

Factor Refinement in Quadratischen Zahlkörpern

Diplomarbeit
von
Friedrich Eisenbrand

nach einem Thema von
Prof. Dr. Johannes Buchmann
Fachbereich 14 – Informatik –
Universität des Saarlandes

4. September 1996

Eidesstattliche Erklärung

„Hiermit versichere ich an Eides statt, daß ich diese Arbeit selbständig und nur unter Verwendung der angegebenen Quellen angefertigt habe.“

Saarbrücken, den 4. September 1996

Friedrich Eisenbrand

Ich danke Herrn Prof. Dr. Johannes Buchmann für die Vergabe des interessanten Themas und seine Unterstützung bei der Bearbeitung. Herrn Dr. Volker Müller danke ich herzlich für Anregungen und Diskussion.

Einleitung

Wie entscheidet man für natürliche Zahlen a, b, c, i, j, k ob

$$a^i b^j = c^k \tag{0.1}$$

gilt? Eine Möglichkeit ist die Binärdarstellungen von $a^i b^j$ und c^k auszurechnen. Die Länge der Binärdarstellung von c^k ist $\Theta(k \text{ size}(c))$, also exponentiell in der Länge der Darstellung von k . Diese Methode ist also ungeeignet. Der Factor Refinement Algorithmus **refine** aus [BDS93] berechnet in quadratischer Zeit paarweise teilerfremde Zahlen $n_1, \dots, n_k \in \mathbb{Z}$, wobei jede der Zahlen a, b und c Potenzprodukte der n_μ sind und jedes n_μ a, b oder c teilt. Durch sukzessives Dividieren lassen sich effizient die Faktorisierungen

$$\begin{aligned} a &= n_1^{\alpha_1} \cdots n_k^{\alpha_k} \\ b &= n_1^{\beta_1} \cdots n_k^{\beta_k} \\ c &= n_1^{\gamma_1} \cdots n_k^{\gamma_k} \end{aligned}$$

ausrechnen. Die Gleichung (0.1) gilt genau dann, wenn $i\alpha_\mu + j\beta_\mu = k\gamma_\mu$, $1 \leq \mu \leq k$. Der Algorithmus **refine** sucht in einer Menge \mathcal{M} von natürlichen Zahlen nach einem Zahlenpaar $m_1, m_2 \in \mathcal{M}$ mit nichttrivialem ggT $d = \text{ggT}(m_1, m_2)$, streicht diese Zahlen aus \mathcal{M} und fügt $m_1/d, d, m_2/d$ in \mathcal{M} ein. Dies wird solange wiederholt, bis es in \mathcal{M} keine Zahlenpaare mit nichttrivialem ggT mehr gibt. In [BDS93] wird außerdem eine Charakterisierung des Outputs von **refine** angegeben und quadratische Laufzeit bewiesen.

Dieses Verfahren läßt sich nicht ohne weiteres auf Ordnungen übertragen, da ein ggT dort im allgemeinen nicht existiert. H.W. Lenstra schlug in [Len92] vor, die Factor Refinement Methode auf Ideale von Ordnungen zu übertragen um effizient zu testen, ob Potenzprodukte von Elementen einer Ordnung eine Einheit der Maximalordnung darstellen. G. Ge konkretisierte diese Idee in [Ge93], gab aber keine expliziten Laufzeiten oder eine Charakterisierung des Outputs seines Algorithmus an.

Ziel meiner Arbeit ist, den Factor Refinement Algorithmus für quadratische Ordnungen zu untersuchen. In Kapitel 1 werden die Grundlagen erklärt. In Kapitel 2 stelle ich den Algorithmus **refine** vor und zeige eine Charakterisierung des Outputs analog zu der Arbeit [BDS93]. Dabei tritt eine interessante Gesetzmäßigkeit zum Vorschein: Findet sich im Verfeinerungsprozess ein nichtinvertierbares Ideal, wird es notwendig in eine höhere Ordnung aufzusteigen und man erhält einen nichttrivialen Faktor der Diskriminante. Es ergibt sich eine Minimalitätseigenschaft der zurückgelieferten Oberordnung, man kommt also der Fundamentaldiskriminante mit **refine** nur so nah wie nötig, um den Input als Potenzprodukt invertierbarer teilerfremder Ideale darstellen zu können.

Kapitel 3 enthält Algorithmen für Arithmetik auf Idealen und deren Bitkomplexitäten. Diese Resultate werden in Kapitel 4 benutzt um kubische Laufzeit von **refine** zu beweisen.

Inhaltsverzeichnis

1 Grundlagen	7
1.1 Arithmetische Operationen	7
1.2 Der euklidische Algorithmus	8
1.3 Abelsche Gruppen	10
1.4 Ideale	12
1.5 Algebraische und ganze Zahlen	13
1.6 Moduln und Multiplikatorenringe	14
1.6.1 Moduln	14
1.6.2 Multiplikatorenringe	15
1.6.3 Normen von Moduln	16
1.6.4 Multiplikation und Addition von Moduln	17
1.7 Diskriminanten und Maximalordnungen	18
1.8 Quadratische Zahlkörper	19
1.8.1 Ideale quadratischer Ordnungen	23
1.8.2 Darstellung im Rechner	26
2 Der Algorithmus Refine	27
2.1 Faktorisierungen	27
2.2 Refine	29
2.3 Der Output von Refine	32

3	Arithmetik auf Idealen	38
3.1	Addition	38
3.2	Liften	40
3.3	Multiplikation	42
4	Analyse des Algorithmus refine	44
4.1	Initialisierung	44
4.2	Liften	45
4.3	Auffinden von nichtteilerfremden Idealen	46
4.4	Berechnen von d in Zeile (6)	46
4.5	Verfeinerungsschritte	46
	Ausblick	47
	Bezeichnungen	48

Kapitel 1

Grundlagen

1.1 Arithmetische Operationen

Eine ganze Zahl $z \neq 0$ ist eindeutig durch ein Tupel

$$(v, a_k, \dots, a_0) \in \{0, 1\}^{k+2}, a_k = 1 \quad (1.1)$$

mit $z = (-1)^v \sum_{j=0}^k a_j 2^j$ darstellbar. Die Zahl 0 soll durch $(0, 0)$ dargestellt werden. Wir definieren auf der Menge der ganzen Zahlen die Funktion

$$\text{size}(z) = \begin{cases} 2 & \text{wenn } z = 0 \\ 2 + \lfloor \log(|z|) \rfloor & \text{sonst.} \end{cases}$$

Dabei steht $\text{size}(z)$ für die Länge der Darstellung der Zahl z .

1.1. Lemma Es gibt Konstanten k_1 und k_2 so daß für alle ganzen Zahlen z mit $|z| \geq 2$

$$\begin{aligned} \text{size}(z) &\leq k_1 \log(|z|), \\ \log(|z|) &\leq k_2 \text{size}(z). \end{aligned}$$

Für ganze Zahlen z_1 und $z_2 \neq 0$ soll mit $z_1 = qz_2 + r$, wobei $0 \leq r < |z_2|$, z_1/z_2 die Zahl q und $z_1 \bmod z_2$ die Zahl r sein.

Die Schulmethoden für Arithmetik liefern uns folgende Laufzeiten:

Operation	Zeit
$c = a \pm b$	$O(\max\{\text{size}(a), \text{size}(b)\})$
$c = ab$	$O(\text{size}(a) \text{size}(b))$
$a = qb + r, 0 \leq r < b $	$O(\text{size}(q) \text{size}(b))$

Beachte, daß für ganze Zahlen z_1, z_2 und eine Operation $\omega \in \{+, -, *, /, \bmod\}$

$$\text{size}(z_1 \omega z_2) \leq \text{size}(z_1) + \text{size}(z_2)$$

gilt.

1.2. Lemma Um einen Ausdruck T mit ganzen Zahlen z_1, \dots, z_s mit $\text{size}(z_i) \leq l$ und k Operationszeichen aus $\{+, -, *, /, \text{ mod } \}$ auszuwerten, braucht man Zeit $O(k^2 l^2)$. Für das Ergebnis $e(T)$ gilt dann $\text{size}(e(T)) \leq (k+1)l$.

Beweis: Die Behauptung sieht man leicht, wenn man annimmt, daß der Term T in polnischer Notation (siehe [LMW86]) vorliegt. Sei c eine Konstante, mit der man für ganze Zahlen a, b den Term $ab\omega$ in Zeit $c \text{size}(a) \text{size}(b)$ auswerten kann. Man behauptet daß die Zeit die zum Auswerten von T benötigt wird kleiner als $ck^2 l^2$ ist.

Ist $k = 0$, dann stimmt die Behauptung.

Ist $k > 0$, dann ist $T = T_1 T_2 \omega$. T_1 hat dann k_1 Operationszeichen und T_2 hat k_2 Operationszeichen mit $k_1 + k_2 = k - 1$. Das Ergebnis $e(T_i)$ von T_i , $i = 1, 2$, kann man in Zeit $ck_i^2 l^2$ berechnen. Die Länge des Ergebnisses $e(T_i)$ ist mit $(k_i + 1)l$ beschränkt. $e(T_1)e(T_2)\omega$ kann man in Zeit $c(k_1 + 1)(k_2 + 1)l^2$ auswerten. Es gilt dann $\text{size}(e(T)) \leq (k_1 + k_2 + 2)l = (k + 1)l$. Die Gesamtkosten sind:

$$\begin{aligned} c(k_1^2 + k_2^2 + k_1 k_2 + k_1 + k_2 + 1)l^2 &= c((k_1 + k_2)^2 - k_1 k_2 + k)l^2 \\ &\leq c((k - 1)^2 + k)l^2 \\ &\leq ck^2 l^2. \end{aligned}$$

■

1.3. Bemerkung Führt ein Algorithmus auf seinem Input eine feste Anzahl an elementaren Operationen durch, dann ist die Bitkomplexität dafür quadratisch in der Länge der Eingabe.

1.2 Der euklidische Algorithmus

Der größte gemeinsame Teiler zweier ganzer Zahlen läßt sich effizient mit dem euklidischen Algorithmus berechnen.

1.4. Algorithmus euklid

EINGABE: $a \geq b \geq 0$

AUSGABE: (d, x, y) mit $d = \text{ggT}(a, b)$ und $xa + yb = d$

- (1) **if** $(b = 0)$ **then**
- (2) **return** $((a, 1, 0))$
- (3) **else**
- (4) Berechne q und r mit $a = qb + r$ und $0 \leq r < b$
- (5) $(d, x', y') := \text{euklid}(b, r)$
- (6) $x := y'$
- (7) $y := x' - y'q$
- (8) **return** $((d, x, y))$
- (9) **fi**

Der Algorithmus beruht auf der Beobachtung, daß $\text{ggT}(a, b) = \text{ggT}(b, r)$, mit $a = qb + r$. Eine ausführliche Behandlung des euklidischen Algorithmus findet man in [BW96]. In dieser Arbeit ist die Bitkomplexität von Algorithmus 1.4 von besonderem Interesse. Es stellt sich heraus, daß, genau wie im Fall der ggT-Berechnung ohne Darstellung des ggT, diese ebenfalls durch $O(\text{size}(a) \text{size}(b))$ beschränkt ist.

1.5. Lemma Ist für $a \geq b > 0$, $(d, x, y) = \mathbf{euklid}(a, b)$, dann ist

$$|x| \leq \frac{b}{d} \tag{1.2}$$

$$|y| \leq \frac{a}{d}. \tag{1.3}$$

Beweis: Induktion über b .

Ist $b = 1$, dann gilt $\mathbf{euklid}(a, b) = (1, 0, 1)$, und die Ungleichungen gelten.

Ist $b > 1$, dann sei $a = qb + r$ das Ergebnis der Division mit Rest aus Zeile (4). Ist $r = 0$, dann ist $\mathbf{euklid}(a, b) = (b, 0, 1)$, und (1.2), (1.3) gelten. Ist $r > 0$, dann gilt nach der Induktionsvoraussetzung mit $\mathbf{euklid}(b, r) = (d, x', y')$, $|x'| \leq \frac{r}{d}$ und $|y'| \leq \frac{b}{d}$. Da $x = y'$ folgt (1.2) und weil $|y| = |x' - y'q| \leq |x'| + |y'q| \leq \frac{r}{d} + \frac{bq}{d} = \frac{a}{d}$, folgt auch (1.3). ■

$T(a, b)$ soll für $a \geq b \geq 0$ die Zeit sein, die $\mathbf{euklid}(a, b)$ benötigt. Eine einfache Überlegung zeigt, daß für $a > 1$, $T(a, 1) \leq c_1 \log(a)$ und $T(a, 0) \leq c_2 \log(a)$ mit Konstanten c_1 und c_2 .

1.6. Satz Ist $a \geq b > 1$, dann gibt es eine Konstante c , so daß $\mathbf{euklid}(a, b)$ mit Zeit $c \log(a) \log(b)$ auskommt.

Beweis: Sei $a \geq b > 1$ und $a = qb + r$ das Ergebnis der Division mit Rest in Zeile (4). Der Test auf 0 in Zeile (1) kann in Zeit $c_1 \log(b) \leq c_1 \log(q+1) \log(b)$ durchgeführt werden. Die Division mit Rest in Zeile (4) braucht weniger Zeit als $c_2 \log(q+1) \log(b)$. In Zeile (7) ist wegen Lemma 1.5 $|x'| \leq b$ und $|y'| \leq b$. Deshalb kann man dort mit Zeit $c_3 \log(q+1) \log(b)$ auskommen. Außerdem gilt $T(b, 0) \leq c_4 \log(q+1) \log(b)$ und $T(b, 1) \leq c_5 \log(q+1) \log(b)$. Setzt man nun $c = c_1 + c_2 + c_3 + c_4 + c_5$, dann gilt

$$T(a, b) \leq c \log(a) \log(b). \tag{1.4}$$

Dies beweist man durch Induktion über die Anzahl der rekursiven Aufrufe von \mathbf{euklid} .

Beachte, daß $q + 1 \leq qb$, da $b > 1$ und $q \geq 1$.

Bei nur einem rekursiven Aufruf ist $r = 0$ in Zeile (4) und c ist so definiert, daß $T(a, b) \leq c \log(q+1) \log(b) \leq c \log(a) \log(b)$.

Bei mehr als einem rekursiven Aufruf ist $r = 1$ oder $r > 1$ in Zeile (4). Ist $r = 1$, dann ist c so definiert, daß $T(a, b) \leq c \log(q+1) \log(b) \leq c \log(a) \log(b)$. Ist $r > 1$, dann ist nach

der Induktionsvoraussetzung $T(b, r) \leq c \log(b) \log(r)$. Somit folgt:

$$\begin{aligned}
 T(a, b) &\leq c \log(q+1) \log(b) + c \log(b) \log(r) \\
 &= c \log(b) (\log(q+1) + \log(r)) \\
 &= c \log(b) \log(qr+r) \\
 &\leq c \log(b) \log(qb+r) \\
 &= c \log(b) \log(a)
 \end{aligned}$$

und es gilt (1.4). ■

1.7. Satz Für zwei Zahlen $a, b \in \mathbb{Z}$ findet man in Zeit $O(\text{size}(a) \text{size}(b))$ Zahlen $x, y \in \mathbb{Z}$ und $d \in \mathbb{N}$ mit $\text{size}(x) \leq \text{size}(b)$, $\text{size}(y) \leq \text{size}(a)$ und $xa + yb = d = \text{ggT}(a, b)$.

Beweis: Man kann davon ausgehen, daß a und b nichtnegative Zahlen und der Größe nach geordnet sind. Ist $b = 0$, dann liefert **euklid** $(a, 1, 0)$ zurück, ist $b = 1$, dann liefert **euklid** $(1, 0, 1)$ zurück. In diesen Fällen gilt die Behauptung. Wegen Satz 1.6 und Lemma 1.5 gilt die Behauptung auch sonst. ■

1.3 Abelsche Gruppen

Dieser Abschnitt enthält eine Aufreihung von Ergebnissen aus der Gruppentheorie. Näheres findet man in [Kun94].

1.8. Lemma Ist G eine abelsche Gruppe, H eine echte Untergruppe von G mit $|G/H|$ endlich, und F eine Untergruppe von G mit $G \supseteq F \supset H$. Dann gilt

$$|G/F| < |G/H|.$$

1.9. Definition Eine abelsche Gruppe $(G, +)$ heißt endlich erzeugt, wenn es Elemente g_1, \dots, g_n in G gibt mit $G = g_1\mathbb{Z} + \dots + g_n\mathbb{Z}$. Die Elemente g_1, \dots, g_n heißen Erzeuger von G und man schreibt $G = \langle g_1, \dots, g_n \rangle$. Sind die Elemente g_1, \dots, g_n linear unabhängig, dann heißt das Tupel (g_1, \dots, g_n) Basis von G . G heißt frei, wenn G eine Basis hat.

Ist G eine freie abelsche Gruppe mit Basis (g_1, \dots, g_n) , dann ist die Abbildung

$$\begin{aligned}
 \phi : \mathbb{Z}^n &\rightarrow G \\
 (z_1, \dots, z_n) &\mapsto z_1g_1 + \dots + z_ng_n
 \end{aligned}$$

ein Isomorphismus, und es folgt sofort, daß alle Basen einer freien abelschen Gruppe gleiche Länge haben.

1.10. Definition Die Länge der Basen einer freien abelschen Gruppe G heißt Rang von G .

1.11. Satz (Hauptsatz der abelschen Gruppen) Ist F eine freie abelsche Gruppe vom Rang n und $H \neq \{0\}$ eine Untergruppe von G , dann gibt es eine Basis (b_1, \dots, b_n) von G und Zahlen $t_1, \dots, t_r \in \mathbb{N}$ mit $t_i | t_{i+1}$ $1 \leq i \leq r-1$ so, daß $(t_1 b_1, \dots, t_r b_r)$ eine Basis von H ist. Insbesondere ist H eine freie abelsche Gruppe vom Rang $r \leq n$.

Aus Satz 1.11 folgt

1.12. Satz Für jede endlich erzeugte abelsche Gruppe G existiert ein Isomorphismus

$$G \cong \mathbb{Z}^k \times \mathbb{Z}_{t_1} \times \dots \times \mathbb{Z}_{t_r},$$

mit $t_i \in \mathbb{N}$, $1 \leq i \leq r$, und $t_i | t_{i+1}$, $1 \leq i \leq r-1$.

1.13. Satz Ist G eine freie abelsche Gruppe und H eine Untergruppe von G , dann ist $|G/H|$ endlich, dann und nur dann, wenn der Rang von H gleich dem Rang von G .

Beweis: Sei (b_1, \dots, b_n) eine Basis von G , und $t_1, \dots, t_r \in \mathbb{N}$ mit $(t_1 b_1, \dots, t_r b_r)$ eine Basis von H .

$$G/H = \{(x_1 b_1 + \dots + x_n b_n) + H : x_i \in \mathbb{Z}\}.$$

Wenn $r < n$ gilt, dann ist $x_n b_n + H = y_n b_n + H$ dann und nur dann wenn $(x_n - y_n) b_n \in H$ und das ist äquivalent zu $x_n = y_n$. Deshalb ist $|G/H|$ nicht endlich. Wenn $r = n$ gilt, dann ist

$$x_1 b_1 + \dots + x_n b_n + H = y_1 b_1 + \dots + y_n b_n + H$$

genau dann, wenn $t_i | (x_i - y_i)$, woraus man $|G/H| = t_1 \dots t_n$ schließen kann. ■

Wenn $(\alpha_1, \dots, \alpha_n)$ und $(\beta_1, \dots, \beta_n)$ Basen der abelschen Gruppe G sind, dann existieren $a_{i,j} \in \mathbb{Z}$ mit

$$\alpha_j = \sum_{1 \leq i \leq n} a_{i,j} \beta_i.$$

In Matrixschreibweise heißt das: $(\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n)A$ mit $A = (a_{i,j}) \in \mathbb{Z}^{n \times n}$. Ebenso gibt es dann auch eine Matrix $B \in \mathbb{Z}^{n \times n}$ mit $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n)B$. Nun muß $BA = I$ sein, denn $(\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_n)BA$ woraus $(\alpha_1, \dots, \alpha_n)(I - BA) = 0$ folgt. Da $\alpha_1, \dots, \alpha_n$ linear unabhängig sind, muß $(I - BA) = 0$ sein. Daraus folgt, daß A und B in $\text{GL}(n, \mathbb{Z})$ sind.

Ist $A \in \text{GL}(n, \mathbb{Z})$ und $(\alpha_1, \dots, \alpha_n)$ eine Basis der Gruppe G , dann ist auch $(\beta_1, \dots, \beta_n)$, mit

$$(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n)A$$

eine Basis von G , da

$$(\beta_1, \dots, \beta_n)A^{-1} = (\alpha_1, \dots, \alpha_n),$$

also die α_i im Erzeugnis von β_1, \dots, β_n liegen und umgekehrt die β_i auch im Erzeugnis der $\alpha_1, \dots, \alpha_n$ liegen. Die lineare Unabhängigkeit von β_1, \dots, β_n folgt dann aus der Invarianz der Länge der Basen von G .

