Ein Algorithmus zur Berechnung der Klassenzahl und des Regulators reellquadratischer Ordnungen

Dissertation
zur Erlangung des Grades
des Doktors der Naturwissenschaften
der Technischen Fakultät
der Universität des Saarlandes
von

Christine Stefanie Abel

Saarbrücken
1994

Tag des Kolloquiums:	1.12.1994
Dekan:	Prof. Dr.-Ing. H. Bley
Berichterstatter:	Prof. Dr. J. Buchmann
	Prof. Dr. K. Mehlhorn

An dieser Stelle danke ich Herrn Professor Johannes Buchmann für die stete, engagierte und gute Betreuung. Er nahm sich immer Zeit, meine Fragen geduldig zu beantworten. Unsere zahlreichen Diskussionen motivierten mich stets aufs neue, und seine Vorschläge waren mir immer von Nutzen.

Ferner danke ich Herrn Professor Kurt Mehlhorn für die Übernahme des Koreferates.

Mein Dank geht auch an die Deutsche Forschungsgemeinschaft, die mir im Rahmen eines Stipendiums am Graduiertenkolleg „Effizienz und Komplexität von Algorithmen und Rechenanlagen“ der Universität des Saarlandes die Arbeit an dieser Dissertation ermöglichte.

Volker Müller und Christoph Thiel danke ich für das Korrekturlesen. Bei Eric Schank bedanke ich mich für sein Interesse an meiner Arbeit und bei Andreas Stein für die anregenden Diskussionen über Kettenbrüche.

Schließlich möchte ich es nicht versäumen, meinem Ehemann Martin zu danken, der mir immer mit Rat und Tat zur Seite stand und für die nötige Entspannung sorgte.

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Einleitung

1801 veröffentlichte C. F. Gauß in seinen Disquisitiones Arithmeticae (vgl. [Ga]) die Theorie binärer quadratischer Formen. Darin untersuchte er hauptsächlich die Äquivalenzklassen binärer quadratischer Formen.

Wir gehen im folgenden von einer ganzen Zahl Δ aus, die die Diskriminante einer binären quadratischen Form ist. Auf ihren Äquivalenzklassen läßt sich eine Multiplikation definieren, so daß wir eine endliche, abelsche[1] Gruppe haben, die sogenannte *Klassengruppe* $Cl(\Delta)$. Die Anzahl ihrer Elemente nennen wir die *Klassenzahl* und bezeichnen sie mit $h(\Delta)$. Neben der Berechnung der Klassenzahl interessieren wir uns für die *Struktur* der Klassengruppe: Damit bezeichnen wir die Darstellung von $Cl(\Delta)$ als Produkt zyklischer Untergruppen, deren Ordnungen sich sukzessive teilen.

Seit den Untersuchungen von Gauß stehen diese Größen immer wieder im Mittelpunkt mathematischer Forschung. Zu Beginn der siebziger Jahre dieses Jahrhunderts ermöglichten leistungsfähige Computer auch einen experimentellen Zugang, und sie verhalfen dieser Thematik zu erneuter Aktualität.

H. Cohen und H. W. Lenstra jr. geben einige Heuristiken über Klassenzahlen und Klassengruppen, wie z.B. die Wahrscheinlickeit, daß für positive Diskriminanten $\Delta > 0$ eine Primzahl p die Klassenzahl $h(\Delta)$ teilt, $1 - \prod_{j \geq 2}(1 - p^{-j})$ ist. (vgl. [CoHL]) Umfangreiche Tabellen bestätigen diese Heuristiken.

Ferner existiert eine Verbindung zur Kryptographie: J. Buchmann, R. Scheidler und H. C. Williams stellen in [BSW] ein Verfahren zum öffentlichen Schlüsselaustausch vor, das auf Klassengruppen $Cl(\Delta)$ für $\Delta > 0$ beruht. Die Sicherheit des Verfahrens begründet sich in der Tatsache, daß sich diskrete Logarithmen in der Klassengruppe nicht effizient berechnen lassen, sofern Δ hinreichend groß gewählt ist. In diesem Zusammenhang erweisen sich große Regulatoren als hilfreich.

[1] Die Namensgleichheit mit der Autorin ist rein zufällig. Die Bezeichnung steht für kommutativ und geht auf Niels Henrik Abel, 1802 - 1829, zurück.

1972 entwickelte D. Shanks zur Berechnung der Klassengruppe und gegebenenfalls des Regulators einen deterministischen Algorithmus, der für vorgegebene Diskriminante Δ Laufzeit $O(|\Delta|^{1/5+\epsilon})$ für jedes $\epsilon > 0$ unter Annahme der verallgemeinerten Riemannschen Vermutung hat. Die Laufzeit ist exponentiell in der Länge der Eingabe. Wegen seiner Methode ist der Algorithmus auch unter dem Namen „baby step – giant step“ Algorithmus bekannt. Für positive Diskriminanten $\Delta > 0$ ist er bis heute das asymptotisch beste Verfahren.

Für negative Diskriminanten $\Delta < 0$ konnten J. Hafner und K. McCurley 1988 erstmals die Klassenzahl sowie die Struktur der KLassengruppe mit Hilfe eines Las-Vegas-Verfahrens in subexponentieller Laufzeit $\exp(\sqrt{\ln|\Delta| \cdot \ln\ln|\Delta|})^{\sqrt{2}+o(1)}$ unter Annahme der verallgemeinerten Riemannschen Vermutung berechnen. (vgl. [HaMc]) Beim Las-Vegas-Typus handelt es sich um probabilistische Algorithmen, die nicht mit Sicherheit erfolgreich sind, im Erfolgsfall jedoch mit Sicherheit das korrekte Resultat ausgeben.

Betrachten wir die Methode von J. Hafner und K. McCurley genauer, vermuten wir, daß sich das Prinzip auf $\Delta > 0$ übertragen läßt. Wir wählen einen anderen Zugang: Ausgehend von *reellquadratischen Ordnungen* $\mathcal{O}_\Delta = \mathbb{Z} + \mathbb{Z}(\Delta + \sqrt{\Delta})/2 \subseteq \mathbb{R}$ und der Idealtheorie werden wir die Klassenzahl $h(\Delta)$ und die Struktur der Klassengruppe berechnen. Zusätzlicher Aufwand besteht in der Bestimmung einer Invarianten von $\mathcal{O}_\Delta$, dem Regulator, um den entwickelten Algorithmus erfolgreich beenden zu können. Wir werden dann ein Verfahren herleiten, das ebenfalls subexponentielle Laufzeit hat, die sich nur geringfügig von der für negative Diskriminanten unterscheidet. Insgesamt haben wir somit verifiziert, daß sich Klassenzahlen $h(\Delta)$ und die Struktur der Klassengruppen sowohl für negative als auch für positive Diskriminanten Δ in subexponentieller Laufzeit berechnen lassen, was eine generelle Verbesserung des Verfahrens von D. Shanks darstellt.

J. Buchmann hat das Prinzip von J. Hafner und K. McCurley auf beliebige Zahlkörper mit Diskriminante Δ übertragen, einen Algorithmus skizziert und eine Analyse durchgeführt: Er erhält eine erwartete Laufzeit von $\exp(\sqrt{\ln|\Delta| \cdot \ln\ln|\Delta|})^{1{,}7+o(1)}$ unter Annahme der verallgemeinerten Riemannschen Vermutung und einer weiteren Vermutung, auf die wir in Kapitel 4 näher eingehen werden. Für unseren Spezialfall erhalten wir geringere Komplexität und können auf letztere zusätzliche Annahme verzichten.

1.2 Gliederung der Arbeit

Im restlichen Teil dieses Kapitel legen wir noch einige Schreibweisen und Abkürzungen fest.

Wir beginnen in Kapitel 2 mit den allgemeinen Grundlagen (algebraischer) Zahlkörper, die wir in unserer Arbeit benötigen. Darauf aufbauend führen wir speziell quadratische Zahlkörper und quadratische Ordnungen ein, für die wir weitere Eigenschaften vorstellen. Insbesondere behandeln wir das Konzept der Reduktionstheorie und der Infrastruktur nach D. Shanks. (vgl. [Sh])

Anschließend zitieren wir die notwendigen Resultate aus der Gittertheorie und geben einige Normalformen an: Mit ihrer Hilfe lassen sich aus einem Erzeugendensystem des zugrundeliegenden Gitters eine Basis gewinnen. Außerdem liefert uns eine weitere Normalform die Struktur einer gegebenen abelschen Gruppe.

In Kapitel 4 schildern wir gemäß dem Verfahren von J. Buchmann aus [Bu1] die Grundidee zur Berechnung der Klassenzahl und des Regulators für beliebige Zahlkörper. Wir fassen diese im Algorithmus *CLASSREG* zusammen, für den wir eine asymptotische Laufzeit unter der verallgemeinerten Riemannschen Vermutung und einer zusätzlichen Glattheitsannahme angeben. Basierend auf diesem Algorithmus leiten wir eine neue Strategie zum Lösen von Normgleichungen her. Wir skizzieren die Methode und lösen die wesentlichen Fragestellungen.

Kapitel 5 beschäftigt sich mit der Anwendung des für Zahlkörper formulierten Algorithmus *CLASSREG* auf quadratische Ordnungen mit positiver Diskriminante. Wir arbeiten die wesentlichen Änderungen des ursprünglich für Zahlkörper konzipierten Verfahrens heraus. Diese berücksichtigen wir bei der anschließenden Ausarbeitung und Anpassung der einzelnen Schritte von *CLASSREG* auf reellquadratische Ordnungen. Dabei liegt die wesentliche Aufgabe in der sogenannten Relationengenerierung, indem wir versuchen, ein bestimmtes Gitter probabilistisch zu erzeugen. Falls es uns gelingt, dieses Gitter aufzuspannen, können wir die Klassenzahl, den Regulator sowie die Struktur der Klassengruppe berechnen. Abschließend fassen wir den umgearbeiteten Algorithmus in *QUCLASSREG* zusammen und optimieren seine erwartete Laufzeit.

In Kapitel 6 übertragen wir die allgemein skizzierte Methode zum Lösen von Normgleichungen auf quadratische Zahlkörper und nutzen dabei spezielle Eigenschaften dieses Zahlkörpertyps aus. Abschließend arbeiten wir eine Laufzeitanalyse aus.

Das letzte Kapitel behandelt sogenannte glatte Zahlen und Ideale. Glatte Zahlen enthalten lediglich Primteiler unterhalb einer vorgegebenen Größe. Dann läßt sich für beschränkte Mengen ganzer Zahlen die Anzahl solcher Zahlen nach unten abschätzen. Wir übertragen diese Idee auf glatte Ideale, wobei es uns gelingt, das Resultat bzgl. ganzer Zahlen auf Ideale zu übertragen. Eine Anwendung auf quadratische Ordnungen benötigen wir zur Analyse von *QUCLASSREG* .

1.3 Bezeichnungen

Zur besseren Lesbarkeit fassen wir die wichtigsten Schreibweisen und Abkürzungen der von uns benutzten Terme und Begriffe zusammen.

Bezeichnung von Zahlbereichen

Wir verwenden folgende Symbole zur Bezeichnung von Zahlbereichen:

$\mathbb{N}$	Menge der natürlichen Zahlen (ohne Null),
$\mathbb{N}_0$	Menge der natürlichen Zahlen einschließlich Null,
$\mathbb{P}$	Menge der Primzahlen,
$\mathbb{Z}$	Menge der ganzen Zahlen,
$\mathbb{Q}$	Menge der rationalen Zahlen,
$\mathbb{R}$	Menge der reellen Zahlen,
$\mathbb{R}_{>0}$	Menge der positiven reellen Zahlen,
$\mathbb{C}$	Menge der komplexen Zahlen.

Für $r \in \mathbb{R}$ bezeichnen wir mit $\lfloor r \rfloor$ die größte ganze Zahl z mit $z \leq r$, analog mit $\lceil r \rceil$ die kleinste ganze Zahl z mit $r \leq z$. Ferner sei $[r]$ der ganze Anteil von r, d.h. die ganze Zahl z mit $z \leq r < z + 1$.

Für $r, s \in \mathbb{R}$ mit $r \leq s$ bezeichnen wir mit $[r, s]$ das abgeschlossene Intervall aller reellen Zahlen von r bis s. Berücksichtigen wir nur die ganzen Zahlen innerhalb eines Intervalls, kennzeichnen wir dies mittels $[\![n, m]\!]$ für $n, m \in \mathbb{Z}$ mit $n \leq m$.

Mit log bezeichnen wir den Logarithmus zur Basis 2 sowie mit ln den natürlichen Logarithmus.

(GRH) – Die verallgemeinerte Riemannsche Vermutung

Wir werden einige Aussagen herleiten, die unter Annahme der unbewiesenen verallgemeinerten Riemannschen Vermutung gelten. Diese Aussagen können wir nur beweisen, wenn wir die Vermutung als wahr annehmen. Solchen Resultaten fügen wir die Abkürzung (GRH) zu.

In der gewöhnlichen Riemannschen Vermutung wird angenommen, daß alle komplexen Nullstellen der Riemannschen Zeta-Funktion $\zeta(x)$, deren Realteil zwischen 0 und 1 liegt, einen Realteil von genau 1/2 haben. Die *verallgemeinerte Riemannsche Vermutung* ist die entsprechende Annahme für bestimmte Verallgemeinerungen der Zeta-Funktion $\zeta(x)$, die sogenannten Dirichletschen L-Reihen. Diese Vermutung spielt in der analytischen Zahlentheorie eine große Rolle.

O–Notation

Sei $f : \mathbb{N}_0 \longrightarrow \mathbb{R}_{>0}$ eine Funktion, dann bezeichnen wir mit $O(f)$ die Menge der Funktionen $g : \mathbb{N}_0 \longrightarrow \mathbb{R}_{>0}$, für die es eine Konstante $c > 0$ gibt, so daß für fast alle $n \in \mathbb{N}_0$ gilt:

$$g(n) \leq c \cdot f(n).$$

Die Funktion L_z

Die Laufzeitanalyse einiger Algorithmen führen wir asymptotisch durch. Hierzu führen wir für $z \in \mathbb{Z}$ die Funktion

$$L_z = \exp \sqrt{\ln |z| \cdot \ln \ln |z|} \tag{1.1}$$

ein. Darauf basierend definieren wir Potenzen von L_z. Für $c \in \mathbb{R}_{>0}$ sei

$$L_z[c] = L_z^{c+o(1)} = \exp \left(\sqrt{\ln |z| \cdot \ln \ln |z|} \cdot (c + o(1)) \right). \tag{1.2}$$

Für diese Schreibweise gelten z.B. $2L_z[c] = L_z[c]$ sowie $L_z[c_1] \cdot L_z[c_2] = L_z[c_1 + c_2]$ und $L_z[c_1] + L_z[c_2] = L_z[\max\{c_1, c_2\}]$ für $c_1, c_2 \in \mathbb{R}_{>0}$ und $|z| \to \infty$.

Die Darstellung von Algorithmen

Zur übersichtlichen Darstellung unserer Algorithmen wählen wir eine modifizierte Form der von I. Nassi und B. Shneiderman in [NaSh] eingeführten Struktogramme. Da diese meist bereits in den Einführungsvorlesungen der Informatik in ähnlicher Form vorgestellt werden und überdies selbsterklärend sind, verzichten wir hier auf eine ausführliche Erläuterung.

Kapitel 2

Grundlagen aus der Zahlentheorie

Wir beginnen mit der Charakterisierung algebraischer Zahlkörper und der Vorstellung der wichtigsten Resultate. Danach beschränken wir uns auf quadratische Zahlkörper sowie quadratische Ordnungen und beschreiben deren spezifische Eigenschaften.

2.1 Beliebige Zahlkörper

Die hier beschriebenen Grundbegriffe und Eigenschaften sowie weitere Details sind unter anderem in [Nk] bzw. [PhZa] zu finden.

2.1.1 Grundbegriffe und Eigenschaften

2.1 Definition *Ein (algebraischer) Zahlkörper ist ein Vektorraum über $\mathbb{Q}$ endlicher Dimension, der zusätzlich ein Teilkörper von $\mathbb{C}$ ist.*

Wir betrachten nun einen Zahlkörper $\mathcal{K}$ der Dimension d. Mit dem Satz über primitive Elemente (vgl. [Hu], Prop. 6.15) existiert ein Element $\rho \in \mathcal{K}$, das für $\mathcal{K}$ eine $\mathbb{Q}$-Basis der Form $\{1, \rho, \rho^2, \ldots, \rho^{d-1}\}$ liefert. Dies kürzen wir mit der Schreibweise

$$\mathcal{K} = \mathbb{Q}(\rho)$$

ab. Dann hat jedes Element $\alpha \in \mathcal{K}$ eine eindeutige Darstellung der Form

$$\alpha = \sum_{j=0}^{d-1} q_j \rho^j, \qquad q_j \in \mathbb{Q} \text{ für } 0 \leq j \leq d-1, \tag{2.1}$$

die wir im folgenden zugrundelegen. Ferner ist ρ Nullstelle eines irreduziblen Polynoms

$$f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Q}[x] - \{0\}, \tag{2.2}$$

das bzgl. ρ eindeutig ist. Die übrigen Nullstellen $\rho^{(2)}, \ldots, \rho^{(d)}$ von $f(x)$ heißen die *Konjugierten* von $\rho = \rho^{(1)}$. Analog definieren wir die Konjugierten von α mit Hilfe von (2.1) als $\alpha^{(i)} = \sum_{j=0}^{d-1} q_j \rho^{(i)j}$ für $1 \leq i \leq d$.

2.2 Definition *Für einen Zahlkörper $\mathcal{K}$ und ein primitives Element ρ heißt das Polynom in (2.2) ein erzeugendes Polynom von $\mathcal{K}$.*

Arithmetik in Zahlkörpern

Gegeben seien zwei beliebige Elemente $\alpha, \beta \in \mathcal{K}$ gemäß (2.1). Da $\mathcal{K}$ Teilkörper von $\mathbb{C}$ ist, sind Addition $\alpha + \beta$ und Produkt $\alpha\beta$ festgelegt, und die Existenz ihrer Inversen ist geklärt. Die Summe $\alpha + \beta$ läßt sich mittels komponentenweiser Addition direkt in einer Darstellung gemäß (2.1) ermitteln. Für das Produkt und Inversenberechung von $\alpha \neq 0$ ermitteln wir mit Hilfe des folgenden Zusammenhanges die gewünschte Darstellung:

2.3 Proposition *Für einen Zahlkörper $\mathcal{K}$ und ein erzeugendes Polynom $f(x) \in \mathbb{Q}[x]$ mit Nullstelle ρ gilt die Isomorphie*

$$\begin{aligned} \mathcal{K} = \mathbb{Q}(\rho) \quad &\simeq \quad \mathbb{Q}[x]/(f(x) \cdot \mathbb{Q}[x]), \\ \alpha = \sum_{j=0}^{d-1} q_j \rho^j \quad &\longmapsto \quad \sum_{j=1}^{d-1} q_j x^j \ \mathit{mod}\ f(x). \end{aligned} \tag{2.3}$$

Ganzheitsring und ganze Zahlen

Wir betrachten Elemente aus $\mathcal{K}$, die eine zusätzliche Eigenschaft aufweisen.

2.4 Definition *Sei α ein Element eines Zahlkörpers $\mathcal{K}$. Ist α darstellbar als Nullstelle eines über $\mathbb{Q}[x]$ irreduziblen Polynoms $f(x) = x^l + a_{l-1}x^{l-1} + \ldots + a_0 \in \mathbb{Z}[x] - \{0\}$, dann heißt α ganze oder ganzalgebraische Zahl von $\mathcal{K}$.*

Wir fassen die ganzen Elemente von $\mathcal{K}$ in der Menge $\mathcal{O}_\mathcal{K}$ zusammen:

2.5 Proposition *Sei $\mathcal{K}$ ein Zahlkörper der Dimension d. Dann gelten:*
i) $\mathcal{O}_\mathcal{K}$ ist ein Integritätsbereich, d.h. ein nullteilerfreier kommutativer Ring mit Eins.
ii) $\mathcal{O}_\mathcal{K}$ ist ein freier $\mathbb{Z}$-Modul vom Rang d.

Jede Zahl $\alpha \in \mathcal{K}$ kann als $\alpha = \beta/\gamma$ mit $\beta, \gamma \in \mathcal{O}_\mathcal{K}$ geschrieben werden, vgl. $\mathbb{Q}$ und $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$. Wir nennen $\mathcal{O}_\mathcal{K}$ daher den *Ganzheitsring* von $\mathcal{K}$ oder auch die *Maximalordnung* von $\mathcal{K}$. $\mathcal{O}_\mathcal{K}$ kann von einer d-elementigen Menge $\{1, \omega_2, \ldots, \omega_d\} \subseteq \mathcal{O}_\mathcal{K}$ ganzer Elemente erzeugt werden, die wir dann eine *Ganzheitsbasis* von $\mathcal{K}$ nennen. Die Größe

$$\Delta = \Delta_\mathcal{K} = \det(\omega_i^{(j)})^2, \qquad 1 \leq i, j \leq d,$$

ist unabhängig von der Wahl der Ganzheitsbasis. Wir nennen diese Größe die *Diskriminante* des Zahlkörpers $\mathcal{K}$.

Einheiten und Assoziierte

Wir betrachten $\mathcal{O}_\mathcal{K}$ bzgl. der Multiplikation:

2.6 Definition *Die Menge aller Elemente von $\mathcal{O}_\mathcal{K}$, für die ein multiplikatives Inverses existiert, ist eine multiplikative, abelsche Gruppe und heißt die Einheitengruppe von $\mathcal{K}$. Ihre Elemente nennen wir die Einheiten von $\mathcal{K}$. Unterscheiden sich zwei beliebige Elemente von $\mathcal{K}$ nur durch eine Einheit, dann sind sie zueinander assoziiert und heißen Assoziierte .*

Dirichlet hat für die Einheitengruppe bewiesen:

2.7 Satz *Sei $\mathcal{K} = \mathbb{Q}(\rho)$ ein Zahlkörper der Dimension d. Unter den d Konjugierten von ρ seien r_1 reell und $2r_2$ komplex. Dann existieren $r = r_1 + r_2$ Einheiten $\xi, \eta_1, \ldots, \eta_{r-1}$, wobei ξ eine n-te Einheitswurzel ist, so daß jede Einheit η eine eindeutige Darstellung*

$$\eta = \xi^{z_0} \cdot \prod_{i=1}^{r-1} \eta_i^{z_i}$$

besitzt mit $z_i \in \mathbb{Z}$ und $0 \leq z_0 < n$.

$r-1$ nennen wir den *Einheitenrang* von $\mathcal{K}$. Für die Einheiten $\eta_1, \ldots, \eta_{r-1}$ führen wir eine charakteristische Größe ein: Dazu sei $\alpha \in \mathcal{K}$ eine beliebige Zahl. Wir stellen uns die Konjugierten in der Reihenfolge $\alpha^{(1)}, \ldots, \alpha^{(r_1)} \in \mathbb{R}$, $\alpha^{(r_1+1)}, \ldots, \alpha^{(r_1+r_2)}$, $\overline{\alpha^{(r_1+1)}}$, ..., $\overline{\alpha^{(r_1+r_2)}} \in \mathbb{C} - \mathbb{R}$ vor. Dann betrachten wir die Beträge

$$|\alpha|_j = |\alpha^{(j)}|, \quad 1 \leq j \leq r_1 \qquad \text{und} \qquad |\alpha|_j = |\alpha^{(j)}|^2, \quad r_1 + 1 \leq i \leq r_1 + r_2.$$

Für die Einheiten aus obigem Satz berechnen wir die folgende Determinante:

$$R = |\det(\ln |\eta_i|_j)|, \qquad 1 \leq i, j \leq r-1.$$

$R > 0$ ist unabhängig von der speziellen Wahl der Einheiten in Satz 2.7. Wir nennen diese Invariante den *Regulator* des Zahlkörpers.

Normen

2.8 Definition *Für eine Zahl α eines Zahlkörpers $\mathcal{K}$ der Dimension d bezeichnen wir das Produkt $\prod_{i=1}^{d} \alpha^{(i)}$ aller Konjugierten von α als die Norm $N(\alpha)$ von α. Wollen wir den speziellen Bezug zum Zahlkörper betonen, schreiben wir auch $N_{\mathcal{K}/\mathbb{Q}}(\alpha)$.*

Normen haben folgende Eigenschaften:

2.9 Proposition *Seien $\mathcal{K}$ ein Zahlkörper mit $\alpha, \beta \in \mathcal{K}$. Dann gelten:*
i) $N(\alpha) \in \mathbb{Q}$. Ist α ganzalgebraisch, dann ist $N(\alpha) \in \mathbb{Z}$.
ii) Eine ganzalgebraische Zahl ist genau dann Einheit, wenn ihre Norm ± 1 beträgt.
iii) Die Norm ist multiplikativ, d.h. $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.
iv) Für einen Körper $\mathcal{K}_0 \subseteq \mathcal{K}$ haben wir $N_{\mathcal{K}/\mathbb{Q}}(\alpha) = N_{\mathcal{K}_0/\mathbb{Q}}(N_{\mathcal{K}/\mathcal{K}_0}(\alpha))$.

Die normale Hülle

Für einen Beweis in Kapitel 7 benötigen wir einen speziellen Oberkörper von $\mathcal{K}$:

2.10 Definition *Seien $\mathcal{K} = \mathbb{Q}(\rho)$ ein Zahlkörper und Ω ein Körper, der alle Nullstellen des irreduziblen Polynoms von ρ enthält. Bezeichne $f_i : \mathcal{K} \longmapsto \Omega$ mit $f_{i|\mathbb{Q}} = id_{\mathbb{Q}}$ die d Einbettungen von $\mathcal{K}$ in Ω. Der Körper $f_1(\mathcal{K}) \cdot \ldots \cdot f_d(\mathcal{K})$ heißt die normale Hülle von $\mathcal{K}$ über $\mathbb{Q}$.*

Im Gegensatz zu $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ haben wir in Ganzheitsringen $\mathcal{O}_{\mathcal{K}}$ im allgemeinen keine eindeutige Faktorisierung in irreduzible Elmente mehr, wie folgendes Beispiel zeigt: Wählen wir $\mathcal{K} = \mathbb{Q}(\sqrt{-5})$, dann gilt $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, wobei 3, $2 \pm \sqrt{-5}$ irreduzible Elemente sind. Wir gehen zu speziellen Teilmengen von $\mathcal{O}_{\mathcal{K}}$ über, bzgl. derer wieder eine eindeutige Faktorisierung vorliegt.

2.1.2 Die Idealtheorie

2.11 Definition *Sei $\mathcal{K}$ ein Zahlkörper. Eine additive Untergruppe A von $\mathcal{O}_{\mathcal{K}}$ mit $A \cdot \mathcal{O}_{\mathcal{K}} \subseteq A$ heißt (ganzes) Ideal von $\mathcal{O}_{\mathcal{K}}$. Ein (gebrochenes) Ideal von $\mathcal{O}_{\mathcal{K}}$ ist eine Teilmenge A von $\mathcal{K}$, so daß nA ein Ideal von $\mathcal{O}_{\mathcal{K}}$ ist für ein $n \in \mathbb{N}$.*

Über der Menge der (gebrochenen) Ideale von $\mathcal{O}_{\mathcal{K}}$ führen wir Operationen ein, die wir Addition und Multiplikation nennen werden. Seien A, B zwei Ideale von $\mathcal{O}_{\mathcal{K}}$: Dann definieren wir ihre *Summe*

$$A + B = \{\alpha + \beta \mid \alpha \in A \text{ und } \beta \in B\}$$

und ihr *Produkt*

$$AB = \Big\{ \sum_{j=1}^{n} \alpha_j \beta_j \mid n \in \mathbb{N} \text{ und } \alpha_j \in A,\ \beta_j \in B \text{ für } 1 \leq j \leq n \Big\}.$$

Bzgl. der Addition bildet die Menge aller Ideale von $\mathcal{O}_{\mathcal{K}}$ eine Halbgruppe mit dem Nullideal $0\mathcal{O}_{\mathcal{K}} = \{0\}$ als Nullelement und bzgl. der Multiplikation ebenfalls eine Halbgruppe mit Einselement $1\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{K}}$. Von nun an schließen wir das Nullideal in unseren Betrachtungen aus:

Invertierbare Ideale

2.12 Definition *Sei $\mathcal{K}$ ein Zahlkörper und A ein gebrochenes Ideal von $\mathcal{O}_{\mathcal{K}}$. Dann heißt A invertierbar, wenn ein Ideal B aus $\mathcal{O}_{\mathcal{K}}$ mit $AB = \mathcal{O}_{\mathcal{K}}$ existiert.*

In dieser Definition ist das Ideal B eindeutig bestimmt. Deshalb nennen wir B das *Inverse* von A. Einfache Umformungen ergeben das folgende Lemma:

2.13 Lemma *Für einen beliebigen Zahlkörper $\mathcal{K}$ bildet die Menge $\mathcal{I}$ aller von $\{0\}$ verschiedenen Ideale von $\mathcal{O}_{\mathcal{K}}$ eine multiplikative abelsche Gruppe.*

Betrachten wir Produkte von Idealen, führen wir den Begriff der Teilbarkeit ein:

2.14 Definition *Seien A,B Ideale aus $\mathcal{I}$. Wir sagen A teilt B, wenn ein ganzes Ideal C in $\mathcal{I}$ existiert mit $AC = B$. A und C heißen Teiler von B.*

In diesem Zusammenhang behandeln wir das Problem der eindeutigen Faktorisierung in sogenannte Primideale, die den Primzahlen in $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ entsprechen.

Primideale

2.15 Definition *Sei P ein ganzes Ideal von $\mathcal{O}_{\mathcal{K}}$. P heißt Primideal von $\mathcal{O}_{\mathcal{K}}$, wenn für jedes Produkt von Elementen α, $\beta \in \mathcal{K}$ mit $\alpha\beta \in P$ folgt, daß mindestens einer der Faktoren in P liegt, d.h. $\alpha \in P$ oder $\beta \in P$ gilt.*

In $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ sind die Primideale genau die Ideale $p\mathbb{Z}$ mit $p \in \mathbb{P}$. Allgemein erhalten wir folgendes Resultat:

2.16 Satz *Sei $A \in \mathcal{I}$ ein beliebiges Ideal von $\mathcal{O}_{\mathcal{K}}$ bzgl. eines Zahlkörpers $\mathcal{K}$, dann besitzt A eine eindeutige – bis auf die Reihenfolge der Faktoren – Darstellung als Produkt von Primidealen P_j von $\mathcal{O}_{\mathcal{K}}$, d.h.*

$$A = \prod_{j=1}^{l} P_j^{e_j},$$

wobei $l \in \mathbb{N}_0$ und $e_j \in \mathbb{Z}$ für $1 \leq j \leq l$ gilt.

Wir wenden dieses Ergebnis auf die Ideale $p\mathcal{O}_{\mathcal{K}}$ mit $p \in \mathbb{P}$ an, dann gilt

$$p\mathcal{O}_{\mathcal{K}} = \prod_{j=1}^{l} P_j^{e_j}, \tag{2.4}$$

wobei $e_j > 0$ und $0 < l \leq d$, der Dimension d von $\mathcal{K}$, gilt. In dieser Zerlegung in Primideale können bestimmte Typen auftreten, die spezielle Namen tragen. Einige spielen auch in unserer Arbeit eine Rolle.

2.17 Definition *In der Situation von (2.4) heißt die Primzahl p total zerlegt bzgl. $\mathcal{O}_\mathcal{K}$, wenn $l = d$ gilt. Ein Primideal P_j in (2.4) heißt unverzweigt bzgl. $\mathcal{O}_\mathcal{K}$, falls der entsprechende Exponent $e_j = 1$ ist, ansonsten heißt P_j verzweigt.*

Normen

Analog zu den Elementen $\alpha \in \mathcal{K}$ führen wir für Ideale Normen ein, wozu wir die eindeutige Zerlegung in Primideale ausnutzen.

2.18 Definition *Sei $\mathcal{K}$ ein beliebiger Zahlkörper und A ein Ideal von $\mathcal{O}_\mathcal{K}$. Die Norm $N(A)$ von A ist der positive Erzeuger des Ideals, das erzeugt wird von den Normen aller Elemente von A , d.h. $N(A) = \mathrm{ggT}\{N(\alpha) \mid \alpha \in A\}$.*

Dann gelten analog zu Proposition 2.9:

2.19 Proposition *Seien $\mathcal{K}$ ein Zahlkörper und $A,\ B \in \mathcal{O}_\mathcal{K}$. Dann gelten:*
i) $N(A) \in \mathbb{Q}$. Ist A ganzes Ideal, dann ist $N(A) \in \mathbb{Z}$.
ii) Falls A das Ideal B teilt, dann teilen sich auch die Normen, d.h. $N(A) \mid N(B)$.
iii) Ist $A = \alpha\mathcal{O}_\mathcal{K}$, dann gilt $N(A) = |N(\alpha)|$.
iv) Die Norm ist multiplikativ, d.h. $N(AB) = N(A) \cdot N(B)$.
v) Für einen Körper $\mathcal{K}_0 \subseteq \mathcal{K}$ haben wir $N_{\mathcal{K}/\mathbb{Q}}(A) = N_{\mathcal{K}_0/\mathbb{Q}}(N_{\mathcal{K}/\mathcal{K}_0}(A))$.

Die Klassenzahl und die Klassengruppe

Wir betrachten nochmals die multiplikative Gruppe $\mathcal{I}$. Jedes Ideal A läßt sich von zwei Elementen $\alpha,\ \beta \in A$ über $\mathcal{O}_\mathcal{K}$ erzeugen, d.h. $A = \alpha\mathcal{O}_\mathcal{K} + \beta\mathcal{O}_\mathcal{K}$. Wir betrachten einen Spezialfall.

2.20 Definition *In einem Zahlkörper nennen wir die Ideale, die sich von genau einem Element über $\mathcal{O}_\mathcal{K}$ erzeugen lassen, Hauptideale.*

Dann folgern wir direkt:

2.21 Lemma *Sei $\mathcal{K}$ ein Zahlkörper. Die Teilmenge $\mathcal{H}$ aller Hauptideale von $\mathcal{I}$ bildet eine Untergruppe von $\mathcal{I}$.*

Daraus resultiert, daß

$$\mathcal{I}/\mathcal{H} = Cl$$

eine multiplikative abelsche Gruppe ist. Diese Zusammenhänge spiegeln sich in der Namensgebung wider.

2.22 Definition *Sei $\mathcal{K}$ ein beliebiger Zahlkörper. Dann heißt Cl die Klassengruppe von $\mathcal{K}$ und ihre Ordnung h die Klassenzahl von $\mathcal{K}$.*

2.23 Satz *Die Klassenzahl eines Zahlkörpers ist endlich, d.h.* $h < \infty$.

Da Cl eine endliche abelsche Gruppe ist, ist Cl darstellbar als endliches direktes Produkt zyklischer Gruppen der Ordnungen $s_1, \ldots, s_l$ mit $s_1 | \ldots | s_l$. (vgl. [Hu], Theorem 2.1) Ist i der kleinste Index mit $s_i \neq 1$, dann nennen wir $(s_i, \ldots, s_l)$ die *Struktur der Gruppe*.

Für das Produkt von Klassenzahl und Regulator haben R. Brauer und C. Siegel einen Zusammenhang mit der Diskriminante bewiesen:

2.24 Satz *Für eine gegebene Dimension d und für alle $\epsilon \in \mathbb{R}_{>0}$ existiert ein Δ_0, so daß für alle Zahlkörper $\mathcal{K}$ der Dimension d mit $|\Delta_{\mathcal{K}}| > \Delta_0$ gilt:*

$$|\Delta_{\mathcal{K}}|^{1/2-\epsilon} \leq h \cdot R \leq |\Delta_{\mathcal{K}}|^{1/2+\epsilon}$$

Zwei Ideale $A,\ B \in \mathcal{I}$ heißen *äquivalent*, wenn sie in der gleichen Äquivalenzklasse liegen, d.h. $A \in B\mathcal{H}$. Wir schreiben

$$A \cong B.$$

Dann existiert ein Element $\beta \in \mathcal{K} - \{0\}$ mit $A = (\beta \mathcal{O}_{\mathcal{K}})B$, A und B unterscheiden sich nur durch ein Hauptideal.

In Kapitel 4 werden wir einen Algorithmus zur Berechnung der Klassenzahl und der Struktur der Klassengruppe vorstellen. Dabei spielen sogenannte reduzierte Ideale eine große Rolle. Diese werden wir jetzt einführen.

Reduzierte Ideale

Zur Definition benötigen wir einige Vorbereitungen. (vgl. [Bu2])

2.25 Definition *Sei A ein ganzes Ideal von $\mathcal{O}_{\mathcal{K}}$.*
i) Eine Zahl $\mu \neq 0$ aus A heißt Minimum von A, falls kein Element $\alpha \in A - \{0\}$ existiert mit $|\alpha|_j < |\mu|_j$, für alle $1 \leq j \leq r_1 + r_2$.
ii) Das Ideal A heißt primitiv, wenn es kein Ideal $z\mathcal{O}_{\mathcal{K}}$ mit $z \in \mathbb{Z}$ gibt, das A teilt.
iii) Mit $L(A)$ bezeichnen wir die kleinste positive ganze Zahl in A. A heißt reduziert, wenn es primitiv und $L(A)$ ein Minimum von A ist.

Für reduzierte Ideale gelten folgende Beschränkungen:

2.26 Satz *Sei $\mathcal{K}$ ein Zahlkörper. Dann gelten:*
i) Die Anzahl aller reduzierten Ideale von $\mathcal{O}_{\mathcal{K}}$ ist endlich.
ii) Ist A reduziert, dann gelten $L(A) \leq \sqrt{|\Delta|}$ und $N(A) \leq |\Delta|^{(d-1)/2}$, wenn $\mathcal{K}$ Dimension d hat.

2.2 Quadratische Zahlkörper

Wir wenden einige der eben geschilderten Resultate speziell auf quadratische Zahlkörper an. Darüber hinaus geben wir noch zusätzliche Eigenschaften.

2.2.1 Grundlegende Eigenschaften

2.27 Definition *Ein Zahlkörper $\mathcal{K}$ der Dimension 2 heißt quadratischer Zahlkörper. Genügt $\mathcal{K} \subseteq \mathbb{R}$, heißt er reellquadratisch, ansonsten imaginärquadratisch.*

Durch elementare Umformungen erhalten wir: (vgl. [We], Seite 233 ff.) Quadratische Zahlkörper $\mathcal{K}$ lassen sich darstellen als

$$\mathcal{K} = \mathbb{Q}(\sqrt{\Delta})$$

mit $\Delta \in \mathbb{Z}$, Δ kein Quadrat und $\Delta \equiv 0, 1 \bmod 4$. Dazu führen wir die Menge

$$\mathcal{D} = \{\Delta \in \mathbb{Z} \mid \Delta \equiv 0, 1 \bmod 4 \text{ und } \Delta \text{ kein Quadrat}\} \tag{2.5}$$

ein, mit der sich alle quadratischen Zahlkörper darstellen lassen. $\{1, \sqrt{\Delta}\}$ ist dann eine $\mathbb{Q}$-Basis von $\mathcal{K}$. Alle Elemente $\alpha \in \mathcal{K}$ sind somit eindeutig darstellbar als $\alpha = q_1 + q_2\sqrt{\Delta}$ mit $q_1,\ q_2 \in \mathbb{Q}$. Mit $\overline{\alpha}$ bezeichnen wir das Konjugierte $q_1 - q_2\sqrt{\Delta}$ von α. Dann berechnet sich die Norm zu $N(\alpha) = \alpha\overline{\alpha} = q_1^2 - \Delta q_2^2$.

Hinsichtlich reellquadratischer Zahlkörper führen wir noch die Teilmenge

$$\mathcal{D}^+ = \{\Delta \in \mathcal{D} \mid \Delta > 0\} \tag{2.6}$$

ein. Allgemein erzeugen zwei Zahlen $\Delta_1, \Delta_2 \in \mathcal{D}$ den gleichen Zahlkörper genau dann, wenn sie sich durch ein Quadrat unterscheiden. Wir führen nun den Begriff der *Ordnung* ein, wo verschiedene Elemente aus $\mathcal{D}$ verschiedene Ordnungen erzeugen.

2.2.2 Quadratische Ordnungen

2.28 Definition *Sei $\Delta \in \mathcal{D}$. Die Menge*

$$\mathcal{O}_\Delta = \mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z}$$

heißt die (quadratische) Ordnung der Diskriminante Δ oder eine Ordnung von $\mathcal{K} = \mathbb{Q}(\sqrt{\Delta})$. Für positive Diskriminante nennen wir die Ordnung reellquadratisch, ansonsten imaginärquadratisch.

Analog zum Zahlkörper definieren wir hier Normen und Konjugierte. Zur Illustration zitieren wir einige Eigenschaften von Ordnungen.

2.29 Proposition *Sei $\mathcal{K}$ ein quadratischer Zahlkörper. Dann gelten:*
i) Eine Teilmenge $\mathcal{O}$ von $\mathcal{K}$ ist eine quadratische Ordnung genau dann, wenn $\mathcal{O}$ ein Teilring mit Eins von $\mathcal{K}$ ist, der als $\mathbb{Z}$-Modul frei vom Rang 2 ist.
ii) Seien $\Delta_1, \Delta_2 \in \mathcal{D}$. Dann ist $\mathcal{O}_{\Delta_1}$ in $\mathcal{O}_{\Delta_2}$ genau dann enthalten, wenn Δ_1/Δ_2 ein Quadrat in $\mathbb{Z}$ ist.
iii) Sei $\mathcal{O}_\Delta$ eine quadratische Ordnung der Diskriminante Δ und Δ_0 der größte quadratfreie Teiler von Δ. Falls $\Delta \equiv 2, 3 \bmod 4$ setze $\Delta_0 = 4\Delta_0$. Dann ist die quadratische Ordnung $\mathcal{O}_{\Delta_0}$ bzgl. der Teilmengenbildung maximal unter allen quadratischen Ordnungen in $\mathcal{K}$.

2.30 Definition *In der Situation von Proposition 2.29iii) heißt die Ordnung $\mathcal{O}_{\Delta_0}$ maximal oder Maximalordnung. Insbesondere heißt die Zahl $f \in \mathbb{N}$ mit $f^2\Delta_0 = \Delta$ der Führer von $\mathcal{O}_\Delta$.*

2.31 Bemerkung Insbesondere gilt in der Situation von Proposition 2.29iii): der Ganzheitsring $\mathcal{O}_\mathcal{K}$ von $\mathcal{K} = \mathbb{Q}(\Delta_0)$ und die Ordnung $\mathcal{O}_{\Delta_0}$ stimmen überein, d.h. $\mathcal{O}_\mathcal{K} = \mathcal{O}_{\Delta_0}$. Maximalordnungen haben günstige Eigenschaften, wie z.B., daß jedes Ideal eine eindeutige Zerlegung in Primideale besitzt. Maximalordnungen zu bestimmen heißt aber, den quadratfreien Anteil von Δ zu berechnen. Dieses Problem hängt mit der Faktorisierung zusammen, was wiederum ein zeitintensives Problem ist.

Wir wenden uns speziellen Teilmengen von Ordnungen zu.

2.2.3 Ideale in quadratischen Ordnungen

2.32 Definition *Seien $\mathcal{K}$ ein quadratischer Zahlkörper und $\mathcal{O}$ eine Ordnung von $\mathcal{K}$. Eine additive Untergruppe A von $\mathcal{O}$ mit $A\mathcal{O} \subseteq A$ heißt (ganzes) Ideal von $\mathcal{O}$. Die Norm $N(A)$ von A ist der positive Erzeuger des Ideals, das erzeugt wird von den Normen aller Elemente von A. Ein (gebrochenes) Ideal von $\mathcal{O}$ ist eine Teilmenge A von $\mathcal{K}$, so daß nA ein Ideal in $\mathcal{O}$ ist für ein $n \in \mathbb{N}$. Die kleinste Zahl mit dieser Eigenschaft heißt der Nenner von A und wird mit $n(A)$ bezeichnet. Die Norm von A ist dann $N(A) = N(n(A)A)/n(A)^2$.*

In unseren Betrachtungen schließen wir von nun an das Null-Ideal der Vereinheitlichung wegen aus.

Ideale in quadratischen Ordnungen lassen sich in einer sogenannten *Standarddarstellung* vereinheitlicht darstellen.

2.33 Proposition *Seien $\mathcal{K}$ ein quadratischer Zahlkörper und $\mathcal{O}_\Delta$ eine Ordnung von $\mathcal{K}$. Eine Teilmenge A von $\mathcal{O}_\Delta$ ist ein (ganzes) Ideal von $\mathcal{O}_\Delta$ genau dann, wenn A in der Form*

$$A = z\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right)$$

dargestellt werden kann mit $a, b, z \in \mathbb{Z}$ und $a, z > 0$ und $4a \mid (\Delta - b^2)$. Bzgl. der Normierung $b \bmod 2a$ ist diese Darstellung eindeutig.

Gebrochene Ideale A von $\mathcal{O}_\Delta$ stellen wir dementsprechend dar als

$$A = \frac{z}{n(A)}\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right) = q\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right). \tag{2.7}$$

Insbesondere gilt für die Standarddarstellung ganzer Ideale:

2.34 Korollar *Ist A ein Ideal von $\mathcal{O}_\Delta$ in Standarddarstellung gemäß (2.7), dann ist $A \subseteq \mathcal{O}_\Delta$ genau dann, wenn $q \in \mathbb{Z}$ gilt.*

Liegen die Ideale in Standarddarstellung vor, lassen sich ihre Normen einfach berechnen. (vgl. [BW])

2.35 Lemma *Sei A ein Ideal von $\mathcal{O}_\Delta$ in Standarddarstellung wie in (2.7). Dann gilt für die Norm von A:*

$$N(A) = q^2 a f(A),$$

wobei wir den Führer $f(A)$ von A wie folgt definieren:

$$f(A) = ggT(a, b, \tfrac{b^2-\Delta}{4a}).$$

Für zwei Ideale in $\mathcal{O}_\Delta$ definieren wir ihr Produkt analog zum Produkt in beliebigen Zahlkörpern. Liegen die Ideale in Standarddarstellung vor, kann das Produkt mit einigen arithmischen Operationen berechnet und wiederum in Standarddarstellung dargestellt werden. (vgl. [SpWi], Seite 624)

2.36 Algorithmus ***MUL***

Eingabe: $\Delta \in \mathcal{D}$, $A_i = z_i(a_i, b_i)$ Ideale in $\mathcal{O}_\Delta$, $i \in \{1, 2\}$
Ausgabe: $z_3(a_3, b_3) = A_3 = A_1A_2$

Berechne den größten gemeinsamen Teiler von a_1, a_2 und $(b_1+b_2)/2$ und seine Darstellung, d.h. $g \leftarrow ggT(a_1, a_2, (b_1+b_2)/2)$ $g \leftarrow ua_1 + va_2 + w(b_1+b_2)/2$	(1)
$z_3 \leftarrow z_1 \cdot z_2 \cdot g$	(2)
$a_3 \leftarrow a_1a_2/g^2$	(3)
$b_3 \leftarrow (ua_1b_2/g + va_2b_1/g + w(b_1+b_2)/(2g)) \bmod 2a_3$	(4)

Aufgrund der durchgeführten Operationen in *MUL* erkennen wir direkt:

2.37 Lemma *Der Algorithmus MUL benötigt bei Eingabe einer Diskriminanten $\Delta \in \mathcal{D}$ und der Standarddarstellung zweier Ideale polynomielle Laufzeit zur Berechnung des Produktes in Standarddarstellung.*

Primideale

Wir wenden uns Primidealen in $\mathcal{O}_\Delta$ zu, die wir analog zu Definition 2.15 einführen. Diese lassen sich in Standarddarstellung auflisten. (vgl. [BW]) Dazu benötigen wir quadratische Reste.

2.38 Definition *Seien $c, l \in \mathbb{Z}$ und $l > 0$. c heißt quadratischer Rest modulo l, wenn eine Zahl $m \in \mathbb{Z}$ existiert mit $m^2 \equiv c \bmod l$.*

Zur Bestimmung aller Primideale in $\mathcal{O}_\Delta$ werden wir unterscheiden, ob Δ ein quadratischer Rest mod $4p$ ist für $p \in \mathbb{P}$. Insbesondere gilt im Quadratfall für die Anzahl der Lösungen: (vgl. [BW])

2.39 Lemma *Seien $\Delta \in \mathcal{D}$ und $p \in \mathbb{P}$. Ist Δ ein quadratischer Rest modulo $4p$, dann existiert genau eine Lösung b_p mit $0 \le b_p \le p$. Für eine weitere Lösung b' gilt $b' \equiv b_p \bmod 2p$.*

Aufgrund dieses Lemmas reden wir daher von *der* Quadratwurzel b_p mod $4p$, wenn wir

$$b_p^2 \equiv \Delta \bmod 4p \qquad \text{mit } 0 \le b_p \le p \tag{2.8}$$

betrachten. Dann ergeben sich alle Primideale aus folgendem Resultat: (vgl. [BW])

2.40 Proposition *Seien $\mathcal{O}_\Delta$ eine Ordnung der Diskriminante $\Delta \in \mathcal{D}$ und $p \in \mathbb{P}$.*
i) Falls Δ quadratischer Rest mod $4p$ ist, dann sind für b_p gemäß (2.8)

$$A_p = p\mathbb{Z} + \frac{b_p + \sqrt{\Delta}}{2}\mathbb{Z} \qquad \textit{und} \qquad \overline{A_p} = p\mathbb{Z} + \frac{2p - b_p + \sqrt{\Delta}}{2}\mathbb{Z}$$

Primideale in $\mathcal{O}_\Delta$ in Standarddarstellung.
ii) Ist Δ kein quadratischer Rest mod $4p$, dann ist

$$A_p = p\mathcal{O}_\Delta$$

Primideal von $\mathcal{O}_\Delta$.
iii) Die Gesamtheit aller Primideale in $\mathcal{O}_\Delta$ wird von den in i) und ii) beschriebenen erfaßt.

In Proposition 2.40i) sind die Ideale A_p und $\overline{A_p}$ genau dann identisch, wenn $b_p = 2p - b_p$ gilt, d.h. $b_p = p$. Daraus folgt wegen (2.8) $p \mid \Delta$. Falls umgekehrt $p \mid \Delta$ gilt, dann folgt aus $b_p^2 - \Delta \equiv 0 \bmod 4p$ die Eigenschaft $p \mid b_p$. Für die drei Fälle in Proposition 2.40 führen wir abkürzend ein Symbol ein:

2.41 Definition *Seien $\Delta \in \mathcal{D}$ und $p \in \mathbb{P}$. Das Kronecker-Symbol ist definiert als*

$$\left(\frac{\Delta}{p}\right) = \begin{cases} -1 & , \textit{ falls } p \nmid \Delta \textit{ und } \Delta \textit{ kein quadratischer Rest mod } 4p \\ 0 & , \textit{ falls } p \mid \Delta \\ 1 & , \textit{ falls } p \nmid \Delta \textit{ und } \Delta \textit{ quadratischer Rest mod } 4p. \end{cases}$$

Zur Berechnung des Kronecker-Symbols verweisen wir auf die ausführliche Beschreibung in [Dü], Seite 43 ff. Für die Laufzeit erhalten wir mit [Co], Seite 23:

2.42 Lemma *Es existiert ein deterministischer Algorithmus, der bei Eingabe von* $\Delta \in \mathcal{D}$ *und* $p \in \mathbb{P}$ *das Kronecker-Symbol* (Δ/p) *in Polynomzeit* $O((\log p)^2 + \log p \cdot \log \Delta)$ *berechnet.*

Wollen wir die Standarddarstellung eines Primideals zu gegebenem $p \in \mathbb{P}$ bestimmen, berechnen wir zuerst (Δ/p). Für $(\Delta/p) = 1$ ermitteln wir eine sogenannte Quadratwurzel b_p gemäß (2.8). Letzteren Fall beinhaltet der folgende Algorithmus:

2.43 Algorithmus *PRIMID*

Eingabe: $\Delta \in \mathcal{D}$, $p \in \mathbb{P}$ mit $(\Delta/p) = 1$
Ausgabe: Primideale A_p und $\overline{A_p}$ in Standarddarstellung

/* Bestimme eine Quadratwurzel b_p mod $4p$ von Δ. */ Löse $b_p^2 \equiv \Delta \bmod 4p$ mit $0 \leq b_p < p$.	(1)
/* Setze A_p, $\overline{A_p}$ gemäß Proposition 2.40 i). */ $A_p = \left(p, (b_p + \sqrt{\Delta})/2\right)$ $\overline{A_p} = \left(p, (2p - b_p + \sqrt{\Delta})/2\right)$	(2)

2.44 Lemma *Der Algorithmus PRIMID ist probabilistisch und berechnet bei Eingabe von* $\Delta \in \mathcal{D}$, $p \in \mathbb{P}$ *mit* (Δ/p) *die Primideale* A_p *und* $\overline{A_p}$. *Die erwartete Laufzeit ist* $O((\log p)^3 + \log \Delta \cdot \log p)$, *also polynomiell.*

Beweis: Wir berechnen eine Quadratwurzel b_p gemäß (2.8). Dazu gibt es eine ausführliche Schilderung in [Dü], Seite 46 ff., die auf der probabilistischen Prozedur RESSOL von D. Shanks beruht. (vgl. [Co], Seite 25 ff.) ■

Invertierbare Ideale

Wir betrachten alle Ideale in $\mathcal{O}$ unter der Verknüpfung der Multiplikation. Wir wissen, daß die Multiplikation assoziativ und $\mathcal{O}$ das Einselement ist. Zu klären bleibt die Existenz von inversen Idealen, wobei wir Definition 2.12 analog übernehmen. Zur Klärung, wann ein Ideal invertierbar ist, zählen wir einige Kriterien auf: (vgl. [BW])

2.45 Proposition *Sei* A *ein Ideal einer quadratischen Ordnung* $\mathcal{O}$. *Dann sind die folgenden Aussagen äquivalent:*
i) A *ist invertierbar.*
ii) Der Führer von A *ist 1, d.h.* $f(A) = 1$.
iii) $A\overline{A} = N(A)\mathcal{O}$, *wobei* $\overline{A}$ *das Ideal bezeichnet, das aus den konjugierten Elementen des Ideals* A *besteht.*

Existiert für ein Ideal in Standarddarstellung das Inverse, kann seine Darstellung direkt bestimmt werden.

2.46 Lemma *Ist $A = \mathbb{Z}a + \mathbb{Z}(b+\sqrt{\Delta})/2$ ein invertierbares Ideal einer quadratischen Ordnung $\mathcal{O}_\Delta$, dann ergibt sich das Inverse zu*

$$A^{-1} = \frac{1}{a}\left(a\mathbb{Z} + \frac{2a-b+\sqrt{\Delta}}{2}\mathbb{Z}\right).$$

Ferner wissen wir für Maximalordnungen, daß jedes gebrochene Ideal invertierbar ist. Überdies besitzen die Normen invertierbarer Ideale die Eigenschaften, wie wir sie von den Maximalordnungen von Zahlkörpern her kennen: (vgl. [BW])

2.47 Lemma *Sei $\mathcal{O}$ eine quadratische Ordnung und A ein Ideal von $\mathcal{O}$. Dann gelten:*
i) Ist A primitives, invertierbares Ideal in Standarddarstellung, dann gilt $N(A) = a$.
ii) Ein primitives Ideal ist genau dann invertierbar, wenn seine Norm und der Führer von $\mathcal{O}$ teilerfremd sind.
iii) Sind A und B invertierbare Ideale von $\mathcal{O}$, dann ist die Norm multiplikativ, d.h. $N(AB) = N(A)N(B)$.
iv) Sei A ein ganzes, invertierbares Ideal, das ein weiteres invertierbares ganzes Ideal B enthält. Dann teilt die Norm von A die Norm von B.

Eindeutige Faktorisierung der Ideale

Ein weiterer Aspekt bzgl. der Primideale ist die eindeutige Faktorisierung eines Ideals in Primideale, wie wir sie für Maximalordnungen von Zahlkörpern kennen. Diese Eindeutigkeit geht uns in beliebigen quadratischen Ordnungen verloren, wie folgendes Gegenbeispiel zeigt: Wähle $\Delta = 20$ und $p = 2$. Dann ist

$$A_2 = 2\mathbb{Z} + \frac{2+\sqrt{20}}{2}\mathbb{Z}$$

Primideal gemäß Proposition 2.40 i) und $b_2 = 2$. Das Quadrat berechnet sich zu

$$A_2^2 = 2\left(2\mathbb{Z} + \frac{2+\sqrt{20}}{2}\right) = (2\mathcal{O}_\Delta)A_2, \qquad (2.9)$$

was wegen $2\mathcal{O}_\Delta \neq A_2$ die eindeutige Zerlegung in Primideale widerlegt. Für einen Spezialfall wissen wir allerdings mit [BW]:

2.48 Satz *Sei $\mathcal{O}_\Delta$ eine quadratische Ordnung der Diskriminante Δ. Dann ist jedes Ideal von $\mathcal{O}_\Delta$, dessen Norm teilerfremd zum Führer von $\mathcal{O}_\Delta$ ist, eindeutig – bis auf die Reihenfolge der Faktoren – darstellbar als Produkt von invertierbaren Primidealen.*

2.2.4 Die Klassenzahl und der Regulator

Zu einer gegebenen quadratischen Ordnung $\mathcal{O}_\Delta$ der Diskriminante Δ bezeichnen wir mit $\mathcal{I}$ die Gesamtheit aller invertierbaren Ideale von $\mathcal{O}_\Delta$. Dann bildet die Menge $\mathcal{I}$ eine multiplikative abelsche Gruppe. Die Teilmenge aller Hauptideale von $\mathcal{O}_\Delta$ nennen wir $\mathcal{H}$. $\mathcal{H}$ ist eine Untergruppe von $\mathcal{I}$, d.h. $\mathcal{H} \leq \mathcal{I}$. Wir erhalten die multiplikative abelsche Faktorgruppe

$$\mathcal{I}/\mathcal{H} = Cl.$$

Wir leiten in Korollar 2.61 des nächsten Abschnittes her, daß Cl eine *endliche* abelsche Gruppe ist, weshalb wir für deren Elementanzahl einen Namen einführen:

2.49 Definition *Zu gegebener quadratischer Ordnung $\mathcal{O}_\Delta$ der Diskriminante Δ heißt die Faktorgruppe Cl bzw. $Cl(\Delta)$ die Klassengruppe von $\mathcal{O}_\Delta$. Deren Ordnung nennen wir die Klassenzahl von $\mathcal{O}_\Delta$ und bezeichnen sie mit h bzw. $h(\Delta)$.*

In diesem Zusammenhang betrachten wir die Einheitengruppe ${\mathcal{O}_\Delta}^\times$ von $\mathcal{O}_\Delta$. Für imaginärquadratische Ordnungen ist sie eine multiplikative, endliche zyklische Gruppe. Für reellquadratische Ordnungen ist ${\mathcal{O}_\Delta}^\times/\langle -1\rangle$ eine multiplikative, unendliche zyklische Gruppe,

$${\mathcal{O}_\Delta}^\times/\langle -1\rangle = \langle \eta \rangle \qquad \text{mit } 1 < \eta \in \mathcal{O}_\Delta$$

eindeutig wählbar. Dann heißt η die *Grundeinheit* von $\mathcal{O}_\Delta$ und mit

$$R_\Delta = R = \ln \eta$$

bezeichnen wir den *Regulator* von $\mathcal{O}_\Delta$.

2.2.5 Reduzierte Ideale in quadratischen Ordnungen

In Analogie zu Maximalordnungen beliebiger Zahlkörper führen wir reduzierte Ideale in quadratischen Ordnungen ein und orientieren uns dabei im wesentlichen an den Arbeiten [KaKw, SpWi, WiWu].

