Über Grundeinheitenberechnung in algebraischen Zahlkörpern

Diplomarbeit
von
Klaus Wildanger
aus
Düsseldorf

Angefertigt am
Mathematischen Institut
der Heinrich–Heine–Universität Düsseldorf
Düsseldorf 1993

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Motivation

Eine der ersten Etappen bei der Entwicklung einer Theorie der algebraischen Zahlen war Dirichlets Beschreibung der Struktur der Einheitengruppe eines Zahlrings $\mathbb{Z}[\rho]$ zu einer ganzen algebraischen Zahl ρ. Dirichlet bewies, daß die Einheitengruppe $\mathrm{U}(\mathbb{Z}[\rho])$ eine direkte Summe endlich vieler zyklischer Gruppen ist. Einen Summanden in dieser direkten Summe bildet die endliche Gruppe $\mathrm{TU}(R)$ der Einheitswurzeln in $\mathbb{Z}[\rho]$, die übrigen Summanden sind alle jeweils unendlich. Mit der Berechnung von erzeugenden Elementen für diese Summanden ist $\mathrm{U}(\mathbb{Z}[\rho])$ vollständig bestimmt. Verhältnismäßig leicht kann ein erzeugendes Element für $\mathrm{TU}(\mathbb{Z}[\rho])$ gefunden werden, weitaus schwieriger dagegen ist die Ermittlung von erzeugenden Elementen für die unendlichen Summanden.

Diese Arbeit behandelt ein neueres Verfahren, mit dem nicht nur die Einheitengruppe eines Zahlrings $\mathbb{Z}[\rho]$, sondern mit dem allgemeiner die Einheitengruppe einer beliebigen Ordnung eines algebraischen Zahlkörpers ausgerechnet werden kann. Nach einer kurzen Zusammenstellung der für das Verfahren relevanten Aussagen aus der algebraischen Zahlentheorie skizziert der folgende Abschnitt die Grundstruktur des Verfahrens. Es wird deutlich werden, daß die Berechnung der Einheitengruppe in drei Schritten erfolgt. Beginnend mit dem zweiten Kapitel wird jeder dieser Schritte in einem eigenen Kapitel erläutert. In diesen drei Kapiteln finden sich zahlreiche Algorithmen, welche jeweils das zuvor beschriebene Vorgehen zusammenfassen. Diese Algorithmen bildeten die Grundlage für eine Implementierung des Verfahrens auf dem Computer. Hiermit wurden die Beispieltabellen im abschließenden fünften Kapitel erstellt.

Die meisten der in dieser Arbeit vorgestellten Verfahren wurden dem neuerschienenen Buch “Computational Algebraic Number Theory” von Herrn Professor Pohst entnommen, dem ich an dieser Stelle für die Betreuung der Arbeit danken möchte.

1.2 Einheiten in Ordnungen

Zur Formulierung des Verfahrens legen wir zunächst unsere Ausgangsposition fest und erwähnen einige für das Verfahren wichtige Eigenschaften von Zahlkörpern. Genaueres hierzu kann in [7, 11] nachgelesen werden.

Es sei $f(t) \in \mathbb{Z}[t]$ ein normiertes und irreduzibles Polynom vom Grad $n > 1$ mit r_1 reellen und $2r_2$ komplexen Nullstellen. Für eine beliebige, aber fest gewählte Nullstelle ρ von f bezeichne F den durch Adjunktion von ρ zu $\mathbb{Q}$ entstehenden Zahlkörper. Dann existieren genau n verschiedene $\mathbb{Q}$–Einbettungen (Konjugationen) $\varphi_1, \ldots, \varphi_n$ von F in $\mathbb{C}$. Sind $\alpha \in F$ und $j \in \{1, \ldots, n\}$ gegeben, so schreiben wir $\alpha^{(j)} = \varphi_j(\alpha)$ für die j–te Konjugierte von α. Die Konjugationen seien in gewohnter Weise numeriert:

(i) $\rho^{(1)}, \ldots, \rho^{(r_1)} \in \mathbb{R}$,

(ii) $\rho^{(r_1+1)}, \ldots, \rho^{(r_1+r_2)} \in \mathbb{C} \setminus \mathbb{R}$,

(iii) $\overline{\rho^{(r_1+r_2+j)}} = \rho^{(r_1+r_2)}$ $(1 \leq j \leq r_2)$.

Auf dem $\mathbb{Q}$–Vektorraum F führen wir mit Hilfe der Konjugierten durch

$$\langle\ ,\ \rangle : F \times F \to \mathbb{R} : (x, y) \mapsto \sum_{j=1}^{n} x^{(j)}\overline{y^{(j)}} \tag{1-1}$$

ein Skalarprodukt ein. Mit diesem definieren wir die Abbildung

$$T_2 : F \to \mathbb{R}^{\geq 0} : x \mapsto \langle x, x\rangle = \sum_{j=1}^{n} |x^{(j)}|^2. \tag{1-2}$$

Wir nennen für ein $\alpha \in F$ den Wert $T_2(\alpha)$ die Länge von α.

In F ist der ganze Abschluß von $\mathbb{Z}$ ein freier $\mathbb{Z}$–Modul vom Rang n, den man als die Maximalordnung $\mathfrak{o}_F$ bezeichnet.

Definition 1.1
Ein unitärer Teilring R von $\mathfrak{o}_F$ heißt Ordnung von F, falls R ein freier $\mathbb{Z}$–Modul vom Rang n ist.

Ab jetzt sei R stets eine beliebige, aber fest gewählte Ordnung von F mit einer $\mathbb{Z}$–Basis $\omega_1, \ldots, \omega_n$. Die Diskriminante von R wird definiert durch

$$\mathrm{disc}(R) := \mathrm{disc}(\omega_1, \ldots, \omega_n) := (\det(\omega_i^{(j)})_{1 \leq i,j \leq n})^2. \tag{1-3}$$

Mit $\mathrm{U}(R)$ bezeichen wir die Gruppe der Einheiten von R.

Lemma 1.2
$\alpha \in R$ ist genau dann eine Einheit von R, falls $|\mathrm{N}(\alpha)| = 1$ gilt.

Eine Sonderrolle spielen die in R gelegenen Einheitswurzeln. Diese bilden in $\mathrm{U}(R)$ eine endliche zyklische Untergruppe, für welche wir $\mathrm{TU}(R)$ schreiben. Im folgenden sei jeweils $\zeta \in R$ ein Erzeuger von $\mathrm{TU}(R)$.

Lemma 1.3
Für $\alpha \in R$ sind äquivalent:

(1) α *ist eine Einheitswurzel,*

(2) $|\alpha^{(i)}| = 1$ *für jedes* $i \in \{1, \ldots, n\}$,

(3) $T_2(\alpha) = n$.

Dirichlets eingangs erwähnte Beschreibung der Einheitengruppe eines Zahlrings läßt sich auf unsere beliebig gewählte Ordnung R übertragen:

Satz 1.4 (Dirichletscher Einheitensatz)
$\mathrm{U}(R)$ *ist die direkte Summe der Gruppe* $\mathrm{TU}(R)$ *und einer freien abelschen Gruppe vom Rang* $r_1 + r_2 - 1$. *Die Zahl* $r_1 + r_2 - 1$ *heißt der Einheitenrang* r *von* F.

In R gibt es also Einheiten $E_1, \ldots, E_r$ so daß sich jede weitere Einheit $\varepsilon \in R$ eindeutig als ein Produkt

$$\varepsilon = \xi \cdot E_1^{m_1} \cdots E_r^{m_r} \tag{1-4}$$

mit ganzen Zahlen $m_1, \ldots, m_r$ und einer Einheitswurzel $\xi \in \mathrm{TU}(R)$ ausdrücken läßt.

Definition 1.5
Ein System von r *Einheiten aus* R, *das eine Basis des torsionsfreien Summanden von* $\mathrm{U}(R)$ *ist, heißt ein Grundeinheitensystem von* R. *Für ein* $\nu \in \{1, \ldots, r\}$ *bezeichnen wir* $\varepsilon_1, \ldots, \varepsilon_\nu \in \mathrm{U}(R)$ *als Grundeinheiten, falls* $\varepsilon_1, \ldots, \varepsilon_\nu$ *zu einem Grundeinheitensystem von* R *ergänzt werden können.*

Definition 1.6
Für $k \in \mathbb{N}$ *heißen Einheiten* $\varepsilon_1, \ldots, \varepsilon_k \in \mathrm{U}(R)$ *unabhängig, falls* $\langle \varepsilon_1, \ldots, \varepsilon_k \rangle$ *eine Untergruppe vom Rang* k *in* $\mathrm{U}(R)$ *ist.*

Die Unabhängigkeit von Einheiten kann effektiv überprüft werden. Hierzu definieren wir $\underline{c} \in \mathbb{R}^r$ durch $c_i = 1$ $(1 \leq i \leq r_1)$, $c_j = 2$ $(r_1 < j \leq r)$ und betrachten die Abbildung

$$L : \mathrm{U}(R) \to \mathbb{R}^r : \varepsilon \mapsto \begin{pmatrix} c_1 \log |\varepsilon^{(1)}| \\ \vdots \\ c_r \log |\varepsilon^{(r)}| \end{pmatrix}. \tag{1-5}$$

Lemma 1.7
$\varepsilon_1, \ldots, \varepsilon_k \in \mathrm{U}(R)$ sind genau dann unabhängig, falls die Vektoren $L(\varepsilon_1), \ldots, L(\varepsilon_k)$ im $\mathbb{R}^r$ linear unabhängig über $\mathbb{R}$ sind.

Schließlich sei noch an die Definition des Regulators erinnert.

Definition 1.8
Für Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$ heißt

$$\mathrm{Reg}(\varepsilon_1, \ldots, \varepsilon_r) = |\det(L(\varepsilon_1), \ldots, L(\varepsilon_r))|$$

der Regulator von $\varepsilon_1, \ldots, \varepsilon_r$. Sind $\varepsilon_1, \ldots, \varepsilon_r$ Grundeinheiten in R, so nennt man $\mathrm{Reg}(\varepsilon_1, \ldots, \varepsilon_r)$ den Regulator $\mathrm{Reg}(R)$ der Ordnung.

1.3 Grundriß des Verfahrens

Nach der Klärung der Ausgangssituation können wir jetzt einen kurzen Überblick über das in dieser Arbeit vorgestellte Verfahren zur Berechnung der Einheitengruppe $\mathrm{U}(R)$ geben. Gemäß dem Dirichletschen Einheitensatz verstehen wir unter der Berechnung von $\mathrm{U}(R)$ natürlich die Bestimmung eines Grundeinheitensystems sowie eines erzeugenden Elementes von $\mathrm{TU}(R)$.

Recht einfach ist die Grundidee des Verfahrens. Zuerst konstruieren wir ein System von r unabhängigen Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ in R. Wie das effektiv geschehen kann, werden wir im **dritten** Kapitel sehen. Von den unabhängigen Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ wissen wir noch nicht, ob es sich bei ihnen bereits um Grundeinheiten handelt. Um dies zu entscheiden und um gegebenenfalls von den unabhängigen Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ zu einem Grundeinheitensystem aufzusteigen, benötigen wir eine Abschätzung des Index $(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle)$. Den Index können wir mittels des Regulators anders ausdrücken.

Lemma 1.9
Sind $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$ unabhängige Einheiten, so gilt

$$(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle) = \frac{\mathrm{Reg}(\varepsilon_1, \ldots, \varepsilon_r)}{\mathrm{Reg}(R)}. \tag{1-6}$$

In dieser Phase des Verfahrens sind zwar die zum Ausrechnen von $\mathrm{Reg}(R)$ notwendigen Grundeinheiten noch nicht bekannt, wie wir aber im **zweiten** Kapitel zeigen werden, ist es möglich, eine untere Abschätzung für den Wert von $\mathrm{Reg}(R)$ zu bestimmen. Mit Hilfe dieser unteren Regulatorabschätzung, deren Berechnung uns im übrigen auch mit einem erzeugenden Element von $\mathrm{TU}(R)$ versorgen wird, erhalten wir aus (1-6) die Indexabschätzung

$$(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle) \leq \left\lfloor \frac{\mathrm{Reg}(\varepsilon_1, \ldots, \varepsilon_r)}{\text{untere Regulatorabschätzung}} \right\rfloor. \tag{1-7}$$

Die Abschätzung gestattet es nun, entweder von $\varepsilon_1, \ldots, \varepsilon_r$ zu einem Grundeinheitensystem aufzusteigen oder aber zu beweisen, daß die unabhängigen Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ bereits ein Grundeinheitensystem bilden. Wie dies im einzelnen funktioniert, ist Gegenstand des **vierten** Kapitels.

Entgegen dem gerade skizzierten Grundriß des Verfahrens beginnt man in der Praxis mit der Bestimmung der unteren Regulatorabschätzung. Bei deren Berechnung nämlich fallen häufig schon einige unabhängige Einheiten an. Diese werden dann mit den Methoden aus dem dritten Kapitel zu einem System unabhängiger Einheiten ergänzt. Wir fassen unser Vorgehen in der folgenden Übersicht zusammen:

Schritt 1 Berechnung einer unteren Regulatorabschätzung und eines erzeugenden Elementes von $\mathrm{TU}(R)$.

Schritt 2 Ergänzung der in Schritt 1 bereits gefundenen unabhängigen Einheiten zu einem System von r unabhängigen Einheiten.

Schritt 3 Bestimmung eines Grundeinheitensystems.

1.4 Der Auszählalgorithmus

In den Algorithmen dieser Arbeit wird mehrfach das Auszählverfahren von Fincke und Pohst [2, 11] verwendet. Um seine Aufgabe kurz zu erläutern, legen wir einige Sprechweisen fest.

Es sei M ein freier $\mathbb{Z}$–Modul vom Rang $k \in \mathbb{N}$ mit einer $\mathbb{Z}$–Basis $\alpha_1, \ldots, \alpha_k$. Wir nennen eine Abbildung $q : M \to \mathbb{R}^{\geq 0}$ eine positiv definite quadratische Form auf M, falls eine positiv definite, symmetrische Matrix $A \in \mathbb{R}^{k \times k}$ existiert, so daß für jedes $x \in M$ mit Darstellung $x = x_1\alpha_1 + \cdots + x_k\alpha_k$ $(x_1, \ldots, x_k \in \mathbb{Z})$ die Gleichung

$$q(x) = (x_1, \ldots, x_k) \cdot A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \tag{1-8}$$

gilt. Die Matrix A ist bezüglich der Basis $\alpha_1, \ldots, \alpha_k$ eindeutig bestimmt; wir nennen A die Grammatrix von q. Als die Determinante der quadratischen Form q bezeichnen wir $\det(A)$.

Zu $C \geq 0$ existieren nur endlich viele $x \in M$ mit $q(x) \leq C$. Diese können mit dem Auszählalgorithmus von Fincke und Pohst effektiv bestimmt werden. Wegen $q(x) = q(-x)$ für alle $x \in M$ berechnet der Auszählalgorithmus aus Effizienzgründen nur die Elemente $x = x_1\alpha_1 + \cdots + x_k\alpha_k$ $(x_1, \ldots, x_k \in \mathbb{Z})$ mit $q(x) \leq C$, für welche gilt

$$x_j \leq 0,\ j := \max\{i \in \{1, \ldots, k\} \mid x_i \neq 0\}. \tag{1-9}$$

Der Auszählalgorithmus wird meist erheblich schneller, wenn zum Auszählen eine LLL–reduzierte Basis von M verwendet wird. Nähere Informationen zu Berechnung

und Eigenschaften von LLL–reduzierten Basen findet der Leser in [6]. Wann immer das Auszählverfahren in einem Algorithmus dieser Arbeit benutzt wird, soll davon ausgegangen werden, daß das Auszählen anhand einer LLL–reduzierten Basis des Moduls M erfolgt.

Auf unserer Ordnung R ist die Länge T_2 eine positiv definite quadratische Form mit Determinante

$$\det(T_2) = |\mathrm{disc}(R)|. \tag{1-10}$$

Wir demonstrieren nun an einem kurzen Beispiel, wie wir das Auszählverfahren in den Algorithmen dieser Arbeit notieren. Zum Verständnis des Beispiels reicht es zu wissen, daß das letzte vom Auszählalgorithmus zurückgelieferte Element stets das Nullelement ist.

Algorithmus 1.10
Eingabe: $C \in \mathbb{R}^{\geq 0}$.
Ausgabe: *alle* $\alpha \in R, \alpha \neq 0$, *mit* $T_2(\alpha) \leq C$.
(1) *Initialisiere den Auszählalgorithmus für* T_2 *und* C.
(2) *Zähle das nächste Element* α *aus.*
(3) *Falls* $\alpha = 0$, *so terminiere.*
(4) *Gebe* $\alpha, -\alpha$ *aus und gehe zu (2).*

1.5 Technik

Die praktische Nutzung der in den nächsten Kapiteln beschriebenen Methoden setzt voraus, daß wir in F mit algebraischen Zahlen, Idealen, usw. *rechnen* können, das heißt, wir benötigen Kenntnisse der Arithmetik in Zahlkörpern. Hierzu verweisen wir den Leser auf die detaillierten und algorithmisch–orientierten Darstellungen in [10, 11, 12]. Dort erfährt man zum Beispiel auch, wie man effektiv eine Ganzheitsbasis von F berechnet. Wir gehen im folgenden nur dann auf Einzelheiten der Arithmetik ein, wenn diese für das Verfahren besonders wichtig sind oder wenn sie in den oben angegebenen Werken nicht beschrieben sind.

Für die Implementierung des Verfahrens wurde das zahlentheoretische Programmpaket KANT verwendet, das an der Technischen Universität Berlin entwickelt wird. Aufbauend auf einer dynamischen Speicherverwaltung sowie einer Langzahl–Arithmetik für ganze und reelle Zahlen stellt das in C geschriebene KANT dem Benutzer Routinen zur Arithmetik in Gittern und Zahlkörpern zur Verfügung.

Alle in der Arbeit angegebenen Rechenzeiten beziehen sich auf einen 486 DX 33 mit 16 MB Hauptspeicher.

Kapitel 2

Eine untere Regulatorabschätzung

Fassen wir den torsionsfreien Summanden von $\mathrm{U}(R)$ in kanonischer Weise als freien $\mathbb{Z}$–Modul vom Rang r auf, so ist hierauf die Abbildung

$$Q : \mathrm{U}(R) \to \mathbb{R}^{\geq 0} : \varepsilon \mapsto \sum_{i=1}^{n} (\log |\varepsilon^{(i)}|)^2. \tag{2-1}$$

eine positiv definite quadratische Form mit Determinante

$$\det(Q) = \frac{n\mathrm{Reg}(R)^2}{2^{r_2}}. \tag{2-2}$$

Dies kann in [11, Chapter 5] nachgelesen werden.

Zu $i \in \{1, \ldots, r\}$ bezeichne im folgenden M_i das i–te sukzessive Minimum von Q, also

$$M_i = \min\{\kappa > 0 \mid \exists\, \varepsilon_1, \ldots, \varepsilon_i \in \mathrm{U}(R) \text{ unabh. mit } Q(\varepsilon_j) \leq \kappa\ (1 \leq j \leq i)\}. \tag{2-3}$$

Ferner sei γ_r^r die Hermitesche Konstante. Nach dem Minkowskischen Satz über sukzessive Minima gilt dann

$$M_1 \cdots M_r \leq \gamma_r^r \det(Q). \tag{2-4}$$

Setzen wir nun (2-2) und (2-4) zusammen, so erhalten wir

$$\sqrt{\frac{2^{r_2} M_1 \cdots M_r}{n\gamma_r^r}} \leq \mathrm{Reg}(R). \tag{2-5}$$

In der Praxis ist die Abschätzung (2-5) natürlich nur dann zu gebrauchen, falls wir auch über untere Abschätzungen für die sukzessiven Minima $M_1, \ldots, M_r$ verfügen, denn ohne Kenntnis eines Grundeinheitensystems können wir ja zunächst einmal auch noch keine Aussage über die Werte von $M_1, \ldots, M_r$ machen. Wir müssen also als nächstes untere Schranken für $M_1, \ldots, M_r$ herleiten.

Sei ab jetzt jeweils $C \in \mathbb{R}, C > n$, beliebig, aber fest gegeben. Wir setzen

$$\tilde{C} := \frac{n}{4}\left(\log\left(\frac{C}{n} + \sqrt{\left(\frac{C}{n}\right)^2 - 1}\right)\right)^2 . \tag{2-6}$$

Entscheidend wird nun sein, daß man für eine Einheit $\varepsilon \in \mathrm{U}(R)$ den Wert $Q(\varepsilon)$ mit Hilfe der Längen von ε und $\frac{1}{\varepsilon}$ abschätzen kann. Dies beruht auf dem folgenden Extremalwertproblem.