Weil $\text{GL}(n, \mathbb{Z})$ gerade aus den Matrizen $U \in \mathbb{Z}^{n \times n}$ mit $\det(U) = \pm 1$ besteht, gilt somit:

1.14. Lemma Ist $(\alpha_1, \dots, \alpha_n)$ eine Basis der Gruppe G , so sind alle Basen von G die Tupel $(\beta_1, \dots, \beta_n)$ mit

$$(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n)A, \quad A \in \mathbb{Z}^{n \times n}, \det(A) = \pm 1.$$

1.15. Lemma Sei G eine freie abelsche Gruppe vom Rang n und H eine Untergruppe von G vom Rang n . Ist (x_1, \dots, x_n) eine Basis von G und (y_1, \dots, y_n) eine Basis von H und $A \in \mathbb{Z}^{n \times n}$, mit

$$(y_1, \dots, y_n) = (x_1, \dots, x_n)A.$$

Dann gilt $|G/H| = |\det(A)|$.

Beweis: Es gibt eine Basis (b_1, \dots, b_n) von G und $t_1, \dots, t_n \in \mathbb{N}$ sodaß $(t_1 b_1, \dots, t_n b_n)$

eine Basis von H ist. Es gilt mit unimodularen U und V und $T = \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix}$:

$$\begin{aligned} (b_1, \dots, b_n) &= (x_1, \dots, x_n)U \\ (y_1, \dots, y_n) &= (b_1, \dots, b_n)TV \end{aligned}$$

Also zusammen:

$$(x_1, \dots, x_n)UTV = (x_1, \dots, x_n)A,$$

und da x_1, \dots, x_n linear unabhängig sind, folgt $UTV = A$, also

$$|\det(A)| = |\det(U)\det(T)\det(V)| = \det(T) = t_1 \cdots t_n,$$

und $t_1 \cdots t_n = |G/H|$, wie im Beweis von Satz 1.13. ■

1.4 Ideale

In dieser Arbeit soll ein Ring immer kommutativ sein und eine 1 enthalten. Eine ausführliche Behandlung von Ringen und Idealen findet man in [Kun94].

1.16. Definition Ein Ideal eines kommutativen Ringes R ist eine abelsche Untergruppe \mathfrak{a} von $(R, +)$ mit der zusätzlichen Eigenschaft $\forall a \in \mathfrak{a}, \forall r \in R$ gilt $ra \in \mathfrak{a}$. Man schreibt $\mathfrak{a} \trianglelefteq R$. \mathfrak{a} heißt echt, wenn $\mathfrak{a} \subset R$.

1.17. Definition (Summe und Produkt von Idealen) Sind \mathfrak{a} und \mathfrak{b} Ideale des Rings R , dann ist $\mathfrak{a} + \mathfrak{b}$ das Ideal $\{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$ und $\mathfrak{a}\mathfrak{b}$ das Ideal $\{\sum_{\text{endlich}} ab : a \in \mathfrak{a}, b \in \mathfrak{b}\}$.

1.18. Definition Ein Ideal $\mathfrak{m} \neq R$ eines kommutativen Ringes R heißt maximal, wenn es kein echtes Ideal $\mathfrak{a} \trianglelefteq R$ gibt, welches \mathfrak{m} enthält.

1.19. Definition Ein Ideal $\mathfrak{p} \neq R$ eines kommutativen Ringes R heißt Primideal, wenn aus $ab \in \mathfrak{p}$, $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.

1.20. Lemma Gilt für ein Primideal $\mathfrak{p} \subseteq R$ und Ideale \mathfrak{a} und \mathfrak{b} von R , $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$, dann folgt $\mathfrak{p} \supseteq \mathfrak{a}$ oder $\mathfrak{p} \supseteq \mathfrak{b}$.

1.21. Satz Ist R ein Ring, dann ist jedes maximale Ideal von R ein Primideal.

1.22. Lemma Ist $\mathfrak{a} \subseteq R$, $\mathfrak{a} \neq R$ und $|R/\mathfrak{a}|$ endlich, dann gibt es ein maximales Ideal \mathfrak{m} , welches \mathfrak{a} enthält.

Beweis: Ist \mathfrak{a} selbst maximal, dann ist man mit $\mathfrak{m} = \mathfrak{a}$ fertig. Andernfalls ist \mathfrak{a} in einem echten Ideal \mathfrak{a}_1 echt enthalten, und mit Lemma 1.8 folgt

$$|R/\mathfrak{a}_1| < |R/\mathfrak{a}|.$$

Ist \mathfrak{a}_1 wiederum nicht maximal, dann gibt es ein echtes Ideal \mathfrak{a}_2 mit $\mathfrak{a}_2 \supset \mathfrak{a}_1$ und es folgt:

$$|R/\mathfrak{a}_2| < |R/\mathfrak{a}_1| < |R/\mathfrak{a}|.$$

Weil die Gruppenordnung der Ideale natürliche Zahlen sind, läßt sich dies nicht beliebig oft fortsetzen, und man kommt schließlich an einem maximalen Ideal \mathfrak{m} an, welches \mathfrak{a} enthält. ■

1.23. Lemma Ist $\mathfrak{a} \subseteq R$ und $|R/\mathfrak{a}|$ endlich, dann gibt es ein Primideal \mathfrak{p} , welches \mathfrak{a} enthält.

Beweis: Lemma 1.22 und Satz 1.21. ■

1.24. Lemma Ist $A \subseteq R$ eine nichtleere Menge, dann ist $AR = \{\sum_{\text{endlich}} ar : a \in A, r \in R\}$ ein Ideal von R .

1.25. Bemerkung Ist \mathfrak{a} ein Ideal des Ringes R und $R' \supseteq R$ ein Oberring von R , dann bezeichnet man das R' Ideal $\mathfrak{a}R'$ als das nach R' geliftete R Ideal \mathfrak{a} .

1.5 Algebraische und ganze Zahlen

Näheres zur Theorie der algebraischen Zahlen findet man in [ST87] und [BS66]. [ST87].

1.26. Definition Eine komplexe Zahl α heißt algebraisch, wenn sie Wurzel eines Polynoms $f(X) \neq 0$ aus $\mathbb{Q}[X]$ ist.

Eine komplexe Zahl heißt ganzalgebraisch oder ganz, wenn sie algebraisch und ihr Minimalpolynom aus $\mathbb{Z}[X]$ ist.

Es gilt:

1.27. Satz Die Menge der algebraischen Zahlen ist ein Unterkörper von \mathbb{C} , und die Menge der ganzen Zahlen ist ein Unterring von \mathbb{C} .

1.28. Definition Ist $K = \mathbb{Q}(\theta)$ ein algebraischer Zahlkörper und $\sigma_1, \dots, \sigma_n$ die Einbettungen von K in \mathbb{C} , dann ist für $\alpha \in K$ die Zahl

$$N(\alpha) = \prod_{i=1, \dots, n} \sigma_i(\alpha)$$

die Norm von α in K .

1.29. Lemma Für $\alpha, \beta \in \mathbb{Q}(\theta)$ gilt:

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Beachte, daß die Norm einer Zahl von dem betrachteten Zahlkörper abhängt.

1.30. Satz Ist $K = \mathbb{Q}(\theta)$ ein algebraischer Zahlkörper, (μ_1, \dots, μ_n) eine Basis von K als \mathbb{Q} -Vektorraum, $\alpha \in K$ und sei

$$\alpha(\mu_1, \dots, \mu_n) = (\mu_1, \dots, \mu_n)A,$$

mit $A \in \mathbb{Q}^{n \times n}$, dann ist $N(\alpha) = \det(A)$.

1.6 Moduln und Multiplikatorenringe

1.6.1 Moduln

1.31. Definition Sei $K = \mathbb{Q}(\theta)$ ein algebraischer Zahlkörper und $\{\alpha_1, \dots, \alpha_n\} \subseteq K$. Die von $\{\alpha_1, \dots, \alpha_n\}$ erzeugte Untergruppe von $(K, +)$, $\alpha_1\mathbb{Z} + \dots + \alpha_n\mathbb{Z}$ heißt Modul von K .

Weil es in $(\mathbb{C}, +)$ außer der 0 keine Elemente von endlicher Ordnung gibt, folgt mit Satz 1.12 daß jeder Modul von K eine Basis besitzt.

1.32. Definition Sei $K = \mathbb{Q}(\theta)$ ein algebraischer Zahlkörper. Ein Modul M heißt vollständig, wenn eine Basis von M auch eine Basis des \mathbb{Q} -Vektorraumes K ist.

1.33. Beispiel Sei $p_\theta(X) = a_0 + \dots + a_{n-1}X^{n-1} + X^n$ das Minimalpolynom von θ . Dann ist der Modul $\mathbb{Z} + \theta\mathbb{Z} + \dots + \theta^{n-1}\mathbb{Z}$ ein vollständiger Modul von $K = \mathbb{Q}(\theta)$.

1.6.2 Multiplikatorenringe

1.34. Definition Sei M ein Modul des algebraischen Zahlkörpers $\mathbb{Q}(\theta)$. Eine Zahl $\alpha \in \mathbb{C}$ heißt Multiplikator von M , wenn $\forall m \in M, \alpha m \in M$.

Natürlich ist jeder Multiplikator von M auch eine Zahl in $\mathbb{Q}(\theta)$.

Gilt $\alpha M \subseteq M$ und $\beta M \subseteq M$, dann ist wegen der additiven Gruppeneigenschaft von M auch $\alpha - \beta$ ein Multiplikator von M , also $\mathcal{O}_M \leq (K, +)$. $\alpha\beta$ ist auch in \mathcal{O}_M , und 1 ist selbstverständlich auch ein Multiplikator des Moduls M .

1.35. Satz Ist M ein Modul in $\mathbb{Q}(\theta)$, dann bildet \mathcal{O}_M einen Unterring mit 1 von $\mathbb{Q}(\theta)$, den sogenannten Multiplikatorenring von M .

1.36. Lemma Ein Multiplikatorenring eines Moduls M von $K = \mathbb{Q}(\theta)$ enthält nur ganzalgebraische Zahlen.

Beweis: Hat M eine Basis (μ_1, \dots, μ_n) und ist α ein Multiplikator von M , dann gilt:

$$\alpha\mu_j = a_{1,j}\mu_1 + \dots + a_{n,j}\mu_n \quad \text{mit} \quad a_{i,j} \in \mathbb{Z}, 1 \leq i, j \leq n$$

Es gibt also eine Matrix $A \in \mathbb{Z}^{n \times n}$, mit

$$\alpha(\mu_1, \dots, \mu_n) = (\mu_1, \dots, \mu_n)A,$$

woraus

$$(\mu_1, \dots, \mu_n)(\alpha I - A) = 0$$

folgt. Somit hat die $\mathbb{C}^{n \times n}$ Matrix $(\alpha I - A)$ einen nichttrivialen Kern, ihre Determinante ist also gleich 0. Das Polynom $p(X) = \det(XI - A)$ hat höchsten Koeffizienten 1 und ist in $\mathbb{Z}[X]$. α ist eine Wurzel davon, also eine ganzalgebraische Zahl. ■

Ist M ein Modul von $\mathbb{Q}(\theta)$ und \mathcal{O}_M sein Multiplikatorenring, so ist klar, daß \mathcal{O}_M endlich erzeugt ist, weil für ein $\gamma \in M, \gamma\mathcal{O}_M \subseteq M$ gilt und somit, $\mathcal{O}_M \subseteq 1/\gamma M$. Hat M eine Basis $(\alpha_1, \dots, \alpha_n)$, dann ist \mathcal{O}_M eine Untergruppe der freien abelschen Gruppe $\langle \alpha_1/\gamma, \dots, \alpha_n/\gamma \rangle$, nach dem Hauptsatz über endlich erzeugte abelsche Gruppen also wieder frei.

1.37. Lemma Ist M ein vollständiger Modul von K mit Basis $(\alpha_1, \dots, \alpha_n)$, dann ist \mathcal{O}_M ein vollständiger Modul von K .

Beweis: Sei $\mu \in K$ beliebig. Da $(\alpha_1, \dots, \alpha_n)$ eine Basis des \mathbb{Q} -Vektorraums K ist, gilt

$$\mu\alpha_i = \sum_{j=1}^n a_{i,j}\alpha_j, \quad a_{i,j} \in \mathbb{Q}.$$

Ist c das kleinste gemeinsame Vielfache der Nenner der Zahlen $a_{i,j}$, dann gilt $c\mu\alpha_i = \sum_{1 \leq j \leq n} b_{i,j}\alpha_j$, mit $b_{i,j} \in \mathbb{Z}$, d.h. $c\mu \in \mathcal{O}_M$. Wir wählen n linear unabhängige Elemente μ_1, \dots, μ_n aus K . Mit obiger Konstruktion gibt es $c_1, \dots, c_n \in \mathbb{Z}$ mit $c_i\mu_i \in \mathcal{O}_M$. Also enthält \mathcal{O}_M n linear unabhängige Elemente, und da \mathcal{O}_M frei ist, gilt die Behauptung. ■

1.38. Definition Ein vollständiger Modul M in $K = \mathbb{Q}(\theta)$, der zusätzlich ein Ring ist, heißt Ordnung des Körpers K .

Ist \mathcal{O} eine Ordnung, dann gilt wegen $1 \in \mathcal{O}$ $\alpha\mathcal{O} \subseteq \mathcal{O}$ dann und nur dann, wenn $\alpha \in \mathcal{O}$. Deshalb ist eine Ordnung der Multiplikatorenring von sich selbst.

1.39. Satz Die Ordnungen des Körpers $K = \mathbb{Q}(\theta)$ sind genau die Multiplikatorenringe vollständiger Moduln in K .

1.40. Lemma Ist M ein Modul in einem algebraischen Zahlkörper $K = \mathbb{Q}(\theta)$, der außer der 0 noch andere rationale Zahlen enthält, dann gibt es eine eindeutige minimale positive rationale Zahl $q \in M$.

Beweis: Q sei die Menge der rationalen Zahlen aus M . Sind q_1 und q_2 zwei rationale Zahlen aus M , dann ist $q_1 - q_2$ eine rationale Zahl aus M , und man sieht so, daß Q eine Untergruppe von M ist. Mit Satz 1.11 ist diese Untergruppe auch frei, es gibt also eine Basis die Q erzeugt. Diese Basis muß Länge 1 haben, weil zwei rationale Zahlen bereits linear abhängig über \mathbb{Z} sind. Es gilt also $Q = q'\mathbb{Z}$, mit einer rationalen Zahl $q' \neq 0$. $q = |q'|$ ist die gesuchte eindeutige minimale positive rationale Zahl in Q . ■

1.41. Lemma Ist \mathcal{O} eine Ordnung des Körpers $K = \mathbb{Q}(\theta)$, und $\mathfrak{a} \subseteq \mathcal{O}$, $\mathfrak{a} \neq \{0\}$, dann ist \mathfrak{a} ein vollständiger Modul in K .

Beweis: Wegen Satz 1.11 ist \mathfrak{a} ein Modul in K . Ist $\alpha \in \mathfrak{a}$ und sind $\mu_1, \dots, \mu_n \in \mathcal{O}$ n linear unabhängige Elemente, dann sind die n Elemente $\alpha\mu_1, \dots, \alpha\mu_n$ in \mathfrak{a} und linear unabhängig. Deshalb ist der Rang von \mathfrak{a} als freie abelsche Gruppe mindestens n . Also ist \mathfrak{a} ein vollständiger Modul. ■

1.42. Lemma Ist \mathcal{O} eine Ordnung in $K = \mathbb{Q}(\theta)$, dann ist jedes echte Ideal von \mathcal{O} in einem maximalen Ideal und somit in einem Primideal enthalten.

Beweis: Sei $\mathfrak{a} \neq \{0\}$ ein echtes Ideal von \mathcal{O} . Wegen Lemma 1.41 gilt mit Satz 1.13 $|\mathcal{O}/\mathfrak{a}|$ ist endlich. Dann folgt aus Lemma 1.22 die Behauptung. $\{0\}$ ist entweder maximal oder in einem echten Ideal $\mathfrak{a} \neq \{0\}$ enthalten. ■

1.6.3 Normen von Moduln

1.43. Definition Sei M ein vollständiger Modul in $K = \mathbb{Q}(\theta)$ mit Basis

$$(\alpha_1, \dots, \alpha_n)A,$$

wobei $(\alpha_1, \dots, \alpha_n)$ eine Basis von \mathcal{O}_M ist und $A \in \mathbb{Q}^{n \times n}$. Dann bezeichnet man $N(M) = |\det(A)|$ als die Norm des Moduls M .

Aus Lemma 1.15 folgt:

1.44. Lemma Für einen vollständigen Modul, der in seinem Multiplikatorenring enthalten ist, gilt $N(M) = |\mathcal{O}/M|$.

1.45. Lemma Sei M ein vollständiger Modul in $K = \mathbb{Q}(\theta)$ und $\alpha \in K$. Dann gilt

$$N(\alpha M) = |N(\alpha)| \cdot N(M).$$

Beweis: M habe eine Basis $(\alpha_1, \dots, \alpha_n)$, \mathcal{O}_M habe eine Basis $(\beta_1, \dots, \beta_n)$ und

$$\alpha(\beta_1, \dots, \beta_n) = (\beta_1, \dots, \beta_n)V.$$

mit $V \in \mathbb{Q}^{n \times n}$. Aus Satz 1.30 folgt $N(\alpha) = \det(V)$. Sei $A \in \mathbb{Q}^{n \times n}$ die Matrix mit

$$(\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n)A,$$

es gilt also $N(M) = |\det(A)|$. Es folgt

$$\begin{aligned} \alpha(\alpha_1, \dots, \alpha_n) &= \alpha(\beta_1, \dots, \beta_n)A \\ &= (\beta_1, \dots, \beta_n)VA, \end{aligned}$$

Also gilt

$$N(\alpha M) = |\det(VA)| = |\det(V)| \cdot |\det(A)| = |N(\alpha)| \cdot N(M)$$

■

1.6.4 Multiplikation und Addition von Moduln

Auf der Menge der Moduln lassen sich Verknüpfungen $+$ und \cdot definieren.

1.46. Definition Sind M_1 und M_2 Moduln eines algebraischen Zahlkörpers K , dann ist

$$M_1 + M_2 = \{m_1 + m_2 : m_1 \in M_1, m_2 \in M_2\}$$

und

$$M_1 \cdot M_2 = \left\{ \sum_{\text{endlich}} m_1 m_2 : m_1 \in M_1, m_2 \in M_2 \right\}.$$

1.47. Lemma Sind $M_1 = \alpha_1 \mathbb{Z} + \dots + \alpha_m \mathbb{Z}$ und $M_2 = \beta_1 \mathbb{Z} + \dots + \beta_n \mathbb{Z}$, dann ist

$$M_1 + M_2 = \alpha_1 \mathbb{Z} + \dots + \alpha_m \mathbb{Z} + \beta_1 \mathbb{Z} + \dots + \beta_n \mathbb{Z}$$

und

$$M_1 M_2 = \alpha_1 \beta_1 \mathbb{Z} + \dots + \alpha_1 \beta_n \mathbb{Z} + \dots + \alpha_m \beta_1 \mathbb{Z} + \dots + \alpha_m \beta_n \mathbb{Z}$$

1.48. Lemma $+$ und \cdot sind kommutative assoziative Verknüpfungen auf der Menge der Moduln eines algebraischen Zahlkörpers K und $(M_1 + M_2)M_3 = M_1 M_3 + M_2 M_3$.

1.7 Diskriminanten und Maximalordnungen

Ist $K = \mathbb{Q}(\theta)$ und $p_\theta(X) = a_0 + \dots + a_{n-1}X^{n-1} + X^n \in \mathbb{Q}[X]$ das Minimalpolynom von θ , dann gibt es genau n Einbettungen $\sigma_1, \dots, \sigma_n$ von $K \rightarrow \mathbb{C}$. Betrachte die Matrix

$$A = \begin{pmatrix} \sigma_1(1) & \dots & \sigma_1(\theta^{n-1}) \\ & \ddots & \\ \sigma_n(1) & \dots & \sigma_n(\theta^{n-1}) \end{pmatrix}.$$

Die Zahl $\det(A)^2$ ist in \mathbb{Q} , denn der Zerfällungskörper $E \supseteq \mathbb{Q}$ von $p_\theta(X)$ ist galoisch über \mathbb{Q} und das Anwenden eines Elements aus der Galoisgruppe $\text{gal}(E : \mathbb{Q})$ bewirkt bei A lediglich das Vertauschen von Zeilen. Die Determinante wechselt also höchstens das Vorzeichen. Das Quadrat der Determinante wird also von einem Element aus $\text{gal}(E : \mathbb{Q})$ festgehalten. Weil $E \supseteq \mathbb{Q}$ galoisch ist, ist $\det(A)^2 \in \mathbb{Q}$.

