Protokoll zur Vorlesung Algorithmische Zahlentheorie WS 25/26

W. Bley

27. Januar 2026

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 Test auf Gleichheit

Seien $L_1, L_2 \subseteq \mathbb{Z}^m$ zwei Gitter, beschrieben durch $A_1 \in \mathbb{Z}^{m\times n_1}$ und $A_2 \in \mathbb{Z}^{m\times n_2}$. Dann gilt:

$$L_1 = L_2 \iff \mathrm{HNF}(A_1) = \mathrm{HNF}(A_2).$$

1.5 Summe von zwei Gittern

Etwas allgemeiner betrachten wir Gitter $L \subseteq \mathbb{Q}^m$. Sei $d \in \mathbb{N}$ minimal mit $dL \subseteq \mathbb{Z}^m$. Dann nennt man d den Nenner von L und unter der HNF von L verstehen wir das Paar $(\mathrm{HNF}(dL), d)$.
Seien nun $L_1, L_2 \subseteq \mathbb{Q}^m$ zwei Gitter gegeben durch ihre jeweilige HNF (W_1, d_1) bzw. (W_2, d_2). Sei $D := \mathrm{kgV}(d_1, d_2)$. Betrachte dann die Matrix $W = (\frac{D}{d_1}W_1 \mid \frac{D}{d_2}W_2)$. Dann sind die nicht-trivialen Spalten von $\mathrm{HNF}(W)$ eine $\mathbb{Z}$-Basis von $D(L_1 + L_2)$.

1.6 Test auf Inklusion

Ohne Einschränkung seien $L_1, L_2 \subseteq \mathbb{Z}^m$. Dann gilt:

$$L_1 + L_2 = L_2 \iff L_1 \subseteq L_2.$$

Dies lässt sich mit den vorherigen Algorithmen testen.

1.7 Smithsche Normalform

Sei G eine endliche abelsche Gruppe. Sei $g_1, \ldots, g_n$ ein Erzeugendensystem von G. Dann induziert der Epimorphismus $\pi\colon \mathbb{Z}^n \longrightarrow G, (x_1, \ldots, x_n)^t \mapsto x_1g_1 + \ldots + x_ng_n$ 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 1.7.1 *Es gilt in obiger Situation:* $|G| = |\det(A)|$.

Definition 1.7.2 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 1.7.3 *Sei* $A \in \mathbb{Z}^{n\times n}$ *mit* $\det(A) \neq 0$. *Dann gibt es genau eine Matrix* B *in SNF von der Form* $B = VAU$ *mit* $U, V \in \mathrm{Gl}_n(\mathbb{Z})$.

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.

1.8 Weitere Algorithmen für endlich erzeugte abelsche Gruppen

Literatur: H.Cohen, Advanced topics in computational number theory, Chapter 4.1

Wir benutzen im Folgenden die folgende Matrixnotation: Sei $\mathcal{A}$ eine e-e abelsche Gruppe und $A = (\alpha_1, \ldots, \alpha_r)$ mit $\alpha_i \in \mathcal{A}$ ein Zeilenvektor von Elementen in $\mathcal{A}$. Für eine Spaltenvektor $X = (x_1, \ldots, x_r)^t \in \mathbb{Z}^r$ sei

$$AX = \sum_{i=1}^{r} x_i\alpha_i \text{ oder } \prod_{i=1}^{r} \alpha_i^{x_i},$$

je nachdem, ob wir die Gruppenoperation in $\mathcal{A}$ additiv oder multiplikativ schreiben. Entsprechend ist für eine Matrix $M = (m_{ij}) \in \mathbb{Z}^{r\times n}$

$$AM = (\beta_1, \ldots, \beta_n) \text{ mit } \beta_j = \sum_{i=1}^{r} m_{ij}\alpha_i \text{ oder } \prod_{i=1}^{r} \alpha_i^{m_{ij}}.$$

Definition 1.8.1 Sei $\mathcal{A}$ eine e-e abelsche Gruppe und $G = (g_1, \ldots, g_r)$ mit $g_i \in \mathcal{A}$. Sei $M \in \mathbb{Z}^{r\times k}$. Dann ist (G, M) ein System von Erzeugern und Relationen, falls

