frac{\operatorname{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F})}{\sqrt{|d_{\mathcal{F}/\mathbb{Q}}|}}).$$

Mit Satz 2.9 und dem Satz von Brauer-Siegel [35, XVI, App. Theorem 5] folgt dann:

$$\text{(4-16)} \qquad P_{\text{rel}} = O(n^{(m+n)/2} |N_{\mathcal{E}/\mathbb{Q}}(\theta)| \frac{1}{h_{\mathcal{F}} \operatorname{reg}_{\mathcal{E}/\mathbb{Q}}(N_{\mathcal{F}/\mathcal{E}}(U_{\mathcal{F}}))}).$$

Als Alternative zu Algorithmus 4.8 können wir eine absolute Variante des Auszählens benutzen ([31, Algorithmus 4.10]), in dem wir in dem entsprechenden $\mathbb{Z}$-Gitter

(Bemerkung 3.12.(1)) mit der Schranke

$$n \sum_{i=1}^{r_1+r_2} \gamma_i |\theta^{(i)}|^{2/n}$$

auszählen. Für die bei diesem Algorithmus zu betrachtende Anzahl von Punkten $P_{\text{rel-abs}}$ gilt unter der zusätzlichen Annahme: $\lambda_1 = \ldots = \lambda_{r_1+r_2}$:

$$P_{\text{rel-abs}} = O(n^{mn/2+m}\,\mathrm{T}_2(\theta)^{m/2} \frac{\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F})}{\sqrt{|d_{\mathcal{F}/\mathbb{Q}}|}}). \tag{4-17}$$

Wenn wir Lemma 4.9.(2) und 4.10.(1) für $\mathcal{E} = \mathbb{Q}$ anwenden, erhalten wir als Abschätzung für die Anzahl P_{abs} der beim Lösen von absoluten Normgleichungen mit dem Verfahren von Fincke zu betrachtenden Punkte:

$$P_{\text{abs}} = O((nm)^{nm/2+nm} |\theta| \frac{\mathrm{reg}_{\mathcal{F}/\mathbb{Q}}(\mathcal{F})}{\sqrt{|d_{\mathcal{F}/\mathbb{Q}}|}}). \tag{4-18}$$

Wie bei (4-16) erhalten wir hier

$$P_{\text{abs}} = O((nm)^{nm/2+nm} |\theta| \frac{1}{h_{\mathcal{F}}}). \tag{4-19}$$

Als nächstes wollen wir das für das Lösen von Thue-Gleichungen wichtige Bestimmen von Lösungen in der Gleichungsordnung untersuchen. Im Prinzip ist es möglich, Algorithmus 4.8 direkt zu benutzen: im Schritt (Einheiten) muß lediglich ein unabhängiges Einheitensystem von $U \cap o_{\mathcal{E}}[\beta]$ bestimmt werden. Algorithmus 3.23 würde sich in diesem Fall sogar vereinfachen, da $o_{\mathcal{E}}[\beta]$ freier $o_{\mathcal{E}}$-Modul ist. Bei der Berechnung von Einheiten hat es sich jedoch gezeigt, daß es i.allg. einfacher ist, die Einheiten in der Maximalordnung auszurechnen, da dort effizientere Algorithmen, die z.B. die Dedekindring-Eigenschaften von $o_{\mathcal{F}}$ ausnützen, bekannt sind. Speziell bei den Normgleichungen können wir diese Eigenschaften z.B. dazu ausnutzen, um die Anzahl der nicht assoziierten Lösungen vorher abzuschätzen oder ggf. sogar auszurechnen. Wenn die Anzahl der Lösungen von (4-11) bekannt ist, reduziert sich die Laufzeit drastisch, da wir Algorithmus 4.8 entsprechend früher beenden können. Wie wir diese Informationen auch für das Lösen in Gleichungsordnungen benutzen können, zeigt

Algorithmus 4.12 (Normgleichungen in beliebigen Ordnungen).

(Input): *Zahlkörper $\mathcal{F}/\mathcal{E}$, o eine Ordnung von $\mathcal{F}$und $\theta \in o_{\mathcal{E}}$.*

(Output): *Eine vollständige Menge $L \subset o$ von Lösungen, d.h., für jedes $x \in o$ mit $N_{\mathcal{F}/\mathcal{E}}(x) = \theta$ existiert ein $\tilde{x} \in L$ mit $N_{\mathcal{F}/\mathcal{E}}(\tilde{x}) = \theta$ und $\tilde{x}/x \in o$.*

Bestimme mit Hilfe von Algorithmus 4.8 *eine vollständige Menge* $\tilde{L}$ *von Lösungen in der Maximalordnung.*

Bestimme mit Hilfe von [55, Algorithmus 4.22] *eine Menge* $U_o \subset U^1_{\mathcal{F}}$ *so, daß*

$$U_o = {}^{U^1_{\mathcal{F}}}/_{U^1_{\mathcal{F}} \cap o}$$

gilt.

Setze

$$L \leftarrow \{\epsilon x \mid x \in \tilde{L} \text{ und } \epsilon \in U_o\} \cap o$$

und terminiere.

Beweis. Zu zeigen ist nur, daß die Menge L vollständig ist: Sei $x \in o$ mit $N_{\mathcal{F}/\mathcal{E}}(x) = \theta$ beliebig. Nach Konstruktion gibt es dann ein $\tilde{x} \in \tilde{L}$ mit $N_{\mathcal{F}/\mathcal{E}}(\tilde{x}) = \theta$ und $\tilde{x}/x \in U^1_{\mathcal{F}}$. Daher gibt es ein $\epsilon \in U_o$ mit $\epsilon\tilde{x}/x \in o$; hierfür gilt aber $\epsilon\tilde{x} \in L$. □

Wenn wir uns nun anschauen, wieviele Punkte wir betrachten müssen —

$$P_2 = O(n^{(m+n)/2}|N_{\mathcal{E}/\mathbb{Q}}(\theta)|\frac{\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F}))}{d_{\mathcal{F}}}) + \#U_o\#\tilde{L} \tag{4-20}$$

für Algorithmus 4.12 und

$$P_2 = O(n^{(m+n)/2}|N_{\mathcal{E}/\mathbb{Q}}(\theta)|\frac{\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(U \cap o))}{d_o}) \tag{4-21}$$

bei Algorithmus 4.8 — so scheint sich dieses Vorgehen nur zu lohnen, wenn $\frac{(o_{\mathcal{F}}:o)}{\#U_o} < 1$ gilt. In der Praxis hat sich dagegen Algorithmus 4.12 als überlegen herausgestellt. Hier werden i.allg. viel weniger quadratische Formen betrachtet.

Mit dem nächsten Algorithmus werden wir nun die Lösbarkeit von (4-10) in $\mathcal{F}$ untersuchen. Hier werden wir nur eine Lösung suchen, da es nicht klar ist, was „assoziiert“ für nicht ganze Elemente bedeuten soll.

Im folgenden sei

$$\mathcal{F}/\mathcal{E} \text{ Galois'sch.}$$

Algorithmus 4.13 (Normgleichungen in Körpern).

(Input): *Zahlkörper* $\mathcal{F}/\mathcal{E}$ *Galois'sch sowie* $\theta \in o_{\mathcal{E}}$.

(Output): *Ein* $x \in \mathcal{F}$ *mit* $N_{\mathcal{F}/\mathcal{E}}(x) = \theta$ *oder „Gleichung hat keine Lösung“*

Bestimme eine Menge M *wie in* Satz 4.7.

Für $S_\mathcal{E} := V_\mathcal{E}^\infty \cup \{v_\mathfrak{p} \mid \exists \mathfrak{a} \in M : v_\mathfrak{p}(N_{\mathcal{F}/\mathcal{E}}(\mathfrak{a})) > 0\}$ *und* $S_\mathcal{F}$ *wie in* (2-1) *berechne*

$$U := U^1_{\mathcal{F},S_\mathcal{F}} = \zeta \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_{r_\mathcal{F} - r_\mathcal{E}} \rangle.$$

Setze

$$\mathfrak{b} := \prod_{\mathfrak{P} \in M} \mathfrak{P}^{\lfloor \sum_{i=1}^{r_\mathcal{F} - r_\mathcal{E}} \frac{1}{2} |V_\mathfrak{P}(\epsilon_i)| \rfloor}.$$

Benutze Algorithmus 4.8 *um eine Lösung* $x \in \mathfrak{b}$ *von* (4-10) *zu finden, d.h., beende den Algorithmus, falls* $L \neq \emptyset$ *gilt.*

Gib entweder eine Lösung x *oder „Gleichung hat keine Lösung“ aus.*

Beweis. Sei $x \in \mathcal{F}$ eine Lösung von (4-10). Nach Satz 4.7 gibt es ein $x_1 \in \mathcal{F}$ mit $V_P(x_1) \geq 0$ für $\mathfrak{P} \in V_\mathcal{F} \setminus S_\mathcal{F}$, d.h. $x_1 \in o_\mathcal{F}^S$. Mit Satz 4.1 folgt dann die Existenz von $x_2 \in \mathfrak{b}$. □

Es bleibt noch das Problem, eine geeignete Menge M zu finden. Gute Schranken bekommen wir, falls die Menge M klein ist, d.h. möglichst nur aus den Erzeugern der zyklischen Faktoren der Klassengruppe besteht. Da wir im nächsten Schritt dann $S_\mathcal{F}$-Einheiten berechnen müssen, bietet es sich an, die Klassengruppe zu bestimmen, da es sehr schnelle kombinierte Algorithmen gibt, mit denen zuerst die Klassengruppe bestimmt werden kann und dann, mit den so gewonnenen Daten, die $S_\mathcal{F}$-Einheiten [26].

