

Algorithmische Zahlentheorie

gelesen von Prof. Dr. Werner Bley

Mitschrift von Stefan Albrecht

Ludwig-Maximilians-Universität München – Wintersemester 2025/26

Inhaltsverzeichnis

0	Überblick	2
1	Lineare Algebra über \mathbb{Z}	3
1.1	\mathbb{Z} -Moduln	3
1.2	Hermiteische Normalform (HNF)	3
1.3	Anwendungen	4
1.4	Smith Normalform (SNF)	5

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

$$\begin{array}{ccc} K & \longleftrightarrow & \mathcal{O}_K \\ \downarrow n & & \downarrow \\ \mathbb{Q} & \longleftrightarrow & \mathbb{Z} \end{array}$$

\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 $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ bestimmen, sodass $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_n$. 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 $\text{cl}_K := I_K/P_K$, 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 $\text{cl}_K = 1$. 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 $d_1 \mid d_2 \mid \dots \mid d_r$, $d_i \in \mathbb{N}_{>1}$ mit $\text{cl}_K \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_r\mathbb{Z}$.

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 $\varepsilon_1, \dots, \varepsilon_r$ mit

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

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

1 Lineare Algebra über \mathbb{Z}

1.1 \mathbb{Z} -Moduln

Konvention Alle \mathbb{Z} -Moduln sind endlich erzeugt, d.h. falls V ein \mathbb{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 \mathbb{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 $V_{tors} \oplus \mathbb{Z}^r$; $\text{rg}(V) := r$ 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 $\text{rg}(W) \leq \text{rg}(V)$.
- (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

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

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

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

Bemerkung 1.3. Sei L ein Gitter und $m = \text{rg}(L)$. 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 $f : \{r+1, \dots, n\} \rightarrow \{1, \dots, m\}$ 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 $W = \langle \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \end{pmatrix} \rangle \subseteq \mathbb{Z}^2$. Durch elementare Spaltenumformungen (die nicht den Modul verändern) erhalten wir

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

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 $B = (0 \mid H) = MU, U \in \text{GL}_n(\mathbb{Z})$

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

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 $\langle M \rangle_{\mathbb{Z}}$ 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 . \square

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

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

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

Test auf Gleichheit von zwei \mathbb{Z} -Gittern in \mathbb{Z}^m Seien L_1, L_2 \mathbb{Z} -Gitter in \mathbb{Z}^m gegeben durch $A_1 \in \mathbb{Z}^{m \times n_1}, A_2 \in \mathbb{Z}^{m \times n_2}$. Sind $(0 \mid H_1), (0 \mid H_2)$ die HNF von A_1 bzw. A_2 , dann ist $L_1 = L_2$ genau dann, wenn $H_1 = H_2$.

Summe von zwei \mathbb{Z} -Moduln in \mathbb{Z}^m Allgemeiner, sei $L \subseteq \mathbb{Q}^m$ ein \mathbb{Z} -Modul. Sei $d \in \mathbb{N}$ minimal mit $dL \subseteq \mathbb{Z}^m$. Unter der HNF von L versteht man das Paar $(\text{HNF}(dL), d)$.

Seien L_1, L_2 \mathbb{Z} -Moduln gegeben durch $W_1, W_2 \in \mathbb{Q}^{m \times n_1}$. Seien $((0 \mid H_i), d_i)$ die HNF von $L_i, i = 1, 2$. Sei $D = \text{kgV}(d_1, d_2)$ und betrachte die Matrix $(\frac{D}{d_1}H_1 \mid \frac{D}{d_2}H_2) \in \mathbb{Z}^{m \times \dots}$ und berechne hiervon wieder die HNF $(0 \mid H)$. Dann sind die Spalten von H eine Basis von $D(L_1 + L_2)$, d.h. die Spalten von $\frac{1}{D}H$ sind eine \mathbb{Z} -Basis von $L_1 + L_2$.

