Protokoll zur Vorlesung Algorithmische Zahlentheorie WS 22/23

W. Bley

14. Februar 2023

1 Lineare Algebra über $\mathbb{Z}$

1.1 Der Hauptsatz für endlich erzeugte $\mathbb{Z}$-Moduln

Für einen $\mathbb{Z}$-Modul V sei $V_{tors} := \{v \in V \mid \exists 0 \neq n \in \mathbb{Z} \text{ mit } nv = 0\}$ der Torsionsuntermodul.

Satz 1.1.1 *Sei V ein endlich erzeugter $\mathbb{Z}$-Modul.*
(1) $V \simeq V_{tors} \oplus \mathbb{Z}^r$ und $|V_{tors}| < \infty$. Hierbei ist $r \in \mathbb{Z}_{\geq 0}$ und heißt Rang von V. Wir schreiben $r = \mathrm{rg}(V)$.
(2) Sei $W \subseteq V$ ein Teilmodul. Dann ist W endlich erzeugt und es gilt $\mathrm{rg}(W) \leq \mathrm{rg}(V)$.
(3) Falls V frei ist und $W \subseteq V$ ein Teilmodul, so ist auch W frei.
(4) Falls V ein endlicher $\mathbb{Z}$-Modul ist, so gibt es eine natürliche Zahl n und einen (freien) $\mathbb{Z}$-Teilmodul $L \subseteq \mathbb{Z}^n$, so dass $V \simeq \mathbb{Z}^n/L$ gilt.

Im Weiteren bezeichnen wir einen freien $\mathbb{Z}$-Modul auch als $\mathbb{Z}$-Gitter. Durch die Wahl einer $\mathbb{Z}$-Basis für ein $\mathbb{Z}$-Gitter V erhalten wir einen nicht-kanonischen Isomorphismus $V \simeq \mathbb{Z}^m$ mit $m = \mathrm{rg}(V)$. Teilmoduln $W \subseteq V$ beschreiben wir dann durch Matrizen $M \in \mathbb{Z}^{m \times n}$, wobei die Spalten von M den Erzeugenden von W entsprechen.

1.2 Hermitesche Normalform

Definition 1.2.1 Eine Matrix $M = (m_{ij}) \in \mathbb{Z}^{m \times n}$ ist in Hermitescher Normalform (kurz HNF), falls es eine streng monoton wachsende Funktion $f\colon \{r+1, \ldots, n\} \longrightarrow \{1, \ldots, m\}$, $0 \leq r \leq n$ geeignet, gibt, die folgende Bedingungen erfüllt.
(1) Für $r+1 \leq j \leq n$ ist $m_{f(j),j} \geq 1$, $m_{ij} = 0$ für $i > f(j)$ und $0 \leq m_{f(j),k} < m_{f(j),j}$ für $k > j$.
(2) Die ersten r Spalten von M sind Nullspalten.

Satz 1.2.2 *Sei $A \in \mathbb{Z}^{m \times n}$. Dann gibt es eine eindeutig bestimmte Matrix $B = (0 \mid H)$ in HNF und eine Matrix $U \in \mathrm{Gl}_n(\mathbb{Z})$ mit $B = AU$.*

Mit einem Algorithmus, der als Verallgemeinerung des Gaußschen Algorithmus angesehen werden kann, lässt sich zu einer gegebenen Matrix A die HNF $B = (0 \mid H)$ sowie die Matrix U berechnen.

1.3 Anwendungen der HNF

1.3.1 Bild einer ganzzahligen Matrix

Wir identifizieren $A \in \mathbb{Z}^{m \times n}$ mit der $\mathbb{Z}$-linearen Abbildung $A\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$. Sei $B = (0 \mid H)$ die HNF zu A. Dann bilden die Spalten von H eine $\mathbb{Z}$-Basis des Bildes von A.

1.3.2 Kern einer ganzzahligen Matrix

Sei $B = AU$ die HNF von A. Sei r wie in der Definition der HNF. Dann ist eine $\mathbb{Z}$-Basis des Kerns von A durch die ersten r Spalten von U gegeben.

1.4 Smithsche Normalform

Sei G eine endliche abelsche Gruppe. Sei $g_1, \ldots, g_n$ ein Erzeugendensystem von G. Dann induziert der Epimorphismus $\pi\colon \mathbb{Z}^n \longrightarrow G, (x_1, \ldots, x_n)^t \mapsto x_1 g_1 + \ldots + x_n g_n$ einen Isomorphismus $\mathbb{Z}^n/L \simeq G$, wobei hier $L := \ker(\pi)$ gesetzt ist. Das $\mathbb{Z}$-Gitter kann dann durch eine Matrix $A \in \mathbb{Z}^{n\times n}$ beschrieben werden, d.h. die Spalten von A sind eine $\mathbb{Z}$-Basis von L.

Lemma 1.4.1 *Es gilt in obiger Situation:* $|G| = |\det(A)|$.

Definition 1.4.2 Eine Matrix $B \in \mathbb{Z}^{n\times n}$ ist in Smithscher Normalform (kurz SNF), falls B eine Diagonalmatrix mit nicht-negativen Koeffizienten ist, so dass $b_{i+1,i+1} \mid b_i$ für $1 \leq i < n$ gilt.

Satz 1.4.3 *Sei $A \in \mathbb{Z}^{n\times n}$ mit $\det(A) \neq 0$. Dann gibt es $U, V \in \mathrm{Gl}_n(\mathbb{Z})$, so dass $B = VAU$ in SNF ist.*

Als Anwendung von HNF und SNF haben wir einen prinzipiellen Algorithmus skizziert, der zu einer gegebenen endlichen abelschen Gruppe G die Struktur als abstrakte abelsche Gruppe bestimmt. Der Algorithmus setzt voraus, dass wir ein endliches $\mathbb{Z}$-Erzeugendensystem von G kennen sowie eine gute Approximation an die Kardinalität von G.

1.5 Gitter und quadratische Formen

Definition 1.5.1 Sei K ein Körper mit $\mathrm{char}(K) \neq 2$. Sei V ein K-Vektorraum. Dann nennen wir $q\colon V \longrightarrow K$ eine quadratische Form, falls die folgenden zwei Bedingungen erfüllt sind:
(1) Für all $\lambda \in K$ und alle $v \in V$ gilt $q(\lambda v) = \lambda^2 q(v)$.
(2) Durch $b(v, w) := \frac{1}{2}(q(v + w) - q(v) - q(w))$ ist eine symmetrische Bilinearform $b\colon V \times V \longrightarrow K$ definiert.

Es gilt dann $q(v) = b(v, v)$. Umgekehrt definiert jede symmetrische Bilinearform b auf V durch $q(v) := b(v, v)$ eine quadratsiche Form.

Definition 1.5.2 Ein Gitter (L, q) ist ein freier endlich erzeugter $\mathbb{Z}$-Modul zusammen mit einer positiv definiten (d.h. die zugeordnete symmetrische Bilinearform ist positiv definit) quadratischen Form auf $\mathbb{R}\otimes_{\mathbb{Z}} L$.

Für ein Gitter (L, q) schreiben wir oft $\langle\ ,\ \rangle_q$ für die zugeordnete Bilinearform. Wenn es der Kontext erlaubt, schreiben wir auch einfach $\langle\ ,\ \rangle$.

Definition 1.5.3 Sei (L, q) ein Gitter und $b_1, \ldots, b_n$ eine $\mathbb{Z}$-Basis von L. Sei $Q = (\langle b_i, b_j \rangle)$ die zugehörige Strukturmatrix. Dann heißt

$$d(L) := \sqrt{\det(Q)}$$

Diskriminante von (L, q).

1.6 Das Gram-Schmidtsche Orthogonalisierungsverfahren

Satz 1.6.1 *Sei $b_1, \ldots, b_n$ eine $\mathbb{R}$-Basis des euklidischen Vektorraums $(V, \langle\ ,\ \rangle)$. Definiere für $i = 1, \ldots, n$ induktiv*

$$b_i^* := b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$$

mit

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}.$$

Dann ist $b_1^*, \ldots, b_n^*$ eine Orthogonalbasis von V.