Andererseits, wenn wir ohnehin die $S_\mathcal{F}$-Einheiten Gruppe für eine genügend große Menge $S_\mathcal{F}$ bestimmt haben, können wir sie auch nutzen, um die Normgleichung direkt zu lösen. Jede Lösung von (4-11) ist eine $S_\mathcal{F}$-Einheit, wenn $S_\mathcal{E}$ alle zur Faktorisierung von θ benötigten Primideale enthält:

Algorithmus 4.14 (Normgleichungen mit $S_\mathcal{F}$-Einheiten).

(Input): *Zahlkörper* $\mathcal{F}/\mathcal{E}$ *sowie* $\theta \in o_\mathcal{E}$.

(Output): *Eine vollständige Menge* $L \subset o_\mathcal{F}$ *von Lösungen, d.h., für jedes* $x \in o_\mathcal{F}$ *mit* $N_{\mathcal{F}/\mathcal{E}}(x) \equiv \theta \mod TU_\mathcal{E}$ *existiert ein* $\tilde{x} \in L$ *mit* $N_{\mathcal{F}/\mathcal{E}}(\tilde{x}) \equiv \theta \mod TU_\mathcal{E}$ *und* $\tilde{x}/x \in o_\mathcal{F}$.

(S-Einheiten): *Setze* $S_\mathcal{E} \leftarrow \{v \in V_\mathcal{E}^{fin.} \mid v(\theta) > 0\} \cup V_\mathcal{E}^\infty$ *und* $S_\mathcal{F}$ *wie in* (2-1). *Berechne Einheiten* ϵ_i $(1 \leq i \leq r_\mathcal{F} - r_\mathcal{E})$ *und* $\tilde{\epsilon}_i$ $(1 \leq i \leq r_\mathcal{E} - 1)$ *für* $A = TU_\mathcal{E}$ *gemäß* Satz 2.5.

(Lösung in $\mathcal{F}$): *Berechne Matrizen* $B \in \mathbb{Z}^{S_\mathcal{E}\times(r_\mathcal{E}-1)}$ *und* $b \in \mathbb{Z}^{S_\mathcal{E}}$ *mit* $B_{v,j} = v(N_{\mathcal{F}/\mathcal{E}}(\tilde{\epsilon}_j))$ *und* $b_v = v(\theta)$

Wenn das lineare Gleichungssystem $Bx = b$ *in* $\mathbb{Z}$ *nicht lösbar ist, setze* $L \leftarrow \emptyset$ *und terminiere, andernfalls sei* $x \in \mathbb{Z}^{r_\mathcal{E}-1}$ *die Lösung.*

Setze $\alpha_0 \leftarrow \prod_{i=1}^{r_\mathcal{E}-1} \tilde{\epsilon}_i^{x_i}$.

(Lösung in $o_\mathcal{F}$): *Berechne Einheiten* $\epsilon_i' \in U_{\mathcal{F},S_\mathcal{F}}^{TU_\mathcal{E}} \setminus U_\mathcal{F}$ $(1 \leq i \leq u := r_\mathcal{F} - r_\mathcal{E} - \#V_\mathcal{F}^\infty + \#V_\mathcal{E}^\infty)$ *mit*

$$U_{\mathcal{F},S_\mathcal{F}}^{TU_\mathcal{E}} / TU_\mathcal{F} = U_\mathcal{F}^{TU_\mathcal{E}} \times \langle \epsilon_1' \rangle \times \cdots \times \langle \epsilon_u' \rangle \tag{4-22}$$

Berechne Matrizen $B \in \mathbb{Z}^{S_\mathcal{F}\times u}$ *und* $b \in \mathbb{Z}^{S_\mathcal{F}}$ *mit* $B_{V,j} = V(\epsilon_j')$ *und* $b_V = V(\alpha_0)$.

Setze

$$L_0 \leftarrow \{x \in \mathbb{Z}^u \mid Bx + b \geq 0\}, \tag{4-23}$$

$$L \leftarrow \{\alpha_0 \prod_{i=1}^{u} {\epsilon_i'}^{x_i} \mid x \in L_0\}$$

und terminiere.

Beweis. Da $N_{\mathcal{F}/\mathcal{E}}(\alpha) \equiv N_{\mathcal{F}/\mathcal{E}}(\alpha_0) \equiv \theta \mod TU_\mathcal{E}$ für jedes $\alpha \in L$ gilt, bleibt noch $\#L \leq \infty$ und die „Vollständigkeit“ von L zu zeigen.

Da das Produkt in (4-22) direkt ist, gilt für α_1, $\alpha_2 \in L$:

$$\frac{\alpha_1}{\alpha_2} \in U_{\mathcal{F},S_\mathcal{F}}^{TU_\mathcal{E}} \setminus U_\mathcal{F} \cup \{1\},$$

d.h., α_1 und α_2 sind nicht assoziiert. Da es nur endlich viele nicht-assoziierte ganze Lösungen gibt und nach Konstruktion $L \subseteq o_\mathcal{F}$ gilt, folgt $\#L < \infty$.

Sei nun $\alpha \in o_\mathcal{F}$ mit $N_{\mathcal{F}/\mathcal{E}}(\alpha) \equiv \theta \mod TU_\mathcal{E}$ beliebig fixiert. Aus $V(\alpha) \geq 0$ für jedes $V \in V_\mathcal{F}^{\text{fin.}}$ erhalten wir $\{V \in V_\mathcal{F}^{\text{fin.}} \mid V(\alpha) > 0\} \subseteq S_\mathcal{F}$, Satz 2.5 impliziert

$$\alpha = \prod_{i=1}^{r_\mathcal{F}-r_\mathcal{E}} \epsilon_i^{x_i} \prod_{i=1}^{r_\mathcal{E}-1} \tilde{\epsilon}_i^{\tilde{x}_i}$$

mit geeigneten Exponenten x_i, $\tilde{x}_i \in \mathbb{Z}$. Weiter folgt aus $N_{\mathcal{F}/\mathcal{E}}(\epsilon_i) \in TU_\mathcal{E}$, daß $(\tilde{x}_i)_{1\leq i\leq r_\mathcal{E}-1}$ eine Lösung von $Bx = b$ in Schritt (Lösung in $\mathcal{F}$) ist. Da B von vollem

Rang ist, gilt $\prod_{i=1}^{r_{\mathcal{E}}-1} \tilde{\epsilon}_i^{\tilde{x}_i} = \alpha_0$. Wiederum mit der Direktheit von (4-22) folgt die Existenz einer Einheit $\epsilon \in U_{\mathcal{F}} \cap U_{\mathcal{F},S_{\mathcal{F}}}^{TU_{\mathcal{E}}}$ sowie Exponenten $y_i \in \mathbb{Z}$ $(1 \leq i \leq u)$ mit

$$\prod_{i=1}^{r_{\mathcal{F}}-r_{\mathcal{E}}} \epsilon_i^{x_i} = \epsilon \prod_{i=1}^{u} \epsilon'^{y_i}.$$

Mit $\alpha \in o_{\mathcal{F}}$ folgt daher $(y_i)_{1 \leq i \leq u} \in L_0$. $\square$

Eine Variante dieses Algorithmus ist offenbar auch geeignet, um Algorithmus 4.13 zu ersetzen. Wir müssen lediglich die Menge $S_{\mathcal{E}}$ wie dort beschrieben erweitern und dann nach Schritt (Lösung in $\mathcal{F}$) terminieren. Der kritische Schritt in 4.14 ist (Lösung in $o_{\mathcal{F}}$). Hier können wir Algorithmus 3.26 einsetzen, haben aber die in Bemerkung 3.27.(2) beschriebenen Probleme, wenn u groß wird. Sind wir nur daran interessiert, die Lösbarkeit zu überprüfen und ggf. eine Lösung zu finden, so können wir mit dem Simplex-Algorithmus (z.B. [15, 6.3]) einen (extremalen) Punkt in L_0 suchen.

Eine weitere Variante von (4-11) ergibt sich, wenn wir statt nach Lösungen in $o_{\mathcal{F}}$ nach Lösungen in einem beliebigen Modul M suchen. Da die Einheiten i.allg. nicht auf M operieren, ist es uns nicht möglich ohne weitere Informationen den Bereich, den wir durchsuchen müssen, einzugrenzen. Wenn wir jedoch Schranken für die Lösung (alle Lösungen) kennen, können wir die Menge $\Gamma_1 + \frac{1}{n} L_1(\theta)$ aus Algorithmus 4.8.(Ceiling) durch die durch die Schranken gegebene Menge ersetzen. Dies ermöglicht es, die hier vorgestellten Verfahren z.B. zum Lösen von Thue-Gleichungen einzusetzen. Denn dort liefert die Theorie der Thue-Gleichungen Schranken für mögliche Lösungen.