- es für jedes $\alpha \in \mathcal{A}$ ein $X \in \mathbb{Z}^r$ mit $\alpha = GX$ gibt.
- für alle $X \in \mathbb{Z}^r$ gilt:
$$GX = 1_{\mathcal{A}} \iff \exists Y \in \mathbb{Z}^k \text{ mit } X = MY.$$

Inbesondere gilt also $GM = (1_{\mathcal{A}}, \ldots, 1_{\mathcal{A}})$. Mit anderen Worten kann man äquivalent sagen:

$$\mathbb{Z}^k \xrightarrow{M} \mathbb{Z}^r \xrightarrow{G} \mathcal{A} \longrightarrow 1$$

ist eine Präsentation von $\mathcal{A}$.

Definition 1.8.2 Sei $\mathcal{A}$ eine e-e abelsche Gruppe und (A, D) ein System von Erzeugern und Relationen. Wir sagen, (A, D) ist in SNF, falls

$$D = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_r \end{pmatrix}$$

mit $d_{i+1} \mid d_i$ für $1 \leq i < r$, $0 \leq d_i$ und $d_i \neq 1$ für $1 \leq i \leq r$.

Der folgende Algorithmus berechnet zu einem System (G, M) von Erzeugern und Relationen für $\mathcal{A}$ eine SNF (A, D) für $\mathcal{A}$ sowie eine Matrix U_a zur Berechnung von diskreten Logarithmen. Zusätzlich setzen wir $|\mathcal{A}| < \infty$ voraus. Sei $n := |G|$.

1. **HNF Schritt:** Berechne die HNF $(0 \mid H)$ von M.
2. **SNF Schritt:** Berechne $U, V \in \mathrm{Gl}_n(\mathbb{Z})$, so dass $UHV = D'$ in SNF ist. Setze
$$A' = (\alpha_1, \ldots \alpha_m, \alpha_{n+1}, \ldots \alpha_r) := GU^{-1},$$
wobei m in Schritt 3 definiert ist.
3. **Lösche triviale Komponenten:** Sei
$$\begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_m & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$
mit $d_m \neq 1$. Setze dann $D := \mathrm{diag}(d_1, \ldots, d_m)$, $A := (\alpha_1, \ldots \alpha_m)$. Ferner sei U_a die Matrix der ersten m Zeilen von U.
4. **Ausgabe:** Gib (A, D) und U_a aus.

Es gilt dann $AU_a = G$, d.h., die alten Erzeuger können mit der Matrix U_a durch die neuen Erzeuger in A ausgedrückt werden.

Sprechweise: Sei $\mathcal{A}$ eine endliche abelsche Gruppe. Wir sagen, dass $\mathcal{A}$ effektiv berechnet ist, wenn

- wir eine System (G, M) von Erzeugern und Relationen haben, oder äquivalent, eine SNF (A, D).
- wir einen effektiven Algorithmus haben, der zu $\alpha \in \mathcal{A}$ ein $X \in \mathbb{Z}^{|A|}$ berechnet mit $\alpha = AX$. Wir nennen X den diskreten Logarithmus von α bezüglich A.

Sprechweise: Sei $\psi \colon \mathcal{A} \longrightarrow \mathcal{B}$ ein Homomophismus von effektiv berechneten (endlichen) abelschen Gruppen. Seien $(A, D_{\mathcal{A}})$ und $(B, D_{\mathcal{B}})$ jeweils Erzeugende und Relationen in SNF. Wir sagen, dass ψ effektiv berechnet ist, wenn man

1. zu $\alpha \in \mathcal{A}$ das Element $\psi(\alpha)$ in der Form $\psi(\alpha) = BY$ mit berechenbarem $Y \in \mathbb{Z}^{|B|}$ schreiben kann.
2. zu $\beta \in \psi(\mathcal{A})$ ein $\alpha \in \mathcal{A}$ berechnen kann mit $\psi(\alpha) = \beta$.