Remark 1.6.2 Für ein Gitter (L, q) und $V = \mathbb{R} \otimes_{\mathbb{Z}} L$, $\langle\ ,\ \rangle = \langle\ ,\ \rangle_q$ gilt:

$$d(L) = \prod_{i=1}^{n} ||b_i^*||.$$

Folgerung 1.6.3 *(Hadamard) Sei (L, q) ein Gitter und $b_1, \ldots, b_n$ eine $\mathbb{Z}$-Basis von L. Dann gilt:*

$$d(L) \leq \prod_{i=1}^{n} ||b_i||.$$

1.7 Der LLL-Algorithmus

Es sei $b_1, \ldots, b_n \in \mathbb{R}^n$ eine $\mathbb{Z}$-Basis des Gitters (L, q) und $b_1^*, \ldots, b_n^*$ die Orthogonalbasis aus dem Gram-Schmidt-Verfahren.

Definition 1.7.1 Die Basis $b_1, \ldots, b_n$ heißt LLL-reduziert, wenn die folgenden zwei Bedingungen erfüllt sind:

(i) $|\mu_{ij}| \leq \frac{1}{2}$ für $1 \leq j < i \leq n$.

(ii) $||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \geq \frac{3}{4} ||b_{i-1}^*||^2$ für $1 \leq i \leq n$.

Satz 1.7.2 *Sei $b_1, \ldots, b_n$ eine LLL-reduzierte $\mathbb{Z}$-Basis des Gitters (L, q). Dann gilt:*

1. $d(L) \leq \prod_{i=1}^{n} ||b_i|| \leq 2^{n(n-1)/4} d(L)$.
2. $||b_j|| \leq 2^{(i-1)/2} ||b_i^*||$ *für* $1 \leq j \leq i \leq n$.
3. $||b_1|| \leq 2^{(n-1)/4} d(L)^{1/n}$.
4. $||b_1|| \leq 2^{(n-1)/2} ||x||$ *für alle* $0 \neq x \in L$.
5. $||b_j|| \leq 2^{(n-1)/2} \max(||x_1||, \ldots, ||x_t||)$ *für alle linear unabhängigen* $x_1, \ldots, x_t \in L$ *und* $1 \leq j \leq t$.

In der Vorlesung haben wir den LLL-Algorithmus in grober Form präsentiert. Die Endlichkeit des Algorithmus beruht auf den folgenden Ausführungen.
Wir setzen für $i = 1, \ldots, n$

$$d_i := \det\left(\langle b_r, b_s \rangle\right)_{1 \leq r,s \leq i}.$$

Dann gilt $d_i = \prod_{j=1}^{i} B_j$ mit $B_j := ||b_i^*||^2$. Insbesondere $d_n = d(L)^2$.
Setze

$$D := \prod_{i=1}^{n-1} d_i.$$

Es gilt dann, dass D nach unten durch eine positive Konstante beschränkt ist, die nur von (L, q) abhängt. Um dies zu zeigen, notieren wir den folgenden Satz.

Satz 1.7.3 *Es gibt eine Konstante $\gamma_n \in \mathbb{R}_{>0}$ mit folgender Eigenschaft. Zu jedem vollen Gitter $(L, q) \subseteq \mathbb{R}^n$ gibt es einen Vektor $0 \neq x \in L$ mit $q(x) = ||x||^2 \leq \gamma_n d(L)^{2/n}$.*

Die γ_n heißen hermitesche Konstanten. Die Existenz der γ_n haben wir aus dem Minkowskischen Gitterpunktsatz hergeleitet.

Satz 1.7.4 *(Minkowsikischer Gitterpunktsatz) Sei $(L, q) \subseteq \mathbb{R}^n$ ein volles Gitter. Sei $C \subseteq \mathbb{R}^n$ konvex, symmetrisch bezüglich dem Nullpunkt und es gelte*

$$\mathrm{Vol}(C) > 2^n \mathrm{Vol}(L) = 2^n d(L).$$

Dann gibt es ein $0 \neq x \in L \cap C$.

2 Zahlkörper

2.1 Darstellung von algebraischen Zahlen

Sei $K/\mathbb{Q}$ ein Zahlkörper vom Grad $[K : \mathbb{Q}] = n$ und

$$\{\sigma_1, \dots \sigma_n\} = \{\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}\}$$

die Einbettungen $K \hookrightarrow \mathbb{C}$. Hierbei bezeichnen $\sigma_1, \dots, \sigma_{r_1}$ die reellen Einbettungen und $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$ die Paare komplex-konjugierter Einbetttungen.

2.1.1 Algebraische Zahlen als Wurzeln der Minimalgleichung

Sei $f \in \mathbb{Q}[X]$ normiert und irreduzibel. Dann ist $K = \mathbb{Q}[X]/(f(X))$ ein Zahlkörper vom Grad $n = \deg(f)$. Oftmals wollen wir K als Teilkörper der komplexen Zahlen $\mathbb{C}$ betrachten. Dazu braucht man Approximationen an die Nullstellen

$$\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$$

von f. Diese entsprechen den Einbettungen $K \hookrightarrow \mathbb{C}$ und werden entsprechend wie oben nummeriert. Es gilt:

$$Q[X]/(f(X)) \simeq \mathbb{Q}(\alpha) \text{ induziert von } g(X) \mapsto g(\alpha).$$

Diese Darstellung nennen wir die Standarddarstellung. Die Rechenoperationen finden in $Q[X]/(f(X))$ statt und benötigen als wesentliche Subroutinen Teilen mit Rest und den erweiterten euklidischen Algorithmus.

2.1.2 Darstellung bezüglich einer $\mathbb{Q}$-Basis

Die weiteren Darstellungen setzen voraus, dass K durch eine $\mathbb{Q}$-Vektorraumbasis $\theta_1, \dots, \theta_n$ gegeben ist. Zum Beispiel ist für $K = \mathbb{Q}[X]/(f(X) = \mathbb{Q}(\alpha)$ eine solche Basis durch $1, \alpha, \dots, \alpha^{n-1}$ gegebenen. Es gelte

$$\theta_i \theta_j = \sum_{k=1}^{n} a_{ij,k} \theta_k.$$

Für die Multiplikation speichert man in der Regel die Koeffizienten $a_{ij,k} \in \mathbb{Q}$ ab. Für die Division muss man umrechnen zur Standarddarstellung.

2.1.3 Die Matrixdarstellung

Sei $\theta_1, \dots, \theta_n$ eine $\mathbb{Q}$-Basis von K und $\beta \in K$. Dann ist die Multiplikation mit β ein Endomorphismus von K,

$$\mu_\beta \colon K \longrightarrow K, \quad \xi \mapsto \beta\xi.$$

Sei $M_\beta \in \mathbb{Q}^{n \times n}$ die Darstellungmatrix bezüglich der fixierten Basis $\theta_1, \dots, \theta_n$. Dann ist $\beta \mapsto M_\beta$ ein basisabhängiger injektiver $\mathbb{Q}$-Algebrenhomomorphismus $K \hookrightarrow \mathbb{Q}^{n \times n}$.

2.1.4 Konjugiertenvektoren

Im Gegensatz zu den bisherigen Darstellungen ist diese Darstellung nicht exakt. Wir stellen $\beta \in K$ durch einen sogenannten Konjugiertenvektor

$$(\sigma_1(\beta), \ldots, \sigma_{r_1}(\beta), \sigma_{r_1+1}(\beta), \ldots, \sigma_{r_1+r_2}(\beta)) \in \mathbb{C}^{r_1+r_2}$$

dar. Die Rechenoperationen sind hier einfach, da komponentenweise, allerdings braucht man in der Regel sehr gute Approximationen, um zu exakten Werten umzurechnen.

