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

$$\begin{array}{ccc} K & \hookleftarrow & \mathcal{O}_K \\ \Big| n & & \Big| \\ \mathbb{Q} & \hookleftarrow & \mathbb{Z} \end{array}$$

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

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*

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

mit $k_1, \dots, k_r \in \mathbb{Z}$ 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 $v_1, \ldots, v_n$ 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 $V_{tors} \oplus \mathbb{Z}^r$; $\mathrm{rg}(V) := r$ heißt Rang von V. Mit anderen Worten: Es gibt $v_1, \ldots, v_n \in V$, 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 $\mathrm{rg}(W) \leq \mathrm{rg}(V)$.

(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 $v_1, \ldots, v_n$ 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. $L \cong \mathbb{Z}^{\mathrm{rg}(L)}$.

Bemerkung 1.3. Sei L ein Gitter und $m = \mathrm{rg}(L)$. Sei $v_1, \ldots, v_m$ 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 $f : \{r+1, \ldots, n\} \to \{1, \ldots, m\}$ 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:

$$M = \begin{pmatrix} & \vert * & * & * & * \\ 0 & \vert * & < * & \ldots & \ddots \\ 0 & \vert 0 & * & < * & \\ & \vert 0 & 0 & * & \end{pmatrix}$$

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 $\langle M \rangle_{\mathbb{Z}}$ 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. □

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

Lecture 2
Oct 21, 2025

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 $(\mathrm{HNF}(dL), d)$.

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 $D = \mathrm{kgV}(d_1, d_2)$ 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 $\pi : \mathbb{Z}^m \to G, e_i \mapsto g_i$ surjektiv, d.h. wir haben eine kurze exakte Sequenz

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

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 $\sum_{i=1}^m k_i e_i$, $0 \le k_i \le h_{ii} - 1$ 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 $0 \le a_i + kh_{ii} < h_{ii}$. Also lässt sich jedes Element von $\mathbb{Z}^m/L$ in der angegebenen Form darstellen.

Angenommen $\sum_{i=1}^m k_i e_i \equiv \sum_{i=1}^m k_i' e_i \bmod L$ 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 $0 \le k_i, k_i' < h_{ii}$ sofort $k_i = k_i'$ impliziert. □

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 for die Hermitsche 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 $b_{ii} \ge 0$ 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 $U, V \in \mathrm{GL}_n(\mathbb{Z})$ gibt mit $S = UAV$.*

Korollar 1.15. *Mit der Notation zu Beginn dieses Abschnitts sei $S = \mathrm{diag}(b_1, \dots, b_m)$ 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. $G = \mathrm{cl}_K$) 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 $\pi : \mathbb{Z}^m \to G,\ e_i \to g_i$ 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 $\mathrm{HNF}(M) = (0 \mid H)$.
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 H eine Untergruppe von L von endlichem Index. 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 $|\,\mathrm{cl}_K\,| \geq 2$. 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

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

$H = \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ hat Determinante 2, erfüllt also das Abbruchkriterium. Wir bringen die Matrix leicht in SNF $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, d.h. $\mathrm{cl}_K \cong \mathbb{Z}/2\mathbb{Z}$. 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).

Lecture 3
Oct 28, 2025

Sei $K/\mathbb{Q}$ ein Zahlkörper und $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ ein Ideal. Dann ist $(\mathcal{O}/\mathfrak{a})^\times$ eine endliche abelsche Gruppe, die wir verstehen wollen. Schreibe $\mathfrak{a} = \mathfrak{p}_i^{e_i} \cdots \mathfrak{p}_r^{e_r}$ für paarweise verschiedene Primideale $\mathfrak{p}_i$. Nach dem Chinesischen Restsatz ist

$$\mathcal{O}_K^\times \cong (\mathcal{O}_K/\mathfrak{p}_1^{e_1})^\times \times \cdots \times (\mathcal{O}_K/\mathfrak{p}_r^{e_r})^\times.$$

Also genügt es, $(\mathcal{O}_K/\mathfrak{p}^e)^\times$ als abelsche Gruppe zu bestimmen. Gehe dazu wiefolgt vor: Betrachte die exakte Sequenz

$$1 \to (1+\mathfrak{p})/(1+\mathfrak{p}^e) \to (\mathcal{O}_K/\mathfrak{p}^e)^\times \to (\mathcal{O}_K/\mathfrak{p})^\times \to 1.$$

Dabei ist $\mathfrak{O}_K/\mathfrak{p}$ ein Körper, also die Einheitengruppe zyklisch; wir brauchen einen Erzeuger. Auf der anderen Seite ist

$$1 \to (1+\mathfrak{p}^2)/(1+\mathfrak{p}^e) \to (1+\mathfrak{p})/(1+\mathfrak{p}^e) \to \underbrace{(1+\mathfrak{p})/(1+\mathfrak{p}^2)}_{\cong \mathfrak{p}/\mathfrak{p}^2} \to 1$$

exakt, wobei $\varphi : \mathfrak{p}/\mathfrak{p}^2 \to (1+\mathfrak{p})/(1+\mathfrak{p}^2)$ gegeben ist durch $[x] \mapsto [1+x]$: Das ist eindeutig eine Bijektion, und

$$\varphi([x]+[y]) = \varphi([x+y]) = [1+x+y] = [1+x+y+xy] = \varphi([x])\varphi([y]).$$

