Zur Klassengruppenberechnung in algebraischen Zahlkörpern

Diplomarbeit
von
Florian Heß

Angefertigt am Fachbereich Mathematik
der Technischen Universität Berlin
Berlin 1996

Inhaltsverzeichnis

1 Einleitung **3**

2 Grundlagen **5**
- 2.1 Moduln 5
- 2.2 Algebraische Zahlkörper 8
- 2.3 Gitter 10
- 2.4 Einheiten 12
- 2.5 Klassengruppe 14

3 Das Verfahren **19**
- 3.1 Klassengruppenberechnung als S-Einheitenberechnung 19
- 3.2 S-Einheitengitter 21
- 3.3 Abbruchbedingungen 25
- 3.4 Konvergenzverhalten des Eulerprodukts 28
- 3.5 Berechnung der Klassengruppenstruktur 37
- 3.6 Verifikation der S-Einheiten 38
- 3.7 Zusammenfassung 44

4 Faktorbasis und Relationensuche **45**
- 4.1 Grundideen der Relationensuche 45
- 4.2 Smoothness-Eigenschaften 47
- 4.3 Die Faktorbasis 53
  - 4.3.1 Reduktion einer Faktorbasis 54
  - 4.3.2 Nachweis der Vollständigkeit 56
  - 4.3.3 Vorgehensweise in der Praxis 60
- 4.4 Relationensuche 61
  - 4.4.1 Test auf S-Einheit 61
  - 4.4.2 Schnelle Relationen 62
  - 4.4.3 Gute Relationen 64
  - 4.4.4 Gezielte Relationen 65
  - 4.4.5 Kombination der verschiedenen Strategien 66
  - 4.4.6 Relationen aus dem Number Field Sieve 68
- 4.5 Ausnahmeprimideale 69

4.5.1 Verbindung zur Methode der reduzierten Ideale 73

5 Anwendungen **75**

5.1 Die Klasse eines Ideals 75

5.2 S-Einheitenberechnung 78

6 Beispiele **79**

Symbolverzeichnis **85**

Literaturverzeichnis **87**

Kapitel 1

Einleitung

Die Klassengruppe ist eine der wichtigen Invarianten eines algebraischen Zahlkörpers K. Sie ist ein Ausdruck dafür, wie weit der Ring der ganzalgebraischen Zahlen von K, der ein Dedekindring ist, von einem faktoriellen Ring oder auch einem Hauptidealring entfernt ist. Ihre Kenntnis hilft bei vielen Fragestellungen weiter, beispielsweise bei der Faktorisierung großer ganzer Zahlen oder bei der Frage nach der Lösbarkeit nicht-linearer diophantischer Gleichungen. Allerdings ist über die Klassengruppe im allgemeinen, außer daß sie abelsch und endlich ist, nur wenig bekannt. Eine der Aufgaben der konstruktiven algebraischen Zahlentheorie besteht daher in der algorithmischen Bestimmung der Klassengruppe. Hierzu wurden Verfahren zuerst von Pohst und Zassenhaus [17] und später durch Buchmann [3] ausgehend von Hafner und McCurley [7] entwickelt. Verbesserungen stammen von v. Schmettow [21] und von Scheid [20]. Diese Verfahren basieren alle auf der Relationenmethode. Die Idee hierbei ist, daß jede (abelsche) Gruppe als Faktorgruppe einer freien (abelschen) Gruppe nach einem von sogenannten Relationen erzeugten Normalteiler dargestellt werden kann. Bei diesem Vorgehen ergeben sich allgemein folgende Fragen: Welche und wieviele Erzeuger werden für die freie (abelsche) Gruppe benötigt? Wie findet man die Relationen? Wann sind genügend Relationen gefunden worden? Im Kontext einer Klassengruppenberechnung muß zur Beantwortung der ersten Frage eine geeignete endliche Menge von Primidealen, genannt Faktorbasis, angegeben werden. Diese Primideale erzeugen mit der Idealmultiplikation eine freie abelsche Gruppe, deren Hauptideale die zu findenden Relationen darstellen.

In dieser Arbeit wird ein kombiniertes Verfahren zur Klassengruppenberechnung basierend auf der Relationenmethode vorgestellt, in welches teilweise verbesserte Techniken der bekannten Verfahren unter Berücksichtigung ihrer Effizienz aus praktischer Sicht eingehen. Zusätzlich wurden auch neue Methoden integriert. Die Schwierigkeit einer Klassengruppenberechnung kann in erster Linie an der Größe des Körpergrads und der Größe der Körperdiskriminante im Verhältnis zum Körpergrad abgelesen werden. Durch das hier dargestellte kombinierte Verfahren konnten (mit Hilfe einer Approximation des Eulerprodukts) Klassengruppen eines Körper vom Grad 4 mit 36-stelliger Diskriminante und eines Körpers vom Grad 46 mit 76-stelliger Diskriminante in relativ kurzer Zeit berechnet werden.

In Kapitel 2 werden die grundlegenden Definitionen und Sätze zusammengestellt, die für die folgenden Kapitel benötigt werden. Kapitel 3 beschreibt die zugrundeliegenden Ideen des Verfahrens. Alle Schritte außer der Berechnung der Faktorbasis und der Relationensuche werden genau erläutert. Die gleichzeitige Berechnung der Klassengruppe und der Einheitengruppe wird als Berechnung der S-Einheiten von K aufgefaßt. Dies ermöglicht den Einsatz des Eulerprodukts, zu dem auch Konvergenzbetrachtungen angestellt werden. Kapitel 4 ist ganz der Berechnung einer Faktorbasis und der Relationensuche gewidmet. Durch Betrachtung von Smoothnesswahrscheinlichkeiten wird gezeigt, wie die Relationensuche durch die Wahl der Faktorbasis beeinflußt wird. Es wird beschrieben, wie eine Faktorbasis reduziert und wie ihre Vollständigkeit algorithmisch bewiesen werden kann. Danach werden verschiedene Methoden der Relationensuche diskutiert. Zum Schluß wird die Methode der Ausnahmeprimideale beschrieben, mit der die zwei wesentlichen Arten der Relationensuche in Verbindung gesetzt werden können. Kapitel 5 zeigt zwei Anwendungsmöglichkeiten der während einer Klassengruppenberechnung erhaltenen Daten. Es wird erläutert, wie die Klasse eines Ideals und wie beliebige S-Einheiten bestimmt werden können. Im Kapitel 6 wird das Verhalten des Klassengruppenverfahrens an einigen nichttrivialen Beispielen demonstriert.

Kapitel 2

Grundlagen

In den folgenden Abschnitten dieses Kapitels werden einige grundlegende Begriffe aus der algebraischen Zahlentheorie, auf die wir uns in dieser Arbeit meist stillschweigend beziehen wollen, kurz aufgelistet. Ausführlichere Darstellungen mit Beweisen können beispielsweise in [13, 16] gefunden werden.

2.1 Moduln

Wir wollen zuerst kurz auf Moduln und zwei damit in Verbindung stehende Matrixnormalformen eingehen. Mehr über Moduln kann in [11] nachgelesen werden.

Unter einem $R-$Modul versteht man einen kommutativen Ring $(R, +, \cdot)$ mit 1 zusammen mit einer abelschen Gruppe $(M, +)$ und einer äußeren Verknüpfung $\cdot : R \times M \longrightarrow M$, welche R und M multiplikativ verbindet: Für beliebige $r, r_1, r_2 \in R$ und $m, m_1, m_2 \in M$ gelten die Gleichungen

$$\begin{aligned} (r_1 r_2) \cdot m &= r_1(r_2 \cdot m), \\ (r_1 + r_2) \cdot m &= r_1 \cdot m + r_2 \cdot m, \\ r \cdot (m_1 + m_2) &= r \cdot m_1 + r \cdot m_2, \\ 1 \cdot m &= m. \end{aligned}$$

Ähnlich wie in R wird das Symbol $\cdot$ meist fortgelassen.

Ein Modul ist demnach sozusagen ein „Vektorraum“ über R. Viele Begriffe werden daher wortwörtlich von Vektorräumen übernommen: Für Moduln wird die lineare Unabhängigkeit von Elementen analog wie für Vektorräume definiert. Eine Basis eines Moduls ist ein linear unabhängiges Erzeugendensystem.
Man sagt, ein Modul sei frei vom Rang n, wenn er eine Basis bestehend aus n Elementen besitzt. Mit obiger Definition ist der Rang stets eindeutig, je zwei Basen haben gleiche Länge. Allerdings existiert nicht für jeden Modul eine Basis.

In unseren Anwendungen werden wir es ausschließlich mit $\mathbb{Z}$-Moduln zu tun haben. Der Ring $\mathbb{Z}$ ist ein Hauptidealring, und wir wollen dies nun für R voraussetzen. Schnell sei noch bemerkt, daß die $\mathbb{Z}$-Moduln nichts anderes sind als abelsche

Gruppen $(M, +)$ — schließlich ist jedes $x \in \mathbb{Z}$ abgesehen vom Vorzeichen Summe von Einsen. Folglich werden wir dann später nicht mehr explizit von $\mathbb{Z}$-Moduln reden.

Satz 2.1.1 *Sei R ein Hauptidealring und M ein freier R-Modul vom Rang n. Jeder Untermodul U von M ist dann frei vom Rang k mit $k \leq n$.*

Einen Überblick über die Struktur endlich erzeugter Moduln über Hauptidealringen liefert

Satz 2.1.2 *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es Zahlen $k, m \in \mathbb{Z}^{\geq 0}$ und $c_1, \ldots, c_k \in \mathbb{Z}^{\geq 2}$, so daß*

$$M \simeq (\mathbb{Z}/c_1\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/c_k\mathbb{Z}) \oplus \mathbb{Z}^m,$$

wobei m eindeutig bestimmt ist. Unter der Bedingung $c_1 \mid \ldots \mid c_k$ werden auch k und die c_i eindeutig durch M bestimmt.

Beweis: Die Beweise finden sich in [11]. □

In enger Verbindung zu diesen Sätzen stehen die Hermite Normalform (HNF) und Smith Normalform für Matrizen über $R = \mathbb{Z}$. Wir befassen uns zuerst mit der Hermite Normalform, die mit Satz 2.1.1 korrespondiert, und beschränken uns speziell auf die Spaltenversion. Wir vereinbaren: $\max \emptyset = -\infty$ und $\min \emptyset = \infty$.

Definition 2.1.3 *Sei $B = (b_{ij}) \in \mathbb{Z}^{n \times m}$ und $I_j = \{\ i \mid b_{ij} \neq 0$ und $1 \leq i \leq n\}$. Wir setzen $m_0 = \max\{\ j \mid I_j \neq \emptyset$ und $1 \leq j \leq m\}$, $f_j = \min I_j$ und definieren: B ist in unterer Hermite Normalform, wenn $f_1 > \ldots > f_{m_0}$ und für jedes $j = 1, \ldots, m_0$ gilt:*

$$\begin{array}{ll} b_{ij} > 0 & \textit{für} \quad i = f_j, \\ 0 \leq b_{f_k j} < b_{f_k k} & \textit{für} \quad j < k \leq m_0. \end{array}$$

Die Matrix B ist in oberer HNF, wenn $\widetilde{B} = (b_{n-i,n-j})$ in unterer HNF ist.

Bei der Hermite Normalform handelt es sich also um eine spezielle Spaltenstufenform. Eine beispielsweise nur aus Nullen bestehende Matrix ist in oberer und unterer HNF. Diese Definition unterscheidet sich für $n \neq m$ von der Definition in [16, 15]. Wenn nichts anderes gesagt ist, so meinen wir im folgenden mit einer Hermite Normalform stets eine untere Hermite Normalform.

Satz 2.1.4 *Sei $A \in \mathbb{Z}^{n \times m}$. Dann gibt es invertierbare Matrizen $T_1, T_2 \in \mathbb{Z}^{m \times m}$, so daß $B = AT_1$ in unterer HNF und $\widetilde{B} = AT_2$ in oberer HNF ist. B und $\widetilde{B}$ sind eindeutig durch A bestimmt.*

Beweis: Zum Beweis verweisen wir auf [16, 5]. Dort finden sich auch Algorithmen zur Berechnung der Hermite Normalform einer Matrix. Die Eindeutigkeit kommt durch folgende Überlegungen zustande: Seien B_1 und B_2 zwei Hermite Normalformen zu A. Die Spalten dieser drei Matrizen erzeugen wegen der unimodularen Transformationen alle denselben Modul $M \subseteq \mathbb{Z}^n$. Für $v \in M$ schreiben wir v_i für die i-te Komponente und definieren $f(v) = \min\{\, i \,|\, v_i \neq 0$ und $1 \leq i \leq n\}$. Offenbar ist $\{f(v) \,|\, v \in M \backslash \{0\}\}$ endlich und stimmt mit $\{f_1, \ldots, f_{m_0}\}$ für B_1 und $\{f_1, \ldots, f_{m_0}\}$ für B_2 aus der Definition der HNF überein. Folglich haben B_1 und B_2 dieselbe Stufengestalt. Zusätzlich stimmen auch die Stufenelemente überein. Wir bezeichnen mit H_j die j-te Spalte einer Matrix H. Betrachte $v = B_{1,j} - B_{2,j}$ für $1 \leq j \leq m_0$. Wir wollen annehmen, daß die Gleichheit der k-ten Spalten von B_1 und B_2 für $j < k \leq m_0$ gezeigt ist. Es ist nicht möglich, daß $f(v) = f_j$, da die f_j-ten Komponenten von $B_{1,j}$ und $B_{2,j}$ gleich sind. Nehmen wir an, daß $f(v) = f_k$ für $j < k \leq m_0$. Die f_k-te Komponente von v ist durch die f_k-ten Komponenten von $B_{1,k}$ bzw. $B_{2,k}$ — die gleich sind — teilbar und daher wegen der Reduktionseigenschaft im Widerspruch zur Annahme gleich Null. Es folgt $v = 0$. □

Die Matrix B bezeichnet man als (untere) Hermite Normalform, $\widetilde{B}$ als obere Hermite Normalform von A.

Invertierbare Matrizen $T \in \mathbb{Z}^{m \times m}$ heißen unimodular. Es gilt

$$T \text{ invertierbar in } \mathbb{Z}^{m \times m} \;\Leftrightarrow\; \det(T) \text{ invertierbar in } \mathbb{Z}.$$

Folglich sind die unimodularen Matrizen über $\mathbb{Z}$ genau die Matrizen mit Determinantenbetrag gleich 1.

Wir wenden die Hermite Normalform auf die Situation eines freien $\mathbb{Z}$-Moduls M vom Rang n mit Untermodul U vom Rang k an. Sei $v_1, \ldots, v_n$ eine Basis von M und $u_1, \ldots, u_m$ ein Erzeugendensystem von U. Wir nehmen an, daß wir die u_i explizit durch die v_i ausdrücken können und wollen eine Basis von U ermitteln. Es gibt also eine Matrix $A \in \mathbb{Z}^{n \times m}$ mit

$$(v_1, \ldots, v_n)\, A = (u_1, \ldots, u_m).$$

Wir können von rechts mit einem geeigneten unimodularen $T \in \mathbb{Z}^{m \times m}$ multiplizieren, welches A in eine HNF B überführt, und erhalten

$$(v_1, \ldots, v_n)\, B = (\widetilde{u}_1, \ldots, \widetilde{u}_k, 0, \ldots, 0)$$

mit $m - k$ vielen Nullen. Die $\widetilde{u}_i$ bilden aufgrund der Gestalt von B und der Invertierbarkeit von T eine Basis von U. Hat U den Rang $k = n$, so ist B eine untere Dreiecksmatrix ohne Nullen auf der Diagonalen mit $m - k$ hinteren Nullspalten. Wir schneiden diese Nullspalten ab und folgern für den Index abelscher Gruppen:

$$(M : U) = |\det B|.$$

Nun zur Smith Normalform (SNF), die mit Satz 2.1.2 in Verbindung steht.

Definition 2.1.5 *Eine Matrix $B = (b_{ij}) \in \mathbb{Z}^{n\times m}$ vom Rang k ist in Smith Normalform, wenn gilt:*

$$\begin{array}{lll} b_{ij} = 0 & \textit{für} & i \neq j, \\ b_{ii} = 0 & \textit{für} & i > k, \\ b_{ii} > 0 & \textit{für} & i \leq k, \end{array}$$

$$\textit{und} \quad b_{11} \mid \ldots \mid b_{kk}.$$

Satz 2.1.6 *Sei $A \in \mathbb{Z}^{n\times m}$. Dann gibt es unimodulare Matrizen $T_1 \in \mathbb{Z}^{n\times n}$ und $T_2 \in \mathbb{Z}^{m\times m}$, so daß $B = T_1AT_2$ in Smith Normalform ist. B ist eindeutig durch A bestimmt.*

Beweis und Algorithmen siehe [16, 5]. Wir bezeichnen B als Smith Normalform von A.

Während wir bei der obigen Anwendung der Hermite Normalform nur Basiswechsel im Untermodul U zulassen, soll dies nun auch in M geschehen dürfen. Wir wollen im Hinblick auf die spätere Anwendung gleich annehmen, daß der Rang von U mit dem Rang von M übereinstimmt. Nach Bildung der Smith Normalform B von A erhält man eine Diagonalmatrix ohne Nullen auf der Diagonalen mit $m-n$ angehängten Nullspalten. Durch das Abschneiden dieser überflüssigen Nullspalten erhalten wir eine Transformationsmatrix $C = (c_{ij})$ einer Basis von M auf eine Basis von U. Wir folgern, daß

$$M/U \simeq (\mathbb{Z}/c_{11}\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/c_{nn}\mathbb{Z})$$

und erhalten damit die eindeutige Darstellung von M aus Satz 2.1.2. Tatsächlich kann dieser Satz mit Hilfe der Smith Normalform und Satz 2.1.1 bewiesen werden.

Wir werden später genau wie hier dargestellt die Hermite Normalform und Smith Normalform dazu verwenden, aus einem M und U die Struktur von M/U zu bestimmen.

2.2 Algebraische Zahlkörper

Es sei $f(t)$ ein normiertes und irreduzibles Polynom aus $\mathbb{Z}[t]$. Ein algebraischer Zahlkörper K wird durch Adjunktion einer Nullstelle $\rho = t + f(t)\mathbb{Q}[t]$ von $f(t)$ zu $\mathbb{Q}$ definiert:

$$K = \mathbb{Q}[t]/f(t)\mathbb{Q}[t] = \mathbb{Q}(\rho).$$

Der Grad der Körpererweiterung stimmt mit dem Grad des Polynoms überein und wird mit n bezeichnet. Die r_1 reellen und $2r_2$ komplexen Nullstellen von $f(t)$ numerieren wir wie folgt:

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

- $\rho^{(r_1+1)}, \ldots, \rho^{(r_1+r_2)} \in \mathbb{C}\backslash\mathbb{R}$,
- $\rho^{(r_1+r_2+i)} = \overline{\rho^{(r_1+i)}}$ für $1 \leq i \leq r_2$.

Man erhält damit die n $\mathbb{Q}$-linearen Einbettungen von K in $\mathbb{C}$

$$\sigma_i : K \longrightarrow \mathbb{C}, \quad \sigma_i(\rho) = \rho^{(i)}$$

für $1 \leq i \leq n$. Das Element $\rho^{(i)}$ wird auch als i-te Konjugierte von ρ bezeichnet. Unter der Signatur von K verstehen wir das Tupel (r_1, r_2).

Ein Element $x \in K$ heißt ganzalgebraisch, wenn es einer Ganzheitsgleichung genügt, wenn also ein normiertes Polynom $g(t)$ aus $\mathbb{Z}[t]$ mit $g(x) = 0$ existiert. Die ganzalgebraischen Zahlen von K bilden einen Ring, der Maximalordnung genannt und mit $\mathfrak{o}_K$ bezeichnet wird. Die Maximalordnung trägt die Struktur eines freien $\mathbb{Z}$-Moduls vom Rang n, dessen Basen Ganzheitsbasen von K heißen. Wir wählen stets eine Ganzheitsbasis $\omega_1, \ldots, \omega_n \in \mathfrak{o}_K$ derart, daß $\omega_1 = 1$ ist; dies ist immer möglich.

Die Norm und die Spur eines Elements $x \in K$ werden definiert durch

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} x^{(i)}$$

und

$$Tr_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} x^{(i)}.$$

Stets sind $N_{K/\mathbb{Q}}(x)$, $Tr_{K/\mathbb{Q}}(x) \in \mathbb{Q}$ und für ein ganzalgebraisches Element x gilt $N_{K/\mathbb{Q}}(x)$, $Tr_{K/\mathbb{Q}}(x) \in \mathbb{Z}$.

Mit Hilfe einer Ganzheitsbasis definieren wir die Körperdiskriminante D_K durch

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

Diese Definition ist von der Wahl der Ganzheitsbasis unabhängig, da sich Diskriminanten bei Basiswechsel um das Quadrat der Determinante der Transformationsmatrix ändern und je zwei Ganzheitsbasen durch unimodulare Transformation ineinander übergehen. Bei D_K handelt es sich stets um einen ganzrationalen Zahl, und nach einem Resultat von Minkowski gilt für von $\mathbb{Q}$ verschiedene Zahlkörper $|D_K| > 0$. Schließlich betrachten wir die Gleichungsordnung $\mathbb{Z}[\rho]$. $\mathbb{Z}[\rho]$ ist ein Untermodul von $\mathfrak{o}_K$ und ebenfalls frei vom Rang n. Der Index $(\mathfrak{o}_K : \mathbb{Z}[\rho])$ ist endlich.

Zur Arithmetik in einem Zahlkörper und zur Berechnung von Ganzheitsbasen, Diskriminanten, Norm usw. siehe [16, 15, 5].

2.3 Gitter

Sei $\Lambda \subset \mathbb{R}^m$ ein freier $\mathbb{Z}$-Modul vom Rang k. Enthält Λ k über $\mathbb{R}$ linear unabhängige Vektoren, so sprechen wir von einem Gitter der Dimension k im $\mathbb{R}^m$. Die Gitterdeterminante $d(\Lambda)$ eines Gitters Λ der Dimension k im $\mathbb{R}^m$ wird definiert als das k-dimensionale Volumen des von einer $\mathbb{Z}$-Basis $v_1, \dots, v_k$ von Λ aufgespannten Parallelotops:

$$d(\Lambda) = |\det((v_i^t\, v_j)_{1\le i,j\le k})|^{\frac{1}{2}}.$$

Ist $k = m$, so nennen wir das Gitter vollständig. Gitter sind diskrete Teilmengen des $\mathbb{R}^m$, jede Kugel (endlichen Durchmessers) enthält nur endlich viele Gitterpunkte.

Für uns wird es wichtig sein, Elemente $x \in \mathfrak{o}_K$ mit kleinen ganzen Normbeträgen zu bestimmen. Die Norm von x ist das Produkt über die n Konjugierten von x; es müssen also alle Konjugierten berücksichtigt werden. Dies geschieht in Konjugiertengittern zu freien $\mathbb{Z}$-Untermoduln M von $\mathfrak{o}_K$ vom Rang n. Wir definieren diese für einen beliebigen freien $\mathbb{Z}$-Untermodul M von K vom Rang n mit Basis $\alpha_1, \dots, \alpha_n \in M$ wie folgt:

Auf dem $\mathbb{Q}$-Vektorraum K ist ein inneres Produkt gegeben durch

$$<\, ,\, > : K \times K \longrightarrow \mathbb{R},\ (x, y) \longmapsto \sum_{i=1}^{n} x^{(i)}\overline{y^{(i)}}.$$

Wir definieren hiermit eine positiv definite quadratische Form, die T_2-Norm, durch

$$T_2 : K \longrightarrow \mathbb{R}^{\ge 0},\ x \longmapsto <x, x> .$$

Mit Hilfe der $\alpha_1, \dots, \alpha_n$, die eine $\mathbb{Q}$-Basis von K bilden, und unter Beachtung der Matrix

$$B = (\alpha_j^{(i)})_{1\le i,j\le n} \in \mathbb{C}^{n\times n}$$

erhalten wir die Grammatrix des inneren Produkts von K durch die positiv definite Matrix

$$A = (<\alpha_i, \alpha_j>)_{1\le i,j\le n} = B^t\overline{B} \in \mathbb{R}^{n\times n}.$$

Ist also $x = \sum_{i=1}^n x_i\alpha_i$ mit $x_i \in \mathbb{Q}$, so gilt für die T_2-Norm

$$T_2(x) = (x_1, \dots, x_n) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Wir definieren nun ein zu M als $\mathbb{Z}$-Modul isomorphes Gitter $\Lambda(M)$ im $\mathbb{R}^n$, in dem das euklidische Skalarprodukt bezüglich der Bilder der α_i unter dem Isomorphismus ebenfalls die Grammatrix A besitzt. Dann fallen offenbar das Quadrat der euklidischen Norm und die T_2-Norm unter Identifizierung von Gitterpunkten mit den Elementen von M zusammen. Wir definieren $\Lambda(M)$ als das Bild des Monomorphismus $M \longrightarrow \mathbb{R}^n$, der ein $x \in M$ auf

$$(x^{(1)}, \ldots, x^{(r_1)}, \sqrt{2}\,\mathrm{Re}\, x^{(r_1+1)}, \sqrt{2}\,\mathrm{Im}\, x^{(r_1+1)}, \ldots, \sqrt{2}\,\mathrm{Re}\, x^{(r_1+r_2)}, \sqrt{2}\,\mathrm{Im}\, x^{(r_1+r_2)})^t$$

aus $\mathbb{R}^n$ abbildet. $\mathbb{Q}$-linear unabhängige Elemente werden hierdurch in $\mathbb{R}$-linear unabhängige Vektoren überführt. Daher handelt es sich bei $\Lambda(M)$ um ein vollständiges Gitter im $\mathbb{R}^n$, welches wir das Konjugiertengitter zu M nennen. Gehen wir von B über zu einer Matrix $\widetilde{B} \in \mathbb{R}^n$, deren Spalten die Bilder der $\alpha_1, \ldots, \alpha_n$ unter obigem Monomorphismus sind, so gilt

$$A = \widetilde{B}^t \widetilde{B}$$

und für die Gitterdeterminante von $\Lambda(M)$ erhalten wir

$$d(\Lambda(M)) = |\det A|^{\frac{1}{2}}.$$

Ist $M \subseteq \mathfrak{o}_K$, so gilt $d(\Lambda(M))^2 \in \mathbb{Z}$. Um den Bezug zur Diskriminante D_K herzustellen, nehmen wir an, daß

$$(\alpha_1, \ldots, \alpha_n) = (\omega_1, \ldots, \omega_n)\, T_M$$

mit einer Transformationsmatrix $T_M \in \mathbb{Z}^{n \times n}$ gilt. Unter dieser Voraussetzung folgt die Gleichheit

$$d(\Lambda(M))^2 = |D_K|\, \det(T_M)^2.$$

Wir wollten das Konjugiertengitter $\Lambda(M)$ für $M \subseteq \mathfrak{o}_K$ zur Bestimmung ganzalgebraischer Zahlen $x \in \mathfrak{o}_K$ kleinen Normbetrags nutzen. Dies geschieht vermöge des folgenden Zusammenhangs von Norm und T_2-Norm, der eine Konsequenz der Ungleichung zwischen arithmetischen und geometrischen Mittel ist:

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{T_2(x)}{n}\right)^{\frac{n}{2}}.$$

Ist die T_2-Norm klein, so auch der Normbetrag. Umgekehrtes gilt jedoch nicht. Die Bestimmung T_2-Norm beschränkter Elemente entspricht dem Auszählen einer Kugel beschränkten Durchmessers in $\Lambda(M)$ und erfolgt mit dem Auszählalgorithmus von Fincke und Pohst für positiv definite quadratische Formen angewendet auf die Grammatrix A, siehe [16, 15]. Hiermit können wir sukzessive alle Elemente dieser beschränkten Kugel in $\Lambda(M)$ bestimmen.

Für manche Gitter mit schlecht konditionierten Basen muß allerdings vorher eine LLL-Reduktion durchgeführt werden. Der LLL-Algorithmus und die Eigenschaften LLL-reduzierter Basen werden eingehend in [16] beschrieben. Wir erwähnen nur kurz, daß die Elemente einer LLL-reduzierten Basis Kandidaten für kurze

Vektoren im Gitter sind. Insbesondere das erste Basiselement stellt im allgemeinen eine gute Approximation eines kürzesten Vektors im Gitter dar.

Gegeben seien linear unabhängige Vektoren $b_1, \ldots, b_k$ eines Gitters Λ im $\mathbb{R}^m$ und ein Vektor $v \in \Lambda \backslash \{0\}$. Wir wollen das von den b_i und v erzeugte Teilgitter bestimmen. Sind $v, b_1, \ldots, b_k$ linear unabhängig, so bilden sie bereits eine Basis dieses Teilgitters. Andernfalls wird eine modifizierte Version des LLL-Algorithmus, der MLLL-Algorithmus, verwendet. Auch er ist in [16] beschrieben. Seine Ausgabe besteht aus einer Basis des gesuchten Teilgitters bzw. einer Transformationsmatrix, die v und die b_i in diese Basis überführt, und aus einer Relation $\lambda v = \sum_{i=1}^{k} \lambda_i b_i$ mit $\lambda, \lambda_i \in \mathbb{Z}$ und $\lambda \neq 0$. Dieser Algorithmus läßt sich übrigens so durchführen, daß nicht im voraus die Abhängigkeit von v und $b_1, \ldots, b_k$ feststehen muß. Sind diese Elemente unabhängig, so werden sie dann einfach LLL-reduziert.

Wir bemerken, daß diese Aufgabe der Berechnung einer Basis ähnlich der aus Abschnitt 2.1 ist. Dort konnte eine Basis des Untermoduls U eines freien Moduls M aus einem Erzeugendensystem von U mit Hilfe einer Hermite Normalform berechnet werden. Die Erzeuger von U ließen sich nämlich durch die Basiselemente von M darstellen. Da uns ein solches M hier fehlt, können wir diesen Weg nicht beschreiten.

2.4 Einheiten

Unter einer Einheit von K versteht man eine ganzalgebraische Zahl $\varepsilon \in \mathfrak{o}_K$, für die auch $\varepsilon^{-1} \in \mathfrak{o}_K$ ist. Ein $\varepsilon \in \mathfrak{o}_K$ ist genau dann eine Einheit, wenn $|N_{K/\mathbb{Q}}(\varepsilon)| = 1$ ist.

Wir kommen zur Einheitengruppe U_K der Maximalordnung eines algebraischen Zahlkörpers K. Mit TU_K werde die endliche zyklische Gruppe der Torsionseinheiten, also der Einheitswurzeln, bezeichnet. Ihre Ordnung sei w_K. Über die Struktur von U_K besagt der folgende Satz:

Satz 2.4.1 (Dirichletscher Einheitensatz) *Die Einheitengruppe U_K ist die direkte Summe der Gruppe TU_K und einer freien abelschen Gruppe vom Rang $r_1 + r_2 - 1$.*

Die Zahl $r_1 + r_2 - 1$ heißt Einheitenrang von K und wird mit r bezeichnet. Es gibt also Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in U_K$ so daß sich jede weitere Einheit $\varepsilon \in U_K$ eindeutig als ein Potenzprodukt der Form

$$\varepsilon = \zeta\, \varepsilon_1^{k_1} \cdots \varepsilon_r^{k_r}$$

mit $\zeta \in TU_K$ und $k_1, \ldots, k_r \in \mathbb{Z}$ darstellen läßt. Solche Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ heißen Fundamentaleinheiten.

In Abschnitt 2.1 wurde erwähnt, daß jede abelsche Gruppe als $\mathbb{Z}$-Modul aufgefaßt werden kann. Dies wollen wir speziell für Untergruppen der multiplikativen Gruppe $K^\times$ tun. Der Addition im Modul entspricht dann die Multiplikation in $K^\times$, der Multiplikation mit Zahlen aus $\mathbb{Z}$ die Potenzbildung mit diesen Zahlen als Exponenten.

Definition 2.4.2 *Eine Menge von algebraischen Zahlen $\alpha_1, \ldots, \alpha_m \in K^\times$ heißt unabhängig, wenn*

$$\alpha_1^{\lambda_1} \cdots \alpha_m^{\lambda_m} = 1 \quad \Rightarrow \quad \lambda_1 = \ldots = \lambda_m = 0$$

gilt.

Offenbar sind Fundamentaleinheiten nach dem oben Gesagten immer unabhängig, Torsionseinheiten sind dagegen schon jede für sich genommen abhängig.

Mit Hilfe der folgenden Abbildung können wir die multiplikative Struktur von Untergruppen von $K^\times$ in die additive Struktur des $\mathbb{R}^r$ überführen. Unter Beachtung von $c_i = 1$ für $1 \leq i \leq r_1$ und $c_i = 2$ für $r_1 < i \leq r$ wird definiert:

$$L : K^\times \longrightarrow \mathbb{R}^r, \quad \alpha \longmapsto \begin{pmatrix} c_1 \log |\alpha^{(1)}| \\ \vdots \\ c_r \log |\alpha^{(r)}| \end{pmatrix}.$$

Diese Abbildung ist ein Homomorphismus der beteiligten $\mathbb{Z}$-Moduln. Wir könnten nun das Bild einer Untergruppe von $K^\times$ mit Methoden der linearen Algebra über $\mathbb{R}$ untersuchen, um Rückschlüsse auf die Untergruppe selbst zu ziehen. L weist allerdings eine Schwäche auf: Unabhängige Elemente von $K^\times$ werden nicht unbedingt auf $\mathbb{R}$-linear unabhängige Vektoren abgebildet. Jedoch sind Einheiten $\varepsilon_1, \ldots, \varepsilon_m \in U_K$ genau dann unabhängig, wenn die Vektoren $L(\varepsilon_1), \ldots, L(\varepsilon_m) \in \mathbb{R}^r$ linear unabhängig über $\mathbb{R}$ sind. Wir werden L also zur Untersuchung von U_K heranziehen.

Sei U eine Untergruppe der Einheitengruppe mit endlichem Index $(U_K : U)$. Das Bild von U unter L ist ein vollständiges Gitter im $\mathbb{R}^r$. Zu einer Basis von $L(U)$ gehörende Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in U$ sind unabhängig und erzeugen U modulo Torsioneinheiten. Die Gitterdeterminante von $L(U)$ bezeichnen wir als den Regulator von U:

$$\operatorname{Reg}(U) = |\det(L(\varepsilon_1), \ldots, L(\varepsilon_r))| = d(L(U)).$$

Der Regulator des Zahlkörpers K wird als Regulator der gesamten Einheitengruppe U_K definiert und mit R_K bezeichnet. Diese Definitionen sind, aus ähnlichen Gründen wie schon oben die Definition der Diskriminante, unabhängig von der Wahl der Einheiten $\varepsilon_1, \ldots, \varepsilon_r$. Sie sind aber auch unabhängig von der Anordnung der Konjugierten.