2.2 Spur, Norm und charakeristisches Polynom

Definition 2.2.1 (a) Sei $\beta \in K$. Dann heißt

$$\chi_\beta(X) := \prod_{i=1}^{n}(X - \sigma_i(\beta))$$

charakteristisches Polynom von β.
(b) Es sei $\chi_\beta(X) = \sum_{i=0}^{n}(-1)^{n-i}s_{n-i}X^i$. Dann nennt man $s_k(\beta)$ die k-te elementarsymmetrische Funktion von β.

Es gilt: $\mathrm{Tr}_{K/\mathbb{Q}}(\beta) = s_1(\beta), N_{K/\mathbb{Q}}(\beta) = s_n(\beta)$.
Die approximative Berechnung von χ_β ist leicht, wenn β als Konjugiertenvektor gegeben ist. Es gilt ferner:

$$\chi_\beta(X) = \det(XE - M_\beta).$$

Insbesondere sind Norm und Spur von β durch die Determinante und Spur von M_β gegeben.

Satz 2.2.2 *Sei $\beta = \sum_{i=0}^{n-1} a_i\alpha^i \in K = \mathbb{Q}(\alpha)$. Sei $A(X) := \sum_{i=0}^{n-1} a_iX^i$. Dann gilt:*

$$\chi_\beta(X) = \mathrm{Res}_Y(f(Y), X - A(Y)).$$

Insbesondere gilt für die Norm

$$N_{K/\mathbb{Q}}(\beta) = \mathrm{Res}_Y(f(Y), A(Y)).$$

Hierbei bezeichnet Res_Y die Resultante bezüglich Y über dem Ring $R = \mathbb{Q}[X]$. Resultanten sind relativ einfach zu berechnen, siehe [Cohen, Lemma 3.3.4].

2.3 Das Teilkörperproblem

Seien die Zahlkörper $K = \mathbb{Q}[x]/(f(x))$ und $L = \mathbb{Q}[x]/(g(x))$ durch die normierten irreduziblen Polynome $f, g \in \mathbb{Q}[x]$ gegeben. Seien α und β Nullstellen von f und g, also $K \simeq \mathbb{Q}(\alpha)$ und $L \simeq \mathbb{Q}(\beta)$. Wir wollen entscheiden, ob es eine Einbettung $K \hookrightarrow L$ gibt, oder mit anderen Worten, ob es eine Konjugierte $\sigma(\alpha)$ mit $\sigma(\alpha) \in L$ gibt. Dazu nutzen wir einen heuristischen Algorithmus unter Verwendung des LLL-Algorithmus.
Zunächst betrachten wir das folgende Problem. Gegeben $z_1, \ldots, z_n \in \mathbb{R}$. Finde eine Relation

$$a_1z_1 + \ldots + a_nz_n = 0 \text{ mit } a_i \in \mathbb{Z},$$

falls eine solche existiert. Dazu betrachten wir auf dem $\mathbb{R}^n$ die positiv definite quadratische Form

$$q(a) = a_2^2 + \ldots + a_n^2 + N(a_1z_1 + \ldots + a_nz_n)$$

mit $N >> 0$ und wenden den LLL-Algorithmus auf das Gitter $(\mathbb{Z}^n, q)$ an.

Falls allgemeiner $z_1, \ldots, z_n \in \mathbb{C}$ gegeben sind, so wende man den LLL auf die quadratische Form

$$q(a) = a_3^2 + \ldots + a_n^2 + N\left|a_1 z_1 + \ldots + a_n z_n\right|^2$$

an. Diese ist genau dann positiv definit, falls z_1, z_2 linear unabhängig über $\mathbb{R}$ sind. Dies kann man stets durch eine Permutation der z_i erreichen, es sei denn es gilt $z_i/z_j \in \mathbb{R}$ für alle $i \neq j$. In diesem Fall wende die reelle Version des Algorithmus auf $1, z_2/z_1, \ldots, z_n/z_1$ an.
Die Anwendung auf das Teilkörperproblem ist wie folgt. Falls $K \hookrightarrow L$, so gibt es eine Konjugierte α_i von α und ein Polynom $P \in \mathbb{Q}[x]$ vom Grad $\deg(P) < n := \deg(g) = [L : \mathbb{Q}]$ mit $\alpha_i = P(\beta)$. D.h. $1, \beta, \ldots, \beta^{n-1}, \alpha_i$ sind linear abhängig über $\mathbb{Q}$ und es gibt eine nicht-triviale Relation

$$a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1} + b\alpha_i = 0$$

mit $a_i, b \in \mathbb{Z}$. Falls diese mit dem obigen LLL-basierten heuristischen Verfahren gefunden wird, so haben wir das Teilkörperproblem eventuell gelöst. Die Korrektheit kann durch den Test $f \circ P \equiv 0 \pmod{g}$ verifiziert werden. Falls wir keine Relation finden, so können wir auch keine Aussage treffen.

2.4 Ordnungen und Ideale

Definition 2.4.1 Eine Ordnung R in K ist ein Teilring $R \subseteq K$, der als $\mathbb{Z}$-Modul endlich erzeugt ist und eine $\mathbb{Q}$-Basis von K enthält.

Sei R eine Ordnung und $I \subseteq R$ ein Ideal. Dann ist R/I stets endlich und wir definieren

$$\mathrm{N}(I) := |R/I| .$$

Definition 2.4.2 Sei $R \subseteq K$ eine Ordnung.
(a) Eine nicht-leere Teilmenge $(0) \neq I \subseteq K$ heißt gebrochenes Ideal von R, falls es ein $d \in \mathbb{Z}$ gibt, so dass $dI \subseteq R$ ein Ideal ist.
(b) Ein gebrochenes Ideal heißt invertierbar, wenn es ein gebrochenes Ideal J gibt mit $IJ = R$.

Lemma 2.4.3 *Sei I eingebrochenes Ideal und $I' := \{\alpha \in K \mid \alpha I \subseteq R\}$. Dann gilt:*

$$I \text{ ist invertierbar} \iff II' = R.$$

2.5 Darstellung von Moduln und Idealen

Definition 2.5.1 Sei $R \subseteq K$ eine Ordnung und sei $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}$-Basis von R. Sei $M \subseteq K$ ein voller $\mathbb{Z}$-Teilmodul. Dann gibt es eine eindeutig bestimmte $\mathbb{Z}$-Basis $\mu_1, \ldots, \mu_n$ von M mit

$$\mu_j = \frac{1}{d}\sum_{i=j}^{n} w_{ij},$$

so dass d, w_{ij} die folgenden Eigenschaften erfüllen:
(1) $d, w_{ij} \in \mathbb{Z}, d > 0, \mathrm{ggT}(d, w_{ij}, \forall i, j) = 1$,
(2) Die Matrix $W = (w_{ij})$ ist in HNF.
Dann heißt das Paar (W, d) HNF von M bezüglich R, genauer bezüglich der fixierten Basis $\omega_1, \ldots, \omega_n$ von R.

Bei dieser Darstellung ist die Berechnung von Modulsumme, der Test auf Gleichheit von zwei Moduln sowie falls $M \subseteq R$ die Berechnung des Index $[R : M]$ einfach. Insbesondere, falls $M \subseteq R$ ein Ideal ist, erhalten wir auf einfache Weise die Norm von M als Produkt der Diagonalelemente der HNF. Ferner lässt sich einfach testen, ob ein Element $\alpha \in K$ in M enthalten ist.
Eine zweite wichtige Art, um Ideale zur Maximalordnung $R = \mathcal{O}_K$ darzustellen, beruht auf folgendem Satz.

Satz 2.5.2 *Sei $\mathfrak{a} \subseteq \mathcal{O}_K$ ein Ideal. Dann gibt es zu jedem $0 \neq \alpha \in \mathfrak{a}$ ein $\beta \in \mathfrak{a}$, so dass $\mathfrak{a} = (\alpha, \beta) = \alpha\mathcal{O}_K + \beta\mathcal{O}_K$ gilt.*

2.6 Zerlegung in Primideale (Teil I)

Satz 2.6.1 *Sei $K = \mathbb{Q}(\theta)$ mit $\theta \in \mathcal{O}_K$. Sei $f := [\mathcal{O}_K : \mathbb{Z}[\theta]]$ und $m(X) \in \mathbb{Z}[x]$ das Minimalpolynom von θ. Sei p eine Primzahl und es gelte $p \nmid f$. Sei*

$$m(x) \equiv \prod_{i=1}^{g} m_i(x)^{e_i} \pmod{p}$$

die Zerlegung von $m(x)$ in $\mathbb{F}_p[x]$. Dann gilt:

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

mit $\mathfrak{p}_i = (p, m_i(\theta))$. Der Restklassengrad f_i von $\mathfrak{p}_i$ ist gegeben durch $\deg(m_i)$.