1.9 Ein Algorithmus zur Berechnung von Quotienten

Sei

$$\mathcal{A} \xrightarrow{\psi} \mathcal{B} \xrightarrow{\phi} \mathcal{C} \longrightarrow 1$$

eine exakte Sequenz von (endlichen) abelschen Gruppen. Wir setzen voraus, dass $\mathcal{A}, \mathcal{B}$ effektiv berechnet sind. Zusätzlich brauchen wir, dass ψ und ϕ folgende Bedingungen erfüllen:

1. Zu $\alpha \in \mathcal{A}$ kann man $\psi(\alpha)$ in der Form $\psi(\alpha) = BY$ mit berechenbarem $Y \in \mathbb{Z}^{|B|}$ schreiben. Dies ist im Wesentlichen das DL-Problem in $\mathcal{B}$.
2. Zu $\gamma \in \varphi(\mathcal{C})$ kann man $\beta \in \mathcal{B}$ berechnen kann mit $\varphi(\beta) = \gamma$.

Sei $C' := \varphi(B)$. Dann ist C' ein Erzeugendensystem von $\mathcal{C}$. Sei $P \in \mathbb{Z}^{|B| \times |A|}$, so dass

$$\psi(A) = (\psi(\alpha_1), \dots, \psi(\alpha_2) = BP$$

gilt. Da wir in $\mathcal{B}$ das DL-Problem lösen können, ist P berechenbar.
Sei nun $V \in \mathbb{Z}^{|C'|}$ eine Relation, d.h. $C'V = 1_{\mathcal{C}}$. Es gilt:

$$C'V = 1_{\mathcal{C}} \iff V \in \operatorname{Im}(P \mid D_{\mathcal{B}}).$$

Also ist $(\phi(B), (P \mid D_{\mathcal{B}})$ ein System von Erzeugern und Relationen, aus dem wir eine SNF $(C, D_{\mathcal{C}})$ berechnen können.
Wir fassen zusammen:

1. **DL Schritt:** Mit dem DL-Algorithmus in $\mathcal{B}$ berechne P mit $\psi(A) = BP$.
2. **SNF Schritt:** Berechne die SNF zu $(\phi(B), (P \mid D_{\mathcal{B}})$ und gib $(C, D_{\mathcal{C}})$ sowie die Matrix U_a aus.

Damit $\mathcal{C}$ effektiv berechnet ist, müssen wir noch einen Algorithmus zur Berechnung des DL-Problems in $\mathcal{C}$ angeben. Sei $\gamma \in \mathcal{C}$ und $\phi(\beta) = \gamma$. Wegen der zweiten Voraussetzung können wir β berechnen. Da wir das DL-Problem in $\mathcal{B}$ lösen können, finden wir $X \in \mathbb{Z}^{|B|}$ mit $\beta = BX$. Dann gilt

$$\gamma = \phi(\beta) = \phi(BX) = \phi(B)X = C'X = CU_aX.$$

Also ist U_aX der DL von γ bezüglich dem Erzeugendensystem C von $\mathcal{C}$.

1.10 Ein Algorithmus zur Berechnung von Gruppenerweiterungen

Seien $\mathcal{A}$ und $\mathcal{C}$ zwei endliche abelsche Gruppen, die effektiv berechnet sind. Seien $(A, D_{\mathcal{A}})$ und $(C, D_{\mathcal{C}})$ Erzeugende und Relationen in SNF. Sei

$$1 \longrightarrow \mathcal{A} \xrightarrow{\psi} \mathcal{B} \xrightarrow{\phi} \mathcal{C} \longrightarrow 1$$

eine exakte Sequenz abelscher Gruppen. Zusätzlich setzen wir voraus:

(i) Zu $\gamma \in \mathcal{C}$ kann man $\beta \in \mathcal{B}$ berechnen mit $\phi(\beta) = \gamma$.

(ii) Zu $\beta \in \psi(\mathcal{A})$ kann man $\alpha \in \mathcal{A}$ mit $\psi(\alpha) = \beta$ berechnen.

Wir wollen $\mathcal{B}$ effektiv berechnen. Hier ist der Algorithmus.

1. **Berechne Erzeugende:** Berechne mittels (i) B' mit $\phi(B') = C$ sowie $\psi(A)$.

2. **DL Schritt:** Setze $B'' := B'D_{\mathcal{C}} = (\beta''_1, \ldots, \beta''_{|C|})$ und $A'' = (\alpha''_1, \ldots, \alpha''_{|C|})$ mit $\psi(\alpha''_i) = \beta''_i$. Dies ist möglich wegen (ii). Berechne mit dem DL-Algorithmus in $\mathcal{A}$ eine Matrix $P \in \mathbb{Z}^{|A| \times |C|}$ mit $A'' = AP$.