Satz 2.1
Für jedes $\underline{x} \in \mathbb{R}^n$, das die drei Nebenbedingungen,

(i) $\sum_{j=1}^{n} x_j = 0,$

(ii) $\sum_{j=1}^{n} \exp(2x_j) \geq C,$

(iii) *mindestens $\lceil \frac{n}{2} \rceil$ Einträge von $\underline{x}$ sind nicht negativ ,*

erfüllt, gilt die Abschätzung

$$\sum_{j=1}^{n} x_j^2 \geq \tilde{C}. \tag{2-7}$$

Beweis Siehe [11, Chapter 5, Theorem 6.17]. □

Folgerung 2.2
Für eine Einheit $\varepsilon \in \mathrm{U}(R)$ mit $T_2(\varepsilon) \geq C$ und $T_2(\frac{1}{\varepsilon}) \geq C$ gilt

$$Q(\varepsilon) = Q(\frac{1}{\varepsilon}) \geq \tilde{C}. \tag{2-8}$$

Beweis Wegen $T_2(\varepsilon) > n$ und 1.3 erfüllt entweder

$$(\log|\varepsilon^{(1)}|, \ldots, \log|\varepsilon^{(n)}|)^t$$

oder

$$(\log|\frac{1}{\varepsilon^{(1)}}|, \ldots, \log|\frac{1}{\varepsilon^{(n)}}|)$$

die drei Nebenbedingungen aus 2.1. Also gilt

$$Q(\varepsilon) = Q(\frac{1}{\varepsilon}) = \sum_{i=1}^{n}(\log|\varepsilon^{(i)}|)^2 = \sum_{i=1}^{n}(\log|\frac{1}{\varepsilon^{(i)}}|)^2 \geq \tilde{C}.$$

□

Lemma 2.3
Gibt es ein $i \in \{1, \ldots, r\}$ mit $M_i \leq \tilde{C}$, so existieren Einheiten $\varepsilon_1, \ldots, \varepsilon_i \in \mathrm{U}(R)$ mit $Q(\varepsilon_j) \leq Q(\varepsilon_i) = M_i$ und $T_2(\varepsilon_j) \leq C$ $(1 \leq j \leq i)$.

Beweis Gemäß Definition existieren unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_i$ mit

$$Q(\varepsilon_j) \leq Q(\varepsilon_i) = M_i \qquad (1 \leq j < i). \tag{2-9}$$

Wir können ohne Einschränkung

$$T_2(\varepsilon_j) \leq T_2(\frac{1}{\varepsilon_j}) \qquad (1 \leq j \leq i) \tag{2-10}$$

annehmen. Aus 2.2 folgt $T_2(\varepsilon_j) \leq C$ $(1 \leq j \leq i)$, womit bereits alles bewiesen ist. □

Die effektive Berechnung einer unteren Regulatorabschätzung basiert auf dem nächsten Lemma. Zu seiner Formulierung definieren wir $k \in \mathbb{Z}^{\geq 0}$ durch

$$k = \max \left\{ i \in \mathbb{Z}^{\geq 0} \;\middle|\; \begin{array}{l} \exists \text{ unabhängige Einheiten } \varepsilon_1, \ldots, \varepsilon_i \in \mathrm{U}(R) \\ \text{mit } T_2(\varepsilon_j) \leq C \text{ und } Q(\varepsilon_j) \leq \tilde{C} \ (1 \leq j \leq i) \end{array} \right\} \tag{2-11}$$

und damit für $i = 1, \ldots, k$ weiter

$$m_i = \max \left\{ \gamma > 0 \;\middle|\; \begin{array}{l} \exists \text{ unabhängige Einheiten } \varepsilon_1, \ldots, \varepsilon_i \in \mathrm{U}(R) \\ \text{mit } T_2(\varepsilon_j) \leq C \text{ und } Q(\varepsilon_j) \leq \gamma \ (1 \leq j \leq i) \end{array} \right\}. \tag{2-12}$$

Lemma 2.4
(a) $M_i = m_i$ $(1 \leq i \leq k)$,

(b) $M_j > \tilde{C}$ $(k < j \leq r)$.

Beweis Konsequenz aus 2.3. □

In Verbindung mit (2-5) erhält man aus 2.4 nun

$$\sqrt{\frac{2^{r_2} M_1 \cdots M_k \tilde{C}^{r-k}}{n \gamma_r^r}} \leq \mathrm{Reg}(R). \tag{2-13}$$

Für die weiteren Betrachtungen setzen wir

$$S_C = \{\alpha \in R \mid T_2(\alpha) \leq C\}. \tag{2-14}$$

Mit dem Auszählalgorithmus von Fincke und Pohst können alle Elemente der endlichen Menge S_C effektiv bestimmt werden, also auch die Elemente der Mengen

$$U_C := S_C \cap \mathrm{U}(R), \tag{2-15}$$
$$U_1 := \{\varepsilon \in U_C \mid 0 < Q(\varepsilon) \leq \tilde{C}\}, \tag{2-16}$$
$$U_2 := \{\varepsilon \in U_C \mid \tilde{C} < Q(\varepsilon)\}, \tag{2-17}$$
$$T_C := \{\varepsilon \in U_C \mid Q(\varepsilon) = 0\}. \tag{2-18}$$

Zur Bestimmung von k und $M_1, \ldots, M_k$ werten wir U_1 aus.

Lemma 2.5
Zu jedem $i \in \{1, \ldots, k\}$ existieren unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_i \in U_1$ mit $Q(\varepsilon_j) = M_j$ $(1 \leq j \leq i)$.

Beweis Für $i = 1$ ist nichts zu zeigen. Sei also $i > 1$, und es seien bereits $\varepsilon_1, \ldots, \varepsilon_{i-1} \in U_1$ gefunden mit $Q(\varepsilon_j) = M_j$ $(1 \leq j < i)$. Nach Definition existieren unabhängige Einheiten $\eta_1, \ldots, \eta_i \in U_1$ mit $Q(\eta_j) \leq M_i$ $(1 \leq j \leq i)$. Es gibt ein $\nu \in \{1, \ldots, i\}$, so daß die Einheiten $\varepsilon_1, \ldots, \varepsilon_{i-1}, \eta_\nu$ unabhängig sind. Wir müssen nun noch $Q(\eta_\nu) = M_i$ zeigen. Ohne Einschränkung können wir dabei $M_1 < M_i$ annehmen. Es existiert also $\mu \in \{2, \ldots, i\}$ mit $M_{\mu-1} < M_\mu = \cdots = M_i$ Da $\varepsilon_1, \ldots, \varepsilon_{\mu-1}, \eta_\nu$ unabhängig sind, muß wegen $Q(\varepsilon_j) \leq M_{\mu-1}$ $(1 \leq j \leq \mu - 1)$ dann $Q(\eta_\nu) = M_\mu = M_i$ gelten. □

Der Beweis zu 2.5 zeigt insbesondere, daß wenn wir für ein $i \in \{1, \ldots, k-1\}$ bereits unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_i \in U_1$ mit $Q(\varepsilon_j) = M_j$ $(1 \leq j \leq i)$ gefunden haben, eine von $\varepsilon_1, \ldots, \varepsilon_i$ unabhängige Einheit $\varepsilon_{i+1} \in U_1$ mit $Q(\varepsilon_{i+1}) = M_{i+1}$ existiert. Dies hilft uns jetzt bei der Bestimmung von k und $M_1, \ldots, M_k$.

Für $U_1 = \emptyset$ gilt natürlich $k = 0$, und wir sind bereits fertig mit der Auswertung von U_1. Andernfalls wählen wir $\varepsilon_1 \in U_1$ derart, daß $Q(\varepsilon_1) \leq Q(\varepsilon)$ $\forall\, \varepsilon \in U_1$. Dann gilt $M_1 = Q(\varepsilon_1)$. Enthält nun U_1 keine von ε_1 unabhängigen Einheiten, so folgt $k = 1$. Andernfalls ermitteln wir unter den von ε_1 unabhängigen Einheiten aus U_1 eine Einheit ε_2, für die $Q(\varepsilon_2)$ minimal ist. Es gilt dann $M_2 = Q(\varepsilon_2)$. Iterieren wir dieses Vorgehen, so erhält man schließlich den exakten Wert von k sowie unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_k \in U_1$ mit $Q(\varepsilon_j) = M_j$ $(1 \leq j \leq k)$.

Falls $k < r$ gilt, so besteht die Möglichkeit, daß in U_2 von $\varepsilon_1, \ldots, \varepsilon_k$ unabhängige Einheiten liegen. Deren Bestimmung empfiehlt sich, da dann in zweiten Schritt des Verfahrens dementsprechend weniger Einheiten zu konstruieren sind. Setzen wir

$$m := \max\{i \in \mathbb{Z}^{\geq 0} \mid \exists \text{ unabhängige Einheiten } \varepsilon_1, \ldots, \varepsilon_i \in U_C\}, \qquad (2\text{-}19)$$

so müssen also $\varepsilon_{k+1}, \ldots, \varepsilon_m \in U_2$ berechnet werden, so daß $\varepsilon_1, \ldots, \varepsilon_m$ unabhängig sind. Hierzu gehen wir wie bei der Auswertung von U_1 vor, das heißt, zuerst wird man versuchen, eine von $\varepsilon_1, \ldots, \varepsilon_k$ unabhängige Einheit $\varepsilon_{k+1} \in U_2$ mit $Q(\varepsilon_{k+1})$ minimal zu ermitteln usf. Die Forderung nach Minimalität von $Q(\varepsilon_{k+1}), \ldots, Q(\varepsilon_m)$ ist dabei, anders als bei der Auswertung von U_1, heuristisch motiviert.

In der Praxis ist man bei der Konstruktion eines unabhängigen Einheitensystems $\eta_1, \ldots, \eta_r \in \mathrm{U}(R)$ stets bestrebt, einen *kleinen* Index $(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle)$ zu bekommen, damit der dritte Schritt des Verfahrens nicht zu zeitaufwendig wird. Der Index ist erfahrungsgemäß umso eher klein, falls es auch die Werte $Q(\eta_1), \ldots, Q(\eta_r)$ sind. Also sind die Einheiten $\varepsilon_1, \ldots, \varepsilon_m$ stets besonders wertvoll als Bausteine für ein System von r unabhängigen Einheiten mit kleinem Index. Diesen Sachverhalt drückt auch das nächste Lemma aus.

Lemma 2.6
Es seien, wie oben konstruiert, unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_k \in \mathrm{U}_1$ mit

$$Q(\varepsilon_i) = M_i \qquad (1 \leq i \leq k)$$

gegeben. Dann gelten:

(a) *Für $\ell := \min(k, 3)$ sind $\varepsilon_1, \ldots, \varepsilon_\ell$ Grundeinheiten.*

(b) *Gelten $k \geq 4$ und $M_4 > M_1$, so sind $\varepsilon_1, \ldots, \varepsilon_4$ Grundeinheiten.*

(c) *Sind für ein $\ell \in \{1, \ldots, k-1\}$ die Einheiten $\varepsilon_1, \ldots, \varepsilon_\ell$ bereits Grundeinheiten, und gilt*

$$3M_{\ell+1} > \sum_{i=1}^{\ell} M_i,$$

so sind $\varepsilon_1, \ldots, \varepsilon_{\ell+1}$ Grundeinheiten.

Beweis Siehe [11, Chapter 3, Theorem 3.32]. □

Speziell also für $k = r \leq 3$ haben wir schon im ersten Schritt des Verfahrens ein Grundeinheitensystem gefunden.

Die Auswertung von U_C beschließen wir mit der Bestimmung eines erzeugenden Elementes von $\mathrm{TU}(R)$. Nach 1.3 gilt

$$\mathrm{TU}(R) = T_C. \tag{2-20}$$

Wir wählen $\xi \in T_C$ mit

$$\arg(\xi^{(1)}) = \min\{\arg(\varepsilon^{(1)}) \mid \varepsilon \in T_C, \varepsilon \neq 1\}, \tag{2-21}$$

wobei das Argument durch die Bedingung $0 \leq \arg(z) < 2\pi \ \forall\, z \in \mathbb{C}^\times$ normiert sei; offensichtlich ist dann ξ ein erzeugendes Element von $\mathrm{TU}(R)$.

Wir fassen unser Vorgehen in einem Algorithmus zusammen. Wie im Abschnitt 1.4 beschrieben, nutzt der Auszählalgorithmus aus Effizienzgründen die Symmetrie von S_C aus, das heißt, statt S_C liefert er die Elemente der Menge

$$S'_C := \{x \in S_C \mid x = x_1\omega_1 + \cdots + x_n\omega_n, \underline{x} \in \mathbb{Z}^n \text{ erfüllt (1-9)}\} \tag{2-22}$$

zurück. Für $i = 1, 2$ bildet man nun $U'_i := U_i \cap S'_C$. Wertet man U'_1 und U'_2 so aus, wie das weiter oben für U_1 und U_2 beschrieben wurde, so erhält man die gleichen Werte für k, ℓ, m und $M_1, \ldots, M_k$, denn Multiplikation mit -1 hat keinen Einfluß auf die Unabhängigkeit von Einheiten, und es gilt $Q(\varepsilon) = Q(-\varepsilon)$ für alle $\varepsilon \in \mathrm{U}(R)$.

Algorithmus 2.7

Eingabe: $C \in \mathbb{R}, C > n$.

Ausgabe: *eine untere Regulatorabschätzung B_R; Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_\ell$ und unabhängige Einheiten $\varepsilon_{\ell+1}, \ldots, \varepsilon_m$ ($\ell, m \in \mathbb{Z}^{\geq 0}$); ein erzeugendes Element ζ von $\mathrm{TU}(R)$.*

(1) $\zeta \leftarrow -1$.

(2) $U'_1 \leftarrow U'_2 \leftarrow \emptyset$.

(3) *Initialisiere den Auszählalgorithmus für T_2 und C.*

(4) *Zähle das nächste Element α aus.*

(5) *Falls $\alpha = 0$, so gehe zu (14).*

(6) *($\alpha \in \mathrm{U}(R)$?) Falls $|\mathrm{N}(\alpha)| > 1$, so gehe zu (4).*

(7) *($\alpha \in \mathrm{TU}(R)$?) Falls $Q(\varepsilon) > 0$, so gehe zu (12).*

(8) *Falls ($\alpha = 1$ oder $\alpha = -1$), so gehe zu (4).*

(9) *Falls* $\arg(\alpha^{(1)}) > \arg(-\alpha^{(1)})$, *so setze* $\alpha \leftarrow -\alpha$.

(10) *Falls* $\arg(\alpha^{(1)}) < \arg(\zeta^{(1)})$, *so setze* $\zeta \leftarrow \alpha$.

(11) *Gehe zu (4).*

(12) *(*α *in* U_1' *oder* U_2' *einsortieren) Falls* $Q(\varepsilon) \leq \tilde{C}$, *so setze* $U_1' \leftarrow U_1' \cup \{\alpha\}$, *sonst setze* $U_2' \leftarrow U_2' \cup \{\alpha\}$.

(13) *Gehe zu (4).*

(14) *(Auswertung von* U_1'*)* $k \leftarrow 0$.

(15) *Falls (*$U_1' = \emptyset$ *oder* $k = r$*), so gehe zu (20).*

(16) *Bestimme ein* $\varepsilon \in U_1'$ *mit* $Q(\varepsilon) = \min\{Q(\varepsilon) \mid \varepsilon \in U_1'\}$.

(17) $U_1' \leftarrow U_1' \setminus \{\varepsilon\}$.

(18) *Falls* $\varepsilon_1, \ldots, \varepsilon_k, \varepsilon$ *nicht unabhängig sind, so gehe zu (15).*

(19) $k \leftarrow k+1, \varepsilon_k \leftarrow \varepsilon$. *Gehe zu (15).*

(20) *(Auswertung von* U_2'*)* $m \leftarrow k$.

(21) *Falls (*$U_2' = \emptyset$ *oder* $k = r$*), so gehe zu (26).*

(22) *Bestimme ein* $\varepsilon \in U_2'$ *mit* $Q(\varepsilon) = \min\{Q(\varepsilon) \mid \varepsilon \in U_2'\}$.

(23) $U_2' \leftarrow U_2' \setminus \{\varepsilon\}$.

(24) *Falls* $\varepsilon_1, \ldots, \varepsilon_m, \varepsilon$ *nicht unabhängig sind, so gehe zu (21).*

(25) $m \leftarrow m+1, \varepsilon_m \leftarrow \varepsilon$. *Gehe zu (21).*

(26) *(Bestimme* ℓ*)* $\ell \leftarrow \min(k, 3)$.

(27) *Falls* $k \leq 3$. *so gehe zu (34).*

(28) *(Lemma 2.6(b)) Falls* $Q(\varepsilon_4) = Q(\varepsilon_1)$, *so gehe zu (34).*

(29) $\ell \leftarrow 4$.

(30) *Falls* $\ell + 1 > k$, *so gehe zu (34).*

(31) *(Lemma 2.6(c)) Falls* $3 \cdot Q(\varepsilon_{\ell+1}) \leq \sum_{i=1}^{\ell} Q(\varepsilon_i)$, *so gehe zu (34).*

(32) $\ell \leftarrow \ell + 1$.

(33) *Gehe zu (30).*

(34) *(Untere Regulatorschranke)* $B_R \leftarrow \sqrt{2^{r_2} Q(\varepsilon_1) \cdots Q(\varepsilon_k) \tilde{C}^{r-k} (n\gamma_r^r)^{-1}}$.

(35) *Terminiere.*

Bemerkung 2.8

(1) *In Schritt (6) von 2.7 kann die Norm von* α *entweder über die Determinante einer Darstellungsmatrix von* α *oder durch das Produkt der Konjugierten von* α *bestimmt werden. Bei der Implementierung von 2.7 unter* KANT *erwies sich die erste Methode für Körpergrade* ≤ 13 *zumeist als schneller, bei höheren Graden dagegen wurde die Norm über das Produkt der Konjugierten berechnet (man beachte, daß die Elemente aus* S_C *erfahrungsgemäß kleine Basiskoeffizienten besitzen).*

(2) *Die Menge* $\mathrm{TU}(R) \cap S_C'$ *enthält im allgemeinen noch kein erzeugendes Element von* $\mathrm{TU}(R)$*; dies wird in Schritt (9) berücksichtigt.*

(3) *Um im Schritt (18) die Unabhängigkeit von* $\varepsilon_1, \ldots, \varepsilon_{k+1}, \varepsilon$ *zu überprüfen, kann man Lemma 1.7 und das Verfahren von E. Schmidt zur Berechnung einer Orthonormalbasis verwenden: Für* $k = 0$ *ist* ε *natürlich stets un-*

abhängig. Wir setzen also $\varepsilon_1 \leftarrow \varepsilon$ *und außerdem noch*

$$v_1 \leftarrow \frac{L(\varepsilon)}{\|L(\varepsilon)\|_2}.$$

Es sei jetzt $k \geq 1$, *und die Vektoren* $v_1, \ldots, v_k \in \mathbb{R}^r$ *seien eine Orthonormalbasis des* $\mathbb{R}$*–Vektorraums, welcher von* $L(\varepsilon_1), \ldots, L(\varepsilon_k)$ *aufgespannt wird. Man bestimmt nun die senkrechte Projektion* w *von* $L(\varepsilon)$ *auf*

$$\mathbb{R} \cdot L(\varepsilon_1) + \cdots + \mathbb{R} \cdot L(\varepsilon_k).$$

Falls $w = \underline{0}$ *gilt, so handelt es sich bei* $\varepsilon_1, \ldots, \varepsilon_k, \varepsilon$ *nach 1.7 um abhängige Einheiten, und man fährt fort mit Schritt (15). Andernfalls setzt man* $\varepsilon_{k+1} \leftarrow \varepsilon$ *und*

$$v_{k+1} \leftarrow \frac{w}{\|w\|_2}.$$

$\varepsilon_1, \ldots, \varepsilon_{k+1}$ *sind dann unabhängige Einheiten, und* $v_1, \ldots, v_{k+1}$ *bilden eine Orthonormalbasis von* $\mathbb{R} \cdot L(\varepsilon_1) + \cdots + \mathbb{R} \cdot L(\varepsilon_{k+1})$.

Im Schritt (24) geht man analog vor.

(4) *Die Mengen* U_1' *und* U_2' *lassen sich im Rechner als dynamische Listen realisieren.* U_1' *und* U_2' *können sortiert nach den* Q*–Werten ihrer Elemente angelegt werden, wenn man im Schritt (12) binäres Einfügen verwendet. Hierdurch vereinfachen sich die Schritte (16) und (22).*

Wir haben bislang nur $C > n$ gefordert, aber noch nichts darüber gesagt, wie groß man C in der Praxis wählt. Betrachtet man nur die Abschätzung (2-13), so wäre ein C optimal, für welches $M_r \leq \tilde{C}$ gelten würde. Da M_r zu diesem Zeitpunkt noch nicht bekannt ist, müßte der Algorithmus 2.7 mit jeweils erhöhtem C solange aufgerufen werden, bis endlich r unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ mit $Q(\varepsilon_i) \leq \tilde{C}$ $(1 \leq i \leq r)$ in S_C' lägen. In der Praxis ist diese Methode völlig unbrauchbar, weil das Auszählen der Menge S_C' umso aufwendiger wird, je größer C ist. Welchen Wert aber nimmt man nun für C ?
Es sei $\alpha_1, \ldots, \alpha_n$ eine bzgl. der Länge T_2 reduzierte $\mathbb{Z}$–Basis von R. Wir wählen für C dann die doppelte Länge von α_n, also $C = 2T_2(\alpha_n)$. Diese Wahl von C beruht auf Erfahrungen und ist in den meisten Fällen ein vernünftiger Kompromiß zwischen der Güte der Regulatorabschätzung und dem Aufwand für das Auszählen von S_C.