Wir bemerken unter Berücksichtigung der Ergebnisse des Abschnitts 2.1, daß der Regulator von U ein ganzzahliges Vielfaches von R_K ist. Mit der Bezeichnung U' für das Erzeugnis von TU_K und U gilt:

$$\frac{\mathrm{Reg}(U)}{R_K} = (U_K : U'). \tag{2.1}$$

Zur Berechnung der Einheiten eines Zahlkörpers siehe [16, 15, 22].

2.5 Klassengruppe

Die Maximalordnung von $\mathbb{Q}$ ist $\mathbb{Z}$. In diesem Ring gilt der Satz von der eindeutigen Zerlegung in Primfaktoren. Mehr noch, $\mathbb{Z}$ ist ein Hauptidealring. Diese beiden Eigenschaften sind für Maximalordnungen beliebiger Zahlkörper äquivalent, treffen allerdings im allgemeinen nicht zu. Erhalten bleibt nur die Faktorisierbarkeit in irreduzible Elemente. Ein häufig genanntes Beispiel hierfür ist der Zahlkörper $K = \mathbb{Q}(\sqrt{-5})$ mit Maximalordnung $\mathbb{Z}[\sqrt{-5}]$. Hierin bestehen beispielsweise folgende verschiedene Zerlegungen der Zahl 6 in irreduzible, aber nicht prime Elemente:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Eine eindeutige Zerlegung in Primfaktoren wird jedoch möglich, wenn man von Elementen zu Idealen übergeht.

Sprechen wir im folgenden von Idealen von $\mathfrak{o}_K$, so schließen wir das Nullideal, das nur aus dem Nullelement besteht, aus. Wir lassen $\mathfrak{o}_K$ als Ideal von $\mathfrak{o}_K$ zu. Ein Primideal $\mathfrak{p}$ von $\mathfrak{o}_K$ ist ein echtes Ideal von $\mathfrak{o}_K$, also $\mathfrak{p} \neq \mathfrak{o}_K$, für das $\mathfrak{o}_K/\mathfrak{p}$ nullteilerfrei ist. Wir definieren Addition und Multiplikation von Idealen $\mathfrak{a}, \mathfrak{b}$ durch

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

und

$$\mathfrak{a}\mathfrak{b} = \{\sum_{i=1}^{k} a_i b_i \mid k \in \mathbb{Z}^{\geq 0} \text{ und } a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \text{ für } 1 \leq i \leq k\}.$$

Man sieht leicht, daß beide Verknüpfungen assoziativ und kommutativ sind und daß $\mathfrak{o}_K$ neutrales Element der Multiplikation ist. Die Ideale von $\mathfrak{o}_K$ bilden mit der Idealmultiplikation daher einen Monoid, ganz ähnlich wie die ganzen Zahlen mit ihrer Multiplikation.

Jedes Ideal $\mathfrak{a}$ einer Maximalordnung $\mathfrak{o}_K$ läßt sich nun eindeutig bis auf die Reihenfolge als ein Potenzprodukt mit positiven Exponenten von paarweise verschiedenen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ von $\mathfrak{o}_K$ schreiben:

$$\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k}.$$

Wir fassen hierbei $\mathfrak{o}_K$ als das „leere" Produkt auf. Man sagt, die Maximalordnung $\mathfrak{o}_K$ sei ein Dedekindring. Auf den Fall des obigen Beispiels bezogen findet man mit

$$\begin{aligned}
\mathfrak{p}_1 &= 2\mathfrak{o}_K + (1+\sqrt{-5})\mathfrak{o}_K = 2\mathfrak{o}_K + (1-\sqrt{-5})\mathfrak{o}_K,\\
\mathfrak{p}_2 &= 3\mathfrak{o}_K + (1+\sqrt{-5})\mathfrak{o}_K,\\
\mathfrak{p}_3 &= 3\mathfrak{o}_K + (1-\sqrt{-5})\mathfrak{o}_K
\end{aligned}$$

die eindeutigen Zerlegungen

$$2\mathfrak{o}_K = \mathfrak{p}_1^2,\ \ 3\mathfrak{o}_K = \mathfrak{p}_2\mathfrak{p}_3,\ \ (1+\sqrt{-5})\mathfrak{o}_K = \mathfrak{p}_1\mathfrak{p}_2,\ \ (1-\sqrt{-5})\mathfrak{o}_K = \mathfrak{p}_1\mathfrak{p}_3$$

und schließlich

$$6\mathfrak{o}_K = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3.$$

Die Primzahlzerlegung in $\mathbb{Z}$ läßt sich unter Hinzunahme negativer Potenzen auf Zahlen aus $\mathbb{Q}$ ausdehnen. Analog kann man die Primidealzerlegung für die Ideale von K definieren. Diese sind die Elemente der Menge

$$I_K = \{\mathfrak{a} \subseteq K \mid x\mathfrak{a} \text{ ist ein Ideal von } \mathfrak{o}_K \text{ für ein } x \in K\},$$

die mit der oben definierten Idealmultiplikation angewendet auf diese verallgemeinerten Ideale eine abelsche Gruppe mit Einselement $\mathfrak{o}_K$ wird. Daß I_K eine Gruppe ist, liegt keineswegs auf der Hand. Diese Eigenschaft ist äquivalent zur Primidealzerlegung in $\mathfrak{o}_K$ und nur der Ring aller ganzalgebraischen Zahlen von K erfüllt diese Eigenschaft. In der Gleichungsordnung $\mathbb{Z}[\rho]$ ist sie beispielsweise im allgemeinen nicht erfüllt.

Unter einem Hauptideal von K verstehen wir ein Ideal $\mathfrak{a} \in I_K$, für das ein $x \in K^\times$ mit $\mathfrak{a} = x\mathfrak{o}_K$ existiert. Die Hauptideale bilden eine Untergruppe von I_K, die mit H_K bezeichnet wird. Wir betrachten die Abbildung

$$I : K^\times \longrightarrow H_K,\ x \longmapsto x\mathfrak{o}_K.$$

Der Kern von I ist U_K und daher besteht die Isomorphie

$$K^\times/U_K \simeq H_K.$$

Da man die Elemente von $K^\times$ in Faktorisierungsfragen nur modulo Einheiten betrachtet, bedeutet der Übergang zu H_K keine wesentliche Veränderung, und wir schreiben für $x \in K^\times$ statt $x\mathfrak{o}_K$ häufig einfach x, wenn möglich.

Jedes Ideal aus I_K besitzt eine eindeutige Zerlegung in ein Potenzprodukt mit ganzrationalen Exponenten von Primidealen von $\mathfrak{o}_K$. Genauer gesagt gibt es für jedes Primideal $\mathfrak{p}$ einen eindeutigen Homomorphismus

$$\nu_{\mathfrak{p}} : I_K \longrightarrow \mathbb{Z},$$

so daß mit der Bezeichnung $\mathbb{P}_K$ für die Menge der Primideale von $\mathfrak{o}_K$ für beliebige Ideale $\mathfrak{a} \in I_K$ die Gleichung

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

gilt. Bei diesem Produkt sind nur endlich viele Exponenten ungleich Null. Wir nennen einen solchen Homomorphismus $\nu_\mathfrak{p}$ exponentielle Bewertung von $\mathfrak{p}$. Aufgrund dieser Eigenschaft handelt es sich bei I_K, ähnlich wie bei $K^\times$ im vorigen Abschnitt, um einen freien $\mathbb{Z}$-Modul. Der Rang ist nicht endlich, denn eine Basis wird offenbar durch die Menge der Primideale $\mathbb{P}_K$ gegeben. Wir übernehmen den Begriff der Unabhängigkeit aus 2.4.2 auch für Ideale.

Wie aus dem Beispiel folgt, liegen im allgemeinen nicht alle Primideale in H_K — sonst wäre eine eindeutige Zerlegung in prime Elemente möglich gewesen. Ein struktureller Ausdruck dieses Mangels ist die Klassengruppe

$$Cl_K = I_K / H_K,$$

ein „quantitativer“ die Klassenzahl

$$h_K = |\, Cl_K|.$$

Die Klassenzahl ist stets endlich. Dies bedeutet allerdings nicht, daß etwa nur endlich viele Primideale von $\mathfrak{o}_K$ in H_K fehlen. Vielmehr verteilen sich die Primideale in gewissem Sinne gleichmäßig auf die Elemente von Cl_K, die Idealklassen, so daß im Fall $h_K = 1$ alle Primideale in H_K liegen, für $h_K > 1$ aber gleich unendlich viele in H_K fehlen. Auf solche Verteilungsfragen wollen wir aber nicht eingehen. Wichtig für uns ist dagegen die Tatsache, daß die Klassengruppe von den Idealklassen endlich vieler Primideale erzeugt wird. Um diesen Sachverhalt genauer zu beleuchten, und auch für die spätere Anwendung, seien ein paar Begriffe im Zusammenhang mit Idealen kurz erläutert:

Ein Ideal $\mathfrak{a} \in I_K$ heißt ganz, wenn $\mathfrak{a} \subseteq \mathfrak{o}_K$, ansonsten gebrochen. Es ist genau dann ganz, wenn in seiner Zerlegung in Primidealpotenzen nur nicht negative Potenzen auftreten, d. h. $\nu_\mathfrak{p}(\mathfrak{a}) \geq 0$ für alle $\mathfrak{p} \in \mathbb{P}_K$. Man sagt, ein Ideal $\mathfrak{a}$ teile ein Ideal $\mathfrak{b}$, wenn es ein ganzes Ideal $\mathfrak{c}$ gibt, so daß $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$, und schreibt $\mathfrak{a} \mid \mathfrak{b}$. Für zwei Ideale $\mathfrak{a}, \mathfrak{b}$ gilt:

$$\mathfrak{a} \mid \mathfrak{b} \;\Leftrightarrow\; \mathfrak{b} \subseteq \mathfrak{a}.$$

Bei der bereits oben verwendeten Addition von Idealen erhält man somit den größten gemeinsamen Teiler (ggT) und entsprechend mit dem Schnitt das kleinste gemeinsame Vielfache (kgV) dieser Ideale.

Jedes Ideal von K, als Untergruppe der additiven Struktur von K betrachtet, ist ein freier $\mathbb{Z}$-Modul vom Rang n. Wir definieren damit die Norm eines Ideals $\mathfrak{a}$ von K als Absolutbetrag der Determinante der Transformationsmatrix einer Ganzheitsbasis von K auf eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ und schreiben hierfür $N(\mathfrak{a})$. Die Idealnorm hat die folgenden Eigenschaften:

(i) $N(\mathfrak{a}) = (\mathfrak{o}_K : \mathfrak{a})$ für $\mathfrak{a} \in I_K$ ganz,

(ii) $N(x\mathfrak{o}_K) = |N_{K/\mathbb{Q}}(x)|$ für $x \in K^\times$,

(iii) $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ für $\mathfrak{a}, \mathfrak{b} \in I_K$.

Der Schnitt eines ganzen Ideals mit $\mathbb{Z}$ ist ein Ideal von $\mathbb{Z}$. Für ein Primideal $\mathfrak{p}$ ist daher $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ mit einer eindeutig bestimmten Primzahl $p \in \mathbb{Z}$. Man sagt, $\mathfrak{p}$ liegt über p. Das Ideal $p\mathfrak{o}_K$ besitzt eine Zerlegung in Potenzen von verschiedenen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ der Form

$$p\mathfrak{o}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

mit $e_1, \ldots, e_g \in \mathbb{Z}^{\geq 1}$. Der Exponent e_i heißt der Verzweigungsindex von $\mathfrak{p}_i$ über p und wird mit $e(\mathfrak{p}_i \,|\, p)$ bezeichnet. Der Faktorring $\mathfrak{o}_K/\mathfrak{p}_i$ ist ein endlicher Körper der Charakteristik p und für seine Elementanzahl gilt:

$$|\mathfrak{o}_K/\mathfrak{p}_i| = N(\mathfrak{p}_i) = p^{f_i} \text{ mit } f_i \in \mathbb{Z}^{\geq 1}.$$

Der Exponent f_i heißt Trägheits- oder Restklassengrad von $\mathfrak{p}_i$ und wird mit $f(\mathfrak{p}_i \,|\, p)$ bezeichnet. Ist für ein Primideal $\mathfrak{p}$ über p der Verzweigungsindex $e(\mathfrak{p} \,|\, p)$ ungleich eins, so heißt das Primideal verzweigt. Verzweigung tritt genau dann auf, wenn p die Körperdiskriminante D_K teilt. Da $|D_K| > 1$ für Zahlkörper vom Grad $n > 1$, existieren in diesem Fall stets verzweigte Primideale.

Wir kommen auf die Erzeuger der Klassengruppe zurück. Mit gittertheoretischen Methoden, angewendet auf das Konjugiertengitter eines beliebigen Ideals $\mathfrak{a}$, kann die Existenz einer Konstanten $C_K \in \mathbb{Z}^{\geq 1}$ gezeigt werden, die nur vom Zahlkörper K abhängt, so daß $\mathfrak{a}$ ein Element $\alpha \in \mathfrak{a}$ besitzt, dessen Norm beschränkt ist:

$$|N(\alpha)| \leq C_K N(\mathfrak{a}). \tag{2.2}$$

Dies hat wichtige Konsequenzen für die Klassengruppe.

Satz 2.5.1 *Die Klassengruppe Cl_K ist endlich und wird von den Klassen endlich vieler Primideale erzeugt.*

Beweis: Sei $\mathfrak{a}H_K$ eine beliebige Idealklasse aus Cl_K. Wir wählen ein ganzes Ideal $\mathfrak{b}$ der inversen Klasse $\mathfrak{a}^{-1}H_K$; dies ist immer möglich. Zu diesem $\mathfrak{b}$ existiert also nach dem oben gesagten ein $\beta \in \mathfrak{b}$ mit beschränkter Norm. Für die Norm des ganzen Ideals $\tilde{\mathfrak{a}} = \beta/\mathfrak{b}$ gilt daher

$$N(\tilde{\mathfrak{a}}) \leq C_K.$$

Offenbar gilt $\tilde{\mathfrak{a}}H_K = \mathfrak{a}H_K$ und wir folgern daraus, daß jede Idealklasse ein ganzes Ideal besitzt, dessen Norm durch C_K beschränkt ist. Weil sich jedes ganze Ideal als Potenzprodukt von Primidealen mit positiven Exponenten darstellen läßt, die

Norm multiplikativ und für Primideale eine Primzahlpotenz ungleich eins ist, muß die Klassengruppe endlich sein und von den Primidealen mit Norm kleiner gleich C_K erzeugt werden. □

Für den minimalen Wert einer solchen Idealschranke C_K eines Zahlkörpers gibt es verschiedene obere Abschätzungen, die sich aus der Signatur und der Diskriminante berechnen. Eine berühmte obere Abschätzung ist die Minkowskischranke

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|D_K|},$$

die sowohl für spezielle Signaturen als auch asymptotisch verbessert wurde. Unter der Voraussetzung einiger spezieller Signaturen kann man sogar bestmögliche Abschätzungen in dem Sinne, daß sie für einen Körper dieser Signatur scharf sind, angeben. Siehe hierzu [25, 21].

Kapitel 3

Das Verfahren der Klassengruppenberechnung

Im wesentlichen teilt sich das Verfahren der Klassengruppenberechnung in drei Hauptarbeitsschritte auf: Zuerst muß eine Menge von Primidealen konstruiert werden. Zweitens müssen dazu geeignete algebraische Zahlen bestimmt werden. Drittens muß die in diesen Zahlen enthaltene Information über die Klassengruppe ausgewertet werden. In diesem Kapitel werden die Ideen des gesamten Verfahrens allgemein und die Methoden des dritten Schritts im Detail besprochen. Das nachfolgende Kapitel beschäftigt sich dann mit der Berechnung der Menge von Primidealen und der Berechnung der geeigneten algebraischen Zahlen.

Man startet mit einem beliebigem Zahlkörper K und einer Ganzheitsbasis von K. Als Ergebnis erwarten wir eine Darstellung der Klassengruppe Cl_K als direktes Produkt endlicher zyklischer Gruppen $\mathbb{Z}/c_1\mathbb{Z}, \ldots, \mathbb{Z}/c_m\mathbb{Z}$ mit $c_i \in \mathbb{Z}^{\geq 1}$ und $c_i | c_{i+1}$ für $1 \leq i < m$. Dies ist nach Satz 2.1.2 stets eindeutig möglich. Ferner sind ganze Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ und algebraische Zahlen $\gamma_1, \ldots, \gamma_m$ zu bestimmen, so daß $\mathfrak{a}_i^{c_i} = \gamma_i \mathfrak{o}_K$ für $1 \leq i \leq m$ und

$$Cl_K \simeq < \mathfrak{a}_1 H_K > \times \cdots \times < \mathfrak{a}_m H_K > \tag{3.1}$$

gilt.

3.1 Klassengruppenberechnung als S-Einheitenberechnung

Die Klassengruppe wird, wie schon im vorigen Kapitel erwähnt, von den Klassen endlich vieler Primideale erzeugt. Wir definieren:

Definition 3.1.1 *Unter einer Faktorbasis S versteht man eine endliche Menge von Primidealen von $\mathfrak{o}_K$. Wir nennen eine Faktorbasis S vollständig, wenn durch die Klassen ihrer Ideale die ganze Klassengruppe Cl_K erzeugt wird.*

Natürlich wird es sich bei S meist um eine vollständige Faktorbasis handeln. Dies soll aber nicht unbedingt immer vorausgesetzt werden. Wie man eine vollständige Faktorbasis erhält, wird im nächsten Kapitel behandelt.

Sei S eine beliebige Faktorbasis. Die Ableitung der Klassengruppenstruktur geschieht mittels folgender allgemeiner Überlegungen. Die von den Idealen aus S erzeugte Untergruppe I_K^S von I_K ist frei vom Rang $s = |S|$. Durch die Inklusion $I_K^S \subset I_K$ und die Restklassenabbildung $I_K \longrightarrow Cl_K$ wird ein Homomorphismus $I_K^S \longrightarrow Cl_K$ induziert, dessen Kern wir mit H_K^S bezeichnen. H_K^S ist eine Untergruppe von H_K und hat endlichen Index in I_K^S, denn die Klassengruppe ist endlich. Folglich handelt es sich bei H_K^S ebenfalls um eine freie Gruppe vom Rang s. Das Urbild von H_K^S unter $x \mapsto x\mathfrak{o}_K$ bezeichnen wir mit U_K^S. Man sieht, daß U_K eine Untergruppe von U_K^S ist.

Definition 3.1.2 *Die Elemente von U_K^S werden S-Einheiten genannt. Eine S-Einheit, die keine Einheit ist, heiße S-Relation oder kurz auch nur Relation. Die Faktorgruppe I_K^S/H_K^S nennen wir S-Klassengruppe Cl_K^S von K. Ihre Ordnung ist die S-Klassenzahl h_K^S.*

Wir merken an, daß die Definition der S-Klassengruppe kein Standard ist und an anderer Stelle mit anderer Bedeutung verwendet werden kann.

Offenbar ist Cl_K^S eine Untergruppe von Cl_K, und im Falle einer vollständigen Faktorbasis gilt
$$Cl_K^S \simeq Cl_K.$$
Wir nähern uns I_K^S, H_K^S und der gesuchten Darstellung von Cl_K^S mit Hilfe der folgenden Abbildung, wobei $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$:
$$\nu_S : I_K \longrightarrow \mathbb{Z}^s,\ \mathfrak{a} \longmapsto \begin{pmatrix} \nu_{\mathfrak{p}_1}(\mathfrak{a}) \\ \vdots \\ \nu_{\mathfrak{p}_s}(\mathfrak{a}) \end{pmatrix}.$$
Diese Abbildung ist ganz analog dem bereits definierten L ein Homomorphismus der multiplikativen Struktur von I_K in die additive von $\mathbb{Z}^s$. Weil die Primideale aus S eine Basis von I_K^S bilden, gilt offenbar
$$I_K^S \simeq \mathbb{Z}^s$$
unter ν_S, und unabhängige Ideale aus I_K^S werden auf $\mathbb{R}$-linear unabhängige Vektoren abgebildet. Wir müssen zur Ermittlung von Cl_K^S noch H_K^S, sprich eine Basis von H_K^S, bestimmen. Dies geschieht mit der Suche nach S-Relationen, die im nächsten Kapitel genau beschrieben wird. Ziel ist es, durch die gefundenen Relationen ganz H_K^S zu erzeugen. Seien $\alpha_1, \ldots, \alpha_m$ S-Relationen. Das Erzeugnis H der α_i in H_K^S kann nun, wie in Abschnitt 2.1 beschrieben, mit der Hermite

Normalform der Matrix $(\nu_S(\alpha_i))_{1\leq i\leq m} \in \mathbb{Z}^{s\times m}$ berechnet werden. Hat diese Hermite Normalform den Rang s, so ist ihre Determinante bereits ein Vielfaches der S-Klassenzahl (die $m-s$ hinteren Nullspalten werden abgeschnitten). Wenn $H = H_K^S$ berechnen wir die Smith Normalform dieser Matrix, um die gesuchte Darstellung von Cl_K^S zu erhalten. Wann jedoch gilt $H = H_K^S$? Hierzu gibt es zwei verschiedene Methoden, auf die im Abschnitt 3.3 eingegangen wird. Für die Methode, die wir verwenden werden, muß die Vollständigkeit von S vorausgesetzt werden.

Wir wollen die S-Einheitengruppe U_K^S etwas genauer betrachten. Wählt man eine Basis $\alpha_1\mathfrak{o}_K, \ldots, \alpha_s\mathfrak{o}_K$ von H_K^S, so sind die α_i unabhängige Nichteinheiten in U_K^S. Jedes $\alpha \in U_K^S$ läßt sich offenbar bis auf eine Einheit durch die α_i eindeutig darstellen. Daraus ergibt sich die Isomorphie

$$U_K^S \simeq H_K^S \times U_K \tag{3.2}$$

und mit dem Einheitensatz folgt:

Satz 3.1.3 *Die S-Einheitengruppe U_K^S wird von $s+r+1$ algebraischen Zahlen erzeugt und ist modulo Torsionseinheiten sogar frei vom Rang $s+r$.*

Wir haben m S-Relationen $\alpha_1, \ldots, \alpha_m$ vorliegen. Aufgrund der genannten Rangzahlen können davon höchstens s Relationen modulo Einheiten unabhängig sein. Für $m > s$ lassen sich also S-Einheiten kombinieren, die $\mathfrak{o}_K$ in H_K^S entsprechen, folglich Einheiten sind. Bezeichnen wir mit U^S das Erzeugnis der gefundenen Relationen in U_K^S, so ist die Einheitengruppe, die wir daraus ableiten können, gleich $U = U^S \cap U_K$. Zur Bestimmung von U und U^S verwenden wir das S-Einheitengitter aus dem nächsten Abschnitt. Wie bei den Hauptidealen H_K^S stellt sich dann auch hier bei den Einheiten die Frage, wann $U = U_K$ ist. In Abschnitt 3.3 wird ein Abbruchkriterium angegeben, welches gleichzeitig $H = H_K^S$ und $U = U_K$ unter der Voraussetzung einer vollständigen Faktorbasis prüft.

Die Berechnung der Klassengruppe mit S-Relationen liefert also auch Einheiten. Wegen der Isomorphie 3.2 läßt sich die simultane Berechnung von H_K^S und U_K zusammenfassen als Berechnung der S-Einheiten U_K^S von K für eine vollständige Faktorbasis S. Allerdings können wir S nicht ganz beliebig wählen. Aufgrund der Methoden, mit denen wir S-Relationen bestimmen werden, muß S aus Primidealen mit kleinen Normen bestehen. Dazu kommen wir später. Es sei noch angemerkt, daß ein Erzeuger von TU_K leicht im voraus oder extra berechnet werden kann — siehe [16] —, so daß wir uns nur um unabhängige S-Einheiten zu kümmern brauchen.

3.2 S-Einheitengitter

Im vorigen Abschnitt wurde gezeigt, daß die S-Einheitengruppe modulo Torsionseinheiten frei vom Rang $s+r$ ist. In diesem Abschnitt wollen wir ein zu

U_K^S/TU_K isomorphes vollständiges Gitter im $\mathbb{R}^{s+r}$ definieren. Durch Kombination von Methoden der Abschnitte 2.1 und 2.3 und mit Hilfe dieses Gitters können wir dann eine Basis des Erzeugnisses endlich vieler S-Einheiten in U_K^S/TU_K berechnen — und zwar bestehend aus unabhängigen S-Relationen und unabhängigen Einheiten. Für die Faktorbasis S müssen in diesem Abschnitt keine besonderen Eigenschaften vorausgesetzt werden.

Es wurde bereits der Homomorphismus $L : K^\times \longrightarrow \mathbb{R}^r$ definiert, welcher unabhängige Einheiten auf $\mathbb{R}$-linear unabhängige Vektoren abbildet. Wir wollen jedoch auch S-Einheiten vernünftig abbilden, die keine Einheiten sind. Hierfür ist L alleine nicht geeignet. Für solche S-Relationen wurde oben $\nu_S : I_K \longrightarrow \mathbb{Z}^s$ mit analogen Eigenschaften wie L definiert. Einheiten werden aber hierdurch auf den Nullvektor abgebildet. Den passenden Homomorphismus erhalten wir durch Kombination von ν_S und L:

$$\Phi_K^S : U_K^S \longrightarrow \mathbb{Z}^s \times \mathbb{R}^r,\ x \longmapsto \begin{pmatrix} \nu_S(x\mathfrak{o}_K) \\ L(x) \end{pmatrix}.$$

Bei Φ_K^S handelt es sich um einen Homomorphismus der multiplikativen Struktur von U_K^S in die additive Struktur von $\mathbb{Z}^s \times \mathbb{R}^r$ mit Kern TU_K. Letzteres gilt, da die Elemente des Kerns Einheiten sein müssen, deren Konjugiertenbeträge sämtlich 1 sind, und dies erfüllen genau die Torsionseinheiten. Also besteht die Isomorphie

$$U_K^S/TU_K \simeq \Phi_K^S(U_K^S).$$

Definition und Satz 3.2.1 *$\Phi_K^S(U_K^S)$ ist ein vollständiges Gitter im $\mathbb{R}^{s+r}$, das S-Einheitengitter von K genannt wird. Die Gitterdeterminante von $\Phi_K^S(U_K^S)$ ist $h_K^S R_K$.*

Beweis: Für die erste Aussage muß gezeigt werden, daß in U_K^S unabhängige Elemente durch Φ_K^S in $\mathbb{R}$-linear unabhängige Vektoren überführt werden. Da U_K^S/TU_K frei vom Rang $s+r$ ist, handelt es sich dann beim Bild von U_K^S unter Φ_K^S um ein vollständiges Gitter im $\mathbb{R}^{s+r}$.
Seien $\alpha_1, \ldots, \alpha_m \in U_K^S$ zunächst beliebige S-Einheiten und bezeichne, analog dem vorigen Abschnitt, mit U^S das Erzeugnis der α_i in U_K^S, mit H das Bild von U^S unter $x \mapsto x\mathfrak{o}_K$ und mit U die erzeugte Einheitengruppe $U^S \cap U_K$. Wir betrachten die Matrix $B \in \mathbb{R}^{(s+r)\times m}$, die von den Spalten $\Phi_K^S(\alpha_1), \ldots, \Phi_K^S(\alpha_m)$ gebildet wird und nennen sie die Relationsmatrix von $\alpha_1, \ldots, \alpha_m$. Der obere Teil von B ist aus $\mathbb{Z}^{s\times m}$. Es gibt eine unimodulare Matrix $T \in \mathbb{Z}^{m\times m}$, so daß dieser Teil durch Multiplikation mit T von rechts in eine untere Hermite Normalform H_α überführt wird, deren Rang mit m_0 bezeichnet sei. Die ersten m_0 Spalten von H_α sind $\mathbb{R}$-linear unabhängig, die anderen Spalten sind Nullspalten. Dies vor Augen wenden wir T von rechts auf B an, erhalten die transformierte Relationsmatrix C und erkennen, daß die ersten m_0 Spalten von C offensichtlich ebenfalls linear

unabhängig sind. Die restlichen Spalten korrespondieren aufgrund der Nullen im $\mathbb{Z}$-Anteil mit Einheiten in U_K^S. Die transformierte Relationsmatrix hat also die Form

$$C = \left(\begin{array}{c|c} H_\alpha & 0 \\ \hline * & C_2 \end{array} \right)$$

mit $H_\alpha \in \mathbb{Z}^{s \times m_0}$ in Hermite Normalform mit Rang m_0 und $C_2 \in \mathbb{R}^{r \times m_1}$, wobei $m_1 = m - m_0$. Wir wenden nun die unimodulare Transformation T — als Potenzprodukt — auf die α_i an und bezeichnen das Ergebnis mit $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_m$. Die unimodulare Transformation schadet nichts; die $\widetilde{\alpha}_i$ erzeugen dieselbe Gruppe wie die α_i, nämlich U^S. Wir erkennen ferner, daß C die Spalten $\Phi_K^S(\widetilde{\alpha}_1), \ldots, \Phi_K^S(\widetilde{\alpha}_m)$ besitzt. Bei den m_1 letzten $\widetilde{\alpha}_i$ handelt es sich demnach um Einheiten. Sie erzeugen U. Die m_0 ersten der $\widetilde{\alpha}_i$ sind S-Relationen. Ihr Erzeugnis in H_K^S ist H.
Unter der Annahme, daß die α_i unabhängig sind, wollen wir jetzt zeigen, daß der Rang von B bzw. C gleich m ist. Wir wissen bereits, daß die ersten m_0 Spalten $\mathbb{R}$-linear unabhängig sind. Die Eigenschaft der Abbildung L, unabhängige Einheiten auf $\mathbb{R}$-linear unabhängige Vektoren zu werfen, ergibt die zur Frage stehende lineare Unabhängigkeit der restlichen Spalten von C. Die letzten m_1 der $\widetilde{\alpha}_i$ sind nämlich unabhängige Einheiten. Hieraus folgt unmittelbar, daß auch B vollen Rang über $\mathbb{R}$ besitzt, und die erste Aussage ist bewiesen.
Aufgrund der Kästchengestalt der transformierten Relationsmatrix C folgt für $s + r$ unabhängige S-Einheiten α_i, daß

$$|\det C| = |\det H_\alpha||\det C_2| = (I_K^S : H)\,\mathrm{Reg}(U).$$

Aus dieser Gleichung folgt die zweite Aussage. □

Das im Beweis Gesagte lehrt, daß wir durch die Bildung einer Hermite Normalform des oberen Teils der Relationsmatrix bzw. durch Anwenden einer unimodularen Transformation S-Relationen und Einheiten trennen können. Genauer gesagt erhält man eine Basis von H und ein Erzeugendensystem für U. Der Index $(I_K^S : H)$ — falls der Rang von H bzw. H_α gleich s ist — ist das Produkt der Diagonalelemente von H_α. In dieser Matrix sammelt sich die Information über die Klassengruppe. Insbesondere ist die Determinante bzw. der Index ein ganzzahliges Vielfaches der S-Klassenzahl.

Wir müssen allerdings eine Basis von U kennen, um den Rang und bei Rang gleich r auch den Regulator von U bestimmen zu können. Der Regulator von U ist in diesem Fall ein ganzzahliges Vielfaches von R_K. Sind also beliebige Einheiten $\varepsilon_1, \ldots, \varepsilon_m$ gegeben, so können wir sukzessive für $i = 1, \ldots, m$ Basen der Erzeugnisse der $\varepsilon_1, \ldots, \varepsilon_i$ mit Hilfe von Φ_K^S bzw. L ausrechnen. Zur i-ten Basis nehmen wir ε_{i+1} dazu und verwenden den MLLL-Algorithmus, um die $(i+1)$-te Basis zu bestimmen. Dieses Vorgehen wurde schon am Ende des Abschnitts 2.3 erläutert.

Mit Hilfe der beschriebenen Methoden kann man zu gegebenen S-Einheiten das von ihnen erzeugte Teilgitter des S-Einheitengitters bestimmen.

Definition 3.2.2 *Die durch Weglassen der Nullspalten aus der unteren Hermite Normalform der Matrix* $(\nu_S(\alpha_i))_{1\le i\le m}$ *entstehende Matrix* H_α *nennen wir die Klassengruppenmatrix der* α_i. *Eine Matrix* B_α, *für die*

$$(\alpha_1,\ldots,\alpha_m)\,B_\alpha = (\mathfrak{p}_1,\ldots,\mathfrak{p}_s)\,H_\alpha$$

ist, heißt Relationsbasismatrix der α_i. *Eine Matrix* U_α, *für die* $(\alpha_1,\ldots,\alpha_m)\,U_\alpha$ *eine Basis von* U *ist, wird Einheitenmatrix der* α_i *genannt.*

Algorithmus 3.2.3 *(Berechnung des* S*-Einheitengitters)*

Eingabe: S*-Einheiten* $\alpha_1,\ldots,\alpha_m$.

Ausgabe: Die Klassengruppenmatrix H_α, *eine Relationsbasismatrix* B_α *und eine Einheitenmatrix* U_α *der* $\alpha_1,\ldots,\alpha_m$.

1. *(Initialisierung) Setze* $L_\alpha \leftarrow ()$ *Matrix mit* r *Zeilen und* 0 *Spalten,* $H_\alpha \leftarrow ()$ *Matrix mit* s *Zeilen und* 0 *Spalten,* $B_\alpha \leftarrow ()$ *Matrix mit* 0 *Zeilen und Spalten,* $U_\alpha \leftarrow ()$ *Matrix mit* 0 *Zeilen und Spalten und schließlich* $i \leftarrow 1$.

2. *(Füge* α_i *hinzu) Sei* k *die Spaltenzahl von* U_α. *Erweitere* $L_\alpha \leftarrow (L_\alpha\,|\,L(\alpha_i))$, $H_\alpha \leftarrow (H_\alpha\,|\,\nu_S(\alpha_i))$, $B_\alpha \leftarrow \begin{pmatrix} B_\alpha & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \in \mathbb{Z}^{i\times i}$ *und* $U_\alpha \leftarrow \begin{pmatrix} U_\alpha \\ \mathbf{0} \end{pmatrix} \in \mathbb{Z}^{i\times k}$.

3. *(Hermite Reduktion) Bilde die untere Hermite Normalform von* H_α *mittels Transformationsmatrix* T: $H_\alpha \leftarrow H_\alpha T$. *Setze* $B_\alpha \leftarrow B_\alpha T$.