Geht die Basis $(\beta_1, \dots, \beta_n)$ aus $(1, \dots, \theta^{n-1})$ durch die Matrix $T \in \mathbb{Q}^{n \times n}$ mit $(\beta_1, \dots, \beta_n) = (1, \dots, \theta^{n-1})T$ hervor, dann gilt mit $B = (b_{i,j}) = (\sigma_i(\beta_j))$, $1 \leq i, j \leq n$:

$$\det(B)^2 = \det(AT)^2 = \det(A)^2 \det(T)^2 \in \mathbb{Q}. \quad (1.5)$$

1.49. Definition Ist (μ_1, \dots, μ_n) eine Basis der \mathbb{Q} -Vektorraums $K = \mathbb{Q}(\theta)$ und sind $\sigma_1, \dots, \sigma_n$ die $n = [K : \mathbb{Q}]$ verschiedenen Einbettungen von $K \rightarrow \mathbb{C}$, dann bezeichnet man mit $\Delta[\mu_1, \dots, \mu_n] = \det(\sigma_i(\mu_j))^2$, $1 \leq i, j \leq n$, die Diskriminante der Basis (μ_1, \dots, μ_n) .

Beachte, daß es bei der Diskriminante $\Delta[\mu_1, \dots, \mu_n]$ nicht auf die Reihenfolge im Basistupel ankommt, da eine Vertauschung von Spalten nur das Vorzeichen der Determinante, also nicht dessen Quadrat ändert.

1.50. Definition Ist M ein vollständiger Modul in K und (μ_1, \dots, μ_n) eine Basis des Moduls M , dann bezeichnet man mit $\Delta_M = \det(\sigma_i(\mu_j))^2$, $1 \leq i, j \leq n$, die Diskriminante von M .

Diese Definition ist legitim, weil Basen von Moduln unimodular ineinander übergehen und das Quadrat der Determinante einer unimodularen Matrix 1 ist. Es ist also egal, mit welcher Basis man die Diskriminante eines Moduls ausrechnet.

Die Diskriminante Δ_M eines Moduls M ist also eine rationale Zahl. Die Diskriminante einer Ordnung \mathcal{O}_M ist sogar in \mathbb{Z} , weil die an der Entwicklung der Determinante beteiligten Zahlen alle ganzzahlgemäß sind, dort nur multipliziert addiert und subtrahiert wird (alles Ringoperationen!) und eine ganzzahlgemäße Zahl entweder irrational oder ganzrational ist.

1.51. Definition (Maximalordnung) Eine Ordnung des Körpers $K = \mathbb{Q}(\theta)$ heißt Maximalordnung, wenn alle anderen Ordnungen des Körpers K darin enthalten sind.

1.52. Satz In jedem algebraischen Zahlkörper $K = \mathbb{Q}(\theta)$ gibt es eine Maximalordnung.

Sie ist nämlich die Ordnung \mathcal{O} in K mit minimalem Absolutbetrag der Diskriminante $\Delta_{\mathcal{O}}$. Ist \mathcal{O} eine solche Ordnung und α eine ganzzahlige Zahl aus $K \setminus \mathcal{O}$, dann ist der Ring $\mathcal{O}[\alpha]$ als \mathcal{O} -Modul endlich erzeugt, weil man ein Polynom $g(X) \in \mathcal{O}[X]$ immer mit Rest durch das Minimalpolynom $p_{\alpha}(X)$ von α teilen kann. (Es ist normiert und in $\mathbb{Z}[X] \subseteq \mathcal{O}[X]$) Deshalb ist $\mathcal{O}[\alpha]$ auch ein vollständiger Modul, eine Ordnung in K . Da \mathcal{O} aber dann eine echte Unterordnung von $\mathcal{O}[\alpha]$ ist, gibt es eine Matrix $A \in \mathbb{Z}^{n \times n}$, die nicht unimodular ist, eine Basis $(\beta_1, \dots, \beta_n)$ von $\mathcal{O}[\alpha]$ und eine Basis $(\gamma_1, \dots, \gamma_n)$ von \mathcal{O} mit

$$\Delta[\gamma_1, \dots, \gamma_n] = \det(A)^2 \Delta[\beta_1, \dots, \beta_n].$$

Weil $\det(A)^2 > 1$ ist, hat man somit einen Widerspruch zur Minimalität des Absolutbetrages der Diskriminante von \mathcal{O} . Also gilt $\mathcal{O}[\alpha] = \mathcal{O}$.

Es folgt:

1.53. Lemma Die ganzen Zahlen eines algebraischen Zahlkörpers $\mathbb{Q}(\theta)$ bilden die Maximalordnung von $\mathbb{Q}(\theta)$.

1.8 Quadratische Zahlkörper

Ein quadratischer Zahlkörper ist eine endliche Erweiterung $\mathbb{Q}(\theta)$ vom Grade 2.

Sei θ eine Wurzel des irreduziblen Polynoms $f_{\theta}(X) = aX^2 + bX + c$ aus $\mathbb{Z}[X]$, mit $\text{ggT}(a, b, c) = 1$.

1.54. Lemma Der Multiplikatorenring von $M = \mathbb{Z} + \theta\mathbb{Z}$ ist die Ordnung $\mathcal{O} = \mathbb{Z} + a\theta\mathbb{Z}$.

Beweis: Sei $x + y\theta \in K$ ein Multiplikator von M . Da $1 \in M$, ist $x + y\theta \in M$ und somit $x, y \in \mathbb{Z}$. Es gilt aber auch $(x + y\theta)\theta \in M$, also

$$\begin{aligned} (x + y\theta)\theta &= x\theta + y \frac{-b\theta - c}{a} \\ &= \frac{ax - by}{a} \theta - \frac{yc}{a} \end{aligned}$$

Da somit $\frac{ax - by}{a}, \frac{yc}{a} \in \mathbb{Z}$, gilt $a|by$ und $a|cy$, woraus wegen $\text{ggT}(a, b, c) = 1$ $a|y$ folgt. Also gilt $x + y\theta \in \mathbb{Z} + a\theta\mathbb{Z}$.

Da außerdem 1 und $a\theta$ Multiplikatoren von M sind, folgt die Behauptung. ■

Es gilt

$$(1, \theta) = (1, a\theta) \begin{pmatrix} 1 & 0 \\ 0 & 1/a \end{pmatrix}.$$

Daher folgt:

1.55. Korollar Die Norm des Moduls $M = \mathbb{Z} + \theta\mathbb{Z}$ ist $1/a = N(\theta)$.

1.56. Lemma Sei $M = \alpha\mathbb{Z} + \beta\mathbb{Z}$ ein vollständiger Modul im quadratischen Zahlkörper K . Dann ist mit $\mu = \beta/\alpha$ und $f_\mu(X) = aX^2 + bX + c$, $\mathbb{Z} + a\mu\mathbb{Z}$ der Multiplikatorenring von M .

Beweis: Die Moduln M und $\frac{1}{\alpha}M$ haben dieselben Multiplikatorenringe. Die Behauptung folgt dann mit Lemma 1.54. ■

1.57. Definition Ein quadratischer Modul M ist ein vollständiger Modul in einem quadratischen Zahlkörper K . Eine quadratische Ordnung ist eine Ordnung eines quadratischen Zahlkörpers.

1.58. Lemma Die quadratischen Ordnungen \mathcal{O} sind die quadratischen Moduln $\mathcal{O} = \mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z}$ mit $\Delta \equiv 0, 1 \pmod{4}$ und Δ kein perfektes Quadrat.

Beweis: $\frac{\Delta + \sqrt{\Delta}}{2}$ ist eine Wurzel von $p(X) = (X - \frac{\Delta + \sqrt{\Delta}}{2})(X - \frac{\Delta - \sqrt{\Delta}}{2}) = X^2 - \Delta X + \frac{\Delta^2 - \Delta}{4}$, ist also eine ganzzahlige Zahl. Darum ist $\mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z} = \mathbb{Z}[\frac{\Delta + \sqrt{\Delta}}{2}]$ ein Ring. Da außerdem Δ kein perfektes Quadrat ist ist $\frac{\Delta + \sqrt{\Delta}}{2}$ irrational, und $\mathcal{O} = \mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z}$ ist ein quadratischer Modul. Also ist \mathcal{O} tatsächlich eine quadratische Ordnung.

Eine quadratische Ordnung \mathcal{O} ist ein Multiplikatorenring von einem vollständigen Modul $\alpha\mathbb{Z} + \beta\mathbb{Z}$ in einem quadratischen Zahlkörper bzw. der Multiplikatorenring von $\mathbb{Z} + \theta\mathbb{Z}$ mit $\theta = \frac{\beta}{\alpha}$. Ist $f_\theta(X) = aX^2 + bX + c$, dann ist nach Lemma 1.54 $\mathcal{O} = \mathbb{Z} + a\theta\mathbb{Z}$. Also ist mit $\Delta = b^2 - 4ac \equiv 0, 1 \pmod{4}$, $\mathcal{O} = \mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z} = \mathbb{Z} + \frac{b - \sqrt{\Delta}}{2}\mathbb{Z} = \mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z}$. Denn $b \equiv \Delta \pmod{2}$, und die unimodulare Matrix

$$\begin{pmatrix} 1 & \frac{\Delta - b}{2} \\ 0 & 1 \end{pmatrix}$$

transformiert die Basis $(1, \frac{b + \sqrt{\Delta}}{2})$ nach $(1, \frac{\Delta + \sqrt{\Delta}}{2})$. ■

Die Darstellung aus Lemma 1.58 ist eindeutig, da $\Delta[1, \frac{\Delta + \sqrt{\Delta}}{2}] = \Delta$ und die Diskriminante eines Moduls eindeutig ist. Man bezeichnet die quadratische Ordnung mit Diskriminante Δ als \mathcal{O}_Δ .

1.59. Definition Eine Zahl $\Delta \equiv 0, 1 \pmod{4}$, die kein perfektes Quadrat ist, heißt quadratische Diskriminante.

1.60. Satz Für quadratische Diskriminanten Δ, Δ' gilt $\mathcal{O}_\Delta \supseteq \mathcal{O}_{\Delta'}$ dann und nur dann, wenn es ein $d \in \mathbb{N}$ gibt mit $d^2\Delta = \Delta'$.

Beweis: Gilt $\mathcal{O}_\Delta \supseteq \mathcal{O}_{\Delta'}$, dann gibt es eine $\mathbb{Z}^{2 \times 2}$ Matrix U mit $(1, \frac{\Delta'+\sqrt{\Delta'}}{2}) = (1, \frac{\Delta+\sqrt{\Delta}}{2})U$, also gilt $\Delta' = \Delta[1, \frac{\Delta'+\sqrt{\Delta'}}{2}] = \det(U)^2 \Delta[1, \frac{\Delta+\sqrt{\Delta}}{2}] = \det(U)^2 \Delta$.

Die Transformation $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ macht aus dem Modul $\mathbb{Z} + \frac{\Delta+\sqrt{\Delta}}{2}\mathbb{Z}$ einen Modul mit Diskriminante $d^2\Delta$. Da aber auch $d\frac{\Delta+\sqrt{\Delta}}{2}$ ganzzahlig ist, ist dies dann auch eine Ordnung. Der Modul ist also die Ordnung $\mathcal{O}_{d^2\Delta}$. ■

1.61. Korollar Die Maximalordnungen sind die Ordnungen \mathcal{O}_Δ mit der Eigenschaft: Gibt es $d \in \mathbb{N}_{>1}$ und $d^2|\Delta$, dann gilt $\Delta/d^2 \not\equiv 0, 1 \pmod{4}$.

1.62. Lemma Sind $\mathcal{O}_{\Delta/d_1^2}$ und $\mathcal{O}_{\Delta/d_2^2}$, $d_1, d_2 \in \mathbb{N}$ quadratische Ordnungen, dann ist die kleinste Ordnung, die $\mathcal{O}_{\Delta/d_1^2}$ und $\mathcal{O}_{\Delta/d_2^2}$ enthält, die Ordnung $\mathcal{O}_{\Delta/\text{kgV}(d_1, d_2)^2}$, insbesondere ist dann die Zahl $\Delta/\text{kgV}(d_1, d_2)^2$ eine quadratische Diskriminante.

Beweis: Die Maximalordnung des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{\Delta})$ umfaßt sowohl $\mathcal{O}_{\Delta/d_1^2}$ als auch $\mathcal{O}_{\Delta/d_2^2}$. Sei $\mathcal{O}_{\Delta'}$ eine minimale Ordnung, die beide enthält. Eine solche existiert, weil die Indizes $|\mathcal{O}_{\Delta'}/\mathcal{O}_{\Delta/d_1^2}|$ und $|\mathcal{O}_{\Delta'}/\mathcal{O}_{\Delta/d_2^2}|$ natürliche Zahlen sind. Außerdem folgt aus Satz 1.60:

$$\Delta' k_1^2 = \Delta/d_1^2 \text{ mit } k_1 \in \mathbb{N}$$

und

$$\Delta' k_2^2 = \Delta/d_2^2 \text{ mit } k_2 \in \mathbb{N}.$$

Also

$$\Delta' = \Delta/(k_1 d_1)^2 = \Delta/(k_2 d_2)^2 = \Delta/(\text{kgV}(d_1, d_2)^2 v^2) \text{ mit } v \in \mathbb{N}, \quad (1.6)$$

weil $k_1 d_1 = k_2 d_2$, und die Zahl offensichtlich ein gemeinsames Vielfaches von d_1 und d_2 ist. Also ist $\Delta/(\text{kgV}(d_1, d_2)^2 v^2)$ eine quadratische Diskriminante und folglich auch $\Delta/\text{kgV}(d_1, d_2)^2$. Mit Satz 1.60 enthält dann $\mathcal{O}_{\Delta/\text{kgV}(d_1, d_2)^2}$ beide Ordnungen. Ist $v^2 > 1$ in (1.6), dann enthält wieder mit Satz 1.60 $\mathcal{O}_{\Delta'}$ echt die Ordnung $\mathcal{O}_{\Delta/\text{kgV}(d_1, d_2)^2}$ und ist insbesondere nicht minimal bezüglich der Inklusion von $\mathcal{O}_{\Delta/d_1^2}$ und $\mathcal{O}_{\Delta/d_2^2}$. ■

1.63. Korollar Sind $\Delta/d_1^2, \dots, \Delta/d_k^2$, $d_i \in \mathbb{N}$ quadratische Diskriminanten, dann ist die kleinste Ordnung, die $\mathcal{O}_{\Delta/d_1^2}, \dots, \mathcal{O}_{\Delta/d_k^2}$ enthält die Ordnung $\mathcal{O}_{\Delta/\text{kgV}(d_1, \dots, d_k)^2}$. Insbesondere ist $\Delta/\text{kgV}(d_1, \dots, d_k)^2$ eine quadratische Diskriminante.

Beweis: Induktion über k . Ist $k = 1$, dann stimmt die Aussage. Sei nun $k > 1$ und $\mathcal{O}_{\Delta'}$ eine bezüglich der Inklusion minimale Ordnung die $\mathcal{O}_{\Delta/d_1^2}, \dots, \mathcal{O}_{\Delta/d_k^2}$ enthält. Mit Induktion ist $\Delta/\text{kgV}(d_1, \dots, d_{k-1})^2$ eine quadratische Diskriminante und $\mathcal{O}_{\Delta/\text{kgV}(d_1, \dots, d_{k-1})^2}$ die minimale Ordnung die $\mathcal{O}_{\Delta/d_1^2}, \dots, \mathcal{O}_{\Delta/d_{k-1}^2}$ enthält. $\mathcal{O}_{\Delta'}$ ist also die minimale Ordnung, die $\mathcal{O}_{\Delta/\text{kgV}(d_1, \dots, d_{k-1})^2}$ und $\mathcal{O}_{\Delta/d_k^2}$ umfaßt. Wegen Lemma 1.62 und weil

$$\text{kgV}(\text{kgV}(d_1, \dots, d_{k-1}), d_k) = \text{kgV}(d_1, \dots, d_k)$$

gilt, ist $\mathcal{O}_{\Delta'}$ die Ordnung $\mathcal{O}_{\Delta/\text{kgV}(d_1, \dots, d_k)^2}$. ■

1.64. Definition Sei M ein quadratischer Modul. Man sagt M gehört zu der Ordnung \mathcal{O}_Δ , wenn \mathcal{O}_Δ der Multiplikatorenring von M ist.

1.65. Lemma Sei $K = \mathbb{Q}(\theta)$ ein quadratischer Zahlkörper und σ der nichttriviale Automorphismus von K . Gehört der Modul $M = \langle 1, \mu \rangle$ zu \mathcal{O}_Δ , dann ist $M\sigma(M) = N(M)\mathcal{O}_\Delta$.

Beweis: Sei $f_\mu(X) = aX^2 + bX + c$. μ ist von der Form $\frac{b \pm \sqrt{\Delta}}{2a}$ mit $\Delta = b^2 - 4ac$. Es gilt $\mu\sigma(\mu) = \frac{c}{a}$ und da $M\sigma(M) = \langle 1, \mu, \sigma(\mu), \mu\sigma(\mu) \rangle$, gilt mit Korollar 1.55 $M\sigma(M) = 1/a \langle a, \frac{b+\sqrt{\Delta}}{2}, \frac{b-\sqrt{\Delta}}{2}, c \rangle = 1/a \langle (a, b, c), \frac{b+\sqrt{\Delta}}{2} \rangle = N(M)\mathcal{O}_\Delta$. ■

1.66. Korollar Gehört der quadratische Modul M zu \mathcal{O}_Δ , dann gilt $M\sigma(M) = N(M)\mathcal{O}_\Delta$.

Beweis: Sei $M = \alpha\mathbb{Z} + \beta\mathbb{Z} = \alpha(\mathbb{Z} + \frac{\beta}{\alpha}\mathbb{Z})$. Da mit Lemma 1.45

$$N\left(\mathbb{Z} + \frac{\beta}{\alpha}\mathbb{Z}\right) = N(M) \left| \frac{1}{N(\alpha)} \right|,$$

folgt

$$\begin{aligned} M\sigma(M) &= \alpha\sigma(\alpha)(\mathbb{Z} + \frac{\beta}{\alpha}\mathbb{Z})\sigma((\mathbb{Z} + \frac{\beta}{\alpha}\mathbb{Z})) \\ &= N(\alpha)N(M) \left| \frac{1}{N(\alpha)} \right| \mathcal{O}_\Delta \\ &= N(M)\mathcal{O}_\Delta. \end{aligned}$$

Beachte dabei, daß \mathcal{O}_Δ das eventuell negative Vorzeichen von $N(\alpha)$ schluckt. ■

1.67. Lemma Gehören M_1 und M_2 zur quadratischen Ordnung \mathcal{O}_Δ , dann gehört M_1M_2 zu \mathcal{O}_Δ und $N(M_1M_2) = N(M_1)N(M_2)$.

Beweis: $(M_1M_2)\sigma(M_1M_2) = N(M_1M_2)\mathcal{O}_{\Delta'}$, wobei $\mathcal{O}_{\Delta'}$ der Multiplikatorenring von M_1M_2 ist. Es gilt aber auch wegen der Kommutativität der Multiplikation und weil $\sigma(M_1M_2) = \sigma(M_1)\sigma(M_2)$:

$$\begin{aligned} (M_1M_2)\sigma(M_1M_2) &= M_1\sigma(M_1)M_2\sigma(M_2) \\ &= N(M_1)\mathcal{O}_\Delta N(M_2)\mathcal{O}_\Delta \\ &= N(M_1)N(M_2)\mathcal{O}_\Delta. \end{aligned}$$

Es gilt also

$$N(M_1M_2)\mathcal{O}_{\Delta'} = N(M_1)N(M_2)\mathcal{O}_\Delta. \quad (1.7)$$

Die kleinste positive rationale Zahl in $N(M_1M_2)\mathcal{O}_{\Delta'}$ ist $N(M_1M_2)$, und die kleinste positive rationale Zahl in $N(M_1)N(M_2)\mathcal{O}_\Delta$ ist $N(M_1)N(M_2)$. Wegen (1.7) gilt also $N(M_1M_2) = N(M_1)N(M_2)$ und $\mathcal{O}_\Delta = \mathcal{O}_{\Delta'}$. ■

1.68. Lemma Ist \mathcal{O}_Δ eine quadratische Ordnung im quadratischen Zahlkörper $K = \mathbb{Q}(\theta)$ und ist σ ein Automorphismus von K , dann gilt $\sigma(\mathcal{O}_\Delta) = \mathcal{O}_\Delta$.

