Protokoll zur Vorlesung Algorithmische Zahlentheorie WS 25/26

W. Bley

29. Oktober 2025

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 $\pi \colon \mathbb{Z}^n \longrightarrow G, (x_1, \ldots, x_n)^t \mapsto x_1 g_1 + \ldots + x_n g_n$ 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 1.7.1 *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 $1 \le i < r$, $0 \le d_i$ und $d_i \neq 1$ für $1 \le i \le r$.

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

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

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:

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

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 Ereugendensystem C von $\mathcal{C}$.