4. *(Einheit gefunden?) Wenn die letzte Spalte von* H_α *eine Nullspalte ist, wurde eine Einheit gefunden. Ist dies nicht der Fall, mache bei Schritt 7 weiter. Ansonsten entferne diese Spalte von* H_α. *Entferne auch die letzte Spalte von* B_α *und nenne sie* u.

5. *(Neue Einheit ist Torsionsenheit?) Wenn* $L_\alpha u$ *der Nullvektor ist, wurde eine Torsionseinheit gefunden. Gehe zu Schritt 7.*

6. *(MLLL-Reduktion) Setze* $U_\alpha \leftarrow (U_\alpha\,|\,u)$. *Bestimme mit Hilfe des MLLL-Algorithmus angewendet auf* $L_\alpha U_\alpha$ *eine Transformationsmatrix* T, *so daß die Spalten von* $L_\alpha U_\alpha T$ *eine Basis des von den Spalten von* $L_\alpha U_\alpha$ *aufgespannten Gitters sind. Setze* $U_\alpha \leftarrow U_\alpha T$.

7. *(Nächste* S*-Einheit) Wenn* $i = m$ *Ausgabe von* $H_\alpha, B_\alpha, U_\alpha$ *und terminiere. Setze sonst* $i \leftarrow i+1$ *und gehe zu Schritt 2.*

Wir wollen einige Bermerkungen zu diesem Algorithmus machen:

Die Nullen in Schritt 2 stehen für Matrizen variabler Zeilen- und Spaltenzahl mit lauter Nulleinträgen. Für $i = 1$ beispielsweise wird $B_\alpha = (1)$ gesetzt.

Die am Ende der MLLL-Reduktion neuberechnete Einheitenmatrix U_α sollte bei zu großen Einträgen LLL-reduziert werden.

Der Test auf Torsionseinheit und die MLLL-Reduktion werden mit reeller Arithmetik ausgeführt. Die dabei verwendete Präzision muß den $\alpha_1, \ldots, \alpha_m$ und insbesondere auch der Größe der Koeffizienten von U_α und u angepaßt werden. Gegebenenfalls ist L_α ganz neu zu berechnen. Im Torsionstest prüfen wir, ob die Einträge von $L_\alpha u$ betraglich kleiner sind als einem gewissen $\varepsilon > 0$, welches von der Präzision abhängt.

Das ausschließliche Arbeiten mit den Transformationmatrizen B_α und U_α ist essentiell. Die Einträge von B_α und U_α sind nämlich aufgrund 3.2.2 als Exponenten von Potenzprodukten der α_i zu interpretieren. Die S-Relationen und Einheiten, die man daraus erhält, sind in der Regel keineswegs mehr gut konditioniert. Die direkte Berechnung von $L_\alpha u$ über $L(\alpha)$ mit $\alpha = (\alpha_1, \ldots, \alpha_m)\, u$ ist daher sehr ungenau und erfordert eine wesentlich höhere Präzision. Allerdings wird die Berechnung dieser Potenzprodukte bereits bei bescheidenen Einträgen in B_α und U_α zeitintensiv oder ist gar nicht mehr möglich. Für etwas kompliziertere Beispiele werden die Einträge von B_α und U_α aber meistens ziemlich groß. Damit können wir auf direktem Wege leider auch keinen algebraischen Test auf Torsioneinheit durchführen.

Wir werden Algorithmus 3.2.3 nicht ganz in der hier dargestellten Form einsetzen. Vielmehr entstehen unsere S-Einheiten $\alpha_1, \ldots, \alpha_m$ der Reihe nach, und mit jeder neuen S-Einheit rufen wir Algrithmus 3.2.3 unter Berücksichtigung der schon eingespeisten S-Einheiten auf. Außerdem kennen wir schon $\nu_S(\alpha_i)$ und können dies an Algorithmus 3.2.3 übergeben.

Praktische Versuche zeigen, daß man Algorithmus 3.2.3 nach Möglichkeit nur für Faktorbasen mit nicht viel mehr als 200 Idealen anwenden sollte. Schließlich ist sukzessive die Hermite Normalform einer $s \times m$-Matrix zu berechnen, wobei m mitunter das doppelte oder dreifache von s beträgt. Außerdem müssen $m \times m$-Transformationsmatrizen gehalten werden, deren Einträge groß werden können. Die Zeit, die von Algorithmus 3.2.3 bei solchen großen Faktorbasen benötigt wird, steht gewöhlich in keinem sinnvollen Verhältnis zur Zeit, die die Berechnung der Faktorbasis und der Relationen erfordert.

3.3 Abbruchbedingungen

Mit Algorithmus 3.2.3 kann man das von einigen S-Einheiten erzeugte Teilgitter des S-Einheitengitters bestimmen. Wir benötigen nun ein Kriterium, mit dem entschieden werden kann, wann das volle S-Einheitengitter bestimmt wurde. Hierzu gibt es zwei Methoden.

p-ter Wurzeltest

Wir bezeichnen mit H wieder das Erzeugnis einiger S-Einheiten in H_K^S und setzen voraus, daß H in H_K^S endlichen Index besitzt. Die Idee der ersten Methode basiert auf der Tatsache, daß zwischen H und I_K^S nur endlich viele Zwischengruppen liegen können, die mit I_K^S ebenfalls frei sind. Wir bestimmen für jede dieser Gruppen eine Basis. Eine solche Basis besteht aus Idealen, von denen zunächst unbekannt ist, ob sie aus H_K^S sind. Dies entscheiden wir dann mit Hilfe eines Hauptidealtests. Stellt sich heraus, daß alle Basisideale Hauptideale sind, so haben wir eine Obergruppe von H gefunden, die ganz in H_K^S enthalten ist. Allerdings macht man sich mit dieser Vorgehensweise zu viel Arbeit. Insbesondere testet man natürlich nicht alle Zwischengruppen ab, sondern nur die jeweils nächstgrößeren von H. Auch kann man den Hauptidealtest durch Ausnutzung der bereits berechneten Informationen wesentlich günstiger ausführen als für beliebig gegebene Ideale. Dazu muß aber ein p-maximales Einheitensystem aus r unabhängigen Einheiten bekannt sein. Wir nennen diese Methode den „p-ten Wurzeltest“. Es handelt sich hierbei nicht nur um ein reines Testkriterium, sondern liefert im Fall, daß H noch nicht maximal ist, ein größeres H zurück. Die genaue Darstellung und Durchführung der beschriebenen Ideen läßt sich in in [16, 15, 21] nachlesen.

Eulerprodukt

Wir kommen zur zweiten Methode, der Methode des „Eulerprodukts“, auf die wir uns in dieser Arbeit ausschließlich stützen wollen. Für diese Methode muß die Vollständigkeit der Faktorbasis vorausgesetzt werden, denn wir benötigen ganzzahlige Vielfache von h_K und R_K bzw. eine Untergruppe endlichen Index von U_K^S/TU_K. Diese Vielfache werden bei Eingabe geeigneter S-Relationen von Algorithmus 3.2.3 geliefert. Die zugrundeliegende Idee ist nun einfach. Wir können nämlich das Produkt $h_K R_K$ auf analytischem Weg approximieren. Durch Vergleich mit dem von uns berechneten Vielfachen dieses Produkts läßt sich ganz einfach feststellen, ob wir mit der berechneten Untergruppe von U_K^S/TU_K schon ganz U_K^S/TU_K erreicht haben oder nicht. Die Approximation von $h_K R_K$ beruht auf folgenden Definitionen und Sätzen:

Definition und Satz 3.3.1 *Wir definieren die Dedekindsche Zetafunktion ζ_K eines Zahlkörpers K für $Re(s) > 1$ durch*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

wobei sich die Summe über alle ganzen Ideale erstreckt. Die Reihe $\zeta_K(s)$ ist absolut und gleichmäßig konvergent im Bereich $Re(s) \geq 1+\delta$ für jedes $\delta > 0$. Im Bereich $Re(s) > 1$ besitzt ζ_K die Darstellung

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}},$$

wobei sich das Produkt über alle Primideale von K erstreckt. Die Dedekindsche Zetafunktion ζ_K hat eine analytische Fortsetzung auf $\mathbb{C}\backslash\{1\}$.

Satz 3.3.2 (Analytische Klassenzahlformel) *Wir bezeichnen wie üblich mit (r_1, r_2) die Signatur, mit D_K die Diskriminante, mit h_K und R_K Klassenzahl und Regulator und mit w_K die Anzahl der Torsionseinheiten von K. Die Dedekindsche Zetafunktion ζ_K hat in $s = 1$ einen einfachen Pol mit dem Residuum*

$$\lim_{s\to 1} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|D_K|}}.$$

Beweis: Zum Beweis dieser Sätze siehe [13], Kapitel VIII Paragraph 5. □

Satz 3.3.3 *Für das Residuum der Zetafunktion ζ_K gilt*

$$\lim_{s\to 1} (s-1)\zeta_K(s) = \prod_{p} \frac{(1-p^{-1})}{\prod_{\mathfrak{p}\,|\,p}(1 - N(\mathfrak{p})^{-1})},$$

wobei p der Reihe nach alle Primzahlen durchläuft.

Beweis: Zum Beweis siehe [23]. Ein wesentliches Argument wird aber auch im nächsten Abschnitt gezeigt. □

Dieser Satz motiviert die folgende Definition:

Definition 3.3.4 *Unter dem Eulerprodukt EP_K von K verstehen wir das Produkt auf der rechten Seite der Gleichung in Satz 3.3.3. Für $x \in \mathbb{Z}^{\geq 0}$ definieren wir $EP_K(x)$ durch*

$$EP_K(x) = \prod_{p \leq x} \frac{(1-p^{-1})}{\prod_{\mathfrak{p}\,|\,p}(1 - N(\mathfrak{p})^{-1})}.$$

Die Berechnung von $h_K R_K$ erfolgt nun durch Approximation des Eulerprodukts und Umstellen der analytischen Klassenzahlformel. Es sei noch bemerkt, daß es in der Literatur „das" Eulerprodukt nicht gibt. Sämtliche Darstellungen von Zetafunktionen als Produkt über Primideale werden üblicherweise als Eulerprodukt bezeichnet.

Von großem Interesse ist jetzt natürlich die Konvergenzgeschwindigkeit unseres Eulerprodukts. Hierzu werden im nächsten Abschnitt Betrachtungen angestellt.

Eine sinnvolle Approximation von $h_K R_K$ ist übrigens nur deshalb möglich, weil die Menge der von uns berechneten Kandidaten für $h_K R_K$ eine Diskretheitsbedingung erfüllt. Wir betrachten $M = \{\log(k\, h_K R_K) \mid k \in \mathbb{Z}^{\geq 1}\}$. Die Approximation von $h_K R_K$ bzw. $\log(h_K R_K)$ soll so genau sein, daß dadurch $\log(h_K R_K)$ eindeutig als Minimum von M charakterisiert wird. Weil der Abstand des Minimums zum nächstgrößeren Element $\log(2)$ beträgt, genügt es, wenn die Approximation im Intervall $[\,-\frac{1}{2}\log(2) + \log(h_K R_K), \frac{1}{2}\log(2) + \log(h_K R_K)\,[$ liegt. Der Wert $\log(h_K R_K)$ wird dann eindeutig durch die Eigenschaft charakterisiert, von der Approximation einen Abstand kleiner gleich $\frac{1}{2}\log(2)$ zu haben. Daraus ergibt sich das folgende Lemma:

Lemma 3.3.5 *Für ein geeignetes $x \in \mathbb{Z}^{\geq 1}$ gelte*

$$\frac{1}{\sqrt{2}} \leq \frac{EP_K(x)}{EP_K} < \sqrt{2}$$

und sei $k \in \mathbb{Z}^{\geq 1}$. Dann besteht die Äquivalenz:

$$k = 1 \quad \Leftrightarrow \quad k\, EP_K \leq \sqrt{2}\, EP_K(x).$$

Die ausreichende Approximation des Eulerprodukts stellt in der Praxis kein Problem dar. Für die Erzeugung der Faktorbasis gibt man sich nämlich üblicherweise eine relativ kleine Schranke vor und berechnet alle Primideale zu Primzahlen unterhalb dieser Schranke. In der Regel ist es vollkommen genügend, diese Primideale zur Berechnung des Eulerprodukts heranzuziehen. Nur bei Körpern mit sehr kleiner Diskriminante kann es nötig sein, weitere Primideale hinzuzunehmen. Bei sämtlichen bisher behandelten Körpern reicht es aus, das Eulerprodukt auf diese Weise unter Verwendung mindestens der Primideale über den ersten 150 Primzahlen zu berechnen. Anstelle von Lemma 3.3.5 wurde hierbei sogar die Bedingung $0.9 \leq k\, EP_K / EP_K(x) \leq 1.1$ getestet. Praktische Untersuchungen zeigen, daß $EP_K(x)$ für wachsendes x zunächst ziemlich schnell zu konvergieren scheint, dann jedoch in einem gewissen kleinen Bereich pendelt, auch wenn x schon verhältnismäßig groß geworden ist. Aus diesem Grund ist es unangenehm, das Eulerprodukt bei Kenntnis des Regulators zur Bestimmung von h_K zu benutzen. Hierfür ist nämlich eine wesentlich höhere Approximationsgenauigkeit vonnöten.

3.4 Konvergenzverhalten des Eulerprodukts

In diesem Abschnitt soll über das Konvergenzverhalten des Eulerprodukts berichtet werden, und zwar mit und ohne Annahme der verallgemeinerten Riemannschen Vermutung (GRH). Die Darstellung lehnt sich an [4] an. Wir gehen wie folgt vor: Zuerst wird das Restglied des Eulerprodukts nach Logarithmierung als Summe dreier Reihen dargestellt. Die Konvergenz zweier dieser Reihen ist absolut und entsprechend unproblematisch. Die dritte Reihe ist nicht absolut konvergent. Ihr Konvergenzverhalten entspricht einer Aussage über die asymptotische Verteilung von Primidealen und wir bestimmen es mit zwei „effektiven“ Versionen des Primidealsatzes.

Geeignete Darstellung des Eulerprodukts

Wir setzen $E(p) = (1-p^{-1})\prod_{\mathfrak{p}\,|\,p}(1-N(\mathfrak{p})^{-1})^{-1}$ und nennen $E(p)$ den Eulerfaktor von p. Wir definieren das Restglied des Eulerprodukts für $x \geq 2$ durch

$$T(x) = \prod_{p>x} E(p).$$

Die Aufgabe besteht nun darin, zu vorgegebenem $\varepsilon > 0$ ein x zu finden, so daß $|\log(T(x))| < \varepsilon$ ist. Laut Lemma 3.3.5 interessiert uns besonders $\varepsilon = \log(\sqrt{2})$.

Wir betrachten zunächst die Eulerfaktoren etwas genauer und wollen dann $T(x)$ logarithmieren. Sei $p = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$ und $f_i = f(\mathfrak{p}_i\,|\,p)$. Wir setzen $f_g = \sum_i f_i$. Dann läßt sich $E(p)$ schreiben als

$$E(p) = \frac{p^{f_g-1}(p-1)}{\prod_{i=1}^{g}(p^{f_i}-1)}. \tag{3.3}$$

Wir fassen diesen Ausdruck für den Moment als eine rationale Funktion der Variablen p auf. Augenscheinlich ist das Nennerpolynom durch $p-1$ teilbar. Dividieren wir auch noch durch p^{f_g-1}, so erhalten wir

$$E(p) = \left(1 + \frac{a_1(p)}{p} + \ldots + \frac{a_{n-1}(p)}{p^{n-1}}\right)^{-1}, \tag{3.4}$$

wobei die $a_i(p) \in \mathbb{Z}$ eindeutig durch die f_i und somit durch das Zerlegungsverhalten von p (als Primzahl) bestimmt werden. Hierbei sind $a_i(p) = 0$ für $f_g \leq i \leq n-1$. Wegen $\sum_i f_i \leq n$ gibt es nur endlich viele Konstellationen $(f_1, \ldots, f_g)$ für verschiedene Primzahlen p und somit auch nur endlich viele $(a_1(p), \ldots, a_{n-1}(p))$. Aus Gründen, die etwas später klar werden, interessieren wir uns speziell für den Wert von $a_1(p)$. Sei g_1 die Anzahl der Primideale mit Grad 1 über p. Ein scharfer Blick auf das Nennerpolynom in (3.3) zeigt, daß es die Spur $-g_1$ besitzt, denn schließlich ist die Spur das Negative der Summe der Nullstellen eines Polynoms. Da nach der Division des Nennerpolynoms durch $p-1$ einmal eine Eins als Nullstelle verloren geht, folgt $a_1(p) = 1 - g_1$.

Wir wollen jetzt $T(x)$ logarithmieren. Für $n \geq 2$ und $p \geq 2$ ist $|E(p)^{-1} - 1| < 1$. Für $x \geq 2$ erhalten wir also

$$-\log(T(x)) = \sum_{p>x} \log\left(1 + \frac{a_1(p)}{p} + \ldots + \frac{a_{n-1}(p)}{p^{n-1}}\right),$$

und mit Hilfe der Reihenentwicklung für den Logarithmus ergibt sich

$$\begin{aligned}
-\log(T(x)) &= \sum_{p>x}\sum_{j=1}^{\infty}\left(\frac{a_1(p)}{p}+\ldots+\frac{a_{n-1}(p)}{p^{n-1}}\right)^j \frac{(-1)^{j+1}}{j} \\
&= \sum_{p>x}\frac{a_1(p)}{p}+\sum_{p>x}\frac{1}{p^2}\sum_{k=2}^{n-1}\frac{a_k(p)}{p^{k-2}}+\sum_{p>x}\sum_{j=2}^{\infty}\frac{(-1)^{j+1}}{jp^j}\left(\sum_{k=1}^{n-1}\frac{a_k(p)}{p^{k-1}}\right)^j .
\end{aligned}$$

In der letzten Gleichung wurde der Term für $j = 1$ aus der Reihe darüber extra geschrieben und so aufgeteilt, daß die Brüche, in denen p als einfache Potenz im Nenner auftritt, die erste Reihe bilden. In der zweiten Reihe sind die übrigen Brüche zusammengefaßt und in der dritten Reihe treten die restlichen Terme für $j > 1$ auf. Diese Gleichung ist verifiziert, wenn die Konvergenz der drei Reihen nachgewiesen ist. Wir betrachten jetzt die zweite und dritte Reihe. Diese sind nämlich absolut konvergent — wie gleich gezeigt wird —, da p mindestens im Quadrat in den Nennern auftritt. Aufgrund der endlich vielen Möglichkeiten für $(a_1(p), \ldots, a_{n-1}(p))$ gibt es nur von n abhängige Konstanten c_1 und c_2, so daß

$$\left|\sum_{k=2}^{n-1} a_k(p)p^{-k+2}\right| \le c_1 \quad \text{und} \quad \left|\sum_{k=1}^{n-1} a_k(p)p^{-k+1}\right| \le c_2$$

für jedes $p > x$ gilt. Konkret läßt sich $|a_k(p)|$ beispielsweise durch 2^n nach oben abschätzen und somit ergibt sich 2^{n+1} als möglicher Wert für c_1 und c_2. Wir fordern, daß ab jetzt $x \ge 2c_2$ gilt. Dann

$$\sum_{p>x}\frac{1}{p^2}\left|\sum_{k=2}^{n-1}\frac{a_k(p)}{p^{k-2}}\right| \le \sum_{p>x}\frac{c_1}{p^2} \le \frac{c_1}{x}$$

und

$$\begin{aligned}
\sum_{p>x}\sum_{j=2}^{\infty}\frac{1}{jp^j}\left|\sum_{k=1}^{n-1}\frac{a_k(p)}{p^{k-1}}\right|^j &\le \sum_{p>x}\sum_{j=2}^{\infty}\left(\frac{c_2}{p}\right)^j \\
&\le \sum_{p>x}\frac{c_2^2}{p^2}\left(\frac{1}{1-c_2/p}\right) \le \frac{2c_2^2}{x},
\end{aligned}$$

wobei die Abschätzung $\sum_{p>x} 1/p^2 < 1/x$ zu beachten ist, die leicht durch Integrieren bewiesen werden kann.

Verwendung des Primidealsatzes

Es bleibt wie angekündigt die Konvergenz der Reihe

$$\sum_{p>x} a_1(p)/p \tag{3.5}$$

zu zeigen. Eine Abschätzung wie oben ist für diese Reihe nicht möglich, denn $\sum_{p>x} 1/p$ ist divergent. Dies bedeutet, daß besondere Eigenschaften der $a_1(p)$ ausgenutzt werden müssen. Daher definieren wir

$$A(t) = \sum_{p \leq t} a_1(p)$$

und werden gleich das Verhalten von $A(t)$ für wachsendes t untersuchen. Die Verbindung zu (3.5) stellen wir mit Hilfe der folgenden Stieltjes-Integrale her, wobei $\lim_{t\to\infty} A(t)/t = 0$ vorausgesetzt sei:

$$\sum_{p>x} \frac{a_1(p)}{p} = \int_x^\infty \frac{1}{t}\, dA(t) = -\frac{A(x)}{x} + \int_x^\infty \frac{A(t)}{t^2}\, dt. \tag{3.6}$$

Durch Einsetzen oberer Abschätzungen für $|A(t)|$ können wir feststellen, ob die rechte Seite überhaupt konvergiert. Ist dies der Fall, so konvergiert auch die linke Seite und man erhält außerdem die gesuchten Abschätzungen für (3.5).

Wir bezeichnen für einen beliebigen Zahlkörper K die Anzahl der Primideale von K mit Norm kleiner gleich einer positiven Zahl t mit $\pi_K(t)$ und die Anzahl der Primideale vom Grad eins unter den letzteren mit $\pi_K^{(1)}(t)$. Weil $a_1(p) = 1 - g_1$, wenn g_1 gleich der Anzahl der Primideale über p in K vom Grad eins ist, kann man $A(t)$ schreiben als

$$A(t) = \pi_{\mathbb{Q}}(t) - \pi_K^{(1)}(t)$$

und daher

$$|A(t)| \leq |\pi_{\mathbb{Q}}(t) - \pi_K(t)| + |\pi_K(t) - \pi_K^{(1)}(t)|. \tag{3.7}$$

Satz 3.4.1 (Primidealsatz) *Sei K ein algebraischer Zahlkörper vom Grad n mit Diskriminante D_K. Wir definieren*

$$\mathrm{li}(t) = \int_2^t \frac{du}{\log u}.$$

Für beliebiges $\varepsilon > 0$ gibt es eine von K unabhängige aber von ε abhängige Konstante $c = c(\varepsilon) > 0$, so daß

$$\pi_K(t) = \mathrm{li}(t) + O(Dt\log(t)^2 \exp(-cn\log(t)^{\frac{1}{2}}/D))$$

mit $D = n^3 c^{-n} |D_K|^\varepsilon$. Die Konstante des O-Terms hängt nicht von K ab. Setzen wir die verallgemeinerte Riemannsche Vermutung für ζ_K voraus, so gilt für $t \geq 2$:

$$|\pi_K(t) - \mathrm{li}(t)| \leq \sqrt{t}\log(t)\,(\log(|D_K|)c_3(t) + nc_4(t))$$

mit $c_3(t) = 1/(\pi\log(t)) + 5.3/\log(t)^2$ und $c_4(t) = 1/(2\pi) + 2/\log(t)$.

Beweis: Die erste Aussage ist ein Spezialfall des in [6] bewiesenen Satzes. Die zweite Aussage ist ein Spezialfall von Satz 3 aus [14]. □

Die Fehlerabschätzung von $\pi_K(t)$ ohne Voraussetzung der GRH ist nicht die bestmögliche. Wir verwenden sie hier, weil die Abhängigkeit der Konstanten von n und D_K angegeben wird.

Lemma 3.4.2 *Für $t \geq 2$ gilt:*

$$|\pi_K(t) - \pi_K^{(1)}(t)| \leq \frac{n}{2}\pi_{\mathbb{Q}}(\sqrt{t}).$$

Außerdem ist

$$\lim_{t\to\infty} \pi_{\mathbb{Q}}(\sqrt{t})/(\sqrt{t}\log(t)) = 0$$

und

$$\lim_{t\to\infty} \sqrt{t}\log(t)/(t\log(t)^2 \exp(-c\log(t)^{\frac{1}{2}})) = 0$$

für $c \geq 0$.

Beweis: Besitzt $\mathfrak{p}$ vom Grad größer eins eine Norm kleiner gleich t, so liegt $\mathfrak{p}$ über einer Primzahl p mit $p \leq \sqrt{t}$. Über p können aber nur maximal $n/2$ solcher Primideale liegen. Für die erste Limes-Aussage ist zu beachten, daß $\mathrm{li}(t) = t/\log(t) + O(t/\log(t)^2)$, siehe [12] S. 372. Also strebt $\mathrm{li}(\sqrt{t})/(\sqrt{t}\log(t))$ für wachsendes t gegen Null. Für die zweite Limesaussage ist zu beachten, daß $\exp(c\log(t)^{\frac{1}{2}})$ schwächer wächst als $\sqrt{t} = \exp(\log(t)/2)$. □

Das Lemma besagt, daß die Primideale vom Grad größer eins „vernachlässigbar" sind. Ihre Anzahl wächst schwächer als der Fehlerterm von $\pi_K(t)$ mit GRH und ohne GRH.

Abschätzung mit GRH

Wir können (3.7) unter Verwendung des Primidealsatzes, des Lemmas und unter Annahme der GRH für $\zeta_{\mathbb{Q}}$ und ζ_K folgendermaßen nach oben abschätzen:

$$\begin{aligned} |A(t)| &\leq \sqrt{t}\log(t)\,(\log(|D_K|)c_3(t) + (n+1)c_4(t)) + \\ &\quad n\left(\mathrm{li}(\sqrt{t}) + \frac{1}{2}\sqrt[4]{t}\log(t)c_4(t)\right) \\ &\leq \sqrt{t}\log(t)\,\left(\frac{n}{2} + \log(|D_K|)c_3(t) + (n+1)c_4(t)\right), \end{aligned}$$

wobei die letzte Ungleichung für $t \geq 20$ gilt. Wir kürzen den geklammerten Ausdruck dieser Ungleichung mit $C(t)$ ab. Offensichtlich ist $C(t)$ monoton fallend. Beachtet man noch, daß $\int \sqrt{t}\log(t)/t^2\,dt = -(4+2\log(t))/\sqrt{t}$, so folgt aus (3.6) für $x \geq 20$:

$$\left|\sum_{p>x} \frac{a_1(p)}{p}\right| \leq C(x)\frac{4+3\log(x)}{\sqrt{x}}. \tag{3.8}$$

und schließlich

$$|\log(T(x))| \leq C(x)\frac{4+3\log(x)}{\sqrt{x}} + \frac{c_1+2c_2^2}{x}. \tag{3.9}$$

Mit dieser Ungleichung kann man die erforderliche Genauigkeit, bis zu der das Eulerprodukt approximiert werden muß, bestimmen. Die rechte Seite muß dazu, wie bereits erwähnt, kleiner als $\log(\sqrt{2})$ werden, was man für ausreichend großes x erreichen kann. Wir wollen jedoch auch wissen, wie sich die minimalen Werte für x bei festem Grad aber wachsender Diskriminante entwickeln. Wir setzen dazu die rechte Seite aus (3.9) gleich $\log(\sqrt{2})$ und bemerken, daß diese Seite für $x \geq 2$ streng monoton fallend in x ist. Hierdurch wird x als Funktion von D_K implizit definiert, also $x = x(D_K)$. Wenn $|D_K| \to \infty$, so gilt auch $x(D_K) \to \infty$.

Für $g, h : \mathbb{R} \longrightarrow \mathbb{R}$ schreiben wir $g(t) \sim h(t)$, wenn $\lim_{t\to\infty} g(t)/h(t) = 1$ ist. Mit dieser Notation und unter Beachtung, daß $x = x(D_K)$ und n fest ist, gilt offenbar

$$\left(\frac{\log(|D_K|)}{\log(x)}\left(\frac{1}{\pi}+\frac{5.3}{\log(x)}\right)+\frac{n+1}{2\pi}+\frac{n}{2}+\frac{2(n+1)}{\log(x)}\right)\frac{4+3\log(x)}{\sqrt{x}} \sim \log(\sqrt{2}),$$

also

$$\frac{3\pi^{-1}\log(|D_K|)}{\sqrt{x}} \quad\sim\quad \log(\sqrt{2}),$$

und daher

$$\frac{36}{(\pi\log(2))^2}\log(|D_K|)^2 \quad\sim\quad x.$$

Der Vorfaktor beträgt ungefähr 7.6. Für geeignet große Diskriminanten brauchen wir daher das Eulerprodukt nur bis beispielsweise $8\log(|D_K|)^2$ zu approximieren. Dieses asymptotisch gute Ergebnis ist leider im konkreten Fall nicht besonders gut. In $c_3(x)$ und $c_4(x)$ treten nämlich Terme der Form $1/\log(x)$ auf und diese Terme konvergieren extrem langsam: Wenn x als ein konstantes Vielfaches des Quadrats des Logarithmus von $|D_K|$ interpretiert wird, gilt $\log(x) \sim 2\log(\log(|D_K|))$. Für $n = 4$ und $D_K = 10^{40}$ beispielsweise muß x ungefähr $100\log(|D_K|)^2$ betragen, damit die Approximationsbedingung erfüllt ist. Interessant ist daher ein Ergebnis von Bach, welches besagt, daß das Eulerprodukt für jeden Zahlkörper nur bis $x = 12\log(|D_K|)^2$ approximiert werden muß, um im Schwankungsbereich $2^{\pm\frac{1}{2}}$ um EP_K zu liegen. Dies wird in [2] gezeigt.

Es sei noch angemerkt, daß in [4] die Abschätzung (3.8) auf anderem Weg als hier dargestellt erhalten wird. Insbesondere wird dort ein anderes $C(t)$ verwendet, in das Daten der normalen Hülle L von K bzw. der Galoisgruppe von L über $\mathbb{Q}$ einfließen. Daher ist es dort nicht möglich, einen expliziten Vorfaktor für die obige asymptotische Aussage anzugeben.

Abschätzung ohne GRH

Die Abschätzung von $|\log(T(x))|$ ist ohne Annahme von GRH für $\zeta_{\mathbb{Q}}$ und ζ_K schwieriger. In der Literatur ist hierüber nichts zu finden.

Wir geben uns jetzt das $\varepsilon > 0$ aus dem Primidealsatz fest vor. Weil die O-Konstante und c unbestimmt sind, können wir keine expliziten Werte für geeignete x angeben und sind von vorneherein am asymptotischen Verhalten von $x = x(D_K)$ interessiert. Aber auch hierfür gibt der Primidealsatz nicht genügend Information her: Die O-Aussage teilt nur mit, daß es von K unabhängige Konstanten C_0 und x_0 gibt, so daß für alle $x \geq x_0$ gilt:

$$|\pi_K(x) - \mathrm{li}(x)| \leq C_0 D x \log(x)^2 \exp(-cn \log(x)^{\frac{1}{2}}/D). \tag{3.10}$$

Hierbei ist $x_0 = x_0(n, D_K)$ und genaueres ist nicht bekannt. Wir wollen jetzt konkret mit dieser Ungleichung arbeiten, um das sich daraus ergebende asymptotische Verhalten für $x = x(D_K)$ analog wie oben zu bestimmen. Natürlich muß für ein korrektes Endresultat auch die Forderung $x(D_K) \geq x_0(n, D_K)$ berücksichtigt werden.

Der Fehlerterm von $\pi_{\mathbb{Q}}(x)$ ist von der Ordnung $c^{-1} x \log(x)^2 \exp(-c^2 \log(x)^{\frac{1}{2}})$. Dieser Ausdruck wird kleiner als der im O-Term von $\pi_K(x)$ für $x \geq 2$, wenn nur $|D_K|^{\varepsilon} \geq c^{n-1}/n^2$, was ab jetzt gelten soll. Also

$$|\pi_{\mathbb{Q}}(x) - \pi_K(x)| \leq 2C_0 D x \log(x)^2 \exp(-cn \log(x)^{\frac{1}{2}}/D) \tag{3.11}$$

für $x \geq \max\{x_0(n, D_K), x_0(1,1), 2\}$. Der Fehlerterm von $\pi_{\mathbb{Q}}(x)$ wächst nach Lemma 3.4.2 stärker als $n\pi_{\mathbb{Q}}(\sqrt{x})/2$. Aus diesem Grund gibt es ein $x_1 = x_1(n)$, so daß für $x \geq x_1$ gilt

$$\frac{n}{2}\pi_{\mathbb{Q}}(x) \leq c^{-1} x \log(x)^2 \exp(-c^2 \log(x)^{\frac{1}{2}}). \tag{3.12}$$

Wir fassen (3.11) und (3.12) zusammen und erhalten mit (3.7):

$$|A(x)| \leq (2C_0 + 1) D x \log(x)^2 \exp(-cn \log(x)^{\frac{1}{2}}/D) \tag{3.13}$$

für $x \geq \max\{x_0(n, D_K), x_0(1,1), x_1(n), 2\}$.

Die Ungleichung (3.13) zeigt, daß $\lim_{x\to\infty} |A(x)|/x = 0$. Da wir (3.6) anwenden wollen, muß die rechte Seite integriert werden. Kürzt man $\log(x)^{\frac{1}{2}}$ durch y ab und schreibt a für cn/D, so erhalten wir für das Integral

$$\int \frac{\log(x)^2 \exp(-cn \log(x)^{\frac{1}{2}}/D)}{x}\, dx$$

die Stammfunktion

$$-2\exp(-ay)\left(\frac{y^5}{a} + \frac{5y^4}{a^2} + \frac{20y^3}{a^3} + \frac{60y^2}{a^4} + \frac{120y}{a^5} + \frac{120}{a^6}\right). \tag{3.14}$$

Für $x \to \infty$ gilt auch $y \to \infty$ und (3.14) strebt gegen Null. Daher erkennt man, daß die Integrale aus (3.6), die Reihe (3.5) und auch das Eulerprodukt konvergieren.

