

Zur Berechnung  
unabhängiger Einheiten  
in Zahlkörpern

---

Diplomarbeit von Friederike Terbeck

Oktober 2009

**Betreut von**

---

Prof. Dr. Dr. h. c. Michael E. Pohst  
Technische Universität Berlin  
Institut für Mathematik



**Eidesstattliche Versicherung**

Ich versichere, dass ich diese Diplomarbeit selbstständig und eigenhändig verfasst und nur die angegebenen Quellen und Hilfsmittel verwendet habe.

---

Berlin, den 12. Oktober 2009



# Inhaltsverzeichnis

<b>Vorwort</b>	<b>1</b>
<b>1 Einheiten in Ordnungen</b>	<b>5</b>
1.1 Zahlentheoretische Grundlagen . . . . .	5
1.2 Berechnung von Grundeinheiten in drei Schritten . . . . .	23
<b>2 Unabhängige Einheiten nach Dirichlet</b>	<b>27</b>
2.1 Konstruktion von Konjugiertenfolgen . . . . .	27
2.2 Berechnung als Quotienten assoziierter Dirichlet-Elemente . . . . .	38
2.3 Andere Konstruktionsmöglichkeiten . . . . .	40
2.4 Variation der Konjugiertenrichtung als Unabhängigkeitsgaranten . . . . .	46
<b>3 Unabhängige Einheiten mit Bewertungsmatrizen</b>	<b>51</b>
3.1 Werkzeuge aus der Klassengruppenberechnung . . . . .	51
3.2 Konstruktion von Einheiten zu Konjugiertenrichtungen . . . . .	54
3.3 Unabhängige Einheiten mit Bewertungsmatrizen . . . . .	63
3.4 Zur Wahl der Faktorbasis . . . . .	65
<b>4 Schlussbetrachtungen</b>	<b>81</b>
4.1 Vergleich der vorgestellten Verfahren . . . . .	81
4.2 Zusammenfassung . . . . .	93
<b>5 Anhang</b>	<b>97</b>
5.1 Beispiele zum Vergleich . . . . .	100
5.2 Beispiele zur Schrankenwahl . . . . .	113
<b>Literaturverzeichnis</b>	<b>129</b>



# Vorwort

Die Kenntnis der Einheitengruppe von Ordnungen algebraischer Zahlkörper ist für das Lösen diophantischer Gleichungen von fundamentaler Bedeutung. Dementsprechend spielt die Entwicklung effizienter Algorithmen zur Berechnung der Einheitengruppe bei der Bestimmung der konstruktiven Lösungen von diophantischen Gleichungen, welche durch die steigende Leistungsfähigkeit der Computertechnologie während der letzten Jahrzehnte von wachsendem praktischen Interesse ist, eine entscheidende Rolle.

Die Struktur der Einheitengruppe von Ordnungen algebraischer Zahlkörper als endlich erzeugte Gruppe ist durch den Dirichletschen Einheitensatz bekannt. Zur Berechnung der Erzeuger des torsionsfreien Anteils, der sogenannten Grundeinheiten, wurden verschiedene Verfahren entwickelt. In reell-quadratischen Körpererweiterungen kann die Grundeinheit als Proportionalitätsfaktor der Periode der Kettenbruchentwicklung einer irrationalen Zahl nach Lagrange berechnet werden. Voronoi verallgemeinerte dieses Vorgehen 1896 mit Hilfe zahlengeometrischer Interpretationen für kubische Erweiterungen. Eine weitere zahlengeometrische Verallgemeinerung ergab das Verfahren zur Berechnung von unabhängigen Einheiten nach Dirichlet für Ordnungen beliebiger algebraischer Zahlkörper, das 1989 in [BP89] vorgestellt wurde. In [Poh93] wird diese Methode in einer erweiterten Version in den Gesamtzusammenhang der Grundeinheitenberechnung eingeordnet. Die darauf basierenden Ausführungen in [Wil93] bilden den Ausgangspunkt für die vorliegende Arbeit. Bei der Berechnung unabhängiger Einheiten nach Dirichlet werden Elemente der Ordnung eines Zahlkörpers mit beschränkter Norm und bestimmten Konjugiertenbetragseigenschaften (*Dirichlet-Elemente*) konstruiert, so dass nach endlich vielen Konstruktionen zwei zueinander assoziierte Elemente auftreten, deren Quotient dann eine Einheit bildet. Die Konjugiertenbetragseigenschaften der Dirichlet-Elemente gewährleisten die Unabhängigkeit der berechneten Einheiten.

Die Berechnung der Einheitengruppe einer Maximalordnung kann innerhalb der Klassengruppenberechnung mit Relationenmethode (siehe [Hes96] und [Poh93]) nach dem folgenden Prinzip geschehen: Elemente des Zahlkörpers  $F$ , deren Hauptideale Potenzprodukte von Primidealen aus einer Menge  $S$  sind, bilden die multiplikative Gruppe der *S-Einheiten*. Durch die Abbildung der Erzeuger der *S-Einheitengruppe* auf Vektoren, deren Komponenten aus Bewertungen über  $S$  und

Logarithmen bestimmter Konjugiertenbeträge der Elemente bestehen, erhält man die Basis eines vollständigen Gitters (*S-Einheitengitter*), dessen Diskriminante dem Produkt des Regulators  $R_F$  und der Klassenzahl  $h_F$  entspricht. Zur Berechnung der Klassengruppe werden die Bewertungsvektoren von *S*-Einheiten in eine Matrix eingefügt, die in Hermite Normalform transformiert wird (*Klassengruppenmatrix*). Tritt eine Nullspalte in der Klassengruppenmatrix auf, ist die entsprechende exponentielle Kombination der *S*-Einheiten eine Einheit. Diese Kombinationen werden in der sogenannten Einheitenmatrix  $U_\alpha$  verwaltet. Den Spalten des Produkts aus Einheitenmatrix und einer Matrix, bestehend aus den Konjugiertenlogarithmenvektoren der *S*-Einheiten  $L_\alpha$ , können Einheiten der Maximalordnung zugeordnet werden. Die Transformation bei der MLLL-Reduktion dieser Spaltenvektoren entspricht der Bestimmung eines minimalen Erzeugendensystems der konstruierten Einheiten und wird auf die Einheitenmatrix angewandt. Die Generierung von *S*-Einheiten und die beschriebenen Berechnungen werden solange durchgeführt, bis der Vergleich des Produkts der Determinanten von  $U_\alpha L_\alpha$  und der Klassengruppenmatrix mit einer analytischen Approximation von  $R_F h_F$  zeigt, dass eine Basis des *S*-Einheitengitters und damit implizit auch ein Grundeinheitensystem gefunden wurde.

Die Grundidee dieser Arbeit besteht darin, den Ansatz zur Berechnung von Einheiten aus dem Klassengruppenverfahren mit der Methode von Dirichlet zu kombinieren. Die Konstruktion der Dirichlet-Elemente als Elemente der Maximalordnung mit beschränkter Norm legt ihre Verwendung als *S*-Einheiten nahe. Durch ganzzahlige lineare Kombination der Bewertungsvektoren von *S*-Einheiten unter den Dirichlet-Elementen können dann Einheiten konstruiert werden. Die Konjugiertenbetragseigenschaften der Dirichlet-Elemente begünstigen zudem die Unabhängigkeit der berechneten Einheiten. Gegenüber der bisherigen Konstruktion unabhängiger Einheiten nach Dirichlet mit Hilfe von Normbetragsvergleichen ergibt sich der Vorteil, dass nicht nur Quotienten zweier Dirichlet-Elemente, sondern auch andere multiplikative Kombinationen in Betracht gezogen werden, so dass die Konstruktion unabhängiger Einheiten beschleunigt werden kann.

## Überblick

In Kapitel 1 dieser Arbeit werden zunächst die zahlentheoretischen und algorithmischen Grundlagen für die folgenden Kapitel gelegt. Anschließend wird das Vorgehen zur Bestimmung des Grundeinheitensystems einer Ordnung dargestellt, in dessen Zusammenhang sich die Berechnung unabhängiger Einheiten, wie wir sie in den späteren Kapiteln betrachten werden, einfügt. Neben der bisherigen Konstruktion eines Dirichlet-Elements als Produkt erster Basiselemente der LLL-reduzierten Basen von Moduln wird in Kapitel 2 eine neue Konstruktionsmethode mit kürzesten Elementen von Moduln vorgestellt. Mit der neuen Konstruktionsmethode gelingt es, die Normbetragschranke, die wir für die Dirichlet-

Elemente zugrundelegen können, zu verringern, so dass durchschnittlich früher Einheiten gefunden werden. In Kapitel 3 erarbeiten wir den oben skizzierten Ansatz, unabhängige Einheiten beliebiger Ordnungen durch Linearkombination von Bewertungsvektoren zu konstruieren. In diesem Zusammenhang wird die Wahl einer günstigen Faktorbasis bei der Berechnung von unabhängigen Einheiten der Maximalordnung untersucht. Zum Abschluss wird in Kapitel 4 das bisherige Vorgehen aus Kapitel 2 mit dem Vorgehen aus Kapitel 3 verglichen, um eine optimale Gesamtstrategie für die Berechnung unabhängiger Einheiten der Maximalordnung eines Zahlkörpers nach Dirichlet abzuleiten.



# 1 Einheiten in Ordnungen

Wir wollen in diesem Kapitel zuerst einige Bezeichnungen festlegen und die theoretischen Ergebnisse vorstellen, die wir später benutzen werden. Anschließend wird das Verfahren zur Berechnung von Grundeinheiten in drei Schritten nach [Poh93] skizziert, zu dessen zweitem Schritt – der Berechnung unabhängiger Einheiten nach Dirichlet – sich die zu dieser Arbeit anregenden Modifikationsideen ergeben.

## 1.1 Zahlentheoretische Grundlagen

Dieser Abschnitt dient vor allem der Benennung der im Folgenden verwendeten Begriffe und Sachverhalte. Viele Aussagen werden der Kürze halber unbewiesen getroffen, sind aber unter anderem in [PZ89] nachzulesen.

Wir betrachten den *algebraischen Zahlkörper*  $F = \mathbb{Q}(\rho)$ , der aus  $\mathbb{Q}$  durch Adjunktion der Nullstelle  $\rho$  eines über  $\mathbb{Q}$  irreduziblen, normierten Polynoms  $f(t) \in \mathbb{Z}[t]$  hervorgeht. Der Grad der Körpererweiterung  $[F : \mathbb{Q}]$  entspricht dem Grad dieses Polynoms, der hier  $n$  sei. In seinem Zerfällungskörper hat das Polynom dann  $n$  Nullstellen. Es sei  $r_1$  die Anzahl der reellen Nullstellen und  $2r_2$  die Anzahl der komplexen Nullstellen, so dass  $n = r_1 + 2r_2$  gilt. Die  $\mathbb{Q}$ -linearen Einbettungen  $\varphi_1, \dots, \varphi_n$  von  $F$  in  $\mathbb{C}$  nennt man *Konjugationen* und die Bilder  $\alpha^{(i)} := \varphi_i(\alpha)$  eines Elements  $\alpha \in F$  unter den Konjugationen nennt man die *Konjugierten* des Elements. Für die Konjugierten eines Elements legen wir die folgende Anordnung fest:

$$\begin{aligned}\alpha^{(1)}, \dots, \alpha^{(r_1)} &\in \mathbb{R} \\ \alpha^{(r_1+1)}, \dots, \alpha^{(r_1+r_2)} &\in \mathbb{C} \setminus \mathbb{R} \\ \alpha^{(r_1+r_2+j)} &= \overline{\alpha^{(r_1+j)}} \text{ für } 1 \leq j \leq r_2.\end{aligned}$$

Die Gesamtheit aller Elemente aus  $F$ , die Nullstellen eines normierten Polynoms aus  $\mathbb{Z}[t]$  sind, nennen wir die *Maximalordnung*  $\mathfrak{o}_F$ . Ein Unterring  $R$  von  $\mathfrak{o}_F$ , der ein freier  $\mathbb{Z}$ -Modul vom Rang  $m \leq n$  ist, heißt *Ordnung* von  $F$ .

**Bemerkung:** Im Folgenden sei  $R$  immer eine Ordnung von  $F$  vom Rang  $n$ , so dass für eine  $\mathbb{Z}$ -Basis  $\omega_1, \dots, \omega_n$  von  $R$  gilt, dass  $F = \mathbb{Q}\omega_1 + \dots + \mathbb{Q}\omega_n$  ist.

## 1 Einheiten in Ordnungen

Mit Hilfe der Konjugierten werden nun Norm und Spur eines Elements  $\alpha \in F$  definiert,

$$N_{F/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \alpha^{(i)} \quad (1.1)$$

$$Tr_{F/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \alpha^{(i)}, \quad (1.2)$$

sowie ein Skalarprodukt auf dem  $\mathbb{Q}$ -Vektorraum  $F$  durch

$$\langle \cdot, \cdot \rangle : F \times F \rightarrow \mathbb{R} : (x, y) \mapsto \sum_{i=1}^n x^{(i)} \overline{y^{(i)}} \quad (1.3)$$

und die davon induzierte positiv definite quadratische Form

$$T_2 : F \rightarrow \mathbb{R}^{\geq 0} : x \mapsto \langle x, x \rangle = \sum_{i=1}^n |x^{(i)}|^2, \quad (1.4)$$

die wir  $T_2$ -Länge nennen.

**Bemerkung:** Statt  $N_{F/\mathbb{Q}}(\alpha)$  schreiben wir im Folgenden auch oft einfach  $N(\alpha)$  für Elemente  $\alpha \in F$ . Für Elemente der Maximalordnung  $\eta \in \mathfrak{o}_F$  gilt, dass  $N_{F/\mathbb{Q}}(\eta) \in \mathbb{Z}$ .

**Proposition 1.1.** *Es sei  $R$  eine Ordnung des Zahlkörpers  $F$ .*

(a) *Die Anzahl nicht-assoziierter Elemente in  $R$  mit beschränkter Norm ist endlich.*

(b) *Für ein  $C \in \mathbb{R}^{>0}$  ist die Menge  $A := \{\alpha \in R \mid |\alpha^{(i)}| \leq C \text{ für alle } i \in \{1, \dots, n\}\}$  endlich.*

Beweis: Siehe Lemma (2.3) und (2.4) in [PZ89, Kapitel 5, Abschnitt 5.2].  $\square$

Ist  $\alpha_1, \dots, \alpha_n$  eine  $\mathbb{Z}$ -Basis der Ordnung  $R$ , so nennen wir

$$disc(\alpha_1, \dots, \alpha_n) := \det(Tr_{F/\mathbb{Q}}(\alpha_i \alpha_j))_{1 \leq i, j \leq n} = \det(\alpha_i^{(j)})_{1 \leq i, j \leq n}^2$$

die *Diskriminante der Ordnung  $R$* . Die Diskriminante einer Ordnung ist von der Wahl der Basis unabhängig. Die *Diskriminante  $D_F$*  des Zahlkörpers  $F$  wird mit Hilfe einer  $\mathbb{Z}$ -Basis der Maximalordnung  $\{\omega_1, \dots, \omega_n\}$ , *Ganzheitsbasis* genannt, definiert und entspricht somit der Diskriminante der Maximalordnung:

$$D_F := \det((Tr_{F/\mathbb{Q}}(\omega_i \omega_j))_{1 \leq i, j \leq n}).$$

### 1.1.1 Einheiten

Die Menge der invertierbaren Elemente der Ordnung  $R$  eines Zahlkörpers  $F$  heißt die *Einheitengruppe* der Ordnung und wird mit  $U(R)$  bezeichnet. Ein Element  $\varepsilon \in R$  ist genau dann eine Einheit von  $R$ , wenn  $|N_{F/\mathbb{Q}}(\varepsilon)| = 1$ . Die Struktur der Einheitengruppe wird durch den **Dirichletschen Einheitensatz** beschrieben.

**Satz 1.2** (Dirichletscher Einheitensatz). *Die Einheitengruppe  $U(R)$  einer Ordnung  $R$  von  $F$  ist das endliche, direkte Produkt der zyklischen Untergruppe der Torsionseinheiten  $TU(R)$  und  $r = r_1 + r_2 - 1$  unendlichen zyklischen Gruppen, die von den sogenannten Grundeinheiten  $E_1, \dots, E_r$  von  $R$  erzeugt werden:  $U(R) = TU(R) \times \langle E_1 \rangle \times \dots \times \langle E_r \rangle$ .*

Beweis: Für einen Beweis dieses Satzes siehe [PZ89, Kapitel 5, Theorem 2.14].  $\square$

Für die Torsionseinheiten  $\alpha \in TU(R)$ , also die in  $R$  gelegenen Einheitswurzeln, ist die Bedingung  $T_2(\alpha) = n$  notwendig und hinreichend. Einen Erzeuger  $\zeta$  von  $TU(R)$  können wir dann mit Hilfe des *Auszählalgorithmus*<sup>1</sup> bestimmen. Komplizierter ist die Bestimmung und Verifizierung der Basis des torsionsfreien Anteils von  $U(R)$ , des *Grundeinheitensystems* von  $R$ . Wir nennen die Anzahl der Elemente eines Grundeinheitensystems von  $R$ , im Folgenden bezeichnet mit  $r$ , den *Einheitenrang* von  $F$ . Eine wesentliche Eigenschaft des Grundeinheitensystems ist die Unabhängigkeit seiner Bestandteile in folgendem Sinne:

**Definition 1.3** (Unabhängige Einheiten). *Die Einheiten  $\eta_1, \dots, \eta_k$  werden **unabhängig** genannt, wenn für*

$$\prod_{i=1}^k \eta_i^{m_i} = 1 \quad \text{mit } m_1, \dots, m_k \in \mathbb{Z}$$

folgt, dass  $m_1 = \dots = m_k = 0$ . Kann man mindestens ein  $m_i \neq 0$  wählen, so dass das Potenzprodukt der Einheiten dennoch 1 ergibt, heißen die Einheiten *abhängig*.

Für die theoretische Überprüfung der Unabhängigkeit von Einheiten betrachten wir die Abbildung

$$L : F^\times \rightarrow \mathbb{R}^r : \varepsilon \mapsto \begin{pmatrix} c_1 \log |\varepsilon^{(1)}| \\ \vdots \\ c_r \log |\varepsilon^{(r)}| \end{pmatrix} \quad \text{mit } c_j = \begin{cases} 1 & \text{für } 1 \leq j \leq r_1 \\ 2 & \text{für } r_1 < j \leq r \end{cases}, \quad (1.5)$$

<sup>1</sup> Siehe Abschnitt „Algorithmische Werkzeuge“. Für alle Elemente  $\alpha \in R \setminus \{0\}$  gilt  $T_2(\alpha) \geq n$ , wegen  $|N_{F/\mathbb{Q}}(\alpha)|^2 \in \mathbb{Z}^{\geq 1}$  und der Ungleichung aus geometrischem und arithmetischem Mittel. Dann ist ein mit der Bedingung  $T_2(\zeta) \leq n$  *ausgezähltes* Element  $\zeta \in R \setminus \{0\}$  der gesuchte Erzeuger von  $TU(R)$ .

## 1 Einheiten in Ordnungen

welche die multiplikative Struktur von  $F^\times$  in eine additive Struktur des  $\mathbb{R}^r$  überführt, so dass das Bild der Einheitengruppe  $U(R)$  unter  $L$  ein vollständiges  $\mathbb{Z}$ -Gitter im  $\mathbb{R}^r$  bildet. Die Bilder von Einheiten unter der Abbildung aus (1.5) nennen wir im Folgenden  $L$ -Vektoren.

**Lemma 1.4.** *Es sei  $c_i = 1$  für  $(1 \leq i \leq r_1)$  und  $c_j = 2$  für  $(r_1 < j \leq r_1 + r_2)$ . Für jede Einheit  $\varepsilon$  von  $R$  gilt*

$$\sum_{j=1}^r c_j \log(|\varepsilon^{(j)}|) = -c_{r_1+r_2} \log(|\varepsilon^{(r_1+r_2)}|).$$

Beweis: Wir wenden den Logarithmus auf die Gleichungen

$$1 = |N_{F/\mathbb{Q}}(\varepsilon)| = \prod_{j=1}^{r_1+r_2} |\varepsilon^{(j)}|^{c_j}$$

an und erhalten dann durch Subtraktion des letzten Summanden die Aussage.  $\square$

Wie ertragreich die Anwendung der  $L$ -Abbildung auf Einheiten für die theoretische Beurteilung ihrer Eigenschaften ist, erschließt sich uns durch den folgenden Satz.

**Satz 1.5.**  *$\varepsilon_1, \dots, \varepsilon_k \in U(R)$  sind genau dann unabhängige Einheiten in  $R$ , wenn  $L(\varepsilon_1), \dots, L(\varepsilon_k)$  linear unabhängig über  $\mathbb{R}$  sind.*

Beweis: „ $\Rightarrow$ “ : Angenommen  $L(\varepsilon_1), \dots, L(\varepsilon_k)$  seien linear abhängig. Dann können wir einen der Vektoren durch eine Linearkombination der anderen ausdrücken. Es existieren ohne Beschränkung der Allgemeinheit  $\lambda_2, \dots, \lambda_k \in \mathbb{R}$ , so dass

$$L(\varepsilon_1) = \sum_{i=2}^k \lambda_i L(\varepsilon_i) \text{ gilt.}$$

Mit  $\mu_i := -\lfloor \lambda_i + \frac{1}{2} \rfloor$  für  $2 \leq i \leq k$  gilt dann:

$$\begin{aligned} L(\varepsilon_1) &= \sum_{i=2}^k (\mu_i + \lambda_i) L(\varepsilon_i) - \sum_{i=2}^k \mu_i L(\varepsilon_i) \\ \Rightarrow L(\underbrace{\varepsilon_1 \varepsilon_2^{\mu_2} \cdots \varepsilon_k^{\mu_k}}_{=: \eta}) &= \sum_{i=2}^k (\mu_i + \lambda_i) L(\varepsilon_i) \end{aligned}$$

$$\Rightarrow \|L(\eta)\|_2 = \left\| \sum_{i=2}^k (\mu_i + \lambda_i) L(\varepsilon_i) \right\|_2 \leq \sum_{i=2}^k |\mu_i + \lambda_i| \cdot \|L(\varepsilon_i)\|_2 \leq \frac{1}{2} \sum_{i=2}^k \|L(\varepsilon_i)\|_2.$$

Somit ist  $\|L(\eta)\|_2$  beschränkt und daraus folgt, dass es eine Schranke  $C \in \mathbb{R}^{>0}$  mit

$|\eta^{(i)}| \leq C$  für alle  $1 \leq i \leq r$  gibt. Mit Hilfssatz 1.4 können wir  $C$  sogar so wählen, dass  $|\eta^{(r_1+r_2)}| \leq C$  gilt. Somit sind alle Konjugierten von  $\eta$  durch  $C$  beschränkt. Die Menge  $\mathcal{U} := \{\varepsilon \in U(R) \mid |\varepsilon^{(i)}| \leq C \text{ für } 1 \leq i \leq n\}$  ist nach Proposition 1.1 endlich.

Wir haben gezeigt, dass wir für  $\varepsilon_1$  entsprechende Exponenten  $\mu_2, \dots, \mu_k \in \mathbb{Z}$  finden, so dass  $\varepsilon_1 \varepsilon_2^{\mu_2} \dots \varepsilon_k^{\mu_k} \in \mathcal{U}$ . Für beliebige Potenzen  $\nu \in \mathbb{N}$  von  $\varepsilon_1$  finden wir mit derselben Argumentation wie oben (aus der ersten Annahme und  $L(\varepsilon_1^\nu) = \nu L(\varepsilon_1)$  folgt, dass auch  $L(\varepsilon_1^\nu), L(\varepsilon_2), \dots, L(\varepsilon_k)$  linear abhängig sind.) Exponenten  $\tilde{\mu}_2, \dots, \tilde{\mu}_k \in \mathbb{Z}$ , so dass  $\varepsilon_1^\nu \varepsilon_2^{\tilde{\mu}_2} \dots \varepsilon_k^{\tilde{\mu}_k} \in \mathcal{U}$ . Da die Menge  $\mathcal{U}$  endlich ist, existieren dann  $\nu_1, \nu_2 \in \mathbb{N}$  mit  $\nu_1 > \nu_2$  und entsprechende Exponenten  $\check{\mu}_2, \dots, \check{\mu}_k$  sowie  $\hat{\mu}_2, \dots, \hat{\mu}_k \in \mathbb{Z}$ , so dass:

$$\begin{aligned} \varepsilon_1^{\nu_1} \cdot \varepsilon_2^{\check{\mu}_2} \dots \varepsilon_k^{\check{\mu}_k} &= \varepsilon_1^{\nu_2} \cdot \varepsilon_2^{\hat{\mu}_2} \dots \varepsilon_k^{\hat{\mu}_k} \\ \Rightarrow \varepsilon_1^{\nu_1 - \nu_2} \cdot \varepsilon_2^{\hat{\mu}_2 - \check{\mu}_2} \dots \varepsilon_k^{\hat{\mu}_k - \check{\mu}_k} &= 1. \end{aligned}$$

Demnach sind  $\varepsilon_1, \dots, \varepsilon_k$  abhängige Einheiten.

„ $\Leftarrow$ “: Angenommen  $\varepsilon_1, \dots, \varepsilon_k$  seien abhängige Einheiten. Dann existieren  $m_1, \dots, m_k \in \mathbb{Z}$  mit  $m_i \neq 0$  für ein  $i \in \{1, \dots, k\}$ , so dass  $\prod_{l=1}^k \varepsilon_l^{m_l} = 1$  gilt. Daraus folgt, dass

$$\begin{aligned} \prod_{l=1}^k \left(\varepsilon_l^{(j)}\right)^{m_l} = 1 \text{ für } 1 \leq j \leq r &\Rightarrow \left| \prod_{l=1}^k \left(\varepsilon_l^{(j)}\right)^{m_l} \right| = 1 \text{ für } 1 \leq j \leq r \\ \Rightarrow \prod_{l=1}^k \left| \left(\varepsilon_l^{(j)}\right)^{m_l} \right| = 1 \text{ für } 1 \leq j \leq r &\Rightarrow \prod_{l=1}^k \left| \varepsilon_l^{(j)} \right|^{m_l} = 1 \text{ für } 1 \leq j \leq r \\ \Rightarrow \prod_{l=1}^k \left| \left(\varepsilon_l^{(j)}\right) \right|^{c_j m_l} = 1 \text{ für } 1 \leq j \leq r \text{ und } c_j = \begin{cases} 1 & \text{für } 1 \leq j \leq r_1 \\ 2 & \text{für } r_1 \leq j \leq r \end{cases} \\ \Rightarrow \sum_{l=1}^k m_l c_j \log\left(\left| \left(\varepsilon_l^{(j)}\right) \right|\right) = 0 \text{ für } 1 \leq j \leq r \text{ (und } c_j \text{ wie oben)} \\ \Rightarrow \sum_{l=1}^k m_l L(\varepsilon_l) = 0. \end{aligned}$$

Nach obiger Wahl von  $m_1, \dots, m_k \in \mathbb{Z}$  gibt es ein  $i \in \{1, \dots, k\}$  mit  $m_i \neq 0$ .  
 $\Rightarrow L(\varepsilon_1), \dots, L(\varepsilon_k)$  sind linear abhängig. □

**Korollar 1.6.** Seien  $\varepsilon_1, \dots, \varepsilon_r$  unabhängige Einheiten aus  $R$ . Dann gilt für jedes weitere Element  $\varepsilon \in U(R)$ , dass die Einheiten  $\varepsilon, \varepsilon_1, \dots, \varepsilon_r$  abhängig sind.

Beweis: (Konsequenz aus Hilfssatz 1.5.)  $L(\varepsilon_1), \dots, L(\varepsilon_r)$  bilden eine Basis des  $\mathbb{R}^r$ .  
 $L(\varepsilon)$  ist davon linear abhängig. □

## 1 Einheiten in Ordnungen

Die Betrachtung der  $L$ -Vektoren liefert ein nützliches, theoretisches Kriterium für die Unabhängigkeit einer Menge von Einheiten<sup>2</sup>. Zusätzlich ermöglicht der Übergang zum  $L$ -Gitter die Überprüfung der Fähigkeit dieser Menge, die ganze Einheitsengruppe zu erzeugen, durch die Betrachtung der Regulatoren:

**Definition 1.7** (Regulator). Für Einheiten  $\varepsilon_1, \dots, \varepsilon_r \in U(R)$  heißt

$$\text{Reg}(\varepsilon_1, \dots, \varepsilon_r) := |\det(L(\varepsilon_1), \dots, L(\varepsilon_r))|$$

der **Regulator** von  $\varepsilon_1, \dots, \varepsilon_r$ .

Es seien  $\varepsilon_1, \dots, \varepsilon_r \in U(R)$  unabhängige Einheiten,  $E_1, \dots, E_r$  ein Grundeinheitensystem von  $R$ ,  $\zeta \in TU(R)$  und  $G$  eine Untergruppe von  $U(R)$  mit  $\{\zeta, \varepsilon_1, \dots, \varepsilon_r\} \subseteq G$ . Der endliche Index von  $G$  in der Gruppe der Einheiten  $U(R)$  lässt sich durch die Regulatoren ausdrücken:

$$(U(R) : G) = (L(U(R)) : L(G)) = \frac{\text{Reg}(G)}{\text{Reg}(U(R))} = \frac{|\det(L(\varepsilon_1), \dots, L(\varepsilon_r))|}{|\det(L(E_1), \dots, L(E_r))|}.$$

Statt  $\text{Reg}(U(R))$  schreiben wir auch  $\text{Reg}_R$ .

### 1.1.2 Ideale

Wir betrachten die Menge der Ideale einer Ordnung  $R$ , wobei wir das Nullideal im Folgenden ausnehmen. Ein Primideal  $\mathfrak{p}$  ist ein echtes Ideal von  $R$ , so dass  $R/\mathfrak{p}$  nullteilerfrei ist.

**Definition 1.8.** Die Addition und Multiplikation von zwei Idealen  $\mathfrak{a}, \mathfrak{b}$  aus  $R$  definieren wir folgendermaßen:

$$\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \text{ beziehungsweise} \quad (1.6)$$

$$\mathfrak{a}\mathfrak{b} := \left\{ \sum_{i=1}^k a_i b_i \mid k \in \mathbb{N} \text{ und } a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \text{ für } 1 \leq i \leq k \right\}. \quad (1.7)$$

**Definition 1.9.** Seien  $\mathfrak{a}, \mathfrak{b}$  Ideale aus  $R$ . Wir bezeichnen die Beziehung der Ideale als  $\mathfrak{a}$  **teilt**  $\mathfrak{b}$ , wenn es ein Ideal  $\mathfrak{c}$  aus  $R$  gibt, so dass  $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ . Es gilt:

$$\mathfrak{a}|\mathfrak{b} \Leftrightarrow \mathfrak{b} \subseteq \mathfrak{a}.$$

**Definition 1.10.** Für ein Ideal  $\mathfrak{a}$  der Ordnung  $R$  definieren wir die **Norm des Ideals**  $\mathfrak{a}$  als  $N(\mathfrak{a}) := (R : \mathfrak{a}) = \#R/\mathfrak{a}$ .

<sup>2</sup> Für die praktische Umsetzung sei wie in Abschnitt 1.1.3. auf [FP85] verwiesen.

## 1.1 Zahlentheoretische Grundlagen

Die Menge von Primidealen der Maximalordnung  $\mathfrak{o}_F$  bezeichnen wir mit  $\mathbb{P}_F$ . Die Maximalordnung eines Zahlkörpers ist ein Dedekindring (siehe [PZ89, Kapitel 4, Theorem (5.9)]). Daraus folgt, dass sich jedes Ideal  $\mathfrak{a}$  einer Maximalordnung eindeutig bis auf die Reihenfolge als Potenzprodukt von Primidealen aus  $\mathfrak{o}_F$  schreiben lässt:

$$\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$$

mit  $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathbb{P}_F$  und  $m_1, \dots, m_r \in \mathbb{N}$ .

Durch Hinzunahme von negativen Potenzen kommen wir zu der Menge der *gebrochenen Ideale* von  $\mathfrak{o}_F$ .

$$I_F := \{\mathfrak{b} \subseteq F \mid x\mathfrak{b} \text{ ist ein Ideal von } \mathfrak{o}_F \text{ für ein } x \in F\}.$$

Mit dem Begriff *Ideal* bezeichnen wir im Folgenden alle Elemente dieser Menge. Die herkömmlichen Ideale  $\mathfrak{a} \subseteq \mathfrak{o}_F$  spezifizieren wir als *ganze Ideale*. Die Ideale  $\mathfrak{a} \in I_F$ , für die es ein  $\alpha \in F^\times$  gibt, so dass  $\mathfrak{a} = \alpha\mathfrak{o}_F$  gilt, nennen wir *Hauptideale* von  $I_F$  und bezeichnen die Menge der Hauptideale mit  $H_F$ .

**Bemerkung:** *In späteren Kapiteln werden wir für  $\alpha \in F^\times$  statt des Hauptideals  $\alpha\mathfrak{o}_F$  hinsichtlich Primidealfaktorisierungsfragen oft vereinfachend  $\alpha$  schreiben. Wegen der Isomorphie  $F^\times/U(\mathfrak{o}_F) \simeq H_F$  ist durch Angabe des Hauptideals  $\mathfrak{a}$  das erzeugende Element  $\alpha \in F^\times$  mit  $\alpha\mathfrak{o}_F = \mathfrak{a}$  modulo Einheiten eindeutig bestimmt.*

Bei Definition der Multiplikation für die Elemente aus  $I_F$  wie in (1.7), bildet  $I_F$  eine multiplikative abelsche Gruppe mit neutralem Element  $\mathfrak{o}_F$ . Für Ideale  $\mathfrak{a}, \mathfrak{b} \in I_F$  gelte  $\mathfrak{a}|\mathfrak{b}$ , wenn es ein ganzes Ideal  $\mathfrak{c} \in I_F$  gibt, so dass  $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ . Zu jedem Primideal  $\mathfrak{p} \in \mathbb{P}_F$  existiert ein eindeutiger Homomorphismus

$$\nu_{\mathfrak{p}} : I_F \rightarrow \mathbb{Z}, \mathfrak{a} \mapsto \max \{k \in \mathbb{Z} \mid \mathfrak{p}^k | \mathfrak{a}\}, \quad (1.8)$$

der für jedes Element aus  $I_F$  den Exponenten aus dem Primidealpotenzprodukt bezüglich des betreffenden Primideals wiedergibt. Jedes Ideal aus  $I_F$  lässt sich darstellen als eindeutiges endliches Produkt

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathbb{P}_F} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}.$$

Das Bild  $\nu_{\mathfrak{p}}(\mathfrak{a})$  eines Elements  $\mathfrak{a} \in I_F$  unter dem Homomorphismus aus (1.8) nennen wir im Folgenden **Bewertung von  $\mathfrak{a}$  über  $\mathfrak{p}$** .

## 1 Einheiten in Ordnungen

**Definition 1.11.** Es sei  $\mathcal{R}$  ein Ring mit Einselement.

Eine Abbildung  $\eta : \mathcal{R} \rightarrow \mathbb{Z} \cup \{\infty\}$  heißt **diskrete exponentielle Bewertung** von  $\mathcal{R}$ , falls für alle  $x, y \in \mathcal{R}$  gilt:

- (i)  $\eta(x) = \infty \Leftrightarrow x = 0$ ,
- (ii)  $\eta(xy) = \eta(x) + \eta(y)$ ,
- (iii)  $\eta(x \pm y) \geq \min(\eta(x), \eta(y))$ ,
- (iv)  $\eta(\pm 1) = 0$ .

**Satz 1.12.** Es seien  $\mathcal{R}$  ein Dedekindring und  $\mathfrak{p}$  ein Primideal  $\neq 0$  in  $\mathcal{R}$ . Dann ist die Abbildung

$$\nu_{\mathfrak{p}} : \mathcal{R} \rightarrow \mathbb{Z} : x \mapsto \begin{cases} n & \text{falls } n \in \mathbb{Z}^{\geq 0} \text{ existiert mit } x \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1} \\ \infty & \text{sonst} \end{cases}$$

eine diskrete exponentielle Bewertung von  $\mathcal{R}$ .

Beweis: Wir zeigen nur (iii):  $x, y \in \mathcal{R}$  beliebig. Da  $x + y \in \mathfrak{p}^{\nu_{\mathfrak{p}}(x)} + \mathfrak{p}^{\nu_{\mathfrak{p}}(y)} = \text{ggT}(\mathfrak{p}^{\nu_{\mathfrak{p}}(x)}, \mathfrak{p}^{\nu_{\mathfrak{p}}(y)}) = \mathfrak{p}^{\min(\nu_{\mathfrak{p}}(x), \nu_{\mathfrak{p}}(y))}$  gilt, ist die Bewertung  $\nu_{\mathfrak{p}}(x + y)$  mindestens  $\min(\nu_{\mathfrak{p}}(x), \nu_{\mathfrak{p}}(y))$ .  $\square$

Der in (1.8) definierte Homomorphismus auf der Gruppe der gebrochenen Ideale  $I_F$  ist eine Fortsetzung einer solchen  **$\mathfrak{p}$ -exponentiellen Bewertung** des Dedekindrings  $\mathfrak{o}_F$ . Die enge Verknüpfung zwischen Elementen und den davon erzeugten Hauptidealen in Bezug auf Bewertungen drückt sich dann nochmals in folgender Aussage aus.

**Korollar 1.13.** Es gilt  $\nu_{\mathfrak{p}}(\alpha) = \nu_{\mathfrak{p}}(\alpha \mathfrak{o}_F) \forall \alpha \in \mathfrak{o}_F$ .

Für ein Element  $\alpha \in F$  und ein Primideal  $\mathfrak{p} \in I_F$  nennen wir den Wert  $\nu_{\mathfrak{p}}(\alpha)$  im Folgenden **Bewertung von  $\alpha$  über  $\mathfrak{p}$** .

Primidealzerlegung in Erweiterungen

Seien nun  $K$  und  $F$  Zahlkörper mit  $K \subseteq F$  und Maximalordnungen  $\mathfrak{o}_K$  und  $\mathfrak{o}_F$ . Für ein Ideal  $\mathfrak{p} \in \mathbb{P}_K$  gibt es eine eindeutige Zerlegung von  $\mathfrak{p}\mathfrak{o}_F$  in Primideale  $\mathfrak{P}_1, \dots, \mathfrak{P}_k$  von  $\mathbb{P}_F$ :

$$\mathfrak{p}\mathfrak{o}_F = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k} \text{ mit } e_1, \dots, e_k \in \mathbb{Z}^{\geq 1}. \quad (1.9)$$

**Definition 1.14.** Der Exponent  $e_i \in \mathbb{Z}^{\geq 1}$  aus der Zerlegung in (1.9) heißt **Verzweigungsindex von  $\mathfrak{P}_i$  über  $\mathfrak{p}$**  und wird mit  $e(\mathfrak{P}_i|\mathfrak{p})$  bezeichnet. Wir sagen, dass die Primideale  $\mathfrak{P}_i$  **über  $\mathfrak{p}$  liegen**.

**Lemma 1.15.** *Es sei  $\mathfrak{P}$  ein Primideal, das über  $\mathfrak{p}$  liegt. Äquivalent dazu ist jede der folgenden Aussagen:*

- (i)  $\mathfrak{P} | \mathfrak{p}\mathfrak{o}_F$ ,
- (ii)  $\mathfrak{P} \supseteq \mathfrak{p}\mathfrak{o}_F$ ,
- (iii)  $\mathfrak{P} \supseteq \mathfrak{p}$ ,
- (iv)  $\mathfrak{P} \cap \mathfrak{o}_K = \mathfrak{p}$ ,
- (v)  $\mathfrak{P} \cap K = \mathfrak{p}$ .

Beweis: siehe Lemma (2.12) in [PZ89, Kapitel 6]. □

**Definition 1.16.** *Es sei  $\mathfrak{P}_i$  ein Primideal von  $\mathfrak{o}_F$ , das über dem Primideal  $\mathfrak{p}$  von  $\mathfrak{o}_K$  liegt. Dann gilt  $N(\mathfrak{P}_i) = \#(\mathfrak{o}_F/\mathfrak{P}_i) = N(\mathfrak{p})^{f_i}$  mit  $f_i \in \mathbb{Z}^{\geq 1}$ . Der Exponent  $f_i$  heißt **Trägheitsgrad von  $\mathfrak{P}_i$  über  $\mathfrak{p}$**  und wird mit  $f(\mathfrak{P}_i|\mathfrak{p})$  bezeichnet.*

**Definition und Lemma 1.17.** *Es sei  $R$  eine Ordnung des Zahlkörpers  $F$ . Wir nennen das Ideal*

$$\mathcal{F} := \{x \in R \mid x\mathfrak{o}_F \subseteq R\}$$

den **Führer von  $R$  in  $\mathfrak{o}_F$** . Dann sind

$$\mathcal{D}_{\mathfrak{o}_F, \mathcal{F}} := \{\mathfrak{a} \subseteq \mathfrak{o}_F \mid \mathfrak{a} \text{ Ideal von } \mathfrak{o}_F, \text{ ungleich dem Nullideal, so dass } \mathfrak{a} + \mathcal{F} = \mathfrak{o}_F\},$$

$$\mathcal{D}_{R, \mathcal{F}} := \{\tilde{\mathfrak{a}} \subseteq \mathfrak{o}_F \mid \tilde{\mathfrak{a}} \text{ Ideal von } R, \text{ ungleich dem Nullideal, so dass } \tilde{\mathfrak{a}} + \mathcal{F} = R\}$$

multiplikative Monoide mit Kürzungsregeln und es gelten die folgenden Aussagen:

- (i)  $\varphi : \mathcal{D}_{R, \mathcal{F}} \rightarrow \mathcal{D}_{\mathfrak{o}_F, \mathcal{F}} : \tilde{\mathfrak{a}} \mapsto \tilde{\mathfrak{a}}\mathfrak{o}_F$  ist ein Isomorphismus mit Umkehrabbildung  $\varphi^{-1} : \mathcal{D}_{\mathfrak{o}_F, \mathcal{F}} \rightarrow \mathcal{D}_{R, \mathcal{F}} : \mathfrak{a} \mapsto \mathfrak{a} \cap R$ .
- (ii) Jedes Ideal  $\tilde{\mathfrak{a}}$  von  $\mathcal{D}_{R, \mathcal{F}}$  hat in  $R$  eine eindeutige Darstellung als Produkt von Primidealen.

Beweis: Siehe Lemma (2.25) und Lemma (2.26) in [PZ89, Kapitel 6]. □

**Lemma 1.18.** *Es seien  $K$  und  $F$  Zahlkörper mit Maximalordnungen  $\mathfrak{o}_F$  beziehungsweise  $\mathfrak{o}_K$  und es sei  $F = K(\rho)$  für  $\rho \in \mathfrak{o}_F$  und  $f(t) \in \mathfrak{o}_K[t]$  Minimalpolynom von  $\rho$  mit Diskriminante  $d(f)$ . Des Weiteren soll  $\mathcal{F}$  den Führer der Gleichungsordnung  $\mathfrak{o}_K[\rho]$  in  $\mathfrak{o}_F$  bezeichnen. Sei  $\mathfrak{p}$  ein Primideal von  $\mathfrak{o}_K$ , dann gilt:*

$$\begin{aligned} \mathfrak{p} \text{ teilt nicht } d(f)\mathfrak{o}_K &\Rightarrow \mathfrak{p}\mathfrak{o}_F + \mathcal{F} = \mathfrak{o}_F \\ &\Rightarrow \mathfrak{p}\mathfrak{o}_F \in \mathcal{D}_{\mathfrak{o}_F, \mathcal{F}}. \end{aligned}$$

Beweis: Siehe Lemma (2.29) in [PZ89, Kapitel 6]. □

### 1.1.3 Algorithmische Werkzeuge

Alle in den folgenden Kapiteln vorgestellten Verfahren und Algorithmen wurden in MAGMA [BCP97] implementiert. Bei der Implementation wurden Algorithmen und Funktionen verwendet, die in MAGMA und KANT [KG06] bereits implementiert sind. Die implizite Verwendung solcher Funktionen soll für die Punkte, die wir für nicht offensichtlich halten, in diesem Abschnitt legitimiert und erläutert werden. Des Weiteren stellen uns die praktischen Berechnungen vor numerische Probleme, worauf wir am Ende dieses Abschnitts kurz zurückkommen.

#### Gitteralgorithmen

Wichtige Algorithmen, die im Folgenden zur Berechnung von Elementen der Ordnung mit bestimmten Eigenschaften benutzt werden, sind der *Auszählalgorithmus von Fincke und Pohst* und der *LLL-Algorithmus*. Diese sind in [PZ89], Kapitel 3, Abschnitt 3.3. zu finden. Die Algorithmen können in der dort angegebenen Form eine Menge von Elementen eines Gitters als Teilmenge des  $\mathbb{C}^n$  mit Eigenschaften bezüglich des Standardskalarprodukts und der davon induzierten, euklidischen Norm berechnen.

Im Folgenden ergibt sich für uns die Notwendigkeit der Berechnung von Elementen eines Gitters mit Eigenschaften bezüglich anderer Skalarprodukte  $\langle \cdot, \cdot \rangle_*$  und davon induzierten, positiv definiten, quadratischen Formen oder Normen. Dabei wollen wir die Skalarprodukte innerhalb der Algorithmen unverändert lassen, da wir auf die Implementation in MAGMA zurückgreifen wollen. Dazu betrachten wir die Grammatrix  $A := (\langle \mathbf{a}_i, \mathbf{a}_j \rangle_*)_{1 \leq i, j \leq k} \in \mathbb{R}^{k \times k}$  für das Gitter  $\Lambda = \bigoplus_{i=1}^k \mathbb{Z} \mathbf{a}_i$  mit innerem Produkt  $\langle \cdot, \cdot \rangle_*$ . Durch die *Cholesky-Zerlegung* der Grammatrix  $A = R^t R$  gewinnt man eine obere Dreiecksmatrix  $R \in \mathbb{R}^{k \times k}$ , deren Spalten  $(\mathbf{r}_1, \dots, \mathbf{r}_k)$  wir dann als Basisvektoren eines Gitters  $\tilde{\Lambda} := \bigoplus_{i=1}^k \mathbb{Z} \mathbf{r}_i$  auffassen können.

Zur Berechnung einer bezüglich der von  $\langle \cdot, \cdot \rangle_*$  induzierten Norm LLL-reduzierten Basis von  $\Lambda$  kann die bezüglich der Standardnorm LLL-reduzierte Basis von  $\tilde{\Lambda}$  berechnet werden (wie in [PZ89, Kapitel 3, Algorithmus (3.40)]): *in MAGMA/KANT kann der LLL-Algorithmus beispielsweise sowohl mit einer Grammatrix  $A = (\langle \mathbf{a}_i, \mathbf{a}_j \rangle_*)_{1 \leq i, j \leq k}$  oder einer Basismatrix  $R := (\mathbf{r}_1, \dots, \mathbf{r}_k)$  als auch mit einem Gitter, das durch Basismatrix oder Grammatrix definiert wurde, initialisiert werden. Es wird eine Transformationsmatrix  $T \in Gl(k, \mathbb{Z})$  berechnet, so dass die Spalten von  $R \cdot T$  und die Spalten von  $B$  aus der Cholesky-Zerlegung von  $T^t A T (= B^t B)$  eine bezüglich der Standardnorm LLL-reduzierte Basis von  $\bigoplus_{i=1}^k \mathbb{Z} \mathbf{r}_i$  sind. Diese Transformationsmatrix angewendet auf die Basisvektoren  $\mathbf{a}_1, \dots, \mathbf{a}_k$  ergibt dann die bezüglich der gewünschten Norm (von  $\langle \cdot, \cdot \rangle_*$  induziert) LLL-reduzierte Basis von  $\bigoplus_{i=1}^k \mathbb{Z} \mathbf{a}_i$ .*

Eine Anwendung des Auszählalgorithmus nach Fincke und Pohst ist die Berechnung kurzer Gittervektoren. Nach Durchführung von quadratischer Ergänzung (siehe [PZ89, Kapitel 3, Algorithmus (3.11)]) für eine positiv definite, symmetrische Matrix  $A \in \mathbb{R}^{k \times k}$  erhält man eine Matrix  $Q = (q_{i,j}) \in \mathbb{R}^{k \times k}$ , so dass für  $\vec{x} = (x_1, \dots, x_k)^t \in \mathbb{Z}^k$  gilt:

$$\vec{x}^t A \vec{x} = \sum_{i=1}^k q_{i,i} (x_i + \sum_{j=i+1}^k q_{i,j} x_j)^2.$$

Bei Eingabe dieser Matrix  $Q$  und einer Schranke  $C$  berechnet der Auszählalgorithmus (siehe [PZ89, Kapitel 3, Algorithmus (3.15)]) die Menge  $\{\vec{x} \in \mathbb{Z}^k \mid \vec{x}^t A \vec{x} \leq C\}$ .

In einem Gitter  $\Lambda = \bigoplus_{i=1}^k \mathbb{Z} \mathbf{a}_i$  mit Skalarprodukt  $\langle \cdot, \cdot \rangle_*$  sei nun die Menge der Vektoren  $\{\mathbf{a} \in \Lambda \mid \langle \mathbf{a}, \mathbf{a} \rangle_* \leq C\}$  zu berechnen. Mit dem Auszählalgorithmus berechnet man die Menge  $\mathcal{M} := \{\vec{x} \in \mathbb{Z}^k \mid \vec{x}^t \mathcal{A} \vec{x} \leq C\}$ , wobei  $\mathcal{A} := (\langle \mathbf{a}_i, \mathbf{a}_j \rangle_*)_{1 \leq i, j \leq k}$  die entsprechende Grammatrix ist.

Aus  $\{\mathbf{a} \in \Lambda \mid \langle \mathbf{a}, \mathbf{a} \rangle_* \leq C\} = \{x_1 \mathbf{a}_1 + \dots + x_k \mathbf{a}_k \mid (x_1, \dots, x_k)^t \in \mathcal{M}\}$  ergeben sich dann die gesuchten Vektoren.