Remarks 2.6.2 a) Es ist also notwendig, gute Algorithmen zur Faktorisierung von Polynomen über endlichen Körpern zu entwickeln.
b) Aus $d(\theta) = f^2 d_K$ erhält man eine obere Abschätzung (bez. Teilbarkeit) für den Index f.
c) Statt $p \nmid f$ genügt es vorauszusetzen $(p, \mathfrak{f}) = 1$ für $\mathfrak{f} := \{\alpha \in K \mid \alpha\mathcal{O}_K \subseteq \mathbb{Z}[\theta]\}$.

2.7 Berechnung von Bewertungen

Für ein Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ und ein Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ wollen wir den Wert $v_\mathfrak{p}(\mathfrak{a})$ berechnen. Naiv könnte man $\mathfrak{p}^e$ für $e = 0, 1, \ldots$ berechnen, denn es gilt:

$$v_\mathfrak{p}(\mathfrak{a}) = \max\{e \mid \mathfrak{p}^e + \mathfrak{a} = \mathfrak{p}^e\}.$$

Eine alternative Vorgehensweise beruht auf folgendem Lemma.

Lemma 2.7.1 *Es gibt ein $a \in K \setminus \mathcal{O}_K$ mit $a\mathfrak{p} \subseteq \mathcal{O}_K$. Für jedes solche a gilt:*

$$\mathfrak{p}^{-1} = \mathcal{O}_K + a\mathcal{O}_K, \quad v_\mathfrak{p}(a) = -1, \quad v_\mathfrak{q}(a) = 0, \forall \mathfrak{q} \neq \mathfrak{p}.$$

Es gilt dann:

$$v_\mathfrak{p}(\mathfrak{a}) = \max\{e \mid a^e\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

2.8 Berechnung der Differente und Idealinversion

Wir errinnern an die Spurform

$$K \times K \longrightarrow \mathbb{Q}, \quad (\alpha, \beta) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta).$$

Die Spurform ist eine nicht-ausgeartete symmetrische Bilinearform auf dem $\mathbb{Q}$-Vektroraum K.
Für eine vollen $\mathbb{Z}$-Teilmodul $M \subseteq K$ sei

$$M^* := \{\alpha \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(\alpha M) \subseteq \mathbb{Z}\}.$$

Falls $M = \langle \gamma_1, \ldots, \gamma_n \rangle_\mathbb{Z}$, so ist

$$M^* = \langle \gamma_1^*, \ldots, \gamma_n^* \rangle_\mathbb{Z}$$

mit der Dualbasis (bez. der Spurform) $\gamma_1^*, \ldots, \gamma_n^*$ definiert durch $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma_i\gamma_j^*) = \delta_{ij}$ (Kronecker delta).
Für ein gebrochenes Ideal I wollen wir nun $I^{-1} = \{\alpha \in K \mid \alpha I \subseteq \mathcal{O}_K\}$ berechnen. Dazu führen wir die folgenden drei Schritte aus.

(1) Berechne $\mathcal{O}_K^*$.

(2) Berechne $I \cdot \mathcal{O}_K^*$.

(3) Berechne $(I \cdot \mathcal{O}_K^*)^*$.

Lemma 2.8.1 *Es gilt* $(I \cdot \mathcal{O}_K^*)^* = I^{-1}$.

Die Berechnungen der Duale in den Schritten (1) und (3) ist lineare Algebra, zur Berechnung des Produkts in Schritt (2) ist eine HNF zu berechnen.

Remark 2.8.2 $\mathcal{O}_K^*$ ist die sogenannte inverse Differente oder Kodifferente.

3 Berechnung der Maximalordnung

3.1 Die Sätze von Pohst-Zassenhaus

Sei $K = \mathbb{Q}(\theta)$, θ ganz, ein algebraischer Zahlkörper. Wir wollen den Ring der ganzen Zahlen $\mathcal{O}_K$ berechnen.

Definition 3.1.1 Sei $\mathcal{O}$ eine Ordnung und p eine Primzahl.

(1) $\mathcal{O}$ heißt p-maximal, falls $p \nmid [\mathcal{O}_K : \mathcal{O}]$.

(2) $I_p := \sqrt{p\mathcal{O}} = \{\alpha \in \mathcal{O} \mid \exists m \in \mathbb{Z}_{>0} \colon \alpha^m \in p\mathcal{O}\}$ heißt p-Radikal von $\mathcal{O}$.

Satz 3.1.2 *Sei $\mathcal{O} \subseteq K$ eine Ordnung in K und p eine Primzahl. Dann gilt:*

- *I_p ist ein Ideal in $\mathcal{O}$.*
- *$I_p = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ die paarweise verschiedenen Primideal von $\mathcal{O}$ über $p\mathbb{Z}$ sind.*
- *Es gibt ein $m > 0$ mit $I_p^m \subseteq \mathcal{O}$.*

Satz 3.1.3 *(Pohst-Zassenhaus) Sei $\mathcal{O} \subseteq K$ eine Ordnung in K und p eine Primzahl. Sei*

$$\mathcal{O}' := \{\alpha \in K \mid \alpha I_p \subseteq I_p\}.$$

Dann ist $\mathcal{O}'$ eine Ordnung und es gilt entweder (i) oder (ii), wobei

(i) $\mathcal{O} = \mathcal{O}'$ und $\mathcal{O}$ ist p-maximal.

(ii) $\mathcal{O} \subseteq \mathcal{O}', \mathcal{O} \neq \mathcal{O}'$ and $p \nmid [\mathcal{O}' : \mathcal{O}] \mid p^n$

Der Satz von Pohst-Zassenhaus legt folgenden groben Algorithmus nahe. Ausgehend von $\mathcal{O} = \mathbb{Z}[\theta]$ berechnen wir für jedes p mit $p^2 \mid d(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 d_K$ sukzessive grössere Ordnungen $\mathcal{O}'$ solange bis $\mathcal{O}'$ p-maximal ist. In der Praxis ist $d(\theta)$ oft sehr groß und die Berechnung der relevanten Primzahlen p daher ein Problem.

3.2 Das Dedekindkriterium

Für Ordnungen der Form $\mathcal{O} = \mathbb{Z}[\theta]$ kann man mit dem Dedekindkriterium effizient (d.h. schneller als mit Pohst-Zassenhaus) feststellen, ob $\mathcal{O}$ p-maximal ist.

Satz 3.2.1 *(Dedekindkriterium) Sei $K = \mathbb{Q}(\theta)$, θ ganz, und $m(x) \in \mathbb{Z}[x]$ das Minimalpolynom von θ. Sei p eine Primzahl. Sei*

$$\bar{m}(x) = \prod_{i=1}^{k} \bar{m}_i(x)^{e_i}$$

die Zerlegung in irreduzible Faktoren in $\mathbb{F}_p[x]$. Sei

$$g(x) := \prod_{i=1}^{k} m_i(x)$$

mit normierten Lifts $m_i(x) \in \mathbb{Z}[x]$ von $\bar{m}_i(x)$. Dann gilt:

- *Das p-Radikal I_p von $\mathcal{O} = \mathbb{Z}[\theta]$ ist gegeben durch*

$$I_p = p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta].$$

- *Sei $h(x) \in \mathbb{Z}[x]$ ein normierter Lift von $\bar{m}(x)/\bar{g}(x)$. Setze*

$$f(x) := \frac{1}{p}\left(g(x)h(x) - m(x)\right).$$

  Dann ist $f(x) \in \mathbb{Z}[x]$ und es gilt

$$\mathcal{O} = \mathbb{Z}[\theta] \text{ ist } p-maximal \iff (\bar{f}, \bar{g}, \bar{h}) = 1 \text{ in } \mathbb{F}_p[x].$$

- *Sei $\mathcal{O}' = \{x \in K \mid xI_p \subseteq I_p\}$. Sei $U(x) \in \mathbb{Z}[x]$ ein normierter Lift von $\bar{m}/(\bar{f}, \bar{g}, \bar{h})$. Dann gilt:*

  (i) $\mathcal{O}' = \mathbb{Z}[\theta] + \frac{1}{p}U(\theta)\mathbb{Z}[\theta]$.