Beweis: Falls σ nicht die Identität ist, dann wird $\frac{\Delta+\sqrt{\Delta}}{2}$ durch σ auf die andere Wurzel von $X^2 - \Delta X + \frac{\Delta^2-\Delta}{4}$ abgebildet, nämlich $\frac{\Delta-\sqrt{\Delta}}{2}$. $\sigma(\mathcal{O}_\Delta)$ wird also von 1 und $\frac{\Delta-\sqrt{\Delta}}{2}$ erzeugt. Nun ist $(1, \frac{\Delta-\sqrt{\Delta}}{2}) = (1, \frac{\Delta+\sqrt{\Delta}}{2}) \begin{pmatrix} 1 & \Delta \\ 0 & -1 \end{pmatrix}$ und diese Transformation ist unimodular. ■

1.69. Korollar Die zu einer quadratischen Ordnung \mathcal{O}_Δ gehörenden Moduln bilden mit der Multiplikation eine abelsche Gruppe.

Beweis: Neutrales Element ist \mathcal{O}_Δ . Wegen Lemma 1.67 ist die Verknüpfung von der Menge der zu \mathcal{O}_Δ gehörenden Moduln in die Menge der zu \mathcal{O}_Δ gehörenden Moduln. Assoziativität und Kommutativität folgen aus Lemma 1.48. Gehört M zu \mathcal{O}_Δ , dann gehört $\sigma(M)$ auch zu \mathcal{O}_Δ , denn wegen Lemma 1.68 ist $\mathcal{O}_\Delta = \sigma(\mathcal{O}_\Delta)$. Weil $M\sigma(M) = N(M)\mathcal{O}_\Delta$ ist das Inverse von M der Modul $1/N(M)\sigma(M)$. ■

1.8.1 Ideale quadratischer Ordnungen

1.70. Lemma Ein Ideal $\mathfrak{a} \neq \{0\}$ von \mathcal{O}_Δ ist ein vollständiger Modul mit $\mathcal{O}_\Delta \supseteq \mathfrak{a}$, der zu einer Oberordnung von \mathcal{O}_Δ gehört.

Beweis: Definition 1.16, Lemma 1.41. ■

1.71. Definition Sind \mathfrak{a} und \mathfrak{b} \mathcal{O}_Δ Ideale, dann schreibt man $\mathfrak{a}|\mathfrak{b}$ (\mathfrak{a} teilt \mathfrak{b}), wenn es ein \mathcal{O}_Δ Ideal \mathfrak{c} gibt mit $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$.

1.72. Definition Ein \mathcal{O}_Δ Ideal \mathfrak{a} heißt invertierbar, wenn es einen quadratischen Modul M gibt mit $\mathfrak{a}M = \mathcal{O}_\Delta$. Man schreibt für M dann \mathfrak{a}^{-1} .

1.73. Lemma Für ein \mathcal{O}_Δ Ideal \mathfrak{a} sind äquivalent:

1. \mathfrak{a} ist invertierbar.
2. \mathfrak{a} gehört zu \mathcal{O}_Δ .

Beweis: Gilt $\mathfrak{a}M = \mathcal{O}_\Delta$ und ist x ein Multiplikator von \mathfrak{a} , dann gilt mit $x\mathfrak{a} \subseteq \mathfrak{a}$, $x\mathfrak{a}M = x\mathcal{O}_\Delta \subseteq \mathcal{O}_\Delta$. Also ist $x \in \mathcal{O}_\Delta$ und \mathcal{O}_Δ der Multiplikatorenring von \mathfrak{a} .

Gehört \mathfrak{a} zu \mathcal{O}_Δ , dann gilt $\mathfrak{a}\frac{1}{N(\mathfrak{a})}\sigma(\mathfrak{a}) = \mathcal{O}_\Delta$, also ist \mathfrak{a} invertierbar. ■

1.74. Lemma Sind \mathfrak{a} und \mathfrak{b} \mathcal{O}_Δ Ideale und ist \mathfrak{a} invertierbar, dann gilt $\mathfrak{a}|\mathfrak{b}$ genau dann, wenn $\mathfrak{a} \supseteq \mathfrak{b}$.

Beweis: Wenn $\mathfrak{a} \supseteq \mathfrak{b}$ gilt $\mathcal{O}_\Delta = \mathfrak{a}^{-1}\mathfrak{a} \supseteq \mathfrak{a}^{-1}\mathfrak{b}$. Also ist $\mathfrak{a}^{-1}\mathfrak{b}$ ein \mathcal{O}_Δ Ideal, und $\mathfrak{a}\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{b}$. Wenn \mathfrak{a} ein Teiler von \mathfrak{b} ist, dann gibt es ein \mathcal{O}_Δ Ideal \mathfrak{c} mit $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$. Da $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}$, gilt dann $\mathfrak{a} \supseteq \mathfrak{b}$. ■

1.75. Lemma Sind \mathfrak{a} und \mathfrak{b} invertierbare \mathcal{O}_Δ Ideale und ist \mathfrak{a} ein Teiler von \mathfrak{b} , dann ist $\mathfrak{b}\mathfrak{a}^{-1}$ ein invertierbares \mathcal{O}_Δ Ideal.

1.76. Definition Zwei \mathcal{O}_Δ Ideale \mathfrak{a} und \mathfrak{b} heißen teilerfremd, wenn

$$\mathfrak{a} + \mathfrak{b} = \mathcal{O}_\Delta$$

gilt.

1.77. Satz Die Ideale $\neq \{0\}$ einer quadratischen Ordnung \mathcal{O}_Δ sind die quadratischen Moduln $m(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z})$, mit $4a|(b^2 - \Delta)$, eindeutigen $a, m \in \mathbb{N}$ und $\pmod{2a}$ eindeutig bestimmtem b .

Beweis: Zuerst die Eindeutigkeit. Ist ein Ideal \mathfrak{a} von der Form $m(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z})$, dann ist die kleinste positive rationale Zahl aus \mathfrak{a} na und als solche nach Lemma 1.40 eindeutig. Andererseits ist $|\mathcal{O}_\Delta/\mathfrak{a}| = n^2a$. Wir haben also mit einer zweiten solchen Darstellung $\mathfrak{a} = n^*(a^*\mathbb{Z} + \frac{b^*+\sqrt{\Delta}}{2}\mathbb{Z})$,

$$n^*a^* = na, \tag{1.8}$$

$$n^{*2}a^* = n^2a. \tag{1.9}$$

Beachte, daß weder $n^*a^* = 0$ noch $na = 0$ gilt. Teilt man (1.9) durch (1.8), dann erhält man

$$n^* = n,$$

und somit auch $a^* = a$. Da dann

$$n \left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z} \right) = n \left(a\mathbb{Z} + \frac{b^* + \sqrt{\Delta}}{2}\mathbb{Z} \right),$$

folgt

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

und somit $\frac{b^*+\sqrt{\Delta}}{2} - \frac{b+\sqrt{\Delta}}{2} = \frac{b^*-b}{2} \in a\mathbb{Z}$. Also hat man

$$b^* \equiv b \pmod{2a}.$$

Eine Untergruppe von \mathcal{O}_Δ der Form

$$\mathfrak{a} = n \left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z} \right),$$

mit $4a|b^2 - \Delta$ ist ein Ideal von \mathcal{O}_Δ , weil

$$\begin{aligned} n \left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z} \right) &= na \left(\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2a}\mathbb{Z} \right) \\ &= na \left(\mathbb{Z} + \frac{b' + \sqrt{\Delta'}}{2a'}\mathbb{Z} \right), \end{aligned}$$

wobei $b' = b/d$, $\Delta' = \Delta/d^2$, $a' = a/d$ mit $d = \text{ggT}(a, b, \frac{b^2 - \Delta}{4a})$. Der Multiplikatorring von \mathfrak{a} ist also \mathcal{O}_{Δ/d^2} und dieser enthält nach Satz 1.60 \mathcal{O}_Δ . \mathfrak{a} hat also tatsächlich die Idealeigenschaft.

Andererseits ist eine Basis eines Ideals \mathfrak{a} mit einer Matrix $A \in \mathbb{Z}^{2 \times 2}$ in der Form

$$\left(1, \frac{\Delta + \sqrt{\Delta}}{2} \right) A$$

beschreibbar. Man kann annehmen, daß diese Matrix in Spaltenstufenform

[Buc96] ist, die Basis also die Form

$$\left(1, \frac{\Delta + \sqrt{\Delta}}{2} \right) \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} = \left(a_1, a_2 + a_3 \frac{\Delta + \sqrt{\Delta}}{2} \right)$$

angenommen hat. Lemma 1.68 zeigt, daß $\frac{\Delta - \sqrt{\Delta}}{2} \in \mathcal{O}_\Delta$ ist, und daher ist $\frac{\Delta - \sqrt{\Delta}}{2}\mathfrak{a} \subseteq \mathfrak{a}$. Es gibt also $x, y \in \mathbb{Z}$, mit

$$\begin{aligned} xa_1 + ya_2 + ya_3 \frac{\Delta + \sqrt{\Delta}}{2} &= \left(a_2 + a_3 \frac{\Delta + \sqrt{\Delta}}{2} \right) \frac{\Delta - \sqrt{\Delta}}{2} \\ &= -a_2 \frac{\Delta + \sqrt{\Delta}}{2} + a_3 \frac{\Delta^2 - \Delta}{4} + a_2 \Delta. \end{aligned}$$

Es folgt $a_3|a_2$. Da auch $a_1 \frac{\Delta + \sqrt{\Delta}}{2}$ in \mathfrak{a} ist gilt $a_3|a_1$. Mit $a'_1 = a_1/a_3$ und $a'_2 = a_2/a_3$ gilt also

$$\begin{aligned} \mathfrak{a} &= a_3 \left(a'_1 \mathbb{Z} + \left(a'_2 + \frac{\Delta + \sqrt{\Delta}}{2} \right) \mathbb{Z} \right) \\ &= m \left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z} \right). \end{aligned}$$

Weil $m \frac{b + \sqrt{\Delta}}{2} \frac{b - \sqrt{\Delta}}{2} = m \frac{b^2 - \Delta}{4} \in m a \mathbb{Z}$, folgt somit $4a|b^2 - \Delta$.

■

1.78. Definition Die Darstellung eines Ideals $\mathfrak{a} \neq \{0\}$ aus Satz 1.77 mit $0 \leq b < 2a$ heißt Standarddarstellung von \mathfrak{a} . Die Zahlen $m(\mathfrak{a})$, $a(\mathfrak{a})$, $b(\mathfrak{a})$ und $c(\mathfrak{a})$ sind die Zahlen m , a , b und $\frac{b^2 - \Delta}{4a}$.

Satz 1.77 zeigt, daß die Standarddarstellung eines Ideals eindeutig ist.

1.79. Lemma Ein \mathcal{O}_Δ Ideal \mathfrak{a} ist genau dann invertierbar, wenn $\text{ggT}(a(\mathfrak{a}), b(\mathfrak{a}), c(\mathfrak{a})) = 1$.

Beweis: Lemma 1.54 zeigt, daß nur in diesem Fall der Multiplikatorenring von \mathfrak{a} \mathcal{O}_Δ ist, also nur im Fall $\text{ggT}(a, b, \frac{b^2-\Delta}{4a}) = 1$ \mathfrak{a} zu \mathcal{O}_Δ gehört. Dann folgt die Behauptung mit Lemma 1.73. ■

1.8.2 Darstellung im Rechner

Die Ordnung \mathcal{O}_Δ wird mit der Zahl Δ kodiert und das Ideal \mathfrak{a} mit dem Tripel

$$(m(\mathfrak{a}), a(\mathfrak{a}), b(\mathfrak{a})).$$

$\text{size}(\mathfrak{a})$ ist dann $\text{size}(m(\mathfrak{a})) + \text{size}(a(\mathfrak{a})) + \text{size}(b(\mathfrak{a}))$ und $\text{size}(\mathcal{O}_\Delta) = \text{size}(\Delta)$. Beachte, daß man die Ordnung \mathcal{O}_Δ kennen muß, um aus der Kodierung von \mathfrak{a} zu erkennen, um welchen Modul es sich dabei handelt.

1.80. Lemma Es gibt Konstanten k_1 und k_2 , so daß für alle \mathcal{O}_Δ Ideale $\mathfrak{a} \neq \{0\}$ gilt:

$$\begin{aligned} \text{size}(\mathfrak{a}) &\leq k_1 \text{size}(\mathbf{N}(\mathfrak{a})), \\ \text{size}(\mathbf{N}(\mathfrak{a})) &\leq k_2 \text{size}(\mathfrak{a}). \end{aligned}$$

Beweis: Sei $\mathfrak{a} = m(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z})$. Dann gilt $\mathbf{N}(\mathfrak{a}) = m^2 da$, wobei $d = \text{ggT}(a, b, c)$. ■

Kapitel 2

Der Algorithmus Refine

In diesem Kapitel beschäftige ich mich mit einem Algorithmus, der zu einer Menge von echten \mathcal{O}_Δ Idealen $\mathfrak{a}_1, \dots, \mathfrak{a}_k \neq \{0\}$ paarweise teilerfremde invertierbare $\mathcal{O}_{\Delta'}$ Ideale $\mathfrak{n}_1, \dots, \mathfrak{n}_s$ findet, wobei $\mathcal{O}_{\Delta'} \supseteq \mathcal{O}_\Delta$ und die $\mathcal{O}_{\Delta'}$ Ideale $\mathfrak{a}_i \mathcal{O}_{\Delta'}$ Potenzprodukte der $\mathfrak{n}_1, \dots, \mathfrak{n}_s$ sind.

2.1 Faktorisierungen

2.1. Definition (Faktorisierung) Eine Faktorisierung ist ein Paar $\mathcal{F} = (\mathcal{O}_\Delta, A)$, wobei \mathcal{O}_Δ eine quadratische Ordnung und A eine Menge von \mathcal{O}_Δ Idealen ist mit $\mathcal{O}_\Delta, \{0\} \notin A$.

2.2. Definition (Relation \leq) Zwei Faktorisierungen $\mathcal{F}_1 = (\mathcal{O}_\Delta, A)$ und $\mathcal{F}_2 = (\mathcal{O}_{\Delta'}, B)$ stehen in der Relation \leq zueinander ($\mathcal{F}_1 \leq \mathcal{F}_2$), wenn

1. $\mathcal{O}_\Delta \subseteq \mathcal{O}_{\Delta'}$,
2. $\forall \mathfrak{a} \in A \quad \mathfrak{a} \mathcal{O}_{\Delta'} = \prod_{\mathfrak{b} \in B} \mathfrak{b}^{e(\mathfrak{a}, \mathfrak{b})}$ mit $e(\mathfrak{a}, \mathfrak{b}) \in \mathbb{N}_0$,
3. $\forall \mathfrak{b} \in B \quad \exists \mathfrak{a} \in A$ mit $\mathfrak{b} \supseteq \mathfrak{a}$.

Man sagt: \mathcal{F}_2 ist eine Verfeinerung von \mathcal{F}_1 .

2.3. Definition (ggT-frei) Eine Faktorisierung $\mathcal{F} = (\mathcal{O}_\Delta, A)$ heißt ggT-frei, wenn alle $\mathfrak{a} \in A$ invertierbar und paarweise teilerfremd sind.

2.4. Lemma \leq ist eine reflexive und transitive Relation auf der Menge aller Faktorisierungen und eine Ordnungsrelation auf der Menge aller ggT-freien Faktorisierungen.

Beweis: Seien $\mathcal{F}_1 = (\mathcal{O}_\Delta, A)$, $\mathcal{F}_2 = (\mathcal{O}_{\Delta'}, B)$ und $\mathcal{F}_3 = (\mathcal{O}_{\tilde{\Delta}}, C)$ Faktorisierungen. Trivialerweise gilt $\mathcal{F}_1 \leq \mathcal{F}_1$, d.h. die Symmetrie.

Gilt $\mathcal{F}_1 \leq \mathcal{F}_2$ und $\mathcal{F}_2 \leq \mathcal{F}_3$, so folgt sofort $\mathcal{O}_\Delta \subseteq \mathcal{O}_{\tilde{\Delta}}$. Außerdem gilt für ein $\mathfrak{a} \in A$

$$\begin{aligned} \mathfrak{a}\mathcal{O}_{\tilde{\Delta}} &= \mathfrak{a}\mathcal{O}_{\Delta'}\mathcal{O}_{\tilde{\Delta}} \\ &= \left(\prod_{\mathfrak{b} \in B} \mathfrak{b}^{e(\mathfrak{a}, \mathfrak{b})}\right)\mathcal{O}_{\tilde{\Delta}} \\ &= \prod_{\mathfrak{b} \in B} (\mathfrak{b}\mathcal{O}_{\tilde{\Delta}})^{e(\mathfrak{a}, \mathfrak{b})} \\ &= \prod_{\mathfrak{b} \in B} \left(\prod_{\mathfrak{c} \in C} \mathfrak{c}^{e(\mathfrak{b}, \mathfrak{c})}\right)^{e(\mathfrak{a}, \mathfrak{b})} \\ &= \prod_{\mathfrak{c} \in C} \mathfrak{c}^{e'(\mathfrak{a}, \mathfrak{c})} \end{aligned}$$

mit $e'(\mathfrak{a}, \mathfrak{c}) = \sum_{\mathfrak{b} \in B} e(\mathfrak{a}, \mathfrak{b})e(\mathfrak{b}, \mathfrak{c}) \in \mathbb{N}_0$. Für ein $\mathfrak{c} \in C$ existiert ein $\mathfrak{b} \in B$ mit $\mathfrak{c} \supseteq \mathfrak{b}$. Für dieses \mathfrak{b} existiert ein $\mathfrak{a} \in A$ mit $\mathfrak{b} \supseteq \mathfrak{a}$. Daraus folgt $\mathfrak{c} \supseteq \mathfrak{a}$. Es gilt also $\mathcal{F}_1 \leq \mathcal{F}_3$, die Transitivität.

Gilt $\mathcal{F}_1 \leq \mathcal{F}_2$ und $\mathcal{F}_2 \leq \mathcal{F}_1$ mit ggT-freien \mathcal{F}_1 und \mathcal{F}_2 , dann gilt $\mathcal{O}_\Delta = \mathcal{O}_{\Delta'}$. Zu zeigen ist $A \subseteq B$, aus Symmetriegründen gilt dann $A = B$ und somit $\mathcal{F}_1 = \mathcal{F}_2$, die Antisymmetrie. Sei $\tilde{\mathfrak{a}} \in A$. Dann gilt wegen $\mathcal{F}_1 \leq \mathcal{F}_2$:

$$\tilde{\mathfrak{a}} = \prod_{\mathfrak{b} \in B} \mathfrak{b}^{e(\tilde{\mathfrak{a}}, \mathfrak{b})}.$$

Da aber auch $\mathcal{F}_2 \leq \mathcal{F}_1$ gilt, gibt es ein $\tilde{\mathfrak{b}} \in B$ mit $\tilde{\mathfrak{a}} \supseteq \tilde{\mathfrak{b}}$. Man hat also

$$\prod_{\mathfrak{b} \in B} \mathfrak{b}^{e(\tilde{\mathfrak{a}}, \mathfrak{b})} \supseteq \tilde{\mathfrak{b}}.$$

Ist für ein $\mathfrak{b}' \in B$ der Exponent $e(\tilde{\mathfrak{a}}, \mathfrak{b}') \geq 1$, dann folgt

$$\mathfrak{b}' \supseteq \mathfrak{b}'^{e(\tilde{\mathfrak{a}}, \mathfrak{b}')} \supseteq \tilde{\mathfrak{b}}.$$

Da dann $\mathfrak{b}' + \tilde{\mathfrak{b}} = \mathfrak{b}' \neq \mathcal{O}_\Delta$ ist, muß mit der ggT-Freiheit von \mathcal{F}_2 $\mathfrak{b}' = \tilde{\mathfrak{b}}$ sein. Weil $N(\mathfrak{b}')$ multiplikativ ist und $\mathfrak{b}' \neq \mathcal{O}_\Delta$, also \mathfrak{b}' echt in seinem Multiplikatorenring enthalten ist, folgt $e(\tilde{\mathfrak{a}}, \mathfrak{b}') = 1$. Wäre $e(\tilde{\mathfrak{a}}, \mathfrak{b}^*) \geq 1$ für ein $\mathfrak{b}^* \neq \mathfrak{b}'$, dann würde mit dem obigen Argument $\mathfrak{b}^* = \mathfrak{b}'$ folgen. Deshalb ist $e(\tilde{\mathfrak{a}}, \mathfrak{b}) = 1$ für genau ein $\mathfrak{b} \in B$ (hier $\tilde{\mathfrak{b}}$) und für alle anderen $\mathfrak{b} \in B$ gilt $e(\tilde{\mathfrak{a}}, \mathfrak{b}) = 0$. Es gilt also $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}}$ und damit $A \subseteq B$. ■

2.5. Bemerkung Es ist zu beachten, daß die Invertierbarkeit der Ideale von ggT-freien Faktorisierungen im Beweis von Lemma 2.4 keine Rolle spielt. Für ein echtes \mathcal{O}_Δ Ideal \mathfrak{a} gilt $\mathfrak{a}^n \subset \mathfrak{a}$, egal, ob \mathfrak{a} invertierbar ist oder nicht. Dies liegt daran, daß die Ordnung von \mathfrak{a} multiplikativ ist, also $|\mathcal{O}_\Delta/\mathfrak{a}^n| = |\mathcal{O}_\Delta/\mathfrak{a}|^n$ gilt. Deshalb ist $\mathfrak{a}^n \subset \mathfrak{a} \forall n > 1$, wenn \mathfrak{a} eine echtes \mathcal{O}_Δ Ideal ist. Dann ist nämlich $|\mathcal{O}_\Delta/\mathfrak{a}| > 1$. Wir haben also eine Ordnungsrelation auf den Faktorisierungen, deren Ideale paarweise teilerfremd sind.