Inklusionstest Seien L_1, L_2 zwei \mathbb{Z} -Moduln. Dann ist $L_1 \subseteq L_2$ genau dann, wenn $L_1 + L_2 = L_2$, was wir durch die letzten beiden Anwendungen testen kann. Alternativ löse man ein lineares Gleichungssystem über \mathbb{Z} . Das geht algorithmisch wie folgt: Ohne Einschränkung seien L_1, L_2 gegeben durch Matrizen $M_1 \in \mathbb{Z}^{m \times n_1}, M_2 \in \mathbb{Z}^{m \times n_2}$. Berechne die HNF $(0 \mid H)$ von M_2 , dann sind die Spalten von H eine \mathbb{Z} -Basis von L_2 , wir müssen also testen, ob jeder Erzeuger e von L_1 sich als ganzzahlige Linearkombination von dieser Basis schreiben lässt. Da H in HNF ist, lässt sich das Gleichungssystem $Hx = e$ einfach schrittweise „von unten nach oben“ auflösen.

1.4 Smith Normalform (SNF)

Sei G eine endliche abelsche Gruppe mit Erzeugendensystem g_1, \dots, g_m . Dann ist die Abbildung $\pi : \mathbb{Z}^m \rightarrow G, e_i \mapsto g_i$ surjektiv, d.h. wir haben eine kurze exakte Sequenz

$$0 \rightarrow L := \ker \pi \rightarrow \mathbb{Z}^m \xrightarrow{\pi} G \rightarrow 0,$$

d.h. $G \cong \mathbb{Z}^m / L$, wobei L ein volles Gitter ist (d.h. vollen Rang hat). Sei $A \in \mathbb{Z}^{m \times n}$ eine zu L korrespondierende Matrix, und $(0 \mid H)$ die HNF von A . Nach Bemerkung 1.6 ist H eine obere Dreiecksmatrix mit positiven Diagonaleinträgen.

Lemma 1.11. $\det(H) = |\mathbb{Z}^m / L| = |G|$.

Beweis. Es reicht zu zeigen, dass $\sum_{i=1}^m k_i e_i, 0 \leq k_i \leq h_{ii} - 1$ ein vollständiges Vertretersystem von \mathbb{Z}^m / L ist. Sei $a \in \mathbb{Z}^m$ gegeben. Man kann zu a ganzzahlige Vielfache der Spalten addieren. Tue dies so von unten nach oben so, dass in jedem Schritt $0 \leq a_i + kh_{ii} < h_{ii}$. Also lässt sich jedes Element von \mathbb{Z}^m / L in der angegebenen Form darstellen.

Angenommen $\sum_{i=1}^m k_i e_i \equiv \sum_{i=1}^m k'_i e_i \pmod{L}$ mit zwei Vektoren wie oben, lies wieder von unten nach oben $Hx = \sum_{i=1}^m (k_i - k'_i) e_i$, um schrittweise $h_{ii} \mid k_i - k'_i$ zu sehen, was aufgrund von $0 \leq k_i, k'_i < h_{ii}$ sofort $k_i = k'_i$ impliziert. \square

Bemerkung 1.12. Allgemeiner gilt $|\det(A)| = |\mathbb{Z}^n / \langle A \rangle_{\mathbb{Z}}|$ für $A \in \mathbb{Z}^{n \times n}$ invertierbar, da für die Hermite Normalform H von A gilt $|\det(H)| = |\det(A)|$ und $\mathbb{Z}^m / H = \mathbb{Z}^m / A$

Bisher haben wir nur Spaltentransformationen durchgeführt, also Rechtsmultiplikationen mit Elementarmatrizen, die die Erzeugenden von L ändern. Nun nutzen wir auch Zeilenumformungen, um die Erzeugenden von \mathbb{Z}^m (bzw. G) zu ändern, korrespondierend zu Linksmultiplikationen.

Definition 1.13. Eine quadratische Matrix $B \in \mathbb{Z}^{m \times m}$ ist in *Smith Normalform* (SNF), falls B eine Diagonalmatrix ist, mit $b_{ii} \geq 0$ für alle i und $b_{i+1,i+1} \mid b_{ii}$ für $i = 1, \dots, m-1$.