Beispiel 2.9
Für $f(t) = t^{12} + 2t^{10} + 2t^9 + 2t^8 + 2t^7 + 2t^6 + 2t^5 + 2t^4 + 2t^3 + 2t^2 + 2t + 2$ *ist* F *total komplex (also* $r_1 = 0$, $r = 6$*) mit Diskriminante*

$$6\,915\,853\,790\,924\,800.$$

Für $R = \mathbb{Z}[\rho] = \mathfrak{o}_F$ *und* $C = 88.21$ *erhält man* $\#S_C' = 3864$ *sowie* $\#U_1' = 1$ *und* $\#U_2' = 4$. *Die Auswertung von* U_1', U_2' *liefert* $k = \ell = 1$ *und* $m = 5$ *mit*

$$\varepsilon_1 \quad = \quad -1 - \rho - \rho^2 - \rho^5 - \rho^6 - \rho^7 - \rho^9,$$

$$\begin{aligned}
\varepsilon_2 &= -1-\rho-3\rho^2-2\rho^3-2\rho^4-\rho^5-\rho^6-2\rho^7-\rho^8-2\rho^9-\rho^{11},\\
\varepsilon_3 &= -1-\rho-\rho^2+\rho^4+\rho^5-\rho^7-\rho^8-\rho^{10},\\
\varepsilon_4 &= -1-\rho^3-\rho^4-\rho^6-2\rho^9+\rho^{10}-\rho^{11},\\
\varepsilon_5 &= -3-\rho-2\rho^2-2\rho^3-2\rho^4-2\rho^5-2\rho^6-2\rho^7-2\rho^8-2\rho^9-\rho^{11}.
\end{aligned}$$

Als untere Regulatorabschätzung erhält man 1670.96*; das erzeugende Element von* $\mathrm{TU}(R)$ *ist* -1*. Die Rechenzeit betrug 247s.*

Das Beispiel 2.9 ist insofern besonders schön, weil $\varepsilon_1,\ldots,\varepsilon_5$ schon Grundeinheiten sind, denn aus (1-7) folgt

$$(\mathrm{U}(R):\langle -1,\varepsilon_1,\ldots,\varepsilon_5\rangle)=\frac{\mathrm{Reg}(\varepsilon_1,\ldots,\varepsilon_5)}{\mathrm{Reg}_R}\le\frac{3083.59}{1670.96}<2.$$

Bei dem Beispiel 2.9 fällt auf, daß nur sehr wenige Elemente aus S_C Einheiten sind. Diese Beobachtung, welche man in der Praxis sehr oft macht, ist der Ansatzpunkt für eine Beschleunigung von 2.7.

Bei einer Analyse der Laufzeit von Algorithmus 2.7 stellt man fest, daß rund 80% der Rechenzeit für das Berechnen der Normen in Schritt (6) verwandt werden, während cirka 20% auf den Auszählalgorithmus entfallen; der Rechenzeitanteil für die Auswertung von U_1' und U_2' sowie für die Bestimmung von ζ liegt meist unter 1%.

Da in S_C zumeist nur sehr wenige Einheiten liegen, könnte die Rechenzeit von 2.7 erheblich reduziert werden, wenn wir ein Kriterium zur *schnellen* Erkennung von Nicht–Einheiten hätten.

Das nächste Lemma ist zwar zunächst einmal in der Praxis wenig hilfreich, auf ihm beruht aber die Idee der Beschleunigung.

Lemma 2.10
$\alpha\in R$ ist genau dann keine Einheit, falls α in einem Primideal von R liegt.

Es sei $\mathfrak{p}$ ein Primideal von R, dessen Norm ein Primzahl p ist. Dann ist $1+\mathfrak{p}$ ein erzeugendes Element von $(R/\mathfrak{p},+)$. Also existiert zu jedem $i\in\{1,\ldots,n\}$ ein eindeutig bestimmtes $k\in\{0,\ldots,p-1\}$ mit

$$\omega_i\equiv k_i \bmod \mathfrak{p}. \tag{2-23}$$

Liefert der Auszählalgorithmus ein Element $\alpha\in S_C, \alpha=a_1\omega_1+\cdots+a_n\omega_n$, so kann α keine Einheit sein, falls α in $\mathfrak{p}$ liegt. Nach Wahl von $k_1,\ldots,k_n$ liegt α aber genau dann in $\mathfrak{p}$, falls gilt

$$a_1k_1+\cdots+a_nk_n\equiv 0 \bmod p. \tag{2-24}$$

Natürlich werden mit (2-24) nicht alle Nicht–Einheiten aus S_C erfaßt, so daß nach wie vor Normberechnungen notwendig sind. Deren Anzahl reduziert sich aber deutlich, wenn in R viele Primideale von kleiner Primzahlnorm liegen, die wir dann alle für den Test in (2-24) verwenden können.

Integrieren wir den Test (2-24) in den Algorithmus 2.7, so brauchen wir nur die Schritte (1) bis (6) abzuändern. Daher haben wir bei dem folgenden Algorithmus ab Schritt (6) auf die Wiedergabe des im Vergleich zu 2.7 unveränderten Teils verzichtet.

Algorithmus 2.11

Eingabe: $C \in \mathbb{R}^{>n}$; *eine endliche Menge* $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ *von Primidealen aus* R *mit* $\mathrm{N}(\mathfrak{p}_i) \in \mathbb{P}$ $(1 \leq i \leq s)$.

Ausgabe: *wie bei 2.7*

(1a) $\zeta \leftarrow -1$.

(1b) $U_1' \leftarrow U_2' \leftarrow \emptyset$.

(2a) *(Repräsentanten für die Basiselemente bestimmen)* $j \leftarrow s$.

(2b) *Falls* $j = 0$, *so gehe zu (3).*

(2c) $p_j \leftarrow \mathrm{N}(\mathfrak{p}_j)$.

(2d) *Für* $i = 1, \ldots, n$ *bestimme* $k_{ji} \in \{0, \ldots, p_j\}$ *mit* $\omega_i - k_{ji} \in \mathfrak{p}_j$.

(2e) *Setze* $j \leftarrow j - 1$ *und gehe zu (2b).*

(3) *Initialisiere den Auszählalgorithmus für* T_2 *und* C.

(4) *Zähle das nächste Element* $\alpha = a_1\omega_1 + \cdots + a_n\omega_n$ *aus.*

(5) *Falls* $\alpha = 0$, *so beginne mit der Auswertung von* U_1' *(Schritt (14) in 2.7).*

(6a) $j \leftarrow s$.

(6b) *Falls* $j = 0$, *so gehe zu (6e).*

(6c) *(*$\alpha \in \mathfrak{p}_j$ *?) Falls* $a_1k_1 + \cdots + a_nk_n \equiv 0 \bmod p_j$, *so gehe zu (4).*

(6d) *Setze* $j \leftarrow j - 1$ *und gehe zu (6b).*

(6e) *(*$\alpha \in \mathrm{U}(R)$ *?) Falls* $|\mathrm{N}(\alpha)| > 1$, *so gehe zu (4).*

...

Um 2.11 anzuwenden, müssen wir Primideale in R mit Primzahlnorm finden. Sei dazu $p \in \mathbb{P}$ beliebig, aber fest gewählt.

Für ein Ideal $\mathfrak{a} \neq \{0\}$ in R nennt man $M_\mathfrak{a} \in \mathbb{Z}^{n\times n}$ eine $\mathbb{Z}$–Basisdarstellung von $\mathfrak{a}$ bzgl. $\omega_1, \ldots, \omega_n$, falls eine $\mathbb{Z}$–Basis $\alpha_1, \ldots, \alpha_n$ von $\mathfrak{a}$ existiert, für die gilt

$$(\alpha_1, \ldots, \alpha_n) = (\omega_1, \ldots, \omega_n) \cdot M_\mathfrak{a}. \tag{2-25}$$

Unter der Bestimmung aller Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_\mu$ aus R, deren Norm gleich p ist, verstehen wir im folgenden die Berechnung von $\mathbb{Z}$–Basisdarstellungen dieser Ideale bzgl. der Basis $\omega_1, \ldots, \omega_n$.

Es sei $v_1, \ldots, v_n$ eine $\mathbb{Z}$–Basis von $\mathfrak{o}_F$. Für $R = \mathfrak{o}_F$ gelte ohne Einschränkung $\omega_i = v_i$ $(1 \leq i \leq n)$; für $R \subsetneqq \mathfrak{o}_F$ sei eine Transformationsmatrix $T \in \mathbb{Z}^{n\times n}$ gegeben mit

$$(\omega_1, \ldots, \omega_n) = (v_1, \ldots, v_n) \cdot T. \tag{2-26}$$

In der Maximalordnung existiert eine Faktorisierung

$$p\mathfrak{o}_F = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_\nu^{e_\nu} \tag{2-27}$$

mit paarweise verschiedenen Primidealen $\mathfrak{P}_1, \ldots, \mathfrak{P}_\nu$ aus $\mathfrak{o}_F$. In [12] wird ausführlich beschrieben, wie man $\mathbb{Z}$–Basisdarstellungen von $\mathfrak{P}_1, \ldots, \mathfrak{P}_\nu$ bzgl. der Basis $v_1, \ldots, v_n$ berechnen kann; hier wollen wir darauf nicht näher eingehen. Falls R die Maximalordnung ist, so sind alle Kandidaten für $\mathfrak{p}_1, \ldots, \mathfrak{p}_\mu$ bereits durch $\mathfrak{P}_1, \ldots, \mathfrak{P}_\nu$ gegeben, und wir müssen für $i = 1, \ldots, \nu$ jeweils nur noch $\mathrm{N}(\mathfrak{P}_i) = p$ überprüfen. Gilt dagegen $R \subsetneqq \mathfrak{o}_F$, so sind alle Kandidaten durch die Ideale $R \cap \mathfrak{P}_1, \ldots, R \cap \mathfrak{P}_\nu$ gegeben. Von diesen Idealen benötigen wir $\mathbb{Z}$–Basisdarstellungen bzgl. $\omega_1, \ldots, \omega_n$.

Wir betrachten dazu ein beliebiges Ideal $\mathfrak{A} \neq \{0\}$ in $\mathfrak{o}_F$ mit einer $\mathbb{Z}$–Basisdarstellung $M_{\mathfrak{A}}$ bzgl. $v_1, \ldots, v_n$. Zu jedem $\alpha \in \mathfrak{A} \cap R$ gibt es dann $\underline{u}, \underline{v} \in \mathbb{Z}^n$ mit

$$\alpha = (v_1, \ldots, v_n) \cdot M_{\mathfrak{A}} \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \tag{2-28}$$

(2-29)

$$\alpha = (\omega_1, \ldots, \omega_n) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = (v_1, \ldots, v_n) \cdot T \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}. \tag{2-30}$$

Hieraus erhalten wir

$$(T| - M_{\mathfrak{A}}) \begin{pmatrix} v_1 \\ \vdots \\ v_n \\ u_1 \\ \vdots \\ u_n \end{pmatrix} = \underline{0}. \tag{2-31}$$

Also gilt für jedes $\underline{x} \in \mathbb{Z}^{2n}$ mit $(T| - M_{\mathfrak{A}}) \cdot \underline{x} = \underline{0}$ dann

$$x_1\omega_1 + \cdots + x_n\omega_n \in \mathfrak{A} \cap R. \tag{2-32}$$

Bestimmen wir eine $\mathbb{Z}$–Basis $\underline{z}_1 = (z_{11}, \ldots, z_{2n,1})^t, \ldots, \underline{z}_n = (z_{1n}, \ldots, z_{2n,n})^t \in \mathbb{Z}^{2n}$ von

$$\{\underline{x} \in \mathbb{Z}^{2n} \mid (T| - M_{\mathfrak{A}}) \cdot \underline{x} = \underline{0}\}, \tag{2-33}$$

so ist

$$\begin{pmatrix} z_{11} & \ldots & z_{1n} \\ \vdots & & \vdots \\ z_{n1} & \ldots & z_{nn} \end{pmatrix} \tag{2-34}$$

eine $\mathbb{Z}$–Basisdarstellung von $\mathfrak{A} \cap R$ bzgl. $\omega_1, \ldots, \omega_n$. Aus den $\mathbb{Z}$–Basisdarstellungen von $\mathfrak{P}_1, \ldots, \mathfrak{P}_\nu$ bzgl. $v_1, \ldots, v_n$ erhalten wir auf diese Weise $\mathbb{Z}$–Basisdarstellungen von $\mathfrak{P}_1 \cap R, \ldots, \mathfrak{P}_\nu \cap R$ bzgl. $\omega_1, \ldots, \omega_n$.

Teilt p nicht den Index $(\mathfrak{o}_F : R)$, so gelten $\mathrm{N}(\mathfrak{P}_i) = \mathrm{N}(\mathfrak{P}_i \cap R)$ $(1 \leq i \leq \nu)$ und $\mathfrak{P}_i \cap R \neq \mathfrak{P}_j \cap R$ $(1 \leq i < j \leq \nu)$ gemäß [11, Chapter 6,Lemma 2.26]. Dies benutzen wir in den Schritten (10) und (13) des folgenden Algorithmus.

Algorithmus 2.12

Eingabe: $p \in \mathbb{P}$.

Ausgabe: $\mathbb{Z}$*–Basisdarstellungen* $M_{\mathfrak{p}_1}, \ldots, M_{\mathfrak{p}_\mu}$ *für alle Primideale aus* R*, deren Norm gleich* p *ist.*

(1) *Bestimme* $\mathbb{Z}$*–Basisdarstellungen* $M_{\mathfrak{P}_1}, \ldots, M_{\mathfrak{P}_\nu}$ *bzgl.* $v_1, \ldots, v_n$ *für alle Primideale aus* $\mathfrak{o}_F$*, die über* p *liegen.*

(2) $\mu \leftarrow i \leftarrow 0$.

(3) $i \leftarrow i + 1$.

(4) *Falls* $i > \nu$*, so terminiere.*

(5) *(Norm von* $\mathfrak{P}_i$ *bestimmen)* $d \leftarrow \det(M_{\mathfrak{P}_i})$.

(6) *Falls* $R \subsetneqq \mathfrak{o}_F$*, so gehe zu (10).*

(7) $(\mathrm{N}(\mathfrak{P}_i) = p$ *?) Falls* $d > p$*, so gehe zu (3).*

(8) $\mu \leftarrow \mu + 1, M_{\mathfrak{p}_\mu} \leftarrow M_{\mathfrak{P}_i}$.

(9) *Gehe zu (3).*

(10) *(*$R \subsetneqq \mathfrak{o}_F$*) Falls* $(p \not| (\mathfrak{o}_F : R)$ *und* $d > p)$*, so gehe zu (3).*

(11) *Bestimme bzgl.* $\omega_1, \ldots, \omega_n$ *eine* $\mathbb{Z}$*–Basisdarstellung* M *von* $\mathfrak{P}_i \cap R$ *(siehe oben).*

(12) $(\mathrm{N}(\mathfrak{P}_i \cap R) = p$ *?) Falls* $\det(M) > p$*, so gehe zu (3).*

(13) *Falls* $p \not| (\mathfrak{o}_F : R)$*, so gehe zu (15).*

(14) *Falls ein* $j \in \{1, \ldots, i-1\}$ *existiert mit* $\mathfrak{P}_j \cap R = \mathfrak{P}_i \cap R$*, so gehe zu (3).*

(15) $\mu \leftarrow \mu + 1, M_{\mathfrak{p}_\mu} \leftarrow M$.

(16) *Gehe zu (3).*

Bei der Implementierung wurden für 2.11 jeweils alle Primideale aus R mit Norm $2, 3, 5$ oder 7 bestimmt. Im Beispiel 2.9 etwa existieren genau vier solche Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$ $(\mathrm{N}(\mathfrak{p}_1) = 2, \mathrm{N}(\mathfrak{p}_2) = 3, \mathrm{N}(\mathfrak{p}_3) = 5, \mathrm{N}(\mathfrak{p}_4) = 7)$. Von den 3859 Nicht–Einheiten aus S'_C lagen 2980 in einem dieser Primideale. Bei gleicher Ausgabe betrug die Rechenzeit (einschließlich der Bestimmung von $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$) nur noch 67s.

Kapitel 3

Berechnung unabhängiger Einheiten

Dieses Kapitel zerfällt in zwei Teile. Davon ist der erste eher taktischer Natur, beim zweiten Teil geht es um Strategien. Um diese Zweiteilung etwas verständlicher zu machen, beginnen wir mit einer Definition.

Definition 3.1

(i) *Wir nennen einen Tupel (I, J) eine Konjugiertenrichtung, falls I, J Teilmengen von $\{1, \ldots, r+1\}$ sind, für welche $I \cap J = \emptyset$ und $1 \leq \#I \leq r$ gelten.*

(ii) *Sind $\alpha \in F$ und eine Konjugiertenrichtung (I, J) gegeben, so sprechen wir bei α von einem Element der Konjugiertenrichtung (I, J), falls gelten:*

$$|\alpha^{(i)}| < 1 \quad \text{für jedes } i \in I, \tag{3-1}$$

$$|\alpha^{(j)}| \geq 1 \quad \text{für jedes } j \in J. \tag{3-2}$$

Der erste Teil des Kapitels (Abschnitt 3.1) wird zunächst zeigen, daß zu jeder vorgegebenen Konjugiertenrichtung effektiv eine Einheit eben dieser Konjugiertenrichtung bestimmt werden kann. Im zweiten Teil (Abschnitt 3.2) werden dann verschiedene Strategien vorgestellt, wie man Einheiten ausgewählter Konjugiertenrichtungen zu einem System von r unabhängigen Einheiten zusammensetzen kann.

3.1 Konjugiertenrichtungen

Wir vereinbaren zuerst einige einfache Schreibweisen. Für zwei Konjugiertenrichtungen $(I, J), (\tilde{I}, \tilde{J})$ setzen wir:

(i) $(I, J) \subseteq (\tilde{I}, \tilde{J}) \quad :\Longleftrightarrow \quad I \subseteq \tilde{I}$ und $J \subseteq \tilde{J}$,

(ii) $\#(I, J) := \#I + \#J$.

Weiter definieren wir

$$\mathcal{I} := \{(\tilde{I}, \tilde{J}) \mid (\tilde{I}, \tilde{J}) \text{ ist eine Konjugiertenrichtung mit } \#(\tilde{I}, \tilde{J}) = r + 1\}. \quad (3\text{-}3)$$

Natürlich sind die Konjugiertenrichtungen aus $\mathcal{I}$ bereits durch ihre erste Komponente eindeutig bestimmt; um aber die Bezeichnungen kohärent zu halten, notieren wir sie stets wie die übrigen Konjugiertenrichtungen.

Es seien $(I, J), (\tilde{I}, \tilde{J})$ zwei beliebige, aber fest gewählte Konjugiertenrichtungen mit $(I, J) \subseteq (\tilde{I}, \tilde{J})$ und $(\tilde{I}, \tilde{J}) \in \mathcal{I}$. Wir wollen eine Einheit ε der Konjugiertenrichtung (I, J) berechnen. Die Grundidee besteht darin, in R rekursiv eine Folge $(\gamma_k)_{k \in \mathbb{Z}^{\geq 0}}$ mit folgenden Eigenschaften zu konstruieren:

(1) $\gamma_0 = 1$,

(2) $|\gamma_{k+1}^{(i)}| < |\gamma_k^{(i)}| \quad \forall\, i \in I, k \in \mathbb{Z}^{\geq 0}$,

(3) $|\gamma_{k+1}^{(j)}| \geq |\gamma_k^{(j)}| \quad \forall\, j \in J, k \in \mathbb{Z}^{\geq 0}$,

(4) es existiert eine Konstante $C \in \mathbb{R}^{\geq 0}$ mit $|\mathrm{N}(\gamma_k)| \leq C \;\forall\, k \in \mathbb{Z}^{\geq 0}$.

Da es in R nur endlich viele nicht–assoziierte Elemente α mit $|\mathrm{N}(\alpha)| \leq C$ gibt, und weil die Folgenglieder gemäß (2) paarweise verschieden sind, existieren Indices $\mu, \nu \in \mathbb{Z}^{\geq 0}, \mu > \nu$, so daß

$$\varepsilon = \frac{\gamma_\mu}{\gamma_\nu} \quad (3\text{-}4)$$

eine Einheit in R ist. Wegen (2) und (3) ist ε die gewünschte Einheit.

Es seien zu $k \in \mathbb{Z}^{\geq 0}$ bereits Folgenglieder $\gamma_0, \ldots, \gamma_k \in R$ gefunden, welche den Bedingungen (1) bis (4) genügen. Wir bestimmen ein $\beta_{k+1} \in F$, für welches gelten:

(5) $\beta_{k+1} \in \frac{1}{\gamma_k} R$,

(6) $|\beta_{k+1}^{(i)}| < 1 \;\forall\, i \in I$,

(7) $|\beta_{k+1}^{(j)}| \geq 1 \;\forall\, j \in J$,

(8) $|\mathrm{N}(\beta_{k+1})| \cdot |\mathrm{N}(\gamma_k)| \leq C$.