2.2 Refine

2.6. Algorithmus refine

Der Algorithmus manipuliert ein Liste $L = ((\mathbf{n}_1, e_1), \dots, (\mathbf{n}_l, e_l))$, wobei $1 \leq i \leq l$, $\mathbf{n}_i \trianglelefteq \mathcal{O}_{\Delta'}$, $1 \leq i \leq l$, echte invertierbare $\mathcal{O}_{\Delta'}$ Ideale und $e_i \in \mathbb{N}$ sind.

EINGABE: \mathcal{O}_{Δ} , \mathcal{O}_{Δ} Ideale $\mathbf{a}_1, \dots, \mathbf{a}_k \neq \mathcal{O}_{\Delta}$, $\{0\}$ in Standarddarstellung.

AUSGABE: Oberordnung $\mathcal{O}_{\Delta'} \supseteq \mathcal{O}_{\Delta}$ und Paare $(\mathbf{n}_1, e_1), \dots, (\mathbf{n}_l, e_l)$, $\mathbf{n}_i \trianglelefteq \mathcal{O}_{\Delta'}$ invertierbar mit

1. $\forall i \neq j \quad \mathbf{n}_i + \mathbf{n}_j = \mathcal{O}_{\Delta'}$
2. $\mathbf{a}_1 \mathcal{O}_{\Delta'} \cdots \mathbf{a}_k \mathcal{O}_{\Delta'} = \mathbf{n}_1^{e_1} \cdots \mathbf{n}_l^{e_l}$.

INITIALISIERUNG

- (1) Berechne für $1 \leq i \leq k$ $d_i = \text{ggT}(a(\mathbf{a}_i), b(\mathbf{a}_i), c(\mathbf{a}_i))$.
- (2) $\mathcal{O}_{\Delta'} := \mathcal{O}_{\Delta} / \text{kgV}(d_1, \dots, d_k)^2$
- (3) $\forall 1 \leq i \leq k \quad \mathbf{n}_i := \mathbf{a}_i \mathcal{O}_{\Delta'}$
- (4) $L := ((\mathbf{n}_1, 1), \dots, (\mathbf{n}_k, 1))$

VERFEINERN

- (5) **while** $(\exists i \neq j \text{ mit } \mathbf{n}_i + \mathbf{n}_j \neq \mathcal{O}_{\Delta'})$ **do**
- (6) **if** $(\text{ggT}(a(\mathbf{n}_i + \mathbf{n}_j), b(\mathbf{n}_i + \mathbf{n}_j), c(\mathbf{n}_i + \mathbf{n}_j)) = d > 1)$ **then**
- (7) $\mathcal{O}_{\Delta'} := \mathcal{O}_{\Delta'} / d^2$
- (8) Ersetze alle Paare (\mathbf{n}, e) aus L mit $(\mathbf{n} \mathcal{O}_{\Delta'}, e)$.
- (9) **fi**
- (10) Lösche die Paare (\mathbf{n}_i, e_i) und (\mathbf{n}_j, e_j) aus L , und füge

 $(\mathbf{n}_i / (\mathbf{n}_i + \mathbf{n}_j), e_i), ((\mathbf{n}_i + \mathbf{n}_j), e_i + e_j), (\mathbf{n}_j / (\mathbf{n}_i + \mathbf{n}_j), e_j)$

 in L ein. Lösche alle Einträge der Form $(\mathcal{O}_{\Delta'}, e)$
- (11) **od**
- (12) **return** $(\mathcal{O}_{\Delta'}, L)$

2.7. Lemma Gehört der quadratische Modul M zu \mathcal{O}_{Δ} und ist $\mathcal{O}_{\Delta'} \supseteq \mathcal{O}_{\Delta}$ eine quadratische Ordnung, dann gehört $M \mathcal{O}_{\Delta'}$ zu $\mathcal{O}_{\Delta'}$ und es gilt

$$N(M) = N(M \mathcal{O}_{\Delta'}).$$

Beweis: Sei $\mathcal{O}_{\tilde{\Delta}}$ der Multiplikatorenring von $M \mathcal{O}_{\Delta'}$. Dann gilt mit Korollar 1.66

$$M \mathcal{O}_{\Delta'} \sigma(M \mathcal{O}_{\Delta'}) = N(M \mathcal{O}_{\Delta'}) \mathcal{O}_{\tilde{\Delta}}. \quad (2.1)$$

Wieder wegen Korollar 1.66 folgt aber auch

$$\begin{aligned} M \mathcal{O}_{\Delta'} \sigma(M \mathcal{O}_{\Delta'}) &= M \sigma(M) \mathcal{O}_{\Delta'} \\ &= N(M) \mathcal{O}_{\Delta} \mathcal{O}_{\Delta'} \sigma(\mathcal{O}_{\Delta'}) \\ &= N(M) \mathcal{O}_{\Delta'}. \end{aligned} \quad (2.2)$$

Denn es gilt $\sigma(\sum_{1 \leq i \leq n} m_i o_i) = \sum_{1 \leq i \leq n} \sigma(m_i) \sigma(o_i)$ und deshalb gilt

$$\sigma(M\mathcal{O}_{\Delta'}) = \sigma(M)\sigma(\mathcal{O}_{\Delta'}).$$

$N(M)$ ist in (2.2) die kleinste positive rationale Zahl, und $N(M\mathcal{O}_{\Delta'})$ ist in (2.1) die kleinste positive rationale Zahl. Daraus folgt $N(M) = N(M\mathcal{O}_{\Delta'})$ und $\mathcal{O}_{\bar{\Delta}} = \mathcal{O}_{\Delta'}$. ■

2.8. Korollar Ist $\mathfrak{a} \leq \mathcal{O}_{\Delta}$, $\mathfrak{a} \neq \{0\}$, $\mathfrak{a} \neq \mathcal{O}_{\Delta}$, und ist $\mathcal{O}_{\mathfrak{a}}$ in $\mathcal{O}_{\Delta'}$ enthalten, dann ist $\mathfrak{a}\mathcal{O}_{\Delta'}$ ein invertierbares echtes $\mathcal{O}_{\Delta'}$ Ideal.

2.9. Lemma Nach dem t -ten Durchlauf durch die **while**-Schleife in Algorithmus 2.6 gilt mit der Liste $L^{(t)} = ((\mathfrak{n}_1, e_1), \dots, (\mathfrak{n}_{l^{(t)}}, e_{l^{(t)}}))$ und der dort berechneten Oberordnung $\mathcal{O}_{\Delta'}^{(t)}$

1. $\mathfrak{n}_1, \dots, \mathfrak{n}_{l^{(t)}} \leq \mathcal{O}_{\Delta'}^{(t)}$ sind invertierbar.
2. $\forall \nu \in \{1, \dots, l^{(t)}\} \quad \exists \mu \in \{1, \dots, k\}$ mit $\mathfrak{n}_{\nu} \supseteq \mathfrak{a}_{\mu}$.
3. $\mathfrak{n}_1^{e_1} \cdots \mathfrak{n}_{l^{(t)}}^{e_{l^{(t)}}} = \mathfrak{a}_1 \mathcal{O}_{\Delta'}^{(t)} \cdots \mathfrak{a}_k \mathcal{O}_{\Delta'}^{(t)}$.
4. $\forall \mu \in \{1, \dots, k\}$ gibt es $\beta_{\mu, \nu} \in \mathbb{N}_0$ mit $\mathfrak{a}_{\mu} \mathcal{O}_{\Delta'}^{(t)} = \prod_{1 \leq \nu \leq l^{(t)}} \mathfrak{n}_{\nu}^{\beta_{\mu, \nu}}$

Beweis: Induktion durch die Anzahl t der **while** Durchläufe.

Der Multiplikatorenring von \mathfrak{a}_i ist $\mathcal{O}_{\Delta/d_i^2}$. Also wird nach Korollar 1.63 in Zeile (2) die kleinste Ordnung $\mathcal{O}_{\Delta'}^{(0)}$ ermittelt, die die Multiplikatorenringe von $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ enthält. \mathfrak{a}_i ist ein invertierbares $\mathcal{O}_{\Delta/d_i^2}$ Ideal, also ist nach Korollar 2.8 $\mathfrak{a}_i \mathcal{O}_{\Delta'}^{(0)}$ ein invertierbares $\mathcal{O}_{\Delta'}^{(0)}$ Ideal. Weil $L^{(0)} = ((\mathfrak{a}_1 \mathcal{O}_{\Delta'}^{(0)}, 1), \dots, (\mathfrak{a}_k \mathcal{O}_{\Delta'}^{(0)}, 1))$ ist, folgt somit Punkt 1. Die Behauptungen 2, 3 und 4 folgen trivialerweise.

Seien nun $t \geq 0$ Durchläufe durch die **while**-Schleife gemacht worden und damit

$$L^{(t)} = ((\mathfrak{n}_1, e_1), \dots, (\mathfrak{n}_{l^{(t)}}, e_{l^{(t)}})) \text{ und } \mathcal{O}_{\Delta'}^{(t)} \supseteq \mathcal{O}_{\Delta}.$$

berechnet. Nach der Induktionsvoraussetzung gelten 1, 2, 3 und 4. \mathfrak{n}_i und \mathfrak{n}_j sollen mit $i < j$ die beiden Ideale aus $L^{(t)}$ sein, die Algorithmus 2.6 in Zeile (5), mit $\mathfrak{n}_i + \mathfrak{n}_j \neq \mathcal{O}_{\Delta'}^{(t)}$ findet. In Zeilen (6)-(9) wird der Multiplikatorenring $\mathcal{O}_{\Delta'}^{(t+1)} \supseteq \mathcal{O}_{\Delta'}^{(t)}$ von $\mathfrak{n}_i + \mathfrak{n}_j$ ermittelt, und $\forall \nu \in \{1, \dots, l^{(t)}\}$ wird \mathfrak{n}_{ν} durch $\tilde{\mathfrak{n}}_{\nu} = \mathfrak{n}_{\nu} \mathcal{O}_{\Delta'}^{(t+1)}$ ersetzt. Nach Lemma 2.7 sind die $\mathcal{O}_{\Delta'}^{(t+1)}$ Ideale $\tilde{\mathfrak{n}}_{\nu}$ invertierbar, und

$$\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j = (\mathfrak{n}_i + \mathfrak{n}_j) \mathcal{O}_{\Delta'}^{(t+1)} = \mathfrak{n}_i + \mathfrak{n}_j$$

gehört zu $\mathcal{O}_{\Delta'}^{(t+1)}$ und ist somit ebenfalls invertierbar. Mit Lemma 1.75 sind dann auch $\tilde{\mathfrak{n}}_i / (\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j)$ und $\tilde{\mathfrak{n}}_j / (\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j)$ invertierbare $\mathcal{O}_{\Delta'}^{(t+1)}$ Ideale. Behauptung 1 ist also bewiesen.

Weil nach Induktionsvoraussetzung

$$\mathfrak{a}_1 \mathcal{O}_{\Delta'}^{(t)} \cdots \mathfrak{a}_k \mathcal{O}_{\Delta'}^{(t)} = \mathfrak{n}_1^{e_1} \cdots \mathfrak{n}_{l^{(t)}}^{e_{l^{(t)}}}$$

gilt, folgt

$$\begin{aligned}
\mathfrak{a}_1 \mathcal{O}_{\Delta'}^{(t+1)} \cdots \mathfrak{a}_k \mathcal{O}_{\Delta'}^{(t+1)} &= \tilde{\mathfrak{n}}_1^{e_1} \cdots \tilde{\mathfrak{n}}_{l^{(t)}}^{e_{l^{(t)}}} \\
&= \tilde{\mathfrak{n}}_1^{e_1} \cdots \tilde{\mathfrak{n}}_{i-1}^{e_{i-1}} (\tilde{\mathfrak{n}}_i / (\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j))^{e_i} \tilde{\mathfrak{n}}_{i+1}^{e_{i+1}} \cdots \tilde{\mathfrak{n}}_{j-1}^{e_{j-1}} (\tilde{\mathfrak{n}}_j / (\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j))^{e_j} \\
&\quad \cdots \tilde{\mathfrak{n}}_{l^{(t)}}^{e_{l^{(t)}}} (\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j)^{e_i + e_j}.
\end{aligned} \tag{2.3}$$

Da $L^{(t+1)}$ schließlich aus denen zur Gleichung (2.3) korrespondierenden Paaren bis auf Paare mit erstem Element gleich $\mathcal{O}_{\Delta'}^{(t+1)}$ besteht folgt 3.

Jedes Ideal aus $L^{(t+1)}$ enthält ein Ideal aus $L^{(t)}$, welches dann wiederum ein \mathfrak{a}_μ enthält. Deshalb gilt 2.

Nach der Induktionsvoraussetzung gibt es für jedes $\mu \in \{1, \dots, k\}$ $\beta_{\mu, \nu} \in \mathbb{N}_0$ mit

$$\mathfrak{a}_\mu \mathcal{O}_{\Delta'}^{(t)} = \prod_{1 \leq \nu \leq l} \mathfrak{n}_\nu^{\beta_{\mu, \nu}}.$$

Deshalb gilt

$$\begin{aligned}
\mathfrak{a}_\mu \mathcal{O}_{\Delta'}^{(t+1)} &= \prod_{1 \leq \nu \leq l^{(t)}} \tilde{\mathfrak{n}}_\nu^{\beta_{\mu, \nu}} \\
&= \left(\prod_{1 \leq \nu \leq l^{(t)}, \nu \neq i, j} \tilde{\mathfrak{n}}_\nu^{\beta_{\mu, \nu}} \right) (\tilde{\mathfrak{n}}_i / (\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j))^{\beta_{\mu, i}} (\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j)^{\beta_{\mu, i} + \beta_{\mu, j}} (\tilde{\mathfrak{n}}_j / (\tilde{\mathfrak{n}}_i + \tilde{\mathfrak{n}}_j))^{\beta_{\mu, j}},
\end{aligned}$$

und es folgt 4. ■

2.10. Lemma Sei $N = N(\mathfrak{a}_1) \cdots N(\mathfrak{a}_k)$. Dann durchläuft Algorithmus 2.6 höchstens $\log(N)$ mal die **while** Schleife.

Beweis: Sei $L^{(t)} = ((\mathfrak{n}_1, e_1), \dots, (\mathfrak{n}_{l^{(t)}}, e_{l^{(t)}}))$ die Liste nach dem t -ten Durchlauf durch die **while** Schleife und $\mathcal{O}_{\Delta'}^{(t)}$ die dort berechnete Oberordnung von \mathcal{O}_Δ . Definiere

$$S_{(t)} = \sum_{1 \leq i \leq l^{(t)}} (e_i^{(t)} - 1).$$

Behauptung: $S_{(t+1)} - S_{(t)} \geq 1$.

Angenommen der Algorithmus hat \mathfrak{n}_i und \mathfrak{n}_j ausgewählt und Zeilen (6) bis (9) durchgeführt. Jetzt gilt immernoch $\mathfrak{n}_i + \mathfrak{n}_j \neq \mathcal{O}_{\Delta'}^{(t+1)}$ und in L sind nur echte $\mathcal{O}_{\Delta'}^{(t+1)}$ Ideale als erster Eintrag in den Paaren zu finden.

1. Fall: $\mathfrak{n}_i / (\mathfrak{n}_i + \mathfrak{n}_j) = \mathcal{O}_{\Delta'}^{(t+1)}$ und $\mathfrak{n}_j / (\mathfrak{n}_i + \mathfrak{n}_j) \neq \mathcal{O}_{\Delta'}^{(t+1)}$. Dann ist

$$S_{(t+1)} = S_{(t)} + (e_i + e_j - 1) - (e_i - 1) = S_{(t)} + e_j > S_{(t)}.$$

2. Fall: $\mathfrak{n}_j / (\mathfrak{n}_i + \mathfrak{n}_j) = \mathcal{O}_{\Delta'}^{(t+1)}$ und $\mathfrak{n}_i / (\mathfrak{n}_i + \mathfrak{n}_j) \neq \mathcal{O}_{\Delta'}^{(t+1)}$. Symmetrisch zum 1. Fall.

3. Fall: $\mathfrak{n}_i/(\mathfrak{n}_i + \mathfrak{n}_j) = \mathcal{O}_{\Delta'}^{(t+1)}$ und $\mathfrak{n}_j/(\mathfrak{n}_i + \mathfrak{n}_j) = \mathcal{O}_{\Delta'}^{(t+1)}$. Dann ist

$$S_{(t+1)} = S_{(t)} - (e_i - 1) - (e_j - 1) + (e_i + e_j - 1) = S_{(t)} + 1.$$

4. Fall: $\mathfrak{n}_i/(\mathfrak{n}_i + \mathfrak{n}_j) \neq \mathcal{O}_{\Delta'}^{(t+1)}$ und $\mathfrak{n}_j/(\mathfrak{n}_i + \mathfrak{n}_j) \neq \mathcal{O}_{\Delta'}^{(t+1)}$. Daraus folgt

$$S_{(t+1)} = S_{(t)} + (e_i + e_j - 1) > S_{(t)}.$$

Es gilt $S_{(t)} \leq \log(N)$, da

$$\begin{aligned} N = N(\mathfrak{a}_1) \cdots N(\mathfrak{a}_k) &= N(\mathfrak{a}_1 \mathcal{O}_{\Delta'}^{(t)}) \cdots N(\mathfrak{a}_k \mathcal{O}_{\Delta'}^{(t)}) \\ &= N(\mathfrak{a}_1 \mathcal{O}_{\Delta'}^{(t)} \cdots \mathfrak{a}_k \mathcal{O}_{\Delta'}^{(t)}) \\ &= N(\mathfrak{n}_1^{e_1} \cdots \mathfrak{n}_l^{e_l^{(t)}}) \\ &= N(\mathfrak{n}_1)^{e_1} \cdots N(\mathfrak{n}_l)^{e_l^{(t)}} \\ &\geq 2^{e_1} \cdots 2^{e_l^{(t)}} \\ &= 2^{\sum_{1 \leq i \leq l^{(t)}} e_i} \\ &\geq 2^{S_{(t)}}. \end{aligned}$$

Daraus folgt die Behauptung. ■

2.11. Satz Algorithmus 2.6 terminiert und ist korrekt.

Beweis: Lemma 2.9, Lemma 2.10 und die Abbruchbedingung von Algorithmus 2.6 zeigen die Behauptung. ■

2.12. Bemerkung Ist $\mathfrak{a}_1, \dots, \mathfrak{a}_k, \mathcal{O}_{\Delta}$ der Input von Algorithmus 2.6 und

$$\mathcal{O}_{\Delta'}, L = ((\mathfrak{n}_1, e_1), \dots, (\mathfrak{n}_l, e_l))$$

der dazugehörige Output, dann zeigen Lemma 2.9 und Satz 2.11, daß die Faktorisierung $\mathcal{F}' = (\mathcal{O}_{\Delta'}, \cup_{1 \leq i \leq l} \{\mathfrak{n}_i\})$ eine ggT-freie Verfeinerung von $\mathcal{F} = (\mathcal{O}_{\Delta}, \cup_{1 \leq i \leq k} \{\mathfrak{a}_i\})$ ist.

2.3 Der Output von Refine

2.13. Lemma Sind $\mathfrak{n}_1, \dots, \mathfrak{n}_l \neq \mathcal{O}_{\Delta}$ paarweise teilerfremde invertierbare \mathcal{O}_{Δ} Ideale, und gilt mit $e_1, \dots, e_l, f_1, \dots, f_l \in \mathbb{N}_0$,

$$\mathfrak{n}_1^{e_1} \cdots \mathfrak{n}_l^{e_l} = \mathfrak{n}_1^{f_1} \cdots \mathfrak{n}_l^{f_l},$$

dann gilt $\forall 1 \leq i \leq l \ e_i = f_i$.