Um die die rechte Seite von (3.6) zusammenzufassen, müssen wir die rechte Seite aus (3.13) durch x dividieren und zum Betrag von (3.14) multipliziert mit $(2C_0 + 1)D$ addieren. Der geklammerte Term wird dadurch um $y^4/2$ vergrößert und besitzt folgende Gestalt:

$$\frac{y^5}{a} + \frac{5y^4}{a^2} + \frac{y^4}{2} + \frac{20y^3}{a^3} + \frac{60y^2}{a^4} + \frac{120y}{a^5} + \frac{120}{a^6}.$$

Dann können wir in diesem Term jede der Potenzen von y durch y^5 ersetzen, dies vergrößert den Ausdruck, wenn $x \geq e$. Zusätzlich erweitern wir jeden der Koeffizienten auf 120. Wenn $|D_K|^\varepsilon \geq c^{n+1}/n^2$ ist , so gilt $a \leq 1$. Der Term wird also höchstens größer, wenn die Potenzen von a bzw. der Nenner 2 durch a^6 ersetzt werden. Durch eine ähnliche Schranke können wir $a^6 \leq 2/D$ erreichen. Wir bezeichnen das Maximum dieser Schranke und der Schranke für $|D_K|^\varepsilon$ vor (3.11), die nur von n abhängen, mit $D(n)$. Man erhält nach diesen Schritten die obere Abschätzung

$$\left|\sum_{p>x} a_1(p)/p\right| \leq 240(2C_0 + 1)\frac{\exp(-cny/D)y^5 D^6}{c^6 n^6}, \tag{3.15}$$

die für $x \geq \max\{x_0(n, D_K), x_0(1, 1), x_1(n), e\}$ und $|D_K|^\varepsilon \geq D(n)$ gültig ist.

Um $|\log(T(x))|$ abzuschätzen, muß noch der Fehlerterm, der durch die beiden absolut konvergenten Reihen gegeben wird, berücksichtigt werden. Er beträgt $(c_1 + 2c_2^2)/x$ wenn $x \geq 2c_2$, wobei c_1, c_2 nur von n abhängen. Weil dieser Term viel schneller fällt als (3.15) für wachsendes x und weil (3.15) monoton in $|D_K|$ wächst, gibt es ein $x_2 = x_2(n) \geq 2c_2$, für das (3.15) größer als $(c_1 + 2c_2^2)/x$ wird, wenn nur $x \geq x_2$ ist.

Wir setzen $x_3(n) = \max\{x_0(1, 1), x_1(n), x_2(n), e\}$, $C_1 = 480n^{12}c^{6(1-n)}(2C_0 + 1)$ und $b = c^{n+1}/n^2$. Dann gilt:

$$|\log(T(x))| \leq C_1 |D_K|^{6\varepsilon} \log(x)^{\frac{5}{2}} \exp(-b \log(x)^{\frac{1}{2}}/|D_K|^\varepsilon) \tag{3.16}$$

für $x \geq \max\{x_0(n, D_K), x_3(n)\}$ und $|D_K|^\varepsilon \geq D(n)$.

Wir wollen jetzt fordern, daß die rechte Seite von (3.16) bei gegebenem D_K für $x = x(D_K)$ echt kleiner $\log(\sqrt{2})$ ist, und das asymptotische Verhalten von $x(D_K)$ für wachsende Diskriminante beschreiben. Dazu definieren wir

$$x_4(n, D_K, \delta) = \exp\left(|D_K|^{2\varepsilon} \left[11 \log(|D_K|^\varepsilon) + 5 \log(\log(|D_K|^\varepsilon)) + \delta\right]^2 / b^2\right)$$

für ein $\delta > 0$. Setzt man $x_4(n, D_K, \delta)$ für x in (3.16) ein, so erhält man

$$\frac{C_1}{b^5 \exp(\delta)} \left[11 + 5 \log(\log(|D_K|^\varepsilon)) / \log(|D_K|^\varepsilon) + \delta / \log(|D_K|^\varepsilon)\right]^5 . \tag{3.17}$$

Dies konvergiert für $|D_K| \to \infty$ gegen $11^5 C_1 b^{-5} \exp(-\delta)$. Durch die geeignete Wahl von δ — abhängig nur von n — läßt sich erreichen, daß (3.17) für genügend großes $|D_K|$ unter Verwendung von $x = x_4(n, D_K, \delta)$ echt kleiner als $\log(\sqrt{2})$ wird. Hieraus resultiert eine weitere untere und nur von n und δ abhängige Schranke für den Diskriminantenbetrag.

Folgerung 3.4.3 *Es gibt $D_0 > 0$ und $\delta > 0$, so daß gilt: Wenn $x_0(n, D_K) \leq x_4(n, D_K, \delta)$ für $|D_K| \geq D_0$, so muß $EP_K(x)$ für maximal $x = x_4(n, D_K, \delta)$ berechnet werden, damit $|\log(EP_K) - \log(EP_K(x))| < \log(\sqrt{2})$ gilt.*

Beweis: Wir wählen δ wie oben passend. D_0 wird zuerst größer als das Maximum der bisherigen unteren Schranken für den Diskriminantenbetrag — die nur von n und mit einer Ausnahme auch von δ abhängen — gewählt. Dann vergrößern wir D_0 solange, bis $x_4(n, D_0, \delta)$ den Wert von $x_3(n)$ überschreitet. Setzen wir jetzt $x_0(n, D_K) \leq x_4(n, D_K, \delta)$ für $|D_K| \geq D_0$ voraus, so gilt (3.16) und durch Einsetzen von $x_4(n, D_K, \delta)$ für x in der rechten Seite von (3.16) erhält man $|\log(T(x_4(n, D_K, \delta)))| < \log(\sqrt{2})$. □

Weil das eingangs gewählte ε beliebig war, kann man unter Annahme der Voraussetzung von 3.4.3 für $\varepsilon/4$ auch $x_4(n, D_K, \delta) = \exp(|D_K|^\varepsilon)$ wählen, wobei D_0 eventuell vergrößert werden muß.

Bemerkungen

Unter der Annahme von GRH muß das Eulerprodukt $EP_K(x)$ bis zu einem x approximiert werden, welches mit der Diskriminante von der Ordnung $\log(|D_K|)^2$ wächst. Wird ein $\varepsilon > 0$ vorgegeben, so erhält man für x unter speziellen Voraussetzungen, aber ohne GRH, ein Wachstum der Ordnung $\exp(|D_K|^\varepsilon)$. Die letztere Aussage steht im Einklang mit einer Form des Primidealsatzes für normale Erweiterungen, die in [24] bewiesen wird. Dort wird ein O-Term angegeben, in dem die Konstanten nicht einmal mehr von D_K abhängig sind. Dies würde dazu führen, daß $x = x(D_K)$ konstant in D_K ist. Daher gibt es dort die Nebenbedingung $x \geq \exp(|D_K|^\varepsilon)$ mit beliebigem $\varepsilon > 0$. Diese Nebenbedingung spielt die Rolle des obigen $x_0(n, D_K)$ und stimmt mit unserem Wachstumsverhalten überein.

Daß die Reihe (3.5) nicht absolut konvergiert, kann man sich mit dem Dichtigkeitssatz von Tschebotareff klar machen. Daß sie konvergiert bedeutet also ein gewisses „oszillatorisches“ Gleichgewicht von Primzahlen, über denen Grad-eins Primideale liegen, und Primzahlen, über denen keine solchen Primideale liegen.

Beim Beweis des Primidealsatzes arbeitet man mit einer mit π_K verwandten Funktion ψ_K. Für diese Funktion erhält man mit funktionentheoretischen Mitteln eine sogenannte explizite Formel, aus der das zu beweisende asymptotische Verhalten problemlos abgeleitet werden könnte, träte dort nicht noch eine Reihe über die Nullstellen von ζ_K im Streifen $0 < \mathrm{Re}(s) < 1$ auf. Für $K = \mathbb{Q}$ beispielsweise hat diese Reihe die Gestalt $\sum_\alpha \frac{k_\alpha x^\alpha}{\alpha}$, wobei k_α die Ordnung des Pols von ζ'/ζ bei α bezeichnet. Es ist zu zeigen, daß sie schwächer wächst als x. Die verallgemeinerte Riemannsche Vermutung besagt nun für Dedekindsche Zetafunktionen ζ_K, daß aus $\zeta_K(s) = 0$ für $0 < \mathrm{Re}(s) < 1$ folgt $\mathrm{Re}(s) = \frac{1}{2}$, und dies hilft bei der Handhabung der Reihe. Wird nichts voraussetzt, so muß man im Streifen $0 < \mathrm{Re}(s) < 1$ spezielle nullstellenfreie Gebiete für ζ_K betrachten. Außer für den Fall $K = \mathbb{Q}$, siehe [19], scheint es keine unkonditionelle Version des Primidealsatzes mit expliziten von n und D_K abhängigen Konstanten zu geben.

3.5 Berechnung der Klassengruppenstruktur

Nachdem wir mit Hilfe des Eulerprodukts davon ausgehen, daß wir für eine vollständige Faktorbasis $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ genügend S-Relationen $\alpha_1, \ldots, \alpha_m$ gefunden haben, um das S-Einheitengitter zu erzeugen, und weiterhin die von Algorithmus 3.2.3 berechnete Klassengruppenmatrix H_α, die Relationsbasismatrix B_α und die Einheitenmatrix U_α vorzuliegen haben, wollen wir jetzt die eingangs geforderten Informationen über die Klassengruppe ermitteln. Die Einheitenmatrix ist hierfür nicht erforderlich.

Ausgangspunkt bildet die Gleichung

$$(\mathfrak{p}_1, \ldots, \mathfrak{p}_s)\, H_\alpha = (\alpha_1, \ldots, \alpha_m)\, B_\alpha, \tag{3.18}$$

wobei H_α den Rang s hat und in unterer Hermite Normalform ist. In dieser Gleichung haben wir den multiplikativen Sachverhalt wie schon oben einmal additiv notiert. Zu jeder Zeile bzw. jedem Diagonaleintrag von H_α korrespondiert wie aus der Gleichung ersichtlich eines der Primideale $\mathfrak{p}_i$. Die Primideale, deren Diagonaleintrag ungleich 1 ist, erzeugen die Klassengruppe, denn alle anderen Primideale werden modulo Hauptidealen durch diese dargestellt. Weil meistens sehr wenige Primideale aus S genügen, um die Klassengruppe zu erzeugen, und diese häufig ziemlich beliebig aus S wählbar sind, ist ein Großteil der Diagonalelemente von H_α gleich 1 und die Diagonaleinträge ungleich 1 sammeln sich in H_α tendenziell unten rechts. Daher ist es sinnvoll, daß die Primideale, die an der Erzeugung der Klassengruppe beteiligt werden sollen, in der Faktorbasis nach hinten sortiert werden. Dies werden im allgemeinen Primideale kleiner Norm sein. Zur Verkleinerung von H_α können nun alle Zeilen und Spalten gestrichen werden, in denen eine 1 auf der Diagonalen steht. Entsprechend sind Primideale aus S und Spalten aus B_α zu entfernen. Wir wollen annehmen, daß nach passender Umbennung die obige Gleichung unverändert gilt.

Von der Matrix H_α wird nun die Smith Normalform gebildet: $S_\alpha = U\,H_\alpha\,V$ mit unimodularen U, V. Entsprechend gilt dann

$$(\mathfrak{p}_1, \ldots, \mathfrak{p}_s)\,U^{-1}S_\alpha = (\alpha_1, \ldots, \alpha_m)\,B_\alpha V. \tag{3.19}$$

Wir sind damit dem Ziel schon sehr nahe. Allerdings kann U^{-1} negative Einträge besitzen; infolgedessen würden gebrochene Ideale als Erzeuger für die zyklischen Faktoren auftreten. Wir dürfen aber zu den Spalten von U^{-1} ganzzahlige Linearkombinationen der Spalten von H_α addieren, denn hierdurch werden diese Erzeuger nur mit Hauptidealen multipliziert, was an den Eigenschaften innerhalb der Klassengruppe nichts ändert. Durch gestaffeltes Addieren geeigneter Vielfacher der Spalten von H_α zu jeder einzelnen Spalte von U^{-1} läßt sich erreichen, daß die Einträge einer i-ten Zeile von U^{-1} größer gleich Null und kleiner gleich dem i-ten Diagonalelement von H_α werden. Bezeichnen wir die so erhaltene neue Matrix mit $\widetilde{U}$, so können wir unter Zuhilfenahme einer weiteren Matrix A diesen Prozeß als verallgemeinerte Division mit Rest für Matrizen notieren: $U^{-1} = \widetilde{U} + H_\alpha A$. Setzen wir dies in (3.19) ein und beachten (3.18), so erhalten wir nach Umformung

$$(\mathfrak{p}_1, \ldots, \mathfrak{p}_s)\,\widetilde{U}S_\alpha = (\alpha_1, \ldots, \alpha_m)\,B_\alpha(V - AS_\alpha). \tag{3.20}$$

Die gesuchten ganzen Ideale $\mathfrak{a}_i$ liefert uns jetzt die linke Seite ohne S_α, wohingegen die zugehörigen γ_i durch die rechte Seite gegeben werden.

Mit dieser Methode erhält man meistens gut konditionierte Erzeuger der zyklischen Faktoren der Klassengruppe. Die γ_i hingegen können schlecht konditioniert sein. Vor einer tatsächlichen Berechnung kann man in diesem Fall beispielsweise die Spalten von $B_\alpha(V - A)$ mit Hilfe von U_α reduzieren. Eine weitere Möglichkeit ist, die γ_i modulo Einheiten im S-Einheitengitter zu reduzieren.

3.6 Verifikation der S-Einheiten

Im Algorithmus 3.2.3 benutzen wir reelle Arithmetik endlicher Präzision, um das von einigen S-Einheiten erzeugte Gitter zu bestimmen. Für eine vollständige Faktorbasis verwenden wir eine Approximation des Eulerprodukts, um zu entscheiden, wann das volle S-Einheitengitter erreicht wird. Dies kann dazu führen, daß die Einheiten nicht korrekt sind oder eine echte Untergruppe der S-Klassengruppe berechnet wurde. Im folgenden soll daher ein Test vorgestellt werden, mit dem unter Ausschaltung dieser Fehlerquellen bestimmt werden kann, ob tatsächlich eine Basis der S-Einheiten modulo Torsionseinheiten gefunden wurde, also insbesondere die korrekte S-Klassengruppe vorliegt. An S werden keine besonderen Vorausetzungen gestellt.

Sei G eine abelsche Gruppe und U eine Untergruppe von G. Für eine Primzahl p nennt man U p-maximal in G, wenn aus $w \in G$ mit $w^p \in U$ folgt $w \in U$.

Lemma 3.6.1

(i) *Sei $(G : U)$ endlich. U ist p-maximal in G genau dann, wenn $p \nmid (G : U)$.*

(ii) *Sei U inneres direktes Produkt zweier weiterer Untergruppen U_1 und U_2 von G, wobei U_1 die Ordnung $n \in \mathbb{N}$ besitzt und $p \nmid n$ gilt. Es folgt, daß U genau dann p-maximal in G ist, wenn U_2 p-maximal in G ist.*

(iii) *Sei U inneres direktes Produkt dreier Untergruppen U_1, U_2 und U_3 von G und $H = H_1 \times H_2$ eine freie abelsche Gruppe. Sei $\phi : G \longrightarrow H$ ein Homomorphismus mit $U_3 \subseteq Kern\,\phi$, $U_1 \cap Kern\,\phi = \emptyset$, $\phi(U_1) \subseteq H_1$ und $\phi(U_2) \subseteq H_2$. Weiter sei $\phi(U_1)$ p-maximal in H_1. U ist p-maximal in G genau dann, wenn U_2U_3 p-maximal in G ist.*

Beweis: Die Aussage (i) folgt aus dem Satz von Cauchy angewendet auf G/U und aus der Multiplikativität von Indizes.
Zur Aussage (ii): „$\Leftarrow$“ Sei $w \in G$ mit $w^p \in U$, also $w^p = u_1u_2$ mit $u_1 \in U_1$ und $u_2 \in U_2$. Nach dem Satz von Bèzout gibt es $k, l \in \mathbb{N}$ mit $1 = kp + ln$. Daher $w^p = u_1^{kp}u_2$. Folglich $(wu_1^{-k})^p = u_2 \in U_2$, so daß $wu_1^{-k} \in U_2$ nach Voraussetzung. Also $w \in U_1U_2 = U$.
„$\Rightarrow$“ Sei $w \in G$ mit $w^p \in U_2 \subseteq U$. Nach Voraussetzung $w \in U$, also $w = u_1u_2$ mit $u_1 \in U_1$ und $u_2 \in U_2$. Wegen $w^p = u_1^pu_2^p$ folgt $u_1^p \in U_1 \cap U_2$ und somit $u_1^p = 1$. Wegen $p \nmid n$ ergibt sich $u_1 = 1$ und deswegen ist $w = u_2 \in U_2$.
Zur Aussage (iii): „$\Leftarrow$“ Sei $w \in G$ mit $w^p \in U$, also $w^p = u_1u_2u_3$ mit $u_i \in U_i$ für $1 \leq i \leq 3$. Wir können schreiben $\phi(w) = h_1h_2$ mit geeignetem $h_1 \in H_1$ und $h_2 \in H_2$. Nach Potenzierung mit p, Anwenden von ϕ und wegen des direkten Produkts folgt aus der Division dieser beiden Gleichungen $h_1^p = \phi(u_1)$ und daraus $h_1 \in \phi(U_1)$. Daher gibt es unter Berücksichtigung der Kernbedingung an ϕ ein $v_1 \in U_1$ mit $v_1^p = u_1$. Durch Einsetzen $w^p = v_1^pu_2u_3$ und wegen der p-Maximalität gilt $wv_1^{-1} \in U_2U_3$. Deswegen gilt also $w \in U$.
„$\Rightarrow$“ Sei $w \in G$ mit $w^p \in U_2U_3$, also $w^p = u_2u_3$. Nach der p-Maximalität von U gilt $w = v_1v_2v_3$ mit $v_i \in U_i$. Hieraus folgt $v_1^p \in U_2U_3$ und somit $v_1^p = 1$. Wegen $\phi(v_1)^p = 1$ und weil H frei ist, ergibt sich $v_1 \in \mathrm{Kern}\,\phi \cap U_1$ und deswegen $v_1 = 1$, also $w \in U_2U_3$. □

Seien jetzt mit $\beta_1, \ldots, \beta_{r+s}$ beliebige S-Einheiten und mit β_{r+s+1} ein Erzeuger der Torsionseinheiten gegeben. Wir wollen an Aussage (ii) des vorangegangenen Lemmas anknüpfen:

Lemma 3.6.2 *Sei $m_1 = r+s+1$ wenn $p \mid w_K$ und $m_1 = r+s$ sonst. Weiter gelte $1 \leq m_0 \leq m_1$. Die von den Elementen $\beta_{m_0}, \ldots, \beta_{m_1}$ erzeugte Untergruppe U von U_K^S ist p-maximal in U_K^S und $\beta_{m_0}, \ldots, \beta_{r+s}$ sind unabhängig genau dann, wenn aus $\beta^p = \prod_{i=m_0}^{m_1} \beta_i^{k_i}$ für beliebiges $\beta \in U_K^S$ folgt, daß $k_{m_0} \equiv \ldots \equiv k_{m_1} \equiv 0 \bmod p$ gilt.*

Beweis: „$\Rightarrow$“ Sei $\beta \in U_K^S$ mit $\beta^p = \prod_{i=m_0}^{m_1} \beta_i^{k_i}$. Nach Voraussetzung gibt es auch eine Darstellung $\beta = \prod_{i=m_0}^{m_1} \beta_i^{l_i}$. Hieraus folgt $k_i - pl_i = 0$, also $k_i \equiv 0 \bmod p$ für $m_0 \leq i \leq r+s$. Wird w_K von p geteilt, so gilt zusätzlich $k_{m_1} - pl_{m_1} \equiv 0 \bmod w_K$, und es ergibt sich $k_{m_1} \equiv 0 \bmod p$.
„$\Leftarrow$“ Sei $\beta \in U_K^S$ mit $\beta^p \in U$, also $\beta^p = \prod_{i=m_0}^{m_1} \beta_i^{k_i}$. Nach Voraussetzung folgt $p \mid k_i$ für $m_0 \leq i \leq m_1$. Der Kern von $x \mapsto x^p$ besteht aus p-ten Einheitswurzeln. Dies liefert $\beta = \zeta \prod_{i=m_0}^{m_1} \beta_i^{k_i/p}$ mit einer geeigneten p-ten Einheitswurzel $\zeta \in U_K^S$. Wird w_K nicht von p geteilt, so folgt $\zeta = 1$. Andernfalls können wir ζ durch β_{r+s+1} ausdrücken. Daher ist $\beta \in U$ und U somit p-maximal. Wählen wir speziell $\beta = 1$, so sind die eben betrachteten k_i/p für $m_0 \leq i \leq r+s$ erneut durch p teilbar usw. Also gehen in den k_i beliebige Potenzen von p auf, so daß nur noch $k_i = 0$ für $m_0 \leq i \leq r+s$ übrig bleibt. $\square$

Wir wollen mit Hilfe der beiden letzten Lemmata testen, ob der von unseren gefundenen (vermeintlich) unabhängigen $r+s$ S-Einheiten erzeugte Untermodul samt Torsionseinheiten p-maximal in U_K^S für jede Primzahl p ist. Dann nämlich ist die Gleichheit nachgewiesen. Natürlich ist es nicht möglich, tatsächlich jedes p einzeln zu testen. Es muß schon von vorneherein für fast alle Primzahlen feststehen, daß p-Maximalität vorliegt. Um dies zu erreichen, verwenden wir eine obere Indexschranke. Aufgrund der Isomorphie 3.2 und Satz 3.2.1, S. 21 und S. 22, können wir den Klassengruppenanteil und den Einheitenanteil getrennt betrachten. Für den Klassengruppenanteil sind die Primteiler der vermeintlichen S-Klassenzahl $\det H_\alpha$ zu testen, weil nur diese im Index zur wahren S-Klassenzahl auftreten können. Beim Einheitenanteil benötigen wir eine untere Regulatorschranke, um den Index der berechneten Einheitengruppe in U_K nach oben abschätzen zu können, vergleiche (2.1), S. 14. Dann sind alle Primzahlen unterhalb der Indexschranke zu testen. Die untere Regulatorschranke erhält man mit Methoden aus [16, 15, 22].

Die Bedingung des Lemmas 3.6.2 zeigt, daß man offenbar in den Exponenten modulo p rechnen muß und außerdem die Eigenschaften der Basiselemente irgendwie greifbar zu machen hat. Dies geschieht durch die Verkettung mehrerer Abbildungen zu einem Homomorphismus der multiplikativen Struktur von U_K^S in die additive von $\mathbb{F}_p$.

Sei $\mathfrak{q}$ ein Primideal mit $\mathfrak{q} \notin S$. Wir wollen die Elemente von U_K^S sinnvoll modulo $\mathfrak{q}$ betrachten. Dazu lokalisieren wir $\mathfrak{o}_K$ nach $\mathfrak{q}$, bilden also den Quotientenring

$$\mathfrak{o}_K^{\mathfrak{q}} = \frac{\mathfrak{o}_K}{\mathfrak{o}_K \setminus \mathfrak{q}}$$

und bezeichnen mit $\pi_1 : \mathfrak{o}_K^{\mathfrak{q}} \longrightarrow \mathfrak{o}_K^{\mathfrak{q}}/\mathfrak{q}\mathfrak{o}_K^{\mathfrak{q}}$ die Restklassenabbildung. Es gilt $U_K^S \subset \mathfrak{o}_K^{\mathfrak{q}}$ und ferner

$$\mathfrak{o}_K/\mathfrak{q} \;\simeq\; \mathfrak{o}_K^{\mathfrak{q}}/\mathfrak{q}\mathfrak{o}_K^{\mathfrak{q}}$$

unter dem durch die Inklusion $\mathfrak{o}_K \subset \mathfrak{o}_K^{\mathfrak{q}}$ induzierten kanonischen Isomorphismus. Durch entsprechende Verknüpfung wird ein Homomorphismus $\pi_2 : U_K^S \longrightarrow \mathfrak{o}_K/\mathfrak{q}$

geliefert, dessen Einschränkung auf $\mathfrak{o}_K \cap U_K^S$ mit der üblichen Restklassenabbildung übereinstimmt. Diese Aussagen können beispielsweise in [18], S. 181, nachgelesen werden.

Wir betrachten den Restklassenkörper $\mathfrak{o}_K/\mathfrak{q}$ mit $N(\mathfrak{q})$ Elementen. $(\mathfrak{o}_K/\mathfrak{q})^\times$ ist eine zyklische Gruppe der Ordnung $N(\mathfrak{q}) - 1$; alle endlichen Untergruppen der multiplikativen Gruppe eines Körpers sind nämlich zyklisch. Also $(\mathfrak{o}_K/\mathfrak{q})^\times = <\xi>$ mit einem geeigneten $\xi \in (\mathfrak{o}_K/\mathfrak{q})^\times$. Jedes $\beta \in (\mathfrak{o}_K/\mathfrak{q})^\times$ hat eine Darstellung $\beta = \xi^k$, wobei k modulo $N(\mathfrak{q}) - 1$ eindeutig bestimmt ist. Dies nutzen wir zur Definition von $\log_\xi : (\mathfrak{o}_K/\mathfrak{q})^\times \longrightarrow \mathbb{Z}/(N(\mathfrak{q}) - 1)\mathbb{Z}$ durch $\log_\xi(\beta) = k$.

Jetzt sei angenommen, daß das Primideal $\mathfrak{q}$ mit $p \mid N(\mathfrak{q}) - 1$ gewählt wird, wobei p eine zu testende Primzahl ist. Damit erhält man ein $\pi_3 : \mathbb{Z}/(N(\mathfrak{q}) - 1)\mathbb{Z} \longrightarrow \mathbb{F}_p$, welches $x + (N(\mathfrak{q}) - 1)\mathbb{Z}$ auf $x + p\mathbb{Z}$ abbildet.

Durch Hintereinanderausführung von π_2, $\log_\xi$ und π_3 läßt sich der angekündigte Homomorphismus $\pi_\xi : U_K^S \longrightarrow \mathbb{F}_p$, der von $\mathfrak{q}$ und der Wahl von ξ abhängt, definieren. Mit Hilfe von π_ξ und mehreren Primidealen $\mathfrak{q}$ können wir die Bedingung aus Lemma 3.6.2 testen:

Satz 3.6.3 *Seien p eine Primzahl und $\beta_{m_0}, \dots, \beta_{r+s}$ S-Einheiten mit $1 \le m_0 \le r+s$. Zusätzlich sei β_{r+s+1} ein Erzeuger der Torsionseinheiten und $m_1 = r+s+1$ wenn $p \mid w_K$, ansonsten $m_1 = r+s$. Schließlich sei eine Menge $Q = \{\mathfrak{q}_{m_0}, \dots, \mathfrak{q}_k\}$ von Primidealen gegeben. Zu jedem $\mathfrak{q}_i \in Q$ wählen wir einen Erzeuger ξ_i von $(\mathfrak{o}_K/\mathfrak{q}_i)^\times$. Gelten nun die Bedingungen*

(i) $\mathfrak{q}_i \notin S$ für $m_0 \le i \le k$,

(ii) $p \mid N(\mathfrak{q}_i) - 1$ für $m_0 \le i \le k$,

(iii) Die Matrix $(\pi_{\xi_i}(\beta_j))_{i,j}$ mit $m_0 \le i \le k$ und $m_0 \le j \le m_1$ hat Rang $m_1 - m_0 + 1$ über $\mathbb{F}_p$,

so ist die von $\beta_{m_0}, \dots, \beta_{r+s+1}$ erzeugte Untergruppe von U_K^S p-maximal. Ist umgekehrt diese Untergruppe p-maximal, so existiert eine Menge Q von Primidealen mit den Eigenschaften (i)–(iii).

Beweis: Die erste Aussage ist klar, wenn man π_{ξ_i} auf die Bedingung aus Lemma 3.6.2 anwendet und bedenkt, daß π_{ξ_i} ein Homomorphismus ist. Außerdem muß Lemma 3.6.1 (ii) beachtet werden. Es sei noch bemerkt, daß die Wahl der ξ_i keinen wesentlichen Einfluß auf die Matrix aus der dritten Bedingung hat. Eine andere Wahl führt zu einer neuen Matrix, die aus den Zeilen der alten Matrix multipliziert mit Elementen aus $\mathbb{F}_p^\times$ besteht. Dies ändert den Rang nicht.
Schwierig ist die zweite Aussage. Im Falle von Einheiten werden die wesentlichen Argumente ausführlich in [22] beschrieben, so daß wir uns an dieser Stelle mit einer knapperen Darstellung begnügen wollen. Wir können davon ausgehen, daß

die von den $\beta_{m_0}, \ldots, \beta_{m_1}$ erzeugte Untergruppe U p-maximal in U_K^S ist und daß jedes β_i ganzalgebraisch ist. Letzteres läßt sich durch eine unimodulare Transformation bewerkstelligen, die man aus der Bildung einer Hermite Normalform der Matrix $(\nu_S(\beta_i))_{m_0 \le i \le m_1}$ erhält. Die Idee ist jetzt, die Matrix aus der obigen dritten Bedingung zeilenweise in unterer Diagonalgestalt aufzubauen, wobei simultan $\beta_{m_0}, \ldots, \beta_{m_1}$ unimodular transformiert werden. Diagonalelemente ungleich Null verschaffen wir uns mit Hilfe der folgenden Überlegungen:
Sei β eine ganzalgebraische S-Einheit, die keine p-te Potenz ist. Das Polynom $g(t) = t^p - \beta$ ist dann irreduzibel. Die Ordnung der Galoisgruppe dieses Polynoms wird von p geteilt, so daß darin nach dem Satz von Cauchy ein Element der Ordnung p existiert. Aufgefaßt als Permutationsgruppe der p Nullstellen von $g(t)$ stellt dieses Element eine Permutation des Zykeltyps (p) dar. Nach dem Dichtigkeitssatz von Tschebotareff gibt es aus diesem Grund unendlich viele Primideale $\mathfrak{q}$, so daß $g(t) \bmod \mathfrak{q}$ irrdeduzibel ist. Es kann sogar gefordert werden, daß $\mathfrak{q}$ den Restklassengrad 1 besitzt. Also ist auch $\beta \bmod \mathfrak{q}$ keine p-te Potenz. Wir können zusätzlich annehmen, daß $\mathfrak{q} \notin S$. Ferner folgt aus der Existenz von β, daß $p \mid N(\mathfrak{q}) - 1$, denn sonst wäre jedes Element von $(\mathfrak{o}_K/\mathfrak{q})^\times$ eine p-te Potenz. Dies alles hat zur Folge, daß $\pi_\xi(\beta) \neq 0$ ist. Durch ξ ist hierbei ein Erzeuger von $(\mathfrak{o}_K/\mathfrak{q})^\times$ gegeben.
Wir gehen jetzt per Induktion über i vor. Seien $m_0 \le i \le m_1$, $\beta_{m_0,i}, \ldots, \beta_{m_1,i}$ die aktuellen S-Einheiten, die U erzeugen, $Q_i = \{\mathfrak{q}_{m_0}, \ldots, \mathfrak{q}_{i-1}\}$ eine Menge von $i - m_0$ Primidealen, die den Bedingungen (i)–(ii) gerecht wird, und $M_i = (\pi_{\xi_g}(\beta_{j,i}))_{g,j}$ mit $m_0 \le g < i$ und $m_0 \le j \le m_1$ eine Matrix in unterer Dreiecksgestalt. Aufgrund der p-Maximalität von U ist keins der $\beta_{m_0,i}, \ldots, \beta_{m_1,i}$ eine p-te Potenz, so daß speziell ein Primideal $\mathfrak{q}_i \notin S$ mit $\pi_{\xi_i}(\beta_{i,i}) \neq 0$ existiert. Dies liefert zunächst eine neue Zeile von M_i, die an der i-ten Stelle den Eintrag $\pi_{\xi_i}(\beta_{i,i})$ hat. Aber hinter der i-ten Stelle können auch noch Einträge ungleich Null auftreten. Angenommen, $\pi_{\xi_i}(\beta_{v,i}) \neq 0$ für ein $v > i$. Da man in $\mathbb{F}_p^\times$ invertieren kann, läßt sich dieser Eintrag mit einem Gauss'schen Eliminationsschritt durch Spaltenoperation nullen. Entsprechend setzen wir $\beta_{v,i+1} = \beta_{v,i}\beta_{i,i}^u$, wobei $0 < u < p$ geeignet. Dies wird für alle solche v getan und für die restlichen Indizes v setzen wir dann $\beta_{v,i+1} = \beta_{v,i}$. Ferner wird $Q_{i+1} = Q_i \cup \{\mathfrak{q}_i\}$ gesetzt. Die $\beta_{m_0,i+1}, \ldots, \beta_{m_1,i+1}$ sind mittels unimodularer Transformation entstanden und erzeugen daher U.
Schließlich ist M_{m_1+1} eine quadratische Matrix in unterer Diagonalgestalt mit Determinante ungleich Null, also Rang $m_1 - m_0 + 1$, was zu zeigen war. □

Wir wollen auf eine Verbesserung hinweisen. Es ist nämlich unter gewissen Voraussetzungen an $\beta_1, \ldots, \beta_{m_1}$ nicht unbedingt nötig, alle diese Elemente zum Testen heranzuziehen. Entsprechend sind weniger Primideale für Q zu berechnen. Wir setzen speziell jetzt $(\beta_1, \ldots, \beta_s) = (\alpha_1, \ldots, \alpha_m)\, B_\alpha V$, wie in der ungekürzten Fassung von (3.19) auf S. 38, $(\beta_{1+s}, \ldots, \beta_{r+s}) = (\alpha_1, \ldots, \alpha_m)\, U_\alpha$ und β_{r+s+1} wie oben. An dieser Stelle ist bewiesen, daß die durch U_α gelieferten Elemente wirklich Einheiten und $\beta_1, \ldots, \beta_s$ unabhängige S-Relationen sind. Sei

$a = \min\{\, i \,:\, p \,|\, d_i$ und $1 \le i \le s\}$. Wir befinden uns in der Situation von Lemma 3.6.1 (iii), wobei $G = U_K^S$, $U_3 = <\beta_{1+s}, \ldots, \beta_{r+s+1}>$ und $\phi = \nu_S$. Weiter $U_1 = <\beta_1, \ldots, \beta_{a-1}>$, $U_2 = <\beta_a, \ldots, \beta_s>$ und $H_1 = \mathbb{Z}^{a-1}$, $H_2 = \mathbb{Z}^{s-a}$. Zum Testen der Primzahl p können also $\beta_1, \ldots, \beta_{a-1}$ weggelassen werden. Weil ein Großteil der ersten d_i in der ungekürzten Fassung aus (3.19) Einsen sind, wird hierdurch eine große Verbesserung erzielt.