#### LLL-reduzierte Basis und kurze Elemente eines freien $\mathbb{Z}$ -Moduls

In Kapitel 2 sowie bei der Berechnung von Torsionseinheiten und zur Regulatorabschätzung wollen wir die Gitteralgorithmen auf einen freien  $\mathbb{Z}$ -Modul  $M$  vom Rang  $n \in \mathbb{N}$  mit Basis  $\alpha_1, \dots, \alpha_n$  anwenden. Wir geben hier an, wie das in der gegebenen Situation umzusetzen ist.

Sei  $\underline{\lambda} \in \mathbb{R}_+^n$  mit  $\lambda_j = \lambda_{j-r_2}$  für  $(r_1 + r_2 + 1 \leq j \leq n)$ . Auf dem Modul ist dann ein inneres Produkt  $\langle \cdot, \cdot \rangle_{\underline{\lambda}}$  und eine davon induzierte, positiv definite, quadratische Form  $T_{2,\underline{\lambda}}$  definiert durch:

$$\langle \cdot, \cdot \rangle_{\underline{\lambda}} : M \times M \rightarrow \mathbb{R} : (x, y) \mapsto \sum_{i=1}^n \frac{1}{\lambda_i^2} x^{(i)} \overline{y^{(i)}}$$

beziehungsweise

$$T_{2,\underline{\lambda}} : M \rightarrow \mathbb{R}^{\geq 0} : x \mapsto \langle x, x \rangle_{\underline{\lambda}} = \sum_{i=1}^n \frac{1}{\lambda_i^2} |x^{(i)}|^2.$$

Die von  $\langle \cdot, \cdot \rangle_{\underline{\lambda}}$  induzierte Norm  $\|\cdot\|_{\underline{\lambda}} : M \rightarrow \mathbb{R}^{\geq 0}, x \mapsto \sqrt{\langle x, x \rangle_{\underline{\lambda}}}$  nennen wir  $T_{2,\underline{\lambda}}$ -Norm.

## 1 Einheiten in Ordnungen

Wie definieren einen Monomorphismus

$$\Phi_{\underline{\lambda}} : M \rightarrow \mathbb{R}^n, \alpha \mapsto \begin{pmatrix} \frac{1}{\lambda_1} \alpha^{(1)} \\ \vdots \\ \frac{1}{\lambda_{r_1}} \alpha^{(r_1)} \\ \frac{\sqrt{2}}{\lambda_{r_1+1}} \operatorname{Re}(\alpha^{(r_1+1)}) \\ \frac{\sqrt{2}}{\lambda_{r_1+1}} \operatorname{Im}(\alpha^{(r_1+1)}) \\ \vdots \\ \frac{\sqrt{2}}{\lambda_{r_1+r_2}} \operatorname{Re}(\alpha^{(r_1+r_2)}) \\ \frac{\sqrt{2}}{\lambda_{r_1+r_2}} \operatorname{Im}(\alpha^{(r_1+r_2)}) \end{pmatrix}. \quad (1.10)$$

Durch das Bild  $\Lambda := \Phi_{\underline{\lambda}}(M)$  wird ein zu  $M$  isomorphes, vollständiges Gitter im  $\mathbb{R}^n$  definiert. Wir nennen  $\Lambda$  das *mit  $\underline{\lambda}$  gewichtete Konjugiertengitter zu  $M$* .

Die euklidische Norm eines Elements  $\Phi_{\underline{\lambda}}(\alpha)$  des Gitters  $\Lambda$  entspricht der  $T_{2,\underline{\lambda}}$ -Norm des entsprechenden Elements  $\alpha \in M$ , denn eine kurze Rechnung zeigt:

$$\begin{aligned} \|\Phi_{\underline{\lambda}}(\alpha)\|_2^2 &= \langle \Phi_{\underline{\lambda}}(\alpha), \Phi_{\underline{\lambda}}(\alpha) \rangle = \Phi_{\underline{\lambda}}(\alpha)^t \Phi_{\underline{\lambda}}(\alpha) \\ &= \left\{ \begin{array}{l} \frac{1}{\lambda_1^2} (\alpha^{(1)})^2 + \dots + \frac{1}{\lambda_{r_1}^2} (\alpha^{(r_1)})^2 \\ + \underbrace{\frac{2}{(\lambda_{r_1+1})^2} (\operatorname{Re}(\alpha^{(r_1+1)}))^2 + \frac{2}{(\lambda_{r_1+1})^2} (\operatorname{Im}(\alpha^{(r_1+1)}))^2}_{=2 \frac{|\alpha^{(r_1+1)}|^2}{(\lambda_{r_1+1})^2}} \\ + \dots + \underbrace{\frac{2}{(\lambda_{r_1+r_2})^2} (\operatorname{Re}(\alpha^{(r_1+r_2)}))^2 + \frac{2}{(\lambda_{r_1+r_2})^2} (\operatorname{Im}(\alpha^{(r_1+r_2)}))^2}_{=2 \frac{|\alpha^{(r_1+r_2)}|^2}{(\lambda_{r_1+r_2})^2}} \end{array} \right. \\ &= \left\{ \begin{array}{l} \frac{1}{\lambda_1^2} |\alpha^{(1)}|^2 + \dots + \frac{1}{\lambda_{r_1}^2} |\alpha^{(r_1)}|^2 + \frac{1}{(\lambda_{r_1+1})^2} |\alpha^{(r_1+1)}|^2 + \underbrace{\frac{1}{(\lambda_{r_1+r_2+1})^2} |\alpha^{(r_1+r_2+1)}|^2}_{= \frac{1}{(\lambda_{r_1+1})^2} |\alpha^{(r_1+1)}|^2} \\ + \dots + \frac{1}{(\lambda_{r_1+r_2})^2} |\alpha^{(r_1+r_2)}|^2 + \underbrace{\frac{1}{(\lambda_{r_1+2r_2})^2} |\alpha^{(r_1+2r_2)}|^2}_{= \frac{1}{(\lambda_{r_1+r_2})^2} |\alpha^{(r_1+r_2)}|^2} \end{array} \right. \end{aligned}$$

$$= \sum_{i=1}^n \frac{1}{\lambda_i^2} |\alpha^{(i)}|^2 = T_{2,\lambda}(\alpha).$$

Damit gilt für die Normen:  $\|\Phi_\lambda(\alpha)\| = \sqrt{\langle \Phi_\lambda(\alpha), \Phi_\lambda(\alpha) \rangle} = (T_{2,\lambda}(\alpha))^{\frac{1}{2}} = \|\alpha\|_\lambda$ .  
 Durch eine ähnliche Rechnung (man benutze, dass für  $x, y \in \mathbb{C}$  gilt:  $x\bar{y} + \bar{x}y = 2\operatorname{Re}(x)\operatorname{Re}(y) + 2\operatorname{Im}(x)\operatorname{Im}(y)$ ) kann man zeigen, dass allgemein gilt:

$$\langle \alpha_i, \alpha_j \rangle_\lambda = \langle \Phi_\lambda(\alpha_i), \Phi_\lambda(\alpha_j) \rangle.$$

Damit gilt für die Diskriminante des Gitters:

$$\begin{aligned} d(\Lambda) &= d(\Phi_\lambda(M)) = \sqrt{\det((\Phi_\lambda(\alpha_i))^t \Phi_\lambda(\alpha_j))_{1 \leq i, j \leq n}} \\ &= \sqrt{\det(\langle \alpha_i, \alpha_j \rangle_\lambda)_{1 \leq i, j \leq n}} = \sqrt{\det(T_{2,\lambda})}, \end{aligned}$$

wobei die Determinante der quadratischen Form als Determinante ihrer Grammatrix  $(\langle \alpha_i, \alpha_j \rangle_\lambda)_{1 \leq i, j \leq n}$  definiert ist. Für die Diskriminante des Moduls mit Spur-Bilinearform

$$\operatorname{Tr}_{M/\mathbb{Z}}^\lambda : M \times M \rightarrow \mathbb{Z}, (\beta, \alpha) \mapsto \sqrt{\langle \beta, \alpha \rangle_\lambda}$$

gilt dann:

$$d(M) = \operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(\operatorname{Tr}_{M/\mathbb{Z}}^\lambda(\alpha_i \alpha_j)_{1 \leq i, j \leq n}) = \sqrt{\det(T_{2,\lambda})} = d(\Lambda).$$

Nun ist die theoretische Grundlage für die Lösung der folgenden beiden Aufgaben gelegt:

**(1.)** Zu berechnen sei eine bezüglich der  $T_{2,\lambda}$ -Norm LLL-reduzierte Basis  $b_1, \dots, b_n$  des Moduls  $M$  mit Ausgangsbasis  $\alpha_1, \dots, \alpha_n$ . Die Basis  $b_1, \dots, b_n$  des Moduls  $M$  sei *bezüglich der  $T_{2,\lambda}$ -Norm LLL-reduziert*, wenn für  $b_1, \dots, b_n$  die Eigenschaften einer LLL-reduzierten Basis (wie in Lemma (3.39) in [PZ89, Kapitel 3]) erfüllt sind, wobei die zugrundeliegende Norm  $\|\cdot\|_\lambda$  und die Gitterdiskriminante  $\sqrt{\det(T_{2,\lambda})}$  ist. Die Eigenschaft des ersten Elements  $b_1$  der bezüglich  $T_{2,\lambda}$  LLL-reduzierten Basis von  $M_k$  lautet dann zum Beispiel

$$\|b_1\|_\lambda \leq 2^{\frac{1}{4}(n-1)} \left( \sqrt{\det(T_{2,\lambda})} \right)^{\frac{1}{n}}. \quad (1.11)$$

Wir halten das Vorgehen zur Berechnung der bezüglich der  $T_{2,\lambda}$ -Norm LLL-reduzierten Basis eines Moduls  $M$  im folgenden Algorithmus fest.

---

**Algorithmus 1** : Bestimmung der bezüglich der  $T_{2,\lambda}$ -Norm LLL-reduzierten Basis eines Moduls  $M$  mit Basis  $\alpha_1, \dots, \alpha_n$

---

**Eingabe** : Basis  $\alpha_1, \dots, \alpha_n$  des Moduls  $M$

**Ausgabe** : Bezüglich der  $T_{2,\lambda}$ -Norm LLL-reduzierte Basis  $b_1, \dots, b_n$  von  $M$

1. Definiere ein Gitter durch die Bilder der Basiselemente unter  $\Phi_\lambda$ :  
 $\Lambda \leftarrow \bigoplus_{i=1}^n \mathbb{Z} \cdot \Phi_\lambda(\alpha_i)$ .
  2. Berechne die LLL-reduzierte Basismatrix  $(\phi_1, \dots, \phi_n)$  des Gitters  $\Lambda$  und die zugehörige Transformationsmatrix  $T \in Gl(n, \mathbb{Z})$ , so dass  $(\Phi_\lambda(\alpha_1), \dots, \Phi_\lambda(\alpha_n))T = (\phi_1, \dots, \phi_n)$  gilt.
  3. Wende die Transformationsmatrix auf die Basis  $\alpha_1, \dots, \alpha_n$  an:  
 $(\alpha_1, \dots, \alpha_n)T = (b_1, \dots, b_n)$ .
  4. **return**  $b_1, \dots, b_n$ .
- 

(2.) Zu berechnen sei die Menge  $\mathcal{M} := \{\beta \in M \mid T_{2,\lambda}(\beta) \leq K\}$  für  $K \in \mathbb{R}_+$ . Es sei  $\beta = \beta_1\alpha_1 + \dots + \beta_n\alpha_n \in M$  und  $\mathbf{b} := (\beta_1, \dots, \beta_n)^t \in \mathbb{Z}^n$ . Dann ist:

$$\|\Phi_\lambda(\beta)\|^2 = T_{2,\lambda}(\beta) = \mathbf{b}^t \mathbf{A} \mathbf{b} \quad \text{mit } \mathbf{A} = (\Phi_\lambda(\alpha_i), \Phi_\lambda(\alpha_j))_{1 \leq i, j \leq n}.$$

Wenn man den Auszählalgorithmus mit der durch quadratische Ergänzung (siehe oben) aus der Matrix  $\mathbf{A}$  gewonnenen Matrix und der Schranke  $K$  initialisiert, erhält man die Menge  $\tilde{\mathcal{M}} = \{\mathbf{x} = (x_1, \dots, x_n)^t \in \mathbb{Z}^n \mid \mathbf{x}^t \mathbf{A} \mathbf{x} \leq K\}$ . Dann ergibt sich die gesuchte Menge als  $\mathcal{M} = \{x_1\alpha_1 + \dots + x_n\alpha_n \mid \mathbf{x} \in \tilde{\mathcal{M}}\}$ .

**Bemerkung 1.19** (Kurze Gittervektoren). *Wir verstehen im Folgenden unter der LLL-reduzierten Basis eines Gitters immer eine Basis mit den Eigenschaften wie in Definition (3.38) und Lemma (3.39) in [PZ89, Kapitel 3] angegeben. Der LLL-Algorithmus sei im Folgenden immer der Algorithmus zur Berechnung einer solchen Basis. Man kann jedoch auch andere Parameter als in der von uns hier festgelegten Definition wählen, bei denen zum Beispiel die Länge des ersten Basisvektors durch eine kleinere Schranke beschränkt ist. Allerdings hat die Berechnung einer solchen Basis mit dem LLL-Algorithmus dann im Allgemeinen keine polynomielle Laufzeit mehr.*

*Für die Länge des kürzesten Elements eines Gitters  $\Lambda$  der Dimension  $n$  kann man folgende Abschätzung aus Theorem (3.34) in [PZ89, Kapitel 3] angeben:*

$$\min \{\|x\|^2 \mid x \in \Lambda\} \leq \mathcal{Y}_n d(L)^{\frac{2}{n}}, \quad (1.12)$$

wobei die Hermitekonstante  $\mathcal{Y}_n^n$  abgeschätzt werden kann durch:

$$\mathcal{Y}_n^n \leq \left(\frac{2}{\pi}\right)^n \Gamma\left(1 + \frac{n+2}{2}\right)^2.$$

Übertragen auf den Modul  $M_k$  gilt damit für das bezüglich der  $T_{2,\underline{\lambda}}$ -Länge kürzeste Element des Moduls:

$$\min \{T_{2,\underline{\lambda}}(\beta) \mid \beta \in M_k\} \leq \mathcal{Y}_n (det(T_{2,\underline{\lambda}}))^{\frac{1}{n}}. \quad (1.13)$$

Die Berechnung eines Elements dieser Länge kann mit dem Auszählalgorithmus geschehen.

Für unsere späteren Berechnungen treffen wir zuletzt noch folgende Definition:

**Definition und Satz 1.20.** Sei  $A = (a_{ij}) \in \mathbb{Z}^{n \times m}$ . Für eine Spalte  $j$  der Matrix  $A$  nennen wir den Eintrag  $a_{i,j}$  mit dem kleinsten Zeilenindex  $i$ , so dass  $a_{i,j} \neq 0$  den **Kopf der Spalte**. Für Nullspalten, die keinen Kopf besitzen, sei der Zeilenindex ihres Kopfes gleich  $\infty$ .

Dann gibt es eine Matrix  $U \in \mathbb{Z}^{m \times m}$ , so dass die Matrix  $H(A) := AU$  folgende Eigenschaften besitzt:

1. Je größer der Spaltenindex einer Spalte der Matrix, desto größer der Zeilenindex ihres Kopfes. (Die Nullspalten stehen somit „hinten“.)
2. Der Kopf einer jeden Spalte ist strikt größer als 0.
3. Für die Elemente in der Zeile links neben jedem Kopf gilt, dass sie strikt kleiner als der jeweilige Kopf und größer gleich 0 sind.

$H(A)$  bezeichnen wir als **Hermite Normalform** von  $A$ .

Beweis: Siehe dazu [PZ89, Kapitel 3, Theorem 2.6]. Dort wird auch ein Algorithmus zur Berechnung angegeben. (Die zusätzliche Reduktion der Einträge rechts neben den Köpfen und die Vertauschung der Nullspalten nach hinten ist mit Multiplikation von unimodularen  $\mathbb{Z}^{m \times m}$ -Matrizen von rechts zu erreichen.)  $\square$

### Unabhängigkeit testen

Die Unabhängigkeit von Einheiten beurteilt und gewährleistet man theoretisch anhand der linearen Unabhängigkeit der  $L$ -Vektoren (siehe (1.5)). Die reellen Einträge dieser Vektoren machen bei praktischen Berechnungen Überlegungen zur numerischen Stabilität notwendig. So würde man zur Entscheidung, dass die berechneten Einheiten unabhängig sind, zum Beispiel gerne den Regulator heranziehen. Es ist jedoch ein numerisches Problem, zu beurteilen, wann dieser tatsächlich ungleich Null ist.

Falls eine Menge von abhängigen Einheiten  $\varepsilon_1, \dots, \varepsilon_{k+1} \in U(R)$  vorliegt, von denen  $\varepsilon_1, \dots, \varepsilon_k$  unabhängig sind, kann die Abhängigkeit häufig folgendermaßen verifiziert werden: Der *MLLL-Algorithmus* (siehe [PZ89, Kapitel 3, Algorithmus (3.48)]) berechnet zu einer Menge von Vektoren  $\mathbf{b}_1, \dots, \mathbf{b}_{k+1}$  (in unserem Fall gegeben durch  $L(\varepsilon_1), \dots, L(\varepsilon_{k+1})$ ) eines  $k$ -dimensionalen Gitters, wobei  $\mathbf{b}_1, \dots, \mathbf{b}_k$  linear unabhängig sind, eine Menge von Vektoren  $\hat{\mathbf{b}}_1, \dots, \hat{\mathbf{b}}_k$  mit der Eigenschaft  $\sum_{i=1}^{k+1} \mathbb{Z}L(\varepsilon_i) = \sum_{i=1}^k \mathbb{Z}\hat{\mathbf{b}}_i$  sowie eine Relation  $m_1, \dots, m_{k+1} \in \mathbb{Z}$  mit  $\sum_{j=1}^{k+1} |m_j| > 0$ , so dass  $m_1L(\varepsilon_1) + \dots + m_{k+1}L(\varepsilon_{k+1}) = \mathbf{0}$  ist. Mit Hilfe der gefundenen Relation lässt sich nun die Abhängigkeit der Einheiten algebraisch verifizieren:  $\varepsilon_1^{m_1} \dots \varepsilon_{k+1}^{m_{k+1}}$  ergibt dann eine Torsionseinheit. *Falls der Algorithmus nicht wie gewünscht unter Rückgabe einer Relation terminiert, heißt dies nicht, dass die Einheiten unabhängig sind. In [FP06, Abschnitt 5] findet sich eine numerisch stabile Alternative zur Verwendung des reellen MLLL.*

Für die spätere Nutzung halten wir das konkrete Vorgehen zur Ermittlung eines minimalen Erzeugendensystems  $\eta_1, \dots, \eta_k$  von  $\langle \varepsilon_1, \dots, \varepsilon_{k+1} \rangle$  fest:

---

#### Algorithmus 2 : MLLL-Reduktion für Einheiten der Ordnung $R$

---

**Eingabe** : Abhängige  $\varepsilon_1, \dots, \varepsilon_{k+1} \in U(R)$ , wobei  $\varepsilon_1, \dots, \varepsilon_k$  unabhängig

**Ausgabe** : Unabhängige  $\eta_1, \dots, \eta_k \in U(R)$  mit

$$\langle \eta_1, \dots, \eta_k \rangle = \langle \varepsilon_1, \dots, \varepsilon_k, \varepsilon_{k+1} \rangle$$

$\eta_i \leftarrow \varepsilon_i \quad (1 \leq i \leq k+1)$

**for**  $i = 1, \dots, k+1$  **do**

$\mathbf{b}_i \leftarrow L(\eta_i)$

$\mu_{i,j} \leftarrow \mathbf{b}_i^t \mathbf{b}_j^* / B_j \quad (1 \leq j \leq i-1)$

$\mathbf{b}_i^* \leftarrow \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*, B_i \leftarrow \langle \mathbf{b}_i^*, \mathbf{b}_i^* \rangle$

**endfor**

$flag \leftarrow false, m \leftarrow 2$

**while**  $flag = false$  **do**

$l \leftarrow m-1$

**if**  $|\mu_{m,l}| > \frac{1}{2}$  **then**

$r \leftarrow \lceil \mu_{m,l} \rceil, \eta_m \leftarrow \eta_m / \eta_l^r, \mu_{m,l} \leftarrow \mu_{m,l} - r$

$\mu_{m,j} \leftarrow \mu_{m,j} - r \mu_{l,j} \quad (1 \leq j \leq l-1)$

**endif**

---

```

if  $T_2(\eta_m) = n$  then
   $flag \leftarrow true$ 
   $\eta_i \leftarrow \eta_{i+1}$  ( $m \leq i \leq k$ )
endif
if  $B_m < (\frac{3}{4} - \mu_{m,m-1}^2)B_{m-1}$  then
   $\mu \leftarrow \mu_{m,m-1}$ 
   $B \leftarrow B_m + \mu^2 B_{m-1}$ 
  if  $B \neq 0$  then
     $\mu_{m,m-1} \leftarrow \mu B_{m-1}/B$ 
     $B_m \leftarrow B_m B_{m-1}/B$ 
    for  $i = m+1, \dots, k+1$  do
      
$$\begin{pmatrix} \mu_{i,m-1} \\ \mu_{i,m} \end{pmatrix} \leftarrow \begin{pmatrix} 1 & \mu_{m,m-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \begin{pmatrix} \mu_{i,m-1} \\ \mu_{i,m} \end{pmatrix}$$

    endfor
  endif
   $B_{m-1} \leftarrow B$ 
  
$$\begin{pmatrix} \eta_{m-1} \\ \eta_m \end{pmatrix} \leftarrow \begin{pmatrix} \eta_m \\ \eta_{m-1} \end{pmatrix}$$

  
$$\begin{pmatrix} \mu_{m-1,j} \\ \mu_{m,j} \end{pmatrix} \leftarrow \begin{pmatrix} \mu_{m,j} \\ \mu_{m-1,j} \end{pmatrix} \text{ f\"ur } (1 \leq j \leq m-2)$$

  if  $m > 2$  then
     $m \leftarrow m - 1$ 
  endif
else
  for  $h = 2, \dots, m-1$  do
     $l \leftarrow m - h$ 
    if  $|\mu_{m,l}| > \frac{1}{2}$  then
       $r \leftarrow \lceil \mu_{m,l} \rceil, \eta_m \leftarrow \eta_m / \eta_l^r, \mu_{m,l} \leftarrow \mu_{m,l} - r$ 
       $\mu_{m,j} \leftarrow \mu_{m,j} - r \mu_{l,j}$  ( $1 \leq j \leq l-1$ )
    endif
    if  $T_2(\eta_m) = n$  then
       $flag \leftarrow true$ 
       $\eta_i \leftarrow \eta_{i+1}$  ( $m \leq i \leq k$ )
    endif
  endfor
   $m \leftarrow m + 1$ 
endif
endwhile
return  $\eta_1, \dots, \eta_k$ 

```

---

## 1 Einheiten in Ordnungen

Unter Voraussetzung einer unbeschränkten Genauigkeit der reellen Werte während der Berechnungen (in diesem Fall bei der Ermittlung der  $\mu_{i,j}$  und der  $B_i$ ), ließe sich der angegebene Algorithmus auch für den Fall nutzen, dass man über die Abhängigkeit der Einheit  $\varepsilon_{k+1}$  von den Einheiten  $\varepsilon_1, \dots, \varepsilon_k$  noch keine Gewissheit hat. In der **while**-Bedingung bräuchte lediglich zusätzlich  $m \leq k + 1$  abgefragt zu werden und als Ausgabe müssten sämtliche Einheiten  $\eta_1, \dots, \eta_{k+1}$  zurückgegeben werden. Wenn nach Termination des Algorithmus Ungleichheit zwischen den beiden letzten ausgegebenen Einheiten besteht, wäre dann während der while-Schleife nie der Fall eingetreten, dass  $T_2(\eta_m) = n$ . In diesem Fall wären die Eingabeeinheiten unabhängig.

Unbeschränkte Genauigkeit ist nicht zu gewährleisten und um herauszufinden, ob eine Einheit  $\varepsilon_{k+1}$  von den unabhängigen Einheiten  $\varepsilon_1, \dots, \varepsilon_k$  unabhängig ist, müssen unter Umständen andere Maßnahmen, welche eine genaue Fehlerabschätzung beinhalten, ergriffen werden. In [FP06] wird ein solcher Test (Algorithmus 4.4.) angegeben, auf den wir uns von nun an praktisch stützen werden.

Im Folgenden werden wir an verschiedenen Stellen davon sprechen, ein minimales Erzeugendensystem  $\eta_1, \dots, \eta_j$  mit  $j \leq k + 1$  von  $\langle \varepsilon_1, \dots, \varepsilon_{k+1} \rangle$  mit MLLL zu bestimmen, wobei  $\varepsilon_1, \dots, \varepsilon_k$  bereits unabhängig sind, die Abhängigkeit von  $\varepsilon_1, \dots, \varepsilon_{k+1}$  aber noch nicht erwiesen ist. Gemeint ist damit immer, dass wir, orientiert an den konkreten numerischen Gegebenheiten, ein geeignetes Verfahren auswählen und benutzen, um zu testen, ob die Einheiten  $\varepsilon_1, \dots, \varepsilon_{k+1}$  abhängig sind und gegebenenfalls ein Erzeugendensystem geeignet ermitteln.

## 1.2 Berechnung von Grundeinheiten in drei Schritten

Das vorgestellte Verfahren zur Berechnung von Grundeinheiten einer Ordnung  $R$  besteht aus drei Schritten, deren Kern die Konstruktion eines Systems von  $r$  unabhängigen Einheiten  $\varepsilon_1, \dots, \varepsilon_r \in U(R)$  nach der sogenannten *Methode von Dirichlet* ist. Der Index  $(U(R) : \langle \zeta, \varepsilon_1, \dots, \varepsilon_r \rangle)$  einer Gruppe, die diese unabhängigen Einheiten und eine Torsionseinheit  $\zeta \in TU(R)$  enthält, in der gesamten Einheitengruppe gibt uns Aufschluss darüber, ob es sich um ein Grundeinheitensystem handelt. Wenn dies nicht der Fall ist, müssen wir uns entlang der Primateiler einer oberen Abschätzung dieses Indexes zum Grundeinheitensystem vorarbeiten. Hier wird nur eine skizzenhafte Zusammenfassung des Vorgehens gegeben, um die kommenden Ausführungen zum zweiten Schritt in den Gesamtzusammenhang einzuordnen. Details, Beweise der folgenden Aussagen, die genauen Algorithmen sowie Beschleunigungsmöglichkeiten sind in [Poh93] und [Wil93] zu finden.

### Schritt 1: Regulatorabschätzung

Da uns die Einheitengruppe  $U(R)$  unbekannt ist, ist der Regulator  $Reg_R$  und somit auch der Index  $(U(R) : \langle \zeta, \varepsilon_1, \dots, \varepsilon_r \rangle)$  für ein konstruiertes System von  $r$  unabhängigen Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  noch unbekannt. Durch eine untere Abschätzung für  $Reg_R$ , erhält man eine obere Schranke für den Index. Die in [Poh93] dargestellte Abschätzung des Regulators beruht auf der Betrachtung der Determinante und sukzessiver Minima einer positiv definiten, quadratischen Form  $Q$  auf  $U(R)$ . Mit dem Minkowskischen Satz über sukzessive Minima ergibt sich die untere Abschätzung für den Regulator als

$$\sqrt{\frac{2^{r^2} M_1 \cdots M_r}{n \mathcal{Y}_r^r}} \leq Reg_R.$$

Nun haben wir das Problem auf die Bestimmung unterer Schranken für die sukzessiven Minima reduziert. Eine Verbindung zwischen den Werten der quadratischen Form  $Q$  und der  $T_2$ -Länge wird uns durch die Lösung eines Extremalwertproblems mit Nebenbedingungen gegeben. Die sukzessiven Minima lassen sich damit nun erstens in solche unterteilen, deren Wert wir bestimmen können, weil es mit dem Übergang zum Gitter wie in (1.5) möglich ist, unabhängige Einheiten als Gitterpunkte bezüglich der  $T_2$ -Norm auszuzählen, die diese Minima annehmen und zweitens in andere, deren untere Schranke  $\tilde{C}$  wir kennen <sup>3</sup>.

<sup>3</sup> Für Details, wie zum Beispiel die Möglichkeit, Aufwand einzusparen, indem man Einheiten, an denen sukzessive Minima angenommen werden, nicht über den Normbetrag ausfindig macht, sondern die ausgezählten Elemente danach aussiebt, ob sie in einem Primideal enthalten sind, sehe man sich die Ausführungen in [Wil93] an.

## 1 Einheiten in Ordnungen

Dieser erste Schritt wird dem zweiten vornehmlich vorangestellt, weil hierbei bereits unabhängige Einheiten bestimmt werden, die wir dann zum Zweck der Aufwandsreduktion in Schritt 2 einbeziehen können.

### Schritt 2: Berechnung unabhängiger Einheiten

Im zweiten Schritt erfolgt die Berechnung eines Systems von  $r$  unabhängigen Einheiten. Im Rahmen dieser Arbeit wollen wir uns mit der Berechnung von unabhängigen Einheiten nach der *Methode von Dirichlet* beschäftigen. Dazu wird diese Methode für die Konstruktion eines solchen Systems in Kapitel 2 beschrieben und in Kapitel 3 eine Modifikationsidee vorgestellt.

### Schritt 3: Berechnung der Grundeinheiten

Aus dem in Schritt 1 und 2 gewonnenen System unabhängiger Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  der Ordnung  $R$  gilt es nun, im dritten Schritt ein Grundeinheitensystem von  $R$  zu gewinnen. Der Index von  $U := \langle \zeta, \varepsilon_1, \dots, \varepsilon_r \rangle$  in  $U(R)$  ist endlich und mit der Regulatorabschätzung aus dem ersten Schritt erhält man eine Schranke  $S \in \mathbb{N}$  mit  $(U(R) : U) \leq S$ . Falls es keine Primzahl  $p$  unterhalb der Indexschranke mehr gibt, so dass die Gruppe der unabhängigen Einheiten  $U$  echt in ihrer  $p$ -maximalen Obergruppe  $U_p := \{x \in U(R) \mid \exists \nu \in \mathbb{N} \text{ mit } x^{p^\nu} \in U\}$  enthalten ist, handelt es sich bei  $U$  um die ganze Einheitengruppe  $U(R)$  und die Erzeuger von  $U$  sind unser gesuchtes Grundeinheitensystem. Man erreicht diesen Fall nun, indem man schrittweise für die Primzahlen  $p$  unterhalb der Indexschranke  $S$  die  $p$ -maximale Obergruppe  $U_p$  von  $U$  mit ihren Erzeugern  $\langle \tilde{\zeta}, \eta_1, \dots, \eta_r \rangle$  berechnet. Falls diese echt größer ist, nimmt man für  $U$  im nächsten Schritt  $\langle \tilde{\zeta}, \eta_1, \dots, \eta_r \rangle$  und setzt das Verfahren mit den Primzahlen unterhalb der modifizierten Indexschranke  $S = \lfloor \frac{S}{(U_p : U)} \rfloor$  fort.

Wir können die  $p$ -maximalen Obergruppen berechnen, indem wir mit dem Auszählalgorithmus bezüglich einer speziellen quadratischen Form  $T_{2,\lambda}$  ermitteln, ob es für

$m_0, \dots, m_r \in \{0, \dots, p-1\}$ ,  $m_1 + \dots + m_r > 0$  eine Lösung  $\eta \in U(R)$  der folgenden Gleichung gibt:

$$\eta^p = \zeta^{m_0} \cdot \varepsilon_1^{m_1} \dots \varepsilon_r^{m_r}.$$

Gibt es eine solche Lösung, ist  $\eta^p$  ein Element in  $U$ , dessen  $p$ -te Wurzel nicht in  $U$  liegt, sondern nur in  $U_p$ . Dann ist  $U$  nicht  $p$ -maximal. Durch Hinzunahme solcher Lösungen  $\eta$  zu  $U$  und der Berechnung eines minimalen Erzeugendensystems von  $\langle \eta, \varepsilon_1, \dots, \varepsilon_r \rangle$  mit dem MLLL-Algorithmus können wir dann das Erzeugendensystem der  $p$ -maximalen Obergruppe  $U_p$  bestimmen.

## 1.2 Berechnung von Grundeinheiten in drei Schritten

*Das soeben dargestellte Vorgehen ist sehr aufwändig, da man für die  $p^r$ -Möglichkeiten von  $m_1, \dots, m_r$  jeweils eine quadratische Form auszählen muss. Für eine schnellere Ermittlung der  $p$ -maximalen Obergruppen (wie in [Wil93, S.38 ff] dargestellt) braucht man die Voraussetzung, dass die Ordnung, deren Einheiten zu berechnen sind, die Maximalordnung ist. In [Wil93, Abschnitt 4.2.] wird eine Methode dargestellt, wie man aus den Grundeinheiten der Maximalordnung die Grundeinheiten einer beliebigen Ordnung gewinnt, so dass man diesen Umweg über die Einheiten der Maximalordnung ohne Effizienzeinbuße nehmen kann.*



## 2 Unabhängige Einheiten nach Dirichlet

In Anlehnung an die Darstellung in [Poh93] und [Wil93] wird das Vorgehen zur Berechnung von unabhängigen Einheiten, welches wir als *Dirichlets Methode* bezeichnen wollen, in den ersten zwei Abschnitten dieses Kapitels beschrieben. Im ersten Abschnitt befassen wir uns mit der Motivation und der genauen Durchführung der Konstruktion von sogenannten *Konjugiertenfolgen*. Im zweiten Abschnitt betrachten wir die Berechnung von Einheiten als Quotienten von assoziierten Elementen der Konjugiertenfolgen. Von diesen Grundbestandteilen ausgehend kann man innerhalb des Verfahrens verschiedene Strategien und Methoden wählen. Im dritten Abschnitt untersuchen wir alternative Methoden zur Konstruktion der Konjugiertenfolgen und im vierten Abschnitt des Kapitels beschreiben wir die Möglichkeit, die Konjugiertenrichtungen zu variieren.

### 2.1 Konstruktion von Konjugiertenfolgen

Die Grundidee der Methode von Dirichlet ergibt sich aus dem folgenden Lemma, nach dem für Mengen von Einheiten, deren Konjugiertenbeträge unterschiedliche Bedingungen erfüllen, Unabhängigkeit gewährleistet ist.

**Lemma 2.1.** *Jede  $r$ -elementige Teilmenge aus  $\{\varepsilon_1, \dots, \varepsilon_{r_1+r_2}\} \subseteq U(R)$  mit der Eigenschaft, dass für alle  $i \in \{1, \dots, r_1 + r_2\}$  jeweils gilt*

$$\begin{aligned} \left| \varepsilon_i^{(i)} \right| &\geq 1 \quad \text{und} \\ \left| \varepsilon_i^{(j)} \right| &< 1 \quad \text{für alle } j \in \{1, \dots, r_1 + r_2\} \setminus \{i\} \end{aligned} \tag{2.1}$$

*ist ein maximales System von unabhängigen Einheiten in  $R$ .*

Beweis: Wir zeigen zunächst, dass Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  mit Eigenschaft (2.1) unabhängig sind. Dazu betrachten wir die entsprechenden Vektoren  $L(\varepsilon_1), \dots, L(\varepsilon_r)$ . Angenommen die Einheiten seien abhängig, dann sind die Vektoren linear abhängig über  $\mathbb{R}$  (Satz 1.5). Aus der Anordnung dieser  $r$  Vektoren in einer  $r \times r$ -Matrix und der Tatsache, dass der Zeilenrang dem Spaltenrang entspricht, schließen wir

## 2 Unabhängige Einheiten nach Dirichlet

auf die Existenz von  $\lambda_1, \dots, \lambda_r \in \mathbb{R}$  mit mindestens einem  $\lambda_i \neq 0$ , so dass  $\sum_{i=1}^r \lambda_i c_i \log(|\varepsilon_l^{(i)}|) = 0$  für alle  $l \in \{1, \dots, r\}$ . Wähle  $k \in \{1, \dots, r\}$  mit  $|\lambda_k| = \max\{|\lambda_i| : 1 \leq i \leq r\}$ . Da man beide Seiten der Gleichung mit  $-1$  multiplizieren kann, gelte ohne Beschränkung der Allgemeinheit  $|\lambda_k| = \lambda_k$ . Dann folgt

$$\begin{aligned} 0 &= \sum_{i=1}^r \lambda_i c_i \log(|\varepsilon_k^{(i)}|) = \sum_{\substack{i=1 \\ i \neq k}}^r \lambda_i c_i \underbrace{\log(|\varepsilon_k^{(i)}|)}_{<0} + \lambda_k c_k \log(|\varepsilon_k^{(k)}|) \\ &\geq \sum_{\substack{i=1 \\ i \neq k}}^r \lambda_k c_i \log(|\varepsilon_k^{(i)}|) + \lambda_k c_k \log(|\varepsilon_k^{(k)}|) \\ &= \lambda_k \left( \sum_{i=1}^r c_i \log(|\varepsilon_k^{(i)}|) \right) = -\lambda_k c_{r_1+r_2} \underbrace{\log(|\varepsilon_k^{(r_1+r_2)}|)}_{<0} > 0. \end{aligned}$$

Es ergibt sich also ein Widerspruch. Zum Beweis der Maximalität des Systems unabhängiger Einheiten kann nun Korollar 1.6 herangezogen werden.  $\square$

Das Konzept einer Folge von unabhängigen Einheiten, die sich hinsichtlich bestimmter Konjugierter unterscheiden, wird in [Poh93] verallgemeinert, um unter anderem die Einheiten aus der Regulatorberechnung miteinbeziehen zu können. Lemma 2.1 garantiert die Unabhängigkeit der zugehörigen Einheiten nur für *einfache* Aufteilungen der Konjugiertenindexmenge  $\{1, \dots, r_1 + r_2\}$  in disjunkte Teilmengen  $I := \{i\}$  und  $J := \{1, \dots, r_1 + r_2\} \setminus \{i\}$ . Man kann jedoch auch andere Aufteilungen betrachten, dann ist die Unabhängigkeit aber sukzessive durch eine bestimmte Wahl von  $(I, J)$  zu sichern. Bevor wir das näher ausführen, definieren wir das Objekt der Diskussion.

**Definition 2.2.** *Ein Paar von Mengen  $(I, J)$  nennen wir **Konjugiertenrichtung**, falls  $I$  und  $J$  disjunkte Teilmengen von  $\{1, \dots, r_1 + r_2\}$  sind und  $1 \leq \#I \leq r$  gilt. Eine Konjugiertenrichtung  $(I, J)$  mit der Eigenschaft  $\#I = 1$  nennen wir **einfache Konjugiertenrichtung**.*

Analog zum Fall der einfachen Konjugiertenrichtungen aus Lemma 2.1 ordnen wir nun einer Aufteilung von Konjugiertenindizes  $(I, J)$  eine Einheit zu, die bezüglich der jeweiligen Konjugiertenindizes bestimmte Betragseigenschaften hat.

**Definition 2.3.** *Eine Einheit  $\varepsilon$  nennen wir **Einheit zu einer Konjugiertenrichtung**  $(I, J)$ , wenn gilt:*

$$|\varepsilon^{(i)}| \geq 1 \quad \forall i \in I \tag{2.2}$$

$$|\varepsilon^{(j)}| < 1 \quad \forall j \in J. \tag{2.3}$$

## 2.1 Konstruktion von Konjugiertenfolgen

Wenn wir nun wissen, wie man eine Einheit zu einer Konjugiertenrichtung konstruiert, ist im Fall einfacher Konjugiertenrichtungen klar, wie man vorgeht, um  $r$  unabhängige Einheiten zu finden: Man wählt eine  $r$ -elementige Teilmenge  $\mathcal{J}$  der Indexmenge  $\{1, \dots, r_1 + r_2\}$ , lässt  $i$  durch die Teilmenge  $\mathcal{J}$  laufen und konstruiert zu jeder dazugehörigen einfachen Konjugiertenrichtung  $(\{i\}, \{1, \dots, r_1 + r_2\} \setminus \{i\})$  jeweils eine Einheit. Dann garantiert uns Lemma 2.1 die Unabhängigkeit dieser  $r$  verschiedenen Einheiten.

Im Falle nicht-einfacher Konjugiertenrichtungen müssen wir die Unabhängigkeit der zugehörigen Einheiten durch eine günstige Wahl der Konjugiertenrichtungen anhand der  $L$ -Vektoren beeinflussen. Wie das geschehen kann, erörtern wir in Abschnitt 2.4.

**Definition:** Eine Menge von  $r$  Konjugiertenrichtungen  $\{(I_1, J_1), \dots, (I_r, J_r)\}$ , so dass die zu den Konjugiertenrichtungen gehörigen Einheiten unabhängig sind, nennen wir im Folgenden *gewährleistendes Konjugiertenrichtungssystem*.

### 2.1.1 Eigenschaften von Konjugiertenfolgen

Wie schon angedeutet, werden sich die Einheiten zu einer Konjugiertenrichtung als Quotienten von Folgengliedern ergeben. Wir nennen ein Tupel  $(\gamma_0, \gamma_1, \dots, \gamma_\mu)$  als Teilfolge von  $(\gamma_k)_{k \in \mathbb{N}}$  *Konjugiertenfolge* zu  $(I, J)$ , wenn die folgenden fünf Eigenschaften erfüllt sind:

- (1)  $\gamma_0 = 1$ ,
- (2)  $\gamma_k \in R \setminus \{0\} \forall k \in \mathbb{Z}^{>0}$ ,
- (3)  $|\gamma_k^{(i)}| \geq |\gamma_{k-1}^{(i)}| \forall i \in I, \forall k \in \mathbb{Z}^{>0}$ ,
- (4)  $|\gamma_k^{(j)}| < |\gamma_{k-1}^{(j)}| \forall j \in J, \forall k \in \mathbb{Z}^{>0}$ ,
- (5)  $|N(\gamma_k)| \leq C$  für eine Konstante  $C \in \mathbb{R}^{>0}, \forall k \in \mathbb{Z}^{>0}$ .

Dabei nennen wir die Elemente der Folge *Konjugiertenfolgeelemente* oder abkürzend *Dirichlet-Elemente* und  $\mu$  die *Länge der Konjugiertenfolge*.

Die Motivation für diese Definition besteht darin, dass bei Konstruktion einer Folge mit den fünf genannten Eigenschaften die Folgeelemente paarweise verschieden sind und beschränkte Norm besitzen. Nach Proposition 1.1 existieren dann Indizes  $\mu > \nu$ , so dass  $\gamma_\mu \sim \gamma_\nu$  und  $\frac{\gamma_\mu}{\gamma_\nu} \in U(R)$ . Damit ergibt sich eine Einheit  $\varepsilon \in U(R)$  zur Konjugiertenrichtung  $(I, J)$  als Quotient dieser Elemente, denn für  $\varepsilon := \frac{\gamma_\mu}{\gamma_\nu}$  sind die Bedingungen (2.2) und (2.3) erfüllt.

Das erste Folgenglied definieren wir als  $\gamma_0 := 1$  und alle weiteren Folgenglieder erhalten wir rekursiv als  $\gamma_{k+1} := \beta_k \cdot \gamma_k$  mit einem *Hilfsfolgeelement*  $\beta_k \in F$ , welches jeweils in Abhängigkeit vom bereits gegebenen Folgenglied  $\gamma_k$  und der Konjugiertenrichtung  $(I, J)$  mit folgenden Eigenschaften definiert wird:

## 2 Unabhängige Einheiten nach Dirichlet

- (i)  $\beta_k \in \frac{1}{\gamma_k} R \setminus \{0\}$ ,
- (ii)  $|\beta_k^{(i)}| \geq 1 \forall i \in I$ ,
- (iii)  $|\beta_k^{(j)}| < 1 \forall j \in J$ ,
- (iv)  $|N(\beta_k)| \cdot |N(\gamma_k)| \leq C$ .

Wir sehen, dass ein solchermaßen definiertes  $\gamma_{k+1}$  die Bedingungen (1) bis (5) erfüllt. Die Multiplikation mit den Konjugiertenbeträgen von  $\beta_k$  verringert beziehungsweise vergrößert die Konjugiertenbeträge von  $\gamma_{k+1}$  im Verhältnis zu denen von  $\gamma_k$  für die Mengen  $I$  beziehungsweise  $J$ . Die Elemente der *Hilfsfolge*  $(\beta_k)_{k \in \mathbb{N}}$  werden gerade so konstruiert, dass sämtliche Folgenglieder von  $(\gamma_k)_{k \in \mathbb{N}}$  durch ein  $C$  beschränkt sind.

### 2.1.2 Konstruktion der Hilfsfolgeelemente

Im Folgenden behalten wir im Hinterkopf, dass unsere Konstruktion sich auf  $(I, J)$  bezieht und verzichten weiterhin auf die explizite Indizierung der Folgeelemente. Um für  $\beta_k$  die Erfüllung der vier oben genannten Eigenschaften zu gewährleisten, wird  $\beta_k$  als Element des Moduls  $M_k := \frac{1}{\gamma_k} R_k$  konstruiert, welches bezüglich einer speziell gewichteten, positiv definiten, quadratischen Form  $T_{2,\lambda}$  beschränkt ist. Die Schranke hängt dabei von  $\gamma_k$  und einem zu wählenden  $\hat{C} \in \mathbb{R}^{>0}$  ab. Bei der Wahl von  $\hat{C}$  und der davon abhängigen Gewichte  $\lambda \in \mathbb{R}^n$  hat man grundsätzlich verschiedene Optionen. Wir werden jetzt zunächst die Zusammenhänge zwischen der Wahl der Gewichte und den Bedingungen für die konstruierten Hilfsfolgen herausarbeiten. Im nächsten Abschnitt stellen wir die in [Poh93] vorgestellte Konstruktion der  $\beta_k$  mit LLL-Reduktion und die damit einhergehende konkrete Wahl der Schranke  $\hat{C}$  dar. Eine andere Möglichkeit ist die Konstruktion der  $\beta_k$  mit Hilfe des Auszählalgorithmus, die wir in Abschnitt 2.3 erarbeiten.

Zunächst benötigen wir zu der gegebenen Konjugiertenrichtung  $(I, J)$  eine komplette Aufteilung der Indexmenge  $\{1, \dots, r_1 + r_2\}$  in disjunkte Teilmengen  $\tilde{I}$  und  $\tilde{J}$  mit den Eigenschaften  $I \subseteq \tilde{I}$  und  $J \subseteq \tilde{J}$  sowie  $\#\tilde{I} + \#\tilde{J} = r + 1$ . Praktisch werden wir uns immer mit der Wahl  $\tilde{I} := I$  und  $\tilde{J} := \{1, \dots, r_1 + r_2\} \setminus I$  begnügen.

**Bemerkung:** *Es sei darauf hingewiesen, dass man durchaus andere Möglichkeiten hat,  $(\tilde{I}, \tilde{J})$  zu wählen. Unser Anliegen wird aber der Vergleich „ceteris paribus“ zweier verschiedener Suchmethoden entlang der Konjugiertenfolgen zu gegebenen Konjugiertenrichtungen sein. Deshalb wollen wir diese Wahl hier festhalten (vergleiche [Wil93, Bemerkung 3.5]).*

## 2.1 Konstruktion von Konjugiertenfolgen

Entsprechend der gegebenen Konjugiertenrichtung  $(I, J)$  und der daraus resultierenden Konjugiertenrichtung  $(\tilde{I}, \tilde{J})$  unterteilen wir die Komponenten eines Gewichtungsvektors  $\underline{\lambda} \in \mathbb{R}^n$ :

$$\lambda_\nu := \begin{cases} \lambda_{\tilde{I}} & \text{für } \nu \in \tilde{I} \\ \lambda_{\tilde{J}} & \text{für } \nu \in \tilde{J} \end{cases} \quad (1 \leq \nu \leq r_1 + r_2), \quad (2.4)$$

$$\lambda_\mu := \lambda_{\mu-r_2} \quad (r_1 + r_2 < \mu \leq n = r_1 + 2r_2). \quad (2.5)$$

Die Häufigkeit der im Gewichtungsvektor auftretenden  $\lambda_{\tilde{I}}$  nennen wir

$$\iota := \#\{i \in \tilde{I} : 1 \leq i \leq r_1\} + 2 \cdot \#\{i \in \tilde{I} : r_1 \leq i \leq r_1 + 1\}. \quad (2.6)$$

Ziel ist es nun, zum Beispiel durch Auszählen oder LLL-Reduktion ein Element  $\beta_k \in M_k$  zu berechnen, für welches die durch

$$T_{2,\underline{\lambda}}(x) := \sum_{i=1}^n \frac{1}{\lambda_i^2} |x^{(i)}|^2 \quad (2.7)$$

definierte *Länge* in Abhängigkeit von  $\gamma_k$  und zu bestimmendem  $\hat{C} \in \mathbb{R}^{>0}$  beschränkt ist. Angenommen es sei ein  $\beta_k \in \frac{1}{\gamma_k} R \setminus \{0\}$  mit der Eigenschaft

$$\boxed{T_{2,\underline{\lambda}}(\beta_k) \leq \frac{\hat{C}^2}{|N(\gamma_k)|^{\frac{2}{n}}}} \quad (2.8)$$

konstruiert worden. Dann schließt man für die Konjugiertenbeträge, dass

$$|\beta_k^{(i)}| < \lambda_i \cdot \left( \frac{\hat{C}^2}{|N(\gamma_k)|^{\frac{2}{n}}} \right)^{\frac{1}{2}} = \lambda_{\tilde{I}} \cdot \frac{\hat{C}}{|N(\gamma_k)|^{\frac{1}{n}}} \quad \forall i \in \tilde{I}, \quad (2.9)$$

$$|\beta_k^{(j)}| < \lambda_j \cdot \left( \frac{\hat{C}^2}{|N(\gamma_k)|^{\frac{2}{n}}} \right)^{\frac{1}{2}} = \lambda_{\tilde{J}} \cdot \frac{\hat{C}}{|N(\gamma_k)|^{\frac{1}{n}}} \quad \forall j \in \tilde{J} \quad (2.10)$$

gilt, wodurch wir die gewünschten Eigenschaften (ii)- (iv) für die Konjugierten von  $\beta_k$  anhand der Wahl des Gewichtungsvektors  $\underline{\lambda}$  gewährleisten wollen.