Beweis: Nehmen wir ohne Einschränkung an $e_1 > f_1$. Dann folgt

$$\mathfrak{n}_1^{e_1 - f_1} \mathfrak{n}_2^{e_2} \cdots \mathfrak{n}_l^{e_l} = \mathfrak{n}_2^{f_2} \cdots \mathfrak{n}_l^{f_l}.$$

Aus Lemma 1.42 folgt, daß es ein Primideal \mathfrak{p} gibt, welches \mathfrak{n}_1 und somit auch $\mathfrak{n}_2^{f_2} \cdots \mathfrak{n}_l^{f_l}$ enthält. Wegen Lemma 1.20 enthält \mathfrak{p} dann außer \mathfrak{n}_1 noch ein \mathfrak{n}_i mit $i > 1$, was ein Widerspruch zur Teilerfremdheit der Ideale $\mathfrak{n}_1, \dots, \mathfrak{n}_l$ ist, denn $\mathfrak{a}_1 + \mathfrak{a}_i \subseteq \mathfrak{p} \subset \mathcal{O}_\Delta$. ■

Sei

$$\mathfrak{a}_1, \dots, \mathfrak{a}_k, \mathcal{O}_\Delta \quad (2.4)$$

der Input von Algorithmus 2.6. (2.4) induziert eine Faktorisierung

$$\mathcal{F} = (\mathcal{O}_\Delta, \cup_{1 \leq i \leq k} \{\mathfrak{a}_i\}). \quad (2.5)$$

Algorithmus 2.6 ist nichtdeterministisch in der Auswahl von \mathfrak{n}_i und \mathfrak{n}_j in Zeile (5). Es wäre also vorstellbar, daß der Output nicht eindeutig ist. Es seien

$$\begin{aligned} \mathcal{O}_1 &= (\mathcal{O}_{\Delta'_{(1)}}, L^{(1)} = ((\mathfrak{n}_1^{(1)}, e_1^{(1)}), \dots, (\mathfrak{n}_{l^{(1)}}^{(1)}, e_{l^{(1)}}^{(1)}))) \\ \mathcal{O}_2 &= (\mathcal{O}_{\Delta'_{(2)}}, L^{(2)} = ((\mathfrak{n}_1^{(2)}, e_1^{(2)}), \dots, (\mathfrak{n}_{l^{(2)}}^{(2)}, e_{l^{(2)}}^{(2)}))) \end{aligned}$$

Rückgabewerte von Algorithmus 2.6 bei Eingabe (2.4). Es ist das Ziel dieses Abschnittes ist zu zeigen, daß die Faktorisierung

$$\mathcal{F}' = (\mathcal{O}_{\Delta'_{(1)}}, \cup_{1 \leq i \leq l^{(1)}} \{\mathfrak{n}_i^{(1)}\}) \quad (2.6)$$

die, bezüglich der Ordnungsrelation \leq aus Definition 2.2, auf der Menge \mathcal{S} der ggT-freien Verfeinerungen von \mathcal{F} das eindeutige minimale Element ist.

Mit diesem Resultat ist die Ordnung im Output von Algorithmus 2.6 schon eindeutig bestimmt, es gilt also

$$\mathcal{O}_{\Delta'_{(1)}} = \mathcal{O}_{\Delta'_{(2)}} = \mathcal{O}_{\Delta'}.$$

Außerdem stimmen dann die in $L^{(1)}$ und $L^{(2)}$ vorkommenden $\mathcal{O}_{\Delta'}$ Ideale überein. Weil in $L^{(1)}$ und $L^{(2)}$ die Ideale ungleich $\mathcal{O}_{\Delta'}$ und paarweise teilerfremd sind, kommt in beiden Listen kein Ideal doppelt vor. Die Listen haben also gleiche Länge. Nimmt man an, daß $L^{(2)}$ so umgeordnet ist, daß für $1 \leq i \leq l$, $\mathfrak{n}_i^{(1)} = \mathfrak{n}_i^{(2)}$ gilt, dann folgt

$$\mathfrak{n}_1^{e_1^{(1)}} \cdots \mathfrak{n}_l^{e_l^{(1)}} = \mathfrak{n}_1^{e_1^{(2)}} \cdots \mathfrak{n}_l^{e_l^{(2)}},$$

und mit Lemma 2.13 folgt dann $e_i^{(1)} = e_i^{(2)}$ für $1 \leq i \leq l$. Der Output ist also bis auf die Reihenfolge der Paare in der Liste L eindeutig.

2.14. Lemma Seien $\mathfrak{a}_1, \dots, \mathfrak{a}_k \leq \mathcal{O}_\Delta$ paarweise teilerfremd, dann gilt $\forall I, J \subseteq \{1, \dots, k\}$ mit $I \cap J = \emptyset$ und $\alpha_i, \beta_j \in \mathbb{N}_0$

$$\prod_{i \in I} \mathfrak{a}_i^{\alpha_i} + \prod_{j \in J} \mathfrak{a}_j^{\beta_j} = \mathcal{O}_\Delta.$$

Beweis: Nehmen wir mal an

$$\prod_{i \in I} \mathfrak{a}_i^{\alpha_i} + \prod_{j \in J} \mathfrak{a}_j^{\beta_j} \neq \mathcal{O}_\Delta.$$

Dann gibt es wegen Lemma 1.42 ein Primideal \mathfrak{p} mit

$$\mathfrak{p} \supseteq \prod_{i \in I} \mathfrak{a}_i^{\alpha_i} + \prod_{j \in J} \mathfrak{a}_j^{\beta_j}.$$

Daraus folgt $\mathfrak{p} \supseteq \prod_{i \in I} \mathfrak{a}_i^{\alpha_i}$ und $\mathfrak{p} \supseteq \prod_{j \in J} \mathfrak{a}_j^{\beta_j}$. Wegen Lemma 1.20 gibt es dann ein $i \in I$ und ein $j \in J$ mit $\mathfrak{p} \supseteq \mathfrak{a}_i$ und $\mathfrak{p} \supseteq \mathfrak{a}_j$. Weil \mathfrak{a}_i und \mathfrak{a}_j teilerfremd sind, gilt

$$\mathfrak{p} \supseteq \mathfrak{a}_i + \mathfrak{a}_j = \mathcal{O}_\Delta$$

ein Widerspruch, weil ein Primideal echt in \mathcal{O}_Δ enthalten ist. ■

2.15. Lemma Seien $\mathfrak{b}_1, \dots, \mathfrak{b}_k \leq \mathcal{O}_\Delta$ paarweise teilerfremd, und

$$\begin{aligned} \mathfrak{n}_1 &= \prod_{\mu=1, \dots, k} \mathfrak{b}_\mu^{\alpha_{1,\mu}} \\ \mathfrak{n}_2 &= \prod_{\mu=1, \dots, k} \mathfrak{b}_\mu^{\alpha_{2,\mu}} \end{aligned}$$

mit $\alpha_{1,\mu}, \alpha_{2,\mu} \in \mathbb{N}_0$. Dann gilt:

$$\mathfrak{n}_1 + \mathfrak{n}_2 = \prod_{\mu=1, \dots, k} \mathfrak{b}_\mu^{\min\{\alpha_{1,\mu}, \alpha_{2,\mu}\}}.$$

Beweis:

$$\begin{aligned} \mathfrak{n}_1 + \mathfrak{n}_2 &= \prod_{\mu=1, \dots, k} \mathfrak{b}_\mu^{\min\{\alpha_{1,\mu}, \alpha_{2,\mu}\}} \\ &\cdot \left(\prod_{\mu=1, \dots, k} \mathfrak{b}_\mu^{\alpha_{1,\mu} - \min\{\alpha_{1,\mu}, \alpha_{2,\mu}\}} + \prod_{\mu=1, \dots, k} \mathfrak{b}_\mu^{\alpha_{2,\mu} - \min\{\alpha_{1,\mu}, \alpha_{2,\mu}\}} \right) \end{aligned}$$

und

$$\prod_{\mu=1, \dots, k} \mathfrak{b}_\mu^{\alpha_{1,\mu} - \min\{\alpha_{1,\mu}, \alpha_{2,\mu}\}} + \prod_{\mu=1, \dots, k} \mathfrak{b}_\mu^{\alpha_{2,\mu} - \min\{\alpha_{1,\mu}, \alpha_{2,\mu}\}} = \mathcal{O}_\Delta$$

nach Lemma 2.14. ■

2.16. Lemma Sind $\mathcal{O}_{\tilde{\Delta}} \supseteq \mathcal{O}_\Delta$ Ordnungen, $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ echte \mathcal{O}_Δ Ideale und $\mathfrak{b}_1, \dots, \mathfrak{b}_s$ invertierbare und paarweise teilerfremde $\mathcal{O}_{\tilde{\Delta}}$ Ideale mit

$$\forall \mu \in \{1, \dots, k\} \quad \exists \alpha_{\mu,\nu} \in \mathbb{N}_0 \quad \text{mit} \quad \mathfrak{a}_\mu \mathcal{O}_{\tilde{\Delta}} = \prod_{\nu=1, \dots, s} \mathfrak{b}_\nu^{\alpha_{\mu,\nu}}. \quad (2.7)$$

Sei $L^{(t)} = ((\mathfrak{n}_1, e_1), \dots, (\mathfrak{n}_{l(t)}, e_{l(t)}))$ die Liste nach dem t -ten Durchlauf durch die **while**-Schleife in Algorithmus 2.6 bei Eingabe

$$\mathfrak{a}_1, \dots, \mathfrak{a}_k, \mathcal{O}_\Delta$$

und $\mathcal{O}_{\tilde{\Delta}}^{(t)}$ die dort berechnete Ordnung. Dann gilt:

1. $\mathcal{O}_{\tilde{\Delta}} \supseteq \mathcal{O}_{\tilde{\Delta}'}^{(t)} \supseteq \mathcal{O}_{\Delta}$
2. $\forall 1 \leq \mu \leq l^{(t)} \quad \exists \beta_{\mu,\nu} \in \mathbb{N}_0$ mit $\mathfrak{n}_{\mu}\mathcal{O}_{\tilde{\Delta}} = \prod_{1 \leq \nu \leq s} \mathfrak{b}_{\nu}^{\beta_{\mu,\nu}}$.

Beweis: Induktion über t . In der Initialisierungsphase wird nach Korollar 1.63 die kleinste Oberordnung $\mathcal{O}_{\tilde{\Delta}'}^{(0)}$ berechnet, die die Multiplikatorenringe von $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ enthält.

$$L^{(0)} = ((\mathfrak{n}_1, e_1), \dots, (\mathfrak{n}_{l^{(0)}}, e_{l^{(0)}})) = ((\mathfrak{a}_1\mathcal{O}_{\tilde{\Delta}'}^{(0)}, 1), \dots, (\mathfrak{a}_k\mathcal{O}_{\tilde{\Delta}'}^{(0)}, 1))$$

Ist x ein Multiplikator von \mathfrak{a}_{μ} , dann ist x auch ein Multiplikator von $\mathfrak{a}_{\mu}\mathcal{O}_{\tilde{\Delta}} = \prod_{1 \leq \nu \leq s} \mathfrak{b}_{\nu}^{\alpha_{\mu,\nu}}$. Weil die $\mathcal{O}_{\tilde{\Delta}}$ Ideale \mathfrak{b}_{ν} invertierbar sind, ist auch $\mathfrak{a}_{\mu}\mathcal{O}_{\tilde{\Delta}}$ invertierbar. Nach Lemma 1.73 ist $x \in \mathcal{O}_{\tilde{\Delta}}$, also gilt $\mathcal{O}_{\tilde{\Delta}'}^{(0)} \subseteq \mathcal{O}_{\tilde{\Delta}}$.

Wegen (2.7) gilt für μ aus $\{1, \dots, l^{(0)}\}$

$$\begin{aligned} \mathfrak{n}_{\mu}\mathcal{O}_{\tilde{\Delta}} &= \mathfrak{a}_{\mu}\mathcal{O}_{\tilde{\Delta}'}^{(0)}\mathcal{O}_{\tilde{\Delta}} \\ &= \mathfrak{a}_{\mu}\mathcal{O}_{\tilde{\Delta}} \\ &= \prod_{1 \leq \nu \leq s} \mathfrak{b}_{\nu}^{\alpha_{\mu,\nu}}. \end{aligned}$$

Mit $\beta_{\mu,\nu} = \alpha_{\mu,\nu}$ folgt also Behauptung 2.

Seien $t \geq 0$ Durchläufe durch die **while**-Schleife gemacht worden, und seien $\mathfrak{n}_i, \mathfrak{n}_j$, $i < j$ die beiden $\mathcal{O}_{\tilde{\Delta}'}^{(t)}$ Ideale aus

$$L^{(t)} = ((\mathfrak{n}_1, e_1), \dots, (\mathfrak{n}_{l^{(t)}}, e_{l^{(t)}})),$$

die der Algorithmus 2.6 in Zeile (5) auswählt. Nach der Induktionsvoraussetzung gilt

$$\forall \mu \in \{1, \dots, l^{(t)}\} \quad \exists \beta_{\mu,\nu} \in \mathbb{N}_0 \text{ mit } \mathfrak{n}_{\mu}\mathcal{O}_{\tilde{\Delta}} = \prod_{1 \leq \nu \leq s} \mathfrak{b}_{\nu}^{\beta_{\mu,\nu}}. \quad (2.8)$$

Insbesondere gilt

$$\begin{aligned} \mathfrak{n}_i\mathcal{O}_{\tilde{\Delta}} &= \prod_{1 \leq \nu \leq s} \mathfrak{b}_{\nu}^{\beta_{i,\nu}} \\ \mathfrak{n}_j\mathcal{O}_{\tilde{\Delta}} &= \prod_{1 \leq \nu \leq s} \mathfrak{b}_{\nu}^{\beta_{j,\nu}}. \end{aligned}$$

Aus Lemma 2.15 folgt dann

$$(\mathfrak{n}_i + \mathfrak{n}_j)\mathcal{O}_{\tilde{\Delta}} = \prod_{1 \leq \nu \leq s} \mathfrak{b}_{\nu}^{\min\{\beta_{i,\nu}, \beta_{j,\nu}\}}.$$

Da die \mathfrak{b}_{ν} 's invertierbar sind, ist der Multiplikatorenring von $(\mathfrak{n}_i + \mathfrak{n}_j)\mathcal{O}_{\tilde{\Delta}}$ gleich $\mathcal{O}_{\tilde{\Delta}}$. Ist x im Multiplikatorenring von $\mathfrak{n}_i + \mathfrak{n}_j$, dann ist x auch ein Multiplikator von $(\mathfrak{n}_i + \mathfrak{n}_j) \cdot \mathcal{O}_{\tilde{\Delta}}$. Mit Lemma 1.73 ist dann $x \in \mathcal{O}_{\tilde{\Delta}}$. Im Algorithmus wird aber gerade in den Multiplikatorenring des quadratischen Moduls $(\mathfrak{n}_i + \mathfrak{n}_j)$ geliftet, und deshalb gilt $\mathcal{O}_{\tilde{\Delta}} \supseteq \mathcal{O}_{\tilde{\Delta}'}^{(t+1)} \supseteq \mathcal{O}_{\Delta}$. Es folgt also Behauptung 1.

$\mathfrak{n}_1, \dots, \mathfrak{n}_{l^{(t)}}$ sollen die in Zeile (8) durch $\mathfrak{n}_1 \mathcal{O}_{\Delta'}^{(t+1)}, \dots, \mathfrak{n}_{l^{(t)}} \mathcal{O}_{\Delta'}^{(t+1)}$ ersetzten Ideale bezeichnen. Weil $\mathcal{O}_{\Delta'}^{(t+1)} \subseteq \mathcal{O}_{\tilde{\Delta}}$ ist, gilt noch immer $\forall \mu \in \{1, \dots, l^{(t)}\} \mathfrak{n}_\mu \mathcal{O}_{\tilde{\Delta}} = \prod_{1 \leq \nu \leq s} \mathfrak{b}_\nu^{\beta_{\mu, \nu}}$, mit den $\beta_{\mu, \nu}$ aus (2.8). Die Ideale aus $L^{(t+1)}$ sind aus der Menge $\{\mathfrak{n}_1, \dots, \mathfrak{n}_{l^{(t)}}, \mathfrak{n}_i + \mathfrak{n}_j, \mathfrak{n}_i / (\mathfrak{n}_i + \mathfrak{n}_j), \mathfrak{n}_j / (\mathfrak{n}_i + \mathfrak{n}_j)\}$. Weil die \mathfrak{b}_ν 's invertierbar sind folgt

$$\begin{aligned} (\mathfrak{n}_i + \mathfrak{n}_j) \mathcal{O}_{\tilde{\Delta}} &= \prod_{1 \leq \nu \leq s} \mathfrak{b}_\nu^{\min\{\beta_{i, \nu}, \beta_{j, \nu}\}} \\ \mathfrak{n}_i / (\mathfrak{n}_i + \mathfrak{n}_j) \mathcal{O}_{\tilde{\Delta}} &= \prod_{1 \leq \nu \leq s} \mathfrak{b}_\nu^{\beta_{i, \nu} - \min\{\beta_{i, \nu}, \beta_{j, \nu}\}} \\ \mathfrak{n}_j / (\mathfrak{n}_i + \mathfrak{n}_j) \mathcal{O}_{\tilde{\Delta}} &= \prod_{1 \leq \nu \leq s} \mathfrak{b}_\nu^{\beta_{j, \nu} - \min\{\beta_{i, \nu}, \beta_{j, \nu}\}}. \end{aligned}$$

Deshalb gilt auch Behauptung 2. ■

2.17. Definition Die \mathcal{O}_Δ Ideale $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ heißen in der Ordnung $\mathcal{O}_{\Delta'} \supseteq \mathcal{O}_\Delta$ ggT-frei darstellbar, wenn es paarweise teilerfremde invertierbare $\mathcal{O}_{\Delta'}$ Ideale $\mathfrak{b}_1, \dots, \mathfrak{b}_s$ gibt, sodaß die $\mathcal{O}_{\Delta'}$ Ideale $\mathfrak{a}_1 \mathcal{O}_{\Delta'}, \dots, \mathfrak{a}_k \mathcal{O}_{\Delta'}$ Potenzprodukte der $\mathfrak{b}_1, \dots, \mathfrak{b}_s$ sind.

2.18. Bemerkung Ist ein \mathcal{O}_Δ Ideal \mathfrak{a} Potenzprodukt paarweiser teilerfremder invertierbarer echter \mathcal{O}_Δ Ideale $\mathfrak{b}_1, \dots, \mathfrak{b}_s$, dann sind die Exponenten in der Potenzproduktdarstellung von \mathfrak{a} notwendigerweise nichtnegativ.

2.19. Korollar Die Ordnung $\mathcal{O}_{\Delta'}$, die von Algorithmus 2.6 bei Eingabe

$$\mathfrak{a}_1, \dots, \mathfrak{a}_k, \mathcal{O}_\Delta$$

zurückgeliefert wird, ist die minimale Oberordnung von \mathcal{O}_Δ , in der die Ideale $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ ggT-frei darstellbar sind.

Beweis: Der Beweis folgt unmittelbar aus Lemma 2.16. ■

2.20. Lemma Sind die \mathcal{O}_Δ Ideale $\mathfrak{b}_1, \dots, \mathfrak{b}_s \neq \mathcal{O}_\Delta$ paarweise teilerfremd, dann gilt für $i \in \{1, \dots, s\}$ und $\alpha_1, \dots, \alpha_s \in \mathbb{N}_0$

$$\mathfrak{b}_i \supseteq \mathfrak{b}_1^{\alpha_1} \cdots \mathfrak{b}_s^{\alpha_s} \text{ genau dann, wenn } \alpha_i > 0.$$

Beweis: Weil $\mathfrak{b}_i \neq \mathcal{O}_\Delta$, gibt es mit Lemma 1.42 ein Primideal \mathfrak{p} , welches \mathfrak{b}_i enthält. Da dann aber auch

$$\mathfrak{p} \supseteq \mathfrak{b}_1^{\alpha_1} \cdots \mathfrak{b}_s^{\alpha_s}$$

gilt, gibt es wegen Lemma 1.20 ein $\mathfrak{b}_j^{\alpha_j}$, welches in \mathfrak{p} enthalten ist und weil $\mathfrak{p} \neq \mathcal{O}_\Delta$, ist dann $\alpha_j > 0$. Dann gilt wieder mit Lemma 1.20 daß $\mathfrak{p} \supseteq \mathfrak{b}_j$. Also gilt $\mathfrak{b}_i + \mathfrak{b}_j \subseteq \mathfrak{p} \subset \mathcal{O}_\Delta$. Wegen der Teilerfremdheit von $\mathfrak{b}_1, \dots, \mathfrak{b}_s$ gilt dann $i = j$, also gilt $\alpha_i > 0$. Die Umkehrung folgt aus der Idealeigenschaft von \mathfrak{b}_i . ■

Wir kommen nun zum zentralen Resultat dieses Abschnitts.