Wir formulieren jetzt einen Algorithmus, der speziell die Korrektheit der S-Klassengruppe testet:

Algorithmus 3.6.4 *(Test der S-Klassengruppe)*

Eingabe: *S, S-Einheiten $\alpha_1, \ldots, \alpha_m$, Matrizen U_α, B_α, V und S_α wie in der ungekürzten Fassung von (3.19). Außerdem ein Erzeuger ζ der Torsionseinheiten und der Torsionsrang w.*

Ausgabe: *Bei Termination ist die Korrektheit der berechneten S-Klassengruppe bewiesen.*

1. *(Initialisierung) Seien $p_1, \ldots, p_l$ die Primfaktoren der Determinante von S_α und $d_1, \ldots, d_s$ die Diagonalelemente von S_α. Setze $a_j \leftarrow \min\{\, i \,:\, p_j \,|\, d_i$ und $1 \le i \le s\}$ für $1 \le j \le l$. Setze $j \leftarrow 0$.*

2. *(Nächste Primzahl) Setze $M \leftarrow ()$ und $j \leftarrow j+1$. Wenn $j > l$ terminiere.*

3. *(Berechne neue Zeile) Setze U bzw. B gleich der Matrix, die aus den U_α bzw. $B_\alpha V$ durch Reduktion der Koeffizienten modulo p_j entsteht. Entferne die ersten $a_j - 1$ Spalten von B. Finde ein für dieses j noch nicht betrachtetes Primideal $\mathfrak{q} \notin S$ über der Primzahl q mit $p \,|\, q-1$ und berechne einen Erzeuger ξ von $(\mathfrak{o}_K/\mathfrak{q})^\times$. Erweitere M um die Zeile, die aus den kleinen Zeilen $(\pi_\xi(\alpha_1), \ldots, \pi_\xi(\alpha_m))\, B$, $(\pi_\xi(\alpha_1), \ldots, \pi_\xi(\alpha_m))\, U$ und $(\pi_\xi(\zeta))$ — letzteres aber nur im Fall $p \,|\, w$ — entsteht.*

4. *(Rang von M?) Hat M den maximalen Rang $s - a_j + 1 + r + 1$ für $p \,|\, w$ oder $s - a_j + 1 + r$ sonst, so ist die p_j-Maximalität getestet, gehe zu Schritt 2. Sonst gehe zu Schritt 3.*

Die Tatsache, daß π_ξ homomorph ist, kann nutzbringend eingesetzt werden. Dadurch läßt sich die direkte Berechnung der $\beta_1, \ldots, \beta_s$ vermeiden und die unter Umständen großen Koeffizienten der Matrizen U_α und $B_\alpha V$ können modulo p reduziert werden. Die benötigten Primideale $\mathfrak{q}$ lassen sich in der Praxis meistens ziemlich leicht finden.

3.7 Zusammenfassung

Wir wollen im folgenden Algorithmus den Ablauf einer Klassengruppenberechnung in der Übersicht angeben und die bisher behandelten Methoden einordnen.

Algorithmus 3.7.1 *(Klassengruppenverfahren)*

Eingabe: *Ein Zahlkörper der Signatur* (r_1, r_2) *mit erzeugendem Polynom* $f(t)$ *und Ganzheitsbasis.*

Ausgabe: *Ganze Ideale* $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$, $c_1, \ldots, c_m \in \mathbb{Z}^{\geq 2}$ *und ganzalgebraische Zahlen* $\gamma_1, \ldots, \gamma_m$ *wie in (3.1).*

1. *(Erstellung der Faktorbasis) Mit den Methoden des nächsten Kapitels und wie in Abschnitt 4.3.3 wird eine geeignete Faktorbasis* S *berechnet. Das Eulerprodukt wird wie in Abschnitt 3.3 erläutert approximiert.*

2. *(Suche nach einer Relation) Mit den Methoden des nächsten Kapitels, Abschnitt 4.4.5 und Abschnitt 4.5, wird eine* S*-Relation* α *berechnet.*

3. *(Auswertung der Relation) Mit Algorithmus 3.2.3 wird die neue* S*-Relation* α *unter Berücksichtigung der bereits berechneten* S*-Relationen ausgewertet.*

4. *(Testen der Abbruchbedingung) Wenn der Rang der Klassengruppenmatrix noch nicht* s *oder der Rang der Einheitenmatrix noch nicht* r *beträgt, gehe zu Schritt 2. Teste mit Hilfe des Eulerprodukts wie in Abschnitt 3.3 beschrieben, ob vermutlich die korrekte Klassenzahl und der korrekte Regulator berechnet wurden. Wenn nein, gehe zu Schritt 2.*

5. *(Ableitung der Klassengruppendaten) Bestimme wie in Abschnitt 3.5 beschrieben die Daten, die für die Ausgabe benötigt werden.*

6. *(Verifikation der Ergebnisse) Führe Algorithmus 3.6.4 durch. Damit wird die Korrektheit der* S*-Klassengruppe bewiesen. Überprüfe auch wie im nächsten Kapitel beschrieben die Vollständigkeit der Faktorbasis* S*.*

7. *(Ausgabe der Ergebnisse) Ausgabe der Klassengruppendaten. Terminiere.*

Für die einzelnen Schritte ist zu beachten, was bereits im Speziellen gesagt wurde und auch noch gesagt werden wird. Häufig möchte man beispielsweise auf die explizite Berechnung der $\gamma_1, \ldots, \gamma_m$ aus Zeitgründen verzichten. Auch kann man die Verifikation der Klassengruppe auslassen oder nur teilweise durchführen. Der Beweis der Vollständigkeit der Faktorbasis ist der kritischste Punkt. Ohne Hinzunahme unbewiesener Vermutungen ist es für Zahlkörper größeren Grades und Diskriminante sehr langwierig oder zeitlich gesehen nicht mehr möglich, die Klassengruppe bewiesen zu berechnen. Durch diesen Algorithmus werden auch Fundamentaleinheiten geliefert, deren Test ebenfalls sehr zeitaufwendig werden kann.

Kapitel 4

Faktorbasis und Relationensuche

In diesem Kapitel wollen wir auf die Berechnung geeigneter Faktorbasen S und die S-Relationensuche eingehen. Eine Faktorbasis S muß verschiedene Eigenschaften aufweisen. Sie muß zuerst einmal vollständig sein, also die ganze Klassengruppe erzeugen. Sie sollte natürlich die S-Relationensuche unterstützen, und sie sollte nicht zu groß sein. Gerade die letzten beiden Forderungen sind in gewissem Sinne konträr, so daß ein Mittelweg beschritten werden muß.

4.1 Grundideen der Relationensuche

Die meisten Methoden der Relationengewinnung beruhen auf der Möglichkeit, ganzalgebraische Zahlen in Idealen von K mit betraglich kleinen Normen zu bestimmen. Sei dazu $\mathfrak{a}$ ein beliebiges ganzes Ideal von K. Wie im Abschnitt 2.3 beschrieben, bestimmen wir im Konjugiertengitter von $\mathfrak{a}$ Elemente mit kleiner oder kleinster T_2-Norm. Für ein solches $\alpha \in \mathfrak{a}$ ist aufgrund der Ungleichung zwischen arithmetischem und geometrischem Mittel und weil $\mathfrak{a} \mid \alpha$ ist zu erwarten, daß $\alpha/\mathfrak{a}$ ein ganzes Ideal mit kleiner Norm, also $N(\alpha/\mathfrak{a})$ ganz und klein ist. Die Bestimmung solcher Elemente kann wie erwähnt mit dem Auszählalgorithmus von Fincke und Pohst sehr effektiv geschehen. Ein bezüglich der T_2-Norm sehr kleines — häufig kleinstes — Element wird mit dem ersten Element einer LLL-reduzierten Basis geliefert, so daß auch die LLL-Reduktion für die Relationensuche verwendet werden kann. Interessant ist an dieser Stelle, wie die Norm eines Element $\alpha \in \mathfrak{a}$ mit kleinster T_2-Norm nach oben beschränkt wird. Aus [21], Lemma 4.3 auf S. 44, erfahren wir, daß

$$|N(\alpha)| \leq \left(\gamma_n^n n^{-n}\right)^{\frac{1}{2}} N(\mathfrak{a})|D_K|^{\frac{1}{2}}, \tag{4.1}$$

wobei γ_n^n die n-te Hermitesche Konstante bezeichnet. Verwenden wir ein erstes Element einer LLL-reduzierten Basis, so gilt

$$|N(\alpha)| \leq \left(2^{n(n-1)} n^{-n}\right)^{\frac{1}{2}} N(\mathfrak{a})|D_K|^{\frac{1}{2}}. \tag{4.2}$$

Siehe dazu [15], S. 62.

Für das folgende wollen wir $\mathfrak{a}$ definieren als Potenzprodukt von Primidealen einer Faktorbasis S, wobei $\mathfrak{a} \neq \mathfrak{o}_K$. Wählen wir S bestehend aus allen Primidealen mit Norm unterhalb der Schranke (4.1), so liefert uns ein $\alpha \in \mathfrak{a}$ kleinster T_2-Norm eine S-Relation, denn $\alpha/\mathfrak{a}$ faktorisiert in Primideale aus S. Erfreulicherweise ist diese Faktorbasis wegen (4.1) und den Konsequenzen aus (2.2), S. 17 vollständig. Wie wir sehen werden, ist es aber häufig möglich und nötig, eine wesentlich kleinere Schranke als (4.1) für die Faktorbasis zu verwenden. In diesem Fall liefert uns ein T_2-Norm-kleinstes Element α von $\mathfrak{a}$ keineswegs mehr unbedingt eine S-Relation, da in der Faktorisierung von $\alpha/\mathfrak{a}$, die zwar tendenziell aus Primidealen kleiner Norm besteht, größere Primideale auftreten können als in der Faktorbasis vorhanden sind. Sofern S nicht zu drastisch verkleinert wurde, ist es natürlich trotzdem noch „recht wahrscheinlich", daß auf diese Weise S-Relationen gewonnen werden können. Will man sich darauf aber nicht allein verlassen, so merkt man sich für mehrere solcher α und $\mathfrak{a}$ die ganzen Ideale $\alpha/\mathfrak{a}$, deren Norm durch die Schranke (4.1) beschränkt ist. Da es nur endlich viele ganze Ideale mit beschränkter Norm gibt, können bei ausreichender Anzahl nicht alle der gemerkten Ideale verschieden sein; also etwa $\alpha/\mathfrak{a} = \beta/\mathfrak{b}$ und folglich $\alpha/\beta = \mathfrak{a}/\mathfrak{b}$. Weil $\mathfrak{a}$ und $\mathfrak{b}$ Potenzprodukte von Primidealen aus S sind, ist α/β eine S-Einheit und im Falle $\mathfrak{a} \neq \mathfrak{b}$ natürlich eine S-Relation.

Die Methode, sich die $\alpha/\mathfrak{a}$ zu merken und auf Gleichheit zu überprüfen, führt auf die Relationengewinnung mittels reduzierter Ideale, die in [20] beschrieben wird, und auf die Relationenerzwingung von v. Schmettow, siehe [21].

Man kann sich nun fragen, wie man die Ideale $\mathfrak{a}$ zu wählen hat, um mit den α erzeugende Elemente von H_K^S zu berechnen, und ob dies überhaupt möglich ist. Die Relationenerzwingung ist eine Strategie, wie man mit den obigen Methoden eine Untergruppe von H_K^S mit endlichem Index berechnen kann. Von hier kann man mit dem p-ten Wurzeltest — sofern Einheiten gegeben sind — zu H_K^S aufsteigen.

Es sei erwähnt, daß es eine weitere Methode der Relationengewinnung gibt, die nicht über die Bestimmung von Elementen kleiner T_2-Norm geht. Es ist die Methode, die im Number Field Sieve (NFS) verwendet wird. Wir kommen darauf später zu sprechen.

Zum Schluß wollen wir die Verwendung des Auszählalgorithmus beschreiben. Für $\alpha \in \mathfrak{a}$ gilt aufgrund der Ungleichung zwischen arithmetischen und geometrischen Mittel $T_2(\alpha) \geq nN(\mathfrak{a})^{2/n}$. Wir bestimmen daher Elemente α mit

$$2^i nN(\mathfrak{a})^{2/n} \leq T_2(\alpha) < 2^{i+1} nN(\mathfrak{a})^{2/n},$$

beginnend bei $i = 0$. Finden sich in diesem Ringbereich keine nicht bereits ausgezählten Elemente mehr, so wird i gleich $i + 1$ gesetzt und das Auszählen fortgeführt. Speziell geht man so vor, daß mit α auch $-\alpha$ als ausgezählt gilt. Diese Methode wird bei sämtlichen Auszählprozessen in dieser Arbeit angewendet.

4.2 Heuristische Schranken und Smoothness-Eigenschaften

Wir wollen die etwas vage Aussage „die Zahl α ist wahrscheinlich eine S-Relation" des vorigen Abschnitts mit Hilfe der folgenden Sätze konkretisieren und dann an einem Beispiel verdeutlichen.

Satz 4.2.1 *Die Anzahl der ganzen Ideale von K mit Norm unterhalb einem $x > 0$ ist gegeben durch*

$$I(x) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K |D_K|^{\frac{1}{2}}} \cdot x + O(x^{1-\frac{1}{n}}).$$

Der Vorfaktor ist das Residuum der Dedekindschen Zetafunktion $\zeta_K(s)$ bei 1.

Beweis: Siehe [12], S. 361 und S. 415. □

Definition 4.2.2 *Seien $x, c \in \mathbb{R}$, $c > 0$ und $x > 1$.*

(i) Wir nennen ein ganzes Ideal $\mathfrak{a}$ von K x-smooth, wenn für jedes Primideal $\mathfrak{p}$ mit $\mathfrak{p} \mid \mathfrak{a}$ gilt, daß $N(\mathfrak{p}) \leq x$ ist.

(ii) Wir setzen

$$f_K(x, c) = |\, \{\mathfrak{a} \mid N(\mathfrak{a}) \leq x \text{ und } \mathfrak{a} \text{ ist } x^c\text{-smooth } \}\,|.$$

Satz 4.2.3 *Für die Funktion $f_K(x, c)$ gilt die asymptotische Aussage*

$$f_K(x, c) = I(x)\Phi(c) + O(x/\log x),$$

wobei Φ die Dickman-de-Bruijn-Funktion bezeichnet.

Beweis: Siehe [21], S. 30-31. Dort werden auch genaue Angaben über Φ gemacht. □

Bei Φ handelt es sich um eine stetige monoton wachsende Funktion $\mathbb{R}^{>0} \longrightarrow \mathbb{R}^{>0}$. Offenbar ist $\Phi(c) = 1$ für $c \geq 1$. Im Bereich $c \in [\frac{1}{2}, 1]$ gilt $\Phi(c) = 1 + \log c$. Ansonsten erfüllt Φ für $0 < c_1 < c_2 < 1$ die Funktionalgleichung

$$\Phi(c_2) - \Phi(c_1) = \int_{c_1}^{c_2} \Phi(\frac{u}{1-u})\frac{du}{u}.$$

Diese kann genutzt werden, um Φ sukzessive in den Intervallen $[\frac{1}{3}, \frac{1}{2})$, $[\frac{1}{4}, \frac{1}{3})$, ... numerisch zu berechnen, denn geschlossene Ausdrücke für $\Phi(c)$ sind hier nämlich nicht bekannt. Mit Hilfe des Computeralgebra-Systems Maple erhalten wir beispielsweise:

c	0.75	0.5	0.33	0.25	0.2
$\Phi(c)$	0.71	0.31	0.046	0.00491	0.000355

Wie schon erwähnt, werden Elemente α kleiner T_2-Norm in Idealen $\mathfrak{a}$ berechnet — wobei $\mathfrak{a}$ über der verwendeten Faktorbasis vollständig faktorisiert —, so daß das Ideal $\alpha/\mathfrak{a}$ beschränkte Norm besitzt. Unter der Voraussetzung, daß diese Ideale beschränkter Norm hinreichend zufällig bestimmt werden, ist es also mehr als nur plausibel, daß mit dieser Methode Relationen gewonnen werden können. Nehmen wir nun an, daß die Ideale $\alpha/\mathfrak{a}$ zufällig mit Norm unterhalb einer Schranke B bestimmt werden und die Faktorbasis S aus den Primidealen mit Norm unterhalb B^c besteht — wobei $0 < c \leq 1$ —, so ist die zu erwartende Anzahl an Relationen unter m Kandidaten α bei Vernachlässigung des O-Terms gleich $\Phi(c) \cdot m$.

Inwieweit die Ideale $\alpha/\mathfrak{a}$ tatsächlich zufällig mit Norm kleiner gleich B bestimmt werden, hängt von der Art der Relationensuche ab. Man ist natürlich bemüht, daß die Normen nicht zufällig bzw. gleichverteilt unter B liegen, sondern eher kleiner sind, denn hierdurch wird die Smoothnesswahrscheinlichkeit erhöht. Entsprechend wird es fraglicher, ob Φ zur Einschätzung dieser Wahrscheinlichkeit herangezogen werden kann. Außerdem muß beachtet werden, daß die Ideale $\alpha/\mathfrak{a}$ auf ganz spezielle Weise erzeugt werden und dies unter Umständen Rückwirkung auf Smoothnesseigenschaften hat. Hierüber scheint aber nichts bekannt zu sein.

Möglichst kleine Normen erhalten wir, wenn nur Elemente α kleinster oder sehr kleiner T_2-Norm bestimmt werden. In einem Ideal $\mathfrak{a}$ erhält man so ein α mit dem ersten Basiselement einer LLL-reduzierten Basis des Ideals. Hierbei handelt es sich häufig um ein Minimum in $\mathfrak{a}$ im Sinne von [5], S. 346-348, bzw. [21], S. 9, und das ganze Ideal $\alpha/\mathfrak{a}$ ist in diesem Fall das Inverse eines reduzierten Ideals. Wir wollen Ideale $\mathfrak{a}/\alpha$, wobei α das erste Element einer LLL-reduzierten Basis von $\mathfrak{a}$ ist, „pseudoreduzierte“ Ideale nennen.

Beispiel 4.2.4 *Es sei K der von $f(t) = t^4 - 3457t^3 + 1127$ erzeugte Zahlkörper mit $r_1 = 2$, $r_2 = 1$ und $\log_{10}(D_K) \approx 19.99$. Die Minkowskischranke beträgt ungefähr $119 \cdot 10^7$. Zur Relationensuche wählen wir der Reihe nach die Primideale $\mathfrak{p}$ mit Norm unterhalb einer Schranke $C \geq 100$. Aus diesen Primidealen erhalten wir durch Multiplikation mit zufälligen Produkten der Form $\prod \mathfrak{p}_i^{k_i}$, in denen höchstens 5 Primideale $\mathfrak{p}_i$ mit $N(\mathfrak{p}_i) \leq 100$ auftreten und die Exponenten $0 \leq k_i \leq 3$ erfüllen, Ideale $\mathfrak{a}$, in deren Konjugiertengitter jeweils das erste Element α einer LLL-reduzierten Basis bestimmt wird. Diese Elemente dienen dann als Relationskandidaten. Eine genaue Beschreibung dieser Art von Relationensuche findet sich weiter unten in Algorithmus 4.4.5.*

Für $C \in \{200, 400, 700, 1000\}$ bestimmen wir mit dieser Methode jeweils 2000 Elemente, so daß $N(\alpha/\mathfrak{a})$ kleiner gleich $B = 75 \cdot 10^7$ ist, und ermitteln darunter die C-smoothen Elemente. Für jedes C wird die Anzahl der Kandidaten und die Anzahl der tatsächlich C-smoothen Elemente, so daß $N(\alpha/\mathfrak{a}) \leq x$ ist, für

$0 \leq x \leq B$ über x in der Abbildung 4.1 aufgetragen. Die Skalierung der x-Achse ist so gewählt, daß 500 dem tatsächlichen Wert von x gleich $75 \cdot 10^7$ entspricht.

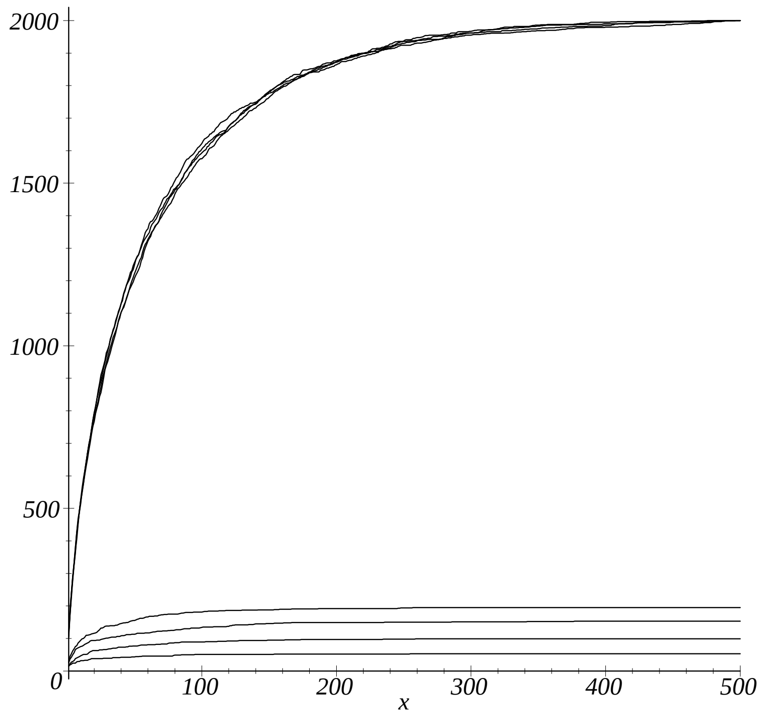

Abbildung 4.1: *Die Normverteilung der Inversen einiger zufälliger pseudoreduzierter Ideale für verschiedene Smoothnessbedingungen*

Die vier Kurven ohne Smoothnessbedingung liegen dicht beieinander, die Größe der Faktorbasis spielt hier keine Rolle. Anders sieht das bei den Smoothnesskurven aus. Diese entsprechen der Größe nach den verschiedenen Werten von C.

Es ist zu beobachten, daß von einer zufälligen Verteilung der Normen nicht die Rede sein kann. Die Kurven ohne Smoothnessbedingung sind charakteristisch für die Art der Relationssuche; auch für andere Anzahlen von zu berechnenden Kandidaten haben sie bis auf einen Skalierungsfaktor diese Form. Mit $\widetilde{I}$ sei die zugehörige (stetige) Funktion gemeint, die man im Mittel aus diesen vier nahe beieinander liegenden Kurven erhält.

Wir wollen jetzt unter Vernachlässigung obiger Bedenken Φ zur Smoothnessbestimmung heranziehen und aber versuchen, der ungleichmäßigen Verteilung der Normen Rechnung zu tragen. Die nachfolgenden Berechnungen erheben keinen

Anspruch auf besondere Exaktheit und dienen vornehmlich der Suche nach heuristischen Aussagen über Smoothnesswahrscheinlichkeiten. Die Idee ist die folgende: Anstatt alle C-smoothen Ideale mit Norm kleiner gleich einem $x \leq B$ auf einmal zu berechnen, unterteilen wir diesen Bereich in Intervalle $[x_i, x_{i+1}]$ mit $1 = x_1 < \ldots < x_k = x$ und bestimmen über Φ die Anzahlen der C-smoothen Ideale mit Norm zwischen x_i und x_{i+1}. Die Wahrscheinlichkeit, daß ein zufälliges gewähltes ganzes Ideal mit Norm größer x_i und kleiner gleich x_{i+1} C-smooth ist, sollte bei

$$\frac{\Phi(\log(C)/\log(x_{i+1}))I(x_{i+1}) - \Phi(\log(C)/\log(x_i))I(x_i)}{I(x_{i+1}) - I(x_i)}$$

liegen. Für x_1 ist $\log(x_1) = 0$; hierfür sei $\Phi(\log(C)/\log(x_1)) = 1$ definiert. Durch Aufsummieren dieser Werte für $i = 1, \ldots, k$ ergibt sich schließlich ungefähr die Gesamtanzahl der C-smoothen Ideale, die bei der durchgeführten Relationensuche auftreten:

$$\sum_{i=1}^{k-1} \frac{\Phi(\log(C)/\log(x_{i+1}))x_{i+1} - \Phi(\log(C)/\log(x_i))x_i}{x_{i+1} - x_i} (\widetilde{I}(x_{i+1}) - \widetilde{I}(x_i)).$$

Den Vorfaktor der Idealzählfunktion I haben wir hier herausgekürzt. Im Grenzprozeß $k \to \infty$ wird aus dieser Summe ein Integral und wir setzen

$$\widetilde{\Phi}_C(x) = \frac{1}{\widetilde{I}(x)} \int_1^x g_C' \, d\widetilde{I}, \tag{4.3}$$

wobei $g_C(t) = t\Phi(\log(C)/\log(t))$ ist. Die Ableitung von g_C ist Null für $t < C$, für $t = C$ existiert sie nicht und für $t > C$ kann man sie mit Hilfe der Funktionalgleichung von Φ wieder durch Φ ausdrücken. Dieses $\widetilde{\Phi}_C(x)$ soll die Wahrscheinlichkeit angeben, daß Relationskandidaten α mit $N(\alpha/\mathfrak{a}) \leq x$ C-smooth sind. In $\widetilde{I}$ gehen die Eigenschaften der verwendeten Relationssuche ein.

Beispiel 4.2.5 *Wir wiederholen das obige Beispiel, beschränken uns diesmal aber auf den interessanten Bereich* $N(\alpha/\mathfrak{a}) \leq B$ *mit* $B = 9 \cdot 10^7$, *was in der Abbildung 4.1 dem Wert 60 auf der x-Achse entspricht. Auf dieselbe Weise wie oben werden jeweils 2000 passende Elemente bestimmt, die auf Smoothnesseigenschaften untersucht werden. Entsprechend werden* $\widetilde{I}$ *und* $\widetilde{\Phi}_C$ *definiert. Zusätzlich approximieren wir* $\widetilde{\Phi}_C(x)\widetilde{I}(x)$ *und tragen die so erhaltenen Smoothnesskurven (grau) zum Vergleich mit den tatsächlichen Kurven (schwarz) in Abbildung 4.2 ein.* C *ist wieder aus* $\{200, 400, 700, 1000\}$. *Die Kurven für* $\widetilde{I}$ *werden fortgelassen.*

Es bietet sich zunächst ein ähnliches Bild wie schon zuvor, nur daß der Normbereich vermieden wird, in dem quasi keine Ideale mehr erzeugt werden. Auffällig ist die relativ gute Übereinstimmung der tatsächlichen mit den über $\widetilde{\Phi}_C$ und $\widetilde{I}$ berechneten Kurven sowohl in Form als auch in absoluter Größe. Übrigens werden die tatsächlichen Kurven umso glatter, je mehr Elemente bestimmt werden.

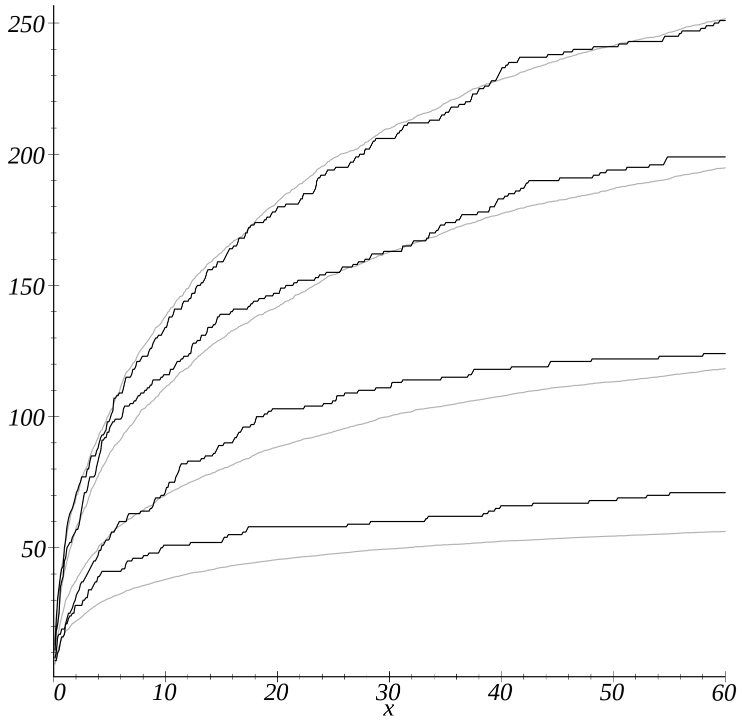

Abbildung 4.2: *Tatsächliche und theoretische Smoothnesskurven im Vergleich*

Durch dieses Beispiel wird nahegelegt, daß man sich tatsächlich mit Φ unter Verwendung der praktisch zu bestimmenden Funktion $\widetilde{I}$ einen Überblick über verschiedene Smoothnesswahrscheinlichkeiten pseudoreduzierter Ideale verschaffen kann. Dies ist jedoch mit Vorsicht zu genießen, da wir einige unbewiesene Annahmen gemacht und O-Terme vernachlässigt haben. Es zeigt sich, daß die vorausgesagten Smoothnesskurven für andere Zahlkörper meistens bis auf einen Skalierungsfaktor oder auch eine Verschiebung ganz gut mit den tatsächlichen übereinstimmen, aber ohne diese Änderungen eher unterhalb liegen. Das Faktorisierungsverhalten ist also eher freundlicher als vorhergesagt.

Eine Möglichkeit, sich bei der Relationensuche nicht nur auf die obige Pseudoreduktion zu stützen, besteht beispielsweise darin, in den Idealen $\mathfrak{a}$ statt des ersten Elements einer LLL-reduzierten Basis eine gewisse Anzahl an Elementen α kleiner T_2-Norm zu bestimmen und dann $\alpha/\mathfrak{a}$ zu betrachten. Auch für solche Ideale können wir entsprechende Smoothnesskurven und ein $\widetilde{I}$ bestimmen; wie zuvor fallen nämlich beim obigen Beispiel die Kurven der absoluten Anzahl quasi zusammen. Der Verlauf dieses $\widetilde{I}$ ist wesentlich linearer und entsprechend treten auch eher größere Normen auf bei gleichzeitig sinkender Smoothnesswahrscheinlichkeiten. Die mit (4.3) vorausgesagten Kurven stimmen wieder von der Form her gut überein, sind aber ebenfalls zu pessimistisch.

Wir wollen jetzt überlegen, welche Schlüsse aus dem bisher gesagten für eine möglichst gut geeignete Faktorbasis gezogen werden können. Es wurde eingangs schon erwähnt, daß eine Faktorbasis, abgesehen von der Bedingung vollständig zu sein, für die Relationensuche weder zu klein noch zu groß sein sollte. In ersterem Fall lassen sich keine Relationen finden — auch wenn nur wenige nötig sind, damit die Klassengruppenmatrix vollen Rang bekommt —, wohingegen im zweiten Fall Relationen zwar leicht gefunden werden, aber auch viele vonnöten sind. A priori gibt es keinen Ansatz, wie die geeignete Größe zu finden ist.

Wir benötigen wieder den Primidealsatz. Für die mit Hilfe obiger Methode bestimmten Relationen zeigt sich, daß sie üblicherweise fast allesamt unabhängig sind und nur wenig mehr davon als Elemente in der Faktorbasis vorhanden zur Bestimmung der Klassengruppe benötigt werden. Daher müßte die Anzahl der während einer Klassengruppenberechnung zu berechnenden Relationskandidaten $\alpha \in \mathfrak{a}$ mit $N(\alpha/\mathfrak{a}) \leq B$ ungefähr

$$\frac{\mathrm{li}(C)}{\widetilde{\Phi}_C(B)} \tag{4.4}$$

betragen. Minimieren wir diese Anzahl für festes B aber variables C, so sollte man mit dem entsprechenden C die optimale Schranke für eine Faktorbasis gefunden haben.

Beispiel 4.2.6 *Wir betrachten das bereits verwendete Beispiel. Für verschiedene Werte von C zwischen 100 und 2500 werden solange Relationskandidaten $\alpha \in \mathfrak{a}$ mit $N(\alpha/\mathfrak{a}) \leq B$ nach der obigen Methode berechnet, bis für jedes Primideal eine Relation gefunden wurde. Die Anzahl der Relationskandidaten tragen wir in Abhängigkeit von C in der folgenden Graphik ein. Hierbei sind die verschiedenen „Meßpunkte" durch kleine Kreise markiert. Zum Vergleich wird die durch (4.4) erhaltene Kurve grau eingezeichnet.*

In Abbildung 4.3 wird deutlich, daß eine Faktorbasis für die Relationensuche zu groß aber auch zu klein sein kann. Dies wird durch beide Kurven angezeigt. Die theoretische Kurve verläuft allerdings besonders für kleine Faktorbasen zu schlecht. Entsprechend liegt die tatsächlich beste Schranke für die Faktorbasis bei 440 während der theoretisch vorgeschlagene Wert ungefähr 630 beträgt.

Durch die Untersuchung einiger Relationskandidaten und unter Verwendung von Φ lassen sich also heuristische Schranken finden, so daß die aus allen Primidealen mit Norm unterhalb einer solchen Schranke bestehende Faktorbasis unter einigen Annahmen besonders gut zur Klasengruppenberechnung geeignet sein müßte. Das obige Beispiel deutet aber schon an, daß Ergebnisse relativ ungenau

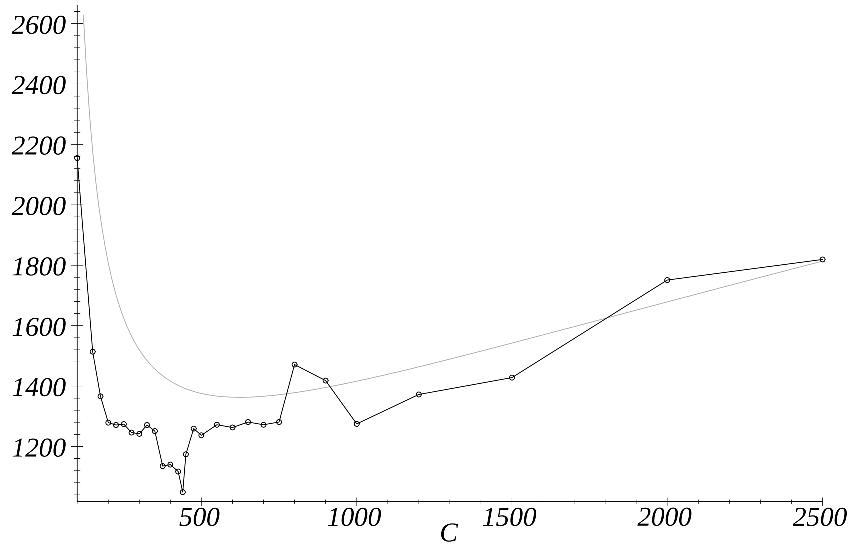

Abbildung 4.3: *Tatsächliche und theoretische Anzahlen zu bestimmender Relationskandidaten für verschiedene Faktorbasisschranken im Vergleich*

sein können (und werden). Immerhin ist die heuristische Schranke 630 im Vergleich zu 440 passabel, wenn man bedenkt, daß eine Schranke zwischen 0 und der Minkowskischranke $119 \cdot 10^7$ ohne Anhaltspunkte zu wählen ist. Wir werden uns im folgenden jedoch nicht auf solche heuristischen Schranken stützen. Die Berechnung ist nämlich einerseits relativ aufwendig und andererseits verwenden wir verschiedene Methoden der Relationensuche, die Relationskandidaten unterschiedlicher Smoothnesswahrscheinlichkeiten liefern. Außerdem können wir zu groß angesetzte Faktorbasen mit einem Reduktionsalgorithmus verkleinern.