3. **SNF Schritt:** Setze $G := (\psi(A) \mid B')$ und $M := \begin{pmatrix} D_{\mathcal{A}} & -P \\ 0 & D_{\mathcal{C}} \end{pmatrix}$. Dann ist (G, M) eine Darstellung von $\mathcal{B}$ durch Erzeugende und Relationen. Berechne hiervon die SNF $(B, D_{\mathcal{B}})$ sowie die Matrix U_a.

Zur Lösung des DL-Problems in $\mathcal{B}$: Sei $\beta \in \mathcal{B}$ gegeben. Da wir den diskreten Logarithmus in $\mathcal{C}$ berechnen können, kann man Y mit $\phi(\beta) = CY = \phi(B')Y$ berechnen. Dann ist $\beta - B'Y \in \ker(\phi) = \mathrm{im}(\psi)$, so dass wir wegen (ii) ein $\alpha \in \mathcal{A}$ mit $\psi(\alpha) = \beta - B'Y$ berechnen können. Mit dem DL-Algorithmus in $\mathcal{A}$ berechnen wir X mit $\alpha = AX$. Dann gilt $\beta = \psi(A)X + B'Y$, d.h. wir können β als Linearkombination der Erzeugenden $G = (\psi(A) \mid B')$ darstellen. Mit der Matrix U_a kann man jetzt den diskreten Logarithmus bezüglich der SNF $(B, D_{\mathcal{B}})$ berechnen.

1.11 Weitere Algorithmen für e-e abelsche Gruppen

Für weitere Algorithmen dieser Art sei auf das Buch von Cohen verwiesen. Insbesondere kann man für eine exakte Sequenz endlicher abelscher Gruppen

$$\mathcal{A} \xrightarrow{\psi} \mathcal{B} \xrightarrow{\phi} \mathcal{C} \xrightarrow{\pi} \mathcal{D} \longrightarrow 1$$

und der effektiven Kenntnis von $\mathcal{A}, \mathcal{B}, \mathcal{D}$ (+ gewisser Anforderungen an ψ, ϕ und π) die Gruppe $\mathcal{C}$ effektiv berechnen.

2 Zahlkörper

2.1 Darstellung von algebraischen Zahlen

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

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

die Einbettungen $K \hookrightarrow \mathbb{C}$. Hierbei bezeichnen $\sigma_1, \ldots, \sigma_{r_1}$ die reellen Einbettungen und $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$ 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

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

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 $\theta_1, \ldots, \theta_n$ gegeben ist. Zum Beispiel ist für $K = \mathbb{Q}[X]/(f(X) = \mathbb{Q}(\alpha)$ eine solche Basis durch $1, \alpha, \ldots, \alpha^{n-1}$ 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 $\theta_1, \ldots, \theta_n$ 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 $\theta_1, \ldots, \theta_n$. 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.
Als Beispiel haben wir die Erzeugung des Hilbertschen Zahlkörpers $K(1)/K$ für einen imaginärquadratischen Körper K betrachtet. Hier gilt $K(1) = K(j(\mathcal{O}_K))$ und die Konjugierten von $j(\mathcal{O}_K)$ sind in natürlicher Weise durch komplexe Zahlen gegeben, die man nur approximativ berechnen kann. Literatur hierzu:

- H. Cohen, Advanced Topics in Computational Number Theory, Chapter 3
- Silverman, Advanced topics in the arithmetic of elliptic curves
- Schertz, Complex multiplication

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 Ordnungen und Ideale

Definition 2.3.1 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 2.3.2 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 2.3.3 *Sei I ein gebrochenes Ideal und $I' := \{\alpha \in K \mid \alpha I \subseteq R\}$. Dann gilt:*

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

2.4 Darstellung von Moduln und Idealen

Definition 2.4.1 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

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

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 2.4.2 *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.*

Zum Beweis verwenden wir den sogenannten schwachen Approximationssatz:

Satz 2.4.3 *Sei $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ eine endliche Menge von maximalen Idealen von $\mathcal{O}_K$ und sei $e_1, \dots, e_r \in \mathbb{Z}_{\geq 0}$. Dann gibt es ein $\beta \in \mathcal{O}_K$ mit $v_{\mathfrak{p}_i}(\beta) = e_i$ für $i = 1, \dots, r$.*

3 Grundlegende Algorithmen in Dedekindringen

3.1 Verallgemeinerter euklidischer Algorithmus

Sei R ein Dedekindring. In aller Regel stellen wir uns R als den Ring der ganzen Zahlen in einem Zahlkörper vor. Dann ist R ein e-e $\mathbb{Z}$-Modul und wir können Resultate aus der Theorie der e-e $\mathbb{Z}$-Moduln benutzen. Ebenso kann man sich auch einen Dedekindring R vorstellen, der über einem Polynomring $k[T]$, wobei k ein Körper ist, vorstellen. Hier können wir dann die Modultheorie für e-e $k[T]$-Moduln verwenden.

Proposition 3.1.1 *Seien $\mathfrak{a}, \mathfrak{b}$ ganze Ideale in R mit $\mathfrak{a} + \mathfrak{b} = R$. Dann kann man in polynomialer Zeit Elemente $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ mit $a + b = 1$ berechnen.*

Satz 3.1.2 *Seien $\mathfrak{a}, \mathfrak{b} \in I_R$ zwei gebrochene Ideale, $a, b \in K$ und es gelte $(a, b) \neq (0, 0)$. Sei $\mathfrak{d} := a\mathfrak{a} + b\mathfrak{b}$. Dann gibt es $u \in \mathfrak{a}\mathfrak{d}^{-1}$ und $v \in \mathfrak{b}\mathfrak{d}^{-1}$ mit $u + v = 1$. Die Elemente u und v können in polynomialer Zeit berechnet werden.*

Der folgende Satz ist eine geringfügige Verallgemeinerung des obigen schwachen Approximationssatzes. Auch hierfür kann man einen polynomialen Algorithmus angeben, der im wesentlichen auf Proposition 3.1.1 beruht.

Satz 3.1.3 *Sei $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ eine endliche Menge von maximalen Idealen von R und sei $e_1, \dots, e_r \in \mathbb{Z}$. Dann gibt es ein $\beta \in R$ mit $v_{\mathfrak{p}_i}(\beta) = e_i$ für $i = 1, \dots, r$ und $v_{\mathfrak{p}}(\beta) \geq 0$ für alle $\mathfrak{p} \notin S$. Das Element β kann in polynomialer Zeit berechnet werden.*

Satz 3.1.4 *(Stärkerer Approximationssatz) Sei S eine endliche Menge von Primidealen in R, $(e_{\mathfrak{p}})_{\mathfrak{p} \in S} \in \mathbb{Z}^{|S|}$ und $(x_{\mathfrak{p}})_{\mathfrak{p} \in S} \in K^{|S|}$. Dann gibt es ein $x \in K$ mit*

$$v_{\mathfrak{p}}(x - x_{\mathfrak{p}}) = e_{\mathfrak{p}}, \forall \mathfrak{p} \in S, \quad v_{\mathfrak{p}}(x) \geq 0, \forall \mathfrak{p} \notin S.$$

Das Element x kann in polynomialer Zeit berechnet werden.

Der Beweis hierfür konnte bislang nicht geführt werden.

3.2 Die HNF in Dedekindringen

Satz 3.2.1 *Sei M ein e-e torsionsfreier R-Modul und $V = KM$. Dann gibt es $\omega_1, \ldots, \omega_n \in V$ und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \in I_R$, so dass*

$$M = \mathfrak{a}_1\omega_1 \oplus \ldots \oplus \mathfrak{a}_n\omega_n.$$

Falls $M = \mathfrak{a}_1'\omega_1' \oplus \ldots \oplus \mathfrak{a}_n'\omega_n'$, so stimmen die Klassen von

$$\mathfrak{a} := \mathfrak{a}_1 \cdots \mathfrak{a}_n \text{ und } \mathfrak{a}' := \mathfrak{a}_1' \cdots \mathfrak{a}_n'$$

in der Klassengruppe cl_R überein.