Dann erfüllt $\gamma_{k+1} := \beta_{k+1} \cdot \gamma_k$ offenbar die Bedingungen (1) bis (4).

Zur Konstruktion von β_{k+1} setzen wir

$$\iota := \#\{i \in \tilde{I} \mid 1 \leq i \leq r_1\} + 2\#\{i \in \tilde{I} \mid r_1 < i \leq r + 1\}. \quad (3\text{-}5)$$

Für ein $\delta \in \mathbb{R}^{\geq 1}$, welches wir später noch genauer bestimmen werden, legen wir $\underline{\lambda} \in \mathbb{R}^n$ fest durch

$$\lambda_\nu := \begin{cases} \delta^{\frac{\iota - n}{\iota}} & \text{falls } \nu \in \tilde{I} \\ \delta & \text{falls } \nu \in \tilde{J} \end{cases} \qquad (1 \leq \nu \leq r + 1), \quad (3\text{-}6)$$

$$\lambda_{\nu + r_2} := \lambda_\nu \qquad (r_1 < \nu \leq r + 1). \quad (3\text{-}7)$$

Offenbar gilt $\prod_{i=1}^{n} \lambda_i = 1$.

Mittels $\underline{\lambda}$ definieren wir auf dem $\mathbb{Z}$–Modul $M_k := \frac{1}{\gamma_k} R$ durch

$$T_{2,\underline{\lambda}} : M_k \to \mathbb{R}^{\geq 0} : x \mapsto \sum_{i=1}^{n} \frac{1}{\lambda_i^2} |x^{(i)}|^2 \tag{3-8}$$

eine positiv definite quadratische Form. Diese besitzt die Determinante

$$\det(T_{2,\underline{\lambda}}) = \frac{|\mathrm{disc}(R)|}{|\mathrm{N}(\gamma_k)|^2}. \tag{3-9}$$

Bezüglich $T_{2,\underline{\lambda}}$ bestimmen wir jetzt eine LLL–reduzierte Basis $b_1, \ldots, b_n$ des Moduls M_k. Nach [6, Proposition 1.6] gilt für das erste Element dieser Basis

$$T_{2,\underline{\lambda}}(b_1) \leq 2^{\frac{1}{2}(n-1)} \det(T_{2,\underline{\lambda}})^{\frac{1}{n}} = 2^{\frac{1}{2}(n-1)} \frac{|\mathrm{disc}(R)|^{\frac{1}{n}}}{|\mathrm{N}(\gamma_k)|^{\frac{2}{n}}}. \tag{3-10}$$

Wir setzen $\beta_{k+1} := b_1$ und außerdem

$$\hat{C} := 2^{\frac{1}{4}(n-1)} |\mathrm{disc}(R)|^{\frac{1}{2n}}. \tag{3-11}$$

Aus (3-10) und der Definition von $T_{2,\underline{\lambda}}$ folgt dann

$$|\beta_{k+1}^{(i)}| < \delta^{\frac{\iota - n}{\iota}} \frac{\hat{C}}{|\mathrm{N}(\gamma_k)|^{\frac{1}{n}}} \qquad \forall\, i \in \tilde{I}, \tag{3-12}$$

$$|\beta_{k+1}^{(j)}| < \delta \frac{\hat{C}}{|\mathrm{N}(\gamma_k)|^{\frac{1}{n}}} \qquad \forall\, j \in \tilde{J}. \tag{3-13}$$

Daraus erhalten wir

$$|\mathrm{N}(\beta_{k+1})| \leq \left(\delta^{\frac{\iota - n}{\iota}} \frac{\hat{C}}{|\mathrm{N}(\gamma_k)|^{\frac{1}{n}}} \right)^{\iota} \left(\delta \frac{\hat{C}}{|\mathrm{N}(\gamma_k)|^{\frac{1}{n}}} \right)^{n-\iota} = \frac{\hat{C}^n}{|\mathrm{N}(\gamma_k)|}. \tag{3-14}$$

Für die Konstante C aus (4) kann demnach $\hat{C}^n$ gewählt werden.

Wegen $\gamma_k \beta_{k+1} \in R \setminus \{0\}$ gilt

$$|\mathrm{N}(\beta_{k+1})| \geq \frac{1}{|\mathrm{N}(\gamma_k)|}. \tag{3-15}$$

Hiermit erhalten wir für jedes $j \in J$ aus (3-13) nun

$$\begin{aligned} |\beta_{k+1}^{(j)}| &= |\mathrm{N}(\beta_{k+1})| \prod_{\substack{i=1 \\ i \neq j}}^{n} \frac{1}{|\beta_{k+1}^{(i)}|} \\ &\geq \frac{1}{|\mathrm{N}(\gamma_k)|} \frac{|\mathrm{N}(\gamma_k)|^{\frac{\iota}{n}}}{\hat{C}^{\iota} \delta^{\iota - n}} \frac{|\mathrm{N}(\gamma_k)|^{\frac{n-\iota-1}{n}}}{\hat{C}^{n-\iota-1} \delta^{n-\iota-1}} \\ &= \frac{\delta}{|\mathrm{N}(\gamma_k)|^{\frac{1}{n}} \hat{C}^{n-1}}. \end{aligned} \tag{3-16}$$

δ wird jetzt so gewählt, daß β_{k+1} auch noch die Bedingungen (6) und (7) erfüllt. Setzen wir

$$d := \left(\frac{\hat{C}}{|\mathrm{N}(\gamma_k)|^{\frac{1}{n}}} \right)^{\frac{\iota}{n-\iota}}, \tag{3-17}$$

$$D := |\mathrm{N}(\gamma_k)|^{\frac{1}{n}} \hat{C}^{n-1}, \tag{3-18}$$

so gilt $D = \max(d, D)$. Wegen (3-12) und (3-16) reicht es also $\delta = D$ zu wählen.

In der Praxis rechnet man zur Bestimmung von ε natürlich nur solange neue Folgenglieder aus, bis $\mu, \nu \in \mathbb{Z}^{\geq 0}$ wie bei (3-4) gefunden sind. Dies ist die Motivation für die folgende Sprechweise:

Sprechweise
Zu $\kappa \in \mathbb{N}$ verstehen wir unter einer Folge zur Konjugiertenrichtung (I, J) ab jetzt einen Tupel $\gamma_{(I,J)} = (\gamma_0, \ldots, \gamma_\kappa)$ mit Elementen aus R, welche in Analogie zu den Bedingungen (1) bis (4) die folgenden Eigenschaften besitzen:

(i) $\gamma_0 = 1$,

(ii) $|\gamma_{k+1}^{(i)}| < |\gamma_k^{(i)}| \quad \forall\, i \in I, k \in \{0, \ldots, \kappa - 1\}$,

(iii) $|\gamma_{k+1}^{(j)}| \geq |\gamma_k^{(j)}| \quad \forall\, j \in J, k \in \{0, \ldots, \kappa - 1\}$,

(iv) $|\mathrm{N}(\gamma_k)| \leq \hat{C}^n \quad \forall\, k \in \{0, \ldots, \kappa\} \qquad (\hat{C}$ wie bei (3-11)),

(v) $\frac{\gamma_\mu}{\gamma_\nu} \notin \mathrm{U}(R) \qquad (0 \leq \mu < \nu \leq \kappa - 1)$,

(vi) es existiert ein $k \in \{0, \ldots, \kappa - 1\}$ derart, daß $\frac{\gamma_\kappa}{\gamma_k} \in \mathrm{U}(R)$.

Als Länge der Folge $\gamma_{(I,J)}$ bezeichnen wir den Wert $\ell(\gamma_{(I,J)}) := \kappa$.
Bei der Konstruktion von β_{k+1} hatten wir nur darauf geachtet, daß β_{k+1} die Bedingungen (6) und (7) erfüllt. Für eine Implementierung spielt darüber hinaus die Effizienz der Bestimmung von β_{k+1} eine wichtige Rolle. Mit den folgenden Zusätzen kann man eine erhebliche Reduzierung der Rechenzeit erreichen:

(1) Die Abschätzung in (3-16), aus der die Wahl von D resultierte, ist nicht sehr scharf. Es ist günstiger, wenn man für δ zunächst den im Vergleich zu D wesentlich kleineren Wert d wählt. Das damit berechnete β_{k+1} leistet $|\beta_{k+1}^{(i)}| < 1 \;\forall\, i \in I$. Falls ein $j \in J$ mit $|\beta_{k+1}^{(j)}| < 1$ existiert, so wird δ vergrößert, und damit anschließend ein neues β_{k+1} berechnet. Diesen Vorgang wiederholt man solange, bis endlich $|\beta_{k+1}^{(j)}| \geq 1 \;\forall\, j \in J$ gilt.

Eine noch kleinere Wahl von δ (z.B. $\delta = \frac{d}{2}$) hat sich in der Praxis nicht bewährt, weil dann β_{k+1} häufig nicht mehr die Bedingung (6) erfüllt.

(2) Zu γ_k existieren $d_k \in \mathbb{N}$ und $\tilde{\gamma}_k \in R$ mit $\frac{1}{\gamma_k} = \frac{1}{d_k}\tilde{\gamma}_k$. Ist $A_k \in \mathbb{Z}^{n \times n}$ die Darstellungsmatrix von $\tilde{\gamma}_k$ bezüglich $\omega_1, \ldots, \omega_n$, so gilt

$$\frac{1}{\gamma_k}(\omega_1, \ldots, \omega_n) = \frac{1}{d_k}(\omega_1, \ldots, \omega_n)A_k. \tag{3-19}$$

Wir bestimmen nun $T \in \mathrm{GL}(n, \mathbb{Z})$, so daß die Matrix $A_k T$ LLL–reduziert ist. Dann bilden $\alpha_1, \ldots, \alpha_n \in F$,

$$(\alpha_1, \ldots, \alpha_n) := \frac{1}{d_k}(\omega_1, \ldots, \omega_n)A_k T \tag{3-20}$$

eine $\mathbb{Z}$–Basis des Moduls M_k. Benutzt man jetzt $\alpha_1, \ldots, \alpha_n$ als Ausgangsbasis für die Berechnung der bezüglich $T_{2,\underline{\lambda}}$ LLL–reduzierten Basis $b_1, \ldots, b_n$,

so ist die LLL–Reduktion hiermit wesentlich schneller, als wenn man stattdessen $\frac{\omega_1}{\gamma_k}, \ldots, \frac{\omega_n}{\gamma_k}$ als Ausgangsbasis wählt. Insbesondere reicht für die LLL–Reduktion bei Verwendung von $\alpha_1, \ldots, \alpha_n$ eine deutlich niedrigere Präzision.

Im Hinblick auf den zweiten Abschnitt des Kapitels wollen wir den Algorithmus, welchen die bisherigen Ausführungen nahelegen, gleich geringfügig allgemeiner formulieren.

Sprechweise

Zu $k \in \mathbb{Z}^{\geq 0}$ nennen wir einen Tupel $\gamma_{(I,J),(\tilde{I},\tilde{J})} = (\gamma_0, \ldots, \gamma_k)$ einen Folgenanfang zu den Konjugiertenrichtungen (I, J) und $(\tilde{I}, \tilde{J})$, falls $\kappa \in \mathbb{N}, \kappa > k$, und Elemente $\gamma_{k+1}, \ldots, \gamma_\kappa$ existieren, so daß der Tupel $(\gamma_0, \ldots, \gamma_\kappa)$ eine Folge zur Konjugiertenrichtung (I, J) ist.

Die zweite Konjugiertenrichtung $(\tilde{I}, \tilde{J})$ bei einem Folgenanfang $\gamma_{(I,J),(\tilde{I},\tilde{J})}$ brauchen wir zur Steuerung des folgenden Algorithmus. Über sie wird ι aus (3-5) und damit $\underline{\lambda}$ in (3-6) gesetzt.

Algorithmus 3.2

Eingabe: *ein Folgenanfang* $\gamma_{(I,J),(\tilde{I},\tilde{J})} = (\gamma_0, \ldots, \gamma_k)$.

Ausgabe: *entweder eine Einheit* ε *der Konjugiertenrichtung* (I, J) *oder einen Folgenanfang* $\gamma'_{(I,J),(\tilde{I},\tilde{J})} = (\gamma'_0, \ldots, \gamma'_{k+1})$ *mit* $\gamma'_i = \gamma_i$ $(1 \leq i \leq k)$.

(1) *(Wähle δ)* $\delta \leftarrow d$.

(2) *Setze $\underline{\lambda}$ wie in (3-6).*

(3) *Bestimme eine bzgl. $T_{2,\underline{\lambda}}$ LLL–reduzierte Basis $b_1, \ldots, b_n$ des Moduls $\frac{1}{\gamma_k}R$ (verwende dazu als Ausgangsbasis $\alpha_1, \ldots, \alpha_n$ aus (3-20)).*

(4) $\beta_{k+1} \leftarrow b_1$.

(5) *Falls kein $j \in J$ mit $|\beta_{k+1}^{(j)}| < 1$ existiert, so gehe zu (8).*

(6) *(δ war zu klein)* $\delta \leftarrow 2\delta$.

(7) *(Neuer Versuch) Gehe zu (2).*

(8) $\gamma \leftarrow \beta_{k+1}\gamma_k$.

(9) $\nu \leftarrow 0$.

(10) *Falls $|\mathrm{N}(\gamma)| \neq |\mathrm{N}(\gamma_\nu)|$, so gehe zu (13).*

(11) *Falls $\frac{1}{\gamma_\nu}\gamma \notin R$, so gehe zu (13).*

(12) *(Einheit zurückliefern) Setze $\varepsilon \leftarrow \frac{\gamma}{\gamma_\nu}$ und terminiere.*

(13) $\nu \leftarrow \nu + 1$.

(14) *Falls $\nu \leq k$, so gehe zu (10).*

(15) *(Folgenanfang zurückliefern)* $\gamma'_{(I,I),(\tilde{I},\tilde{J})} \leftarrow (\gamma_0, \ldots, \gamma_k, \gamma)$.

(16) *Terminiere.*

Bemerkung 3.3

(a) *Mögliche Präzisionsfehler bei der LLL–Reduktion kann man dadurch abfangen, daß man im Schritt (5) von 3.2 zusätzlich $|\beta_{k+1}^{(i)}| < 1 \; \forall \, i \in I$ prüft.*

(b) *Wir benutzen von $\beta_{k+1} = b_1$ nur die Eigenschaft*

$$T_{2,\underline{\lambda}}(b_1) \leq \frac{\hat{C}^2}{|\mathrm{N}(\gamma_k)|^{\frac{2}{n}}} \tag{3-21}$$

aus (3-10). Insofern könnte ein geeignetes Element für β_{k+1} auch mit dem Auszählalgorithmus ermittelt werden. Weiterhin bestände die Möglichkeit, daß man die LLL–Reduktion vorzeitig abbricht, sobald ein Basiselement b_1 berechnet ist , welches (3-21) leistet, da ja die anderen Basiselemente nicht benötigt werden. Diese beiden Alternativen für die Bestimmung von β_{k+1} haben sich in der Praxis nicht bewährt. Die hiermit gebildeten Folgen waren zumeist wesentlich länger.

Die Bestimmung einer Einheit zu einer vorgegebenen Konjugiertenrichtung ist nun trivial.

Algorithmus 3.4

Eingabe: *eine Konjugiertenrichtung (I, J).*

Ausgabe: *eine Einheit ε der Konjugiertenrichtung (I, J).*

(1) $(\tilde{I}, \tilde{J}) \leftarrow (I, \{1, \ldots, r+1\} \setminus I)$.

(2) *(Folgenanfang initialisieren)* $\gamma_{(I,J),(\tilde{I},\tilde{J})} \leftarrow (1)$.

(3) *Rufe Algorithmus 3.2 mit $\gamma_{(I,J),(\tilde{I},\tilde{J})}$ auf. Falls eine Einheit ε zurückgegeben wird, so terminiere, sonst ersetze $\gamma_{(I,J),(\tilde{I},\tilde{J})}$ durch den zurückgegebenen Folgenanfang.*

(4) *Gehe zu (3).*

Bemerkung 3.5

Die Wahl von $(\tilde{I}, \tilde{J})$ in Schritt (1) von 3.4 hat sich in der Praxis zwar bewährt, ist aber nicht immer zwingend. Falls mehrere Konjugiertenrichtungen

$$(\tilde{I}_1, \tilde{J}_1), \ldots, (\tilde{I}_k, \tilde{J}_k) \in \mathcal{I}$$

existieren mit $(I, J) \subseteq (\tilde{I}_\nu, \tilde{J}_\nu)$ $(1 \leq \nu \leq k)$, so kann man sich eine Liste $\mathcal{L}$ mit k Folgenanfängen $\gamma_{(I,J),(\tilde{I}_1,\tilde{J}_1)}, \ldots, \gamma_{(I,J),(\tilde{I}_k,\tilde{J}_k)}$ anlegen, welche zunächst alle initialisiert werden als der triviale Folgenanfang (1). Wendet man nun 3.2 so auf die Folgenanfänge aus $\mathcal{L}$ an, daß die Folgenanfänge gleichmäßig an Länge gewinnen, so hat dieses Vorgehen in der Praxis häufig den Vorteil, daß man die Einheit ε zur Konjugiertenrichtung (I, J) aus einem kürzeren Folgenanfang gewinnt, als wenn man nur mit einem einzigen Folgenanfang rechnet. Die Schwierigkeit dabei besteht allerdings in einer geeigneten Wahl von k und danach bei der Auswahl von $(\tilde{I}_1, \tilde{J}_1), \ldots, (\tilde{I}_k, \tilde{J}_k)$. Der Verfasser hat hierzu verschiedene Varianten ausprobiert. In den meisten Fällen wurde dabei der Algorithmus 3.4 deutlich ineffizienter als bei der Wahl nur eines Folgenanfangs. Insbesondere erscheint es wenig zweckmäßig, bei den Folgenanfängen in die Breite zu gehen, wenn man, wie in der speziellen Situation von 3.4, nur eine Einheit zu einer bestimmten Konjugiertenrichtung berechnen möchte.

Bevor wir uns im zweiten Abschnitt den Strategien zuwenden, mit denen Systeme von r unabhängigen Einheiten konstruiert werden können, erwähnen wir noch kurz, wie man zu gegebenen Einheiten $\varepsilon_1, \ldots, \varepsilon_s \in \mathrm{U}(R) \setminus \mathrm{TU}(R), s \in \mathbb{N}$, ein minimales

Erzeugendensystem von $\langle \varepsilon_1, \ldots, \varepsilon_s \rangle$ berechnen kann. Man betrachtet hierzu die Vektoren $L(\varepsilon_1), \ldots, L(\varepsilon_s)$ im $\mathbb{R}^r$.
Mit dem MLLL–Algorithmus (siehe [11, Chapter 3]) lassen sich $\mathbb{R}$–linear unabhängige Vektoren $v_1, \ldots, v_t \in \mathbb{Z} \cdot L(\varepsilon_1) + \cdots + \mathbb{Z} \cdot L(\varepsilon_s)$ ermitteln mit

$$\mathbb{Z} \cdot v_1 + \cdots + \mathbb{Z} \cdot v_t = \mathbb{Z} \cdot L(\varepsilon_1) + \cdots + \mathbb{Z} \cdot L(\varepsilon_s).$$

Die Vektoren $v_1, \ldots, v_t$ korrespondieren zu unabhängigen Einheiten $\eta_1, \ldots, \eta_t \in \mathrm{U}(R)$, für welche gilt

$$\langle \eta_1, \ldots, \eta_t \rangle = \langle \varepsilon_1, \ldots, \varepsilon_s \rangle.$$

3.2 Strategien

Für die Konstruktion eines Systems von r unabhängigen Einheiten gibt es sehr unterschiedliche Vorgehensweisen (Strategien), wie wir gleich sehen werden. Da die Bestimmung eines solchen Systems im Zusammenhang mit den beiden anderen Schritten des Verfahrens zur Berechnung von $\mathrm{U}(R)$ gesehen werden muß, sollte eine gute Strategie die folgenden drei Kriterien erfüllen:

- Die Strategie ist effizient (schnell).
- Der Index des mit der Strategie berechneten Systems in der Einheitengruppe $\mathrm{U}(R)$ ist klein, damit die Grundeinheitenberechnung im dritten Schritt nicht zu aufwendig wird.
- Die eventuell schon bei der Regulatorabschätzung gewonnenen unabhängigen Einheiten werden von der Strategie berücksichtigt.

Diese Kriterien sind relativ. Um also eine Strategie zu beurteilen, muß man sie mit anderen Strategien vergleichen.

In diesem Abschnitt nun werden zunächst vier Strategien vorgestellt und danach miteinander verglichen.

3.2.1 Strategie 1 (Dirichlet–Einheiten)

Wir können mit Algorithmus 3.4 Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$ konstruieren, so daß gelten:

(i) $\quad |\varepsilon_i^{(i)}| \geq 1 \ (1 \leq i \leq r)$,

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

Diese Einheiten — auch Dirichlet–Einheiten genannt — bilden ein System von r unabhängigen Einheiten (siehe etwa [11, Chapter 5,Lemma 2.12]), womit die erste Strategie bereits beschrieben ist.