Theorem 1.14 (Elementarteilersatz). *Sei $A \in \mathbb{Z}^{m \times m}$ mit $\det(A) \neq 0$. Dann lässt sich A eindeutig durch Zeilen- und Spaltenumformungen in SNF überführen, d.h. gibt es genau eine Matrix $S \in \mathbb{Z}^{m \times m}$ in SNF, sodass es $U, V \in \text{GL}_n(\mathbb{Z})$ gibt mit $S = UAV$.*

Korollar 1.15. *Mit der Notation zu Beginn dieses Abschnitts sei $S = \text{diag}(b_1, \dots, b_m)$ die SNF von H . Dann gilt*

$$G \cong \mathbb{Z}^m / \langle S \rangle_{\mathbb{Z}} \cong \bigoplus_{i=1}^m \mathbb{Z} / b_i \mathbb{Z}.$$

Die sogenannten Invariantenteiler b_i bestimmen G eindeutig bis auf Isomorphie.

Zusammengefasst können wir also nun einen Algorithmus zur Bestimmung des Isomorphietyps einer endlichen abelschen Gruppe G (z.B. $G = \text{cl}_K$) angeben:

Algorithm 1: Isomorphietyp einer endlichen abelschen Gruppe

Input: Ein Erzeugendensystem g_1, \dots, g_m ,

Eine Approximation d von $|G|$ mit $|G| \leq d < 2|G|$.

- 1 Sei $\pi : \mathbb{Z}^m \rightarrow G$, $e_i \rightarrow g_i$ wie oben. Sei $L := \ker \pi$.
 - 2 Bestimme viele Relationen, d.h. Elemente $x \in L$. Bilde eine Matrix $M \in \mathbb{Z}^{m \times n}$ mit diesen Relationen als Spaltenvektoren.
 - 3 Berechne $\text{HNF}(M) = (0 \mid H)$.
 - 4 Falls $\det(H) = 0$ oder $\det(H) > d$, gehe zurück zu 2 und finde mehr Relationen.
 - 5 Berechne die SNF von H und lies die Invariantenteiler ab.
-

Sobald in Schritt 4 $\det(H) \neq 0$ gilt, ist \mathbb{Z}^m / L eine Untergruppe von \mathbb{Z}^m / H . Ist $L \neq H$, dann ist der Index mindestens 2, also $\det(H) \geq 2|G| > d$. Ist also $\det(H) \leq d$, dann ist die volle Gruppe gefunden und man kann mit der SNF fortfahren. Damit ist der Algorithmus korrekt. Natürlich bleibt unklar, wie man ein solches d und Relationen wie in Schritt 2 effizient finden kann, was auch davon abhängt, was über die Gruppe bekannt ist.

Beispiel 1.16. $K = \mathbb{Q}(\sqrt{-6}) \supseteq \mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$. Wegen $-2 \cdot 3 = \sqrt{-6}^2$ ist \mathcal{O}_K kein Hauptidealring, also ist $|\text{cl}_K| \geq 2$. Sei $\mathfrak{p}_2 = \langle 2, \sqrt{-6} \rangle$, $\mathfrak{p}_3 = \langle 3, \sqrt{-6} \rangle$. Aus der Minkowski-Theorie folgt, dass $[\mathfrak{p}_2]$ und $[\mathfrak{p}_3]$ die Gruppe cl_K erzeugen. Man rechnet nach, dass $(2) = \mathfrak{p}_2^2$, $(3) = \mathfrak{p}_3^2$ und $(\sqrt{-6}) = \mathfrak{p}_2 \mathfrak{p}_3$. Das liefert die Matrix von Relationen

$$M = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix} \xrightarrow{\text{HNF}} \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$H = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ hat Determinante 2, erfüllt also das Abbruchkriterium. Wir bringen die Matrix leicht in SNF $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$, d.h. $\text{cl}_K \cong \mathbb{Z}/2\mathbb{Z}$. Wenn man in jedem Schritt die Umformungen protokolliert, erhält man zusätzlich Informationen über minimale Erzeuger und Relationen von cl_K (was in diesem Beispiel natürlich trivial ist).