Als erste Konsequenz ergibt sich nun die Beschränkung von  $|N(\beta_k)| \cdot |N(\gamma_k)|$ , also Bedingung (iv) an  $\beta_k$ , denn es gilt:

$$\begin{aligned} |N(\beta_k)| &= \prod_{i=1}^n |\beta_k^{(i)}| \leq \left( \lambda_{\tilde{I}} \frac{\hat{C}}{|N(\gamma_k)|^{\frac{1}{n}}} \right)^\iota \left( \lambda_{\tilde{J}} \frac{\hat{C}}{|N(\gamma_k)|^{\frac{1}{n}}} \right)^{n-\iota} \\ &\Rightarrow |N(\beta_k)| \cdot |N(\gamma_k)| \leq \lambda_{\tilde{I}}^\iota \lambda_{\tilde{J}}^{n-\iota} \hat{C}^n. \end{aligned} \quad (2.11)$$

## 2 Unabhängige Einheiten nach Dirichlet

Für die Normbetragsschranke  $C$  der Konjugiertenfolgeelemente aus (iv) und (5) kann also der rechtsseitige Ausdruck aus (2.11) gewählt werden, der allerdings noch vom  $\underline{\lambda}$ -Gewichtungsvektor abhängt. Da mit den Gewichten die Erfüllung der Eigenschaften (ii) und (iii) von  $\beta_k$  in Abhängigkeit von  $\gamma_k$  gesteuert werden soll, die Schranke  $C$  aber unabhängig von  $\gamma_k$  sein soll, sind diese so zu wählen, dass sie sich in dem rechtsseitigen Ausdruck gegenseitig aufheben. Für eine Konstante  $\delta \in \mathbb{R}$  setzen wir  $\lambda_{\tilde{I}} := \delta^x$  und  $\lambda_{\tilde{J}} := \delta^y$  und bestimmen die Exponenten so, dass  $\lambda_{\tilde{I}}^\iota \lambda_{\tilde{J}}^{n-\iota} = 1$  gilt. Dann muss  $(\delta^x)^\iota (\delta^y)^{n-\iota} = \delta^0$  gelten und damit  $x\iota + y(n-\iota) = 0$ . Daraus ergibt sich  $y = \frac{x\iota}{\iota-n}$ . Mit der vereinfachenden Wahl  $x = 1$  ergibt sich dann für die Gewichte:

$$\lambda_{\tilde{I}} := \delta, \quad (2.12)$$

$$\lambda_{\tilde{J}} := \delta^{\frac{\iota}{\iota-n}}. \quad (2.13)$$

Nun bleibt noch,  $\delta$  so zu bestimmen, dass die Ungleichungsrelationen der Konjugiertenbeträge für  $\beta_k$  bezüglich 1 erfüllt sind:

(1) Die Abschätzung der Konjugiertenbeträge von  $\beta_k$  für die Indizes aus  $\tilde{I}$  erhalten wir aufgrund der Tatsache, dass  $|N(\alpha)| \geq 1$  für Elemente  $\alpha$  aus  $R \setminus \{0\}$  gilt. Aus  $\beta_k \in \frac{1}{\gamma_k} R \setminus \{0\}$  folgt  $\gamma_k \beta_k \in R \setminus \{0\}$  und daher

$$|N(\beta_k)| \geq \frac{1}{|N(\gamma_k)|}. \quad (2.14)$$

Für alle Konjugiertenindizes  $i \in \tilde{I}$  können wir also wie folgt abschätzen:

$$\begin{aligned} |\beta_k^{(i)}| &= |N(\beta_k)| \prod_{\substack{j=1 \\ j \neq i}}^n \frac{1}{|\beta_k^{(j)}|} \stackrel{2.14}{\geq} \frac{1}{|N(\gamma_k)|} \left( \frac{|N(\gamma_k)|^{\frac{1}{n}}}{\lambda_{\tilde{I}} \hat{C}} \right)^{\iota-1} \cdot \left( \frac{|N(\gamma_k)|^{\frac{1}{n}}}{\lambda_{\tilde{J}} \hat{C}} \right)^{n-\iota} \\ &= \frac{1}{|N(\gamma_k)|} \frac{|N(\gamma_k)|^{\frac{1}{n}(n-1)}}{\hat{C}^{n-1} \cdot \lambda_{\tilde{I}}^{\iota-1} \cdot \lambda_{\tilde{J}}^{n-\iota}} = \frac{1}{|N(\gamma_k)|^{\frac{1}{n}} \hat{C}^{n-1} \cdot \delta^{\iota-1} \delta^{\left(\frac{\iota}{\iota-n}\right)(n-\iota)}} = \frac{\delta}{|N(\gamma_k)|^{\frac{1}{n}} \hat{C}^{n-1}}. \end{aligned} \quad (2.15)$$

Für alle  $i \in \tilde{I}$  soll  $|\beta_k^{(i)}| \geq 1$  gelten. Das ist unter Berücksichtigung der in (2.15) gegebenen Ungleichung bereits erfüllt, wenn:

$$\frac{\delta}{|N(\gamma_k)|^{\frac{1}{n}} \hat{C}^{n-1}} \geq 1. \quad (2.16)$$

Also sollte  $\delta$  mindestens gleich

$$D := |N(\gamma_k)|^{\frac{1}{n}} \hat{C}^{n-1} \quad (2.17)$$

sein, um (2.16) und damit  $|\beta_k^{(i)}| \geq 1$  für alle  $i \in \tilde{I}$  zu gewährleisten.

## 2.1 Konstruktion von Konjugiertenfolgen

(2) Des Weiteren soll  $|\beta_k^{(j)}| < 1$  für alle  $j \in \tilde{J}$  gelten. Mit (2.10) erkennen wir, dass dies die Gültigkeit folgender Ungleichung gewährleisten würde:

$$1 \geq \lambda_{\tilde{J}} \cdot \frac{\hat{C}}{|N(\gamma_k)|^{\frac{1}{n}}}. \quad (2.18)$$

Somit erhalten wir eine weitere Bedingung für die Wahl von  $\delta$  durch die folgenden Umformungen:

$$\frac{|N(\gamma_k)|^{\frac{1}{n}}}{\hat{C}} \geq \lambda_{\tilde{J}} = \delta^{\frac{\iota}{\iota-n}} \Leftrightarrow \delta^{\frac{\iota}{n-\iota}} \geq \frac{\hat{C}}{|N(\gamma_k)|^{\frac{1}{n}}} \Leftrightarrow \delta \geq \left( \frac{\hat{C}}{|N(\gamma_k)|^{\frac{1}{n}}} \right)^{\frac{n-\iota}{\iota}}.$$

Das bedeutet, unser  $\delta$  muss mindestens gleich

$$d := \left( \frac{\hat{C}}{|N(\gamma_k)|^{\frac{1}{n}}} \right)^{\frac{n-\iota}{\iota}} \quad (2.19)$$

sein, damit (2.18) und  $|\beta_k^{(j)}| < 1 \forall j \in \tilde{J}$  gilt.

Diese zweite Bedingung an  $\delta$  ist schwächer als die obenstehende, denn es gilt  $D \geq d$ . Mit  $\iota - 1 \geq 0$  und  $n/\iota > 1$  sieht man, dass

$$D/d = |N(\gamma_k)|^{\frac{1}{\iota} \hat{C}^{\frac{n}{\iota}(\iota-1)}} \geq |N(\gamma_k)|^{\frac{1}{\iota}} \geq 1$$

gilt. Also können wir mit der Wahl von  $\delta = D$  die Erfüllung aller Bedingungen für das konstruierte Element  $\beta_k$  gewährleisten.

Unbestimmt ist jetzt nur noch die Schranke  $\hat{C}$ . Wir stellen im Anschluss die in [Poh93] ausgeführte Idee dar, bei der die Schranke  $\hat{C}$  entsprechend der LLL-Reduktion gesetzt wird.

**Konstruktion mit LLL**

Zu berechnen ist eine Konjugiertenfolge  $(\gamma_k)_{k \in \mathbb{N}}$  zur Konjugiertenrichtung  $(I, J)$ . Im vorletzten Abschnitt haben wir gesehen, dass wir die Elemente der Konjugiertenfolge sukzessive konstruieren, in dem wir zu jedem bereits berechneten Dirichlet-Element  $\gamma_k$  ein  $\beta_k$  mit

$$T_{2,\underline{\lambda}}(\beta_k) \leq \frac{\hat{C}^2}{|N(\gamma_k)|^{\frac{2}{n}}} \quad (2.8)$$

berechnen. Dabei erfolgt die Wahl der Gewichtungskomponenten von  $\underline{\lambda}$  wie im vorigen Abschnitt und gewährleistet wie wir dort gesehen haben im Zusammenspiel mit Bedingung (2.8) die Erfüllung aller definierenden Eigenschaften der  $\gamma_k$ .

In diesem Abschnitt berechnen wir  $\beta_k$  als erstes Element einer LLL-reduzierten Basis  $b_1, \dots, b_n$  des Moduls  $M_k := \frac{1}{\gamma_k}R$  (siehe Abschnitt 1.1.3). Für die quadratische, positiv definite Form  $T_{2,\underline{\lambda}}$  gilt:

$$\det(T_{2,\underline{\lambda}}) = \frac{|\text{disc}(R)|}{|N(\gamma_k)|^2} \quad (2.20)$$

und für das erste Basiselement  $b_1 = \beta_k$  gilt:

$$\|b_1\|_{\underline{\lambda}} \leq 2^{\frac{1}{4}(n-1)} \left( \sqrt{\det(T_{2,\underline{\lambda}})} \right)^{\frac{1}{n}} \quad (2.21)$$

$$\Rightarrow T_{2,\underline{\lambda}}(\beta_k) \leq 2^{\frac{1}{2}(n-1)} \det(T_{2,\underline{\lambda}})^{\frac{1}{n}} = 2^{\frac{1}{2}(n-1)} \frac{|\text{disc}(R)|^{\frac{1}{n}}}{|N(\gamma_k)|^{\frac{2}{n}}}. \quad (2.22)$$

Damit ist  $\hat{C}$  bei dieser Konstruktion festgelegt durch

$$\hat{C} := 2^{\frac{1}{4}(n-1)} |\text{disc}(R)|^{\frac{1}{2n}}. \quad (2.23)$$

Dann sind durch die Bedingung (2.8) alle gewünschten Ungleichungseigenschaften für die Konjugierten von  $\beta_k$  erfüllt. Für die Normbetragschranke  $C$  der Konjugiertenfolge  $(\gamma_k)_{k \in \mathbb{N}}$  ergibt sich mit der Folgerung  $|N(\beta_k)| \cdot |N(\gamma_k)| \leq \hat{C}^n$  in (2.11) dann:

$$C := \hat{C}^n = 2^{\frac{1}{4}n(n-1)} |\text{disc}(R)|^{\frac{1}{2}}. \quad (2.24)$$

Wir geben zusammenfassend den Algorithmus (Algorithmus 3) an, mit dem eine Konjugiertenfolge  $(\gamma_k)_{k \in \mathbb{N}}$  zu  $(I, J)$  berechnet werden kann. Die hier angegebene Version berechnet eine Konjugiertenfolge  $(\gamma_0, \gamma_1, \dots, \gamma_\mu)$  der Länge  $\mu$  unter Berücksichtigung eventuell bereits berechneter Dirichlet-Elemente  $\gamma_0, \gamma_1, \dots, \gamma_l$ .

## 2.1 Konstruktion von Konjugiertenfolgen

**Bemerkung 2.4.** Die Bedingung (2.16) und damit die Wahl von  $\delta$  als  $D$ , aus der wir die Gültigkeit von  $|\beta_k^{(i)}| \geq 1$  für  $i \in \tilde{I}$  herleiten, ist schärfer als nötig. Praktisch stellt die Wahl von  $\delta = D$  bei der Konstruktion der Hilfsfolgeelemente durch die resultierende Größe der  $\lambda$ -Gewichte ein Problem hinsichtlich der benötigten Präzision und Rechenzeit dar. Deshalb sollte nach [Wil93] zu Anfang der Konstruktion für  $\delta$  die kleinere Schranke  $d$  gewählt werden. Dann gilt alle  $j \in \tilde{J}$  bereits die geforderte Bedingung  $|\beta_k^{(j)}| < 1$ . Getestet werden muss dann, ob es ein  $i \in \tilde{I}$  mit  $|\beta_k^{(i)}| < 1$  gibt. Wenn dies der Fall ist, wird  $\delta$  verdoppelt und die Konstruktion mit diesem Wert erneut durchgeführt, bis das damit konstruierte  $\beta_k$  Bedingung (ii) erfüllt. Die Empfehlung, die man aus experimentellen Untersuchungen ableiten kann, legt in bestimmten Fällen eine erhöhte Wahl von  $\delta$  zu Anfang jeder Konstruktion nahe. Wir haben für das Verhältnis von  $D$  und  $d$  die Abschätzung  $D/d \geq |N(\gamma_k)|^{\frac{1}{\iota}}$  angegeben. Sobald die Konjugiertenrichtung so gewählt wird, dass  $\iota > 1$  ist, geht ein Faktor  $\hat{C}^m$  mit  $m \in \mathbb{Q}^{>1}$  in die untere Schranke des Quotienten ein und  $D$  fällt in Abhängigkeit vom Körpergrad erheblich größer aus als  $d$ . In Fällen, in denen  $\iota$  groß ist, ist es zur Verringerung des Konstruktionsaufwands für ein Element zweckmäßig,  $\delta$  erhöht zu initialisieren. Wir empfehlen  $\delta := \nu \cdot d$  mit

$$\nu := \begin{cases} 2^{\frac{\iota-1}{2}} & \text{falls } \iota \text{ ungerade} \\ 2^{\frac{\iota}{2}} & \text{falls } \iota \text{ gerade} \end{cases} \quad (2.25)$$

zu wählen, um zu viele Konstruktionen von Modulelementen, die Bedingung (ii) nicht erfüllen, zu verhindern. Durch die Veränderung der Gewichte kann dies allerdings nachteilige Auswirkungen auf den Konstruktionsaufwand und die Eigenschaften der Konjugiertenfolge hinsichtlich des frühen Auffindens von Einheiten haben (siehe im Anhang Tabelle 5.4). Sofern nichts anderes gesagt wird, rechnen wir in den Beispielen mit der klassischen Wahl von  $\delta$ , also  $\nu = 1$ .

---

**Algorithmus 3** : Konstruktion einer Konjugiertenfolge der Länge  $\mu$  zur Konjugiertenrichtung  $(I, J)$  mit LLL

---

**Eingabe** : Ordnung  $R$ , Konjugiertenrichtung  $(I, J)$ , Folge

$L = (1, \gamma_1, \dots, \gamma_l)$  bereits berechneter Dirichlet-Elemente zu  $(I, J)$ , Länge  $\mu$  der zu berechnenden Konjugiertenfolge, Wert  $\nu$  der  $\delta$ -Erhöhung

**Ausgabe** : Konjugiertenfolge  $(\gamma_k)_{k \in \mathbb{N} \leq \mu} \in R$  zu  $(I, J)$

```

1   $(\tilde{I}, \tilde{J}) \leftarrow (I, \{1, \dots, r_1 + r_2\} \setminus I)$ 
2   $\hat{C} \leftarrow 2^{\frac{1}{4}(n-1)} |\text{disc}(R)|^{\frac{1}{2n}}$ 
3  if  $L = \emptyset$  then
4  |    $k \leftarrow 0, \gamma_k \leftarrow 1$ 
5  |    $L \leftarrow (\gamma_k)$ 
6  else
7  |    $k \leftarrow l, \gamma_k \leftarrow \gamma_l$ 
8  endif
9  while  $k < \mu$  do
10 |    $flag \leftarrow false$ 
11 |    $\delta \leftarrow \nu \cdot d$  // Zur Wahl von  $d$  siehe (2.19)
12 |   while  $flag = false$  do
13 |   |   Setze  $\underline{\lambda} \in \mathbb{R}^n$  mit  $\lambda_\nu \leftarrow \begin{cases} \delta & \text{für } \nu \in \tilde{I} \\ \delta^{\frac{\nu}{n}} & \text{für } \nu \in \tilde{J} \end{cases} \quad (1 \leq \nu \leq r_1 + r_2)$ 
14 |   |   und  $\lambda_{\mu+r_2} \leftarrow \lambda_\mu \quad \text{für } (r_1 < \mu \leq r_1 + r_2)$ 
15 |   |    $\beta_k \leftarrow b_1$  mit  $\{b_1, \dots, b_n\}$  bezüglich  $T_{2, \underline{\lambda}}$ -Norm LLL-reduzierte
16 |   |   Basis des Moduls  $M_k = \frac{1}{\gamma_k} R$  (Berechnung siehe Algorithmus 1).
17 |   |    $flag \leftarrow true$ 
18 |   |   for  $i \in \tilde{I}$  do
19 |   |   |   if  $|\beta_k^{(i)}| < 1$  then
20 |   |   |   |    $flag \leftarrow false$ 
21 |   |   |   |    $\delta \leftarrow 2\delta$ 
22 |   |   |   |   break for // neue Konstruktion mit erhöhtem  $\delta$ 
23 |   |   |   endif
24 |   |   endfor
25 |   |    $\gamma_{k+1} \leftarrow \beta_k \cdot \gamma_k$ 
26 |   |    $L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1})$ 
27 |   |    $k \leftarrow k + 1$ 
28 |   endwhile
29 return  $L = (\gamma_k)_{k \in \mathbb{N} \leq \mu}$ 

```

---

## 2.1 Konstruktion von Konjugiertenfolgen

**Bemerkung 2.5.** Die Hilfsfolgeelemente werden als Elemente eines Moduls berechnet, dessen Basis von den vorhergehenden Konjugiertenfolgeelementen abhängt. (1) Wir benutzen eine hinsichtlich der vorzunehmenden LLL-Reduktion günstige Basis des Moduls (wie in [Wil93] auf S. 23 beschrieben): Sei  $\omega_1, \dots, \omega_n$  die  $\mathbb{Z}$ -Basis von  $R$ . Dann ist  $\frac{\omega_1}{\gamma_k}, \dots, \frac{\omega_n}{\gamma_k}$  eine Basis von  $M_k$ . Zu  $\gamma_k$  berechnen wir  $d_k \in \mathbb{N}$  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  $\omega_1, \dots, \omega_n$ , so dass  $\tilde{\gamma}_k(\omega_1, \dots, \omega_n) = (\omega_1, \dots, \omega_n)A_k$  ist, gilt

$$\frac{1}{\gamma_k}(\omega_1, \dots, \omega_n) = \frac{1}{d_k}(\omega_1, \dots, \omega_n)A_k.$$

Mit Hilfe einer Matrix  $T \in GL(n, \mathbb{Z})$ , so dass  $A_k T$  LLL-reduziert ist, definieren wir

$$(\alpha_1, \dots, \alpha_n) := \frac{1}{d_k}(\omega_1, \dots, \omega_n)A_k T. \quad (2.26)$$

Dann bildet  $\alpha_1, \dots, \alpha_n$  die  $\mathbb{Z}$ -Basis des Moduls  $M_k$ , die wir bei der Berechnung des gewichteten Konjugiertengitters verwenden.

(2) Die Benutzung von  $\alpha_1, \dots, \alpha_n$  aus (1) statt  $\frac{\omega_1}{\gamma_k}, \dots, \frac{\omega_n}{\gamma_k}$  als Ausgangsbasis von  $M_k$  ist hinsichtlich der Verringerung des Aufwands und der bei der folgenden LLL-Reduktion benötigten Präzision unerlässlich. Denn die Konstruktion eines Hilfsfolgeelements erfordert mit zunehmender Länge der Konjugiertenfolge mehr Operationen, da die Koeffizientenbeträge der Basisdarstellung der Konjugiertenfolgeelemente kontinuierlich größer werden (ebenso nimmt die Anzahl der signifikanten Stellen der Konjugiertenabsolutbeträge der Konjugiertenfolgeelemente zu, da diese größer bzw. kleiner werden, wenn der Konjugiertenindex in  $I$  bzw.  $J$  ist). Diese Dynamik gilt es abzufangen und dabei hilft uns die LLL-Reduktion der Spalten der Darstellungsmatrix (ganzzahlig). Wählen wir die Basis des Moduls  $M_k$  wie in (1) beschrieben, wird die Zunahme des Berechnungsaufwands auf diese Berechnung begrenzt. Die darauf aufbauende Bestimmung der bezüglich  $T_{2, \underline{\lambda}}$  LLL-reduzierten Basis von  $M_k$  (reell) braucht dann unabhängig von der erreichten Länge der Konjugiertenfolge durchschnittlich konstant viel Zeit. Der zusätzliche Aufwand durch die Berechnung von  $\alpha_1, \dots, \alpha_n$  ist wesentlich geringer als der Aufwand der Berechnung einer bezüglich  $T_{2, \underline{\lambda}}$  LLL-reduzierten Basis von  $M_k$  ohne eine solchermaßen reduzierte Basis.

(3) Fehlerfortpflanzung: Bei der Abbildung der Basiselemente des Moduls in das gewichtete Konjugiertengitter (siehe Abschnitt 1.1.3 Abbildung in (1.10)) mit reellen Koeffizienten ist auf eine ausreichend hohe Präzision zu achten. Das betrifft die Gewichte  $\underline{\lambda}$ , den Real- und Imaginärteil der Konjugierten und den Faktor  $\sqrt{2}$ . Um die präzisionsbedingten Fehler abzufangen, kann nach der Konstruktion von  $\beta_k$  zusätzlich abgefragt werden, ob für die Konjugierten  $i \in I$  gilt, dass  $|\beta_k^{(i)}| \geq 1$  ist. Gegebenenfalls muss die Präzision erhöht werden.

Neben der Konstruktion mit LLL bestehen noch andere Möglichkeiten, die Hilfsfolgeelemente zu konstruieren. Zur Beurteilung ihrer Güte müssen wir jedoch die Zielsetzung der Berechnung von Einheiten vor Augen haben. Wir beschreiben nun zunächst, wie aus Konjugiertenfolgen Einheiten gewonnen werden und kommen im Anschluss auf die anderen Konstruktionsmöglichkeiten zurück.

## 2.2 Berechnung als Quotienten assoziierter Dirichlet-Elemente

Wie bereits beschrieben, sucht man in der zu einer Konjugiertenrichtung  $(I, J)$  konstruierten Konjugiertenfolge  $(\gamma_k)_{k \in \mathbb{N}}$  zwei zueinander assoziierte Elemente  $\gamma_\mu$  und  $\gamma_\nu$ , um die Einheit zu der Konjugiertenrichtung als Quotienten dieser Folgeelemente zu erhalten. Ob zwei Elemente zueinander assoziiert sein können, kann durch Vergleichen der Normbeträge der Elemente geprüft werden. Das kanonische Vorgehen ist der Vergleich des Normbetrags eines jeden neuen Folgenglieds mit den Normbeträgen aller zuvor konstruierten Folgenglieder, wie im folgenden Algorithmus dargestellt:

---

**Algorithmus 4** : Berechnung der Einheit zu einer Konjugiertenrichtung mit Normvergleichen

---

**Eingabe** : Ordnung  $R$ , Konjugiertenrichtung  $(I, J)$

**Ausgabe** : Einheit  $\varepsilon \in U(R)$  zu der Konjugiertenrichtung  $(I, J)$

**Initialisierung**:  $k \leftarrow 0, \gamma_k \leftarrow 1, L \leftarrow (\gamma_k), \varepsilon \leftarrow 1$

**while**  $\varepsilon = 1$  **do**

Konstruiere nächstes Element  $\gamma_{k+1}$  der Konjugiertenfolge zu  $(I, J)$ :  
 Rufe dazu Algorithmus (3) mit  $(R, (I, J), L, \mu = k + 1)$  auf und setze  $\gamma_{k+1}$  als letztes Element der dort konstruierten Folge

$i \leftarrow 0$

**while**  $\varepsilon = 1$  und  $i \leq k$  **do**

**if**  $|N(\gamma_{k+1})| = |N(\gamma_i)|$  **then**

**if**  $\frac{1}{\gamma_i} \gamma_{k+1} \in R$  **then**  $\varepsilon \leftarrow \frac{\gamma_{k+1}}{\gamma_i}$  **endif**

**endif**

$i \leftarrow i + 1$

**endwhile**

$L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1}), k \leftarrow k + 1$

**endwhile**

**return**  $\varepsilon$

---

Der Algorithmus terminiert in endlicher Zeit, da es nach Proposition 1.1 nur endlich viele nicht-assozierte Elemente der Ordnung mit beschränkter Norm gibt. Man sieht allerdings, dass die Normbetragsschranke  $C = 2^{\frac{1}{4}n(n-1)} |\text{disc}(R)|^{\frac{1}{2}}$ , die

wir für alle  $(\gamma_k)_{k \in \mathbb{N}}$  zugrunde legen können, exponentiell im Körpergrad und unterproportional in der Größe der Diskriminante wächst. Unter der Annahme, dass die Normbeträge der Konjugiertenfolgeelemente unabhängig identisch verteilte Zufallsvariablen (mit Gleichverteilung auf der Menge  $\{1, \dots, C\}$ ) sind, sind bei höherem Körpergrad und größerer Diskriminante durchschnittlich entsprechend mehr Konstruktionen erforderlich bis zwei zueinander assoziierte Elemente gefunden werden. Aus der Beobachtung, dass diese Annahme in konkreten Fällen zutrifft, leiten sich die beiden Modifikationsideen ab, die wir erarbeiten wollen: In Abschnitt 2.3 werden wir eine andere Konstruktionsmethode für die Konjugiertenfolgeelemente entwickeln, bei der sich eine kleinere Schranke für die Normbeträge ergibt. Dadurch erhöht sich die Wahrscheinlichkeit, dass in einer gegebenen Menge von Dirichlet-Elementen zwei mit gleichem Normbetrag enthalten sind. In Kapitel 3 sollen neben den Quotienten zweier Dirichlet-Elemente auch andere Potenzprodukte von Dirichlet-Elementen, deren Normbetrag 1 ergibt, berücksichtigt werden.

**Bemerkung 2.6** (Kollisionssuche). *Die Menge der Normbeträge der Konjugiertenfolge ist endlich. Bei fortlaufender Konstruktion von Elementen  $\gamma_k$  geraten wir an einen Punkt, bei dem der Normbetrag des Folgenrechts dem eines früheren Folgenrechts entspricht. Wir nennen dies im Folgenden eine Kollision. Durch Modifikation<sup>1</sup> der Hilfsfolgenkonstruktion könnte erreicht werden, dass man bei der Konstruktion der Konjugiertenfolgeelemente in einen Kreislauf hinsichtlich der Normbeträge gerät. Theoretisch ermöglicht dies die Kollisionssuche in der Menge der Normbeträge mit Hilfe eines cycle-detection-Algorithmus, z.B. Hase-Igel-Algorithmus (siehe [Flo67]). Der Flaschenhals der vorgestellten Methode zur Einheitenkonstruktion ist jedoch nicht der Speicherbedarf, sondern – wegen des hohen Konstruktionsaufwands – die Rechenzeit bis zum Auffinden einer Kollision. Die sukzessive Konstruktion macht es notwendig, dass auch bei einer Suchmethode, welche nur jeweils die Normbeträge zweier Elemente vergleicht, die in der gesamten Menge der Elemente mit unterschiedlicher Schrittgröße (Zeigergeschwindigkeit) angesteuert werden, für den größeren Schritt trotzdem alle zwischen den bezeichneten Elementen liegenden Elemente konstruiert werden müssen. Bei der Implementation von Algorithmus 4 fügen wir alle Elemente und die Normbeträge aller Elemente in eine Liste ein. Wir prüfen dann, ob der Normbetrag des neu eingefügten Elements bereits einem Normbetrag aus der Liste entspricht. In MAGMA ist diese Abfrage mit `in` auf nummerierten Listen und zu Grunde liegender*

<sup>1</sup> Bei der bisher beschriebenen Konstruktion sind die Normbeträge zweier Hilfsfolgeelemente  $\beta_\mu, \beta_\nu$  zu zwei zueinander assoziierten Dirichlet-Elementen  $\gamma_\mu, \gamma_\nu \in R$  mit  $\mu > \nu$  nicht unbedingt gleich, da zwar die Moduln  $M_\mu = 1/\gamma_\mu \cdot R$  und  $M_\nu = 1/\gamma_\nu \cdot R$  gleich sind, aber eventuell unterschiedliche Modulbasen (siehe Bemerkung 2.5 (2.26)) berechnet werden. Die Darstellungsmatrix, die zur Berechnung dieser Basen LLL-reduziert wird, könnte eventuell zusätzlich normiert werden, so dass sich für  $M_\mu$  und  $M_\nu$  eine eindeutige Basis ergibt. Mit der Konstruktion der Hilfsfolgen als kürzeste Elemente der Moduln (wie im kommenden Abschnitt vorgestellt) würde dann  $N(\beta_\mu) = N(\beta_\nu)$  gelten.

## 2 Unabhängige Einheiten nach Dirichlet

Suche mit Hilfe von Hashtabellen optimal realisiert. In Relation zu möglichen anderen Kollisionssuchmethoden mit konstantem Speicherbedarf benötigen wir zwar mehr Speicherplatz, es sind aber für die Zugriffe auf die Liste der Normbeträge wie gesagt weniger Konstruktionen erforderlich (bei erwarteter gleicher Anzahl an Zugriffen). Somit ist der elementweise Vergleich des Normbetrags mit den Normbeträgen aller vorhergehenden Elemente hinsichtlich des Gesamtaufwands zum Auffinden der besagten Kollision effizient.

### Berechnung eines Systems von $r$ unabhängigen Einheiten

Wir fassen das bisher vorgestellte Vorgehen zur Berechnung eines Systems von  $r$  unabhängigen Einheiten, wie wir es in diesem Kapitel erarbeitet haben, abschließend in zwei Stichpunkten zusammen:

1. Es wird ein System von gewährleistenden Konjugiertenrichtungen gewählt: je nach Strategie wählt man diese entweder *sukzessive* (d.h. nach  $k$  konstruierten unabhängigen Einheiten wird die gewährleistende Konjugiertenrichtung  $(I_{k+1}, J_{k+1})$  wie in Abschnitt 2.4 beschrieben gewählt, so dass die Einheit  $\varepsilon_{k+1}$  unabhängig von den vorhergehenden ist) oder man nimmt die *einfachen* Konjugiertenrichtungen.
2. Zu der gegebenen Konjugiertenrichtung  $(I_{k+1}, J_{k+1})$  wird eine Konjugiertenfolge konstruiert und entlang der Konjugiertenfolge nach zwei zueinander assoziierten Elementen gesucht, deren Quotient die Einheit zu der Konjugiertenrichtung  $(I_{k+1}, J_{k+1})$  erbringt (siehe Algorithmus 4).

## 2.3 Andere Konstruktionsmöglichkeiten

Zur Berechnung der Konjugiertenfolge  $(\gamma_n)_{n \in \mathbb{N}}$  zu einer gegebenen Konjugiertenrichtung  $(I, J)$  soll zu jedem bereits berechneten Folgenglied  $\gamma_k$  ein  $\beta_k \in \frac{1}{\gamma_k} R \setminus \{0\}$  konstruiert werden, das die Bedingung

$$T_{2, \underline{\lambda}}(\beta_k) \leq \frac{\hat{C}^2}{|N(\gamma_k)|^{\frac{2}{n}}} \quad (2.8)$$

(bei Wahl von  $\underline{\lambda}$  wie in Abschnitt 2.1.2 dargelegt) erfüllt. Diese Aufgabe ist mit dem Auszählalgorithmus lösbar. Wir stellen dies in Algorithmus 5 dar. Die in die Schranke aus (2.8) eingehende Konstante  $\hat{C}$  ist dann, anders als bei der Konstruktion mit LLL, nicht mehr auf den Wert  $2^{\frac{1}{4}(n-1)} |\text{disc}(R)|^{\frac{1}{2}}$  festgelegt und kann entsprechend dem Ziel, Konjugiertenfolgeelemente mit kleiner Normbetragschranke zu konstruieren, kleiner gewählt werden. Bei einer gänzlich freien Wahl von  $\hat{C}$  ist allerdings die Existenz eines nicht-trivialen Modulelements mit

einer Länge kleiner als  $\hat{C}^2 |N(\gamma_k)|^{-\frac{2}{n}}$  nicht mehr von vorneherein gesichert, so dass die Schranke eventuell erhöht werden muss.

---

**Algorithmus 5** : Konstruktion einer Konjugiertenfolge mit Auszählalgorithmus

---

**Eingabe** : Ordnung  $R$ , Konjugiertenrichtung  $(I, J)$ , Länge  $\mu$  der zu berechnenden Folge, Startwert  $\hat{C}_1$  für die Schranke  $\hat{C}$ , Wert  $\nu$  der  $\delta$ -Erhöhung

**Ausgabe** : Konjugiertenfolge  $(\gamma_k)_{k \in \mathbb{N} \leq \mu} \in R$  zu  $(I, J)$ , Schranke  $\hat{C}$  am Ende der Konstruktion

$(\tilde{I}, \tilde{J}) \leftarrow (I, \{1, \dots, r_1 + r_2\} \setminus I)$

$k \leftarrow 0, \gamma_k \leftarrow 1$

$\hat{C} \leftarrow \hat{C}_1$

**while**  $k < \mu$  **do**

$flag \leftarrow false$

$\delta \leftarrow \nu(\hat{C} |N(\gamma_k)|^{-1/n})^{\frac{n-t}{t}}$

**while**  $flag = false$  **do**

        Setze  $\underline{\lambda} \in \mathbb{R}^n$  mit  $\lambda_\nu \leftarrow \begin{cases} \delta & \text{für } \nu \in \tilde{I} \\ \delta^{\frac{t}{t-n}} & \text{für } \nu \in \tilde{J} \end{cases} \quad (1 \leq \nu \leq r_1 + r_2)$   
         und  $\lambda_{\mu+r_2} \leftarrow \lambda_\mu$  für  $(r_1 < \mu \leq r_1 + r_2)$

$\beta_k \leftarrow$  ausgezähltes Element von  $\left\{ \alpha \in \frac{1}{\gamma_k} R \mid T_{2,\underline{\lambda}}(\alpha) \leq \frac{\hat{C}^2}{|N(\gamma_k)|^{\frac{2}{n}}} \right\}$

$flag \leftarrow true$

**if**  $\beta_k = 0$  **then**

$flag \leftarrow false$

$\hat{C} \leftarrow \hat{C} + 1$

$\delta \leftarrow \nu(\hat{C} |N(\gamma_k)|^{-1/n})^{\frac{n-t}{t}}$

**else**

**for**  $i \in \tilde{I}$  **do**

**if**  $|\beta_k^{(i)}| < 1$  **then**

$flag \leftarrow false$

$\delta \leftarrow 2\delta$

**break for** // neue Konstruktion mit erhöhtem  $\delta$

**endif**

**endfor**

**endif**

**endwhile**

$\gamma_{k+1} \leftarrow \beta_k \cdot \gamma_k$

$k \leftarrow k + 1$

**endwhile**

**return**  $(\gamma_k)_{k \in \mathbb{N} \leq \mu}, \hat{C}$

---

## 2 Unabhängige Einheiten nach Dirichlet

Die Entscheidung über die Wahl des freien Parameters  $\hat{C}_1$  und der Vergleich mit der LLL-Konstruktion orientiert sich an der Gesamtzielsetzung, Konjugiertenfolgen zu konstruieren, entlang derer wir schnell Einheiten finden können. Insoweit müsste die Diskussion eigentlich vertagt werden, bis auch das andere Verfahren für die Konstruktion von Einheiten vorgestellt wurde. Wir legen nun zunächst das möglichst frühe Auftreten zweier zueinander assoziierter Elemente in der Konjugiertenfolge als Kriterium für die Beurteilung der Güte eines Konstruktionsverfahrens zu Grunde. Da mit jedem Konjugiertenfolgeelement der Konstruktionsaufwand steigt, könnten bezüglich des Konstruktionsaufwands einzelner Elemente teure Verfahren gegenüber billigeren Verfahren hinsichtlich des Gesamtaufwands gerechtfertigt sein, da sie vielleicht Konjugiertenfolgen ergeben, entlang derer man schneller fündig wird.

In [Wil93] kommt der Autor zu dem Ergebnis, dass die Konstruktion von Konjugiertenfolgen mit dem Auszählalgorithmus von der Konstruktion mit LLL hinsichtlich des schnellen Auffindens assoziierter Elemente dominiert wird. Wählt man  $\hat{C}$  in Algorithmus 5 entsprechend der LLL-Bedingungen gleich  $\mathcal{C} := 2^{\frac{1}{4}(n-1)} |\text{disc}(R)|^{\frac{1}{2n}}$ , so ist die Konstruktion mit dem Auszählalgorithmus nicht nur eventuell hinsichtlich der Komplexität ungünstiger als die Konstruktion mit LLL, sondern vor allem hinsichtlich des schnellen Auffindens von assoziierten Elementen, wie man in folgendem Beispiel sieht.

**Beispiel 2.7.** *In der Maximalordnung des Körpers  $F \cong \mathbb{Q}/(t^{14} + 2)\mathbb{Q}$  findet man ein System von 6 unabhängigen Einheiten zu den einfachen Konjugiertenrichtungen bei der Konstruktion mit Algorithmus 3 (Konstruktion mit LLL) nach insgesamt (wir zählen die Anzahl der konstruierten Konjugiertenfolgeelemente bis eine Einheit gefunden wird für alle Einheiten zusammen. Der Anfangswert jeder Konjugiertenfolge  $\gamma_0 = 1$  wird hier und im Folgenden nicht als konstruiertes Element gezählt) 34 Konjugiertenfolgeelementen. Bei der Konstruktion mit Algorithmus 5 mit  $\hat{C}_1 = \mathcal{C} \approx 49$  werden insgesamt 1131 Elemente berechnet, bis die Einheiten gefunden werden.*

Die Erklärung dafür liegt in folgendem Sachverhalt: bei der Wahl von  $\beta_k$  als erstes Element einer LLL-reduzierten Basis des Moduls ist dieses Hilfsfolgeelement hinsichtlich  $T_{2,\lambda}$ -Länge sicher durch  $\mathcal{C}^2 |N(\gamma_k)|^{-\frac{2}{n}}$  beschränkt. Praktisch zeigt sich, dass man jedoch oft kürzere Elemente erhält. Dadurch bleiben in der Regel, wie die Ungleichung zwischen geometrischem und arithmetischem Mittel nahelegt, auch die Normbeträge  $|N(\gamma_k)|$  der Konjugiertenfolgeelemente in einem kleinen Bereich. Wenn wir hingegen  $\beta_k$  als das erste Element des Moduls wählen, das uns der Auszählalgorithmus zur gleichen Schranke  $\mathcal{C}$  liefert, ist dies nicht mehr der Fall, da dieses Element häufig annähernd eine  $T_{2,\lambda}$ -Länge von  $\mathcal{C} |N(\gamma_k)|^{-\frac{2}{n}}$  hat. Der Bereich, in dem sich die Normbeträge abspielen ( $\leq \mathcal{C}^n$ ), wird durch diese Konjugiertenfolgeelemente stärker ausgeschöpft, mit dem Ergebnis, dass

### 2.3 Andere Konstruktionsmöglichkeiten

es länger dauert, bis wir zwei Elemente derselben Norm und somit eine Einheit finden.

Nun wollen wir die Möglichkeit ausnutzen, die Schranke  $\hat{C}$  kleiner als  $\mathcal{C}$  zu wählen. Daran sind wir besonders interessiert, da die Schranke, die wir für die Normbeträge gewinnen,  $\hat{C}^n$  entspricht und somit auch entsprechend kleiner ist. Wir überlegen uns, wie weit wir  $\hat{C}$  mindestens absenken können, so dass der Auszählalgorithmus in jedem Fall ein nicht-triviales Element entsprechender Länge findet. Nach der Ungleichung (1.13) können wir für das kürzeste Element  $\beta_{min}$  des Moduls  $M_k$  annehmen, dass

$$T_{2,\lambda}(\beta_{min}) \leq \mathcal{Y}_n \left( \det(T_{2,\lambda}) \right)^{\frac{1}{n}} = \mathcal{Y}_n \frac{|disc(R)|^{\frac{1}{n}}}{|N(\gamma_k)|^{\frac{2}{n}}}$$

gilt. Wenn wir dementsprechend  $\mathcal{K} := \mathcal{Y}_n^{\frac{1}{2}} |disc(R)|^{\frac{1}{2n}}$  setzen, ist es immer möglich, mit dem Auszählalgorithmus ein Element  $\beta \in M_k$  mit der Eigenschaft

$$T_{2,\lambda}(\beta) \leq \frac{\mathcal{K}^2}{|N(\gamma_k)|^{\frac{2}{n}}}$$

zu berechnen. Für den Startwert  $C_1 = \mathcal{K}$  muss die Schranke während des Algorithmus also nicht erhöht werden, da immer nicht-triviale Elemente entsprechender Länge gefunden werden.

**Beispiel 2.7.** (fortgesetzt) *Wählt man bei der Konstruktion mit dem Auszählalgorithmus den Startwert  $\hat{C}_1 = \mathcal{K} \approx 8.78$ , werden insgesamt **368** Elemente berechnet, bis alle Einheiten gefunden werden. Das sind immer noch wesentlich mehr als bei der Konstruktion mit LLL.*

Eine weitere Absenkung scheint zweckmäßig zu sein, obgleich sie mit dem Nachteil verbunden ist, dass man eventuell nachbessern muss. Wir wollen dies an dieser Stelle aber nicht stückweise weiter verfolgen, sondern stattdessen gleich den Ansatz betrachten, direkt jeweils die kürzesten Elemente des Moduls als Hilfsfolgelemente zu wählen. Zum Abschluss zeigen wir am Beispiel, wie weit wir mit einer Absenkung von  $\hat{C}$  kommen.

**Beispiel 2.7.** (fortgesetzt) *Wählt man bei der Konstruktion mit dem Auszählalgorithmus den Startwert  $\hat{C}_1 = \mathcal{Y}_n^{\frac{1}{r-1}} |disc(R)|^{\frac{1}{2n}} \approx 6.38$ , werden insgesamt **46** Elemente berechnet, bis alle  $r = 6$  Einheiten gefunden werden. Hierbei war keine Erhöhung von  $\hat{C}$  während der Konstruktion mit Algorithmus 5 nötig.*

## 2 Unabhängige Einheiten nach Dirichlet

### Konstruktion mit kürzesten Konjugiertengittervektoren

Es besteht die Möglichkeit, als Hilfsfolgenelemente die den kürzesten Vektoren des gewichteten Konjugiertengitters entsprechenden Elemente des Moduls zu berechnen. Wir geben den Algorithmus (Algorithmus 6) an, der eine Konjugiertenfolge der Länge  $\mu$  mit diesem Vorgehen konstruiert.

---

#### Algorithmus 6 : Konjugiertenfolge mit kürzesten Elementen

---

**Eingabe** : Ordnung  $R$ , Konjugiertenrichtung  $(I, J)$ , Startwert  $C_1$  der Schranke  $\hat{C}$ , Wert  $\nu$  der  $\delta$ -Erhöhung

**Ausgabe** : Konjugiertenfolge  $(\gamma_k)_{k \in \mathbb{N} \leq \mu} \in R$  zu  $(I, J)$  mit Schranke  $\hat{C}$

```

1  $(\tilde{I}, \tilde{J}) \leftarrow (I, \{1, \dots, r_1 + r_2\} \setminus I)$ 
2  $k \leftarrow 0, \gamma_k \leftarrow 1, \hat{C} \leftarrow C_1$ 
3 while  $k < \mu$  do
4    $flag \leftarrow false,$ 
5    $\delta \leftarrow \nu(\hat{C}|N(\gamma_k)|^{-1/n})^{\frac{n-t}{t}}$ 
6   while  $flag = false$  do
7     Setze  $\underline{\lambda} \in \mathbb{R}^n$  mit  $\lambda_\nu \leftarrow \begin{cases} \delta & \text{für } \nu \in \tilde{I} \\ \delta^{\frac{t}{t-n}} & \text{für } \nu \in \tilde{J} \end{cases} \quad (1 \leq \nu \leq r_1 + r_2)$ 
8     und  $\lambda_{\mu+r_2} \leftarrow \lambda_\mu$  für  $(r_1 < \mu \leq r_1 + r_2)$ 
9     Berechne  $M \leftarrow \min \left\{ T_{2,\underline{\lambda}}(\alpha) \mid \alpha \in \frac{1}{\gamma_k} R \right\}$ 
10    und  $\beta_k \leftarrow \alpha$  mit  $T_{2,\underline{\lambda}}(\alpha) = M.$ 
11    if  $\sqrt{M \cdot |N(\gamma_k)|^{2/n}} > \hat{C}$  then
12       $\hat{C} \leftarrow \sqrt{M \cdot |N(\gamma_k)|^{2/n}}$ 
13       $\delta \leftarrow \nu(\hat{C}|N(\gamma_k)|^{-1/n})^{\frac{n-t}{t}}$ 
14    else
15       $flag \leftarrow true$ 
16      for  $i \in \tilde{I}$  do
17        if  $|\beta_k^{(i)}| < 1$  then
18           $flag \leftarrow false$ 
19           $\delta \leftarrow 2\delta$ 
20          break for // neue Konstruktion mit erhöhtem  $\delta$ 
21        endif
22      endfor
23    endif
24  endwhile
25   $\gamma_{k+1} \leftarrow \beta_k \cdot \gamma_k$ 
26   $k \leftarrow k + 1$ 
27 endwhile
28 return  $(\gamma_k)_{k \in \mathbb{N} \leq \mu}, \hat{C}$ 

```

---

### 2.3 Andere Konstruktionsmöglichkeiten

Hierbei ist allerdings zu beachten, dass vor der Ausführung des Auszählalgorithmus auch noch das Minimum des Gitters ermittelt werden muss, so dass sich die Komplexität der Berechnung eines solchen Hilfsfolgenelements gegenüber der Konstruktion mit LLL nachteilig gestalten kann. Allerdings rechtfertigt die kleinere Normbetragsschranke und damit das durchschnittlich frühere Auffinden von Einheiten diesen Ansatz in vielen Fällen, wie wir sehen werden.

Der Algorithmus terminiert sicher, wenn für  $C_1$  die Schranke  $\mathcal{K} = \mathcal{Y}_n^{\frac{1}{2}} |disc(R)|^{\frac{1}{2n}}$  gewählt wird, da ein Element der  $T_{2,\lambda}$ -Länge  $\mathcal{Y}_n^{\frac{1}{2}} \frac{|disc(R)|^{\frac{1}{n}}}{|N(\gamma_k)|^{\frac{1}{n}}}$  im Modul  $\frac{1}{\gamma_k} R$  existiert. Zur Demonstration der praktischen Vorteile der Konstruktion mit Hilfe kürzester Vektoren knüpfen wir an das vorige Beispiel an und geben weitere Beispiele.

**Beispiel 2.7.** (fortgesetzt) Wählt man bei der Berechnung eines Systems von 6 unabhängigen Einheiten der Maximalordnung von  $F \cong \mathbb{Q}/(t^{14} + 2)\mathbb{Q}$  mit Algorithmus 6 den Startwert  $\hat{C}_1 = \mathcal{Y}_n^{\frac{1}{r-1}} |disc(R)|^{\frac{1}{2n}} \approx 6.38$ , werden insgesamt **34** Elemente berechnet, bis alle 6 Einheiten gefunden werden. Dabei musste die Schranke während des Algorithmus nicht erhöht werden.

**Beispiel 2.8.** Verglichen mit dem vorherigen Beispiel hat die Maximalordnung des Zahlkörpers  $F \cong \mathbb{Q}/(t^{14} + 9t^6 + 3)\mathbb{Q}$  eine im Verhältnis zum Einheitenrang betragsmäßig größere Diskriminante. Ein System von 6 unabhängigen Einheiten der Maximalordnung finden wir bei der Konstruktion mit LLL nach insgesamt **779** berechneten Konjugiertenfolgenelementen (Rechenzeit 310 Sek.). Demgegenüber müssen zur Berechnung der Einheiten mit Konjugiertenfolgen aus Algorithmus 6 und  $\hat{C}_1 = \mathcal{K} \approx 16.52$  nur **329** Dirichlet-Elemente konstruiert werden (Rechenzeit 42 Sek.).

**Beispiel 2.9.** Sei  $F = \mathbb{Q}/(t^{20} - 3)\mathbb{Q}$ . Ein System von 10 unabhängigen Einheiten der Maximalordnung  $\mathfrak{o}_F$  finden wir bei der Konstruktion mit LLL nach insgesamt **412** berechneten Konjugiertenfolgenelementen (Rechenzeit 318 Sek.).

Mit Algorithmus 6 und  $\hat{C}_1 = \mathcal{K} \approx 14.43$  werden **368** Dirichlet-Elemente konstruiert bis alle 10 Einheiten zu den Konjugiertenrichtungen gefunden werden (Rechenzeit 96 Sek.). Wählen wir  $\hat{C}_1 = \mathcal{Y}_n^{1/3} |disc(R)|^{\frac{1}{2n}} \approx 11.62$  für Algorithmus 6 müssen nur **281** Dirichlet-Elemente konstruiert werden (Rechenzeit 34 Sek.). Eine weitere Absenkung ist nicht immer zweckmäßig: Bei  $\hat{C}_1 = \mathcal{Y}_n^{\frac{1}{r-1}} |disc(R)|^{\frac{1}{2n}} \approx 8.7$  werden **320** Dirichlet-Elemente konstruiert bis das System unabhängiger Einheiten berechnet wurde (Rechenzeit 57 Sek.).