4.3 Die Faktorbasis

Die Idealschranken für vollständige Faktorbasen sind fast immer viel zu groß was sowohl die Vollständigkeit als auch die Eignung zur Relationensuche im Sinne des Abschnitts 4.2 betrifft. Wir werden daher mit kleinen Idealschranken beziehungsweise kleinen Faktorbasen arbeiten, von denen wir zunächst nur annehmen können, daß sie vollständig sind. Diese Faktorbasen sollten also möglichst so balanciert sein, daß die Relationensuche aufgrund geringer Faktorisierungswahrscheinlichkeiten nicht zu schwierig wird, aber aufgrund eines hohen S-Einheitenrangs auch nicht zuviele Relationen zu bestimmen sind. Insbesondere sollten keine kleinen Primideale fehlen. Es ist natürlich außerdem erforderlich, die

Vollständigkeit einer solchen Faktorbasis unter Verwendung korrekter Schranken zu beweisen.

Die Berechnung der Primideale der Faktorbasis über einer Primzahl p erfolgt mit Satz (2.27) Kapitel 6.2 aus [16] und mit dem Berlekamp-Verfahren [15] für den Fall, daß der Index der Gleichungsordnung in der Maximalordnung nicht von p geteilt wird. Im Indexteilerfall wird Algorithmus 6.2.9 auf S. 314 in [5] verwendet. Wir ordnen die Primideale der Faktorbasis üblicherweise so an, daß Primideale zu gleichen Primzahlen beieinander stehen und zuerst die Primideale über großen Primzahlen, danach die über kleineren Primzahlen usw. kommen. Man kann auch andere Anordnungen wählen, vergleiche aber Abschnitt 3.5.

4.3.1 Reduktion einer Faktorbasis

Wir wollen eine Methode beschreiben, mit der eine Faktorbasis, die aus allen Primidealen mit Norm unterhalb einer Schranke C besteht, verkleinert werden kann, ohne daß sich das Erzeugnis in der Klassengruppe ändert. Unsere Methode basiert auf einer ähnlichen Methode aus [21].

Lemma 4.3.1 *Sei S eine Faktorbasis bestehend aus allen Primidealen mit Norm kleiner gleich C und $R \subseteq S$. Für beliebige Primzahlen p definiere $m(R,p) = \min\{N(\mathfrak{p}) \mid \mathfrak{p} \in S \backslash R$ und $\mathfrak{p} \mid p\}$, wobei das Minimum im Falle einer leeren Menge als ∞ gesetzt wird. Sei $\mathfrak{q} \in S\backslash R$, $\alpha \in \mathfrak{q}$ und $N = N(\alpha/\mathfrak{q})$, so daß für jedes p mit $p \mid N$ gilt: $p^{\nu_p(N)} < m(R,p)$ und $p^{\nu_p(N)} \leq C$. Dann wird $\mathfrak{q}$ in der Klassengruppe durch Primideale aus R dargestellt.*

Beweis: Gilt $\mathfrak{p} \mid \alpha\mathfrak{q}^{-1}$, so folgt aus der ersten Bedingung wegen $N(\mathfrak{p}) \leq p^{\nu_p(N)}$, daß $\mathfrak{p} \in R$ ist, falls $\mathfrak{p} \in S$ gilt. Insbesondere ist $\mathfrak{p} = \mathfrak{q}$ nicht möglich. Die zweite Bedingung fordert $\mathfrak{p} \in S$. Dies zeigt, daß $\alpha/\mathfrak{q}$ nur in Primideale aus R faktorisiert. □

Algorithmus 4.3.2 *(Reduktion einer Faktorbasis)*

Eingabe: *Eine Faktorbasis $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ bestehend aus allen Primidealen mit Norm kleiner gleich C.*

Ausgabe: *Eine evtl. verkleinerte Faktorbasis S' mit gleichem Erzeugnis in der Klassengruppe wie S.*

1. *(Initialisierung) Setze $C' \leftarrow \min\{M_K, 30+M_K^{\frac{1}{4}}\}$, $S' \leftarrow \{\mathfrak{p} \in S \mid N(\mathfrak{p}) \leq C'\}$ und $R \leftarrow S'$. Berechne für jedes Primideal aus $S\backslash R$ eine im Konjugiertengitter des Primideals LLL-reduzierte Basis.*

2. *(Schwaches Reduzieren) Prüfe der Reihe nach für jedes Primideal* $\mathfrak{p} \in S \backslash R$ *unter Verwendung der Elemente der vorberechneten LLL-reduzierten Basis von* $\mathfrak{p}$ *mit Lemma 4.3.1, ob* $\mathfrak{p}$ *sich in der Klassengruppe bereits durch Primideale aus* R *darstellen läßt, und setze in diesem Fall* $R \leftarrow R \cup \{\mathfrak{p}\}$.

3. *(Wiederhole) Wenn* R *in Schritt 2 vergrößert werden konnte, wiederhole Schritt 2. Wenn* $R = S$, *so Ausgabe von* S' *und terminiere.*

4. *(Starkes Reduzieren) Prüfe der Reihe nach für jedes Primideal* $\mathfrak{p} \in S \backslash R$, *ob es ein Element der LLL-reduzierten Basis von* $\mathfrak{p}$ *gibt, so daß* $\alpha/\mathfrak{p}$ *nur in Primideale aus* R *faktorisiert, und setze in diesem Fall* $R \leftarrow R \cup \{\mathfrak{p}\}$.

5. *(Wiederhole) Wenn* R *in Schritt 4 vergrößert werden konnte, wiederhole Schritt 4. Wenn* $R = S$, *so Ausgabe von* S' *und terminiere.*

6. *(Vergrößere* S'*) Setze* $C' \leftarrow 2C'$, $S' \leftarrow \{\mathfrak{p} \in S \mid N(\mathfrak{p}) \leq C'\}$ *und* $R \leftarrow R \cup S'$ *solange, bis sich* S' *vergrößert hat. Gehe zu Schritt 4.*

Im Schritt 4 genügt es, $\alpha/\mathfrak{p}$ nur über der Faktorbasis zu faktorisieren. Dazu kann man eine leicht abgewandelte Version des weiter unten vorgestellten Algorithmus 4.4.1 verwenden. Hat man einmal solche Faktorisierungen für ein $\mathfrak{p}$ berechnet und fällt $\mathfrak{p}$ noch nicht fort, so werden sie für den etwaigen späteren Gebrauch gespeichert.

Beispiel 4.3.3 *Wir betrachten den Zahlkörper* K, *der durch* $f(t) = t^5 - 7t^2 + 117$ *erzeugt wird. Es gilt* $r_2 = 2$ *und* $\log_{10}(D_K) \approx 10.81$. *Die Minkowskischranke beträgt* 15876. *Es gibt 1869 Primideale mit Norm unter 15876. Wir wenden Algorithmus 4.3.2 auf die Faktorbasis* S *an, die aus diesen Primidealen besteht, und erhalten ein* S' *mit nur 16 Primidealen. Alle 1853 anderen Primideale konnten durch dreimalige Ausführung von Schritt 2 fortgelassen werden. Dazu wurden ungefähr 100 Sekunden benötigt. Die Berechnung der Primideale unterhalb der Minkowskischranke brauchte zuvor 53 Sekunden.*

Zu den angegebenen Zeiten in diesem und allen folgenden Beispielen siehe Kapitel 6. Man könnte nun befürchten, daß durch die Reduktion einer Faktorbasis vorher gute Smoothnesseigenschaften zerstört werden und die Relationensuche entsprechend erschwert wird. In der Praxis läßt sich dies nicht beobachten. Die beiden Reduktionsschritte hängen selbst von Smoothnesseigenschaften ab und gehen nicht zu gründlich vor. Umso schlechter die Smoothnesseigenschaften sind, umso weniger wird reduziert. Im Beispiel können wir ohne Probleme für die Klassengruppen- und Einheitenberechnung ausreichend viele S'-Relationen finden (Algorithmus 4.4.9 benötigt 5 Sekunden).

4.3.2 Nachweis der Vollständigkeit

Wir arbeiten üblicherweise mit einer im Vergleich zur Minkowskischranke kleinen Schranke C, von der wir nur annehmen, daß alle Primideale mit Norm unterhalb dieser Schranke eine vollständige Faktorbasis bilden. Wir wollen dies algorithmisch bestätigen und brauchen dazu „bewiesene" Schranken dieser Eigenschaft.

Es gibt eine ganze Reihe solcher bewiesener Schranken. Bekannt aber verbessert ist die Minkowskischranke M_K aus Abschnitt 2.5. Eine asymptotisch bessere Schranke liefert (4.1), S. 45 unter Einsetzen oberer Abschätzungen für die Hermiteschen Konstanten, siehe [21, 16]. Allerdings tritt die Verbesserung hierdurch beispielsweise für total reelle Körper erst ab Grad 36 und für total komplexe Körper ab Grad 6 auf. Ist der Grad kleiner gleich 8, so sind die Hermiteschen Konstanten bekannt und genaue Aussagen möglich. Das Verhältnis der Schranke (4.1) zu M_K schwankt hier ungefähr zwischen 0.5 und 1.5 und kann in [16] nachgelesen werden. Von Zimmert stammen weitere Schranken für spezielle Grade und Signaturen, siehe z. B. [20], S. 90-91. Alle diese Schranken sind $O(\sqrt{D_K})$ mit von n und r_2 abhängiger O-Konstante.

Eine weitere wichtige Schranke ist die Bachschranke

$$B_K = 12 \log^2 |D_K|.$$

Die Primideale mit Norm kleiner gleich dieser Schranke erzeugen die Klassengruppe unter Annahme der verallgemeinerten Riemannschen Vermutung (GRH), siehe [1]. Diese Schranke ist asymptotisch bedeutend besser als die oben genannten Schranken. Allerdings kommt dies aufgrund des im Vergleich sehr großen Vorfaktors „12" erst bei größeren Diskriminanten zum Tragen.

Wir wählen also eine solche bewiesene Schranke C_K und gehen dann wie folgt vor: Wir durchlaufen mit p alle Primzahlen unter C_K der Reihe nach beginnend bei 2. Für jedes Primideal $\mathfrak{p}$ über p mit $C < N(\mathfrak{p}) \leq C_K$ suchen wir in $\mathfrak{p}$ nach einer Relation der Form

$$\alpha = \mathfrak{p} \cdot \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_m^{k_m}, \tag{4.5}$$

wobei für jedes $\mathfrak{p}_i$ entweder $N(\mathfrak{p}_i) \leq C$ gilt oder bereits ein solches α gefunden wurde: Es ist klar, daß damit $\mathfrak{p}$ „bewiesen" wird.

Für ein $\alpha \in \mathfrak{p}$ können wir (4.5) wie folgt hinreichend überprüfen. Wir setzen $\widetilde{C} = C$, falls $p \leq C$ und $\widetilde{C} = C_K$ sonst. Dann muß für jede Primzahl q mit $q \mid N(\alpha/\mathfrak{p})$ gelten, daß $q \leq \max\{C, p-1\}$, und für $k = \nu_q(N(\alpha/\mathfrak{p}))$ muß $q^k \leq \widetilde{C}$ sein. Sind diese Bedingungen erfüllt, so gilt (4.5).

Wir fassen diese Bemerkungen im folgenden Algorithmus zusammen:

Algorithmus 4.3.4 *(Beweis der Vollständigkeit einer Faktorbasis)*

Eingabe: *Schranken C, C_K mit $0 < C < C_K$.*

Ausgabe: *Bei Termination ist bewiesen, daß die Primideale $\mathfrak{p}$ mit $C < N(\mathfrak{p}) \leq C_K$ in der Klassengruppe durch Primideale mit Norm unterhalb C dargestellt werden.*

1. *(Initialisierung) Setze $P \leftarrow \{q_1, \ldots, q_k\}$ Liste der Primzahlen kleiner gleich C. Setze $p \leftarrow 1$.*

2. *(Nächstes p) Setze $p \leftarrow$ nächste Primzahl größer p. Wenn $p > C_K$ terminiere. Wenn $p \leq C$ setze $\widetilde{C} \leftarrow C$ sonst $\widetilde{C} \leftarrow C_K$. Sei $L \leftarrow \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ Liste der Primideale über p mit $C < N(\mathfrak{p}) \leq C_K$, $i \leftarrow 1$.*

3. *(Prüfe $\mathfrak{p}_i$) Zähle solange $\alpha \in \mathfrak{p}_i$ mit kleiner T_2-Norm aus, bis folgende zwei Bedingungen erfüllt sind: (i) Setze $N \leftarrow N(\alpha)/N(\mathfrak{p}_i)$. Für $j = 1, \ldots, k$ und solange $N \neq 1$ bestimme $k_j = \nu_{q_j}(N)$; es muß gelten $q_j^{k_j} \leq \widetilde{C}$. Setze in diesem Fall $N \leftarrow N/q_j^{k_j}$. (ii) Zum Schluß muß gelten $N = 1$.*

4. *(Nächstes $\mathfrak{p}_i$) Wenn $i < m$ setze $i \leftarrow i + 1$ und gehe zu Schritt 3.*

5. *(Füge p hinzu) Setze $q_{k+1} \leftarrow p$, $P \leftarrow P \cup \{q_{k+1}\}$, $k \leftarrow k + 1$. Gehe zu Schritt 2.*

Bemerkungen:

Algorithmus 4.3.4 terminiert nicht, wenn die Schranke C zu klein ist. Seine Anwendung sollte nach einer Klassengruppenberechnung erfolgen, da dann mit Hilfe des Eulerprodukts und des S-Einheitentests die Vollständigkeit der Faktorbasis quasi feststeht. Ein anderer Grund ist, daß wegen der teilweise sehr hohen bewiesenen Schranken C_K dieser Algorithmus ein Vielfaches der Zeit einer Klassengruppenberechnung unter Verwendung einer kleinen Faktorbasis benötigt.

In Schritt 3 sehen wir von der Faktorisierung von α in Primideale ab und verwenden stattdessen die nur hinreichenden Bedingungen. Auch hierdurch kann es theoretisch geschehen, daß Algorithmus 4.3.4 nicht terminiert. Deswegen ist es günstig, bei vielen vergeblichen Versuchen zur genauen Faktorisierung in bereits getestete Primideale überzugehen. In der Praxis werden aber bei vielen Beispielen nur wenig darstellende Relationen übergangen. Dieses Vorgehen bringt zwei wesentliche Vorteile mit sich. Wir sparen den Speicherplatz für die Primideale über den Primzahlen aus P und profitieren von der Zeitersparnis.

Beispiel 4.3.5 *Wir wollen das Verhalten von Algorithmus 4.3.4 für ein paar Zahlkörper untersuchen. Dazu notieren wir in der folgenden Tabelle der Reihe nach die Werte f, C, C'_K, wobei C'_K eine beliebige, nicht unbedingt bewiesene Schranke bezeichne, danach die Anzahl s_1 der Primideale mit Norm unterhalb C, die Anzahl s_2 der zu testenden Primideale mit Norm unterhalb C'_K, die Anzahl A_1 aller in Schritt 3 bestimmten Elemente α, die Anzahl A_2 der Elemente α, für die* *wir eine Darstellung 4.5 mit bereits bewiesenen Primidealen bei genauer Faktorisierung erhalten hätten, und schließlich die Anzahl A_3 von letzteren Elementen, für die der Test in Schritt 3 (unnötigerweise) nicht zutraf.*

f	C	C'_K	s_1	s_2	A_1	A_2	A_3
$x^6 - x + 22$	500	15619	93	1729	1731	1729	0
$x^6 + 71x^5 - 37x + 220$	500	36561	97	3845	22218	3946	101
$x^{25} - 2$	1000	3000	163	260	636	262	2

Die Körperdiskriminante des ersten Beispiels besitzt 12 Dezimalstellen. Die Minkowskischranke fällt dadurch nicht zu groß aus; es ist die verwendete Schranke C'_K. An diesem Beispiel lesen wir ab, daß fast jedes erzeugte α eine darstellende Relation liefert. Außerdem wird durch den Test nichts verschenkt. Anders sieht die Situation beim zweiten Beispiel aus. Die Diskriminante besitzt hier 24 Stellen, entsprechend groß ist die Minkowskischranke mit 11 Stellen. Bei der verwendeten Schranke C'_K handelt es sich jetzt um die Bachschranke. Mit dem Test schneiden wir hier nicht so gut ab. Trotzdem ist das Verhältnis von A_3 zu A_2 noch relativ gut. Die im Vergleich zu s_2 hohe Anzahl A_1 an Elementen zeigt, daß die Schranke C etwas klein gewählt wurde; wir können schlecht faktorisieren. Die genauere Betrachtung zeigt, daß bis zum Zeitpunkt $p = 5351$ in Algorithmus 4.3.4 ca. 640 Ideale behandelt und aber 11873 Elemente dazu bestimmt wurden. Von diesen hätten nur 715 verwendet werden können, also fielen 75 Elemente unnötigerweise durch den Test. Für diese Ideale wurden demnach durchschnittlich ca. 18 Elemente zur Darstellung benötigt. Für die restlichen 3205 Ideale waren dazu dann durchschnittlich nur noch ca. 3 Elemente erforderlich. Entsprechend entfällt ein Großteil der unnötigen negativen Testergebnisse in diesen Anfangsbereich. Beim dritten Beispiel besitzt die Diskriminante 43, die Minkowskischranke 13 und die Bachschranke 6 Dezimalstellen. Wir verwenden einfach $C'_K = 3000$. Der Test funktioniert gut und auch das Verhältnis s_2 zu A_1 ist passabel.

Die Berechnung der zu testenden Primideale aber auch die Berechnung der Kandidaten α stellt den zeitlich dominierenden Teil von Algorithmus 4.3.4 dar. Bevor wir hierfür Zahlen angeben, soll bereits auf Verbesserungen eingegangen werden.

Eine günstige Berechnung der zu testenden Primideale erhalten wir durch die folgenden Überlegungen. Nach dem Primzahlsatz gibt es $\pi_{\mathbb{Q}}(x) \approx x/\log x$ viele Primzahlen unterhalb einer Zahl x. Die Anzahl der Primzahlen mit $p^2 \leq x$ im Verhältnis zu $\pi_{\mathbb{Q}}(x)$ ist somit ungefähr gleich

$$\frac{\pi_{\mathbb{Q}}(\sqrt{x})}{\pi_{\mathbb{Q}}(x)} \approx \frac{2}{\sqrt{x}},$$

also für großes x ziemlich gering. Bei einem Großteil der Primideale mit Norm unterhalb x handelt es sich also um Primideale vom Grad eins. Dies müssen wir bei der Bestimmung der Primideale $\mathfrak{p} \mid p$, die fast immer durch die Faktorisierung des den Zahlkörper erzeugenden Polynoms $f(t)$ modulo p geschieht, berücksichtigen. Entsprechend Satz (2.27) Kapitel 6.2 aus [16] sind wir nur an Linearfaktoren von $f(t)$ modulo p interessiert.

Lemma 4.3.6 *Das durch*

$$g(t) = ggT_p(f(t), t^p - t)$$

definierte Polynom $g(t) \in \mathbb{F}_p[t]$ besteht genau aus den Linearfaktoren von $f(t)$ modulo p.

Beweis: Die Behauptung ist klar, wenn man berücksichtigt, daß $t^p - t = \prod_{a \in \mathbb{F}_p}(t-a)$ ist. □

Durch die Faktorisierung von $g(t)$ mit der Methode von Cantor und Zassenhaus können wir nun erheblich schneller die gesuchten Primideale $\mathfrak{p}$ bestimmen, siehe [15].

Die nächsten Überlegungen richten sich auf die schnellere Generierung der Kandidaten $\alpha \in \mathfrak{p}$. Wie schon erwähnt verwenden wir hierfür den Auszählalgorithmus. Entsprechend [16] benötigen wir als Eingangsdatum die Grammatrix $A_\mathfrak{p}$ der T_2-Norm bezüglich einer Basis von $\mathfrak{p}$. Aus dieser Matrix wird dann als wesentliche Vorbereitung eine Cholesky-artige Zerlegung der Form

$$A_\mathfrak{p} = Q_\mathfrak{p}^t \, D_\mathfrak{p} \, Q_\mathfrak{p} \tag{4.6}$$

berechnet, wobei $Q_\mathfrak{p}, D_\mathfrak{p} \in \mathbb{R}^{n \times n}$, $D_\mathfrak{p}$ eine Diagonalmatrix mit positiven Diagonalelementen und $Q_\mathfrak{p}$ eine obere Dreiecksmatrix mit Einsen auf der Diagonalen ist. Die Berechnung dieser Zerlegung für jedes $\mathfrak{p}$ muß nicht mit $A_\mathfrak{p}$ starten, sondern kann auch aus einer solchen Zerlegung der Grammatrix $A_{\mathfrak{o}_K}$ der T_2-Norm bezüglich einer Ganzheitsbasis $\omega_1, \ldots, \omega_n$ erfolgen, $A_{\mathfrak{o}_K} = Q_{\mathfrak{o}_K}^t \, D_{\mathfrak{o}_K} \, Q_{\mathfrak{o}_K}$ in der obigen Form. Ist nämlich $M \in \mathbb{Z}^{n \times n}$ eine reguläre Matrix, so besitzt die Grammatrix der T_2-Norm bezüglich der Basis $(\omega_1, \ldots, \omega_n)\, M$ die Darstellung $M^t \, A_{\mathfrak{o}_K} \, M$. Es existiert nun eine Basis des Primideals $\mathfrak{p}$, so daß die zugehörige Übergangsmatrix M der Ganzheitsbasis in die Idealbasis in oberer Hermite Normalform ist. Folglich handelt es sich bei $Q_{\mathfrak{o}_K} M$ ebenfalls um eine obere Dreiecksmatrix. Allerdings hat diese Matrix nicht nur Einsen auf der Diagonalen. Um dies und somit (4.6) herzustellen, können wir $Q_{\mathfrak{o}_K} M$ mit einer geeigneten Diagonalmatrix D' von links multiplizieren. Wir erhalten $Q_\mathfrak{p} = D' \, Q_{\mathfrak{o}_K} M$ und $D_\mathfrak{p} = (D')^{-2} D$.

Durch dieses Vorgehen können wir das Gitter, in dem wir auszählen, nicht mehr direkt LLL-reduzieren. Dies ist jedoch häufig kein schwerwiegender Nachteil. Natürlich kann man wenigstens noch von einer LLL-reduzierten Ganzheitsbasis ausgehen.

Beispiel 4.3.7 *Wir wenden uns dem zeitlichen Verhalten von Algorithmus 4.3.4 zu. In den folgenden Tabellen notieren wir unter Fortführung obigen Beispiels die Zeit t_p, die für die Berechnung der Primideale $\mathfrak{p}$ über p mit $C < N(\mathfrak{p}) \leq C'_K$ und $C < p \leq C'_K$ benötigt wurde, die Zeit t_α, die für die Berechnung der Kandidaten α samt Initialisierung des Auszählalgorithmus benötigt wurde, und die Zeit t_T, die die Berechnung der Normen und das Testen dieser Elemente in Anspruch nahm. In der ersten Tabelle sind die Zeiten ohne Berücksichtigung der geschilderten speziellen Methoden angegeben. Insbesondere wird hier genau geprüft, ob die Kandidaten α entsprechend (4.5) faktorisieren. Die Angaben sind in Sekunden.*

f	t_p	t_α	t_T	*gesamt*
$t^6 - t + 22$	34	125	17	176
$t^6 + 71t^5 - 37t + 220$	133	481	184	798
$t^{25} - 2$	60	3625	31	3716

f	t_p	t_α	t_T	*gesamt*
$t^6 - t + 22$	10	13	2	25
$t^6 + 71t^5 - 37t + 220$	33	60	133	226
$t^{25} - 2$	10	50	9	69

Bei diesen Beispielen ergibt sich der größte Teil der zeitlichen Verbesserung durch die Verwendung der vorberechneten Cholesky-artigen Zerlegung (4.6). Es ist aber zu erwarten, daß die spezielle Berechnung der Primideale vom Grad eins unter Verwendung größerer Idealschranken den Hauptanteil der Verbesserung liefern wird.

4.3.3 Vorgehensweise in der Praxis

Aufgrund der Beschränkung der Zeilenzahl der Klassengruppenmatrix durch Algorithmus 3.2.3 sollten Faktorbasen im Moment nicht aus mehr als ungefähr 200 Primidealen bestehen. Dies ist gleichbedeutend mit Idealschranken im Bereich um 1200. Eine solche Idealschranke ist für die Vollständigkeit der Faktorbasis in der Praxis so gut wie immer ausreichend. Dem Verfasser ist kein Beispiel bekannt, wo nicht eine Schranke von 100 für die Vollständigkeit gereicht hätte. Aber auch für die Relationensuche ist dies häufig vollig ausreichend. Das Beispiel 4.2.4 aus Abschnitt 4.2 hatte eine 20-stellige Diskriminante, was für einen Körper vierten Grades schon relativ groß ist, und für eine gute Faktorbasis wurde die Schranke 440 ermittelt. Später wird eine Methode beschrieben, mit der die Wirkung einer größeren Faktorbasis erzielt werden kann.

In der Praxis hat sich das folgende Vorgehen bewährt: Man wähle eine Schranke zwischen 100 und 1000 in Abhängigkeit der Größe der Koeffizienten des erzeugenden Polynoms oder der Diskriminante, und reduziere die daraus resultierende

Faktorbasis mit Algorithmus 4.3.2. Dann wendet man die Methoden der Relationssuche aus dem nächsten Abschnitt an, sieht, ob eine Berechnung der Klassengruppe überhaupt möglich ist und erhält auch schon ein Ergebnis. Zu einem späteren Zeitpunkt verwendet man dann Algorithmus 4.3.4, um die Vollständigkeit nachzuweisen.

4.4 Relationensuche

In diesem Abschnitt sollen verschiedene Strategien der Relationengewinnung besprochen werden. Wir arbeiten mit einer fest vorgegebenen Faktorbasis und stützen uns meist, aber nicht ausschließlich, auf die Smoothnesseigenschaften der erzeugten Relationenkandidaten. Im nächsten Abschnitt wird sich dies dann ändern.

4.4.1 Test auf S-Einheit

Für die Relationensuche wird ein Test benötigt, der prüft, ob ein $\alpha \in K$ eine S-Einheit ist oder nicht. Da gefundene S-Einheiten an Algorithmus 3.2.3 weitergeleitet werden und dort $\nu_S(\alpha)$ benötigt wird, können wir $\nu_S(\alpha)$ auch schon hier berechnen.

Algorithmus 4.4.1 *(Test auf S-Einheit)*

Eingabe: *Eine Faktorbasis $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ und ein $\alpha \in K$.*

Ausgabe: *„Wahr“ und $\nu_S(\alpha)$, wenn α eine S-Einheit ist. Sonst „falsch“.*

1. *(Initialisierung) Setze $P \leftarrow \{\, p \mid$ es gibt ein $\mathfrak{p} \in S$ mit $\mathfrak{p} \mid p\}$. Für jedes $p \in P$ setze $S_p \leftarrow \{\mathfrak{p} \mid \mathfrak{p} \in S$ und $\mathfrak{p} \mid p\}$ und $S'_p \leftarrow \{\mathfrak{p} \mid \mathfrak{p} \notin S$ und $\mathfrak{p} \mid p\}$.*

2. *(Aufspalten) Schreibe $\alpha = \beta/d$ mit $\beta \in \mathfrak{o}_K$ und $d \in \mathbb{Z}^{\geq 0}$ minimal.*

3. *(Sieben) Bestimme $N \leftarrow N(\beta)$. Für jede Primzahl $p \in P$ setze $\beta_p \leftarrow \nu_p(N)$ und setze danach $N \leftarrow N/p^{\beta_p}$. Außerdem $d_p \leftarrow \nu_p(d)$ und $d \leftarrow d/p^{d_p}$. Ist zum Schluß $N \neq 1$ oder $d \neq 1$, so ist α keine S-Einheit, Ausgabe „falsch“ und terminiere.*

4. *(Schleife über p) Für jedes $p \in P$:*

5. *(Bewertung β) Für jedes $\mathfrak{p} \in S_p$ berechne $v_\mathfrak{p} \leftarrow \nu_\mathfrak{p}(\beta)$ und setze $\beta_p \leftarrow \beta_p - v_\mathfrak{p} f(\mathfrak{p} \mid p)$. Wenn β_p Null ist, gilt für alle restlichen $\mathfrak{p}$, daß $\nu_\mathfrak{p}(\beta) = 0$ ist. Ist nach Abarbeitung dieser Schritte β_p nicht Null, aber $\alpha \in \mathfrak{o}_K$, so ist α keine S-Einheit, Ausgabe „falsch“ und terminiere. Ist $\alpha \notin \mathfrak{o}_K$, führe diese Schritte auch noch für alle $\mathfrak{p} \in S'_\mathfrak{p}$ durch.*

6. *(Bewertung d) Wenn* $d_p \neq 0$ *so setze für jedes* $\mathfrak{p} \in S_p$ *und dann* $\mathfrak{p} \in S'_\mathfrak{p}$ $v_\mathfrak{p} \leftarrow v_\mathfrak{p} - d_p e(\mathfrak{p} \mid p)$.

7. *(Nächstes p) Wiederhole ab Schritt 4.*

8. *(Schlußfolgerung) Wenn* $v_\mathfrak{p} = 0$ *für jedes* $\mathfrak{p} \in S'_\mathfrak{p}$, *so ist* α *eine S-Einheit. Ausgabe „wahr“ und* $\nu_S(\alpha) \leftarrow (v_{\mathfrak{p}_1}, \ldots, v_{\mathfrak{p}_s})$. *Sonst Ausgabe „falsch“. Terminiere.*

Die Berechnung von $\nu_\mathfrak{p}(\beta)$ in Schritt 5 erfolgt mit dem Algorithmus 4.8.17 auf S. 201 in [5].

Zu diesem Algorithmus ist ansonsten nicht viel zu sagen. Wichtig ist, daß Nicht-S-Einheiten schnell erkannt werden. Wie in Abschnitt 4.2 gesehen, ist der Anteil an solchen Elementen nämlich sehr groß. An Schritt 3 scheitert üblicherweise ein Großteil der Nicht-S-Einheiten, und bis dahin läuft der Algorithmus schnell ab. Die Berechung der Bewertungen ist dagegen ziemlich teuer. Weil für nicht ganzalgebraische Zahlen zusätzlich die Bewertungen an Primidealen aus S'_p berechnet werden müssen, versucht man sich bei der Relationensuche nach Möglichkeit auf ganzalgebraische Zahlen zu konzentrieren.

4.4.2 Schnelle Relationen

Wir beschreiben jetzt eine Methode, mit der man auf schnellem Wege Relationen erhalten kann. Mit Algorithmus 4.4.1 stellt man fest, ob es sich bei einem Kandidaten um eine S-Einheit handelt oder nicht.

Algorithmus 4.4.2 *(Schnelle Relationen)*

Eingabe: *Eine Faktorbasis* $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$.

Ausgabe: *S-Relationen* $\alpha_1, \alpha_2, \ldots$.

1. *(Initialisierung) Initialisiere den Auszählalgorithmus für jedes Primideal der Faktorbasis. Setze* $i \leftarrow 1$ *und* $l \leftarrow 1$.

2. *(Suche) Fahre mit dem Auszählen von Elementen von* $\mathfrak{p}_i$ *fort, bis eine S-Relation* α *gefunden wurde.*

3. *(Nächstes* $\mathfrak{p}_i$*) Ausgabe von* $\alpha_l \leftarrow \alpha$ *und setze* $l \leftarrow l + 1$. *Wenn* $i = s$ *dann* $i \leftarrow 1$ *sonst* $i \leftarrow i + 1$. *Gehe zu Schritt 2.*

Der Schritt 2 wird nicht verlassen, bevor nicht eine Relation in $\mathfrak{p}_i$ gefunden wurde. Dies ist (wenigstens theoretisch) immer möglich, da beispielsweise beliebige Potenzen von $\mathfrak{p}_i^{h_K}$ Hauptideale liefern, deren Erzeuger durch Auszählen der Elemente von $\mathfrak{p}_i$ gefunden werden können. Es ist sogar möglich, durch eine endliche Zahl an von Algorithmus 4.4.2 bestimmten Relationen ganz H_K^S zu erzeugen. In der Praxis finden sich in $\mathfrak{p}_i$ meist sehr schnell Relationen. Durch dieses Beharren auf $\mathfrak{p}_i$ wird erreicht, daß gefundene Relationen „einigermaßen unabhängig“ sind. Für viele Beispiele genügt das zwei- bis dreifache von s an solchen Relationen, um Einheiten und Klassengruppe zu berechnen.

Es gibt aber auch so ungünstig beschaffene Körper, daß man mit Algorithmus 4.4.2 aus praktischer Sicht nicht in vernünftiger Zeit zum Ziel kommen kann. Die bei den folgenden Beispielen angegebenen Zeiten beinhalten auch die Zeit, die von Algorithmus 3.2.3 benötigt wird.

Beispiel 4.4.3 *Wir betrachten den Zahlkörper K, der durch $f(t) = t^8 + 2t^7 + 72t^6 - 130t^5 - 4018t^4 - 11504t^3 - 136379t^2 + 515628t + 6454324$ gegeben wird. Es gilt $r_2 = 4$ und $\log_{10}(D_K) \approx 13.91$. Der Regulator beträgt ungefähr 4643.02 und die Klassengruppe ist isomorph zu $\mathbb{Z}/6\mathbb{Z}$. Für die Faktorbasis verwenden wir die 114 Primideale mit Norm kleiner gleich 500. Nach den ersten 112 von Algorithmus 4.4.2 bestimmten Relationen beträgt der Rang der Klassengruppenmatrix 60 und der Rang der Einheitenmatrix 1. Nach weiteren 312 Relationen hat sich nichts geändert. Bei Relation 548 hat sich der Rang der Klassengruppenmatrix auf 78 erhöht. Wir brechen das Beispiel schließlich „kurz vor Schluß“ bei Rang 113 bzw. 3 nach 1952 Relationen und ungefähr 8500 Sekunden ab.*

Interessanterweise gibt es bei diesem Beispiel auch für andere Faktorbasisschranken stets beim Rang der Klassengruppenmatrix von ungefähr $s/2$ das erste Plateau, an dem der Rang nicht weiter wächst.