KAPITEL V

Beispiele

Hier präsentieren wir einige Beispiele, die sowohl die Vorteile der neuen Methoden als auch deren Grenzen demonstrieren sollen. Wir beginnen mit dem Reduktionsalgorithmus 3.29.

1. Reduktion

Den Reduktionsalgorithmus werden wir in zwei Anwendungen demonstrieren: zum einen zum Beschleunigen des Auszählens (analog [20, (2.15)]) und zum anderen zum Auffinden eines „schöneren“ Polynoms, um einen Zahlkörper zu erzeugen.

1.1. „Schönere“ Polynome. Bei Problemen, bei denen das erzeugende Polynom der Relativerweiterung ausgerechnet oder von einem Anwender vorgegeben wird, stellt sich oft das Problem, daß dieses spezielle Polynom „schlecht konditioniert ist“, d.h., nachfolgende Berechnungen brauchen zu viel Zeit. Oft kann dies dadurch beschleunigt werden, daß ein anderes Polynom mit kleineren Koeffizienten (weniger Stellen) oder kleinerem Index (kleinerer Norm des Indexideals) benutzt wird. Um ein solches Polynom zu finden, gibt es auch im absoluten Fall keinen Algorithmus, der garantiert, daß das bestmögliche Polynom gefunden wird. Es ist nicht einmal klar, was „ein“ bestmögliches Polynom sein soll. Die Verfahren, mit denen in der Praxis versucht wird, ein „besseres“ Polynom zu finden, berechnen eine LLL-reduzierte reelle Basis der Maximalordnung und testen dann, ob die neuen Basiselemente „bessere“ definierende Polynome liefern. Da es passieren kann, daß kein Basiselement primitiv ist (d.h. den Körper erzeugt), werden „kleine“ Linearkombinationen der Basiselemente betrachtet. Nach dem Satz von Sonn und Zassenhaus [46, 2 (12.23)] ist dies ausreichend, da es unter allen Linearkombinationen von Basiselementen mit den Koeffizienten 0 und 1 mindestens ein primitives Element gibt.

Um nun ein „schöneres“ Polynom zu finden, gehen wir wie folgt vor: Zunächst berechnen wir eine geeignete Oberordnung o der Gleichungsordnung; i.allg. ist dies die Maximalordnung. Dann erzeugen wir das zugehörige Gitter wie in Beispiel 3.10.(1), das wir mit Hilfe von Algorithmus 3.29 reduzieren. Sei nun $(\mathfrak{a}_i, \alpha_i)$ eine reduzierte Pseudobasis für o für die o.B.d.A. $\alpha_i \in o$ gelten soll. Für jedes primitive $x = \sum_{i=1}^{n} x_i \alpha_i$ mit $x_i \in \{-1, 0, 1\}$ berechnen wir nun den Index der von x erzeugten Gleichungsordnung in o. Unter allen x mit minimalem Index wählen wir nun eines mit minimalem $\tau \circ \mathrm{T}_2^{\mathcal{F}/\mathcal{E}}(x)$. Wenn der Körpergrad zu groß wird, um alle diese 3^n Elemente zu testen, hat es sich bewährt, abzubrechen, wenn der Minimalindex in den letzten 20 (30, 40, ...) Versuchen nicht mehr kleiner geworden ist.

Im Unterschied zu der absoluten Variante dieses Algorithmus hat es sich gezeigt, daß Algorithmus 3.29 wesentlich empfindlicher auf schlecht konditionierte Eingangspseudobasen reagiert, d.h., wenn das Relativpolynom extrem schlecht konditioniert ist, kann es auf diese Art nicht (oder nur minimal) verbessert werden.

Die ersten Beispiele sind erzeugende Polynome für Hilbert'sche Klassenkörper, wie sie mit dem in [16] beschriebenen Verfahren berechnet worden sind.

Wir starten mit einem kubischen Körper mit Klassenzahl 3:

$\mathcal{E} := \mathbb{Q}(\alpha)$	$\alpha^3 + \alpha^2 - 11\alpha + 37 = 0$
$\omega_1 = 1,\ \omega_2 = \alpha,\ \omega_3 = \frac{\alpha^2-1}{2}$	
$[o_{\mathcal{E}} : \mathbb{Z}[\alpha]] = 2,\ d_{\mathcal{E}} = -9748$	
$\mathcal{F} := \mathcal{E}(\beta)$	$\beta^3 + (18759\omega_1 - 1362\omega_2 - 2256\omega_3)\beta$ $- (495907\omega_1 + 338576\omega_2 + 101840\omega_3) = 0$
$\mu_1 = 1$	$\mathfrak{a}_1 = o_{\mathcal{E}}$
$\mu_2 = 2\omega_2 + 2\omega_3 + \beta$	$\mathfrak{a}_2 = \frac{1}{3} o_{\mathcal{E}}$
$\mu_3 = 5\omega_1 + 4\omega_2 + 8\omega_3 + (\omega_2 + \omega_3)\beta + \beta^2$	$\mathfrak{a}_3 = \frac{1}{9} o_{\mathcal{E}}$
$[o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]] = 27 o_{\mathcal{E}},\ N_{\mathcal{E}/\mathbb{Q}}([o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]]) = 19683$	

Wir erhalten folgende reduzierte Darstellung:

$\mathcal{F} = \mathcal{E}(\beta)$	$\beta^3 + (7\omega_1 - \omega_2 + \omega_3)\beta^2 - (165\omega_1 + 22\omega_2 - 21\omega_3)\beta + (1329\omega_1 - 10\omega_2 - 82\omega_3) = 0$	
$\mu_1 = 1$		$\mathfrak{a}_1 = o_\mathcal{E}$
$\mu_2 = \frac{1}{5}((46\omega_1 - 23\omega_2 + 11\omega_3) + (6\omega_1 - 3\omega_2 + \omega_3)\beta)$		$\mathfrak{a}_2 = o_\mathcal{E} + \frac{1}{6}(\omega_1 + 3\omega_2 - 2\omega_3)o_\mathcal{E}$
$\mu_3 = \frac{1}{25}((1223\omega_1 - 489\omega_2 + 408\omega_3) - (174\omega_1 - 82\omega_2 + 54\omega_3)\beta - (47\omega_1 - 21\omega_2 + 12\omega_3)\beta^2)$		$\mathfrak{a}_3 = o_\mathcal{E} + \frac{1}{4}(\omega_1 - 2\omega_2 + \omega_3)o_\mathcal{E}$
$[o_\mathcal{F} : o_\mathcal{E}[\beta]] = 125 o_\mathcal{E} + (61\omega_1 + \omega_2 - \omega_3)o_\mathcal{E}$, $N_{\mathcal{E}/\mathbb{Q}}([o_\mathcal{F} : o_\mathcal{E}[\beta]]) = 125$		

Nun ein kubischer Körper mit V_4 als Klassengruppe:

$\mathcal{E} := \mathbb{Q}(\alpha)$	$\alpha^3 + \alpha^2 - 92\alpha + 236 = 0$	
$\omega_1 = 1$, $\omega_2 = \alpha$, $\omega_3 = \frac{2-\alpha+\alpha^2}{4}$		
$[o_\mathcal{E} : \mathbb{Z}[\alpha]] = 4$, $d_\mathcal{E} = 76729$		
$\mathcal{F} := \mathcal{E}(\beta)$	$\beta^4 - (21684\omega_1 - 8992\omega_2 + 3688\omega_3)\beta^2 + (648910592\omega_1 - 308968480\omega_2 + 134927632\omega_3) = 0$	
$\mu_1 = 1$		$\mathfrak{a}_1 = o_\mathcal{E}$
$\mu_2 = \beta$		$\mathfrak{a}_2 = \frac{1}{2}o_\mathcal{E} + \frac{1}{26}(4\omega_1 + 3\omega_2 + \omega_3)o_\mathcal{E}$
$\mu_3 = (600\omega_1 + 40\omega_2 + 4\omega_3) + 26\beta + \beta^2$		$\mathfrak{a}_3 = \frac{1}{8}o_\mathcal{E} + \frac{1}{1352}(74\omega_1 + 10\omega_2 - \omega_3)o_\mathcal{E}$
$\mu_4 = (23207296\omega_1 + 64\omega_2 + 8\omega_3) + (1028796\omega_1 + 40\omega_2 + 4\omega_3)\beta + \beta^3$		$\mathfrak{a}_4 = \frac{1}{16}o_\mathcal{E} + \frac{1}{50759488}(1353829\omega_1 - 371426\omega_2 - \omega_3)o_\mathcal{E}$
$[o_\mathcal{F} : o_\mathcal{E}[\beta]] = 1784297522176 o_\mathcal{E} + (34924894208\omega_1 + 35982444544\omega_2 + 263697664\omega_3)o_\mathcal{E}$, $N_{\mathcal{E}/\mathbb{Q}}([o_\mathcal{F} : o_\mathcal{E}[\beta]]) = 19762137087852150784$		

Nach der Reduktion, die wir in diesem Fall in mehreren Schritten durchführen, wobei wir die Teilkörper, die den zyklischen Untergruppen entsprechen, berücksichtigen, erhalten wir:

$\mathcal{F} = \mathcal{E}(\beta)$	$\beta^4 + (2\omega_1 - 2\omega_2)\beta^3 - (257\omega_1 - 14\omega_2 - 14\omega_3)\beta^2$ $+ (354\omega_1 + 26\omega_2 - 30\omega_3)\beta + (12309\omega_1 - 592\omega_2 - 666\omega_3) = 0$
$\mu_1 = 1$	$\mathfrak{a}_1 = o_{\mathcal{E}}$
$\mu_2 = \beta$	$\mathfrak{a}_2 = o_{\mathcal{E}}$
$\mu_3 = 71 + 31\beta + \beta^2$	$\mathfrak{a}_3 = \frac{1}{2}o_{\mathcal{E}} + \frac{1}{76}(15\omega_1 - 12\omega_2 - \omega_3)o_{\mathcal{E}}$
$\mu_4 = 15798322 + 52369461\beta$ $+ 330469\beta^2 + \beta^3$	$\mathfrak{a}_4 = \frac{1}{2}o_{\mathcal{E}} + \frac{1}{52861876}$ $(8982425\omega_1 - 1504142\omega_2 + \omega_3)o_{\mathcal{E}}$
$[o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]] = 4017502576 o_{\mathcal{E}} + (515467344\omega_1 - 3555016\omega_2 + 1718332\omega_3)o_{\mathcal{E}}$, $N_{\mathcal{E}/\mathbb{Q}}([o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]]) = 64280041216$	

Das nächste Beispiel, ein Klassenkörper zu einem kubischen Körper mit C_6 als Klassengruppe:

$\mathcal{E} := \mathbb{Q}(\alpha)$	$\alpha^3 - 26\alpha + 26 = 0$
$o_{\mathcal{E}} = \mathbb{Z}[\alpha]$, $d_{\mathcal{E}} = 52052$	
$\mathcal{F} := \mathcal{E}(\beta)$	$\beta^6 - (27 - 162\alpha + 156\alpha^2)\beta^4 + (2696 - 5392\alpha + 2696\alpha^2)\beta^3$ $+ (316611 - 474660\alpha + 164280\alpha^2)\beta^2$ $- (15909096 - 21497904\alpha + 5993208\alpha^2)\beta$ $+ (179567975 - 230236702\alpha + 55754180\alpha^2) = 0$
$\mu_1 = 1$	$\mathfrak{a}_1 = o_{\mathcal{E}}$
$\mu_2 = 1 + \beta$	$\mathfrak{a}_2 = o_{\mathcal{E}} + \frac{1}{2}\alpha o_{\mathcal{E}}$
$\mu_3 = (3 + 2\alpha^2) + 2\alpha^2\beta + \beta^2$	$\mathfrak{a}_3 = \frac{1}{6}o_{\mathcal{E}} + \frac{1}{12}\alpha^2 o_{\mathcal{E}}$
$\mu_4 = (15+4\alpha+7\alpha^2)+(3+4\alpha)\beta+(1+\alpha^2)\beta^2+\beta^3$	$\mathfrak{a}_4 = \frac{1}{12}o_{\mathcal{E}} + \frac{1}{24}\alpha^2 o_{\mathcal{E}}$
$\mu_5 = (249+52\alpha+197\alpha^2)+(348+128\alpha+67\alpha^2)\beta$ $+(42+52\alpha+27\alpha^2)\beta^2+13\alpha^2\beta^3+\beta^4$	$\mathfrak{a}_5 = \frac{1}{360}o_{\mathcal{E}}$
$\mu_6 = (75442207413663971255+262\alpha+174\alpha^2)$ $+(13897937400522597750 1+162\alpha+254\alpha^2)\beta$ $+(5721673554934634426+50\alpha+22\alpha^2)\beta^2$ $+(2562641507007649960 2+6\alpha+6\alpha^2)\beta^3$ $+415978533546881951\beta^4+\beta^5$	$\mathfrak{a}_6 = \frac{1}{360}o_{\mathcal{E}} + \frac{1}{3101472918460214848 80}$ $(61409109199271370-82813770501046977\alpha+\alpha^2)o_{\mathcal{E}}$
$[o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]] = 16078035609297753776179200 o_{\mathcal{E}}$ $+ (7989247021565132057088 00 + 37324800\alpha + 37324800\alpha^2)o_{\mathcal{E}}$, $N_{\mathcal{E}/\mathbb{Q}}([o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]]) = 223989657036149425820570752835911680000 00$	

Reduziert:

$\mathcal{F} = \mathcal{E}(\beta)$	$\beta^6 + (1-\alpha)\beta^5 - (19+\alpha-\alpha^2)\beta^4 + (43-2\alpha-\alpha^2)\beta^3$ $- (19+\alpha-\alpha^2)\beta^2 + (1-\alpha)\beta + 1 = 0$
$\mu_1 = \frac{1}{25}(1 + (15+9\alpha+23\alpha^2)\beta$ $+ (22+\alpha+4\alpha^2)\beta^2$ $+ (11+8\alpha+6\alpha^2)\beta^3$ $+ (7+16\alpha^2)\beta^4$ $+ (22+21\alpha+21\alpha^2)\beta^5)$	$\mathfrak{a}_1 = 25o_{\mathcal{E}} + (1-9\alpha-3\alpha^2)o_{\mathcal{E}}$
$\mu_i = \beta^{i-1} \quad (2 \le i \le 6)$	$\mathfrak{a}_i = o_{\mathcal{E}} \quad (1 \le i \le 6)$
$[o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]] = 25o_{\mathcal{E}} + (181-9\alpha-6\alpha^2)o_{\mathcal{E}}$, $N_{\mathcal{E}/\mathbb{Q}}([o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]]) = 25$	

Als letztes ein Beispiel vom Gesamtgrad 12 von Cartwright und Steger ([9]): Seien $s^2 = -23$, $s' = \frac{s-1}{2}$, $u^2 = -83$ und $u' = \frac{u-1}{2}$. Wir betrachten den Körper $\mathcal{E} = \mathbb{Q}(s', u')$ und darüber die kubische Erweiterung $\mathcal{F} = \mathcal{E}(\beta)$ mit

$$\beta^3 + (-2s'+6)\beta^2 - (18s'-18)\beta - (90s'-54) = 0.$$

$\mathcal{F}$ ist zyklisch über $\mathcal{E}$ und besitzt über $\mathbb{Q}$ die Galoisgruppe D_6. Die Klassengruppe von $\mathcal{F}$ ist isomorph zu $C_{18} \times C_{18}$.

In einem ersten Reduktionsschritt wird der Körper vom Grad 4 in eine schönere Darstellung gebracht: Es gilt $\mathcal{E}_1 = \mathbb{Q}(s') = \mathbb{Q}(\alpha_1)$ mit $\alpha_1^2 - \alpha_1 + 6 = 0$, $\mathcal{E} = \mathbb{Q}(s', u') = \mathcal{E}_1(\alpha_2)$ mit $\alpha_2^2 + \alpha_2 + 21 = 0$ und

$\mathcal{E} = \mathbb{Q}(\alpha)$	$\alpha^4 + 4\alpha^3 + 59\alpha^2 + 110\alpha + 279 = 0$
$\omega_1 = 1$, $\omega_2 = \alpha$, $\omega_3 = \frac{1}{2}(1+\alpha+\alpha^2)$, $\omega_4 = \frac{1}{30}(24+11\alpha+3\alpha^2+\alpha^3)$	
$[o_{\mathcal{E}} : \mathbb{Z}[\alpha]] = 60$, $d_{\mathcal{E}} = 3644281$	

Für s' und u' erhalten wir folgende Darstellungen: $s' = -\omega_1 - \omega_2 - \omega_4$ und $u' = -2\omega_1 - 2\omega_2 - \omega_4$. Damit folgt für $\mathcal{F}$:

$\mathcal{F} := \mathcal{E}(\beta)$	$\beta^3 + (8\omega_1 + 2\omega_2 + 2\omega_4)\beta^2 + (36\omega_1 + 18\omega_2 + 18\omega_4)\beta$ $+ (36\omega_1 + 90\omega_2 + 90\omega_4) = 0$
$\mu_1 = 1$	$\mathfrak{a}_1 = o_{\mathcal{E}}$
$\mu_2 = \beta$	$\mathfrak{a}_2 = o_{\mathcal{E}} + \frac{1}{6}(\omega_1 - \omega_3 - 2\omega_4)o_{\mathcal{E}}$
$\mu_3 = (4680\omega_1 + 1368\omega_2)$ $+ (860\omega_1 + 98\omega_2 + 2\omega_4)\beta + \beta^2$	$\mathfrak{a}_3 = \frac{1}{3}o_{\mathcal{E}} + \frac{1}{5976}(375\omega_1 - 911\omega_2 + \omega_4)o_{\mathcal{E}}$
$[o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]] = 35856o_{\mathcal{E}} + (-9480\omega_1 + 1128\omega_2 + 3\omega_3 + 3\omega_4)o_{\mathcal{E}}$, $N_{\mathcal{E}/\mathbb{Q}}([o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]]) = 11570874624$, $d_{\mathcal{F}} = 4o_{\mathcal{E}}$	

Reduzieren:

$\mathcal{F} = \mathcal{E}(\beta)$	$\beta^3 + (2\omega_1 - \omega_2 - \omega_4)\beta^2 - (6\omega_1 - \omega_2 - \omega_4)\beta - (18\omega_1 + 3\omega_2 + 3\omega_4) = 0$
$\mu_1 = 1$	$\mathfrak{a}_1 = o_{\mathcal{E}}$
$\mu_2 = 1 + \beta$	$\mathfrak{a}_2 = \frac{1}{2}(2\omega_1 - \omega_2 - \omega_4)o_{\mathcal{E}} + (\omega_1 - \omega_4)o_{\mathcal{E}}$
$\mu_3 = \frac{1}{996}((4806\omega_1 + 579\omega_2 + 180\omega_3 - 129\omega_4) + (3256\omega_1 + 212\omega_2 + 110\omega_3 - 46\omega_4)\beta - (34\omega_1 + 11\omega_2 + 2\omega_3 + 5\omega_4)\beta^2)$	$\mathfrak{a}_3 = (34\omega_1 + 11\omega_2 + 2\omega_3 + 5\omega_4)o_{\mathcal{E}} + \frac{1}{2}(75\omega_1 - 5\omega_2 - 2\omega_3 - 21\omega_4)o_{\mathcal{E}}$
$[o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]] = 1992 o_{\mathcal{E}} + (420\omega_1 + 134\omega_2 + 78\omega_3 + 338\omega_4)o_{\mathcal{E}}$, $N_{\mathcal{E}/\mathbb{Q}}([o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]]) = 15872256$	

Hieraus erhalten wir folgende absolute Darstellung:

$\mathcal{F} = \mathbb{Q}(\alpha)$	$\alpha^{12} + 45\alpha^{10} + 172\alpha^9 + 90\alpha^8 - 264\alpha^7 + 2321\alpha^6 + 5772\alpha^5 - 6186\alpha^4 + 6668\alpha^3 + 24465\alpha^2 - 36972\alpha + 13689 = 0$
$[o_{\mathcal{F}} : \mathbb{Z}[\alpha]] = 2294947495113882473087308$8	
$d_{\mathcal{F}/\mathbb{Q}} = 123901206583479910504 96$	

1.2. Schnelleres Auszählen. Der für die Gesamtlaufzeit von Algorithmus 4.8 und 4.13 entscheidende Teil ist das Auszählen mit Hilfe von Algorithmus 3.23.

Wir betrachten die gewichtete quadratische Form aus Beispiel 3.10.(1), wobei wir die Gewichte von der Form $w_{i,j} = \lambda_i^{r_{i,j}}$ wie in Algorithmus 4.8.(Auszählen) wählen.

Zunächst betrachten wir den folgenden Körper:

$\mathcal{E} := \mathbb{Q}(\alpha)$	$\alpha^2 - \alpha - 36 = 0$
$o_{\mathcal{E}} = \mathbb{Z}[\alpha]$, $d_{\mathcal{F}} = 145$	
$\mathcal{F} := \mathcal{E}(\beta)$	$\beta^2 + 3\beta - 39 = 0$
$\mu_1 = 1$	$\mathfrak{a}_1 = o_{\mathcal{E}}$
$\mu_2 = 1 - \beta$	$\mathfrak{a}_2 = o_{\mathcal{E}} + \frac{1}{5}(2 + \alpha)o_{\mathcal{E}}$
$[o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]] = 5o_{\mathcal{E}} + (2 + \alpha)o_{\mathcal{E}}$, $N_{\mathcal{E}/\mathbb{Q}}([o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]]) = 5$	
$d_{\mathcal{F}} = 33 o_{\mathcal{E}}$	

Die Tabelle ist wie folgt aufgebaut: In der 1. Spalte stehen die λ_i, $1 \le i \le r_1 + r_2$, dann kommen die Exponenten $r_{i,j}$, $1 \le i \le n$, und die obere Schranke fürs

Auszählen. Mit „next“ ist die Gesamtzahl aller Punkte aus den Koeffizientenidealen gemeint, die untersucht werden mußten, insbesondere auch die, die nicht zu Lösungen geführt haben. „Punkte“ bezeichnet die Anzahl der Lösungen, „Zeit“ die Zeit zum Auszählen inklusive der Zeit zum Reduzieren. Die Angaben in den letzten beiden Spalten beziehen sich auf Auszählen mit Reduktion, die beiden davor auf Auszählen ohne Reduktion.

<table>
<tr><th>λ_i</th><th>$r_{i,j}$
$r_{i,j}$</th><th>c_i</th><th>next
Punkte</th><th>Zeit ohne
Reduktion</th><th>next
Punkte</th><th>Zeit mit
Reduktion</th></tr>
<tr><td>8,3146</td><td>0
0</td><td>115,93</td><td rowspan="2">42
39</td><td rowspan="2">0,21sec</td><td rowspan="2">42
39</td><td rowspan="2">0,36sec</td></tr>
<tr><td>8,3146</td><td>0
0</td><td>129,50</td></tr>
<tr><td>8,3146</td><td>2
-2</td><td>115,93</td><td rowspan="2">90
59</td><td rowspan="2">0,68sec</td><td rowspan="2">66
59</td><td rowspan="2">0,48sec</td></tr>
<tr><td>8,3146</td><td>1
-1</td><td>129,50</td></tr>
<tr><td>8,3146</td><td>3
-3</td><td>115,93</td><td rowspan="2">276
29</td><td rowspan="2">3,41sec</td><td rowspan="2">42
29</td><td rowspan="2">0,61sec</td></tr>
<tr><td>8,3146</td><td>2
-2</td><td>129,50</td></tr>
<tr><td>8,3146</td><td>1
-1</td><td>879,86</td><td rowspan="2">1302
849</td><td rowspan="2">7,55sec</td><td rowspan="2">906
849</td><td rowspan="2">2,60sec</td></tr>
<tr><td>8,3146</td><td>3
-3</td><td>469,15</td></tr>
</table>

Als nächstes betrachten wir einen Körper vom Absolutgrad 6 über $\mathbb{Q}$.

<table>
<tr><td>$\mathcal{E} := \mathbb{Q}(\alpha)$</td><td colspan="2">$\alpha^2 + 17 = 0$</td></tr>
<tr><td colspan="3">$o_{\mathcal{E}} = \mathbb{Z}[\alpha]$, $d_{\mathcal{E}} = -68$</td></tr>
<tr><td>$\mathcal{F} := \mathcal{E}(\beta)$</td><td colspan="2">$\beta^3 + (5 - 19\alpha)\beta^2 + (2 + 14\alpha)\beta - (18 + 2\alpha) = 0$</td></tr>
<tr><td colspan="2">$\mu_1 = 1$</td><td>$\mathfrak{a}_1 = o_{\mathcal{E}}$</td></tr>
<tr><td colspan="2">$\mu_2 = \beta$</td><td>$\mathfrak{a}_2 = o_{\mathcal{E}} + \frac{1}{2}(1 + \alpha)o_{\mathcal{E}}$</td></tr>
<tr><td colspan="2">$\mu_3 = \beta^2$</td><td>$\mathfrak{a}_3 = \frac{1}{2}o_{\mathcal{E}}$</td></tr>
<tr><td colspan="3">$[o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]] = 4o_{\mathcal{E}} + (2 + 2\alpha)o_{\mathcal{E}}$, $N_{\mathcal{E}/\mathbb{Q}}([o_{\mathcal{F}} : o_{\mathcal{E}}[\beta]]) = 8$</td></tr>
<tr><td colspan="3">$d_{\mathcal{F}} = (-392164 + 982235\alpha)o_{\mathcal{E}}$</td></tr>
</table>

12,1179	0 0 0	7324,56	10170 6614	33sec	10170 6614	34sec
12,1179	2 0 -2	7324,56	870 264	4,28sec	461 264	2,66sec
12,1179	4 0 -4	7324,56	58532 21	384sec	7387 21	22sec

An diesen beiden Beispielen zeigt sich, daß Algorithmus 3.29 nötig ist, um schlecht gewichtete Formen überhaupt auszählen zu können. Da bei allen Beispielen die Ausgangsbasis reduziert ist, tritt bei nicht gewichteten Formen (Exponenten 0) kein positiver Effekt auf; die Laufzeit verlängert sich um die Zeit für die Reduktion.

2. Normgleichungen

Bei den Normgleichungen müssen wir zwischen verschiedenen Fragestellungen unterscheiden, da die Algorithmen 4.8 und 4.14 stark unterschiedlich auf die verschiedenen Probleme reagieren. Ein direkter Vergleich der Laufzeiten ist etwas problematisch, da unterschiedlich viele Körperinvarianten benötigt werden, und sich die Relationen daher verschieben können, wenn in einem Körper mehrere Normgleichungen gelöst werden. Die Zeiten sind jeweils ohne die Zeit zum Ausrechnen der Maximalordnungen und der Einheiten angegeben. In allen Beispielen wurden die Einheiten mit einem kombinierten Einheiten– und Klassengruppenalgorithmus berechnet, so daß auch die für Algorithmus 4.14 benötigten Informationen bereits vorhanden waren.