Algorithmus 3.6 (Strategie 1)
Ausgabe: *Dirichlet–Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ von R.*

(1) $i \leftarrow 1$.
(2) $I \leftarrow \{1, \ldots, r+1\} \setminus \{i\}$.
(3) *Bestimme mit Algorithmus 3.4 eine Einheit ε_i der Konjugiertenrichtung $(I, \emptyset)$.*
(4) $i \leftarrow i + 1$.
(5) *Falls $i \leq r$, so gehe zu (2).*
(6) *Terminiere.*

3.2.2 Strategie 2

Es seien unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_m \in \mathrm{U}(R)$ bekannt ($m \in \{0, \ldots, r-1\}$). Wir wollen zeigen, wie man eine Konjugiertenrichtung (I_{m+1}, J_{m+1}) so wählen kann, daß die hierzu mit Algorithmus 3.4 ausgerechnete Einheit ε_{m+1} unabhängig von $\varepsilon_1, \ldots, \varepsilon_m$ ist.

Hierzu definieren wir die Matrix $A \in \mathbb{R}^{m \times r}$ durch

$$A := \begin{pmatrix} L(\varepsilon_1)^t \\ \vdots \\ L(\varepsilon_m)^t \end{pmatrix}. \tag{3-22}$$

Wir berechnen $V \in \mathrm{GL}(m, \mathbb{R})$ und $U \in \mathrm{GL}(r, \mathbb{Z})$, so daß die Matrix

$$B = (\beta_{ij}) = V \cdot A \cdot U \tag{3-23}$$

Zeilenstufenform besitzt (also $\beta_{ij} = 0$ $(1 \leq j < i \leq m), \beta_{ii} > 0$ $(1 \leq i \leq m)$). Dabei soll die Matrix U nur für eventuell notwendige Spaltenvertauschungen benutzt werden. Sei nun ein $\underline{v} \in \mathbb{R}^r$ gegeben mit

(i) $v_i < 0$ für alle $i \in \{1, \ldots, m\}$ mit $\beta_{i,m+1} < 0$,

(ii) $v_j \geq 0$ für alle $j \in \{1, \ldots, m\}$ mit $\beta_{j,m+1} \geq 0$,

(iii) $v_{m+1} < 0$.

Dann ist $\underline{v}^t$ linear unabhängig von den Zeilen aus B, wie man leicht nachprüft, indem man $\underline{v}^t$ als Zeile $m+1$ zur Matrix B hinzufügt und anschließend die Zeilenstufenform der auf diese Weise vergrößerten Matrix ausrechnet. Mit 3.4 läßt sich eine Einheit $\varepsilon_{m+1} \in \mathrm{U}(R)$ derart konstruieren, daß $L(\varepsilon_{m+1})^t \cdot U$ alle von $\underline{v}$ geforderten Eigenschaften besitzt. Wegen 1.7 sind $\varepsilon_1, \ldots, \varepsilon_m, \varepsilon_{m+1}$ unabhängig. Dieses Vorgehen läßt sich problemlos iterieren.

Algorithmus 3.7
Eingabe: *unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_m \in R$ $(0 \leq m < r)$.*
Ausgabe: *eine Konjugiertenrichtung (I, J), so daß eine Einheit dieser Konjugiertenrichtung unabhängig von $\varepsilon_1, \ldots, \varepsilon_m$ ist.*

(1) *Falls* $m = 0$, *so setze* $(I, J) \leftarrow (\{1\}, \emptyset)$ *und terminiere.*
(2) *Bilde* $A \in \mathbb{R}^{m \times r}$ *wie in (3-22).*
(3) *Berechne* $V \in GL(m, \mathbb{R})$ *und* $U \in GL(r, \mathbb{Z})$, *so daß die Matrix*

$$B = (\beta_{ij}) = V \cdot A \cdot U$$

Zeilenstufenform besitzt (U *nur für Spaltenvertauschungen).*
(4) $k \leftarrow 1$.
(5) $\underline{v}^t = (v_1, \ldots, v_r) \leftarrow (0, \ldots, 0)$.
(6) *Falls* $\beta_{k,m+1} < 0$, *so setze* $v_k \leftarrow -1$, *sonst* $v_k \leftarrow 1$.
(7) $k \leftarrow k + 1$.
(8) *Falls* $k \leq m$, *so gehe zu (6).*
(9) $v_{m+1} \leftarrow -1$.
(10) $\underline{v}^t \leftarrow \underline{v}^t \cdot U^{-1}$.
(11) *(Bestimmung der Konjugiertenrichtung)* $k \leftarrow 1, I \leftarrow J \leftarrow \emptyset$.
(12) *Falls* $v_k = 0$, *so gehe zu (14).*
(13) *Falls* $v_k = -1$, *so setze* $I \leftarrow I \cup \{k\}$, *sonst* $J \leftarrow J \cup \{k\}$.
(14) $k \leftarrow k + 1$.
(15) *Falls* $k \leq r$, *so gehe zu (12).*
(16) *Terminiere.*

Wir haben diesen Algorithmus separat notiert, weil wir ihn später in der vierten Strategie verwenden.

Algorithmus 3.8 (Strategie 2)
Eingabe: *unabhängige Einheiten* $\varepsilon_1, \ldots, \varepsilon_m \in R$ $(0 \leq m \leq r)$.
Ausgabe: *Einheiten* $\varepsilon_{m+1}, \ldots, \varepsilon_r \in R$, *so daß* $\varepsilon_1, \ldots, \varepsilon_r$ *unabhängig sind.*

(1) $i \leftarrow m + 1$.
(2) *Falls* $i > r$, *so terminiere.*
(3) *Bestimme mit 3.7 eine Konjugiertenrichtung* (I_i, J_i) *zu* $\varepsilon_1, \ldots, \varepsilon_{i-1}$, *so daß eine Einheit der Konjugiertenrichtung* (I_i, J_i) *unabhängig von* $\varepsilon_1, \ldots, \varepsilon_{i-1}$ *ist.*
(4) *Berechne mit 3.4 eine Einheit* ε_i *der Konjugiertenrichtung* (I_i, J_i).
(5) *Setze* $i \leftarrow i + 1$ *und gehe zu (2).*

Bemerkung 3.9
Falls für die in Schritt (3) ermittelte Konjugiertenrichtung $\#J_i > \#I_i$ *gilt, so hat es sich in der Praxis bewährt,* ε_i *aus der Konjugiertenrichtung* (J_i, I_i) *zu bestimmen.*

3.2.3 Strategie 3

Ziel der dritten Strategie ist es, kürzest mögliche Folgen zu finden. Dazu legen wir uns eine Liste $\mathcal{L}$ mit allen Folgenanfängen der Form $\gamma_{(I,\emptyset),(I,\{1,\ldots,r+1\}\setminus I)}$ an, wobei zu Beginn alle Folgenanfänge dieser Liste initialisiert sind als der triviale Folgenanfang (1). Die Folgenanfänge in $\mathcal{L}$ werden nun mit Hilfe von Algorithmus 3.2 gleichmäßig verlängert, und zwar solange, bis wir schließlich ein System von r unabhängigen Einheiten haben. Das Verfahren terminiert spätestens, wenn es Dirichlet–Einheiten berechnet hat.

Algorithmus 3.10 (Strategie 3)
Ausgabe: *unabhängige Einheiten* $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$.

(1) *(Folgenanfänge initialisieren) Für jede Konjugiertenrichtung* $(\tilde{I}, \tilde{J}) \in \mathcal{I}$ *setze* $\gamma_{(\tilde{I},\emptyset),(\tilde{I},\tilde{J})} \leftarrow (1)$.

(2) *(Liste* $\mathcal{L}$ *anlegen)* $\mathcal{L} \leftarrow \emptyset$.

(3) *Für jede Konjugiertenrichtung* $(\tilde{I}, \tilde{J}) \in \mathcal{I}$ *setze* $\mathcal{L} \leftarrow \mathcal{L} \cup \{\gamma_{(\tilde{I},\emptyset),(\tilde{I},\tilde{J})}\}$.

(4) $k \leftarrow 0$.

(5) *(Folgenanfang minimaler Länge aus* $\mathcal{L}$ *wählen) Wähle einen Folgenanfang* $\gamma_{(\tilde{I}',\emptyset),(\tilde{I}',\tilde{J}')}$ *aus* $\mathcal{L}$ *mit*

$$\ell(\gamma_{(\tilde{I}',\emptyset),(\tilde{I}',\tilde{J}')}) = \min\{\ell(\gamma_{(\tilde{I},\emptyset),(\tilde{I},\tilde{J})}) \mid \gamma_{(\tilde{I},\emptyset),(\tilde{I},\tilde{J})} \in \mathcal{L}\}.$$

(6) $\mathcal{L} \leftarrow \mathcal{L} \setminus \gamma_{(\tilde{I}',\emptyset),(\tilde{I}',\tilde{J}')}$.

(7) *Rufe Algorithmus 3.2 mit* $\gamma_{(\tilde{I}',\emptyset),(\tilde{I}',\tilde{J}')}$ *auf. Falls eine Einheit* ε *zurückgegeben wird, so gehe zu (9), sonst lege den zurückgegebenen Folgenanfang in der Liste* $\mathcal{L}$ *ab.*

(8) *Gehe zu (5).*

(9) *Bestimme mit dem MLLL–Algorithmus ein minimales Erzeugendensystem* $\eta_1, \ldots, \eta_j$ *von* $\langle \varepsilon_1, \ldots, \varepsilon_k, \varepsilon \rangle$.

(10) $k \leftarrow j$.

(11) $\varepsilon_i \leftarrow \eta_i$ $(1 \le i \le j)$.

(12) *Falls* $k = r$, *so terminiere.*

(13) *Gehe zu (5).*

3.2.4 Strategie 4

Die letze Strategie ist eine Kombination der zweiten und dritten. Wir bestimmen mit 3.7 zunächst eine Konjugiertenrichtung (I, J), so daß eine Einheit zu dieser Konjugiertenrichtung unabhängig von den bereits vorhandenen Einheiten ist. Zu (I, J) wählen wir $(\tilde{I}, \tilde{J}) \in \mathcal{I}$ wie in Schritt (2) von Algorithmus 3.4, also $(\tilde{I}, \tilde{J}) = (I, \{1, \ldots, r+1\} \setminus I)$. Danach initialisieren wir den Folgenanfang $\gamma_{(I,J),(\tilde{I},\tilde{J})}$, rufen dann aber den Algorithmus 3.2 mit $\gamma_{(I,J),(\tilde{I},\tilde{J})}$ höchstens k_1 mal auf, wobei wir $k_1 \in \mathbb{N}$ vor Beginn der Strategie festlegen. Haben wir bis dahin keine Einheit zur Konjugiertenrichtung (I, J) erhalten, verzweigen wir in den Algorithmus 3.10. In

diesem soll nun höchstens k_2 mal der Schritt (7) durchlaufen werden, wobei wir $k_2 \in \mathbb{N}$ ebenfalls zu Beginn setzen müssen. Anschließend, sofern in 3.10 keine Einheiten gefunden worden ist, wird erneut Algorithmus 3.4 mit dem Folgenanfang $\gamma_{(I,J),(\tilde{I},\tilde{J})}$ aufgerufen usf.. Den genauen Ablauf, der etwas verwickelt ist, kann man dem nachfolgenden Algorithmus entnehmen.

Algorithmus 3.11 (Strategie 4)
Eingabe: *unabhängige Einheiten* $\varepsilon_1, \ldots, \varepsilon_m \in R$ $(0 \leq m \leq r)$;
$k_1, k_2 \in \mathbb{Z}^{\geq 0}, k_1 + k_2 > 0$.
Ausgabe: *unabhängige Einheiten* $\eta_1, \ldots, \eta_r \in R$.

(1) $s \leftarrow m$.
(2) *(Folgenanfänge initialisieren) Für jede Konjugiertenrichtung* $(\tilde{I}, \tilde{J}) \in \mathcal{I}$ *setze* $\gamma_{(\tilde{I},\emptyset),(\tilde{I},\tilde{J})} \leftarrow (1)$.
(3) *(Liste* $\mathcal{L}$ *anlegen)* $\mathcal{L} \leftarrow \emptyset$.
(4) *Für jede Konjugiertenrichtung* $(\tilde{I}, \tilde{J}) \in \mathcal{I}$ *setze* $\mathcal{L} \leftarrow \mathcal{L} \cup \{\gamma_{(I,\emptyset),(\tilde{I},\tilde{J})}\}$.
(5) *(Flag zurücksetzen)* $\ell \leftarrow 0$.
(6) $\eta_i \leftarrow \varepsilon_i$ $(1 \leq i \leq s)$.
(7) *Falls* $s = r$, *so terminiere.*
(8) *(Flag prüfen) Falls* $\ell \neq 0$, *so gehe zu (12).*
(9) *Bestimme mit 3.7 eine Konjugiertenrichtung* (I_{s+1}, J_{s+1}) *zu* $\eta_1, \ldots, \eta_s$, *so daß eine Einheit der Konjugiertenrichtung* (I_{s+1}, J_{s+1}) *unabhängig von* $\eta_1, \ldots, \eta_s$ *ist.*
(10) $\gamma_{(I_{s+1},J_{s+1}),(I_{s+1},\{1,\ldots,r+1\}\setminus I_{s+1})} \leftarrow (1)$.
(11) *(Flag setzen)* $\ell \leftarrow 1$.
(12) $k \leftarrow 0$.
(13) *Falls* $k = k_1$, *so gehe zu (17).*
(14) *Rufe Algorithmus 3.2 mit* $\gamma_{(I_{s+1},J_{s+1}),(I_{s+1},\{1,\ldots,r+1\}\setminus I_{s+1})}$ *auf. Falls eine Einheit* ε *zurückgegeben wird, so gehe zu (24), sonst speichere den zurückgegebenen Folgenanfang in* $\gamma_{(I_{s+1},J_{s+1}),(I_{s+1},\{1,\ldots,r+1\}\setminus I_{s+1})}$ *ab.*
(15) $k \leftarrow k + 1$.
(16) *Gehe zu (13).*
(17) $k \leftarrow 0$.
(18) *Falls* $k = k_2$, *so gehe zu (12).*
(19) *(Folgenanfang minimaler Länge aus* $\mathcal{L}$ *wählen) Wähle einen Folgenanfang* $\gamma_{(\tilde{I}',\emptyset),(\tilde{I}',\tilde{J}')}$ *aus* $\mathcal{L}$ *mit*

$$\ell(\gamma_{(\tilde{I}',\emptyset),(\tilde{I}',\tilde{J}')}) = \min\{\ell(\gamma_{(\tilde{I},\emptyset),(\tilde{I},\tilde{J})}) \mid \gamma_{(\tilde{I},\emptyset),(\tilde{I},\tilde{J})} \in \mathcal{L}\}.$$

(20) $\mathcal{L} \leftarrow \mathcal{L} \setminus \gamma_{(\tilde{I}',\emptyset),(\tilde{I}',\tilde{J}')}$.
(21) *Rufe Algorithmus 3.2 mit* $\gamma_{(\tilde{I}',\emptyset),(\tilde{I}',\tilde{J}')}$ *auf. Falls eine Einheit* ε *zurückgegeben wird, so gehe zu (28), sonst lege den zurückgegebenen Folgenanfang in der Liste* $\mathcal{L}$ *ab.*
(22) $k \leftarrow k + 1$.
(23) *Gehe zu (18).*
(24) *(Einheit aus Strategie 2)* $s \leftarrow s + 1$.

(25) $\eta_s \leftarrow \varepsilon$.
(26) *(Flag zurücksetzen)* $\ell \leftarrow 0$.
(27) *Gehe zu (7).*
(28) *(Einheit aus Strategie 3) Bestimme mit dem MLLL–Algorithmus ein minimales Erzeugendensystem* $e_1, \ldots, e_j$ *von* $\langle \eta_1, \ldots, \eta_s, \varepsilon \rangle$.
(29) *(Flag zurücksetzen ?) Falls* $j > s$, *so setze* $\ell \leftarrow 0$.
(30) $\eta_i \leftarrow e_i$ $(1 \leq i \leq j)$.
(31) $s \leftarrow j$.
(32) *Gehe zu (7).*

Bemerkung 3.12
Durch einige technische Modifikationen läßt sich erreichen, daß nicht die dieselben Folgenanfänge mehrfach berechnet werden.

Der Vorteil der vierten Strategie besteht darin, daß sie bei den Folgenanfängen in die Breite geht und dadurch eventuell sehr kurze Folgen findet, andererseits aber durch das Einbinden von Strategie 2 sicherstellt, daß unabhängige Einheiten auch dann schnell gefunden werden, wenn es keine kurzen Folgen gibt.

Nach der Vorstellung der vier Strategien beginnen wir nun mit dem Vergleich. Da es klar ist, daß nur die Strategien 2 und 4 in der Lage sind, bereits vorhandene Einheiten bei der Berechnung eines Systems von r unabhängigen Einheiten zu berücksichtigen, konzentrieren wir uns im folgenden auf die ersten beiden Kriterien. Dazu betrachten wir zwei Beispiele, bei denen wir den ersten Schritt des Verfahrens, also die Bestimmung der unteren Regulatorabschätzung, ausgelassen haben, so daß in allen Körpern jeweils noch r unabhängige Einheiten zu konstruieren waren. Bei Strategie 4 wurden k_1, k_2 gesetzt als $(k_1, k_2) \leftarrow (5, 5)$.

Die 287 Körper des ersten Beispiels, welche [14] entnommen wurden, sind alle vom Grad 5. 186 von ihnen besitzen den Einheitenrang 2, 79 den Einheitenrang 3. Die restlichen 22 sind total reell. Gerechnet wurde jeweils in der von dem Körperpolynom erzeugten Gleichungsordnung. In 188 Fällen war die Gleichungsordnung maximal.

In der folgenden Tabelle werden die Strategien paarweise verglichen. In der ersten Spalte findet sich jeweils die Rechenzeit, die jede einzelne Strategie für die Berechnung aller 287 Beispiele benötigte. Hiermit kann also die Effizienz der Strategien überprüft werden. In den nachfolgenden Spalten, welche horizontal zu lesen sind, werden die Strategien in Bezug auf das zweite Kriterium verglichen. Wir erklären das an einem Beispiel: In der zweiten Zeile der letzten Spalte steht die Zahl 53, gefolgt von einer eingeklammerten 33. Dies bedeutet, daß die Regulatoren der unabhängigen Einheitensysteme, welche mit der ersten Strategie (Dirichlet–Einheiten) berechnet wurden, in 53 Fällen kleiner oder gleich waren, als die jeweiligen Regulatoren der Einheitensysteme, die mit der vierten Strategie berechnet wurden. Die eingeklammerte 33 sagt aus, daß mit der ersten Strategie genau 33 mal ein unabhängiges System ausgerechnet wurde, dessen Regulator echt kleiner war als der

Regulator des Systems, welches für die gleiche Ordnung von der vierten Strategie errechnet wurde.

	Rechenzeit	Strategie 1	Strategie 2	Strategie 3	Strategie 4
Strategie 1	10617s		68(55)	32(1)	53(33)
Strategie 2	7242s	232(219)		95(9)	222(3)
Strategie 3	12486s	286(255)	268(192)		261(153)
Strategie 4	8927s	254(234)	284(65)	134(26)	

Beim nächsten Beispiel geben wir die exakten Ergebnisse an. In den ersten beiden Spalten stehen Körperpolynom und Einheitenrang, in den nachfolgenden Spalten sind für jede Strategie die Rechenzeit und der Index des berechneten unabhängigen Systems in $\mathrm{U}(R)$ angegeben. Gerechnet wurde jeweils in der Maximalordnung.