Wir bemerken zum Schluß, daß man den Initialisierungsschritt mit Hilfe der vorberechneten Zerlegung (4.6), S. 59, — unter Vorbehalt — verschnellern kann, wenn die Konjugiertengitter der beteiligten Primideale nicht zu schlecht konditioniert sind.

Beispiel 4.4.4 *Wir betrachten jetzt den Zahlkörper K, der durch $f(t) = x^{18} + 4608$ erzeugt wird. Es gilt $r_2 = 9$ und $\log(-D_K) \approx 32.94$. Der Regulator beträgt ungefähr 5682014322.3 und die Klassenzahl ist eins. Für die Faktorbasis verwenden wir die 62 Primideale mit Norm kleiner gleich 300. Nach 118 Relationen und 310 Sekunden ist die Klassengruppe und Einheitengruppe bestimmt. Wird zur Initialisierung des Auszählalgorithmus für die Primideale der Faktorbasis auf die vorberechnete Zerlegung (4.6) zurückgegriffen, so ist die Berechnung nach 182 Relationen und 242 Sekunden zu Ende. Offenbar sind die Konjugiertengitter der Primideale schon etwas ungünstiger ausgelegt als zuvor. Trotzdem wird weniger Zeit benötigt als zuvor. Arbeiten wir bezüglich einer LLL-reduzierten Ganzheitsbasis von K unter Verwendung der Zerlegung (4.6), so ergibt sich mit 118 Relationen bei 120 Sekunden die schnellste Berechnung.*

4.4.3 Gute Relationen

Wir beschreiben jetzt eine Methode, wie man Relationen gewinnen kann, die eine gute Unabhängigkeit aufweisen. Von diesen Relationen werden meist nur wenig mehr als $r+s$ Stück benötigt, um das S-Einheitengitter zu erzeugen.

Algorithmus 4.4.5 *(Gute Relationen)*

Eingabe: *Eine Faktorbasis* $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$.

Ausgabe: S*-Relationen* $\alpha_1, \dots, \alpha_l$.

1. *(Initialisierung) Setze* $S' \leftarrow \{\, \mathfrak{p} \mid \mathfrak{p} \in S$ *und* $N(\mathfrak{p}) \le \min\{2\log(|D_K|), \frac{1}{5}C\}\}$, *wobei* C *die zur Herstellung der Faktorbasis verwendete Schranke bezeichne. Setze* $a \leftarrow \min\{5, |S'|\}$ *und* $b \leftarrow 3$. *Setze* $i \leftarrow 1$ *und* $l \leftarrow 1$.
2. *(Suche) Wähle* $\mathfrak{q}_1, \dots, \mathfrak{q}_a$ *zufällig aus* S' *aus. Wähle zufällige* $k_1, \dots, k_a$ *mit* $0 \le k_j \le b$ *für* $1 \le j \le a$. *Bestimme das erste Element* α *einer LLL-reduzierten Basis von* $\mathfrak{p}_i \prod_{j=1}^{a} \mathfrak{q}_j^{k_j}$.
3. *(Relation gefunden?) Wenn* α *keine* S*-Relation ist, so gehe zu Schritt 2.*
4. *(Nächstes* $\mathfrak{p}_i$*) Wenn* α *bisher nicht gefunden wurde, so Ausgabe von* $\alpha_l \leftarrow \alpha$ *und setze* $l \leftarrow l+1$. *Wenn der Anteil mehrfach gefundener Relationen 20 Prozent übersteigt, so terminiere. Wenn* $i = s$ *so* $i \leftarrow 1$ *sonst* $i \leftarrow i+1$. *Gehe zu Schritt 2.*

Die Größe von S' und die Konstanten des Initialisierungsschritts und der Terminationsbedingung sind heuristisch gewählt. Für die Idealgewichte $\prod_{j=1}^{a} \mathfrak{q}_j^{k_j}$ muß man einen Kompromiß zwischen dem Aufwand ihrer Berechnung und ihrer Vielfältigkeit finden. Insbesondere sollte S' nicht zu klein sein. Es ist nämlich denkbar, daß für sämtliche Kombinationen in Schritt 2 keine S-Einheit oder nur wenige verschiedene gefunden werden können. Dies wird umso unwahrscheinlicher, je größer S' ist. Ein zu großes S' führt allerdings zu schlechteren Faktorisierungseigenschaften der Relationskandidaten. Durch den Algorithmus können im übrigen nur endlich viele verschiedene Relationskandidaten erzeugt werden, so daß ein geeignetes Abbruchkriterium hinzugefügt werden muß.

Eine Möglichkeit, die Anzahl der Kandidaten für S-Einheiten im Schritt 2 zu erhöhen, besteht in der Gewichtung der T_2-Norm beziehungsweise der Gewichtung der Vektoren des Konjugiertengitters, in dem die LLL-Reduzierung vorgenommen wird. Dies scheint zumindest theoretisch auch den Vorteil mit sich zu bringen, daß ungünstige Einflüsse schlecht konditionierter Einheiten ausgeglichen werden können. Schließlich suchen wir Elemente auf Normflächen zu möglichst kleinen Normen, und diese Elemente können bezüglich der ungewichteten T_2-Norm auch „weit draußen“ liegen.

Die Berechnung der Idealgewichte ist besonders für größeren Grad n ziemlich zeitaufwendig. Man kann zwar die Potenzen $q_j^{k_j}$ zum Anfang auf Vorrat berechnen, dies bringt aber nicht sehr viel. Die meisten Primideale liegen in 2-Elementdarstellung vor und lassen sich somit sehr leicht potenzieren. Die einzelnen Potenzen setzen wir dann sukzessive durch Idealmultiplikation eines Ideals in $\mathbb{Z}$-Basisdarstellung mit einem Ideal in 2-Elementdarstellung zusammen. Zu diesen verschiedenen Idealdarstellungen siehe [16, 15].

Außerdem darf bei der Zeitkomponente nicht vergessen werden, daß in jedem Suchschritt das Gitter erzeugt und eine LLL-Reduktion durchgeführt werden muß.

Beispiel 4.4.6 *Wir testen Algorithmus 4.4.5 an dem Zahlkörper aus Beispiel 4.4.3. Nach 117 Relationen hat die Klassgruppenmatrix den maximalen Rang 114 und die Einheitenmatrix den Rang 3. Allerdings ist der korrespondierende S-Einheitenindex laut Eulerprodukt noch nicht eins. Es werden weitere 5 Relationen benötigt, um diesen Index zu eins zu machen. Die Berechnung benötigt insgesamt ungefähr 192 Sekunden.*

Für dieses Beispiel ist es also quasi unerläßlich, die Relationensuche mit Algorithmus 4.4.5 durchzuführen. Umgekehrt ist es bei dem anderen Beispiel.

Beispiel 4.4.7 *Wir probieren jetzt Beispiel 4.4.4 mit Algorithmus 4.4.5 aus. Als Schranke für S' verwenden wir 60, was 15 Primideale liefert. Nach 73 Relationen und 462 Sekunden ist die Berechung beendet. Die Verwendung eines größeren S' führt zu erheblich längeren Zeiten.*

4.4.4 Gezielte Relationen

Bei der Relationensuche — besonders bei Algorithmus 4.4.2 — stellt man fest, daß es gegen Ende immer schwieriger wird, von den bisherigen Relationen unabhängige Relationen zu finden. Die Klassengruppenmatrix ist dann nicht mehr weit von einer unteren Dreiecksmatrix mit Einträgen ungleich Null auf der Diagonalen entfernt. Für manche Primideale gibt es aber noch keine eigene Stufe. Eine Idee könnte sein, gezielt nur in diesen Primidealen nach Relationen zu suchen, in der Hoffnung, eine neue Stufe in der Klassengruppenmatrix zu erzeugen. Es zeigt sich allerdings, daß bei Verwendung von Algorithmus 4.4.2 die Einschränkung nur auf diese „Nichtstufenideale“ ungünstig ist. Die Laufzeiten liegen meist höher als vorher und es scheint, als wäre die beste Vorgehensweise, die Informationen aus allen Primidealen der Faktorbasis „gleichmäßig herauszuholen“. Immerhin hängt es auch von der Anordnung der Faktorbasis ab, ob ein Primideal ein „Stufen-“ oder „Nichtstufenideal“ ist.

Auf die Laufzeit wirkt sich mitunter auch die folgende Situation ungünstig aus: Die Klassengruppenmatrix ist regulär, aber die Determinante ist noch ein Vielfaches der Klassenzahl. Dies bedeutet, daß ein oder mehrere Diagonalelemente zu groß sind und man könnte nun speziell in den korrespondierenden Primidealen nach Relationen suchen, um kleinere Diagonalelemente zu erhalten. Dies erweist sich als günstig, wenn man (unter Umständen) auf Idealgewichte wie in Algorithmus 4.4.5 zurückgreift. Da meistens nur sehr wenige Diagonalelemente ungleich 1 sind, fallen etwaige Nachteile von Algorithmus 4.4.5 nicht sehr ins Gewicht.

Beispiel 4.4.8 *Wir betrachten den Zahlkörper K, der durch $f(t) = t^9+3t^8-5t^7-6t^5+9t^4+5t^3-25t^2-50t+45$ erzeugt wird. Es gilt $r_1 = 3$, $r_2 = 3$ und $\log(-D_K) \approx 21.97$. Der Regulator beträgt ungefähr 146323318.14 und die Klassenzahl ist 1. Für die Faktorbasis wählen wir eine Schranke von 300. Dies liefert 76 Primideale. Mit Algorithmus 4.4.5 sind wir nach 82 Relationen fast am Ziel: der Regulator ist schon berechnet und die Klassengruppenmatrix hat Determinante 2. Aber erst nach weiteren 59 Relationen und insgesamt 443 Sekunden wird die Determinante 1. Durch Auszählen in dem verantwortlichen Primideal hätten dafür 4 weitere Relationen genügt.*

4.4.5 Kombination der verschiedenen Strategien

Die beschriebenen Strategien waren für die Relationensuche bei manchen Körpern von Vorteil, bei anderen aber auch von Nachteil. Wir wollen jetzt eine Kombination dieser Strategien mit Rückkopplung zu Algorithmus 3.2.3 beschreiben. Die Schritte 2-4 des Klassengruppenverfahren 3.7.1 werden zu einem Unteralgorithmus zusammengefaßt:

Algorithmus 4.4.9 *(Relationensuche)*

Eingabe: *Eine Faktorbasis $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ und das approximierte Eulerprodukt $EP_K(x)$.*

Ausgabe: *S-Relationen $\alpha_1, \ldots, \alpha_m$, die Klassengruppenmatrix H_α, die Relationsbasismatrix B_α, die Einheitenmatrix U_α, und laut Eulerprodukt die korrekte Klassenzahl h_K und der korrekte Regulator R_K.*

1. *(Initialisierung) Definiere das Idealgewicht $\mathfrak{a} \leftarrow \mathfrak{o}_K$. Initialisiere den Auszählalgorithmus für jedes Ideal $\mathfrak{p}\mathfrak{a}$ mit $\mathfrak{p} \in S$. Setze $i \leftarrow 0$, $m \leftarrow 0$ und $t \leftarrow 0$. Initialisiere auch Algorithmus 3.2.3.*

2. *(Neues Idealgewicht?) Wenn $t > 10$ oder wenn $t > 4$ falls sowohl H_α den Rang s und U_α den Rang r besitzen, so setze $t \leftarrow 0$ und bestimme ein neues Idealgewicht $\mathfrak{a}$ durch Berechnung eines zufälligen Produkts wie in Algorithmus 4.4.2.*

3. *(Wähle Primideal) Wenn der Rang von H_α gleich s und der Rang von U_α gleich r ist und wenn auf der Diagonalen von H_α ein Eintrag größer 1 steht, dann wird i die Nummer der nächsten Zeile unter der i-ten Zeile von H_α,*

in der sich ein Diagonalelement größer 1 befindet. Gibt es keine solche Zeile mehr, dann wird i die Nummer der obersten Zeile in H_α mit einem Diagonalelement größer 1. Trifft aber eine der obigen drei Bedingungen nicht zu, so setze $i \leftarrow i+1$ und wenn $i > s$ setze $i \leftarrow 1$.

4. *(Suche Relation) Wenn der Auszählalgorithmus für $\mathfrak{p}_i\mathfrak{a}$ noch nicht initialisiert wurde, so geschieht das jetzt. Fahre mit dem Auszählen in $\mathfrak{p}_i\mathfrak{a}$ fort, bis eine Relation α gefunden wurde. Setze $m \leftarrow m+1$ und $\alpha_m \leftarrow \alpha$.*

5. *(Auswerten der Relation) Mit Algorithmus 3.2.3 wird die neue Relation unter Berücksichtigung der bereits berechneten Relationen ausgewertet. Wir setzen $t \leftarrow t+1$, wenn sich weder der Rang von H_α noch der Rang von U_α noch der S-Einheitenindex — wenn endlich — verändert haben.*

6. *(Testen der Abbruchbedingung) Wenn der S-Einheitenindex nicht endlich oder laut Eulerprodukt nicht 1 ist, so gehen wir zu Schritt 2.*

7. *(Ausgabe) Die erforderlichen Daten sind berechnet und können ausgegeben werden. Terminiere.*

Informell und nicht ganz korrekt gesagt handelt es sich also bei Algorithmus 4.4.9 zunächst um Algorithmus 4.4.2, und wenn dieser keine guten Relationen bringt, geht man zu Algorithmus 4.4.5 oder zur gezielten Suche wie beschrieben über. Wieder sind die Konstanten in Schritt 2 heuristisch gewählt. Wenn sich nach 10 beziehungsweise 4 Relationen nichts verändert hat, wird ein neues Idealgewicht berechnet. Man könnte diese Konstanten auch während des Algorithmus für jedes neue Idealgewicht um einen gewissen Wert bis zu einer gewissen unteren Schranke heruntersetzen und so erreichen, daß bei Beispielen wie 4.4.3 häufiger neue Idealgewichte berechnet werden.

Primzahlen, über denen nur Primideale der Faktorbasis liegen, sind Relationen, die wir „umsonst“ bekommen. Diese sollten bereits im Initialisierungsschritt berücksichtigt werden. Entsprechend empfiehlt es sich, im Suchschritt nur Relationskandidaten zuzulassen, die keine ganzrationalen Zahlen sind. Hat man eine Relation gefunden, so ist es günstig zu prüfen, ob diese Relation schon einmal gefunden wurde.

Beispiel 4.4.10 *Wir wenden Algorithmus 4.4.9 auf die drei obigen Beispiele unter Benutzung einer LLL-reduzierten Ganzheitsbasis und der vorberechneten Zerlegung (4.6) an. Für Beispiel 4.4.4 ergeben sich unverändert 118 Relationen nach 120 Sekunden. Für Beispiel 4.4.3 ergeben sich 142 Relationen nach 59 Sekunden und für Beispiel 4.4.8 bekommen wir 99 Relationen nach 40 Sekunden.*

4.4.6 Relationen aus dem Number Field Sieve

Die bisherigen Methoden der Relationengewinnung beruhten im wesentlichen auf der Bestimmung von Elementen kleiner T_2-Norm in geeigneten Idealen. Durch die Ungleichung zwischen arithmetischem und geometrischem Mittel wurde gewährleistet, daß die Normen der entsprechenden algebraischen Zahlen klein blieben. Ein anderer Ansatz der Relationengewinnung wird im Number Field Sieve verwendet. Beim Number Field Sieve handelt es sich um die zur Zeit asymptotisch beste Methode zum Faktorisieren großer ganzer Zahlen. Beschreibungen dieses Verfahrens sind zu finden in [10], [5], [15]. Die Methode der Relationengewinnung, die jetzt beschrieben wird, ist nicht so universell einsetzbar wie die bisherigen Methoden, und ist als Ergänzung gedacht. Man kann damit manchmal auf schnellem Weg einige gute Relationen dazubekommen. Eine besondere Stärke scheint diese Methode in Verbindung mit der Methode der Ausnahmeprimideale aus dem nächsten Abschnitt bei zufällig erzeugten Körpern kleinen Grades und großer Diskriminante zu entfalten.

Satz 4.4.11 *Sei $\alpha \in K$ und $m_\alpha(t)$ das zugehörige Minimalpolynom aus $\mathbb{Q}[t]$. Dann ist der Normbetrag von $a + b\alpha$ für ganze Zahlen $a, b \in \mathbb{Z}$ mit $b \neq 0$ durch*

$$|N_{K/\mathbb{Q}}(a + b\alpha)| = b^n |m_\alpha(-a/b)|^{[K:\mathbb{Q}(\alpha)]}$$

gegeben.

Beweis: Setze $d_1 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ und $d_2 = [K : \mathbb{Q}(\alpha)]$. Das Minimalpolynom von $a + b\alpha$ ist $b^{d_1} m_\alpha((t - a)/b)$. Folglich $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(a + b\alpha) = (-b)^{d_1} m_\alpha(-a/b)$. Unter Beachtung der Transitivität der Norm erhält man

$$|N_{K/\mathbb{Q}}(a + b\alpha)| = |N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(a + b\alpha)|^{d_2} = b^n |m_\alpha(-a/b)|^{d_2}.$$

□

Satz 4.4.12 *Sei $\alpha \in K$ mit $K = \mathbb{Q}(\alpha)$. Seien $a, b \in \mathbb{Z}$ teilerfremd mit $b \neq 0$. Jedes Primideal $\mathfrak{p}$ mit $a + b\alpha \in \mathfrak{p}$ ist vom Grad eins oder teilt den Index $f = (\mathfrak{o}_K : \mathbb{Z}[\alpha])$. Teilt $\mathfrak{p}$ den Index nicht, so liegt $a + b\alpha$ in keinem weiteren Primideal über derselben Primzahl wie $\mathfrak{p}$.*

Beweis: Sei p die Primzahl von $\mathfrak{p}$. Wir wissen $p \nmid b$, denn sonst $a \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ und a, b nicht teilerfremd. Wir nehmen nun an, daß $p \nmid f$, und wählen $c, d \in \mathbb{Z}$ mit $bc \equiv 1 \bmod p$ und $fd \equiv 1 \bmod p$. Dann ist $\alpha \equiv -ac \bmod \mathfrak{p}$. Für $x \in \mathfrak{o}_K$ ist $fx \in \mathbb{Z}[\alpha]$, also etwa $fx = g(\alpha)$ mit $g(t) \in \mathbb{Z}[t]$ und weiter $x \equiv dg(-ac) \bmod \mathfrak{p}$. Somit ist jedes Element aus $\mathfrak{o}_K$ zu einem Element aus $\{0, 1, \ldots, p-1\}$ kongruent modulo $\mathfrak{p}$ und die erste Behauptung bewiesen. Ist $\mathfrak{q}$ ein weiteres Primideal über p mit $a + b\alpha \in \mathfrak{q}$, so wählen wir oben speziell ein $x \in \mathfrak{p} \backslash \mathfrak{q}$. Wegen $x \equiv dg(-ac) \equiv 0 \bmod \mathfrak{p}$ folgt $p | dg(-ac)$. Wegen $x \equiv dg(-ac) \not\equiv 0 \bmod \mathfrak{q}$ folgt aber $p \nmid dg(-ac)$. Dies ist ein Widerspruch und die zweite Behauptung bewiesen. □

Algorithmus 4.4.13 *(NFS Relationen)*

Eingabe: *Eine Faktorbasis S sowie $\alpha \in K$ mit $K = \mathbb{Q}(\alpha)$ und $a, b \in \mathbb{Z}^{\geq 1}$.*

Ausgabe: *S-Relationen $\alpha_1, \ldots, \alpha_m$.*

1. *(Initialisierung) Setze $k \leftarrow 1$, $l \leftarrow a$ und $m \leftarrow 0$. Berechne das Minimalpolynom von α.*

2. *(Relation gefunden?) Wenn a und b teilerfremd sind, prüfe unter Zuhilfenahme von Satz 4.4.11, ob $l + k\alpha$ eine S-Relation ist. Wenn ja, $m \leftarrow m + 1$ und Ausgabe von $\alpha_m \leftarrow l + k\alpha$.*

3. *(Nächster Kandidat) Wenn $l > -a$, setze $l \leftarrow l - 1$ und gehe zu Schritt 2. Sonst setze $l \leftarrow a$ und $k \leftarrow k + 1$. Wenn $k \leq b$ gehe zu Schritt 2. Terminiere.*

Die Relationskandidaten, die von diesem Algorithmus erzeugt werden, haben keine besonders kleine Norm mehr. Daher müssen große Faktorbasen verwendet werden, um überhaupt Relationen zu erhalten. Entsprechend mehr Relationen sind natürlich zu finden. Die Philosophie hinter Algorithmus 4.4.13 ist, möglichst viele Kandidaten möglichst schnell durchzutesten. Dies steht im Gegensatz zu Algorithmus 4.4.5, bei dem mit Zeitaufwand Relationskandidaten möglichst kleiner Norm erzeugt werden. Algorithmus 4.4.2 steht unter dieser Betrachtungsweise zwischen beiden letzteren Algorithmen. Die Verwendung großer Faktorbasen stößt jedoch bei Klassengruppenberechnungen im Gegensatz zum Number Field Sieve auf ein unangenehmes Problem. Es wurde bereits erwähnt, daß die Berechnung der Hermite Normalform und der Transformationsmatrizen für große Faktorbasen schnell zu aufwendig wird. Algorithmus 4.4.13 ist daher nicht ohne Verwendung von Algorithmus 4.5.1 aus dem nächsten Abschnitt einsetzbar. Wir geben auch dort erst ein kombiniertes Beispiel zur NFS Relationensuche. Es sei noch vorausgreifend angemerkt, daß sich Algorithmus 4.4.13 (momentan) nur für kleine Grade — ungefähr $n \leq 5$ — eignet. Die beteiligten Normen wachsen üblicherweise sehr stark mit n an, große meist doppelte Ausnahmeprimfaktoren treten auf. In entsprechendem Volumen ist die Relationensuche durchzuführen, wobei die Faktorbasis trotz Verwendung von Algorithmus 4.5.1 ziemlich, beziehungsweise zu groß sein muß. Damit zerschlägt sich auch die Hoffnung, aus der besonders bei größeren Graden günstigen Berechnung der Normen der NFS Relationskandidaten Profit zu schlagen.

4.5 Ausnahmeprimideale

Wie in Abschitt 4.3 erläutert liegen sinnvolle Faktorbasisschranken aufgrund der Einschränkung durch Algorithmus 3.2.3 maximal bei ungefähr 1200. Bei festem

Grad n und fester Schranke für die Faktorbasis aber wachsender Diskriminante werden die Smoothnesseigenschaften der Relationskandidaten rasant schlechter, entsprechend dem Verhalten der Kurven in Abbildung 4.3, S. 53, für fallendes C. In dieser Situation können wir uns mit der Methode der Ausnahmeprimideale helfen. Die Idee dieser Methode basiert auf der Beobachtung, daß relativ häufig Relationskandidaten nur deshalb keine Relationen sind, weil ein zu großes Primideal in einfacher Potenz in ihnen aufgeht. Findet man zwei Relationskandidaten α und β, in denen dasselbe große Primideal aufgeht, so kürzt sich dieses Ausnahmeprimideal bei Division heraus und α/β ist eine Relation. Die durch „relativ häufig" angegebene Wahrscheinlichkeit hängt (vermutlich) unter anderem von der Größe der Diskriminante ab und wird für beliebig große Diskriminante beliebig klein werden. Entsprechend kann diese Methode kein vollwertiger Ersatz für eine größere Faktorbasis sein.

Algorithmus 4.5.1 *(Relationensuche mit Ausnahmeprimidealen)*

Eingabe: *Eine Faktorbasis S und eine Schranke $C_e > 0$.*

Ausgabe: *S-Einheiten α_1, α_2, ...*

1. *(Initialisierung) Setze $S_e \leftarrow \{\}$ und $l \leftarrow 0$.*
2. *(Suche) Suche mit einer beliebigen Methode einen ganzalgebraischen Kandidaten α für eine S-Relation.*
3. *(Relation gefunden?) Wir testen mit Algorithmus 4.4.1, ob α eine S-Relation ist, und merken uns den Rest N der Norm von α nach dem Siebschritt. Wenn α eine S-Relation ist, so $l \leftarrow l+1$, Ausgabe von $\alpha_l \leftarrow \alpha$ und gehe zu Schritt 2.*
4. *(Ausnahmeprimideal?) Wenn $N > C_e$ oder N keine Primzahl ist, so gehe zu Schritt 2.*
5. *(Eliminieren) Prüfe für jedes Paar $(N, \beta) \in S_e$, ob α/β eine S-Einheit und nicht rational ist. Wenn ja, so $l \leftarrow l+1$, Ausgabe von $\alpha_l \leftarrow \alpha/\beta$ und gehe zu Schritt 2.*
6. *(Hinzufügen) Setze $S_e \leftarrow S_e \cup \{(N, \alpha)\}$ und gehe zu Schritt 2.*

Die Menge S_e kann als dynamische Erweiterung der Faktorbasis angesehen werden. Ist $(p, \alpha) \in S_e$, so wird durch α und p eindeutig ein Primideal gekennzeichnet. S_e wächst während der Relationensuche und in Abhängigkeit der gefundenen Kandidaten. So ist es möglich, daß man eine erweiterte Faktorbasis erhält, die nur aus „wesentlichen" Primidealen besteht. Auf der anderen Seite wird man bei sehr großen Diskriminanten gar keine Erweiterung bekommen, weil sich keine geeigneten Elemente α (und besonders keine Relationen) finden lassen.

Über die Wahl der Schranke C_e, die einer Schranke für die Faktorbasis entspricht, können wir keine genauen Angaben machen. Sicher ist nur, daß sie wie bei einer normalen Faktorbasis nicht zu groß sein darf, denn dann wird S_e bei großen Diskriminanten zu groß, und auch nicht zu klein, sonst wird die Relationensuche nicht ausreichend unterstützt. Ein erster Ansatz ist, C_e in der Größenordnung von $M_K{}^{\frac{1}{2}}$ zu wählen.

Algorithmus 4.5.1 kann zu verschiedenen Methoden der Relationsuche hinzugeschaltet werden. Der Einsatz lohnt sich erst bei schlechten Faktorisierungseigenschaften der Relationskandidaten bzw. größeren Diskriminanten.

Bei der praktischen Umsetzung von Algorithmus 4.5.1 muß darauf geachtet werden, daß eine möglichst große Zahl an Relationskandidaten in möglichst kurzer Zeit verarbeitet wird. Dies ist ganz wesentlich, weil man von einer sehr geringen Wahrscheinlichkeit ausgeht, Ausnahmeprimidealtreffer zu erzielen. Wir filtern daher die Nichtrelationen zunächst mit der Bedingung $N > C_e$. Danach führen wir ein paar nur notwendige Tests mit Miller-Rabin [5], S. 414, durch, ob N eine Primzahl ist. Dies geht erheblich schneller als der genaue Test, und es bringt keinen Nachteil, sollte einmal ein nichtprimes N durchrutschen. Anschließend muß in S_e nach den Paaren mit vorderem Eintrag N gesucht werden. Es ist günstig, diese Paare von vorneherein zu einem Tupel zusammenzufassen. Für S_e brauchen wir also eine Suchstruktur — Suchschlüssel ist N —, die darauf ausgelegt ist, möglichst schnell Elemente zu finden und einzufügen. Hierfür bieten sich beispielsweise 2-3-4-Bäume an, siehe [8] S. 533 ff. Im Eliminationsschritt schließlich gehen wir wie folgt vor: Sind $(N, \alpha_1), \ldots, (N, \alpha_m) \in S_e$ und α neu, so berechnen wir der Reihe nach $\alpha/\alpha_1, \ldots, \alpha/\alpha_m$ und bestimmen den jeweils minimalen positiven ganzrationalen Nenner d_i, $1 \leq i \leq m$. Gilt $N \nmid d_i$ für ein i, so ist α/α_i eine S-Einheit, sofern N prim ist. Wenn es kein solches i gibt, dann wird α in S_e unter N aufgenommen.

Beispiel 4.5.2 *Wir betrachten den Zahlkörper K, der von $f(t) = t^4 + 213421t^3 - 17777t^2 + 7676768$ erzeugt wird. Die Signatur ist $(2, 1)$ und es gilt $\log_{10}(-D_K) \approx 35.31$, weiter per Eulerprodukt $\log_{10}(R_K) \approx 15.96$, $Cl_K \simeq \mathbb{Z}/6\mathbb{Z}$. Für die Faktorbasis verwenden wir als Schranke 1000, was 153 Primideale vom Grad 1 und 7 Primideale größeren Grades liefert. C_e wird auf 10^8 gesetzt. Für die Relationensuche greifen wir zuerst auf NFS Relationen mit $a = 3000$ und $b = 1000$ und $\alpha = \rho$ zurück. Hiermit können wir höchstens den Rang 153 erreichen, tun dies auch nach 170 Relationen, 719233 Relationskandidaten und 3900 Sekunden. Der Rang der Einheitenmatrix ist zu diesem Zeitpunkt bereits 2. Nun benutzen wir Algorithmus 4.4.9 und erhalten nach weiteren 19 Relationen, 819695 Relationskandidaten und 6700 Sekunden die volle Klassengruppenmatrix vom Rang 160. Das mit Hilfe von h_K und R_K berechnete Residuum der Zetafunktion ζ_K dividiert durch die Approximation des Eulerprodukts $EP_K(1000)$ ergibt einen Wert von 1.0055.*

Nach der NFS Relationensuche enthält S_e 9260 Primzahlen und 9406 *Elemente. 707426 Nichtrelationen wurden nicht näher betrachtet, weil ihr N größer als C_e war. Dann fielen weitere 2297 Nichtrelationen durch den Primzahltest. Übrig blieben 9510 Elemente, von denen 250 zu Treffern gemeinsamer Primzahlen führten. Aus diesen konnten durch Elimination des Ausnahmeprimideals 104 S-Relationen gewonnen werden. Von diesen 104 Relationen war keine rational.*

Bei der anschließenden normalen Relationensuche passieren ungefähr 2150 von 819695 Nichtrelationen den Test $N \leq C_e$. Ungefähr 400 davon scheitern am Primzahltest. Die restlichen 1750 liefern Treffer gemeinsamer Primzahlen, und von diesen werden 500 neu in S_e aufgenommen. Bei den restlichen 1250 Elementen wird das Ausnahmeprimideal eliminiert. Aber bis auf 18 Stück sind alle diese Relationen rational.

Die Verwendung der NFS Relationen und die Berücksichtigung von Ausnahmeprimidealen liefern einen entscheidenden Beitrag zur Klassengruppenberechnung dieses Körpers. 90 Prozent der benötigten Relationen kommen während der NFS Relationensuche in einem Drittel der Gesamtzeit zustande. Ungefähr 60 Prozent der während der NFS Relationensuche gefundenen Relationen und 95 Prozent der während der normalen Relationensuche gefundenen Relationen werden durch Elimination von Ausnahmeprimidealen erzeugt. Übrigens wird die Klassengruppe schon von den 153 Primidealen ersten Grades unter 1000 erzeugt, so daß wir uns auch nur auf NFS Relationen hätten beschränken können.

Algorithmus 4.5.1 kann variiert werden. Eine Idee besteht darin, anstelle eines zwei (oder mehrere) Ausnahmeprimideale zuzulassen. Man würde dazu auf den Primzahltest verzichten. Wie sich zeigt, verschlechtert sich dann die Laufzeit. Es ist ein Mehraufwand zu betreiben, der sich nicht rentiert. Die Wahrscheinlichkeit, daß die Ausnahmeprimideale zweier Elemente übereinstimmen, ist nämlich extrem gering (man kann sie vermutlich ungefähr als Quadrat der Wahrscheinlichkeit, daß nur ein Ausnahmeprimideal übereinstimmt, ansetzen). Ähnliches wird in [10], S. 34, berichtet. Ein Test an unserem Beispiel zeigt, daß keine einzige Relation durch Elimination doppelter Ausnahmeprimideale gewonnen wird.

Eine weitere Idee besteht darin, in S_e zwar nur Elemente mit einem Ausnahmeprimideal aufzunehmen, aber zu versuchen, aus Elementen mit zwei oder mehreren Ausnahmeprimidealen diese Ideale zu eliminieren. Diese Idee hat zwei Nachteile. N muß faktorisiert werden, um die einzelnen Primbestandteile in Erfahrung zu bringen. Einerseits wird der Durchsatz an Kandidaten vermindert und andererseits mit S_e die Eliminationswahrscheinlichkeit vergrößert. Für obiges Beispiel wiegt ersteres schwerer und unter dem Strich verlängert sich die Laufzeit. Der zweite Nachteil besteht darin, daß gefundene S-Relationen schlechter konditioniert sind und in Algorithmus 3.2.3 eine größere Präzision erfordern. Man kann diese Idee mit Algorithmus 4.5.1 durch Einführung einer weiteren kleinen

Schranke, unterhalb derer N dann faktorisiert werden würde, verbinden. Dies könnte vielleicht günstig sein, es liegt aber keine Praxiserfahrung vor.

4.5.1 Verbindung zur Methode der reduzierten Ideale

Die Methode der reduzierten Ideale besteht darin, zu zufällig erzeugten ganzen Idealen $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$, die nur in Primideale der Faktorbasis faktorisieren, bezüglich der T_2-Norm sehr kurze Elemente $\alpha_1 \in \mathfrak{a}_1, \alpha_2 \in \mathfrak{a}_2, \ldots$ zu finden. Dies geschieht am besten mit dem LLL-Algorithmus. Die ganzen Ideale $\alpha_1/\mathfrak{a}_1, \alpha_2/\mathfrak{a}_2, \ldots$ haben dann beschränkte Norm und bei ausreichender Anzahl muß es daher l, k geben mit $\alpha_l/\mathfrak{a}_l = \alpha_k/\mathfrak{a}_k$. Folglich ist α_l/α_k eine S-Einheit. Die Methode wird genau in [20] beschrieben.