  (ii) Für $d = \deg((\bar{f}, \bar{g}, \bar{h})$ gilt

$$[\mathcal{O}' : \mathbb{Z}[\theta]] = p^d, \quad d(\mathcal{O}') = d(\theta)/p^{2d}.$$

Für den Beweis des Dedekindkriteriums verweisen wir auf die Literatur.

3.3 Der Round2-Algorithmus

Ausgehend von der HNF von $\mathcal{O}$ sind die HNF von I_p und $\mathcal{O}'$ zu bestimmen.

Lemma 3.3.1 *Sei $n = [K : \mathbb{Q}]$ und $j \geq 1$, so dass $p^j \geq n$. Dann gilt:*

$$\mathrm{Rad}(\mathcal{O}/p\mathcal{O}) = \ker(x \mapsto x^{p^j}).$$

Man beachte, dass $\mathcal{O}/p\mathcal{O} \longrightarrow \mathcal{O}/p\mathcal{O}$, $x \mapsto x^{p^j}$, eine $\mathbb{F}_p$-lineare Abbildung ist. Der Kern kann also mit Methoden der linearen Algebra berechnet werden. Es gilt dann:

$$I_p = \mathrm{Lift}(\mathrm{Rad}(\mathcal{O}/p\mathcal{O})) + p\mathcal{O}.$$

Lemma 3.3.2 *Sei U der Kern der $\mathbb{F}_p$-linearen Abbildung*

$$\mathcal{O}/p\mathcal{O} \longrightarrow \mathrm{End}(I_p/pI_p), \quad \bar{\alpha} \mapsto (\bar{\beta} \mapsto \bar{\alpha}\bar{\beta}).$$

Dann gilt: $\mathcal{O}' = \mathrm{Lift}(\frac{1}{p}U) + p\mathcal{O}$.

Den Kern U kann man wieder mit Methoden der linearen Algebra berechnet werden.

3.4 Zerlegung in Primideale (Teil II)

Für Teiler p von $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ kann man das Polynomzerlegungsgesetz aus Satz 2.6.1 nicht anwenden. Falls man aber bereits $\mathcal{O}_K$ berechnet hat (oder allgemeiner eine p-maxinmale Ordnung $\mathcal{O}$) so kann man die sogenannte Buchmann-Lenstra-Methode verwenden. Der Einfachheit halber setzen wir $\mathcal{O} = \mathcal{O}_K$.
Sei $I_p = \sqrt{p\mathcal{O}_K}$ das p-Radikal. Wir definieren für $j \geq 0$ das Ideal $K_j := I_p^j$ und für $j \geq 1$

$$J_j := K_j/K_{j-1}, \quad H_j := J_j/J_{j+1}.$$

Falls $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ gilt, so ist

$$H_j = \prod_{i \text{ mit } j=e_i} \mathfrak{p}_i.$$

Sei $e := \max(e_1, \ldots, e_i)$. Dann gilt $e \leq [K : \mathbb{Q}]$ und

$$p\mathcal{O}_K = \prod_{j=1}^{e} H_j^j.$$

Es genügt also die Primidealzerlegung der ganzen Ideale H_j zu berechnen.
Die $\mathbb{F}_p$-Algebra

$$\mathcal{O}_K/H_j \simeq \prod_{i \text{ mit } j=e_i} \mathcal{O}_K/\mathfrak{p}_i$$

ist ein endliches Produkt von Körpern. Nach dem Satz vom primitiven Element gilt

$$\mathcal{O}_K/H_j = \mathbb{F}_p[\bar{\alpha}_j] \text{ mit einem } \alpha_j \in \mathcal{O}_K.$$

Sei $\bar{h}_j \in \mathbb{F}_p[x]$ das charakteristische Polynom und

$$\bar{h}_j(x) = \prod_{i=1}^{r_j} \bar{q}_{ji}(x)$$

seine Zerlegung in irreduzible Faktoren in $\mathbb{F}_p[x]$. Sei $q_{ji}(x) \in \mathbb{Z}[x]$ ein normierter Lift von $\bar{q}_{ji}(x)$ und

$$\mathfrak{q}_{ji} := H_j + q_{ji}(\alpha_j)\mathcal{O}_K.$$

Dann gilt:

$$H_j = \prod_{i=1}^{r_j} \mathfrak{q}_{ji}.$$

Zur Konstruktion des primitiven Elements $\bar{\alpha}_j$ wird folgender Satz verwendet.

Satz 3.4.1 *Sei A eine endliche separable $\mathbb{F}_p$-Algebra (d.h. eine endliches Produkt von endlichen Körpererweiterungen von $\mathbb{F}_p$). Dann gibt es einen effizienten Algorithmus, der entweder zeigt, dass A ein Körper ist, oder ein nicht-triviales Idempotent $\varepsilon \in A$ berechnet.*

Remark 3.4.2 Der Beweis ist konstruktiv. Man erhält dann $A = A_1 \oplus A_2$ mit $A_1 := \varepsilon A$ und $A_2 := (1 - \varepsilon)A$ und kann somit A iterativ als ein Produkt von Körpern darstellen. Letzendlich braucht man also "nur noch" einen Algorithmus zur Auffindung von primitiven Elementen in endlichen Körpererweiterungen von $\mathbb{F}_p$.

4 Berechnung von Klassengruppe, Regulator und Fundamentaleinheiten

4.1 Definitionen und Notationen, grundlegende Resultate

Sei K ein algebraischer Zahlkörper. Es sei

- $I(K)$ die Gruppe der gebrochenen Ideale,
- $P(K)$ die Untergruppe der Hauptideale,
- $\mathrm{cl}(K) = I(K)/P(K)$ die Idealklassengruppe,
- $h_K = |\mathrm{cl}(K)|$ die Klassenzahl,
- $U(K) = \mathcal{O}_K^\times$ die Einheitengruppe und
- $\mu(K)$ die Gruppe der in K gelegenen Einheitswurzeln.

Zentrale Resultate der algebraischen Zahlentheorie sind die beiden folgenden Sätze.

Satz 4.1.1 $h_K < \infty$.

Satz 4.1.2 $U(K) \simeq \mu(K) \times \eta_1^{\mathbb{Z}} \times \ldots \times \eta_{r_u}^{\mathbb{Z}}$ *mit sogenannten Fundamentaleinheiten* $\eta_1, \ldots \eta_{r_u} \in U(K)$. *Hierbei ist* $r_u = r_1 + r_2 - 1$, *wobei* r_1 *die Anzahl der reellen Einbettungen und* r_2 *die Anzahl der Paare komplex-konjugierter Einbettungen bezeichnet.*

Für das Weitere legen wir die folgende Numerierung zugrunde. Es sei

$$\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+1}, \ldots, \bar{\sigma}_{r_1+r_2}$$

die Gesamtheit der $\mathbb{Q}$-Einbettungen $\sigma\colon K \hookrightarrow \mathbb{C}$.
Wir definieren

$$|\alpha|_\sigma = ||\sigma(\alpha)|| = \begin{cases} |\sigma(\alpha)|, & \text{falls } \sigma \text{ reell ist,} \\ |\sigma(\alpha)|^2, & \text{falls } \sigma \text{ komplex ist.} \end{cases}$$

Definition 4.1.3 Sei $\eta_1, \ldots \eta_{r_u}$ ein System von Fundamentaleinheiten. Sei M eine beliebige $r_u \times r_u$-Matrix, die aus

$$(\log \sigma_j(\eta_i))_{\substack{1 \le i \le r_u, \\ 1 \le j \le r_u+1}}$$

durch Streichen einer beliebigen Spalte entsteht. Dann setzt man:

$$R(K) := |\det(M)|$$

und nennt dies den Regulator von K.