Man kann erkennen, dass sich das Auszählen kürzester Gittervektoren des Konjugiertengitters vor allem bei höheren Körpergraden lohnt, da sich hier die geringe  $T_{2,\lambda}$ -Länge stärker zugunsten einer kleineren Normbetragsschranke für die Konjugiertenfolgenelemente auswirkt.

**Bemerkung 2.10.** Bei der Implementation, welche die experimentellen Ergebnisse in diesem Abschnitt erbringt, wurden die LLL- und die Auszähl-Routine von MAGMA verwendet. Die LLL-Routine von MAGMA wählt unter verschiedenen LLL-Varianten die günstigste aus (siehe MAGMA-Dokumentation [BCP97]). Wir führen die LLL-Reduktion mit den klassischen Parametern ( $\eta = \frac{1}{2}, \delta = \frac{3}{4}$ ) durch. Die MAGMA-Funktion zur Berechnung kürzester Vektoren und des Minimums, die wir bei der Implementation der Algorithmen 6 und 5 benutzen, beruht auf dem Auszählalgorithmus wie in Abschnitt 1.1.3 beschrieben (für Details siehe zum Beispiel [FP85] und [SE93]).

## 2.4 Variation der Konjugiertenrichtung als Unabhängigkeitsgaranten

Die Motivation für die Einführung des Begriffs Konjugiertenrichtung  $(I, J)$  als Aufteilung der Indexmenge  $\{1, \dots, r_1 + r_2\}$  war die Tatsache, dass Einheiten zu  $r$  verschiedenen Konjugiertenrichtungen *a priori* unabhängig sein sollen.

Bisher haben wir nur gezeigt, dass dies im Fall von Einheiten zu  $r$  verschiedenen *einfachen* Konjugiertenrichtungen  $(I, J)$  mit  $I := \{i\}$  und  $J := \{1, \dots, r_1 + r_2\} \setminus \{i\}$  für  $i \in \mathcal{I}$ , wobei  $\mathcal{I}$  eine  $r$ -elementige Teilmenge von  $\{1, \dots, r_1 + r_2\}$  ist, gewährleistet ist. Wir wollen aber grundsätzlich auch andere Konjugiertenrichtungen berücksichtigen, um zum Beispiel bereits berechnete unabhängige Einheiten einzubeziehen oder Konjugiertenrichtungen zu finden, deren zugehörige Konjugiertenfolgen eventuell besser konditioniert<sup>2</sup> sind als die der einfachen. In beiden Fällen ist es nötig, durch eine spezielle Wahl der Konjugiertenrichtung für die Unabhängigkeit der zugehörigen Einheit von bereits berechneten Einheiten sorgen zu können.

Wir befinden uns in folgender Situation: gegeben seien  $\varepsilon_1, \dots, \varepsilon_m$  unabhängige Einheiten von  $R$ . Gesucht ist die Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$ , so dass  $\varepsilon_{m+1}$  als Einheit zu  $(I_{m+1}, J_{m+1})$  unabhängig von  $\varepsilon_1, \dots, \varepsilon_m$  ist. Der nachstehende Algorithmus (Algorithmus 7) aus [Wil93] beruht auf der Idee aus [Poh93, S.51] und berechnet die gewünschte Konjugiertenrichtung.

**Bemerkung 2.11.** In Zeile 6 des Algorithmus soll eine Zeilenstufenform berechnet werden. Für die Matrix  $A = (L(\varepsilon_1), \dots, L(\varepsilon_m))^t \in \mathbb{R}^{m \times r}$  gibt es Matrizen  $V \in Gl(m, \mathbb{R})$  und  $U \in Gl(r, \mathbb{Z})$ , so dass  $B = V \cdot A \cdot U$  in der gewünschten Zeilenstufenform (mit  $B = (b_{i,j})_{1 \leq i \leq m, 1 \leq j \leq r}$ , so dass  $b_{i,i} > 0$  für  $(1 \leq i \leq m)$ ) ist, da  $\varepsilon_1, \dots, \varepsilon_m$  unabhängig sind. Dabei sollen in der Matrix  $V$  nur die Zeilenreduktionen und in der Matrix  $U$  die Spaltenvertauschungen verwaltet werden. Konkret

<sup>2</sup> „Besser konditioniert“ bedeutet an dieser Stelle noch, dass in einer Konjugiertenfolge früher zueinander assoziierte Elemente auftreten als in einer anderen.

## 2.4 Variation der Konjugiertenrichtung als Unabhängigkeitsgaranten

erhalten wir die Matrix  $V$  in MAGMA/KANT mit  $D, V := \text{EchelonForm}(A)$ . Um aus  $D$  die gewünschte Zeilenstufenform  $B$  zu gewinnen, müssen die Spalten von  $D$  eventuell noch vertauscht und die entsprechenden Transformationsmatrizen zu  $U$  zusammengefasst werden. Da wir mit reellen Vektoren arbeiten, ist hier auf die Verwendung einer ausreichend hohen Präzision zu achten.

---

### Algorithmus 7 : Berechnung der passenden Konjugiertenrichtung

---

**Eingabe :** Menge unabhängiger Einheiten  $G \subset U(R)$

**Ausgabe :** eine Konjugiertenrichtung  $(I, J)$ , so dass die Einheit zu  $(I, J)$  unabhängig von den Elementen von  $G$  ist.

```

1 Initialisierung:  $I \leftarrow \{\}, J \leftarrow \{\}, \underline{v} = (v_1, \dots, v_r) \leftarrow (0, \dots, 0), m \leftarrow \#G$ 
2 if  $m = 0$  then
3   return  $(\{1\}, \{\})$ 
4 else
5    $\{\varepsilon_1, \dots, \varepsilon_m\} \leftarrow G$ 
6    $A \leftarrow (L(\varepsilon_1), \dots, L(\varepsilon_m))^t \in \mathbb{R}^{m \times r}$ 
7   Berechne  $V \in Gl(m, \mathbb{R})$  und  $U \in Gl(r, \mathbb{Z})$ , so dass für
       $B = (b_{i,j})_{1 \leq i \leq m, 1 \leq j \leq r} = V \cdot A \cdot U$  gilt:  $b_{i,i} > 0$  für  $1 \leq i \leq m$  und
       $b_{i,j} = 0$  für  $1 \leq i, j \leq m, j \neq i$ .
      // Berechnung eines Vektors, der linear unabhängig von den
      Zeilen von A ist
8   for  $k$  von 1 bis  $m$  do
           $v_k \leftarrow \text{sign}(b_{k,m+1})$  // mit  $\text{sign}(x) := \begin{cases} \frac{x}{|x|} & \text{für } x \neq 0 \\ 0 & \text{für } x = 0 \end{cases}$ 
9
10  endfor
11   $v_{m+1} \leftarrow -1$ 
12   $\underline{v} \leftarrow \underline{v} \cdot U^{-1}$ 
      // Bestimmung der Konjugiertenrichtung
13  for  $k$  von 1 bis  $r_1 + r_2 - 1$  do
14    if  $v_k = -1$  then
15       $J \leftarrow J \cup \{k\}$ 
16    else
17       $I \leftarrow I \cup \{k\}$ 
18    endif
19  endfor
20  return  $(I, J)$ 
21 endif

```

---

**Korrektheit des Algorithmus:** Es ist zu zeigen, dass für  $m \geq 1$  die Einheit  $\varepsilon_{m+1}$  zu der mit Algorithmus 7 berechneten Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$

## 2 Unabhängige Einheiten nach Dirichlet

tatsächlich unabhängig von den Einheiten  $\varepsilon_1, \dots, \varepsilon_m$  ist. Dazu zeigt man, dass die Vektoren  $L(\varepsilon_1), \dots, L(\varepsilon_m), L(\varepsilon_{m+1})$  linear unabhängig sind. Wir betrachten die Matrix  $M$ , die aus der Matrix  $A$  durch Erweiterung mit  $\underline{w} := L(\varepsilon_{m+1})^t$  als letzte Zeile hervorgeht:

$$M := \begin{pmatrix} A \\ \underline{w} \end{pmatrix} = \begin{pmatrix} L(\varepsilon_1)_1 & \dots & L(\varepsilon_1)_r \\ \vdots & & \vdots \\ L(\varepsilon_m)_1 & \dots & L(\varepsilon_m)_r \\ L(\varepsilon_{m+1})_1 & \dots & L(\varepsilon_{m+1})_r \end{pmatrix}.$$

Es ist zu zeigen, dass  $\text{Rang}(M) = m + 1$  ist. Wir führen für die ersten  $m$  Zeilen von  $A$  die Zeilenreduktionen durch Multiplikation mit  $V \in \text{Gl}(m, \mathbb{R})$  aus dem Algorithmus durch, so dass für  $D = (d_{i,j}) = V \cdot A$  gilt, dass  $D^t$  in Hermite Normalform ist:

$$\begin{pmatrix} V & \underline{0} \\ \underline{0} & 1 \end{pmatrix} \cdot M = \begin{pmatrix} V & \underline{0} \\ \underline{0} & 1 \end{pmatrix} \cdot \begin{pmatrix} A \\ \underline{w} \end{pmatrix} = \begin{pmatrix} d_{1,1} & \dots & d_{1,r} \\ \vdots & & \vdots \\ d_{m,1} & \dots & d_{m,r} \\ L(\varepsilon_{m+1})_1 & \dots & L(\varepsilon_{m+1})_r \end{pmatrix}.$$

Es gilt  $\text{Rang}(A) = \text{Rang}(D) = m$ , da  $\varepsilon_1, \dots, \varepsilon_m$  unabhängig sind. Nun multiplizieren wir die letzte Matrix mit  $U \in \text{Gl}(r, \mathbb{Z})$ , so dass  $B = (b_{i,j}) = DU$  in der oben definierten Zeilenstufenform ist. Wir definieren  $\underline{\tilde{w}}$  als den Vektor, der durch diese Umsortierungen aus  $L(\varepsilon_{m+1})^t$  entsteht. Es sei  $(\tilde{w}_1, \dots, \tilde{w}_r) := L(\varepsilon_{m+1})^t \cdot U$ . Wir erhalten:

$$\tilde{M} := V \cdot M \cdot U = \begin{pmatrix} d_{1,1} & \dots & d_{1,r} \\ \vdots & & \vdots \\ d_{m,1} & \dots & d_{m,r} \\ L(\varepsilon_{m+1})_1 & \dots & L(\varepsilon_{m+1})_r \end{pmatrix} \cdot U = \begin{pmatrix} b_{1,1} & \dots & b_{1,r} \\ \vdots & & \vdots \\ b_{m,1} & \dots & b_{m,r} \\ \tilde{w}_1 & \dots & \tilde{w}_r \end{pmatrix}.$$

Für den Vektor  $\underline{w} = L(\varepsilon_{m+1})^t$  gilt nach Definition der Einheit  $\varepsilon_{m+1}$  zu der Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$ , dass  $(\text{sign}(w_1), \dots, \text{sign}(w_r)) =: \underline{v}$ , wobei  $\underline{v}$  dem Vektor entspricht, den wir in Zeile 11 des Algorithmus erhalten. Dann gilt  $(\text{sign}(\tilde{w}_1), \dots, \text{sign}(\tilde{w}_r)) = \underline{v} \cdot U =: \tilde{v}$ , wobei  $\tilde{v}$  dem Vektor entspricht, den wir in Zeile 7 bis 10 des Algorithmus bestimmt haben. Für  $1 \leq i \leq m$  gilt dann wegen der Bestimmung des Vektors  $\tilde{v}$  im Algorithmus  $\text{sign}(\tilde{w}_i) = \tilde{v}_i = \text{sign}(b_{i,m+1})$  und

## 2.4 Variation der Konjugiertenrichtung als Unabhängigkeitsgaranten

somit  $\tilde{w}_i = \text{sign}(b_{i,m+1})|\tilde{w}_i|$ . Außerdem gilt  $\text{sign}(\tilde{w}_{m+1}) = \tilde{v}_{m+1} = -1$  und damit  $\tilde{w}_{m+1} < 0$ .

Die letzte berechnete Matrix hat die folgende Form mit  $b_{i,i} > 0$  ( $1 \leq i \leq m$ ):

$$\tilde{M} = \begin{pmatrix} b_{1,1} & 0 & \dots & 0 & b_{1,m+1} & * \\ 0 & b_{2,2} & 0 & \vdots & b_{2,m+1} & * \\ \vdots & 0 & \ddots & 0 & \vdots & * \\ 0 & \dots & 0 & b_{m,m} & b_{m,m+1} & * \\ \tilde{w}_1 & \tilde{w}_2 & \dots & \tilde{w}_m & \tilde{w}_{m+1} & \underline{\mathbf{0}} \end{pmatrix}.$$

Diese Matrix reduzieren wir nun durch Zeilenoperationen (Gauß-Elimination) durch Multiplikation von links mit einer Matrix  $T = (t_{i,j}) \in Gl(m+1, \mathbb{R})$  mit

- (1)  $t_{i,j} := \delta_{i,j}$  für ( $1 \leq i \leq m$ ) und ( $1 \leq j \leq m+1$ )
- (2)  $t_{m+1,j} := -\tilde{w}_j \prod_{k=1, k \neq j}^m b_{k,k}$  für ( $1 \leq j \leq m$ )
- (3)  $t_{m+1,m+1} := \prod_{k=1}^m b_{k,k}$

so, dass Nullen unter den  $b_{i,i}$  für ( $1 \leq i \leq m$ ) stehen:

$$T\tilde{M} = \begin{pmatrix} b_{1,1} & 0 & \dots & 0 & b_{1,m+1} & * \\ 0 & b_{2,2} & 0 & \vdots & b_{2,m+1} & * \\ \vdots & 0 & \ddots & 0 & \vdots & * \\ 0 & \vdots & 0 & b_{m,m} & b_{m,m+1} & * \\ 0 & 0 & \dots & 0 & a & * \end{pmatrix}.$$

Für den  $m+1$ -ten Eintrag der letzten Zeile der reduzierten Matrix gilt:

$$a = \underbrace{b_{1,1} \cdots b_{m,m}}_{>0} \cdot \underbrace{\tilde{w}_{m+1}}_{<0} - \sum_{i=1}^m \left( \underbrace{\tilde{w}_i b_{i,m+1}}_{\substack{=|\tilde{w}_i| |b_{i,m+1}| \\ \geq 0}} \cdot \underbrace{\prod_{\substack{j=1 \\ j \neq i}}^m b_{j,j}}_{>0} \right).$$

Es gilt also  $a < 0$ . Demnach gilt  $\text{Rang}(T\tilde{M}) = m+1$ . Da wir mit unimodularen Matrizen  $V, U, T$  gearbeitet haben, gilt  $\text{Rang}(M) = \text{Rang}(\tilde{M}) = \text{Rang}(T\tilde{M})$ . Das bedeutet, dass die Zeilenvektoren  $L(\varepsilon_1)^t, \dots, L(\varepsilon_m)^t, L(\varepsilon_{m+1})^t$  von  $M$  linear unabhängig sind. Die Einheit  $\varepsilon_{m+1}$  zur Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$  ist damit unabhängig von den gegebenen unabhängigen Einheiten  $\varepsilon_1, \dots, \varepsilon_m$ .  $\square$

### Nutzung der Variationsmöglichkeiten

Wie in [Wil93, Abschnitt 3.2.] ausführlich beschrieben und analysiert, ermöglicht diese Verallgemeinerung der einfachen Konjugiertenrichtungen die Wahl verschiedener Strategien, um unabhängige Einheiten aus den Konjugiertenfolgen zu konstruieren.

**Strategie 1** Es werden  $r$  einfache Konjugiertenrichtungen aus der Menge  $\{(\{i\}, \{1, \dots, r_1 + r_2\} \setminus \{i\}) \mid i \in \{1, \dots, r_1 + r_2\}\}$  gewählt. Zu jeder Konjugiertenrichtung wird eine Einheit konstruiert. Diese sind, wie in Lemma 2.1 bewiesen, unabhängig.

**Strategie 2** Es werden sukzessive gewährleistende Konjugiertenrichtungen wie in Algorithmus 7 bestimmt, so dass die dazu konstruierte Einheit von den vorhergehenden unabhängig ist.

**Strategie 3** Es werden zu einer großen Auswahl beliebiger Konjugiertenrichtungen Konjugiertenfolgen simultan elementweise erweitert. Sobald eine Einheit  $\varepsilon$  zu einer Konjugiertenfolge auftritt, wird ein minimales Erzeugendensystem  $\eta_1, \dots, \eta_j$  mit  $j \leq k + 1$  von  $\langle \varepsilon_1, \dots, \varepsilon_k, \varepsilon \rangle$  mit MLLL berechnet, wobei  $\varepsilon_1, \dots, \varepsilon_k$  die zuvor bereits berechneten unabhängigen Einheiten sind (Die Unabhängigkeit muss aufgrund der Beliebigkeit der Konjugiertenrichtung durch die Bestimmung eines minimalen Erzeugendensystems gesichert werden). Die Berechnung der Einheiten zu den verschiedenen Konjugiertenrichtungen wird solange fortgesetzt, bis  $j = r$  ist.

**Strategie 4** Nach einer gewissen Anzahl von systematischen Konstruktionen von Konjugiertenfolgeelementen zu einer Konjugiertenrichtung (wie in Strategie 2) verzweigt man bei Erfolglosigkeit in die Erweiterung kurzer Konjugiertenfolgen zu beliebigen Konjugiertenrichtungen (wie in Strategie 3).

Im nächsten Kapitel wollen wir eine Alternative zur bisherigen Suche nach Einheiten als Quotienten assoziierter Elemente vorstellen. Bei Strategie 2 und 4 nehmen die gefundenen Einheiten Einfluss auf die anschließend berechneten Konjugiertenrichtungen und diese bedingen wiederum unterschiedlich geartete Konjugiertenfolgen. Da bei den Suchmethoden unterschiedliche Einheiten konstruiert werden, werden wir, um die Methoden unabhängig von diesen internen Einflüssen vergleichen zu können, im nächsten Kapitel vor allem Strategie 1 wählen, um unabhängige Einheiten zu berechnen. Eine Übertragung der anderen Strategien auf die Einheitenkonstruktion mit Bewertungsmatrizen nehmen wir in Kapitel 4 vor.

# 3 Unabhängige Einheiten mit Bewertungsmatrizen

Im vorhergehenden Kapitel wurde beschrieben, wie Einheiten zu Konjugiertenrichtungen gewonnen werden. Dabei wurde die Konstruktion von Konjugiertenfolgen und die bisherige Konstruktion von Einheiten als Quotient von assoziierten Elementen dieser Folgen dargelegt. Die Konstruktion von Einheiten aus Konjugiertenfolgeelementen wollen wir nun in diesem Kapitel mit Ideen aus der Klassengruppenberechnung modifizieren.

## 3.1 Werkzeuge aus der Klassengruppenberechnung

Zunächst sollen hier die Begriffe und Konzepte der Klassengruppenberechnung vorgestellt werden, die wir später auf die Elemente der Konjugiertenfolgen anwenden wollen. Wir geben diese in Anlehnung an [Poh93] und [Hes96] wieder.

**Definition 3.1.** *Eine endliche Menge von Primidealen von  $\mathfrak{o}_F$  wird mit **Faktorbasis**  $S$  bezeichnet. Die Elemente  $x \in F$ , für die gilt, dass  $x\mathfrak{o}_F$  ein Potenzprodukt der Primideale aus  $S$  ist, nennt man  **$S$ -Einheiten**. Ein Element  $x \in F$ , welches eine  $S$ -Einheit ist, bezeichnen wir als **glatt** über  $S$ .*

Bei der Berechnung der Klassengruppe arbeitet man mit linearen Operationen. Dazu betrachten wir folgende Abbildung, die zu einer Faktorbasis  $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$  den ganzzahligen Vektor der Bewertungen eines Ideals über den Elementen der Faktorbasis angibt:

$$\nu_S : I_F \longrightarrow \mathbb{Z}^s, \mathfrak{a} \longmapsto \begin{pmatrix} \nu_{\mathfrak{p}_1}(\mathfrak{a}) \\ \vdots \\ \nu_{\mathfrak{p}_s}(\mathfrak{a}) \end{pmatrix} \quad (3.1)$$

**Bemerkung:** *Die Bilder dieser Abbildung nennen wir im Folgenden **Bewertungsvektoren**. Entsprechend der Überlegungen zu Korollar 1.13 schreiben wir für Elemente  $\alpha \in F$  abkürzend  $\nu_S(\alpha)$  und meinen damit das Bild des von  $\alpha$  erzeugten Hauptideals  $\nu_S(\alpha\mathfrak{o}_F)$ .*

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

Eine wichtige Beobachtung ist, dass  $\nu_S(\varepsilon_{\mathfrak{o}_F})$  für  $\varepsilon \in U(\mathfrak{o}_F)$  unabhängig von der Wahl von  $S$  der Nullvektor ist.

Zu einer gegebenen Faktorbasis  $S$  möchten wir prüfen, ob es sich bei einem Dirichlet-Element  $\gamma \in \mathfrak{o}_F$  um eine  $S$ -Einheit handelt und gegebenenfalls den Vektor  $\nu_S(\gamma)$  für die Verwaltung in einer Matrix bestimmen. Dafür können wir wie im Algorithmus aus [Hes96, S.61, Algorithmus 4.4.1] vorgehen. Der darauf beruhende folgende Algorithmus ist auf die Situation angepasst, dass die zu testenden Elementen in unserem Fall Elemente der Maximalordnung  $\mathfrak{o}_F$  sind.

---

**Algorithmus 8** : Test auf  $S$ -Einheit und Berechnung von  $\nu_S(\gamma)$  für  $\gamma \in \mathfrak{o}_F$

---

**Eingabe:** Zahlkörper  $F$ , Faktorbasis  $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ ,  $\gamma \in \mathfrak{o}_F$

**Ausgabe:** „wahr“ sowie  $\nu_S(\gamma)$  oder „falsch“

1. (Initialisierung)  $\mathcal{N} \leftarrow \{N(\mathfrak{p}) : \mathfrak{p} \in S\}$ ,  $\mathcal{P} \leftarrow \{q \in \mathbb{P} : q \text{ teilt } N \text{ für } N \in \mathcal{N}\}$   
 Setze für alle  $p \in \mathcal{P}$ :  
 $S_p \leftarrow \{\mathfrak{p} \in \mathbb{P}_F : p \text{ teilt } N(\mathfrak{p}) \text{ und } \mathfrak{p} \in S\}$ .
  2. (Sieben) Setze  $N \leftarrow |N_{F/\mathbb{Q}}(\gamma)|$ .  
 Für alle  $p \in \mathcal{P}$  setze:  
 $\gamma_p \leftarrow \nu_{p\mathbb{Z}}(N)$ ,  $N \leftarrow N/(p^{\gamma_p})$ .  
 Falls anschließend  $N \neq 1$  gilt, **return** „falsch“ und terminiere.
  3. ( $\nu_S(\gamma)$  berechnen)  
 Für jedes  $p \in \mathcal{P}$ :  
 Setze  $N \leftarrow |N_{F/\mathbb{Q}}(\gamma)|$  und  $\gamma_p \leftarrow \nu_{p\mathbb{Z}}(N)$ .  
 Für jedes  $\mathfrak{p} \in S_p$ :  
 Solange  $\gamma_p \neq 0$  berechne:  $v_{\mathfrak{p}} \leftarrow \nu_{\mathfrak{p}}(\gamma)$ ,  $\gamma_p \leftarrow \gamma_p - v_{\mathfrak{p}}f(\mathfrak{p}|p)$ .  
 (Sobald  $\gamma_p = 0$ , setze  $v_{\mathfrak{p}} \leftarrow 0$  für alle restlichen  $\mathfrak{p} \in S_p$ .)  
 Falls  $\gamma_p \neq 0$  nach der Schleife über alle  $\mathfrak{p} \in S_p$ , **return** „falsch“ und terminiere.  
 (Andernfalls weiter mit dem nächsten  $p \in \mathcal{P}$ .)
  4. (Ausgabe nach Schleifendurchlauf)  
**return** „wahr“ und  $\nu_S(\gamma) \leftarrow (v_{\mathfrak{p}_1}, \dots, v_{\mathfrak{p}_s})^t$ .
- 

Wenn  $S$ -Einheiten unter den Dirichlet-Elementen gefunden werden, sollen die linearen Abhängigkeiten der zugehörigen Bewertungsvektoren herausgearbeitet werden. Dazu benötigen wir eine Matrix, in der die Informationen über die Bewertungsvektoren verstaut und bearbeitet werden und eine andere Matrix, die analog dazu die entsprechenden Transformationen für die  $S$ -Einheiten selbst festhält. In Anlehnung an [Hes96, Definition 3.2.2.] treffen wir dazu folgende Definition.

### 3.1 Werkzeuge aus der Klassengruppenberechnung

**Definition 3.2.** Eine **Bewertungsmatrix**  $H_{\mathfrak{A}}$  zu einer gegebenen Menge von  $S$ -Einheiten  $\mathfrak{A} = \{\alpha_1, \dots, \alpha_m\} \subseteq \mathfrak{o}_F$  sei die Hermite Normalform der Matrix  $(\nu_S(\alpha_i))_{1 \leq i \leq m}$ .

Die **Relationenmatrix**  $B_{\mathfrak{A}}$  zu  $\mathfrak{A} = \{\alpha_1, \dots, \alpha_m\}$  wird durch die folgende Gleichung definiert:

$$(\mathfrak{p}_1, \dots, \mathfrak{p}_s) H_{\mathfrak{A}} = (\alpha_1, \dots, \alpha_m) B_{\mathfrak{A}}. \quad (3.2)$$

**Bemerkung:** (1) Die Zeilen der Matrixprodukte auf beiden Seiten der Gleichung sind als Potenzprodukte der Einträge des Primidealvektors (bzw. des Vektors von Hauptidealen zu den  $S$ -Einheiten) mit den Spalteneinträgen von  $H_{\mathfrak{A}}$  (bzw.  $B_{\mathfrak{A}}$ ) als Exponenten zu verstehen. Bei dieser Gleichung werden die  $S$ -Einheiten  $\alpha \in \mathfrak{o}_F$  wieder mit den von ihnen erzeugten Hauptidealen  $\alpha \mathfrak{o}_F$  identifiziert. Die multiplikative Kombination von Hauptidealen, die wir durch Verknüpfung mit der Matrix dann auf der rechten Seite vornehmen, ergibt wieder ein Hauptideal. Der Schritt zurück von diesem Hauptideal zum erzeugenden Element in der Ordnung ist modulo Einheiten wohldefiniert. (2) Bewertungs- und Relationenmatrix sind abhängig von der Reihenfolge der Elemente in  $\mathfrak{A}$  und  $S$ . Wir definieren  $\mathfrak{A}$  und  $S$  zwar als Mengen und verwenden bei der Beschreibung der Algorithmen dementsprechend Mengenoperationen. Wir benötigen aber eine festliegende Reihenfolge und arbeiten dazu praktisch mit Listen.

Zu einer Menge von  $S$ -Einheiten zu einer Faktorbasis  $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$  werden die Matrizen aus Definition 3.2 folgendermaßen berechnet:

---

**Algorithmus 9 :** Berechnung von Bewertungs- und Relationenmatrix

---

**Eingabe :** Menge von  $S$ -Einheiten  $\mathfrak{A} = \{\alpha_1, \dots, \alpha_m\}$

**Ausgabe :** Bewertungsmatrix  $H_{\mathfrak{A}}$  und Relationenmatrix  $B_{\mathfrak{A}}$

**Initialisierung:**

$H_{\mathfrak{A}} \leftarrow ()$  mit  $s$  Zeilen und 0 Spalten

$B_{\mathfrak{A}} \leftarrow ()$  mit 0 Zeilen und Spalten

**for**  $i$  von 1 bis  $m$  **do**

$H_{\mathfrak{A}} \leftarrow (H_{\mathfrak{A}} | \nu_S(\alpha_i)) // \nu_S(\alpha_i)$  aus Algorithmus 8

$B_{\mathfrak{A}} \leftarrow \begin{pmatrix} B_{\mathfrak{A}} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \in \mathbb{Z}^{i \times i}$

$T \leftarrow$  Transformationsmatrix  $\in \mathbb{Z}^{i \times i}$ , so dass  $H_{\mathfrak{A}} T$  die Hermite Normalform von  $H_{\mathfrak{A}}$  ist.

$H_{\mathfrak{A}} \leftarrow H_{\mathfrak{A}} T, B_{\mathfrak{A}} \leftarrow B_{\mathfrak{A}} T$

**endfor**

**return**  $H_{\mathfrak{A}}, B_{\mathfrak{A}}$

---

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

Da wir die Menge unserer  $S$ -Einheiten innerhalb der nachfolgenden Algorithmen elementweise vergrößern, werden wir Algorithmus 9 etwas abgewandelt verwenden: Nach dem Auffinden einer neuen  $S$ -Einheit werden Bewertungs- und Relationenmatrix mit den für die zuvor gegebene Menge von  $S$ -Einheiten berechneten Matrizen initialisiert. Die Berechnungen in der *for*-Schleife werden dann nur einmal für die neu gewonnene  $S$ -Einheit durchgeführt.

## 3.2 Konstruktion von Einheiten zu Konjugiertenrichtungen

Wir wollen ein System  $r$  unabhängiger Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  einer beliebigen Ordnung  $R$  berechnen. In diesem Abschnitt verfolgen wir die Idee, die Einheiten wie im vorigen Kapitel als *Einheiten zu Konjugiertenrichtungen* zu konstruieren, so dass die Unabhängigkeit aufgrund der Konjugiertenbetragseigenschaften erfüllt sein muss. Einen alternativen Ansatz werden wir im nächsten Abschnitt beschreiben. Zunächst stellen wir die Grundidee zur Berechnung der Einheit der Maximalordnung  $\mathfrak{o}_F$  zu einer gegebenen Konjugiertenrichtung dar. Danach überlegen wir, wie man dies auf beliebige Ordnungen übertragen kann.

### 3.2.1 Berechnung in der Maximalordnung $\mathfrak{o}_F$

Die Berechnung der Einheiten gestaltet sich nun wie in Kapitel 2 in zwei Teilen: der Konstruktion der Konjugiertenfolgen und der Konstruktion von Einheiten aus Elementen dieser Folgen.

Dazu wählen wir zunächst eine Strategie für die Konstruktion des gewährleistetesten Konjugiertenrichtungssystems (siehe in Kapitel 2, Abschnitt 2.4), so dass die dazu berechneten Einheiten unabhängig sind und konstruieren dann zu jeder Konjugiertenrichtung eine Konjugiertenfolge. Anders als in Kapitel 2 jedoch gestaltet sich die Konstruktion von Einheiten entlang der Konjugiertenfolge. Wir vergleichen nicht mehr die Normbeträge der Elemente, sondern speisen die Bewertungen der davon erzeugten Hauptideale über einer Faktorbasis  $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$  in eine Bewertungsmatrix ein, sofern es sich bei den Elementen um  $S$ -Einheiten handelt. Sobald bei der Reduktion der Bewertungsmatrix auf Hermite Normalform die letzte Spalte einer Nullspalte entspricht, können wir mit der letzten Spalte der zugehörigen Relationenmatrix eine Einheit aus dem Vektor der  $S$ -Einheiten kombinieren.

**Lemma 3.3.** *Es sei  $\mathfrak{o}_F$  die Maximalordnung des Zahlkörpers  $F$ ,  $S = \{\mathfrak{p}_1 \dots \mathfrak{p}_s\}$  eine Faktorbasis und  $H_\Gamma$  die Bewertungsmatrix zu einer Menge von  $S$ -Einheiten  $\Gamma = \{\gamma_1, \dots, \gamma_l\} \subseteq \mathfrak{o}_F$  mit  $l \geq 1$  sowie  $(b_1, \dots, b_l)^t \in \mathbb{Z}^l$  die letzte Spalte der*

### 3.2 Konstruktion von Einheiten zu Konjugiertenrichtungen

zugehörigen Relationenmatrix  $B_\Gamma$ . Wenn  $\text{Rang}(H_\Gamma) < \text{Spaltenzahl}(H_\Gamma)$ , so ist die letzte Spalte von  $H_\Gamma$  eine Nullspalte und dann ist  $\varepsilon := \gamma_1^{b_1} \cdots \gamma_l^{b_l}$  eine Einheit von  $\mathfrak{o}_F$ .

Beweis: Aufgrund von Definition 3.2 gilt die folgende Gleichung:

$$\mathfrak{p}_1^0 \cdots \mathfrak{p}_s^0 = (\gamma_1 \mathfrak{o}_F)^{b_1} \cdots (\gamma_l \mathfrak{o}_F)^{b_l} = \mathfrak{o}_F.$$

Wir setzen  $\varepsilon := \gamma_1^{b_1} \cdots \gamma_l^{b_l}$  und sehen, dass  $\nu_{\mathfrak{p}_i}(\varepsilon) = 0$  für alle  $\mathfrak{p}_i \in S$  gilt. Außerdem ist  $\gamma_1^{b_1} \cdots \gamma_l^{b_l}$  eine  $S$ -Einheit. Denn für alle  $S$ -Einheiten  $\gamma_i \in F$  gilt:  $\nu_{\mathfrak{q}}(\gamma_i) = 0$  für alle  $\mathfrak{q} \in \mathbb{P}_F \setminus S$  und somit

$$\nu_{\mathfrak{q}}(\gamma_1^{b_1} \cdots \gamma_l^{b_l}) = b_1 \underbrace{\nu_{\mathfrak{q}}(\gamma_1)}_{=0} + \dots + b_l \underbrace{\nu_{\mathfrak{q}}(\gamma_l)}_{=0} = 0$$

für alle  $\mathfrak{q} \in \mathbb{P}_F$  mit  $\mathfrak{q} \notin S$ .

Also sind sämtliche Bewertungen von  $\varepsilon = \gamma_1^{b_1} \cdots \gamma_l^{b_l}$  über allen Primidealen von  $F$  gleich Null und  $\varepsilon$  ist eine Einheit von  $\mathfrak{o}_F$ .  $\square$

Es ist dann allerdings noch zu prüfen, ob ein Potenzprodukt von Konjugiertenfolgeelementen, das wir solchermaßen gefunden haben, eine Einheit zu der Konjugiertenrichtung  $(I, J)$  ist. Wie dieser Test realisiert werden kann, wollen wir im Anschluss thematisieren. Zunächst dokumentieren wir das konkrete Vorgehen im Falle einer vorab gegebenen Faktorbasis  $S$  im folgenden Algorithmus (Algorithmus 10).

**Bemerkung 3.4.** *Wenn die letzte Spalte der Bewertungsmatrix  $H_\Gamma$  eine Nullspalte ist, kann es passieren, dass die zugehörige Einheit noch nicht die gesuchte Einheit ist. In diesem Fall müssen wir die Nullspalte, die sich dazu ergeben hat, bei den darauffolgenden Berechnungen ignorieren, da sie nach jeder Reduktion wieder als letzte Spalte der Bewertungsmatrix auftreten kann. Erst, wenn sich eine weitere Nullspalte ergibt, erhalten wir eine neue Einheit. Deshalb zählen wir die Nullspalten, die gefunden werden, deren zugehörige Einheiten den Anforderungen aber nicht genügen. Eine weitere zu untersuchende Einheit ergibt sich, wenn der Rang von  $H_\Gamma$  kleiner ist als die Anzahl der Spalten von  $H_\Gamma$  minus die Anzahl der zuvor gefundenen Nullspalten. In späteren Algorithmen bezeichnen wir diese Bedingung zur Abkürzung in den Algorithmen mit „ $H_\Gamma$  weist neue Nullspalte auf“. Es kann bei der Transformation auf Hermite Normalform vorkommen, dass eine der bereits erkannten Nullspalten hinter der sich neu ergebenden Nullspalte steht. Dann müssen wir natürlich auch die zu der neuen Nullspalte gehörige Spalte der Relationenmatrix auswählen. Abkürzend werden wir in den folgenden Algorithmen davon sprechen, dass wir die „entsprechende Spalte von  $B_\Gamma$ “ auswählen. In der Praxis entfernen wir ein Dirichlet-Element, dessen Bewertungsvektor*

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

eine lineare Abhängigkeit in der Bewertungsmatrix erbracht hat, ohne dass die zugehörige Einheit den Anforderungen genügt, wieder aus der Liste der betrachteten  $S$ -Einheiten und setzen Bewertungs- und Relationenmatrix wieder zurück. Um in den folgenden Algorithmen aber das Wesentliche darzustellen, bleiben wir bei den festgelegten Sprechweisen.

---

**Algorithmus 10** : Berechnung einer Einheit der Maximalordnung zur Konjugiertenrichtung  $(I, J)$  mit Bewertungsmatrixmethode

---

**Eingabe** : Zahlkörper  $F$ , Faktorbasis  $S$ , Konjugiertenrichtung  $(I, J)$

**Ausgabe** : eine Einheit  $\varepsilon \in U(\mathfrak{o}_F)$  zur Konjugiertenrichtung  $(I, J)$

**Initialisierung:**

Menge der  $S$ -Einheiten unter den Dirichlet-Elementen  $\Gamma \leftarrow \{\}$

Bewertungsmatrix  $H_\Gamma \leftarrow ()$ , Relationenmatrix  $B_\Gamma \leftarrow ()$

$k \leftarrow 0, \gamma_k \leftarrow 1, L \leftarrow (\gamma_k)$

$flag \leftarrow false, \text{Nullspaltenzahl} \leftarrow 0$

**while**  $flag = false$  **do**

Konstruiere nächstes Element  $\gamma_{k+1}$  der Konjugiertenfolge zu  $(I, J)$ :

Rufe dazu *Algorithmus 3* mit  $(\mathfrak{o}_F, (I, J), L, \mu = k + 1)$  auf und setze

$\gamma_{k+1}$  als das letzte Element der dort konstruierten Folge.

**if**  $|N(\gamma_{k+1})| = 1$  **then**

$\varepsilon \leftarrow \gamma_{k+1}$

$flag \leftarrow true$

**else**

**if**  $\gamma_{k+1}$  ist  $S$ -Einheit (siehe *Algorithmus 8*) **then**

$\Gamma \leftarrow \Gamma \cup \{\gamma_{k+1}\}, l \leftarrow \#\Gamma$

Bilde  $H_\Gamma$  und  $B_\Gamma$  zu  $\Gamma$  (mit *Algorithmus 9*).

**if**  $\text{Rang}(H_\Gamma) < \text{Spaltenzahl}(H_\Gamma) - \text{Nullspaltenzahl}$  **then**

$\{\hat{\gamma}_1, \dots, \hat{\gamma}_l\} \leftarrow \Gamma$

$(b_1, \dots, b_l)^t \leftarrow$  entsprechende Spalte von  $B_\Gamma$

$\varepsilon \leftarrow \hat{\gamma}_1^{b_1} \dots \hat{\gamma}_l^{b_l}$

**if**  $\varepsilon$  Einheit zur Konjugiertenrichtung  $(I, J)$  **then**

$flag \leftarrow true$

**else**

$\text{Nullspaltenzahl} \leftarrow \text{Nullspaltenzahl} + 1$

**endif**

**endif**

**endif**

**endif**

$L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1})$

$k \leftarrow k + 1$

**endwhile**

**return**  $\varepsilon$

---

### 3.2 Konstruktion von Einheiten zu Konjugiertenrichtungen

Falls ein Konjugiertenfolgeelement selbst eine Einheit ist, brauchen die anschließenden Berechnungen und der Test nicht durchgeführt zu werden. In obenstehendem Algorithmus haben wir eine entsprechende Abfrage eingefügt, in den späteren Algorithmen dieses Kapitels wollen wir der Kürze halber darauf verzichten, das extra zu vermerken. Innerhalb der Beispielerrechnungen wird dies aber durchgeführt.

**Korrektheit des Algorithmus:** Der Algorithmus terminiert spätestens, wenn in der Konjugiertenfolge ein Element auftritt, das zu einem vorherigen assoziiert ist. Entsprechend der vormaligen Überlegungen muss dieser Fall in endlicher Zeit eintreten, da es nur endlich viele nicht-assoziierte Elemente einer Ordnung mit beschränkter Norm gibt. Nun könnte man sich theoretisch vorstellen, dass nach einigen Konjugiertenfolgeelementen, die  $S$ -Einheiten waren, innerhalb der Konjugiertenfolgen keine weiteren  $S$ -Einheiten auftreten. Dieses Problem lässt sich theoretisch umgehen, indem man eine Faktorbasis wählt, die alle Primideale mit Norm unterhalb der Normbetragsschranke  $C$  enthält. Dass eine wesentlich kleinere Faktorbasis praktisch ausreicht, werden wir später sehen. So scheinen die Bewertungen der Konjugiertenfolgeelementen über einem Primideal nach den Beobachtungen in Abschnitt 3.4 zufällig und unabhängig verteilt, so dass man selbst im Falle einer relativ kleinen Faktorbasis in einer unendlichen Folge von Konjugiertenfolgeelementen auch immer eine unendliche Teilfolge von  $S$ -Einheiten findet. Innerhalb dieser Teilfolge existieren ebenfalls nur endlich viele nicht-assoziierte Elemente mit beschränkter Norm.

#### Test: Einheit zur Konjugiertenrichtung

Es sei  $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$  eine Faktorbasis und  $\Gamma = \{\gamma_1, \dots, \gamma_l\}$  seien  $S$ -Einheiten aus einer Menge von Dirichlet-Elementen zu  $(I, J)$ , so dass die Gleichung

$$\mathfrak{p}_1^0 \cdots \mathfrak{p}_s^0 = (\gamma_1 \sigma_F)^{b_1} \cdots (\gamma_l \sigma_F)^{b_l} \quad \text{gilt.}$$

Nicht jede Einheit, die sich als ein solches Potenzprodukt ergibt, ist eine Einheit zur Konjugiertenrichtung. So können sich zum Beispiel Torsionseinheiten ergeben (siehe Beispiel 5.1 im Anhang auf S. 97). Deshalb benötigen wir einen Test dafür, dass die gewonnene Einheit  $\varepsilon = \gamma_1^{b_1} \cdots \gamma_l^{b_l}$  die folgenden Eigenschaften besitzt:

$$\begin{aligned} |\varepsilon^{(i)}| &\geq 1 \quad \forall i \in I \\ |\varepsilon^{(j)}| &< 1 \quad \forall j \in J. \end{aligned} \tag{3.3}$$

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

Aufgrund der Gültigkeit der Bedingungen

$$\begin{aligned} |\gamma_{k+1}^{(i)}| &\geq |\gamma_k^{(i)}| \quad \forall i \in I \\ |\gamma_{k+1}^{(i)}| &< |\gamma_k^{(i)}| \quad \forall j \in J \end{aligned}$$

für alle Elemente der Konjugiertenfolge  $(\gamma_n)_{n \in \mathbb{N}}$  zu  $(I, J)$  waren in Kapitel 2 die Bedingungen aus (3.3) für den Quotienten zweier zueinander assoziierter Konjugiertenfolgenglieder  $\varepsilon = \gamma_\mu / \gamma_\nu$  mit  $\mu > \nu$  gewährleistet. Die Überlegung, welche Potenzprodukte die Bedingungen aus (3.3) sicher erfüllen, orientiert sich an dieser Grundidee: Es muss im Potenzprodukt  $\gamma_1^{b_1} \cdots \gamma_l^{b_l}$  zu jedem  $\gamma_i$  mit negativer Potenz  $b_i$  ein  $\gamma_j$  mit positiver Potenz  $b_j$  vorliegen, so dass  $i < j$  und  $b_i \leq b_j$ . Wir stellen in Algorithmus 11 einen Test für dieses Kriterium dar. Dabei berücksichtigen wir, dass der Kehrwert des Potenzprodukts ebenfalls eine Einheit ergibt. Falls also das Dirichlet-Element mit dem höchsten Index im Nenner steht, testen wir gleich den Kehrwert.

---

**Algorithmus 11** : Spaltentest: Ist  $\gamma_1^{b_1} \cdots \gamma_l^{b_l}$  Einheit zur Konjugiertenrichtung?

---

**Eingabe** : Entsprechende Spalte  $(b_1, \dots, b_l)^t \in \mathbb{Z}^l$  der Relationenmatrix

**Ausgabe** : *true* und passende Einheit  $\varepsilon$ , falls die Potenzen im Nenner durch Potenzen im Zähler aufgewogen werden, andernfalls

*false*

```

if  $b_l < 0$  then
  |  $(b_1, \dots, b_l)^t \leftarrow (-b_1, \dots, -b_l)^t$ 
endif
 $sum \leftarrow 0$ 
 $j \leftarrow l$ 
while  $sum \geq 0$  und  $j \geq 1$  do
  |  $sum \leftarrow sum + j$ 
  |  $j \leftarrow j - 1$ 
endwhile
if  $sum < 0$  then
  | return false
else
  | return true,  $\gamma_1^{b_1} \cdots \gamma_l^{b_l}$ 
endif

```

---

Es werden durch diesen Test zwar keine Einheiten falsch positiv getestet, allerdings ist nicht jede Einheit, die wir aussortieren, keine Einheit zur Konjugiertenrichtung. Das Bestehen des Tests stellt nur eine hinreichende Bedingung dar. Das liegt daran, dass sich eventuell auch andere Dirichlet-Elemente in dem Produkt

### 3.2 Konstruktion von Einheiten zu Konjugiertenrichtungen

noch ausgleichen, zum Beispiel könnte bei

$$\frac{\cdots \gamma_{k-3} \gamma_{k-2} \gamma_k^3}{\cdots \gamma_{k-1}^4}$$

das „übriggebliebene“  $\gamma_{k-1}$  eventuell durch das Produkt  $\gamma_{k-3} \gamma_{k-2}$  ausgeglichen werden (siehe wiederum Beispiel 5.1 im Anhang). Das hängt allerdings von den genauen Werten ab und wir würden uns, um dies zu testen, wieder auf die Ebene der Konjugiertenbeträge begeben müssen. Das ist aus zwei Gründen ungünstig: Auf der einen Seite ist die Berechnung der Konjugierten relativ aufwändig. Auf der anderen Seite wurde bereits erheblichen Aufwand zur Konstruktion der Konjugiertenfolgeelemente betrieben, um für diese spezielle Konjugiertenbetrags-eigenschaften zu gewährleisten. Diese Eigenschaften der Dirichlet-Elemente sollten nun zur Anwendung kommen, da sich sonst kein Vorteil gegenüber dem Vorgehen ergibt, beliebige glatte Elemente der Ordnung zu konstruieren, die zugehörigen Bewertungsvektoren zu reduzieren und im Falle des Auftretens einer Nullspalte die Konjugiertenbetrags-eigenschaften der resultierenden Einheiten zu untersuchen.

**Bemerkung 3.5.** (1) *Günstigerweise sollte der Test vor Berechnung der Einheit direkt für die entsprechende Spalte der Relationenmatrix durchgeführt werden, da die Berechnung des Potenzprodukts selbst verhältnismäßig aufwändig ist. Bei großen Koeffizienten der entsprechenden Relationenmatrixspalte kann dies sehr zeitintensiv und es daher zweckmäßig sein, zusätzlich solche Relationenmatrixspalten auszusortieren, deren Einträge eine gewisse Größe überschreiten. Es sind verschiedene Kriterien denkbar: Man könnte eine Obergrenze für die Summe der Beträge der Koeffizienten festlegen oder nur solche Relationenmatrixspalten verwenden, deren einzelne Koeffizientenbeträge unter einer gewissen Schranke liegen. Sofern jedoch nichts anderes gesagt wird, wird in den kommenden Beispielen ohne eine solche zusätzliche Bedingung an die Relationenmatrixspalten gerechnet.*

(2) *Es ist weiterhin anzumerken, dass neben diesem Test, der bereits zu viele der berechneten Einheiten fälschlicherweise aussortiert, auch die strikte Erfüllung von Bedingung (3.3) als Kriterium für die Unabhängigkeit der Einheiten zu scharf ist. Experimentell kann man feststellen, dass bei der Konstruktion eines Systems von Einheiten zu  $r$  verschiedenen einfachen Konjugiertenrichtungen mit dem oben beschriebenen Algorithmus ohne das Aussieben mit Hilfe des Spalten-tests, lediglich unter Ausnahme von Torsionseinheiten, in vielen Beispielen dennoch Unabhängigkeit zwischen den Einheiten besteht. Der Grund dafür liegt darin, dass die Konstruktion aus Potenzprodukten von Konjugiertenfolgeelementen zu verschiedenen Konjugiertenrichtungen eine starke Variation hinsichtlich der Konjugiertenbeträge der resultierenden Einheiten bedingt. Durch diese Variation der Konjugiertenbeträge ergibt sich lineare Unabhängigkeit für die  $L$ -Vektoren und damit Unabhängigkeit für die Einheiten. Wie man dies ausnutzen kann, sehen wir in Abschnitt 3.3.*

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

Der wesentliche Vorteil des in diesem Abschnitt vorgestellten Vorgehens zur Berechnung von Einheiten zu einer gegebenen Konjugiertenrichtung besteht darin, dass man (abgesehen von der Konstruktion der Konjugiertenfolgeelemente wie bisher) keine weiteren Schwierigkeiten durch Verwendung reeller Arithmetik bekommt, da ausschließlich mit den Einträgen ganzzahliger Matrizen gearbeitet wird. Bei Wahl von einfachen Konjugiertenrichtung  $(I_i, J_i) = (\{i\}, \{1, \dots, r_1 + r_2\} \setminus \{i\})$  mit  $(1 \leq i \leq r)$  und Berechnung von Einheiten zu diesen Konjugiertenrichtungen (mit Algorithmus 10) garantiert das Bestehen des Spaltentests die Unabhängigkeit der berechneten Einheiten. Es ist keine weitere Berechnung und Überprüfung im Reellen (durch Übergang zu den  $L$ -Vektoren) erforderlich.

### 3.2.2 Berechnung in beliebigen Ordnungen

In diesem Abschnitt übertragen wir das Vorgehen für die Berechnung eines Systems von  $r$  unabhängigen Einheiten der Maximalordnung  $\mathfrak{o}_F$  aus dem vorherigen Abschnitt auf die Berechnung in beliebigen Ordnungen  $R \subseteq \mathfrak{o}_F$ . Im Allgemeinen kann man Hauptideale in einer beliebigen Ordnung nicht mehr eindeutig faktorisieren. Deshalb müssen wir weitere Bedingungen an die Primideale, die wir in die Faktorbasis  $S$  aufnehmen, stellen.