Ein *primitives* Ideal von $\mathcal{O}_\Delta$ ist in Standarddarstellung gegeben als

$$A = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z},$$

und $L(A) = a$ ist das kleinste positive ganze Element in A.

2.50 Definition *Sei A ein primitives Ideal einer quadratischen Ordnung $\mathcal{O}$. A heißt reduziert in $\mathcal{O}$, falls $L(A)$ ein Minimum von A ist, d.h. falls ein Element $\alpha \in A$ mit $|\alpha| < L(A)$ und $|\overline{\alpha}| < L(A)$ existiert, dann gilt $\alpha = 0$.*

Wir geben eine geometrische Interpretation: Betrachten wir für ein Ideal A das zweidimensionale Gitter $\{(\alpha, \overline{\alpha}) \mid \alpha \in A\}$. Dann impliziert A reduziert, daß das offene Rechteck $\{(x,y) \in \mathbb{R}^2 \mid |x| < L(A) \text{ und } |y| < L(A)\}$ keine von 0 verschiedenen Gitterpunkte enthält.

2.51 Bemerkung Da das Produkt primitiver Ideale im allgemeinen nicht mehr primitiv ist, folgern wir, daß auch das Produkt reduzierter Ideale nicht notwendig reduziert ist. Reduzierte Ideale besitzen also keine Gruppenstruktur. Wir werden später feststellen, daß sie eine sogenannte Infrastruktur aufweisen.

Dennoch weisen reduzierte Ideale bedeutende und vorteilhafte Eigenschaften auf.

2.52 Lemma *Sei A ein ganzes Ideal einer quadratischen Ordnung $\mathcal{O}_\Delta$. Dann gelten:*
i) Falls A reduziert ist in $\mathcal{O}_\Delta$, dann gilt $L(A) < \sqrt{\Delta}$.
ii) Falls A primitiv ist und $L(A) < \sqrt{\Delta}/2$, dann ist A reduziert in $\mathcal{O}_\Delta$.

Die Aussage i) und die Tatsache, daß in der Standarddarstellung $b \bmod 2a$ eindeutig bestimmt ist, liefern uns:

2.53 Korollar *i) Ein reduziertes Ideal in Standarddarstellung erfüllt $a < \sqrt{\Delta}$ und $b < 2\sqrt{\Delta}$.*
ii) In quadratischen Ordnungen existieren nur endlich viele reduzierte Ideale.

Dieses Korollar unterstreicht die Bedeutung reduzierter Ideale. Rechnen wir in den nachfolgenden Kapiteln mit reduzierten Idealen, werden wir stets eine Beschränkung von $a,\ b$ bzgl. der Eingabegröße Δ haben.

Für imaginärquadratische Ordnungen gilt sogar: (vgl. [Dü], Satz 2.8)

2.54 Satz *In imaginärquadratischen Ordnungen enthält jede Idealklasse genau ein reduziertes Ideal.*

Wir interessieren uns für die Berechnung reduzierter Ideale. Wie lassen sich alle reduzierten Ideale einer Ordnung bestimmen? Kann zu einem gegebenen (ganzen) Ideal ein äquivalentes reduziertes Ideal ermittelt werden? Zur Beantwortung dieser Fragen stoßen wir auf die Theorie der Kettenbrüche. Hierzu betrachten wir ein primitives Ideal in Standarddarstellung in einer leicht abgewandelten Schreibweise:

$$\begin{aligned} A &= a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z} = a\Big(\mathbb{Z} + \underbrace{\frac{b+\sqrt{\Delta}}{2a}}_{=:\,\phi}\mathbb{Z}\Big) \\ &=: a(\mathbb{Z}, \phi\mathbb{Z}) \end{aligned} \tag{2.10}$$

Von nun an konzentrieren wir uns auf reellquadratische Ordnungen. In diesem Zusammenhang erweist sich der folgende Satz als grundlegendes Resultat:

2.55 Satz *Seien $\Delta \in \mathcal{D}^+$ und $A = \mathbb{Z}a + \mathbb{Z}(b+\sqrt{\Delta})/2$ ein primitives Ideal in $\mathcal{O}_\Delta$ gemäß (2.10). Definiere die Größen q, ϕ', a', b' durch*

$$\begin{aligned} q &= [\phi] = \left[\frac{b+\sqrt{\Delta}}{2a}\right] \\ \frac{1}{\phi'} &= \phi - q \\ b' &= 2aq - b \\ a' &= \frac{\Delta - b'^2}{4a} \end{aligned}$$

Dann ist $a' \in \mathbb{Z}$, und mit

$$\phi' = \frac{b'+\sqrt{\Delta}}{2a'}$$

ist $A' = a'(\mathbb{Z}, \phi'\mathbb{Z})$ ein primitives Ideal von $\mathcal{O}_\Delta$, so daß

$$A' = \frac{a'}{a}\phi' A = -\frac{1}{\overline{\phi'}}A.$$

Auf diese Weise erhalten wir eine iterative Vorschrift, um primitive Ideale zu konstruieren. Ausgehend von einem primitiven Ideal $A_0 = a_0(\mathbb{Z}, \phi_0\mathbb{Z})$ mit $\phi_0 = (b_0 + \sqrt{\Delta})/2a_0$ erhalten wir dann folgende Vorschrift für $j \in \mathbb{N}$:

$$q_{j-1} = [\phi_{j-1}] \tag{2.11}$$

$$b_j = 2a_{j-1}q_{j-1} - b_{j-1} \tag{2.12}$$

$$a_j = \frac{\Delta - b_j^2}{4a_{j-1}}, \tag{2.13}$$

wobei wir wiederum

$$\phi_j = \frac{b_j + \sqrt{\Delta}}{2a_j}$$

setzen. Gemäß einer Bemerkung in [WiWu, SpWi] können wir in (2.11) anstatt $\sqrt{\Delta}$ auch $\lfloor\sqrt{\Delta}\rfloor := D$ nehmen, wobei D in polynomieller Zeit berechnet werden kann. (vgl. [Co], Seite 30 ff.) Wir bestimmen dann q_{j-1} in (2.11) gemäß

$$q_{j-1} = \left[\frac{b_{j-1}+D}{2a_{j-1}}\right]. \tag{2.14}$$

Anwenden von Satz 2.55 impliziert:

2.56 Korollar *Seien $\Delta \in \mathcal{D}^+$ und A_0 ein primitives Ideal von $\mathcal{O}_\Delta$. Dann sind die gemäß (2.11) - (2.13) bestimmten A_j, $j \in \mathbb{N}$, primitive Ideale in $\mathcal{O}_\Delta$, und es gilt*

$$A_j = \Theta_j A_0 \qquad \textit{mit } \Theta_j = \prod_{i=1}^{j} \frac{1}{\overline{\phi_i}} = (-1)^j \frac{a_j}{a_0} \prod_{i=1}^{j} \phi_i, \tag{2.15}$$

wobei sich die Norm zu $N(\Theta_j) = (-1)^j a_j/a_0$ berechnet.

Der Vollständigkeit wegen setzen wir für spätere Anwendungen $\phi_0 = 1$ sowie

$$\Theta_0 = 1 \qquad \textit{und} \qquad A_0 = \Theta_0 A_0.$$

Bzgl. dieser iterativen Entwicklung der ϕ_j und der Reduziertheit des entsprechenden Ideals A_j lassen sich folgende Resultate beweisen:

2.57 Satz *Sei $\mathcal{O}_\Delta$ eine reellquadratische Ordnung. Dann gelten:*
i) Ist $\overline{\phi_j} < 0$, dann ist A_j ein reduziertes Ideal in $\mathcal{O}_\Delta$.
ii) Umgekehrt, falls A_j ein reduziertes Ideal in $\mathcal{O}_\Delta$ ist, dann gilt $-1 < \overline{\phi_j} < 0$.
iii) Falls A_j ein reduziertes Ideal ist, dann sind alle nachfolgend berechneten Ideale A_i mit $i > j$ ebenfalls reduziert.
iv) Sei A_0 ein primitives Ideal und

$$j_0 = \max\left\{2, \frac{\log(a_0/\sqrt{\Delta})}{2\log((1+\sqrt{5})/2)} + \frac{5}{2}\right\}, \tag{2.16}$$

dann ist $\overline{\phi_j} < 0$ für alle $j \geq j_0$. Also sind alle Ideale A_j mit $j \geq j_0$ reduziert.

Wenden wir die Aussage von Satz 2.57ii) auf die Definition des Produktes Θ_j an, erhalten wir:

2.58 Korollar *Starten wir mit einem reduzierten Ideal A_0, ist $|\Theta_j|$ streng monoton wachsend bzgl. $j \in \mathbb{N}_0$.*

Dementsprechend nennen wir die Ausführung einer Iteration von (2.11) - (2.13) auch für nichtreduzierte Ideale einen *Vorwärtsschritt.* Anstatt A_j, A_{j+1}, A_{j+2}, ... schreiben wir in diesem Zusammenhang gelegentlich auch

$$A,\ A_+,\ A_{++},\ \dots\ .$$

Einen solchen Vorwärtsschritt führt der nachfolgend beschriebene Algorithmus aus:

2.59 Algorithmus *FORWARD*

Eingabe: $\Delta \in \mathcal{D}^+$, $D = \lfloor\sqrt{\Delta}\rfloor$, $A = (a, b)$ primitives Ideal in $\mathcal{O}_\Delta$
Ausgabe: $A_+ = (a_+, b_+)$ und q

/* Wende die Iterationen in (2.11) - (2.14) an. */ $q \leftarrow [(b + D)/(2a)]$	(1)
$b_+ \leftarrow 2aq - b$	(2)
$a_+ \leftarrow (\Delta - b_+^2)/(4a)$	(3)

Aus den Operationen in (1) - (3) ergibt sich die Laufzeit:

2.60 Lemma *Der Algorithmus FORWARD benötigt bei Eingabe einer Diskriminanten $\Delta \in \mathcal{D}^+$, $D = \lfloor\sqrt{\Delta}\rfloor$ und der Standarddarstellung von A polynomielle Laufzeit $O((\log a)^2 + (\log \Delta)^2)$ zur Berechnung von A_+. Insbesondere beträgt die Laufzeit für reduzierte Ideale $L_\Delta[0]$.*

Diese Resultate ziehen eine Reihe von Folgerungen nach sich. Starten wir mit einem primitiven Ideal A_0, erhalten wir nach endlich vielen Vorwärtsschritten gemäß Satz 2.57iv) ein reduziertes Ideal A_j, welches äquivalent zum Ausgangsideal A_0 ist. (vgl. (2.15)) Dies impliziert, daß zu jedem beliebigen Ideal in $\mathcal{O}_\Delta$ ein äquivalentes reduziertes Ideal bestimmt werden kann.

Aus diesen Aussagen folgern wir, daß jede Idealklasse von $\mathcal{O}_\Delta$ mindestens ein reduziertes Ideal enthält. Da wegen Lemma 2.53ii) nur endlich viele reduzierte Ideale in $\mathcal{O}_\Delta$ existieren, kann Cl nur endlich viele Elemente, d.h. Idealklassen, besitzen. Also ist ihre Ordnung, die Klassenzahl, endlich. Insgesamt folgt für quadratische Ordnungen. (vgl. Satz 2.54)

2.61 Korollar *Die Klassenzahl quadratischer Ordnungen ist endlich.*

2.62 Satz *Sind $A = A_0$, B zwei reduzierte äquivalente Ideale einer reellquadratischen Ordnung. Dann existiert ein $j \in \mathbb{N}$, so daß $B = A_j$ ist, d.h. aus A_0 wird nach j vielen Vorwärtsschritten B berechnet.*

Insgesamt wissen wir: Falls A_0 ein primitives Ideal ist, erreichen wir nach endlich vielen Iterationen ein reduziertes äquivalentes Ideal, und im Laufe der nachfolgenden Iterationen werden alle reduzierten Ideale dieser Idealklasse bestimmt. Da jede Idealklasse nur endlich viele reduzierte Ideale enthält, wird die Ausführung der Iterationen periodisch. Ist die Länge der Periode l, dann nennen wir die Menge $\{A_0, \ldots, A_{l-1}\}$ einen *Zykel* der Idealklasse von A_0. Innerhalb dieser Zykel führen wir ein Maß ein.

Abstände zwischen reduzierten Idealen

Wir betrachten zwei reduzierte äquivalente Ideale A_0 und B in $\mathcal{O}_\Delta$. Wegen Satz 2.62 wissen wir $B = A_j$ für ein $j \geq 0$. Dabei kann A_j so gewählt werden, daß es innerhalb eines Zykels vorkommt, d.h. $0 \leq j < l$. Dann gilt wegen Korollar 2.15

$$B = A_j = \Theta_j A_0.$$

Ferner folgt aus der Periodizität $B = A_{j+l} = \Theta_{j+l} A_0 = \Theta_l \Theta_j A_0$, wobei $\Theta_l = \eta > 1$ die Grundeinheit von $\mathcal{O}_\Delta$ ist. Allgemein gilt dann für $n \in \mathbb{N}_0$

$$B = A_{j+nl} = \eta^n \Theta_j A_0. \tag{2.17}$$

Aufgrund dieser Zusammenhänge führen wir den *Abstand* $\delta(B, A_0)$ zwischen A_0 und B ein:

$$\delta(B, A_0) = \min\{\ln|\Theta_j| \geq 0 \mid B = \Theta_j A_0\}. \tag{2.18}$$

In dieser Definition nehmen wir den Logarithmus von Θ_j, um den üblichen Vorstellungen von Abständen zu entsprechen. Gemäß Korollar 2.58 ist der Abstand $\delta(A_j, A_0)$ streng monoton wachsend bzgl. $0 \leq j < l$. Ferner ist zum Beispiel $\delta(A_j, A_0) = 0$ genau dann, wenn $j \mid l$, also $A_j = A_0$ gilt. Unter bestimmten Voraussetzungen folgt dann auch die Additivität der Abstände.

Wegen $\ln \eta = R$ folgern wir aus den Herleitungen in (2.17) und der Definition in (2.18)

$$0 \leq \delta(B, A_0) < R.$$

Wir verallgemeinern das Konzept der Abstandsdefinition. Dazu führen wir sogenannte Rückwärtsschritte ein.

Dazu nehmen wir ähnlich wie in (2.11 - 2.13) für ein reduziertes Ideal A_j einen *Rückwärtsschritt* vor, um zu A_{j-1} zu gelangen. Dieser Notation entsprechend schreiben wir auch

$$\ldots,\ A_{--},\ A_{-},\ ,\ A.$$

Die Grundidee zur formalen Beschreibung liegt darin, die ursprünglichen Formeln in (2.11) - (2.13) umzukehren. Ausgehend von einem reduzierten Ideal $A_j = \mathbb{Z}a_j + \mathbb{Z}(b_j + \sqrt{\Delta})/2$ erhalten wir bzgl. $j \in \mathbb{Z}$:

$$\begin{aligned} a_{j-1} &= \frac{\Delta - b_j^2}{4a_j} && (2.19)\\ q_{j-1} &= \left\lfloor \frac{b_j + \sqrt{\Delta}}{2a_{j-1}} \right\rfloor && (2.20)\\ b_{j-1} &= 2q_{j-1}a_{j-1} - b_j. && (2.21) \end{aligned}$$

Dann erhalten wir:

$$\begin{aligned} A_{j-1} &= a_{j-1}\mathbb{Z} + \frac{b_{j-1} + \sqrt{\Delta}}{2}\mathbb{Z} = a_{j-1}\Bigg(\mathbb{Z} + \underbrace{\frac{b_{j-1} + \sqrt{\Delta}}{2a_{j-1}}}_{=:\ \varphi_{j-1}}\mathbb{Z}\Bigg)\\ &=: a_{j-1}(\mathbb{Z}, \varphi_{j-1}\mathbb{Z}). && (2.22) \end{aligned}$$

Durch einen Vorwärtsschritt von A_{j-1} erreichen wir wieder A_j. Den Vorwärtsschritten entsprechend erhalten wir auch hier einen multiplikativen Zusammenhang zwischen A_0 und A_{-j} für $j \in \mathbb{N}_0$:

2.63 Lemma *Seien $\Delta \in \mathcal{D}^+$ und A_0 ein reduziertes Ideal von $\mathcal{O}_\Delta$. Dann sind die gemäß (2.19) - (2.21) bestimmten Ideale A_{-j}, $j \in \mathbb{N}_0$, reduziert in $\mathcal{O}_\Delta$, und es gilt:*

$$A_{-j} = \Upsilon_{-j} A_0 \qquad \textit{mit } \Upsilon_{-j} = \prod_{i=1}^{j} \overline{\varphi_{-i}} = (-1)^j \frac{a_{-j}}{a_0} \prod_{i=1}^{j} \frac{1}{\varphi_{-i}}, \qquad (2.23)$$

wobei wir $\Upsilon_0 = 1$ setzen. Die Norm ergibt sich zu $N(\Upsilon_{-j}) = (-1)^j a_{-j}/a_0$.

Aus der Konstruktion der Rückwärtsschritte können wir einen Zusammenhang zu den Vorwärtsschritten herstellen. Aus $A_{-1} = \overline{\varphi_{-1}} A_0$ erhalten wir $A_l = A_0 =$

$(1/\overline{\varphi_{-1}})A_{-1} = (1/\overline{\varphi_{-1}})A_{l-1}$, woraus wir $\overline{\varphi_{-1}} = \overline{\phi_{l-1}}$ folgern. Analog erhalten wir allgemein für $0 \leq i < l$

$$\overline{\varphi_{-i}} = \overline{\phi_{l-i}}.$$

Aus diesen Vorüberlegungen ergeben elementare Umformungen einen Zusammenhang zwischen Vorwärts- und Rückwärtsschritten.

2.64 Korollar *Sei A_0 ein reduziertes Ideal von $\mathcal{O}_\Delta$ und $j \in \mathbb{N}_0$. Dann gilt für das nach j Rückwärtsschritten erreichte Ideal A_{-j}:*
i) $\Upsilon_{-l} = 1/\eta$
ii) Sei $-j = ql + i$ mit $q, i \in \mathbb{Z}$ und $q < 0$, $0 \leq i < l$. Dann ist $\Upsilon_{-j} = \eta^q \Theta_i$, das entspricht $|ql| > j$ Rückwärtsschritten und i Vorwärtsschritten.

Wir liefern den Algorithmus zum Rückwärtsgehen nach:

2.65 Algorithmus *BACKWARD*

Eingabe: $\Delta \in \mathcal{D}^+$, $D = \lfloor\sqrt{\Delta}\rfloor$, $A = (a, b)$ reduziertes Ideal in $\mathcal{O}_\Delta$
Ausgabe: $A_- = (a_-, b_-)$ und q

/* Wende die Iterationen in (2.19) - (2.21) an. */ $a_- \leftarrow (\Delta - b^2)/(4a)$	(1)
$q \leftarrow [(b + D)/(2a_-)]$	(2)
$b_- \leftarrow 2qa_- - b$	(3)

Aus den Operationen in (1) - (3) ergibt sich folgende Laufzeit:

2.66 Lemma *Der Algorithmus BACKWARD benötigt bei Eingabe einer Diskriminanten $\Delta \in \mathcal{D}^+$, $D = \lfloor\sqrt{\Delta}\rfloor$ und der Standarddarstellung eines reduzierten Ideals A polynomielle Laufzeit zur Berechnung von A_-.*

Zur Vereinfachung werden wir gelegentlich bei einem reduzierten Ideal A von dem *rechten Nachbarn A_+* und dem *linken Nachbarn A_-* sprechen. Innerhalb eines Zykels können wir uns mit Hilfe der Abstände kontrolliert vorwärts- und rückwärtsbewegen.

Wege zwischen reduzierten Idealen

Über den Rahmen der Literatur hinausgehend benötigen wir in dieser Arbeit ein Maß, das auch die Anzahl der Perioden berücksichtigt. Ähnlich wie eben gehen wir von zwei reduzierten äquivalenten Idealen A_j und A_0 aus. Für $j \in \mathbb{N}_0$ erhalten wir bzgl. $A_j = \Theta_j A_0$ analog zur Situation in (2.17)

$$\begin{aligned} \ln|\Theta_j| &= \ln|\Theta_{ql}| + \ln|\Theta_i| \\ &= qR + \delta(A_i, A_0), \end{aligned}$$

wobei wir $j = ql + i$ mit $q, l \in \mathbb{N}_0$ und $0 \leq i < l$ anwenden. Falls j negativ ist, d.h. $A_j = \Upsilon_j A_0$ gilt, gehen wir wiederum von der eindeutigen Darstellung von $j = ql + i$ mit $q, i \in \mathbb{Z}$ und $0 \leq i < l$ aus. Dann gilt mit Korollar 2.64

$$\begin{aligned} \ln|\Upsilon_j| &= \ln|\Upsilon_{ql}| + \ln|\Theta_i| \\ &= qR + \delta(A_i, A_0). \end{aligned}$$

Allgemein definieren wir für $j \in \mathbb{N}_0$

$$\omega(A_j, A_0) = qR + \delta(A_i, A_0) \tag{2.24}$$

und nennen $\omega(A_j, A_0)$ einen (gerichteten) *Weg* von A_0 nach A_j. Diesen Namen wählen wir in Anlehnung daran, daß im alltäglichen Sprachgebrauch Wege zwischen zwei Punkten länger sein können als ihr Abstand. Negative Werte von $\omega(A_j, A_0)$ interpretieren wir als Rückwärtsgehen von A_0 aus, positive Werte entsprechen dann Vorwärtsgehen bzgl. A_0.

Bzgl. der Wege gelten einige Rechenregeln, die sich mittels elementarer Umformungen zeigen lassen.

2.67 Lemma *Seien A_j, A_i beliebige reduzierte, äquivalente Ideale einer reellquadratischen Ordnung $\mathcal{O}_\Delta$. Dann gelten:*
i) Falls $\omega(A_j, A_i) < 0$, dann gilt $j < i$, sonst ist $j \geq i$.
ii) $\omega(A_j, A_i) = \omega(A_j, A_m) + \omega(A_m, A_i)$ für alle $m \in \mathbb{Z}$ zwischen j und i.
iii) $\omega(A_i, A_j) = -\omega(A_j, A_i)$

Wir geben noch einige Abschätzungen für die Weglänge eines oder zweier Vorwärts- bzw. Rückwärtsschritte.

2.68 Lemma *Seien $\mathcal{O}_\Delta$ eine reellquadratische Ordnung und A_j ein reduziertes Ideal von $\mathcal{O}_\Delta$ bzgl. $j \in \mathbb{N}_0$. Dann gelten:*
i) $q_j < 1/|\overline{\phi_{j+1}}| < q_j + 1$
ii) Ist $|\Theta| = 1/(\overline{\phi_{j+1}\phi_{j+2}})$, dann ist $|\Theta| > 2$, d.h. gehen wir von A_j zwei Schritte vorwärts, dann legen wir einen Weg der Länge $> \ln 2$ zurück.
iii) $1 + 1/\sqrt{\Delta} < 1/|\overline{\phi_{j+1}}| < \sqrt{\Delta}$
iv) Entsprechend gelten die Resultate in i) - iii) für Rückwärtsschritte.

Mit Hilfe dieser Abschätzungen erhalten wir obere und untere Schranken für den Regulator. Anwenden eines Resultates aus der analytischen Zahlentheorie verhilft uns zu einer schärferen oberen Schranke.

2.69 Satz *Sei $\mathcal{O}_\Delta$ eine reellquadratische Ordnung. Dann genügt der Regulator den Schranken*

$$\frac{\ln 2}{2} < R < \frac{\sqrt{\Delta}}{4} \cdot (\ln \Delta + 2)\,.$$

Beweis: Für die untere Schranke betrachten wir die Periodenlänge l. Ist $l > 1$, impliziert Lemma 2.68ii) $R \geq \ln|\Theta_2| > \ln 2$. Für $l = 1$ wissen wir $R = (\ln|\Theta_2|)/2 > (\ln 2)/2$, woraus die untere Schranke folgt.
Bzgl. der oberen Schranke wenden wir ein Resultat von H. W. Lenstra jr. aus [HwL], Seite 132 - 133, an, das aus der analytischen Zahlentheorie stammt. Wir wissen dann

$$hR < \frac{\sqrt{\Delta}}{2} \cdot \left(\ln\sqrt{\Delta} + 1\right), \tag{2.25}$$

woraus wegen $h \geq 1$ die Behauptung folgt. ■

2.70 Bemerkung Die Schranken in Satz 2.69 und $\ln|\Theta_l| = R$ legen eine Methode zur Regulatorbestimmung nahe: Mittels l Vorwärtsschritten erhalten wir die Grundeinheit $\eta = \Theta_l$ bzw. den Regulator R. Allerdings können dazu exponentiell viele Vorschrittsschritte bzgl. Δ benötigt werden. Diese Methode erscheint daher weniger geeignet.

Abschließend betrachten wir noch einen anderen Aspekt, die sogenannte

Infrastruktur reellquadratischer Ordnungen,

die auf D. Shanks in [Sh] zurückgeht. Wie bereits in Bemerkung 2.51 erwähnt, haben reduzierte Ideale i. a. keine Gruppenstruktur. Bzgl. der Abstandsdefinition können wir jedoch feststellen, daß reduzierte Ideale innerhalb einer Idealklasse eine gruppenähnliche Struktur besitzen, eine sogenannte *Infrastruktur*.

Wir konzentrieren uns daher auf eine Idealklasse von Cl. Seien H_m ein reduziertes Hauptideal und $A_n \cong A_0$ beliebige reduzierte Ideale. Berechnen wir das Produkt $A_n H_m$, ist gemäß Algorithmus MUL das Ideal

$$\frac{1}{g} A_n H_m \in [A_0]$$

primitiv. Anschließend wird dieses in endlich vielen Vorwärtsschritten (vgl. Satz 2.57) in ein äquivalentes reduziertes Ideal B überführt,

$$B = \frac{\Theta''}{g} A_n H_m \cong A_0.$$

Deshalb existiert wegen Satz 2.62 und der Periode l ein $i \in \mathbb{N}_0$ mit $B = A_i$ reduziert, d.h.

$$A_i = \frac{\Theta''}{g} A_n H_m \cong A_0.$$

Dann läßt sich für $A_n = \Theta_n A_0$ sowie $H_m = \Theta'_m H_0$ mit $H_0 = 1\mathcal{O}_\Delta$ zeigen, daß

$A_i = \Theta_i A_0$ mit

$$\Theta_i = (\Theta''\Theta'_m\Theta_n)/g.$$

Wir interessieren uns für $\omega(A_i, A_0) = \ln|\Theta_i|$, d.h.

$$\omega(A_i, A_0) = \omega(A_n, A_0) + \omega(H_m, H_0) + \ln(|\Theta''|/g).$$

Insbesondere schätzen wir den „Fehler“ $\ln|\Theta''/g|$ ab. Dabei gilt analog zu [SpWi]

$$-\ln\Delta < \ln(|\Theta''|/g) < \ln 2. \tag{2.26}$$

Multiplizieren wir also ein beliebiges reduziertes Ideal mit einem reduzierten Hauptideal und reduzieren das Produkt, ergibt sich der Standort des Ergebnisses aus der Addition der Wege bis auf einen „Fehler“ der Größenordnung $|\ln\Delta|$. Diese Eigenschaft wird als Infrastruktur oder innere Struktur einer Idealklasse bezeichnet. Den „Fehler“ werden wir daher als *Abweichung* bezeichnen. Sie ist relativ gering im Vergleich zum Regulator, wenn wir von einem Regulator der Größenordnung $> \ln|\Delta|$ ausgehen.

Da wir allgemein zwei beliebige reduzierte Ideale A_n, B_m multiplizieren, geben wir im folgenden eine allgemeine algorithmische Formulierung. Mit Algorithmus *MUL* berechnen wir das Produkt A_nB_m und daraus das primitive Ideal $(1/g)A_nB_m$. Dieses transformieren wir mit Hilfe des folgenden Algorithmus in ein äquivalentes reduziertes Ideal. Da wir ferner Θ benötigen, müssen wir es bestimmen. Dies tun wir nicht mittels der iterativen Produktdefinition aus (2.15), sondern wir wenden analog zu [WiWu] folgendes Resultat an:

2.71 Proposition *Sei $A_0 = \mathbb{Z}a_0 + \mathbb{Z}(b_0+\sqrt{\Delta})/2$ ein primitives Ideal einer reellquadratischen Ordnung $\mathcal{O}_\Delta$. Dann gilt für das bzgl. nach j Vorwärtsschritten berechnete Ideal $A_j = \mathbb{Z}a_j + \mathbb{Z}(b_j+\sqrt{\Delta})/2$:*

$$|\Theta_j| = \frac{1}{2a_0}(2a_jv_{j-2} + v_{j-1}b_0 + v_{j-1}\sqrt{\Delta}) \tag{2.27}$$

$$\textit{mit} \quad v_j = q_jv_{j-1} + v_{j-2} \tag{2.28}$$

$$\textit{und} \quad v_{-2} = 1,\ v_{-1} = 0. \tag{2.29}$$

Auf diese Weise berechnen wir $|\Theta_j|$ als iterative Summe. Nun reduzieren wir das Ideal $(1/g)A_nB_m$.

2.72 Algorithmus *REDUCTION*

Eingabe: $\Delta \in \mathcal{D}^+$, $D = \lfloor\sqrt{\Delta}\rfloor$, $A = (a, b)$ primitives Ideal von $\mathcal{O}_\Delta$
Ausgabe: reduziertes zu A äquivalentes Ideal $A_j = (a_j, b_j)$, $|\Theta_j| = (2a, V_j, V_j')$

/* Initialisierung */ $v_{-2} \leftarrow 1, v_{-1} \leftarrow 0, j \leftarrow 1, A_0 \leftarrow A$	(1)
/* Führe einen Vorwärtsschritt aus. */ $(A_j, q_{j-1}) \leftarrow FORWARD\ (\Delta, D, A_{j-1})$	(2)
$v_{j-1} \leftarrow q_{j-1}v_{j-2} + v_{j-3}$	(3)
UNTIL $a_j \leq \lfloor\sqrt{\Delta}\rfloor$	(4)
/* A_j ist reduziert. Bestimme $\|\Theta_j\|$ */	(5)
$V_j \leftarrow 2a_jv_{j-2} + v_{j-1}b_0$	(6)
$V_j' \leftarrow v_{j-1}$	(7)

Bevor wir die Laufzeit abschätzen, ziehen wir ein Resultat aus [WiWu] über die Größe von $|\Theta|$ hinzu.

2.73 Lemma *i) Die in Algorithmus REDUCTION auftretenden Größen erfüllen bei Abbruch nach j_0 Vorwärtsschritten: $|a_j| \leq a_0$ für $0 \leq j \leq j_0$ sowie*

$$0 \leq v_j \leq v_{j_0-1} < a_0/\sqrt{\Delta} \qquad \textit{und} \qquad |V_{j_0}| < a_0.$$

ii) Allgemein gilt auf reduzierten Idealen für Θ_j nach j Vorwärtsschritten in (6), (7) von REDUCTION : $V_j' := v_{j-1} \leq (2\sqrt{\Delta})^{j-1}$ und $|V_j := 2a_jv_{j-2} + b_0v_{j-1}| \leq 3\sqrt{\Delta}V_j'$.

Dann erhalten wir bzgl. der Laufzeit:

2.74 Proposition *Seien A_n, B_m reduzierte Ideale einer reellquadratischen Ordnung $\mathcal{O}_\Delta$. Dann erfordert die Berechnung von $(\Theta/g)A_nB_m$ bei Eingabe von Δ, $\lfloor\sqrt{\Delta}\rfloor$ und A_n, B_m mit den Algorithmen MUL und REDUCTION polynomielle Laufzeit, d.h. $L_\Delta[0]$.*

Beweis: Wir analysieren *MUL* und *REDUCTION* bzgl. $A_nB_m = C_0$.
Die Berechnung des Produktes $(1/g)A_nB_m$ mit *MUL* erfordert gemäß Lemma 2.37 polynomielle Laufzeit bzgl. Δ.
Die anschließende Reduktion und die Bestimmung von $|\Theta|$ mit *REDUCTION* erfordert ebenso polynomielle Laufzeit bzgl. Δ: Ein Vorwärtsschritt in (2) mit *FORWARD* benötigt gemäß Lemma 2.60 Polynomzeit. Ferner braucht die Berechnung von $v_j \in \mathbb{Z}$ in (3) wegen Lemma 2.73 Polynomzeit. Wegen $a_0 < \Delta$ und Satz 2.57iv) wird die Schleife in (2) – (4) $O(\log\Delta)$-mal ausgeführt, so daß sie insgesamt Polynomzeit braucht. Analoges gilt für die anschließende Berechnung von V_j, V_j'. ■

Kapitel 3

Matrix- und Gitternormalformen

Wir führen in diesem Kapitel die Grundbegriffe und Zusammenhänge aus der Gittertheorie ein, auf die wir im Laufe unserer Arbeit zurückgreifen. Wir werden Gitter bzw. ihre Basen gelegentlich mittels Matrizen darstellen, für die wir verschiedene Normalformen berechnen. Diese ermöglichen uns direkt, einige charakteristische Größen abzulesen. Insbesondere bestimmen wir aus Erzeugendensystemen Basen und die Determinante des aufgespannten Gitters. Wir beginnen mit der Klärung der Grundbegriffe. (vgl. [Dü])

3.1 Grundlagen aus der Gittertheorie

Wir starten mit dem Begriff des Gitters und geben einige Eigenschaften.

3.1 Definition *Eine diskrete, additive Untergruppe* Γ *von* $\mathbb{R}^d$ *heißt Gitter. Ist* Γ *sogar in* $\mathbb{Z}^d$ *enthalten, heißt* Γ *auch Gitter in* $\mathbb{Z}^d$*, ansonsten Gitter in* $\mathbb{R}^d$*. Wir schreiben* $\Gamma \leq \mathbb{Z}^d$ *bzw.* $\Gamma \leq \mathbb{R}^d$*. Die maximale Anzahl linear unabhängiger Vektoren in* Γ *bzgl.* $\mathbb{Z}^d$ *bzw.* $\mathbb{R}^d$ *wird als Dimension bezeichnet und als* $\dim \Gamma$ *geschrieben.*

In den nächsten Kapiteln führen wir Gitter Γ in $\mathbb{R}^d$ ein, für die wir $\Gamma \leq \mathbb{Z}^k \times \mathbb{R}^r$ schreiben. Wir verdeutlichen mit dieser Schreibweise, daß die ersten k Koordinaten eines jeden Gittervektors von Γ ganzzahlig sind. Dort spielen auch sogenannte Teilgitter eine wichtige Rolle.

3.2 Definition *Eine nichtleere Teilmenge* Γ_1 *eines Gitters* Γ*, die additive Untergruppe von* Γ *ist, heißt Teilgitter von* Γ*.*

In diesem Sinne ist Γ selbst Teilgitter von $\mathbb{Z}^d$ bzw. $\mathbb{R}^d$. Wir gehen nun von einem d-dimensionalen Gitter aus und interessieren uns für Erzeugendensysteme, insbesondere für solche mit d Elementen, was die kleinstmögliche Anzahl ist. Ferner wissen wir, daß solche stets existieren.

3.3 Definition *Es seien $\underline{v}_1, \ldots, \underline{v}_m$ Vektoren in $\mathbb{R}^d$. Dann bezeichnen wir mit*

$$\Gamma = \mathbb{Z}\underline{v}_1 + \ldots + \mathbb{Z}\underline{v}_m = \Big\{ \sum_{i=1}^{m} z_i \underline{v_i} \mid z_i \in \mathbb{Z} \Big\}$$

das von $\underline{v}_1, \ldots, \underline{v}_m$ aufgespannte Gitter. Unter diesen Bedingungen heißt die Menge $\{\underline{v}_1, \ldots, \underline{v}_m\}$ ein Erzeugendensystem von Γ, besteht sie aus genau $m = \dim \Gamma$ linear unabhängigen Elementen, nennen wir sie eine Basis von Γ.

Wir führen für die Erzeugendensysteme eine Matrixschreibweise ein, die uns eine bessere Handhabung ermöglicht. Für das Erzeugendensystem aus obiger Definition konstruieren wir eine Matrix M, deren Spalten aus den Vektoren $\underline{v}_1, \ldots, \underline{v}_m$ bestehen,

$$M = M(\underline{v}_1, \ldots, \underline{v}_m) = (m_{i,j}).$$

Haben wir umgekehrt eine Matrix M, identifizieren wir mit $\Gamma(M)$ das Gitter, das von den Spalten von M aufgespannt wird. Wir bezeichnen daher auch mit $\Gamma(M)$ *das von M aufgespannte Gitter*. In diesem Zusammenhang erhalten wir:

3.4 Definition *Sei M eine reguläre $d \times d$ Matrix über $\mathbb{Z}$ oder $\mathbb{R}$. Dann heißt $|\det M|$ die Determinante des von M aufgespannten Gitters. Wir schreiben hierfür $\det \Gamma(M) = |\det M|$.*

Die Gitterdeterminante kann geometrisch interpretiert werden als das Volumen des Fundamentalbereichs. Wir stellen noch einen Zusammenhang zwischen Gitterbasen und den entsprechenden Matrizen vor:

3.5 Proposition *Seien M_1, M_2 zwei $d \times m$ Matrizen über $\mathbb{Z}$ oder $\mathbb{R}$. M_1 und M_2 spannen genau dann das gleiche Gitter auf, wenn es eine Martrix $U \in \mathbb{Z}^{m \times m}$ mit Determinante ± 1 und $M_2 = M_1 \cdot U$ gibt.*

Die Matrizen $U \in \mathbb{Z}^{m \times m}$ mit Determinante ± 1 bezeichnen wir als *unimodular*. Sie bilden genau die über $\mathbb{Z}$ invertierbaren Matrizen. Ihre Gesamtheit bildet dann eine multiplikative Gruppe, wir bezeichnen sie mit $\mathrm{GL}(m)$.

Proposition 3.5 verdeutlicht die Unabhängigkeit der Gitterdeterminante von der jeweiligen Wahl der Gitterbasis. Speziell für Teilgitter erhalten wir:

3.6 Korollar *Für zwei Gitter Γ_1, Γ_2 gleicher Dimension und Γ_2 Teilgitter von Γ_1 gelten:*
i) $\det \Gamma_1 \mid \det \Gamma_2$.
ii) $\det \Gamma_1 = \det \Gamma_2$ *ist genau dann, wenn beide Gitter gleich sind, d.h.* $\Gamma_1 = \Gamma_2$.

Proposition 3.5 ermöglicht uns eine weitere Folgerung, für die wir einige Vorüberlegungen anstellen. Ausgehend von einer Matrix $M \in \mathbb{Z}^{d\times m}$ führen wir sogenannte elementare Spaltentransformationen durch: Diese können die Vertauschung zweier Spalten von M sein, die Multiplikation einer Spalte von M mit -1 oder die Addition eines ganzzahligen Vielfachen einer Spalte von M zu einer anderen Spalte von M. Eine Folge elementarer Spaltentransformationen nennen wir eine *unimodulare Spaltentransformation*. Das folgende Resultat zeigt uns einen Zusammenhang zwischen unimodularen Spaltentransformationen und unimodularen Matrizen:

3.7 Proposition *Seien M_1, M_2 zwei $d\times m$ Matrizen über $\mathbb{Z}$ oder $\mathbb{R}$. M_1 geht genau dann durch unimodulare Spaltentransformationen in M_2 über, wenn es eine Matrix $U \in GL(m)$ mit $M_2 = M_1 U$ gibt.*

Damit wissen wir in der Situation von Proposition 3.5: Starten wir mit einem Erzeugendensystem eines Gitters, läßt sich mittels unimodularer Spaltentransformationen ein weiteres Erzeugendensystem konstruieren. Wir werden im nächsten Abschnitt bestrebt sein, auf diese Weise Gitterbasen aus Erzeugendensystemen zu konstruieren oder „einfachere" Basen zu erhalten.

Gelegentlich wollen wir die Determinante von $d\times d$ Matrizen $M = (m_{i,j})$ abschätzen. Dazu verwenden wir die zeilenorientierte *Hadamard-Schranke*

$$|\det M| \leq H(M) := \prod_{i=1}^{d} \Big(\sum_{j=1}^{d} |m_{i,j}|^2 \Big)^{1/2}. \tag{3.1}$$

Wegen $\det M = \det M^t$ für die transponierte Matrix M^t ist auch $H(M^t)$ eine obere Schranke für die Determinante, so daß $|\det M| \leq \min\{H(M), H(M^t)\}$ folgt. Speziell für $|M| = \max\{|m_{i,j}| \mid 1 \leq i,j \leq d\}$ ergibt sich die Schranke zu

$$H(M) \leq (\sqrt{d} \cdot |M|)^d. \tag{3.2}$$

3.2 Hermite-Normalform

Wir ziehen uns auf Gitter Γ über $\mathbb{Z}^d$ zurück. Ferner gehen wir davon aus, ein Erzeugendensystem für Γ zu kennen. Wir wollen eine Basis konstruieren, die bzgl. ihrer Determinante aus „relativ kleinen" Einträgen besteht. Wir wählen wieder die Matrixdarstellung des Erzeugendensystems. Im folgenden greifen wir auf Resultate von Ac. Müller zurück. (vgl. [BuMü])

3.8 Definition *Eine Matrix $M \in \mathbb{Z}^{d\times m}$ vom Rang d ist in Hermite-Normalform, wir schreiben $HNF(M) = (h_{i,j})$, wenn gilt:*

$$\begin{array}{rcl} h_{i,j} = 0 & , & \textit{falls } i > j \textit{ oder } j > d \\ h_{i,i} > 0 & , & \textit{falls } 1 \leq i \leq d \\ 0 \leq h_{i,j} < h_{i,i} & , & \textit{sonst.} \end{array}$$

In der Literatur war die Definition ursprünglich nur für quadratische Matrizen gegeben. Dann hat die Hermite-Normalform obere Dreiecksgestalt mit der geforderten Größeneigenschaft. Die ursprüngliche Definition läßt sich – wie hier geschehen – auf nichtquadratische Matrizen mit der Zusatzbedingung bzgl. des Ranges verallgemeinern. Die Resultate folgen analog.

3.9 Korollar *Ist $M \in \mathbb{Z}^{d\times m}$ eine Matrix vom Rang d in Hermite-Normalform, dann gilt für die Determinante des von M aufgespannten Gitters:*

$$\det \Gamma(HNF(M)) = \prod_{i=1}^{d} h_{i,i} \; .$$

Dem Korollar entnehmen wir, daß die Diagonalelemente $h_{i,i}$ und damit auch alle Elemente $h_{i,j}$ in den Beträgen durch die Gitterdeterminante beschränkt sind.

3.10 Satz *Zu jeder Matrix $M \in \mathbb{Z}^{d\times m}$ vom Rang d existiert eine eindeutig bestimmte Matrix $HNF(M) \in \mathbb{Z}^{d\times m}$ in Hermite-Normalform. Diese läßt sich insbesondere mittels unimodularer Spaltentransformationen erreichen, d.h. es existiert eine Matrix $T \in GL(m)$, die $HNF(M) = M \cdot T$ ergibt.*

Die Matrix T nennen wir in dieser Situation *Transformationsmatrix.* Sie ist i.a. nicht eindeutig bestimmt. Für jedes Erzeugendensystem eines Gitters impliziert Satz 3.10 die Existenz einer eindeutig bestimmten Basis in Hermite-Normalform. Wir verzichten auf die detaillierte Formulierung von Algorithmen. Wir skizzieren lediglich die Grundidee.

3.11 Algorithmus *HNF*

Eingabe: $M \in \mathbb{Z}^{d\times m}$ mit $m \geq d$ und Rang d
Ausgabe: $H \in \mathbb{Z}^{d\times d}$ in Hermite-Normalform, wobei die rechten $m-d$ Nullspalten in $HNF(M)$ entfernt werden.

$H \leftarrow M$	(1)
/* Bringe H auf Dreiecksgestalt mit positiven Diagonaleinträgen */	(2)
FOR $i \leftarrow d$ *DOWNTO* 1	(3)
Führe elementare Spaltentransformationen auf den Spalten 1 bis i und $d+1$ bis m von H durch, so daß $h_{i,i} > 0$ und $h_{i,j} = 0$ für $i > j$ oder $j > d$ gilt.	(4)
Entferne die Nullspalten $d+1$ bis m in H.	(5)
/* Reduziere die Einträge oberhalb der Diagonalen */	(6)
FOR $i \leftarrow d-1$ *DOWNTO* 1	(7)
Führe elementare Spaltentransformationen auf den Spalten i bis d von H durch, so daß $0 \leq h_{i,j} < h_{i,i}$ für $i < j \leq d$ gilt.	(8)

Führen wir dieses Verfahren aus, erhalten wir im Laufe unserer Operationen eine sogenannte *entry explosion*, d.h. die Größen der Zwischenergebnisse wachsen so stark, daß der Algorithmus einen enormen Zeitaufwand erfordert. (vgl. Beispiel für eine 8×8 Matrix in [DKT]) Für größere Matrizen wachsen Speicherplatz- und Rechenzeitbedarf so stark an, daß der Algorithmus für die Praxis nicht mehr geeignet ist. Deshalb wählen P. Domich, R. Kannan und L. Trotter in [DKT] eine sogenannte unimodulare Berechnung der Hermite-Normalform. Sie bestimmen ein Vielfaches D der Determinante der Ausgangsmatrix M und führen obigen Algorithmus modulo D aus, d.h. nach jeder Operation reduzieren sie die berechneten Zahlen modulo D, so daß die auftretenden Größen stets beschränkt sind. Abschließend rekonstruieren sie $HNF(M)$ aus der modulo D bestimmten Matrix. Ac. Müller bringt diese Ideen und einige Verbesserungen ein, die eine Beschränkung der Größe der Zwischenergebnisse zulassen und somit erstmals eine Laufzeitanalyse ermöglichen. (vgl. [BuMü])

3.12 Satz *Zu einer gegebenen Matrix $M \in \mathbb{Z}^{d\times m}$ vom Rang d kann die Hermite-Normalform in Zeit $O(d^2m \cdot (d^2+m) \cdot (\log(d|M|))^2)$ berechnet werden.*

Für spätere Anwendungen benötigen wir noch die Transformationsmatrix. (vgl. [BuMü])

3.13 Satz *Sei $M \in \mathbb{Z}^{d\times m}$ eine Matrix vom Rang d. Für die Hermite-Normalform kann die Transformationsmatrix $T \in GL(m)$ in Zeit $O(m^3d^2 \cdot (\log(d|M|))^2)$ bestimmt werden. Ihr maximaler Eintrag $|T|$ ist beschränkt durch*

$$|T| \leq (m-d+1) \cdot d|M| \cdot H^{\square},$$

wobei wir festlegen:

$$\begin{aligned} H^{\square} \;\; := \;\; & \min\{\max\{H(M') \mid M' \textit{ quadratische Teilmatrix von } M\}, \\ & \max\{H(M'^t) \mid M' \;\; \textit{quadratische Teilmatrix von } M\}\}. \end{aligned}$$

Wir betrachten eine weitere Normalform.

3.3 Smith-Normalform

Bevor wir genauer auf diese Normalform eingehen, motivieren wir ihre Anwendung in unserer Arbeit. Starten wir mit einer endlichen abelschen Gruppe G, genügt diese gemäß dem Hauptsatz für abelsche Gruppen der Isomorphie (vgl. [Hu], Theorem 2.1)

$$G \cong \mathbb{Z}/s_1\mathbb{Z} \times \ldots \times \mathbb{Z}/s_l\mathbb{Z}$$

mit $s_1 \mid \ldots \mid s_l$. Ist i der kleinste Index mit $s_i \neq 1$, dann nennen wir $(s_i, \ldots, s_l)$ die *Struktur der Gruppe G*.

Wir ziehen uns speziell auf quadratische Matrizen über $\mathbb{Z}$ zurück, sei $M \in \mathbb{Z}^{d\times d}$ regulär. Dann ist $\Gamma(M) \leq \mathbb{Z}^d$ ein d-dimensionales Gitter und $\mathbb{Z}^d/\Gamma(M)$ eine additive, endliche abelsche Gruppe. Wollen wir ihre Struktur bestimmen, dient uns die sogenannte Smith-Normalform als Werkzeug.

3.14 Definition *Eine Matrix $M \in \mathbb{Z}^{d\times d}$ hat Smith-Normalform, wenn für $M = SNF(M) = (s_{i,j})$ gilt:*

$$\begin{array}{ll} s_{i,j} = 0 & ,\ \text{falls } 1 \le i,j \le d \text{ und } i \ne j \\ s_{i,i} > 0 & ,\ \text{falls } 1 \le i \le d \\ s_{i,i} \mid s_{i+1,i+1} & ,\ \text{falls } 1 \le i \le d-1. \end{array}$$

Wir wollen aus M eine Matrix in Smith-Normalform konstruieren. Dazu führen wir analog zu den unimodularen Spaltentransformationen Operationen auf den Zeilen von M ein, die wir *unimodulare Zeilentransformationen* nennen.

3.15 Proposition *Seien M_1, M_2 $d\times m$ Matrizen über $\mathbb{Z}$ oder $\mathbb{R}$. Dann geht M_1 genau dann durch unimodulare Zeilentransformation in M_2 über, wenn es eine Matrix $V \in GL(d)$ mit $M_2 = V \cdot M_1$ gibt.*

Mittels unimodularer Zeilentransformationen auf dem quadratischen Teil der Hermite-Normalform von M erhalten wir eine Matrix in Smith-Normalform.

3.16 Satz *Zu jeder regulären Matrix $M \in \mathbb{Z}^{d\times d}$ gibt es Matrizen $U, V \in GL(d)$, so daß $S = VMU$ Smith-Normalform hat. Mit den Diagonaleinträgen $s_i := s_{i,i}$ gilt*

$$\mathbb{Z}^d/\Gamma(M) \cong \mathbb{Z}/s_1\mathbb{Z} \times \ldots \times \mathbb{Z}/s_l\mathbb{Z}.$$

Wir können also mit Hilfe der Smith-Normalform die Struktur der Gruppe $\mathbb{Z}^d/\Gamma(M)$ herleiten. Aus dem Hauptsatz für endliche, abelsche Gruppen wissen wir von der Eindeutigkeit der s_i, woraus wir folgern:

3.17 Korollar *Seien $M_1, M_2 \in \mathbb{Z}^{d\times d}$ reguläre Matrizen, die das gleiche Gitter aufspannen, d.h. $\Gamma(M_1) = \Gamma(M_2)$. Dann stimmen ihre Smith-Normalformen überein.*

Wir verzichten auch hier auf die Formulierung von Algorithmen zur Bestimmung einer Matrix in Smith-Normalform, wir geben lediglich eine Skizze.

3.18 Algorithmus SNF

Eingabe: Matrix $M \in \mathbb{Z}^{d\times d}$ vom Rang d
Ausgabe: $s_1, \ldots, s_l \in \mathbb{N}$, die Diagonaleinträge der Smith-Normalform von $\Gamma(M)$

$S \leftarrow M$		(1)
/* Bringe M auf Diagonalgestalt. */		(2)
FOR $i \leftarrow 1$ *TO* d		(3)
	Führe elementare Zeilen- und Spaltentransformationen aus, so daß $s_{i,j} = 0$ und $s_{j,i} = 0$ für alle $i+1 \le j \le d$, ohne die bereits vorhandenen Diagonalelmente $s_{1,1}, \ldots, s_{i-1,i-1}$ zu verändern.	(4)
	Zusätzlich soll $s_{i,i}$ alle verbleibenden $s_{i,j}$ teilen.	(5)

Um die Zwischenergebnisse zu beschränken, führen wir hier analog zur Bestimmung der Hermite-Normalform eine unimodulare Berechnung durch. Liegt die Matrix M in $HNF(M)$ vor, wählen wir $D = |\det M|$, was wir direkt bestimmen können. (vgl. Korollar 3.9) Die unimodularen Spalten- und Zeilentransformationen führen wir dann modulo D durch und rekonstruieren zum Schluß die Diagonaleinträge. Eine ausführliche Beschreibung inklusive einer Laufzeitanalyse findet sich in [Dü], Abschnitt 3.4:

3.19 Satz *Für eine reguläre Matrix $M \in \mathbb{Z}^{d\times d}$ kann die Smith-Normalform in Zeit $O(d^2 \cdot (\log|M|)^3 \cdot (\log\log|M|)^2 \cdot (d + \log\log|M|))$ berechnet werden.*

Bisher haben wir Normal-Formen für Gitter in $\mathbb{Z}^d$ betrachtet. Dabei haben wir mit der Hermite-Normalform ein Werkzeug, um aus Erzeugendensystemen für Gitter in $\mathbb{Z}^d$ Basen zu konstruieren. Wir stellen nun ein Verfahren vor, daß dieses Ziel auch allgemein für Gitter in $\mathbb{R}^d$ realisiert.

3.4 Konstruktion von Gitterbasen in $\mathbb{R}^d$

Wir wenden ein Resultat von J. Buchmann und V. Kessler an, das wir im folgenden skizzieren: (vgl. [BuKe])

Wir gehen von einem $d = (d_1 + d_2)$-dimensionalen Gitter in $\mathbb{Z}^{d_1} \times \mathbb{R}^{d_2}$ aus, für das wir bereits ein Erzeugendensystem

$$\{\underline{v}_1, \ldots, \underline{v}_N\}$$

kennen, d.h. $\Gamma = \mathbb{Z}\underline{v}_1 + \ldots + \mathbb{Z}\underline{v}_N$. Gesucht ist eine Basis für Γ basierend auf dem vorgegebenen Erzeugendensystem.

Wollen wir ein Verfahren anwenden, das sich implementieren läßt, benötigen wir für die d_2 reellen Koordinaten der Gittervektoren von Γ Approximationen.

3.20 Definition *Seien $c \in \mathbb{C}$ und $n \in \mathbb{N}_0$. Eine Approximation von c der Präzision n ist eine Zahl $\hat{c} \in 2^{-n-1}\mathbb{Z}$ mit $|c - \hat{c}| < 2^{-n}$. Für eine solche Zahl $\hat{c}$ schreiben wir auch $appr(c, n)$.*

Das Verfahren in [BuKe] berechnet eine Basis für Γ, indem es den LLL-Algorithmus (vgl. [LLL]) auf ein sogenanntes approximiertes Gitter $\hat{\Gamma}$ anwendet, das aus rationalen Approximationen $\hat{\underline{v}}_j$ der erzeugenden Vektoren $\underline{v}_j$ besteht.

Sei $n \in \mathbb{N}$ eine noch genauer zu spezifizierende Präzisionskonstante. Für einen Vektor $\underline{v}_j = (v_{i,j})^t$ bestimmen wir einen rationalen Approximationsvektor $\hat{\underline{v}}_j$ derart, daß wir für jede Koordinate $v_{i,j}$ von $\underline{v}_j$

$$\hat{v}_{i,j} := [2^n v_{i,j}] \tag{3.3}$$

berechnen und $\underline{\hat{v}}_j$ entsprechend setzen:

$$\underline{\hat{v}}_j := (\hat{v}_{i,j})^t.$$

In [BuKe] wird die Präzisionskonstante n so gewählt, daß die Darstellung der Basisvektoren bzgl. $\{\underline{\hat{v}}_1, \ldots, \underline{\hat{v}}_N\}$ aus dem LLL-Algorithmus für das approximierte Gitter

$$\hat{\Gamma} = \mathbb{Z}\underline{\hat{v}}_1 + \ldots + \mathbb{Z}\underline{\hat{v}}_N$$

auch eine Darstellung einer Basis für Γ bzgl. $\{\underline{v}_1, \ldots, \underline{v}_N\}$ ergibt.

Zur Analyse werden noch einige Konstanten eingeführt:

$$\lambda \leq \min\{\|\underline{v}\| \mid \underline{0} \neq \underline{v} \in \Gamma\}, \tag{3.4}$$

wobei $\|.\|$ die euklidische Norm bezeichnet, und

$$\nu \geq \max\{\|\underline{v}_j\| \mid 1 \leq j \leq N\}. \tag{3.5}$$

Seien o.B.d.A. $\{\underline{v}_1, \ldots, \underline{v}_d\}$ linear unabhängige Vektoren aus dem vorgegebenen Erzeugendensystem. Dann führen wir ein:

$$\lambda_j = \|\underline{v}_j\|, \qquad 1 \leq j \leq d. \tag{3.6}$$

J. Buchmann und V. Kessler erhalten in [BuKe], Theorem 4.1:

3.21 Satz *Sei Γ ein $d = (d_1 + d_2)$-dimensionales Gitter in $\mathbb{Z}^{d_1} \times \mathbb{R}^{d_2}$ mit Erzeugendensystem $\{\underline{v}_1, \ldots, \underline{v}_N\}$, und ∇ bezeichne eine Konstante*

$$\nabla = \Big(\frac{N\sqrt{d_2}}{2} + \sqrt{N}\Big) \cdot \frac{\nu^d}{\det \Gamma}. \tag{3.7}$$

Falls die Präzisonskonstante n

$$2^n > \frac{(\sqrt{d_2 N} + 2) \cdot \nabla \cdot 2^{(N-3)/2}}{\lambda} \tag{3.8}$$

genügt, kann eine Basis $\{\underline{b}_1, \ldots, \underline{b}_d\}$ von Γ folgender Gestalt berechnet werden:

$$\underline{b}_j = \sum_{i=1}^{N} z_{i,j}\underline{v}_i, \qquad 1 \leq j \leq d, \tag{3.9}$$

wobei für $\underline{z}_j \in \mathbb{Z}^N$ die Beschränkung

$$\|\underline{z}_j\| \leq 2^{(N-1)/2+n+1}\lambda_j, \qquad 1 \leq j \leq d, \tag{3.10}$$

gilt. Insbesondere gilt für die Längen der Basisvektoren

$$\|\underline{b}_j\| \leq (\sqrt{d_2 N} + 2) \cdot 2^{(N-1)/2} \cdot \lambda_j, \qquad 1 \leq j \leq d. \tag{3.11}$$

Für die Laufzeit ihres Verfahrens schätzen J. Buchmann und V. Kessler ab:

3.22 Satz *In der Situation von Satz 3.21 kann die Gitterbasis $\{\underline{b}_1, \ldots, \underline{b}_d\}$ für Γ in Zeit $O((d_1+d_2+N)^6 \cdot N^3 \cdot (\log|\nu/\lambda|)^3)$ berechnet werden, falls die Präzisionskonstante n in (3.8) optimal gewählt ist und die approximierten Vektoren in (3.3) der Präzision n gemäß (3.8) vorberechnet sind.*

Kapitel 4

Grundidee für die Berechnung der Klassenzahl und das Lösen von Normgleichungen

Wir werden einen Algorithmus von J. Buchmann zur Bestimmung der Klassenzahl und des Regulators *beliebiger* Zahlkörper herleiten. Zu deren Berechnung werden während der Durchführung des Algorithmus noch weitere Größen ermittelt, die bisher ungenutzt blieben. Wir werden eine neue Methode präsentieren, die mit diesen Daten anschließend zu vorgegebenem $m \in \mathbb{Z}$ alle – bis auf Assoziierte – ganzen Elemente der Norm m berechnet. Dabei wird auch ein neuer Hauptidealtest vorgestellt.

In den nachfolgenden Kapiteln ziehen wir uns auf *reellquadratische* Ordnungen zurück. Dort ändern wir die in diesem Kapitel für beliebige Zahlkörper vorgestellten Verfahren entsprechend ab und geben Laufzeitanalysen an.

4.1 Die Berechnung der Klassenzahl

Wir beginnen mit den theoretischen Grundlagen und Ideen zur Berechnung der Klassenzahl. Diese arbeiten wir zu einem vorläufigen Algorithmus aus.

K. McCurley stellt diesen Ansatz bereits in [Mc] für imaginärquadratische Zahlkörper vor, in [HaMc] gibt er zusammen mit J. Hafner eine Anwendung inklusive ihrer Laufzeitanalyse. J. Buchmann verallgemeinert diese Idee in [Bu1] auf beliebige Zahlkörper, worauf wir uns im wesentlichen beziehen.