Remark 4.1.4 Diese Definition ist unabhängig von der Wahl der Fundamentaleinheiten sowie der Wahl der zu streichenden Spalte.

4.2 Berechnung von $\mu(K)$

Lemma 4.2.1 *Sei $\alpha \in \mathcal{O}_K$. Dann gilt:*

$$\alpha \in \mu(K) \iff |\sigma(\alpha)| = 1 \text{ für alle } \mathbb{Q}\text{-Einbettungen } \sigma\colon K \hookrightarrow \mathbb{C}.$$

Für $r_1 > 0$ ist $\mu(K) = \{\pm 1\}$. Daher sei im Weiteren $r_1 = 0$.
Sei $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \ldots \oplus \mathbb{Z}\omega_n$. Dann ist jede Einheitswurzel ζ von der Form

$$\zeta = \sum_{i=1}^{n} x_i \omega_i$$

mit ganzen Zahlen $x_1, \ldots, x_n$. Die Ungleichnung zwischen geometrischen und arithmetischen Mittel zeigt, dass die Einheitswurzeln in K genau durch die Minima auf dem Gitter $\mathbb{Z}^n$ der positiv definiten quadratischen Form

$$Q(x_1, \ldots, x_n) := \sum_{j=1}^{n} |\sigma_j(\sum_{i=1}^{n} x_i \omega_i)|^2$$

gegeben sind. Diese kann man z.B. mit dem Fincke-Pohst-Algorithmus bestimmen.‘

4.3 Die Dedekindsche Zeta-Funktion

Definition 4.3.1 Die Dedekindesche Zetafunktion ist für $\mathrm{Re}(s) > 1$ definiert durch

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

wobei $\mathfrak{a} \neq (0)$ die ganzen Ideale und $\mathfrak{p} \neq (0)$ die Primideale von $\mathcal{O}_K$ durchläuft.

Definition 4.3.2 Die Funktion

$$\Lambda_K(s) = |d_K|^{s/2} \left(\pi^{-s/2}\Gamma(s/2)\right)^{r_1+r_2} \left(\pi^{(1-s)/2}\Gamma((s+1)/2)\right)^{r_2} \zeta_K(s)$$

heißt vervollständigte Dedekindsche Zetafunktion.

Satz 4.3.3 *(Analytische Klassenzahlformel)*

- *$\zeta_K(s)$ hat eine meromorphe Fortsetzung auf $\mathbb{C}$. Sie ist holomorph auf $\mathbb{C} \setminus \{1\}$ und hat einen einfachen Pol bei $s = 1$.*
- *Die vervollständigte Zetafunktion genügt der Funktionalgleichung*

$$\Lambda(1 - s) = \Lambda(s).$$

- *$\zeta_K(s)$ hat eine Nullstelle der Ordnung r_u bei $s = 0$ und es gilt*

$$\lim_{s \to 0} s^{-r_u} \zeta_K(s) = -h(K)R(K)/|\mu(K)|.$$

- *$\zeta_K(s)$ hat einen Pol der Ordnung 1 bei $s = 1$ und es gilt*

$$\lim_{s \to 0} (s-1)\zeta_K(s) = 2^{r_1}(2\pi)^{r_2} \frac{h(K)R(K)}{|\mu(K)|\sqrt{|d_K|}}.$$

4.4 Idealreduktion

Definition 4.4.1 a) Sei $\mathfrak{a} \in I(K)$ ein gebrochenes Ideal und $\alpha \in \mathfrak{a}, \alpha \neq 0$. Dann nennt man α ein Minimum von $\mathfrak{a}$, falls für alle $\beta \in \mathfrak{a}$ gilt:

$$|\sigma_i(\beta)| < |\sigma_i(\alpha)| \text{ für } i = 1, \ldots, n \implies \beta = 0.$$

b) $\mathfrak{a}$ heißt reduziert, falls $\ell(\mathfrak{a})$ ein Minimum von $\mathfrak{a}$ ist. Hierbei ist $\ell(\mathfrak{a})\mathbb{Z} = \mathfrak{a} \cap \mathbb{Q}$.

Definition 4.4.2 Sei $\alpha \in K$ und $v = (v_1, \ldots, v_{r_1}, v_{r_1+1}, \ldots, v_{r_1+r_2}, v_{r_1+1}, \ldots, v_{r_1+r_2}) \in \mathbb{R}^n$. Dann heißt

$$||\alpha||_v := \sqrt{\sum_{i=1}^{n} e^{v_i} |\sigma_i(\alpha)|^2}$$

v-Norm von α.

Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$. Sei

$$q_{ij} := \sum_{k=1}^{n} e_{v_k} \overline{\sigma_k(\alpha_i)} \sigma_k(\alpha_j).$$

Dann definiert $Q = (q_{ij})_{1 \leq i,j \leq n}$ eine positiv-definite symmetrische Bilinearform auf $\mathbb{R}^n$ und für $\alpha = \sum_{i=1}^{n} x_i \alpha_i \in \mathfrak{a}$ und $x = (x_1, \ldots, x_n)^t \in \mathbb{Z}^n$ gilt:

$$x^t Q x = ||\alpha||_v^2.$$

Satz 4.4.3 *Falls $\alpha \in \mathfrak{a}$ ein Element kürzester Länge in $\mathfrak{a}$ bez. der v-Norm ist, so ist $\alpha^{-1}\mathfrak{a}$ reduziert.*

Mit dem LLL-Algorithmus kann man nun kurze Elemente in $\beta \in \mathfrak{a}$ berechnen. Dann ist $\mathfrak{b} := \beta^{-1}\mathfrak{a}$ "fast" reduziert und man hofft, dass $\mathfrak{b}$ dann ausschließlich kleine Primidealteiler hat.

4.5 Berechnung einer Relationenmatrix

Sei $\mathcal{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ eine Menge von Primidealen, deren Klassen $[\mathfrak{p}_i]$ die Klassengruppe $\mathrm{cl}(K)$ erzeugen. Dann ist der Gruppenhomomorphismus

$$\pi \colon \mathbb{Z}^k \longrightarrow \mathrm{cl}(K), \quad (x_1, \ldots, x_k)^t \mapsto \left[\prod_{i=1}^{k} \mathfrak{p}_i^{x_i} \right]$$

surjektiv und wir wollen $\Lambda_f := \ker(\pi)$ bestimmen. Dazu berechne man zufällige Produkte $I = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ und mittels LLL einen kurzes Element α bezüglich der v-Norm. Falls dann $J := \alpha^{-1} I$ über $\mathcal{P}$ faktorisiert, d.h.

$$J = \prod_{i=1}^{k} \mathfrak{p}_i^{d_i},$$

so gilt $\alpha \mathcal{O}_K = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i - d_i}$ und $(e_1 - d_1, \ldots, e_k - d_k)^t$ liefert eine Spalte in der Relationenmatrix. Zusätzlich zu dieser "nicht-archimedischen" Information speichern wir den Vektor

$$L(\alpha) := (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_{r_1}(\alpha)|, 2\log|\sigma_{r_1+1}(\alpha)|, \ldots, 2\log|\sigma_{r_1+r_2}(\alpha)|)^t$$

ab. Wir generieren auf diese Weise $k_2 > k$ Relationen und eine Matrix Λ der Form

$$\Lambda = \begin{pmatrix} \Lambda_f \\ \cdots \\ \Lambda_\infty \end{pmatrix}$$

4.6 Berechnung eines ganzzahligen Vielfachen des Regulators und unabhängiger Einheiten (Grobform)

Berechne den ganzzahligen Kern W von Λ_f. Sei $V \in \mathbb{Z}^{k_2 \times s}$ eine Matrix, deren Spalten eine $\mathbb{Z}$-Basis von W sind. Sei v_i, $i = 1, \ldots, s$, eine Spalte von V. Dann ist

$$\epsilon_i := \prod_{j=1}^{k_2} \alpha_j^{v_{ij}}$$

eine Einheit und die i-te Spalte in $\Lambda_\infty V$ ist gegeben durch $L(\epsilon_i)$.
Falls $s \geq r_u$ gilt, so kann man beliebige $r_u \times r_u$-Minoren von $\Lambda_\infty V$ betrachten und erhält entweder 0 oder im günstigen Fall ein ganzzahliges Vielfaches R des Regulators $R(K)$. Aus verschiedenen Werten R kann man durch Berechnung eines reellen ggT kleinere ganzzahlige Vielfache von R_K berechnen. Im folgenden Abschnitt stellen wir die benötigten Grundlagen dar und skizzieren einen einfachen Algorithmus.