**Lemma 3.6.** *Es sei  $F = \mathbb{Q}[\rho]$  der algebraische Zahlkörper, der aus  $\mathbb{Q}$  durch Adjunktion der Nullstelle  $\rho$  des über  $\mathbb{Q}$  normierten, irreduziblen Polynoms  $f(t) \in \mathbb{Z}[t]$  mit Diskriminante  $d(f)$  hervorgeht. Weiter sei  $\mathcal{F} = \{x \in \mathfrak{o}_F \mid x\mathfrak{o}_F \subseteq \mathbb{Z}[\rho]\}$  der Führer von  $\mathbb{Z}[\rho]$  in  $\mathfrak{o}_F$  und  $\tilde{\mathcal{F}} = \{x \in \mathfrak{o}_F \mid x\mathfrak{o}_F \subseteq R\}$  sei der Führer der beliebigen Ordnung  $R$  in  $\mathfrak{o}_F$ . Dann gilt für alle Primideale  $\mathfrak{P}$  aus  $\mathfrak{o}_F$ , deren Norm eine Primzahlpotenz ist, deren Primfaktor nicht  $d(f)$  teilt, dass  $\mathfrak{P} \in \mathcal{D}_{\mathfrak{o}_F, \tilde{\mathcal{F}}}$ :*

$$\{\mathfrak{P} \text{ Primideal von } \mathfrak{o}_F \mid N(\mathfrak{P}) = p^k \text{ und } p \nmid d(f)\} \subseteq \mathcal{D}_{\mathfrak{o}_F, \tilde{\mathcal{F}}}. \quad (3.4)$$

Beweis: Es sei nun  $p \in P$  eine feste, beliebige Primzahl mit  $p \nmid d(f)$ . Aus Lemma 1.18 mit  $K = \mathbb{Q}$  und  $\mathfrak{o}_K = \mathbb{Z}$  wissen wir, dass dann das Ideal  $p\mathfrak{o}_F$  in  $\mathcal{D}_{\mathfrak{o}_F, \mathcal{F}}$  ist. Sei  $\mathfrak{P}$  ein Primideal aus  $\mathfrak{o}_F$ , das als Norm eine Potenz dieser Primzahl hat. Dann liegt  $\mathfrak{P}$  über  $p$ , es gilt also  $p\mathfrak{o}_F \subseteq \mathfrak{P}$ . Daraus folgt, dass  $\mathfrak{P} \in \mathcal{D}_{\mathfrak{o}_F, \mathcal{F}}$ . Angenommen  $\mathfrak{P} \notin \mathcal{D}_{\mathfrak{o}_F, \tilde{\mathcal{F}}}$ . Dann würde  $\mathfrak{P} + \mathcal{F} \subsetneq \mathfrak{o}_F$  gelten und daraus würde folgen, dass  $p\mathfrak{o}_F + \mathcal{F} \subseteq \mathfrak{P} + \mathcal{F} \subsetneq \mathfrak{o}_F$  gilt. Dies steht im Widerspruch zur Voraussetzung. Des Weiteren gilt, dass  $\mathcal{F} \subseteq \tilde{\mathcal{F}}$ . Angenommen es existierte ein  $x \in \mathfrak{o}_F$  mit  $x\mathfrak{o}_F \subseteq \mathbb{Z}[\rho]$  und  $x\mathfrak{o}_F \not\subseteq R$ . Dann existiert ein  $y \in x\mathfrak{o}_F$  mit  $y \in \mathbb{Z}[\rho]$  und  $y \notin R$ . Dies stände im Widerspruch zu  $\mathbb{Z}[\rho] \subseteq R$ . Und somit gilt, dass  $\mathcal{D}_{\mathfrak{o}_F, \mathcal{F}} \subseteq \mathcal{D}_{\mathfrak{o}_F, \tilde{\mathcal{F}}}$ . (Die Ideale, die in  $\mathfrak{o}_F$  komaximal zum kleineren Ideal  $\mathcal{F}$  sind, sind erst recht komaximal zum größeren Ideal  $\tilde{\mathcal{F}}$ .) Daher können wir folgern, dass  $\mathfrak{P} \in \mathcal{D}_{\mathfrak{o}_F, \tilde{\mathcal{F}}}$ .  $\square$

Für eine Faktorbasis  $\tilde{S} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} \subseteq \mathcal{D}_{\mathfrak{o}_F, \tilde{\mathcal{F}}}$  und eine  $\tilde{S}$ -Einheit  $\gamma \in R \subseteq \mathfrak{o}_F$  sei  $\mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_s^{v_s}$  die eindeutige Primidealfaktorisierung von  $\gamma\mathfrak{o}_F$ . Dann ist wegen der Isomorphie  $\mathcal{D}_{\mathfrak{o}_F, \tilde{\mathcal{F}}} \simeq \mathcal{D}_{R, \tilde{\mathcal{F}}}$  (siehe Lemma 1.17)  $(\mathfrak{p}_1 \cap R)^{v_1} \cdots (\mathfrak{p}_s \cap R)^{v_s}$  die eindeutige Primidealfaktorisierung des Hauptideals  $\gamma R$ . Zur Berechnung der Einheit einer beliebigen Ordnung  $R$  zur Konjugiertenrichtung  $(I, J)$  arbeiten wir also weiterhin mit den Bewertungsvektoren der Hauptideale von Dirichlet-Elementen in  $\mathfrak{o}_F$ . Es ist lediglich die Faktorbasis, wie im folgenden Algorithmus 12 dargestellt, zu modifizieren.

---

**Algorithmus 12** : Berechnung einer Einheit der Ordnung  $R$  des algebraischen Zahlkörpers  $F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$  zur Konjugiertenrichtung  $(I, J)$

---

**Eingabe** : Zahlkörper  $F$ , Faktorbasis  $S$ , beliebige Ordnung  $R$  von  $F$ ,  
Konjugiertenrichtung  $(I, J)$

**Ausgabe** : Einheit  $\varepsilon \in U(R)$  zur Konjugiertenrichtung  $(I, J)$

**Initialisierung**:

$\tilde{S} \leftarrow \{\mathfrak{p} \in S \mid N(\mathfrak{p}) = p^k, k \in \mathbb{Z}^{\geq 1}, p \nmid d(f)\}$

Menge der  $\tilde{S}$ -Einheiten aus den Dirichlet-Elementen  $\Gamma \leftarrow \{\}$

Bewertungsmatrix  $H_\Gamma \leftarrow ()$ ,  $\tilde{S}$ -Einheitenmatrix  $B_\Gamma \leftarrow ()$

$k \leftarrow 0, \gamma_k \leftarrow 1, L \leftarrow \{\gamma_0\}$

$flag \leftarrow false$

**while**  $flag = false$  **do**

Konstruiere nächstes Element  $\gamma_{k+1}$  der Konjugiertenfolge zu  $(I, J)$ :

Rufe dazu *Algorithmus 3* mit  $(R, (I, J), L, \mu = k + 1)$  auf und setze

$\gamma_{k+1}$  als letztes Element der dort konstruierten Folge.

**if**  $\gamma_{k+1}$  ist  $\tilde{S}$ -Einheit (siehe *Algorithmus 8*) **then**

$\Gamma \leftarrow \Gamma \cup \{\gamma_{k+1}\}, l \leftarrow \#\Gamma$

Berechne  $H_\Gamma$  und  $B_\Gamma$  zu  $\Gamma$  wie in *Algorithmus 9*.

**if**  $H_\Gamma$  weist neue Nullspalte auf **then**

$(b_1, \dots, b_l)^t \leftarrow$  entsprechende Spalte von  $B_\Gamma$

$\{\hat{\gamma}_1, \dots, \hat{\gamma}_l\} \leftarrow \Gamma$

$\varepsilon \leftarrow \hat{\gamma}_1^{b_1} \cdots \hat{\gamma}_l^{b_l}$

**if**  $\varepsilon \in R$  und Einheit zur Konjugiertenrichtung  $(I, J)$  **then**

$flag \leftarrow true$

**endif**

**endif**

**endif**

$L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1})$

$k \leftarrow k + 1$

**endwhile**

**return**  $\varepsilon$

---

**Bemerkung 3.7.** In Bezug auf die Gesamtzielsetzung, Grundeinheiten einer beliebigen Ordnung zu berechnen, würde die eben vorgestellte Methode nicht zum Tragen kommen, deshalb vertiefen wir die noch offenen Punkte, z.B. Wahl einer günstigen Faktorbasis, hier nicht weiter. Wie bereits in Kapitel 1 angesprochen, kann der dritte Schritt zur Berechnung von Grundeinheiten einer beliebigen Ordnung beschleunigt werden, wenn wir zunächst unabhängige Einheiten der Maximalordnung berechnen und dann wie in [Wil93, Algorithmus 4.20] die Erzeuger der  $p$ -maximalen Obergruppen in  $U(\mathfrak{o}_F)$  bestimmen, um zunächst die Grundeinheiten der Maximalordnung zu berechnen. Danach können wie in [Wil93,

*Abschnitt 4.2.] die Grundeinheiten der beliebigen Ordnung bestimmt werden. Da für die Berechnung von Grundeinheiten beliebiger Ordnungen also ohnehin zunächst die Berechnung von unabhängigen Einheiten der Maximalordnung durchgeführt wird, werden wir uns im Folgenden auf letzteres konzentrieren.*

### 3.3 Unabhängige Einheiten mit Bewertungsmatrizen

Im vorherigen Abschnitt haben wir den Ansatz beschrieben, unabhängige Einheiten von  $\mathfrak{o}_F$  als Einheiten zu Konjugiertenrichtungen zu konstruieren. Dazu werden die Konjugiertenrichtungen so gewählt, dass sie sukzessive die Unabhängigkeit der zugehörigen Einheiten garantieren. Bei diesem Ansatz pochen wir für jede zur Konjugiertenrichtung  $(I, J)$  konstruierte Einheit  $\varepsilon$  auf Einhaltung der Bedingungen  $|\varepsilon^{(i)}| \geq 1 \forall i \in I$  und  $|\varepsilon^{(j)}| < 1 \forall j \in J$ , da wir sonst die Unabhängigkeit a priori nicht gewährleisten können. Das Bestehen auf diesen Bedingungen, das wir noch dazu in einem nur hinreichenden Test realisieren können, führt aber dazu, dass die Vorzüge des Bewertungsmatrixansatzes nicht vollständig zum Tragen kommen können. Zur Verdeutlichung geben wir ein Beispiel an.

**Beispiel 3.8.** *Es sei  $F \cong \mathbb{Q}/(t^{17} - 5)\mathbb{Q}$ . Wir wollen 8 unabhängige Einheiten der Maximalordnung berechnen. Dazu wählen wir zunächst einfache Konjugiertenrichtungen und konstruieren mit Algorithmus 10 die zugehörigen Einheiten. Als Faktorbasis  $S$  nehmen wir die Primideale mit Norm unterhalb von 85, so dass  $\#S = 23$  ist. Zur Konstruktion der Konjugiertenfolgen wählen wir Algorithmus 3. Zur Berechnung der 8 Einheiten werden dann insgesamt 971 Konjugiertenfolgeelemente berechnet, von denen 811 keine  $S$ -Einheiten sind. Aus den verbleibenden 160 Konjugiertenfolgeelementen, die in die Bewertungsmatrizen eingespeist werden, gewinnen wir 43 mal eine Nullspalte. Von den entsprechenden Spalten der Relationenmatrix verwirft der Test (Algorithmus 11) auf die Erfüllung der Konjugiertenrichtungsbedingung 25 Spalten. Tatsächlich haben 17 der zugehörigen Einheiten nicht die Konjugiertenbedingungen (3.3) erfüllt, wie man nachträglich prüft (drei davon waren Torsionseinheiten).*

An dem Beispiel kann man erkennen, dass die Ausbeute an Einheiten pro  $S$ -Einheit eigentlich sehr hoch ist. Experimentell zeigt sich zudem, dass wenn wir bei der Konstruktion zu jeder Konjugiertenrichtung gleich die erste Nicht-Torsionseinheit, die sich im Verlauf der Konstruktion ergibt, wählen (ohne die Bedingung (3.3) zu gewährleisten) dennoch in den meisten Fällen Unabhängigkeit besteht. Wir stellen einen Algorithmus zur Berechnung unabhängiger Einheiten der Maximalordnung vor, der diesem Punkt Rechnung trägt.

---

**Algorithmus 13** : Algorithmus zur Berechnung von  $r$  unabhängigen Einheiten der Maximalordnung mit vorab gewählter Faktorbasis

---

**Eingabe** : Zahlkörper  $F$  vom Grad  $n$ , bereits berechnete unabhängige Einheiten  $\varepsilon_1, \dots, \varepsilon_m$  von  $\mathfrak{o}_F$ , Faktorbasis  $S$

**Ausgabe** : Unabhängige Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  von  $\mathfrak{o}_F$

**while**  $m < r$  **do**

Berechne mit Algorithmus 7 die gewährleistende Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$  zu  $\varepsilon_1, \dots, \varepsilon_m$ .

// Berechne  $\varepsilon_{m+1}$ :

Menge der  $S$ -Einheiten unter den Dirichlet-Elementen  $\Gamma \leftarrow \{\}$

Bewertungsmatrix  $H_\Gamma \leftarrow ()$ , Relationenmatrix  $B_\Gamma \leftarrow ()$

$k \leftarrow 0, \gamma_k \leftarrow 1, L \leftarrow (\gamma_0)$

$j \leftarrow m$

**while**  $j = m$  **do**

Konstruiere nächstes Element  $\gamma_{k+1}$  der Konjugiertenfolge zu

$(I_{m+1}, J_{m+1})$ : Rufe dazu *Algorithmus 3* mit

$(\mathfrak{o}_F, (I_{m+1}, J_{m+1}), L, \mu = k + 1)$  auf

und setze  $\gamma_{k+1}$  als das letzte Element der dort konstruierten Folge.

**if**  $\gamma_{k+1}$  ist  $S$ -Einheit (siehe *Algorithmus 8*) **then**

$\Gamma \leftarrow \Gamma \cup \{\gamma_{k+1}\}$

Bilde  $H_\Gamma$  und  $B_\Gamma$  zu  $\Gamma$  (mit *Algorithmus 9*)

$l \leftarrow \#\Gamma$

**if**  $H_\Gamma$  weist neue Nullspalte auf **then**

$\{\hat{\gamma}_1, \dots, \hat{\gamma}_l\} \leftarrow \Gamma$

$(b_1, \dots, b_l)^t \leftarrow$  entsprechende Spalte von  $B_\Gamma$

$\varepsilon \leftarrow \hat{\gamma}_1^{b_1} \dots \hat{\gamma}_l^{b_l}$

Bestimme mit MLLL ein minimales Erzeugendensystem

$\eta_1, \dots, \eta_{\hat{m}}$  mit  $(\hat{m} \leq m + 1)$  von  $\langle \varepsilon_1, \dots, \varepsilon_m, \varepsilon \rangle$

und setze  $j \leftarrow \hat{m}$  sowie  $\varepsilon_i \leftarrow \eta_i$  ( $1 \leq i \leq \hat{m}$ ).

**endif**

$L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1})$

$k \leftarrow k + 1$

**endif**

**endwhile**

$m \leftarrow m + 1$

**endwhile**

**return**  $\varepsilon_1, \dots, \varepsilon_r$

---

Zur Sicherung der Unabhängigkeit der berechneten Einheiten kommen bei diesem Vorgehen allerdings an zwei Stellen (Berechnung der gewährleistenden Konjugiertenrichtung und MLLL-Reduktion der berechneten Einheiten) die reellen  $L$ -Vektoren der Einheiten ins Spiel. Wir behandeln diese Punkte wie in [FP06, Abschnitt 5 und 6] dargelegt.

**Beispiel 3.8** (fortgesetzt): *Wir lassen 8 unabhängige Einheiten der Maximalordnung von  $F \cong \mathbb{Q}/(t^{17} - 5)\mathbb{Q}$  mit dem Algorithmus 13 berechnen. Als Faktorbasis wählen wir wieder alle Primideale mit Norm unterhalb von 85. Wir betrachten die insgesamt für alle Einheiten zusammengenommen durchgeführten Berechnungen. Es werden 652 Konjugiertenfolgeelemente berechnet. 537 davon sind keine  $S$ -Einheiten. Aus den verbleibenden 115  $S$ -Einheiten unter den Konjugiertenfolgeelementen wird elf mal eine Nullspalte gewonnen, die zugehörige Einheit war in drei Fällen eine Torsionseinheit, in den restlichen acht Fällen war die gewonnene Einheit von den vorherigen unabhängig.*

Wie man an vielen Beispielen sieht, reicht das Aussortieren der Torsionseinheiten, die sich aus den Potenzprodukten der Konjugiertenfolgeelemente ergeben, häufig bereits aus, um die passenden Einheiten zu finden. Es muss aber nicht jede Einheit  $\varepsilon_{m+1}$ , die wir aus dem Potenzprodukt der  $S$ -Einheiten unter den Konjugiertenfolgeelementen zur gewährleistenden Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$  gewonnen haben und die keine Torsionseinheit ist, von den vorhergehenden Einheiten  $\varepsilon_1, \dots, \varepsilon_m$  unabhängig sein (siehe Beispiel 5.1 im Anhang). Die Tatsache, dass dies in vielen Fällen dennoch zutrifft, zeichnet die Verwendung von Konjugiertenfolgeelementen gegenüber dem Vorgehen in der Klassengruppenberechnung, beliebige  $S$ -Einheiten zu verwenden, um Einheiten zu gewinnen, aus.

### 3.4 Zur Wahl der Faktorbasis

Zur Berechnung der Einheiten mit Bewertungsmatrizen benötigen wir eine Menge von Primidealen, die wir Faktorbasis genannt haben. Für die bisher vorgestellten Algorithmen ist die Wahl dieser Faktorbasis vorab zu treffen. Bei der Wahl dieser Menge besteht nun ein Konflikt zwischen zwei Aspekten. Einerseits möchten wir, dass viele der Konjugiertenfolgeelemente glatt über der Faktorbasis sind. Andererseits wachsen mit der Anzahl der Primideale in der Faktorbasis (*Größe der Faktorbasis*):

- der Aufwand für die Berechnung der Faktorbasis,
- der Aufwand zu prüfen, ob ein Element glatt ist und gegebenenfalls der Aufwand für die Berechnung der Bewertungsvektoren  $\nu_S$ ,
- der Aufwand für die Bestimmung der Bewertungs- und Relationenmatrix.

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

Im Folgenden nennen wir diese Aufwände zusammenfassend **Faktorisierungsaufwand**.

Man ist also daran interessiert, als Faktorbasis eine Menge von Primidealen zu wählen, bei der ein Ausgleich zwischen der jeweiligen Zunahme des Gesamtrechenaufwands durch Verkleinerung oder Vergrößerung der Faktorbasis besteht.

#### Faktorbasis: Primideale mit Norm unterhalb einer Schranke $B$

Wir verwenden und untersuchen in diesem Abschnitt den Ansatz, als Faktorbasis die Primideale mit Norm unterhalb einer Schranke  $B$  zu verwenden. Bevor wir uns dem Versuch zuwenden, eine Empfehlung für die Wahl der Schranke  $B$  zu geben, führen wir ein Beispiel aus unseren experimentellen Untersuchungen an, um den Zusammenhang zwischen Schrankengröße, Faktorbasisgröße und Rechenzeit zu verdeutlichen und einen ersten Einblick in die Größenordnungen der zu wählenden Parameter zu bekommen.

**Beispiel 3.9.** *Es sei  $F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$  mit  $f(t) = t^{14} - 4t^6 - t^3 + 8$  und Einheitsrang  $r = 6$ . Wir lassen für verschiedene Schranken jeweils solange Konjugiertenfolgelemente der Maximalordnung zu den  $r$  verschiedenen einfachen Konjugiertenrichtungen konstruieren, bis für jede Konjugiertenrichtung eine Nullspalte in der Bewertungsmatrix auftritt (ob die dazugehörige Einheit zur Konjugiertenrichtung passt oder eine Nicht-Torsionseinheit ist, lassen wir hier noch außer Acht) und betrachten die aus der Höhe der Schranke  $B$  resultierende Anzahl der Faktorbasiselemente, die benötigte Gesamtzeit, die Anzahl der insgesamt berechneten Dirichlet-Elemente und die Anzahl der  $S$ -Einheiten unter den Dirichlet-Elementen, sowie den Anteil der Dirichlet-Elemente, die keine  $S$ -Einheiten waren, an der Gesamtzahl berechneter Dirichlet-Elemente (Ausschussquote). Ausführliche Ergebnisse findet man im Anhang (Abschnitt 5.2).*

Tabelle 3.1: Rechenzeiten, Ausschussquoten und Faktorbasisgrößen für verschiedene Schranken

Schranke $B$	10	25	75	125	150	250	450	650
$\#S$	6	10	25	35	37	57	115	129
Rechenzeit (sec)	151	39.19	32.69	38.47	39.97	49.24	69.91	89.77
Dirichlet-Elemente	663	390	322	321	321	312	301	301
$S$ -Einheiten	6	58	101	128	129	159	198	217
Ausschussquote	0.94	0.85	0.68	0.60	0.59	0.49	0.34	0.28

*Exemplarisch erkennt man folgende Struktur: zunächst nimmt die Berechnungszeit mit dem Anwachsen der Größe der Schranke (und damit der Faktorbasisgröße) bis zu einem gewissen Wert ab. Nach diesem kritischen Wert ist dann wieder ein Anstieg der Berechnungszeit zu bemerken. Dieser Effekt ergibt sich, wie oben bereits beschrieben, aus dem ambivalenten Einfluss, den eine Vergrößerung der Faktorbasis auf den Berechnungsaufwand hat. Zuerst hat man eine kleine Faktorbasis und eine hohe Ausschussquote, so dass viele Dirichlet-Elemente zu konstruieren sind, um darunter glatte Elemente zu finden, deren (relativ kurze)  $\nu_S$ -Vektoren man in die Bewertungsmatrix einspeisen kann. Je mehr wir dann die Schranke vergrößern, desto mehr der konstruierten Dirichlet-Elemente können wir verwenden, so dass der Konstruktionsaufwand zunächst abnimmt. Dann kommt jedoch der Punkt, an dem durch die zunehmende Größe der Faktorbasis  $S$  der Umfang der  $\nu_S$ -Vektoren und damit auch die Größe der Bewertungsmatrix ein Maß erreicht, an dem die Einsparung an Konstruktionszeit durch diese aufwändiger gewordenen Berechnungen wieder aufgehoben wird. Ein interpretationsbedürftiges Merkmal sind die Plateaus bei der Anzahl der Dirichlet-Elemente, die trotz Verbesserung der Ausschussquote bestehen bleiben. Es stellt sich die Frage, warum trotz besserer Verwertung gleichviele Dirichlet-Elemente berechnet werden müssen, um eine lineare Abhängigkeit zu finden. Bei einem Plateau haben die  $S$ -Einheiten unter den Dirichlet-Elementen, die wir durch eine Vergrößerung der Faktorbasis dazugewinnen, Bewertungen über Primidealen, die bei den über einer kleineren Faktorbasis glatten Elementen nicht in die Faktorisierung ihres Hauptideals eingegangen sind. In der Matrix erscheinen bei diesen neuen Spalten Einträge an Stellen, an denen für alle bei kleineren Faktorbasen eingespeisten Elemente Nullen stehen. Insoweit leisten sie zunächst keinen Beitrag für ein schnelleres Auffinden von linearen Abhängigkeiten.*

Sofern wir den experimentellen Untersuchungen für eine Auswahl diskreter Schrankenwerte Glauben schenken, stellen wir fest, dass der gesamte Berechnungsaufwand im Allgemeinen bis zu einem gewissen Schrankenwert  $B_{min}$  zu fallen und anschließend wieder zu steigen scheint. Gerne würde man diesen optimalen Wert vor Initialisierung der Bewertungsmatrix-Algorithmen angeben können. Der systematische Ansatz würde die Ermittlung der Zeitkomplexität zur Berechnung einer Einheit von  $\mathfrak{o}_F$  zu einer Konjugiertenrichtung  $(I, J)$  mit dem Bewertungsmatrixansatz erfordern. Dazu müssten folgende Größen in Abhängigkeit von  $B$ , bestimmten Parametern von  $\mathfrak{o}_F$  und  $(I, J)$  abgeschätzt werden:

- (1) Größe einer Faktorbasis  $S(B)$ , bestehend aus Primidealen mit Norm unterhalb von  $B$ , und dem Aufwand zur Berechnung von  $S(B)$ ,
- (2) Aufwand zur Konstruktion eines Dirichlet-Elements,
- (3) Aufwand zur Durchführung des Glattheitstests für ein Dirichlet-Element zur Faktorbasis  $S(B)$  und gegebenenfalls der Berechnung des Bewertungsvektors,

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

- (4) Wahrscheinlichkeit dafür, dass ein Dirichlet-Element  $S(B)$ -glatt ist,
- (5) Aufwand für die Berechnung der Bewertungs- und Relationenmatrix zu einer Menge von  $S(B)$ -Einheiten
- (6) Wahrscheinlichkeit für das Auftreten einer linearen Abhängigkeit in einer Menge von Bewertungsvektoren zu  $S(B)$ -glatten Dirichlet-Elementen,
- (7) Wahrscheinlichkeit dafür, dass eine Einheit, die sich als Potenzprodukt aus  $S(B)$ -glatten Dirichlet-Elementen und der Relationenmatrixspalte zu einer Nullspalte der Bewertungsmatrix ergibt, eine Einheit zur Konjugiertenrichtung ist.

Vereinfachend könnte man, wie in der Literatur zu Faktorisierungsalgorithmen, versuchen, die asymptotische Entwicklung von  $B_{min}$  in Abhängigkeit von der Normbetragsschranke ( $C \rightarrow \infty$ ) zu ermitteln, um einen Anhaltspunkt für die zu wählende Größenordnung von  $B_{min}$  für den konkreten Fall (mit festem  $C$ ) zu erhalten. Für die Größen aus Punkt (1), (3), (4) und (5) sind dementsprechende asymptotische Abschätzungen unter gewissen heuristischen Annahmen bekannt<sup>1</sup>. Für (2), (6) und (7) konnten keine solchen Abschätzungen gefunden werden.

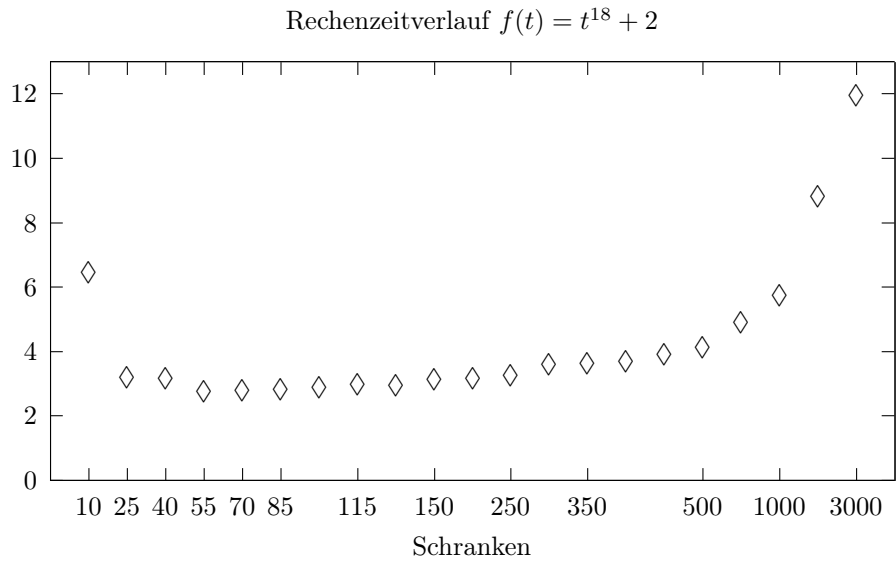
Wir versuchen, uns der Größenordnung für die Wahl einer günstigen Schranke durch experimentelle Untersuchungen zu nähern.

#### Experimentelle Untersuchung verschiedener Schranken

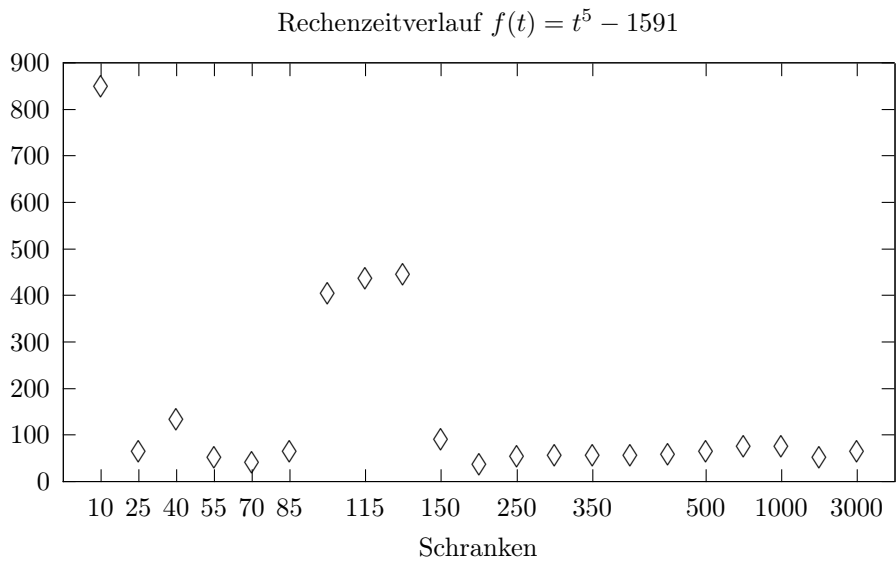
Wir möchten heuristisch einen Wert für die Schranke  $B$  angeben, für den bei der Berechnung von Einheiten ein Ausgleich zwischen effektiver Verwertung der konstruierten Konjugiertenfolgeelemente und zusätzlichem Faktorisierungsaufwand besteht. Um die Dynamik unabhängig von der Wahl einer speziellen Konjugiertenrichtung zu betrachten, wurden für verschiedene Beispiele zu  $r$  verschiedenen Konjugiertenrichtungen Dirichlet-Elemente konstruiert bis jeweils eine „passende“<sup>2</sup> Nullspalte in der Bewertungsmatrix zu den  $S$ -Einheiten unter den Dirichlet-Elementen auftrat. Die Schrankengröße  $B$  wurde dabei innerhalb einer stichprobenartigen Auswahl von Werten variiert. Die ausführlichen Ergebnisse der Beispielberechnungen findet man im Anhang in Abschnitt 5.2. In den folgenden Abbildungen sind die Gesamtrechenzeiten (in Sekunden) für die Berechnung eines Systems von  $r$  unabhängigen Einheiten der Maximalordnung des Zahlkörpers  $F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$  zu den einfachen Konjugiertenrichtungen mit Algorithmus 10 in Abhängigkeit von der Schrankengröße (unskaliert) grafisch dargestellt.

<sup>1</sup> Die Wahrscheinlichkeit dafür, dass das Hauptideal eines Zahlkörperelements (mit Normbetrag kleiner als  $C$ ) über einer Faktorbasis, bestehend aus Primidealen mit Norm unterhalb von  $B$ , faktorisiert, kann zum Beispiel wie in [Abe94, Kapitel 7] für  $C \rightarrow \infty$  abgeschätzt werden.

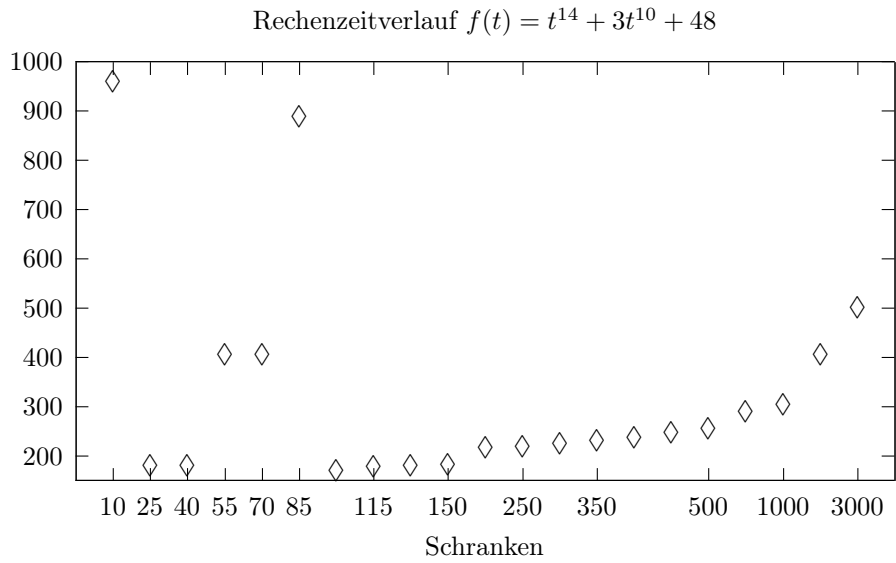
<sup>2</sup> Hier wurden verschiedene Kriterien getestet: Erstens mussten die entsprechenden Spalten der Relationenmatrix den Test aus Algorithmus 11 bestehen. Da dieser wie gesagt oftmals zu strikt ist und die zu untersuchende Dynamik möglichst unverfälscht durch das spezielle Beispiel deutlich werden soll, wurde zweitens auch die Berechnung von Dirichlet-Elementen bis zum Auftreten einer Nicht-Torsionseinheit separat durchgeführt und erfasst. Drittens wurde ein System unabhängiger Einheiten mit Algorithmus 13 berechnet.



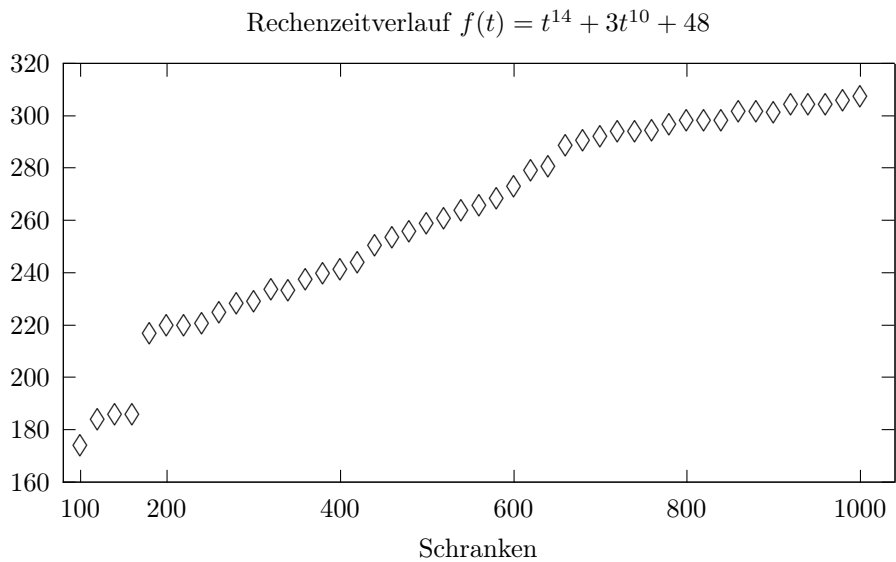
Für viele Beispiele zeigt der Graph, bei dem die Rechenzeit gegen die Schrankengröße abgetragen wird, den Verlauf, den wir nach den theoretischen Überlegungen erwarten würden (wobei Abweichungen um Zehntelsekunden durch den Rechner bedingt sein und vernachlässigt werden können.). Für manche Beispiele, wie die zwei folgenden, ergibt sich ein abweichender Verlauf.



### 3 Unabhängige Einheiten mit Bewertungsmatrizen

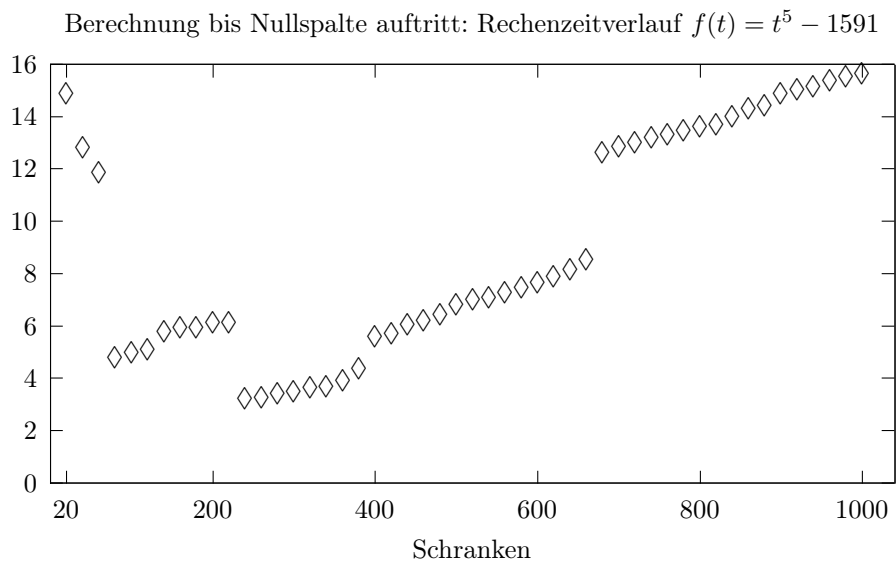


Es scheint, dass vor allem für Körper mit im Verhältnis zum Körpergrad großer Diskriminante (wie bei den letzten beiden Beispielen) ein solches Verhalten, mit stark schwankenden Berechnungszeiten für kleine Schranken, auftritt. Für das vorherige Beispiel haben wir die Schrittweite für die Schrankenwerte von 100 bis 1000 feiner gewählt (Schrittweite = 20). Es zeigt sich, dass nach dem Gebiet mit unregelmäßigem Verhalten tatsächlich ein regelmäßiger Verlauf vorzuliegen scheint.



Wie ist es nun zu erklären, dass es in dem Schrankenbereich, in dem die Verwertung der Dirichlet-Elemente noch nicht gut genug ist, um auch für die nachfolgenden

Schrankenwerte eine relativ niedrige Rechenzeit zu bedingen, zu solchen Sprüngen kommt? In den Graphen findet man die Ergebnisse zu den Berechnungen eines Systems von  $r$  unabhängigen Einheiten zu den einfachen Konjugiertenrichtung mit Algorithmus 10 unter Benutzung des Konjugiertenrichtungstests aus Algorithmus 11. Das Verwerfen der entsprechenden Relationenmatrixspalten und zugehöriger Einheiten, die diesen Test nicht bestehen, verzerrt das Bild, das man erhalte, wenn man das bloße Auftreten einer Nullspalte in der Bewertungsmatrix als Kriterium für die erfolgreiche Beendigung der Konjugiertenfolgenkonstruktion nähme. In diesem Fall ergibt sich der Verlauf, der unseren Erwartungen eher entspricht, wie man an folgendem Graphen sieht.



Wenn wir als Kriterium zur Beendigung der Konstruktion das Auftreten einer Nullspalte wählen, so dass die zugehörige Einheit keine Torsionseinheit ist, ergibt sich bereits ein Verlauf, der sich den Erwartungen annähert. (siehe zum Vergleich die Tabellen zu den unterschiedlichen Berechnungen in Abschnitt 5.2).

Für die experimentell untersuchten Beispiele geben wir die Werte, die sich unter den getesteten Schranken als optimal erwiesen haben, in der folgenden Tabelle 3.2 an. Bei den Beispielen, die für kleine Schranken schwankende Rechenzeiten aufweisen, wählen wir die kleinste Schranke, von der an wir davon ausgehen können, dass sie außerhalb des Bereichs liegt, in dem es zu unerwartet hohen Anstiegen kommt (dies ist dann insgesamt gesehen nicht unbedingt der optimale Wert). Zusätzlich geben wir die Menge der  $S$ -Einheiten unter den Dirichlet-Elementen ( $SE$ ) zu dieser Schranke, sowie den Quotienten der  $S$ -Einheiten und der konstruierten Dirichlet-Elemente ( $SQ$ ) an.

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

Tabelle 3.2: Günstige Schranken bei der Berechnung von  $r$  unabhängigen Einheiten von  $\mathfrak{o}_F$

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$ mit $f(t) =$	$ D_F  \approx$	$r$	bei Schranke	$\#S$	Zeit in Sekunden (SE, $SQ$ )
$t^5 - 1591$	$2,00 \cdot 10^{16}$	2	200	43	42.32 (90 , 0.15)
$t^{12} + 2$	$1,83 \cdot 10^{16}$	5	40	6	0.14 (10, 0.71 )
$t^6 - 2738$	$7,18 \cdot 10^{16}$	3	25	15	0.13 (16, 0.53)
$t^{15} + 2$	$7,17 \cdot 10^{16}$	7	25	6	0.82 (21, 0.68)
$t^{14} - 4t^6 - t^3 + 8$	$6,11 \cdot 10^{27}$	6	400	103	281 (260, 0.64)
$t^{18} + 2$	$5,16 \cdot 10^{27}$	8	55	18	2.82 (28, 0.68)
$t^{13} + 27$	$4,55 \cdot 10^{31}$	6	25	9	0.81 (16, 0.52)
$t^{20} + 2$	$5,50 \cdot 10^{31}$	9	85	24	30.3 (72, 0.45)
$t^{14} + 3t^{10} + 48$	$-8,21 \cdot 10^{37}$	6	100	37	174 (127, 0.35)
$t^{23} + 2$	$-8,76 \cdot 10^{37}$	11	40	12	718 (98, 0.19 )
$t^{20} - 3$	$-1.22 \cdot 10^{35}$	10	25	9	242 (63, 0.16 )
$t^{25} + 2$	$1.49 \cdot 10^{42}$	12	100	21	4135 (175, 0.16 )
$t^{16} - 3$	$-2.65 \cdot 10^{26}$	8	70	14	11.8 (51, 0.44)
$t^{19} + 2$	$-5.29 \cdot 10^{29}$	9	40	12	11.2 (68, 0.45 )
$t^{20} + 2$	$5.5 \cdot 10^{31}$	9	400	87	17.2 (119, 0.73 )
$t^{21} + 2$	$6.3 \cdot 10^{33}$	10	70	14	35.6 (71, 0.34 )
$t^{17} + t^6 - 3t^2 - 2$	$5.24 \cdot 10^{25}$	8	25	7	2.86 (26, 0.5 )
$t^{22} - 2$	$-7.26 \cdot 10^{35}$	11	85	19	38.7 (72, 0.27)
$t^{16} - 4t^5 + 2$	$6.07 \cdot 10^{25}$	8	25	9	7.0 (48, 0.4)

Man sieht, dass keine einfachen Zusammenhänge zwischen den Parametern der Maximalordnung, zum Beispiel  $C = 2^{\frac{1}{4}n(n-1)}|\text{disc}(\mathfrak{o}_F)|^{\frac{1}{2}}$ , und dem optimalen Schrankenwert zu erkennen sind. Wir müssen uns mit einer heuristischen Empfehlung begnügen: Um zu einer einigermaßen angemessenen Rechenzeit zu kommen, kommt es, wie wir überlegt haben und auch in den Beispielen sehen, vor allem darauf an, die Schranke  $B$  nicht zu klein zu wählen. Bei der Wahl einer zu kleinen Schranke und damit einer zu kleinen Faktorbasis müssen zu viele der relativ aufwändig zu konstruierenden Elemente berechnet werden. Wählen wir die Schranke hingegen etwas höher als optimal, wirkt sich dies weniger stark aus, da der Faktorisierungsaufwand durch den Konstruktionsaufwand der Konjugierfolgenelemente für einen großen Bereich der von uns betrachteten Schranken

dominiert wird. Wir haben Zahlkörper mit Körpergrad  $n \leq 25$  und Diskriminante  $\log_{10}(|D_F|) < 42$  betrachtet. Sinnvoll scheint in den meisten Fällen, als Schranke mindestens den Wert 85 zu wählen. Bei Körpern, für die kleinere Schranken optimal sind, vergibt man sich mit dieser Wahl nicht viel, da die Berechnungen insgesamt sehr schnell vonstatten gehen. Eine Ausnahme bilden die Körper, für die erst größere Schrankenbereiche eine gesichert niedrige Rechenzeit erbringen (wir vermuten, dass dies vor allem für Körper mit im Verhältnis zur Diskriminante kleinem Körpergrad zutrifft. Es gibt jedoch wie man oben sieht auch dabei Ausnahmen.). Im Zweifelsfall empfehlen wir als Schrankenwert 400 zu wählen. Auch dabei scheint zu gelten: sollte für einen solchen Körper eine kleinere Schranke optimal sein, ist entweder der Aufwand für alle getesteten Schranken sehr niedrig, so dass diese Wahl unproblematisch ist, oder aber der zusätzliche Rechenaufwand, welcher durch die zu große Wahl entsteht, ist in Bezug auf den ermittelten minimalen Rechenaufwand relativ gering.

Bisher unberücksichtigt gelassen haben wir ein Kriterium, das sich hinsichtlich der Gesamtzielsetzung ein System von Grundeinheiten zu berechnen, ergibt. Der Index der berechneten Einheiten in der Einheitengruppe, ausgedrückt durch den Quotienten der Regulatoren, sollte zur Verringerung des Aufwands bei der anschließenden Bestimmung der Grundeinheiten, möglichst klein sein. Es scheint, dass in den meisten Fällen hierfür die Wahl einer größeren Schranke günstiger ist, doch auch hier gibt es Ausnahmen (siehe Anhang Tabelle 5.27).

### **Faktorbasis simultan ermitteln**

Die Verwendung eines jeden Dirichlet-Elements bei der Einheitenkonstruktion mit Bewertungsmatrizen kann gewährleistet werden, indem man die Faktorbasis aus den Primidealen bildet, die in die Faktorisierung der von den Dirichlet-Elementen erzeugten Hauptideale eingehen. Wir nennen dies *simultane Ermittlung der Faktorbasis*. Allerdings wächst mit jedem Dirichlet-Element, das nicht glatt über der bis dahin ermittelten Faktorbasis ist, dann notwendigerweise nicht nur die Anzahl der Spalten der Bewertungsmatrix, sondern auch die Größe der Bewertungsvektoren und damit die Anzahl der Zeilen. Somit wächst der Aufwand für die Berechnung der Bewertungs- und Relationenmatrix bei diesem Vorgehen in der Anzahl der berechneten Dirichlet-Elemente stärker als bei einer vorab fixierten Faktorbasis. Es stellt sich die Frage, inwieweit die Verwendung aller konstruierten Dirichlet-Elemente diesen Effekt ausgleicht. Wir geben zunächst den Algorithmus zur Berechnung einer Einheit der Maximalordnung zu einer Konjugiertenrichtung

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

mit simultaner Ermittlung der Faktorbasis an.

---

**Algorithmus 14** : Berechnung einer Einheit zur Konjugiertenrichtung mit unbeschränkter simultaner Ermittlung der Faktorbasis

---

**Eingabe** : Zahlkörper  $F$ , Konjugiertenrichtung  $(I, J)$   
**Ausgabe** : eine Einheit  $\varepsilon$  von  $\mathfrak{o}_F$  zu der Konjugiertenrichtung  
**Initialisierung**: Faktorbasis  $S \leftarrow \{\}$ ,  $k \leftarrow 0$ ,  $\gamma_k \leftarrow 1$ ,  $\Gamma \leftarrow (\gamma_0)$ ,  
Bewertungsmatrix  $H_\Gamma \leftarrow ()$ , Relationenmatrix  $B_\Gamma \leftarrow ()$ ,  $flag \leftarrow false$   
**while**  $flag = false$  **do**  
    Konstruiere nächstes Element  $\gamma_{k+1}$  der Konjugiertenfolge zu  $(I, J)$ :  
    Rufe dazu Algorithmus (3) mit  $(\mathfrak{o}_F, (I, J), \Gamma, \mu = k + 1)$  auf und setze  
     $\gamma_{k+1}$  als letztes Element der dort konstruierten Folge.  
     $\Gamma \leftarrow (\gamma_1, \dots, \gamma_k, \gamma_{k+1})$   
    Berechne  $P \leftarrow \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$  mit  $\gamma_{k+1}\mathfrak{o}_F = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$  und setze  
     $S \leftarrow S \cup P$ .  
    **for**  $\gamma$  *aus*  $\Gamma$  **do**  
        Berechne  $\nu_S(\gamma)$  zu neuem  $S$  (siehe Bemerkung 3.10 )  
         $H_\Gamma \leftarrow (H_\Gamma | \nu_S(\gamma))$   
    **endfor**  
     $H_\Gamma \leftarrow \text{HNF}(H_\Gamma)$   
     $T \leftarrow$  Transformationsmatrix mit  $H_\Gamma T = \text{HNF}(H_\Gamma)$   
     $B_\Gamma \leftarrow I_{k+1} T$  mit  $I_{k+1}$  Einheitsmatrix aus  $\mathbb{Z}^{k+1 \times k+1}$   
    **if**  $H_\Gamma$  *weist neue Nullspalte auf* **then**  
         $(b_1, \dots, b_{k+1})^t \leftarrow$  entsprechende Spalte von  $B_\Gamma$   
         $\varepsilon \leftarrow \gamma_1^{b_1} \cdots \gamma_{k+1}^{b_{k+1}}$   
        **if**  $\varepsilon$  *ist Einheit zu*  $(I, J)$  **then**  $flag \leftarrow true$  **endif**  
    **endif**  
     $k \leftarrow k + 1$   
**endwhile**  
**return**  $\varepsilon$

---

**Bemerkung 3.10.** *Bei der Berechnung der Bewertungsvektoren  $\nu_S(\gamma)$  in obigem Algorithmus ist es im Prinzip unnötig wieder mit Algorithmus 8 zu arbeiten, denn jedes Element, das wir berechnet haben, ist eine  $S$ -Einheit und somit ist dessen Bewertung gleich Null über allen Primidealen, die bei einer späteren Erweiterung zu  $S$  dazukommen. Wenn wir  $S$  mit den Primidealen aus der Faktorisierung von  $\gamma_{k+1}$  erweitern, müssen wir die Bewertungsvektoren der zuvor berechneten Elemente  $\gamma_1, \dots, \gamma_k$  eigentlich nur um Nullen an den Stellen dieser neuen Primideale strecken, anstatt diese komplett neu zu berechnen. Dazu können wir ähnlich<sup>3</sup> wie*

<sup>3</sup> Bei der Verwendung von Algorithmus 16 innerhalb von Algorithmus 14 führen wir die Initialisierung in Schritt 2 dann für die zuvor berechneten Dirichlet-Elemente  $\gamma_1, \dots, \gamma_k$  abgewandelt durch, indem wir die erneute Faktorisierung auslassen und stattdessen  $\mathcal{P}$  als das bisherige  $S$  (vor der Erweiterung um die Primideale der Faktorisierung von  $\gamma_{k+1}\mathfrak{o}_F$ ) und  $\mathcal{V}$  als den Bewertungsvektor bezüglich des bisherigen  $S$  initialisieren.

in folgendem Algorithmus vorgehen, der wie Algorithmus 8 zu jedem Element der Maximalordnung testet, ob es sich um eine  $S$ -Einheit handelt und gegebenenfalls den Bewertungsvektor berechnet.