Bezeichne $\mathcal{K}$ im folgenden einen beliebigen Zahlkörper.

4.1.1 Theoretische Herleitung

Ausgehend von $\mathcal{K}$ betrachten wir eine endliche Menge von Primidealen,

$$F = \{P_1, \ldots, P_k \mid P_i \text{ Primideal von } \mathcal{O}_\mathcal{K}\},$$

die der zusätzlichen Bedingung genügen, daß ihre zugehörigen Äquivalenzklassen die Klassengruppe erzeugen, d.h.

$$\langle\ [P_1], \ldots, [P_k]\ \rangle = Cl.$$

Über der Menge F bilden wir Produkte. Daher nennen wir eine solche Idealmenge auch *Faktorbasis*. Von nun an beschränken wir uns auf die spezielle Idealmenge

$$F_C = \{P \mid P \text{ Primideal von } \mathcal{O}_\mathcal{K} \text{ und } N(P) \leq C\} \tag{4.1}$$

bzgl. einer Normschranke $C \in \mathbb{R}_{>0}$. F_C ist dann eine endliche Menge, deren Ordnung wir mit $k = k(C)$ bezeichnen. Wie E. Bach in [Ba] unter Annahme der verallgemeinerten Riemannschen Vermutung bewiesen hat, bildet F_C für

$$C \geq 12 \cdot (\ln|\Delta|)^2$$

eine Faktorbasis. Liegt ein imaginärquadratischer Zahlkörper zugrunde, dann genügt es bereits, $C \geq 6 \cdot (\ln|\Delta|)^2$ zu wählen.

Über F_C berechnen wir Produkte und wenden folgende Abbildung an:

$$\begin{array}{rccc} \vartheta : & \mathbb{Z}^k & \longrightarrow & Cl, \\ & \underline{v} = (v_1, \ldots, v_k) & \longmapsto & \left[\prod_{i=1}^k P_i^{v_i}\right]. \end{array}$$

Wir verifizieren direkt, daß ϑ ein Homomorphismus ist. Bildet F_C eine Faktorbasis, ist ϑ sogar surjektiv. Anwenden des Homomorphiesatzes (vgl. [Hu], Cor. 5.7) liefert dann die Isomorphie

$$\mathbb{Z}^k_{/\text{Kern } \vartheta} \cong Cl, \tag{4.2}$$

wobei sich der Kern von ϑ wie folgt berechnet:

$$\begin{aligned} \text{Kern } \vartheta &= \left\{\underline{v} \in \mathbb{Z}^k \mid \vartheta(\underline{v}) = 1_{Cl} = [\mathcal{O}_\mathcal{K}]\right\} \\ &= \left\{\underline{v} \in \mathbb{Z}^k \mid \prod_{i=1}^k P_i^{v_i} \text{ ist Hauptideal}\right\} \\ &\leq \mathbb{Z}^k. \end{aligned}$$

Dann ist Kern ϑ ein Gitter in $\mathbb{Z}^k$. Da $\sharp Cl = h$ endlich ist, hat dieses wegen der Isomorphie in (4.2) endlichen Index in $\mathbb{Z}^k$, d.h. Dimension k sowie

$$\det \text{Kern } \vartheta = h.$$

Demnach läßt sich die Klasssenzahl berechnen, wenn wir die Determinante des Kerns von ϑ – als Gitter betrachtet – ermitteln. Mit einer Ergänzung dieser Idee läßt sich auch der Regulator bestimmen.

Deshalb betrachten wir die den Gittervektoren $\underline{v}$ entsprechenden Hauptideale sowie ihre Erzeugenden $\alpha \in \mathcal{O}_{\mathcal{K}}$ und setzen sie in „Relation", es gilt

$$\prod_{i=1}^{k} P_i^{v_i} = \alpha \mathcal{O}_{\mathcal{K}}. \tag{4.3}$$

Wir berechnen den Logarithmus bzgl. der Konjugierten des Erzeugenden α und fügen diese Werte dem bisherigen Vektor $\underline{v}$ hinzu. Wir erhalten dann in (4.3) Vektoren der Form

$$(v_1, \ldots, v_k, \ln|\alpha|_1, \ldots, \ln|\alpha|_r).$$

(Im Hinblick auf die nachfolgenden Kapitel kommt für reellquadratische Zahlkörper wegen Einheitenrang $r = 1$ nur eine Koordinate hinzu.) Die beschriebenen Vektoren fassen wir in der Menge Γ_C zusammen, d.h.

$$\Gamma_C = \Big\{(v_1, \ldots, v_k, \ln|\alpha|_1, \ldots, \ln|\alpha|_r) \mid (v_1, \ldots, v_k) \in \mathbb{Z}^k \text{ und } \prod_{i=1}^{k} P_i^{v_i} = \alpha \mathcal{O}_{\mathcal{K}}\Big\}. \tag{4.4}$$

Um den Zusammenhang von Γ_C mit Kern ϑ zu verdeutlichen, setzen wir

$$\Gamma'_C := \text{Kern } \vartheta.$$

Für Einheitenrang $r = 0$ sind beide Mengen gleich. Insbesondere wird in [Bu1], Theorem 2.1 bewiesen:

4.1 Satz *(GRH) Sei $C \in \mathbb{R}_{>0}$ mit $C \geq 12 \cdot (\ln|\Delta|)^2$ beliebig. Dann ist die Menge Γ'_C ein k-dimensionales Gitter der Determinante h und die Menge Γ_C ein $(k+r)$-dimensionales Gitter der Determinante hR.*

Aus der Definition von Γ_C und Γ'_C folgern wir direkt:

4.2 Korollar *Ist M eine Basis oder ein Erzeugendensystem für Γ_C, dann erhalten wir ein Erzeugendensystem für Γ'_C, indem wir in den Elementen von M die letzten r Koordinaten streichen.*

Abschließend führen wir noch einige Begriffe ein:

4.3 Definition *Zu gegebenem $C \in \mathbb{R}_{>0}$ und Zahlkörper $\mathcal{K}$ heißt Γ'_C Relationengitter und Γ_C (erweitertes) Relationengitter, ihre Elemente nennen wir Relationen bzw. (erweiterte) Relationen.*

Die geschilderten Zusammenhänge legen zur Berechnung der Klassenzahl und des Regulators folgende Vorgehensweise nahe: Zuerst ermitteln wir genügend erweiterte Relationen, um danach die Determinante des von diesen Relationen aufgespannten Gitters zu bestimmen. Falls sie das erweiterte Relationengitter Γ_C aufspannen, ist die Determinante dieses Gitters hR, und wir erhalten mit Korollar 4.2 ein Erzeugendensystem für das Relationengitter Γ'_C, woraus wir dessen Determinante h berechnen. Aus diesen Größen läßt sich der Regulator bestimmen. Ferner können wir aus den vorliegenden Informationen die Struktur der Klassengruppe errechnen. (vgl. die Methoden aus Kapitel 3)

4.1.2 Skizze des Algorithmus *CLASSREG*

Wir werden die eben beschriebene Methode zu einem vorläufigen Algorithmus ausarbeiten und auf einige Aspekte näher eingehen. Dabei treten zwei zentrale Probleme in den Vordergrund:

- *Relationenengenerierung:* Wie können wir Relationen erzeugen? Wieviele Relationen müssen wir erzeugen?
- *Teilgitterbeziehungen:* Hat das von den erzeugten Relationen aufgespannte Gitter volle Dimension? Falls dies der Fall ist, wie können wir testen, ob das Teilgitter gleich dem Relationengitter ist?

In [Bu1] werden diese Aufgaben für beliebige Zahlkörper bereits gelöst. Wir verzichten daher auf eine detaillierte Schilderung.

Relationengenerierung

Wir beschreiben das Prinzip der Relationengenerierung, bleiben dabei bewußt allgemein. Für die gesuchten erweiterten Relationen benötigen wir Hauptideale und ihre Erzeugende. Da wir jedoch von einem Ideal nicht direkt wissen, ob es Hauptideal ist oder nicht, und wir gegebenenfalls sein Erzeugendes nicht effizient bestimmen können, wenden wir folgenden Trick an: Wir bestimmen zwei äquivalente Ideale A, B und das Ideal $\alpha\mathcal{O}_\mathcal{K}$, wodurch sie sich unterscheiden. Dann wissen wir $B = (\alpha\mathcal{O}_\mathcal{K})A$. Zerfällt BA^{-1} über der Faktorbasis F_C, haben wir eine erweiterte Relation gefunden. Unsere Relationensuche gestaltet sich dann wie folgt:

Bestimme zuerst eine Idealklasse. Wähle dazu zufällig und gleichverteilt einen Exponentenvektor $\underline{e} \in_R [\![0, \text{const}]\!]^k$ (, wobei const $\in \mathbb{N}$ eine noch zu bestimmende Schranke ist). Berechne dann bzgl. $\underline{e}$ und der Faktorbasis F_C das Ideal

$$A = \prod_{i=1}^{k} P_i^{e_i} \,, \tag{4.5}$$

und wir konzentrieren uns auf die Idealklasse $[A]$.

Bestimme dann zufällig und gleichverteilt in $[A]$ ein (reduziertes) Ideal B und $\alpha \in \mathcal{K}$ mit

$$B = (\alpha\mathcal{O}_\mathcal{K})A. \tag{4.6}$$

Falls B über der Faktorbasis F_C zerfällt, d.h. $B = \prod_{i=1}^{k} P_i^{z_i}$ gilt, wissen wir:

$$\prod_{i=1}^{k} P_i^{z_i - e_i} = BA^{-1} = \alpha\mathcal{O}_\mathcal{K}, \tag{4.7}$$

d.h. wir haben die erweiterte Relation $(z_1 - e_1, \ldots, z_k - e_k, \ln|\alpha|_1, \ldots, \ln|\alpha|_r)$ gefunden.

Das vorgestellte Verfahren ist probabilistisch, wobei eine Iteration nicht notwendig erfolgreich ist. Sie ist erfolgreich, wenn das Ideal B aus (4.6) über der Faktorbasis F_C zerfällt. Diese Methode ist daher vom Typ Las-Vegas.

Speziell für imaginärquadratische Zahlkörper beschreiben J. Hafner und K. McCurley eine probabilistische Methode (vgl. [HaMc]), die auf speziellen Eigenschaften dieses Zahlkörpertyps basiert. Für beliebige Zahlkörper skizziert J. Buchmann ebenfalls eine Prozedur vom Typ Las-Vegas (vgl. Prozedur PV in [Bu1], Abschnitt 3.3), die eine Weiterführung der Idee von J. Hafner und K. McCurley ist. Da ein Aufruf seiner Prozedur nicht immer eine Relation liefert, müssen in der Regel mehrere erfolgen, bis eine Relation gefunden wird.

Für reellquadratische Ordnungen werden wir ein Verfahren entwickeln, das die besondere Struktur dieser Ordnungen ausnutzt.

Teilgitterbeziehungen

Wir können davon ausgehen, daß eine bestimmte Anzahl zufällig und gleichverteilt gewählter Relationen Γ_C bzw. Γ'_C erzeugt. Allgemein wissen für die Determinante eines Teilgitters $\Gamma' \leq \mathbb{Z}^k$ von Γ'_C mit Korollar 3.6:

$$(h = \det \Gamma'_C) \mid \det \Gamma'$$

Wir konstruieren eine Kette von Teilgittern von Γ'_C, $\Gamma'_{(1)} \leq \Gamma_{(2)} \leq \ldots \leq \Gamma'_C$, deren Determinanten sich sukzessive teilen: $\det \Gamma'_C \mid \ldots \mid \det \Gamma'_{(2)} \mid \det \Gamma'_{(1)}$. Haben wir ein Teilgitter Γ' mit $\det \Gamma' = \det \Gamma'_C$, dann folgt gemäß Korollar 3.6 die Gleichheit beider Gitter. Also haben wir $\det \Gamma' = h$. Analog unterscheiden sich die Determinanten von Teilgittern von Γ_C ebenfalls nur um ganzzahlige Vielfache von $\det \Gamma_C$.

Daher bietet sich folgendes Vorgehen an. Unter der Annahme, daß wir eine hinreichend gute obere Schranke H für hR kennen, wissen wir für die Determinante eines Teilgitters Γ von Γ_C: Falls $\det \Gamma < H$, muß $\det \Gamma = hR = \det \Gamma_C$ gelten. Wir haben also hR mittels $\det \Gamma$ berechnet.

Solch eine Schranke für hR läßt sich tatsächlich bestimmen und zwar mit Hilfe der analytischen Klassenzahlformel. (vgl. [BuWi]) Insbesondere existiert eine Zahl $H^* \in \mathbb{R}_{>0}$ mit $H^* < hR < 2H^*$. Wir weisen darauf hin, daß sich allgemein keine solche Schranke H^* für die Klassenzahl h allein bestimmen läßt, da außer für imaginärquadratische Zahlkörper nicht bekannt ist, wie sich eine hinreichend gute obere Schranke für h bestimmen läßt. Ferner ist es naheliegend, Regulator und Klassenzahl gleichzeitig zu berechnen, da diese Invarianten eng zusammenhängen.

Zusammenfassend skizzieren wir Algorithmus *CLASSREG*.

4.4 Algorithmus *CLASSREG*

Eingabe: Zahlkörper $\mathcal{K}$, Schranke $C \geq 12 \cdot (\ln |\Delta|)^2$
Ausgabe: h, R, Struktur von Cl

Berechne eine Abschätzung H^* mit $H^* < hR < 2H^*$.		(1)
Bestimme die Faktorbasis F_C.		(2)
	Erzeuge N erweiterte Relationen $\underline{v}_1, \ldots, \underline{v}_N$.	(3)
	Berechne die Determinante d des von $\underline{v}_1, \ldots, \underline{v}_N$ aufgespannten Gitters.	(4)
UNTIL $d < 2H^*$ /* Abbruchbedingung */		(5)
Streiche in den erweiterten Relationen $\underline{v}_1, \ldots, \underline{v}_N$ die letzten r Koordinaten. Berechne mit der Hermite-Normalform H die Determinante dieses aufgespannten Gitters, d.h. h.		(6)
Berechne die Struktur von Cl, indem aus H die Smith-Normalform $SNF(H)$ berechnet wird.		(7)
Gib h, R aus und die Diagonalelemente von $SNF(H)$, die $\neq 1$ sind.		(8)

4.5 Bemerkung In Schritt (4) wendet J. Buchmann ein Verfahren an, in dessen Verlauf eine Basis aus dem Erzeugendensystem $\{\underline{v}_1, \ldots, \underline{v}_N\}$ berechnet wird. (vgl. [BuKe]) In Schritt (6) wird mit der Hermite-Normalform eine Basis für Γ'_C berechnet.

Wir gehen noch kurz auf die Bedeutung der Größe der Normschranke C ein. Einerseits zieht eine große Normschranke eine hohe Wahrscheinlichkeit nach sich, daß ein während der Relationengenerierung gewähltes Ideal über der Faktorbasis F_C zerfällt. (vgl. Ideal B in (4.6)) Andererseits ergeben große Normschranken C wegen (4.1) große Ordnungen k der Faktorbasen F_C. Da die Ordnung k der Faktorbasis F_C wiederum in der Dimension k bzw. $k + r$ der Relationengitter auftritt, spielt sie eine erhebliche Rolle hinsichtlich der Komplexität der in *CLASSREG* angewandten Gitteralgorithmen. (vgl. Kapitel 3) Daher müssen wir eine geeignete Wahl für die Normschranke finden, um die Laufzeit zu optimieren. Wie in [Bu1] setzen wir

$$C = L_\Delta^c, \qquad c \in \mathbb{R}_{>0}.$$

Folgen wir dem Beweis in [Bu1] ist die Laufzeit des Algorithmus optimal für $c = \sqrt{7}/14$. Dann ist für hinreichend großes $|\Delta|$ die Bedingung $C = L_\Delta^c \geq 12 \cdot (\ln |\Delta|)^2$ erfüllt und die Aussage von Satz 4.1 anwendbar. Ferner ist in *CLASSREG* die erwartete Anzahl der erweiterten Relationen, die Γ_C erzeugen, $N = L_\Delta[c]$.

Im Laufe der Analyse formuliert J. Buchmann eine sogenannte *Glattheitsvermutung*: Die Anzahl aller reduzierten Ideale, deren Primideale Norm $\leq C$ genügen, ist nach unten durch $\sqrt{|\Delta|} \cdot L_\Delta[-1/(4c)]$ beschränkt. Vermutlich läßt sie sich mit Satz 7.5 beweisen. (vgl. [BuHo]) Insgesamt wissen wir mit[Bu1]:

4.6 Satz *(GRH) Die Klassenzahl, die Struktur der Klassengruppe sowie der Regulator eines Zahlkörpers $\mathcal{K}$ vom Grad d können unter der Glattheitsannahme probabilistisch in erwarteter Laufzeit $L_\Delta[1,7]$ für festen Grad d und $|\Delta| \to \infty$ berechnet werden.*

4.2 Das Lösen von Normgleichungen

Wir wenden uns folgendem Problem zu: Suche zu gegebenem Zahlkörper $\mathcal{K}$ und $m \in \mathbb{Z}$ alle *ganzen* Lösungen $\gamma \in \mathcal{O}_\mathcal{K}$, die

$$N(\gamma) = m \tag{4.8}$$

genügen. Gleichungen der Form (4.8) werden als *Normgleichungen* bezeichnet.

Wir werden eine Lösungsmethode zeigen, die auf dem Algorithmus *CLASSREG* aufbaut. Dabei nutzen wir aus, daß in *CLASSREG* mehr Größen berechnet werden als benötigt werden. Diese bleiben bisher ungenutzt. Insbesondere werden in Schritt (4) und (6) Gitterbasen für die Relationengitter bestimmt. (vgl. Bemerkung 4.5) Wir werden ein neuartiges Verfahren zum Lösen von Normgleichungen vorstellen, das diese Basen zur Lösung heranzieht. Insbesondere werden dabei die erwähnten Basen bei einem neuen Hauptidealtest eine wesentliche Rolle spielen.

Da die Relationengitter Zusammenhänge zwischen Idealen beschreiben, die Normgleichung in (4.8) jedoch elementbezogen ist, werden wir zunächst einen Bezug zwischen diesen Elementen und Idealen herstellen.

4.2.1 Übergang zu Idealen

Einheiten spielen für Normgleichungen eine besondere Rolle, wie dem folgenden Lemma zu entnehmen ist.

4.7 Lemma *Sei $\mathcal{K}$ ein beliebiger Zahlkörper und η eine Einheit. Ist $\gamma \in \mathcal{O}_\mathcal{K}$ eine Lösung der Normgleichung mit $N(\gamma) = m$, dann gilt auch $|N(\gamma \cdot \eta)| = |m|$.*

Beweis: Der Beweis folgt direkt aus der Multiplikativität der Norm (vgl. Proposition 2.9). ■

Lemma 4.7 zeigt: Existieren Einheiten η mit $N(\eta) = 1$, ist jedes $\gamma \cdot \eta^i$, $i \in \mathbb{Z}$, Lösung von (4.8). Unter dieser Bedingung und der Existenz einer Lösung können wir direkt unendlich viele angeben (, falls der Einheitenrang $r \geq 1$ genügt). Deshalb verzichten wir in (4.8) auf solche Lösungen und wenden uns der Suche aller Lösungen bis auf Assoziierte zu. Da es höchstens endlich viele nichtassoziierte Lösungen gibt (siehe z.B. in [PhZa], Seite 409), können wir dieses Problem algorithmisch zu lösen.

Außerdem erzeugen assoziierte Elemente das gleiche Hauptideal. Umgekehrt sind verschiedene Erzeugende eines Hauptideals assoziiert. Betrachten wir dann die zugehörigen Ideale $\gamma\mathcal{O}_\mathcal{K}$ anstatt der Lösungen γ in (4.8), spielen Einheiten keine Rolle mehr. Deshalb gehen wir von der elementbezogenen Betrachtungsweise zur idealbezogenen über. Im übrigen gilt diesbezüglich folgender Zusammenhang.

4.8 Lemma *Sei $\mathcal{K}$ ein beliebiger Zahlkörper und $m \in \mathbb{Z}$. Es existiert eine Lösung γ in $\mathcal{O}_\mathcal{K}$ der Norm $|m|$ genau dann, wenn ein ganzes Hauptideal A der Norm $|m|$ existiert.*

Beweis: Existiert eine Lösung $\gamma \in \mathcal{O}_\mathcal{K}$ mit $|N(\gamma)| = |m|$, dann hat das Ideal $A = \gamma\mathcal{O}_\mathcal{K}$ die gewünschte Eigenschaft. Existiert umgekehrt ein Hauptideal A in $\mathcal{O}_\mathcal{K}$ der Norm $|m|$, enthält A ein Erzeugendes $\gamma \in \mathcal{O}_\mathcal{K}$ mit $A = \gamma\mathcal{O}_\mathcal{K}$, und es gilt $|N(\gamma)| = N(\gamma\mathcal{O}_\mathcal{K}) = |m|$. ■

Wollen wir eine Normgleichung der Form (4.8) lösen, folgern wir aus den Überlegungen zu Lemma 4.7 und Lemma 4.8: Die nichtassoziierten ganzen Lösungen γ von (4.8) lassen sich bijektiv auf die ganzen Hauptideale $\gamma\mathcal{O}_\mathcal{K}$ der Norm $|m|$ abbilden. Deshalb konzentrieren wir uns nun auf die Suche aller ganzen Hauptideale der Norm $|m|$ und ihrer Erzeugenden. Wie können wir (ganze) Ideale der Norm $|m|$ finden? Dazu benötigen wir noch einige Zusammenhänge zwischen Primidealen und ihren Normen. Wir nutzen dabei die Multiplikativität der Norm aus: (vgl. Proposition 2.9)

4.9 Lemma *In einem Zahlkörper $\mathcal{K}$ gelten für ein Ideal A mit der Primidealzerlegung $A = \prod_{j=1}^{l} P_j^{z_j}$ und eine Primzahl p:*

$$\log_p N(A) = \sum_{P_j | p\mathcal{O}_\mathcal{K}} z_j \cdot \log_p N(P_j). \tag{4.9}$$

Da ganze Ideale ganzzahlige Normen besitzen (vgl. Proposition 2.19) und wegen (2.4), ist $N(P_j)$ eine Potenz von p. Damit sind die Logarithmen ganze Zahlen, und aus (4.9) folgen direkt die Aussagen des Korollars für ganze Ideale:

4.10 Korollar *Für einen Zahlkörper $\mathcal{K}$ und ein Ideal A von $\mathcal{O}_\mathcal{K}$ gelten:*
i) Wird die Norm eines ganzen Ideals A von einer Primzahl p geteilt, dann existiert in der Primidealzerlegung von A ein Primideal, das $p\mathcal{O}_\mathcal{K}$ teilt.
ii) Existiert in der Primidealzerlegung eines ganzen Ideals A ein Primideal, das $p\mathcal{O}_\mathcal{K}$ teilt, dann muß in der Norm von A eine $p-$Potenz vorkommen.

Damit formulieren wir abschließend unsere Methode zum Lösen von Normgleichungen der Form (4.8): Bestimme *zuerst* die endlich vielen ganzen Ideale der Norm $|m|$. Dies läßt sich mit Hilfe von (4.9) bewerkstelligen. Wähle dann diejenigen aus, die Hauptideale sind, und ermittle jeweils ein erzeugendes Element γ. Wegen Lemma 4.8 ist für die Erzeugenden abschließend noch zu klären, ob $N(\gamma) = m$ oder $-m$, d.h. wir müssen einen Vorzeichentest machen.

Es steht noch aus, wie wir die erwähnten Hauptidealtests gestalten. Dies ist Gegenstand des nächsten Abschnitts.

4.2.2 Zusammenhang mit der Klassenzahlberechnung

Ziel dieses Abschnitts ist die Lösung folgenden Problems: Ist ein gegebenes Ideal Hauptideal? Falls ja, bestimme ein Erzeugendes.

Erinnern wir uns an die Definitionen der Relationengitter Γ'_C und Γ_C. Wie Bemerkung 4.5 zu entnehmen ist, existiert nach Ausführung von *CLASSREG* eine Gitterbasis für Γ_C. Bezeichne B_C eine Matrix, deren Spalten eine Gitterbasis für Γ_C bilden.

$$B_C = \left(\begin{array}{ccc|cc} b_{1,1} & \dots & b_{1,k+s} & \dots & b_{1,k+r} \\ & \vdots & & \vdots & \\ & \vdots & & \vdots & \\ b_{k,1} & \dots & b_{k,k+s} & \dots & b_{k,k+r} \\ \hline \ln|\beta_1|_1 & \dots & \ln|\beta_{k+s}|_1 & \dots & \ln|\beta_{k+r}|_1 \\ & \vdots & & \vdots & \\ \ln|\beta_1|_r & \dots & \ln|\beta_{k+s}|_r & \dots & \ln|\beta_{k+r}|_r \end{array}\right) \tag{4.10}$$

Gemäß dieser Notation wissen wir $(b_{1,j}, \dots, b_{k,j}, \ln|\beta_j|_1, \dots, \ln|\beta_j|_r) \in \Gamma_C$ und folgern

$$\prod_{i=1}^{k} P_i^{b_{i,j}} = \beta_j \mathcal{O}_K, \qquad 1 \le j \le k+r. \tag{4.11}$$

In der Matrix B_C streichen wir die letzten r Zeilen. Seien dann die Spalten $1, \dots, k+s$ ein Erzeugendensystem für Γ'_C. Solch eine Zahl s mit $0 \le s \le r$ existiert wegen Korollar 4.2. Bilde aus diesen Spalten eine Matrix, und nenne sie B'_C. Es gilt dann $B'_C \in \mathbb{Z}^{k \times (k+s)}$. Sie entspricht dem in (4.10) markierten oberen linken Quadranten der Matrix B_C.

Wie können wir anhand der Matrizen B_C und B'_C einen Hauptidealtest vornehmen? Bezeichne A das zu testende Ideal. Wir unterscheiden, ob A über der zugrundeliegenden Faktorbasis F_C zerfällt oder nicht.

A zerfällt über F_C

A ist dann als Potenzprodukt von Primidealen aus F_C darstellbar, wobei gilt:

$$\begin{aligned} A = \prod_{i=1}^{k} P_i^{z_i} \text{ ist Hauptideal} \quad &\Longleftrightarrow \quad \underline{z} = (z_1, \dots, z_k) \in \Gamma'_C \\ &\Longleftrightarrow \quad \exists \underline{x} \in \mathbb{Z}^{k+s} : B'_C \cdot \underline{x} = \underline{z}. \end{aligned} \tag{4.12}$$

Demnach besteht der Hauptidealtest für A im wesentlichen im Lösen des linearen Gleichungssystems in (4.12) über $\mathbb{Z}^{k+s}$. Ist A Hauptideal, läßt sich mit Hilfe des Lösungsvektors $\underline{x}$ ein Erzeugendes bestimmen. Dabei gilt mit $z_i = \sum_{j=1}^{k+s} b_{i,j} \cdot x_j$

wegen (4.12):

$$\begin{aligned} A &= \prod_{i=1}^{k} P_i^{z_i} = \prod_{i=1}^{k}\Big(\prod_{j=1}^{k+s} P_i^{b_{i,j}\cdot x_j}\Big) \\ &= \prod_{j=1}^{k+s}\underbrace{\Big(\prod_{i=1}^{k} P_i^{b_{i,j}}\Big)}_{=\beta_j\mathcal{O}_\mathcal{K}}{}^{x_j} \qquad \text{wegen (4.11)} \\ &= \Big(\prod_{j=1}^{k+s}\beta_j^{x_j}\Big)\mathcal{O}_\mathcal{K}. \end{aligned} \tag{4.13}$$

Also ist $\prod_{j=1}^{k+s}\beta_j^{x_j}$ ein Erzeugendes für A. Damit haben wir wegen (4.12) und (4.13) bewiesen:

4.11 Lemma *Seien $\mathcal{K}$ ein Zahlkörper mit einer Faktorbasis F_C und $B'_C \in \mathbb{Z}^{k\times(k+s)}$ eine Matrix, deren Spalten ein Erzeugendensystem für Γ'_C bilden. Dann gilt für ein Ideal $A = \prod_{i=1}^{k} P_i^{z_i}$:*
i) A ist Hauptideal genau dann, wenn das Gleichungssystem $B'_C \cdot \underline{x} = \underline{z}$ über $\mathbb{Z}^{k+s}$ lösbar ist.
ii) Falls A Hauptideal und $\underline{x}$ eine Lösung von $B'_C \cdot \underline{x} = \underline{z}$ ist, dann erzeugt $\prod_{j=1}^{k+s}\beta_j^{x_j}$ das Ideal A.

A zerfällt nicht über F_C

Dann treten in der Primidealzerlegung von A Primideale auf, die nicht in F_C liegen. Daher ist die eben beschriebene Methode nicht direkt anwendbar. Dieser Mangel läßt sich beheben, wenn wir einen Trick anwenden, der sich an der Technik der Relationengenerierung orientiert. Unsere Idee besteht darin, ein zu A äquivalentes Ideal zu bestimmen, das über F_C zerfällt. Für dieses machen wir dann stellvertretend für A einen Hauptidealtest, auf das sich die eben beschriebene Methode wieder anwenden läßt. Diese Idee formuliert sich ähnlich zur Relationengenerierung:

Bestimme zuerst eine Idealklasse. Wähle dazu zufällig und gleichverteilt einen Exponentenvektor $\underline{e} \in_R [\![0, \mathrm{const}]\!]^k$, und betrachte die Idealklasse

$$\Big[A\prod_{i=1}^{k} P_i^{e_i}\Big].$$

Bestimme dann etwa zufällig und gleichverteilt ein (reduziertes) Ideal B in $\Big[A\prod_{i=1}^{k} P_i^{e_i}\Big]$ und $\alpha \in \mathcal{K}$ mit

$$B = (\alpha\mathcal{O}_\mathcal{K})A\prod_{i=1}^{k} P_i^{e_i}.$$

Falls B über der Faktorbasis F_C zerfällt, d.h. B ist darstellbar als $\prod_{i=1}^{k} P_i^{z_i}$, wissen wir:

$$\prod_{i=1}^{k} P_i^{z_i-e_i} = B\prod_{i=1}^{k} P_i^{-e_i} = (\alpha\mathcal{O}_\mathcal{K})A \tag{4.14}$$

Demzufolge ist A Hauptideal genau dann, wenn $\prod_{i=1}^{k} P_i^{z_i - e_i}$ Hauptideal ist. Anwenden von Lemma 4.11 liefert für (4.14):

$$A \text{ ist Hauptideal} \iff B_C' \cdot \underline{x} = \underline{z} - \underline{e} \text{ lösbar über } \mathbb{Z}^{k+s}.$$

Ferner wissen wir mit Lemma 4.11ii) und (4.14): Falls A Hauptideal ist, dann wird es von $1/\alpha \cdot \prod_{i=1}^{k} \beta_i^{x_i}$ erzeugt.

Diese Methode funktioniert auch, wenn A über F_C zerfällt, so daß wir abschließend folgenden Teilalgorithmus formulieren können.

4.12 Algorithmus *HITEST* (Teilalgorithmus)

Eingabe: Ideal A , Faktorbasis F_C, Matrix $B_C' \in \mathbb{Z}^{k\times(k+s)}$ bzgl. eines Zahlkörpers $\mathcal{K}$

Ausgabe: Lösungsvektor $\underline{x} \in \mathbb{Z}^{k+s}$ und α gemäß (4.14), falls A Hauptideal und „nein“ sonst.

<table>
<tr><td rowspan="2"></td><td colspan="2">/* Wahl der Idealklasse */
Wähle zufällig und gleichverteilt einen Exponentenvektor
$\underline{e} \in_R [\![0, \mathrm{const}]\!]^k$,
und bestimme $A \prod_{i=1}^{k} P_i^{e_i}$.</td><td>(1)</td></tr>
<tr><td colspan="2">/* Wahl eines Testideals */
Wähle etwa zufällig und gleichverteilt ein (reduziertes) Ideal B und $\alpha \in \mathcal{K}$ mit
$B \leftarrow (\alpha\mathcal{O}_\mathcal{K}) A \prod_{i=1}^{k} P_i^{e_i}$.</td><td>(2)</td></tr>
<tr><td colspan="3">UNTIL B zerfällt über F_C.</td><td>(3)</td></tr>
<tr><td colspan="3">$B \leftarrow \prod_{i=1}^{k} P_i^{z_i}$</td><td>(4)</td></tr>
<tr><td colspan="3">Löse $B_C' \cdot \underline{x} = \underline{z} - \underline{e}$ über $\mathbb{Z}^{k+s}$.</td><td>(5)</td></tr>
<tr><td colspan="3">IF Existenz einer Lösung</td><td>(6)</td></tr>
<tr><td>THEN</td><td colspan="2">Gib $\underline{x}$ und α aus.</td><td>(7)</td></tr>
<tr><td>ELSE</td><td colspan="2">Gib „nein“ aus.</td><td>(8)</td></tr>
</table>

In Kapitel 6 werden wir speziell für reellquadratische Zahlkörper eine exakte Ausarbeitung und Laufzeitanalyse von *HITEST* vornehmen.

4.2.3 Skizze des Algorithmus *NORMEQ*

Zur Lösung einer Normgleichung $N(\gamma) = m$ (vgl. 4.8) über einem beliebigen Zahlkörper formulieren wir die am Ende von Abschnitt 4.1.1 beschriebene Methode algorithmisch und wenden die Resultate für den Hauptidealtest aus Lemma 4.11 an. Damit erhalten wir den folgenden Algorithmus:

4.13 Algorithmus *NORMEQ*

Eingabe: $m \in \mathbb{N}$, Zahlkörper $\mathcal{K}$, Faktorbasis F_C, Basismatrix B_C für Γ_C, Spaltenindex s mit $0 \leq s \leq r$ für B'_C

Ausgabe: alle ganzen Lösungen der Normgleichung $N(\gamma) = m$ bis auf Assoziierte, falls welche existieren

<table>
<tr><td colspan="4">Bestimme alle ganzen Ideale A_j der Norm $|m|$ in $\mathcal{K}$ mit (4.9).</td><td>(1)</td></tr>
<tr><td colspan="4">Bestimme die Matrix B'_C aus B_C und s gemäß (4.10).</td><td>(2)</td></tr>
<tr><td colspan="4">FOR jedes Ideal A_j</td><td>(3)</td></tr>
<tr><td rowspan="7"></td><td colspan="3">erg $\leftarrow$ *HITEST* (A_j, F_C, B'_C)</td><td>(4)</td></tr>
<tr><td colspan="3">IF erg $\neq$ „nein“</td><td>(5)</td></tr>
<tr><td rowspan="5">THEN</td><td colspan="2">/* A_j ist Hauptideal und erg $= (\alpha, \underline{x})$ */
$\gamma \leftarrow 1/\alpha \cdot \prod_{i=1}^{k} \beta_i^{x_i}$</td><td>(6)</td></tr>
<tr><td colspan="2">/* Teste, ob $N(\gamma) = m$ oder $-m$. */</td><td>(7)</td></tr>
<tr><td colspan="2">IF sgn $N(\gamma) =$ sgn m</td><td>(8)</td></tr>
<tr><td>THEN</td><td>Gib γ aus.</td><td>(9)</td></tr>
<tr><td>ELSE</td><td>Multipliziere γ mit einer Einheit negativer Norm, falls eine solche existiert, und gib das Resultat aus.</td><td>(10)</td></tr>
</table>

Bzgl. der Vorzeichenabfrage der Norm von γ in (8) verfahren wir gemäß den Überlegungen zu Lemma 4.7. Wir setzen hier bei Existenz voraus, daß uns eine Einheit negativer Norm von $\mathcal{K}$ vorliegt. Dabei berücksichtigen wir, daß in Zahlkörpern ungeraden Körpergrades -1 stets ein solche Einheit ist.

Eine Ausarbeitung inklusive Laufzeitanalyse von *NORMEQ* werden wir speziell für reellquadratische Zahlkörper in Kapitel 6 vornehmen.

Kapitel 5

Die Berechnung der Klassenzahl in reellquadratischen Ordnungen

Wir werden den im vorangegangenen Kapitel skizzierten Algorithmus *CLASSREG* auf reellquadratische Ordnungen ausrichten. Spezialisierten wir uns auf quadratische Zahlkörper $\mathbb{Q}(\sqrt{\Delta})$, bräuchten wir als Eingabe $\Delta \in \mathcal{D}$ mit Δ *quadratfrei*, um *CLASSREG* anwenden zu können. Mit Bemerkung 2.31 wissen wir, daß dies ein zeitaufwendiges Problem ist. Deshalb werden wir die Methode von *CLASSREG* für quadratische Ordnungen verallgemeinern.

Ist die Ordnung maximal, können wir *CLASSREG* direkt auf den entsprechenden reellquadratischen Zahlkörper anwenden. Falls die Ordnung nicht maximal ist, müssen wir uns zusätzlich überlegen, wie sich die beschriebene Methode übertragen läßt und sie gegebenenfalls abändern.

Insbesondere spielt dabei die Wahl der Faktorbasis eine zentrale Rolle: Generell ist die Gültigkeit von Satz 4.1 für reellquadratische Ordnungen zu überprüfen. Wir überlegen, welche Probleme diesbezüglich auftreten können. Wir benötigen die Faktorbasis an zwei wesentlichen Stellen in *CLASSREG* : Zur Erzeugung der Klassengruppe Cl und zur Feststellung, ob das in (4.6) berechnete Ideal B über der Faktorbasis zerfällt. Dabei wäre eine eindeutige Zerlegung von B in Primideale günstig, was im allgemeinen nicht gewährleistet ist. (vgl. (2.9))

Bezüglich der Wahl der Faktorbasis und ihrer Erzeugendeneigenschaft leiten wir ein Resultat her, das auf binären quadratischen Formen beruht. Folgen wir der Argumentation von H. W. Lenstra jr. in [HwL], Seite 128 ff., wissen wir: Für jedes $\Delta \in \mathcal{D}$ existiert eine Bijektion, die die Klassengruppe $Cl(\Delta)$ auf die Äquivalenzklassen primitiver, binärer quadratischer Formen der Diskriminante Δ abbildet und die Gruppenstruktur von $Cl(\Delta)$ auf die Bildmenge überträgt. Deshalb ist es äquivalent, Ideale oder primitive, quadratische binäre Formen zu betrachten. Aus diesem Grund können wir ein Resultat von R. Schoof auf Ideale in quadratischen Ordnungen anwenden, vgl. [Dü], Satz 4.4:

5.1 Satz *(GRH) Sei $\Delta \in \mathcal{D}$. Dann existiert eine absolute, effektiv berechenbare Konstante $c_1 \in \mathbb{R}_{>0}$, so daß die Idealmenge*

$$F = \left\{ A_p,\ \overline{A_p} \mid A_p \text{ Primideal in } \mathcal{O}_\Delta \text{ mit } p \in \mathbb{P},\ \left(\tfrac{\Delta}{p}\right) = 1 \text{ und } p \leq c_1(\ln|\Delta|)^2 \right\}$$

eine Faktorbasis für die Klassengruppe $Cl(\Delta)$ liefert.

Mit E. Bach wissen wir aus [Ba], Seite 25, daß für negative Diskriminanten $c_1 = 6$ und für reellquadratische Diskriminanten $c_1 = 12$ gewählt werden kann. Deshalb betrachten wir von nun an für reellquadratische Ordnungen folgende Faktorbasen:

5.2 Korollar *(GRH) Sei $\Delta \in \mathcal{D}^+$. Dann liefert die Idealmenge*

$$F_C = \left\{ A_p,\ \overline{A_p} \mid p \in \mathbb{P}, \left(\tfrac{\Delta}{p}\right) = 1 \text{ und } p \leq C \right\}$$

für alle $C \geq 12(\ln\Delta)^2$ eine Faktorbasis für $Cl(\Delta)$.

Wir stellen fest, daß die Ideale $A_p, \overline{A_p} \in F_C$ Norm p haben, d.h. die Bedingung $p \leq C$ ist äquivalent zur Forderung $N(A_p) \leq C$ bzw. $N(\overline{A_p}) \leq C$. Deshalb bezeichnen wir hier analog zum allgemeinen Fall in (4.1) die Faktorbasis ebenfalls mit F_C bzgl. der Normschranke C. Von nun an setzen wir voraus, daß in F_C die Normschranke C stets gemäß Korollar 5.2 hinreichend groß gewählt ist, so daß die Idealmenge F_C eine Faktorbasis bildet.

Außerdem hat die gemäß Korollar 5.2 gewählte Faktorbasis positive Eigenschaften hinsichtlich der eindeutigen Zerlegung in Primideale, wie wir sehen werden. Auf einer Faktorbasis F_C gemäß Korollar 5.2 aufbauend führen wir analog zu Maximalordnungen $\mathcal{O}_\mathcal{K}$ von Zahlkörpern $\mathcal{K}$ für reellquadratische Ordnungen die Menge

$$\Gamma'_C = \{\underline{v} \in \mathbb{Z}^k \mid \textstyle\prod_{i=1}^k A_{p(i)}^{v_i} \text{ ist Hauptideal}\}$$

ein. Γ'_C ist ein Gitter in $\mathbb{Z}^k$. Entsprechend zu Kapitel 4, (4.4) definieren wir auch hier die Menge Γ_C. Dann erhalten wir analog zu Satz 4.1:

5.3 Korollar *(GRH) Seien $\Delta \in \mathcal{D}^+$, $C \in \mathbb{R}_{>0}$ mit $C \geq 12(\ln\Delta)^2$ beliebig. Dann ist die Menge Γ'_C ein k-dimensionales Gitter der Determinante h und die Menge Γ'_C ein $(k+1)$-dimensionales Gitter der Determinante hR.*

Daher bezeichnen wir die Gitter Γ'_C, Γ_C analog als *Relationengitter* und Γ_C auch als *erweitertes Relationengitter.* Ihre Elemente nennen wir *Relationen* bzw. *erweiterte Relationen.*

Mit Korollar 5.3 sehen wir, daß sich das Prinzip der Relationengenerierung für die Berechnung der Klassenzahl und des Regulators auf reellquadratische Ordnungen übertragen läßt. Daher wenden wir uns Algorithmus *CLASSREG* erneut zu: Wir werden die einzelnen Teilaufgaben genauer untersuchen, entsprechende Teilalgorithmen formulieren und diese analysieren. Abschließend bestimmen wir die Komplexität des gesamten Algorithmus, die sich bei der Übertragung auf reellquadratische Ordnungen ergibt.

In den nächsten beiden Abschnitten beschäftigen wir uns mit der Initialisierung des Algorithmus, was den Schritten (1) und (2) in *CLASSREG* entspricht. Dann wenden wir uns detailliert der Relationengenerierung zu. (vgl. (3)) Danach geben wir ein Verfahren an, das die Determinanten beider Relationengitter berechnet. (vgl. (4) und (6) in *CLASSREG*)

5.1 Die Bestimmung der Abbruchkonstanten $2H^*$

Wie wir gesehen haben, wird in Schritt (5) von Algorithmus *CLASSREG* die Abbruchbedingung mit Hilfe einer sogenannten Abbruchkonstanten $2H^*$ formuliert. Wir werden eine Konstante H^* bestimmen, die der Bedingung

$$H^* < hR < 2H^* \tag{5.1}$$

genügt. Im folgenden wenden wir uns daher der Bestimmung von H^* zu.

5.1.1 Theoretischer Hintergrund

Zur Bestimmung der Konstanten H^* wählen wir einen Zugang aus der analytischen Zahlentheorie: Für $\Delta \in \mathcal{D}$ und $p \in \mathbb{P}$ definieren wir zunächst die *Eulerfaktoren*

$$E(\Delta, p) = \left(1 - \left(\frac{\Delta}{p}\right) \cdot \frac{1}{p}\right)^{-1}.$$

Dann erhalten wir mit der *analytischen Klassenzahlformel* auch für nichtmaximale Ordnungen $\mathcal{O}_\Delta$ der Diskriminante Δ: (vgl. [Sc], Seite 261 ff.)

5.4 Satz *Für $\Delta \in \mathcal{D}^+$ gilt:*

$$hR = \frac{\sqrt{\Delta}}{2} \cdot \prod_{p \in \mathbb{P}} E(\Delta, p). \tag{5.2}$$

Die Gleichung in (5.2) enthält ein unendliches Produkt. Wegen seiner langsamen Konvergenz läßt sich hR auf diesem Weg für große $\Delta \in \mathcal{D}^+$ nicht effizient berechnen. Wir formulieren daher eine Approximation aus endlich vielen Faktoren. Dazu führen wir eine obere Schranke $Q \in \mathbb{N}$ für die Primzahlen p der Eulerfaktoren $E(\Delta, p)$ ein:

$$H(\Delta, Q) = \frac{\sqrt{\Delta}}{2} \cdot \prod_{p \in \mathbb{P}, p \leq Q} E(\Delta, p). \tag{5.3}$$

Mit einem Resultat von R. Schoof können wir die Konvergenzrate für die Produktentwicklung in $H(\Delta, Q)$ abschätzen, woraus wir eine Schranke für den Fehler in (5.3) herleiten.

5.5 Satz *(GRH) Es existiert eine absolute, effektiv berechenbare Konstante $c_4 \in \mathbb{R}_{>0}$, so daß für alle $\Delta \in \mathcal{D}^+$ und für alle $Q > c_4 \cdot (\ln \Delta)^2$ gilt:*

$$\frac{3}{4} < \frac{hR}{H(\Delta, Q)} < \frac{3}{2}.$$

Beweis: Wir erhalten mit [Sc], Theorem 6.3 unter (GRH): Es existieren absolute, effektiv berechenbare Konstanten $c_2, c_3 \in \mathbb{R}_{>0}$, so daß für alle $\Delta \in \mathcal{D}^+$ und für alle $Q > c_2(\ln |\Delta|)^2$

$$\left| 1 - \prod_{p \in \mathbb{P}, p > Q} E(\Delta, p)^{-1} \right| < c_3 \cdot \frac{\ln |\Delta Q|}{\sqrt{Q}}$$

gilt. Unter der Voraussetzung $(\ln \Delta)^2 < Q/c_2$ ergibt sich für die obere Schranke

$$c_3 \cdot \frac{\ln(\Delta Q)}{\sqrt{Q}} < c_3 \cdot \frac{\sqrt{Q/c_2} + \ln Q}{\sqrt{Q}} = c_3 \cdot \left(\sqrt{\frac{1}{c_2}} + \frac{\ln Q}{\sqrt{Q}} \right).$$

Daraus folgern wir die Existenz einer absoluten, effektiv berechenbaren Konstanten $c_4 \in \mathbb{R}_{>0}$, so daß für alle $Q > c_4 \cdot (\ln \Delta)^2$

$$\left| 1 - \prod_{p \in \mathbb{P}, p > Q} E(\Delta, p)^{-1} \right| < c_3 \cdot \left(\sqrt{\frac{1}{c_2}} + \frac{\ln Q}{\sqrt{Q}} \right) < \frac{1}{3}.$$

gilt. Multiplizieren wir die Ungleichung mit $(\sqrt{\Delta}/2) \cdot \prod_{p \in \mathbb{P}} E(\Delta, p)$ und wenden (5.2) sowie (5.3) an, ergibt sich $|hR - H(\Delta, Q)| < (1/3) \cdot hR$, was äquivalent ist zu

$$\frac{2}{3} < \frac{H(\Delta, Q)}{hR} < \frac{4}{3},$$

woraus durch Invertieren die Behauptung folgt. ∎

Sei $\Delta \in \mathcal{D}^+$. Unter Verwendung der Konstanten c_4 aus Satz 5.5 erhalten wir für $Q > c_4 \cdot (\ln \Delta)^2$ eine Approximation H^* für hR, indem wir

$$H^* = \frac{3}{4} H(\Delta, Q)$$

wählen. H^* genügt dann der Bedingung für eine Abbruchkonstante aus (5.1). Gemäß Lemma 5.5 wissen wir nun zwar von der Existenz der Konstanten c_4, jedoch sind weder dort noch in [Sc] Angaben über deren explizite Bestimmung zu finden. Daher wählen wir zur Bestimmung einer geeigneten Konstanten den folgenden Ansatz, der sich an der Idee von [Dü] orientiert: Setze

$$H^* = \mu \cdot H(\Delta, Q) \tag{5.4}$$

mit einem geeigneten Parameter $\mu \in \mathbb{R}_{>0}$ und $1/2 < \mu < 1$, so daß die folgende Bedingung analog zu (5.1) erfüllt ist:

$$\mu \cdot H(\Delta, Q) < hR < 2\mu \cdot H(\Delta, Q). \tag{5.5}$$

Abhängig vom zugrundeliegenden Δ bestimmen wir eine Schranke $Q_0 = Q_0(\Delta) \in \mathbb{N}$, so daß für alle $Q > Q_0$ und geeignet gewähltes μ H^* der Forderung in (5.5) genügt.

Den in (5.3) bzgl. $H(\Delta, Q)$ entstehenden Fehler betrachten wir multiplikativ und bezeichnen ihn mit $T(Q)$, (vgl. [BuWi])

$$T(Q) = \frac{hR}{H(\Delta, Q)}. \tag{5.6}$$

Die Forderung in (5.5) ist demnach genau dann erfüllt, wenn $\mu < T(Q) < 2\mu$ gilt. Wir betrachten die äquivalente Gleichung

$$\ln \mu < \ln T(Q) < \ln(2\mu). \tag{5.7}$$

Zuerst wenden wir uns der Wahl eines geeigneten Parameters μ zu. Genügt $\ln T(Q)$ der Bedingung

$$|\ln T(Q)| < \min\{-\ln \mu, \ln(2\mu)\}, \tag{5.8}$$

dann können wir die Gültigkeit von (5.7) garantieren. (Dies folgt aus einer Fallunterscheidung nach dem Vorzeichen von $\ln T(Q)$ in (5.8) und $1/2 < \mu < 1$.) Da wir in (5.6) den entstehenden Fehler $T(Q)$ möglichst gering halten wollen, betrachten wir die Werte, die in (5.8) angenommen werden.

$$\min\{-\ln \mu, \ln(2\mu)\} = \begin{cases} \ln(2\mu) & \text{, falls } 1/2 < \mu < \sqrt{2}/2 \\ -\ln \mu & \text{, falls } \sqrt{2}/2 \leq \mu < 1 \end{cases}$$

Aufgrund des Monotonieverhaltens beider Argumentfunktionen wird $\min\{-\ln \mu, \ln(2\mu)\}$ maximal für $\mu = \sqrt{2}/2$. Dann wissen wir, daß aus dieser Wahl für μ die Forderung in (5.8)

$$|\ln T(Q)| < \ln \sqrt{2} \tag{5.9}$$

lautet. Falls diese erfüllt ist, folgt (5.7) für $\mu = \sqrt{2}/2$. Daher leiten wir im folgenden eine obere Schranke für $|\ln T(Q)|$ her, um ein Q_0 zu finden, so daß (5.9) für alle $Q > Q_0$ erfüllt ist. Dazu greifen wir auf Resultate von [BuWi] zurück, die wir speziell auf reellquadratische Ordnungen anwenden.

5.6 Lemma *(GRH) Für alle $\Delta \in \mathcal{D}^+$ und $Q \geq 2$ gilt:*

$$|\ln T(Q)| \leq C(Q) \cdot \frac{4 + 3\ln Q}{\sqrt{Q}} + \frac{2}{Q}$$

mit

$$C(Q) = \ln \Delta \cdot \left(\frac{1}{\pi \ln Q} + \frac{5,3}{(\ln Q)^2} \right) + \frac{1}{\pi} + \frac{4}{\ln Q}.$$

Beweis: Sei $\Delta \in \mathcal{D}^+$. Aus der Definition von $T(Q)$ in (5.6) folgt $T(Q) = \prod_{p \in \mathbb{P}, p > Q} E(\Delta, p)$. Für einige p berechnen sich die entsprechenden Eulerfaktoren zu $E(\Delta, p) = 1$ wegen des Kronecker-Symbols $(\Delta/p) = 0$. Damit vereinfacht sich $T(Q)$ zu

$$\begin{aligned} T(Q) &= \prod_{\substack{p>Q,\\ (\Delta/p)\neq 0}} E(\Delta, p) \\ &= \prod_{\substack{p>Q,\\ (\Delta/p)\neq 0}} \left(1 + \frac{a(p)}{p}\right)^{-1} \end{aligned}$$

mit $a(p) = -(\Delta/p) \in \{-1, 1\}$. Da die einzelnen Eulerfaktoren stets positiv sind, folgt

$$-\ln T(Q) = \sum_{\substack{p>Q,\\ (\Delta/p)\neq 0}} \ln\left(1 + \frac{a(p)}{p}\right).$$

Wegen $|a(p)/p| < 1$ können wir die Potenzreihenentwicklung des Logarithmus anwenden.

$$-\ln T(Q) = \sum_{\substack{p>Q,\\ (\Delta/p)\neq 0}} \sum_{j=1}^{\infty} \left(\frac{a(p)}{p}\right)^j \cdot \frac{(-1)^{j+1}}{j}$$

Da diese Reihe absolut konvergent ist, dürfen wir sie umordnen.

$$-\ln T(Q) = \underbrace{\sum_{\substack{p>Q,\\ (\Delta/p)\neq 0}} \frac{a(p)}{p}}_{S_1(Q)} + \underbrace{\sum_{\substack{p>Q,\\ (\Delta/p)\neq 0}} \sum_{j=2}^{\infty} \left(\frac{a(p)}{p}\right)^j \cdot \frac{(-1)^{j+1}}{j}}_{S_2(Q)} \tag{5.10}$$

Für die erste Teilsumme erhalten wir mit [Dü], Lemma 7.1, speziell auf reellquadratische Ordnungen angewandt: Für $Q \geq 2$ und (GRH) gilt

$$|S_1(Q)| < C(Q) \cdot \frac{4 + 3\ln Q}{\sqrt{Q}}$$

mit $C(Q)$ wie oben angegeben. Für die zweite Teilsumme leiten wir analog zu [Dü], Lemma 7.2 her, daß für $Q \in \mathbb{N}$ gilt

$$|S_2(Q)| \leq \frac{2}{Q}.$$

Insgesamt resultiert dann aus (5.10) und $|\ln T(Q)| \leq |S_1(Q)| + |S_2(Q)|$ die Behauptung. ∎

Setzen wir in die Ungleichung von Lemma 5.6 $C(Q)$ ein, stellen wir Abhängigkeiten zwischen Q und $\ln \Delta$ fest, die sich nicht direkt nach Q auflösen lassen. Wir stellen jedoch fest, daß die rechte Seite der Ungleichung für festes Δ streng monoton fallend bzgl. Q ist. Daher existiert eine Zahl Q_0 mit der Eigenschaft, daß für alle $Q > Q_0$

$$C(Q) \cdot \frac{4 + 3\ln Q}{\sqrt{Q}} + \frac{2}{Q} < \ln\sqrt{2}, \tag{5.11}$$

gilt, woraus wiederum $|\ln T(Q)| < \ln\sqrt{2}$ wegen Lemma 5.6 folgt. Um eine geeignete Schranke Q_0 zu finden, schätzen wir die linke Seite in (5.11) nach oben ab.

5.7 Lemma *Für alle $Q \geq 2$ und $\Delta \in \mathcal{D}^+$ gilt*

$$C(Q) \cdot \frac{4 + 3\ln Q}{\sqrt{Q}} + \frac{2}{Q} \leq 155 \cdot Q^{-1/4} \cdot \ln \Delta.$$

Beweis: Sei $Q \geq 2$. Dann gilt mit der Definition von $C(Q)$ in Lemma 5.6:

$$C(Q) \cdot \frac{4 + 3\ln Q}{\sqrt{Q}} + \frac{2}{Q} \leq \frac{4 + 3\ln Q}{\sqrt{Q}} \cdot (12\ln\Delta + 7) + \frac{2}{\sqrt{Q}}.$$

Wegen $Q \geq 2$ wissen wir $4 + 3\ln Q \leq 9\ln Q$, und wegen $\Delta \in \mathcal{D}^+$ gilt $\Delta \geq 5$, so daß $12\ln\Delta + 7 \leq 17\ln\Delta$ sowie $2 \leq 2\ln\Delta \cdot \ln Q$ gelten. Daraus folgt:

$$\begin{aligned} C(Q) \cdot \frac{4 + 3\ln Q}{\sqrt{Q}} + \frac{2}{Q} &\leq (9 \cdot 17\ln Q \cdot \ln\Delta + 2\ln Q \cdot \ln\Delta)/\sqrt{Q} \\ &= \frac{\ln Q}{\sqrt{Q}} \cdot 155\ln\Delta \end{aligned}$$

Wir benutzen, daß $\ln Q \leq Q^{1/4}$ für $Q \geq 2$, und erhalten dann die Behauptung. ■

Auf der Grundlage von Lemma 5.7 lassen sich dann eine geeignete Schranke Q_0 sowie eine Abbruchkonstante H^* herleiten:

5.8 Korollar *(GRH) Für alle $Q > 620^4 \cdot \lceil\ln\Delta\rceil^4 = Q_0(\Delta)$ und $\Delta \in \mathcal{D}^+$ ist*

$$2H^* = \sqrt{2} \cdot H(\Delta, Q)$$

eine geeignete Abbruchkonstante, die der Bedingung $H^* < hR < 2H^*$ genügt.

Beweis: In unserer Herleitung setzten wir formal $H^* = \mu \cdot H(\Delta, Q)$ (vgl. (5.4)) und forderten in (5.5), daß $\mu \cdot H(\Delta, Q) < hR < 2\mu \cdot H(\Delta, Q)$ in Analogie zur Ausgangsforderung in (5.1) gilt. Dann zeigten wir in (5.9): Falls $|\ln T(Q)| < \ln\sqrt{2}$ für $\mu = \sqrt{2}/2$, dann gilt auch die Forderung bzgl. der Abbruchbedingung in (5.5) für $\mu = \sqrt{2}/2$.
Mit Lemma 5.6 und Lemma 5.7 wissen wir für $Q \geq 2$ und (GRH) $|\ln T(Q)| < 155 \cdot Q^{-1/4} \cdot \ln\Delta$. Wir fordern daher $155 \cdot Q^{-1/4} \cdot \ln\Delta < \ln\sqrt{2}$, was äquivalent zu

$$\left(\frac{310}{\ln 2} \cdot \ln\Delta\right)^4 < Q$$

ist. Durch Aufrunden erhalten wir die Behauptung. ■

5.9 Bemerkung Gemäß Satz 5.5 wissen wir zwar von der Existenz einer Schranke $Q_0 \geq c_4 \cdot (\ln\Delta)^2$, wobei $c_4 \in \mathbb{R}_{>0}$ eine Konstante ist, über deren Bestimmung uns jedoch keine Information vorliegt. Wir haben deshalb in obigem Korollar $Q_0 > 620^4 \cdot \lceil\ln\Delta\rceil^4$ bestimmt, was asymptotisch eine größere untere Schranke ist. Im Hinblick auf die Gesamtlaufzeit ist diese Schranke völlig ausreichend. In der Praxis wird man jedoch bestrebt sein, auf der Grundlage von Lemma 5.6 eine bessere Schranke für Q_0 zu finden. Dies kann z.B. mit einer Intervallschachtelung für jedes $\Delta \in \mathcal{D}^+$ erreicht werden.