Unabhängig von der angegebenen Darstellung der Körper verwenden die Algorithmen teilweise andere, reduzierte Darstellungen, was sich einerseits auf die Körper selbst bezieht (Algorithmus 4.14 z.B. rechnet in absoluten Darstellungen, da die entsprechenden Daten nicht relativ bereitgestellt werden können. Die zugehörigen Probleme sind für Relativerweiterungen noch nicht konstruktiv gelöst worden.) als auch auf die Darstellung der algebraischen Zahlen (teilweise wird intern eine Produktdarstellung verwendet, d.h., alle Zahlen werden als Exponentenvektoren für ein geeignetes multiplikatives Erzeugendensystem gespeichert), so daß kurze Laufzeiten auch die Existenz geeigneter Datenstrukturen wiederspiegeln.

Wir beginnen mit einem CM-Körper [31, Beispiel 1, Seite 84]:

$\mathcal{E} := \mathbb{Q}(\alpha)$	$\alpha^2 - 19\alpha + 86 = 0$
$o_{\mathcal{E}} = \mathbb{Z}[\alpha]$, $d_{\mathcal{E}} = 17$	
$\mathcal{F} := \mathcal{E}(\beta)$	$\beta^2 + (18 - 2\alpha)\beta + \alpha = 0$
$o_{\mathcal{F}} = \mathcal{E}[\beta]$, $d_{\mathcal{F}} = -20 o_{\mathcal{E}}$	

Da $\mathcal{F}$ ein CM-Körper ist, müssen wir in Algorithmus 4.8 nur eine quadratische Form betrachten.

θ	$N_{\mathcal{E}/\mathbb{Q}}(\theta)$	$\#L$	4.8	4.14
$35 - 3\alpha$	4	1	0,5	1,5
-3	9	0	0,4	0,4
$14 - \alpha$	16	1	0,4	1,4
$130 - 11\alpha$	136	0	0,5	0,2
$(4 + 4\alpha)$	1696	0	1,0	0,3
$-(14 - 11\alpha)$	7676	0	2,7	0,7
$-(2 + 10\alpha)$	8984	2	3,2	2,1
$-(8 - 15\alpha)$	17134	0	5,8	0,6
$-(10 - 19\alpha)$	27536	2	8,8	2,0
$-(17 + 20\alpha)$	41149	2	13,0	2,0
$35337 - 3048\alpha$	1233369	8	360	3,1

(In den letzten beiden Spalten steht die Laufzeit in Sekunden der entsprechenden Algorithmen.) Während die Laufzeit von Algorithmus 4.8 etwa linear in $N_{\mathcal{E}/\mathbb{Q}}(\theta)$ zu sein scheint, ist die von 4.14 annähernd konstant. Für kleine θ, die Lösungen haben, ist daher 4.8 vorzuziehen. Auch wenn wir nur an einer Lösung interessiert sind und wissen, daß sie existiert, ist 4.8 oft vorzuziehen; im letzten Beispiel benötigen wir nur 1,3 sec. um die erste Lösung zu finden. Bei zufälligen rechten Seiten ist Algorithmus 4.14 in jedem Fall vorzuziehen, i.allg. kann dort schon nach dem Schritt (Lösung in $\mathcal{F}$) abgebrochen werden.

Das nächste Beispiel ist [18] entnommen, es zeigt, daß die in den letzten Kapiteln bereitgestellte Theorie [18, Algorithm 6.1] deutlich verbessert.

$\mathcal{E} := \mathbb{Q}(\alpha)$	$\alpha^3 + 2\alpha^2 + -1\alpha + 2 = 0$
$\omega_1 = 1$, $\omega_2 = \alpha$, $\omega_3 = \frac{\alpha+\alpha^2}{2}$	
$[o_{\mathcal{E}} : \mathbb{Z}[\alpha]] = 2$, $d_{\mathcal{E}} = -59$	
$\mathcal{F} := \mathcal{E}(\beta)$	$\beta^3 + \beta^2 + (\omega_1 + 2\omega_2 + 3\omega_3)\beta - (2\omega_1 - \omega_3) = 0$
$o_{\mathcal{F}} = o_{\mathcal{E}}[\beta]$, $d_{\mathcal{F}} = (15\omega_1 - 48\omega_2 - 48\omega_3) o_{\mathcal{E}}$	

Für die Regulatoren gilt $\mathrm{reg}_{\mathcal{F}/\mathbb{Q}} \sim 31,412$, $\mathrm{reg}_{\mathcal{F}/\mathcal{E}} \sim 9,928$ und $\mathrm{reg}_{\mathcal{E}/\mathbb{Q}} \sim 0,791$, so daß nach Satz 2.9 die Norm $U_{\mathcal{F}}$ surjektiv auf $U_{\mathcal{E}}$ abbildet. Während der in [18, Algorithm 6.1] vorgestellte Algorithmus noch 14289 quadratische Formen auszählen mußte, kommt Algorithmus 4.8 mit 133 aus. Da der wesentliche Unterschied dieser Algorithmen in der Verwendung der Relativeinheiten liegt, illustriert dies deren Wichtigkeit.

θ	$N_{\mathcal{E}/\mathbb{Q}}(\theta)$	$\#L$	4.8	4.14
$\omega_2 + 2\omega_3$	8	1	6144	4,5
8	512	1	60 Std	11
12326391000	1872870801843041394471000000000	320	10^{23} Jahre	118

(Die Zeit für 4.8 im letzten Beispiel ist natürlich nur geschätzt, sie ergibt sich daraus, daß die Laufzeit im wesentlichen linear von $N_{\mathcal{E}/\mathbb{Q}}(\theta)$ abhängt.) Wenn wir mit einer Lösung zufrieden sind, können wir die Zeit in dem ersten Fall auf 2,6 sec. und im zweiten auf 5 sec. reduzieren, wobei diese Zeiten „zufällig“ sind, sie hängen ausschließlich von der in Algorithmus 3.23 gewählten Reihenfolge, die Mengen K_i zu durchlaufen, ab.

Der nächste Körper ist wiederum [31, Beispiel 5, Seite 87] entnommen.

$\mathcal{E} := \mathbb{Q}(\alpha)$	$\alpha^4 - 4\alpha^2 + 7 = 0$
$\omega_1 = 1$, $\omega_2 = \frac{-3+\alpha^2}{2}$, $\omega_3 = \alpha$, $\omega_4 = \frac{-3\alpha+\alpha^3}{2}$	
$[o_{\mathcal{E}} : \mathbb{Z}[\alpha]] = 1$, $d_{\mathcal{E}} = 1008$	
$\mathcal{F} := \mathcal{E}(\beta)$	$\beta^5 - \omega_3 = 0$
$o_{\mathcal{F}} = o_{\mathcal{E}}[\beta]$, $d_{\mathcal{F}} = (15625\omega_1 + 25000\omega_2)o_{\mathcal{E}}$	

Für die Regulatoren gilt: $\mathrm{reg}_{\mathcal{F}} \sim 541829969,76$, $\mathrm{reg}_{\mathcal{F}/\mathcal{E}} \sim 1385082,90$ und $\mathrm{reg}_{\mathcal{E}} \sim 2,42$. Daher ist zu erwarten, daß in Algorithmus 4.8 mehr als 10^6 quadratische Formen betrachtet werden müßten. Daher haben wir für Algorithmus 4.8 nur die Zeit zum Finden der ersten Lösung gemessen.

θ	$N_{\mathcal{E}/\mathbb{Q}}(\theta)$	$\#L$	4.8	4.14
$-(\omega_1 + \omega_2 + \omega_3 + \omega_4)$	4	1	(45)	45
$-(2\omega_3 + 3\omega_4)$	343	1	∞	45
8	4096	10	∞	130
343	343^4	16	∞	270

Im letzten Beispiel betrachten wir wieder den Körper von Cartwright und Steger [9] (Seite 73); sie haben mit dem Hasse'schen Normensatz nachgewiesen, daß die Gleichung $N_{\mathcal{F}/\mathcal{E}}(x) = \theta$ für $\theta = 264s'u' - 328u' + 643s' + 3369$ mit $N_{\mathcal{E}/\mathbb{Q}}(\theta) = 44681791589136$ in $\mathcal{F}$ lösbar ist. Wir haben sowohl mit Hilfe von Algorithmus 4.13 als auch mit einer Variante von Algorithmus 4.14 versucht, diese Normgleichung zu lösen. Die Menge M aus Algorithmus 4.13 enthält drei Primideale: eines über der 2 und zwei über der 3. Wir erhalten damit $S_{\mathcal{E}}$ mit ebenfalls drei Primidealen. Aufgrund der auftretenden Zerlegung enthält $S_{\mathcal{F}}$ dann sieben Ideale. Das Ideal $\mathfrak{b}$ errechnet sich dann zu

$$\begin{aligned}\mathfrak{b} &= o_{\mathcal{F}} + \frac{1}{18}((4\omega_1 - 2\omega_2 - 6\omega_3 - 2\omega_4)\mu_1 - (6\omega_1 + 6\omega_2 + 9\omega_3 - 3\omega_4)\mu_2 \\ &\quad +(7\omega_1 + \omega_3 - 6\omega_4)\mu_3)o_{\mathcal{F}},\end{aligned}$$

und es gilt $N_{\mathcal{F}/\mathbb{Q}}(\mathfrak{b}) = 1/531441$.