Wie wir gesehen haben, besteht bei nicht zu großer Diskriminante meist eine gute Wahrscheinlichkeit, daß bereits viele der α_i selbst S-Einheiten sind. Umso größer die Diskriminante wird, umso häufiger treten aber in $\alpha_i/\mathfrak{a}_i$ Ausnahmeprimideale auf. Im obigen Beispiel ist das (fast) immer der Fall. Eine Gleichung $\alpha_i/\mathfrak{a}_i = \alpha_j/\mathfrak{a}_j$ bedeutet nun eine Übereinstimmung der Ausnahmeprimideale (in gleicher Potenz) sowie eine Übereinstimmung des Anteils, der durch Primideale aus S geliefert wird. Aufgrund der obigen Überlegungen und des Beispiels kann man davon ausgehen, daß Übereinstimmung der Ausnahmeprimideale im wesentlichen nur dann auftritt, wenn nur ein Ausnahmeprimideal in α_i und α_j vorhanden ist. In diesem Fall hätten wir unter Eingabe von α_i und α_j in Algorithmus 4.5.1 durch Elimination eine Relation erhalten, vorausgesetzt, C_e ist groß genug. Für die Gleichheit $\alpha_i/\mathfrak{a}_i = \alpha_j/\mathfrak{a}_j$ muß aber noch der S-Anteil übereinstimmen, um wie oben eine Relation zu bekommen. Diese Überlegungen zeigen, daß die Methode der reduzierten Ideale im wesentlichen durch Algorithmus 4.4.5 kombiniert mit Algorithmus 4.5.1 abgedeckt wird und daß letztere vermutlich für die Relationensuche sogar günstiger sind. Immerhin benötigt die Methode der reduzierten Ideale eine gewisse Vorlaufzeit, bis aufgrund ausreichend vieler gespeicherter Ideale Relationen gefunden werden können. Gegenüber Beispielen aus [20] ergeben sich für die Relationensuche unter Verwendung von Algorithmus 4.4.9 statt Algorithmus 4.4.5 tatsächlich Verschnellerungen um Faktoren im Bereich 100-1000.

Nach demselben Prinzip, wie die Methode der reduzierten Ideale, funktioniert auch die Relationenerzwingung von v. Schmettow, siehe hierzu [21]. Grob gesagt werden zu einem vorgegebenen Primideal $\mathfrak{p}$ ganze Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ beschränkter Norm und algebraische Zahlen $\alpha_1, \alpha_2, \ldots$ mit $\alpha_i \mathfrak{a}_i = \mathfrak{p}^i$ bestimmt. Bei ausreichender Anzahl gibt es $l > k$ mit $\mathfrak{p}^{l-k} = \alpha_l/\alpha_k$. Bei Beispiel 4.5.2 liegen die Werte solcher l für ein paar Primideale getestet im Bereich 2000-5000. Hier ist also auch eine gewisse Vorlaufzeit nötig, die allerdings im Vergleich mit den obigen Werten relativ klein erscheint. Wir verwenden diese Methode jedoch nicht für unser auf das Eulerprodukt gestützte Klassengruppenverfahren. Man erhält zwar eine Klassengruppenmatrix vom Rang s, aber die Determinante ist bei größeren Beispielen ein enormes Vielfaches der eigentlichen Klassenzahl, und es sind noch ähnlich viele Relationen wie ohne Zuhilfenahme der Relationen $\alpha_l/\alpha_k = \mathfrak{p}^{l-k}$ zu finden, bis die Determinante gleich der Klassenzahl bzw. der Rang gleich s wird. Außerdem kann $l-k$ für eine Potenz ziemlich groß werden (bei Beispiel 4.5.2 im Tausender-Bereich), so daß die Relationen dann riesige Einträge besitzen, und es werden auch keine Einheiten geliefert.

Kapitel 5

Anwendungen

In diesem Kapitel werden zwei Anwendungen vorgestellt, welche die während einer Klassengruppenberechnung ermittelten Daten benutzen. Diese Daten sind konkret eine vollständige Faktorbasis S, Relationen $\alpha_1, \ldots, \alpha_k$, welche das ganze S-Einheitengitter erzeugen, und die Ausgaben von Algorithmus 3.2.3 für die Faktorbasis und diese Relationen.

5.1 Die Klasse eines Ideals

In diesem Abschnitt soll beschrieben werden, wie die Klasse eines gegebenen Ideals $\mathfrak{a}$ bestimmt werden kann. Genau gesagt ist die Darstellung von $\mathfrak{a}$ der Form

$$\mathfrak{a} = \alpha \prod_{i=1}^{m} \mathfrak{a}_i^{k_i} \tag{5.1}$$

gesucht, wobei entsprechend (3.1), S. 19, die $\mathfrak{a}_i$ Erzeuger der zyklischen Faktoren der Klassengruppe der Ordnungen c_i sind und $\alpha \in K$, $0 \leq k_i < d_i$ für $1 \leq i \leq m$ gilt.

Wir gehen in zwei Schritten vor. Zuerst ermitteln mit den Methoden des letzten Kapitels ein $\alpha_1 \in \mathfrak{a}$, so daß

$$\alpha_1/\mathfrak{a} = (\mathfrak{p}_1, \ldots, \mathfrak{p}_s)\, v \tag{5.2}$$

mit $v \in \mathbb{Z}^s$ gilt, also $\alpha_1/\mathfrak{a}$ über der Faktorbasis vollständig faktorisiert. Diese Darstellung übersetzen wir im zweiten Schritt in eine Darstellung über $(\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$, wobei ein weiteres $\alpha_2 \in K$ dazukommt.

Zur Erreichung des zweiten Schritts folgen wir zunächst genau dem Vorgehen aus Abschnitt 3.5, jedoch ohne die Diagonalelemente gleich 1 aus H_α herauszukürzen. Dies entspricht einer Verkleinerung der Faktorbasis, und es würde den ersten Schritt unnötig schwierig machen, wählte man diese Faktorbasis. Natürlich ist es auch möglich, eine Zwischenlösung zu wählen; die nachfolgenden Überlegungen verlaufen dann ganz analog.

Wir bilden also die Smith Normalform S_α der unverkleinerten $s \times s$ Matrix H_α und erhalten unimodulare Matrizen U und V, so daß

$$(\mathfrak{p}_1, \ldots, \mathfrak{p}_s)\, U^{-1} S_\alpha = (\alpha_1, \ldots, \alpha_m)\, B_\alpha V. \tag{5.3}$$

An U, V sollen gleich noch Bedingungen gestellt werden.

Die Anzahl der Diagonalelemente ungleich 1 von S_α stimmt mit m überein. Bezeichne S'_α die $m \times m$ Teilmatrix von S_α, die genau alle Diagonalelemente ungleich 1 von S_α enthält:

$$S_\alpha = \left(\begin{array}{c|c} \mathbf{1} & \mathbf{0} \\ \hline \mathbf{0} & S'_\alpha \end{array}\right). \tag{5.4}$$

S'_α stimmt mit der in Abschnitt 3.5 bestimmten Smith Normalform überein.

Sei M eine $s \times s$ Matrix. Wir vereinbaren, daß M_1 die Teilmatrix von M bestehend aus den ersten $s-m$ Spalten und M_2 die Teilmatrix von M bestehend aus den letzen m Spalten ist.

Die Berechnung von S_α muß konsistent zu 3.5 erfolgen. Schließlich sollten in

$$(\mathfrak{p}_1, \ldots, \mathfrak{p}_s)\, (U^{-1})_2$$

dieselben eventuell gebrochenen Ideale als Erzeuger der zyklischen Faktoren auftreten, die dort erhalten werden. Durch genaues Betrachten von H_α ist aber ersichtlich, daß und wie dies möglich ist. Durch elementare Zeilenoperationen läßt sich erstens erreichen, daß in jeder Spalte, deren Diagonalelement 1 ist, ansonsten nur noch Nullen stehen. Zweitens können wir durch simultane Zeilen- und Spaltenvertauschungen die Diagonalelemente ungleich 1 — bei Erhaltung der Reihenfolge — nach unten auf die Diagonale sortieren. Es bietet sich nun im wesentlichen dieselbe Situation wie in Abschnitt 3.5. Die Matrix, von der dort die Smith Normalform berechnet wird, steht jetzt unten rechts. Schließlich ist zu beachten, daß die inversen Transformationen angewendet auf $(\mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ die erzeugenden Primideale unverändert nach hinten bringen.

Wie in Abschnitt 3.5 reduzieren wir jetzt $(U^{-1})_2$ modulo H_α, also $\widetilde{U} = (U^{-1})_2 - H_\alpha A$ mit einem geeigneten A. $\widetilde{U}$ und A stimmen bis auf zwischengeschobene Nullzeilen mit den schon einmal berechneten $\widetilde{U}$ und A überein.

Es folgt daraus, daß analog

$$(\mathfrak{a}_1, \ldots, \mathfrak{a}_m)\, S'_\alpha = (\mathfrak{p}_1, \ldots, \mathfrak{p}_s)\, \widetilde{U} S'_\alpha = (\alpha_1, \ldots, \alpha_k)\, B_\alpha (V_2 - A S'_\alpha) \tag{5.5}$$

gilt.

Wir stellen jetzt den Bezug zur linearen Algebra vollständig her und benutzen die Addition von Zeilenvektoren von Idealen als komponentenweise Multiplikation. Die bisherigen Überlegungen liefern uns

$$\begin{aligned}(\mathfrak{a}_1,\ldots,\mathfrak{a}_m) &= (\mathfrak{p}_1,\ldots,\mathfrak{p}_s)\,\widetilde{U}\\ &= (\mathfrak{p}_1,\ldots,\mathfrak{p}_s)\,(U^{-1})_2 - (\mathfrak{p}_1,\ldots,\mathfrak{p}_s)\,H_\alpha A\\ &= (\mathfrak{p}_1,\ldots,\mathfrak{p}_s)\,(U^{-1})_2 - (\alpha_1,\ldots,\alpha_k)\,B_\alpha A\end{aligned}$$

und daher

$$(\mathfrak{p}_1,\ldots,\mathfrak{p}_s)\,(U^{-1})_2 = (\mathfrak{a}_1,\ldots,\mathfrak{a}_m) + (\alpha_1,\ldots,\alpha_k)\,B_\alpha A. \tag{5.6}$$

Aufgrund der Gestalt von S_α gilt weiter

$$(\mathfrak{p}_1,\ldots,\mathfrak{p}_s)\,(U^{-1})_1 = (\alpha_1,\ldots,\alpha_k)\,B_\alpha V_1. \tag{5.7}$$

Es sollen jetzt die $\mathfrak{p}_i$ durch die $\mathfrak{a}_i$ dargestellt werden. Dazu kombinieren wir (5.6) und (5.7) durch Aneinanderfügen von Zeilenvektoren, denn es gilt $U^{-1} = ((U^{-1})_1|(U^{-1})_2)$, und multiplizieren von rechts mit U. Dies liefert

$$(\mathfrak{p}_1,\ldots,\mathfrak{p}_s) = (\mathfrak{o}_K,\ldots,\mathfrak{o}_K,\mathfrak{a}_1,\ldots,\mathfrak{a}_m)\,U + (\alpha_1,\ldots,\alpha_k)\,B_\alpha(V_1|A)U, \tag{5.8}$$

und die gesuchte Formel zum Umrechnen einer Darstellung in den $\mathfrak{p}_i$ in eine Darstellung in den $\mathfrak{a}_i$ ist gefunden.

Durch Einsetzen von (5.8) in (5.2) sieht man, daß sich die k_i aus den m letzten Einträgen von $-Uv$ ergeben. Allerdings sollte noch $0 \le k_i < c_i$ sein, wobei die c_i die Diagonaleinträge von S'_α sind. Sei U' die Matrix, die aus den letzen m Zeilen von U besteht. Mit der „verallgemeinerten Division mit Rest für Matrizen“ aus Abschnitt 3.5 schreiben wir $-U'v = S'_\alpha Q + R$. Die Einträge von R bilden jetzt die k_i, und wir erhalten alles in allem unter Beachtung von (5.5)

$$\mathfrak{a} = \alpha_1 + (\alpha_1,\ldots,\alpha_k)B_\alpha M + (\mathfrak{a}_1,\ldots,\mathfrak{a}_m)\,R, \tag{5.9}$$

wobei $M = -(V_1|A)Uv + (V_2 - AS'_\alpha)Q$.

Bemerkungen:

Alle beteiligten Matrizen außer v, Q und R brauchen nur einmal berechnet und können dann immer wieder verwendet werden. Die eigentliche Aufgabe besteht nur noch darin, ein $\alpha_1 \in \mathfrak{a}$ zu finden, so daß (5.2) gilt. Eine für viele Körper ausreichende Vorgehensweise ist, in $\mathfrak{a}$ so lange auszuzählen, bis ein geeignetes α_1 gefunden wird. Meistens sind dafür recht wenig Elemente zu bestimmen.

Zur konkreten Berechnung des Hauptidealanteils in (5.1) kann es nötig sein, vorher im Einheitengitter modulo Einheiten oder ähnlich $(B_\alpha M|U_\alpha)$ zu reduzieren.

Mit diesem Verfahren zur Bestimmung der Klasse eines Ideals kann man natürlich auch Hauptidealtests durchführen, und dies sehr effizient. Wir verzichten auf Beispiele an dieser Stelle.

5.2 S-Einheitenberechnung

In Kapitel 3 wurde einiges über die S-Einheitengruppe gesagt. Dort wurde erläutert, daß eine Abbruchbedingung erforderlich ist, die entscheidet, ob mit einigen S-Einheiten bereits die ganze Gruppe erzeugt wurde, und wie dies mit dem Eulerprodukt für vollständige Faktorbasen zu bewerkstelligen ist. Für beliebige Faktorbasen kann zu diesem Zweck mit der Methode des p-ten Wurzelziehens vorgegangen werden. Besteht die Faktorbasis aber nur aus großen Primidealen, ist unklar, wie überhaupt die erforderlichen S-Einheiten bestimmt werden können. Auf direktem Weg ist dies mit den Methoden der Relationensuche des Kapitels 4 nämlich nicht möglich. Es soll jetzt beschrieben werden, wie über den Umweg einer Klassengruppenberechnung beliebige S-Einheiten berechnet werden können.

Wir gehen davon aus, daß die Klassengruppenberechnung bereits durchgeführt wurde und die eingangs erwähnten Daten vorliegen. Zusätzlich sei mit S' die beliebige Faktorbasis gegeben, für welche die S'-Einheiten berechnet werden sollen. Die Idee ist die folgende: Es werden einfach $(S \cup S')$-Einheiten berechnet und die S'-Einheiten daraus als Untergruppe abgeleitet. Weil $S \cup S'$ mit S ebenfalls vollständig ist, wissen wir schon, welche Determinante die resultierende Klassengruppenmatrix haben muß, um fertig zu sein. Auch sollte die Relationensuche kein schwierigeres Problem als bei der vorangegangenen Klassengruppenberechnung darstellen. Die Ableitung der Unterguppenstruktur geschieht mit Hilfe einer Hermite Normalform. Die Ideale aus S' werden in $S \cup S'$ nach hinten sortiert und dazu die Klassengruppenmatrix in unterer Hermite Normalform berechnet. Die $|S'|$ letzen Spalten der zugehörigen Relationsbasismatrix liefern eine Basis der S'-Einheiten (modulo Torsionseinheiten).

Konkret ist es zweckmäßig, wie folgt vorzugehen: Für jedes Primideal $\mathfrak{p} \in S' \backslash S$ suchen wir nach einer $(S \cup S')$-Relation $\alpha \in \mathfrak{p}$, für die $\alpha/\mathfrak{p}$ nur in Primideale aus S faktorisiert. Dann ist man schon fast fertig. Man erweitert die bereits bekannte Klassengruppenmatrix um geeignete Nullzeilen und fügt die Spalten $\nu_{S \cup S'}(\alpha)$ für jedes der obigen α an. Sind nun die Zeilen passend geordnet, so berechnet man eine untere Hermite Normalform und kann dann S'-Einheiten und sogar die S'-Klassengruppe erhalten. Die Details der Handhabung der Transformationsmatrizen sind einfach und werden nicht näher beschrieben. Die Berechnung der speziellen Relationen α setzt im übrigen voraus, daß S ausreichend groß ist.

Zum Schluß sei angemerkt, daß man mit Hilfe der S-Klassengruppe auch Normgleichungen $|N(\alpha)| = k$ lösen kann, wenn S aus allen Primidealen über den Primfaktoren von k besteht.

Kapitel 6

Beispiele

Anhand einiger Beispiele soll nun in tabellarischer Form die Leistungsfähigkeit des Klassengruppenverfahrens verdeutlicht werden. Die Implementierung der Algorithmen erfolgte im Computeralgebra-System KANT V4. Näheres hierzu ist in [9] zu erfahren. Für die Berechnungen wurde eine Sun SparcStation 20 unter SunOS 5.5 verwendet.

In den folgenden Tabellen besteht jeder Eintrag für einen Körper aus drei Zeilen. Die Einträge der ersten Zeile sind:

- K — eine Darstellung des Zahlkörpers (ζ_k bezeichnet eine k-te primitive Einheitswurzel),
- n — der Grad,
- r_2 — der komplexe Anteil der Signatur,
- $\log_{10}(|D_K|)$ — Logarithmus des Diskriminantenbetrags zur Basis 10,
- R_K — der Regulator,
- Cl_K — die Struktur der Klassengruppe notiert als $c_1 \times \ldots \times c_m$, wobei die c_i die Ordnungen der zyklischen Faktoren der Klassengruppe bezeichnen.

In der zweiten Zeile steht

- $f(t)$ — ein den Zahlkörper erzeugendes Polynom.

Die dritte Zeile besteht aus

- C — eine kleine Faktorbasisschranke,
- C'_K — entweder die Minkowskischranke oder die Bachschranke, gekennzeichnet durch ein „M“ oder ein „B“,

- t_C — gibt die Zeit an, die für die Berechnung der Faktorbasis aus Primidealen mit Norm unterhalb von C benötigt wurde. Hierin ist die Reduktion mit Algorithmus 4.3.2 und die Berechnung des Eulerprodukts enthalten,

- $t_{C'_K}$ — gibt die Zeit an, die der Beweis der Vollständigkeit der Faktorbasis mit Algorithmus 4.3.4 unter Verwendung der Schranke C'_K benötigte,

- t_R — die Zeit, die für die Relationensuche mit Algorithmus 4.4.9 notwendig war,

- t_V — die Zeit, die für die Verifikation der S-Klassengruppe mit Algorithmus 3.6.4 gebraucht wurde.

Der Beweis der Vollständigkeit der Faktorbasis hängt unter Verwendung der Bachschranke von GRH ab. Er wurde ausgelassen, wenn sich anstelle von $t_{C'_K}$ ein „–“ findet. Bei zwei Beispielen ist t_R mit einem „*“ gekennzeichnet. Hier wurde anstelle von Algorithmus 4.4.9 der Algorithmus 4.4.5 angewendet. Durch die Verifikation der S-Klassengruppe wird der Regulator nur für die Primteiler von h_K^S getestet und hängt ansonsten von der ausreichenden Approximation des Eulerprodukts ab. Wir beginnen mit einigen durch zufällig gewählte Polynome erzeugten Körpern und gehen dann zu spezielleren Körpern mit interessanteren Klassenzahlen über.

K	n	r_2	$\log_{10}(\|D_K\|)$	R_K	Cl_K	
$f(t)$						
C	C'_K	t_C	$t_{C'_K}$	t_R	t_V	*gesamt*
$\mathbb{Q}(\rho)$	5	2	12.88	217330.08	1	
$t^5 + 7t - 222$						
500	171507_M	6s	590s	5s	0s	601s
$\mathbb{Q}(\rho)$	7	3	12.64	2614.14	1	
$t^7 + 5t^3 - 31$						
500	26279_M	10s	72s	4s	0s	86s
$\mathbb{Q}(\rho)$	9	4	29.21	94425050371.45	9	
$t^9 + 1133$						
500	54266_B	6s	2000s	177s	1s	2184s
$\mathbb{Q}(\rho)$	11	5	16.23	10563.85	1	
$t^{11} + t^7 - 3$						
500	60765_M	17s	900s	10s	0s	927s
$\mathbb{Q}(\rho)$	13	6	29.25	7594433941.11	1	
$t^{13} + 17$						
500	54420_B	12s	920s	310s	0s	1242s
$\mathbb{Q}(\rho)$	15	7	28.89	993382933.54	1	
$t^{15} + t^{14} + t^{13} - 7$						
500	53048_B	29s	1000s	105s	0s	1134s
$\mathbb{Q}(\rho)$	17	8	36.74	$1.578 \cdot 10^{12}$	1	
$t^{17} + 5t^{11} - t + 12$						
300	85866_B	27s	–	170s	0s	197s
$\mathbb{Q}(\rho)$	19	9	32.16	646567462.10	1	
$t^{19} - t^{12} + t^{11} + 4$						
300	65796_B	50s	–	80s	0s	130s

Tabelle 6.1: Beispiele I.

K	n	r_2	$\log_{10}(\lvert D_K\rvert)$	R_K	Cl_K	
$f(t)$						
C	C'_K	t_C	$t_{C'_K}$	t_R	t_V	*gesamt*
$\mathbb{Q}(\rho)$	4	1	9.97	2106.38	2×2	
$t^4 + 8t^3 - 5t^2 + 112t - 93$						
300	11484_M	4s	11s	5s	0s	20s
$\mathbb{Q}(\rho)$	4	1	15.61	195722.90	2×6	
$t^4 + 97t^3 - 552t^2 + 1032t + 481$						
300	15499_B	2s	33s	19s	0s	54s
$\mathbb{Q}(\rho)$	5	1	11.44	9922.48	2	
$t^5 - 37t^4 - 36t^3 + 4t^2 - 5$						
300	25709_M	3s	41s	5s	0s	49s
$\mathbb{Q}(\rho)$	6	3	13.85	84373.90	2	
$t^6 - 2t^5 + t^3 + 42t^2 - 21t + 35$						
300	12199_B	3s	33s	5s	0s	41s
$\mathbb{Q}(\rho)$	6	3	17.31	1175109.39	5	
$t^6 + 9t^5 + 8t^4 - 85t^3 + 43t^2 + 39t + 69$						
300	19067_B	6s	38s	10s	0s	54s
$\mathbb{Q}(\rho)$	7	3	11.15	675.15	2×2	
$t^7 + 2t^6 + t^5 - 7t^2 + 5t + 2$						
300	4760_M	5s	12s	7s	1s	24s
$\mathbb{Q}(\rho)$	8	2	20.59	24226386.96	2	
$t^8 + 3t^7 - 5t^6 - 4t^5 + t^4 - 50t^3 + 96t^2 - 8t - 21$						
300	26971_B	10s	80s	20s	1s	111s
$\mathbb{Q}(\rho)$	9	3	21.85	196733720.90	1	
$t^9 + 3t^8 + 7t^7 - 9t^5 + 12t^4 + 46t^3 + 14t^2 - 64t - 32$						
300	30374_B	7s	122s	14s	0s	143s
$\mathbb{Q}(\rho)$	10	5	18.74	23617.47	10	
$t^{10} - t^8 + 2t^7 + t^6 + t^5 - 2t^4 - t^3 + 5t^2 - 14t + 9$						
300	22337_B	8s	114s	34s	1s	157s

Tabelle 6.2: Beispiele II.

K	n	r_2	$\log_{10}(\lvert D_K\rvert)$	R_K	Cl_K	
$f(t)$						
C	C'_K	t_C	$t_{C'_K}$	t_R	t_V	*gesamt*
$\mathbb{Q}((-23)^{\frac{1}{2}})$	2	1	1.96	1	3	
t^2+23						
3	3_M	0s	0s	0s	0s	1s
$\mathbb{Q}((-23)^{\frac{1}{2}},3^{\frac{1}{2}})$	4	2	4.88	2.63	2×6	
$t^4-2t^3+7t^2-6t+78$						
41	41_M	1s	0s	2s	0s	3s
$\mathbb{Q}((-23)^{\frac{1}{2}},3^{\frac{1}{3}})$	6	3	8.86	56.75	12	
$t^6-3t^5+21t^4-43t^3+135t^2-9t+174$						
500	853_M	8s	1s	3s	0s	12s
$\mathbb{Q}((-23)^{\frac{1}{2}},3^{\frac{1}{4}})$	8	4	13.13	574.27	2×12	
$t^8-4t^7+30t^6-76t^5+283t^4$ $-444t^3+1278t^2-1068t+1158$						
500	23094_M	12s	90s	8s	2s	112s
$\mathbb{Q}((-23)^{\frac{1}{2}},3^{\frac{1}{5}})$	10	5	17.62	103020.51	3	
$t^{10}-5t^9+40t^8-130t^7+545t^6-1207t^5+3285t^4$ $-4350t^3+8130t^2-7215t+8238$						
500	19742_B	17s	103s	26s	1s	147s
$\mathbb{Q}((-23)^{\frac{1}{2}},3^{\frac{1}{6}})$	12	6	22.28	359158.11	$2\times 2\times 12$	
$t^{12}+6t^{11}+51t^{10}+200t^9+915t^8+2526t^7+7735t^6$ $+15138t^5+33435t^4+44220t^3+63891t^2+43938t+47094$						
500	31580_B	29s	310s	39s	10s	388s
$\mathbb{Q}((-23)^{\frac{1}{2}},3^{\frac{1}{7}})$	14	7	27.1	178632294.12	3	
$t^{14}-7t^{13}+63t^{12}-287t^{11}+1421t^{10}-4641t^9+15757t^8$ $-38059t^7+94563t^6-166383t^5+305151t^4-377097t^3$ $+499401t^2-323589t+276798$						
500	46687_B	50s	730s	183s	3s	966s
$\mathbb{Q}((-23)^{\frac{1}{2}},3^{\frac{1}{8}})$	16	8	32.00	559555865.53	2×24	
$t^{16}-8t^{15}+76t^{14}-392t^{13}+2086t^{12}-7784t^{11}+28924t^{10}$ $-81656t^9+227131t^8-489912t^7+1042188t^6-1684200t^5$ $+2693166t^4-3022824t^3+3557868t^2-2264664t+1680198$						
500	65243_B	43s	1850s	909s	8s	2810s

Tabelle 6.3: $\mathbb{Q}((-23)^{\frac{1}{2}},3^{\frac{1}{m}})$ für $m=1,\ldots,8$.

K	n	r_2	$\log_{10}(\lvert D_K\rvert)$	R_K	Cl_K	
$f(t)$						
C	C'_K	t_C	$t_{C'_K}$	t_R	t_V	*gesamt*
$\mathbb{Q}(2^{\frac{1}{2}}, \zeta_{13})$	24	12	35.34	34260599.80	13	
$t^{24} + 2t^{23} - 21t^{22} - 40t^{21} + 211t^{20} + 382t^{19}$ $-1313t^{18} - 2244t^{17} + 5639t^{16} + 9034t^{15} - 17477t^{14}$ $-25920t^{13} + 40507t^{12} + 55092t^{11} - 68957t^{10} - 83134t^{9}$ $+94247t^{8} + 99640t^{7} - 72553t^{6} - 72922t^{5} + 74467t^{4}$ $+34828t^{3} - 15621t^{2} - 14718t + 8191$						
500	79476_B	458s	–	3100s	9s	3567s
$\mathbb{Q}(2^{\frac{1}{35}})$	35	17	64.28	$2.956 \cdot 10^{18}$	1	
$t^{35} - 2$						
500	262862_B	70s	–	4100s	0s	4170s
$\mathbb{Q}(\zeta_{47})$	46	23	75.24	$2.8612 \cdot 10^{17}$	695	
$(t^{47} - 1)/(t - 1)$						
1000	360214_B	111s	–	3300s	120s	3531s

Tabelle 6.4: Beispiele größeren Grades.

K	n	r_2	$\log_{10}(\lvert D_K\rvert)$	R_K	Cl_K	
$f(t)$						
C	C'_K	t_C	$t_{C'_K}$	t_R	t_V	*gesamt*
$\mathbb{Q}((-1234577)^{\frac{1}{2}}, 3^{\frac{1}{2}})$	4	2	14.34	2.63	21×6552	
$t^4 + 617287t^2 + 95261736025$						
800	13085_B	5s	280s	940s*	1s	1226s
$\mathbb{Q}((-4711)^{\frac{1}{2}}, \zeta_5)$	8	4	18.89	7513.29	1144	
$t^8 + 4716t^6 + 8328466t^4 + 6527679671t^2 + 1915873990801$						
500	22693_B	270s	2600s	1600s*	2s	4472s
$\mathbb{Q}(\rho)$	12	6	23.56	30696.62	5×170	
$t^{12} + 36t^{10} - t^9 + 1296t^8 + 108t^7 + 46657t^6 + 2592t^5$ $+1679544t^4 + 46655t^3 + 1296t^2 + 36t + 1$						
500	19721_B	50s	970s	815s	6s	1841s

Tabelle 6.5: Beispiele mit größerer Klassengruppe.

Symbolverzeichnis

B_α	Relationsbasismatrix der S-Einheiten $\alpha_1, \ldots, \alpha_m$
C_K	Idealschranke für K
Cl_K	Klassengruppe von K, $Cl_K = I_K/H_K$
Cl_K^S	S-Klassengruppe von K, $Cl_K^S = I_K^S/H_K^S$
D_K	Diskriminante von K
EP_K, $EP_K(x)$	Eulerprodukt und Anfang des Eulerprodukts von K
K	Algebraischer Zahlkörper
$\mathbb{F}_p$	Endlicher Körper mit p Elementen
H_α	Klassengruppenmatrix der S-Einheiten $\alpha_1, \ldots, \alpha_m$
H_K	Hauptidealgruppe von K
H_K^S	$H_K \cap I_K^S$
I_K	Idealgruppe von K
I_K^S	Von den Primidealen aus S erzeugte Idealgruppe
L	Logarithmenabbildung
M_K	Minkowskischranke von K
$N(\mathfrak{a})$	Norm von $\mathfrak{a} \in I_K$
$\mathfrak{o}_K$	Maximalordnung von K
$\mathbb{P}_K$	Primideale des Zahlkörpers K
Φ_K^S	ν_S kombiniert mit der Logarithmenabbildung L
R_K	Regulator von K
S	Faktorbasis: endliche Menge von Primidealen
S_α	Smith Normalform von H_α
$T_2(x)$	T_2-Norm von $x \in K$
U_α	Einheitenmatrix der S-Einheiten $\alpha_1, \ldots, \alpha_m$
TU_K	Torsionseinheitengruppe von K
U_K	Einheitengruppe von K
U_K^S	$K^\times \cap I_K^S$
$\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$	Ideale von K
α, β, γ	algebraische Zahlen aus K
h_K	Klassenzahl von K
h_K^S	S-Klassenzahl von K
$\nu_S(x)$	gleich $(\nu_{\mathfrak{p}_1}(x), \ldots, \nu_{\mathfrak{p}_s}(x))^t$ wobei $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$
$\nu_\mathfrak{p}$	exponentielle Bewertung zum Primideal $\mathfrak{p}$

$\mathfrak{p}$, $\mathfrak{q}$	Primideale von K
ρ, $\rho^{(i)}$	Nullstellen von $f(t)$
$\zeta_K(s)$	Dedekindsche Zetafunktion von K
$f(t)$	K definierendes Polynom
n	Grad von K
r_1, r_2	Signatur von K
w_K	Anzahl der Torsionseinheiten von K

Literaturverzeichnis

[1] E. Bach: *Explicit bounds for primality testing and related problems*; Math. Comp. 55 (1990); 355-380

[2] E. Bach: *Improved approximations for Euler products*; CMS Conf. Proc. v. 15 (1995); 13-28

[3] J. Buchmann: *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*; Séminaire de Théorie des Nombres, Paris 1988-1989; Birkhäuser; 1990; 27-41

[4] J. Buchmann und H. C. Williams: *On the computation of the class number of an algebraic number field*; Mathematics of Computation 53, 188; 1989; 679-688

[5] H. Cohen: *A Course in Computational Algebraic Number Theory*; Springer-Verlag; Berlin - Heidelberg - New York; 1993

[6] L. J. Goldstein: *A generalization of the Siegel-Walfisz theorem*; Transactions of the American Mathematical Society 149; Providence; 1970; 417-429

[7] J. Hafner und K. McCurley: *A rigorous subexponential algorithm for computation of class groups*; J. Amer. Math. Soc. 2; 1989; 837-850

[8] E. Horowitz, S. Sahni, S. Anderson-Freed: *Grundlagen von Datenstrukturen*; International Thomson Publishing GmbH; Bonn; 1994

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

[10] A. K. Lenstra und H. W. Lenstra, Jr.: *The developement of the number field sieve*; Springer-Verlag; Berlin - Heidelberg - New York; 1993

[11] K. Meyberg: *Algebra, Teil I*; Carl Hanser Verlag; München - Wien; 1980

[12] W. Narkiewicz: *Elementary and Analytic Theory of Algebraic Numbers*; Springer-Verlag; PWN; Polish Scientific Publishers; Warszawa; 1990

[13] J. Neukirch: *Algebraische Zahlentheorie*; Springer-Verlag; Berlin - Heidelberg - New York; 1992

[14] J. Oesterlé: *Versions effectives du Théorèmé de Čhebotarev sous l'Hypothèse de Riemann généralisée*; Astérisque 61; 1979; 165-167

[15] M. Pohst: *Computational Algebraic Number Theory*; Birkhäuser; Basel - Boston - Berlin; 1993

[16] M. Pohst und H. Zassenhaus: *Algorithmic Algebraic Number Theory*; Cambridge University Press; 1989

[17] M. Pohst und H. Zassenhaus: *Über die Berechnung von Klassenzahlen und Klassengruppen algebraischer Zahlkörper*; J. Reine Angew. Math. 361; 1985; 50-72

[18] P. Ribenboim: *Algebraic Numbers*; Wiley-Interscience; New York - London - Sydney; 1972

[19] J. B. Rosser und L. Schoenfeld: *Approximate formulas for some functions of prime numbers*; Illinois J. Math. 6; 1962; 64-94

[20] E. Scheid: *Ein neuer Algorithmus zur Berechnung der Klassenzahl algebraischer Zahlkörper*; Diplomarbeit; Saarbrücken; 1993

[21] J. Graf v. Schmettow: *Beiträge zur Klassengruppenberechung*; Dissertation; Düsseldorf; 1991

[22] K. Wildanger: *Über Grundeinheitenberechnung in algebraischen Zahlkörpern*; Diplomarbeit; Düsseldorf; 1993

[23] A. Wintner: *A factorization of the densities of ideals in algebraic number fields*; American Journal of Mathematics 68; 1946; 273-284

[24] K. Wiertelak: *On the density of some sets of primes II*; Acta Arithmetica 34; 1978; 197-210

[25] H. Zantema: *Class numbers and units*; Computational Methods in Number Theory; Part II; Mathematisch Centrum; Amsterdam; 1987; 213-234