4.7 Unabhängige Einheitensysteme

Lemma 4.7.1 *a) Seien $\eta_1, \ldots, \eta_{r_u}$ Einheiten. Dann gilt:*

$$[U(K) : \langle \eta_1, \ldots, \eta_{r_u} \rangle] < \infty \iff R(\eta_1, \ldots, \eta_{r_u}) \neq 0.$$

Es gilt dann: $[U(K) : \langle \eta_1, \ldots, \eta_{r_u} \rangle] = \frac{R(\eta_1, \ldots, \eta_{r_u})}{R(K)}$.
b) Seien allgemeiner $\eta_1, \ldots, \eta_{r_u}$ und $\epsilon_1, \ldots, \epsilon_{r_u}$ unabhängige Einheitensysteme und es gelte $\langle \eta_1, \ldots, \eta_{r_u} \rangle \subseteq \langle \epsilon_1, \ldots, \epsilon_{r_u} \rangle$. Dann gilt:

$$[\langle \epsilon_1, \ldots, \epsilon_{r_u} \rangle : \langle \eta_1, \ldots, \eta_{r_u} \rangle] = \frac{R(\eta_1, \ldots, \eta_{r_u})}{R(\epsilon_1, \ldots, \epsilon_{r_u})}.$$

Lemma 4.7.2 *Seien $\eta_1, \eta_2, \ldots, \eta_{r_u}$ und $\eta_1', \eta_2, \ldots, \eta_{r_u}$ zwei unabhängige Einheitensysteme mit Regulatoren R und R'. Sei $d = uR + vR'$ der reelle ggT. Dann ist $\eta_1^u \eta_1'^v, \eta_2, \ldots, \eta_{r_u}$ ein unabhängiges Einheitensystem mit Regulator d.*

Aufbauend auf diesem Lemma kann man z.B. folgendermaßen vorgehen. Wir haben bereits Einheiten $\epsilon_1, \ldots, \epsilon_s$ mit $s \geq r_u$ berechnet. Aus der Matrix $C := \Lambda_\infty \cdot V$ berechnen wir $R_1 := R(\epsilon_1, \ldots, \epsilon_{r_u})$ und $R_2 := R(\epsilon_2, \ldots, \epsilon_{r_u+1})$. Falls $R_1 R_2 \neq 0$, so berechne man den reellen ggT $d = uR_1 + vR_2$. Dann hat $\epsilon_2, \ldots, \epsilon_{r_u}, \epsilon_1^{(-1)^{r_u-1}u} \epsilon_{r_u+1}$ den Regulator d. Entsprechend ersetzen wir in C die (r_u+1)-te Spalte durch $(-1)^{r_u-1} L(\epsilon_1) + vL(\epsilon_{r_u+1})$. Im nächsten Schritt nehmen wir auf diese Weise die Einheit ϵ_{r_u+2} dazu und erhalten letztendlich hoffentlich Einheiten $\eta_1, \ldots \eta_{r_u}$ mit $R = R(\eta_1, \ldots \eta_{r_u}) \neq 0$. Dieses R ist dann ein ganzzahliges Vielfaches von R_K.

4.8 Der vollständige Algorithmus

1. Berechne eine Ganzheitsbasis $\omega_1, \ldots, \omega_n$ von $\mathcal{O}_K$ sowie die Diskriminante d_K.
2. Berechne eine Menge von Primidealen $\mathcal{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$, so dass die Klassen der $\mathfrak{p}_i$ die Idealklassengruppe erzeugen. Zum Beispiel kann man die Menge aller Primideal $\mathfrak{p}$ mit Norm $\leq M_K$ nehmen, wobei M_K die Minkowsischranke bezeichnet.
3. Setze $k_2 := k + r_u + 10$.
4. Finde k_2 Relationen, z.B. so wie in Abschnitt 4.5 beschrieben.
5. Berechne die HNF von Λ_f. Falls Λ_f nicht vollen Rang hat, gehe zu Schritt 4 und nimm 10 weitere Relationen dazu.

6. (Λ_f hat nun vollen Rang.) Berechne den ganzzahligen Kern von Λ_f und mit dem Verfahren aus Abschnitt 4.7 Einheiten $\eta_1, \ldots, \eta_{r_u}$, so dass $R = R(\eta_1, \ldots, \eta_{r_u}) \neq 0$ gilt. Falls dies nicht gelingt, gehe zu Schritt 4 und nimm 10 weitere Relationen dazu.

7. Sei $h = \det(H)$, wobei H die HNF von Λ_f bezeichnet. Dann ist hR ein ganzzahliges Vielfaches von $h(K)R(K)$.

8. Berechne $\mu(K)$.

9. Berechne $\tilde{z} := \prod_p \frac{(1-1/p)}{\prod_{\mathfrak{p}|p}(1-1/N\mathfrak{p})}$ und

$$z := \tilde{z}\frac{|\mu(K)|\sqrt{|d_K|}}{2^{r_1}(2\pi)^{r_2}},$$

   wobei p die Primzahlen unterhalb einer geeigneten Schranke durchläuft. Dann gilt $z \sim h_K R_K$.

10. Falls $hR \geq z\sqrt{2}$, so gehe zu Schritt 4 und nimm 10 weitere Relationen dazu. Andernfalls gilt $hR = h(K)R(K)$.

11. Berechne die SNF von H. Dies liefert die Gruppenstruktur von $\mathrm{cl}(K)$ sowie deren Erzeuger. Aus Schritt 6 haben wir Fundamentaleinheiten $\eta_1, \ldots, \eta_{r_u}$.

5 Das Zahlkörpersieb

Sei N eine große zu faktorisierende Zahl. Die allgemeine Idee der besten Faktorisierungsalgorithmen ist wie folgt. Finde ganze Zahlen x, y mit

$$x^2 \equiv y^2 \pmod{N}, \quad x \not\equiv \pm y \pmod{N}.$$

Dann liefert $\mathrm{ggT}(x \pm y, N)$ einen nicht-trivialen Teiler von N.
Zur Konstruktion von x und y sucht man n Kongruenzen (n groß genug) der Form

$$x^k \equiv (-1)^{e_{0k}} p_1^{e_{1k}} \cdots p_m^{e_{mk}} \pmod{N} \tag{1}$$

mit einer Faktorbasis $\{-1, p_1, \ldots, p_m\}$. Sei $e_k = (e_{0k}, e_{1k}, \ldots e_{mk})$ der Zeilenvektor der Exponenten, $k = 1, \ldots, n$. Durch Lösen eines linearen Gleichungssytems über $\mathbb{F}_2$ finden wir $\epsilon_1, \ldots, \epsilon_n \in \{0, 1\}$ mit

$$\sum_{k=1}^{n} \epsilon_k e_k = 2(v_0, v_1, \ldots, v_m), \quad v_i \in \mathbb{Z}.$$

Dann gilt für $x := \prod_{k=1}^n x_k^{\epsilon_k}$ und $y := (-1)^{v_0} p_1^{v_1} \cdots p_m^{v_m}$ die Kongruenz $x^2 \equiv y^2 \pmod{N}$.
Zur Erzeugung der Kongruenzen (1) gibt es verschiedene Methoden. Die besten sind das quadratische Sieb und das Zahlkörpersieb.