$f(t)$	r	Strategie 1		Strategie 2		Strategie 3		Strategie 4	
t^5+2	2	1s	9	1s	2	4s	1	1s	2
t^6+2	2	2s	9	3s	11	9s	3	3s	11
t^7+2	3	9s	51	5s	8	11s	1	5s	8
t^8+2	3	8s	48	8s	14	27s	8	8s	14
t^9+2	4	26s	2915	15s	24	22s	1	15s	24
$t^{10}+2$	4	91s	1344	109s	1537	57s	4	65s	3
$t^{11}+2$	5	106s	138741	71s	624	94s	1	70s	624
$t^{12}+2$	5	379s	8892224	128s	8548	288s	6	144s	216
$t^{13}+2$	6	1410s	569936835	297s	18750	226s	4	459s	42
t^5+3	2	2s	5	2s	1	4s	1	2s	1
t^6+3	2	3s	14	2s	1	6s	1	2s	1
t^7+3	3	8s	45	13s	45	17s	1	12s	1
t^8+3	3	10s	288	11s	46	15s	1	11s	46
t^9+3	4	105s	8064	39s	361	15s	3	11s	12
$t^{10}+3$	4	56s	31310	26s	510	35s	1	26s	510
$t^{11}+3$	5	339s	917404	101s	15611	118s	7	154s	7
t^5+5	2	4s	5	2s	1	8s	1	2s	1
t^6+5	2	3s	4	3s	2	10s	2	3s	2
t^7+5	3	27s	171	26s	35	44s	1	21s	3
t^8+5	3	28s	128	23s	13	34s	2	24s	13
t^9+5	4	56s	978	290s	828	119s	2	149s	3
$t^{10}+5$	4	72s	1580	57s	6	255s	1	48s	6
$t^{11}+5$	5	2131s	3492925	1740s	45214	1358s	16	682s	11
t^5+7	2	2s	4	2s	1	7s	2	2s	1
t^6+7	2	2s	4	2s	2	6s	1	2s	2
t^7+7	3	54s	109	61s	18	139s	9	87s	24
t^8+7	3	18s	342	8s	4	23s	1	8s	12
t^9+7	4	60s	2405	160s	471	131s	5	227s	10
$t^{10}+7$	4	76s	42456	25s	298	32s	5	25s	298
Σ		5088s		3220s		3196s		2308s	

Bewerten wir die Strategien nach den drei eingangs erwähnten Kriterien, so ist die vierte Strategie am ehesten geeignet, alle Kriterien *gleichmäßig* zu erfüllen. Sie hat noch einen weiteren Vorteil, den wir kurz erläutern wollen:

Für ein System von r unabhängigen Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ können wir den Index $(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle)$ mit Hilfe der Regulatorschranke abschätzen. Setzen wir

$$S := \left\lfloor \frac{\mathrm{Reg}(\varepsilon_1, \ldots, \varepsilon_r)}{\text{untere Regulatorabschätzung}} \right\rfloor, \tag{3-24}$$

so gilt nach (1-7) nämlich

$$(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle) \leq S. \tag{3-25}$$

Falls S noch *sehr groß* ist, empfiehlt es sich, einige weitere Einheiten $\varepsilon_{r+1}, \ldots, \varepsilon_{r+k}$ zu berechnen, um damt $\langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle)$ zu vergrößern. Hierzu könnnen die Folgenanfänge aus der Liste $\mathcal{L}$ der vierten Strategie verwendet werden. Bei der Implementierung wurden zusätzlich $\lfloor \frac{r}{2} \rfloor$ Einheiten berechnet, falls $S \geq r^2$ galt (sobald die aktualisierte Indexschranke allerdings unter den Wert von r^2 fiel, wurde die Berechnung gestoppt). Dazu wurden aus $\mathcal{L}$ rund r Folgenanfänge genommen, auf die der Algorithmus 3.4 so angewandt wurde, daß die Folgenanfänge gleichmäßig an Länge gewannen.

Kapitel 4

Aufstieg zu Grundeinheiten

Wir knüpfen an die Situation vom Ende des letzten Kapitels an. Es seien also unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$ sowie ein $S \in \mathbb{N}, S > 1$, gegeben mit

$$(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle) \leq S. \tag{4-1}$$

Mit den Verfahren aus diesem Kapitel können wir entweder zeigen, daß $\varepsilon_1, \ldots, \varepsilon_r$ bereits Grundeinheiten sind, oder aber von $\varepsilon_1, \ldots, \varepsilon_r$ zu einem Grundeinheitensystem von $\mathrm{U}(R)$ aufsteigen.

Die Grundidee beruht dabei auf drei einfachen Aussagen aus der Gruppentheorie.

Lemma 4.1
Es sei G eine abelsche Gruppe mit einer Untergruppe $H \subseteq G$, für welche der Index $(G : H)$ endlich ist. Für jedes $p \in \mathbb{P}$ ist

$$H_p := \{x \in G \mid \exists\, \nu \in \mathbb{N} \text{ mit } x^{p^\nu} \in H\} \tag{4-2}$$

eine Untergruppe von G mit $H \subseteq H_p \subseteq G$. Wir nennen H_p die p–maximale Obergruppe von H in G; H heißt p–maximal, wenn $H = H_p$ gilt.

Lemma 4.2
Seien G und H wie in 4.1. Ferner sei $p \in \mathbb{P}$ beliebig, aber fest vorgegeben.

(a) Es existiert $\nu \in \mathbb{Z}^{\geq 0}$ mit $p^\nu = (H_p : H)$.

(b) Ist H' eine weitere Untergruppe von G mit $H_p \subseteq H' \subseteq G$, so gilt $H' = H'_p$.

Beweis

(a) Offenbar ist H_p/H eine p–Gruppe.

(b) Angenommen $H' \subsetneqq H'_p$. Wegen (a) teilt p den Index $(H'_p : H_p)$. Also existiert nach dem Satz von Cauchy ein Element $x \in H'_p \setminus H_p$ mit $x^p \in H_p$. Hieraus folgt $x \in H_p$, was zu einem Widerspruch führt. □

Lemma 4.3
Seien G und H wie in 4.1. Dann gilt $H = G$ genau dann, falls kein $p \in \mathbb{P}$ mit $H \subsetneqq H_p$ existiert.

Bezeichnet jetzt U_p die p–maximale Obergruppe von $U = \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle$ in $\mathrm{U}(R)$, so sind $\varepsilon_1, \ldots, \varepsilon_r$ bereits Grundeinheiten nach 4.3, falls kein $p \in \mathbb{P}, p \leq S$, mit $U \subsetneqq U_p$ existiert. Es wird nun unsere nächste Aufgabe sein, ein Verfahren herzuleiten, mit dem wir zu jedem $p \in \mathbb{P}$ die Gruppe U_p bestimmen können, wobei unter der Bestimmung von U_p natürlich die Berechnung von unabhängigen Einheiten $\eta_1, \ldots, \eta_r$ mit $U_p = \langle \zeta, \eta_1, \ldots, \eta_r \rangle$ zu verstehen ist.

Bevor wir uns dieser Aufgabe widmen, beschreiben wir zunächst, wie man die p–maximale Obergruppe bei der Berechnung eines Grundeinheitensystems einsetzt. Dazu wird zuerst eine Liste $P = \{p_1, \ldots, p_t\}$ der Primzahlen unterhalb von S angelegt. Die Liste P verwaltet alle Primzahlen p, für welche U möglicherweise noch nicht p–maximal ist. Nach 4.2 gilt insbesondere

$$U \subseteq U_{p_1} \subseteq (U_{p_1})_{p_2} \subseteq \ldots \subseteq (\ldots((U_{p_1})_{p_2})\ldots)_{p_k} = \mathrm{U}(R), \tag{4-3}$$

wobei wir die Primzahlen in P beliebig durchnumerieren können. Aus P wählen wir jetzt eine beliebige Primzahl p, zu der wie die p–maximale Obergruppe U_p von U in $\mathrm{U}(R)$ ermitteln. Wir ersetzen dann U durch U_p und können neben p anschließend auch alle Primzahlen aus P entfernen, welche größer als die neue Indexschranke $\lfloor \frac{S}{(U_p:U)} \rfloor$ sind. Falls die Liste P nun noch nicht leer ist, wählen wir eine neue Primzahl aus P und gehen analog wie oben vor. Nach endlich vielen Schritten ist man bei $\mathrm{U}(R)$ angelangt. Daraus ergibt sich der folgende Algorithmus.

Algorithmus 4.4
Eingabe: *unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$;*
ein $S \in \mathbb{N}$ mit $(U(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle) \leq S$.
Ausgabe: *Grundeinheiten $E_1, \ldots, E_r$ von $\mathrm{U}(R)$*

(1) *(Liste P anlegen)* $P \leftarrow \mathbb{P} \cap \{1, \ldots, S\}$.
(2) $E_i \leftarrow \varepsilon_i$ $(1 \leq i \leq r)$.
(3) *Falls $P = \emptyset$, so terminiere.*
(4) *(p wählen)* $p \leftarrow \min(P)$.
(5) *Bestimme $\eta_1, \ldots, \eta_r \in \mathrm{U}(R)$, so daß $\langle \zeta, \eta_1, \ldots, \eta_r \rangle$ die p–maximale Obergruppe von $\langle \zeta, E_1, \ldots, E_r \rangle$ ist.*
(6) *(Indexschranke anpassen)*

$$S \leftarrow \left\lfloor \frac{S}{(\langle \zeta, \eta_1, \ldots, \eta_r \rangle : \langle \zeta, E_1, \ldots, E_r \rangle)} \right\rfloor .$$

(7) $E_i \leftarrow \eta_i$ $(1 \leq i \leq r)$.
(8) $P \leftarrow P \setminus \{p\}$.
(9) $P \leftarrow P \cap \{1, \ldots, S\}$.
(10) *Gehe zu (2).*

4.1 Bestimmung p–maximaler Obergruppen

In diesem Abschnitt seien $p \in \mathbb{P}$, unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$ sowie $S \in \mathbb{N}$ mit $(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle) \leq S$ vorgegeben. Berechnet werden soll die p–maximale Oberordnung von $\langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle$ in $\mathrm{U}(R)$.

Lemma 4.5
Die Gruppe $\langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle$ ist genau dann p–maximal in $\mathrm{U}(R)$, falls für alle $m_0, \ldots, m_r \in \{0, \ldots, p-1\}, m_1 + \cdots + m_r > 0$, keine Lösung $\eta \in R$ existiert von

$$\eta^p = \zeta^{m_0} \cdot \varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}. \tag{4-4}$$

Beweis Konsequenz aus der Definition 4.1. □

Falls ζ eine p–te Potenz in R ist, so kann zusätzlich $m_0 = 0$ in (4-4) gefordert werden. Es gilt:

Lemma 4.6
ζ ist genau dann eine p–te Potenz in R, falls $\mathrm{ggT}(p, \#\mathrm{TU}(R)) = 1$ gilt.

Um Lemma 4.5 effektiv einzusetzen, brauchen wir ein Verfahren, mit dem wir Wurzeln in einer Ordnung ziehen können. Bei dem hier vorgestellten Verfahren wird dazu der Auszählalgorithmus verwendet.

Es seien $\varepsilon \in \mathrm{U}(R)$ und $m \in \mathbb{N}$ fest vorgegeben. Wir wollen wissen, ob ein $\eta \in R$ mit $\eta^m = \varepsilon$ existiert, und dieses η auch — sofern existent — berechnen. Hierzu legen wir $\underline{\lambda} \in \mathbb{R}^n$ fest durch

$$\lambda_j := \sqrt[m]{|\varepsilon^{(j)}|} \qquad (1 \leq j \leq n). \tag{4-5}$$

Mittels $\underline{\lambda}$ definieren wir auf R durch

$$T_{2,\underline{\lambda}} : R \to \mathbb{R}^{\geq 0} : x \mapsto \sum_{j=1}^{n} \frac{1}{\lambda_j^2} |x^{(j)}|^2 \tag{4-6}$$

eine positiv definite quadratische Form. Man prüft leicht nach:

Lemma 4.7
Falls es ein $\eta \in R$ mit $\eta^m = \varepsilon$ gibt, so gilt

$$T_{2,\underline{\lambda}}(\eta) = n. \tag{4-7}$$

Wir wollen die Aussage von 4.7 für unsere Zwecke leicht verschärfen. Für jedes $x \in R \setminus \{0\}$ folgt aus der Ungleichung zwischen arithmetischem und geometrischem Mittel die Beziehung

$$1 = \frac{1}{|\mathrm{N}(\varepsilon)|^{\frac{2}{nm}}} \leq \left(\frac{|\mathrm{N}(x)|^2}{|\mathrm{N}(\varepsilon)|^{\frac{2}{m}}} \right)^{\frac{1}{n}} = \left(\prod_{j=1}^{n} \frac{1}{\lambda_j^2} |x^{(j)}|^2 \right)^{\frac{1}{n}} \leq \frac{T_{2,\underline{\lambda}}(x)}{n}. \tag{4-8}$$

Gilt nun $T_{2,\underline{\lambda}}(x) = n$, so tritt in (4-8) überall Gleichheit ein. Hieraus folgt

$$|x^{(j)}| = \sqrt[m]{|\varepsilon^{(j)}|} \qquad (1 \leq j \leq n), \tag{4-9}$$

denn die Ungleichung zwischen arithmetischem und geometrischem Mittel ist genau dann scharf, falls alle beteiligten Werte gleich sind. Somit erhalten wir:

Lemma 4.8
Existiert ein $x \in R$ mit $0 < T_{2,\underline{\lambda}}(x) \leq n$, so gilt $\varepsilon = x^m$ modulo einer Einheitswurzel. Insbesondere ist x eine Einheit.

Zur späteren Verwendung notieren wir den Algorithmus zu Lemma 4.8 separat.

Algorithmus 4.9
Eingabe: $\varepsilon \in \mathrm{U}(R); m \in \mathbb{N}$.
Ausgabe: *Falls existent, ein $\eta \in \mathrm{U}(R)$ mit $\eta^m \equiv \varepsilon \bmod \mathrm{TU}(R)$, sonst 0.*

(1) *(Auszählen nötig ?) Falls $p = 2$ und $\mathrm{N}(\varepsilon) = -1$, so terminiere mit $\eta \leftarrow 0$.*
(2) *Initialisiere den Auszählalgorithmus bzgl. $T_{2,\underline{\lambda}}$ und n.*
(3) *Zähle das nächste Element η aus.*
(3) *Terminiere.*

Mit 4.9 kann die Aussage von 4.5 effektiv zum Bestimmen der p–maximalen Obergruppe verwendet werden. Da das Vorgehen kanonisch ist, formulieren wir es gleich als Algorithmus.

Algorithmus 4.10
Eingabe: *unabhängige Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$; $p \in \mathbb{P}$; ein $S \in \mathbb{N}$ mit $(\mathrm{U}(R) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle) \leq S$.*
Ausgabe: *Einheiten $e_1, \ldots, e_r \in \mathrm{U}(R)$, so daß $\langle \zeta, e_1, \ldots, e_r \rangle$ die p–maximale Obergruppe von $\langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle$ in $\mathrm{U}(R)$ ist.*

(1) $e_i \leftarrow \varepsilon_i$ $(1 \leq i \leq r)$.
(2) $s \leftarrow S$.
(3) *Falls $s < p$, so terminiere.*
(4) *Prüfe mit Algorithmus 4.9, ob $m_1, \ldots, m_r \in \{0, \ldots, p-1\}$, $m_1 + \cdots + m_r > 0$, und ein $\eta \in \mathrm{U}(R)$ existieren mit*

$$\eta^p \equiv \varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r} \bmod \mathrm{TU}(R).$$

Falls kein solches η existiert, so terminiere.
(5) *Berechne mit dem MLLL–Algorithmus ein minimales Erzeugendensystem $\eta_1, \ldots, \eta_r \in \mathrm{U}(R)$ von $\langle e_1, \ldots, e_r, \eta \rangle$.*
(6) $e_i \leftarrow \eta_i$ $(1 \leq i \leq r)$.
(7) *(Indexschranke anpassen)* $s \leftarrow \lfloor \frac{s}{p} \rfloor$.
(8) *Gehe zu (3).*

Für größere Werte von p und r ist der Algorithmus 4.10 nicht praktikabel, da im Schritt (2) p^r quadratische Formen ausgezählt werden müssen, sofern $\langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle$ schon p–maximal ist. Wir werden jetzt einen Algorithmus darstellen, welcher die Zahl der in Schritt (2) auszuzählenden quadratischen Formen auf maximal r Stück begrenzt. Der Algorithmus setzt dabei an einer Stelle voraus, daß R die Maximalordnung $\mathfrak{o}_F$ ist. Im nächsten Abschnitt werden wir beschreiben, wie wir die Vorteile des Algorithmus auch für unsere beliebig gewählte Ordnung R nutzen können. Da der Algorithmus nicht mehr so elementar ist wie die bislang vorgestellten Verfahren, brauchen wir zunächst eine etwas längere Vorbereitung.

Lemma 4.11
Seien K ein Körper und $a \in K$. Das Polynom $t^p - a$ ist genau dann über K irreduzibel, wenn a keine p–te Potenz in K ist.

Beweis Siehe [5, Chapter VII,Theorem 9.1]. □

Es sei ab jetzt ein $a \in \mathfrak{o}_F$ fest vorgegeben, welches in $\mathfrak{o}_F$ keine p–te Potenz ist. Dann ist $t^p - a$ wegen 4.11 in F irreduzibel. Sei nun $\mathcal{P}(a)$ die Menge aller Primideale $\mathfrak{p}$ aus $\mathfrak{o}_F$, für die $t^p - a$ in $\mathfrak{o}_F/\mathfrak{p}[t]$ irreduzibel bleibt. Wir werden zunächst zeigen, daß $\mathcal{P}(a)$ unendlich viele Primideale enthält. Dies beruht auf den folgenden beiden Aussagen.

Satz 4.12 (Frobenius)
Es sei $L|K$ eine endliche galoissche Erweiterung eines Zahlkörpers K. Für jeden Automorphismus σ aus der Galoisgruppe $\mathrm{G}(L|K)$ ist die Menge der in L unverzweigten Primideale $\mathfrak{p}$ aus $\mathfrak{o}_K$, zu denen jeweils ein Primideal $\mathfrak{P}$ in $\mathfrak{o}_L$ sowie ein $k \in \mathbb{N}$ mit $\Phi(\mathfrak{P}|\mathfrak{p}) = \sigma^k$ und $\mathrm{ggT}(k, \mathrm{ord}(\sigma)) = 1$ existieren, unendlich (hierbei sei $\Phi(\mathfrak{P}|\mathfrak{p})$ der Frobenius–Automorphismus von $\mathfrak{P}$ über $\mathfrak{p}$).

Beweis Siehe [3, Chapter IV, Theorem 5.2]. □

Folgerung 4.13
Seien K ein Zahlkörper sowie $g(t)$ ein normiertes und irreduzibles Polynom aus $\mathfrak{o}_K[t]$ vom Grad p. Dann existieren unendlich viele Primideale $\mathfrak{p}$ in $\mathfrak{o}_K$, für welche $g(t)$ in $\mathfrak{o}_K/\mathfrak{p}[t]$ irreduzibel bleibt.

Beweis Sei $a \in \mathbb{C}$ eine beliebige Nullstelle von $g(t)$. Setze $L := K(a)$, und sei ferner M der Zerfällungskörper von $g(t)$ über L. Dann ist die Erweiterung $M|K$ galoissch.

Da p den Grad $[M : K]$ teilt, existiert nach dem Satz von Cauchy ein K–Automorphismus σ in der Galoisgruppe $\mathrm{G}(M|K)$ mit $\mathrm{ord}(\sigma) = p$. Nach 4.12 existieren dann unendlich viele Primideale $\mathfrak{p}$ in $\mathfrak{o}_K$, zu denen es jeweils ein Primideal $\mathfrak{P}$ in $\mathfrak{o}_M$ und ein $k \in \mathbb{N}$ mit $\Phi(\mathfrak{P}|\mathfrak{p}) = \sigma^k$ und $\mathrm{ggT}(k, \mathrm{ord}(\sigma)) = 1$ gibt. Sei nun ein solches $\mathfrak{p}$ mit zugehörigem $\mathfrak{P}$ beliebig, aber fest gewählt. Es gilt

$$\mathrm{ord}(\Phi(\mathfrak{P}|\mathfrak{p})) = \mathrm{ord}(\sigma^k) = \frac{\mathrm{ord}(\sigma)}{\mathrm{ggT}(\mathrm{ord}(\sigma), k)} = \frac{p}{\mathrm{ggT}(\mathrm{ord}(\sigma), k)} = p. \qquad (4\text{-}10)$$

Nach Konstruktion des Frobenius–Automorphismus entspricht $\mathrm{ord}(\Phi(\mathfrak{P}|\mathfrak{p}))$ dem Trägheitsgrad $f_{M|K}(\mathfrak{P}|\mathfrak{p})$ von $\mathfrak{P}$ über $\mathfrak{p}$. Also erhalten wir

$$p = f_{M|K}(\mathfrak{P}|\mathfrak{p}) = f_{M|L}(\mathfrak{P}|\mathfrak{P} \cap \mathfrak{o}_L) \cdot f_{L|K}(\mathfrak{P} \cap \mathfrak{o}_L|\mathfrak{p}). \tag{4-11}$$

Da die Erweiterung $M|L$ galoissch ist, teilt $f_{M|L}(\mathfrak{P}|\mathfrak{P} \cap \mathfrak{o}_L)$ den Grad $[M : L]$. Andererseits teilt p nicht den Grad $[M : L]$, denn es gilt $[M : K] \leq p!$ und $[L : K] = p$. Daraus ergibt sich

$$f_{L|K}(\mathfrak{P} \cap \mathfrak{o}_L|\mathfrak{p}) = p. \tag{4-12}$$

Setzen wir nun ohne Einschränkung voraus, daß $\mathfrak{p}$ nicht die Polynomdiskriminante von g enthält, so ist $g(t)$ gemäß dem Zerlegungssatz in $\mathfrak{o}_K/\mathfrak{p}[t]$ irreduzibel. □

Bemerkung 4.14
Die Aussage aus 4.13 ist falsch, sofern der Grad von $g(t)$ keine Primzahl ist. Beispielsweise ist $x^4 + 1$ in $\mathbb{Z}[t]$ irreduzibel, aber reduzibel in $\mathbb{Z}/q \cdot \mathbb{Z}[t]$ für alle $q \in \mathbb{P}$ (siehe [4, Section 4.6.2]).