2.21. Satz Sei $\mathcal{O}_{\Delta'}, L = ((\mathbf{n}_1, e_1), \dots, (\mathbf{n}_l, e_l))$ ein Output von Algorithmus 2.6 bei Eingabe $\mathcal{O}_{\Delta}, \mathbf{a}_1, \dots, \mathbf{a}_k$. Die Faktorisierung

$$\mathcal{F}' = (\mathcal{O}_{\Delta'}, \cup_{1 \leq i \leq l} \{\mathbf{n}_i\})$$

ist die eindeutige minimale ggT-freie Verfeinerung von

$$\mathcal{F} = (\mathcal{O}_{\Delta}, \cup_{1 \leq i \leq k} \{\mathbf{a}_i\}).$$

Beweis: Sei \mathcal{S} die Menge der ggT-freien Verfeinerungen von \mathcal{F} . Lemma 2.9 zeigt, daß $\mathcal{F}' \in \mathcal{S}$. Sei $\tilde{\mathcal{F}} = (\mathcal{O}_{\tilde{\Delta}}, C) \in \mathcal{S}$. Es gilt also $\mathcal{O}_{\tilde{\Delta}} \supseteq \mathcal{O}_{\Delta}$,

$$\forall i \in \{1, \dots, k\} \quad \mathbf{a}_i \mathcal{O}_{\tilde{\Delta}} = \prod_{\mathbf{c} \in C} \mathbf{c}^{e(\mathbf{a}_i, \mathbf{c})}, \quad e(\mathbf{a}_i, \mathbf{c}) \in \mathbb{N}_0, \quad (2.9)$$

und Eigenschaft 3 aus Definition 2.2 bedeutet mit Lemma 2.20:

$$\forall \mathbf{c} \in C \quad \exists i \in \{1, \dots, k\} \text{ mit } e(\mathbf{a}_i, \mathbf{c}) > 0.$$

Lemma 2.16 zeigt $\mathcal{O}_{\Delta} \subseteq \mathcal{O}_{\Delta'} \subseteq \mathcal{O}_{\tilde{\Delta}}$ und jedes $\mathbf{n}_i \mathcal{O}_{\tilde{\Delta}}$ ist Potenzprodukt von Idealen aus C mit nichtnegativen Exponenten, d.h.

$$\mathbf{n}_i \mathcal{O}_{\tilde{\Delta}} = \prod_{\mathbf{c} \in C} \mathbf{c}^{e(\mathbf{n}_i, \mathbf{c})}. \quad (2.10)$$

Die Eigenschaften 1 und 2 aus Definition 2.2 gelten also. Mit (2.9) und (2.10) folgt

$$\begin{aligned} \prod_{\mathbf{c} \in C} \mathbf{c}^{e(\mathbf{a}_1, \mathbf{c})} \dots \prod_{\mathbf{c} \in C} \mathbf{c}^{e(\mathbf{a}_k, \mathbf{c})} &= \mathbf{a}_1 \mathcal{O}_{\tilde{\Delta}} \dots \mathbf{a}_k \mathcal{O}_{\tilde{\Delta}} \\ &= \mathbf{a}_1 \mathcal{O}_{\Delta'} \mathcal{O}_{\tilde{\Delta}} \dots \mathbf{a}_k \mathcal{O}_{\Delta'} \mathcal{O}_{\tilde{\Delta}} \\ &= \mathbf{a}_1 \mathcal{O}_{\Delta'} \dots \mathbf{a}_k \mathcal{O}_{\Delta'} \mathcal{O}_{\tilde{\Delta}} \\ &= \mathbf{n}_1^{e_1} \dots \mathbf{n}_l^{e_l} \mathcal{O}_{\tilde{\Delta}} \\ &= (\mathbf{n}_1 \mathcal{O}_{\tilde{\Delta}})^{e_1} \dots (\mathbf{n}_l \mathcal{O}_{\tilde{\Delta}})^{e_l} \\ &= \left(\prod_{\mathbf{c} \in C} \mathbf{c}^{e(\mathbf{n}_1, \mathbf{c})} \right)^{e_1} \dots \left(\prod_{\mathbf{c} \in C} \mathbf{c}^{e(\mathbf{n}_l, \mathbf{c})} \right)^{e_l}. \end{aligned}$$

Weil die Zerlegung eines Produktes in paarweise teilerfremde echte invertierbare Ideale mit Lemma 2.13 eindeutig ist und es für jedes $\mathbf{c} \in C$ ein $\mathbf{a}_i \in \{\mathbf{a}_1, \dots, \mathbf{a}_k\}$ mit $e(\mathbf{a}_i, \mathbf{c}) > 0$ gibt, muß für dieses $\mathbf{c} \in C$ die Summe $\sum_{1 \leq s \leq l} e(\mathbf{n}_s, \mathbf{c}) e_s > 0$ sein. Also muß für ein \mathbf{n}_s der Exponent $e(\mathbf{n}_s, \mathbf{c}) > 0$ sein. Es gilt also auch Punkt 3 aus Definition 2.2. Also folgt $\mathcal{F}' \leq \tilde{\mathcal{F}}$. Weil \leq auf \mathcal{S} eine Ordnungsrelation ist, folgt die Behauptung. ■

Zusammen mit der obigen Diskussion folgt

2.22. Satz Bis auf die Reihenfolge der Paare in der Liste L ist der Output von **refine** eindeutig.

2.23. Bemerkung Die maximale ggT-freie Verfeinerung von (2.5) ist die Maximalordnung $\mathcal{O}_{\Delta_{\max}}$ die \mathcal{O}_{Δ} enthält, zusammen mit den Primidealen die das Ideal $\mathbf{a}_1 \dots \mathbf{a}_k \mathcal{O}_{\Delta_{\max}}$ teilen.

Kapitel 3

Arithmetik auf Idealen

3.1 Addition

3.1. Lemma Die Summe der \mathcal{O}_Δ Ideale $\mathfrak{a}_1 = m_1(a_1\mathbb{Z} + \frac{b_1+\sqrt{\Delta}}{2}\mathbb{Z})$ und $\mathfrak{a}_2 = m_2(a_2\mathbb{Z} + \frac{b_2+\sqrt{\Delta}}{2}\mathbb{Z})$ mit $\text{ggT}(m_1, m_2) = 1$ ist das \mathcal{O}_Δ Ideal

$$\left(\text{ggT}(m_1 a_1, m_2 a_2, m_1 m_2 \frac{b_1 - b_2}{2}) \mathbb{Z} + \frac{x m_1 b_1 + y m_2 b_2 + \sqrt{\Delta}}{2} \mathbb{Z} \right),$$

für $x, y \in \mathbb{Z}$ mit $x m_1 + y m_2 = 1$.

Beweis:

Die unimodulare Matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & m_2 & x \\ 0 & 0 & -m_1 & y \end{pmatrix}$$

transformiert das Erzeugendensystem

$$\left(m_1 a_1, m_2 a_2, \frac{m_1 b_1 + m_1 \sqrt{\Delta}}{2}, \frac{m_2 b_2 + m_2 \sqrt{\Delta}}{2} \right)$$

zu

$$\left(m_1 a_1, m_2 a_2, m_1 m_2 \frac{b_2 - b_1}{2}, \frac{x m_1 b_1 + y m_2 b_2 + \sqrt{\Delta}}{2} \right).$$

Somit ist

$$\begin{aligned} \mathfrak{a}_1 + \mathfrak{a}_2 &= m_1 a_1 \mathbb{Z} + m_2 a_2 \mathbb{Z} + m_1 m_2 \frac{b_2 - b_1}{2} \mathbb{Z} + \frac{x m_1 b_1 + y m_2 b_2 + \sqrt{\Delta}}{2} \mathbb{Z} \\ &= \text{ggT} \left(m_1 a_1, m_2 a_2, m_1 m_2 \frac{b_2 - b_1}{2} \right) \mathbb{Z} + \frac{x m_1 b_1 + y m_2 b_2 + \sqrt{\Delta}}{2} \mathbb{Z}. \end{aligned}$$

■

3.2. Korollar Sind $\mathfrak{a}_1 = m_1(a_1\mathbb{Z} + \frac{b_1 + \sqrt{\Delta}}{2}\mathbb{Z})$ und $\mathfrak{a}_2 = m_2(a_2\mathbb{Z} + \frac{b_2 + \sqrt{\Delta}}{2}\mathbb{Z})$ \mathcal{O}_Δ Ideale und ist $d = \text{ggT}(m_1, m_2)$ und $m'_1 = m_1/d$, und $m'_2 = m_2/d$ und $x, y \in \mathbb{Z}$ mit $xm'_1 + ym'_2 = 1$, dann ist

$$\mathfrak{a}_1 + \mathfrak{a}_2 = d \left(\text{ggT}(m'_1 a_1, m'_2 a_2, m'_1 m'_2 \frac{b_1 - b_2}{2}) \mathbb{Z} + \frac{xm'_1 b_1 + ym'_2 b_2 + \sqrt{\Delta}}{2} \mathbb{Z} \right).$$

Beweis: $\mathfrak{a}_1 + \mathfrak{a}_2 = d(m'_1(a_1\mathbb{Z} + \frac{b_1 + \sqrt{\Delta}}{2}\mathbb{Z}) + m'_2(a_2\mathbb{Z} + \frac{b_2 + \sqrt{\Delta}}{2}\mathbb{Z}))$. Die Behauptung folgt dann aus Lemma 3.1. ■

3.3. Satz Kennt man Zahlen $m_1, m_2, a_1, a_2, b_1, b_2$ mit

$$\mathfrak{a}_1 = m_1(a_1\mathbb{Z} + \frac{b_1 + \sqrt{\Delta}}{2}\mathbb{Z})$$

und

$$\mathfrak{a}_2 = m_2(a_2\mathbb{Z} + \frac{b_2 + \sqrt{\Delta}}{2}\mathbb{Z})$$

dann kann man die Standarddarstellung von $\mathfrak{a}_1 + \mathfrak{a}_2$ in Zeit $O(\text{size}(k_1) \text{size}(k_2))$ berechnen, wobei

$$\begin{aligned} k_1 &= \max\{|m_1|, |a_1|, |b_1|\} \\ k_2 &= \max\{|m_2|, |a_2|, |b_2|\}. \end{aligned}$$

3.4. Bemerkung Wir gehen also nicht unbedingt davon aus, daß wir $b(\mathfrak{a}_1)$ und $b(\mathfrak{a}_2)$ kennen.

Beweis: Es soll ohne Einschränkung $k_1 \geq k_2$ gelten.

Um $d = \text{ggT}(m_1, m_2)$, m_1/d und m_2/d zu berechnen, braucht man Zeit

$$O(\text{size}(k_1) \text{size}(k_2)).$$

Das heißt wir können uns auf den Fall $\text{ggT}(m_1, m_2) = 1$ aus Lemma 3.1 beschränken.

Um nun die Summe von \mathfrak{a}_1 und \mathfrak{a}_2 berechnen zu können müssen wir erst $x, y \in \mathbb{Z}$ mit $xm_1 + ym_2 = 1$ finden. Dies geht mit Algorithmus **euklid** in Zeit $O(\text{size}(k_1) \text{size}(k_2))$. Es gilt $|x| \leq |m_2|$ und $|y| \leq |m_1|$.

Nun berechnen wir $\text{ggT}(m_1 a_1, m_2 a_2, m_1 m_2 \frac{b_1 - b_2}{2})$, indem wir erst $d_1 = \text{ggT}(m_1 a_1, m_2 a_2)$ herausfinden. Beachte $\text{ggT}(a, b) = \text{ggT}(a \bmod b, b)$. Deshalb berechnet man erst die Zahl $m_2 a_2$. Das Ergebnis dieser Multiplikation hat höchstens doppelte Länge von k_2 . Dann berechnet man die Zahlen $m_1 \bmod (m_2 a_2)$ und $a_1 \bmod (m_2 a_2)$ und anschließend ihr Produkt in Zeit $O(\text{size}(k_1) \text{size}(k_2))$. Nun muß man den ggT zweier Zahlen berechnen, die kürzer als $4 \text{size}(k_2)$ sind, und das geht in Zeit $O(\text{size}(k_2)^2)$. Jetzt muß man noch $\text{ggT}(d_1, m_1 m_2 \frac{b_1 - b_2}{2})$ bestimmen. Zuerst berechnen wir $\frac{b_1 - b_2}{2}$ in Zeit $O(\text{size}(k_1))$. Dann reduziert man die Zahlen $\frac{b_1 - b_2}{2}, m_1$ modulo d_1 und berechnet das Produkt $(m_1 \bmod d_1) m_2 (\frac{b_1 - b_2}{2} \bmod d_1)$ in Zeit $O(\text{size}(k_1) \text{size}(k_2))$. Da das Produkt dann höchstens

sechsfache Länge von k_2 hat, können wir anschließend $d = \text{ggT}(d_1, m_1 m_2 \frac{b_1 - b_2}{2})$ in Zeit $O(\text{size}(k_2)^2)$ bestimmen.

Um $b(\mathfrak{a}_1 + \mathfrak{a}_2)$ zu bestimmen, reduzieren wir erst alle Zahlen aus $xm_1b_1 + ym_2b_2$ modulo $2d$ und berechnen erst dann das Ergebnis, um es schließlich wieder modulo $2d$ zu reduzieren. Dies geht auch wie man leicht sieht, in Zeit $O(\text{size}(k_1), \text{size}(k_2))$.

Insgesamt ergibt sich die gewünschte Laufzeit. ■

3.5. Korollar Sind die Ideale \mathfrak{a}_1 und \mathfrak{a}_2 in Standarddarstellung gegeben, dann kann $\mathfrak{a}_1 + \mathfrak{a}_2$ in Zeit $O(\text{size}(\mathfrak{a}_1) \text{size}(\mathfrak{a}_2))$ berechnet werden.

3.2 Liften

Wir haben ein \mathcal{O}_Δ Ideal $\mathfrak{a} = m(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z})$ in Standarddarstellung, kennen eine Oberordnung $\mathcal{O}_{\tilde{\Delta}} \supseteq \mathcal{O}_\Delta$, wobei $\Delta = d^2\tilde{\Delta}$ mit $d \in \mathbb{N}$ und sind an der Standarddarstellung des $\mathcal{O}_{\tilde{\Delta}}$ Ideals $\mathfrak{a}\mathcal{O}_{\tilde{\Delta}}$ interessiert. Das Berechnen von $\mathfrak{a}\mathcal{O}_{\tilde{\Delta}}$ nennt man Liften.

Dazu berechnen wir getrennt die von a und $\frac{b+\sqrt{\Delta}}{2}$ erzeugten $\mathcal{O}_{\tilde{\Delta}}$ Hauptideale. $\mathfrak{a}\mathcal{O}_{\tilde{\Delta}}$ ist ganz einfach

$$a \left(\mathbb{Z} + \frac{(\tilde{\Delta} \bmod 2) + \sqrt{\tilde{\Delta}}}{2} \mathbb{Z} \right).$$

Ein Erzeugendensystem des von $\frac{b+\sqrt{\Delta}}{2} = \frac{b+d\sqrt{\tilde{\Delta}}}{2}$ erzeugten $\mathcal{O}_{\tilde{\Delta}}$ -Hauptideals ist

$$\left(\frac{b+d\sqrt{\tilde{\Delta}}}{2}, \frac{b+d\sqrt{\tilde{\Delta}}}{2} \frac{\tilde{\Delta} + \sqrt{\tilde{\Delta}}}{2} \right) = \left(\frac{b+d\sqrt{\tilde{\Delta}}}{2}, \frac{(b+d)\tilde{\Delta}}{2} + \frac{b+d\tilde{\Delta}}{2} \sqrt{\tilde{\Delta}} \right). \quad (3.1)$$

Mit **euklid** berechnen wir nun $x, y \in \mathbb{Z}$, mit

$$xd + y \frac{b+d\tilde{\Delta}}{2} = \text{ggT}(d, \frac{b+d\tilde{\Delta}}{2}) = g. \quad (3.2)$$

Transformiert man die Basis aus (3.1) mit der unimodularen Matrix

$$U = \begin{pmatrix} \frac{b+d\tilde{\Delta}}{2g} & x \\ -\frac{d}{g} & y \end{pmatrix},$$

dann verschwindet im ersten Basiselement der durch $\sqrt{\tilde{\Delta}}$ zustandekommende irrationale Anteil und das zweite Basiselement wird

$$\frac{bx + \frac{(b+d)\tilde{\Delta}}{2}y + g\sqrt{\tilde{\Delta}}}{2}.$$

Es handelt sich bei diesem Modul um ein $\mathcal{O}_{\tilde{\Delta}}$ Ideal. Wir wissen wegen Lemma 1.45, daß $N(\frac{b+\sqrt{\tilde{\Delta}}}{2}\mathcal{O}_{\tilde{\Delta}}) = ac$. Es folgt aus dem Beweis von Satz 1.77 $g | (\frac{bx+(b+d)\tilde{\Delta}}{2}y)$ und $g^2 | ac$. Somit ist die Standarddarstellung von $\frac{b+\sqrt{\tilde{\Delta}}}{2}\mathcal{O}_{\tilde{\Delta}}$

$$g \left(\frac{ac}{g^2} \mathbb{Z} + \frac{((bx + \frac{(b+d)\tilde{\Delta}}{2}y)/g) \bmod (2\frac{ac}{g^2}) + \sqrt{\tilde{\Delta}}}{2} \mathbb{Z} \right).$$

3.6. Lemma Liegt das \mathcal{O}_{Δ} Ideal $\mathfrak{a} = m(a\mathbb{Z} + \frac{b+\sqrt{\tilde{\Delta}}}{2}\mathbb{Z})$ in Standarddarstellung vor, ist $\mathcal{O}_{\tilde{\Delta}} \supseteq \mathcal{O}_{\Delta}$ eine Oberordnung von \mathcal{O}_{Δ} , und kennt man die Zahl $d \in \mathbb{N}$ mit $d^2\tilde{\Delta} = \Delta$, dann kann man die Standarddarstellung von $\mathfrak{a}\mathcal{O}_{\tilde{\Delta}}$ in Zeit $O(\text{size}(d) \text{size}(\Delta) + \text{size}(\mathfrak{a}) \text{size}(\Delta) + \text{size}(\mathfrak{a})^2)$ berechnen.

Beweis: Die Standarddarstellung von $\mathfrak{a}\mathcal{O}_{\tilde{\Delta}}$ kann man in Zeit $O(\text{size}(\mathfrak{a}))$ ausrechnen.

Wir berechnen nun Die Zahlen $g, x, y, ac/g^2$ und $(bx + \frac{(b+d)\tilde{\Delta}}{2}y)/g$ aus der obigen Diskussion. Wir unterscheiden folgende Fälle:

1. Fall: $\text{size}(\mathfrak{a}) \geq \text{size}(\Delta)$.

Um die oben genannten Zahlen zu berechnen muß man eine feste Anzahl von elementaren Operationen (+, -, ·, /, **euklid**) auf Zahlen durchführen deren Länge durch $\text{size}(\mathfrak{a})$ beschränkt ist. In diesem Fall ist die Laufzeit zur Berechnung der Zahlen $g, x, y, ac/g^2$ und $(bx + \frac{(b+d)\tilde{\Delta}}{2}y)/g$ also durch $O(\text{size}(\mathfrak{a})^2)$ beschränkt.

2. Fall: $\text{size}(\mathfrak{a}) < \text{size}(\Delta)$. Dann kann man $\frac{b+d\tilde{\Delta}}{2}$ in Zeit $O(\text{size}(\Delta) \text{size}(d))$ berechnen. **euklid** braucht dann bei Eingabe d und $\frac{b+d\tilde{\Delta}}{2}$ Zeit $O(\text{size}(\Delta) \text{size}(d))$. x hat dann höchstens so viele Bits wie $\frac{b+d\tilde{\Delta}}{2}$, also bis auf eine multiplikative Konstante so viele Bits wie Δ , und y hat höchstens so viele Bits wie d . Weil g ein Teiler von d ist hat auch g höchstens so viele Bits wie d . Somit kostet das Berechnen von

$$\left(bx + \frac{(b+d)\tilde{\Delta}}{2}y \right) / d$$

$O(\text{size}(\mathfrak{a}) \text{size}(\Delta) + \text{size}(d) \text{size}(\Delta))$ viele Bitoperationen. Um ac/g^2 zu berechnen, muß man erst $c = \frac{b^2-\Delta}{4a}$ bestimmen. Das kostet $O(\text{size}(\Delta) \text{size}(\mathfrak{a}) + \text{size}(\mathfrak{a})^2)$ viele Bitoperationen. Die Zahl ac/g^2 kann man dann in Zeit $O(\text{size}(\mathfrak{a}) \text{size}(\Delta) + \text{size}(d) \text{size}(\Delta))$ berechnen.