Die Menge der Primideale die in Algorithmus 4.14 betrachtet werden müssen, ist größer, dort geht die Zerlegung von θ noch mit ein. Wir erhalten $\#S_{\mathcal{E}} = 8$ und $\#S_{\mathcal{F}} = 20$.

Mit Hilfe von Algorithmus 4.14 war es möglich, innerhalb von 10 Minuten eine Lösung zu finden, die jedoch nicht in $\mathfrak{b}$ liegt. Algorithmus 4.13 hat innerhalb von 30 Tagen 10^8 Punkte in der ersten Ellipse ausgezählt und getestet, ohne eine Lösung zu finden. Auch mit 4.14 war es nicht möglich, zu entscheiden, ob es eine Lösung $x \in o_{\mathcal{F}}$ gibt. Das Problem hier ist Schritt (Lösung in $o_{\mathcal{F}}$). Als Lösung erhalten wir

$$\begin{aligned}x &= \frac{1}{7774}((412006\omega_1 - 19672\omega_2 + 71192\omega_3 + 36364\omega_4)\mu_1 \\ &\quad +(584856\omega_1 - 68161\omega_2 + 28072\omega_3 - 13105\omega_4)\mu_2 \\ &\quad -(134124\omega_1 - 88676\omega_2 + 12914\omega_3 - 113648\omega_4)\mu_3)\end{aligned}$$

mit

$$N_{\mathcal{F}/\mathcal{E}}(x) = \theta.$$

Symbolverzeichnis

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	natürliche, ganze, rationale, reelle, komplexe Zahlen
$A \leq B$ $(A < B)$	für Gruppen A, B: A ist (echte) Untergruppe von B
$A \subseteq B$ $(A \subset B)$	für Mengen A, B: A ist (echte) Teilmenge von B
$\mathcal{E}$, $\mathcal{F}$	Zahlkörper, 3
$\mathcal{K}$, k	beliebige Zahlkörper
f, g	Polynome, 3
$o_{\mathcal{E}}$, $o_{\mathcal{F}}$	Maximalordnungen von $\mathcal{E}$ und $\mathcal{F}$, 3
m	Grad von $\mathcal{E}$ über $\mathbb{Q}$, 3
n	Grad von $\mathcal{F}$ über $\mathcal{E}$, 3
$N_{\mathcal{F}/\mathcal{E}}$	Norm von $\mathcal{F}/\mathcal{E}$, 4
(r_1, r_2)	Signatur von $\mathcal{E}$, 4
$(s_i, t_i)_i$	relative Signatur von $\mathcal{F}/\mathcal{E}$, 4
$\tilde{V}_k, V_k$	(normalisierte) Bewertungen von k, 4
$\mathbb{P}_k$	Primideale von k, 4
$\lvert.\rvert$	Beträge, 4
$n_{v,k}$, $n_{V\|v}$	lokaler Grad, 5
$S_{\mathcal{E}}$, $S_{\mathcal{F}}$, $\dot{S}_{\mathcal{F}}$	Mengen von Bewertungen, 8
$r_{\mathcal{E}}$, $r_{\mathcal{F}}$	$:= \#S_{\mathcal{E}}$ bzw. $\#S_{\mathcal{F}}$, 8
r_v	Anzahl der Fortsetzungen von v, 9
$M_{i,j}$, $(M)_{i,j}$	M eine Matrix, das (i,j)-te Element von M, 5
I_n	Einheitsmatrix, 5
$\delta_{i,j}$	Kroneckersymbol, 5
$(M\|N)$	5
U_k	Einheitengruppe von o_k, 7
TU_k	Torsionseinheiten von o_k, 7
$\dot{P}_v$, P_v	Fortsetzungen von v, 9
$U_{\mathcal{F},S_{\mathcal{F}}}$, $U_{\mathcal{E},S_{\mathcal{E}}}$	$S_{\mathcal{F}}$ bzw. $S_{\mathcal{E}}$-Einheiten, 9

$U^A_{\mathcal{F},S_\mathcal{F}}$	$:= {N_{\mathcal{F}/\mathcal{E}}}^{-1}(A) \cap U_{\mathcal{F},S_\mathcal{F}}$, 9
$U^1_{\mathcal{F},S_\mathcal{F}}$	$:= {N_{\mathcal{F}/\mathcal{E}}}^{-1}(1) \cap U_{\mathcal{F},S_\mathcal{F}}$
$L_\mathcal{F}$, $\dot{L}_\mathcal{F}$	Abbildungen in den „Logarithmenraum“, 10
$\mathrm{vol}(B)$	Volumen von B
$\mathrm{vol}_u(B)$	u-Dimensionale Volumen von B
$\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(U)$, $\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(\mathcal{F})$	relativer Regulator von U bzw. von $\mathcal{F}$, 13
T_2	25
$[A]_R$	das R Erzeugnis von A (als Modul oder Vektorraum)
$[\![a, b]\!]$	$:= [a, b] \cap \mathbb{Z}$
$\lfloor a \rceil$	die am dichtesten an a gelegene ganze Zahl, $\lfloor a \rceil := \lfloor a + \frac{1}{2} \rfloor$
Q, B	Q eine quadratische Form, B die zug. bilineare Form, 26, 30
$d_\mathbb{Z}(\Lambda)$	$\mathbb{Z}$-Gitterdiskriminante von Λ, 26
τ, η	29, 29
K	$:= \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, 29
$\mathrm{T}_2^{\mathcal{F}/\mathcal{E}}$	relative T_2-Norm, 31
$\mathrm{cl}(\mathfrak{a})$	Klasse von $\mathfrak{a}$ in der Klassengruppe
$\mathrm{St}(\Lambda)$	Steinitzklasse von Λ, 32
$\mathfrak{a}_{x,\Lambda}$	Koeffizientenideal zu x in Λ, 32
$d(\Lambda)$	Gitterdiskriminante von Λ, 34
d_k	Körperdiskriminante von k
$e_{\mathfrak{P}/\mathfrak{p}}$, $f_{\mathfrak{P}/\mathfrak{p}}$	Verzweigungsindex, Trägheitsgrad, 57
$\lfloor a \rfloor$	$:= \max\{r \in \mathbb{Z} \mid r \leq a\}$, („Floor-Funktion“)
$\lceil a \rceil$	$:= \min\{r \in \mathbb{Z} \mid r \geq a\}$, („Ceiling-Funktion“)
γ_r^r	hermitesche Konstante [46, 3 (3.35a)]
B_r^2	euklidische Kugel mit dem Radius r
B_r^∞	Kugel in der Maximumsnorm mit dem Radius r

Literaturverzeichnis

[1] V. Acciaro. *Local global methods in number theory.* Dissertation, Carleton University Ottawa, 1995.

[2] E. Artin. Über Einheiten relativ galoisscher Zahlkörper, *J. Reine Angew. Math.* **167** (1931), 153–156.

[3] H.-J. Bartels. Über Normen algebraischer Zahlen, *Math. Ann.* **251** (1980), 191–212.

[4] A. M. Bergé und J. Martinet. Sur les minorations géométriques des régulateurs. In C. Goldstein, Hrsg., *Séminaire de Théorie des Nombres de Paris 1987–1988*, Band 81 aus *Progress in Mathematics*, Seiten 23–50. Birkhäuser, 1990.

[5] Y. Bilu und G. Hanrot. Solving Thue equations of high degree, *J. Number Theory.* **60** (1996), 373–392.

[6] E. Bombieri und J. Vaaler. On Siegel's lemma, *Invent. Math.* **73** (1983), 11–32.

[7] W. Bosma und M. E. Pohst. Computations with finitely generated modules over Dedekind domains. In S. M. Watt, Hrsg., *Proceedings ISSAC'91*, Seiten 151–156, 1991.

[8] D. A. Cantor. On the elementary theory of diophantine approximation over the ring of adeles I, *Ill. J. Math.* **9** (1965), 677–700.

[9] D. Cartwright und T. Steger. Manuskript. Apr. 1991.

[10] J. W. S. Cassels und A. Fröhlich, Hrsg. *Algebraic Number Theory.* London Mathematical Society, Academic Press, 1967.

[11] J. H. H. Chalk. Algebraic lattices, *C. R. Math. Acad. Sci. Soc. R. Can.* **II** (1980), 5–10.

[12] H. Cohen. Diskussion in Bordeaux. Mai 1996.

[13] H. Cohen. Hermite and Smith normal form algorithms over Dedekind domains, *Math. Comput.* **65** (1996), 1681–1699.

[14] A. Costa und E. Friedman. Ratios of regulators in totally real extensions of number fields, *J. Number Theory.* **37** (1991), 288–297.

[15] C. G. Cullen. *Linear Algebra with Applications.* Scott, Foresman and Company, 1988.

[16] M. Daberkow und M. E. Pohst. On the computation of Hilbert Class Fields. *Manuskript* (1996).

[17] J.-H. Evertse. Reduced bases of lattices over number fields, *Indag. Mathem. N. S.* **3** (1992), 153–168.

[18] C. Fieker, A. Jurk, und M. E. Pohst. On solving relative norm equations in algebraic number fields, *Math. Comput.* **66** (1997), 399–410.

[19] C. Fieker und M. E. Pohst. Lattices over number fields. In H. Cohen, Hrsg., *ANTS II*, Band 1122 aus *LNCS*, Seiten 147–157. Springer, 1996.

