Algorithmische Zahlentheorie

gelesen von Prof. Dr. Werner Bley

Mitschrift von Stefan Albrecht

Ludwig-Maximilians-Universität München – Wintersemester 2025/26

Inhaltsverzeichnis

0 Überblick

Lecture 1
Oct 14, 2025

Sei $K/\mathbb{Q}$ ein Zahlkörper, also eine endliche Körpererweiterung. Sei $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$ in K, der sog. *Ring der ganzen Zahlen* von K

$$\begin{tikzcd} K \arrow[r, hookleftarrow] \arrow[d, dash, "n"] & \mathcal{O}_K \arrow[d, dash] \\ \mathbb{Q} \arrow[r, hookleftarrow] & \mathbb{Z} \end{tikzcd}$$

$\mathcal{O}_K$ ist ein Dedekindring, d.h. noethersch, ganz abgeschlossen (=normal) und eindimensional, d.h. jedes nicht-Null-Ideal ist maximal.

Ein Ziel dieser Vorlesung wird sein, $\mathcal{O}_K$ zu berechnen. $\mathcal{O}_K$ ist ein freier $\mathbb{Z}$-Modul vom Rang n. Man will also $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ bestimmen, sodass $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \ldots \oplus \mathbb{Z}\omega_n$. Dazu brauchen wir Algorithmen für endlich erzeugte $\mathbb{Z}$-Moduln (d.h. abelsche Gruppen).

Beispiel 0.1. (1) Sei $K = \mathbb{Q}(i) \supseteq \mathcal{O}_K = \mathbb{Z}[i]$. $\mathbb{Z}[i]$ ist euklidisch, also insbesondere ein Hauptidealring.

(2) $K = \mathbb{Q}(\sqrt{-5}) \supseteq \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring.

Um zu untersuchen, wie "weit"$\mathcal{O}_K$ davon entfernt ist, ein Hauptidealring zu sein, untersucht man

Definition 0.2. Die Klassengruppe eines Zahlkörpers ist $\mathrm{cl}_K := I_K/P_K$, wobei I_K die Gruppe der gebrochenen Ideale $\neq 0$ (mit dem Produkt von Idealen als Produkt), und P_K die Untergruppe der Hauptideale ist.

$\mathcal{O}_K$ ist ein Hauptidealring genau dann, wenn $\mathrm{cl}_K = 1$. In der Algebraischen Zahlentheorie zeigt man, dass cl_K eine endliche Gruppe ist. Ein weiteres Ziel dieser Vorlesung wird sein, diese Klassengruppe zu berechnen, d.h. gemäß dem Elementarteilersatz $d_1 \mid d_2 \mid \ldots \mid d_r$, $d_i \in \mathbb{N}_{>1}$ mit $\mathrm{cl}_K \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \mathbb{Z}/d_r\mathbb{Z}$.

Schließlich wollen wir die Einheitengruppe von $\mathcal{O}_K$ berechnen.

Theorem 0.3 (Dirichlet)**.** *$\mathcal{O}_K^\times$ ist eine endlich erzeugte abelsche Gruppe, d.h. es existiert eine Einheitswurzel ζ und $\varepsilon_1, \ldots, \varepsilon_r$ mit*

$$\mathcal{O}_K^\times \ni u = \zeta^{k_0}\varepsilon_1^{k_1} \cdots \varepsilon_r^{k_r}$$

mit $k_1, \ldots, k_r \in \mathbb{Z}$ und $k_0 \in \mathbb{Z}/\operatorname{ord}(\zeta)$ eindeutig.

1 Lineare Algebra über $\mathbb{Z}$

1.1 $\mathbb{Z}$-Moduln

Konvention Alle Z-Moduln sind endlich erzeugt, d.h. falls V ein Z-Modul ist, so gibt es $v_1, \dots, v_n$ mit $V \ni v = \sum_{i=1}^n a_i v_i$, $a_i \in \mathbb{Z}$.

Theorem 1.1 (Hauptsatz über endlich erzeugte abelsche Gruppen)**.** *Sei V ein endlich erzeugter Z-Modul.*

(1) $V_{tors} := \{v \in V \mid \exists a \in \mathbb{Z} \setminus \{0\} : av = 0\}$ ist eine endliche Gruppe und es gilt $V_{tors} \oplus \mathbb{Z}^r$; $\operatorname{rg}(V) := r$ heißt Rang von V. Mit anderen Worten: Es gibt $v_1, \dots, v_n \in V$, so dass jedes $v \in V$ eine eindeutige Darstellung der Form $v = t + \sum_{i=1}^n a_i v_i$ mit $t \in V_{tors}$ und $a_i \in \mathbb{Z}$ hat.

(2) Sei $W \subseteq V$ ein Untermodul. Dann ist W endlich erzeugt und es gilt $\operatorname{rg}(W) \leq \operatorname{rg}(V)$.

(3) Sei $W \subseteq V$ und V ein freier $\mathbb{Z}$-Modul. Dann ist auch W frei.

(4) Falls $|V| < \infty$, so gibt es einen freien $\mathbb{Z}$-Modul $L \subseteq \mathbb{Z}^n$ für geeignetes $n \in \mathbb{N}$ mit $\mathbb{Z}^n/L \cong V$.