Es ist wichtig jetzt anzumerken, daß es eine Konstante k gibt, so, daß alle berechneten Zahlen weniger als $k(\text{size}(\Delta) + \text{size}(\mathfrak{a}))$ viele Bits haben. Deshalb kostet das Berechnen von $\mathfrak{a}\mathcal{O}_{\tilde{\Delta}} + \frac{b+\sqrt{\tilde{\Delta}}}{2}\mathcal{O}_{\tilde{\Delta}}$ nun mit Satz 3.3 $O(\text{size}(\mathfrak{a}) \text{size}(\Delta) + \text{size}(\mathfrak{a})^2)$. ■

3.3 Multiplikation

Hier wird gezeigt, daß man zwei invertierbare \mathcal{O}_Δ Ideale \mathfrak{a} und \mathfrak{b} mit $\text{size}(\mathfrak{a}) \geq \text{size}(\mathfrak{b})$ in Zeit $O(\text{size}(\mathfrak{a})^2 + \text{size}(\Delta)^2)$ multiplizieren kann.

Sind

$$\begin{aligned}\mathfrak{a} &= m_1 \left(a_1 \mathbb{Z} + \frac{b_1 + \sqrt{\Delta}}{2} \mathbb{Z} \right), \\ \mathfrak{b} &= m_2 \left(a_2 \mathbb{Z} + \frac{b_2 + \sqrt{\Delta}}{2} \mathbb{Z} \right)\end{aligned}$$

in Standarddarstellung, $g = \text{ggT}(a_1, a_2, \frac{b_1+b_2}{2})$ und $u, v, w \in \mathbb{Z}$, mit

$$ua_1 + va_2 + w \frac{b_1 + b_2}{2} = g$$

dann ist

$$\mathfrak{a}\mathfrak{b} = m_1 m_2 g \left(\frac{a_1 a_2}{g^2} \mathbb{Z} + \frac{b' + \sqrt{\Delta}}{2} \mathbb{Z} \right),$$

mit $b' = \frac{ua_1 b_2 + va_2 b_1 + w(b_1 b_2 + \Delta)/2}{g} \pmod{(2a_1 a_2 / g^2)}$, siehe [BW96].

Man benutzt also **euklid**, um erst $x, y \in \mathbb{Z}$ mit

$$d = \text{ggT}(a_1, a_2) = xa_1 + ya_2$$

und dann $x', y' \in \mathbb{Z}$ mit

$$g = \text{ggT}(d, \frac{b_1 + b_2}{2}) = x'd + y' \frac{b_1 + b_2}{2}$$

zu berechnen. Die Zahl $\frac{b_1+b_2}{2}$ kann man in Zeit $O(\text{size}(\mathfrak{a}))$ berechnen. x, y, x', y', d und g findet man nach Satz 1.7 in Zeit $O(\text{size}(\mathfrak{a})^2)$. Dann gilt

$$g = x'(xa_1 + ya_2) + y' \frac{b_1 + b_2}{2} = x'xa_1 + x'ya_2 + y' \frac{b_1 + b_2}{2}.$$

Also sind die gesuchten Zahlen u, v und w die Zahlen $x', x'y, y'$. Wegen Lemma 1.5 sind x', x, y' und y Zahlen, die höchstens $\text{size}(\mathfrak{a})$ viele Bits haben. Die Terme

$$\frac{x'xa_1 b_2 + x'ya_2 b_1 + y'(b_1 b_2 + \Delta)/2}{g} \pmod{(a_1 a_2 / g^2)}, \quad m_1 m_2 g, \quad \frac{a_1 a_2}{g^2}$$

haben eine feste Anzahl von elementaren Operationen (+, −, ·, /). Die dort vorkommenden Zahlen haben alle kürzere Länge als $\text{size}(\mathfrak{a}) + \text{size}(\Delta)$. Mit der konstanten Anzahl der Operationszeichen k hat man also mit Bemerkung 1.3 eine Laufzeit für die Auswertung der Terme von $O((\text{size}(\mathfrak{a}) + \text{size}(\Delta))^2)$. Es folgt:

3.7. Lemma Für zwei invertierbare \mathcal{O}_Δ Ideale \mathfrak{a} und \mathfrak{b} mit $N(\mathfrak{a}) \geq N(\mathfrak{b})$, die in Standarddarstellung gegeben sind, kann man in Zeit $O(\text{size}(\Delta)^2 + \text{size}(\mathfrak{a})^2)$ die Standarddarstellung von $\mathfrak{a}\mathfrak{b}$ berechnen.

3.8. Lemma Sind $\mathfrak{a}_1 \supseteq \mathfrak{a}_2$ invertierbare \mathcal{O}_Δ Ideale, dann kann man das \mathcal{O}_Δ Ideal $\mathfrak{a}_2\mathfrak{a}_1^{-1}$ in Zeit $O(\text{size}(\mathfrak{a}_2)^2 + \text{size}(\Delta)^2)$ berechnen.

3.9. Bemerkung Beachte daß $N(\mathfrak{a}_1) \leq N(\mathfrak{a}_2)$ und somit wegen Lemma 1.80 $\text{size}(\mathfrak{a}_1) \leq k \text{size}(\mathfrak{a}_2)$ mit einer Konstanten k .

Beweis: $\mathfrak{a}_2\mathfrak{a}_1^{-1} = \mathfrak{a}_2\sigma(\mathfrak{a}_1)\frac{1}{N(\mathfrak{a}_1)}$. Die Standarddarstellung von $\sigma(\mathfrak{a}_1)$ kann man in Zeit $O(\text{size}(\mathfrak{a}_1))$ berechnen. Man muß lediglich die Zahl $-b(\mathfrak{a}_1) + 2a(\mathfrak{a}_1)$ berechnen und das nur, falls $b(\mathfrak{a}_1) \neq 0$. Die Zahl $N(\mathfrak{a}_1)$ kann man in Zeit $O(\text{size}(\mathfrak{a}_1)^2)$ berechnen. Anschließendes Berechnen von $\mathfrak{a}_2\sigma(\mathfrak{a}_1)$ geht in Zeit $O(\text{size}(\mathfrak{a}_2)^2 + \text{size}(\Delta)^2)$. Die Zahl $\text{size}(m(\mathfrak{a}_2\sigma(\mathfrak{a}_1)))$ ist höchstens doppelt so groß wie die Zahl $\text{size}(\mathfrak{a}_2)$, und deshalb kann man die Zahl $m(\mathfrak{a}_2\mathfrak{a}_1^{-1}) = m(\mathfrak{a}_2\sigma(\mathfrak{a}_1))/N(\mathfrak{a}_1)$ in Zeit $O(\text{size}(\mathfrak{a}_2)^2)$ bestimmen. ■

3.10. Bemerkung Es ist mir nicht gelungen die Multiplikation so billig zu machen wie die ggT-Berechnung. Ist $N(\mathfrak{a}_1) \geq N(\mathfrak{a}_2)$, dann wissen wir über das von **euklid** berechnete y nur, daß $|y| \leq a_1$. Außerdem wissen wir über x' nur, daß $|x'| \leq b_1$. Wir müssen aber $x'y$ berechnen. Mit diesen Abschätzungen bekommen wir dafür aber Laufzeit $O(\text{size}(N(\mathfrak{a}_1))^2)$. Das ist mit ein Grund dafür, daß eventuelle quadratische Laufzeit von Algorithmus 2.6 nicht offensichtlich ist.

Kapitel 4

Analyse des Algorithmus refine

In diesem Kapitel zeige ich, daß die Bitkomplexität von Algorithmus 2.6 kubisch in der Länge der Eingabe ist. Die Laufzeiten für die Arithmetik aus Kapitel 3 sind in Abhängigkeit des Speicherbedarfs der Ideale und des Speicherbedarfs der Diskriminante angegeben. Wegen Lemma 1.80 gilt für ein echtes \mathcal{O}_Δ Ideal $\mathfrak{a} \neq \{0\}$ mit einer Konstanten c_1 , $\text{size}(\mathfrak{a}) \leq c_1 \log(N(\mathfrak{a}))$. Weil eine quadratische Diskriminante Δ kein perfektes Quadrat und kongruent 0 oder 1 modulo 4 ist, ist $|\Delta| > 1$ und somit der Speicherbedarf für Δ mit $c_2 \log(|\Delta|)$ beschränkt, wobei c_2 eine positive Konstante ist.

Ist $\mathfrak{a}_1, \dots, \mathfrak{a}_k, \mathcal{O}_\Delta$ eine korrekte Eingabe von Algorithmus 2.6, dann ist die Gesamtlänge der Eingabe

$$c_1(\log(N(\mathfrak{a}_1)) + \dots + \log(N(\mathfrak{a}_k))) + c_2 \log(|\Delta|) \leq (c_1 + c_2) \log(N(\mathfrak{a}_1) \cdots N(\mathfrak{a}_k) |\Delta|).$$

Sei N die Zahl $N(\mathfrak{a}_1) \cdots N(\mathfrak{a}_k)$.

Initialisierung

In Zeile (1) kostet für ein \mathfrak{a}_i , das Berechnen von d_i Zeit $O(\text{size}(\Delta)^2 + \text{size}(\mathfrak{a}_i)^2)$, da dazu eine feste Anzahl an elementare Operationen auf Zahlen ausgeführt werden, die höchstens $\text{size}(\mathfrak{a}_i) + \text{size}(\Delta)$ viele Bits haben. Für Zeile (1) ergibt sich bis auf eine multiplikative Konstante also die Laufzeit

$$k \log(|\Delta|)^2 + \log(N(\mathfrak{a}_1))^2 + \dots + \log(N(\mathfrak{a}_k))^2.$$

Weil $k \leq \log(N)$ gilt, kann man diese Laufzeit mit

$$\log(N) \log(|\Delta|)^2 + \log(N)^2$$

nach oben abschätzen.

Beachte, daß

$$\text{kgV}(d_1, \dots, d_k) = \frac{d_1 \cdots d_k}{\text{ggT}(d_1, \dots, d_k)}.$$

Das Produkt $d_1 \cdots d_k$ kann man bis auf eine Multiplikative Konstante in Zeit $\log(N) \log(d_1) + \cdots + \log(N) \log(d_k) \leq \log(N)^2$ berechnen. Diese Abschätzung folgt aus der Tatsache, daß $d_1 \cdots d_k$ höchstens so viele Bits wie die Zahl N hat. Eine analoge Betrachtung zeigt, daß man den ggT von d_1, \dots, d_k ebenfalls mit $O(\log(N)^2)$ Bitoperationen berechnen kann. Also kann man die Zahl

$$\text{kgV}(d_1, \dots, d_k) = \frac{d_1 \cdots d_k}{\text{ggT}(d_1, \dots, d_k)}$$

in Zeit $O(\log(N)^2)$ berechnen. Die Zahl $\Delta / \text{kgV}(d_1, \dots, d_k)^2$ berechnet man dann in Zeit $O(\text{size}(\Delta)^2)$.

Die Kosten, die beim Liften des Ideals $\mathfrak{a}_i \mathcal{O}_{\Delta'}$ entstehen, sind bis auf eine multiplikative Konstante

$$\log(d) \log(|\Delta|) + \log(N(\mathfrak{a}_i)) \log(|\Delta|) + \log(N(\mathfrak{a}_i))^2.$$

Also braucht man zum Liften der Ideale $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ weniger Zeit als

$$O(\log(N) \log(d) \log(|\Delta|) + \log(N) \log(|\Delta|) + \log(N)^2).$$

Man sieht also, daß die Initialisierung kubisch in der Länge der Eingabe ist.

Liften

Wir schätzen nun die Anzahl der Bitoperationen ab, die insgesamt für Lifts durchgeführt werden müssen. Ist d_t die t -te Zahl > 1 aus Zeile (6) und $L = ((\mathfrak{n}_1, e_1), \dots, (\mathfrak{n}_l, e_l))$ die Liste L zu diesem Zeitpunkt, dann kostet das Liften von \mathfrak{n}_i

$$c(\log(d_t) \log(|\Delta|) + \log(N(\mathfrak{n}_i)) \log(|\Delta|) + \log(N(\mathfrak{n}_i))^2)$$

wobei c eine multiplikative Konstante ist. Rechnet man dann die Gesamtkosten für alle Ideale aus L zusammen, ergibt sich

$$c \left(l \log(d_t) \log(|\Delta|) + \log(|\Delta|) \sum_{1 \leq \mu \leq l} \log(N(\mathfrak{n}_\mu)) + \sum_{1 \leq \mu \leq l} \log(N(\mathfrak{n}_\mu))^2 \right).$$

Weil $l \leq \log(N)$ und $N(\mathfrak{n}_1) \cdots N(\mathfrak{n}_l) \leq N$ ist, kann man dies mit

$$c(\log(N) \log(d_t) \log(|\Delta|) + \log(N) \log(|\Delta|) + \log(N)^2)$$

nach oben abschätzen. Findet man insgesamt s Zahlen d_1, \dots, d_s zum Liften, dann hat man bis auf eine multiplikative Konstante weniger Kosten als

$$\begin{aligned} \log(N) \log(|\Delta|) \sum_{1 \leq \mu \leq s} \log(d_\mu) + s \log(N) \log(|\Delta|) + s \log(N)^2 \\ \leq 2 \log(N) \log(|\Delta|)^2 + \log(|\Delta|) \log(N)^2. \end{aligned}$$

Also sind die Kosten aller Lifts zusammengenommen kubisch in der Länge der Eingabe.

Auffinden von nichtteilerfremden Idealen

Ist $L = ((\mathbf{n}_1, e_1), \dots, (\mathbf{n}_l, e_l))$ die Liste zu einem gewissen Zeitpunkt, dann können wir bis auf eine multiplikative Konstante in Zeit

$$\begin{aligned}
 \sum_{1 \leq i \leq l} \sum_{1 \leq j \leq l} \log(N(\mathbf{n}_i)) \log(N(\mathbf{n}_j)) &\leq \log(N(\mathbf{n}_1)) \sum_{1 \leq j \leq l} \log(N(\mathbf{n}_j)) + \dots \\
 &\quad + \log(N(\mathbf{n}_l)) \sum_{1 \leq j \leq l} \log(N(\mathbf{n}_j)) \\
 &= \log(N(\mathbf{n}_1)) \log(N(\mathbf{n}_1) \cdots N(\mathbf{n}_l)) + \dots \\
 &\quad + \log(N(\mathbf{n}_l)) \log(N(\mathbf{n}_1) \cdots N(\mathbf{n}_l)) \\
 &\leq \log(N(\mathbf{n}_1)) \log(N) + \dots + \log(N(\mathbf{n}_l)) \log(N) \\
 &\leq \log(N)^2
 \end{aligned}$$

die ganze Liste auf nichtteilerfremde Paare durchsuchen.

Berechnen von d in Zeile (6)

Dies geht, wie man leicht sieht, in Zeit $O(\text{size}(\mathbf{n}_i)^2 + \text{size}(\mathbf{n}_j)^2 + \text{size}(\Delta)^2)$. Die anschließende Berechnung von Δ/d^2 ist in Zeit $O(\text{size}(\Delta)^2)$ durchführbar.

Verfeinerungsschritte

Sind \mathbf{n}_i und \mathbf{n}_j die beiden Ideale, mit denen ein Verfeinerungsschritt durchgeführt wird, dann braucht man dafür Zeit $O(\text{size}(\mathbf{n}_i)^2 + \text{size}(\mathbf{n}_j)^2 + \text{size}(\Delta)^2)$.

Weil die Anzahl der **while** Durchläufe wegen Lemma 2.10 linear ist, hat man damit den Folgenden Satz:

4.1. Satz Die Laufzeit von `refine` bei korrekter Eingabe $\mathbf{a}_1, \dots, \mathbf{a}_k, \mathcal{O}_\Delta$ ist

$$O((\text{size}(\mathbf{a}_1) + \dots + \text{size}(\mathbf{a}_k) + \text{size}(\Delta))^3).$$

Ausblick

Man kann weiter untersuchen, ob sich die in Kapitel 2 gefundenen Ergebnisse auf den refinement Algorithmus in [Ge93] übertragen lassen. Untersuchenswert scheint mir auch die Frage, ob die Aufteilung eines zu bearbeitenden quadratischen Ideals $m(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z})$ in das \mathbb{Z} Hauptideal $m\mathcal{O}_\Delta$ und das primitive Ideal $a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$ einen schnelleren refinement Algorithmus ermöglicht.

Bezeichnungen

\log	Logarithmus zur Basis 2.
\mathbb{N}	Menge der natürlichen Zahlen ohne 0.
\mathbb{N}_0	Menge der natürlichen Zahlen mit 0.
\mathbb{Z}	Menge der ganzzahligen Zahlen $\{\dots, -1, 0, 1, \dots\}$.
\mathbb{Q}	Menge der rationalen Zahlen.
$\sqrt{\Delta}$	Wurzel von $X^2 - \Delta$ mit echt positivem Realteil oder aus $\mathbb{R}_{\geq 0}$.
f_θ	Polynom aus $\mathbb{Z}[X] \setminus \{0\}$ mit $f_\theta(\theta) = 0$, minimalem Grad, positivem Leitkoeffizienten und Inhalt 1.
p_θ	Minimalpolynom von θ aus $\mathbb{Q}[X]$.
$\mathbb{Q}(\theta)$	Von θ erzeugter algebraischer Zahlkörper.
\mathcal{O}	Ordnung eines algebraischen Zahlkörpers.
\mathcal{O}_Δ	Ordnung eines quadratischen Zahlkörpers mit Diskriminante Δ .
$\mathcal{O}_{\Delta_{\max}}$	Maximalordnung eines quadratischen Zahlkörpers.
M	Modul eines algebraischen Zahlkörpers.
\mathcal{O}_M	Multiplikatorenring des Moduls M .
σ	Die nichttriviale Einbettung eines quadratischen Zahlkörpers nach \mathbb{C} .
$\text{GL}(n, \mathbb{Z})$	Menge der invertierbaren Matrizen aus $\mathbb{Z}^{n \times n}$.
$M \subseteq N$	M ist in N enthalten.
$M \subset N$	M ist in N echt enthalten.

Literaturverzeichnis

- [BDS93] Eric Bach, James Discroll, and Jeffrey Shallit. Factor refinement. *Journal of Algorithms*, 15:199–222, 1993.
- [BS66] Z.I. Borevich and I.R. Shafarevich. *Number Theory*. Academic Press, 1966.
- [Buc96] Johannes Buchmann. Skriptum zur Vorlesung Algebra für Informatiker, WS 1995/96.
- [BW96] Johannes Buchmann and Hugh Williams. Algorithms for quadratic fields, 1996. Manuskript.
- [Ge93] Guoqiang Ge. *Algorithms Related to Multiplicative Representations of Algebraic Numbers*. PhD thesis, U.C. Berkeley, 1993.
- [Kun94] Ernst Kunz. *Algebra*. Vieweg, 1994.
- [Len92] H.W. Lenstra. Algorithms in algebraic number theory. *Bulletin of the American Mathematical Society*, 26:211–244, 1992.
- [LMW86] Jaques Loeckx, Kurt Mehlhorn, and Reinhard Wilhelm. *Grundlagen der Programmiersprachen*. B.G. Teubner Stuttgart, 1986.
- [ST87] I.N. Stewart and D.O. Tall. *Algebraic Number Theory*. Chapman and Hall, 1987.

Stichwortverzeichnis

- abelsche Gruppe, 10
- abelsche Gruppe
 - Basis, 10
 - endlich erzeugte, 10
 - Erzeuger, 10
 - frei, 10
 - Hauptsatz , 11
- Arithmetik
 - auf ganzen Zahlen, 7
 - auf Idealen, 38
- Basis, 10
- Diskriminante, 18
 - Modul, 18
 - quadratische, 20
- euklid, 8
- euklidischer Algorithmus, 8
- Faktorisierung, 27
 - ggT-frei, 27
- ggT-frei darstellbar, 36
- Ideal, 12
 - echt, 12
 - invertierbar, 23
 - maximal, 12
 - prim, 13
 - Produkt, 12
 - Standarddarstellung, 25
 - Summe, 12
 - teilerfremd, 24
- Länge einer Zahl, 7
- Liften, 13, 40
- log, 48
- Maximalordnung, 18
- mod, 7
- Modul, 14
 - Addition, 17
 - gehört zu , 22
 - Multiplikation, 17
 - quadratischer, 20
 - vollständig, 14
- Multiplikator, 15
- Multiplikatorenring, 15
- Norm
 - einer Zahl, 14
 - eines Moduls, 16
- Ordnung, 16
 - quadratische, 20
- quadratischer Zahlkörper, 19
- refine, 29
- size
 - Ordnung, 26
 - ganze Zahl, 7
 - Ideal, 26
- Verfeinerung, 27
- Zahl
 - algebraisch, 13
 - ganzalgebraisch, 13