[20] U. Fincke. *Ein Ellipsoidverfahren zur Lösung von Normgleichungen*. Dissertation, Universität Düsseldorf, 1984.

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

[22] E. Friedman und N.-P. Skoruppa. Relative regulators of number fields. Forschergruppe Automorphe Formen, Universitäten Mannheim und Heidelberg, Feb. 1996.

[23] F. R. Gantenbacher. *Matrix Theory*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1958.

[24] D. A. Garbanati. The Hasse norm theorem for non–cyclic extensions of the rationals, *Proc. London Math. Soc.* **37** (1978), 143–164.

[25] D. A. Garbanati. An algorithm for finding an algebraic number whose norm is a given rational number, *J. Reine Angew. Math.* **316** (1980), 1–13.

[26] F. Heß. Zur Klassengruppenberechnung in algebraischen Zahlkörpern. Diplomarbeit, Technische Universität Berlin, 1996.

[27] M. Holzberg. Zur Berechnung der Einheitengruppe der Galoisschen Hülle von Zahlkörpern vierten Grades. Diplomarbeit, Heinrich–Heine–Universität Düsseldorf, 1991.

[28] A. Hoppe. Normal Forms for Modules over Dedekind Rings - Efficient Implementation in the Computer Number Theory System KANT. preprint, 1997.

[29] P. Humbert. Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique k fini, *Comment. Math. Helv.* **12** (1939–1940), 263–306.

[30] A. Jurk. Über die Berechnung von kürzesten Gittervektoren. Diplomarbeit, Heinrich–Heine–Universität Düsseldorf, 1989.

[31] A. Jurk. *Über die Berechnung von Lösungen relativer Normgleichungen in algebraischen Zahlkörpern*. Dissertation, Heinrich–Heine–Universität Düsseldorf, 1993.

[32] KANT Group. KANT V4. *J. Symb. Comput.* (to appear).

[33] M. Klebel. *Zur Theorie der Potenzganzheitsbasen bei relativ galoisschen Zahlkörpern*. Dissertation, Augsburg, 1995.

[34] S. G. Krantz. *Function theory of several complex variables*. Wadsworth & Brooks/Cole, 2. Auflage, 1992.

[35] S. Lang. *Algebraic Number Theorie*, Band 110 aus *Graduate Texts in Mathematics*. Springer, zweite Auflage, 1994.

[36] A. K. Lenstra, H. W. Lenstra Jr., und L. Lovász. Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.

[37] H. W. Leopoldt. Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, *Abh. Deutsch. Akad. Wiss. Berlin Kl. Math. Nat* **2** (1953), 48ff.

[38] H. W. Leopoldt. Über ein Fundamentalproblem der Theorie der Einheiten algebraischer Zahlkörper, *Bayer. Akad. Wiss. Math.-Natur. K. S.-B.* (1956), 41–48.

[39] R. B. McFeat. Geometry of numbers in adele spaces, *Diss. Math.* **88** (1969), 1–49.

[40] K. Meyberg. *Algebra 1*. Carl Hanser Verlag, 1975.

[41] H. Minkowski. *Geometrie der Zahlen*. 1896.

[42] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer, zweite Auflage, 1989.

[43] O. T. O'Meara. *Introduction to Quadratic Forms*, Band 117 aus *Grundlehren der Mathematischen Wissenschaften*. Springer, 1963.

[44] W. Plesken und B. Souvignier. Constructing rational representations of finite groups, *Exp. Math.* **5** (1996), 39–47.

[45] M. E. Pohst und K. Wildanger. Tables of unit groups and class groups of quintic fields and a regulator bound. *Math. Comput.* (to appear).

[46] M. E. Pohst und H. Zassenhaus. *Algorithmic Algebraic Number Theory.* Encyclopaedia of mathematics and its applications. Cambridge University Press, 1989.

[47] K. Rogers und H. P. F. Swinnerton-Dyer. The geometry of numbers over algebraic number fields, *Trans. Am. Math. Soc.* **88** (1958), 227–242.

[48] C. L. Siegel. Normen algebraischer Zahlen, *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* **11** (1973), 197–215.

[49] B. M. Trager. Algebraic factoring and rational function integration. In *Procedings of the 76 ACM Symposium on Symbolic and Algebraic Computation*, Seiten 219–226, 1976.

[50] S. N. Tschernikow. *Lineare Ungleichungen*, Band 69 aus *Hochschulbücher für Mathematik.* VEB Deutscher Verlag der Wissenschaften, 1971.

[51] P. van Emde Boas. Another NP–complete partition problem and the complexity of computing short vectors in a lattice. Mathematical Institute University of Amsterdam, 1981.

[52] L. C. Washington. *Introduction to Cyclotomic Fields*, Band 83 aus *Graduate texts in mathematics.* Springer, 1982.

[53] H. Weyl. Theory of reduction for arithmetical equivalence I, *Trans. Am. Math. Soc.* **48** (1940), 126–164.

[54] H. Weyl. Theory of reduction for arithmetical equivalence II, *Trans. Am. Math. Soc.* **51** (1942), 203–231.

[55] K. Wildanger. Über Grundeinheitenberechnung in algebraischen Zahlkörpern. Diplomarbeit, Heinrich–Heine–Universität Düsseldorf, 1993.

Zusammenfassung

Seien $\mathcal{F}/\mathcal{E}/\mathbb{Q}$ algebraische Zahlkörper, $N_{\mathcal{F}/\mathcal{E}} : \mathcal{F} \to \mathcal{E}$ die Relativnorm und $o_\mathcal{E}$ die Maximalordnung von $\mathcal{E}$. Ziel dieser Arbeit ist es, für eine gegebene Zahl $\theta \in o_\mathcal{E}$, zu entscheiden, ob es ein $x \in M \subseteq \mathcal{F}$ mit

$$N_{\mathcal{F}/\mathcal{E}}(x) = \theta$$

gibt, wobei M eine Ordnung, ein $o_\mathcal{E}$-Modul von vollem Rang oder, für $\mathcal{F}/\mathcal{E}$ Galois'sch, ganz $\mathcal{F}$ sein kann.

Zunächst wird dazu die Einheitengruppe $U_\mathcal{F}$ von $o_\mathcal{F}$ untersucht. Wir bestimmen für die Untergruppe

$$U^1_\mathcal{F} := \{x \in o_\mathcal{F} \mid N_{\mathcal{F}/\mathcal{E}}(x) = 1\}$$

der Einheitengruppe ein Erzeugendensystem und definieren ein Maß für die „Größe“ dieser Menge, den relativen Regulator $\mathrm{reg}_{\mathcal{F}/\mathcal{E}}(U^1_\mathcal{F})$. In Analogie zur Einheitenberechnung in Erweiterungen von $\mathbb{Q}$ geben wir ein Verfahren zur Berechnung dieser Gruppe an.

Im nächsten Kapitel der Arbeit entwickeln wir eine Theorie für Gitter über Zahlkörpern, die es uns ermöglicht, Verfahren aus der „Geometrie der Zahlen“ in unserem Fall anzuwenden. Speziell erarbeiten wir einen Reduktionsalgorithmus, der den bekannten LLL-Algorithmus kanonisch erweitert und verbessern darüber hinaus das von A. Jurk entwickelte Verfahren, um alle Elemente mit beschränkter Länge in einem „Relativ“-Gitter zu finden.

Im letzten Kapitel übertragen wir dann zunächst das Fincke'sche Ellipsoidverfahren zum Lösen von Normgleichungen in Ordnungen auf den relativen Fall, wobei wir die in den ersten Kapiteln entwickelten Methoden verwenden. Dies benutzen wir dann, um für relativ Galois'sche Erweiterungen Normgleichungen in Körpern zu lösen, wobei wir, ausgehend von den Methoden von D. Garbanati, ein (gebrochenes) Ideal bestimmen, das die gesuchte Lösung enthalten muß. Nach einigen Untersuchungen über die Komplexität der betrachteten Verfahren, geben wir noch einen Algorithmus an, der statt geometrische Methoden algebraische verwendet, um Normgleichungen zu lösen; wir versuchen, eine Lösung als Potenzprodukt gewisser S-Einheiten zu erhalten.

Wir schließen diese Arbeit mit einigen Beispielen, die das Potential der verschiedenen Verfahren demonstrieren.

Lebenslauf

Persönliche Daten

Claus Fieker
geb. am 3.5.1969 in Haan
ledig

Schulausbildung

1975 – 1979	Grundschule Bollenberg, Haan
1979 – 1982	Städtisches Gymnasium Haan
1982 – 1988	Helmholtz Gymnasium Hilden
15.06.1988	Abitur am Helmholtz Gymnasium Hilden

Studium

Okt. 1988 – Sept. 1993	Studium der Mathematik an der Heinrich–Heine–Universität Düsseldorf
23.10.1990	Vordiplom in Mathematik
21.09.1993	Diplom in Mathematik
Okt. 1993 – Jan. 1997	Anfertigung der Dissertation an der Technischen Universität Berlin
Okt. 1993 –	Wissenschaftlicher Mitarbeiter von Prof. Dr. M. E. Pohst am Fachbereich 3 Mathematik der Technischen Universität Berlin.
29.04.1997	Tag der wissenschaftlichen Aussprache