Definition 3.2.2 Setze $\mathrm{St}(M) :=$ Klasse von $\mathfrak{a}$. Dann nennt man $\mathrm{St}(M)$ die Steinitzklasse von M.

Für zwei e-e torsionsfreie R-Moduln gilt: $N \simeq M \iff \mathrm{rg}(N) = \mathrm{rg}(M)$ und $\mathrm{St}(N) = \mathrm{St}(M)$.

Definition 3.2.3 Sei M ein e-e torsionsfreier R-Modul und $V = KM$.

1. Sei $0 \neq \omega \in V$ und $\mathfrak{a} \in I_R$. Dann nennen wir die Äquivalenzklasse des Paares $(\mathfrak{a}, \omega)$ ein Pseudoelement, wobei wir definieren:

$$(\mathfrak{a}, \omega) \sim (\mathfrak{b}, \eta) :\iff \mathfrak{a}\omega = \mathfrak{b}\eta.$$

2. Das Pseudoelement $(\mathfrak{a}, \omega)$ heißt ganz, falls $\mathfrak{a}\omega \subseteq M$.

3. Seien $(\mathfrak{a}_i, \omega_i), i = 1, \ldots, k$, Pseudoelemente. Dann nennt man $\{(\mathfrak{a}_i, \omega_i) : i = 1, \ldots, k\}$ ein Pseudoerzeugendensystem, falls

$$M = \mathfrak{a}_1\omega_1 + \ldots + \mathfrak{a}_k\omega_k.$$

4. Seien $(\mathfrak{a}_i, \omega_i), i = 1, \ldots, k$, Pseudoelemente. Dann nennt man $\{(\mathfrak{a}_i, \omega_i) : i = 1, \ldots, k\}$ eine Pseudobasis, falls

$$M = \mathfrak{a}_1\omega_1 \oplus \ldots \oplus \mathfrak{a}_k\omega_k.$$

Wegen Satz 3.2.1 besitzt jeder e-e torsionsfreie R-Modul M eine Pseudobasis. Die folgende Proposition beschreibt den Übergang zwischen zwei Pseudobasen.

Proposition 3.2.4 *Sei*

$$M = \bigoplus_{i=1}^{n} \mathfrak{a}_i\omega_i = \bigoplus_{j=1}^{n} \mathfrak{b}_j\eta_j.$$

Sei $(\eta_1, \ldots, \eta_n) = (\omega_1, \ldots, \omega_n)U$ mit einer Matrix $U \in \mathrm{Gl}_n(K)$. Seien $\mathfrak{a} := \mathfrak{a}_1 \cdots \mathfrak{a}_n$ und $\mathfrak{b} := \mathfrak{b}_1 \cdots \mathfrak{b}_n$. Dann gilt $u_{ij} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$ und $\mathfrak{a} = \det(U)\mathfrak{b}$.
Sei umgekehrt $M = \bigoplus_{i=1}^n \mathfrak{a}_i\omega_i$. Seien weiter $\mathfrak{b}_1, \ldots, \mathfrak{b}_n \in I_R$ und $U \in \mathrm{Gl}_n(K)$ gegeben. Es gelte $\mathfrak{a} = \det(U)\mathfrak{b}$ und $u_{ij} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$. Definiert man dann $\eta_1, \ldots, \eta_n$ durch $(\eta_1, \ldots, \eta_n) = (\omega_1, \ldots, \omega_n)U$, dann gilt

$$M = \bigoplus_{j=1}^{n} \mathfrak{b}_j\eta_j.$$

Definition 3.2.5

1. Eine Pseudomatrix ist ein Paar (A, I), wobei $A \in K^{n \times k}$ und $I = (\mathfrak{a}_1, \ldots, \mathfrak{a}_k), \mathfrak{a}_j \in I_R$.

2. Man nennt $M := \sum_{j=1}^{k} \mathfrak{a}_j A_j \subseteq K^n$ den von (A, I) erzeugten R-Modul. Hierbei bezeichnet wie üblich A_j die j-te Spalte der Matrix A.

   Die Abbildung

$$f\colon \mathfrak{a}_1 \oplus \ldots \oplus \mathfrak{a}_k \longrightarrow M, \quad (a_1, \ldots, a_k) \mapsto \sum_{j=1}^{k} a_j A_j,$$

   nennt man die von (A, I) induzierte Abbildung.