---

**Algorithmus 15** :  $S$ -Einheiten-Test und Berechnung der Bewertungsvektoren für Elemente aus  $\mathfrak{o}_F$

---

**Eingabe** : Zahlkörper  $F$ , Maximalordnung  $\mathfrak{o}_F$ , Faktorbasis

$S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ , Element der Maximalordnung  $\gamma$

**Ausgabe** : „wahr“ sowie  $\nu_S(\gamma)$  oder „falsch“

```

1 Initialisierung:
2  $\mathcal{P} \leftarrow \{\mathfrak{q}_1, \dots, \mathfrak{q}_m\}$  und  $\mathcal{V} \leftarrow \{e_1, \dots, e_m\}$  für  $\gamma \mathfrak{o}_F = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_m^{e_m}$ 
3 for  $\mathfrak{q} \in \mathcal{P}$  do
4   if  $\mathfrak{q} \notin S$  then
5     return „falsch“
6   endif
7 endfor
   // hat  $\gamma$  diesen Test bestanden, ist es eine  $S$ -Einheit
   // Nun berechnen wir die Bewertungen für alle  $\mathfrak{p}_i$  aus  $S$ :
8 for  $i = 1$  to  $s$  do
9   if  $\mathfrak{p}_i \notin \mathcal{P}$  then
10     $v_{\mathfrak{p}_i} \leftarrow 0$ 
11   else es existiert  $\mathfrak{q}_j \in \mathcal{P}$  mit  $\mathfrak{q}_j = \mathfrak{p}_i$ 
12     $v_{\mathfrak{p}_i} \leftarrow e_j$ 
13   endif
14 endfor
15 return „wahr“,  $\nu_S(\gamma) \leftarrow (v_{\mathfrak{p}_1}, \dots, v_{\mathfrak{p}_s})^t$ 

```

---

Bei der Auswertung der experimentellen Ergebnisse stellt man fest, dass die Einheitenberechnung mit fester Faktorbasis (aus Primidealen unterhalb einer günstig gewählten Schranke) weniger Rechenzeit erfordert als die Einheitenberechnung mit unbeschränkter simultaner Erweiterung der Faktorbasis. Die effektivere Verwendung der Dirichlet-Elemente gleicht den zusätzlichen Faktorisierungsaufwand nicht aus. Zudem ist die Anzahl an Dirichlet-Elementen, die konstruiert werden müssen bis eine Einheit zur Konjugiertenrichtung gefunden wurde, bei simultaner Ermittlung der Faktorbasis nicht wesentlich geringer als bei einer vorab gewählten Faktorbasis.

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

Wie verhält es sich nun, wenn wir die simultane Erweiterung der Faktorbasis beschränken, so dass die durch das Wachstum der Dimension der Bewertungsvektoren verstärkte Zunahme des Faktorisierungsaufwands begrenzt wird? Vielleicht bedingt eine Faktorbasis, bestehend aus Primidealen der Faktorisierungen der von einigen Dirichlet-Elementen erzeugten Hauptideale, hohe Glattheitswahrscheinlichkeiten der nachfolgend konstruierten Elemente. Um dies zu untersuchen, kombinieren wir die bisher vorgestellten Algorithmen zur Berechnung von Einheiten mit Bewertungsmatrizen: Zunächst wird die Faktorbasis simultan berechnet, dann aber, falls bis zu einer noch zu bestimmenden Größe  $\mathfrak{s}$  der Faktorbasis keine Einheit gefunden wurde, verzweigt man mit der bis dahin berechneten Faktorbasis in Algorithmus 13. Wir geben den Algorithmus (Algorithmus 16) an, der ein System von  $r$  unabhängigen Einheiten der Maximalordnung mit diesem Vorgehen berechnet.

---

**Algorithmus 16** : Berechnung eines Systems  $r$  unabhängiger Einheiten von  $\mathfrak{o}_F$  mit beschränkter simultaner Berechnung der Faktorbasis

---

**Eingabe** : Zahlkörper  $F$  vom Grad  $n$ , bereits berechnete unabhängige Einheiten  $\varepsilon_1, \dots, \varepsilon_m$  von  $\mathfrak{o}_F$ , obere Schranke  $\mathfrak{s}$  der Faktorbasisgröße

**Ausgabe** : Unabhängige Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  von  $\mathfrak{o}_F$

**while**  $m < r$  **do**

Berechne mit Algorithmus 7 die gewährleistende Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$  zu  $\varepsilon_1, \dots, \varepsilon_m$ .

// **Berechne**  $\varepsilon_{m+1}$ :

$k \leftarrow 0, \gamma_k \leftarrow 1, L \leftarrow (\gamma_0)$

Menge der  $S$ -Einheiten unter den Dirichlet-Elementen  $\Gamma \leftarrow \{\}$

Bewertungsmatrix  $H_\Gamma \leftarrow ()$ , Relationenmatrix  $B_\Gamma \leftarrow ()$

$j \leftarrow m$

**while**  $j = m$  und  $\#S < \mathfrak{s}$  **do**

$\gamma_{k+1} \leftarrow$  letztes Element der Konjugiertenfolge aus dem Aufruf von Algorithmus 3 mit den Parametern  $(\mathfrak{o}_F, (I, J), L, \mu = k + 1)$ .

$\Gamma \leftarrow \Gamma \cup \{\gamma_{k+1}\}$

Berechne  $P \leftarrow \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$  mit  $\gamma_{k+1}\mathfrak{o}_F = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$  und setze

$S \leftarrow S \cup P$

**for**  $\gamma$  aus  $\Gamma$  **do**

Berechne  $\nu_S(\gamma)$  mit neuem  $S$

$H_\Gamma \leftarrow (H_\Gamma | \nu_S(\gamma))$

**endfor**

$H_\Gamma, T \leftarrow \text{HNF}(H_\Gamma)$ , Transformationsmatrix mit  $H_\Gamma T = \text{HNF}(H_\Gamma)$

$B_\Gamma \leftarrow I_{k+1} T$  mit  $I_{k+1}$  Einheitsmatrix aus  $\mathbb{Z}^{k+1 \times k+1}$

// Fortsetzung auf der nächsten Seite

---

---

```

if  $H_\Gamma$  weist neue Nullspalte auf then
   $(b_1, \dots, b_{k+1})^t \leftarrow$  entsprechende Spalte von  $B_\Gamma$ 
   $\varepsilon \leftarrow \gamma_1^{b_1} \dots \gamma_{k+1}^{b_{k+1}}$ 
  Bestimme ein minimales Erzeugendensystem  $\eta_1, \dots, \eta_{\hat{m}}$ 
  ( $\hat{m} \leq m + 1$ ) von  $\langle \varepsilon_1, \dots, \varepsilon_m, \varepsilon \rangle$  mit MLLL und setze  $j \leftarrow \hat{m}$  sowie
   $\varepsilon_i \leftarrow \eta_i$  ( $1 \leq i \leq \hat{m}$ ).
endif
 $L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1})$ 
 $k \leftarrow k + 1$ 
endwhile
if  $j = m$  then
  while  $j = m$  do
    Konstruiere nächstes Element  $\gamma_{k+1}$  der Konjugiertenfolge zu
     $(I_{m+1}, J_{m+1})$ : Rufe dazu Algorithmus 3 mit
     $(\mathfrak{o}_F, (I_{m+1}, J_{m+1}), L, \mu = k + 1)$  auf und setze  $\gamma_{k+1}$  als das letzte
    Element der dort konstruierten Folge.
    if  $\gamma_{k+1}$  ist S-Einheit then
       $\Gamma \leftarrow \Gamma \cup \{\gamma_{k+1}\}$ 
      Bilde  $H_\Gamma$  und  $B_\Gamma$  zu  $\Gamma$  (mit Algorithmus 9).
       $l \leftarrow \#\Gamma$ 
      if  $H_\Gamma$  weist neue Nullspalte auf then
         $\{\hat{\gamma}_1, \dots, \hat{\gamma}_l\} \leftarrow \Gamma$ 
         $(b_1, \dots, b_l)^t \leftarrow$  entsprechende Spalte von  $B_\Gamma$ 
         $\varepsilon \leftarrow \hat{\gamma}_1^{b_1} \dots \hat{\gamma}_l^{b_l}$ 
        Bestimme ein minimales Erzeugendensystem  $\eta_1, \dots, \eta_{\hat{m}}$ 
        ( $\hat{m} \leq m + 1$ ) von  $\langle \varepsilon_1, \dots, \varepsilon_m, \varepsilon \rangle$  mit MLLL und setze
         $j \leftarrow \hat{m}$  sowie  $\varepsilon_i \leftarrow \eta_i$  ( $1 \leq i \leq \hat{m}$ ).
      endif
    endif
     $L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1})$ 
     $k \leftarrow k + 1$ 
  endwhile
endif
 $m \leftarrow m + 1$ 
endwhile // wenn  $m = r$ 
return  $\varepsilon_1, \dots, \varepsilon_r$ 

```

---

### 3 Unabhängige Einheiten mit Bewertungsmatrizen

Wir vergleichen nun die Ansätze zur Wahl der Faktorbasis und betrachten dazu die Ergebnisse der Berechnung eines Systems von  $r$  unabhängigen Einheiten der Maximalordnung für einige Zahlkörper mit Algorithmus 13 und Algorithmus 16 in Tabelle 3.3. Für das Vorgehen aus Algorithmus 13 wählen wir als Schranke  $B$  sowohl 85 als auch 400. Bei Algorithmus 16 lassen wir die Faktorbasis bis zu einer Größe  $\mathfrak{s} = 10, 20$  und  $30$  simultan bestimmen. Zusätzlich betrachten wir die unbeschränkte simultane Bestimmung (wir wählen  $\mathfrak{s}$  ausreichend groß). Erfasst werden die insgesamt berechneten Dirichlet-Elemente (DE), die Nicht- $S$ -Einheiten unter den berechneten Dirichlet-Elementen (NSE), die Gesamtrechenzeit und die Anzahl an Torsionseinheiten (TE), die sich während der Konstruktion als Einheit zu einer Nullspalte ergeben haben. Zur Konstruktion der Dirichlet-Elemente benutzen wir in allen Fällen Algorithmus 3.

Tabelle 3.3: Beispiele für den Vergleich der Algorithmen

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$ mit $f(t) =$		$t^{12} + 6t^5 + 6$	$t^{22} + 2$	$t^{17} - 3$	$t^{15} + 7$
$S(B)$ feste Faktorbasis $B = 85$	DE (NSE)	158 (76)	406 (287)	200 (116)	130 (61)
	<i>Zeit in Sek.</i>	<i>6.11</i>	<i>82</i>	<i>11</i>	<i>4.87</i>
	TE (#S(B))	5 (27)	2 (21)	2 (23)	0 (25)
$S(B)$ feste Faktorbasis $B = 400$	DE (NSE)	157 (41)	383 (164)	195 (72)	120 (22)
	<i>Zeit in Sek.</i>	<i>12.35</i>	<i>108</i>	<i>19.6</i>	<i>7</i>
	TE (#S(B))	5 (91)	4 (92)	2 (76)	0 (92)
$S$ simultan erweitern bis $\#S = \mathfrak{s} = 10$	DE (NSE)	190 (115)	525 (417)	228 (155)	169 (109)
	<i>Zeit in Sek.</i>	<i>8.46</i>	<i>141</i>	<i>13</i>	<i>12</i>
	TE	7	5	2	0
$S$ simultan erweitern bis $\#S = \mathfrak{s} = 20$	DE (NSE)	167 (56)	468 (270)	215 (82)	127 (23)
	<i>Zeit in Sek.</i>	<i>8.45</i>	<i>130</i>	<i>14.47</i>	<i>11.26</i>
	TE	4	6	2	0
$S$ simultan erweitern bis $\#S = \mathfrak{s} = 30$	DE (NSE)	165 (25)	398 (111)	209 (38)	127 (0)
	<i>Zeit in Sek.</i>	<i>10</i>	<i>120</i>	<i>17.5</i>	<i>14.37</i>
	TE	4	3	2	0
$S$ unbeschränkt simultan erweitern	DE (NSE)	153 (0)	391 (0)	203 (0)	127 (0)
	<i>Zeit in Sek.</i>	<i>10.71</i>	<i>169</i>	<i>22</i>	<i>14.37</i>
	TE	4	5	2	0

*Wahl von  $\mathfrak{s}$ : Wir sehen, dass hinsichtlich der Anzahl der konstruierten Dirichlet-Elemente eine unbeschränkte simultane Ermittlung günstig scheint. Hinsichtlich der Rechenzeit ergibt sich wegen der zunehmenden Dimension der Bewertungsvektoren ein anderes Bild. In Bezug darauf scheint je nach Beispiel die Wahl eines kleineren Wertes für  $\mathfrak{s}$  zweckmäßig. Da sich die beschränkte simultane Berechnung im Gesamtvergleich nicht gegenüber der Wahl einer festen Faktorbasis auszeichnet (siehe unten), vertiefen wir diese Überlegungen nicht weiter.*

Wir stellen fest, dass Algorithmus 13 bei entsprechender Wahl der Schranke  $B$  den Algorithmus 16 bezüglich der Rechenzeiten dominiert. Weiterhin scheint die Menge der Primideale, die bei der simultanen Ermittlung die Faktorbasis konstituiert, keine erhöhten Glattheitswahrscheinlichkeiten der nachfolgend berechneten Dirichlet-Elemente zu bedingen. Sonst müsste der Quotient  $\text{NSE}/\text{DE}$  (bei vergleichbarer Faktorbasisgröße) bei einer simultan ermittelten Faktorbasis wesentlich kleiner sein als bei einer Faktorbasis, bestehend aus Primidealen mit Norm unterhalb der entsprechenden Schranke. Bei den Ergebnissen aus der Tabelle ist dieser Quotient in der vierten Zeile zwar tatsächlich immer kleiner als in der ersten Zeile, der geringe Unterschied lässt aber vermuten, dass die Bewertungen  $\nu_{\mathfrak{p}}(\gamma_1), \nu_{\mathfrak{p}}(\gamma_2), \dots$  von Dirichlet-Elementen über einem Primideal  $\mathfrak{p} \in I_F$  (mit Norm unterhalb der Normbetragsschranke  $C$  der Konjugiertenfolge) unabhängig verteilte Zufallszahlen sind.

Abschließend kann man sagen, dass auch bei der beschränkten simultanen Ermittlung der Faktorbasis der zusätzliche Aufwand für die elementweise Faktorisierung der Hauptideale und das Rechnen mit den stärker anwachsenden Bewertungs- und Relationenmatrizen nicht durch die leicht verbesserte Verwertung der konstruierten Dirichlet-Elemente ausgeglichen wird.



## 4 Schlussbetrachtungen

In diesem Kapitel wollen wir die Verfahren zur Konstruktion unabhängiger Einheiten der Maximalordnung  $\mathfrak{o}_F$  eines algebraischen Zahlkörpers  $F$  aus Kapitel 2 und Kapitel 3 vergleichen und am Ende eine Zusammenfassung der Ergebnisse der gesamten Arbeit vornehmen.

### 4.1 Vergleich der vorgestellten Verfahren

Die Einheitenkonstruktionsmethoden aus Kapitel 2 und Kapitel 3 fußen auf der Konstruktion von Konjugiertenfolgen zu gegebenen Konjugiertenrichtungen. Die vorgestellten Methoden, mit denen wir aus den Konjugiertenfolgeelementen die Einheit zu einer gegebenen Konjugiertenrichtung gewinnen, nennen wir - wegen ihres Zwecks, entlang der Konjugiertenfolgen eine bestimmte Konstellation von Normbeträgen aufzufinden - im Folgenden *Suchmethoden*. Wir nennen die zwei Suchmethoden, die wir in diesem Abschnitt vergleichen, abkürzend *Bewertungsmatrixmethode* und *Normvergleichmethode*:

- Bei der Normvergleichmethode werden solange Konjugiertenfolgeelemente zu der Konjugiertenrichtung  $(I, J)$  konstruiert, bis der Normbetrag eines Konjugiertenfolgeelements dem eines Vorhergehenden entspricht. Die Einheit zur Konjugiertenrichtung  $(I, J)$  ergibt sich dann als Quotient dieser zwei Konjugiertenfolgeelemente. Dieses Vorgehen wurde in Algorithmus 4 beschrieben.
- Bei der Bewertungsmatrixmethode werden solange Konjugiertenfolgeelemente zu  $(I, J)$  konstruiert, bis in der Bewertungsmatrix eine Nullspalte auftritt, deren zugehörige Einheit (die sich als Potenzprodukt von Konjugiertenfolgeelementen ergibt) eine Einheit zur Konjugiertenrichtung  $(I, J)$  ist. Dieses Vorgehen wurde in Algorithmus 10 beschrieben.

Die Suchmethoden sollen in den verschiedenen Strategien, die es gibt, um ein System von  $r$  unabhängigen Einheiten zu berechnen, zur Anwendung kommen. Eine *Strategie* umfasst für uns im Folgenden: die Entscheidung über die zugrundeliegende Konstruktionsmethode der Konjugiertenfolgeelemente (siehe Abschnitt 2.3), die Wahl einer Suchmethode und das Vorgehen, um die Unabhängigkeit der konstruierten Einheiten zu gewährleisten. Eine Strategie, welche die Bewertungs-

#### 4 Schlussbetrachtungen

matrixmethode beinhaltet, wird zum Beispiel in Algorithmus 13 realisiert. Am Ende von Abschnitt 2.4 haben wir die vier verschiedenen Strategien aus [Wil93] angegeben, die als Suchmethode alle die Normvergleichsmethode benutzen und zur Konstruktion der Konjugiertenfolgeelemente den Algorithmus 3 verwenden.

Für den Vergleich der beiden Suchmethoden und die spätere Auswahl einer optimalen Strategie zur Berechnung eines Systems von  $r$  unabhängigen Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  der Maximalordnung legen wir drei Merkmale fest, anhand derer die Güte der Methoden beurteilt werden soll:

- die Anzahl zu konstruierender Dirichlet-Elemente bis das System von unabhängigen Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  gefunden wurde,
- die benötigte Rechenzeit,
- der Index  $(U(\mathfrak{o}_F) : \langle \eta, \varepsilon_1, \dots, \varepsilon_r \rangle) = \frac{\text{Reg}(\varepsilon_1, \dots, \varepsilon_r)}{\text{Reg}_{\mathfrak{o}_F}}$  (mit  $\eta \in TU(\mathfrak{o}_F)$ ).

Dabei ist die Anzahl zu konstruierender Dirichlet-Elemente als Kriterium besonders zu berücksichtigen, da mit wachsender Länge der Konjugiertenfolge die Konstruktionen der einzelnen Elemente durch das Anwachsen der Koeffizienten und Konjugiertenbeträge aufwändiger werden. Die Rechenzeit hingegen ist von der konkreten Implementation der Algorithmen abhängig. Da wir bei der Normvergleichsmethode davon ausgehen können, dass sie effizient implementiert wurde (siehe Bemerkung 2.6), würde aber zumindest der Fall, dass die benötigte Rechenzeit bei der Bewertungsmatrixmethode kleiner als bei der Normvergleichsmethode ist, auf die Überlegenheit der Bewertungsmatrixmethode hinsichtlich des Gesamtrechenaufwands hindeuten. Die Größe des Index schließlich sollte in Bezug auf die mögliche Zielsetzung, Grundeinheiten der Maximalordnung zu berechnen, in die Beurteilung der Methoden einbezogen werden.

##### 4.1.1 Vergleich der Suchmethoden

Ein komplexitätstheoretischer Vergleich der Suchmethoden würde sich zunächst an der grundsätzlichen Frage orientieren, nach wie vielen Konstruktionen von Dirichlet-Elementen zu einer Konjugiertenrichtung mit der jeweiligen Suchmethode eine Einheit zur Konjugiertenrichtung gefunden wird.

Bei der Normvergleichsmethode finden wir eine Einheit  $\varepsilon \in U(\mathfrak{o}_F)$  zur Konjugiertenrichtung, falls zwei Konjugiertenfolgeelemente denselben Normbetrag aufweisen. Die Normbeträge der Konjugiertenfolgeelemente sind beschränkt durch  $C = 2^{\frac{1}{4}(n-1)n} |\text{disc}(\mathfrak{o}_F)|^{\frac{1}{2}}$ . Wir wissen, dass es endlich viele nicht-assoziierte Elemente der Maximalordnung mit Normbetrag unterhalb von  $C$  gibt. Über die Anzahl der Elemente dieser Menge gibt es keine allgemeine Aussage. Genauso wenig kennen wir den Anteil der Konjugiertenfolgeelemente an dieser Menge. Um die beiden Methoden hinsichtlich der zu konstruierenden Elemente zumindest

#### 4.1 Vergleich der vorgestellten Verfahren

im Worst Case zu vergleichen, treffen wir die Annahme, dass die Normbeträge der Konjugiertenfolgeelemente zuerst alle Werte bis  $C$  annehmen, bis wir ein Element finden, das denselben Normbetrag aufweist wie ein vorhergehendes Element. Es wären im Worst Case somit  $C$  Konstruktionen notwendig.

Bei der Bewertungsmatrixmethode finden wir eine Einheit (dies ist aber per se noch keine Einheit zur Konjugiertenrichtung), wenn Bewertungsvektoren zu den  $S$ -Einheiten unter den Konjugiertenfolgeelementen auftreten, die linear abhängig sind. Die Anzahl der Zeilen der Bewertungsmatrix beträgt  $s := \#S$ . Im Worst Case müssen  $s + 1$  der  $S$ -Einheiten konstruiert werden, damit der Rang der Bewertungsmatrix kleiner als die Anzahl der Spalten ist und sich eine Einheit ergibt. Wie viele Dirichlet-Elemente dazu konstruiert werden müssen, hängt von der Faktorbasis ab. Wenn wir als Faktorbasis alle Primideale mit Norm unterhalb von  $B = C$  wählen, sind alle konstruierten Konjugiertenfolgeelemente glatt über  $S(B)$ . Bei einer solchen Wahl der Faktorbasis müssen im Worst Case  $s + 1$  Konjugiertenfolgeelemente konstruiert werden, um eine Einheit zu finden. Es sei  $\pi_F(C)$  die Funktion, welche die Anzahl der Primideale von  $\mathfrak{o}_F$  mit Norm unterhalb von  $C$  angibt. Aufgrund des Primidealsatzes (siehe zum Beispiel [Hes96, Satz 3.4.1]) wissen wir dann, dass  $\lim_{C \rightarrow \infty} C - (s + 1) = \lim_{C \rightarrow \infty} C - \pi_F(C) - 1 = \infty$  gilt. Es gilt demnach  $(s + 1) = \pi_F(C) + 1 < C$  für ausreichend hohes  $C$ . Für die Konstruktion einer *beliebigen* Einheit sind bei der Bewertungsmatrixmethode unter den getroffenen Annahmen im Worst Case also weniger Dirichlet-Elemente zu konstruieren als bei der Normvergleichsmethode. Allerdings ist die mit der Bewertungsmatrix gefundene Einheit eventuell keine Einheit zur Konjugiertenrichtung. Wir finden bei der Bewertungsmatrixmethode erst dann eine Einheit zur Konjugiertenrichtung, wenn die der Nullspalte der Bewertungsmatrix entsprechende Spalte der Relationenmatrix den Test aus Algorithmus 11 besteht. Dies muss aber im schlechtesten Fall erst dann zwangsläufig eintreten, wenn aufgrund der Endlichkeit der Menge nicht-assoziierter Elemente mit beschränkter Norm zwei Konjugiertenfolgeelemente mit gleicher Norm auftreten. Im Worst Case müssen wir also bei der Bewertungsmatrixmethode ebenso viele Konjugiertenfolgeelemente konstruieren wie bei der Normvergleichsmethode, um eine Einheit zur Konjugiertenrichtung zu gewinnen.

Für einen Average Case-Vergleich der Methoden müsste Gewissheit über die Verteilung der Konjugiertenfolgeelemente in der Menge nicht-assoziierter Elemente mit Normbetrag unterhalb der Schranke  $C$  und die Anzahl der nicht-assoziierter Elemente einer Ordnung mit beschränkter Norm bestehen. Des Weiteren müsste die Verteilung günstiger Relationenmatrixspalten unter den sich ergebenden Relationenmatrixspalten und die Wahrscheinlichkeit für das Auftreten einer linearen Abhängigkeit unter den sich ergebenden Bewertungsvektoren ermittelt werden. Letzteres ist schon unter stark vereinfachenden Annahmen nicht trivial.

#### 4 Schlussbetrachtungen

Aus den bisherigen Überlegungen halten wir dennoch fest, was bereits ganz offensichtlich als der grundsätzliche Vorteil der Bewertungsmatrixmethode zu erkennen ist: Die Bewertungsmatrixmethode wird zwar spätestens fündig, wenn zwei assoziierte Elemente auftreten, die Wahrscheinlichkeit dafür, dass sich aber bereits zuvor Konjugiertenfolgeelemente ergeben, deren Normbeträge sich multiplikativ zu 1 kombinieren lassen, ist recht hoch. In Abhängigkeit von der Größe der Faktorbasis  $s$ , die wie wir gesehen haben nicht sehr groß gewählt werden muss, um zu einer guten Glatthewahrscheinlichkeit zu kommen, müssen nur wenig mehr als  $s$  (häufig reichen sogar weniger)  $S$ -Einheiten unter den Konjugiertenfolgeelementen konstruiert werden, um eine Einheit zur Konjugiertenrichtung zu erhalten. Der Nachteil der Bewertungsmatrixmethode besteht in dem zusätzlichen Aufwand für die Berechnung der Faktorbasis, der Bewertungsvektoren und der Bewertungs- und Relationenmatrix. Wir wollen nun an einigen Beispielen betrachten, inwieweit sich Vor- und Nachteil ausgleichen.

#### **Experimenteller Vergleich hinsichtlich Strategie 1 und gegebener Konjugiertenrichtungen**

Um die Suchmethoden unmittelbar zu vergleichen, müssen zwei Dinge festgelegt werden: die Konjugiertenrichtung und damit die Konjugiertenfolge, aus der eine Einheit konstruiert werden soll, und die Konstruktionsmethode der Hilfsfolgeelemente. Das im zweiten Kapitel bereits als *Strategie 1* vorgestellte Vorgehen zur Berechnung von  $r$  unabhängigen Einheiten der Maximalordnung erfordert die Berechnung von Einheiten zu den  $r$  verschiedenen einfachen Konjugiertenrichtungen  $(I_i, J_i) = (\{i\}, \{1, \dots, r_1 + r_2\} \setminus \{i\})$  mit  $(1 \leq i \leq r)$ . Wir berechnen für verschiedene Zahlkörper Einheiten zu den einfachen Konjugiertenrichtungen jeweils mit Algorithmus 10 und Algorithmus 4 und betrachten die Ergebnisse hinsichtlich der von uns festgelegten drei Kriterien. Als Konstruktionsmethoden für die Konjugiertenfolgeelemente verwenden wir jeweils den Algorithmus 3 und den Algorithmus 6. Zusätzlich berechnen wir für einige Beispiele die Einheit zu einer speziellen Konjugiertenrichtung. Die Beispieltabellen mit den Ergebnissen findet man im Anhang in Abschnitt 5.1.1.

**Auswertung der experimentellen Ergebnisse:** Man stellt fest, dass bei der Bewertungsmatrixmethode tatsächlich in der überwiegenden Zahl der Fälle erheblich weniger Konstruktionen von Konjugiertenfolgeelementen nötig sind, bis eine Einheit zur gegebenen Konjugiertenrichtung gefunden wurde. Dieses Ergebnis wird schon mit einer kleinen Faktorbasis (Primideale mit Norm unterhalb der Schranke  $B = 85$ ) erreicht. In seltenen Ausnahmen sehen wir, dass bei der Bewertungsmatrixmethode mehr Konstruktionen von Dirichlet-Elementen erforderlich sind bis Einheiten gefunden werden. Dieser Fall kann eintreten, wenn gerade die Dirichlet-Elemente, deren Quotient die Einheit bei der Normvergleichsmethode er-

#### 4.1 Vergleich der vorgestellten Verfahren

bringt, nicht glatt über  $S$  sind. Meist tritt dann aber nach wenigen weiteren Konstruktionen eine passende Nullspalte in der Bewertungsmatrix auf. *Um diesen Fall trotzdem zu vermeiden, sollte die Normvergleichsmethode nicht durch die Bewertungsmatrixmethode ersetzt, sondern um diese ergänzt werden. Zur Berechnung der Einheit zu einer gegebenen Konjugiertenrichtung wird dann wie in Algorithmus 10 vorgegangen, zusätzlich wird aber eine Liste der Normbeträge der konstruierten Dirichlet-Elemente geführt und bei jeder erneuten Konstruktion überprüft, ob bereits ein Dirichlet-Element mit demselben Normbetrag vorliegt.*

Der Vergleich der Rechenzeit zeigt weiterhin, dass der zusätzliche Aufwand (Berechnung der Bewertungsmatrix etc.) durch die Verringerung der erforderlichen Konstruktionen ausgeglichen wird, so dass die Bewertungsmatrixmethode die Normvergleichsmethode in Bezug auf den Gesamtaufwand dominiert. Die Berechnung der Einheit zu einer gegebenen Konjugiertenrichtung kann also durch die Verwendung der Bewertungsmatrixmethode beschleunigt werden.

Allerdings ist der Index des mit Strategie 1 konstruierten Systems unabhängiger Einheiten bei Konstruktion mit Normvergleichsmethode in den meisten Fällen kleiner als oder gleich dem Index, der sich für ein Einheitensystem aus der Bewertungsmatrixmethode ergibt.

**Bemerkung 4.1.** *Hinsichtlich der Konstruktionsmethoden können wir erkennen, dass in den von uns betrachteten Beispielen die Konstruktion der Dirichlet-Elemente mit Algorithmus 6 (kürzesten Elementen des Moduls) einen kleineren Index der berechneten Einheiten in der ganzen Einheitengruppe bedingt als die Konstruktion mit Algorithmus 3 (LLL-reduzierte Basis). Hinsichtlich der Rechenzeit und der Anzahl berechneter Elemente ergibt sich aus der Konstruktion mit kürzesten Elementen zwar nicht in allen Fällen ein Vorteil. In den Fällen, in denen die Konstruktion mit LLL dominiert, ist jedoch der Unterschied in der Anzahl zu konstruierender Dirichlet-Elemente gering. Dagegen ist in den Fällen, in denen die Konstruktion mit kürzesten Elementen kleiner ist, ein großer Unterschied zu verzeichnen ist. Aus dieser Beobachtung leiten wir die Empfehlung ab, die Konstruktion der Dirichlet-Elemente stets mit dem Algorithmus 6 durchzuführen.*

### 4.1.2 Andere Strategien zur Berechnung unabhängiger Einheiten

In Kapitel 2 haben wir am Ende von Abschnitt 2.4 die vier Strategien zur Berechnung von unabhängigen Einheiten mit der Normvergleichsmethode aus [Wil93, Abschnitt 3.2] angegeben. In all diesen Strategien kann als Suchmethode auch die Bewertungsmatrixmethode, wie wir sie in Algorithmus 10 festgelegt haben, zur Anwendung kommen.

Innerhalb der vierten Strategie wird die Variierbarkeit der Konjugiertenrichtungen, die entsprechend der Erweiterung der Dirichletschen Methode in [Poh93] möglich ist, durch folgendes Vorgehen ausgenutzt, das wir kurz skizzieren: Es seien  $\varepsilon_1, \dots, \varepsilon_m$  bereits konstruierte unabhängige Einheiten. Dann wird zunächst eine Einheit entlang der Dirichlet-Elemente zu der gewährleistenden Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$  gesucht. Wenn nach einer gewissen Anzahl von Schritten keine Einheit gefunden wurde, wird mehrmals jeweils die kürzeste Konjugiertenfolge aus der Menge von Konjugiertenfolgen zu beliebigen Konjugiertenrichtungen verlängert. Falls sich dabei eine Einheit  $\varepsilon$  entlang einer kürzesten Folge ergibt, wird mit dem MLLL-Algorithmus ein minimales Erzeugendensystem  $\eta_1, \dots, \eta_j$  ( $m \leq j \leq m+1$ ) von  $\langle \varepsilon_1, \dots, \varepsilon_m, \varepsilon \rangle$  berechnet. Falls  $j = m$  ist, wird die Suche mit der bisherigen gewährleistenden Konjugiertenrichtung nach dem beschriebenen Schema wiederholt. Andernfalls beginnt die Methode mit der zu  $\eta_1, \dots, \eta_{m+1}$  berechneten gewährleistenden Konjugiertenrichtung von neuem.

Wir stellen die Anwendung der Bewertungsmatrixmethode innerhalb von Strategie 4 in folgendem Algorithmus (Algorithmus 17) ausführlich dar. Festzulegen ist noch die Anzahl der Konstruktionen von Konjugiertenfolgenelementen zur gewährleistenden Konjugiertenrichtung ( $k_1$ -mal) bis bei Erfolglosigkeit die jeweils kürzeste Konjugiertenfolge aus der Menge aller möglichen Konjugiertenfolgen erweitert wird und wie oft diese Erweiterung geschehen soll ( $k_2$ -mal). Wenn dabei keine Einheit auftritt, wird wieder die Konjugiertenfolge zur gewährleistenden Konjugiertenrichtung erweitert. Letztere muss dann nicht neuerlich berechnet werden; ein Statusindikator ( $flag_{(I,J)}$ ) soll dies anzeigen.

---

**Algorithmus 17** : Zur Berechnung von  $r$  unabhängigen Einheiten der Maximalordnung mit Bewertungsmatrizen (Strategie 4)

---

**Eingabe** : Zahlkörper  $F$  mit Einheitenrang  $r$ , bereits berechnete unabhängige Einheiten  $\varepsilon_1, \dots, \varepsilon_m$  von  $\mathfrak{o}_F$ , Faktorbasis  $S$ , Parameter  $k_1, k_2$

**Ausgabe** : Unabhängige Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  von  $\mathfrak{o}_F$

**Initialisierung**: Lege eine Liste  $\mathfrak{L}$  mit Tupeln  $((I, J), L, \Gamma, H_\Gamma, B_\Gamma)$  aus Konjugiertenrichtung, Menge dazu bereits berechneter Dirichlet-Elemente, Menge der  $S$ -Einheiten darunter und dazu berechneter Bewertungs- und Relationenmatrix an. Lege für jede Konjugiertenrichtung  $(I_i, J_i)$  ein Tupel mit den Anfangswerten  $((I_i, J_i), \{1\}, \{\}, (), ())$  in  $\mathfrak{L}$  ab.

$flag_{(I, J)} \leftarrow true$

**while**  $m < r$  **do**

**if**  $flag_{(I, J)} = true$  **then**

    Berechne mit Algorithmus 7 die gewährleistende

    Konjugiertenrichtung  $(I_{m+1}, J_{m+1})$  zu  $\varepsilon_1, \dots, \varepsilon_m$  und setze

$flag_{(I, J)} \leftarrow false$ .

    Wähle aus der Liste  $\mathfrak{L}$  das Tupel zu  $(I_{m+1}, J_{m+1})$  aus, initialisiere

$L, \Gamma, H_\Gamma, B_\Gamma$  mit den entsprechenden Komponenten und setze

$k \leftarrow \#L$ .

**endif**

$flag_\varepsilon \leftarrow false$

  // Konstruktion für die gewährleistende

  Konjugiertenrichtung:

$l_1 \leftarrow 0$

**while**  $l_1 < k_1$  und  $flag_\varepsilon = false$  **do**

    Konstruiere nächstes Element  $\gamma_{k+1}$  der Konjugiertenfolge zu  $(I_{m+1}, J_{m+1})$ .

**if**  $\gamma_{k+1}$  ist  $S$ -Einheit **then**

$\Gamma \leftarrow \Gamma \cup \{\gamma_{k+1}\}, l \leftarrow \#\Gamma$

      Bilde  $H_\Gamma$  und  $B_\Gamma$  zu  $\Gamma$ .

**if**  $H_\Gamma$  weist neue Nullspalte auf **then**

$\{\hat{\gamma}_1, \dots, \hat{\gamma}_l\} \leftarrow \Gamma$

$(b_1, \dots, b_l)^t \leftarrow$  entsprechende Spalte von  $B_\Gamma$

$\varepsilon \leftarrow \hat{\gamma}_1^{b_1} \dots \hat{\gamma}_l^{b_l}$

**if**  $\varepsilon$  Einheit zur Konjugiertenrichtung  $(I, J)$  **then**

$flag_\varepsilon \leftarrow true$

**endif**

**endif**

**endif**

  // Fortsetzung auf der nächsten Seite

---

---

```

     $L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1}), k \leftarrow k + 1, l_1 \leftarrow l_1 + 1$ 
endwhile// solange  $l_1 < k_1$  und  $flag_\varepsilon = false$ 
Aktualisiere in  $\mathcal{L}$  die Komponenten  $L, \Gamma, H_\Gamma, B_\Gamma$  des Tupels zu
 $(I_{m+1}, J_{m+1})$ .
// Suche entlang kürzester Konjugiertenfolge:
if  $flag_\varepsilon = false$  then
     $l_2 \leftarrow 0$ 
    while  $l_2 < k_2$  und  $flag_\varepsilon = false$  do
        Wähle aus  $\mathcal{L}$  das Tupel zur Konjugiertenrichtung  $(I_i, J_i)$ , deren
        zugehörige Konjugiertenfolge  $L$  minimale Länge hat; initialisiere
         $(I_i, J_i), L, \Gamma, H_\Gamma, B_\Gamma$  mit den entsprechenden Komponenten und
        setze  $k \leftarrow \#L$ .
        Konstruiere nächstes  $\gamma_{k+1}$  der Konjugiertenfolge zu  $(I_i, J_i)$ .
        if  $\gamma_{k+1}$  ist S-Einheit then
             $\Gamma \leftarrow \Gamma \cup \{\gamma_{k+1}\}$ 
             $l \leftarrow \#\Gamma$ 
            Bilde  $H_\Gamma$  und  $B_\Gamma$  zu  $\Gamma$ .
            if  $H_\Gamma$  weist neue Nullspalte auf then
                 $\{\hat{\gamma}_1, \dots, \hat{\gamma}_l\} \leftarrow \Gamma$ 
                 $(b_1, \dots, b_l)^t \leftarrow$  entsprechende Spalte von  $B_\Gamma$ 
                 $\varepsilon \leftarrow \hat{\gamma}_1^{b_1} \dots \hat{\gamma}_l^{b_l}$ 
                Bestimme ein minimales Erzeugendensystem  $\eta_1, \dots, \eta_j$ 
                ( $j \leq m + 1$ ) von  $\langle \varepsilon_1, \dots, \varepsilon_m, \varepsilon \rangle$  mit MLLL und setze
                 $\varepsilon_i \leftarrow \eta_i$  ( $1 \leq i \leq j$ ).
                if  $j = m + 1$  then
                     $flag_\varepsilon \leftarrow true$ 
                     $m \leftarrow m + 1$ 
                endif
            endif
        endif
    endif
     $L \leftarrow (\gamma_0, \dots, \gamma_k, \gamma_{k+1}), l_2 \leftarrow l_2 + 1$ 
    Aktualisiere in  $\mathcal{L}$  die Komponenten  $L, \Gamma, H_\Gamma, B_\Gamma$  des Tupels zu
     $(I_i, J_i)$ .
endwhile
else // falls Einheit in gewährleistender Konjugiertenfolge
    gefunden:
        Setze  $\varepsilon_{m+1} \leftarrow \varepsilon$  und  $m \leftarrow m + 1$ .
endif
    Setze Statusindikator  $flag_{(I,J)} \leftarrow flag_\varepsilon$ .
endwhile // wiederholen solange  $m < r$ 
return  $\varepsilon_1, \dots, \varepsilon_r$ .

```

---

**Bemerkung 4.2.** (1) Entsprechend der vormaligen Überlegungen kann zu jedem Tupel in  $\mathfrak{L}$  zusätzlich eine Liste mit den Normbeträgen der Dirichlet-Elemente der zugehörigen Konjugiertenfolge angelegt und bei jeder erneuten Konstruktion abgefragt werden, ob ein Element gleichen Normbetrags in der Folge vorliegt. Wenn dieser Fall eintritt, wird eine Einheit als Quotient konstruiert. Bei diesem Vorgehen stellt die Bewertungsmatrixmethode eine Ergänzung der Normvergleichsmethode dar. In den Beispielberechnungen führen wir Algorithmus 17 allerdings noch wie oben angegeben aus, um die unterschiedlichen Suchmethoden getrennt zu vergleichen.

(2) Konjugiertenrichtungen  $(I, J)$  sind für uns per Definition Paare von disjunkten Teilmengen der Konjugiertenindexmenge  $\{1, \dots, r_1 + r_2\}$  mit der Eigenschaft  $\#I < r$ . Zur Berechnung der Hilfsfolgenelemente brauchen wir vollständige Konjugiertenrichtungen  $(\tilde{I}, \tilde{J})$  mit  $\#\tilde{I} + \#\tilde{J} = r_1 + r_2$ . Wir haben in Kapitel 2 festgelegt, dass wir immer  $(\tilde{I}, \tilde{J}) = (I, \{1, \dots, r_1 + r_2\} \setminus I)$  wählen. Trotz dieser Festlegung kann die Menge der Möglichkeiten, verschiedene vollständige Konjugiertenrichtungen zu wählen, bei entsprechend hohem Körpergrad sehr groß sein. Hier muss eventuell eine weitere Einschränkung getroffen werden.

(3) Für die Parameter  $k_1$  und  $k_2$  wurde in [Wil93] die Wahl  $(k_1, k_2) = (5, 5)$  vorgeschlagen. In Kapitel 2 am Ende des Abschnitts 2.4 haben wir zwei weitere Strategien aus [Wil93] vorgestellt. Wenn man  $k_1 = 0$  und  $k_2 > 0$  wählt, entspricht dies der Strategie 3. Wenn man  $k_2 = 0$  und  $k_1 > 0$  wählt, entspricht dies der Strategie 2. Die Wahl eines hohen Wertes für  $k_2$  und eines niedrigeren Wertes für  $k_1$  trägt eventuell zu einer Verringerung der Rechenzeit bei, da die Konstruktion des nächsten Konjugiertenfolgenelements einer kurzen Folge weniger aufwändig ist als die Konstruktion eines Konjugiertenfolgenelements einer längeren Folge. Auch hinsichtlich des Index kann man davon ausgehen, dass ein gegenüber dem Wert von  $k_1$  erhöhter Wert von  $k_2$  zumindest nicht ungünstiger ist als  $k_1 = k_2$  zu wählen, da die Einheit, die sich zu kürzesten Folgen ergibt, oftmals bereits das erste konstruierte Dirichlet-Element selbst und somit das erste Element einer LLL-reduzierten Basis (oder bezüglich  $T_{2,\underline{\lambda}}$  kürzeste Element) der Ordnung ist. Letztendlich ist es für den Einzelfall wegen der gegenseitigen Einflüsse innerhalb des Algorithmus schwer, im Vorhinein optimale Werte für  $k_1$  und  $k_2$  festzulegen. Im Folgenden werden wir in Algorithmus 17 mit  $(k_1, k_2) = (5, 20)$  arbeiten, da sich dies bei gleichmäßiger Berücksichtigung der Anzahl konstruierter Elemente, der Rechenzeit und des Index für verschiedene Beispiele als sinnvoll erwiesen hat. (Wir haben für verschiedene Beispiele verschiedene Kombinationen für  $(k_1, k_2)$  getestet. Einen Auszug aus den Testreihen findet man im Anhang in Tabelle 5.5 und 5.6.)

#### 4 Schlussbetrachtungen

(4) Da wir innerhalb von Algorithmus 17 nun systematisch auch nicht-einfache Konjugiertenrichtungen verwenden, sei an die Möglichkeit erinnert, bei der Konstruktion der Hilfsfolgeelemente den Wert  $\delta$ , der in die Gewichtung des Konjugiertengitters eingeht und die Konjugiertenbedingungen gewährleistet, höher zu initialisieren (siehe Kapitel 2, Bemerkung 2.4). Wenn wir den Erhöhungsfaktor  $\nu$  wie in (2.25) wählen, unterbinden wir zu viele vergebliche Konstruktionen von Modulelementen. Dies nimmt einerseits einen positiven Einfluss auf die Rechenzeit. Andererseits ist der Gesamteinfluss dieser Erhöhung im Allgemeinen wieder schwer abzusehen: so kann es in Ausnahmen passieren, dass daraus die Konstruktion von mehr Konjugiertenfolgeelementen bis zum Auftreten der Einheit resultiert, da die Konjugiertenbetragseigenschaften und somit die Normbeträge verändert werden (siehe Tabelle 5.4 im Anhang und vergleiche die Tabellen in Abschnitt 5.1.3).

Um Strategie 4 aus [Wil93], die er als optimale Strategie zur Berechnung unabhängiger Einheiten nach Dirichlet mit Normvergleichsmethode entwickelt hat, mit Algorithmus 17 zu vergleichen, haben wir wieder für verschiedene Zahlkörper ein System von  $r$  unabhängigen Einheiten der Maximalordnung berechnet. Dabei wählen wir als Konstruktionsmethoden der Konjugiertenfolgen Algorithmus 3 (LLL) oder Algorithmus 6 (Auszählen kürzester Elemente). Die Ergebnisse der vergleichenden Beispielergebnisse sind im Anhang (Abschnitt 5.1.3) zu finden.

**Auswertung der experimentellen Ergebnisse:** Anders als bei den Berechnungen zu Strategie 1 beeinflussen die gefundenen Einheiten hier die nachfolgend berechnete Konjugiertenrichtung und dadurch wiederum die Konjugiertenfolge, entlang derer nach Einheiten gesucht wird. Da die beiden Suchmethoden zu einer gegebenen Konjugiertenfolge unterschiedliche Einheiten finden können, ergeben sich dementsprechend im Anschluss unterschiedliche gewährleistende Konjugiertenrichtungen und Konjugiertenfolgen. So kann es bei den Berechnungen zu Strategie 4 dazu kommen, dass bei der Bewertungsmatrixmethode die Anzahl zu konstruierender Dirichlet-Elemente, bedingt durch die unterschiedlichen Konjugiertenfolgen, entlang derer gesucht wird, in einigen Beispielen höher ist als bei der Normvergleichsmethode. Wegen dieser inneren Einflüsse bietet sich bei den Beispielen zu Strategie 4 also kein vergleichbar klares Bild hinsichtlich der drei Kriterien wie bei Strategie 1.

#### 4.1 Vergleich der vorgestellten Verfahren

Um einen Überblick über die Ergebnisse zu bekommen, betrachten wir die Kontingenztafel zu den Tabellen 5.7, 5.8 und 5.10. Wir betrachten als Merkmale die Anzahl zu berechnender Dirichlet-Elemente ( $\#DE$ ) und den Index. Wir geben für die 62 Beispiele, bei denen der Index berechnet wurde, die absoluten Häufigkeiten von vier verschiedenen Kombinationen von zwei Merkmalsausprägungen<sup>1</sup> an.

	BM Index $\leq$	NV Index $<$	Summe
BM $\#DE \leq$	21	29	50
NV $\#DE <$	8	4	12
Summe	29	33	62

Wegen der Aufteilung in je zwei Merkmalsausprägungen kann aus der Kontingenztafel natürlich nicht ersehen werden, wie hoch die Unterschiede hinsichtlich Anzahl und Index sind. Wir sehen aber, dass bei Verwendung der Bewertungsmatrixmethode dennoch meistens weniger Elemente zu konstruieren sind und somit weniger Rechenzeit erforderlich ist, wohingegen die Normvergleichsmethode häufiger einen kleineren Index bedingt. Allgemein lässt sich feststellen, dass der Index eines mit Strategie 4 berechneten Einheitensystems kleiner ist als bei der Berechnung mit Strategie 1. Die Unterschiede zwischen dem Index bei Bewertungsmatrix- und Normvergleichsmethode sind bei Strategie 4 im Vergleich zu Strategie 1 geringer und in relativ vielen Fällen ist der Index bei der Bewertungsmatrixmethode sogar kleiner. In wenigen Fällen benötigte die Bewertungsmatrixmethode - anders als bei den Ergebnissen zu Strategie 1 - mehr Rechenzeit als die Normvergleichsmethode, obwohl weniger Dirichlet-Elemente zu berechnen waren. Dies liegt zum einen an der Implementation der Berechnung der gewährleistenden Konjugieretenrichtung (Algorithmus 7); bei der Bewertungsmatrixmethode ergeben sich die Einheiten als Potenzprodukte der Dirichlet-Elemente und die Reduktion der zugehörigen  $L$ -Vektoren erfordert eine hohe Präzision. Zum anderen zeigte sich in einigen Beispielen zu Strategie 4, dass die Berechnung der Potenzprodukte selbst sehr zeitaufwändig sein kann. Um solche Berechnungen von vorneherein zu verhindern, können zum Beispiel entsprechende Relationenmatrixspalten, deren Koeffizienten eine gewisse Größe überschreiten, ähnlich wie beim Spaltentest (siehe Bemerkung 3.5, S. 59) aussortiert werden<sup>2</sup>.