5.1.2 Die Formulierung von Algorithmus *INITH**

Jetzt sind wir in der Lage, einen Algorithmus zur Berechnung der Abbruchkonstanten $2H^*$ anzugeben. Dabei bringen wir die Darstellung aus Korollar 5.8 und die Definition von $H(\Delta, Q)$ aus (5.3) ein:

$$\begin{aligned} 2H^* &= \sqrt{2} \cdot H(\Delta, Q) = \sqrt{\Delta/2} \cdot \prod_{p \in \mathbb{P}, p \leq Q} E(\Delta, p) \\ &= \sqrt{\Delta/2} \cdot \prod_{p \in \mathbb{P}, p \leq Q} \frac{p}{p - (\Delta/p)} \end{aligned}$$

für $Q \geq Q_0$, wobei wir das Euler-Produkt so umformen, wie es im nachfolgenden Algorithmus berechnet wird. Zur Berechnung von (Δ/p) verweisen wir auf [Co], Algorithm 1.4.10. Für eine Approximation der Wurzel verweisen wir auf [Br].

5.10 Algorithmus *INITH** (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$
Ausgabe: $2\hat{H}^*$, eine Approximation der Abbruchkonstanten $2H^*$ der Präzision 4

/* Primzahlgrenze für Eulerfaktoren $E(\Delta, p)$ */ $Q_0 \leftarrow 620^4 \cdot \lceil \ln \Delta \rceil^4$	(1)
/* Erstelle eine Liste aller Primzahlen $\leq Q_0$ und deren Länge l. */ $L \leftarrow \mathit{PRIMLIST}\,(Q_0)$ $l \leftarrow \sharp L$	(2)
Lies das erste Element p aus der Primzahlliste L ein.	(3)
/* Initialisiere E. j gibt die aktuelle Position in L an. */ $E \leftarrow 1$, $j \leftarrow 1$.	(4)
WHILE $j \leq l$	(5)
Berechne das Kronecker-Symbol (Δ/p), und setze $E \leftarrow E \cdot \frac{p}{p-(\Delta/p)}$.	(6)
Lies die nächste Primzahl p aus der Primzahlliste L ein, falls noch eine existiert, und setze $j \leftarrow j+1$.	(7)
Bestimme eine Approximation $2\hat{H}^*$ von $\sqrt{E^2\Delta/2}$ der Präzision 4.	(8)

5.11 Bemerkung Für die Approximationen greifen wir auf Methoden inklusive ihrer Laufzeiten von R. Brent zurück, die sich allerdings auf relative Fehler beziehen. (vgl. [Br]) Wir können die Resultate mit einer leichten Änderung übernehmen: Wir brauchen eine Approximation $\hat{c}$ der Präzision n von $c \in \mathbb{C}$ (bzgl. totalem Fehler in Definition 3.20) Für die gemäß [Br] bestimmte Approximation c' der Präzision n' wissen wir

$$\frac{|c - c'|}{|c|} < 2^{-n'} \iff |c - c'| < 2^{-n'}|c|.$$

Daraus erkennen wir: $\hat{c} = c'$ ist eine Approximation der Präzision n in unserem Sinne, wenn wir $2^{-n'}|c| < 2^{-n}$ fordern, d.h. $n' = \lceil n + \log|c| \rceil$ erfüllt diese Bedingung. In der Regel wird bei uns $\log|c|$ polynomielle Länge in $\log \Delta$ haben.

Die in (2) beschriebene Primzahlliste erstellen wir mit dem *Sieb des Eratosthenes*, das wir in algorithmischer Form vorstellen. Für die Siebphase (vgl. (7) - (10) von *PRIMLIST*) existieren einige Verbesserungen, auf deren Anwendung wir des besseren Verständnisses wegen verzichten. Sie schlagen sich in der asymptotischen Laufzeitanalyse nur geringfügig nieder.

5.12 Algorithmus *PRIMLIST* (Teilalgorithmus)

Eingabe: $N \in \mathbb{N}$
Ausgabe: L, die Liste aller Primzahlen $\leq N$

/* Initialisierung */ Lege eine Liste *test* an mit $test[j] \leftarrow 1$, für alle $2 \leq j \leq N$, und $test[1] \leftarrow 0$. Setze L auf die leere Liste und $j \leftarrow 1$.	(1)
WHILE $j^2 \leq N$	(2)
/* Suche kleinste Primzahl in $test[j..N]$. */	(3)
WHILE $test[j] = 0$	(4)
$j \leftarrow j + 1$.	(5)
/* Falls $test[j]$ definiert ist, enthält es Primzahl j. */	(6)
$i \leftarrow 2j$	(7)
WHILE $i \leq N$ /* Streichen der Vielfachen von $test[j]$ */	(8)
$test[i] \leftarrow 0$ /* markiert, daß keine Primzahl */	(9)
$i \leftarrow i + j$	(10)
$j \leftarrow j + 1$	(11)
/* Sammle alle Primzahlen aus *test*. */	(12)
FOR $1 \leq j \leq N$	(13)
Füge $test[j]$ mit Eintrag 1 der Liste L hinten an.	(14)
$j \leftarrow j + 1$.	(15)

5.13 Lemma *Bei Eingabe einer positiven ganzen Zahl $N \in \mathbb{N}$ bestimmt der deterministische Algorithmus PRIMLIST alle Primzahlen $\leq N$ in Zeit $O(N \cdot \log N \cdot \log\log N)$.*

Beweis: Sei $N \in \mathbb{N}$ beliebig. Die Initialisierung in (1) und die Schlußabfrage in (13) - (15) benötigen Zeit $O(N \cdot \log N)$.

Die Abfrage der Bedingung in (2) braucht jeweils $O((\log N)^2)$ und wird so oft durchgeführt, wie wir Primzahlen in N haben, also $O(N/\log N)$-mal. (vgl. [RoSc], Cor.2) Wir brauchen demnach Zeit $O(N \cdot \log N)$ für alle Abfragen.
Die Suche nach der nächsten Primzahl in (4) - (5) erfordert jeweils Zeit $O((p_{i+1} - p_i)\log N)$ Zeit, wobei $p_{i+1}, p_i \leq N$ zwei aufeinanderfolgende Primzahlen in $test[1..N]$ sind. Insgesamt braucht das Auffinden der nächsten Primzahl Zeit $O(N \cdot \log N)$.
Das Streichen der Vielfache in (7) - (10) erfordert je Primzahl p Zeit $O(\log N \cdot N/p)$. Das ergibt für alle Primzahlen in *test*

$$O(N \cdot \log N) \cdot \sum_{p \leq N} \frac{1}{p} = O(N \cdot \log N \cdot \log\log N),$$

wobei wir für die Summe eine Abschätzung von [RoSc] (Cor. zu Theorem 5) wählen. Damit benötigen wir für diese Schleife Zeit $O(N \cdot \log N \cdot \log\log N)$, woraus die gesamte Laufzeit folgt. ∎

Abschließend analysieren wir *INITH** und wenden das Ergebnis von *PRIMLIST* an.

5.14 Satz *(GRH) Der deterministische Algorithmus INITH* berechnet bei Eingabe von $\Delta \in \mathcal{D}^+$ eine Approximation der Abbruchkonstanten $2H^*$ der Präzision 4 in polynomieller Laufzeit, asymptotisch beträgt sie $L_\Delta[0]$.*

Beweis: Wir analysieren *INITH** schrittweise bzgl. $\Delta \in \mathcal{D}^+$.
In (1) ist die aufwendigste Operation die Berechnung von $\lceil \ln \Delta \rceil$. Dazu benötigen wir eine Approximation für $\ln \Delta$ mit einer Nachkommastelle Präzision, was in Polynomzeit bewältigt werden kann. (vgl. [Br], Theorem 9.1)
Die Erstellung der Primzahlliste und deren Länge in (2) erfordert gemäß Lemma 5.13 Polynomzeit wegen $Q_0 = O((\log \Delta)^4)$.
Für die Berechnung von E in der Schleife (5) - (7) bestimmen wir je Primzahl das Kronecker-Symbol (Δ/p), was wegen Lemma 2.42 in Polynomzeit geschieht. Da wir $\leq Q_0$ viele Primzahlen haben, erfordert die Berechnung aller Kronecker-Symbole Polynomzeit. Zu berücksichtigen bleibt noch die Produktbildung von $E \in \mathbb{Q}$. Zähler und Nenner der Faktoren, die an E ranmultipliziert werden, sind in (6) stets $\leq p+1$. Somit hat E Länge $O(\log \prod_{p \leq Q_0} p) = O(Q_0)$ wegen [RoSc], Theorem 4. Daraus folgern wir, daß die Bestimmung von E Polynomzeit erfordert.
Abschließend geschieht in (8) die Multiplikation und die Approximation der Wurzel in Polynomzeit (vgl. [Br]), da das Produkt polynomielle Länge in $\log \Delta$ hat. Fassen wir alle Teilabschätzungen zusammen, folgt die Behauptung. ∎

5.2 Die Konstruktion einer Faktorbasis

Teilaufgabe (2) von *CLASSREG* besteht darin, eine Faktorbasis zu bestimmen. Wie bereits erwähnt betrachten wir speziell für quadratische Ordnungen gemäß Korollar 5.2 Faktorbasen der Form

$$F_C = \{A_p, \overline{A_p} \mid p \in \mathbb{P}, (\tfrac{\Delta}{p}) = 1 \text{ und } p \leq C\}.$$

Demnach müssen wir die Ideale $A_p, \overline{A_p}$ berechnen. Somit haben wir alle Vorbereitungen getroffen, um die Konstruktion einer Faktorbasis algorithmisch anzugeben.

Zum Aufbau von F_C ist zu beachten, daß wir wie immer

$$k = \sharp F_C$$

setzen. Die Primideale A_p, $\overline{A_p}$ sind bzgl. aufsteigendem p sortiert. $\overline{A_p}$ kommt direkt nach A_p, z.B. $\{A_2, \overline{A_2}, A_5, \overline{A_5}, A_{11}, \overline{A_{11}}, \ldots\}$ entspräche einer solchen Sortierung.

5.15 Algorithmus *FAKBAS* (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$, $C \in \mathbb{N}$ Normschranke
Ausgabe: F_C Idealmenge und $k = \sharp F_C$

/* Erstelle eine Liste aller Primzahlen $\leq C$ und deren Länge. */ $L \leftarrow \mathit{PRIMLIST}\ (C)$ $l \leftarrow \sharp L$			(1)
Lies die erste Primzahl p aus der Primzahlliste L ein. Initialisiere die aktuelle Position j in L mit 1, $j \leftarrow 1$.			(2)
/* k bezeichne die aktuelle Ordnung von F_C. */ $k \leftarrow 0$			(3)
WHILE $j \leq l$			(4)
	Berechne das Kronecker-Symbol. $s \leftarrow (\Delta/p)$		(5)
	IF $s = 1$		(6)
	THEN	/* Bestimme A_p und $\overline{A}_p$. */ $(A_p, \overline{A_p}) \leftarrow \mathit{PRIMID}\ (\Delta, p)$	(7)
		Füge A_p, $\overline{A_p}$ der Menge F_C hinten an.	(8)
		/* Aktualisiere die Größe der Faktorbasis. */ $k \leftarrow k + 2$	(9)
	Lies die nächste Primzahl p aus L ein, falls noch eine existiert, und setze $j \leftarrow j + 1$.		(10)

Wir analysieren die Laufzeit asymptotisch bzgl. C. Dazu führen wir wie bereits in Kapitel 2 für C die Schreibweise

$$C = {L_\Delta}^c, \qquad c \in \mathbb{R}_{>0} \tag{5.12}$$

ein. Am Ende des Kapitels bestimmen wir ein optimales c bzw. C, um die Gesamtlaufzeit von *CLASSREG* bzgl. reellquadratischer Ordnungen zu optimieren.

5.16 Satz *Der probabilistische Algorithmus FAKBAS berechnet bei Eingabe von $\Delta \in \mathcal{D}^+$ und $C \in \mathbb{N}$ die Idealmenge F_C in erwarteter Laufzeit $L_\Delta[c]$.*

Beweis: Wir analysieren *FAKBAS* schrittweise bzgl. $\Delta \in \mathcal{D}^+$ und $C \in \mathbb{N}$.
In (1) erfordert die Bestimmung der Primzahlliste und deren Länge Zeit $L_\Delta[c]$ wegen Lemma 5.13 und $C = {L_\Delta}^c$. Beachte dabei, daß $\log C = L_\Delta[0]$ gilt.
In der Schleife (4) – (10) bestimmen wir jeweils das Kronecker-Symbol (Δ/p), was wegen Lemma 2.42 für $p \leq C$ Polynomzeit bzgl. $\log C$ erfordert, also $L_\Delta[0]$. Für $(\Delta/p) = 1$ berechnen wir in (7) mit dem probabilistischen Algorithmus *PRIMID* die Darstellungen von A_p und $\overline{A_p}$, was mit Lemma 2.44 in erwarteter polynomieller Laufzeit bzgl. $\log \Delta$ und $\log p \leq \log C$ geschieht, also in $L_\Delta[0]$. Die Schleife wird insgesamt $\sharp L$-mal ausgeführt. Mit [RoSc], Cor. 2 zu Theorem 1 gilt $\sharp L = O(C/\log C) = L_\Delta[c]$. Demnach benötigt die Ausführung der Schleife in (4) – (10) Zeit $L_\Delta[c]$, woraus die Behauptung folgt. ∎

Für spätere Anwendungen untersuchen wir die Ideale der Faktorbasis F_C.

5.17 Lemma *Die Ideale A_p, $\overline{A_p}$ der Faktorbasis F_C sind invertierbar.*

Beweis: Wir wenden Proposition 2.45 an. Dazu zeigen wir, daß die Führer von A_p bzw. $\overline{A_p}$ 1 sind.
Gemäß Lemma 2.35 ist $f(A_p) = \mathrm{ggT}(p, b_p, \ldots)$ bzgl. der Standarddarstellung von A_p. Mit (2.8) gilt $b_p^2 \equiv \Delta \bmod 4p$ und $0 \leq b_p \leq p$. Aus $b_p \in \{0, p\}$ folgt $p \mid \Delta$, was im Widerspruch zu $(\Delta/p) = 1$ bzw. $A_p \in F_C$ steht. Also ist $1 = \mathrm{ggT}(p, b_p, \ldots) = f(A_p)$. Analog berechnen wir $f(\overline{A_p})$. ∎

Dann berechnen sich die Normen von A_p, $\overline{A_p}$ gemäß Lemma 2.47 zu

$$N(A_p) = p \qquad \text{und} \qquad N(\overline{A_p}) = p.$$

Im nächsten Abschnitt betrachten wir reduzierte Ideale B in $\mathcal{O}_\Delta$. Sie genügen $N(B) \leq \sqrt{\Delta}$. (vgl. Lemma 2.52) Zerfallen sie zusätzlich über F_C, können wir wegen der Multiplikativität der Norm invertierbarer Ideale für die Normschranke C sowie für die Ordnung k von F_C o.B.d.A. annehmen:

$$C < \sqrt{\Delta} \qquad \text{und} \qquad k \leq 2\sqrt{\Delta}. \tag{5.13}$$

5.3 Die Relationengenerierung

Wir wenden uns nun einer der Hauptaufgaben zu, der Erzeugung von (erweiterten) Relationen, vgl. Schritt (3) von *CLASSREG* . Diesen Prozeß des Suchens bzw. Erzeugens von Relationen bezeichnen wir als *Relationengenerierung.*

Wir orientieren uns dabei an dem in Kapitel 4 geschilderten Prinzip: Zuerst wählen wir eine Idealklasse von Cl, indem wir stellvertretend gemäß (4.5) ein Produkt von Idealen bzgl. einer vorgegebenen Faktorbasis wählen. Anschließend wählen wir in dieser Idealklasse ein Ideal aus. (vgl. (4.6)) Falls dieses Ideal über der zugrundeliegenden Faktorbasis zerfällt, konstruieren wir gemäß (4.7) eine erweiterte Relation.

Diese Methode funktioniert insbesondere immer, wenn eine eindeutige Faktorisierung ganzer Ideale in Primideale möglich ist, wie z.B. in Maximalordnungen. Obwohl wir wegen (2.9) wissen, daß dies in quadratischen Ordnungen im allgemeinen nicht möglich ist, läßt sich das beschriebene Prinzip mit Hilfe unserer Faktorbasis F_C übertragen, wie wir sehen werden.

5.18 Algorithmus *RELATION* (Skizze)

Eingabe: $\Delta \in \mathcal{D}^+$, $F_C = \{P_1, \ldots, P_k\}$ eine Faktorbasis
Ausgabe: erweiterte Relation $(v_1, \ldots, v_k, -\ln|\alpha|)$, falls die Relationengenerierung erfolgreich ist.

/* Wahl einer Idealklasse */ Wähle zufällig und gleichverteilt einen Exponentenvektor, d.h. $\underline{e} \in_R [\![0, \Delta]\!]^k$.		(1)
/* Wahl eines Ideals in dieser Idealklasse */ Wähle zufällig und gleichverteilt ein reduziertes Ideal B mit $B = (\alpha\mathcal{O}_\Delta)\prod_{i=1}^k P_i^{e_i}$.		(2)
IF B zerfällt über F_C		(3)
THEN	$B \leftarrow \prod_{i=1}^k P_i^{z_i}$ /* $(1/\alpha)\mathcal{O}_\Delta = \prod_{i=1}^k P_i^{e_i - z_i}$ */	(4)
	$(v_1, \ldots, v_k, -\ln|\alpha|) \leftarrow (e_1 - z_1, \ldots, e_k - z_k, -\ln|\alpha|)$ /* ist eine erweiterte Relation */	(5)

Im folgenden wenden wir uns der Realisierung sowie der Analyse der einzelnen Teilschritte von *RELATION* zu, wobei folgende zentrale Fragen zu beantworten sind:

- Wie läßt sich in (2) ein Ideal B bestimmen?
- Wie kann in (3) festgestellt werden, ob ein Ideal B über einer gegebenen Faktorbasis zerfällt, wobei allgemein in $\mathcal{O}_\Delta$ keine eindeutige Zerlegung in Primideale möglich ist?

Wir beginnen mit der einfacheren Analyse von (1), der Wahl einer Idealklasse.

5.3.1 Die Wahl einer Idealklasse

Mit der in Schritt (1) von *RELATION* vorgestellten Methode ordnen wir jedem Exponentenvektor $\underline{e} \in [\![0, \Delta]\!]^k$ die entsprechende Idealklasse

$$\Big[\prod_{i=1}^k P_i^{e_i}\Big]$$

in Cl zu. Wir interessieren uns für die Verteilung der Idealprodukte $\prod_{i=1}^{k} P_i^{e_i}$ auf die Idealklassen von Cl, wenn wir $\underline{e}$ zufällig und gleichverteilt in $[\![0, \Delta]\!]^k$ wählen. Aus einem Resultat von A. K. Lenstra folgern wir:

5.19 Lemma *Seien $\Delta \in \mathcal{D}^+$, F_C eine Faktorbasis gemäß Korollar 5.2 und $[A_j]$ eine Idealklasse von Cl. Dann gilt:*

$$\frac{1}{h} \cdot \left(1 - \frac{h-1}{\Delta+1}\right) \leq \frac{\sharp\{\underline{e} \in [\![0, \Delta]\!]^k \mid [\prod_{i=1}^{k} P_i^{e_i}] = [A_j]\}}{(\Delta+1)^k} \leq \frac{1}{h} \cdot \left(1 + \frac{h-1}{\Delta+1}\right).$$

Beweis: Gemäß Korollar 5.3 wissen wir bzgl. $\Delta \in \mathcal{D}^+$ und einer Faktorbasis F_C aus Korollar 5.2: $\mathbb{Z}^k/\Gamma'_C \cong Cl$, und das Relationengitter Γ'_C hat Determinante h. Darauf können wir Lemma 4.1 in [AkL] anwenden und erhalten das Resultat. ■

Wir untersuchen die Aussage des Lemmas:

5.20 Korollar *In Schritt (1) von RELATION liefert die zufällige und gleichverteilte Wahl der Exponentenvektoren $\underline{e} \in [\![0, \Delta]\!]^k$ asymptotisch eine Gleichverteilung der Idealprodukte $\prod_{i=1}^{k} P_i^{e_i}$ auf die Klassen von Cl.*

Beweis: Wir gehen von einer zufällig und gleichverteilten Wahl der Exponentenvektoren $\underline{e}$ und einer beliebigen Idealklasse $[A_j]$ aus. Dann ist die Wahrscheinlichkeit $p([A_j])$, daß mittels der berechneten Idealprodukte $\prod_{i=1}^{k} P_i^{e_i}$ die Klasse $[A_j]$ erreicht wird, gleich dem in Lemma 5.19 angegebenen Quotienten. Also gilt

$$\frac{1}{h} \cdot \left(1 - \frac{h-1}{\Delta+1}\right) \leq p([A_j]) \leq \frac{1}{h} \cdot \left(1 + \frac{h-1}{\Delta+1}\right),$$

wobei wir für die Schranken

$$\frac{1}{h} \cdot \left(1 \pm \frac{h-1}{\Delta+1}\right) = \frac{1}{h} \pm \frac{h-1}{h} \cdot \frac{1}{\Delta+1}$$

herleiten. Insbesondere gilt $0 \leq (h-1)/h < 1$, woraus wir

$$\frac{1}{h} - \frac{1}{\Delta+1} \leq p([A_j]) \leq \frac{1}{h} + \frac{1}{\Delta+1},$$

folgern, so daß sich obere und untere Schranke um $2/(\Delta+1)$ unterscheiden, was für $\Delta \to \infty$gegen 0 konvergiert. Dies gilt für jede der h Klassen von Cl, woraus die Gleichverteilung folgt. ■

Schritt (1) von *RELATION* simuliert also eine zufällig und gleichverteilte Wahl einer Idealklasse von Cl für hinreichend großes Δ. Als nächstes beschäftigen wir uns mit der probabilistischen Wahl eines reduzierten Ideals in dieser Klasse. (vgl (2) in *RELATION*)

5.3.2 Die Wahl eines Ideals in einer Idealklasse

Wir suchen ein Werkzeug, das die probabilistische Wahl eines Ideals B innerhalb einer vorgegebenen Klasse simuliert. Insbesondere benötigen wir eine Aussage über die Wahrscheinlichkeitsverteilung. Diese brauchen wir in der anschließenden Analyse für die Wahrscheinlichkeit, daß das gewählte Ideal B über der Faktorbasis zerfällt. (vgl. Teilaufgabe (3)) Vor diesem Hintergrund erweisen sich reduzierte Ideale als geeignete Kandidaten. In diesem Zusammenhang ermöglicht uns das Konzept der Abstände und Wege aus (2.18), die Wahrscheinlichkeitsverteilung zu kontrollieren.

Wir leiten daraus eine vorläufige Fassung von *RELATION* her.

5.21 Algorithmus *RELATION* (vorläufige Fassung)

Eingabe: $\Delta \in \mathcal{D}^+$, $F_C = \{P_1, \ldots, P_k\}$ Faktorbasis und $k = \sharp F_C$
Ausgabe: $(v_1, \ldots, v_k, -\ln|\alpha|)$ erweiterte Relation, falls die Relationengenerierung erfolgreich ist.

<table>
<tr><td colspan="2">/* Wahl einer Idealklasse */
Wähle zufällig und gleichverteilt einen Exponentenvektor, d.h.
$\underline{e} \in_R [\![0, \Delta]\!]^k$</td><td>(1)</td></tr>
<tr><td colspan="2">/* Wahl eines reduzierten Ideals in dieser Idealklasse */
(a) Wähle zufällig und gleichverteilt eine Zahl y mit
$y \in_R [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z}$.
(b) Bestimme ein reduziertes Ideal B mit
$B = (\alpha\mathcal{O}_\Delta) \prod_{i=1}^k P_i^{e_i}$
und
$\ln|\alpha| \sim y$.</td><td>(2)</td></tr>
<tr><td colspan="2">IF B zerfällt über F_C</td><td>(3)</td></tr>
<tr><td rowspan="2">THEN</td><td>$B \leftarrow \prod_{i=1}^k P_i^{z_i}$</td><td>(4)</td></tr>
<tr><td>$(v_1, \ldots, v_k, -\ln|\alpha|) \leftarrow (e_1 - z_1, \ldots, e_k - z_k, -\ln|\alpha|)$</td><td>(5)</td></tr>
</table>

Wir wenden uns der Realisierung von Teilaufgabe (2) zu. Zuerst skizzieren wir die Vorgehensweise. In diesem Zusammenhang wird die Bedeutung reduzierter Ideale für die Relationengenerierung deutlich.

Die Grundidee zur Berechnung eines Ideals B

Wir übernehmen das Konzept der Abstände und Wege reduzierter Ideale aus Kapitel 2. Seien ein reduziertes Ideal B_0 und eine Zahl $y_1 \in \mathbb{Q}$ gegeben. Dann können wir ein Verfahren entwickeln, das von B_0 aus nach Zurücklegen eines Weges der ungefähren Länge $|y_1|$ ein weiteres reduziertes Ideal B berechnet, das zu B_0 äquivalent ist, d.h.

$$B = (\alpha_1\mathcal{O}_\Delta)B_0 \qquad \text{mit } \ln|\alpha_1| \sim y_1. \tag{5.14}$$

Für die Realisierung von Teilaufgabe (2) bietet sich daher an: Wir berechnen zuerst ein zu $\prod_{i=1}^{k} P_i^{e_i}$ äquivalentes reduziertes Ideal B_0 und α_0 mit

$$B_0 = (\alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^{k} P_i^{e_i}. \tag{5.15}$$

Weil B_0 reduziert ist, können wir das eben beschriebene Verfahren auf B_0 anwenden und erhalten ein zu $\prod_{i=1}^{k} P_i^{e_i}$ äquivalentes, reduziertes Ideal B,

$$\begin{aligned} B &= (\alpha_1 \mathcal{O}_\Delta) B_0 \\ &= \underbrace{(\alpha_0 \alpha_1 \mathcal{O}_\Delta)}_{=:\, \alpha \mathcal{O}_\Delta} \prod_{i=1}^{k} P_i^{e_i} \end{aligned}$$

mit $\alpha = \alpha_0 \cdot \alpha_1$. Wollen wir y erreichen, streben wir

$$y \sim \ln|\alpha| = \ln|\alpha_0| + \ln|\alpha_1|$$

an. Wir berücksichtigen also $\ln|\alpha_0|$ aus der Reduktion in (5.15) in y. Wollen wir dann y erreichen, wählen wir y_1 in (5.14) gemäß

$$y_1 \sim \ln|\alpha_1| \sim y - \ln|\alpha_0|. \tag{5.16}$$

Wir wenden uns zunächst dem Problem der Annäherung an y_1 von B_0 aus zu, um anschließend die Wahl von B in algorithmischer Form anzugeben.

Annähern an y_1

Wir nutzen die sogenannte Infrastrukur reellquadratischer Ordnungen aus. (vgl. (2.26)) Da diese sich lediglich auf die Multiplikation reduzierter Hauptideale mit beliebigen reduzierten Idealen bezieht, gehen wir wie folgt vor: Zuerst bestimmen wir ein reduziertes Hauptideal H, das von $\mathcal{O}_\Delta$ etwa y_1 entfernt ist. Dies geschieht auf Grundlage der Infrastruktur:

$$H = \kappa \mathcal{O}_\Delta$$

ist reduziert mit $\ln|\kappa| \sim y_1$. Anschließend multiplizieren wir das reduzierte Ideal B_0 aus (5.15) mit H und erhalten ein zu B_0 äquivalentes Ideal B_1,

$$B_1 = (\kappa \mathcal{O}_\Delta) B_0 = (\kappa \alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^{k} P_i^{e_i},$$

wobei B_1 nicht notwendig reduziert ist. Erneutes Ausnutzen der Infrastruktur liefert ein reduziertes Ideal B, das von y nicht „weit entfernt“ ist,

$$B = \underbrace{\left(\frac{\Theta}{g} \kappa \alpha_0 \mathcal{O}_\Delta \right)}_{=\, \alpha \mathcal{O}_\Delta} \prod_{i=1}^{k} P_i^{e_i} \tag{5.17}$$

mit $\ln|\alpha| = \ln|\Theta/g| + \ln|\kappa| + \ln|\alpha_0| \sim \ln|\Theta/g| + y_1 + y - y_1 = \ln|\Theta/g| + y$ wegen (5.16). Danach nehmen wir noch ein paar Vorwärts- oder Rückwärtsschritte zur besseren Annäherung an y vor.

Wir fassen dieses Konzept zur Realisierung von Teilaufgabe (2b) in Algorithmus *REACH* zusammen. Danach untersuchen wir die einzelnen Schritte detailliert:

5.22 Algorithmus *REACH* (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$, $F_C = \{P_1, \ldots, P_k\}$ Faktorbasis, $k = \sharp F_C$, $\underline{e} \in [\![0, \Delta]\!]^k$ Exponentenvektor, $y \in \mathbb{Q}$

Ausgabe: B, zu $\prod_{i=1}^k P_i^{e_i}$ äquivalentes reduziertes Ideal nahe an y, $\hat{y}$ sein approximierter Standort der Präzision 3 und $\alpha_0 \circ \kappa \circ \gamma = \alpha$ in komprimierter Darstellung

/* Berechne ein zu $\prod_{i=1}^k P_i^{e_i}$ äquivalentes reduziertes Ideal B_0 mit $B_0 = (\alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^k P_i^{e_i}$. */ $(B_0, \alpha_0, y_0) \leftarrow \mathit{POTPROD}\ (\Delta, \underline{e}, F_C, k)$ /* y_0 ist eine Approximation von $\ln \|\alpha_0\|$ der Präzision 5. */	(1)
$y_1 \leftarrow y - y_0$ /* verbleibender Weg */	(2)
/* Bestimme ein reduziertes Hauptideal H nahe an y_1. */ $q \leftarrow \max\{q \in \frac{1}{3}\mathbb{Z} \mid q \leq y_1\}$ $(H, \kappa, \hat{h}) \leftarrow \mathit{HREACH}\ (\Delta, q)$	(3)
/* Multipliziere B_0 mit H, mache es primitiv und reduziere. */ $B \leftarrow (\Theta / g\mathcal{O}_\Delta)\ B_0 H$	(4)
/* Führe eine Abschlußkorrektur durch. */ $\gamma \leftarrow \Theta / g$ $(B, \hat{x}, \gamma) \leftarrow \mathit{CORRECT}\ (\Delta, B, y, y_0, \hat{h}, \gamma)$	(5)
/* Wähle B „gestreut“ aus. */ $B \in_R \{B_{--}, B_{-}, B, B_{+}, B_{++}, B_{+++}\} := M_y$, Setze γ entsprechend, $\hat{x} \leftarrow \mathit{appr}(\ln \|\gamma\|, 5)$.	(6)
/* Es gelten $\alpha = \alpha_0 \circ \kappa \circ \gamma$, und $y_0 + \hat{h} + \hat{x}$ ist der approximierte Standort von B der Präzision 3. */ $\hat{y} \leftarrow y_0 + \hat{h} + \hat{x}$	(7)

Den Begriff der komprimierten Darstellung werden wir bei der nachfolgenden Ausarbeitung erklären. Ferner wird dort deutlich, daß die „Streuung“ in (6) aus Gründen der Verteilung reduzierter Ideale in den Klassen erfolgt. Für die Approximationen betrachten wir den totalen Fehler bzgl. einer Präzision n gemäß Definition 3.20.

Die Berechnung von B_0 mit *POTPROD*

Berechnen des Potenzproduktes $\prod_{i=1}^k P_i^{e_i}$ und anschließendes Reduzieren liefern bereits große Längen der Zwischenergebnisse. Für die Norm des Potenzproduktes gilt

$$N\Big(\prod_{i=1}^{k} P_i^{e_i}\Big) = \prod_{i=1}^{k} p_i^{e_i} \leq \prod_{i=1}^{k} p_i^{\Delta},$$

wobei $N(P_i) = p_i$ für die invertierbaren Ideale von F_C gilt. Daraus folgern wir, daß bei Reduktion die Anzahl der Iterationen exponentiell in $\log \Delta$ werden kann. (vgl. Satz 2.57)

Deshalb reduzieren wir in der Regel nach jeder Multiplikation; d.h. wir machen zuerst jedes berechnete Produkt primitiv (vgl. *MUL*), indem wir durch $g\mathcal{O}_\Delta$ teilen. Danach reduzieren wir dieses primitive Ideal, wodurch ein Faktor $\Theta\mathcal{O}_\Delta$ durch die damit verbundenen Vorwärtsschritte entsteht. Zu Beginn arbeiten wir alle Faktoren $P_i^{e_i}$ mit dieser Strategie separat ab. Wir erhalten also reduzierte Ideale $\wp_i$ der Form

$$\wp_i = (\rho_i\mathcal{O}_\Delta)P_i^{e_i}, \qquad 1 \le i \le k. \tag{5.18}$$

Da wir die Methode des binären Shiftens zur Berechnung der Potenzen $P_i^{e_i}$ anwenden, besteht ρ_i aus Potenzen der jeweiligen Θ/g, wie wir Algorithmus *POT* in 5.26 entnehmen. Dann multiplizieren wir die $\wp_i$ mit der gleichen Methode, d.h. wir erhalten

$$(\Theta_{(i)}/g_i\mathcal{O}_\Delta)\wp_i\wp_{i+1} = (\Theta_{(i)}/g_i\cdot\rho_i\cdot\rho_{i+1}\mathcal{O}_\Delta)P_i^{e_i}P_i^{e_{i+1}}$$

und fahren iterativ fort, bis alle $\wp_i$ verarbeitet sind. Schließlich haben wir ein zu $\prod_{i=1}^k P_i^{e_i}$ äquivalentes reduziertes Ideal B_0. (vgl. (5.15)) Den zugehörigen Faktor α_0 erhalten wir, indem wir das Produkt aus den Faktoren ρ_i sowie $\Theta_{(i)}/g_i$, $1 \le i \le k$, berechnen. Auf dieser Idee beruht der nachfolgende Algorithmus *POTPROD* .

Zuvor stellen wir einige Überlegungen für die Darstellung von α_0 an: Die bereits erwähnten Faktoren Θ/g sowie $\Theta_{(i)/g_i}$ lassen sich mit Hilfe von Proposition 2.71 beschreiben: Bezeichne $\mathbb{Z}a_0 + \mathbb{Z}(b_0+\sqrt{\Delta})/2$ die Standarddarstellung des zu reduzierenden Ideals und n die Anzahl der Iterationen von *REDUCTION* , dann gilt für Θ/g:

$$\begin{aligned}\frac{\Theta}{g} &= \frac{2a_nv_{n-2}+v_{n-1}b_0+v_{n-1}\sqrt{\Delta}}{2ga_0}\\ &=: \frac{V_n+V_n'\sqrt{\Delta}}{2ga_0}.\end{aligned} \tag{5.19}$$

Analoges gilt für $\Theta_{(i)}/g_i$. Dann lassen sich mit Lemma 2.73 und *MUL* aus 2.36 Zähler und Nenner durch

$$g_i, g_j \le \Delta, \qquad |V_n| < a_0 \quad \text{und} \quad |V_n'| < a_0/\sqrt{\Delta} \tag{5.20}$$

beschränken. Wegen $a_0 < \Delta^2$ aus *MUL* in 2.36 läßt sich die Länge der auftretenden Faktoren polynomiell in $\log\Delta$ beschränken. Da unter anderem ρ_i aus Potenzen der Θ/g besteht, ist es vom Aspekt der Länge der Darstellung her günstiger, den Exponenten und die Darstellung von Θ/g bzw. $\Theta_{(i)}/g_i$ zugrundezulegen als die Potenz auszurechnen. Deshalb werden wir in unseren Algorithmen diese Faktoren nicht ausrechnen, sondern sie mit sogenannten Faktor-Exponenten-Listen identifizieren, die wir als *komprimierte Darstellungen* bezeichnen. Wir betrachten α_0 als Menge von komprimierten Darstellungen, d.h. die komprimierten Darstellungen bilden Faktoren von α_0. Dann haben wir eine Darstellung von α_0, die auch eine effiziente Berechnung einer Approximation von $\ln|\alpha_0|$ ermöglicht.

5.23 Bemerkung Für unsere Algorithmen vereinbaren wir folgende Konvention: Hinsichtlich der Listenschreibweise komprimierter Darstellungen betrachten wir die Θ/g bzw. $\Theta_{(i)}/g_i$ gemäß (5.19) als (g, a_0, V_n, V_n') mit Exponent 1, wobei wir V_n, V_n' aus *REDUCTION* für Θ erhalten. Multiplizieren wir zwei Elemente α_0, α_1, gegeben in komprimierter Darstellung, erhöhen wir die Exponenten gemeinsamer Faktoren entsprechend, die übrigen Faktoren werden inklusive ihrer Exponenten dieser Liste hinzugefügt. (vgl. Konkatenation $\circ$) Zur Hervorhebung dieses Zusammenhangs schreiben wir auch $\alpha_0 \circ \alpha_1$.

Wir geben die bereits erwähnten Algorithmen *POTPROD* und *POT* an, wodurch der Aufbau einer komprimierten Darstellung von α_0 verdeutlicht wird.

5.24 Algorithmus *POTPROD* (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$, $\underline{e} \in [\![0, \Delta]\!]^k$, $F_C = \{P_1, \ldots, P_k\}$ Faktorbasis und $k = \sharp F_C$

Ausgabe: B_0, zu $\prod_{i=1}^{k} P_i^{e_i}$ äquivalentes reduziertes Ideal, α_0 als Menge komprimierter Darstellungen mit $B_0 = (\alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^{k} P_i^{e_i}$ und $y_0 \in \mathbb{Q}$ eine Approximation von $\ln |\alpha_0|$ der Präzision 5

/* Initialisierung */ $l \leftarrow \lceil \log_3 k \rceil$, $\alpha_0 \leftarrow$ komprimierte Darstellung für 1	(1)
/* Berechne $\wp_i$ und ρ_i gemäß (5.18) */	(2)
FOR $1 \leq i \leq k$	(3)
/* Berechne $\wp_i = (\rho_i \mathcal{O}_\Delta) P_i^{e_i}$ und eine Approximation $\hat{c}_i$ von ρ_i der Präzision $5 + l + \lceil \log k \rceil$. */ $(\wp_i, \rho_i, \hat{c}_i) \leftarrow POT\ (\Delta, P_i, e_i, 5 + l + \lceil \log k \rceil)$	(4)
/* Beweis-Invariante: $\alpha_0 \leftarrow \prod_{i=1}^{k} \rho_i$ */	(5)
/* Zusammenfassen der $\wp_i$. */ $\rho'_1 \leftarrow \ldots \leftarrow \rho'_{\lceil k/3 \rceil} \leftarrow$ komprimierte Darstellung von 1	(6)
WHILE $k > 1$	(7)
$\wp_{k+1} \leftarrow \wp_{k+2} \leftarrow \mathcal{O}_\Delta$, $\hat{c}_{k+1} \leftarrow \hat{c}_{k+2} \leftarrow 0$ /* wegen (10) */	(8)
FOR $i \leftarrow 1$ *TO* k	(9)
/* Berechne $\wp_i \wp_{i+1} \wp_{i+2}$, mache es primitiv und reduziere. */ $\wp_{(i+2)/3} \leftarrow (\Theta_{(i+2)/3} / g_{(i+2)/3} \mathcal{O}_\Delta) \wp_i \wp_{i+1} \wp_{i+2}$	(10)
$\rho'_{(i+2)/3} \leftarrow \rho'_{(i+2)/3} \circ$ komprimierte Darst. von $\Theta_{(i+2)/3} / g_{(i+2)/3}$	(11)
/* Beweis-Invariante: $\alpha_0 \leftarrow \alpha_0 \circ \Theta_{(i+2)/3} / g_{(i+2)/3}$. */	(12)
$h_{(i+2)/3} \leftarrow appr(\ln \lvert \Theta_{(i+2)/3} / g_{(i+2)/3} \rvert, 5 + l + 1 + \lceil \log(k/3) \rceil)$	(13)
$\hat{c}_{(i+2)/3} \leftarrow \hat{c}_i + \hat{c}_{i+1} + \hat{c}_{i+2} + h_{(i+2)/3}$	(14)
$i \leftarrow i + 3$	(15)
$k \leftarrow \lceil k/3 \rceil$, $l \leftarrow l - 1$	(16)
$B_0 \leftarrow \wp_1$, $y_0 \leftarrow \hat{c}_1$	(17)

5.25 Bemerkung Am Ende des Algorithmus entspricht α_0 dem Produkt der komprimierten Darstellungen der $\rho_1, \ldots, \rho_k, \rho'_1, \ldots, \rho'_{k/3}$, d.h. wir haben gemäß Bemerkung 5.23 $\alpha_0 = \rho_1 \circ \ldots \circ \rho_k \circ \rho'_1 \circ \ldots \circ \rho'_{k/3}$.

Wir liefern die noch ausstehende Berechnung von $\wp_i$ und ρ_i in kompakter Darstellung mit POT, woraus wir die genaue Gestalt der ρ_i, ρ_i' und somit von α_0 ableiten können.

5.26 Algorithmus *POT* (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$, Ideal $P \in F_C$, $e \in [\![0, \Delta]\!]$ Exponent, $n \in \mathbb{N}_0$

Ausgabe: $\wp$, zu P^e äquivalentes reduziertes Ideal, ρ in komprimierter Darstellung mit $\wp = (\rho\mathcal{O}_\Delta)P^e$ und $\hat{c} \in \mathbb{Q}$ eine Approximation von $\ln|\rho|$ der Präzision n

/* Initialisierungen */ $\wp \leftarrow \mathcal{O}_\Delta$, $\rho \leftarrow$ komprimierte Darstellung von 1, $\hat{c} \leftarrow 0$ $A \leftarrow (\Theta\mathcal{O}_\Delta)P$ /* Reduziere P. */ $\gamma \leftarrow$ komprimierte Darstellung von Θ /* $A = (\gamma\mathcal{O}_\Delta)P$ */ $m \leftarrow 2\lfloor \log e \rfloor$ $\hat{c}(\gamma) \leftarrow appr(\ln|\Theta|, 2(m+2)+n)$	(1)
IF e ungerade	(2)
THEN /* Berechne $\wp A$, mache es primitiv und reduziere. */ $\wp \leftarrow (\Theta'/g'\mathcal{O}_\Delta)\wp A$ /* = A*/	(3)
$\rho \leftarrow \rho \circ \gamma \circ$ komprimierte Darst. von (Θ'/g') /* = γ */	(4)
$\hat{c} \leftarrow \hat{c} + \hat{c}(\gamma) + appr(\ln|\Theta'/g'|, 2(m+1)+n)$	(5)
$e \leftarrow \lfloor e/2 \rfloor$, $m \leftarrow m-1$	(6)
WHILE $e > 0$ /* binäres Shiften */	(7)
/* Berechne A^2, mache es primitiv und reduziere. */ $A \leftarrow (\Theta''/g''\mathcal{O}_\Delta)A^2$	(8)
$\gamma \leftarrow \gamma \circ \gamma \circ$ komprimierte Darstellung von (Θ''/g'')	(9)
$\hat{c}(\gamma) \leftarrow 2\hat{c}(\gamma) + appr(\ln|\Theta''/g''|, 2(m+2)+n)$	(10)
IF e ungerade	(11)
THEN /* Berechne $\wp A$, mache es primitiv und reduziere. */ $\wp \leftarrow (\Theta'/g'\mathcal{O}_\Delta)\wp A$	(12)
$\rho \leftarrow \rho \circ \gamma \circ$ komprimierte Darstellung von (Θ'/g')	(13)
$\hat{c} \leftarrow \hat{c} + \hat{c}(\gamma) + appr(\ln|\Theta'/g'|, 2(m+1)+n)$	(14)
$e \leftarrow \lfloor e/2 \rfloor$, $m \leftarrow m-1$	(15)

Wir untersuchen POT auf Korrektheit und Laufzeit, in deren Verlauf sich die Größe der Präzision und der Aufbau der ρ_i klären. Wie in der Originalversion des binären Shiftens (vgl. [Dü], Algorithmus 2.15) führen wir in POT $\lfloor \log e \rfloor$ Iterationen und maximal $2\lfloor \log e \rfloor + 1$ Multiplikationen aus. Bzgl. der j-ten Iteration bezeichnen wir γ mit γ_j sowie $\hat{c}$ mit $\hat{c}_j$ und erhalten für die Präzision von $\hat{c}_j$ und $\hat{c}(\gamma_j)$:

5.27 Lemma *In jeder der $\lfloor \log e \rfloor$ Iterationen von POT gilt: $\hat{c}(\gamma_j)$ ist eine Approximation von $\ln|\gamma_j|$ der Präzision $2(\lfloor \log e \rfloor - j + 1) + n$ und $\hat{c}_j$ eine Approximation von $\ln|\rho_j|$ der Präzision $2(\lfloor \log e \rfloor - j) + n$.*

Beweis: Für $j = 0$ erhalten wir die Behauptungen direkt aus der Initialisierung in (1): $\ln|\rho_0| = 0 = \hat{c}_0$ und $\hat{c}(\gamma_0) = appr(\ln|\gamma_0 = \Theta|, 2(\lfloor \log e \rfloor + 2) + n)$. Für $j \geq 1$ leiten wir für γ_j und $\hat{c}(\gamma_j)$ her, wobei sich m_j zu $\lfloor \log e \rfloor - j$ ergibt:

$$
\begin{aligned}
|\ln|\gamma_j| - \hat{c}(\gamma_j)| &= \Big|\ln|\gamma_{j-1}^2 \cdot (\Theta''_{(j)}/g''_j)| \\
&\quad -(2\hat{c}(\gamma_{j-1}) + appr(\ln|\Theta''_{(j)}/g''_j|, 2(\lfloor \log e \rfloor - j + 2) + n))\Big| \\
&\leq 2\,|\ln|\gamma_{j-1}| - \hat{c}(\gamma_{j-1})| + \\
&\quad \Big|\ln|\Theta''_{(j)}/g''_j| - appr(\ln|\Theta''_{(j)}/g''_j|, 2(\lfloor \log e \rfloor - j + 2) + n)\Big| \\
&< 3 \cdot 2^{-2(\lfloor \log e \rfloor - j + 2) - n} \\
&< 2^{-2(\lfloor \log e \rfloor - j + 1) - n}.
\end{aligned}
$$

Analog erhalten wir eine Abschätzung für $\hat{c}_j$:

$$
\begin{aligned}
|\ln|\rho_j| - \hat{c}_j| &= \Big|\ln|\rho_{j-1} \cdot \gamma_j \cdot (\Theta'_{(j)}/g'_j)| \\
&\quad -(\hat{c}_{j-1} + \hat{c}(\gamma_j) + appr(\ln|\Theta'_{(j)}/g'_j|, 2(\lfloor \log e \rfloor - j + 1) + n))\Big| \\
&\leq |\ln|\rho_{j-1}| - \hat{c}_{j-1}| + |\ln|\gamma_j| - \hat{c}(\gamma_j)| + \\
&\quad |\ln|\Theta'_{(j)}/g'_j| - appr(\ln|\Theta'_{(j)}/g'_{(j)}|, 2(\lfloor \log e \rfloor - j + 1) + n)| \\
&< 3 \cdot 2^{-2(\lfloor \log e \rfloor - j + 1) - n} \\
&< 2^{-2(\lfloor \log e \rfloor - j) - n}.
\end{aligned}
$$

■

Dann können wir zeigen:

5.28 Lemma *Bei Eingabe von $\Delta \in \mathcal{D}^+$, eines Ideals $P \in F_C$, eines Exponenten $e \in \mathbb{N}_0$ sowie $n \in \mathbb{N}_0$ berechnet POT ein reduziertes, zu P^e äquivalentes Ideal $\wp$, ρ in komprimierter Darstellung mit $\wp = (\rho\mathcal{O}_\Delta)P^e$ und eine Approximation $\hat{c}$ von ρ der Präzision n.*

Beweis: Die Äquivalenz von P^e und $\wp$ erhalten wir analog zu [Dü], indem wir in der Methode des binären Shiftens Gleichheit durch Äquivalenz ersetzen.
Die Korrektheit von ρ ergibt sich analog, denn es gelten mit (1) und (8) von *POT* in jeder Iteration: $0 \leq j < \lfloor \log e \rfloor$

$$
\begin{aligned}
A_{j+1} &= (\Theta''_{(j+1)}/g''_{j+1}\mathcal{O}_\Delta)A_j^2 \\
&= (\underbrace{\Theta''_{(j+1)}/g''_{j+1} \cdot \gamma_j^2}_{=\gamma_{j+1}}\mathcal{O}_\Delta)P^{2^{j+1}}
\end{aligned}
\tag{5.21}
$$

sowie mit (12) von *POT* :

$$
\begin{aligned}
\wp_{j+1} &= (\Theta'_{(j+1)}/g'_{j+1}\mathcal{O}_\Delta)\wp_j A_{j+1} \\
&= (\underbrace{\Theta'_{(j+1)}/g'_{j+1} \cdot \rho_j \cdot \gamma_{j+1}}_{=\rho_{j+1}}\mathcal{O}_\Delta)\wp_{j-1}P^{n_j + 2^{j+1}}
\end{aligned}
\tag{5.22}
$$

mit $n_j \in \mathbb{N}_0$. Mit Lemma 5.27 folgt Präzision n für die Approximation von $\ln|\rho = \rho_{j=\lfloor\log e\rfloor}|$, da wir $\lfloor\log e\rfloor$ Iterationen der while-Schleife ausführen. ∎

Diese Resultate liefern uns den Aufbau der ρ_i in (5.22):

5.29 Korollar *Für die ρ_i, $1 \le i \le k$, in POTPROD gilt:*

$$\rho_i = \prod_{j=0}^{\lceil\log e_i\rceil} \left(\frac{\Theta'_{(j)}}{g'_j}\right)^{z'_j} \cdot \prod_{j=1}^{\lfloor\log e_i\rfloor} \left(\frac{\Theta''_{(j)}}{g''_j}\right)^{z''_j}$$

mit ganzzahligen Exponenten z'_j, z''_j, die $0 \le z'_j, z''_j \le e_i$ genügen. Insbesondere entsteht jeder Faktor $\Theta'_{(j)}$ bzw. $\Theta''_{(j)}$ aus maximal $O(\log\Delta)$ vielen Vorwärtsschritten.

Nun ermitteln wir die Laufzeit von *POT* bezüglich der Anwendung in *POTPROD* :

5.30 Lemma *Der Algorithmus POT benötigt bei Eingabe von $\Delta \in \mathcal{D}^+$, eines Ideals $P \in F_C$ sowie eines Exponenten $e \in [\![0, \Delta]\!]$ und $n \in \mathbb{N}_0$ mit $n = O(\log\Delta)$ polynomielle Laufzeit, asymptotisch beträgt sie $L_\Delta[0]$.*

Beweis: Wir starten mit einer Reduktion von $P \in F_C$, die wegen $C < \sqrt{\Delta}$ aus (5.13) in Polynomzeit gemäß Satz 2.57 und Lemma 2.73 erfolgt. Wir führen insgesamt maximal $2\lfloor\log e\rfloor + 1 = O(\log\Delta)$ Multiplikationen reduzierter Ideale mit anschließender Reduktion inklusive der Bestimmung von Θ''/g'', Θ'/g' aus, was jeweils in Polynomzeit wegen Proposition 2.74 geschieht.
Die erforderlichen Präzisionen in den jeweiligen Iterationen genügen $2(m+2)+n = O(\log\Delta)$, so daß die Approximationen mit Bemerkung 5.11 und [Br], Theorem 9.1 jeweils Polynomzeit brauchen, von denen wir insgesamt $2\lfloor\log\Delta\rfloor + 1 = O(\log\Delta)$ viele ermitteln.
Die Erstellung der komprimierten Darstellung von ρ braucht wegen Korollar 5.29 Polynomzeit. ∎

Damit haben wir alle Vorbereitungen zur Analyse von *POTPROD* getroffen. Bzgl. der j-ten Iteration bezeichnen wir α_0 mit $\alpha_{0,j}$ und l mit l_j, k mit k_j.

5.31 Lemma *Nach jeder Iteration $1 \le j \le \lceil\log_3 k\rceil$, der while-Schleife von POTPROD gilt: $\sum_{i=1}^{k_j} \hat{c}_{i,j}$ ist eine Approximation von $\ln|\alpha_{0,j}|$ der Präzision $5 + l_{j-1}$.*

Beweis: Für $j = 0$, d.h. vor Aufruf der while-Schleife, erhalten wir gemäß (4) und (5) von *POTPROD* : $\alpha_{0,0}$ ist das Produkt aller ρ_i und mit Lemma 5.27 gilt:

$$\begin{aligned}\left|\ln|\alpha_{0,0} = \prod_{i=1}^{k}\rho_i| - \sum_{i=1}^{k}\hat{c}_{i,0}\right| &\le \sum_{i=1}^{k}|\ln|\rho_i| - \hat{c}_{i,0}| \\ &< k \cdot 2^{-5-l_0-\lceil\log k\rceil} \\ &\le 2^{-5-l_0}.\end{aligned}$$

Für $j \geq 1$ leiten wir nach Ausführung der for-Schleife und (16) her: $\alpha_{0,j} = \alpha_{0,j-1} \cdot \prod_{i=1}^{k_j}(\Theta_{(i)/g_i})$. Daraus erhalten wir mit (14)

$$\begin{aligned}
\left| \ln|\alpha_{0,j}| - \sum_{i=1}^{k_j} \hat{c}_{i,j} \right| &\leq \left| \ln|\alpha_{0,j-1}| - \sum_{i=1}^{k_j} (\hat{c}_{3i,j-1} + \hat{c}_{3i+1,j-1} + \hat{c}_{3i+2,j-1}) \right| \\
&\quad + \sum_{i=1}^{k_j} |\ln(\Theta_{(i)/g_i}) - h_i| \\
&< 2^{-5-l_{j-2}} + k_j \cdot 2^{-5-l_{j-1}-1-\lceil \log k_j \rceil} \\
&\leq 2 \cdot 2^{-5-l_{j-1}-1} \\
&= 2^{-5-l_{j-1}}.
\end{aligned}$$

■

Dann können wir zeigen:

5.32 Lemma *Bei Eingabe von $\Delta \in \mathcal{D}^+$, eines Exponentenvektors $\underline{e} \in [\![0, \Delta]\!]^k$, einer Faktorbasis F_C sowie ihrer Ordnung k berechnet POTPROD ein reduziertes, zu $\prod_{i=1}^{k} P_i^{e_i}$ äquivalentes Ideal B_0 sowie α_0 als Menge komprimierter Darstellungen mit $B_0 = (\alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^{k} P_i^{e_i}$ und eine Approximation y_0 von $\ln|\alpha_0|$ der Präzision 5.*

Beweis: Wir zeigen: Nach jeder der $\lceil \log_3 k \rceil$ for-Schleifen gilt für $0 \leq j \leq \lceil \log_3 k \rceil$

$$B_{0,j} := \prod_{i=1}^{k_j} \wp_{i,j} = (\alpha_{0,j} \mathcal{O}_\Delta) \prod_{i=1}^{k} P_i^{e_i}, \tag{5.23}$$

woraus die Behauptung für $B_0 := B_{0,\lceil \log_3 k \rceil}$ und $\alpha_0 := \alpha_{0,\lceil \log_3 k \rceil}$ folgt. Insbesondere ist B_0 laut Konstruktion (vgl. (10)) reduziert: Für $j = 0$ folgt (5.23) direkt wegen $\wp_{i,0} = (\rho_i \mathcal{O}_\Delta) P_i^{e_i}$ aus Lemma 5.28. Für $j \geq 1$ leiten wir her:

$$\begin{aligned}
B_{0,j} &= \prod_{i=1}^{k_j} \wp_{i,j} = \prod_{i=1}^{k_j} \Big(\wp_{3i,j-1} \wp_{3i+1,j-1} \wp_{3i+2,j-1} (\Theta_{(i)}/g_i \mathcal{O}_\Delta) \Big) \\
&= B_{0,j-1} \prod_{i=1}^{k_j} (\Theta_{(i)}/g_i \mathcal{O}_\Delta) \\
&= \underbrace{\Big(\alpha_{0,j-1} \cdot \prod_{i=1}^{k_j} (\Theta_{(i)}/g_i) \Big)}_{= \alpha_{0,j}} \mathcal{O}_\Delta \prod_{i=1}^{k} P_i^{e_i}.
\end{aligned}$$

Bzgl. der Approximation y_0 in (17) wissen wir: $y_0 := \hat{c}_{1,\lceil \log_3 k \rceil}$ ist eine Approximation von α_0 der Präzision 5 wegen Lemma 5.31. ■

Anwenden von (5.23) und Korollar 5.29 impliziert:

5.33 Korollar *Für α_0 gilt nach Beenden von POTPROD :*

$$\alpha_0 = \prod_{i=1}^{k} \rho_i \cdot \prod_{j=1}^{\lceil \log_3 k \rceil} \prod_{i=1}^{k_j} (\Theta_{(i)}/g_i).$$

α_0 besteht aus $k \cdot O(\log e_i) + O(k)$ Faktoren der Form Θ/g, die beim Primitivmachen und Reduzieren entstehen, wozu wir jeweils maximal $O(\log \Delta)$ Vorwärtsschritte unternehmen.

Dann leiten wir für die Laufzeit von *POTPROD* her:

5.34 Lemma *Der deterministische Algorithmus POTPROD benötigt bei Eingabe von $\Delta \in \mathcal{D}^+$, eines Exponentenvektors $\underline{e} \in [\![0, \Delta]\!]^k$, einer Faktorbasis sowie deren Ordnung k Laufzeit $L_\Delta[c]$.*

Beweis: Die aufwendigsten Aufgaben bilden die Schleifen.
In der for-Schleife in (3) benötigt jeder der k Aufrufe von *POT* gemäß Lemma 5.30 polynomielle Laufzeit wegen $e_i \leq \sqrt{\Delta}$ und Präzision $O(\log \Delta)$, so daß wir insgesamt Zeit $L_\Delta[c]$ brauchen.
Vor Betreten der while-Schleife brauchen wir zur Initialisierung der $\rho'_1, \ldots, \rho'_{\lceil k/3 \rceil}$ Zeit $L_\Delta[c]$. Die Laufzeit der for-Schleifen in (9) - (15) entspricht im wesentlichen der Laufzeit der Iterationen der while-Schleife. In jeder Iteration, $1 \leq j \leq \lceil \log_3 k \rceil$, führen wir aus: $2k_j$ Multiplikationen, k_j Reduktionen, k_j komprimierte Darstellungen und k_j Approximationen sowie $3k_j$ Additionen von Approximationen. Daraus erhalten wir jeweils für die Anzahl dieser Operationen in allen for-Schleifen

$$\sum_{j=1}^{\lceil \log_3 k \rceil} k_j = O(k/3 + k/3^2 + \ldots) = O(k). \tag{5.24}$$

Der Multiplikation liegen jeweils Ideale zugrunde, die für *MUL* Eingabegrößen $< \Delta$ haben, so daß wir Polynomzeit benötigen. (vgl. Algorithmus 2.36) Bzgl. der anschließenden Reduktion mit *REDUCTION* liegen daher Ideale vor, deren Größen durch $\Delta^{3/2}$ beschränkt sind, so daß wir ebenfalls Polynomzeit brauchen wie auch für die darauf aufbauenden Approximationen der Präzision $O(\log \Delta)$. (vgl. Lemma 2.73 und Bemerkung 5.11, [Br]) Insgesamt benötigen also alle Multiplikationen, Reduktionen und Approximationen der while-Schleife Zeit $L_\Delta[c]$. (vgl. (5.24))
Zu klären bleiben noch die jeweiligen Bestimmungen der komprimierten Darstellungen von ρ' sowie die Berechnungen der $\hat{c}_{(i+2)/3}$. Die Größe der $\hat{c}_{(i+2)/3}$ läßt sich mit Hilfe von $\ln|\alpha_0|$ und Korollar 5.33 durch $2k \cdot O((\log \Delta)^2)$ beschränken, so daß ihre Länge $O(\log \Delta)$ wegen (5.13) ist. Die komprimierten Darstellungen $\rho'_1, \ldots, \rho'_{\lceil k/3 \rceil}$ entstehen aus jeweils maximal $l = O(\log \Delta)$ Einträgen, wobei stets Listen der Länge $O(\log \Delta)$ hinzugefügt werden. (vgl. Bemerkung 5.19) Dann erfordert die Erstellung aller ρ' Zeit $L_\Delta[c]$. ∎

Kehren wir zu Algorithmus *REACH* zurück, haben wir nun B_0, α_0 und y_0 gemäß (5.15) berechnet. Als nächstes steht in (2) von *REACH* die Berechnung von y_1 aus $y - y_0$ an.