Folgerung 4.15
$\mathcal{P}(a)$ enthält unendlich viele Primideale.

Bei der praktischen Bestimmung eines Primideals aus $\mathcal{P}(a)$ werden wir die beiden folgenden Lemmata verwenden.

Lemma 4.16
Für jedes $\mathfrak{p} \in \mathcal{P}(a)$ ist p ein Teiler von $\mathrm{N}(\mathfrak{p}) - 1$.

Beweis Angenommen p teilt nicht $\mathrm{N}(\mathfrak{p}) - 1$. Dann gilt $\mathrm{ggT}(p, \mathrm{N}(\mathfrak{p}) - 1) = 1$, also existiert ein $u \in \mathbb{N}$ mit $up \equiv 1 \bmod (\mathrm{N}(\mathfrak{p}) - 1)$. Hieraus folgt $(a^u)^p \equiv a \bmod \mathfrak{p}$, was im Widerspruch zur Irreduzibilität von $t^p - a$ in $\mathfrak{o}_F/\mathfrak{p}[t]$ steht. □

Lemma 4.17
Sei $\mathfrak{p}$ ein beliebiges Primideal aus $\mathfrak{o}_F$, für welches $p|(\mathrm{N}(\mathfrak{p}) - 1)$ gilt. $\beta \in \mathfrak{o}_F$ ist genau dann eine p-te Potenz modulo $\mathfrak{p}$, falls gilt

$$\beta^{\frac{N(\mathfrak{p})-1}{p}} - 1 \in \mathfrak{p}. \tag{4-13}$$

Beweis Falls $\beta \equiv \gamma^p \bmod \mathfrak{p}$ für ein $\gamma \in \mathfrak{o}_F$ gilt, so folgt

$$\beta^{\frac{N(\mathfrak{p})-1}{p}} \equiv \gamma^{N(\mathfrak{p})-1} \equiv 1 \bmod \mathfrak{p}. \tag{4-14}$$

Nun gelte umgekehrt (4-13). Zu $\xi \in \mathfrak{o}_F$ mit $\langle \xi + \mathfrak{p} \rangle = (\mathfrak{o}_F/\mathfrak{p})^\times$ wähle $v \in \mathbb{Z}^{\geq 0}$ mit $\beta \equiv \xi^v \bmod \mathfrak{p}$. Wegen $\mathrm{ord}(\xi + \mathfrak{p}) = \mathrm{N}(\mathfrak{p}) - 1$ ist dann $\mathrm{N}(\mathfrak{p}) - 1$ ein Teiler von $\frac{v(N(\mathfrak{p})-1)}{p}$. Also teilt p die Zahl v. □

Mit $\mathcal{P}(a)$ enthält auch die Menge

$$\mathcal{P}'(a) = \{\mathfrak{p} \in \mathcal{P}(a) \mid (\mathfrak{o}_F : \mathbb{Z}[\rho]) \notin \mathfrak{p}\} \tag{4-15}$$

unendlich viele Primideale. Zur Ermittlung eines Primideals aus $\mathcal{P}'(a)$ bestimmen wir durch (gezieltes) Ausprobieren $q \in \mathbb{P}$ minimal derart, daß über q ein Primideal $\mathfrak{p}$ aus $\mathcal{P}(a)$ liegt. Zu $\mathfrak{p}$ und q existiert ein $s \in \{1, \ldots, n\}$ mit $\mathrm{N}(\mathfrak{p}) = q^s$. Nach Lemma 4.16 gilt dann $p|(q^s - 1)$.

Bei der Suche nach q beginnen wir also mit der kleinsten Primzahl $\tilde{q} \in \mathbb{P}$, welche nicht den Index $(\mathfrak{o}_F : \mathbb{Z}[\rho])$ teilt und zu der ein $\tilde{s} \in \{1, \ldots, n\}$ existiert mit $p|(\tilde{q}^{\tilde{s}} - 1)$. Es sei $f_1(t)^{e_1} \cdots f_g(t)^{e_g}$ eine Faktorisierung von $f(t)$ modulo $\tilde{q}\mathbb{Z}[t]$ mit normierten, nicht konstanten, in $\tilde{q}\mathbb{Z}[t]$ irreduziblen und modulo $\tilde{q} \cdot \mathbb{Z}[t]$ paarweise primen Polynomen $f_1(t), \ldots, f_g(t) \in \mathbb{Z}[t]$ sowie mit $e_1, \ldots, e_g \in \mathbb{N}$. Setzen wir dann

$$\mathfrak{p}_i := \tilde{q} \cdot \mathfrak{o}_F + f_i(\rho) \cdot \mathfrak{o}_F \qquad (1 \leq i \leq g) \tag{4-16}$$

so gilt

$$\tilde{q} \cdot \mathfrak{o}_F = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \tag{4-17}$$

denn $\tilde{q}$ ist kein Teiler von $(\mathfrak{o}_F : \mathbb{Z}[\rho])$. Wenn also $\tilde{q} = q$ gelten sollte, müßte eines der Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ in $\mathcal{P}'(a)$ liegen. Nach 4.11 und 4.17 ist letzteres aber äquivalent dazu, daß ein $i \in \{1, \ldots, g\}$ existiert mit

$$p|(\mathrm{N}(\mathfrak{p}_i) - 1) \qquad \text{und} \qquad a^{\frac{N(\mathfrak{p}_i)-1}{p}} - 1 \notin \mathfrak{p}_i. \tag{4-18}$$

Diese Überlegungen münden in den folgenden Algorithmus:

Algorithmus 4.18
Eingabe: $a \in \mathfrak{o}_F$, *welches keine* p*–te Potenz in* $\mathfrak{o}_F$ *ist.*
Ausgabe: *ein Primideal* $\mathfrak{p}$ *in* $\mathfrak{o}_F$, *für das* $t^p - a$ *irreduzibel in* $\mathfrak{o}_F/\mathfrak{p}[t]$ *ist.*

(1) $q \leftarrow p$.
(2) $q \leftarrow \min(\mathbb{P}^{>q})$.
(3) *Falls* $q|(\mathfrak{o}_F : \mathbb{Z}[\rho])$, *so gehe zu (2).*
(4) *Falls kein* $s \in \{1, \ldots, n\}$ *existiert mit* $p|(q^s - 1)$, *so gehe zu (2).*
(5) *Bestimme alle Primideale* $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ *aus* $\mathfrak{o}_F$, *welche über* q *liegen (mittels Faktorisierung von* $f(t)$ *modulo* $q\mathbb{Z}[t]$*).*
(6) $i \leftarrow 1$.
(7) *Falls* p *kein Teiler von* $\mathrm{N}(\mathfrak{p}_i) - 1$ *ist, so gehe zu (3).*
(8) *Falls* $a^{\frac{N(\mathfrak{p}_i)-1}{p}} - 1 \notin \mathfrak{p}_i$, *so gehe zu (12).*
(9) $i \leftarrow i + 1$.
(10) *(Nächstes Primideal) Falls* $i \leq g$, *so gehe zu (7).*
(11) *(Nächste Primzahl) Gehe zu (2).*
(12) *Setze* $\mathfrak{p} \leftarrow \mathfrak{p}_i$ *und terminiere.*

Mit dem nächsten Lemma schließen wir die Vorbereitung des Algorithmus ab.

Lemma 4.19
Zu $\beta \in \mathfrak{o}_F$ *und* $\mathfrak{p} \in \mathcal{P}(a)$ *beliebig existiert ein eindeutig bestimmtes* $\nu \in \{0, \ldots, p-1\}$, *so daß* $a^\nu \beta$ *eine* p*–te Potenz modulo* $\mathfrak{p}$ *ist.*

Beweis Für $H := (R/\mathfrak{p})^\times$ gilt $\#H = \mathrm{N}(\mathfrak{p}) - 1$. Da H zyklisch ist, existiert ein $\xi \in H$ mit $H = \langle \xi \rangle$. Setzen wir nun

$$U := \{x^p \mid x \in H\}, \tag{4-19}$$

so folgt $(H : U) = p$. Nach Wahl von $\mathfrak{p}$ gilt $a + \mathfrak{p} \notin U$ und somit $\mathrm{ord}((a+\mathfrak{p})+U) = p$. Also erhält man $H/U = \langle (a+\mathfrak{p}) + U \rangle$, und hieraus unmittelbar die Behauptung. □

Es seien $e_1, \ldots, e_r \in \mathrm{U}(\mathfrak{o}_F)$ nun unabhängige Einheiten. e_0 bezeichne ein erzeugendes Element von $\mathrm{TU}(\mathfrak{o}_F)$. Wir wollen prüfen, ob für ein $i \in \{0, \ldots, r\}$ Exponenten $m_i, \ldots, m_r \in \{0, \ldots, p-1\}$, $m_i + \cdots + m_r > 0$, und ein $\eta \in \mathfrak{o}_F$ existieren, für welche gilt

$$\eta^p = e_i^{m_i} \cdots e_r^{m_r}. \tag{4-20}$$

Falls e_0 eine p–te Potenz ist, und $i = 0$ gilt, ersetzen wir zunächst i durch 1. Gilt jetzt oder von Anfang an $i \geq 1$, so prüfen wir mit Algorithmus 4.9, ob e_i eine p–te Potenz ist. Ist dies der Fall, so ersetzen wir e_i solange durch seine p–ten Wurzeln, bis endlich e_i keine p–te Potenz mehr in $\mathfrak{o}_F$ ist.
Wir wählen ein beliebiges Primideal $\mathfrak{p} \in \mathcal{P}(e_i)$. Nach 4.19 existieren dann Exponenten $\nu_{i+1}, \ldots, \nu_r \in \{0, \ldots, p-1\}$, so daß für jedes $j \in \{i+1, \ldots, r\}$ das Produkt $e_i^{\nu_j} e_j$ eine p–te Potenz modulo $\mathfrak{p}$ ist. Wir setzen $\tilde{e}_j := e_i^{\nu_j} e_j$ $(i < j \leq r)$. Angenommen es existieren Exponenten $m_i, \ldots, m_r \in \{0, \ldots, p-1\}$ und $\eta \in \mathfrak{o}_F$, welche die Gleichung (4-20) lösen. Definieren wir dann $m \in \mathbb{Z}$ durch

$$m = m_i - (m_{i+1}\nu_{i+1} + \cdots + m_r\nu_r), \tag{4-21}$$

so folgt

$$\eta^p = e_i^m \cdot \tilde{e}_{i+1}^{m_{i+1}} \cdots \tilde{e}_r^{m_r}. \tag{4-22}$$

Da (4-22) auch modulo $\mathfrak{p}$ gilt, und weil $\tilde{e}_{i+1}, \ldots, \tilde{e}_r$ nach Konstruktion p–te Potenzen modulo $\mathfrak{p}$ sind, so muß auch e_i^m eine p–te Potenz modulo $\mathfrak{p}$ sein. Nach Wahl von $\mathfrak{p}$ erhalten wir $m \equiv 0 \bmod p$. Ersetzen wir nun $e_{i+1}, \ldots, e_r$ durch $\tilde{e}_{i+1}, \ldots, \tilde{e}_r$, so ist die Zahl der relevanten Einheiten in (4-20) um eins kleiner geworden.

Dadurch, daß die übriggebliebenen Einheiten rekursiv bestimmt werden, ist der nächste Algorithmus sehr technisch. Einige Details werden in der nachfolgenden Bemerkung erläutert.

Algorithmus 4.20

Eingabe: *unabhängige Einheiten* $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(\mathfrak{o}_F)$; $p \in \mathbb{P}$;
ein $S \in \mathbb{N}$ *mit* $(\mathrm{U}(\mathfrak{o}_F) : \langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle) \leq S$.

Ausgabe: *Einheiten* $e_1, \ldots, e_r \in \mathrm{U}(\mathfrak{o}_F)$, *so daß* $\langle \zeta, e_1, \ldots, e_r \rangle$ *die p–maximale Obergruppe von* $\langle \zeta, \varepsilon_1, \ldots, \varepsilon_r \rangle$ *in* $\mathrm{U}(\mathfrak{o}_F)$ *ist.*

(1) $e_i \leftarrow \varepsilon_i$ $(1 \leq i \leq r)$.

(2) $s \leftarrow S$.

(3) $e_o \leftarrow \zeta$.

(4) $C \leftarrow (c_{ij})_{0 \leq i,j \leq r} \leftarrow I_{r+1}$.

(5) *(Lemma 4.6) Falls* $\mathrm{ggT}(p, \#\mathrm{TU}(\mathfrak{o}_F)) = 1$, *so setze* $k \leftarrow 1$, *sonst setze* $k \leftarrow 0$.

(6) $i \leftarrow k$.

(7) *Falls* $i > 0$, *so gehe zu (9).*

(8) *Setze* $\tilde{e}_0 \leftarrow e_0$ *und gehe zu (21).*

(9) $\tilde{e}_i \leftarrow e_i$.

(10) $j \leftarrow k$.

(11) *Bestimme* $\nu \in \{0, \ldots, p-1\}$, *so daß* $\tilde{e}_j^{\nu} \tilde{e}_i$ *eine* p*–te Potenz modulo* $\mathfrak{p}_j$ *ist (vergleiche 4.17 und 4.19).*

(12) *(Addiere in* C *das* ν*–fache der Spalte* j *zur Spalte* i*)* $c_{\ell i} \leftarrow c_{\ell i} + c_{\nu j}$ $(k \leq \ell \leq j)$.

(13) $\tilde{e}_i \leftarrow e_k^{c_{ki}} \cdots e_{i-1}^{c_{i-1,i}} e_i$.

(14) $j \leftarrow j + 1$.

(15) *Falls* $j < i$, *so gehe zu (11).*

(16) *(Einträge in Spalte* i *modulo* p *reduzieren)* $c_{\ell i} \leftarrow c_{\ell i} \pmod{p}$ $(k \leq \ell < i)$.

(17) *Falls kein* $\eta \in \mathfrak{o}_F$ *existiert mit* $\eta^p \equiv \tilde{e}_i \bmod \mathrm{TU}(\mathfrak{o}_F)$ *(Algorithmus 4.9), so gehe zu (21).*

(18) $e_i \leftarrow \eta$.

(19) $s \leftarrow \lfloor \frac{s}{p} \rfloor$.

(20) *Gehe zu (9).*

(21) *Berechne mittels Algorithmus 4.18 ein Primideal* $\mathfrak{p}_i \in \mathcal{P}(e_i)$.

(22) $i \leftarrow i + 1$.

(23) *Falls* $i \leq r$, *so gehe zu (9).*

(24) *Terminiere.*

Bemerkung 4.21

(a) *Der rekursiv berechnete Wert von* $\tilde{e}_i$ *ist ein Potenzprodukt der Form*

$$e_k^{\mu_k} \cdots e_{i-1}^{\mu_{i-1}} \cdot e_i^{\mu_i} \tag{4-23}$$

mit $\mu_k, \ldots, \mu_{i-1} \in \mathbb{Z}^{\geq 0}, \mu_i = 1$ *und* k *wie in Schritt (5). Die Exponenten* $\mu_k, \ldots, \mu_i$ *werden — modulo* p *reduziert — in der Matrix* C *verwaltet. Wegen* $\mu_i = 1$ *kann man* e_i *in Schritt (18) direkt durch* η *ersetzen.*

(b) *Aus der Berechnung der unteren Regulatorschranke kennen wir schon Grundeinheiten* $e_1, \ldots, e_\ell$ $(\ell \in \{0, \ldots, r\})$. *In Schritt (17) kann dann* $\tilde{e}_i$ *modulo* $\mathrm{TU}(\mathfrak{o}_F)$ *keine* p*–te Potenz sein, solange* $1 \leq i \leq \ell$ *gilt. Also muß für kein* $i \in \{1, \ldots, \ell\}$ *der Algorithmus 4.9 aufgerufen werden. Voraussetzng dafür ist allerdings, daß die Grundeinheiten* $e_1, \ldots, e_\ell$ *nicht bei einer MLLL–Reduktion im zweiten Schritt des Verfahrens verloren gegangen sind. Letzteres ist sehr unwahrscheinlich und kann anhand der Transformationsmatrizen überprüft werden.*

(c) *Der Algorithmus kann nicht auf die Ordnung* R *angewandt werden, wenn* $R \subsetneqq \mathfrak{o}_F$ *gilt: Ist* $a \in R$ *keine* p*–te Potenz in* R, *so folgt daraus nämlich nicht die Irreduzibilität von* $t^p - a$ *über* $\mathfrak{o}_F$ *(!). Ist aber* $t^p - a$ *in* $\mathfrak{o}_F$ *reduzibel, so auch in* $\mathfrak{o}_F/\mathfrak{p}[t]$ *für jedes Primideal* $\mathfrak{p}$ *aus* $\mathfrak{o}_F$. *Da für jedes Primideal aus* $\mathfrak{o}_F$, *welches nicht den Index* $(\mathfrak{o}_F : R)$ *enthält, die Ringe* $\mathfrak{o}_F/\mathfrak{p}$ *und* $R/(R \cap \mathfrak{p})$

isomorph sind (siehe [11, Chapter 6, Lemma 2.26]), ist nicht garantiert, daß ein Primideal $\mathfrak{p}$ in R existiert, für welches $t^p - a$ irreduzibel in $R/\mathfrak{p}[t]$ ist.

4.2 Grundeinheitenberechnung in beliebigen Ordnungen

In diesem Abschnitt seien bereits Grundeinheiten $E_1, \ldots, E_r$ von $\mathrm{U}(\mathfrak{o}_F)$ gefunden. Ferner sei ζ_F ein erzeugendes Element von $\mathrm{TU}(\mathfrak{o}_F)$. Wir werden ein gruppentheoretisches Verfahren angeben, mit dem wir Einheiten $\varepsilon_0 \in \mathrm{TU}(R)$, $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{U}(R)$ bestimmen können, so daß gilt

$$\langle \varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r \rangle = \langle \zeta_F, E_1, \ldots, E_r \rangle \cap R. \tag{4-24}$$

Offenbar bilden dann die Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ ein Grundeinheitensystem von R; ε_0 ist ein erzeugendes Element von $\mathrm{TU}(R)$. Das Verfahren ist eine Übertragung der Methoden, mit denen bei der Klassengruppenberechnung die Klassengruppenmatrix ausgewertet wird (siehe [11, Chapter 6]).

Wir setzen $e_i := E_i$ $(1 \le i \le r)$ und $e_0 := \zeta_F$. Da der Index $(\mathrm{U}(\mathfrak{o}_F) : \mathrm{U}(R))$ endlich ist, können wir durch Ausprobieren minimale Exponenten $\nu_0, \ldots, \nu_r \in \mathbb{N}$ ermitteln mit $e_i^{\nu_i} \in R$ $(0 \le i \le r)$. Wir legen $C = (c_{ij})_{0 \le i,j \le r} \in \mathbb{Z}^{r+1 \times r+1}$ fest durch $c_{ij} = \delta_{ij} \cdot \nu_i$ $(0 \le i, j \le r)$.

$c_{0,0}$ ist dann die Ordnung von ζ_F modulo $\mathrm{U}(R)$, und es gilt $\langle e_0^{c_{0,0}} \rangle = \langle e_0 \rangle \cap \mathrm{U}(R)$.

Die Matrix C und $e_0, \ldots, e_r$ werden nun in einem induktiven Verfahren abgeändert. Wir gehen davon aus, daß nach $(s+1)$ Schritten $(0 \le s \le r)$ die Matrix C und $e_0, \ldots, e_r$ wie folgt modifiziert sind:

(1) $e_i = E_i \quad (s < i \le r)$.

(2) Es existiert eine Matrix $T = (t_{ij})_{0 \le i,j \le s} \in \mathrm{GL}(s+1, \mathbb{Z})$ mit

$$e_i = \zeta_F^{t_{0,i}} \cdot E_1^{t_{1,i}} \cdots E_r^{t_{r,i}} \qquad (0 \le i \le s). \tag{4-25}$$

(3) $\langle e_0 \cdot \mathrm{U}(R), \ldots, e_s \cdot \mathrm{U}(R) \rangle = \prod_{j=0}^{s} \langle e_j \cdot \mathrm{U}(R) \rangle$.

(4) C ist eine obere Hermite–Spalten–reduzierte Dreiecksmatrix mit $c_{ij} = 0$ $(1 \le i < j \le s)$.

(5) $\langle e_0^{c_{0,0}}, \ldots, e_s^{c_{s,s}} \rangle = \mathrm{U}(R) \cap \langle \zeta, E_1, \ldots, E_s \rangle$.

(6) $\mathrm{ord}(e_j \cdot \mathrm{U}(R)) = c_{jj}$ $(0 \le j \le s)$.

(7) $e_0^{c_{0,i}} \cdots e_s^{c_{ii}} \in R$ $(0 \le i \le s)$.

Die Berechnung von $c_{0,0} = \nu_0$ entsprach somit dem Schritt $s = 0$.