<sup>1</sup> Die Merkmalsausprägung „NV Index  $<$ “ bedeutet dabei, dass der Index der mit Normvergleichsmethode berechneten Einheiten kleiner war als der Index der mit Bewertungsmatrixmethode berechneten Einheiten. Die Merkmalsausprägung „BM  $\#DE \leq$ “ steht dafür, dass die Anzahl zu berechnender Dirichlet-Elemente bei der Bewertungsmatrixmethode kleiner als die (oder gleich der) Anzahl bei der Normvergleichsmethode war.

<sup>2</sup> Wir haben dies für die problematischen Fälle mit Koeffizientenbetragsschranke gleich 10 oder 50 durchgeführt. Tatsächlich kann mit einem solchen Vorgehen erreicht werden, dass der Rechenaufwand der Bewertungsmatrixmethode dann, bedingt durch die kleineren Anzahl zu konstruierender Elemente, kleiner ist als der Rechenaufwand der Normvergleichsmethode (siehe S.110 unten).

#### 4 Schlussbetrachtungen

Aus diesen Beobachtungen lässt sich für die Konstruktion unabhängiger Einheiten im Rahmen der Berechnung von Grundeinheiten die Empfehlung ableiten, den Algorithmus 17 mit den folgenden Ergänzungen und Parametern zu verwenden:

- zusätzliches Führen einer Normbetragsliste zu jeder Konjugiertenfolge, so dass die Bewertungsmatrixmethode als Ergänzung der Normvergleichsmethode fungiert,
- Wahl der Parameter  $k_1 > 0$  und  $k_2 > 0$  (Verwendung von Strategie 4) mit  $k_1 \leq k_2$ ,
- Vermeidung aufwändiger Potenzproduktberechnungen durch Aussortieren entsprechender Relationenmatrixspalten,
- Konstruktion der Konjugiertenfolgenelemente mit Algorithmus 6,
- Wahl der Faktorbasis als Menge von Primidealen mit Norm unterhalb von  $B = 85$ .

Bei diesem Vorgehen können einerseits bereits berechnete unabhängige Einheiten aus der Regulatorabschätzung miteinbezogen werden. Andererseits wird durch die Verringerung der Anzahl zu konstruierender Dirichlet-Elemente bei Verwendung der Bewertungsmatrixmethode eine niedrigere Rechenzeit erzielt als bei bloßer Verwendung der Normvergleichsmethode. Und schließlich ist der Index des Systems unabhängiger Einheiten in der Einheitengruppe vergleichsweise klein.

Falls das übergeordnete Ziel nicht die Berechnung von Grundeinheiten sein sollte, sondern ausschließlich ein System unabhängiger Einheiten einer beliebigen Ordnung berechnet werden soll, sollte Strategie 1 (Berechnung von Einheiten zu einfachen Konjugiertenrichtungen mit Ergänzung der Normvergleichsmethode durch Bewertungsmatrixmethode) verwendet werden, da die Anzahl zu konstruierender Elemente und somit die Rechenzeit geringer ist als bei der Berechnung mit Strategie 4.

## 4.2 Zusammenfassung

In diesem Abschnitt werden die Ergebnisse der vorliegenden Arbeit zusammengefasst.

Im zweiten Kapitel wurde zunächst die Berechnung unabhängiger Einheiten nach Dirichlet in der bisher bekannten Form, wie sie in [Wil93] und [Poh93] zu finden ist, dargestellt. Die Dirichlet-Elemente werden bei diesem Vorgehen als Produkte von Hilfsfolgeelementen, die sich als erstes Element der LLL-reduzierten Basis eines Moduls ergeben, konstruiert. Im Verlauf der Darstellung fanden wir heraus, dass die  $T_{2,\lambda}$ -Normschränke der Hilfsfolgeelemente, die sich bei der bisherigen Konstruktion entsprechend der LLL-Bedingungen ergab, gesenkt werden kann, wenn das dem kürzesten Vektor des gewichteten Konjugiertengitters entsprechende Modulelement als Hilfsfolgeelement gewählt wird. Die Verwendung dieser neuen Konstruktionsmethode der Konjugiertenfolgeelemente, die wir in Algorithmus 6 in Abschnitt 2.3 vorgestellt haben, ist bei der Konstruktion von unabhängigen Einheiten als Quotienten assoziierter Konjugiertenfolgeelemente der Verwendung der bisherigen Konstruktionsmethode überlegen: sowohl die Gesamtrechenzeit als auch der Index und die Anzahl zu konstruierender Konjugiertenfolgeelemente sind bei der Berechnung unabhängiger Einheiten mit Verwendung von Algorithmus 6 für Ordnungen mit hoher Diskriminante kleiner als bei der bisherigen Konstruktion mit LLL.

Hinsichtlich der Suche nach zwei Dirichlet-Elementen mit gleichem Normbetrag kamen wir zu dem Schluss, dass das bisherige Vorgehen (Vergleich des Normbetrags jedes neu konstruierten Elements mit den Normbeträgen aller zuvor konstruierten Elemente) nicht durch eine Suchmethode mit konstantem Speicherbedarf ersetzt werden sollte.

Des Weiteren wurde untersucht, ob die Konstruktion von Konjugiertenfolgen zu nicht-einfachen Konjugiertenrichtungen beschleunigt werden kann, indem die Komponente  $\delta$  der Gewichtung des Konjugiertengitters höher als beim bisherigen Vorgehen initialisiert wird. Tatsächlich kann mit der vorgestellten Initialisierung die Konstruktion von Modulelementen, die aufgrund ihrer Konjugiertenbetrags-eigenschaften keine Hilfsfolgeelemente sind, verhindert und in manchen Fällen sogar eine Beschleunigung des gesamten Verfahrens zur Konstruktion von Einheiten erreicht werden.

Die Idee, nicht nur Quotienten von Dirichlet-Elementen, sondern auch andere Potenzprodukte, deren Normbetrag 1 ergibt, bei der Konstruktion von unabhängigen Einheiten beliebiger Ordnungen zu berücksichtigen, wurde in Kapitel 3 ausgearbeitet. Zunächst wurde der Algorithmus zur Konstruktion einer Einheit der Maximalordnung zu einer bestimmten Konjugiertenrichtung  $(I, J)$  vorgestellt: Zu einer gegebenen Faktorbasis wird die Matrix, bestehend aus den Bewertungsvektoren

#### 4 Schlussbetrachtungen

ren glatter Konjugiertenfolgeelemente zu  $(I, J)$ , auf Hermite Normalform transformiert. Wenn eine Nullspalte auftritt, ist das entsprechende Potenzprodukt der verwendeten Konjugiertenfolgeelemente zu  $(I, J)$  eine Einheit. Diese Einheit ist nicht in allen Fällen eine Einheit zur Konjugiertenrichtung  $(I, J)$ , es können sich zum Beispiel Torsionseinheiten ergeben (siehe Beispiel 5.1, S. 97). Um den hohen Aufwand für die Prüfung der Konjugiertenbetrageigenschaften der berechneten Einheit zu sparen, wurde ein hinreichender Test für die entsprechende Relationenmatrixspalte entwickelt. Potenzprodukte von Konjugiertenfolgeelementen, deren Exponentenvektoren diesen algebraischen Test bestehen, sind Einheiten zur Konjugiertenrichtung.

Die Konstruktion der Einheit einer beliebigen Ordnung zu gegebener Konjugiertenrichtung mit Bewertungsmatrixmethode und der dazu notwendigen Modifikation der Faktorbasis wurde in Abschnitt 3.2.2 erarbeitet.

Die Motivation der Konstruktion von Einheiten als Potenzprodukte von Dirichlet-Elementen (und nicht etwa beliebigen glatten Elementen der Ordnung) besteht in der Unabhängigkeit, die durch die unterschiedlichen Konjugiertenbetrageigenschaften gewährleistet werden soll. Es zeigte sich, dass die Unabhängigkeit von Einheiten, die aus den Konjugiertenfolgen zu einem System gewährleistender Konjugiertenrichtungen mit Bewertungsmatrixmethode berechnet wurden, in vielen Fällen dennoch besteht, auch wenn die Einheiten keine Einheiten zur Konjugiertenrichtung sind. Mit Algorithmus 13 wurde eine Methode vorgestellt, in welcher dies zum Tragen kommt. Die Unabhängigkeit der berechneten Einheiten wird dabei durch MLLL-Reduktion und Berechnung gewährleistender Konjugiertenrichtungen, wie dies in Abschnitt 2.4 dargestellt wurde, garantiert.

Hinsichtlich der Wahl der Faktorbasis wurden zwei verschiedene Ansätze untersucht. Aus den Ergebnissen experimenteller Untersuchungen wurde eine Empfehlung für die heuristische Wahl einer Schranke  $B$  abgeleitet, so dass bei Verwendung der Faktorbasis, die aus Primidealen mit Norm unterhalb von  $B$  besteht, die Konstruktion von unabhängigen Einheiten mit Bewertungsmatrizen effektiv erfolgen kann. Das Ergebnis der Untersuchung einer Faktorbasis aus Primidealen, die in die Faktorisierungen einer gewissen Menge der von Dirichlet-Elementen erzeugten Hauptideale eingehen, deutete darauf hin, dass die Bewertungen von Dirichlet-Elementen über einem Primideal (mit Norm unterhalb der Normbetragsschranke der Konjugiertenfolge) unabhängig verteilte Zufallsgrößen sind. Die Wahl der Faktorbasis als Menge von Primidealen mit Norm unterhalb einer günstigen Schranke erwies sich dementsprechend gegenüber der simultanen Ermittlung der Faktorbasis in Bezug auf den Gesamtrechnaufwand bei der Konstruktion unabhängiger Einheiten als zweckmäßig.

In Kapitel 4 wurde schließlich die Konstruktion unabhängiger Einheiten als Quotienten von assoziierten Dirichlet-Elementen (Normvergleichsmethode) mit der neu-

en Konstruktion unabhängiger Einheiten als spezieller Potenzprodukte von Dirichlet-Elementen (Bewertungsmatrixmethode) verglichen. In den Ergebnissen der Beispielberechnungen bestätigt sich die theoretische Überlegung, dass bei der Konstruktion der Einheit zu einer gegebenen Konjugiertenrichtung mit Bewertungsmatrixmethode weniger Konstruktionen von Dirichlet-Elementen notwendig sind als bei der Normvergleichsmethode. Gerade bei Zahlkörpern mit hoher Diskriminante und dementsprechend hoher Normbetragsschranke der Konjugiertenfolgen kann die Methode von Dirichlet zur Konstruktion unabhängiger Einheiten somit wesentlich beschleunigt werden. Im Zuge des Vergleichs konnte weiterhin festgestellt werden, dass auch bei der Einheitenkonstruktion mit Bewertungsmatrixmethode, die in Kapitel 2 eingeführte Konstruktion der Konjugiertenfolgen (Hilfsfolgenkonstruktion mit kürzesten Elementen) verwendet werden sollte.

Um die Variationsmöglichkeit von Konjugiertenrichtungen, welche durch die Verallgemeinerung der Methode von Dirichlet nach [Poh93] nutzbar gemacht wurde, anwenden zu können, wurden die verschiedenen Strategien zur Berechnung unabhängiger Einheiten aus [Wil93] in Algorithmus 17 auf die Berechnung mit Bewertungsmatrixmethode übertragen.

Der abschließende Vergleich der verschiedenen Strategien (Kombinationen von Konstruktionsmethode der Konjugiertenfolge, Suchmethode und Wahl der Konjugiertenrichtung) ergab, dass innerhalb des Verfahrens zur Berechnung von Grundeinheiten die Strategie, die Algorithmus 17 zugrunde liegt, gewählt werden sollte. Die Konstruktion der Konjugiertenfolgen sollte dabei mit Algorithmus 6 erfolgen. Mit diesem kombinierten Vorgehen können erstens unabhängige Einheiten, die sich bei den Berechnungen zur Regulatorabschätzung ergeben haben, einbezogen werden. Zweitens wird durch die Anwendung der Bewertungsmatrixmethode die Berechnung der unabhängigen Einheiten beschleunigt und drittens trägt die Variation zwischen Konstruktion zu gewährleistender Konjugiertenrichtung und Konstruktion entlang kürzester Konjugiertenfolgen zu einer wesentlichen Verringerung des Index des berechneten Systems unabhängiger Einheiten in der Einheitengruppe bei.



## 5 Anhang

Gerechnet wurde auf einem 64bit UNIX-System mit Intel Core2Duo-Prozessor (2.66 GHz oder 3.00 GHz) und 2 GB RAM. Innerhalb eines Beispiels (Tabelle oder Zeile zu einem Zahlkörper) wurde jeweils derselbe Prozessortyp benutzt und es wurde darauf geachtet, dass keine anderen Berechnungen auf dem Rechner durchgeführt werden, um bei den Rechenzeiten Vergleichbarkeit zu gewährleisten.

### Kleines ausführliches Beispiel zur Berechnung unabhängiger Einheiten von $\mathfrak{o}_F$

**Beispiel 5.1.** Wir betrachten den Zahlkörper  $F$ , der durch Adjunktion einer Wurzel  $\rho$  des Polynoms  $f(t) = t^7 + 6t^5 + 6$  erzeugt wird. Die Potenzbasis  $\omega_i := \rho^{i-1} (1 \leq i \leq 7)$  ist eine Ganzheitsbasis. Wir berechnen drei unabhängige Einheiten der Maximalordnung von  $F$  mit dem Algorithmus 13, wobei wir als Faktorbasis die Primideale mit Norm unterhalb von 85 wählen. Zunächst werden Dirichlet-Elemente zur Konjugiertenrichtung  $(\{1\}, \{2, 3, 4\})$  berechnet. Nach 20 konstruierten Dirichlet-Elementen wird aus den Bewertungsvektoren der 14  $S$ -Einheiten unter den Dirichlet-Elementen eine Nullspalte gewonnen. Die zugehörige Einheit

$$\varepsilon_1 := \frac{\gamma_{20}}{\gamma_{10}} = -1288\omega_7 + 1251\omega_6 - 8943\omega_5 + 8686\omega_4 - 8436\omega_3 + 8193\omega_2 - 7957\omega_1$$

ist keine Torsionseinheit. Es gilt  $T_2(\varepsilon_1) = 1759645699$ . Mit Algorithmus 7 wird daraufhin die gewährleistende Konjugiertenrichtung  $(\{1, 2\}, \{3, 4\})$  berechnet, zu der 10 Konjugiertenfolgeelemente (7 davon sind  $S$ -Einheiten) konstruiert werden bis die nächste Nullspalte auftritt. Die zugehörige Einheit

$$\varepsilon_2 := \frac{\gamma_9^9 \gamma_{11}^2}{\gamma_4^9 \gamma_6^6} = 11894854377780009967850872583300410493816\omega_7 -$$

$$58083263114871883882117019668579424459523\omega_6 -$$

$$1637343917399117700996284367630689813460\omega_5 -$$

$$1965347780805511229570370757150012945069\omega_4 +$$

$$9829649626133839024027946075220967996503\omega_3 +$$

$$11666397539021003938428757756778647407917\omega_2 -$$

$$58460528132408727985120069301165274529633\omega_1$$

## 5 Anhang

ist ebenfalls keine Torsionseinheit. Es gilt  $T_2(\varepsilon_2) = 6.628 \cdot 10^{85}$ . In Algorithmus 13 wird nun mit dem MLLL ein minimales Erzeugendensystem berechnet. Es stellt sich heraus, dass  $\varepsilon_1$  und  $\varepsilon_2$  unabhängig sind. Zu den MLLL-reduzierten Einheiten wird die gewährleistende Konjugiertenrichtung  $(\{1, 2, 3\}, \{4\})$  berechnet. Nach Konstruktion von 14 Konjugiertenfolgeelementen, von denen 6 S-Einheiten sind, ergibt sich die erste Nullspalte in der Bewertungsmatrix. Aus der entsprechenden Kombination von Relationenmatrixspalte und S-Einheiten ergibt sich die Torsionseinheit

$$\zeta := \frac{\gamma_8 \gamma_{14}}{\gamma_9 \gamma_{13}} = \omega_1.$$

Es werden zwei weitere Dirichlet-Elemente konstruiert, bis sich eine weitere S-Einheit ergibt. Nach Reduktion der um den Bewertungsvektor von  $\gamma_{16}$  erweiterten Bewertungsmatrix auf Hermite Normalform ergibt sich eine neue Nullspalte. Die zugehörige Einheit

$$\varepsilon_3 := \frac{\gamma_{16} \gamma_8^3}{\gamma_{13}^3} = \omega_2 + \omega_1$$

ist keine Torsionseinheit, da  $T_2(\varepsilon_2) = 24$  gilt. Bei der MLLL-Reduktion stellt sich allerdings heraus, dass  $\varepsilon_1 \varepsilon_3^3 = -1$  gilt. Die als Potenzprodukt von Konjugiertenfolgeelementen zu der gewährleistenden Konjugiertenrichtung gewonnene Einheit  $\varepsilon_3$  ist also von den zuvor konstruierten Einheiten nicht unabhängig. Nach insgesamt 36 konstruierten Dirichlet-Elementen ergibt sich eine weitere Nullspalte. Die zugehörige Einheit

$$\varepsilon_4 := \frac{\gamma_{36}}{\gamma_8 \gamma_{31} \gamma_{33}}$$

ist keine Torsionseinheit und von den anderen unabhängig. Bei der letzten MLLL-Reduktion werden die drei Erzeuger

$$\begin{aligned} \eta_1 = & 2864299496263375689950612140716139878003749598197\omega_7 - \\ & 43716398411733135474378549073329160412525132498597\omega_6 - \\ & 1219089051605759631045839596680681574325419739256\omega_5 - \\ & 409554892886729219893045673962257617935938901322\omega_4 + \\ & 7305989170262402994083661663246587020781007181302\omega_3 + \\ & 2660906864256743783207939930276927870157828976017\omega_2 - \\ & 43778998223606953493225609160061447759323771018049\omega_1, \end{aligned}$$

$$\begin{aligned}
\eta_2 = & 119928705080975151443619281735272089742027597724644471850174916\omega_7 - \\
& 174135667559185710121983520321485403351629274225483025713313839\omega_6 + \\
& 712089413602702195801443423801276469467854312436870684306041363\omega_5 - \\
& 855574201799526980642295527166922759648754280950806751106756341\omega_4 - \\
& 166651749520746787134646551683467426295491951739321349044325897\omega_3 + \\
& 1018782655963654885377951580751693528993318002391956650865540049\omega_2 - \\
& 521866055928224276714164354075234669186712664726856731196699129\omega_1, \\
\eta_3 = & -1288\omega_7 + 1251\omega_6 - 8943\omega_5 + 8686\omega_4 - 8436\omega_3 + 8193\omega_2 - 7957\omega_1
\end{aligned}$$

mit  $\langle \eta_1, \eta_2, \eta_3 \rangle = \langle \varepsilon_1, \varepsilon_2, \varepsilon_4 \rangle$  berechnet. Dies sind die unabhängigen Einheiten, die von Algorithmus 13 zurückgegeben werden.

## 5.1 Beispiele zum Vergleich

### 5.1.1 Beispiele zu Strategie 1 und gegebenen Konjugiertenrichtungen

1.) Für verschiedene algebraische Zahlkörper  $F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$  werden mit Algorithmus 4 (Normvergleichmethode) oder Algorithmus 10 (Bewertungsmatrixmethode) Einheiten der Maximalordnung  $\mathfrak{o}_F$  zu den  $r$  einfachen Konjugiertenrichtungen  $(I_i, J_i) = (\{i\}, \{1, \dots, r_1 + r_2\} \setminus \{i\})$  für  $(1 \leq i \leq r)$  berechnet. Als Konstruktionsmethoden für die Dirichlet-Elemente verwenden wir entweder den Algorithmus 3 (Konstruktion mit LLL) oder den Algorithmus 6 (Konstruktion mit ausgezähltem kürzestem Element: für  $\hat{C}_1$  in Algorithmus 6 wählen wir  $\mathcal{K} = \mathcal{Y}_n^{\frac{1}{2}} |disc(R)|^{\frac{1}{2n}}$ ). Für die vier verschiedenen Algorithmuskombinationen werden ermittelt: die Anzahl zu berechnender Dirichlet-Elemente (DE), die Rechenzeit (Zeit) und der Quotient  $\frac{|\det(L(\varepsilon_1), \dots, L(\varepsilon_r))|}{Reg_{\mathfrak{o}_F}}$  (Index) für die  $r$  berechneten unabhängigen Einheiten  $\varepsilon_1, \dots, \varepsilon_r$ . Für die Bewertungsmatrixmethode betrachten wir zusätzlich: die Größe der verwendeten Faktorbasis  $\#S$ , bestehend aus Primidealen mit Norm kleiner als  $B = 85$  (falls  $B = 400$  verwendet wird, setzen wir die entsprechenden Ergebnisse in **Schreibmaschinenschrift**), die Anzahl der  $S(B)$ -Einheiten unter den Dirichlet-Elementen (SE) und die Anzahl zusätzlich konstruierter Nullspalten (zNSp), die aufgrund des Tests (Algorithmus 11) verworfen werden.

2.) Für beliebige nicht-einfache Konjugiertenrichtungen (zum Beispiel  $I_{spez} = \{2, 3, 4, 5\}$ ) werden mit Algorithmus 4 (Normvergleichmethode) und Algorithmus 10 (Bewertungsmatrixmethode) Einheiten zu dieser Konjugiertenrichtung berechnet. Als Konstruktionsmethoden für die Dirichlet-Elemente verwenden wir Algorithmus 3. Da hier nicht-einfache Konjugiertenrichtungen verwendet werden, werden bei der Initialisierung von  $\delta$  verschiedene Erhöhungsfaktoren (siehe Bemerkung 2.4) verwendet. Wir ermitteln für die vier verschiedenen Algorithmuskombinationen die Anzahl zu berechnender Dirichlet-Elemente (DE), die Rechenzeit (Zeit) bis eine Einheit zu dieser Konjugiertenrichtung gefunden wurde. Für die Bewertungsmatrixmethode betrachten wir zusätzlich die Größe der verwendeten Faktorbasis  $\#S$ , bestehend aus Primidealen mit Norm kleiner als  $B = 85$  (falls  $B = 400$  verwendet wird, setzen wir die entsprechenden Ergebnisse in **Schreibmaschinenschrift**), die Anzahl der  $S(B)$ -Einheiten unter den Dirichlet-Elementen (SE) und die Anzahl zusätzlich konstruierter Nullspalten (zNSp), die aufgrund des Tests (Algorithmus 11) verworfen werden.

**Bemerkung:** Da die Indexberechnung in manchen Beispielen nicht in absehbarer Zeit terminiert, fügen wir an diesen Stellen ein Sternchen (\*) ein. In den Fällen,

### 5.1 Beispiele zum Vergleich

bei denen die Einheitenberechnung selbst vor Termination abgebrochen wurde, geben wir die Zeitspanne bis zum Abbruch der Berechnungen in Tagen an (Abbruch: Zeitspanne).

Tabelle 5.1: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 1: Konstruktion der Konjugiertenfolge mit Algorithmus 3 (LLL)

$f(t)$	Bewertungsmatrixmethode					Normvergleichsmethode		
	$\#S$	$zNSp$	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^{17} + 2$	23	2	50 (42)	4.73	5.020E12	52	3.48	6.172E12
$t^{18} + 2$	22	0	41 (28)	3.60	9.087E11	42	3.18	9.235E11
$t^{19} + 2$	23	10	144 (79)	49.55	1.367E18	127	19.88	6.287E16
$t^{20} + 2$	24	4	159 (72)	44.65	5.045E20	227	60.78	6.300E19
$t^{21} + 2$	15	1	133 (51)	38.44	7.085E21	198	60.58	2.989E21
$t^{22} + 2$	21	12	308 (99)	273	2.540E26	492	545	4.999E24
$t^{23} + 2$	22	8	499 (134)	1273	9.530E32	559	763	4.696E24
$t^{24} + 2$	18	6	663 (105)	4180	9.472E37	1094	5133	5.265E29
$t^{25} + 2$	19	13	1129 (168)	3790	*	1636	8890	*
$t^{26} + 2$	19	190	2472 (487)	51944	*	6357	407810	*
$t^{27} + 2$	20	43	2700 (225)	94797	*	4221	188145	*
$t^{28} + 2$	20	21	4199 (200)	170943	*	-	Abbruch:	7 Tage
$t^{29} + 2$	-	-	Abbruch:	9 Tage	-	-	Abbruch:	9 Tage
$t^{15} + 3$	26	16	153 (101)	14.18	1.208E14	249	27.36	2.921E13
$t^{16} + 3$	29	0	20 (17)	1.52	6.572E9	20	1.17	6.572E9
$t^{17} + 3$	23	7	216 (96)	30.86	4.348E18	349	66.08	2.582E17
$t^{18} + 3$	21	0	21 (19)	1.9	3.049E10	21	1.65	3.049E10
$t^{19} + 3$	23	8	344 (99)	158.86	2.028E22	513	304.59	3.649E19
$t^{20} + 3$	19	5	65 (41)	11.23	4.446E15	65	9.54	4.446E15
$t^{14} + 5$	21	13	265 (79)	70.53	3.925E11	363	42.17	1.620E11
$t^{15} + 5$	15	8	315 (102)	178	5.570E18	711	274	9.558E15
$t^{16} + 5$	20	6	441 (196)	595	1.004E25	1622	2487	1.135E17
$t^{17} + 5$	23	32	907 (159)	1861	2.843E22	1516	3204	1.118E20
$t^{18} + 5$	22	15	1632 (135)	4918	3.882E25	4234	43039	5.744E22
$t^{19} + 5$	23	78	3817 (259)	85552	1.338E35	7049	224734	1.934E25

5 Anhang

Tabelle 5.2: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 1:  
Konstruktion der Konjugiertenfolgen mit Algorithmus 6 (Aus zählen)

$f(t)$	Bewertungsmatrixmethode					Normvergleichmethode		
	# $S$	$zNSp$	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^{17} + 2$	23	3	53 (44)	2.70	1.792E11	72	5.87	8.205E10
$t^{18} + 2$	22	0	48 (36)	2.62	1.286E9	76	4.120	4.964E9
$t^{19} + 2$	23	6	90 (59)	6.36	1.630E14	128	12.07	9.796E13
$t^{20} + 2$	24	7	140 (54)	11.42	2.204E16	184	18.49	7.880E12
$t^{21} + 2$	15	5	154 (60)	17.59	1.584E17	186	43.50	2.938E17
$t^{22} + 2$	21	1	203 (71)	29.14	1.101E19	225	50.52	4.901E17
$t^{23} + 2$	22	3	190 (72)	37.64	1.342E19	243	71.60	1.217E18
$t^{24} + 2$	69	6	408 (224)	159	2.348E29	653	334	6.945E22
$t^{25} + 2$	19	16	566 (71)	395	4.755E27	804	726	6.671E26
$t^{26} + 2$	19	31	931 (242)	1035	*	1299	2652	*
$t^{27} + 2$	20	11	1300 (160)	1826	*	1389	7430	*
$t^{28} + 2$	20	29	2601 (211)	10548	*	2960	15110	*
$t^{29} + 2$	22	8	2245 (223)	8610	*	3032	27068	*
$t^{15} + 3$	62	7	84 (72)	7.64	4.944E10	103	4.22	2.013E10
$t^{16} + 3$	76	0	17 (17)	1.89	1.182E7	17	1.25	1.182E7
$t^{17} + 3$	76	9	169 (120)	31.62	1.981E15	305	49.63	7.317E13
$t^{18} + 3$	93	0	33 (33)	3.23	3.235E9	33	2.34	3.235E9
$t^{19} + 3$	82	12	370 (201)	193	2.390E20	784	427	3.663E16
$t^{20} + 3$	74	2	59 (53)	8.99	3.150E12	59	5.18	3.150E12
$t^{14} + 5$	74	36	301 (175)	29.04	1.140E9	439	47.66	1.413E8
$t^{15} + 5$	76	4	138 (79)	13.01	2.021E12	378	104	2.144E9
$t^{16} + 5$	70	35	352 (174)	89.99	9.847E11	700	275	7.440E11
$t^{17} + 5$	76	33	759 (295)	345	6.378E19	1189	552	1.338E18
$t^{18} + 5$	73	94	1933 (408)	3742	2.532E20	3367	7647	8.419E19
$t^{19} + 5$	82	207	3023 (658)	14379	*	8270	80015	5.042E26
$t^{30} + 2$	64	19	3096 (374)	29465	*	4170	102779	*
$t^{31} + 2$	86	111♣	5447 (921)	131144	*	9844	321092	*

♣ Hier wurden Relationenmatrixspalten mit Koeffizientenbeträgen größer als 50 aussortiert.

5.1 Beispiele zum Vergleich

Tabelle 5.3: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 1:  
Konstruktion der Konjugiertenfolgen mit Algorithmus 6 (Auszählen)

$f(t)$	Bewertungsmatrixmethode					Normvergleichmethode		
	#S	zNSp	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^4 - 3t^2 - 20$	28	0	4 (4)	0.09	5	4	0.04	5
$t^5 + 9t + 12$	24	0	7 (7)	0.07	22	26	0.11	13
$t^6 - 4t^5 - 6$	23	2	25 (24)	0.22	753	54	0.29	207
$t^7 + 6t^4 - 8$	18	1	8 (8)	0.17	157	8	0.10	157
$t^8 + 8t^5 + 9$	21	11	38 (37)	0.45	1684	40	0.34	1684
$t^9 + 7t^4 + 5$	23	0	53 (28)	0.61	3996	50	0.45	3996
$t^{10} - 5t^8 - 4$	19	10	44 (44)	0.68	3.227E5	44	0.60	3.227E5
$t^{11} - 5t^7 + 3$	22	3	73 (53)	1.34	3.431E6	185	4.78	1.284E8
$t^7 + 11$	22	4	34 (28)	0.34	287	41	0.26	132
$t^7 + 13$	22	1	18 (16)	0.23	27	18	0.14	27
$t^7 + 15$	22	14	69 (51)	0.74	216	120	0.86	52
$t^7 + 20$	20	2	28 (27)	0.32	1356	66	0.46	542
$t^7 + 23$	22	0	64 (34)	0.56	1.244E4	205	1.77	120
$t^7 + 35$	22	7	92 (51)	0.95	8.570E4	688	16.25	4730
$t^7 + 36$	27	2	11 (11)	0.19	91	17	0.14	91
$t^7 + 37$	29	15	168 (80)	2.01	1.723E4	345	5.79	24.
$t^7 + 43$	23	15	130 (59)	1.31	2.797E4	187	1.48	1569
$t^7 + 44$	27	0	54 (29)	0.55	655	61	0.42	655
$t^7 + 51$	22	2	107 (31)	1.00	150	481	12.22	237
$t^7 + 52$	20	1	22 (13)	0.26	43	22	0.17	43
$t^7 + 53$	22	36	298 (91)	5.38	2.056E6	731	20.11	1.053E4
$t^7 + 60$	20	0	38 (16)	0.36	11	40	0.29	9
$t^7 + 67$	23	3	97 (51)	1.05	1.780E6	417	8.76	525
$t^7 + 101$	22	52	588 (113)	20.61	2.048E4	733	23.96	800
$t^7 + 113$	22	13	382 (65)	6.68	2.080E5	683	26.79	385
$t^7 + 126$	20	7	168 (50)	1.87	2.092E4	310	4.13	2565
$t^7 + 154$	20	25	903 (75)	43.88	1.715E5	1737	167	2.063E4
$t^7 + 263$	23	7	350 (69)	15.32	*	2959	702	4892

Tabelle 5.4: Vergleich hinsichtlich beliebiger Konjugiertenrichtungen

$\nu = 1$		BewMatr. mit Algo. 3				NormVgl. mit Algo. 3	
$f(t) =$	$I_{spez} =$	$\#S$	zNSp	DE (SE)	Zeit	DE	Zeit
$t^{13} - 8t^6 + 2$	$\{2, 3, 4, 5\}$	19	0	55 (12)	2.15	59	1.66
$t^{25} + 2$	$\{4, 7, 11\}$	19	0	66 (12)	62	66	71
$t^{16} - 5t^{13} - 4$	$\{2, 5, 7\}$	26	2	161 (23)	49	224	79.89
$t^{15} - 11$	$\{1, 2, 6\}$	96	3	259 (63)	119	298	105
$t^6 - 17953$	$\{1, 2\}$	34	1	57 (16)	0.44	397	7.74
$t^{20} + 9$	$\{1, 3, 5, 7, 9\}$	21	0	60 (13)	11.73	60	12.21
$t^{18} - t^{17} + 5$	$\{4, 6, 8\}$	27	32	661 (59)	1948	107	23
$t^{12} + 241$	$\{1, 6\}$	24	0	27 (7)	0.69	70	1.39
$t^{14} + 7t^{11} + 8$	$\{3, 4, 6\}$	21	1	51 (11)	2.78	98	6.18
$t^{17} + 6$	$\{2, 3, 6, 7\}$	23	2	238 (21)	122	770	1844
$t^{28} + 2$	$\{2, 5, 8, 11\}$	20	3	619 (21)	18985	1537	222387
$t^{24} - 3$	$\{1, 7, 12\}$	15	1	1462 (16)	13287	338	3992
$\nu$ wie in (2.25)		BewMatr. mit Algo. 3				NormVgl. mit Algo. 3	
$f(t) =$	$I_{spez} =$	$\#S$	zNSp	DE (SE)	Zeit	DE	Zeit
$t^{13} - 8t^6 + 2$	$\{2, 3, 4, 5\}$	19	0	40 (13)	1.81	44	1.4
$t^{25} + 2$	$\{4, 7, 11\}$	19	1	100 (16)	159	100	162
$t^{16} - 5t^{13} - 4$	$\{2, 5, 7\}$	26	6	126 (26)	31.86	394	365
$t^{15} - 11$	$\{1, 2, 6\}$	96	6	200 (65)	118	472	766
$t^6 - 17953$	$\{1, 2\}$	34	3	73 (21)	0.66	356	7.84
$t^{20} + 9$	$\{1, 3, 5, 7, 9\}$	21	2	71 (18)	35	39	9.7
$t^{18} - t^{17} + 5$	$\{4, 6, 8\}$	27	1	176 (19)	117	217	154
$t^{12} + 241$	$\{1, 6\}$	24	3	86 (9)	2.6	86	2.12
$t^{14} + 7t^{11} + 8$	$\{3, 4, 6\}$	21	3	70 (13)	5.65	158	24.74
$t^{17} + 6$	$\{2, 3, 6, 7\}$	74	17	348 (76)	579	852	5529
$t^{28} + 2$	$\{2, 5, 8, 11\}$	20	1	335 (15)	5205	355	5712
$t^{24} - 3$	$\{1, 7, 12\}$	15	6	328 (21)	6942	799	33812

## 5.1.2 Strategie 2, 3 und 4 im Vergleich

Bei den Berechnungen mit Algorithmus 17 wurden für  $k_1$  und  $k_2$  unterschiedliche Werte gewählt. Zum Vergleich wurde die Berechnung zusätzlich mit Algorithmus 3.11 aus [Wil93, S.30] durchgeführt (abgekürzt *NormVgl.*). Es werden dieselben Werte wie bei Strategie 1 erfasst.

Tabelle 5.5: Zur Wahl von  $k_1$  und  $k_2$ 

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$		Algo 17 (mit Algo 3)			NormVgl. (mit Algo 3)		
$f(t) =$	$(k_1, k_2)$	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^{19} - 2$	(5, 5)	144 (90)	16.28	1.183E11	183	27.12	2.663E10
	(5, 10)	169 (103)	15.62	1.183E11	205	21.37	1.012E8
	(10, 5)	119 (71)	14.60	3.191E11	180	31.99	6.123E13
	(5, 20)	175 (102)	11.14	3.705E8	170	11.67	1.012E8
	(5, 50)	160 (94)	7.94	3.705E8	287	18.64	1.470E8
	(10, 20)	159 (96)	15.27	1.183E11	210	24.70	1.012E8
	(1, 0)	111 (63)	18.13	2.191E16	149	30.37	5.262E14
	(0, 1)	377 (221)	17.28	5.085E4	397	24.20	3.977E4
$t^{14} + 5$	(5, 5)	301 (133)	23.66	1.057E8	480	50.68	1.551E6
	(5, 10)	549 (230)	29.46	3.943E7	545	51.46	1.551E6
	(10, 5)	212 (83)	15.23	3.752E8	367	22.02	1.071E5
	(5, 20)	506 (212)	28.00	1.198E5	502	19.88	9.673E4
	(5, 50)	460 (195)	16.22	1.198E5	460	14.62	9.673E4
	(10, 20)	562 (235)	30.16	3.943E7	555	52.01	1.551E6
	(1, 0)	305 (105)	29.00	4.122E14	494	85.27	3.114E10
	(0, 1)	443 (190)	20.11	1.198E5	443	13.66	9.673E4
$t^{17} + 3$	(5, 5)	312 (142)	20.29	2.066E9	357	16.72	3.338E7
	(5, 10)	302 (132)	16.98	1.451E6	299	11.65	1.095E6
	(10, 5)	253 (116)	19.84	6.335E14	490	45.43	9.383E9
	(5, 20)	252 (112)	12.03	1.451E6	392	13.66	1.035E6
	(5, 50)	347 (149)	14.41	1.035E6	347	10.52	1.035E6
	(10, 20)	283 (131)	16.52	2.066E9	314	12.64	1.095E6
	(1, 0)	204 (97)	22.35	2.353E17	497	107.68	5.794E16
	(0, 1)	313 (141)	12.36	1.035E6	313	9.08	1.035E6

5 Anhang

Bei der Konstruktion der Konjugiertenfolgen wurde Algorithmus 3 und Algorithmus 6 (jeweils mit  $\nu = 1$ ) verwendet. Dabei entspricht die Wahl  $(k_1, k_2) = (1, 0)$  einer Berechnung von unabhängigen Einheiten nach Strategie 2 und die Wahl  $(k_1, k_2) = (0, 1)$  entspricht der Berechnung von unabhängigen Einheiten nach Strategie 3.

Tabelle 5.6: Zur Wahl von  $k_1$  und  $k_2$

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$		Algo 17 (mit Algo 6)			NormVgl. (mit Algo 6)		
$f(t) =$	$(k_1, k_2)$	DE (SE)	<i>Zeit</i>	Index	DE	<i>Zeit</i>	Index
$t^{22} + 2$	(5, 5)	449 (151)	<i>86.22</i>	1.832E10	643	<i>100.54</i>	3.227E13
	(5, 10)	355 (133)	<i>36.87</i>	9.179E6	658	<i>89.03</i>	1.090E14
	(10, 5)	425 (140)	<i>129.83</i>	7.350E15	489	<i>111.08</i>	3.877E13
	(5, 20)	331 (128)	<i>25.51</i>	3.692E4	573	<i>48.31</i>	1.635E11
	(5, 50)	301 (116)	<i>20.14</i>	3.692E4	1437	<i>261.70</i>	8.191E9
	(10, 20)	286 (101)	<i>46.20</i>	9.649E9	653	<i>90.40</i>	1.090E14
	(1, 0)	333 (108)	<i>104.74</i>	4.735E24	437	<i>133.23</i>	2.514E17
	(0, 1)	263 (106)	<i>120.13</i>	1.136E4	1366	<i>251.82</i>	1.929E8
$t^{25} - 2$	(5, 5)	1364 (237)	<i>1103</i>	1.410E23	958	<i>493.51</i>	1.979E21
	(5, 10)	1339 (251)	<i>608.23</i>	2.258E19	1490	<i>678.15</i>	1.450E19
	(10, 5)	903 (161)	<i>856.05</i>	4.752E25	1089	<i>1103</i>	2.163E22
	(5, 20)	1890 (350)	<i>433.22</i>	5.435E6	1763	<i>568.17</i>	2.611E9
	(5, 50)	1760 (332)	<i>197.98</i>	6.377E4	2884	<i>872.30</i>	5.982E10
	(10, 20)	1344 (248)	<i>618.07</i>	2.258E19	1505	<i>693.84</i>	1.450E19
	(1, 0)	1259 (183)	<i>3174</i>	2.365E36	760	<i>1058</i>	1.257E24
	(0, 1)	1574 (310)	<i>125.44</i>	6.377E4	2704	<i>645.91</i>	5.063E7
$t^{21} - 3$	(5, 5)	1313 (292)	<i>785.62</i>	1.035E18	2090	<i>1240</i>	1.393E11
	(5, 10)	1794 (404)	<i>435.07</i>	4.180E11	3197	<i>1250</i>	3.520E11
	(10, 5)	943 (198)	<i>495.19</i>	1.058E18	1899	<i>3394</i>	1.038E15
	(5, 20)	1883 (440)	<i>230.46</i>	7.160E5	3352	<i>829.78</i>	3.520E11
	(5, 50)	1683 (395)	<i>113.85</i>	4.360E4	4288	<i>761.32</i>	1.488E8
	(10, 20)	1814 (408)	<i>444.50</i>	4.180E11	3212	<i>1285</i>	3.520E11
	(1, 0)	833 (178)	<i>977.02</i>	7.011E29	1877	<i>4891</i>	6.214E22
	(0, 1)	1519 (363)	<i>67.29</i>	4.360E4	3119	<i>377.89</i>	4.210E8

## 5.1.3 Beispiele zu Strategie 4

Es wird ein System von  $r$  unabhängigen Einheiten der Maximalordnung  $\mathfrak{o}_F$  mit Strategie 4 und Algorithmus 4 (Normvergleichsmethode) (siehe [Wil93, S.30, Algorithmus 3.11]) und Algorithmus 17 (Bewertungsmatrixmethode) berechnet. Es werden dieselben Werte erfasst wie bei den Beispielen zu Strategie 1.

Tabelle 5.7: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 4: Konstruktion der Konjugiertenfolge mit Algorithmus 6 (kürzeste Elemente) mit  $\nu = 1$

$f(t)$	Bewertungsmatrix (Algo. 17)					Normvergleich (Strat. 4)		
	# $S$	zNSp	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^4 - 3t^2 - 20$	28	0	4 (4)	0.01	2	4	0.01	2
$t^4 + 179$	32	8	28 (28)	0.11	2	70	0.15	1
$t^5 + 9t + 12$	24	0	8 (8)	0.04	16	52	0.11	3
$t^5 + 12t + 36$	22	0	7 (7)	0.09	3	13	0.06	3
$t^6 - 4t^5 - 6$	23	1	56 (49)	0.25	1	64	0.16	1
$t^7 + 6t^4 - 8$	18	0	6 (6)	0.04	15	6	0.02	15
$t^7 + 16t^4 - 12$	25	14	70 (55)	0.70	3.228E4	111	0.66	2.230E4
$t^8 + 8t^5 + 9$	21	1	29 (29)	0.22	3	30	0.13	8
$t^8 + 15t^7 - 24$	76	30	2084 (687)	50.03	5.705E4	3647	77.02	126
$t^9 + 7t^4 + 5$	21	5	170 (116)	2.84	45	153	0.79	75
$t^{10} - 5t^8 - 4$	19	1	24 (24)	0.24	4	42	0.28	56
$t^{10} + 4t^6 + 15$	24	1	126 (98)	3.30	2298	363	3.91	224
$t^{11} - 5t^7 + 5$	22	0	152 (99)	1.34	220	62	0.45	71
$t^{12} - 7t^3 - 9$	18	0	563 (164)	8.70	42	243	2.83	190
$t^{13} + 6t^{11} - 4$	23	11	2020 (446)	64	4.179E5	2342	62	4.211E5
$t^{14} - 5t^6 + 7$	24	11	2075 (380)	42.53	132	2614	67.05	244
$t^{15} - 7t^9 + 5$	16	0	4505 (185)	220	1.858E4	4139	224	4720
$t^{15} + 6t^3 - 9$	23	58(♣)	2062 (650)	168	2.314E8	3477	278	1.341E6
$t^{16} + 3t^8 + 6$	23	13	1287 (447)	34.35	2.682E7	2525	73.02	4.080E6

(♣) In diesem Fall wurden Relationenmatrixspalten mit Einträgen, deren Betrag größer als 10 ist, aussortiert. Die Ergebnisse für  $t^{15} + 6t^3 - 9$  ohne Aussortieren: 16 zNSp; 2050 DE; 29021 Sek.; 1.965E12 (Index);

5 Anhang

Tabelle 5.8: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 4: Konstruktion der Konjugiertenfolge mit Algorithmus 6 (kürzeste Elemente) mit  $\nu = 1$

$f(t)$	Bewertungsmatrix (Algo. 17)					Normvergleich (Strat. 4)		
	#S	zNSp	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^7 + 13$	22	0	43 (39)	0.31	4	53	0.23	2
$t^7 + 14$	27	4	96 (78)	0.78	7448	271	1.39	251
$t^7 + 15$	22	8	160 (122)	1.37	16	394	2.15	162
$t^7 + 20$	20	1	73 (65)	0.66	600	109	0.57	12
$t^7 + 23$	22	1	167 (84)	1.35	483	222	1.12	4
$t^7 + 37$	29	4	483 (265)	434	194	1204	11.22	3
$t^7 + 39$	22	7	299 (133)	3.33	54	306	1.97	17
$t^7 + 51$	22	1	506 (130)	4.41	180	2187	31.36	44
$t^7 + 52$	20	0	105 (51)	0.83	4	135	0.74	17
$t^7 + 53$	22	18	720 (198)	9.74	6354	2535	44.14	1320
$t^7 + 60$	20	1	242 (102)	2.20	1	226	1.35	8
$t^7 + 67$	23	4	376 (195)	4.54	1624	1597	20.95	394
$t^7 + 101$	22	8	1255 (210)	15.98	1.00E4	3397	76.53	1003
$t^7 + 113$	22	0	764 (124)	8.75	165	1096	9.59	40
$t^7 + 127$	73	7	1083 (450)	18.9	21	1229	18.24	21
$t^7 + 129$	24	0	304 (120)	2.54	51	428	4.99	51
$t^7 + 131$	22	27(♣)	2361 (309)	92.90	6.057E4	3494	168	20
$t^7 + 263$	23	75(♣)	2591 (401)	203	1.652E4	6510	507	1082
$t^7 + 333$	22	9	1313 (203)	743	5.170E7	3100	65.14	21
$t^7 + 520$	21	4	170 (69)	1.87	644	601	4.32	6
$t^7 + 725$	87	23	1419 (544)	43.68	35	3708	144	20
$t^7 + 729$	22	0	8 (8)	0.28	39	14	0.33	11
$t^7 + 1024$	20	0	4 (4)	0.16	17	4	0.13	7
$t^7 + 30000$	20	1	264 (103)	2.15	1	373	2.8	2
$t^7 + 450000$	20	2	342 (138)	3.59	2	443	2.7	1

(♣) Da die Berechnung in diesen Fällen zu aufwändig war, wurden Relationenmatrixspalten mit Einträgen, deren Betrag größer als 50 ist, aussortiert.