Die Berechnung von y_1

Für die Abschätzung der Laufzeit leiten wir eine Aussage über die Größenordnung von y_0 her. Wir ziehen hierzu $\ln|\alpha_0|$ heran, da y_0 wegen Lemma 5.32 eine Approximation von $\ln|\alpha_0|$ der Präzision 5 ist.

5.35 Lemma *Für die in (1) von REACH berechnete Approximation y_0 gilt $|y_0| = O(k \cdot \Delta \cdot (\log\Delta)^2) = O(\Delta^{3/2} \cdot (\log\Delta)^2)$.*

Beweis: Mit Lemma 5.32 gilt $y_0 = appr(\ln|\alpha_0|, 5)$, d.h.

$$|y_0 - \ln|\alpha_0|| < 2^{-5} \implies |y_0| \le |\ln|\alpha_0|| + 2^{-5}.$$

Deshalb schätzen wir $|\ln|\alpha_0||$ ab. Mit Korollar 5.33 erhalten wir:

$$\begin{aligned} |\ln|\alpha_0|| &\le \sum_{i=1}^{k} \ln|\rho_i| + \sum_{j=1}^{\lceil \log_3 k\rceil} \sum_{i_j=1}^{k_j} \ln|\Theta_{(i_j)}/g_{i_j}| \\ &\le k \cdot \max_i\{|\ln|\rho_i||\} + O(k) \cdot \max_{i_j}\{|\ln|\Theta_{(i_j)}/g_{i_j}||\}. \end{aligned} \tag{5.25}$$

Anwenden von Korollar 5.29 liefert uns:

$$\ln|\rho_i| \le 2(\log\Delta + 1) \cdot \Delta \cdot \max_j\{|\ln|\Theta'_{(j)}/g'_j||, |\ln|\Theta''_{(j)}/g''_j||\} = O(\Delta \cdot (\log\Delta)^2),$$

wobei wir $|\Theta'_{(j)}/g'_j|$, $|\Theta''_{(j)}/g''_j| < \Delta$ aus (5.20) mit $a_0 < \Delta$ herleiten.
Für $\ln|\Theta_{(i_j)}/g_{i_j}|$ erhalten wir wegen zweifacher Multiplikation mit $a_0 < \Delta^{3/2}$ eine analoge Schranke, $\ln|\Theta_{(i_j)}/g_{i_j}| < (3/2)\ln\Delta$, so daß wir insgesamt in (5.25) erhalten:

$$|\ln|\alpha_0|| = O(k \cdot \Delta \cdot (\log\Delta)^2 + k \cdot \log\Delta) = O(k \cdot \Delta \cdot (\log\Delta)^2),$$

woraus wegen $k = O(\sqrt{\Delta})$ gemäß (5.13) die Behauptung folgt. ■

Daraus schließen wir zwei Resultate für $y_1 = y - y_0$ und $y \in [-\Delta, 0]$:

5.36 Korollar *Die Berechnung von y_1 in (2) von REACH erfordert polynomielle Laufzeit bzgl. $\log\Delta$, d.h. $L_\Delta[0]$.*

Hinsichtlich der Analyse der restlichen Teilalgorithmen von *REACH* ergibt sich für die Größenordnung von y_1:

5.37 Korollar *Die in (2) von REACH berechnete Größe y_1 genügt $|y_1| = O(\Delta^2)$.*

Wir werden uns der nächsten Teilaufgabe von *REACH* zu, ein reduziertes Hauptideal nahe bei y_1 zu bestimmen.

Die Bestimmung eines Hauptideals nahe bei y_1

Da wir *HREACH* nur auf der diskreten Menge $\frac{1}{3}\mathbb{Z}$ arbeiten lassen, bestimmen wir zunächst in (3) von *REACH* ein bzgl. y_1 geeignetes q, das relativ nahe an y_1 liegt, was in Polynomzeit bzgl. $\log\Delta$ wegen Korollar 5.37 geschieht. Von nun an setzen wir $q \in \frac{1}{3}\mathbb{Z}$ voraus.

Unser Ziel ist es, vom reduzierten $\mathcal{O}_\Delta$ aus ein reduziertes Hauptideal nahe bei q zu erreichen. Mit dem in Kapitel 2 vorgestellten Algorithmus *FORWARD* können wir mittels Vorwärtsschritten q erreichen, was allerdings wegen Lemma 2.68 $O(y_1)$ Anwendungen erfordern kann. Hat $|y_1|$ Größenordnung Δ, benötigt diese Methode exponentielle Laufzeit bzgl. $\log\Delta$. Um dies zu vermeiden, legen wir in *HREACH* eine Verdoppelungsstrategie zugrunde.

5.38 Algorithmus *HREACH* (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$, $q \in \frac{1}{3}\mathbb{Z}$
Ausgabe: H reduziertes Hauptideal in $\mathcal{O}_\Delta$, $\kappa \in \mathcal{O}_\Delta$ in komprimierter Darstellung mit $H = \kappa\mathcal{O}_\Delta$, relativ nahe an q und $\hat{h} \in \mathbb{Q}$ eine Approximation von $\ln|\kappa|$ der Präzision 4

/* Anzahl der Verdoppelungsschritte */ $l \leftarrow \min\{j \in \mathbb{N}_0 \mid q \cdot 2^{-j} \leq (\ln\sqrt{\Delta} + 1/8)/2\}$		(1)
/* Initialisierungen */ $H \leftarrow \mathcal{O}_\Delta$, $\hat{h}_0 \leftarrow 0$ /* aktueller Standort */ $s \leftarrow 0$ /* Sollstandort */ $\kappa \leftarrow$ komprimierte Darstellung von 1		(2)
/* Verdoppeln */		(3)
FOR $j \leftarrow 1$ *TO* l		(4)
	/* Quadriere H, mache es primitiv und reduziere. */ $H \leftarrow (\Theta/g\mathcal{O}_\Delta)H^2$	(5)
	$s \leftarrow q \cdot 2^{-l+j}$ /* neuer Sollstandort */	(6)
	/* Korrigiere H bis Abweichung von $s \leq (\ln\sqrt{\Delta} + 1/8)/2$. */ $\gamma \leftarrow \Theta/g$	(7)
	$(H, \hat{h}_j, \gamma) \leftarrow$ *RELATIVE* $(\Delta, H, \gamma, \hat{h}_{j-1}, s, l-j)$ /* $\hat{h}_j$ ist neuer aktueller Standort */	(8)
	$\kappa \leftarrow \kappa \circ \kappa \circ$ komprimierte Darstellung von γ	(9)
	$j \leftarrow j + 1$	(10)

Zum „relativ“ guten Annähern von H an den Sollstandort s nehmen wir Vorwärts- oder Rückwärtsschritte vor. Auf dieser Idee basiert *RELATIVE* .

5.39 Algorithmus *RELATIVE* (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$, H reduziertes Hauptideal von $\mathcal{O}_\Delta$, γ in der Form (g, a, V, V'), $\hat{h}_{j-1},\ s \in \mathbb{Q}$ Approximationen, Präzision $n \in \mathbb{N}_0$
Ausgabe: H reduziertes Hauptideal, $\hat{h}_j$ aktueller Standort, $\gamma = (g, a, V, V')$

/* approximierter aktueller Standort von H */ $x \leftarrow appr(\ln\|\gamma\|, 2n+5)$ /* „Abweichung" */ $\hat{h}_j \leftarrow 2\hat{h}_{j-1} + x$	(1)
/* Vorwärtskorrektur */	(2)
WHILE $\hat{h}_j \leq s - (\ln\sqrt{\Delta} + 1/8)/2$	(3)
$H \leftarrow H_+$, $\gamma \leftarrow \gamma_+$ /* mit *FORWARD* */	(4)
$x \leftarrow appr(\ln\|\gamma\|, 2n+5)$	(5)
$\hat{h}_j \leftarrow 2\hat{h}_{j-1} + x$	(6)
/* Rückwärtskorrektur */	(7)
WHILE $\hat{h}_j > s + (\ln\sqrt{\Delta} + 1/8)/2$	(8)
$H \leftarrow H_-$, $\gamma \leftarrow \gamma_-$ /* mit *BACKWARD* */	(9)
$x \leftarrow appr(\ln\|\gamma\|, 2n+5)$	(10)
$\hat{h}_j \leftarrow 2\hat{h}_{j-1} + x$	(11)

Wir analysieren *RELATIVE* in Abhängigkeit von *HREACH*. Ferner wird die Laufzeit von *RELATIVE* bestimmend für *HREACH* sein.

Wir beginnen mit der Untersuchung der berechneten Hauptideale H in beiden Algorithmen. Beziehen wir uns dabei lediglich auf *HREACH*, schreiben wir H_j bzgl. der j-ten Iteration der for-Schleife. Wollen wir jeweils noch die i-te Iteration einer der while-Schleifen von *RELATIVE* berücksichtigen, schreiben wir auch $H_{j,i}$, analog für $\gamma_{j,i}$. Wir untersuchen die Erzeugenden von $H_{j,i}$:

5.40 Lemma *In den Iterationen (j,i) von HREACH sowie RELATIVE ist $\kappa_{j-1}^2 \cdot \gamma_{j,i}$ ein Erzeugendes von $H_{j,i}$, d.h. es gilt $H_{j,i} = \kappa_{j-1}^2 \cdot \gamma_{j,i}\mathcal{O}_\Delta$, und $2\hat{h}_{j-1} + x_{j,i}$ ist eine Approximation von $\kappa_{j-1}^2 \cdot \gamma_{j,i}$ der Präzision $2(l-j)+4$.*

Beweis: Wir starten in *HREACH* mit $H_0 = \mathcal{O}_\Delta$ mit $\kappa_0 = 1$. Nach dem Quadrieren in der ersten Iteration der for-Schleife gilt $\gamma_1 = \gamma_{1,0} = 1$ und $H_{1,0} = \kappa_0^2 \cdot \gamma_0\mathcal{O}_\Delta$. Beim anschließenden Aufruf von *RELATIVE* gilt in jeder Iteration i einer der while-Schleifen: In $\gamma_{1,i}$ wird über die zurückgelegten Schritte von H_0 Rechnung getragen, d.h. es gilt $H_{1,i} = H_{1,0}(\gamma_{1,i}\mathcal{O}_\Delta) = \kappa_0^2 \cdot \gamma_{1,i}\mathcal{O}_\Delta$.
Analog argumentieren wir für die nachfolgenden Iterationen $j > 1$ und erhalten gemäß $H_{j+1,0} = H_j^2(\Theta/g\mathcal{O}_\Delta) = \kappa_j^2 \cdot \gamma_{j+1,0}\mathcal{O}_\Delta$ die Behauptung.
Für die Approximationsaussage von $\ln|\kappa_{j-1}^2 \cdot \gamma_{j,i}|$ ergibt sich für $j = 1$

$$|\ln|\kappa_0^2 \cdot \gamma_{1,i}| - (2\hat{h}_0 + x_{1,i})| = |\ln|\gamma_{1,i}| - x_{1,i}| < 2^{-2(l-1)-5}$$

aus (5), (10) von *RELATIVE* wie für $j > 1$

$$\begin{aligned} |\ln|\kappa_{j-1}^2 \cdot \gamma_{j,i}| - (2\hat{h}_{j-1} + x_{j,i})| &\leq 2|\ln|\kappa_{j-1}| - \hat{h}_{j-1}| + |\ln|\gamma_{j,i}| - x_{j,i}| \\ &< 2 \cdot 2^{-2(l-j+1)-4} + 2^{-2(l-j)-5} \\ &= 2^{-2(l-j)-4}. \end{aligned}$$ ■

Aus diesem Beweis und der iterativen Konstruktion des Algorithmus leiten wir den Aufbau von κ her.

5.41 Korollar *Für κ aus $H = \kappa\mathcal{O}_\Delta$ gilt nach Beenden von HREACH :*

$$\kappa = \prod_{j=1}^{l} \left(\Theta_{(j)/g_j} \cdot \Theta_{(l_{j+})} \cdot \Upsilon_{(l_{j-})}\right)^{2^{l-j}},$$

wobei in $\Theta_{(l_{j+})}$ die $O(\log\Delta)$ viele Vorwärtsschritte und in $\Upsilon_{(l_{j-})}$ die $O(\log\Delta)$ viele Rückwärtsschritte gespeichert werden. $l_{j+}, l_{j-} = O(\log\Delta)$ bezeichnet die jeweilige Anzahl der Iterationen einer der while-Schleifen von RELATIVE .

Für die weitere Analyse ist von Bedeutung:

5.42 Lemma *Bei Verlassen von RELATIVE gilt $|\hat{h}_j - s| < (\ln\sqrt{\Delta} + 1/8)/2$ für $1 \leq j \leq l$.*

Beweis: In *HREACH* gilt vor Betreten der for-Schleife $\hat{h}_0 = 0 = s$. Sei nun $1 \leq j \leq l$. Wir zeigen: In *RELATIVE* wird höchstens eine der beiden while-Schleifen durchlaufen, wobei anschließend beide Schleifenbedingungen verletzt sind.
Wir betrachten den Sollstandort s bzgl. dessen ein reduziertes Hauptideal $\Theta\mathcal{O}_\Delta$ mit $|\ln|\Theta| - s| < (\ln\sqrt{\Delta})/2$ existiert, denn wir wissen mit Lemma 2.68 $\ln|\Theta_+| - \ln|\Theta| < \ln\sqrt{\Delta}$. Berücksichtigen wir für $\ln|\Theta|$ Approximationen der Präzision 4 (vgl. Lemma 5.40), dann existiert ein reduziertes Hauptideal $\Theta\mathcal{O}_\Delta$ mit $|appr(\ln|\Theta|, 4) - s| < (\ln\sqrt{\Delta} + 2 \cdot 2^{-4})/2 = (\ln\sqrt{\Delta} + 1/8)/2$. (vgl. (7) in *HREACH*)
1. Fall: Die erste while-Schleife wird betreten. Dann gilt $\hat{h}_{j,i} - s \leq -(\ln\sqrt{\Delta} + 1/8)/2$ für das Ideal $H_{j,i} = \kappa_{j-1}^2 \cdot \gamma_{j,i}\mathcal{O}_\Delta$ (vgl. Lemma 5.40):

$$\begin{aligned} \ln|\kappa_{j-1}^2 \cdot \gamma_{j,i}| - s &= \ln|\kappa_{j-1}^2 \cdot \gamma_{j,i}| - \hat{h}_{j,i} + \hat{h}_{j,i} - s \\ &< 2^{-4} - (\ln\sqrt{\Delta} + 1/8)/2 \\ &= -(\ln\sqrt{\Delta})/2 < 0, \end{aligned}$$

d.h. das Ideal $H_{j,i}$ liegt links von s. Wegen $\ln|\gamma_{++}| - \ln|\gamma| > \ln 2$ für zwei Vorwärtsschritte (vgl. Lemma 2.68) erhalten wir aus den entsprechenden Approximationen $x_{j,i},\ x_{j,i+2}$ in (5) für die Erzeugenden von $H_{j,i}$

$$\hat{h}_{j,i+2} - \hat{h}_{j,i} = x_{j,i+2} - x_{j,i} > \ln 2 - 2 \cdot 2^{-5} > 0, \tag{5.26}$$

so daß $(\hat{h}_{j,2i})_i$ streng monoton wachsend in i ist. Deshalb brechen wir nach endlich vielen Iterationen die erste while-Schleife mit $\hat{h}_{j,i} - s > -(\ln\sqrt{\Delta} + 1/8)/2$ ab. Wir nehmen an, die zweite Schleife wird auch durchlaufen, d.h. es gilt $\hat{h}_{j,i} > s + (\ln\sqrt{\Delta} + 1/8)/2$ in (8). Dann wird mindestens ein Rückwärtsschritt unternommen, von dem wir den ersten betrachten: Dabei ist $\hat{h}_{j,i+1} = \hat{h}_{j,i-1}$, da in (9) $\gamma_{j,i+1} = \gamma_{j,i-1}$ gilt.

$$\begin{aligned}\hat{h}_{j,i} - \hat{h}_{j,i+1} &= \hat{h}_{j,i} - s + s - \hat{h}_{j,i-1} \\ &> (\ln\sqrt{\Delta} + 1/8)/2 + (\ln\sqrt{\Delta} + 1/8)/2 \\ &= \ln\sqrt{\Delta} + 1/8,\end{aligned}$$

wobei zu beachten ist, daß $\hat{h}_{j,i-1} - s \leq -(\ln\sqrt{\Delta} + 1/8)/2$ ist, da Abbruch der ersten while-Schleife erst bei i erfolgt. Nun wissen wir aber: Durch einen Rückwärtsschritt unterscheiden sich zwei benachbarte Ideale um höchstens $\ln\sqrt{\Delta}$. Berücksichtigen wir zusätzlich Präzision 4 der Approximationen, dann kann der Höchstabstand der approximierten Standorte maximal $\ln\sqrt{\Delta} + 2\cdot 2^{-4}$ sein. Die eben betrachteten Approximationen $\hat{h}_{j,i}$, $\hat{h}_{j,i+1}$ unterscheiden sich um mehr, was zum Widerspruch führt.
2. Fall: Die erste while-Schleife wird nicht durchlaufen. Dann gilt $\hat{h}_{j,i} - s > -(\ln\sqrt{\Delta} + 1/8)/2$. Wird die zweite while-Schleife betreten, erhalten wir analog zum 1. Fall nach endlich vielen Iterationen Abbruch. Mit dem entsprechenden Wert für $\hat{h}_{j,i}$ wird die erste Schleifenbedingung verletzt, was ebenfalls analog bewiesen wird.
In beiden Fällen ergeben die verletzten Schleifenbedingungen die Ungleichung der Behauptung. ■

Dann können wir zeigen:

5.43 Lemma *Bei Eingabe von $\Delta \in \mathcal{D}^+$ und $q \in \frac{1}{3}\mathbb{Z}$ berechnet HREACH ein reduziertes Hauptideal $H = \kappa\mathcal{O}_\Delta$, κ in komprimierter Darstellung und eine Approximation $\hat{h}$ von $\ln|\kappa|$ der Präzision 4 mit $|\hat{h} - q| < (\ln\sqrt{\Delta} + 1/8)/2$.*

Beweis: Gemäß Lemma 5.40 erzeugt $\kappa = \kappa_l$ das Ideal H, und $\hat{h}_l = 2\hat{h}_{l-1} + x_{l,i}$ ist eine Approximation der Präzison 4. Aus Lemma 5.42 folgt für $s = q$ die Abweichung von $H = \kappa\mathcal{O}_\Delta$ von q. ■

Für die Laufzeit von *REACH* erhalten wir:

5.44 Lemma *Bei Eingabe von $\Delta \in \mathcal{D}^+$ und q aus (3) von REACH benötigt der deterministische Algorithmus HREACH polynomielle Laufzeit, d.h. $L_\Delta[0]$.*

Beweis: Die aufwendigste Aufgabe ist die for-Schleife, von der wir $l = O(\log|q|) = O(\log\Delta)$ Iterationen ausführen wegen $q = O(y_1) = O(\Delta^2)$ (vgl. Korollar 5.37).
Jede Iteration führt eine Multiplikation mit anschließender Reduktion in Polynomzeit aus und ruft *RELATIVE* auf, dessen Laufzeit wir nun abschätzen: Dort berechnen wir Approximationen $\hat{h}_j$ sowie Vor- oder Rückwärtsschritte. Bei jedem Aufruf j

von *RELATIVE* gilt zu Beginn für die Abweichung von $\hat{h}_j = \hat{h}_{j,0}$ vom Sollstandort $s = s_j$ wegen (1) von *RELATIVE*:

$$\begin{aligned} |\hat{h}_j - s_j| &\leq |2\hat{h}_{j-1} + appr(\ln|\gamma|, 2(l-j)+5) - 2s_{j-1}| \\ &\leq 2|\hat{h}_{j-1} - s_{j-1}| + |appr(\ln|\gamma|, 2(l-j)+5)| \\ &< \ln\sqrt{\Delta} + 1/8 + |\ln|\gamma|| + 2^{-5} \\ &= O(\log\Delta) \end{aligned} \tag{5.27}$$

wegen Lemma 5.42 sowie $\ln|\gamma| = \ln|\Theta/g| = O(\log\Delta)$ aus der Reduktion des Quadrates in (5) von *HREACH* . Gemäß dem Beweis von Lemma 5.42 betreten wir höchstens eine der while-Schleifen, und die Folge $(\hat{h}_{j,2i})_i$ ist streng monoton wachsend in i (vgl. (5.26)) und die der zweiten Schleife streng monoton fallend. Wegen der maximalen Abweichung um $O(\log\Delta)$ von s_j in (5.27) verlassen wir die while-Schleifen nach $O(\log\Delta)$ Iterationen. (vgl. Lemma 2.68) Da eine Iteration der Schleife jeweils polynomielle Laufzeit bzgl. $\log\Delta$ benötigt, braucht *RELATIVE* polynomielle Laufzeit. ■

Die Berechnung von B_0H

In (4) von *REACH* kehren wir mittels Multiplikation von B_0 mit H in die Idealklasse $[B_0]$ zurück. Da B_0 und H reduziert sind, wissen wir mit Proposition 2.74:

5.45 Korollar *Die Berechnung des reduzierten Ideals* $B = (\Theta/g\mathcal{O}_\Delta)B_0H$ *in (4) von REACH erfordert polynomielle Laufzeit bzgl.* $\log\Delta$, *d.h.* $L_\Delta[0]$.

Wir fragen uns, wie nahe dieses reduzierte Ideal B am angestrebten Ziel y liegt. Wir wenden die Abschätzungen der Ideale aus den Teilalgorithmen von *REACH* an:

5.46 Lemma *Das in (4) von REACH berechnete reduzierte Ideal* B *weicht vom gewünschten Standort* y *maximal* $\frac{3}{4}\ln\Delta + \frac{1}{2} = O(\log\Delta)$ *ab.*

Beweis: Sei B wie in (4) von *REACH* angegeben. Dann erhalten wir $B = (\Theta/g\cdot\alpha_0\cdot\kappa\mathcal{O}_\Delta)\prod_{i=1}^{k}P_i^{e_i}$ gemäß Lemma 5.32 und Lemma 5.43. Als Abweichung von $y = y_0 + y_1$ (vgl. (2) von *REACH*) errechnen wir

$$\begin{aligned} |\ln|\Theta/g\cdot\alpha_0\cdot\kappa| - y| &\leq |\ln|\alpha_0| - y_0| + |\ln|\kappa| - y_1| + |\ln|\Theta/g|| \\ &\leq 2^{-5} + |\ln|\kappa| - \hat{h}| + |\hat{h} - q| + |q - y_1| + \ln\sqrt{\Delta} \\ &< 2^{-5} + 2^{-4} + (\ln\sqrt{\Delta} + 1/8)/2 + 1/3 + \ln\sqrt{\Delta} \\ &< (3/2)\ln\sqrt{\Delta} + 1/2 \end{aligned}$$

mit Hilfe der Lemmata 5.32 und 5.43 und der Infrastruktur reellquadratischer Ordnungen aus (2.26). ■

Diese Abweichung wollen wir verringern, indem wir versuchen, möglichst nahe an ein zu B äquivalentes reduziertes Ideal, das y am nächsten liegt, heranzukommen. Dieses Ziel verfolgen wir im nachfolgend beschriebenen Algorithmus *CORRECT* .

Die Abschlußkorrektur

Wir beschreiben den Algorithmus allgemein, analysieren ihn lediglich für Eingaben, die Berechnungen von *REACH* entstammen. Wir übernehmen die Grundidee von Algorithmus *nearest* aus [BiBu], Algorithm 6.7.

5.47 Algorithmus *CORRECT* (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$, B reduziertes Ideal von $\mathcal{O}_\Delta$, $y, y_0, \hat{h} \in \mathbb{Q}$, γ in komprimierter Darstellung

Ausgabe: $\hat{B}$, zu B äquivalentes reduziertes Ideal, möglichst nahe an y, $\hat{x} \in \mathbb{Q}$ Approximation und $\hat{\gamma}$ in komprimierter Darstellung

/* Aktueller Standort $\hat{y}$ von B */ $x \leftarrow appr(\ln\lvert\gamma\rvert, 5)$ $\hat{y} \leftarrow y_0 + \hat{h} + x$	(1)
/* Vorwärtskorrektur durch jeweils 2 Vorwärtsschritte */	(2)
WHILE $(y_0 + \hat{h} + appr(\ln\lvert\gamma_{++}\rvert, 5)) \leq y$	(3)
$B \leftarrow B_{++}$, $\gamma \leftarrow \gamma_{++}$	(4)
$x \leftarrow appr(\ln\lvert\gamma\rvert, 5)$ /* $\hat{y} = y_0 + \hat{h} + x$ als Beweisinvariante */	(5)
/* Rückwärtskorrektur durch jeweils 2 Rückwärtsschritte */	(6)
WHILE $(y_0 + \hat{h} + appr(\ln\lvert\gamma\rvert, 5)) > y$	(7)
$B \leftarrow B_{--}$, $\gamma \leftarrow \gamma_{--}$	(8)
$x \leftarrow appr(\ln\lvert\gamma\rvert, 5)$ /* $\hat{y} = y_0 + \hat{h} + x$ als Beweisinvariante */	(9)
Mache 3 Vor- und 1 Rückwärtsschritt von B aus und wähle $x \in \{appr(\ln\lvert\gamma_-\rvert, 5),\ appr(\ln\lvert\gamma\rvert, 5), appr(\ln\lvert\gamma_+\rvert, 5),\ appr(\ln\lvert\gamma_{++}\rvert, 5),$ $appr(\ln\lvert\gamma_{+++}\rvert, 5)\}$ aus mit $\lvert y - (y_0 + \hat{h} + x)\rvert$ minimal.	(10)
Setze $\hat{B}$, $\hat{\gamma}$ und $\hat{x}$ auf die entsprechenden Werte des gewählten Ideals.	(11)

Für die Analyse erhalten wir:

5.48 Lemma *Bei Eingabe von $\Delta \in \mathcal{D}^+$, einem reduzierten Ideal B von $\mathcal{O}_\Delta$, y, y_0, $\hat{h} \in \mathbb{Q}$ sowie $\gamma = \Theta/g$ gemäß REACH erzeugt CORRECT mit $(\alpha_0 \cdot \kappa \cdot \gamma_j \mathcal{O}_\Delta) \prod_{i=1}^k P_i^{e_i}$ in jeder Iteration ein reduziertes Ideal mit approximiertem Standort $y_0 + \hat{x} + x_j$ von $\ln\lvert\alpha_0 \cdot \kappa \cdot \gamma_j\rvert$ der Präzision 3.*

Beweis: Auf dem Ideal $B = (\alpha_0 \cdot \kappa \cdot \gamma \mathcal{O}_\Delta) \prod_{i=1}^k P_i^{e_i}$ werden lediglich (doppelte) Vor- oder Rückwärtsschritte unternommen, die in γ_j berücksichtigt werden. Dann gilt für die Approximation des Standortes mit den Lemmata 5.32 und 5.43:

$$\begin{aligned} |\ln|\alpha_0 \cdot \kappa \cdot \gamma_j| - (y_0 + \hat{h} + x_j)| &\le |\ln|\alpha_0| - y_0| + |\ln|\kappa| - \hat{h}| = |\ln|\gamma_j| - x_j| \\ &< 2^{-5} + 2^{-4} + 2^{-5} = 2^{-3}. \end{aligned}$$ ■

Optimal wäre das Ideal B, das y am nächsten liegt. Es existieren maximal zwei solcher Ideale, die wir mit $B(y)$ bezeichnen werden. (Links und rechts von y können reduzierte Ideale mit gleichem Abstand zu y liegen.) Nun untersuchen wir, wie nahe das mit *CORRECT* berechnete (approximierte) Ideal B an $B(y)$ gelegen ist.

5.49 Proposition *Sei B ein mit CORRECT berechnetes Ideal, dessen Eingabedaten REACH entstammen. Dann wird bei Verlassen von CORRECT ein reduziertes Ideal B zurückgegeben mit $B \in \{B(y)_{---}, B(y)_{--}, B(y)_{-}, B(y), B(y)_{+}\}$, und $y_0 + \hat{h} + x$ ist eine Approximation seines Standortes $\alpha_0 \cdot \kappa \cdot \gamma$ der Präzision 3.*

Dies bedeutet, daß wir nach (5) von *REACH* maximal drei Ideale links und ein Ideal rechts vom optimalen $B(y)$ liegen.

Beweis: Seien B das Ideal, das wir in *CORRECT* eingeben und $\hat{B}$ das berechnete Ideal. Dann wird gemäß den Bedingungen der while-Schleifen in der Menge

$$\{\ldots, B_{--}, B, B_{++}, \ldots\}$$

das erste Element (bzgl. der Größe) $\alpha_0 \cdot \kappa \cdot \gamma$ mit

$$y_0 + \hat{h} + appr(\ln|\gamma|, 5) \le y \tag{5.28}$$

bestimmt. (In der ersten while-Schleife in (3) kommen wir von unten bzw. links und in der zweiten in (6) von oben bzw. rechts.)
Wir beweisen die Behauptung mittels Widerspruch:
1. Fall: $\ln|\alpha_0 \cdot \kappa \cdot \gamma| > y$.
1. Annahme: $B(y)$ liegt in der Menge der rechten Nachbarn von $\hat{B}$.
Dann liegt $\hat{B}$ näher an y als $B(y)$, was ein Widerspruch ist.
2. Annahme: $B(y)$ liegt in der Menge der linken Nachbarn von $\hat{B}_-$. Dann wissen wir für $\hat{B}$

$$0 < \ln|\kappa \cdot \alpha_0 \cdot \gamma| - y < 2^{-3}$$

wegen $\ln|\kappa \cdot \alpha_0 \cdot \gamma| - 2^{-3} < y_0 + \hat{h} + appr(\ln|\gamma|, 5) \le y$ und Lemma 5.48 sowie (5.28). Dies impliziert einerseits $|\ln|\alpha_0 \cdot \kappa \cdot \gamma| - y| < 2^{-3}$. Andererseits sei $B' = (\alpha_0 \cdot \kappa \cdot \gamma' \mathcal{O}_\Delta) \prod_{i=1}^k P_i^{e_i}$ ein linker Nachbar von $\hat{B}_-$, dann gilt:

$$\begin{aligned} \ln|\alpha_0 \cdot \kappa \cdot \gamma'| - y &= \ln|\alpha_0 \cdot \kappa \cdot \gamma'| - \ln|\alpha_0 \cdot \kappa \cdot \gamma| + \ln|\alpha_0 \cdot \kappa \cdot \gamma| - y \\ &< -\ln 2 + 2^{-3} < 0, \end{aligned}$$

woraus folgt, daß $|\ln|\alpha_0 \cdot \kappa \cdot \gamma'| - y| > \ln 2 - 2^{-3}$. Wegen $|\ln|\alpha_0 \cdot \kappa \cdot \gamma| - y| < 2^{-3}$ bedeutet dies, daß $\hat{B}$ näher an y liegt als B' und damit auch näher als $B(y)$, was zum Widerspruch führt.

2. Fall: $\ln|\alpha_0 \cdot \kappa \cdot \gamma| \leq y$
1. Annahme: $B(y)$ liegt in der Menge der linken Nachbarn von $\hat{B}_-$.
Dann liegt $\hat{B}$ näher an y als $B(y)$, was zum Widerspruch führt.
2. Annahme: $B(y)$ liegt in der Menge der rechten Nachbarn von $\hat{B}_{+++}$.
Dann wissen wir nach Beenden der zweiten while-Schleife $y_0+\hat{h}+appr(\ln|\gamma_{++}|,5) > y$, woraus wir wegen $\ln|\alpha_0 \cdot \kappa \cdot \gamma_{++}| + 2^{-3} > y_0 + \hat{h} + appr(\ln|\gamma_{++}|,5) > y$ folgern:

$$\ln|\alpha_0 \cdot \kappa \cdot \gamma_{++}| - y > -2^{-3}.$$

Sei $B' = (\alpha_0 \cdot \kappa \cdot \gamma' \mathcal{O}_\Delta)\prod_{i=1}^k P_i^{e_i}$ ein rechter Nachbar von $\hat{B}_{+++}$, dann gilt:

$$\begin{aligned} \ln|\alpha_0 \cdot \kappa \cdot \gamma'| - y &= \ln|\alpha_0 \cdot \kappa \cdot \gamma'| - \ln|\alpha_0 \cdot \kappa \cdot \gamma_{++}| + \ln|\alpha_0 \cdot \kappa \cdot \gamma_{++}| - y \\ &> \ln 2 - 2^{-3}, \end{aligned}$$

woraus folgt, daß B_{++} näher an y liegt als B' und somit auch näher als $B(y)$, was zum Widerspruch führt.
Negieren beider Annahmen führt in beiden Fällen zur Behauptung. ■

Wir ermitteln noch die Laufzeit von *CORRECT*.

5.50 Lemma *Bei Eingabe von $\Delta \in \mathcal{D}^+$, einem reduzierten Ideal B von $\mathcal{O}_\Delta$, Approximationen $y, y_0, \hat{h}$ und γ in komprimierter Darstellung als Daten, die sich in REACH ergeben, berechnet der deterministische Algorithmus CORRECT ein reduziertes Ideal $B \in \{B(y)_{---}, B(y)_{--}, B(y)_-, B(y), B(y)_+\}$ in polynomieller Laufzeit, d.h. $L_\Delta[0]$.*

Beweis: Gemäß Lemma 5.46 haben wir bei Eintritt in *CORRECT* eine maximale Abweichung $|y_0 + \hat{h} + x - y|$ von y der Größenordnung $O(\log \Delta)$.
Wenn wir die erste while-Schleife betreten, wird das größte Element mit $y_0 + \hat{h} + appr(\ln|\gamma|,5) \leq y$ in der Menge $\{B, B_{++}, \ldots\}$ berechnet. In der Schleife gilt für die approximierten Abstände zweier iterierter Ideale

$$\begin{aligned} y_0 + \hat{h} + appr(\ln|\gamma_{++}|,5) - (y_0 + \hat{h} + appr(\ln|\gamma|),5) &> \ln 2 - 2 \cdot 2^{-5} \\ &= \ln 2 - 2^{-4} > 0, \end{aligned}$$

so daß wir nach $O(\log \Delta)$ Iterationen die Schleife verlassen. Wird die zweite while-Schleife betreten, liegt ebenfalls maximale Abweichung der Größenordnung $O(\log \Delta)$ vor. Mit analoger Argumentation brechen wir nach $O(\log \Delta)$ vielen Iterationen ab. In beiden Schleifen führt jede Iteration Vorwärts- oder Rückwärtsschritte auf reduzierten Idealen aus und berechnet Approximationen der Präzision 5, so daß wir jeweils Polynomzeit benötigen. ■

Die „gestreute“ Auswahl von B

In Proposition 5.49 haben wir gesehen, daß das berechnete Ideal B innerhalb eines bestimmten „Rahmens“ liegt. Es wird allerdings keine Aussage darüber gemacht, welche der angegebenen Ideale überhaupt vorkommen. Da wir im übernächsten Abschnitt Aussagen über die relative Häufigkeit dieser berechneten reduzierten Ideale herleiten, wollen wir erreichen, daß jedes reduzierte Ideal in der Klasse von B mindestens einmal in einer der Mengen M_y in (6) von *REACH* für ein $y \in [-\Delta, 0]$ berechnet wird. Deshalb nehmen wir in *REACH* abschließend eine sogenannte „Streuung" vor.

Es werden dazu in (6) von *REACH* jeweils drei Vorwärts- und zwei Rückwärtsschritte unternommen, was polynomielle Laufzeit bzgl. $\log \Delta$ erfordert:

5.51 Korollar *Die probabilistische „gestreute" Wahl von B in (6) von REACH erfordert polynomielle Laufzeit, d.h. $L_\Delta[0]$.*

Für den Aufbau von γ erhalten wir:

5.52 Korollar *Gemäß (5) von REACH gilt für γ nach Beenden von CORRECT und der „gestreuten" Wahl:*

$$\gamma = \Theta/g \cdot \prod_{i=1}^{l'} \Theta_{(i)} \cdot \prod_{i=1}^{l''} \Upsilon_{(i)},$$

wobei l', $l'' = O(\log \Delta)$ genügen, und $\Theta_{(i)}$ aus $i = O(\log \Delta)$ Vorwärtsschritten sowie $\Upsilon_{(i)}$ aus $i = O(\log \Delta)$ Rückwärtsschritten bestehen.

Die Zusammenfassung von *REACH*

Wir fassen die Resultate und Laufzeiten der Teilaufgaben (1) - (7) von *REACH* zusammen:

5.53 Satz *Seien $\Delta \in \mathcal{D}^+$, F_C eine Faktorbasis, k ihre Ordnung, $\underline{e} \in [\![0, \Delta]\!]^k$ ein Exponentenvektor und $y \in \mathbb{Q}$ mit $\log |y| = O(\log \Delta)$ die Eingaben von REACH . Dann bestimmt der probabilistische Algorithmus REACH in Zeit $L_\Delta[c]$ ein reduziertes Ideal B, α_0, κ, γ als Menge komprimierter Darstellungen und $\hat{y} \in \mathbb{Q}$, so daß $B = (\alpha_0 \cdot \kappa \cdot \gamma \mathcal{O}_\Delta) \prod_{i=1}^{k} P_i^{e_i}$ mit $B \in \{B(y)_{-----}, \ldots, B(y)_{++++}\}$ und $\hat{y}$ eine Approximation von $\ln |\alpha_0 \cdot \kappa \cdot \gamma|$ der Präzision 3 ist.*

Beweis: Die Behauptung folgt aus den Lemmata 5.32, 5.34, 5.36, 5.44, 5.45, 5.49, 5.50 sowie 5.51. Der Algorithmus wird durch die „gestreute" Wahl in (6) probabilistisch. ■

REACH ermöglicht uns, ein reduziertes Ideal innerhalb einer vorgegebenen Idealklasse $[\prod_{i=1}^{k} P_i^{e_i}]$ zufällig zu wählen. Im übernächsten Abschnitt untersuchen wir die Verteilung der auf diese Weise berechneten reduzierten Ideale in der Klasse.

Zunächst kehren wir zu *RELATION* zurück. In Teilaufgabe (3) steht noch eine Methode zur Feststellung aus, ob das soeben berechnete Ideal B über F_C zerfällt und gegebenenfalls in (4) seinen Zerlegungsvektor $(z_1, \ldots, z_k)$ zu bestimmen.

5.3.3 Das Zerlegen von Idealen über der Faktorbasis

Wegen des Verlustes der Eindeutigkeit der Faktorisierung in quadratischen Ordnungen können wir nicht mehr allgemein von *der* Zerlegung in Primideale reden. Speziell für die Wahl von F_C in Korollar 5.2 werden wir jedoch einen Sonderfall herleiten. Wegen Lemma 5.17 enthält F_C lediglich invertierbare Ideale. Daraus leiten wir ein notwendiges Zerfallskriterium her:

5.54 Korollar ***(1. Zerfallskriterium)***
Zerfällt ein Ideal über F_C, dann ist es invertierbar.

Die Normen von A_p, $\overline{A_p}$ berechnen sich gemäß Lemma 2.35 zu p,

$$N(A_p) = p \qquad \text{und} \qquad N(\overline{A_p}) = p. \tag{5.29}$$

Dann können wir für die Eindeutigkeit der Faktorisierung zeigen:

5.55 Proposition *Besitzt ein Ideal B von $\mathcal{O}_\Delta$ eine Zerlegung über der Faktorbasis F_C, dann ist sie eindeutig.*

Beweis: Wir wenden Satz 2.48 an und zeigen hierzu, daß die Norm von B und der Führer f von $\mathcal{O}_\Delta$ teilerfremd sind.
Sei q ein Primteiler von $\mathrm{ggT}(N(B), f)$. Einerseits teilt q dann den Führer f von $\mathcal{O}_\Delta$, woraus wir $q \mid \Delta$ folgern. Andererseits teilt q auch $N(B)$. Da B über F_C zerfällt, besteht B wegen Lemma 5.17 nur aus invertierbaren Primidealen, so daß die Norm multiplikativ ist. (vgl. Lemma 2.47) Also hat $N(B)$ wegen (5.29) nur Primfaktoren p, die $(\Delta/p) = 1$ bzw. $p \nmid \Delta$ genügen, was zum Widerspruch mit $q \mid \Delta$ und $q \mid N(B)$ führt. ∎

Dieses Resultat enthüllt einen weiteren Vorteil für die gemäß Korollar 5.2 gewählte Faktorbasis F_C: Bzgl. F_C haben wir eindeutige Zerlegungen, was die Relation in (5) *unabhängig* von der jeweils gefundenen Zerlegung für B macht. Ferner leiten wir ein notwendiges Kriterium für den Zerfall über F_C her, mit dem sich aus der Norm von B Rückschlüsse auf seine möglichen Primideale ziehen lassen.

5.56 Lemma ***(2. Zerfallskriterium)***
Falls ein Ideal B einer reellquadratischen Ordnung über F_C zerfällt, dann genügt jeder Primteiler p_j der Norm $N(B)$ der Forderung $A_{p_j} \in F_C$.

Beweis: Sei B ein Ideal, das über F_C zerfällt. Wegen (5.29) und der Multiplikativität der Norm enthält $N(B)$ nur Primzahlen p_j, für die A_{p_j} oder $\overline{A_{p_j}}$ B teilt, diese also Elemente von F_C sind. ∎

Die beiden Zerfallskriterien legen folgende Strategie nahe: Zuerst wenden wir das 1. Zerfallskriterium an und testen mittels des Führers $f(B)$, ob B invertierbar ist. Falls dies zutrifft, wenden wir das 2. Zerfallskriterium an. Bei dessen positiver Beantwortung bestimmen wir die Teiler von B aus F_C. Wir erhalten dann

$$B = A \prod_{i=1}^{k} P_i^{z_i}. \tag{5.30}$$

Falls $A \neq \mathcal{O}_\Delta$, d.h. $N(A) \neq 1$, zerfällt B nicht über F_C wegen der eindeutigen Zerlegung von B gemäß dem nachfolgenden Lemma 5.58. Damit können wir zur algorithmischen Realisierung übergehen.

5.57 Algorithmus *ZERLEGUNG* (Teilalgorithmus)

Eingabe: B reduziertes Ideal in $\mathcal{O}_\Delta$ in Standarddarstellung, Faktorbasis $F_C = \{P_1, \ldots, P_k\}$, $k = \sharp F_C$

Ausgabe: Exponentenvektor $\underline{z} \in \mathbb{Z}^k$ von B, falls B über F_C zerfällt, sonst $\underline{z}$ = leere Liste.

```
IF   (f(B) ← ggT(a, b, (b²−Δ)/(4a))) > 1      /* 1. Zerfallskriterium */
THEN   z ← leere Liste, EXIT
ELSE   N ← a        /* = Norm N(B) */
FOR  i ← 1 TO k       /* 2. Zerfallskriterium */
    WHILE  p_i | N
        N ← N/p_i
    i ← i + 2
IF   N > 1       /* 2. Zerfallskriterium verletzt */
THEN   z ← leere Liste, EXIT
N ← a       /* Versuche, B über F_C zu zerlegen. */
FOR  i ← 1 TO k
    IF   p_i | N
    THEN   z_i ← EXPO(B, P_i)
           z_{i+1} ← EXPO(B, P_{i+1})       /* P_{i+1} = \overline{P_i} */
           N ← N/(p_i^{z_i + z_{i+1}})
    ELSE   z_i ← z_{i+1} ← 0
    i ← i + 2
IF   N > 1       /* A ≠ O_Δ, vgl. (5.30) */
THEN   z ← leere Liste
```

Wir liefern einige Erläuterungen nach: Erfüllt ein Ideal B beide Zerfallskriterien, muß es nicht notwendig über F_C zerfallen. Wir beweisen allerdings folgendes hilfreiches Resultat:

5.58 Lemma *Ist B ganzes Ideal in $\mathcal{O}_\Delta$, das dem 2. Zerfallskriterium genügt, dann ist B eindeutig faktorisierbar.*

Beweis: Gemäß Lemma 5.56 wissen wir für B in $\mathcal{O}_\Delta$: Alle Primteiler p_j von $N(B)$ genügen $p_j \not| \Delta$ wegen $A_{p_j} \in F_C$. Deshalb ist $\mathrm{ggT}(N(B), \Delta) = 1$, woraus wir $\mathrm{ggT}(N(B), f) = 1$ folgern wegen $\Delta = f^2\Delta_0$. Also besitzt B eine eindeutige Faktorisierung wegen Satz 2.48. ■

In (13) von *ZERLEGUNG* steht noch die Bestimmung der Exponenten z_i der Zerlegung von B bzgl. F_C aus. Rufen wir *EXPO* auf, wissen wir bereits, daß B eindeutig faktorisierbar ist. Daher schlagen wir folgenden Weg ein:

$$z_i = \max\{n \in \mathbb{N}_0 \mid BP_i^{-n} \subseteq \mathcal{O}_\Delta\}. \tag{5.31}$$

Wir suchen solch ein maximales n, das (5.31) genügt. Dazu benötigen wir eine praktikable Methode zur Überprüfung der Ganzheitsbedingung. Aus $p_i\mathcal{O}_\Delta = A_{p_i}\overline{A_{p_i}}$ bzw. in der momentanen Schreibweise $p_i\mathcal{O}_\Delta = P_i\overline{P_i}$ erhalten wir:

$$\begin{aligned} BP_i^{-n} &= B\,\underbrace{P_i^{-n}\overline{P_i}^{-n}}_{=p_i^{-n}\mathcal{O}_\Delta}\,\overline{P_i}^{n} \\ &= (p_i^{-n}\mathcal{O}_\Delta)B\overline{P_i}^{n}. \end{aligned} \tag{5.32}$$

Es bleibt noch zu klären, wie wir die Ganzheitsbedingung überprüfen. Hierzu liefert Korollar 2.34 ein Ganzheitskriterium auf der Grundlage der Standarddarstellung des zu testenden Ideals.

5.59 Korollar *(p_i-Ganzheitskriterium)*
Sei $m(\mathbb{Z}a+\mathbb{Z}(b+\sqrt{\Delta})/2)$ die Standarddarstellung von $B\overline{P_i}^n$. Dann ist BP_i^{-n} genau dann ganzes Ideal von $\mathcal{O}_\Delta$, wenn $p_i^n \mid m$ gilt.

Beweis: Sei $m(\mathbb{Z}a + \mathbb{Z}(b + \sqrt{\Delta})/2)$ die Standarddarstellung von $B\overline{P_i}^n$. Dann berechnet sich die Standarddarstellung von $(p_i^{-n}\mathcal{O}_\Delta)B\overline{P_i}^n$ zu $(m/p_i^n)(\mathbb{Z}a + \mathbb{Z}(b + \sqrt{\Delta})/2)$. Anwenden von Korollar 2.34 sowie (5.32) liefert die Behauptung. ■

Damit haben wir ein einfach zu überprüfendes Kriterium, so daß wir den Algorithmus zur Bestimmung von z_i formulieren können. Wir beachten, daß $\overline{P_i}$ sich mittels der Faktorbasis einfach bestimmen läßt, indem wir das andere Primideal gleicher Norm in der Faktorbasis nehmen. Aufgrund der vorgenommenen Sortierung von F_C in Abschnitt 5.2 ist dies das Ideal davor oder danach.

5.60 Algorithmus *EXPO* (Teilalgorithmus)

Eingabe: B eindeutig zu faktorisierendes Ideal in $\mathcal{O}_\Delta$ in Standarddarstellung, P Primideal aus F_C
Ausgabe: n, der Exponent von P bzgl. B

/* n bezeichnet den aktuellen Exponenten*/ $n \leftarrow 0$	(1)
WHILE $(p^{-n}\mathcal{O}_\Delta)\, B\overline{P}^n \subseteq \mathcal{O}_\Delta$	(2)
$n \leftarrow n+1$	(3)
$n \leftarrow n-1$ /* ist der maximale Wert für n in (5.31) */	(4)

Abschließend führen wir eine Analyse des Zerlegungsverfahren durch.

Analyse und Komplexität des Zerlegungsverfahrens

Der Aufbau des Zerfallstests legt es nahe, Teilaufgabe (3) und (4) in *RELATION* gemeinsam zu analysieren. In (3) wissen wir, daß B reduziert ist, was in der Analyse eine besondere Rolle spielen wird. Wir beginnen mit der Analyse von *EXPO* .

5.61 Lemma *Bei Eingabe eines eindeutig zu faktorisierenden Ideals B in Standarddarstellung und $P_i \in F_C$ berechnet EXPO den Exponenten von P_i bzgl. B.*

Beweis: Wegen $B \subseteq \mathcal{O}_\Delta$ ist $n \geq 0$. Nach Beenden der while-Schleife liegt der kleinste Wert für n vor, so daß die Bedingung verletzt ist. Nach Ausführung von (4) haben wir den maximalen Wert für die Gültigkeit von $BP_i^{-n} \subseteq \mathcal{O}_\Delta$ mit (5.32). Dies liefert den Exponenten z_i wegen (5.31). ■

Daraus schließen wir für die Laufzeit:

5.62 Lemma *Der deterministische Algorithmus EXPO benötigt bei Eingabe eines eindeutig zu faktorisierenden, reduzierten Ideals B von $\mathcal{O}_\Delta$ in Standarddarstellung sowie $P_i \in F_C$ zur Bestimmung des Exponenten z_i polynomielle Laufzeit bzgl.* $\log \Delta$, *d.h.* $L_\Delta[0]$.

Beweis: Die aufwendigste Operation ist die Ausführung der Schleife, wozu wir die Anzahl der Iterationen und den jeweiligen Aufwand abschätzen.
Die Anzahl der Iterationen resultiert aus der Abschätzung

$$N(P_i^{z_i}) = p_i^{z_i} \leq N(B) < \sqrt{\Delta},$$

da B reduziert ist. Daraus leiten wir $z_i = O(\log \Delta)$ her.
Die aufwendigste Aufgabe ist die Überprüfung der Schleifenbedingung. Zur Berech-

nung der Standarddarstellung von $B\overline{P_i}^n$ wenden wir *MUL* an. (vgl. Algorithmus 2.36) Wegen $n \leq z_i = O(\log \Delta)$ bleiben die Eingabelängen für die jeweiligen Aufrufe von *MUL* polynomiell beschränkt in $\log \Delta$, so daß *MUL* gemäß Lemma 2.37 polynomielle Laufzeit benötigt. Der anschließende Ganzheitstest mittels $p_i^n \mid m$ gemäß Lemma 5.59 erfordert ebenfalls polynomielle Laufzeit bzgl. $\log \Delta$. ■

Diese Aussagen bringen wir bei der Analyse von *ZERLEGUNG* ein.

5.63 Lemma *Bei Eingabe eines reduzierten Ideals B von $\mathcal{O}_\Delta$ in Standarddarstellung, einer Faktorbasis F_C sowie deren Ordnung k berechnet ZERLEGUNG den Zerlegungsvektor $\underline{z}$ von B, falls B über F_C zerfällt. Sonst ergibt sich $\underline{z}$ als leere Liste.*

Beweis: Die Berechnung des Führers $f(B)$ überprüft, ob B invertierbar ist. Dann liegen bei Abfrage des 2. Zerfallskriteriums in (5) nur noch invertierbare Ideale der Norm $N = a$ vor. Gilt nach der sich anschließenden for-Schleife $N > 1$, enthält N einen Primfaktor p_j, für den es kein Primideal in F_C gibt. Dann kann B gemäß Lemma 5.54 nicht über F_C zerfallen. Also brechen wir ab. Demnach liegen wegen Lemma 5.58 in (10) nur noch eindeutig zu faktorisierende Ideale vor. Deshalb bestimmt wegen Lemma 5.61 die anschließende for-Schleife für B die Exponenten z_i von $P_i \in F_C$. Dabei wird N durch die entsprechenden Normen $p_i^{z_i} = N(P_i^{z_I})$ dividiert. Abschließend wird in (28) gemäß (5.30) überprüft, ob $N(A) = 1$, d.h. ob B über F_C zerfällt.
Somit liefert *ZERLEGUNG* die leere Liste genau dann, wenn B nicht über F_C zerfällt. Ansonsten erhalten wir den Zerlegungsvektor $\underline{z}$. ■

Für die Laufzeit erhalten wir dann:

5.64 Lemma *Der deterministische Algorithmus ZERLEGUNG benötigt bei Eingabe eines reduzierten Ideals B in Standarddarstellung, einer Faktorbasis F_C sowie deren Ordnung k Laufzeit $L_\Delta[c]$.*

Beweis: Weil B reduziert ist, wissen wir $N = a$ und b aus der Standarddarstellung sind durch $O(\sqrt{\Delta})$ beschränkt. Ferner folgt aus $A_{p_i} \in F_C$: $p_i \leq C \leq \sqrt{\Delta}$. Die aufwendigsten Operationen beinhaltet die 2. for-Schleife.
Wir haben $k/2 \leq C = L_\Delta[c]$ Iterationen auszuführen.
Je Iteration teilen wir N durch p_i und rufen *EXPO* maximal zweimal auf, teilen N durch $p_i^{z_i + z_{i+1}} \leq N$, was jeweils polynomielle Laufzeit bzgl. $\log \Delta$ wegen Lemma 5.62 erfordert. ■

Dann erhalten wir für den Test von B auf Zerfall über F_C in *RELATION*:

5.65 Korollar *In (3) und (4) von RELATION benötigt der Zerlegungstest und die eventuelle Bestimmung des Zerlegungsvektors $\underline{z}$ von B Zeit $L_\Delta[c]$.*

Nun haben wir alle Teilaufgaben von *RELATION* gelöst und analysiert.

5.3.4 Zusammenfassung der Relationengenerierung

Wir fassen die Relationengenerierung in einer endgültigen Version zusammen und bringen dabei die Resultate unserer Untersuchungen ein. Aus der vorläufigen Version von *RELATION* aus Algorithmus 5.21 erhalten wir abschließend:

5.66 Algorithmus *RELATION* (endgültige Fassung)

Eingabe: $\Delta \in \mathcal{D}^+$, Faktorbasis $F_C = \{P_1, \ldots, P_k\}$, $k = \sharp F_C$
Ausgabe: approximierte Relation $(v_1, \ldots, v_k, -\hat{y})$, α_0, κ, γ als Menge komprimierter Darstellungen mit Approximation $\hat{y}$ von $\ln|\alpha = \alpha_0 \circ \kappa \circ \gamma|$ der Präzision 3, falls die Relationengenerierung erfolgreich ist.

<table>
<tr><td colspan="2">/* Wahl einer Idealklasse */
Wähle zufällig und gleichverteilt einen Exponentenvektor, d.h.
$\underline{e} \in_R [\![0, \Delta]\!]^k$.</td><td>(1)</td></tr>
<tr><td colspan="2">/* Wahl eines reduzierten Ideals in dieser Idealklasse */
(a) Wähle zufällig und gleichverteilt eine Zahl y mit
$y \in_R [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z}$.
(b) /* Bestimme ein reduziertes Ideal B mit $B = (\alpha\mathcal{O}_\Delta)\prod_{i=1}^k P_i^{e_i}$
und $\ln|\alpha| \sim y$. */
$(B, \hat{y}, \alpha_0, \kappa, \gamma) \leftarrow REACH\ (\Delta, F_C, k, \underline{e}, y)$
/* $\alpha = \alpha_0 \circ \kappa \circ \gamma$ und $\hat{y}$ ist Approximation von $\ln|\alpha|$ der Präzision 3 */</td><td>(2)</td></tr>
<tr><td colspan="2">$L \leftarrow ZERLEGUNG\ (B, F_C, k)$</td><td>(3)</td></tr>
<tr><td colspan="2">IF $L \neq$ Leere Liste</td><td>(4)</td></tr>
<tr><td>THEN</td><td>/* L ist Zerlegungsvektor von B */
$(v_1, \ldots, v_k, -\hat{y}) \leftarrow (e_1 - z_1, \ldots, e_k - z_k, -\hat{y})$</td><td>(5)</td></tr>
</table>

Wie wir Schritt (4) von *RELATION* entnehmen, wird nicht immer eine erweiterte Relation bestimmt. Die Suche ist nur dann erfolgreich, wenn das in (2) berechnete Ideal B über der Faktorbasis zerlegbar ist. Es handelt sich bei *RELATION* um einen probabilistischen Algorithmus vom Typ *Las-Vegas*. Zur Abkürzung bezeichnen wir erweiterte Relationen, wie sie mit *RELATION* bestimmt werden, auch als *approximierte Relationen* der Präzision 3.

5.67 Satz *Bei Eingabe von $\Delta \in \mathcal{D}^+$, einer Faktorbasis und ihrer Ordnung bestimmt der Las-Vegas-Algorithmus RELATION im Erfolgsfall eine approximierte Relation der Präzision 3 in Zeit $L_\Delta[c]$.*

Beweis: Die Behauptung folgt aus Satz 5.53 sowie Lemma 5.64 und Korollar 5.65. ■

Im Zusammenhang mit der Erzeugung des erweiterten Relationengitters werden wir im nächsten Abschnitt eine untere Schranke für die Wahrscheinlichkeit erhalten, daß ein Aufruf von *RELATION* erfolgreich beendet wird.

Die Verteilung der berechneten reduzierten Ideale

Wir sind daran interessiert, wie sich zu gegebenem Exponentenvektor $\underline{e}$ die mit *RELATION* berechneten reduzierten Ideale B in der Klasse $[\prod_{i=1}^{k} P_i^{e_i}]$ bzgl. $y \in [-\Delta, 0] \cap \mathbb{Z}\frac{1}{3}$ verteilen. Dies werden wir untersuchen, wozu wir wegen (2) von *RELATION* Teilalgorithmus *REACH* genauer betrachten.

Nach Teilaufgabe (1) von *REACH* haben wir mit Hilfe des deterministischen Algorithmus *POTPROD* das reduzierte Ideal $B_0 = (\alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^{k} P_i^{e_i}$ und den approximierten Standort y_0. (vgl. Lemma 5.32) Um y zu erreichen, verbleibt noch der Weg

$$y_1 \sim y - y_0,$$

vgl. (5.16). Wir lassen $y \in [-\Delta, 0] \cap \mathbb{Z}\frac{1}{3}$ variieren und untersuchen, wie sich auf dieser Strecke die reduzierten Ideale in der Klasse $[B_0] = [\prod_{i=1}^{k} P_i^{e_i}]$ verteilen. Dabei ist die Idealmenge M_y in (6) von *REACH* entscheidend. Daher steht sie im Mittelpunkt der nachfolgenden Untersuchungen der Auswahl in M_y basierend auf B_0 und y_1 bzw. y.