Beweis. Nur (4): Sei $v_1, \dots, v_n$ ein Erzeugendensystem von V. Dann ist

$$\pi : \mathbb{Z}^n \to V, \quad x \mapsto \sum_{i=1}^n x_i v_i$$

surjektiv. Sei $L := \ker \pi$, dann ist L frei nach (3), und nach dem Isomorphiesatz ist $\mathbb{Z}^n/L \cong V$. □

Definition 1.2. Ein $\mathbb{Z}$-Gitter L ist ein torsionsfreier (endlich erzeugter) $\mathbb{Z}$-Modul, d.h. $L \cong \mathbb{Z}^{\operatorname{rg}(L)}$.

Bemerkung 1.3. Sei L ein Gitter und $m = \operatorname{rg}(L)$. Sei $v_1, \dots, v_m$ eine $\mathbb{Z}$-Basis und $W \subseteq L$ ein Teilmodul. Dann kann W durch eine Matrix $M \in \mathbb{Z}^{m \times n}$ repräsentiert werden, d.h. die Spalten von M entsprechen Elementen von W.

Ziel ist es nun, eine standardisierte Form für solche Matrizen M zu finden.

1.2 Hermitesche Normalform (HNF)

Definition 1.4. Eine Matrix $M = (m_{ij}) \in \mathbb{Z}^{m \times n}$ ist in HNF, falls es eine streng monoton wachsende Abbildung $f : \{r+1, \dots, n\} \to \{1, \dots, m\}$ mit $r \leq n$ gibt, die folgende Eigenschaften erfüllt:

(a) Für $r + 1 \leq j \leq n$ gilt $m_{f(j),j} \geq 1$, für $i > f(j)$ ist $m_{ij} = 0$, und für $k > j$ gilt $0 \leq m_{f(j),k} < m_{f(j),j}$.

(b) Die ersten r Spalten von M sind 0.

Konkret:

$$M = \left(\begin{array}{c|cccc} & * & * & * & * \\ 0 & * & <* & \dots & \ddots \\ 0 & 0 & * & <* & \\ & 0 & 0 & * & \end{array}\right)$$

Beispiel 1.5. $M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ korrespondiert zu $W = \langle \binom{1}{4}, \binom{2}{5}, \binom{3}{6} \rangle \subseteq \mathbb{Z}^2$. Durch elementare Spaltenumformungen (die nicht den Modul verändern) erhalten wir

$$M \to \begin{pmatrix} 2 & 3 & 1 \\ 5 & 6 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 \\ 1 & 2 & 4 \end{pmatrix} \to \begin{pmatrix} 2 & 1 & 1 \\ 2 & 4 & 1 \end{pmatrix} \to \begin{pmatrix} 0 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

in HNF ($r = 1, f(2) = 1, f(3) = 2$)

Bemerkung 1.6. Sei $n \geq m$ und $W \subseteq \mathbb{Z}^m$ von vollem Rang. Dann hat M eine HNF von der Form $(0 \mid A)$, wobei A eine obere Dreiecksmatrix mit positiven Diagonaleinträgen ist.

Theorem 1.7. *Sei $M \in \mathbb{Z}^{m \times n}$. Dann gibt es eine eindeutig bestimmte Matrix B in HNF von der Form $B = (0 \mid H) = MU$, $U \in \mathrm{GL}_n(\mathbb{Z})$*

Beweis. Spaltentransformationen entsprechen Multiplikation von rechts mit Elementarmatrizen. Eindeutigkeit ist aufwendiger. □

Bemerkung 1.8. B ist eindeutig, U jedoch nicht!

1.3 Anwendungen

Ganzzahliges Bild von Matrizen Sei $M \in \mathbb{Z}^{m \times n}$. Dann sind die letzten $n-r$ Spalten der HNF von M eine $\mathbb{Z}$-Basis des Bildes von M.

Ganzzahliger Kern von Matrizen Sei wieder $M \in \mathbb{Z}^{m \times n}$

Theorem 1.9. *Sei $B = (0 \mid H) = MU$ die HNF von M. Dann ist eine $\mathbb{Z}$-Basis von $\ker(M) \subseteq \mathbb{Z}^n$ durch die ersten r Spalten von U gegeben.*

Beweis. Sei U_i die i-te Spalte von U, etc. Dann gilt $B_i = MU_i = 0$ für $1 \leq i \leq r$. D.h. $U_i \in \ker(M)$. Sei umgekehrt $X \in \ker(M)$. Sei $Y := U^{-1}X$, dann ist $MX = 0$ genau dann, wenn $BY = 0$. Löse sukzessive $BY = 0$ von unten nach oben. Es folgt: Die letzten $n - r$ Einträge von Y sind 0, während die ersten r Einträge beliebig sind. D.h. $X = UY$ ist eine Linearkombination der ersten r Spalten von U. □

Beispiel 1.10. Wir wollen den Kern von $M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ berechnen.

$$\begin{pmatrix} M \\ I_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(132)} \begin{pmatrix} 2 & 3 & 1 \\ 5 & 6 & 4 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \xrightarrow{s_1, s_2 - s_3} \begin{pmatrix} 1 & 2 & 1 \\ 1 & 2 & 4 \\ -1 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\xrightarrow{(132)} \begin{pmatrix} 2 & 1 & 1 \\ 2 & 4 & 1 \\ -1 & 1 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \xrightarrow[s_2 \cdot (-1)]{s_1 - 2s_3, s_2 - 4s_3} \begin{pmatrix} 0 & 3 & 1 \\ 0 & 0 & 1 \\ 1 & -5 & -1 \\ -2 & 4 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Folglich ist $\ker(M) = \langle (1, -2, 1)^t \rangle$