5.1 Beispiele zum Vergleich

Tabelle 5.9: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 4:  
Konstruktion der Konjugiertenfolge mit Algorithmus 3 (LLL) mit  
 $\nu = 1$

$f(t)$	Bewertungsmatrix (Algo. 17)					Normvergleich (Strat. 4)		
	$\#S$	$zNSp$	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^{17} + 2$	23	0	73 (56)	3.6	3.294E6	73	2.13	3.294E6
$t^{18} + 2$	22	0	75 (51)	4.21	7.011E8	84	2.67	9.360E5
$t^{19} + 2$	23	2	370 (226)	24.54	1.034E7	369	15.43	4.610E5
$t^{20} + 2$	24	0	471 (196)	27.48	1.477E8	475	24.66	5.326E7
$t^{21} + 2$	15	0	337 (98)	28.21	2.613E6	337	23.79	2.613E6
$t^{22} + 2$	21	1	626 (181)	60.65	3.201E6	627	52.51	2.566E6
$t^{23} + 2$	22	2	1551 (429)	34844	4.106E8	1550	286	1.486E7
$t^{24} + 2$	18	1	1457 (292)	230	5.132E6	1457	229	2.190E7
$t^{25} + 2$	19	2	2786 (405)	2516	6.260E14	2047	394	3.012E13
$t^{26} + 2$	31	4	4065 (710)	128783	2.856E16	9848	70952	5.363E9
$t^{17} + 3$	76	2	309 (216)	27.93	4.549E7	584	29.68	1.818E8
$t^{18} + 3$	93	0	54 (54)	4.12	1.491E9	77	4.78	4.392E8
$t^{19} + 3$	82	6	1379 (731)	386	9.321E13	1638	210	1.506E11
$t^{20} + 3$	74	0	59 (47)	10.89	3.801E7	63	6.52	1.377E7
$t^{21} + 3$	71	4	1869 (667)	547	6.016E12	2881	645	1.060E8
$t^{22} + 3$	72	0	31 (31)	7.11	4.409E10	32	4.7	2.990E10
$t^{14} + 5$	74	6	743 (256)	23.03	1.541E6	738	21.52	2.491E5
$t^{15} + 5$	76	0	678 (310)	20.74	8.586E4	642	14.87	4.626E5
$t^{16} + 5$	70	33	1971 (1010)	119	6.149E6	1937	144	3.528E4
$t^{17} + 5$	23	8	3627 (558)	71219	3.616E18	4227	698	2.298E13
$t^{18} + 5$	73	6	2798 (761)	406	1.051E6	2791	335	7.476E5
$t^{19} + 5$	82	44	11029 (2257)	141495	*	18697	20408	1.199E19

5 Anhang

Tabelle 5.10: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 4: Konstruktion der Konjugiertenfolge mit Algorithmus 6 (kürzeste Elemente) mit  $\nu = 1$

$f(t)$	Bewertungsmatrix (Algo. 17)					Normvergleich (Strat. 4)		
	$\#S$	zNSp	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^{17} + 2$	23	3	163 (127)	9.21	58	83	3.53	2.369E5
$t^{18} + 2$	22	0	76 (58)	5.73	3.192E5	187	7.20	1.348E5
$t^{19} + 2$	23	1	177 (105)	17.09	5.247E6	338	17.11	6.526E4
$t^{20} + 2$	24	1	169 (80)	14.64	1.021E5	598	32.48	3.534E5
$t^{21} + 2$	15	2	339 (131)	37.42	8.542E4	334	22.17	2.613E6
$t^{22} + 2$	21	0	464 (161)	59.36	2.362E8	492	37.77	5.836E4
$t^{23} + 2$	22	0	466 (173)	93.63	1.013E4	857	108	1.596E10
$t^{24} + 2$	18	0	828 (207)	142	5.005E5	617	71.33	6.516E6
$t^{25} + 2$	19	1	1303 (257)	561	944	2022	374	1.322E12
$t^{26} + 2$	31	7	3710 (998)	2994( $\diamond$ )	1.373E14	3055	707	1.178E12
$t^{17} + 3$	76	7	660 (459)	28.29	2.046E6	675	31.54	4.968E5
$t^{18} + 3$	93	0	33 (33)	2.58	1.309E5	90	6.65	7.333E5
$t^{19} + 3$	82	4	722 (387)	55.03	3156	1741	138	6.070E9
$t^{20} + 3$	74	1	40 (35)	4.85	1.321E6	50	6.39	1.636E7
$t^{21} + 3$	71	8	1823 (774)	4922( $\diamond$ )	7.333E8	2879	532	3.810E6
$t^{22} + 3$	72	0	25 (25)	4.88	8.801E7	25	3.77	8.801E7
$t^{14} + 5$	74	1	480 (156)	32.97	4.952E4	421	9.62	2.530E5
$t^{15} + 5$	15	1	771 (218)	18.11	2.303E4	845	20.45	4.738E4
$t^{16} + 5$	36	11	1199 (731)	97.66	6.136E4	1937	103	3.528E4
$t^{17} + 5$	23	9	3268 (512)	21475( $\diamond$ )	1.846E14	4425	409	5.084E13
$t^{18} + 5$	22	3	4137 (466)	706	3.979E7	2071	138	4.780E4
$t^{19} + 5$	82	38	10561 (2201)	183910( $\diamond$ )	1.761E26	20053	11383	1.916E16
$t^{27} + 2$	20	12	3475 (349)	2310	4.918E5	3384	1211	1.077E12
$t^{28} + 2$	62	7	6610 (1348)	14685	*	7113	6116	*

( $\diamond$ ) In diesen Fällen werden mit dem Aussortieren von Relationenmatrixspalten mit Koeffizienten, deren Betrag über 10 liegt, folgende Ergebnisse erzielt:  $t^{26} + 2$ : 10 zNSp; 3710 DE; 1723 Sek; 1.009E13 (Index);  $t^{21} + 3$ : 13 zNSp; 2085 DE; 182 Sek.; 5.064E4 (Index);  $t^{17} + 5$ : 33 zNSp; 3717 DE; 227 Sek; 3.718E9 (Index);  $t^{19} + 5$ : 184 zNSp; 16268 DE; 5441 Sek; 7.301E21 (Index);

5.1 Beispiele zum Vergleich

Tabelle 5.11: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 4:  
Konstruktion der Konjugiertenfolge mit Algorithmus 3 (LLL) mit  $\nu$   
wie in (2.25)

$f(t)$	Bewertungsmatrix (Algo. 17)					Normvergleich (Strat. 4)		
	$\#S$	$zNSp$	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^{17} + 2$	23	5	96 (80)	3.4	9.213E7	99	2.86	2.977E6
$t^{18} + 2$	22	0	96 (56)	3.5	8.680E5	96	3.39	8.680E5
$t^{19} + 2$	23	7	426 (251)	28.01	3.178E11	268	14.78	2.688E10
$t^{20} + 2$	24	2	301 (134)	17.73	5.152E5	301	17.51	5.152E5
$t^{21} + 2$	15	1	323 (113)	25.60	2.273E8	323	25.30	2.273E8
$t^{22} + 2$	21	3	912 (296)	142	4.100E11	912	141	4.100E11
$t^{23} + 2$	22	1	1492 (476)	462	9.690E20	1804	398	7.073E12
$t^{24} + 2$	18	0	981 (173)	167	2.567E8	1965	1210	1.811E5
$t^{25} + 2$	19	2	2036 (301)	749	1.572E13	2036	741	2.962E13
$t^{26} + 2$	31	4	2121 (427)	1167	1.084E13	2584	1513	2.305E10
$t^{17} + 3$	76	4	250 (172)	17.16	1.451E6	392	16.42	1.035E6
$t^{18} + 3$	93	0	39 (38)	2.4	1.636E9	48	2.58	2.557E9
$t^{19} + 3$	82	1	925 (457)	141	3.712E10	1806	172	1.808E12
$t^{20} + 3$	74	2	73 (67)	7.45	6.246E7	73	6.38	6.246E7
$t^{21} + 3$	71	1	1498 (574)	250	1.186E10	3840	2135	2.544E9
$t^{22} + 3$	72	0	19 (19)	3.67	1.581E10	19	2.63	1.581E10
$t^{14} + 5$	74	9	506 (345)	23.97	1.198E5	502	19.84	9.673E4
$t^{15} + 5$	76	1	590 (329)	27.13	1.092E4	777	34.75	8.424E4
$t^{16} + 5$	70	30	1601 (821)	137.28	1.622E12	2449	296	9.792E9
$t^{17} + 5$	76	14	3017 (997)	778	9.261E18	5335	1854	8.377E13
$t^{18} + 5$	73	12	2666 (762)	2613	4.987E14	6159	7513	5.083E10
$t^{19} + 5$	82	87	10358 (2246)	17322	2.605E26	18336	41161	4.169E20

5 Anhang

Tabelle 5.12: Beispiele für den Vergleich der Methoden hinsichtlich Strategie 4: Konstruktion der Konjugiertenfolge mit Algorithmus 6 (kürzeste Elemente) mit  $\nu$  wie in (2.25)

$f(t)$	Bewertungsmatrix (Algo. 17)					Normvergleich (Strat. 4)		
	$\#S$	$zNSp$	DE (SE)	Zeit	Index	DE	Zeit	Index
$t^{17} + 2$	23	0	62 (47)	3.02	1538	102	3.7	9.707E4
$t^{18} + 2$	22	1	177 (133)	7.33	3.580E6	100	4.11	1.126E5
$t^{19} + 2$	23	4	118 (70)	6.06	1.506E6	301	15.29	2.908E9
$t^{20} + 2$	24	15	382 (160)	23.18	7.342E5	239	12.92	1.731E8
$t^{21} + 2$	15	2	218 (78)	15.23	3.301E6	218	14.54	2.339E8
$t^{22} + 2$	21	3	350 (137)	31.91	1.136E4	573	47.26	1.635E11
$t^{23} + 2$	22	7	1076 (378)	219	1.698E12	1503	180	2.790E13
$t^{24} + 2$	18	18	1667 (418)	466	1.490E7	541	64.95	6.289E7
$t^{25} + 2$	19	2	1317 (256)	621	6.415E11	1460	265	4.218E12
$t^{26} + 2$	31	1	2083 (582)	1493	2.093E10	2122	746	2.592E11
$t^{17} + 3$	76	7	658 (466)	36.31	6.535E8	247	7.89	1.519E5
$t^{18} + 3$	93	0	33 (33)	2.38	4.720E5	63	2.91	2.245E7
$t^{19} + 3$	82	6	1373 (729)	167	8.510E9	1584	108	4.569E9
$t^{20} + 3$	74	2	68 (61)	5.69	3.428E6	94	6.90	6.951E6
$t^{21} + 3$	71	1	1530 (630)	427	5.600E12	1501	152	1.256E10
$t^{22} + 3$	72	0	21 (21)	3.81	1.998E11	21	1.84	1.998E11
$t^{14} + 5$	74	10	658 (458)	20.45	8.948E4	506	15.63	9.673E4
$t^{15} + 5$	76	6	829 (443)	52.24	3.502E8	782	24.55	1.092E4
$t^{16} + 5$	70	18	943 (507)	177	2.580E7	2690	236	1.326E10
$t^{17} + 5$	23	9	2269 (382)	668	6.228E7	3513	413	4.307E10
$t^{18} + 5$	73	4	2822 (806)	247	8.956E9	7767	10823	5.559E10
$t^{19} + 5$	82	29	4244 (3006)	27180	*	18049	16522	4.637E20

## 5.2 Beispiele zur Schrankenwahl

In diesem Abschnitt halten wir die experimentellen Ergebnisse der Berechnung von Einheiten mit Bewertungsmatrizen für verschiedene Faktorbasisschranken fest.

### 5.2.1 Rechenzeit und Schrankenwahl

Aus den Beispielen soll eine Empfehlung für die Wahl einer optimalen Schranke hinsichtlich des Rechenaufwands abgeleitet werden, daher betrachten wir drei Arten von Beispielen:

**Bis Spaltentest bestanden** In diesen Tabellen werden die Ergebnisse zur Berechnung eines Systems  $r$  unabhängiger Einheiten von  $\mathfrak{o}_F$  (als Einheiten zu den einfachen Konjugiertenrichtungen mit  $(I_i, J_i) = (\{i\}, \{1, \dots, r_1 + r_2\} \setminus \{i\})$  für  $(1 \leq i \leq r)$ ) mit dem Algorithmus 10 (Aussortieren von Einheiten mit dem Spaltentest aus Algorithmus 11) erfasst.

**Bis Nicht-Torsionseinheit auftritt** In diesen Tabellen werden die Ergebnisse der Berechnung eines Systems von  $r$  Einheiten von  $\mathfrak{o}_F$  (nicht unbedingt unabhängig) erfasst, wobei zu den einfachen Konjugiertenrichtungen  $(I_i, J_i) = (\{i\}, \{1, \dots, r_1 + r_2\} \setminus \{i\})$  für  $(1 \leq i \leq r)$  Konjugiertenfolgeelemente konstruiert und in die Bewertungsmatrix eingespeist werden, bis sich jeweils eine Nullspalte ergibt, deren zugehörige Einheit keine Torsionseinheit ist.

**Mit Algorithmus 13** In diesen Tabellen werden die Ergebnisse der Berechnung eines Systems  $r$  unabhängiger Einheiten von  $\mathfrak{o}_F$  mit dem Algorithmus 13 erfasst.

Die Berechnungen werden jeweils für verschiedene Faktorbasen durchgeführt. Als Faktorbasis wird die Menge von Primidealen ausgewählt, deren Norm unterhalb einer Schranke  $B$  liegt. Dies wurde jeweils mit der MAGMA-Methode `S:=FactorBasis(F, B)` berechnet. Dabei wurden die Schranken variiert. Ermittelt wurden für jede Schranke  $B$ :

- $\#S$  = Faktorbasisgröße
- Zeit = Gesamtrechenzeit in Sekunden
- DE = Anzahl insgesamt berechneter Dirichlet-Elemente
- NSE = Anzahl der Dirichlet-Elemente, die keine  $S$ -Einheiten waren
- SE = Anzahl der Dirichlet-Elemente, die  $S$ -Einheiten waren

Die Rechenzeit und die Anzahl der Elemente verstehen sich jeweils als Gesamtzahlen für alle  $r$  Konjugiertenrichtungen zusammengenommen.

Tabelle 5.13: Bis Spaltentest bestanden wurde

$F = \mathbb{Q}/f(t)\mathbb{Q}$ mit $\log_{10}( D_F ) \approx 16.3$						
Schranke	$f(t) = t^{12} + 2$			$f(t) = t^5 - 1591$		
	# $S$	Zeit	DE (NSE)	# $S$	Zeit	DE (NSE, SE)
10	4	0.37	14 (5)	4	855	3610 (3597, 13)
25	6	0.15	14 (4)	9	68.38	1178 (1156, 22)
40	6	0.14	14 (4)	11	136.97	1331 (1294, 37)
55	12	0.15	14 (2)	14	57.45	910 (879, 31)
70	14	0.16	14 (0)	16	45.72	705 (670, 35)
85	16	0.17	14 (0)	20	70.22	654 (609, 45)
100	20	0.18	14 (0)	22	409.38	1971 (1829, 142)
115	26	0.20	14 (0)	26	441.07	1955 (1788, 167)
130	31	0.20	14 (0)	27	449.51	1955 (1781, 174)
150	33	0.21	14 (0)	35	94.67	581 (509, 72)
200	35	0.22	14 (0)	43	42.34	581 (491, 90)
250	41	0.24	14 (0)	48	58.95	536 (444, 92)
300	63	0.28	14 (0)	54	60.12	536 (439, 97)
350	71	0.30	14 (0)	60	60.49	536 (434, 102)
400	75	0.31	14 (0)	70	61.82	536 (423, 113)
450	79	0.33	14 (0)	86	63.86	536 (409, 127)
500	89	0.36	14 (0)	97	68.96	536 (394, 142)
750	144	0.47	14 (0)	140	79.51	368 (239, 129)
1000	166	0.53	14 (0)	179	81.32	368 (228, 140)
2000	333	1.00	14 (0)	336	56.33	368 (194, 174)
3000	489	1.49	14 (0)	444	68.32	368 (174, 194)

*Zusätzliche Messung zu  $f(t) = t^5 - 1591$ :* Bei  $B = 85$  wurden 5 Einheiten durch den Spaltentest verworfen (2 davon waren tatsächlich Torsionseinheiten). Bei  $B = 90$  wurden 1971 Dirichlet-Elemente berechnet (1837 waren keine  $S$ -Einheiten). Aus den verbleibenden 144  $S$ -Einheiten wurden 94 Einheiten gewonnen, davon wurden 92 durch den Spaltentest verworfen (17 davon waren tatsächlich Torsionseinheiten). Bei  $B = 100$  werden aus den 142  $S$ -Einheiten 100 Nullspalten gewonnen, wovon 98 der entsprechenden Relationenmatrixspalten aufgrund des Spaltentests verworfen werden (18 der zugehörigen Einheiten ergaben Torsionseinheiten).

5.2 Beispiele zur Schrankenwahl

Tabelle 5.14: Bis Nicht-Torsionseinheit auftritt

$F = \mathbb{Q}/f(t)\mathbb{Q}$ mit $\log_{10}( D_F ) \approx 16.3$						
Schranke	$f(t) = t^{12} + 2$			$f(t) = t^5 - 1591$		
	# $S$	Zeit	DE (NSE)	# $S$	Zeit	DE (NSE, SE)
10	4	0.37	14 (5)	4	556.52	3137 (3127, 10)
25	6	0.15	14 (4)	9	27.76	1100 (1079, 21)
40	6	0.14	14 (4)	11	23.54	982 (956, 26)
55	12	0.15	14 (2)	14	29.12	910 (879, 31)
70	14	0.16	14 (0)	16	9.42	690 (657, 33)
85	16	0.17	14 (0)	20	15.65	639 (597, 42)
100	20	0.18	14 (0)	22	9.74	626 (579, 47)
115	26	0.20	14 (0)	26	9.00	603 (548, 55)
130	31	0.20	14 (0)	27	9.09	603 (546, 57)
150	33	0.21	14 (0)	35	12.24	481 (419, 62)
200	35	0.22	14 (0)	43	5.48	379 (315, 64)
250	41	0.24	14 (0)	48	3.62	377 (308, 69)
300	63	0.28	14 (0)	54	4.14	377 (303, 74)
350	71	0.30	14 (0)	60	4.66	377 (300, 77)
400	75	0.31	14 (0)	70	4.75	377 (291, 86)
450	79	0.33	14 (0)	86	5.44	377 (282, 95)
500	89	0.36	14 (0)	97	6.34	362 (261, 101)
750	144	0.47	14 (0)	140	10.53	349 (230, 119)
1000	166	0.53	14 (0)	179	11.92	349 (221, 128)
2000	333	1.00	14 (0)	336	21.79	347 (186, 161)
3000	489	1.49	14 (0)	444	31.34	347 (167, 180)

Tabelle 5.15: feinere Schrittweite: bis Nullspalte auftritt

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$							
$f(t) = t^5 - 1591$				$f(t) = t^5 - 1591$			
Schranke	#S	Zeit	DE (NSE, SE)	Schranke	#S	Zeit	DE (NSE, SE)
20	8	14.98	842 (827, 15)	520	99	7.10	329 (237, 92)
40	11	12.90	659 (638, 21)	540	100	7.16	329 (237, 92)
60	15	11.94	653 (625, 28)	560	107	7.39	329 (236, 93)
80	18	4.86	507 (478, 29)	580	110	7.55	329 (236, 93)
100	22	5.06	507 (466, 41)	600	113	7.75	329 (235, 94)
120	26	5.18	449 (403, 46)	620	117	8.01	329 (234, 95)
140	34	5.90	369 (316, 53)	640	122	8.25	329 (231, 98)
160	36	6.02	369 (313, 56)	660	126	8.64	329 (228, 101)
180	40	6.04	369 (312, 57)	680	128	12.71	326 (222, 104)
200	43	6.21	369 (307, 62)	700	134	12.96	326 (218, 108)
220	43	6.24	369 (307, 62)	720	136	13.10	326 (218, 108)
240	48	3.33	329 (269, 60)	740	139	13.29	326 (218, 108)
260	49	3.37	329 (268, 61)	760	141	13.41	326 (218, 108)
280	52	3.50	329 (267, 62)	780	148	13.57	326 (216, 110)
300	54	3.60	329 (265, 64)	800	150	13.70	326 (216, 110)
320	57	3.75	329 (264, 65)	820	151	13.77	326 (216, 110)
340	58	3.78	329 (264, 65)	840	155	14.09	326 (214, 112)
360	62	4.01	329 (261, 68)	860	160	14.39	326 (213, 113)
380	67	4.45	329 (259, 70)	880	162	14.53	326 (213, 113)
400	70	5.68	329 (255, 74)	900	169	14.97	326 (211, 115)
420	72	5.80	329 (253, 76)	920	171	15.12	326 (211, 115)
440	84	6.13	329 (249, 80)	940	173	15.25	326 (211, 115)
460	87	6.32	329 (247, 82)	960	175	15.45	326 (210, 116)
480	90	6.52	329 (246, 83)	980	177	15.60	326 (209, 117)
500	97	6.93	329 (239, 90)	1000	179	15.74	326 (209, 117)

5.2 Beispiele zur Schrankenwahl

Tabelle 5.16: Bis Spaltentest bestanden

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$ mit $\log_{10}( D_F ) \approx 21.86$						
Schranke	$f(t) = t^{15} + 2$			$f(t) = t^6 - 2738$		
	#S	Zeit	DE (NSE)	#S	Zeit	DE (NSE)
10	3	1.25	34 (15)	8	0.22	30 (16)
25	6	0.82	31 (10)	15	0.13	30 (14)
40	7	0.84	31 (9)	15	0.15	30 (14)
55	12	0.91	31 (6)	19	0.16	30 (12)
70	13	0.95	31 (5)	19	0.16	30 (12)
85	15	0.97	31 (5)	27	0.17	30 (9)
100	16	0.98	31 (5)	35	0.19	30 (7)
115	21	1.06	31 (4)	37	0.19	30 (6)
130	24	1.11	31 (3)	40	0.20	30 (6)
150	26	1.15	31 (3)	42	0.22	30 (6)
200	33	1.36	31 (2)	55	0.24	30 (6)
250	42	1.42	31 (2)	65	0.26	30 (3)
300	58	1.67	31 (1)	79	0.31	30 (2)
350	64	1.76	31 (1)	93	0.34	30 (2)
400	71	1.91	31 (1)	99	0.34	30 (2)
450	85	2.03	31 (1)	117	0.40	30 (1)
500	93	2.14	31 (1)	125	0.42	30 (1)
750	127	2.78	31 (0)	147	0.52	30 (0)
1000	163	3.43	31 (0)	186	0.6	30 (0)
2000	274	5.57	31 (0)	291	0.94	30 (0)
3000	406	8.30	31 (0)	420	1.35	30 (0)

Tabelle 5.17: Bis Spaltentest bestanden

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$ mit $\log_{10}( D_F ) \approx 27,7$						
Schranke	$f(t) = t^{18} + 2$			$f(t) = t^{14} - 4t^6 - t^3 + 8$		
	#S	Zeit	DE (NSE, SE)	#S	Zeit	DE (NSE, SE)
10	3	6.51	76 (55, 21)	6	3259	812 (761, 51)
25	10	3.26	47 (22, 25)	10	993	441 (375, 66)
40	10	3.24	47 (22, 25)	12	230	493 (404, 89)
55	18	2.82	41 (13, 28)	17	1595	402 (298, 104)
70	20	2.86	41 (13, 28)	20	1612	402 (287, 115)
85	22	2.90	41 (13, 28)	28	5756	436 (271, 165)
100	24	2.94	41 (13, 28)	30	5771	436 (263, 173)
115	28	3.04	41 (13, 28)	34	5306	436 (253, 183)
130	30	3.02	41 (13, 28)	35	5312	436 (250, 186)
150	34	3.13	41 (11, 30)	37	5309	436 (248, 188)
200	36	3.24	41 (9, 32)	50	979	436 (217, 219)
250	40	3.34	41 (9, 32)	57	990	436 (203, 233)
300	60	3.66	41 (4, 37)	73	1011	436 (180, 256)
350	62	3.72	41 (4, 37)	90	399	422 (158, 264)
400	64	3.77	41 (4, 37)	103	280	402 (142, 260)
450	72	3.98	41 (4, 37)	115	294	402 (133, 269)
500	88	4.20	41 (4, 37)	120	300	402 (131, 271)
750	127	4.99	41 (4, 37)	161	358	402 (104, 298)
1000	153	5.81	41 (2, 39)	194	402	402 (93, 309)
2000	301	8.89	41 (0, 41)	329	604	402 (71, 331)
3000	455	12.02	41 (0, 41)	471	799	402 (57, 345)

5.2 Beispiele zur Schrankenwahl

Tabelle 5.18: feinere Schrittweite: Bis Spaltentest bestanden

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$							
$f(t) = t^{14} - 4t^6 - t^3 + 8$				$f(t) = t^{14} - 4t^6 - t^3 + 8$			
Schranke	#S	Zeit	DE (NSE, SE)	Schranke	#S	Zeit	DE (NSE, SE)
400	103	285	402 (142, 260)	2300	377	678.75	402 (69, 333)
450	115	302	402 (133, 269)	2350	382	684	402 (69, 333)
500	120	309	402 (131, 271)	2400	391	699	402 (69, 333)
550	129	319	402 (126, 276)	2450	398	709	402 (69, 333)
600	137	334	402 (118, 284)	2500	402	712	402 (68, 334)
650	146	345	402 (112, 290)	2550	404	716	402 (68, 334)
700	152	352	402 (108, 294)	2600	405	718	402 (68, 334)
750	161	365	402 (104, 298)	2650	409	723	402 (67, 335)
800	164	369	402 (104, 298)	2700	420	748	402 (63, 339)
850	176	384	402 (100, 302)	2750	431	761	402 (61, 341)
900	181	393	402 (98, 304)	2800	442	776	402 (60, 342)
950	189	399	402 (97, 305)	2850	450	788	402 (59, 343)
1000	194	408	402 (93, 309)	2900	455	795	402 (58, 344)
1050	204	422	402 (92, 310)	2950	459	801	402 (58, 344)
1100	212	432	402 (91, 311)	2850	450	788	402 (59, 343)
1150	217	448	402 (90, 312)	2900	455	795	402 (58, 344)
1200	225	462	402 (86, 316)	2950	459	801	402 (58, 344)
1250	234	470	402 (85, 317)	3000	471	818	402 (57, 345)
1300	240	479	402 (84, 318)	3050	479	831	402 (56, 346)
1350	244	486	402 (84, 318)	3100	483	831	402 (56, 346)
1400	250	495	402 (84, 318)	3150	484	839	402 (55, 347)
1450	251	497	402 (84, 318)	3200	489	845	402 (55, 347)
1500	260	516	402 (82, 320)	3250	493	852	402 (55, 347)
1550	264	523	402 (81, 321)	3300	498	854	402 (54, 348)
1600	274	52	402 (80, 322)	3350	502	868	402 (54, 348)
1650	279	537	402 (80, 322)	3400	508	879	402 (54, 348)
1700	290	557	402 (77, 325)	3450	512	883	402 (54, 348)
1750	294	562	402 (77, 325)	3500	518	896	402 (53, 349)
1800	301	572	402 (76, 326)	3550	524	906	402 (53, 349)
1850	308	579	402 (75, 327)	3600	534	916	402 (53, 349)
1900	314	588	402 (75, 327)	3650	544	931	402 (52, 350)
1950	322	602	402 (73, 329)	3700	551	942	402 (52, 350)
2000	329	617	402 (71, 331)	3750	556	946	402 (52, 350)
2050	335	627	402 (70, 332)	3800	562	961	402 (51, 351)
2100	345	636	402 (70, 332)	3850	567	971	402 (50, 352)
2150	358	655	402 (70, 332)	3900	575	986	402 (49, 353)
2200	359	655	402 (70, 332)	3950	590	1009	402 (48, 354)
2250	368	668	402 (70, 332)	4000	590	1005	402 (48, 354)

Tabelle 5.19: Bis Spaltentest bestanden

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$ mit $\log_{10}( D_F ) \approx 31.7$						
Schranke	$f(t) = t^{20} + 2$			$f(t) = t^{13} + 27$		
	#S	Zeit	DE (NSE, SE)	#S	Zeit	DE (NSE, SE)
10	4	36.04	189 (154, 35)	4	1.28	39 (28, 11)
25	6	35.33	185 (140, 45)	9	0.81	31 (14, 16)
40	6	35.24	185 (140, 45)	12	0.88	31 (11, 20)
55	10	36.59	185 (131, 54)	15	0.92	31 (9, 22)
70	14	38.49	185 (118, 67)	18	1.00	31 (8, 23)
85	24	30.33	159 (87, 72)	21	1.09	31 (6, 25)
100	28	31.30	159 (85, 74)	23	1.12	31 (5, 26)
115	34	32.63	159 (80, 79)	28	1.22	31 (5, 26)
130	34	32.61	159 (80, 79)	29	1.24	31 (5, 26)
150	36	33.13	159 (80, 79)	32	1.28	31 (5, 26)
200	40	34.15	159 (76, 83)	42	1.53	31 (4, 27)
250	46	35.72	159 (71, 88)	49	1.72	31 (3, 28)
300	64	38.72	157 (59, 98)	58	1.91	31 (3, 28)
350	72	40.69	157 (57, 100)	65	2.09	31 (3, 28)
400	87	42.80	157 (53, 104)	73	2.24	31 (3, 28)
450	91	45.64	157 (49, 108)	81	2.40	31 (3, 28)
500	95	47.68	157 (48, 109)	89	2.58	31 (3, 28)
750	138	60.33	157 (38, 119)	138	3.56	31 (2, 29)
1000	164	66.99	157 (34, 123)	171	4.62	31 (0, 31)
2000	283	106.84	157 (20, 137)	321	8.10	31 (0, 31)
3000	413	146.15	157 (15, 142)	437	11.46	31 (0, 31)

5.2 Beispiele zur Schrankenwahl

Tabelle 5.20: Bis Nicht-Torsionseinheit auftritt

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$ mit $\log_{10}( D_F ) \approx 31.7$						
Schranke	$f(t) = t^{20} + 2$			$f(t) = t^{13} + 27$		
	#S	Zeit	DE (NSE, SE)	#S	Zeit	DE (NSE, SE)
10	4	24.15	148 (120, 28)	4	1.75	39 (28, 11)
25	6	21.55	144 (107, 37)	9	0.76	29 (13, 16)
40	6	21.54	144 (107, 37)	12	0.81	29 (10, 19)
55	10	22.04	144, 102, 42)	15	0.86	29 (9, 20)
70	14	22.74	144 (94, 50)	18	0.91	29 (8, 21)
85	24	17.03	122 (67, 55)	21	0.99	29 (6, 23)
100	28	17.27	122 (65, 57)	23	1.03	29 (5, 24)
115	34	17.75	122 (61, 61)	28	1.12	29 (5, 24)
130	34	17.74	122 (61, 61)	29	1.12	29 (5, 24)
150	36	17.93	122 (61, 61)	32	1.19	29 (5, 24)
200	40	18.89	122 (59, 63)	42	1.40	29 (4, 25)
250	46	19.95	122 (54, 68)	49	1.57	29 (3, 26)
300	64	21.3	122 (47, 75)	58	1.77	29 (3, 26)
350	72	22.12	122 (45, 77)	65	1.97	29 (3, 26)
400	87	19.3	113 (38, 75)	73	2.08	29 (3, 26)
450	91	19.84	113 (36, 77)	81	2.27	29 (3, 26)
500	95	20.52	113 (36, 77)	89	2.40	29 (3, 26)
750	138	24.48	113 (28, 85)	138	3.34	29 (2, 27)
1000	164	27.07	113 (24, 89)	171	4.38	29 (0, 29)
2000	283	39.78	113 (13, 100)	321	7.66	29 (0, 29)
3000	413	53.02	113 (9, 104)	437	10.81	29 (0, 29)

Tabelle 5.21: Bis Spaltentest bestanden

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$ mit $\log_{10}( D_F ) \approx 37.9$						
Schranke	$t^{14} + 3t^{10} + 48$			$t^{23} + 2$		
	# $S$	Zeit	DE (NSE, SE)	# $S$	Zeit	DE (NSE, SE)
10	3	963.61	1098 (1078, 20)	4	1730.17	729 (693, 36)
25	15	185.09	479 (415, 64)	9	886.14	597 (510, 87)
40	15	185.35	479 (415, 64)	12	718.21	523 (425, 98)
55	29	409.35	478 (355, 123)	15	934.58	499 (393, 106)
70	29	409.69	478 (355, 123)	18	954.96	499 (379, 120)
85	35	893.62	474 (324, 150)	22	1005.69	499 (365, 134)
100	37	174.38	365 (238, 127)	24	957.06	467 (335, 132)
115	39	184.17	365 (233, 132)	29	1005.69	450 (300, 150)
130	44	185.43	365 (220, 145)	30	1249.12	445 (291, 154)
150	46	186.44	365 (214, 151)	33	1300.97	445 (282, 163)
200	56	221.05	365 (196, 169)	44	1446.51	445 (260, 185)
250	60	222.91	364 (191, 173)	51	1221.23	423 (234, 189)
300	74	230.26	364 (174,190)	59	1312.45	423 (228, 195)
350	82	235.91	364 (168, 196)	67	1431.08	422 (215, 207)
400	95	242.60	364 (158, 206)	75	1539.54	422 (209, 213)
450	111	252.65	364 (144, 220)	84	1673.82	422 (202, 220)
500	121	259.85	364 (135, 229)	91	1765.39	422 (197, 225)
750	165	295.59	364 (109, 255)	126	2274.47	422 (182, 240)
1000	181	308.58	364 (107, 257)	160	2674.12	415 (163, 252)
2000	325	411.81	364 (86, 278)	287	5055.02	415 (123, 292)
3000	434	504.98	364 (79, 285)	411	7184.28	415 (106, 309)

5.2 Beispiele zur Schrankenwahl

Tabelle 5.22: feinere Schrittweite: Bis Spaltentest bestanden

$F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$							
$f(t) = t^{14} + 3t^{10} + 48$				$f(t) = t^{14} + 3t^{10} + 48$			
Schranke	#S	Zeit	DE (NSE, SE)	Schranke	#S	Zeit	DE (NSE, SE)
20	11	109.70	479 (433, 46)	520	123	261.48	364 (133, 231)
40	15	185.35	479 (415, 64)	540	127	264.79	364 (130, 234)
60	29	410.22	478 (355, 123)	560	129	266.40	364 (129, 235)
80	33	351.28	478 (339, 139)	580	135	269.34	364 (126, 238)
100	37	174.98	365 (238, 127)	600	141	273.92	364 (124, 240)
120	39	184.60	365 (233, 132)	620	149	279.91	364 (118, 246)
140	46	186.69	365 (214, 151)	640	151	281.46	364 (118, 246)
160	46	186.64	365 (214, 151)	660	159	289.61	364 (111, 253)
180	52	217.83	365 (203, 162)	680	161	291.59	364 (110, 254)
200	56	220.63	365 (196, 169)	700	163	293.15	364 (110, 254)
220	56	220.63	365 (196, 169)	720	165	294.71	364 (109, 255)
240	58	221.66	365 (195, 170)	740	165	294.69	364 (109, 255)
260	64	225.78	364 (184, 180)	760	165	295.18	364 (109, 255)
280	70	229.11	364 (178, 186)	780	167	297.49	364 (108, 256)
300	74	230.09	364 (174, 190)	800	169	298.90	364 (108, 256)
320	80	234.40	364 (168, 196)	820	169	299.07	364 (108, 256)
340	80	234.19	364 (168, 196)	840	169	299.20	364 (108, 256)
360	86	238.40	364 (163, 201)	860	173	302.35	364 (107, 257)
380	91	240.47	364 (161, 203)	880	173	302.42	364 (107, 257)
400	95	241.97	364 (158, 206)	900	173	302.25	364 (107, 257)
420	101	244.97	364 (155, 209)	920	177	305.32	364 (107, 257)
440	109	251.43	364 (145, 219)	940	177	305.37	364 (107, 257)
460	115	254.07	364 (140, 224)	960	177	305.38	364 (107, 257)
480	119	256.57	364 (137, 227)	980	179	306.79	364 (107, 257)
500	121	259.74	364 (135, 229)	1000	181	308.36	364 (107, 257)

Tabelle 5.23: Mit Algorithmus 13

Zahlkörper $F_i = \mathbb{Q}/f_i(t)\mathbb{Q}$ , $D_{F_1} \approx -5.19 \cdot 10^{29}$ , $D_{F_2} \approx 5.5 \cdot 10^{31}$ , $D_{F_3} \approx 6.13 \cdot 10^{33}$									
Schranke	$f_1(t) = t^{19} + 2$			$f_2(t) = t^{20} + 2$			$f_3(t) = t^{21} + 2$		
	#S	Zeit	DE (NSE)	#S	Zeit	DE (NSE)	#S	Zeit	DE (NSE)
10	4	254.	211 (177)	4	44.9	247 (220)	3	50.6	273 (248)
25	9	12.6	169 (109)	6	22.1	244 (207)	7	63.9	271 (231)
40	12	11.2	151 (83)	6	22.1	244 (207)	10	36.5	258 (205)
55	16	11.9	151 (74)	10	19.5	225 (175)	13	36.0	251 (183)
70	19	12.5	151 (66)	14	19.9	225 (166)	14	35.6	251 (180)
85	23	13.4	151 (59)	24	18.8	210 (132)	15	36.0	251 (176)
100	25	13.8	151 (58)	28	19.2	210 (119)	16	36.1	251 (175)
115	30	14.9	151 (53)	34	18.9	204 (106)	21	37.8	251 (159)
130	31	15.0	151 (53)	34	18.9	204 (106)	22	37.7	251 (158)
150	35	16.1	151 (52)	36	19.1	204 (106)	25	38.6	251 (153)
200	45	18.2	151 (47)	40	19.7	204 (104)	32	40.9	251 (144)
250	51	19.7	151 (42)	46	18.7	179 (77)	40	39.1	240 (128)
300	60	22.1	151 (37)	64	20.0	179 (70)	52	41.8	240 (120)
350	74	24.1	151 (34)	72	20.8	179 (66)	59	44.0	240 (112)
400	82	26.1	151 (28)	87	17.2	162 (43)	66	46.0	240 (106)
450	90	28.0	151 (25)	91	17.6	162 (41)	76	49.1	240 (99)
500	97	30.0	151 (23)	95	18.1	162 (41)	85	52.2	240 (94)
750	132	39.0	151 (18)	138	21.7	162 (28)	120	63.4	240 (81)
1000	167	48.4	151 (14)	164	23.9	162 (25)	152	74.5	240 (74)
2000	329	81.2	151 (12)	283	34.3	162 (20)	285	122.	240 (55)
3000	448	113.	151 (10)	413	45.6	162 (16)	444	181.	240 (40)

5.2 Beispiele zur Schrankenwahl

Tabelle 5.24: Bis Spaltentest bestanden

Zahlkörper $F_i = \mathbb{Q}/f_i(t)\mathbb{Q}$ , $D_{F_1} \approx -1.22 \cdot 10^{35}$ , $D_{F_2} \approx -5.81 \cdot 10^{28}$ , $D_{F_3} \approx 1.49 \cdot 10^{42}$									
Schranke	$f_1(t) = t^{20} - 3$			$f_2(t) = t^{22} + 3$			$f_3(t) = t^{25} + 2$		
	#S	Zeit	DE (NSE, SE)	#S	Zeit	DE (SE)	#S	Zeit	DE (NSE, SE)
10	2	791	528 (506, 22)	4	6.31	33 (23)	4	6718	1472 (1414, 58)
25	9	241	388 (325, 63)	9	5.06	30 (27)	8	5530	1274 (1172, 102)
40	9	244	388 (325, 63)	13	5.16	30 (27)	10	6048	1292 (1170, 122)
55	13	260	386 (303, 83)	15	5.25	30 (27)	13	6159	1277 (1133, 144)
70	15	270	386 (299, 87)	17	5.30	30 (27)	15	4616	1178 (1035, 143)
85	17	276	386 (295, 91)	21	5.44	30 (27)	19	4216	1129 (961, 168)
100	17	275	386 (295, 91)	23	5.51	30 (27)	21	4135	1089 (914, 175)
115	23	281	386 (291, 95)	27	5.65	30 (27)	25	4468	1089 (898, 191)
130	23	282	386 (291, 95)	31	5.76	30 (27)	26	4512	1089 (897, 192)
150	23	282	386 (291, 95)	33	5.83	30 (27)	29	4632	1089 (887, 202)
200	31	305	386 (287, 99)	43	6.22	30 (28)	37	5080	1088 (821, 267)
300	45	389	386 (266, 120)	58	6.77	30 (28)	53	5793	1088 (800, 288)
350	51	402	386 (262, 124)	66	7.07	30 (28)	59	5569	1042 (752, 290)
400	65	459	386 (242, 144)	72	7.31	30 (28)	69	6090	1042 (734, 308)
450	83	492	386 (233, 153)	80	7.64	30 (28)	80	6842	1042 (702, 340)
500	97	529	386 (218, 168)	86	7.86	30 (28)	86	7211	1042 (696, 346)
750	133	685	386 (201, 185)	118	9.24	30 (30)	124	8916	975 (579, 396)
1000	161	843	386 (182, 204)	149	10.49	30 (30)	163	11338	975 (536, 439)
2000	285	1569	386 (143, 243)	290	15.80	30 (30)	275	19021	943 (445, 498)
3000	420	2182	386 (127, 259)	398	20.45	30 (30)	423	24992	943 (402, 541)

Tabelle 5.25: Mit Algorithmus 13

Zahlkörper $F_i = \mathbb{Q}/f_i(t)\mathbb{Q}$ , $D_{F_1} \approx 5.42 \cdot 10^{25}$ , $D_{F_2} \approx 7.16 \cdot 10^{35}$ , $D_{F_3} \approx -6.07 \cdot 10^{25}$									
Schranke	$f_1(t) = t^{17} + t^6 - 3t^2 - 2$			$f_2(t) = t^{22} - 2$			$f_3(t) = t^{16} - 4t^5 + 2$		
	#S	Zeit	DE (NSE)	#S	Zeit	DE (NSE)	#S	Zeit	DE (NSE)
10	4	7.32	52 (31)	4	66.6	358 (327)	4	15.3	158 (128)
25	7	2.68	52 (26)	7	63.1	331 (289)	9	7.00	121 (73)
40	10	2.81	52 (20)	9	46.5	318 (270)	13	7.16	126 (65)
55	14	3.00	52 (15)	13	40.9	278 (219)	16	7.44	126 (59)
70	14	3.01	52 (15)	13	40.9	278 (219)	18	7.69	126 (56)
85	14	3.02	52 (15)	19	38.7	267 (195)	19	7.92	126 (53)
100	16	3.10	52 (14)	21	39.0	267 (193)	20	8.08	126 (52)
115	20	3.20	52 (13)	25	39.3	266 (184)	22	8.58	126 (46)
130	21	3.26	52 (13)	28	39.8	266 (181)	24	8.80	126 (41)
150	24	3.47	52 (11)	30	40.1	266 (179)	28	9.20	126 (40)
200	35	3.82	52 (9)	39	41.9	266 (170)	42	10.7	126 (37)
250	40	4.05	52 (9)	47	43.6	266 (159)	46	11.1	126 (34)
300	48	4.47	52 (6)	55	45.5	266 (153)	56	12.4	126 (27)
350	55	4.83	52 (4)	61	47.2	266 (150)	65	13.2	126 (25)
400	63	5.16	52 (4)	68	48.8	266 (148)	70	13.8	126 (25)
450	72	5.50	52 (4)	80	51.1	266 (143)	76	14.6	126 (23)
500	86	5.96	52 (3)	86	52.3	266 (141)	83	15.6	126 (22)
750	131	7.45	52 (1)	114	56.8	259 (121)	127	19.7	126 (15)
1000	160	8.83	52 (1)	149	66.8	259 (106)	164	24.2	126 (11)
2000	303	15.1	52 (0)	305	106.	257 (77)	316	43.0	126 (6)
3000	444	21.4	52 (0)	420	144.	257 (64)	457	60.6	126 (4)

## 5.2 Beispiele zur Schrankenwahl

Tabelle 5.26: Bis Spaltentest bestanden

Zahlkörper $F_i = \mathbb{Q}/f_i(t)\mathbb{Q}$ , $D_{F_1} \approx -1.76 \cdot 10^{22}$ , $D_{F_2} \approx -2.65 \cdot 10^{26}$ , $D_{F_3} \approx -1.0 \cdot 10^{25}$									
$B$	$f_1(t) = t^{12} - 7$			$f_2(t) = t^{16} - 3$			$f_3(t) = t^{18} + 4$		
	#S	Zeit	DE (NSE, SE)	#S	Zeit	DE (NSE, SE)	#S	Zeit	DE (NSE, SE)
10	6	3.88	93 (64, 29)	2	13.79	139 (123, 16)	4	2.12	29 (10, 19)
25	12	5.26	107 (60, 47)	10	14.37	131 (86, 45)	8	1.75	29 (9, 20)
40	16	5.50	107 (52, 55)	10	14.83	131 (86, 45)	14	1.75	28 (5, 23)
70	20	6.11	107 (46, 61)	14	11.82	117 (66, 51)	14	1.74	28 (5, 23)
85	22	6.35	107 (44, 63)	18	12.84	117 (57, 60)	14	1.77	28 (5, 23)
100	22	6.34	107 (44, 63)	18	13.06	117 (57, 60)	16	1.79	28 (3, 25)
115	26	6.57	107 (44, 63)	24	13.72	117 (55, 62)	20	1.86	28 (3, 25)
130	32	6.77	107 (44, 63)	27	13.70	117 (51, 66)	23	1.86	28 (3, 25)
150	34	7.03	107 (42, 65)	29	14.77	117 (47, 70)	27	1.93	28 (3, 25)
200	36	7.45	107 (40, 67)	41	17.20	117 (36, 81)	37	2.05	28 (2, 26)
250	44	8.56	107 (32, 75)	49	18.90	117 (28, 89)	45	2.12	28 (2, 26)
300	46	8.87	107 (28, 79)	57	20.44	117 (27, 90)	67	2.30	28 (1, 27)
350	48	9.15	107 (28, 79)	69	22.39	117 (20, 97)	69	2.32	28 (1, 27)
400	63	9.99	107 (28, 79)	73	24.52	117 (15, 102)	91	2.44	28 (1, 27)
450	75	10.84	107 (28, 79)	99	28.01	117 (12, 105)	95	2.52	28 (1, 27)
500	79	11.43	107 (28, 79)	105	29.75	117 (12, 105)	103	2.57	28 (1, 27)
750	112	16.00	107 ( 18, 89)	150	38.03	117 (8, 109)	138	3.04	28 (1, 27)
1000	138	18.35	107 (18, 89)	198	45.28	117 (8, 109)	171	3.56	28 (0, 28)
2000	242	29.12	107 (14, 93)	318	73.61	117 (4, 113)	326	5.34	28 (0, 28)
3000	369	43.54	107 (10, 97)	419	105.14	117 (1, 116)	455	7.16	28 (0, 28)

*Zusätzliche Messung für  $f_1(t) = t^{12} - 7$ : Bei  $B = 10$  werden 12 Nullspalten gefunden. Von den entsprechenden Relationenmatrixspalten werden 6 durch den Spaltentest verworfen. Bei  $B = 25$  werden 18 Nullspalten gefunden, aber 12 aufgrund des Spaltentests verworfen.*

### 5.2.2 Schrankenwahl und Index

Wir berechnen für einige Zahlkörper  $F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$  mit Algorithmus 10 zu verschiedenen Schranken  $r$  unabhängige Einheiten  $\varepsilon_1, \dots, \varepsilon_r$  der Maximalordnung  $\mathfrak{o}_F$  und betrachten den Index  $(U(\mathfrak{o}_F) : \langle \eta, \varepsilon_1, \dots, \varepsilon_r \rangle) = \frac{|\det(L(\varepsilon_1), \dots, L(\varepsilon_r))|}{\text{Reg}_{\mathfrak{o}_F}}$  der berechneten Einheiten (wobei  $\eta \in TU(\mathfrak{o}_F)$ ) in der Einheitengruppe  $U(\mathfrak{o}_F)$ . Die Einheitengruppe  $U(\mathfrak{o}_F)$  ist bekannt, so dass wir nicht mit einer unteren Abschätzung des Regulators  $\text{Reg}_{\mathfrak{o}_F}$  arbeiten. Wir erfassen 4 signifikante Stellen und den Exponenten der Exponentialdarstellung des Index.

Tabelle 5.27: Index in Abhängigkeit von der Schranke

	$t^{18} + 2$	$t^{13} + 27$	$t^{17} - 3$	$t^{21} + 2$	$t^{19} + 2$	$t^{10} - 37$	$t^{16} + 15$
10	3.37E12	1.97E7	8.51E20	3.442E22	3.576E19	1.060E11	8.67E11
25	3.32E12	9.13E6	6.079E20	2.609E21	1.25E19	6.255E11	8.67E11
40	3.32E12	9.13E6	7.522E20	7.085E21	5.564E18	6.255E11	8.67E11
55	9.08E11	9.13E6	1.363E19	7.085E21	5.564E18	7.698E10	8.67E11
70	9.08E11	9.13E6	9.951E18	7.085E21	5.564E18	7.698E10	8.67E11
85	9.08E11	9.13E6	9.951E18	7.085E21	1.367E18	7.698E10	8.67E11
100	9.08E11	9.13E6	9.951E18	7.085E21	1.367E18	7.698E10	8.67E11
200	9.08E11	9.13E6	6.637E17	7.085E21	2.87E17	1.75E11	6.902E11
300	9.08E11	9.13E6	6.637E17	7.085E21	2.87E17	1.75E11	6.902E11
400	9.08E11	9.13E6	4.542E17	7.085E21	2.87E17	1.54E11	6.902E11
500	9.08E11	9.13E6	4.542E17	7.085E21	2.87E17	1.54E11	6.902E11
1000	9.08E11	9.13E6	4.542E17	7.085E21	2.87E17	3.78E11	6.902E11
2000	9.08E11	9.13E6	4.542E17	7.085E21	2.87E17	3.78E11	6.902E11
3000	9.08E11	9.13E6	4.542E17	7.085E21	2.87E17	3.78E11	6.902E11

Wir betrachten hinsichtlich des Unterschieds zwischen Algorithmus 10 und 13 für das Beispiel  $F \cong \mathbb{Q}[t]/f(t)\mathbb{Q}[t]$  mit  $f(t) = t^{20} + 2$  einige Werte.

Schranke	10	25	55	85	200	1000
Algorithmus 10	4.824E19	1.914E20	1.914E20	5.045E20	5.045E20	2.37E20
Algorithmus 13	2.095E17	2.149E17	1.767E16	4.978E15	7.617E16	1.336E14

# Literaturverzeichnis

- [Abe94] ABEL, C. S.: *Ein Algorithmus zur Berechnung der Klassenzahl und des Regulators reellquadratischer Ordnungen*, Universität des Saarlandes, PhD Thesis, 1994
- [BCP97] BOSMA ; CANNON ; PLAYOUST: The Magma algebra system. I. The user language. In: *J. Symbolic Computation* 24(3-4) (1997), S. 235–265. – <http://magma.maths.usyd.edu.au/magma/>
- [BP89] BUCHMANN, J. ; PETHÖ, A.: Computation of Independent Units in Number Fields by Dirichlet’s Method. In: *MC* 52 (1989), S. 149–159
- [Flo67] FLOYD, R.W.: Non-deterministic Algorithms. In: *J. Ass. f. Comp. Machinery* 14 (1967), S. 636–644
- [FP85] FINCKE, U. ; POHST, M. E.: Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis. In: *Mathematics of Computation* 44 (1985), Nr. 170, S. 463–471
- [FP06] FIEKER, C. ; POHST, M. E.: Dependency of units in number fields. In: *Mathematics of Computation* 75 (2006), S. 1507–1518
- [Hes96] HESS, F.: *Zur Klassengruppenberechnung in algebraischen Zahlkörpern*, Technische Universität Berlin, Diplomarbeit, 1996
- [KG06] KANT-GROUP: KASH Introduction to KASH3. (2006). – <http://www.math.tu-berlin.de/~kant/KASH/pdf/kash3intro.pdf>
- [Poh93] POHST, M. E.: *Computational algebraic number theory*. Birkhäuser Verlag, 1993 (DMV-Seminar 21)
- [PZ89] POHST, M. E. ; ZASSENHAUS, H.: *Algorithmic Algebraic Number Theory*. Cambridge University Press, 1989
- [SE93] SCHNORR, C. P. ; EUCHNER, M.: Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. In: *Math. Programming*, 1993, S. 181–191
- [Wil93] WILDANGER, K.: *Über Grundeinheitenberechnung in algebraischen Zahlkörpern*, Heinrich-Heine Universität Düsseldorf, Diplomarbeit, 1993