5.68 Lemma *Seien B_0 ein in (1) von REACH berechnetes reduziertes Ideal und $B \in [B_0]$ ein beliebiges reduziertes Ideal. Dann ist B in mindestens $\lfloor \Delta/R \rfloor$ vielen Mengen M_y enthalten für $y \in [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z}$.*

Beweis: Seien B_0, α_0 gemäß (1) von *REACH* und $B \in [B_0]$ ein reduziertes Ideal. Dann existiert nach Satz 2.62 ein Θ als Produkt von Vorwärtsschritten mit $B = (\Theta \mathcal{O}_\Delta) B_0$ und $0 \leq \ln|\Theta| < R = \ln \eta$. Ferner gilt $B = (\eta^j \cdot \Theta \mathcal{O}_\Delta) B_0$ für alle $j \in \mathbb{Z}$, woraus

$$B = (\eta^j \cdot \Theta \cdot \alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^{k} P_i^{e_i}$$

wegen Lemma 5.32 folgt. B hat den Standort $jR + \ln|\Theta \cdot \alpha_0|$. Wir betrachten diejenigen $j \in \mathbb{Z}$, die $-\Delta \leq jR + \ln|\Theta \cdot \alpha_0| \leq 0$ genügen. Geeignete Umformungen liefern

$$\frac{-\Delta - \ln|\Theta \cdot \alpha_0|}{R} \leq j \leq -\frac{\ln|\Theta \cdot \alpha_0|}{R}, \tag{5.33}$$

so daß es mindestens $\lfloor \Delta/R \rfloor$ viele solcher $j \in \mathbb{Z}$ gibt. Für jedes dieser j existiert ein $m := m_j \in \mathbb{Z}$ mit

$$\frac{m}{3} - \frac{1}{3} < \ln|\eta^j \cdot \Theta \cdot \alpha_0| \leq \frac{m}{3}. \tag{5.34}$$

Wegen der Wahl von j liegt $m/3$ in $[-\Delta, 0]$. Deshalb können wir $y = m/3$ setzen. Dann wird in (5) von *REACH* wegen Proposition 5.49 ein Ideal aus $\{B(m/3)_{---}, \ldots, B(m/3)_+\}$ berechnet. Die anschließenden drei Vorwärts- und zwei Rückwärtsschritte (vgl. (6) in *REACH*) ergeben für die entsprechende Idealmenge $M_{m/3}$:

$$M_{m/3} \supseteq \{B(m/3)_-, B(m/3)\}.$$

Wir werden zeigen, daß unser Ausgangsideal B in $\{B(m/3)_-, B(m/3)\}$ liegt, d.h. für das gemäß (5.34) gewählte m wird B bzgl. $M_{m/3}$ berechnet. Insgesamt haben wir $\lfloor \Delta/R \rfloor$ solcher j und Mengen $M_{(m=m_j)/3}$, so daß die Aussage des Lemmas folgt. Wir führen den noch ausstehenden Beweis mittels Widerspruch. *Annahme:* $B \notin$

$\{B(m/3)_-, \ B(m/3)\}$. Dann ist wegen (5.34) B ein linker Nachbar von $B(m/3)_-$. Falls B sogar linker Nachbar von $B(m/3)_{--}$ ist, gilt für seinen Standort bzgl. $B(m/3)_- = (\Theta' \cdot \eta^j \alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^k P_i^{e_i}$;

$$\begin{aligned} \ln|\Theta \cdot \eta^j \cdot \alpha_0| &= \ln|\Theta \cdot \eta^j \cdot \alpha_0| - \ln|\Theta' \cdot \eta^j \cdot \alpha_0| + \ln|\Theta' \cdot \eta^j \cdot \alpha_0| \\ &< -\ln 2 + m/3 \\ &< (m-1)/3, \end{aligned}$$

was im Widerspruch zu (5.34) steht. Also betrachten wir $B = B(m/3)_{--}$, wobei wir den Standort von $B(m/3) = (\Theta' \cdot \eta^j \alpha_0 \mathcal{O}_\Delta) \prod_{i=1}^k P_i^{e_i}$ berechnen:

$$\begin{aligned} \ln|\Theta' \cdot \eta^j \cdot \alpha_0| &= \ln|\Theta' \cdot \eta^j \cdot \alpha_0| - \ln|\Theta \cdot \eta^j \cdot \alpha_0| + \ln|\Theta \cdot \eta^j \cdot \alpha_0| \\ &> \ln 2 + (m-1)/3 \\ &> (m+1)/3. \end{aligned}$$

Wegen (5.34) liegt B näher an $m/3$ als $B(m/3)$, was zum Widerspruch führt. ■

In obigem Beweis können wir sogar zeigen, daß das Ideal B auch für $M_{(m+1)/3}$ oder $M_{(m-1)/3}$ berechnet wird, sofern $(m \pm 1)/3$ noch in $[-\Delta, 0]$ liegen. Da der Beweis umständlich und die Aussage für uns nicht relevant ist, verzichten wir auf ihn. Wegen Satz 2.69 gilt $\lfloor \Delta/R \rfloor > 1$ für hinreichend großes Δ, so daß jedes reduzierte Ideal in $[B_0]$ auch tatsächlich für mindestens ein y in M_y berechnet wird.

Wir bestimmen eine obere Schranke für die Anzahl der möglichen y, für die B in M_y enthalten ist.

5.69 Lemma *Seien B_0 ein in (1) von REACH berechnetes reduziertes Ideal und $B \in [B_0]$ ein beliebiges reduziertes Ideal. Dann ist B in höchstens $\lceil \Delta/R \rceil \cdot \lceil 30 \ln \sqrt{\Delta} \rceil$ vielen Mengen M_y enthalten für $y \in [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z}$.*

Beweis: Wir starten analog zum Beweis von Lemma 5.68. Dann erhalten wir den Faktor $\lceil \Delta/R \rceil$ als obere Schranke der j aus (5.33). Wir betrachten analog zu (5.34) jeweils $y = m_j/3$.
Aufgrund der Abweichungen sowie der Vor- und Rückwärtsschritte gemäß Proposition 5.49 und (6) von *REACH* gilt $M_y \subseteq \{B(y)_{-----}, \ldots, B(y)_{++++}\}$. Wir liegen also maximal fünf reduzierte Ideale links von $B(y)$, und $B(y)$ ist maximal $(\ln \sqrt{\Delta})/2$ von y entfernt. (Gemäß Lemma 2.68 sind benachbarte reduzierte Ideale maximal $\ln \sqrt{\Delta}$ voneinander entfernt.) Ist also $y_1 < y - (5 + 1/2) \ln \sqrt{\Delta}$, so sind M_{y_1} und M_y disjunkt.
Ferner liegen wir maximal vier reduzierte Ideale rechts von $B(y)$. Analog wie eben erhalten wir für $y_2 > y + (4 + 1/2) \ln \sqrt{\Delta}$ disjunkte Mengen M_y und M_{y_2}.
Aus $y \in \frac{1}{3}\mathbb{Z}$ erhalten wir die Behauptung. ■

Mit Hilfe der letzten beiden Lemmata erhalten wir obere und untere Schranken für die Wahrscheinlichkeit, daß in *REACH* bei zufällig und gleichverteilter Wahl von $y \in [-\Delta, 0] \cap \frac{1}{3}$ ein beliebiges reduziertes Ideal B in $[B_0]$ zurückgegeben wird. Daraus leiten wir schließlich Aussagen über die Verteilung der reduzierten berechneten Ideale her.

5.70 Satz *Sei B_0 das bzgl. $\underline{e} \in [\![0,\Delta]\!]^k$ in (1) von REACH berechnete reduzierte Ideal und $B \in [B_0]$ ein beliebiges reduziertes Ideal. Dann läßt sich die Wahrscheinlichkeit $p(B)$, daß B bei zufälliger und gleichverteilter Wahl von $y \in [-\Delta, 0] \cap \frac{1}{3}$ mit REACH zurückgegeben wird, wie folgt beschränken:*

$$\frac{\lfloor \Delta/R \rfloor}{6(3\Delta+1)} \leq p(B) \leq \frac{\lceil \Delta/R \rceil}{3\Delta+1} \cdot O(\ln\sqrt{\Delta})$$

Beweis: Die Wahl von B geschieht in zwei Stufen: Zuerst wird zufällig und gleichverteilt ein $y \in [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z}$ gewählt. Danach wird in der 6-elementigen Menge M_y zufällig und gleichverteilt ein Ideal ausgewählt. Dabei kann M_y aus lauter verschiedenen Idealen bestehen, maximal stimmen sie alle überein. (bei kleiner Zykellänge) Dann haben wir für die Wahrscheinlichkeit, daß B gewählt wird:

$$\frac{\sharp\{y \in [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z} \mid B \in M_y\}}{6(3\Delta+1)} \leq p(B) \leq \frac{6 \cdot \sharp\{y \in [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z} \mid B \in M_y\}}{6(3\Delta+1)}.$$

Anwenden der Lemmata 5.68 und 5.69 auf die Schranken der Abschätzung ergibt die Behauptung. ■

Asymptotisch erhalten wir für die Wahrscheinlichkeit $p(B)$:

5.71 Korollar *In der Situation von Satz 5.70 erhalten wir $p(B) = (1/R) \cdot L_\Delta[0]$, d.h. in Schritt (2) von RELATION zieht die zufällige und gleichverteilte Wahl von $y \in [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z}$ eine Gleichverteilung der reduzierten Ideale in $[B_0]$ (für $\Delta \to \infty$) nach sich.*

5.72 Bemerkung Die Aussage des Korollars ermöglicht ein allgemeineres Resultat: Die Teilschritte (3) - (7) von *REACH* liefern ein Tool zur zufälligen und gleichverteilten Wahl reduzierter Ideale in einer Klasse $[B_0]$, wenn wir von einem reduzierten Ideal B_0 ausgehen.

Im nächsten Abschnitt wollen wir die Relationengitter mit etwa zufällig und gleichverteilt gewählten Relationen erzeugen. Dazu klären wir noch folgende Frage: Gegeben sei eine mit *RELATION* berechnete erweiterte Relation, die wir mit $(\underline{v}, -\ln|\alpha|)$ identifizieren. Wie viele $(\underline{e}, y) \in [\![0,\Delta]\!]^k \times ([-\Delta, 0] \cap \frac{1}{3}\mathbb{Z})$ ergeben $(\underline{v}, -\ln|\alpha|)$? Wegen der Auswahl in M_y betrachten wir statt dessen die Frage: Wie viele $(\underline{e}, y) \in [\![0,\Delta]\!]^k \times ([-\Delta, 0] \cap \frac{1}{3}\mathbb{Z})$ können $(\underline{v}, -\ln|\alpha|)$ ergeben, in dem Sinne, daß in M_y das entsprechende Ideal gewählt wird? Zur Klärung dieser Frage brauchen wir außerdem eine Abschätzung für die Anzahl aller reduzierten Ideale in $\mathcal{O}_\Delta$, die über der zugrundeliegenden Faktorbasis F_C zerlegbar sind, d.h. wir betrachten

$$\mathcal{Z} := \{B \mid B \text{ reduziertes Ideal von } \mathcal{O}_\Delta \text{ und über } F_C \text{ zerlegbar}\}. \tag{5.35}$$

Wir schätzen $\sharp\mathcal{Z}$ später ab und können mit $\sharp\mathcal{Z}$ die Frage vorläufig beantworten:

5.73 Lemma *Sei* $(\underline{v}, -\ln|\alpha|)$ *eine erweiterte Relation, die einer Berechnung von RELATION entstammt. Dann existieren maximal* $\sharp\mathcal{Z}\cdot O(\ln\sqrt{\Delta})$ *viele* $(\underline{e}, y) \in [\![0, \Delta]\!]^k \times ([-\Delta, 0] \cap \frac{1}{3}\mathbb{Z})$, *für die RELATION* $(\underline{v}, -\ln|\alpha|)$ *liefern kann.*

Beweis: Wir gehen von einer mit *RELATION* bestimmten erweiterten Relation $(\underline{v}, -\ln|\alpha|)$ aus. Dann existiert zu jedem $\underline{z}$ mit $\prod_{i=1}^k P_i^{z_i} \in \mathcal{Z}$ ein $\underline{e} \in \mathbb{Z}^k$ mit

$$(1/\alpha)\mathcal{O}_\Delta = \prod_{i=1}^k P_i^{v_i} = \prod_{i=1}^k P_i^{e_i - z_i}.$$

Damit existieren bzgl. $\underline{v}$ $\sharp\mathcal{Z}$ viele Exponentenvektoren $\underline{e}$, die nicht notwendig alle in $[\![0, \Delta]\!]^k$ liegen.
Für jedes solche $\underline{e}$ untersuchen wir die Anzahl der y, für die M_y das Ideal $\prod_{i=1}^k P_i^{z_i} \in \mathcal{Z}$ enthält und $\ln|\alpha|$ ergibt. Wegen der letzten Bedingung ist im Beweis von Lemma 5.69 j durch $\ln|\alpha| = jR + \ln|\Theta|$ festgelegt, so daß maximal $O(\ln\sqrt{\Delta})$ viele M_y das Ideal $\prod_{i=1}^k P_i^{z_i}$ enthalten können. ■

5.74 Bemerkung Da die Normen reduzierter Ideale durch $\sqrt{\Delta}$ beschränkt sind (vgl. Lemma 2.52), sind die Koordinaten von $\underline{z}$ im Beweis von Lemma 5.73 durch $0 \leq z_i \leq \log\sqrt{\Delta}$ beschränkt. Vernachlässigen wir die Vektoren $\underline{e} = \underline{v} + \underline{z}$, die nicht in $[\![\Delta, 0]\!]^k$ liegen, erhalten wir eine asymptotische Abschätzung: Jeweils

$$\sharp\mathcal{Z} \cdot L_\Delta[0]$$

viele $(\underline{e}, y) \in [\![0, \Delta]\!]^k \times ([-\Delta, 0] \cap \frac{1}{3}\mathbb{Z})$ können $(\underline{v}, -\ln|\alpha|)$ ergeben. Asymptotisch können wir daher von einer zufällig und gleichverteilten Wahl der Relationen reden.

Wir fassen die Relationengenerierung zusammen: Mit Hilfe von *RELATION* haben wir einen Algorithmus vom Las-Vegas-Typ, der etwa zufällig und gleichverteilt erweiterte Relationen liefert. Mit *RELATION* versuchen wir das erweiterte Relationengitter Γ_C zu erzeugen, um im Anschluß daran seine Determinante zu berechnen.

5.4 Die Berechnung der Determinante des Relationengitters

Wir beginnen mit einer allgemeinen Untersuchung zur Erzeugung von Γ_C. Daraus leiten wir die Anzahl der Iterationen von *RELATION* her, nach der wir erwarten dürfen, daß das aufgespannte Teilgitter gleich Γ_C ist. Ferner können wir mit Hilfe eines Tricks garantieren, daß dieses Teilgitter vollen Rang hat. Danach stellen wir eine Methode zur Berechnung der Determinante vor.

5.4.1 Die Erzeugung des Relationengitters

Wir leiten ein allgemeines Resultat zur Erzeugung von Γ_C her. Daraus folgt eine untere Schranke für die Wahrscheinlichkeit, daß das in (2) von *RELATION* berechnete reduzierte Ideal B über der Fakorbasis zerlegbar ist. Darauf aufbauend werden wir unsere Strategie zur Erzeugung von Γ_C vorstellen.

Theoretische Vorüberlegungen

Wir übertragen die Ideen aus [Bu1] von beliebigen Zahlkörpern auf reellquadratische Ordnungen. Wie dort beginnen wir mit der Beschreibung von $(k+1)$-dimensionalen „Würfeln“ $\mathcal{W}_-, \mathcal{W}_+$, in denen die mit *RELATION* erzeugten Relationen liegen. Zuerst suchen wir $\mathcal{W}_+$, der alle mit *RELATION* erzeugten Relationen $(\underline{v}, -\ln|\alpha|)$ enthält. Gemäß Bemerkung 5.74 gilt $\underline{v} = \underline{e} - \underline{z}$ und $0 \leq z_i \leq \log\sqrt{\Delta}$. Im Beweis von Lemma 5.69 erhalten wir für den Standort $\ln|\alpha|$ des gewählten Ideals eine maximale Abweichung von y um $(5+1/2)\ln\sqrt{\Delta}$ nach links und $(4+1/2)\ln\sqrt{\Delta}$ nach rechts.

$$\mathcal{W}_+ = [-\log\sqrt{\Delta}, \Delta]^k \times [-(4+1/2)\ln\sqrt{\Delta}, \Delta + (5+1/2)\ln\sqrt{\Delta}] \tag{5.36}$$

enthält dann alle Relationen $(\underline{v}, -\ln|\alpha|)$ aus *RELATION* . Ferner suchen wir einen Würfel, der nur Relationen enthält, für die alle Ausgangsvektoren $(\underline{e} = \underline{v} + \underline{z}, y)$ in $[\![0, \Delta]\!]^k \times ([-\Delta, 0] \cap \frac{1}{3}\mathbb{Z})$ liegen. Wir setzen daher:

$$\mathcal{W}_- = [0, \Delta - \log\sqrt{\Delta}]^k \times [(4+1/2)\ln\sqrt{\Delta}, \Delta - (5+1/2)\ln\sqrt{\Delta}]. \tag{5.37}$$

Daraus folgern wir direkt: (vgl. Bemerkung 5.74)

5.75 Korollar *i) Sei $(\underline{v}, -\ln|\alpha|) \in \Gamma_C \cap \mathcal{W}_-$. Dann ist $\sharp\mathcal{Z} \cdot L_\Delta[0]$ die Anzahl N_{rel} der Wahlmöglichkeiten für $(\underline{e}, y) \in [\![0, \Delta]\!]^k \times ([-\Delta, 0] \cap \frac{1}{3}\mathbb{Z})$, die mittels RELATION und M_y $(\underline{v}, -\ln|\alpha|)$ liefern können, d.h. $N_{rel} = \sharp\mathcal{Z} \cdot L_\Delta[0]$.*
ii) Liegt eine erweiterte Relation nicht in $\mathcal{W}_+$, dann gibt es in $[\![0, \Delta]\!]^k \times ([-\Delta, 0] \cap \frac{1}{3}\mathbb{Z})$ keine Elemente, die diese Relation mit RELATION berechnen, d.h. $N_{rel} = 0$.
iii) Liegt die Relation in $\mathcal{W}_+$, so ist $N_{rel} \leq \sharp\mathcal{Z} \cdot L_\Delta[0]$.

Wir schätzen nun ab, wie viele Iterationen von *RELATION* wir ausführen müssen, um Γ_C zu erzeugen. Seien $(\underline{e}_1, -\ln|\alpha_1|), \ldots, (\underline{e}_j, -\ln|\alpha_j|)$ bereits gefundene Relationen. Für $j = 0$ haben wir noch keine gefunden. Mit Γ_j bezeichnen wir das von diesen Relationen aufgespannte Teilgitter von Γ_C,

$$\Gamma_j = \mathbb{Z}(\underline{e}_1, -\ln|\alpha_1|) + \ldots + \mathbb{Z}(\underline{e}_j, -\ln|\alpha_j|),$$

und mit d_j seine Dimension. Falls $d_j = k+1$, d.h. Γ_j hat volle Dimension, dann führen wir den Index I_j von Γ_j in Γ_C ein, d.h.

$$I_j = [\Gamma_C : \Gamma_j].$$

I_j kann als Maß für die Abweichung des Teilgitters Γ_j vom zu erreichenden Gitter Γ_C interpretiert werden.

Wir schätzen die Wahrscheinlichkeit p_{j+1} ab, daß wir eine Relation $(\underline{e}_{j+1}, -\ln|\alpha_{j+1}|) \in \Gamma_C - \Gamma_j$ finden, d.h. daß wir Γ_j ergänzen.

Dazu betrachten wir wieder die beiden Würfel. Mit ihnen läßt sich p_{j+1} nach unten abschätzen. Wir führen dazu ein:

$$N_1 = \sharp(\Gamma_j \cap \mathcal{W}_+) \qquad \text{und} \qquad N_2 = \sharp(\Gamma_C \cap \mathcal{W}_-).$$

Damit erhalten wir

$$p_{j+1} \geq \frac{N_{rel}}{6(\Delta+1)^k(3\Delta+1)}(N_2 - N_1), \tag{5.38}$$

denn wir wählen jeweils zufällig und gleichverteilt $(\underline{e}, y) \in [\![0, \Delta]\!]^k \times ([-\Delta, 0] \cap \frac{1}{3}\mathbb{Z})$ und anschließend in der 6-elementigen Menge M_y ein Ideal aus. Für jede Relation existieren dann gemäß Korollar 5.75 maximal $N_{rel} = \sharp\mathcal{Z} \cdot L_\Delta[0]$ Wahlmöglickeiten.

Wollen wir eine untere Schranke für p_{j+1}, suchen wir eine untere Schranke für N_2 und eine obere für N_1. Dazu erhalten wir folgende Abschätzungen:

5.76 Lemma *i) Falls $d_j = k+1$ gilt, ergibt sich*

$$N_1 \leq \frac{1}{hRI_j}(\Delta + 6I_j \cdot \sqrt{\Delta} \cdot \ln \Delta)^{k+1}.$$

ii) Falls $d_j < k+1$ ist, sei Γ_{j+1} ein Teilgitter der Dimension $k+1$, das Γ_j als Teilmenge enthält. Dann gilt

$$N_1 \leq \frac{1}{hRI_{j+1}}(\Delta + 6I_{j+1} \cdot \sqrt{\Delta} \cdot \ln \Delta)^{k+1}.$$

Beweis: Wir übertragen die Beweise der Lemmata 3.4 und 3.5 aus [Bu1] auf reellquadratische Ordnungen.
i) Analog zu Lemma 3.4 in [Bu1] beweisen wir, daß Γ_j eine Basis in $[0, I_j \cdot \sqrt{\Delta} \cdot \ln \Delta]^{k+1}$ hat, weil wir $\det \Gamma_j = I_j \cdot hR \leq I_j \cdot \sqrt{\Delta} \cdot \ln \Delta$ gemäß (2.25) wissen. Darauf aufbauend erhalten wir dem Beweis von Lemma 3.5 in [Bu1] folgend die Behauptung.
ii) Dieser Argumentation folgend besitzt Γ_C eine Basis in $[0, \sqrt{\Delta} \cdot \ln \Delta]^{k+1}$, wobei $I_j = 1$ gilt. Demnach finden wir ein Teilgitter Γ_{j+1} der Dimension $k+1$ mit Erzeugenden aus $\mathcal{W}_+$, das Γ_j umfaßt. Dann folgt mit i) die Abschätzung für N_1. ■

Zuletzt wird noch N_2 analog zu Lemma 3.6 in [Bu1] abgeschätzt:

5.77 Lemma *Es gilt $N_2 \geq (\Delta - 6\sqrt{\Delta} \cdot \ln \Delta)^{k+1}/hR$.*

Wir setzen diese Resultate zusammen und schätzen p_{j+1} ab. Ähnlich zu Cor. 3.1 in [Bu1] erhalten wir:

5.78 Korollar *Haben wir in der j-ten Iteration Γ_C noch nicht erzeugt, dann gilt*

$$p_{j+1} \geq \frac{1}{36} \cdot \frac{\sharp\mathcal{Z}}{hR} \cdot L_\Delta[0] \cdot (1 - o(1)).$$

Beweis: Gemäß (5.38) schätzen wir für p_{j+1} den Faktor

$$\frac{N_2 - N_1}{(\Delta+1)^k \cdot (3\Delta+1)} \tag{5.39}$$

ab. N_2 und N_1 sind Potenzen mit Exponenten $k+1$ wie der Nenner auch. Geeignetes Umformen von (5.39) liefert dann, daß er $\geq 1/(2 \cdot 3) \cdot (1 - o(1))$ ist für $\Delta \to \infty$ und $I_j \geq 2$. Anwenden von (5.38) und Korollar 5.75 liefert die Behauptung. ■

Da wir für die weitere Analyse eine besser zu handhabende Abschätzung für p_{j+1} benötigen, ersetzen wir hR und $\sharp\mathcal{Z}$ durch geeignetere Terme.

5.79 Proposition *(GRH) Haben wir in der j-ten Iteration Γ_C noch nicht erzeugt, dann gilt für $12(\ln\Delta)^2 \leq C \leq \sqrt{\Delta}/2$:*

$$p_{j+1} \geq L_\Delta\left[-\frac{1}{4c}\right].$$

Beweis: Für $12(\ln\Delta)^2 \leq C \leq \sqrt{\Delta}/2$ haben wir wegen Korollar 7.23 mit (GRH):

$$\sharp\mathcal{Z} \geq (\sqrt{\Delta}/2)\cdot L_\Delta[-1/(4c)].$$

Aus (2.25) erhalten wir

$$hR < \sqrt{\Delta}/2\cdot(\ln\sqrt{\Delta}+1) = (\sqrt{\Delta}/2)\cdot L_\Delta[0],$$

woraus wir $\sharp\mathcal{Z}/hR \geq L_\Delta[-1/(4c)]$ erhalten. Aus Korollar 5.78 folgt die Behauptung. ∎

Gemäß unserer Festlegung ist p_{j+1} die Wahrscheinlichkeit, daß *RELATION* eine Relation $(\underline{v}, -\ln|\alpha|) \in \Gamma_C - \Gamma_j$ liefert. Dies setzt unter anderem voraus, daß in Schritt (3) der Test auf Zerfall über F_C erfolgreich ist. Insofern wissen wir auch:

5.80 Korollar *(GRH) Sei B ein in (2) von RELATION (etwa zufällig und gleichverteilt) berechnetes Ideal. Falls $12(\ln\Delta)^2 \leq C \leq \sqrt{\Delta}/2$ gilt, dann ist die Wahrscheinlichkeit $p(F_C)$, daß B über F_C zerfällt, $\geq L_\Delta[-1/(4c)]$.*

Jetzt haben wir eine Abschätzung für p_{j+1}, die eine Analyse der Relationengenerierung hinsichtlich der Laufzeitoptimierung erlaubt.

Wir beginnen mit der Erzeugung eines Teilgitters Γ_j voller Dimension. Hierzu bedienen wir uns eines Tricks, um die Laufzeit der Relationengenerierung zu begrenzen und für spätere Anwendungen Dimension $k+1$ garantieren zu können.

Erzeugung eines Teilgitters von Dimension $k+1$

Wir beschreiben diesen Trick mit folgender Skizze:

- Wir wählen wie bisher zufällig und gleichverteilt einen Exponentenvektor $\underline{e} \in_R [\![0,\Delta]\!]^k$ und $y \in_R [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z}$.
- Bei der Berechnung der j-ten Relation wird für $1 \leq j \leq k$ die Koordinate e_j um $2k\Delta$ erhöht, d.h. wir setzen $e_j \leftarrow e_j + 2k\Delta$.
- Bei der Berechnung der $(k+1)$-ten Relation wird y um $2k\Delta$ erhöht, d.h. wir setzen $y \leftarrow y + 2k\Delta$.

- Auf diese Eingabevektoren lassen wir die Schritte (2b) - (5) von *RELATION* wie bisher operieren.

Wir wiederholen diesen Trick, bis wir ein Teilgitter von Γ_C der Dimension $k+1$ erzeugt haben. Die Laufzeit von *RELATION* mit diesen Eingabedaten bleibt asymptotisch unverändert, da die maximalen Werte der Eingabevektoren durch $\Delta \cdot (2k+1) \leq 5\Delta^{3/2}$ beschränkt sind wegen (5.13). Wir „sammeln" die auf diese Weise gewonnenen Relationen im Teilgitter Γ_{k+1}:

5.81 Lemma *Das Teilgitter Γ_{k+1} hat Dimension $k+1$.*

Beweis: Wir haben die Eingabevektoren zur Erzeugung der Relationen so konstruiert, daß die Γ_{k+1} entsprechende Matrix diagonaldominant ist. Dies impliziert, daß die entsprechende Matrix regulär ist, Γ_{k+1} also Dimension $k+1$ hat. ■

5.82 Korollar *Die auf diese Weise erzeugten Relationen sind asymptotisch gesehen zufällig und gleichverteilt.*

Beweis: Sei $1 \leq j \leq k$ eine Relation, deren Eingabevektor auf der j-ten Komponente um $2k\Delta$ erhöht wurde. Dann betrachten wir in (2) von *RELATION* die Idealklasse $[\prod_{i=1}^{k} P_i^{e_i}][P_j^{2k\Delta}]$. Gemäß Korollar 5.20 ist die Wahl der Idealklasse $[\prod_{i=1}^{k} P_i^{e_i}]$ bzgl. $[\![0,\Delta]\!]^k$ zufällig und gleichverteilt. Da die Abbildung $[A] \mapsto [A][P_j^{2k\Delta}]$ bijektiv ist, bleibt die Gleichverteilung erhalten. Die zufällige und gleichverteilte Wahl des reduzierten Ideals in (2) von *RELATION* bleibt davon unberührt.
Sei $j = k+1$, d.h. die (k+1)-te Komponente des Eingabevektors wird um $2k\Delta$ erhöht. Die Wahl der Idealklasse bleibt davon unberührt. Die Wahl des reduzierten Ideals bzgl. eines weiter entfernten Standortes beeinträchtigt die Gleichverteilung nicht, da die Länge $\Delta > R$ des zugrundeliegenden Intervalles $[-\Delta + 2k\Delta, 2k\Delta]$ unverändert bleibt. (vgl. Bemerkung 5.74) ■

Gitterverfeinerung

Wir versuchen nun, das gewonnene Teilgitter der Dimension $k+1$ so zu verfeinern, daß wir schließlich ein Erzeugendensystem für Γ_C finden.

5.83 Satz *(GRH) Seien $\Delta \in \mathcal{D}^+$ und F_C eine Faktorbasis mit $12(\ln \Delta)^2 \leq C \leq \sqrt{\Delta}/2$. Dann kann ein Erzeugendensystem für das Relationengitter Γ_C bestehend aus $2L_\Delta[c]$ Relationen in erwarteter Laufzeit $L_\Delta[2c + 1/4c]$ berechnet werden.*

Beweis: Um ein Teilgitter der Dimension $k+1$ zu erzeugen, bedienen wir uns des beschriebenen Tricks. Da die Gleichverteilung der Relationengenerierung asymptotisch erhalten bleibt, beläuft sich die erwartete Anzahl der Iterationen von *RELATION*, bis wir ein solches Teilgitter der Dimension $k+1$ haben, auf $(k+1) \cdot 1/p(F_C) = L_\Delta[c + 1/(4c)]$. (vgl. Korollar 5.80)
Dann hat das Teilgitter Γ_{k+1} Dimension $k+1$, und wir schätzen seinen Index in Γ_C

nach oben ab. Wir wissen $[\Gamma_C : \Gamma_{k+1}] = \det\Gamma_{k+1}/\det\Gamma_C$. Dabei ist $\det\Gamma_C = hR > \ln 2/2$ (vgl. Satz 2.69). Für eine obere Schranke von $\det\Gamma_{k+1}$ wenden wir die Ungleichung von Hadamard in (3.2) an. Der betragsgrößte Eintrag in der zugehörigen Matrix ist beschränkt durch $\Delta + 2k\Delta + (5+1/2)\ln\sqrt{\Delta} \leq \Delta\cdot(7+2k)$ (vgl. 5.36):

$$\begin{aligned}
\det\Gamma_{k+1} &\leq (\sqrt{k+1}\cdot\Delta\cdot(7+2k))^{k+1}\\
&\leq (k+1)^{(k+1)/2}\cdot(11\Delta^{3/2})^{k+1}\\
&= \exp((k+1)\cdot(\ln(k+1)+3\ln(11\Delta))/2)\\
&= \exp(L_\Delta[c]),
\end{aligned}$$

wobei wir $k/2 \leq C = L_\Delta{}^c \leq \sqrt{\Delta}$ aus (5.13) anwenden. Dann müssen wir für $[\Gamma_C : \Gamma_{k+1}] \leq \exp(L_\Delta[c])$ maximal $L_\Delta[c]$ Relationen finden, die jeweils eine Gitterverfeinerung ergeben. Die erwartete Anzahl der Iterationen von *RELATION* beläuft sich wegen $p_{j+1} \geq L_\Delta[-1/(4c)]$ auf $L_\Delta[c+1/(4c)]$. (vgl. Proposition 5.79)
Je Aufruf von *RELATION* benötigen wir gemäß Satz 5.67 Zeit $L_\Delta[c]$, so daß wir insgesamt Zeit $L_\Delta[2c+1/(4c)]$ brauchen. ■

Mit statistischen Methoden (vgl. [HeFe]) erhalten wir:

5.84 Korollar *(GRH) In der Situation von Satz 5.83 erhalten wir mit Hilfe des beschriebenen Tricks nach $4L_\Delta[c+1/(4c)]$ Iterationen von RELATION ein Erzeugendensystem für Γ_C mit einer Wahrscheinlichkeit $\geq 1/2$.*

Die Menge der auf diese Weise gewonnenen Relationen spannt ein $(k+1)$-dimensionales Teilgitter auf, das mit einer Wahrscheinlichkeit $\geq 1/2$ gleich Γ_C ist. Ehe wir uns der „Weiterverarbeitung“ des Erzeugendensystems zuwenden, vereinbaren wir folgende abkürzende Schreibweise:

Γ bezeichne das nach den Aufrufen von *RELATION* aufgespannte $(k+1)$-dimensionale Teilgitter von Γ_C. Wir erwarten, daß es aus

$$N = L_\Delta[c] = 4L_\Delta[c] \tag{5.40}$$

Relationen besteht. Streichen wir in den Gittervektoren von Γ die reelle $(k+1)$-te Koordinate, erhalten wir ein k-dimensionales Teilgitter Γ' von Γ'_C. Die Erzeugendensysteme beider Teilgitter stellen wir mittels Matrixschreibweise dar. Die entsprechenden Matrizen bezeichnen wir mit M bzgl. Γ und M' bzgl. Γ' und nennen sie auch *Relationenmatrizen*. Wie bereits im Beweis von Satz 5.83 gesehen lassen sich ihre Einträge beschränken:

5.85 Korollar *Die Beträge der Einträge der Relationenmatrizen sind durch $|M| \leq \Delta\cdot(7+2k) = O(\Delta^{3/2})$ beschränkt.*

Um die Klassenzahl und den Regulator von $\mathcal{O}_\Delta$ zu bestimmen, berechnen wir nun die Determinanten der aufgespannten Teilgitter, die Vielfache von $\det\Gamma'_C$ bzw. $\det\Gamma_C$ sind. Stimmen sie mit denen der Relationengitter überein, sind die jeweiligen Gitter identisch. Wir haben also die Klassenzahl und den Regulator von $\mathcal{O}_\Delta$ gefunden. (vgl. Korollar 3.6)

5.4.2 Die Berechnung der Determinante eines Teilgitters von Γ_C

In Kapitel 3, Abschnitt 3.4 stellen wir eine Methode vor, mit der wir aus einem Erzeugendensystem für $\Gamma \leq \mathbb{Z}^k \times \mathbb{R}$ eine Basis konstruieren können. Diese wenden wir nicht direkt an, wie folgende Argumente nahelegen:

- Gemäß Satz 3.22 enthält bereits der von der Anzahl der Erzeugenden N und der Dimension $k+1$ des Gitters dominierte Faktor $(k+1+N)^6 \cdot N^3 = L_\Delta[9c]$ in der Laufzeit eine neunte Potenz von $L_\Delta[c]$, was eine nicht unerhebliche Gesamtlaufzeit nachsichzieht.
- Wollen wir im Anschluß an die Klassenzahlberechnung, wie in Kapitel 4, Algorithmus *HITEST* skizziert, Hauptidealtests auf der Grundlage der Basis von Γ_C ausführen, ist es sinnvoll, dünn besetzte Basisvektoren bzw. solche von kleiner euklidischer Norm zu haben. Insbesondere erweisen sich hierzu bei den entsprechenden Matrizen Dreiecksformen als günstig.

Wir werden einen Lösungsweg beschreiten, der in erheblich geringerer Laufzeit zum Ziel führt. Im ursprünglich für Zahlkörper konzipierten Algorithmus *CLASSREG* berechnen wir die Klassenzahl aus $\det \Gamma'_C$ *nach* der Schleife, wenn wir wissen, daß das Relationengitter tatsächlich erzeugt wird. (vgl. (6) von *CLASSREG*) Wir ziehen diese Berechnung vor, indem wir *zuerst* die Determinante des Teilgitters $\Gamma' \leq \mathbb{Z}^k$ von Γ'_C bestimmen. Dies geschieht durch Berechnung der Hermite-Normalform der Relationenmatrix M' und ihrer Transformationsmatrix T. *Danach* wenden wir auf ein modifiziertes Erzeugendensystem für $\Gamma \leq \Gamma_C$ die erwähnte Methode zur Herstellung von Basen in reellen Gittern aus Kapitel 3 an. Wir haben somit die Aufgabe in zwei Teilaufgaben aufgespaltet.

Die Korrektheit der Aufspaltung

Wir untersuchen den Aufbau der Matrix M genauer, die Spalten der Matrizen sind Relationen. Die Definition des Relationengitters ergibt dann für M:

$$M = \begin{pmatrix} v_{1,1} & \ldots & v_{1,k} & \ldots & v_{1,N} \\ \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots \\ v_{k,1} & \ldots & v_{k,k} & \ldots & v_{k,N} \\ -\ln|\alpha_1| & \ldots & -\ln|\alpha_k| & \ldots & -\ln|\alpha_N| \end{pmatrix} \tag{5.41}$$

Für die Spalten $\underline{m}_j$ von M erhalten wir:

$$\underline{m}_j = (v_{1,j}, \ldots, v_{k,j}, -\ln|\alpha_j|)^t \in \mathbb{Z}^k \times \mathbb{R}, \tag{5.42}$$

wobei $(1/\alpha_j)\mathcal{O}_\Delta = \prod_{i=1}^k P_i^{m_{i,j}}$ und $m_{k+1,j} = -\ln|\alpha_j|$ gelten.

Die Berechnung der Hermite-Normalform von $M' \in \mathbb{Z}^{k \times N}$ verändert die ersten k Zeilen von M, vernachlässigt jedoch die $(k+1)$-te reelle Zeile. Wir haben daher kein Erzeugendensystem für Γ mehr. Dieses Problem läßt sich einfach lösen:

5.86 Korollar *Sei T die Transformationsmatrix aus der Bestimmung der Hermite-Normalform von M'. Dann ist MT ein Erzeugendensystem von Γ.*

Beweis: Mit Satz 3.10 wissen wir $T \in GL(N)$. Daher spannen die Matrizen M und MT das Gitter Γ auf. (vgl. Proposition 3.5) ∎

Die Hermite-Normalform $HNF(M') = (h_{i,j})$ von M' hat definitionsgemäß obere Dreiecksform. Dies spiegelt sich entsprechend im transformierten Erzeugendensystem $H := MT$ für Γ wider:

$$H = \left(\begin{array}{ccc|ccc} h_{1,1} & \dots & h_{1,k} & 0 & \dots & 0 \\ 0 & \ddots & h_{i.k} & 0 & \vdots & 0 \\ 0 & 0 & h_{k,k} & 0 & \dots & 0 \\ \hline h_{k+1,1} & \dots & h_{k+1,k} & h_{k+1,k+1} & \dots & h_{k+1,N} \end{array}\right), \tag{5.43}$$

wobei wir für die reellen Einträge der letzten Zeile von H und $T = (t_{i,j})$ wissen:

$$h_{k+1,j} = -\sum_{i=1}^{N} \ln|\alpha_i| \cdot t_{i,j} = \ln\left|\prod_{i=1}^{N} \alpha_i^{-t_{i,j}}\right| \tag{5.44}$$

und $(\prod_{i=1}^{N} \alpha_i^{-t_{i,j}})\mathcal{O}_\Delta = \prod_{i=1}^{k} P_i^{h_{i,j}}$, was aus der Definition von Γ_C resultiert. In (5.43) gilt $\det\Gamma = |\det\Gamma(H)|$. Ferner folgern wir aus der Konstruktion von H:

$$\det\Gamma = \prod_{i=1}^{k} h_{i,i} \cdot |\det\left(\mathbb{Z}h_{k+1,k+1} + \ldots + \mathbb{Z}h_{k+1,N}\right)|. \tag{5.45}$$

Zunächst bestimmen wir die Hermite-Normalform von M', woraus wir direkt $\prod_{i=1}^{k} h_{i,i}$ erhalten. (vgl. Korollar 3.9) Auf die Berechnung der Determinante des von $h_{k+1,k+1}$ $\ldots, h_{k+1,N}$ aufgespannten Gitters kommen wir anschließend zurück.

Die Bestimmung der Hermite-Normalform von M'

Wir übernehmen die Resultate von Ac. Müller und J. Buchmann aus [BuMü].

5.87 Satz *Für die Relationenmatrix $M' \in \mathbb{Z}^{k\times N}$ erfordert die Bestimmung der Hermite-Normalform $HNF(M')$ und ihrer Transformationsmatrix T erwartete Zeit $L_\Delta[5c]$.*

Beweis: Anwenden der Sätze 3.12 sowie 3.13 und Korollar 5.85 für den maximalen Eintrag $|M'|$ in $M' \in \mathbb{Z}^{k\times N}$ liefern für die Berechnung von $HNF(M')$ Zeit

$$\begin{aligned} O(k^2N \cdot (k^2+N) \cdot (\log k|M'|)^2) &= L_\Delta[3c] \cdot L_\Delta[2c] \cdot O((\log\Delta)^2) \\ &= L_\Delta[5c], \end{aligned}$$

wobei wir $N = L_\Delta[c]$ gemäß (5.40) erwarten und $k = O(\sqrt{\Delta})$ gemäß (5.13) anwenden. Analog argumentieren wir für die Laufzeit der Transformationsmatrix T mit Satz 3.13. ∎

Analog zu diesem Beweis schätzen wir den maximalen Eintrag der Transformationsmatrix T mit Hilfe von Satz 3.13 und Korollar 5.85 ab:

5.88 Korollar *Für den maximalen Eintrag* $|T|$ *der Transformationsmatrix bzgl. der Hermite-Normalform von* M' *gilt:* $|T| \le (N-k+1) \cdot k^{k+k/2+2} \cdot \Delta^{k+1} \cdot 9^{k+1}$.

Beweis: Wir rechnen die in Satz 3.13 angegebene Schranke für $|T|$ bzgl. M' aus, wobei wir für $H^{\square} = (\sqrt{k} \cdot |M'|)^k$ aus der Hadamard-Schranke in 3.2 herleiten. Dies liefert dann $|T| \le (N-k+1) \cdot k^{k/2+1} \cdot |M'|^{k+1}$. Einsetzen von $|M'| \le \Delta \cdot (7+2k) \le 9k\Delta$ ergibt die Behauptung. (vgl. Korollar 5.85) ∎

Der Aufspaltung der Determinante des Teilgitters Γ in (5.45) folgend berechnen wir $\prod_{i=1}^{k} h_{i,i} = \det \Gamma'$:

5.89 Korollar *Für die Relationenmatrix* $M' \in \mathbb{Z}^{k \times N}$ *kann die Determinante* $\det \Gamma'$ *des von* M' *aufgespannten Gitters* Γ' *in erwarteter Zeit* $L_\Delta[5c]$ *berechnet werden.*

Beweis: Wir erhalten $\prod_{i=1}^{k} h_{i,i}$ aus den Diagonaleinträgen von $HNF(M')$ (vgl. Korollar 3.9), die gemäß obigem Satz in erwarteter Zeit $L_\Delta[5c]$ berechnet wird.
Für die anschließende Produktbildung schätzen wir die Größe der $h_{i,i}$ durch

$$\begin{aligned} h_{i,i} &\le \det HNF(M') = \det \Gamma' \\ &\le (\sqrt{k} \cdot O(\Delta^{3/2}))^k \\ &= O(k^{k/2} \cdot \Delta^{3k/2}) \end{aligned}$$

mit der Hadamard-Schranke aus (3.2) und Korollar 5.85 ab. Da wir für $\prod_{i=1}^{k} h_{i,i}$ dann $k-1$ Produkte berechnen, benötigen wir Zeit $(k-1) \cdot O(k^2 \cdot (\log k + \log \Delta)^2) = L_\Delta[3c]$ ∎

Unserer Überlegung in (5.45) folgend verbleibt noch die

Bestimmung von $\det(\mathbb{Z}h_{k+1,k+1} + \ldots + \mathbb{Z}h_{k+1,N})$.

Dieses eindimensionale Gitter in $\mathbb{R}$ hat $\{h_{k+1,k+1}, \ldots, h_{k+1,N}\}$ als Erzeugendensystem, wozu wir die in Kapitel 3 vorgestellte Methode von J. Buchmann und V. Kessler heranziehen. Wenden wir das Verfahren auf das $(N-k)$-elementige Erzeugendensystem an, erhalten wir wiederum für den von Dimension und Anzahl der Erzeugenden dominierten Term in der Laufzeit von Satz 3.22 $L_\Delta[9c]$.

Daher schlagen wir eine iterierte Anwendung dieser Methode vor, mit dem Ziel, die Laufzeit von $L_\Delta[5c]$ (vgl. Satz 5.87) nicht zu übersteigen. Wir teilen das $(N-k)$-elementige Erzeugendensystem in Teilmengen auf, worauf wir jeweils das erwähnte Verfahren anwenden. Wir präsentieren zunächst die Idee in algorithmischer Form, um sie zu skizzieren. In der anschließenden Analyse klären wir die Detailfragen.

Zur Vereinfachung der Schreibweise verzichten wir hier auf den Index der $(k+1)$-ten Zeile in den Erzeugenden $h_{k+1,j}$, d.h. wir schreiben

$$h_{k+1,j} := h_j, \qquad 1 \le j \le N.$$

5.90 Algorithmus ESTOBAS (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$, $k \in \mathbb{N}$ die Ordnung der zugrundeliegenden Faktorbasis, $N \in \mathbb{N}$ die Anzahl der Spalten der Relationenmatrix, $T = (t_{i,j}) \in GL(N)$ Transformationsmatrix aus der Hermite-Normalform, $|T|$ und $|M| \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_N$ in komprimierter Darstellung

Ausgabe: $\hat{h}_{k+1} \in \mathbb{Q}$, Approximation eines Erzeugenden von $\mathbb{Z}h_{k+1} + \ldots + \mathbb{Z}h_N$ vgl. (5.45)

/* Bestimme die notwendige Präzision n für die Methode in [BuKe]. */ $n \leftarrow \min\{n \in \mathbb{N} \mid n \text{ genügt } (3.8)\}$	(1)
$l \leftarrow \lceil (N-k)^{1/8} \rceil$ /* Größe der jeweiligen Teilsysteme */	(2)
$z \leftarrow 2^{(N-k+1)/2+n+1} \cdot N \cdot \lvert T \rvert \cdot \lceil \lvert M \rvert \rceil$ /* vgl. (3.10) */	(3)
/* Bestimme die notwendige Präzision n_0 für die Approx. der $\ln \lvert \alpha_i \rvert$. */ $n_0 \leftarrow \min\{n_0 \in \mathbb{N} \mid n_0 > 4 + n + \log N + \log \lvert T \rvert + 8(\log l + \log z) + \log(\sqrt{\Delta} \log \Delta)\}$	(4)
/* Bestimme Approximationen $\hat{h}_i$ der $h_{k+1}, \ldots, h_N$. */	(5)
FOR $j \leftarrow 1$ *TO* N	(6)
$\hat{a}_j \leftarrow appr(\ln \lvert \alpha_j \rvert, n_0)$	(7)
FOR $j \leftarrow k+1$ *TO* N	(8)
$\hat{h}_j \leftarrow \sum_{i=1}^{N} \hat{a}_i \cdot t_{i,j}$ /* Approximationen der h_j, vgl. (5.44). */	(9)
/* Konstruiere aus dem Erzeugendensystem eine Basis. */	(10)
$N_k \leftarrow N - k$ /* aktuelle Anzahl der Erzeugenden */	(11)
WHILE $N_k > 1$	(12)
Fülle eventuell einige $\hat{h}_i \leftarrow 0$ auf für $i > N$.	(13)
FOR $i \leftarrow 1$ *TO* N_k	(14)
Für das Erzeugendensystem $\{\hat{h}_{k+i}, \ldots, \hat{h}_{k+i+l-1}\}$ bestimme ein Basiselement inklusive seiner Darstellung $\underline{z} = (z_{k+i}, \ldots, z_{k+i+l-1}) \in \mathbb{Z}^l$ gemäß der Methode in [BuKe] basierend auf Approximationen der Präzision n. Setze das Basiselement auf $\hat{h}_{k+(i+l-1)/l}$, und bestimme die Approximation $\hat{h}_{k+(i+l-1)/l} \leftarrow \sum_{j=0}^{l-1} z_{k+i+j} \cdot \hat{h}_{k+i+j}$.	(15)
$i \leftarrow i + l$	(16)
$N_k \leftarrow \lceil N_k / l \rceil$ /* $\{h_{k+1}, \ldots, h_{k+N_k}\}$ erzeugt das gleiche Gitter. */	(17)

Als Eingabe für das Verfahren in [BuKe] nehmen wir Approximationen der Präzision n, um die angegebenen Laufzeiten und Größenbeschränkungen aus den Sätzen 3.21 und 3.22 übernehmen zu können sowie unnötiges Größenwachstum der Darstellungsvektoren $\underline{z}$ zu vermeiden. Die Präzisionen für die $\hat{h}_j$ nehmen im Laufe der Iterationen ab, bleiben aber stets $\geq n$. Benötigen wir welche der Präzision n, „schneiden" wir von den vorhandenen entsprechende Approximationen ab.

Wir starten auf dem $N_k = (N-k)$-elementigen Erzeugendensystem und führen wegen (2) und (17) die while-Schleife maximal 8-mal aus. In den nachfolgenden Untersuchungen kennzeichnen wir die jeweils berechneten Größen der m-ten Iteration mit einem zusätzlichen Index m, wie z.B. $N_{k,m}$. Für die Präzision der Zwischenergebnisse erhalten wir dann:

5.91 Lemma *Nach jeder Iteration,* $0 \leq m \leq 8$, *der while-Schleife von ESTOBAS ist die Menge* $\{h_{k+1,m}, \ldots, h_{k+N_k,m}\}$ *ein Erzeugendensystem von* $\mathbb{Z}h_{k+1} + \ldots + \mathbb{Z}h_N$*, und die berechneten Approximationen* $\hat{h}_{i,m}$ *von* $h_{i,m}$ *haben Präzision* $4 + n + (8 - m) \cdot (\log l + \log z) + \log(\sqrt{\Delta} \log \Delta)$.

Beweis: Mit $m = 0$ bezeichnen wir die Situation vor Betreten der while-Schleife. Zu überprüfen ist die Präzisionsaussage: Wegen (5.44) und den Approximationen der $\ln |\alpha_i|$ der Präzision n_0 wissen wir für alle $k+1 \leq i \leq N$

$$|h_{i,0} - \hat{h}_{i,0}| \leq N \cdot |T| \cdot 2^{-n_0} < 2^{-8(\log l + \log z) - \log(\sqrt{\Delta}\log\Delta) - n - 4}$$

wegen der Festlegung von n_0 in (4) von *ESTOBAS* .
Für die nachfolgenden Iterationen leiten wir mit Satz 3.21 her: Aus den maximal 1-dimensionalen l-elementigen Erzeugendensystemen $\{h_{k+i,j-1}, \ldots, h_{k+i+l,j-1}\}$ und Präzisionskonstante n erhalten wir jeweils ein Basiselement bzw. einen Darstellungsvektor $\underline{z} \in \mathbb{Z}^l$, wenn wir für die Erzeuger Approximationen der Präzision n zugrundelegen. Dann erzeugen diese Elemente, $h_{k+1,m}, \ldots, h_{k+N_k,m}$, ebenfalls das Gitter $\mathbb{Z}h_{k+1} + \ldots + \mathbb{Z}h_N$. Für sie berechnen wir die Approximationen $\hat{h}_{k+i,m}$, $1 \leq i \leq N_k$,

$$\begin{aligned} |h_{k+i,m} - \hat{h}_{k+i,m}| &\leq \sum_{j=0}^{l-1} |z_{k+i+j}| \cdot |h_{k+i+j,m-1} - \hat{h}_{k+i+j,m-1}| \\ &< l \cdot z \cdot 2^{-(8-(m-1))\cdot(\log l + \log z) - \log(\sqrt{\Delta}\log\Delta) - n - 4} \\ &= 2^{-(8-m)\cdot(\log l + \log z) - \log(\sqrt{\Delta}\log\Delta) - n - 4}, \end{aligned}$$

wobei wir für den Darstellungsvektor $\underline{z} \in \mathbb{Z}^l$ die maximale Koordinate $|z_{k+i+j}| \leq \|z\|$ abschätzen. Anwenden von (3.6) auf (3.10) liefert uns

$$\|z\| \leq 2^{(N-k-1)/2+n+1} \cdot N \cdot |T| \cdot \lceil |M| \rceil = z$$

in jeder Iteration der Schleife: Bei der ersten Iteration lassen sich alle Erzeugenden h_i betragsmäßig durch z beschränken. Für alle weiteren ergeben sich die Erzeugenden aus Basiselementen l-elementiger Teilmengen in 1-dimensionalen Gittern, so daß ihre Längen nicht zunehmen. ∎

Zu klären bleibt noch, wie wir die Approximationen der $\ln|\alpha|$ in (7) von *ESTOBAS* bestimmen, wobei $|\alpha|$ in komprimierter Darstellung vorliegt. (vgl. Bemerkung 5.23) Aus der Relationengenerierung wissen wir

$$\alpha = \alpha_0 \circ \kappa \circ \gamma \quad \Longrightarrow \quad \ln|\alpha| = \ln|\alpha_0| + \ln|\kappa| + \ln|\gamma|,$$

vgl. *RELATION*, Schritt (2b) in Algorithmus 5.66. Im Laufe der Entwicklung der Relationengenerierung haben wir auch den Aufbau der Faktoren α_0, κ, γ dargelegt: Die Korollare 5.29, 5.33 zeigen eine Produktdarstellung für α_0, Korollar 5.41 eine Produktdarstellung von κ und Korollar 5.52 analog für γ. Daraus folgt eine Summendarstellung für die Logarithmen der einzelnen Faktoren. Um in *ESTOBAS* für die Approximationen der $\ln|\alpha|$ Präzision n_0 zu erhalten, untersuchen wir die dazu notwendigen Präzisionen der approximierten Teilsummanden. Insbesondere wissen wir $n_0 = L_\Delta[c]$. (vgl. (4) in *ESTOBAS* und Korollar 5.88)

5.92 Lemma *Für alle während der Relationengenerierung mit RELATION bestimmten $\alpha = \alpha_0 \circ \kappa \circ \gamma$ müssen für die Teilfaktoren von α_0, κ, γ jeweils Approximationen der Präzision $O(n_0) = L_\Delta[c]$ bestimmt werden, um für $\ln|\alpha|$ eine Approximation der Präzision n_0 zu erhalten.*

Beweis: Ausgehend von einem α aus der Relationengenerierung wenden wir uns den Teilfaktoren α_0, κ, γ zu, wobei wir uns vorerst auf γ zurückziehen.
Aus Korollar 5.52 wissen wir, daß $\ln|\gamma|$ aus $1 + l' + l'' = O(\log\Delta)$ Summanden besteht. Daraus ergeben sich die jeweils notwendigen Präzisionen der Approximationen der Teilsummanden zu $O(n_0)$.
Analoges ergibt sich für die Präzisionen bzgl. $\ln|\alpha_0|$ und $\ln|\kappa|$. (vgl. Korollare 5.29, 5.33 und 5.41) Dabei bleibt der eingeführte Trick, die Erhöhung einer der Koordinaten des Eingabevektors für *RELATION* um $2k\Delta$, ohne Auswirkung auf die Größenordnung $O(n_0)$ der Präzision. ∎

Daraus leiten wir dann für die Laufzeit für *ESTOBAS* her:

5.93 Proposition *Bei Eingabe von $\Delta \in \mathcal{D}^+$, der Ordnung k der zugrundeliegenden Faktorbasis, der Anzahl N der Spalten der Relationenmatrix M, deren maximalem Eintrag $|M|$ und der Transformationsmatrix T aus $HNF(M)$ sowie $|T|$ und $\alpha_1, \dots \alpha_N$ in komprimierter Darstellung berechnet ESTOBAS eine approximierte Determinante des Gitters $\mathbb{Z}h_{k+1} + \ldots + \mathbb{Z}h_N$ der Präzision $4 + n + \log(\sqrt{\Delta}\log\Delta)$ in erwarteter Laufzeit $L_\Delta[5c]$.*

Beweis: Wir analysieren *ESTOBAS* schrittweise: In (1) ergibt sich die Präzision n für das Verfahren in [BuKe] zu $\lceil \log(\sqrt{N-k}+2) + \log\nabla + (N-k-3)/2 - \log\lambda \rceil$ gemäß (3.8). Für λ leiten wir aus (3.4) $\lambda \geq R \geq 1/3$ her. (vgl. (2.25)) Mit (3.7) schätzen wir ∇ nach oben durch $((N-k)/2 + \sqrt{N-k}) \cdot 3\nu$ ab. Daraus errechnen wir Präzision n der Größenordnung $O(N + \log\nu) = L_\Delta[c]$, wobei wir $\nu \leq N \cdot |M| \cdot |T|$ aus (3.5) einsetzen. (vgl. Korollare 5.85 und 5.88)
In (4) ergibt sich für die Startpräzision n_0 Größenordnung $O(n + \log z) = L_\Delta[c]$.

Die for-Schleife in (6) - (7) ermittelt Approximationen für die $\ln|\alpha_i|$ der Präzision n_0. Mit Lemma 5.92 müssen die jeweiligen Teilsummanden mit Präzisionen der Größenordnung $O(n_0) = L_\Delta[c]$ approximiert werden. Je $\ln|\alpha_i|$ haben wir $O(k \cdot (\log\Delta)^2) = L_\Delta[c]$ viele Teilsummanden der Größe $O((\log\Delta)^2)$. (vgl. Aufspaltung der α_0, κ, γ in den Korollaren 5.29, 5.33, 5.41 bzw. 5.52) Daher benötigen wir für jede einzelne Approximation der Präzision n_0 Zeit $L_\Delta[c]$ (vgl. [Br]), für alle Teilsummanden eines $\ln|\alpha_i|$ dann Zeit $L_\Delta[2c]$. Da sich die jeweiligen Längen der Approximationen auf $L_\Delta[c]$ belaufen, benötigt die anschließende Summation der Teilsummanden Zeit $L_\Delta[3c]$. Dies gilt für jede der N Approximationen von $\ln|\alpha_i|$, so daß die for-Schleife Zeit $L_\Delta[4c]$ verbraucht.
Die for-Schleife in (8) - (9) berechnet in jeder Iteration $N = L_\Delta[c]$ Produkte von Faktoren der Länge $L_\Delta[c] = \log|T|$ für $t_{i,j}$ sowie $L_\Delta[2c]$ für $\hat{a}_i$, was Zeit $L_\Delta[4c]$ erfordert. Die Summation der Produkte ergibt Zeit $L_\Delta[3c]$. Die Schleife wird $(N-k)$-mal iteriert, so daß sie insgesamt Zeit $L_\Delta[5c]$ verbraucht.
Wir untersuchen die while-Schleife in (12). Die Konstruktion der Basis erfolgt in 8 Iterationen der while-Schleife. Dabei stellen die for-Schleifen die aufwendigsten Operationen dar. In jeder Ausführung der for-Schleife wird aus einem $l = L_\Delta[c/8]$-elementigen Erzeugendensystem ein Basiselement ermittelt, was wegen Satz 3.22 maximal Zeit $O((N-k)^{6/8} \cdot (N-k)^{3/8} \cdot \log(\nu/\lambda)^3) = L_\Delta[c/8 + 4c]$ benötigt. (vgl. $\nu \leq N \cdot |M| \cdot |T|$, $\lambda \geq 1/3$ zu Beginn des Beweises) Die anschließende Bestimmung der neuen Approximationen $\hat{h}_{k+(i+l-1)/l,j}$ erfordert l Produkte von Faktoren der maximalen Länge $L_\Delta[c]$ für z und $L_\Delta[2c]$ für $\hat{h}_{k+i+c,j-1}$. (Es gilt $|\hat{h}_{k+(i+l-1)/l,j}| \leq l^7 \cdot z^7 \cdot N \cdot |\hat{h}_{i,0}|$.) Dann erfordert die Berechnung der $l = L_\Delta[c/8]$ Produkte Zeit $L_\Delta[c/8 + 3c]$. Die anschließende Summation verbraucht Zeit $L_\Delta[c/4 + 2c]$. Jede der $N_k/l = L_\Delta[(7/8)c]$ Iterationen der for-Schleife verbraucht dann maximal Zeit $L_\Delta[c/8 + 4c]$, so daß wir insgesamt Zeit $L_\Delta[5c]$ verbrauchen. ■

Mittels der soeben in *ESTOBAS* berechneten Approximation $\hat{h}_{k+1}$ der Determinante des von $\mathbb{Z}h_{k+1} + \ldots + \mathbb{Z}h_N$ aufgespannten Gitters ermitteln wir eine approximierte Gitterdeterminante des Teilgitters Γ gemäß der Aufspaltung in (5.45).