Sei nun $s \geq 1$. Gesucht ist die Ordnung von e_s modulo $\langle e_0 \cdot \mathrm{U}(R), \ldots, e_{s-1} \cdot \mathrm{U}(R) \rangle$. Ist $m_s \in \mathbb{N}$ hierfür ein Kandidat, so müssen

$$m_0, \ldots, m_{s-1} \in \mathbb{Z}^{\geq 0} \qquad (0 \leq m_i < c_{ii} \ (0 \leq i \leq s-1)),$$

existieren mit

$$e_0^{m_0} \cdots e_s^{m_s} \in R. \tag{4-26}$$

Ferner existiert $m \in \mathbb{N}$ mit $m_s m = c_{ss}$. Aus

$$e_0^{c_{0,s}} \cdots e_s^{c_{ss}} \in R \tag{4-27}$$

folgt dann

$$m_i m \equiv c_{is} \bmod c_{ii} \qquad (0 \leq i < s) \tag{4-28}$$

aus Bedingung (3). Zur Bestimmung der Ordnung von e_s modulo $\langle e_0 \cdot \mathrm{U}(R), \ldots, e_s \cdot \mathrm{U}(R) \rangle$ müssen wir also die Gültigkeit von (4-26) für endlich viele $\underline{m} \in \mathbb{Z}^{s+1}$ prüfen, wobei durch die Kongruenzbedingung (4-28) die Zahl der Tests eingeschränkt werden kann. Ist nun

$$c_{ss} = p_1^{\mu_1} \cdots p_k^{\mu_k} \tag{4-29}$$

die Primzahlfaktorisierung von c_{ss} mit paarweise verschiedenen $p_1, \ldots, p_k \in \mathbb{P}$ und $\mu_1, \ldots, \mu_k \in \mathbb{N}$, so ersetzen wir zunächst den Exponenten μ_1 solange jeweils durch $\mu_1 - 1$, so daß zwar noch Exponenten $m_{0,1}, \ldots, m_{s-1,1} \in \mathbb{Z}$ existieren mit

$$e_0^{m_{0,1}} \cdots e_{s-1}^{m_{s-1,1}} e_s^{p_1^{\mu_1} \cdot p_2^{\mu_2} \cdots p_k^{\mu_k}} \in R, \tag{4-30}$$

aber eben keine Exponenten $\tilde{m}_0, \ldots, \tilde{m}_{s-1} \in \mathbb{Z}$ mehr existieren mit

$$e_0^{\tilde{m}_0} \cdots e_{s-1}^{\tilde{m}_{s-1}} e_s^{p_1^{\mu_1 - 1} \cdot p_2^{\mu_2} \cdots p_k^{\mu_k}} \notin R. \tag{4-31}$$

Analog verfährt man mit $\mu_2, \ldots, \mu_k$. Auf diese Weise erhalten wir schließlich Exponenten $m_{0,k}, \ldots, m_{s-1,k} \in \mathbb{Z}$ mit

$$e_0^{m_{0,k}} \cdots e_{s-1}^{m_{s-1,k}} e_s^{p^{\mu_1} \cdot p_2^{\mu_2} \cdots p_k^{\mu_k}} \in R, \tag{4-32}$$

wobei $p_1^{\mu_1} \cdots p_k^{\mu_k}$ die gesuchte Ordnung von e_s modulo $\langle e_0 \cdot \mathrm{U}(R), \ldots, e_{s-1} \cdot \mathrm{U}(R) \rangle$ ist. Setzen wir $c_{ss} \leftarrow p_1^{\mu_1} \cdots p_k^{\mu_k}$ und $c_{is} \leftarrow m_{i,k}$ $(0 \leq i < s)$, so erfüllt C die Bedingung (7).

Damit die übrigen Bedingungen auch für den nächsten Induktionsschritt gelten, berechnen wir zuerst die Smith–Normalform $C'' = (c''_{ij})$ von $C' := (c_{ij})_{0 \leq i,j \leq s}$ (also $C'' = U \cdot C' \cdot V$ für $U, V \in \mathrm{GL}(s+1, \mathbb{Z})$) und setzen damit

$$c_{ij} \leftarrow c''_{ij} \qquad (0 \leq i, j \leq s). \tag{4-33}$$

Für $U^{-1} = (\tilde{u}_{ij})$ passen wir durch

$$e_i \leftarrow e_0^{\tilde{u}_{0,i}} \cdots e_s^{\tilde{u}_{si}} \qquad (0 \leq i \leq s) \tag{4-34}$$

die Einheiten $e_0, \ldots, e_s$ an den veränderten oberen linken Teil der Matrix C an. Mittels

$$(c_{1j}, \ldots, c_{sj})^t \leftarrow U \cdot (c_{1j}, \ldots, c_{sj})^t \qquad (s < j \leq r) \tag{4-35}$$

muß dann der obere rechte Teil von C an die in (4-34) veränderten Einheiten $e_0, \ldots, e_i$ angepaßt werden. Schließlich definieren wir $\tilde{T} = (\tilde{t}_{ij})_{0 \leq i,j \leq s} \in \mathrm{GL}(s+1, \mathbb{Z})$ durch

$$\tilde{t}_{ij} := t_{ij} \quad (0 \leq i, j < s), \qquad \tilde{t}_{si} := \tilde{t}_{is} := 0 \quad (0 \leq i < s), \qquad \tilde{t}_{ss} := 1, \tag{4-36}$$

und ersetzen damit T durch $\tilde{T} \cdot U^{-1}$. Berechnen wir danach noch die Hermite–Spalten–Normalform von C als obere Dreiecksmatrix, so sind die Bedingungen für den nächsten Induktionsschritt alle erfüllt.

Nachdem wir das obige Verfahren $(r+1)$–mal durchgeführt haben, müssen wir die Matrix C noch an die ursprünglichen Einheiten $\zeta_F, E_1, \ldots, E_r$ anpassen. Dazu setzen wir $C \leftarrow T \cdot C$ und ersetzen darauf C wiederum durch seine Hermite–Spalten–Normalform (obere Dreiecksmatrix). Dann leisten $\varepsilon_0, \ldots, \varepsilon_r \in R$,

$$\varepsilon_i := \zeta_F^{c_{0,i}} \cdot E_1^{c_{1,i}} \cdots E_r^{c_{r,i}} \qquad (0 \leq i \leq r), \tag{4-37}$$

das gewünschte.

Algorithmus 4.22

Eingabe: *Grundeinheiten $E_1, \ldots, E_r$ von $\mathrm{U}(\mathfrak{o}_F)$;*
ein erzeugendes Element ζ_F von $\mathrm{TU}(\mathfrak{o}_F)$.

Ausgabe: *Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_r$ von $\mathrm{U}(R)$;*
ein erzeugendes Element ε_0 von $\mathrm{TU}(R)$.

(1) $e_0 \leftarrow \zeta_F$.

(2) $e_i \leftarrow E_i$ $(1 \leq i \leq r)$.

(3) $C = (c_{ij})_{0 \leq i,j \leq r} \leftarrow I_{r+1}$.

(4) $T \leftarrow I_1$.

(5) $i \leftarrow 0$.

(6) *Bestimme $\nu \in \mathbb{N}$ minimal mit $e_i^\nu \in R$.*

(7) $c_{ii} \leftarrow \nu$.

(8) $i \leftarrow i + 1$.

(9) *Falls $i \leq r$, so gehe zu (6).*

(10) $s \leftarrow 0$.

(11) *Bestimme die Primzahlfaktorisierung*

$$c_{ss} = p_1^{\mu_1} \cdots p_k^{\mu_k}$$

mit $p_1, \ldots, p_k \in \mathbb{P}$ paarweise verschieden und $\mu_1, \ldots, \mu_k \in \mathbb{N}$.

(12) $j \leftarrow 1$.

(13) *Falls $\mu_j = 0$, so gehe zu (29).*

(14) $\mu_j \leftarrow \mu_j - 1$.

(15) $m \leftarrow p_j$.

(16) $m_s \leftarrow \frac{c_{ss}}{m}$.

(17) $m_0 \leftarrow 0$ $(0 \le i < s)$.

(18) *(Kongruenzbedingung (4-28) testen) Falls ein* $i \in \{0, \dots, s-1\}$ *existiert mit* $m_i m \not\equiv c_{ij} \bmod c_{ii}$, *so gehe zu (22).*

(19) *Falls* $e_0^{m_0} \cdots e_s^{m_s} \notin R$, *so gehe zu (22).*

(20) $c_{is} \leftarrow m_i$ $(0 \le i \le s)$.

(21) *(Dieselbe Primzahl noch einmal) Gehe zu (13).*

(22) *(Neue Exponenten* $m_0, \dots, m_{s-1}$ *bestimmen)* $m_0 \leftarrow m_0 + 1 \pmod{c_{0,0}}$.

(23) $i \leftarrow 0$.

(24) *Falls* $(i = s$ *oder* $m_i \neq 0)$, *so gehe zu (27).*

(25) $m_i \leftarrow m_i + 1 \pmod{c_{ii}}$.

(26) *Gehe zu (24).*

(27) *(Alle Exponenten getestet ?) Falls* $m_0 + \cdots + m_{s-1} = 0$, *so gehe zu (29).*

(28) *Gehe zu (18).*

(29) $j \leftarrow j + 1$.

(30) *(Nächste Primzahl) Falls* $j \le k$, *so gehe zu (13).*

(31) *Falls* $s = r$, *so gehe zu (44).*

(32) *(Transformationen)* $C' \leftarrow (c_{ij})_{0 \le i,j \le s}$.

(33) *Bestimme* $U, V \in \mathrm{GL}(s+1, \mathbb{Z})$, *so daß* $C'' = (c''_{ij})_{0 \le i,j \le s}$ *die Smith–Normalform von* C' *ist.*

(34) $c_{ij} \leftarrow c''_{ij}$ $(0 \le i, j \le s)$.

(35) $\tilde{U} = (\tilde{u}_{ij}) \leftarrow U^{-1}$.

(36) $\tilde{e}_i \leftarrow e_0^{\tilde{u}_{0,i}} \cdots e_s^{\tilde{u}_{s,i}}$ $(0 \le i \le s)$.

(37) $e_i \leftarrow \tilde{e}_i$ $(0 \le i \le s)$.

(38) $(c_{0j}, \dots, c_{sj})^t \leftarrow U \cdot (c_{0j}, \dots, c_{sj})^t$ $(s < j \le r)$.

(39) $\tilde{T} \leftarrow (\tilde{t}_{ij})_{0 \le i,j \le s}$ *mit* $\tilde{t}_{ij}$ *wie in(4-36).*

(40) $T \leftarrow \tilde{T} \cdot U^{-1}$.

(41) *Berechne die Hermite–Spalten–Normalform von* C *als obere Dreiecksmatrix.*

(42) $s \leftarrow s + 1$.

(43) *Gehe zu (11).*

(44) $C \leftarrow T \cdot C$.

(45) *Berechne die Hermite–Spalten–Normalform von* C *als obere Dreiecksmatrix.*

(46) $\varepsilon_i \leftarrow \zeta_F^{c_{0,i}} \cdot E_1^{c_{1,i}} \cdots E_r^{c_{1,r}}$ $(0 \le i \le r)$.

(47) *Terminiere.*

Beispiel 4.23

Für $f(t) = t^4 - 108t^2 - 2304$ *ist* $F = \mathbb{Q}[\sqrt{3}, \sqrt{51}]$ *total reell (also* $r_1 = 4, r_2 = 0, r = 3$*) mit Diskriminante* 41 616. *Die Elemente*

$$v_1 = 1, \quad v_2 = \frac{1}{2}\rho, \quad v_3 = \frac{1}{12}\rho^2, \quad v_4 = \frac{1}{96}(36\rho + \rho^3)$$

bilden eine $\mathbb{Z}$*–Basis von* $\mathfrak{o}_F$. *Grundeinheiten von* $\mathrm{U}(\mathfrak{o}_F)$ *sind gegeben durch*

$$\begin{aligned} E_1 &= 2 + 2v_2 - v_4, \\ E_2 &= 5 - 2v_3, \\ E_3 &= 17 - 9v_2 - 3v_3 + 4v_4. \end{aligned}$$

Es gilt $\mathrm{Reg}(\mathfrak{o}_F) = 25.41$. *Wir wollen Grundeinheiten von* $\mathbb{Z}[\rho]$ *bestimmen* $((\mathfrak{o}_F : \mathbb{Z}[\rho]) = 2304)$. *Wir bestimmen zunächst* $\nu_0, \dots, \nu_4$ *wie in Schritt (5) von 4.22.*

Wegen $\mathrm{TU}(\mathfrak{o}_F) = \langle -1 \rangle = \mathrm{TU}(\mathbb{Z}[\rho])$ *gilt* $\nu_0 = 1$. *Durch Ausprobieren erhält man* $\nu_1 = 48, \nu_2 = 4$ *und* $\nu_3 = 12$. *Damit gilt*

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 48 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 12 \end{pmatrix}. \tag{4-38}$$

Für $s = 0, 1$ *ist nach Wahl von* ν_0, ν_1 *nichts zu prüfen. Aufgrund der Kongruenzbedingung und der Wahl von* ν_2 *ist für* $s = 2$ *nur der Vektor* $(m_0, m_1, m_2) = (0, 24, 2)$ *zu untersuchen. Wegen* $E_1^{24} E_2^2 \notin \mathbb{Z}[\rho]$ *erhalten wir nach den Transformationen*

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 48 & 0 \\ 0 & 0 & 0 & 12 \end{pmatrix}, \tag{4-39}$$

wobei nun gilt $e_1 = E_2, e_2 = E_1$. *Für* $s = 3$ *schließlich müssen die fünf Vektoren* $(0, 2, 0, 6)$,$(0, 24, 0, 6)$,$(0, 2, 24, 6)$,$(0, 0, 0, 4)$ *und* $(0, 0, 16, 4)$ *getestet werden. Die ersten vier Tests verlaufen negativ. Danach erhält man*

$$e_2^{16} \cdot e_3^4 = E_1^{16} \cdot E_3^4 \ \in \mathbb{Z}[\rho].$$

Da mit dem letzen Test das Verfahren abgeschlossen ist, bilden die Einheiten

$$\varepsilon_1 = E_1^{48}, \quad \varepsilon_2 = E_2^4, \quad \varepsilon_3 = E_1^{16} \cdot E_3^4$$

ein Grundeinheitensystem von $\mathbb{Z}[\rho]$. *Es gilt* $\mathrm{Reg}(\mathbb{Z}[\rho]) = 48 \cdot 4 \cdot 4 \cdot \mathrm{Reg}(\mathfrak{o}_F) = 19514.88$.

Kapitel 5

Beispieltabellen

Die Tabellen umfassen folgende Angaben:

r	Einheitenrang
m	Anzahl der unabhängigen Einheiten aus dem ersten Schritt
t_1	Rechenzeit für den ersten Schritt
t_2	Rechenzeit für den zweiten Schritt
S	Indexschranke zu Beginn des dritten Schrittes
i	Index der unabhängigen Einheiten aus dem zweiten Schritt
t_3	Rechenzeit für den dritten Schritt
t	Gesamtrechenzeit

Berechnet wurden jeweils Grundeinheitensysteme der Maximalordung. Im zweiten Schritt wurde die vierte Strategie verwendet ($(k_1, k_2) = (5, 5)$).

$f(t)$	r	m	t_1	t_2	S	i	$\mathrm{Reg}(\mathfrak{o}_F)$	t_3	t
t^5+2	2	2	2s	0s	1	1	4.83	0s	2s
t^6+2	2	2	1s	2s	4	3	10.46	5s	8s
t^7+2	3	2	1s	3s	2	2	26.78	4s	10s
t^8+2	3	1	2s	5s	6	4	75.01	6s	13s
t^9+2	4	4	6s	0s	2	1	165.95	14s	20s
$t^{10}+2$	4	2	2s	136s	2	1	427.84	12s	150s
$t^{11}+2$	5	4	17s	91s	5	2	1650.52	26s	134s
$t^{12}+2$	5	3	27s	64s	8	2	4264.87	97s	188s
$t^{13}+2$	6	4	50s	378s	5	1	19704.66	216s	644s
$t^{14}+2$	6	3	82s	556s	8	1	52742.75	1377s	2015s
$t^{15}+2$	7	5	143s	754s	12	1	140588.61	1607s	2504s
$t^{16}+2$	7	1	179s	2552s	92	7	770827.55	2363s	5094s

$f(t)$	r	m	t_1	t_2	S	i	$\mathrm{Reg}(\mathfrak{o}_F)$	t_3	t
t^5+3	2	1	0s	1s	1	1	12.25	0s	1s
t^6+3	2	0	1s	2s	1	1	12.75	0s	3s
t^7+3	3	1	3s	4s	2	1	116.79	5s	12s
t^8+3	3	2	8s	5s	3	3	24.08	16s	29s
t^9+3	4	3	25s	34s	8	3	1056.78	106s	165s
$t^{10}+3$	4	3	25s	14s	12	8	160.06	28s	67s
$t^{11}+3$	5	5	24s	0s	2	1	1213.75	32s	66s
$t^{13}+3$	6	1	588s	1416s	18	2	201787.36	499s	2503s
$t^{14}+3$	6	2	677s	267s	9	3	9520.75	220s	1164s

$f(t)$	r	m	t_1	t_2	S	i	$\mathrm{Reg}(\mathfrak{o}_F)$	t_3	t
t^5+5	2	1	1s	1s	2	1	36.89	2s	4s
t^6+5	2	0	3s	9s	5	2	69.70	3s	15s
t^7+5	3	0	13s	64s	4	1	591.07	7s	84s
t^8+5	3	1	34s	37s	8	2	753.79	9s	80s
t^9+5	4	0	199s	153s	16	2	9123.39	71s	423s
$t^{10}+5$	4	3	374s	78s	51	10	9762.57	87s	539s
$t^{11}+5$	5	0	1911s	1230s	14	1	158012.33	572s	3713s
$t^{12}+5$	5	3	4463s	650s	23	3	128061.88	203s	5316s

$f(t)$	r	m	t_1	t_2	S	i	$\mathrm{Reg}(\mathfrak{o}_F)$	t_3	t
t^5+7	2	0	0s	2s	1	1	15.35	0s	2s
t^6+7	2	2	9s	0s	1	1	18.08	0s	9s
t^7+7	3	0	39s	211s	114	12	1753.78	25s	245s
t^8+7	3	2	25s	9s	9	5	50.74	19s	53s
t^9+7	4	1	763s	283s	7	1	10421.07	53s	1099s
$t^{10}+7$	4	4	34s	0s	1	1	178.85	0s	34s

Literaturverzeichnis

[1] J. Dieudonné, *Geschichte der Mathematik 1700–1900*, Vieweg, 1985.

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

[3] G. J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.

[4] D.E. Knuth, *The Art of Computer Programming, Volume 2 : Seminumerical Algorithms*, Addison–Wesley, 1981.

[5] S. Lang, *Algebra*, Addision–Wesley, 1984.

[6] A.K.Lenstra, H.W. Lenstra Jr., L.Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[7] D. A. Marcus, *Number Fields*, Springer, 1977.

[8] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.

[9] J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1992.

[10] M. Pohst, *Computational Algebraic Number Theory*, Birkhäuser, 1993.

[11] M. Pohst und H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989.

[12] J. Graf von Schmettow, *Über die Berechnung von Klassengruppen algebraischer Zahlkörper*, Diplomarbeit, Düsseldorf 1987.

[13] J. Graf von Schmettow, *Beiträge zur Klassengruppenberechnung*, Dissertation, Düsseldorf 1991.

[14] A. Schwarz, *Berechung von Zahlkörpern fünften Grades mit kleiner Diskriminante*, Diplomarbeit, Düsseldorf 1991.

Bezeichnungen

$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{P}$	Menge der Primzahlen
$\mathbb{Q}$	Menge der rationalen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{C}$	Menge der komplexen Zahlen
p	Primzahl
$\underline{x}$	Vektor mit Komponenten x_i
I_k	Einheitsmatrix der Dimension k
$\mathrm{GL}(k,\mathbb{Z})$	Gruppe der unimodularen $k \times k$–Matrizen über $\mathbb{Z}$
$\mathrm{GL}(k,\mathbb{R})$	Gruppe der invertierbaren $k \times k$–Matrizen über $\mathbb{R}$
$\mathrm{ord}(x)$	Ordnung eines Gruppenelementes x
log	natürlicher Logarithmus
F	algebraischer Zahlkörper
n	Körpergrad von F
f	ein erzeugendes Polynom von F
ρ	eine Nullstelle von f
r	Einheitenrang von F
r_1	Anzahl der reellen Nullstellen von f
r_2	halbe Anzahl der komplexen Nullstellen von f
$\mathfrak{o}_F$	Maximalordnung von F
R	eine Ordnung von F
$\omega_1, \ldots, \omega_n$	$\mathbb{Z}$–Basis von R
$\mathrm{disc}(R)$	Diskriminante von R
$\mathrm{U}(R)$	Einheitengruppe von R
$\mathrm{Reg}(R)$	Regulator von R
$\mathrm{TU}(R)$	Torsionseinheitengruppe von R
ζ	ein erzeugendes Element von $\mathrm{TU}(R)$
$\mathfrak{p}$	ein Primideal
$\alpha^{(j)}$	j–te Konjugierte einer algebraischen Zahl
γ_r^r	r–te Hermitesche Konstante

Hiermit erkläre ich, daß ich die vorliegende Arbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Düsseldorf, den 28. Oktober 1993