3. $\ker(f)$ nennt man den Kern von (A, I).

Satz 3.2.6 *Sei (A, I) eine Pseudomatrix. Sei $\mathrm{rg}(A) = n$ und M der von (A, I) erzeugten R-Modul. Dann gibt es Ideale $\mathfrak{b}_1, \ldots, \mathfrak{b}_k \in I_R$ und eine Matrix $U = (u_{ij}) \in \mathrm{Gl}_k(K)$ mit den folgenden Eigenschaften:*

1. $u_{ij} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}, \forall 1 \le i, j \le k$.

2. $\mathfrak{a} = \det(U)\mathfrak{b}$, *wobei* $\mathfrak{a} := \mathfrak{a}_1 \cdots \mathfrak{a}_k$ *und* $\mathfrak{b} := \mathfrak{b}_1 \cdots \mathfrak{b}_k$.

3. $AU = (0|H)$ *mit* $H = \begin{pmatrix} 1 & * & * & \ldots & * \\ & 1 & * & \ldots & * \\ & & \ddots & & \\ & & & & 1 \end{pmatrix}$

4. *Sei* $\mathfrak{c}_j = \mathfrak{b}_{k-n+1}, j = 1, \ldots, n$ *und seien* $\omega_j = H_j, j = 1, \ldots, n$ *die entsprechenden Spalten von* H. *Dann gilt*

$$M = \mathfrak{c}_1\omega_1 \oplus \ldots \oplus \mathfrak{c}_n\omega_n,$$

   d.h. $(\mathfrak{c}_j, \omega_j)_{j=1,\ldots,n}$ *ist eine Pseudobasis von* M.

5. $(U_j, \mathfrak{b}_j)_{1 \le j \le k-n}$ *ist eine Pseudobasis von* $\ker(f)$.

Der Beweis wurde in Form eines Algorithmus erbracht, siehe [Cohen, Advanced Topics, Algorithmus 1.4.7].

Proposition 3.2.7 *Sei S_{ij} ein Vertretersystem von $K/\mathfrak{c}_i\mathfrak{c}_j^{-1}$. Dann kann man oE für alle $j > i$ annehmen, dass $h_{ij} \in S_{ij}$. In diesem Fall ist dann die Matrix H eindeutig.*

Literatur: Biasse, Fieker, Hofmann, J.Symb.Comp. (2017), On the computation of the HNF over the ring of integers of a number field.

3.3 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 3.3.1 *Es gibt ein $a \in K \setminus \mathcal{O}_K$ mit $a\mathfrak{p} \subseteq \mathcal{O}_K$. Für jedes solche a gilt:*

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

Es gilt dann:

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

3.4 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 3.4.1 *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 3.4.2 $\mathcal{O}_K^*$ ist die sogenannte inverse Differente oder Kodifferente.

4 Berechnung der Maximalordnung

4.1 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 4.1.1 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 4.1.2 *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 4.1.3 *(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.

4.2 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 4.2.1 *(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*

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

4.3 Der Round2-Algorithmus

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

Lemma 4.3.1 *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 4.3.2 *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.

5 Berechnung von Klassengruppe, Regulator und Fundamentaleinheiten

5.1 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 5.1.1 $h_K < \infty$.

Satz 5.1.2 *$U(K) = \mu(K) \times \eta_1^{\mathbb{Z}} \times \ldots \times \eta_{r_u}^{\mathbb{Z}}$ 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 5.1.3 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 5.1.4 Diese Definition ist unabhängig von der Wahl der Fundamentaleinheiten sowie der Wahl der zu streichenden Spalte.

5.2 Berechnung von $\mu(K)$

Lemma 5.2.1 *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.‘

5.3 Die Dedekindsche Zeta-Funktion

Definition 5.3.1 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 5.3.2 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 5.3.3 *(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*

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

5.4 Idealreduktion

Definition 5.4.1 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 5.4.2 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 5.4.3 *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.

5.5 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

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

5.6 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.

5.7 Unabhängige Einheitensysteme

Lemma 5.7.1 *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 5.7.2 *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.

5.8 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 5.5 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 5.7 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 $\eta_1, \ldots, \eta_{r_u}$.