5.94 Satz *Für die Relationenmatrix $M \in \mathbb{R}^{(k+1)\times N}$ erfordert die approximierte Bestimmung der Determinante des von M aufgespannten Teilgitters Γ von Γ_C erwartete Laufzeit $L_\Delta[5c]$. Insbesondere hat die Approximation Präzision $4 + n + \log(\sqrt{\Delta}\log\Delta) - \log\det\Gamma'$.*

Beweis: Gemäß der Aufspaltung von $\det\Gamma$ in (5.45) folgt die Laufzeit aus Satz 5.87 und Proposition 5.93. Für die Präzision leiten wir her:

$$\begin{aligned} |\det\Gamma - \det\Gamma' \cdot \hat{h}_{k+1}| &\leq \det\Gamma' \cdot |\det(\mathbb{Z}h_{k+1} + \ldots + \mathbb{Z}h_N) - \hat{h}_{k+1}| \\ &< \det\Gamma' \cdot 2^{-4-n-\log(\sqrt{\Delta}\log\Delta)}. \end{aligned}$$ ■

Stimmt Γ bereits mit dem Relationengitter überein, haben wir mit $\det\Gamma'$ die Klassenzahl h von $\mathcal{O}_\Delta$ und mit $\hat{h}_{k+1}$ eine Approximation des Regulators R. Anwenden von (2.25) ermöglicht uns wegen $h < \sqrt{\Delta}\log\Delta$ eine Aussage über die Präzision:

5.95 Korollar *(GRH) Aus den gemäß Korollar 5.84 bestimmten Relationen lassen sich mit einer Wahrscheinlichkeit* $\geq 1/2$ *die Klassenzahl und eine Approximation des Regulators der Präzision* 4 *in erwarteter Laufzeit* $L_\Delta[5c]$ *berechnen.*

Um hier eine relativ gute Approximation für den Regulator garantieren zu können, haben wir wegen der Präzisionsaussage in Satz 5.94 die Startpräzision n_0 in (4) von *ESTOBAS* um $\log(\sqrt{\Delta}\log\Delta)$ erhöht.

5.96 Bemerkung Aus der Basisdarstellung des Erzeugenden des Gitters $\mathbb{Z}h_{k+1} + \ldots + \mathbb{Z}h_N$ in *ESTOBAS* können wir auch eine Produktdarstellung der Grundeinheit gewinnen, falls $\Gamma = \Gamma_C$ gilt. Das Erzeugende, der Regulator, ist eine Linearkombination der $\ln|\alpha_i|$, so daß wir analog zu (5.44) eine Produktdarstellung der Grundeinheit erhalten. Allerdings liegt die Grundeinheit nur in komprimierter Darstellung vor.

Nach Ausführen von *ESTOBAS* haben wir eine Gitterbasis folgender Form:

$$\left(\begin{array}{ccc|cccc} h_{1,1} & \ldots & h_{1,k} & 0 & \ldots & \ldots & 0 \\ 0 & \ddots & h_{i.k} & 0 & \vdots & \vdots & 0 \\ 0 & 0 & h_{k,k} & 0 & \ldots & \ldots & 0 \\ \hline h_{k+1,1} & \ldots & h_{k+1,k} & h_{k+1} & 0 & \ldots & 0 \end{array}\right), \tag{5.46}$$

wobei h_{k+1} das $\hat{h}_{k+1}$ entsprechende Basiselement bezeichnet. Stimmt das Teilgitter Γ mit dem erweiterten Relationengitter Γ_C überein, enthalten die ersten $k+1$ Spalten eine Gitterbasis für Γ_C, und die entsprechende Matrix bezeichnen wir in Analogie zu Kapitel 4, (4.10) mit B_C. Streichen der $(k+1)$-ten Zeile und Spalte von B_C liefert uns die ganzzahlige Matrix B'_C in oberer Dreiecksform, die eine Basis für das Relationengitter Γ'_C liefert.

Mit dieser approximierten Determinante testen wir wie in *CLASSREG* , ob die Abbruchbedingung erfüllt ist, d.h. ob das Teilgitter Γ mit dem Relationengitter Γ_C übereinstimmt.

5.5 Die Überprüfung der Abbruchbedingung

In *CLASSREG* haben wir einen Vergleich der Gitterdeterminante $\det\Gamma$ mit einer bereits berechneten sogenannten Abbruchkonstanten $2H^*$,

$$\det\Gamma < 2H^*,$$

(vgl. auch Abschnitt 5.1). Uns liegen nur Approximationen von $\det\Gamma$ und $2\hat{H}^*$ der Präzision 4 vor. (vgl. Sätze 5.14 und 5.94) Wir wollen einen Vergleich mit der approximierten Gitterdeterminante, der bei positiver Antwort bzgl. der approximierten Determinante eine positive Antwort für $\det\Gamma < 2H^*$ impliziert. Dann wissen wir mit Sicherheit, daß $\Gamma = \Gamma_C$ gilt.

Deshalb vermindern wir im Test die Abbruchkonstante $2H^*$ um den maximal möglichen absoluten Fehler beider Approximationen. Wir testen dann, ob

$$\det\Gamma' \cdot \hat{h}_{k+1} < 2\hat{H}^* - 2^{-4-n-\log(\sqrt{\Delta}\log\Delta)+\log\det\Gamma'} - 2^{-4} \tag{5.47}$$

gilt. Ist diese Bedingung erfüllt, wissen wir mit Sicherheit $\det\Gamma < 2H^*$. Wir haben also $\Gamma = \Gamma_C$.

Die Laufzeit dieses Vergleichs kann hinsichtlich der Laufzeiten für die Bestimmung der approximierten Gitterdeterminante vernachlässigt werden. (vgl. Satz 5.94)

Ist die Abbruchbedingung verletzt, starten wir mit einer neuen Iteration der Schleife, analog zur Schleife in (3) - (5) von *CLASSREG* .

Wir nehmen nun an, wir hätten die Schleife erfolgreich beendet, kennen also Klassenzahl und Regulator und haben $\det\Gamma = \det\Gamma_C$.

5.6 Die Bestimmung der Struktur der Klassengruppe

Wegen der Isomorphie $\mathrm{Cl} \cong \mathbb{Z}^k / \det\Gamma'_C$ und Satz 3.16 erhalten wir die Struktur der Klassengruppe aus den Diagonalelementen der Smith-Normalform bzgl. der Relationenmatrix M'. Für die Laufzeit leiten wir her:

5.97 Satz *Die Struktur der Klassengruppe kann in Zeit $L_\Delta[3c]$ bestimmt werden.*

Beweis: Wir bestimmen die Smith-Normalform bzgl. der Hermite-Normalform von M', die wir bereits kennen. Der maximale Eintrag von $HNF(M')$ ist durch die Klassenzahl $h = O(\sqrt{\Delta}\cdot\ln\Delta)$ beschränkt wegen $|\det HNF(M')| = \det\Gamma'_C = h$. (vgl. Korollar 3.9 und (2.25)). Dann resultiert durch Einsetzen in die Laufzeitschranke von Satz 3.19 die Behauptung. ■

Damit haben wir alle Teilaufgaben des ursprünglich für Zahlkörper konzipierten Algorithmus *CLASSREG* auf reellquadratische Ordnungen übertragen.

5.7 Zusammenfassung

Wir tragen die Resultate der Abschnitte 5.1 - 5.6 in einem speziell für reellquadratische Ordnungen formulierten Algorithmus zusammen. Naheliegend nennen wir ihn *QUCLASSREG* .

5.98 Algorithmus *QUCLASSREG*

Eingabe: $\Delta \in \mathcal{D}^+$, Schranke $C = L_\Delta^c \geq 12 \cdot (\ln \Delta)^2$ mit $C \in \mathbb{N}$
Ausgabe: h, die Klassenzahl, $\hat{h}_{k+1}$, eine Approximation des Regulators R der Präzision 4, $(s_1, \ldots, s_l)$ die Struktur der Klassengruppe Cl und eine Gitterbasis für das Relationengitter Γ_C

/* Berechne eine Abschätzung $2H^*$ mit $H^* < h \cdot R < 2H^*$. */ $2\hat{H}^* \leftarrow$ *INITH** (Δ)	(1)
/* Bestimme eine Faktorbasis F_C und deren Ordnung k. */ $(F_C, k) \leftarrow FAKBAS\ (\Delta, C)$	(2)
Führe $L \in \mathbb{N}$ mit $L = 4L_\Delta[c + 1/(4c)]$ Iterationen von *RELATION* aus. Sei $N \in \mathbb{N}$ die Anzahl der gefundenen Relationen $\underline{v}_1, \ldots, \underline{v}_N$, die ein Gitter der Dimension $k+1$ aufspannen. M bezeichne die entsprechende Relationenmatrix.	(3)
/* Berechne eine Approximation der Determinante des von $\underline{v}_1, \ldots, \underline{v}_N$ aufgespannten Gitters. */ (4a) Bestimme die Hermite-Normalform von M' und ihre Transformationsnmatrix $T \in GL(N)$. Berechne die Determinante von $\det HNF(M') = \prod_{i=1}^k h_{i,i}$. (4b) Bestimme mit *ESTOBAS* aus dem Erzeugendensystem des von der $(k+1)$-ten Zeile der Matrix MT aufgespannten Gitters ein Basiselement und eine Approximation $\hat{h}_{k+1}$. (4c) $d \leftarrow \prod_{i=1}^k h_{i,i} \cdot \hat{h}_{k+1}$ /* approx. Gitterdeterminante */	(4)
UNTIL $d < 2\hat{H}^* - 2^{-4-n-\log(\sqrt{\Delta}\log\Delta)+\log\det\Gamma'} - 2^{-4}$	(5)
/* Berechne die Struktur von Cl. */ $(s_1, \ldots, s_l) \leftarrow SNF(HNF(M'))$ /* Smith-Normalform */	(6)

QUCLASSREG ist ein probabilistischer Algorithmus, was u. a. aus der probabilistischen Wahl der Eingabevektoren für die Relationengenerierung folgt. (vgl. Schritte (1) und (2a) in *RELATION* von Algorithmus 5.66)

Aus *QUCLASSREG* konstruieren wir einen Algorithmus, der die Schleife in (3) - (5) nur einmal iteriert. Wird sie erfolgreich beendet, wissen wir wegen der Konstruktion der Abbruchbedingung mit Sicherheit, daß die Klassenzahl und eine Approximation des Regulators von $\mathcal{O}_\Delta$ bestimmt wurden. Danach wird in (6) die Struktur der Klassengruppe von $\mathcal{O}_\Delta$ berechnet. Dieser Algorithmus ist also vom Typ Las-Vegas. Wir untersuchen seine Laufzeit:

Die Berechnung der Abbruchkonstanten in (1) erfordert polynomielle Laufzeit. (vgl. Satz 5.14) Die Konstruktion einer Faktorbasis in (2) benötigt erwartete Laufzeit $L_\Delta[c]$. (vgl. Satz 5.16) Unter Annahme der verallgemeinerten Riemannschen Vermutung erzeugen in (3) $4L_\Delta[c+1/(4c)]$ Aufrufe von *RELATION* mit einer Wahrscheinlichkeit $\geq 1/2$ das Relationengitter in erwarteter Laufzeit $L_\Delta[2c+1/(4c)]$. (vgl. Satz 5.83 und Korollar 5.84) Die Bestimmung einer Approximation der Determinante des auf diese Weise aufgespannten Gitters braucht gemäß Satz 5.94 erwartete Laufzeit $L_\Delta[5c]$. Die eventuelle Bestimmung der Smith-Normal-Form in (6) verbraucht Zeit $L_\Delta[3c]$. Insgesamt erwarten wir dann Laufzeit

$$\max\{L_\Delta[2c + 1/(4c)], L_\Delta[5c]\}. \tag{5.48}$$

Wir optimieren sie durch Gleichsetzen der Exponenten beider Laufzeiten:

$$2c + 1/(4c) = 5c \quad \Longleftrightarrow \quad 1 = 12c^2 \quad \Longleftrightarrow \quad c = \sqrt{3}/6$$

wegen $c \in \mathbb{R}_{>0}$. Daraus ergibt sich die Gesamtlaufzeit zu $L_\Delta[5c = 5\sqrt{3}/6] = L_\Delta[1,44]$. Die optimale Normschranke C berechnet sich zu $L_\Delta^{\sqrt{3}/6}$. Als zentrales Resultat unserer Untersuchungen erhalten wir schließlich:

5.99 Satz *(GRH) Es existiert ein Las-Vegas-Algorithmus, der bei Eingabe einer Diskriminanten $\Delta \in \mathcal{D}^+$ die Klassenzahl h, eine Approximation des Regulators R der Präzision 4, die Struktur der Klassengruppe Cl und eine Basis des Relationengitters Γ_C für $C = L_\Delta^{\sqrt{3}/6}$ der quadratischen Ordnung $\mathcal{O}_\Delta$ in erwarteter Laufzeit $L_\Delta[1,44]$ berechnet.*

Damit sind auch die Klassenzahlen reellquadratischer Ordnungen in subexponentieller Laufzeit berechenbar. Unser Algorithmus ist (asymptotisch) nur unwesentlich langsamer als jener für imaginärquadratische Ordnungen von J. Hafner und K. McCurley, der $L_\Delta[\sqrt{2}]$ Zeit braucht. Insgesamt haben wir verifiziert, daß sich Klassenzahlen und Strukturen von Klassengruppen quadratischer Ordnungen $\mathcal{O}_\Delta$ in subexponentieller Laufzeit $L_\Delta[1,44]$ berechnen lassen. Die Grundidee beider Verfahren basiert auf der Methode der Relationengenerierung, wir müssen für $\Delta > 0$ zusätzlich berücksichtigen, daß die Klassen von Cl mehrere reduzierte Ideale enthalten können, und eine Approximation des Regulators bestimmen. Ohne diese Approximation können wir nicht sicher sein, daß die berechnete Determinante des Teilgitters Γ' wirklich die Klassenzahl ist.

Wir vergleichen die Exponenten beider Laufzeiten genauer:

$$\frac{5/6\sqrt{3}}{\sqrt{2}} = \sqrt{1 + \frac{1}{24}} \sim 1,02.$$

Daher können wir die Exponenten beider Verfahren als „relativ“ gleich betrachten.

Abschließend wenden wir uns dem von J. Buchmann in [Bu1] skizzierten Verfahren für Zahlkörper $\mathcal{K}$ zu. Bis auf die Bestimmung einer approximierten Gitterdeterminante in Abschnitt 5.4.2 erhält er die gleichen Laufzeiten für die Teilaufgaben. Dort veranschlagt er Zeit $L_\Delta[9c]$, so daß er analog zu (5.48) für die optimale Laufzeit eine Konstante $c = \sqrt{7}/14$ und erwartete Gesamtlaufzeit $L_{\Delta_\mathcal{K}} = [9c = 1,7]$ erhält, wobei $\Delta_\mathcal{K}$ die Determinante des Zahlkörpers $\mathcal{K}$ bezeichnet. Wir vermuten, daß die von uns vorgeschlagene Aufspaltung des Erzeugendensystems zur Bestimmung einer Basis in Abschnitt 5.4 auch für Zahlkörper eine Verbesserung der Laufzeit nachsichzieht. Damit dürfte sich die Gesamtlaufzeit senken.

Kapitel 6

Das Lösen von Normgleichungen in reellquadratischen Zahlkörpern

Wir lösen folgende Aufgabe: Suche zu gegebenem (reell)quadratischem Zahlkörper $\mathbb{Q}(\sqrt{\Delta})$ und $m \in \mathbb{Z}$ alle – bis eventuell auf Assoziierte – ganzen Lösungen $\gamma \in \mathcal{O}_\Delta$ der Norm m, d.h.

$$N(\gamma) = m. \tag{6.1}$$

In Kapitel 4 haben wir allgemein eine Methode zum Lösen von Normgleichungen für beliebige Zahlkörper vorgestellt. (vgl. 4.8) Sie beruht auf Hauptidealtests von ganzen Idealen der Norm $|m|$. (vgl. *NORMEQ* und *HITEST*) Für die Tests wird die explizite Kenntnis einer Gitterbasis des Relationengitters vorausgesetzt. Solch eine Basis wird z.B. während der Klassenzahlberechnung ermittelt. Daher legen wir die entsprechenden Schreibweisen und Notationen aus Kapitel 5 zugrunde.

Am Beispiel reellquadratischer Zahlkörper untersuchen wir die in Kapitel 4 vorgestellte Methode genauer. Für imaginärquadratische Zahlkörper gestaltet sich das Verfahren einfacher. Da in imaginärquadratischen Zahlkörpern $\mathbb{Q}(\sqrt{\Delta})$ jede Idealklasse genau ein reduziertes Ideal enthält (vgl. Satz 2.54) und $\mathcal{O}_\Delta$ reduziert ist, testen wir ein Ideal auf Hauptideal, indem wir es reduzieren und sein Ergebnis überprüfen, ob es mit $\mathcal{O}_\Delta$ übereinstimmt. Das restliche Verfahren kann aus dem für reellquadratische Zahlkörper abgeleitet werden.

Zunächst werden wir spezielle Eigenschaften für Primideale in quadratischen Zahlkörpern vorstellen, die aus der Tatsache folgen, daß die Ganzheitsringe $\mathcal{O}$ quadratischer Zahlkörper Maximalordnungen sind. (vgl. Bemerkung 2.31) Diese Eigenschaften erweisen sich als besonders günstig beim Bestimmen aller ganzen Ideale der Norm $|m|$. Anschließend arbeiten wir die erwähnten Hauptidealtests aus. Dabei übernehmen wir die zentralen Resultate aus der Relationengenerierung für reellquadratische Ordnungen.

Darauf aufbauend analysieren wir den in Kapitel 4 vorgestellten Algorithmus *NORMEQ* für reellquadratische Zahlkörper.

Zur Vereinfachung schließen wir o.B.d.A. $m = 0$ aus, dann ist $\gamma = 0$ ohnehin einzige Lösung. Sonst bezeichnen wir mit

$$m = \pm \prod_{i=1}^{l} p_i^{n_i}$$

für $n_i \in \mathbb{N}$ und $l \in \mathbb{N}_0$ die Primfaktorzerlegung von m.

6.1 Spezielle Eigenschaften quadratischer Zahlkörper

Wir betrachten in diesem Abschnitt beliebige quadratische Zahlkörper $\mathbb{Q}(\sqrt{\Delta})$ mit $\Delta \in \mathcal{D}^+$ und Δ frei von quadratischen Teilern bis auf 1 oder 4. Dann ist $\mathcal{O}_\Delta$ Maximalordnung. (vgl. Bemerkung 2.31) Alle Ideale in $\mathcal{O}_\Delta$ besitzen eine eindeutige Zerlegung in invertierbare Primideale. (vgl. Proposition 2.45 und Satz 2.48)

Zu vorgegebenem $|m|$ existieren höchstens endlich viele ganze Ideale der Norm $|m|$, und wir können die in Kapitel 4 beschriebene Methode zur Konstruktion solcher Ideale anwenden. Sie ist nicht ohne weiteres auf quadratische Ordnungen übertragbar, da i.a. die eindeutige Zerlegung in Primideale verloren geht. (vgl. Lemmata 4.8 und 4.9)

Für die Primideale A_p aus Proposition 2.40 ergeben sich zusätzlich folgende multiplikative Zusammenhänge, wobei wir die Primzahlen p entsprechend ihres Verhaltens charakterisieren. (vgl. (2.4) und Definition 2.17)

6.1 Lemma *Seien $\mathcal{O}_\Delta$ eine Maximalordnung mit $\Delta \in \mathcal{D}$ und $p \in \mathbb{P}$. Dann gelten:*

$$\begin{cases} A_p\overline{A_p} = p\mathcal{O}_\Delta & \text{, } \textit{falls } (\Delta/p) = 1, \textit{ und } p \textit{ heißt zerlegt,} \\ A_p^2 = p\mathcal{O}_\Delta & \text{, } \textit{falls } p \mid \Delta, \textit{ und } p \textit{ heißt verzweigt,} \\ A_p = p\mathcal{O}_\Delta & \text{, } \textit{falls } (\Delta/p) = -1, \textit{ und } p \textit{ heißt träge.} \end{cases}$$

Zum Aufsuchen aller ganzen Ideale der Norm $|m|$ wenden wir Lemma 4.9 an: Dazu ziehen wir die Primfaktorzerlegung von $|m|$ hinzu und die Normen der Primideale A_p. Hinsichtlich der multiplikativen Zusammenhänge gilt für die Normen:

$$\begin{cases} N(A_p) = N(\overline{A_p}) = p & \text{, falls } p \text{ zerlegt,} \\ N(A_p) = p & \text{, falls } p \text{ verzweigt,} \\ N(A_p) = p^2 & \text{, falls } p \text{ träge.} \end{cases} \tag{6.2}$$

Anwenden dieser Sachverhalte ergibt uns direkt die Anzahl aller ganzen Ideale der Norm $|m|$. O.B.d.A. führen wir bzgl. vorgegebenem Δ eine Schreibweise ein, die das Verhalten von $\Delta \bmod 4p$ berücksichtigt.

$$m = \pm \prod_{i=1}^{l_1} p_i^{n_i} \cdot \prod_{i=1}^{l_2} p_i^{n_i} \cdot \prod_{i=1}^{l_3} p_i^{n_i} \tag{6.3}$$

mit den l_1 trägen Primteilern p_i, den l_2 verzweigten Primteilern und l_3 zerlegten Primteilern p_i von m bzgl. Δ.

6.2 Lemma *Seien $\mathcal{O}_\Delta$ Maximalordnung mit $\Delta \in \mathcal{D}$ und $m \in \mathbb{Z}$ mit einer Primfaktorzerlegung gemäß (6.3). Dann existieren entweder keine oder genau*

$$\prod_{i=1}^{l_3}(n_i+1)$$

ganze Ideale der Norm $|m|$ in $\mathcal{O}_\Delta$.

Beweis: Seien $m \in \mathbb{Z}$ und $\Delta \in \mathcal{D}$ mit $\mathcal{O}_\Delta$ Maximalordnung beliebig. Wegen Lemma 6.2 existiert jeweils für die l_1 trägen Primteiler p_i das Ideal $A_{p_i}^{n_i/2}$ der Norm $p_i^{n_i}$, falls $2 \mid n_i$ gilt. Ansonsten existiert keines.
Für die l_2 verzweigten Primteiler p_i existiert jeweils genau ein Ideal der Norm $p_i^{n_i}$. Analog existieren für die l_3 zerlegten Primteiler jeweils n_i+1 Primideale der Norm $p_i^{n_i}$, nämlich $A_{p_i}^{n_i}\overline{A_{p_i}}^0, A_{p_i}^{n_i-1}\overline{A_{p_i}}^1 \ldots, A_{p_i}^0\overline{A_{p_i}}^{n_i}$. ■

Der Strategie in *NORMEQ* folgend sind die ganzen Ideale der Norm $|m|$ auf Hauptideale hin zu untersuchen. Dabei lassen sich an Stelle der Idealprodukte „einfachere“ Kandidaten testen.

6.2 Hauptidealtests in reellquadratischen Zahlkörpern

In Lemma 6.2 und dessen Beweis haben wir die Ideale der Norm $|m|$ als Potenzprodukte ermittelt und daraus ihre Anzahl bestimmt. Einfache Resultate erlauben uns, zum einen stellvertretend Ideale kleinerer Norm zu testen und zum anderen halb so viele Tests auszuführen wie es Ideale der Norm $|m|$ gibt.

6.2.1 Die Kür von Testidealen

Wir nutzen einfache Zusammenhänge aus. Dabei bezeichnen wir bzgl. eines Ideals A sein konjugiertes Ideal mit $\overline{A}$, d.h.

$$\overline{A} = \{\overline{\gamma} \mid \gamma \in A\}.$$

Die Ideale A und $\overline{A}$ nennen wir auch zueinander konjugiert. Insbesondere gilt $\overline{\overline{A}} = A$.

6.3 Lemma *i) Ein Ideal $A = (\alpha\mathcal{O}_\Delta)B$ mit $\alpha \in \mathcal{O}_\Delta$ ist genau dann Hauptideal in $\mathcal{O}_\Delta$, wenn B Hauptideal in $\mathcal{O}_\Delta$ ist.*
ii) $\overline{A}$ ist genau dann Hauptideal in $\mathcal{O}_\Delta$, wenn A Hauptideal in $\mathcal{O}_\Delta$ ist.

Die multiplikativen Zusammenhänge in (6.2) ermöglichen, die erwähnten Potenzprodukte zu „kürzen“, d.h. wir betrachten äquivalente Testkandidaten kleinerer Norm.

6.4 Korollar *Seien $\mathcal{O}_\Delta$ eine Maximalordnung mit $\Delta \in \mathcal{D}$ und $m \in \mathbb{Z}$ gemäß (6.3), so daß ganze Ideale der Norm $|m|$ existieren.*

i) Für jeden trägen Primteiler p_i ist das Ideal $A_{p_i}^{n_i/2} = p_i^{n_i/2}\mathcal{O}_\Delta$ Hauptideal.
ii) Für jeden verzweigten Primteiler p_i gilt $A_{p_i}^{n_i} = (p_i^{\lfloor n_i/2 \rfloor}\mathcal{O}_\Delta)A_{p_i}^{n_i \bmod 2}$.

iii) Für die zerlegten Primteiler p_i betrachten wir $A_{p_i}^{n_{i1}}\overline{A_{p_i}}^{n_{i2}}$ mit $n_{i1} + n_{i2} = n_i$. Falls $n_{i1} \geq n_{i2}$, dann gilt $A_{p_i}^{n_{i1}}\overline{A_{p_i}}^{n_{i2}} = (p_i^{n_{i2}}\mathcal{O}_\Delta)A_{p_i}^{n_{i1}-n_{i2}}$. Sonst gilt $A_{p_i}^{n_{i1}}\overline{A_{p_i}}^{n_{i2}} = (p_i^{n_{i1}}\mathcal{O}_\Delta)\overline{A_{p_i}}^{n_{i2}-n_{i1}}$.

Die beiden letzten Resultate erlauben uns einige Folgerungen: Falls ganze Ideale der Norm $|m|$ existieren, können wir uns anstatt auf m auf die Aufgabenstellung in (6.1) für

$$m_2 := \prod_{i=1}^{l_2} p_i^{n_i \bmod 2} \cdot \prod_{i=1}^{l_3} p_i^{n_i} \tag{6.4}$$

konzentrieren. Außerdem beschränken wir uns bei den Potenzprodukten bzgl. zerlegter Primteiler p_i jeweils auf Potenzen, die entweder auf A_{p_i} oder $\overline{A}_{p_i}$ basieren. Ferner wissen wir, daß wir für zueinander konjugierte Ideale nur einen Hauptidealtest durchzuführen brauchen. Dies liefert uns dann: (vgl. Lemma 6.3)

6.5 Korollar *Seien $\mathcal{O}_\Delta$ eine Maximalordnung mit $\Delta \in \mathcal{D}$ und $m \in \mathbb{Z}$ gemäß (6.3), so daß ganze Ideale der Norm $|m|$ existieren. Dann müssen wir maximal*

$$\left\lceil \frac{1}{2} \cdot \prod_{i=1}^{l_3} (n_i + 1) \right\rceil$$

Hauptidealtests ausführen, um zu wissen, ob die $\prod_{i=1}^{l_3}(n_i+1)$ ganzen Ideale der Norm $|m|$ Hauptideale in $\mathcal{O}_\Delta$ sind.

Die diesem Korollar zugrundeliegende Methode testet – bis auf Konjugierte – die gemäß Korollar 6.4 „gekürzten" Potenzprodukte auf Hauptideale. Es liegen auch andere Testverfahren nahe, wie z.B. Teilfaktoren zu untersuchen und die Ergebnisse auf die Produkte zu übertragen. Dann kann die optimale Anzahl der Hauptidealtests unter der von Korollar 6.5 liegen, der worst-case ist allerdings in der Regel schlechter. Der Durchschnittswert hängt unter anderem von der Größe der Klassenzahl $h(\Delta)$ bzw. der Struktur der Klassengruppe ab, da z.B. $A_p^{h(\Delta)}$ stets Hauptideal ist.

Die konstruierten Ideale sind Kandidaten für Hauptideale. Wir unterziehen sie einem Hauptidealtest analog zu *HITEST* .

6.2.2 Ein Hauptidealtest

Wir orientieren uns am allgemein formulierten Algorithmus *HITEST* und richten ihn speziell auf reellquadratische Zahlkörper aus. Die Methode beruht auf dem Prinzip der Relationengenerierung. Deshalb greifen wir auf unser Verfahren und unsere Resultate in *RELATION* aus 5.66 zurück.

6.6 Algorithmus *QUHITEST* (Teilalgorithmus)

Eingabe: $\Delta \in \mathcal{D}^+$ mit $\mathcal{O}_\Delta$ Maximalordnung, A Ideal in $\mathcal{O}_\Delta$, F_C eine Faktorbasis und $k \in \mathbb{N}$ deren Ordnung sowie $B'_C \in \mathbb{Z}^{k \times k}$, Matrix einer Gitterbasis von Γ'_C

Ausgabe: $L = (\underline{x}, \alpha)$, Liste mit einem Lösungsvektor $\underline{x} \in \mathbb{Z}^k$ und α in komprimierter Darstellung, falls A Hauptideal und „nein" sonst.

	/* Wahl der Idealklasse */ Wähle zufällig und gleichverteilt einen Exponentenvektor $\underline{e} \in_R [\![0, \Delta]\!]^k$.	(1)
	/* Wahl eines Testideals in der Idealklasse $[A \prod_{i=1}^k P_i^{e_i}]$. */ (a) Wähle zufällig und gleichverteilt eine Zahl y mit $y \in_R [-\Delta, 0] \cap \frac{1}{3}\mathbb{Z}$. (b) /* Bestimme ein reduziertes Ideal B mit $B = (\alpha\mathcal{O}_\Delta)A \prod_{i=1}^k P_i^{e_i}$ und $\ln\lvert\alpha\rvert \sim y$. */ $(B, \hat{y}, \alpha_0, \kappa, \gamma') \leftarrow$ *REACH* $(\Delta, F_C, k, \underline{e}, y)$ /* $\alpha = \alpha_0 \circ \kappa \circ \gamma'$ */	(2)
UNTIL	$(\underline{z} \leftarrow$ *ZERLEGUNG* $(B, F_C, k)) \neq$ leere Liste /* D.h. B zerfällt über F_C, $B = \prod_{i=1}^k P^{z_i}$. */	(3)
/* Nun gilt: $A = (1/\alpha\mathcal{O}_\Delta)\ B\ \prod_{i=1}^k\ P_i^{-e_i} = (1/\alpha\mathcal{O}_\Delta)\ \prod_{i=1}^k P_i^{z_i - e_i}$		(4)
Teste ob A Hauptideal, d.h. löse $B'_C \cdot \underline{x} = \underline{z} - \underline{e}$ über $\mathbb{Z}^k$.		(5)
IF	Existenz einer Lösung	(6)
THEN	$L \leftarrow (\underline{x}, \alpha)$	(7)
ELSE	$L \leftarrow$ „nein"	(8)

Die Schritte (1) - (3) entsprechen einer iterierten Anwendung der Schritte (1) - (3) von *RELATION*. Sie werden sooft wiederholt, bis eine Relation bzw. ein geeigneter Testkandidat B gefunden ist. Wir schätzen die Laufzeit ab, die *QUHITEST* zum Überprüfen der Testideale bzgl. der ganzen Ideale der Norm $|m|$ benötigt. Wir gehen davon aus, daß wir für die Testideale äquivalente, reduzierte Vertreter eingeben.

6.7 Proposition *(GRH) Seien $\mathcal{O}_\Delta$ eine Maximalordnung mit $\Delta \in \mathcal{D}^+$ und $m \in \mathbb{Z} - \{0\}$ gemäß (6.3), so daß ganze Ideale der Norm $|m|$ existieren. Dann ist QUHITEST vom Typ Las-Vegas. Bei iterierter Anwendung auf alle reduzierten Vertreter der Testideale bzgl. ganzer Ideale der Norm $|m|$ benötigt QUHITEST bei Eingabe von Δ, einer Faktorbasis F_C mit $12(\ln\Delta)^2 \leq C = L_\Delta{}^c \leq \sqrt{\Delta}/2$, ihrer Ordnung k sowie einer Basismatrix $B'_C \in \mathbb{Z}^{k\times k}$ des Relationengitters Γ'_C gemäß (5.46) erwartete Laufzeit $L_\Delta[4c] + \prod_{i=1}^{l_3} n_i \cdot (L_\Delta[c + 1/(4c)] + L_\Delta[3c])$.*

Beweis: Seien $\Delta \in \mathcal{D}^+$ und $m \in \mathbb{Z}$ der Voraussetzung genügend beliebig gewählt. *QUHITEST* ist vom Typ Las-Vegas, weil die Schritte (1) - (3) denen vom Las-Vegas

Verfahren *RELATION* entsprechen. (vgl. Satz 5.67) Gemäß Korollar 6.5 liegen maximal $\prod_{i=1}^{k}(n_i+1)/2$ viele Testideale vor.
Wir wenden uns den Schritten (1) - (3) zu. Sie unterscheiden sich von denen in *RELATION* durch die Wahl der um $[A]$ transformierten Idealklasse. Algorithmisch ändern wir das Verfahren nur dadurch ab, daß wir in Schritt (1) von *REACH* das mit *POTPROD* berechnete reduzierte Ideal B_0 mit einem reduzierten Vertreter des Testideals aus $[A]$ multiplizieren und anschließend reduzieren. Die Laufzeit bleibt asymptotisch gleich, d.h. die Schritte (1) - (3) benötigen erwartete Laufzeit $L_\Delta[c]$. (vgl. Satz 5.67) Da die (multiplikative) Transformation um die gewählte Idealklasse $[A]$ bijektiv ist, bleibt die in (1) von *RELATION* bewiesene (asymptotisch) gleichverteilte Wahl einer Idealklasse erhalten. (vgl. Korollar 5.20) Deshalb können wir auch die Analyse von *RELATION* übernehmen: Nach $1/p(F_C) \leq L_\Delta[1/(4c)]$ Iterationen der Schleife erwarten wir für $12(\ln\Delta)^2 \leq C \leq \sqrt{\Delta}/2$ einen Zerfall des berechneten reduzierten Ideals B über der Faktorbasis F_C. (vgl. Korollar 5.80) Bis zum erfolgreichen Beenden der Schleife verbrauchen wir also erwartete Zeit $L_\Delta[c+1/(4c)]$.
Zur Lösung der Gleichungssysteme in (5) wenden wir ein Resultat von J. Buchmann und Ac. Müller aus [BuMü] an und treffen noch einige Vorüberlegungen. Da B'_C in Hermite-Normalform vorliegt und ihre Determinante die Klassenzahl ist, sind ihre Einträge durch $O(\sqrt{\Delta}\ln\Delta)$ beschränkt. (vgl. (2.25)) Die Einträge der Vektoren $\underline{z}-\underline{e}$ sind betragsmäßig durch $O(\Delta)$ beschränkt. Dann benötigt das Lösen der $\frac{1}{2}\prod_{i=1}^{l_3}(n_i+1)$ Gleichungssysteme Zeit

$$\begin{aligned} O\Big(k^3(k+\prod_{i=1}^{l_3}(n_i+1))\cdot(\log(k|B'_C|)+\log\Delta)^2\Big) &= O\Big(k^3(k+\prod_{i=1}^{l_3}n_i)\cdot \\ &\qquad (\log k+\log\Delta)^2\Big) \\ &= L_\Delta[4c]+L_\Delta[3c]\cdot\prod_{i=1}^{l_3}n_i. \end{aligned}$$

■

Schließen wir zusätzlich die Normgleichung an die Klassenzahlberechnung an, ist die Laufzeit bereits bzgl. der Klassenzahlberechnung optimiert mit $c=\sqrt{3}/6$. (vgl. Kapitel 5) Einsetzen in die eben ermittelte Laufzeit ergibt:

6.8 Korollar *(GRH) Unter der Voraussetzung der vorangegangenen Proposition ergibt sich für $c=\sqrt{3}/6$ eine erwartete Laufzeit von $L_\Delta[1,155]\cdot\prod_{i=1}^{l_3}n_i$.*

Zum Lösen einer Normgleichung in (6.1) sind alle Vorbereitungen getroffen, so daß wir uns der Anpassung von *NORMEQ* auf reellquadratische Zahlkörper zuwenden.

6.3 Der Algorithmus *QUNORMEQ*

Wir übernehmen die Grundidee von *NORMEQ* und bringen die speziellen Eigenschaften reellquadratischer Zahlkörper, insbesondere die Resultate des vorangegangenen Abschnitts ein. Dabei haben wir „gekürzte“ Testideale konstruiert, für die wir stellvertretend Hauptidealtests ausführen. Für diese sogenannten Testideale wollen wir die Abfrage organisieren.

6.3.1 Eine Sortierung der Testideale

Zur Organisation der Abfrage der Testideale führen wir eine Reihenfolge ein, die sich am Prinzip lexikographischer Ordnungen orientiert und eine günstige Berechnung zuläßt. Alle Testideale haben bzgl. der verzweigten Primteiler p_i von m den gemeinsamen Faktor $\prod_{i=1}^{l_2} A_{p_i}^{n_i \bmod 2}$. Für die zerlegten Primteiler kommen jeweils als Faktor nur eine Potenz von A_{p_i} oder $\overline{A_{p_i}}$ vor, wobei wir die Reihenfolge der Faktoren gemäß der Größe der entsprechenden Primzahlen p_i wählen. Bzgl. der jeweiligen Primzahlen p_i unterscheiden wir gemäß aufsteigender Exponenten, wobei $\overline{A_{p_i}}$ nach A_{p_i} kommt. Dies illustrieren wir anhand eines Beispiels: Wir wählen $\Delta = 12$ und $m = 5^2 \cdot 3 \cdot 11^3 \cdot 13^4$, wobei 5 träge, 3 verzweigt und 11, 13 zerlegt sind. Wir untersuchen die $(3+1) \cdot (4+1)/2$ Testideale in der Reihenfolge

$$\begin{array}{l} A_3A_{11}A_{13}^0,\ A_3A_{11}A_{13}^2,\ A_3A_{11}A_{13}^4,\ A_3A_{11}\overline{A_{13}}^2,\ A_3A_{11}\overline{A_{13}}^4 \\ A_3A_{11}^3A_{13}^0,\ A_3A_{11}^3A_{13}^2,\ A_3A_{11}^3A_{13}^4,\ A_3A_{11}^3\overline{A_{13}}^2,\ A_3A_{11}^3\overline{A_{13}}^4 \end{array} .$$

Wir bringen diese Ideen in *QUNORMEQ* und *LEX* ein. Wir formulieren zuerst *QUNORMEQ* , klären danach die Bestimmung des Vorzeichens der Norm einer Lösung γ. Dies wenden wir dann im verbleibenden Teilalgorithmus *LEX* an.

6.3.2 Die Formulierung von *QUNORMEQ*

Wir durchlaufen die Testideale in der Reihenfolge, wie wir sie eben beschrieben haben. Sie bestehen aus Potenzen der A_{p_i} bzw. $\overline{A_{p_i}}$. Für die Testideale berechnen wir stellvertretend reduzierte, äquivalente Ideale, indem wir jeweils nach jeder Idealmultiplikation das Produkt primitiv machen und es reduzieren. (vgl. $(\Theta/g\mathcal{O}_\Delta)AB$ als Schreibweise wie in Kapitel 5) Diese Faktoren Θ/g und ein Erzeuger des Stellvertreters des Testideals – sofern es Hauptideal ist – ergeben dann ein Erzeugendes für das Testideal, woraus wir wiederum ein Erzeugendes für das entsprechende Hauptideal der Norm $|m|$ konstruieren. Diese Erzeugenden geben wir analog zu Kapitel 5 in komprimierter Darstellung an. (vgl. Bemerkung 5.23)

6.9 Algorithmus *QUNORMEQ*

Eingabe: L als Faktor-Exponenten-Liste von $m \in \mathbb{Z} - \{0\}$, $\Delta \in \mathcal{D}^+$ mit $\mathcal{O}_\Delta$ Maximalordnung, F_C eine Faktorbasis und $k \in \mathbb{N}$ ihre Ordnung, $B'_C \in \mathbb{Z}^{k\times k}$ Matrix einer Gitterbasis von Γ'_C

Ausgabe: nichtassoziierte ganze Lösungen γ der Normgleichung $N(\gamma) = m$ in komprimierter Darstellung, falls welche existieren

/* Aussortieren der verzweigten und trägen Primteiler */ $vorfak[0] \leftarrow 1$, $test[0] \leftarrow \mathcal{O}_\Delta$, $L_3 \leftarrow$ leere Liste	(1)
WHILE $L \neq$ leere Liste	(2)
Kürze L um die ersten beiden Elemente $p_i,\ n_i$.	(3)
IF $(\Delta/p_i) = -1$ /* p_i träge */	(4)
THEN IF $n_i = 1 \bmod 2$ /* vgl. (6.2) */	(5)
THEN exit /* existiert keine Lösung */	(6)
ELSE $vorfak[0] \leftarrow vorfak[0] \circ p_i^{n_i/2}$	(7)
ELSE IF $(\Delta/p_i) = 0$ /* p_i verzweigt */	(8)
THEN $test[0] \leftarrow (\Theta\mathcal{O}_\Delta)test[0]A_{p_i}^{\lfloor n_i/2\rfloor}$	(9)
$vorfak[0] \leftarrow vorfak[0] \circ p_i^{\lfloor n_i/2\rfloor} \circ \Theta^{-1}$	(10)
ELSE Ergänze L_3 um $p_i,\ n_i$. /* p_i träge */	(11)
$\wp_i[1] \leftarrow (\Theta(p_i,1)\mathcal{O}_\Delta)A_{p_i}$, $\wp_i[2] \leftarrow (\Theta(p_i,2)\mathcal{O}_\Delta)A_{p_i}^2$, $\wp_i[-1] \leftarrow (\Theta(p_i,-1)\mathcal{O}_\Delta)\overline{A_{p_i}}$, $\wp_i[-2] \leftarrow (\Theta(p_i,-2)\mathcal{O}_\Delta)\overline{A_{p_i}}^{-2}$	(12)
/* Abfragen der Testkandidaten */ $l_3 \leftarrow (\sharp L_3)/2$ /* Anzahl der trägen Primteiler */	(13)
IF $l_3 = 0$	(14)
THEN $LEX(sgn\ m, L_3, 1, test, vorfak, \Delta, F_C, k, B'_C)$, exit	(15)
Entnimm $p_1,\ n_1$ aus L_3. /* $l_3 > 0$ */	(16)
FOR $j \leftarrow n_1 \bmod 2$	(17)
IF $j > 1$	(18)
THEN $test[1] \leftarrow (\Theta/g\mathcal{O}_\Delta)\ test[0]\ \wp_i[2]$	(19)
$vorfak[1] \leftarrow vorfak[1]/p_i \circ g/\Theta \circ \Theta(p_i,2)^{-1}$	(20)
ELSE $vorfak[1] \leftarrow p_i^{\lfloor n_i/2\rfloor}$	(21)
IF $j = 1$	(22)
THEN $test[1] \leftarrow (\Theta/g\mathcal{O}_\Delta)\ test[0]\ \wp_i[1]$	(23)
$vorfak[1] \leftarrow vorfak[1] \circ g/\Theta \circ \Theta(p_i,1)^{-1}$	(24)
ELSE $test[1] \leftarrow test[0]$	(25)
$LEX(sgn\ m, L_3, 1, test, vorfak, \Delta, F_C, k, B'_C)$, $j \leftarrow j+2$	(26)

Wir realisieren die Reihenfolge der Testideale mit *LEX* im übernächsten Abschnitt. Ferner benötigen wir für $\gamma \in \mathcal{O}_\Delta$ in komprimierter Darstellung das Vorzeichen seiner Norm und $\overline{\gamma}$. $\overline{\gamma}$ läßt sich mit Bemerkung 5.23 in komprimierter Darstellung direkt herleiten, da die jeweiligen Faktoren in der komprimierten Darstellung von γ 4-Tupel entsprechen, wobei für $\overline{\gamma}$ der vierte Eintrag mit -1 multipliziert wird.

6.3.3 Die Vorzeichenabfrage der Norm

Diese Abfrage benötigen wir zur Klärung, ob das Vorzeichen der Norm des ermittelten Elementes mit dem von m übereinstimmt. (vgl. (8) in *NORMEQ*) Sonst wird es mit einer Einheit negativer Norm multipliziert, falls eine existiert. Die Existenz muß ebenfalls geklärt werden. Dabei erweist sich folgendes Resultat als hilfreich:

6.10 Lemma *Seien $m \in \mathbb{Z} - \{0\}$, $\Delta \in \mathcal{D}^+$ mit $\mathcal{O}_\Delta$ Maximalordnung und A ein Ideal in $\mathcal{O}_\Delta$. Falls $\gamma \in \mathcal{O}_\Delta$ das Ideal A erzeugt mit $N(\gamma) = -m$ und die Grundeinheit η Norm 1 hat, dann existiert kein Element, das A erzeugt und Norm m hat.*

Beweis: Wir nehmen das Gegenteil an, indem $\tilde{\gamma} \in \mathcal{O}_\Delta$ mit $A = \tilde{\gamma}\mathcal{O}_\Delta$ und $N(\tilde{\gamma}) = m$ existiere. Dann unterscheiden sich γ und $\tilde{\gamma}$ nur durch eine Einheit, da sie beide A erzeugen, d.h. $\gamma = \pm\tilde{\gamma} \cdot \eta^z$ mit $z \in \mathbb{Z}$. Dies führt wegen der Voraussetzung zum Widerspruch $-m = N(\gamma) = N(\tilde{\gamma}) = m$. ∎

Wir wenden uns dem Vorzeichentest zu: In *QUHITEST* gilt für das eingegebene Ideal A gemäß Schritt (4) $A = (1/\alpha\mathcal{O}_\Delta)\prod_{i=1}^k P_i^{z_i - e_i}$. Ist A Hauptideal, wird es von $1/\alpha$ und einem Erzeugenden von $\prod_{i=1}^k P_i^{z_i - e_i}$ erzeugt. Dazu haben wir das Gleichungssystem $B'_C\underline{x} = \underline{z} - \underline{e}$ zu lösen, sofern es lösbar ist. Unserer zugrundeliegenden Basismatrix B_C gemäß (5.46) entnehmen wir: In der $(k+1)$-ten Zeile entsprechen den Elementen $h_{k+1,i}$ jeweils Erzeugende $\beta_i \in \mathbb{Q}(\sqrt{\Delta})$. (analog zu (5.44)) Insbesondere gilt $\beta_{k+1} = \pm\eta$. (vgl. Bemerkung 5.96) Haben wir also eine Lösung $\underline{x} \in \mathbb{Z}^k$ des Gleichungssystems $B'_C \cdot \underline{x} = \underline{z} - \underline{e}$ in (5) von *QUHITEST* , erzeugt

$$\prod_{i=1}^k \beta_i^{x_i} \qquad \text{bzw.} \qquad 1/\alpha \cdot \prod_{i=1}^k \beta_i^{x_i}$$

das Ideal $\prod_{i=1}^k P_i^{z_i - e_i}$ bzw. A. (vgl. Lemma 4.11) Das Vorzeichen der Norm ist

$$sgn\ N\left(\prod_{i=1}^k \beta_i^{x_i}\right) = \prod_{i=1}^k sgn\ N(\beta_i)^{x_i \bmod 2} \tag{6.5}$$

bzw. muß noch $sgn\ N(\alpha)$ berückichtigt werden. Wir benötigen das Vorzeichen der $N(\beta_i)$ und $x_i \bmod 2$. Für das Vorzeichen von $N(\beta_i)$ brauchen wir nähere Aussagen über β_i, die wir uns bereits während der Klassenzahlberechnung besorgen müssen. Daher ändern wir *QUCLASSREG* geringfügig ab, um eventuell bei einer anschließenden Normgleichung über die notwendigen Informationen zu verfügen. Hierzu beleuchten wir den Aufbau der β_i genauer:

Für $1 \le i \le k$ wissen wir für β_i analog zu (5.44) die Produktdarstellung

$$\prod_{i=1}^N \alpha_j^{-t_{i,j}} = \beta_i \tag{6.6}$$

bzgl. der Transformationsmarix $T = (t_{i,j})$. Analog zu (6.5) reduziert sich die Bestimmung des Vorzeichens von $N(\beta_i)$ auf $\prod_{i=1}^N\ sgnN(\alpha_j)^{t_{i,j} \bmod 2}$. Demnach benötigen wir Aussagen über das Vorzeichen der $N(\alpha_i)$, $1 \leq i \leq N$. Die α_i ergeben sich wiederum aus der Relationengenerierung. (vgl. *RELATION*) Sie liegen jeweils in komprimierter Darstellung vor. Wie bereits in den Beweisen der Lemmata 5.92 und 5.93 erwähnt, bestehen die α_i aus $O(k \cdot (\log \Delta)^2)$ vielen Faktoren, die lediglich aus Potenzen von Vorwärts- oder Rückwärtsschritten bestehen. Für l Vorwärts- Θ_l oder Rückwärtsschritte Υ_l können wir gemäß Lemma 2.15 bzw. Lemma 2.23

$$sgn\ N(\Theta_l) = sgn\ (-1)^{l \bmod 2} \qquad \text{bzw.} \qquad sgn\ N(\Upsilon_l) = sgn\ (-1)^{l \bmod 2}$$

folgern. Deshalb fügen wir den entsprechenden Algorithmen einen Zähler modulo 2 hinzu, der uns die notwendigen Werte verschafft. Im Laufe der Relationengenerierung berücksichtigen wir für jeden dieser Faktoren Θ_l, Υ_l die Exponenten modulo 2. Am Ende des Aufrufs einer Relationengenerierung liegt dann für α_j eine 0 oder 1 vor, die das Signum $(-1)^0$ bzw. $(-1)^1$ von $N(\alpha_j)$ ergibt. Diesen Wert speichern wir in einem Vektor $\underline{vz}$ mit vz_i für $sgn\ N(\alpha_i)$ ab. Dann läßt sich $sgnN(\beta_i)$ in (6.5) mit Hilfe von (6.6) einfach bestimmen und abspeichern. Dies können wir ohne asymptotische Änderung der Gesamtlaufzeit von *QUCLASSREG* bewerkstelligen.

Für das noch ausstehende Vorzeichen der Norm der Grundeinheit $N(\beta_{k+1} = \pm\eta)$ berücksichtigen wir zusätzlich *ESTOBAS* : Gemäß (5.43) und (5.44) bestimmen wir aus dem Erzeugendensystem der $\ln \prod_{j=1}^{N} \alpha_j^{-t_{i,j}}$ für $k+1 \leq i \leq N$ ein Basiselement, das in unserem Fall eine Approximation des Regulators $R = \ln|\beta_{k+1} = \pm\eta|$ liefert. Dies geschieht mittels 8-facher Iteration einer Schleife in *ESTOBAS* , die jeweils Linearkombinationen der Logarithmen bzgl. ganzzahliger Vektoren $\underline{z}$ berechnet. (vgl. (15) von *ESTOBAS*) Bzgl. der entsprechenden Argumente der Logarithmen bedeutet dies, daß wir entsprechend $\underline{z}$ potenzieren. Für das Vorzeichen von $N(\beta_{k+1})$ heißt dies: Wie für (6.6) beschrieben bestimmen wir das Vorzeichen der Norm der $\prod_{j=1}^{N} \alpha_j^{-t_{i,j}}$ für $k+1 \leq i \leq N$. In *ESTOBAS* fügen wir den jeweiligen Erzeugenden stets das Vorzeichen der Norm ihrer Argumente hinzu, indem wir die Potenzen bzgl. $\underline{z}$ berücksichtigen. (vgl. (6.5)) Bei Beenden von *ESTOBAS* liegt dann das Vorzeichen von $N(\beta_{k+1} = \pm\eta)$ vor. Auch dies kann ohne asymptotische Änderung der Laufzeit von *QUCLASSREG* erledigt werden.

Deshalb gehen wir im folgenden davon aus, daß uns bzgl. B_C für die $N(\beta_i)$, $1 \leq i \leq k+1$, ein „Vorzeichenvektor“ $\underline{sgn} \in \{\pm 1\}^{k+1}$ vorliegt mit

$$sgn_i = sgn\ N(\beta_i). \tag{6.7}$$

Wir benötigen das Vorzeichen der Norm eines Erzeugenden eines Testideals, das sich gemäß *QUHITEST* zu $sgn\ N(\alpha) \cdot \prod_{i=1}^{k} sgn\ N(\beta_i)^{x_i \bmod 2}$ berechnet, wobei wir das noch fehlende $sgn\ N(\alpha)$ (vgl. (4) von *QUHITEST*) mit der eben beschriebenen Methode erhalten, da (1) - (3) von *QUHITEST* den entsprechenden Schritten von *RELATION* entspricht. Auch hier bleibt die Laufzeit asymptotisch unverändert.

6.11 Algorithmus *LEX* (Teilalgorithmus)

Eingabe: $sgn\ m$, L_3 Liste zerlegter Primteiler von $m \neq 0$, $l \in \mathbb{N}_0$, neue Rekursionstiefe, *test* jeweilige reduzierte Vertreter der Testideale mit *vorfak* der Liste der Vorfaktoren, $\Delta \in \mathcal{D}^+$ mit $\mathcal{O}_\Delta$ Maximalordnung, F_C eine Faktorbasis und $k \in \mathbb{N}$ deren Ordnung, $B'_C \in \mathbb{Z}^{k \times k}$ Matrix einer Gitterbasis von Γ'_C

Ausgabe: nichtassoziierte ganze Lösungen $\gamma \in \mathcal{O}_\Delta$ der Normgleichung $N(\gamma) = m$ in komprimierter Darstellung, falls welche existieren

IF $l > (l_3 = \sharp L_3)$				(1)
THEN	$L \leftarrow QUHITEST\ (\Delta, test[l-1], F_C, k, B'_C)$			(2)
	IF $L \neq$ leere Liste			(3)
	THEN	Teste, ob das Vorzeichen des Erzeugers von $test[l-1]$ mit $sgn\ m$ übereinstimmt. Falls nicht, exit. Sonst liefern $\prod_{i=1}^{l_3} vorfak[i]$ und der Erzeuger des Testideals sowie das Konjugierte Elemente der Norm m. exit		(4)
	ELSE	exit /* $test[l_3]$ kein Hauptideal */		(5)
/* $l \leq l_3$ noch Faktoren suchen */				(6)
Entnimm p_l, n_l aus L_3.				(7)
FOR $j \leftarrow n_l \bmod 2\ TO\ n_l$				(8)
	IF $j > 1$			(9)
	THEN	$test[l] \leftarrow (\Theta/g\mathcal{O}_\Delta)\ test[l]\ \wp_l[2]$		(10)
		$vorfak[l] \leftarrow vorfak[l]/p_l\ \circ\ g/\Theta\ \circ\ \Theta(p_{l,2})^{-1}$		(11)
	ELSE	$vorfak[l] \leftarrow p_l^{\lfloor n_l/2 \rfloor}$		(12)
		IF $j = 1$		(13)
		THEN	$test[l] \leftarrow (\Theta/g\mathcal{O}_\Delta)\ test[l-1]\ \wp_l[1]$	(14)
			$vorfak[l] \leftarrow vorfak[l]\ \circ\ g/\Theta\ \circ \Theta(p_l, 1)^{-1}$	(15)
		ELSE	$test[l] \leftarrow test[l-1]$	(16)
	$LEX(sgn\ m, L_3, l+1, test, vorfak, \Delta, F_C, k, B'_C)$, $j \leftarrow j+2$			(17)
/* Konjugierte Potenzen von $\overline{A_{p_i}}$ abarbeiten. */				(18)
FOR $j \leftarrow n_l \bmod 2\ TO\ n_l$				(19)
	IF $j > 1$			(20)
	THEN	$test[l] \leftarrow (\Theta/g\mathcal{O}_\Delta)\ test[l]\ \wp_l[-2]$		(21)
		$vorfak[l] \leftarrow vorfak[l]/p_i\ \circ\ g/\Theta\ \circ\ \Theta(p_l, -2)^{-1}$		(22)
	ELSE	IF $j = 1$		(23)
		THEN	$test[l] \leftarrow (\Theta/g\mathcal{O}_\Delta)\ test[l-1]\ \wp_l[-1]$	(24)
			$vorfak[l] \leftarrow p_l^{\lfloor n_l/2 \rfloor}\ \circ\ g/\Theta\ \circ\ \Theta(p_l, -1)^{-1}$	(25)
		ELSE	$j \leftarrow j+2$ /* wegen $\overline{A_{p_i}}^0 = A_{p_i}$ */	(26)
			$test[l] \leftarrow (\Theta/g\mathcal{O}_\Delta)\ test[l-1]\ \wp_l[-2]$	(27)
			$vorfak[l] \leftarrow p_l^{n_l/2-1}\ \circ\ g/\Theta\ \circ\ \Theta(p_l, -2)^{-1}$	(28)
	$LEX(sgn\ m, L_3, l+1, test, vorfak, \Delta, F_C, k, B'_C)$, $j \leftarrow j+2$			(29)

6.3.4 Die Analyse von *QUNORMEQ*

In jedem Aufruf von *LEX* wird eine Potenz mehr bzgl. der zerlegten Primteiler von m berücksichtigt, so daß wir nach jeweils l_3 Iterationen einen reduzierten Vertreter eines Testideals bestimmt haben und einen Hauptidealtest für das Ideal $test[l_3]$ vornehmen. Die Rekursionstiefe beträgt also l_3. Ist das Testideal Hauptideal, erhalten wir von *QUHITEST* eine Liste $(\underline{x}, \alpha)$ zurück. Dann wissen wir mit Abschnitt 6.3.3:

6.12 Lemma *Wird LEX in der Situation von QUNORMEQ aufgerufen, gilt jeweils beim Hauptidealtest, daß* $(\prod_{i=0}^{l_3} vorfak[i]\mathcal{O}_\Delta)\ test[l_3]$ *ein Ideal der Norm* $|m|$ *ist. Ist es Hauptideal, dann haben wir nach Beenden von QUHITEST bzgl. der Ergebnisliste* $(\underline{x}, \alpha)$*:* $1/\alpha \cdot \prod_{i=0}^{l_3} vorfak[i] \cdot \prod_{i=1}^{k} \beta_i^{x_i}$ *hat Norm* $\pm m$.

Der Beweis folgt iterativ analog zu den Methoden aus Kapitel 5. Wir wenden uns der Laufzeitabschätzung zu.

6.13 Satz *(GRH) Bei Eingabe einer Faktor-Exponenten-Liste einer ganzen Zahl* $m \in \mathbb{Z} - \{0\}$*, einer Diskriminanten* $\Delta \in \mathcal{D}^+$ *mit* $\mathcal{O}_\Delta$ *Maximalordnung, einer Faktorbasis* F_C *sowie deren Ordnung* k *und einer Basismatrix* $B'_C \in \mathbb{Z}^{k\times k}$ *von* Γ'_C *bestimmt der Las-Vegas-Algorithmus QUNORMEQ alle nichtassoziierten ganzen Elemente* $\gamma \in \mathcal{O}_\Delta$ *der Norm* m *in komprimierter Darstellung in erwarteter Laufzeit* $L_\Delta[4c] + \prod_{i=1}^{l_3} n_i \cdot (L_\Delta[c + 1/(4c)] + L_\Delta[3c]) + L_\Delta[0] \cdot \log|m| + O((\log|m|)^3)$.