5.1 Das quadratische Sieb

Betrachte das Polynom

$$Q(a) = \left([\sqrt{N}] + a\right)^2 - N.$$

Dann gilt $Q(a) \equiv x^2 \pmod{N}$ für $x = [\sqrt{N}] + a$. Falls $Q(a)$ über der Faktorbasis faktorisiert, so haben wir eine Kongruenz der Form (1) gefunden. Aufgrund der Beobachtung

$$m \mid Q(a) \implies m \mid Q(a + km), \forall k \in \mathbb{Z},$$

kann man sieben. Wir haben das am Beispiel demonstriert.

5.2 Das Zahlkörpersieb

5.2.1 Die prinzipielle Idee

Es sei $K = \mathbb{Q}(\theta)$, $f \in \mathbb{Z}[x]$ das Minimalpolynom von θ. Es gelte für ein $m \in \mathbb{N}$ und ein kleines $k \in \mathbb{N}$ die Beziehung $f(m) = kN$.

Example 5.2.1 *Sei $N = r^e - s$ mit kleinem r, s. Wähle dann ein geeignetes d und setze $k := \lceil \frac{e}{d} \rceil$. Betrachte $f(x) = x^d - sr^{kd-e}$. Dann gilt für $m = r^k$ die Gleichung $f(m) = r^{kd-e}$. Für die Fermatsche Zahl $N = 2^{512} + 1$ erhält man so $f(x) = x^5 + 8$. Anfang der 90er Jahre wurde N mit dem Zahlkörpersieb faktorisiert. Es gilt $N = p_7 p_{49} p_{99}$, wobei in dieser Notation p_m eine m-stellige Primzahl bedeutet.*

Den Ringhomomorphismus $\tilde{\phi}\colon \mathbb{Z}[\theta] \longrightarrow \mathbb{Z}/N\mathbb{Z}$, $\theta \mapsto m + N\mathbb{Z}$, kann man unter der Voraussetzung $([\mathcal{O}_K : \mathbb{Z}[\theta]], N) = 1$ fortsetzen zu einem Ringhomomorphismus

$$\phi\colon \mathcal{O}_K \longrightarrow \mathbb{Z}/N\mathbb{Z}.$$

Der Einfachheit halber setzten wir zunächst $h(K) = 1$ voraus. Sei $t = r_1 + r_2 - 1$ der Einheitenrang, $\langle u_0 \rangle = \mu(K)$ und $u_1, \ldots, u_t$ ein System von Fundamentaleinheiten. Setze

$$U := \{u_0, u_1, \ldots, u_t\}.$$

Sei $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{k_1}\}$ die Menge der Primideale mit Norm kleiner gleich einer geeigneten Schranke B_1. Fixiere Elemente π_i mit $\pi_i \mathcal{O}_K = \mathfrak{p}_i$ und setze

$$G := \{\pi_1, \ldots, \pi_{k_1}\}.$$

Sei

$$\mathcal{P} = \{p_0 = -1, p_1, \ldots, p_{k_2}\}$$

eine geeignete Faktorbasis mit rationalen Primzahlen $p_1, \ldots, p_{k_2}$.
Wir suchen nun ℓ ganze Zahlen

$$\alpha_n = \prod_{i=0}^{t} u_i^{a_{in}} \prod_{j=1}^{k_1} \pi_j^{b_{jn}} \tag{2}$$

und betrachten einen Vertreter von $\phi(\alpha_n)$ in $[-\frac{N-1}{2}, \frac{N+1}{2}]$. Falls dieser über $\mathcal{P}$ faktorisiert, so gilt

$$\phi(\alpha_n) \equiv \prod_{k=0}^{k_2} p_k^{c_{kn}} \pmod{N}$$

mit $c_{kn} \in \mathbb{Z}$. Dies produziert ℓ Zeilenvektoren

$$w_n = (a_{0n}, \ldots, a_{tn}, b_{1n}, \ldots, b_{k_2 n}, c_{0n}, \ldots, c_{k_2 n}).$$

Wir lösen wieder ein lineares Gleichungssystem über $\mathbb{F}_2$ und im günstigen Fall finden wir $\epsilon_1, \ldots, \epsilon_\ell$ mit

$$\sum_{n=1}^{\ell} \epsilon_n w_n = 2(a_{0n}, \ldots, a_t, b_1, \ldots, b_{k_2}, c_0, \ldots, c_{k_2}).$$

Setzt man nun

$$\alpha := \prod_{i=0}^{t} u_i^{a_i} \cdot \prod_{j=1}^{k_1} \pi_j^{b_j}, \quad x := \prod_{k=0}^{k_2} p_k^{c_k},$$

so gilt

$$\phi(\alpha)^2 \equiv x^2 \pmod{N}.$$

5.3 Eine konkrete Umsetzung im Spezialfall (sehr vereinfact)

Der Einfachheit halber setzen wir nun $\mathcal{O}_K = \mathbb{Z}[\theta]$ voraus. Für $\alpha = \alpha_n$ betrachten wir ausschließlich Zahlen der Form

$$\alpha = a + b\theta \text{ mit } a, b \in \mathbb{Z}, \quad (a, b) = 1.$$

Lemma 5.3.1 *Sei α wie eben und $\mathfrak{p}$ ein Primidealteiler von α. Dann ist $\mathfrak{p}$ von Grad 1, d.h. $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = 1$, wobei $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ gilt.*

Sei wie früher f das Minimalpolynom von θ. Nach dem Polynomzerlegungsgesetz korrespondieren die Primidealteiler $\mathfrak{p}$ von p zu den irreduziblen Teilern von f modulo p. Für ein $\mathfrak{p}$ mit $\mathfrak{p} \mid \alpha$ sind dies aufgrund des Lemmas allesamt lineare Polynome der Form $X - c_p$, $c_p \in \{0, 1, \ldots, p-1\}$. Es ist dann $\mathfrak{p} = (p, \theta - c_p)$ und es gilt $v_\mathfrak{p}(\alpha) = v_p(N(\alpha))$.
Wir wählen nun eine geeignete obere Schranke B. Als Faktorbasen wählen wir

$$FB := \{\pm 1\} \cup \{p \colon p \leq B\}$$

für die Faktorisierung von $a + bm$ sowie

$$FB_2 := \{\mathfrak{p} \colon \mathfrak{p} \text{ von Grad 1 und } \mathfrak{p} \mid p \in FB\}.$$

für die Faktroisierung von $a + b\theta$. Jedes $\mathfrak{p}$ in der zweiten Faktorbasis ist von der Form $(p, \theta - c_p)$. Die folgenden Beobachtungen erlauben es uns zu sieben:

$$\begin{aligned} p^k \mid a + bm \quad &\iff \quad p^k \mid (a + xp^k) + (b + yp^k)m, \forall x, y \in \mathbb{Z}, \\ \mathfrak{p} \mid \alpha \quad &\iff \quad p \mid a + bc_p \end{aligned}$$

Siebe zunächst nach $a + bm$. Unter denjenigen $a + bm$, die auf 1 reduziert werden konnten, d.h. die über FB faktorisieren, siebe jetzt $N(a + b\theta)$ modulo p. Beachte, dass wir hier nur modulo p sieben können. In allen Zeilen, wo $N(a + b\theta)$ nun hinreichend klein ist, führe, falls möglich, eine vollständige Faktorisierung von $a + b\theta$ über der zweiten Faktorbasis durch.
Insgesamt erhält man also, falls die Faktorsierungen vollständig gelingen,

$$\alpha\mathcal{O}_K = (a + b\theta)\mathcal{O}_K = \prod_{\mathfrak{p} \in FB_2} \mathfrak{p}^{a_\mathfrak{p}} \text{ mit } a_\mathfrak{p} \in \mathbb{Z}.$$

Hieraus kann man nun eine Darstellung der Form (2) berechnen.