Beweis: Wir rufen den Teilalgorithmus *QUHITEST* auf, der vom Typ Las-Vegas ist, so daß auch *QUNORMEQ* dieses Typs ist. (vgl. Proposition 6.7)
QUNORMEQ bestimmt alle nichtassoziierten Elemente der Norm m, weil wir die Reihenfolge der Testideale aus Abschnitt 6.3.1 übernehmen sowie die anfallenden Vorfaktoren und Konjugierten berücksichtigen: Mit Hilfe von *LEX* starten wir mit einem reduzierten Vertreter bzgl. des Testideals, das „kleinste Ordnung" hat. Dann wird auf Position l_3 kontinuierlich das „nächst größere" genommen, bis wir die obere Grenze n_{l_3} des Exponenten erreicht haben. Auf dieser Position verfahren wir analog bzgl. des konjugierten Ideals $\overline{A_{p_{l_3}}}$. Anschließend rücken wir auf Position $l_3 - 1$ vor und wiederholen diesen Prozeß für beide Positionen. Durch Iteration dieses Vorgangs bis auf die erste Position arbeiten wir insgesamt alle Testideale ab.
Die Initialisierung in (1) – (12) bestimmt jeweils das Kronecker-Symbol (Δ/p_i) für alle l Primteiler von m. Für die l_2 verzweigten Primteiler wird eventuell die Standarddarstellung der Primideale A_{p_i} und ein reduzierter Vertreter berechnet, analog wird für die l_3 zerlegten Primteiler und die Quadrate ihrer Primideale verfahren. Wir bauchen Zeit: (vgl. Lemmata 2.42, 2.44, 2.60 und Satz 2.57 und $\sum_{i=1}^{l} \log p_i = \log m$)

$$O\Big(\sum_{i=1}^{l}(\log\Delta \cdot \log p_i + (\log p_i)^2) + \sum_{i=1}^{l_2+l_3}(\log p_i(\log\Delta + (\log p_i)^2) + (\log\Delta)^3)\Big) \quad = \quad L_\Delta[0]\cdot\log|m| + O\Big(\log|m|)^3\Big)$$

Wir bestimmen nun die Anzahl der Multiplikationen und Reduktionen auf reduzierten Idealen, die wir im Laufe der rekursiven Aufrufe von *LEX* ausführen: Wir

stellen uns dazu einen Baum der Tiefe l_3 vor, in dem jeder Knoten eine Potenz der A_{p_i} bzw. $\overline{A_{p_i}}$ aus den Testidealen hat. Dann entspricht die Anzahl der Knoten dieses Baumes der Anzahl der Multiplikationen und Reduktionen, die wir ausführen müssen. Sie beläuft sich auf $O(\prod_{i=1}^{l_3} n_i)$(vgl. Korollar 6.5), und wir benötigen Zeit $L_\Delta[0] \cdot \prod_{i=1}^{l_3} n_i$.
Ferner haben wir $O(\prod_{i=1}^{l_3} n_i)$ viele Hauptidealtests auszuführen, womit wir wegen Proposition 6.7 Zeit $L_\Delta[4c] + \prod_{i=1}^{l_3} n_i \cdot (L_\Delta[c + 1/(4c)] + L_\Delta[3c])$ benötigen.
Die übrigen Operationen wie Erstellen der komprimierten Listen und Vorzeichentest werden von dieser Laufzeit erfaßt. ■

Daraus folgern wir: Gehen wir wir davon aus, daß uns die Basismatrix B'_C bereits vorliegt und diese aus der Klassenzahlberechnung mit *QUCLASSREG* bzgl. optimalem Parameter $c = \sqrt{3}/6$ stammt, dann errechnen wir für die Laufzeit wegen $3c < 4c = c + 1/(4c)$ aus (5.48):

6.14 Korollar *(GRH) In der Situation von Satz 6.13 gilt: Liegt eine mittels QUCLASSREG bestimmte Basismatrix B'_C vor, dann benötigen wir bzgl. des optimalen Parameters $c = \sqrt{3}/6$ erwartete Laufzeit $L_\Delta[1, 12] \cdot \prod_{i=1}^{l_3} n_i + L_\Delta[0] \cdot \log|m| + O((\log|m|)^3)$.*

Liegt uns allerdings keine Basismatrix vor, dann bestimmen wir mit *QUCLASSREG* eine solche. Dabei können wir die Relationengenerierung für die Bestimmung einer Basismatrix B'_C mit der Relationensuche für die Hauptidealtests verbinden. Wir ermitteln den optimalen Wert für den Parameter c abhängig von der Anzahl $\prod_{i=1}^{l_3}(n_i + 1)/2$ der Testideale. Wir setzen für $x \in \mathbb{R}_{>0}$

$$\frac{1}{2}\prod_{i=1}^{l_3}(n_i + 1) = L_\Delta{}^x. \tag{6.8}$$

Dann erhalten wir die optimale Wahl für c in Abhängigkeit von x:

6.15 Korollar *(GRH) Bei Eingabe einer Faktor-Exponenten-Liste einer ganzen Zahl $m \in \mathbb{Z} - \{0\}$, einer Diskriminanten $\Delta \in \mathcal{D}^+$ mit $\mathcal{O}_\Delta$ Maximalordnung bestimmt der Las-Vegas-Algorithmus QUNORMEQ im Anschluß an QUCLASSREG alle nichtassoziierten ganzen Elemente $\gamma \in \mathcal{O}_\Delta$ der Norm m in komprimierter Darstellung in erwarteter Laufzeit:*
i) $L_\Delta[1, 44]$, falls $x \leq c$ gilt,
ii) $L_\Delta[5/8 \cdot (x + \sqrt{x^2 + 4})] \sim L_\Delta[1, 25x]$, wenn $c < x < 2c$ genügt.
iii) $L_\Delta[1, 06 + x]$, falls $x \geq 2c$ erfüllt.

Beweis: Gemäß (5.48) braucht *QUCLASSREG* erwartete Laufzeit $\max\{L_\Delta[2c + 1/(4c)], L_\Delta[5c]\}$. Dann haben wir wegen Satz 6.13 für die Laufzeit die Summe

$$L_\Delta[c + 1/(4c)] \cdot (L_\Delta[c] + L_\Delta[x]) + L_\Delta[3c] \cdot (L_\Delta[2c] + L_\Delta[x]) \tag{6.9}$$

zu gegebenem m bzw. x zu minimieren, wenn wir die Terme mit $\log|m|$ vernachlässigen: Dies kann o.B.d.A. geschehen, da wir $\prod_{i=1}^{l_3} n_i \geq \sum_{i=1}^{l} n_i = O(\log|m|)$ wissen.
1. Fall: $x \leq c$

Dann ist in (6.9) $L_\Delta[2c + 1/(4c)] + L_\Delta[5c]$ zu minimieren. Wie in (5.48) ergibt sich der optimale Wert für c zu $\sqrt{3}/6$, und die Gesamtzeit für die Normgleichung wird von der Laufzeit von *QUCLASSREG* mit $L_\Delta[1,44]$ dominiert.
2. Fall: $c < x < 2c$
Wir müssen $L_\Delta[c + 1/(4c) + x] + L_\Delta[5c]$ minimieren, was bei $c = (x + \sqrt{x^2+4})/8$ erreicht wird. Die Gesamtzeit berechnet sich dann zu $L_\Delta[5/8 \cdot (x + \sqrt{x^2+4})]$
3. Fall: $x \geq 2c$
Zu minimieren bleibt $L_\Delta[c + 1/(4c) + x] + L_\Delta[3c + x]$, was für $c = \sqrt{2}/4$ geschieht. Dann ergibt sich die Gesamtlaufzeit zu $L_\Delta[1,06 + x]$. ■

Das Korollar verdeutlicht, daß die Gesamtlaufzeit weniger von der Größe von m als von der Anzahl der Primfaktoren p_i und ihrer Größe der Exponenten n_i abhängt. (vgl. (6.8)) Insofern ist unsere Methode besonders geeignet für m, die aus wenig Primfaktoren mit kleinen Exponenten n_i bestehen.

Unsere Methode setzt voraus, daß wir die Faktor-Exponentenliste von m, d.h. die Faktorisierung, kennen. Bisher sind wir davon ausgegangen, daß diese uns vorliegt. Falls dies nicht zutrifft, dann müssen wir m zuerst faktorisieren: Die asymptotisch schnellste, aber komplizierteste, Faktorisierungsmethode ist das Number-Field-Sieve (NFS). (vgl. [LL]) Sie benötigt die heuristische, subexponentielle Laufzeit

$$\exp\Big((\log|m|)^{1/3} \cdot (\log\log|m|)^{2/3} \cdot ((4/3^{2/3}) + o(1))\Big) \sim \exp((\log|m|)^{1/3} \cdot (\log\log|m|)^{2/3})^{1,9+o(1)}.$$

Diese Zeit enthüllt: Für feste Diskriminante Δ und wachsendes $|m|$ benötigt die Faktorisierung von m immer mehr Zeit, wobei die Laufzeit zur Lösung der entsprechenden Normgleichung $N(\gamma) = m$ über $\mathcal{O}_\Delta$ stark variieren kann.

Kapitel 7

Glatte Zahlen und Ideale

Wir betrachten ganze Ideale in Zahlkörpern von beschränkter Norm, die ausschließlich in Primideale kleiner Norm zerfallen. Für deren Anzahl leiten wir eine untere Schranke her. Hierzu verallgemeinern wir ein Resultat, das bereits für $\mathcal{K} = \mathbb{Q}$ bekannt ist.

Abschließend ziehen wir uns auf den Spezialfall reellquadratischer Ordnungen zurück. Wir schätzen die Anzahl aller reduzierten Ideale, die ausschließlich in Primideale kleiner Norm zerfallen, nach unten ab. Dieses Resultat benötigen wir unter anderem zur Analyse von Algorithmus *RELATION* . Dort können wir dann die Wahrscheinlichkeit folgern, mit der ein zufällig und gleichverteilt gewähltes reduziertes Ideal über einer gegebenen Faktorbasis mindestens zerfällt.

Zunächst wenden wir uns dem rationalen Zahlkörper zu, d.h. wir betrachten $\mathcal{K} = \mathbb{Q}$.

7.1 Glatte Zahlen

Wie H.W. Lenstra jr. und C. Pomerance in [HLPo, Po] definieren wir glatte Zahlen:

7.1 Definition *Gegeben sei eine Zahl $y \in \mathbb{R}_{>0}$. Gilt für alle Primteiler p einer positiven ganzen Zahl n*

$$p \leq y,$$

dann heißt n y-glatt.

Wir sind daran interessiert, wieviele y-glatte Zahlen es bis zu einer oberen Schranke $x \in \mathbb{R}_{>0}$ gibt. Dazu führen wir die Zählfunktion

$$\psi(x, y) = \sharp\{n \in \mathbb{N} \mid n \leq x \text{ und } n \text{ ist } y\text{-glatt}\} \tag{7.1}$$

ein. Für sie existieren zahlreiche Abschätzungen, unter anderem hat C. Pomerance bewiesen: (vgl. [Po])

7.2 Satz *Für alle $\epsilon, x, y \in \mathbb{R}_{>0}$ mit*

$$x > 10 \qquad \text{und} \qquad (\ln x)^{1+\epsilon} < y < \exp\left((\ln x)^{1-\epsilon}\right)$$

gilt die folgende Ungleichung, wobei wir $u = \ln x / \ln y$ setzen:

$$\psi(x,y) \geq x \cdot \exp\left(-u \cdot (\ln u + \ln\ln u + O(1))\right).$$

Wir wollen dieses Konzept auf beliebige Zahlkörper $\mathcal{K}$ übertragen.

7.2 Glatte Ideale

Da ganze Elemente in Zahlkörpern $\mathcal{K}$ im allgemeinen keine eindeutige Zerlegung in Primelemente aus $\mathcal{O}_\mathcal{K}$ besitzen, läßt sich der Begriff der Glattheit nicht direkt auf Zahlkörper übertragen. Gehen wir zu Idealen über, besitzt jedes Ideal eine eindeutige Zerlegung in Primideale. Dann definieren wir den Begriff glatter Ideale. Zur Betonung des zugrundeliegenden Zahlkörpers $\mathcal{K}$ schreiben wir für die Normen $N_{\mathcal{K}/\mathbb{Q}}$.

7.3 Definition *Gegeben sei eine Zahl $y \in \mathbb{R}_{>0}$ und ein Zahlkörper $\mathcal{K}$. Gilt für alle Primideale P, die ein ganzes Ideal A von $\mathcal{K}$, $A \neq 0$, teilen,*

$$N_{\mathcal{K}/\mathbb{Q}}(P) \leq y,$$

dann heißt A y-glatt.

7.4 Bemerkung Für $\mathcal{K} = \mathbb{Q}$ läßt sich jedes ganze Ideal A darstellen als $A = n\mathbb{Z}$ mit $n \in \mathbb{N}$. Die Primideale P sind alle Ideale $p\mathbb{Z}$, wobei $p \in \mathbb{P}$ gilt. Dann ist unsere Definition mit Definition 7.1 konsistent.

Analog führen wir auch hier eine Zählfunktion ein. Für einen zugrundeliegenden Zahlkörper $\mathcal{K}$ sowie $x, y \in \mathbb{R}_{>0}$ setzen wir:

$$\Psi_\mathcal{K}(x,y) = \sharp\{A \neq 0\mathcal{O}_\mathcal{K} \text{ Ideal in } \mathcal{O}_\mathcal{K} \mid N_{\mathcal{K}/\mathbb{Q}}(A) \leq x \text{ und } A \text{ ist } y\text{-glatt}\} \qquad (7.2)$$

Wir sind an einer unteren Schranke für $\Psi_\mathcal{K}(x,y)$ interessiert.

7.2.1 Eine untere Schranke für $\Psi_\mathcal{K}(x,y)$

7.5 Satz *(GRH) Für alle $d \in \mathbb{N}$ und für alle $\epsilon \in \mathbb{R}_{>0}$ existiert eine effektiv berechenbare Konstante $x_0(\epsilon, d) \in \mathbb{R}_{>0}$, so daß für alle $x, y \in \mathbb{R}_{>0}$ mit*

$$x > x_0(\epsilon, d)$$

und für alle Zahlkörper $\mathcal{K}$ vom Grade d mit

$$\max\{(\ln|\Delta_\mathcal{K}|)^{2+\epsilon}, (\ln x)^{1+\epsilon}\} \leq y \leq \exp\left((\ln x)^{1-\epsilon}\right) \qquad (7.3)$$

die folgende Ungleichung gilt:

$$\Psi_{\mathcal{K}}(x,y) \geq x \cdot \exp\left(-u \cdot \left(\ln u + \ln\ln u + O\left(\ln \tilde{d} + \tfrac{1}{\epsilon}\right)\right)\right),$$

wobei $u = \ln x / \ln y$ *und* $\tilde{d}$ *der Grad der normalen Hülle* $\mathcal{N}$ *von* $\mathcal{K}$ *über* $\mathbb{Q}$ *ist.*

Bevor wir diesen Satz im nächsten Abschnitt beweisen, sehen wir uns seine Aussage genauer an und stellen fest:

- Aus $\mathcal{K} = \mathbb{Q}$ folgt die Aussage von Satz 7.2, wobei wir auf die Annahme der verallgemeinerten Riemannschen Vermutung verzichten können. Ferner erhalten wir für den Spezialfall imaginärquadratischer Zahlkörper M. Seysens untere Schranke. (vgl. [Se1, Se2]) Satz 7.5 ist eine Verallgemeinerung auf beliebige Zahlkörper.
- Hazlewood und andere (vgl. [Hz]) erhalten Resultate, die Satz 7.5 ähnlich sehen. In ihren Aussagen ist der zugrundeliegende Zahlkörper jedoch fest, während bei uns die Abschätzungen lediglich vom Grad $\tilde{d}$ der normalen Hülle $\mathcal{N}$ abhängen. Wegen $\tilde{d} \mid d!$ erhalten wir eine Abhängigkeit vom Körpergrad d des zugrundeliegenden Zahlkörpers.

7.2.2 Beweis der unteren Schranke von $\Psi_{\mathcal{K}}(x,y)$

Seien $\epsilon, x, y \in \mathbb{R}_{>0}$, $d \in \mathbb{N}$ und $\mathcal{K}$ ein beliebiger Zahlkörper vom Grad d, der den Bedingungen von Satz 7.5 genügt.

Wir beweisen Satz 7.5, indem wir im wesentlichen der Beweisidee von C. Pomerance aus [Po] sowie von M. Seysen aus [Se1] folgen. Die Verallgemeinerung auf Zahlkörper zieht einige Änderungen nach sich. So basiert der Beweis in [Po] auf einem Zählproblem bzgl. ganzer Zahlen. Um diese Idee zu übernehmen, suchen wir eine Möglichkeit, anstatt ganzer Ideale ganze Zahlen zu betrachten. Dabei legen wir das nachfolgend beschriebene Konzept zugrunde.

Betrachte die normale Hülle $\mathcal{N}$ von $\mathcal{K}$ über $\mathbb{Q}$. Wir beschränken uns auf diejenigen Primzahlen $p \in \mathbb{P}$, die in $\mathcal{N}$ *total zerlegt* sind, d.h. p ist unverzweigt in $\mathcal{N}$, und alle Primideale von $\mathcal{N}$ über p haben Norm p:

$$\mathcal{P} = \{p \in \mathbb{P} \mid p \text{ ist total zerlegt in } \mathcal{N}\}. \tag{7.4}$$

Wir bilden Produkte n über der Menge $\mathcal{P}$. Insbesondere nehmen wir nur Primfaktoren $p \leq y$. n ist dann y-glatt mit der zusätzlichen Eigenschaft, daß alle Primfaktoren $p \in \mathcal{P}$ genügen. Dies berücksichtigen wir bei der Bezeichnung dieser Zahlen.

7.6 Definition *Gegeben seien eine Zahl* $y \in \mathbb{R}_{>0}$ *sowie* $\mathcal{P}$ *gemäß (7.4). Gilt für alle Primteiler einer positiven ganzen Zahl* n

$$p \leq y \qquad \text{und} \qquad p \in \mathcal{P},$$

dann heißt n *y-$\mathcal{P}$-glatt.*

Im folgenden zählen wir alle y-$\mathcal{P}$-glatten Zahlen bis einschließlich x.

$$\psi_{\mathcal{P}}(x,y) = \sharp\{n \in \mathbb{N} \mid n \leq x \text{ und } n \text{ ist } y\text{-}\mathcal{P}\text{-glatt}\} \tag{7.5}$$

Wir zeigen, daß $\psi_{\mathcal{P}}(x,y)$ eine untere Schranke für $\Psi_{\mathcal{K}}(x,y)$ ist. Anschließend schätzen wir $\psi_{\mathcal{P}}(x,y)$ nach unten ab, wobei wir ein Zählproblem bzgl. ganzer Zahlen haben und uns dabei am Beweis von [Po] orientieren.

7.7 Lemma *Für einen Zahlkörper $\mathcal{K}$ und $x, y \in \mathbb{R}_{>0}$ gilt:*

$$\Psi_{\mathcal{K}}(x,y) \geq \psi_{\mathcal{P}}(x,y).$$

Beweis: Sei n eine von $\psi_{\mathcal{P}}(x,y)$ gezählte ganze Zahl und

$$n = \prod_{p \in \mathcal{P}} p^{e_p}$$

ihre Primfaktorzerlegung. Dann existiert für jeden Primfaktor $p \in \mathcal{P}$ ein Primideal der Norm p in $\mathcal{N}$. Deshalb existiert auch ein Primideal $P(p)$ der Norm $p \leq y$ in $\mathcal{K}$.

$$A(n) = \prod_{p \in \mathcal{P}} P(p)^{e_p}$$

ist dann ganzes Ideal von $\mathcal{O}_{\mathcal{K}}$ der Norm $n \leq x$, das von $\Psi_{\mathcal{K}}(x,y)$ gezählt wird. Wir können also eine Abbildung $n \mapsto A(n)$ angeben, die jede von $\psi_{\mathcal{P}}(x,y)$ gezählte Zahl n auf ein von $\Psi_{\mathcal{K}}(x,y)$ erfaßtes Ideal $A(n)$ abbildet. Da diese Abbildung injektiv ist, folgt die Behauptung. ∎

Von nun an schätzen wir $\psi_{\mathcal{P}}(x,y)$ nach unten ab. Ziel ist es, die von $\psi_{\mathcal{P}}(x,y)$ gezählten Zahlen auf mehrere Mengen „aufzuteilen". Dies beschreiben wir genauer:

Sei dazu $u = \ln x / \ln y$ wie in Satz 7.5. Aus (7.3) folgt, daß

$$\ln u \geq \ln\ln x - (1-\epsilon) \cdot \ln\ln x = \epsilon \cdot \ln\ln x.$$

Wir wählen $x_1 = x_1(\epsilon)$ so, daß $\ln u \geq 3$ für alle $x \geq x_1$. Dann definieren wir

$$w_1 = y^{1-2/(3\ln u)} \qquad \text{und} \qquad w_2 = y^{1-1/(3\ln u)}, \tag{7.6}$$

woraus $w_1 < w_2 < y$ folgt. Wir bilden Produkte, deren Primfaktoren zwischen w_1 und w_2 liegen; genauer betrachten wir die Menge

$$\mathcal{M} = \{m \in \mathbb{N} \mid m \text{ hat genau } [u] \text{ Primfaktoren } p \in \mathcal{P} \text{ mit } w_1 < p \leq w_2\}. \tag{7.7}$$

Dann können wir ähnlich wie in [Po] folgern:

7.8 Lemma *Für alle $x, y \in \mathbb{R}_{>0}$ mit $x > x_1$ gilt:*

$$\psi_{\mathcal{P}}(x,y) \geq \sum_{m \in \mathcal{M}} \psi_{\mathcal{P}}\left(\frac{x}{m}, w_1\right). \tag{7.8}$$

Beweis: Sei $n \in \mathbb{N}$ eine Zahl, die von $\psi_{\mathcal{P}}(x/m, w_1)$ für ein $m \in \mathcal{M}$ gezählt wird, dann gilt $n \leq x/m$, woraus

$$n \cdot m \leq x$$

folgt, und n ist w_1-$\mathcal{P}$-glatt, d.h. jeder Primfaktor p von k erfüllt $p \in \mathcal{P}$ sowie $p \leq w_1$. Ebenso genügt jeder Primfaktor p von m gemäß (7.7) $p \in \mathcal{P}$ und $p \leq w_2$. Wegen (7.6) besteht das Produkt $n \cdot m$ nur aus Primfaktoren $\leq y$ aus $\mathcal{P}$, somit wird $n \cdot m$ von $\psi_{\mathcal{P}}(x, y)$ erfaßt.
Weiterhin wissen wir, falls

$$n \cdot m = n' \cdot m',$$

für ein weiteres $m' \in \mathcal{M}$ und n' bzgl. $\psi_{\mathcal{P}}(x/m', w_1)$ gilt, dann erhalten wir $m = m'$ und $n = n'$. Dies folgt aus der Tatsache, daß n, n' nur Primfaktoren $\leq w_1$ und m, m' nur Primfaktoren $> w_1$ enthalten. Es finden demnach bei der Summenbildung in (7.8) keine Mehrfachzählungen statt. ■

Sei nun $m \in \mathcal{M}$ beliebig. Wir fahren fort, indem wir jeweils eine untere Schranke für $\psi_{\mathcal{P}}(x/m, w_1)$ bestimmen: Dazu zählen wir lediglich solche Zahlen $\leq x/m$, die aus genau $u(m)$ verschiedenen Primfaktoren $p \in \mathcal{P}$ und $p \leq w(m)$ bestehen, wobei $u(m)$, $w(m)$ noch genauer zu spezifizierende Größen sind. Daraus erhalten wir ein kombinatorisches Zählproblem, dessen Lösung eine untere Schranke für $\psi_{\mathcal{P}}(x/m, w_1)$ liefert.

Zunächst definieren wir die bereits erwähnten Größen $u(m)$ und $w(m)$:

$$u(m) = 1 + \left[\frac{\ln(x/m)}{\ln w_1}\right] \qquad \text{und} \qquad w(m) = \left(\frac{x}{m}\right)^{1/u(m)}. \tag{7.9}$$

Zur weiteren Untersuchung benötigen wir einige Abschätzungen für $u(m), w(m)$. Wie in [Se1], Nummer (5.7) erhalten wir:

7.9 Lemma *Es existiert eine effektiv berechenbare Konstante $x_2 = x_2(\epsilon) \in \mathbb{R}_{>0}$, so daß für alle $x > x_2$ gilt:*

$$x^{1/(3\ln u)} \leq \frac{x}{m} < x^{1/\ln u}. \tag{7.10}$$

Daraus folgern wir für $u(m)$ mit Hilfe von (7.9) wie in [Se1], Nummer (5.8):

$$u(m) \leq \frac{u}{\ln u} \cdot \left(1 + O\left(\frac{1}{\ln u}\right)\right). \tag{7.11}$$

Ebenfalls wie in [Se1], Nummer (5.9) leiten wir für $w(m)$ her:

7.10 Lemma *Für alle $x > x_2$ gilt:*

$$w_1^{1-(3\ln u)/u} \leq w(m) \leq w_1. \tag{7.12}$$

Dann folgern wir zunächst $\psi_{\mathcal{P}}\left(x/m, w_1\right) \geq \psi_{\mathcal{P}}\left(x/m, w(m)\right)$ für alle $x > x_2$. Definieren wir für $w \in \mathbb{R}_{>0}$

$$\pi_{\mathcal{P}}(w) = \sharp\{p \in \mathcal{P} \mid p \leq w\}, \tag{7.13}$$

beweisen wir für $\psi(x/m, w_1)$ das folgende Resultat:

7.11 Lemma *Für alle $x \in \mathbb{R}_{>0}$ mit $x > x_2$ gilt:*

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w_1\right) \geq \left(\frac{\pi_{\mathcal{P}}(w(m))}{u(m)}\right)^{u(m)}. \tag{7.14}$$

Beweis: Wie bereits erwähnt folgt aus (7.12) für alle $x > x_2$:

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w_1\right) \geq \psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) \geq \binom{\pi_{\mathcal{P}}(w(m))}{u(m)},$$

wobei die letzte Ungleichung mit Hilfe der Definition von $w(m)$ in (7.9) und folgendem kombinatorischen Argument gilt: $\psi_{\mathcal{P}}(x/m, w(m))$ zählt mindestens alle Zahlen, die aus genau $u(m)$ *verschiedenen* Primfaktoren $p \leq w(m)$ aus $\mathcal{P}$ bestehen. Dann folgt die Behauptung. ■

Als nächstes bestimmen wir eine untere Schranke für $\pi_{\mathcal{P}}(w(m))$. Dazu benötigen wir einige Vorbereitungen. Detaillierte Schilderungen des nachfolgend beschriebenen Sachverhaltes finden sich in [We], Abschnitt 4.10. Die normale Hülle $\mathcal{N}$ von $\mathcal{K}$ über $\mathbb{Q}$ ist galoissch. Mit

$$G = gal(\mathcal{N}, \mathbb{Q})$$

bezeichnen wir die *Galoisgruppe* von $\mathcal{N}/\mathbb{Q}$. Für jedes $p \in \mathbb{P}$, p unverzweigt in $\mathcal{N}$ sei $\wp$ ein Primideal in $\mathcal{O}_{\mathcal{N}}$ der Norm q. Dann existiert ein eindeutiger Automorphismus $\sigma_p \in G$ bzgl. p, der den Automorphismus $x \mapsto x^q$, $x \in \mathbb{F}_q$, auf den endlichen Körper $\mathbb{F}_q$ der Charakteristik p induziert. Wir nennen

$$\sigma_p = \left[\frac{\mathcal{N}, \mathbb{Q}}{p}\right]$$

den *Frobenius-Automorphismus* bzgl. p und

$$[\sigma_p] = \{\tau \circ \sigma_p \circ \tau^{-1} \mid \tau \in G\}$$

die zugehörige Konjugiertenklasse. Wir konzentrieren uns auf die Anzahl

$$\pi_{id}(w) = \sharp\{p \in \mathbb{P} \mid p \text{ unverzweigt in } \mathcal{N},\ p \leq w \text{ und } [\sigma_p] \subseteq [id]\}$$

für $w \in \mathbb{R}_{>0}$. Dann stellen wir fest:

7.12 Lemma *Für alle $w \in \mathbb{R}_{>0}$ und $p \in \mathcal{P}$ gilt:*

$$\pi_{id}(w) = \pi_{\mathcal{P}}(w). \tag{7.15}$$

Beweis: Seien $w \in \mathbb{R}_{>0}$ und $p \in \mathcal{P}$. Dann gilt für $\pi_{id}(w)$:

$$\pi_{id}(w) = \sharp\{p \in \mathbb{P} \mid p \text{ unverzweigt in } \mathcal{N},\ p \leq w \text{ und } [\sigma_p] = [id]\}$$

Gemäß [We], Proposition 4-10-11 wissen wir: $[\sigma_p] = [id]$ genau dann, wenn p total zerlegt ist in $\mathcal{N}$. Damit erhalten wir gemäß der Definition von $\pi_{\mathcal{P}}(w)$ in (7.13):

$$\begin{aligned} \pi_{id}(w) &= \sharp\{p \in \mathbb{P} \mid p \text{ total zerlegt in } \mathcal{N} \text{ und } p \leq w\} \\ &= \pi_{\mathcal{P}}(w). \end{aligned}$$ ■

Wollen wir $\pi_{\mathcal{P}}(w(m))$ abschätzen, wenden wir wegen (7.15) Resultate für $\pi_{id}(w(m))$ an, die sich aus dem Satz von Chebotarev ([Nk], Theorem 7.10) ergeben. Das ist auch der Grund, weshalb wir zu Beginn des Beweises von $\mathcal{K}$ zur normalen Hülle $\mathcal{N}$ übergehen. Wie in Satz 7.5 bezeichnen wir mit $\tilde{d}$ den Grad von $\mathcal{N}$ über $\mathbb{Q}$.

7.13 Lemma *(GRH) Für alle $\delta \in \mathbb{R}_{>0}$ existiert eine effektiv berechenbare Konstante $w_3 = w_3(\delta, d) > 0$, so daß für alle $w \in \mathbb{R}_{>0}$ mit $w \geq \max\{w_3, (\ln|\Delta_{\mathcal{K}}|)^{2+\delta}\}$ gilt:*

$$\pi_{\mathcal{P}}(w) \geq \frac{1}{2\tilde{d}} \cdot \frac{w}{\ln w}. \tag{7.16}$$

Beweis: Mit (GRH) gilt gemäß einem Resultat von J. Oesterlé (vgl. Theorem 4 in [Oe]), einer sogenannten effektiven Version des Satzes von Chebotarev, für alle $w \in \mathbb{R}_{\geq 2}$:

$$\left|\pi_{\mathcal{P}}(w) - \frac{1}{\tilde{d}} \cdot Li(w)\right| \leq \frac{1}{\tilde{d}} \cdot \sqrt{w} \cdot (2\ln|\Delta_{\mathcal{N}}| + \tilde{d}\ln w),$$

wobei $Li(w) = \int_2^w 1/\ln t \; dt$ das *logarithmische Integral* ist. Wir schätzen $Li(w)$ ab und ersetzen $\Delta_{\mathcal{N}}$ durch einen Term bzgl. $\Delta_{\mathcal{K}}$. Letzteres läßt sich mit einem Resultat von H. Stark (vgl. Lemma 7 in [St]) erreichen: Mit $\Delta_{\mathcal{N}} \mid \Delta_{\mathcal{K}}^{\tilde{d}}$ erhalten wir:

$$\begin{aligned}\left|\pi_{\mathcal{P}}(w) - \frac{1}{\tilde{d}} \cdot \int_2^w \frac{1}{\ln t}\, dt\right| &\leq \frac{1}{\tilde{d}}\sqrt{w} \cdot (2\tilde{d}\ln|\Delta_{\mathcal{K}}| + \tilde{d}\ln w) \\ &= \sqrt{w} \cdot (2\ln|\Delta_{\mathcal{K}}| + \ln w).\end{aligned}$$

Anwenden des Mittelwertsatzes auf $\int_2^w 1/\ln t \; dt$ liefert schließlich:

$$\pi_{\mathcal{P}}(w) \geq \frac{1}{\tilde{d}} \cdot \frac{w-2}{\ln w} - \sqrt{w} \cdot (2\ln|\Delta_{\mathcal{K}}| + \ln w).$$

Falls $w \geq (\ln|\Delta_{\mathcal{K}}|)^{2+\delta}$, gilt $\ln|\Delta_{\mathcal{K}}| \leq w^{1/(2+\delta)}$, und wir folgern:

$$\pi_{\mathcal{P}}(w) \geq \frac{1}{\tilde{d}} \cdot \left(\frac{w-2}{\ln w} - \tilde{d}\sqrt{w} \cdot (2w^{1/(2+\delta)} + \ln w)\right),$$

woraus für hinreichend großes w, d.h. $w \geq w_3 = w_3(\delta, d)$, die Behauptung folgt. ■

Mit diesem allgemeinen Resultat bestimmen wir eine untere Schranke für $\pi_{\mathcal{P}}(w(m))$.

7.14 Lemma *(GRH) Es existiert eine effektiv berechenbare Konstante $x_3 = x_3(\epsilon, d) \in \mathbb{R}_{>0}$, so daß für alle $x > x_3$ gilt:*

$$\pi_{\mathcal{P}}(w(m)) \geq \frac{1}{2\tilde{d}} \cdot \frac{w(m)}{\ln w(m)}. \tag{7.17}$$

Beweis: Um (7.16) anzuwenden, müssen wir klären, ob die Voraussetzungen erfüllt sind:

$$w(m) \geq w_1^{1-(3\ln u)/u} \geq y^{1-2/(3\ln u)-(3\ln u)/u}$$

gilt für $w(m)$ gemäß (7.12) und (7.6). Aus der Voraussetzung für y in (7.3) ergibt sich dann:

$$\begin{aligned} w(m) &\geq (\ln|\Delta_{\mathcal{K}}|)^{2+\epsilon-(2+\epsilon)(2/(3\ln u)+(3\ln u)/u)} \\ &\geq (\ln|\Delta_{\mathcal{K}}|)^{2+\epsilon/2} \end{aligned}$$

für x hinreichend groß gemäß (7.3) bzgl. x und $\ln|\Delta_{\mathcal{K}}|$; daraus ist ersichtlich, daß $x \to \infty$ $y \to \infty$ impliziert, woraus $w(m) \to \infty$ folgt. Wegen (7.11) und (7.16) existiert dann eine berechenbare Konstante $x_3 = x_3(\epsilon, d)$, so daß für $x > x_3$ die Behauptung folgt. ∎

Daraus folgern wir eine Abschätzung für $\psi_{\mathcal{P}}(x/m, w_1)$ mit (7.11):

7.15 Korollar *(GRH) Es existieren effektiv berechenbare Konstanten $c_1 \in \mathbb{R}_{>0}$ und $x_4 = x_4(\epsilon, d) \in \mathbb{R}_{>0}$, so daß für alle $x > x_4$ gilt:*

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) \geq \frac{x}{m} \cdot \exp\left(-u \cdot c\left(\frac{1}{\epsilon} + \ln \tilde{d}\right)\right).$$

Beweis: Anwenden von (7.17) auf Lemma 7.11 liefert direkt: Für $x > x_3$ gilt

$$\begin{aligned} \psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) &\geq \left(\frac{w(m)}{2\tilde{d} \cdot \ln w(m) \cdot u(m)}\right)^{u(m)} \\ &= \frac{x}{m} \cdot \exp\left(-u(m) \cdot \left(\ln u(m) + \ln\ln w(m) + \ln(2\tilde{d})\right)\right) \end{aligned}$$

gemäß der Definition für $w(m)$ in (7.9). Wegen $w(m) \leq w_1 \leq y$ gemäß (7.12) sowie der Abschätzung für $u(m)$ in (7.11) folgt:

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) \geq \frac{x}{m} \cdot \exp\left(-u(m) \cdot \left(\ln u - \ln\ln u + \ln\ln y + \ln \tilde{d} + O(1)\right)\right).$$

Aus der Definition von u in Satz 7.5 und (7.3) leiten wir $\ln\ln y \leq (1-\epsilon)/\epsilon \cdot \ln u$ her und folgern, daß

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) \geq \frac{x}{m} \cdot \exp\left(-u(m) \cdot \left(\frac{1}{\epsilon}\ln u - \ln\ln u + \ln \tilde{d} + O(1)\right)\right)$$

gilt. Ebenso wissen wir $\ln\ln u \geq 0$ wegen $x > x_1$. Deshalb können wir

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) \geq \frac{x}{m} \cdot \exp\left(-u(m) \cdot \ln u \left(\frac{1}{\epsilon} + \ln \tilde{d} + O(1)\right)\right)$$

für alle $x > x_4$ abschätzen, wobei $x_4 = x_4(\epsilon, d) \in \mathbb{R}_{>0}$ eine effektiv berechenbare Konstante ist. Mit der Abschätzung für $u(m)$ in (7.11) finden wir schließlich eine berechenbare Konstante $c_1 \in \mathbb{R}_{>0}$, so daß für alle $x > x_4$ gilt:

$$\psi_{\mathcal{P}}\left(\frac{x}{m}, w(m)\right) \geq \frac{x}{m} \cdot \exp\left(-u \cdot c_1\left(\frac{1}{\epsilon} + \ln \tilde{d}\right)\right).$$

∎

Daraus folgt mit der Summenaufspaltung in (7.8) sowie $w(m) \leq w_1$ aus (7.12):

7.16 Korollar *(GRH) Für alle $x > x_4$ gilt:*

$$\psi_{\mathcal{P}}(x,y) \geq x \cdot \exp\left(-u \cdot c_1 \cdot \left(\frac{1}{\epsilon} + \ln \tilde{d}\right)\right) \cdot \sum_{m \in \mathcal{M}} \frac{1}{m}.$$

Um den Beweis von Satz 7.5 zu beenden, verbleibt die Summe bzgl. $\mathcal{M}$ abzuschätzen.

7.17 Lemma *(GRH) Es existiert eine effektiv berechenbare Konstante $x_6 = x_6(\epsilon, d) \in \mathbb{R}_{>0}$, so daß für alle $x > x_6$ gilt:*

$$\sum_{m \in \mathcal{M}} \frac{1}{m} \geq \exp\left(-u \cdot (\ln u + \ln\ln u + \ln(5\tilde{d}))\right). \tag{7.18}$$

Beweis: Benutzen wir die Definition von $\mathcal{M}$ aus (7.7), erhalten wir analog zu [Po]

$$\sum_{m \in \mathcal{M}} \frac{1}{m} \geq \frac{1}{[u]!} \cdot \Bigg(\sum_{\substack{p \in \mathcal{P}, \\ w_1 < p \leq w_2}} \frac{1}{p} \Bigg)^{[u]}.$$

Der Argumentation von Seysen in [Se2] folgend erhalten wir analog, daß für $x > x_5$ für $x_5 = x_5(\epsilon, d)) \in \mathbb{R}_{>0}$, eine effektiv berechenbare Konstante, ein $\epsilon_1 \in \mathbb{R}_{>0}$ existiert, so daß gilt:

$$\sum_{\substack{p \in \mathcal{P}, \\ w_1 < p \leq w_2}} \frac{1}{p} \geq \frac{1}{\tilde{d}} \cdot \left(\ln\ln w_2 - \ln\ln w_1 - O(w_1^{-\epsilon_1})\right).$$

Anwenden der Definition von w_1, w_2 auf die Differenz aus (7.6), impliziert die Existenz einer berechenbaren Konstanten $x_6 = x_6(\epsilon, d) \in \mathbb{R}_{>0}$, so daß für $x > x_6$ gilt:

$$\sum_{m \in \mathcal{M}} \frac{1}{m} \geq \exp\left(-u \cdot \left(\ln u + \ln\ln u + \ln(5\tilde{d})\right)\right).$$

■

Einsetzen von (7.18) in Lemma 7.16 liefert die Behauptung von Satz 7.5.

7.3 Anwendung auf reellquadratische Ordnungen

Wir leiten ein Resultat her, das für imaginärquadratische Ordnungen $\mathcal{O}_\Delta$ bereits von M. Seysen bewiesen ist. (vgl. [Se1, Se2]) In der Analyse von *QUCLASSREG* für reellquadratsiche Ordnungen $\mathcal{O}_\Delta$ benötigen wir eine untere Schranke für die Ordnung der Menge

$$\mathcal{Z} = \{A \text{ Ideal in } \mathcal{O}_\Delta \mid A \text{ ist reduziert und zerlegbar über } F_C\}$$

(vgl. 5.35), wobei F_C die zugrundeliegende Faktorbasis aus Korollar 5.2 ist.

Wir übertragen den Beweis der unteren Abschätzung von $\Psi_{\mathcal{K}}(x,y)$, der sich auf beliebige Zahlkörper $\mathcal{K}$ bezieht, auf reellquadratische Ordnungen $\mathcal{O}_\Delta$. Gemäß Lemma 7.7 schätzen wir für $\Psi_{\mathcal{K}}(x,y)$ die Anzahl $\psi_{\mathcal{P}}(x,y)$ ab, was Inhalt des sich dort anschließenden Beweises ist. Genau diesen Beweis werden wir imitieren.

Wir betrachten analog zu (7.4) für $\Delta \in \mathcal{D}^+$

$$\mathcal{P}_\Delta := \mathcal{P} = \{p \in \mathbb{P} \mid (\Delta/p) = 1\}. \tag{7.19}$$

Ist $\mathcal{O}_\Delta$ Maximalordnung, stimmen $\mathcal{P}_\Delta$ und $\mathcal{P}$ aus (7.4) überein. Analog zu (7.5) zählen wir in $\psi_{\mathcal{P}}(x,y)$ alle positiven ganzen y-$\mathcal{P}$-glatten Zahlen $\leq x$. Wir folgern:

7.18 Lemma *Für $\Delta \in \mathcal{D}^+$ und eine Faktorbasis F_C gemäß Korollar 5.2 mit Normschranke $C \in \mathbb{R}_{>0}$ gilt*

$$\sharp\mathcal{Z} \geq \psi_{\mathcal{P}}\ (\sqrt{\Delta}/2, C) - 1.$$

Beweis: Zerfällt ein Ideal A aus $\mathcal{O}_\Delta$ über F_C, besteht es aus invertierbaren Primidealen. (vgl. Lemma 5.17) Deshalb enthält seine Norm $N(A)$ lediglich Primzahlen $p \in \mathcal{P}$ mit $p \leq C$. (vgl. Proposition 2.45 und (5.29)). $N(A)$ ist also C-$\mathcal{P}$-glatt.
Genügt ferner ein primitives Ideal A der Bedingung $L(A) < \sqrt{\Delta}/2$, dann ist es reduziert. (vgl. Lemma 2.52)
Wir zeigen: Jeder C-$\mathcal{P}$-glatten Zahl $n < \sqrt{\Delta}/2$ ordnen wir injektiv ein primitives Ideal der Norm n zu. Dann haben wir jeder – bis eventuell auf $\sqrt{\Delta}/2$ – von $\psi_{\mathcal{P}}(\sqrt{\Delta}/2, C)$ gezählten Zahl ein Ideal aus $\mathcal{Z}$ zugeordnet. Daraus folgt die Behauptung.
Wir geben den ausstehenden Beweis: Sei n eine von $\psi_{\mathcal{P}}(\sqrt{\Delta}/2, C)$ gezählte Zahl,

$$n = \prod_{p \in \mathcal{P}} p^{e_p}$$

ihre Primfaktorzerlegung. Dann liegt für jeden Primfaktor $p \in \mathcal{P}$ das Primideal A_p in F_C; A_p hat Norm p und ist primitiv. (vgl. Proposition 2.40) Ferner ist $A_p^{e_p}$ primitiv wie wir der Konstruktion von *MUL* in 2.36 entnehmen. Analog ist das Ideal

$$A(n) = \prod_{p \in \mathcal{P}} A_p^{e_p}$$

primitiv und hat Norm $n < \sqrt{\Delta}/2$, $A(n)$ ist somit reduziert und zerfällt über F_C, d.h. $A(n) \in \mathcal{Z}$. Diese Abbildung ist injektiv. ■

Im folgenden schätzen wir $\psi_{\mathcal{P}}(\sqrt{\Delta}/2, C)$ nach unten ab, indem wir allgemeiner $\psi_{\mathcal{P}}(x,y)$ für $x, y \in \mathbb{R}_{>0}$ untersuchen. Dazu übernehmen wir den Beweis bzgl. Zahlkörper aus dem vorangegangenen Abschnitt und ändern ihn an den notwendigen Stellen ab.
Bis einschließlich Lemma 7.11 ergeben sich keinerlei Änderungen. Danach haben wir $\pi_{\mathcal{P}}(w(m))$ bzw. wie in (7.13) allgemein für $w \in \mathbb{R}_{>0}$ abzuschätzen:

$$\pi_{\mathcal{P}}(w) = \sharp\{p \in \mathcal{P} \mid p \leq w\}.$$

Die Änderung des Beweises wird hier notwendig, weil wir im ursprünglichen Beweis eine Anwendung des Satzes von Chebotarev benutzen, die auf Zahlkörpern beruht. Daher ziehen wir uns auf die Maximalordnung $\mathcal{O}_{\Delta_0}$ von $\mathcal{O}_\Delta$ mit dem Führer f zurück:

7.19 Lemma *Für $w \in \mathbb{R}_{>0}$ gilt $|\pi_{\mathcal{P}_\Delta} - \pi_{\mathcal{P}_{\Delta_0}}| = O(\ln f)$.*

Beweis: Für $p \in \mathcal{P}_\Delta$ gilt: $(\Delta/p) = 1$, d.h. $p \not| (\Delta = f^2\Delta_0)$ und Δ ist quadratischer Rest mod $4p$. Dies impliziert

$$\begin{aligned} \mathcal{P}_\Delta &= \{p \in \mathbb{P} \mid p \not| f \text{ und } p \not| \Delta_0 \text{ und } (\Delta/p) = 1\} \\ &\subseteq \{p \in \mathbb{P} \mid p \not| \Delta_0 \text{ und } (\Delta_0/p) = 1\} \\ &= \mathcal{P}_{\Delta_0}. \end{aligned}$$

Die Anzahl aller Primzahlen $p \mid f$ ist $O(\ln f)$. (vgl. [RoSc], Nummer (2.29)) ∎

Wir haben einen Bezug zwischen $\pi_{\mathcal{P}_\Delta}$ und $\pi_{\mathcal{P}_{\Delta_0}}$ hergestellt. Dann wenden wir Lemma 7.13 auf $\pi_{\mathcal{P}_{\Delta_0}}$ an, indem wir den Zahlkörper $\mathcal{K} = \mathbb{Q}(\sqrt{\Delta_0})$ vom Grad $d = 2$ mit der normalen Hülle $\mathcal{N} = \mathbb{Q}(\sqrt{\Delta_0})$ vom Grad $\tilde{d} = 2$ zugrundelegen. Wir erhalten:

7.20 Lemma *(GRH) Für alle $\delta \in \mathbb{R}_{>0}$ existiert eine effektiv berechenbare Konstante $w_3' = w_3'(\delta) > 0$, so daß für alle $w \in \mathbb{R}_{>0}$ mit $w \geq \max\{w_3', \ln|4\Delta|^{2+\delta}\}$ gilt:*

$$\pi_{\mathcal{P}_\Delta}(w) \geq O\left(\frac{w}{\ln w}\right).$$

Beweis: $\mathbb{Q}(\Delta_0)$ hat Diskriminante Δ_0 oder $4\Delta_0$, je nachdem, ob $\Delta_0 \equiv 2, 3 \bmod 4$ ist oder nicht. Für $w \in \mathbb{R}_{>0}$ gilt mit Lemma 7.19 und dem Beweis von Lemma 7.13:

$$\begin{aligned} |\pi_{\mathcal{P}_\Delta}(w) - Li(w)/2| &\leq |\pi_{\mathcal{P}_\Delta}(w) - \pi_{\mathcal{P}_{\Delta_0}}(w)| + |\pi_{\mathcal{P}_{\Delta_0}}(w) - Li(w)/2| \\ &\leq O(\ln f) + \sqrt{w} \cdot (2\ln(4\Delta_0) + \ln w) \\ &\leq O(\sqrt{w} \cdot (\ln \Delta + \ln w)). \end{aligned}$$

Dann übertragen wir den Beweis von Lemma 7.13 analog. ∎

Die Konstante in der oberen Schranke $O(w/\ln w)$ spiegelt sich auch in der weiteren Abschätzung für $\pi_{\mathcal{P}_\Delta}(w(m))$ wider. Zu (7.17) erhalten wir völlig analog:

7.21 Korollar *(GRH) Es existiert eine effektiv berechenbare Konstante $x_3' = x_3'(\epsilon) \in \mathbb{R}_{>0}$, so daß für alle $x > x_3'$ gilt:*

$$\pi_{\mathcal{P}}(w(m)) \geq O\left(\frac{w(m)}{\ln w(m)}\right).$$

Die restlichen Aussagen können analog zum Zahlkörperfall übernommen werden, da wir immer von der Existenz einer berechenbaren Konstanten c_1 ausgehen dürfen. Wir erhalten schließlich entsprechend zu Satz 7.5 mit $d = 2$:

7.22 Proposition *(GRH) Für alle $\epsilon \in \mathbb{R}_{>0}$ existiert eine effektiv berechenbare Konstante $x_0(\epsilon)' \in \mathbb{R}_{>0}$, so daß für alle $x, y \in \mathbb{R}_{>0}$ mit $x > x_0(\epsilon)'$ und für alle $\Delta \in \mathcal{D}^+$ mit*

$$\max\{(\ln\Delta)^{2+\epsilon}, (\ln x)^{1+\epsilon}\} \le y \le \exp\left((\ln x)^{1-\epsilon}\right) \tag{7.20}$$

die folgende Ungleichung gilt, wobei wir $u = \ln x / \ln y$ setzen:

$$\psi_{\mathcal{P}}(x,y) \ge x \cdot \exp\left(-u \cdot (\ln u + \ln\ln u + O\left(1/\epsilon\right))\right).$$

Nun kehren wir zu unserem Ausgangsproblem zurück, $\sharp\mathcal{Z}$ in der Analyse von *QU-CLASSREG* nach unten abzuschätzen. Mit Lemma 7.18 wissen wir bereits $\sharp\mathcal{Z} \ge \psi_{\mathcal{P}}(\sqrt{\Delta}/2, C) - 1$. Wir überprüfen Bedingung (7.20) in obiger Proposition, die für $x = \sqrt{\Delta}/2$ und $y = C$ erfüllt sein muß. Wir bestimmen die Schranken in (7.20) für $\epsilon \to 0$ und erhalten für die Bedingung asymptotisch

$$\max\{(\ln\Delta)^2, \ln(\sqrt{\Delta}/2)\} \le C \le \sqrt{\Delta}/2. \tag{7.21}$$

Wegen Korollar 5.2 gehen wir von $C \ge 12(\ln\Delta)^2$ aus und wegen (5.13) von $C \le \sqrt{\Delta}$. Wie wir Abschnitt 5.7 entnehmen, beläuft sich der endgültige Wert von C auf einen subexponentiellen Wert von $\log\Delta$, so daß auch die obere Schranke in (7.20) im Limes erfüllt ist. Es steht noch die Bestimmung von u und $\ln u$ aus. Im Hinblick auf die Anwendung der Abschätzung auf die (asymptotische) Analyse in Kapitel 5 übernehmen wir $C = {L_\Delta}^c$:

7.23 Korollar *(GRH) Für $\Delta \in \mathcal{D}^+$ und $C = {L_\Delta}^c$ mit $c \in \mathbb{R}_{>0}$ und $12(\ln\Delta)^2 \le C \le (\sqrt{\Delta}/2)$ erhalten wir*

$$\sharp\mathcal{Z} \ge \frac{\sqrt{\Delta}}{2} \cdot L_\Delta\left[-\frac{1}{4c}\right].$$

Beweis: Wegen Lemma 7.18 genügt es, $\psi_{\mathcal{P}}(\sqrt{\Delta}/2, C)$ abzuschätzen. Mit Proposition 7.22 gilt dann:

$$\begin{aligned} \psi_{\mathcal{P}}(\sqrt{\Delta}/2, C) &\ge \sqrt{\Delta}/2 \cdot \exp(-u \cdot (\ln u + \ln\ln u + O(1/\epsilon))) \\ &\ge \sqrt{\Delta}/2 \cdot \exp(-u \cdot \ln u \cdot (1 + o(1))). \end{aligned}$$

Wir schätzen die Faktoren u und $\ln u$ ab. Für $u = (\ln(\sqrt{\Delta}/2))/(\ln {L_\Delta}^c)$ ergibt sich:

$$u \le \frac{(\ln\Delta)/2}{c \cdot \sqrt{\ln\Delta \cdot \ln\ln\Delta}} \le \frac{1}{2c} \cdot (\ln\Delta)^{1/2} \cdot (\ln\ln\Delta)^{-1/2}.$$

Damit erhalten wir $\ln u \le \frac{1}{2}\ln\ln\Delta \cdot (1 + o(1))$. Dann ergibt sich insgesamt:

$$\begin{aligned} \exp(-u \cdot \ln u \cdot (1 + o(1))) &\ge \exp(-1/(4c) \cdot (\ln\Delta)^{1/2} \cdot (\ln\ln\Delta)^{1/2} \cdot (1 + o(1))) \\ &= \exp(\sqrt{\ln\Delta \cdot \ln\ln\Delta} \cdot (-1/(4c) + o(1))) \\ &= L_\Delta[-1/(4c)], \end{aligned}$$

woraus die Behauptung folgt. ■

Literaturverzeichnis

[AkL] A. K. Lenstra, *Fast and rigorous factorization under the generalized Riemann hypothesis*, Technical report, University of Chicago, **87 - 007**, (1987).

[Ba] E. Bach, *Explicit bounds for primality testing and related problems*, Mathematics of Computation **55**, (1990), 355 - 380.

[BiBu] I. Biehl & J. Buchmann, *Algorithms for quadratic orders*, Proceedings of Symposium on Mathematics of Computation, (1993).

[Br] R. Brent, *Multiple-precision zero-finding methods and the complexity of elementary function evaluation*, Proceedings of the Symposium on Analytical Computational Complexity, edited by J. F. Traub, Academic Press, New York, (1976), 151 - 176.

[BSW] J. Buchmann & R. Scheidler & H. C. Williams, *A key exchange protocol using real quadratic fields*, Journal of Cryptology, (1994).

[Bu1] 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, 28 - 41.

[Bu2] J. Buchmann, *On the computation of units and class numbers by a generalization of Lagrange's algorithm*, Journal of Number Theory, **26**, (1987), 8 - 30.

[BuHo] J. Buchmann & C. Hollinger, *On smooth ideals in number fields*, erscheint in Journal of Number Theory.

[BuKe] J. Buchmann & V. Kessler, *Computing a reduced lattice basis from a generating system*, Manuskript, (1992).

[BuMü] J. Buchmann & Ac. Müller, *Linear algebra over* $\mathbb{Z}$, Manuskript, (1994), wird veröffentlicht.

[BuWi] J. Buchmann & H.C. Williams, *On the computation of the class number of an algebraic number field*, Mathematics of Computation, **53**, (1989), 679 - 688.

[BW] J. Buchmann & H. C. Williams, *Algorithms for quadratic orders*, Manuskript, (1994).

[Co] H. Cohen, *A course in computational algebraic number theory*, Springer Verlag, (1991).

[CoHL] H. Cohen & H. W. Lenstra jr., *Heuristics on class groups of number fields*, Lecture Notes in Mathematics, **1068**, Number Theory, (1983), 33 - 62.

[DKT] P. D. Domich & R. Kannan & L. E. Trotter jr., *Hermite normal form computation using modulo determinant arithmetic*, Mathematics of operation research, **12**, (1987).

[Dü] S. Düllmann, *Ein Algorithmus zur Bestimmung der Klassengruppe positiv definiter binärer quadratischer Formen*, Dissertation, Universität des Saarlandes, (1991).

[HaMc] J. L. Hafner & K. S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, Journal American Mathematical Society **2**, (1989), 837 - 850.

[Ga] C. F. Gauß, *Disquisitiones Arithmeticae*, Leipzig, Fleischer, (1801).

[HeFe] F. Heigl & J. Feuerpfeil, *Stochastik*, BSV, (1974).

[HLPo] H. W. Lenstra jr. & C. Pomerance, *A rigorous time bound for factoring integers*, J. American Society, **5**, (1992), 483 - 516.

[HwL] H. W. Lenstra jr., *On the calculation of regulators and class numbers of quadratic fields*, London Mathematical Society Lecture Notes, **56**, (1982), 123 -150.

[Hu] T. W. Hungerford, *Algebra*, Springer Verlag, (1989).

[Hz] D. G. Hazlewood, *On ideals having only small prime factors*, Rocky Mountain Journal of Mathematics, **7**, (1977), 753 - 768.

[KaKw] P. Kaplan & K. S. Williams, *The distance between ideals in the orders of a real quadratic field*, preprint.

[LL] A. K. Lenstra & H. W. Lenstra jr., *The development of the number field sieve*, Lecture Notes in Mathematics, **1554**, (1993).

[LLL] A. K. Lenstra & H. W. Lenstra jr. & C. Lovacz, *Factoring polynomials with rational coefficients*, Mathematsche Annalen, **261**, (1982), 515 - 534.

[NaSh] I. Nassi, B. Shneiderman, *Flowchart techniques for structured programming*, SIGPLAN Notices **8**, (1973), 12–26.

[Mc] K. S. McCurley, *Cryptographic key distribution and computation in class groups*, Number Theory and applications, edited by R. A. Mollin, NATO ASI series, Series C **265**, Dordrecht 1989, 459 - 479.

[Nk] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Scientific Publishers, (1974).

[Oe] J. Oesterlé, *Versions effectives du théorème de Chebotarev sous l' hypothèse de Riemann généralisée*, Société mathématique de France, Astérisque **61**, (1979), 165 - 167.

[Po] C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational methods in number theory I, edited by H.W. Lenstra jr. & R. Tijdeman, Mathematical Centre Tracts, (1987), 89 -140.

[PhZa] M. Pohst & H. Zassenhaus, *Algorithmic number theory*, Cambridge University Press, (1989).

[RoSc] J. Rosser & L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics, **6**, (1985), 64 - 94.

[Se1] M. Seysen, *A probabilistic factorization algorithm with quadratic forms of negative discriminant*, Mathematics of Computation, **48**, no. 178, (1987), 757 - 780.

[Se2] M. Seysen, *Ein probabilistischer Faktorisierungsalgorithmus mit quadratischen Formen negativer Diskriminante*, Dissertation, Universität Frankfurt am Main, (1984).

[Sc] R. Schoof, *Quadratic fields and factorization*, Computational methods in number theory II, edited by H.W. Lenstra jr. & R. Tijdeman, Mathematical Centre Tracts, (1987), 235 - 286.

[Sh] D. Shanks, *The infrastructure of a real quadratic field and its applications*, Proceedings 1972 Number Theory Conference, Boulder, (1972), 217 - 224.

[SpWi] A. J. Stephens & H. C. Williams, *Some computational results on a problem concerning powerful numbers*, Mathematics of computation, **50**, (1988), 619 - 632.

[St] H.M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Inventiones mathematicae, **23**, (1974), 135 - 152.

[We] E. Weiss, *Algebraic number theory*, McGraw-Hill Book Company Inc., (1963).

[WiWu] H. C. Williams & M. C. Wunderlich, *On the parallel generation of the residues for the continued fraction factoring algorithm*, Mathematics of computation, **177**, (1987), 1 - 31.

Stichwortverzeichnis