Weiter ist $\mathfrak{p}/\mathfrak{p}^2$ durch die Berechnung von $\mathbb{Z}$-Basen bestimmbar. Nun können wir iterativ fortfahren: In der exakten Sequenz

$$1 \to (\mathfrak{p}^4)/(1+\mathfrak{p}^e) \to (1+\mathfrak{p}^2)/(1+\mathfrak{p}^e) \to (1+\mathfrak{p}^2)/(1+\mathfrak{p}^4) \to 1,$$

wobei der Quotient wie oben isomorph zu der berechenbaren Gruppe $\mathfrak{p}^2/\mathfrak{p}^4$ ist, etc. Somit lassen sich schrittweise alle äußeren Terme der obigen exakten Sequenzen berechnen, und es bleibt die Frage, wie sich diese Terme zusammensetzen lassen.

Notation: Im folgenden sei $\mathcal{A}$ stets eine abelsche Gruppe und $A = (\alpha_1, \ldots, \alpha_r)$ mit $\alpha_i \in \mathcal{A}$ Erzeuger. Ist $X \in \mathbb{Z}^r$, dann ist $AX = \sum_{i=1}^r x_i\alpha_i \in \mathcal{A}$ oder $\prod_{i=1}^r \alpha_i^{x_i} \in \mathfrak{A}$. Genauso für $M \in \mathbb{Z}^{r\times k}$ setzen wir $AM = (\beta_1, \ldots, \beta_k)$ mit $\beta_j = \sum_{i=1}^r m_{ij}\alpha_i$ oder $\prod_{i=1}^r \alpha_i^{m_{ij}}$.

Definition 1.17. Sei $\mathcal{A}$ eine endlich erzeugte abelsche Gruppe und $G = (g_1, \ldots, g_r)$, $g_i \in \mathcal{A}$. Sei $M \in \mathbb{Z}^{r\times k}$. Dann ist (G, M) ein *System von Erzeugenden und Relationen*, falls für jedes $\alpha \in \mathcal{A}$ es ein $X \in \mathbb{Z}^r$ gibt mit $GX = \alpha$, und $GX = 1_{\mathcal{A}}$ genau dann der Fall ist, wenn $X = MY$ für ein geeignetes $Y \in \mathbb{Z}^k$ ist.

Insbesondere gilt dann: $GM = (1, \ldots, 1)$. Mit anderen Worten: (G, M) definieren eine *Präsentation*, also eine exakte Sequenz $\mathbb{Z}^k \xrightarrow{M} \mathbb{Z}^r \xrightarrow{G} \mathcal{A} \to 1$

Definition 1.18. Sei $\mathcal{A}$ eine endlich erzeugte abelsche Gruppe und (A, D) ein System von Erzeugenden und Relationen. Man sagt (A, D) ist in SNF, falls D in SNF ist.

Wir wiederholen den Algorithmus zur Berechnung von $\mathcal{A}$ in SNF, falls $|\mathcal{A}| < \infty$:

Algorithm 2: Smith-Normalform von Präsentationen

Input: (G, M) ein System von Erzeugenden und Relationen
Output: (A, D) eine SNF für $\mathcal{A}$,
Eine Matrix U_A zur Berechnung von diskreten Logarithmen

1 Berechne die HNF $(0 \mid H)$ von M. Dann ist H eine obere Dreiecksmatrix mit positiven Diagonaleinträgen.
2 Berechne $U, V \in \mathrm{GL}_r(\mathbb{Z})$, $r = |G|$, mit $UHV = D' = \mathrm{diag}(\mathrm{d}_1, \ldots, \mathrm{d}_\mathrm{n}, 1, \ldots, 1)$ in SNF. Dann gilt $(\beta_1, \ldots, \beta_r) = GH$ genau dann, wenn

$$(\beta_1, \ldots, \beta_r)V = GU^{-1}UHV = GU^{-1}D,$$

d.h. Setze also $A' := (\alpha'_1, \ldots, \alpha'_r) := GU^{-1}$
3 Lösche triviale Komponenten: Sei $D = \mathrm{diag}(d_1, \ldots, d_n)$ und $A = (\alpha'_1, \ldots, \alpha'_n)$. Weiter ist U_a die Matrix der ersten n Zeilen von U.
4 Gib (A, D) und U_a aus.

Bemerkung 1.19. Mit der Notation des Algorithmus' gilt $AU_a = G$.

Erläuterung zu diskreten Logarithmen: Sei (A, D) eine Präsentation für $\mathcal{A}$, $|\mathcal{A}| < \infty$. Falls $\alpha \in \mathcal{A}$, so gibt es $x_1, \ldots, x_n \in \mathbb{Z}$ mit $\alpha = \prod_{i=1}^{n} \alpha_i^{x_i}$. Die x_i sind eindeutig modulo d_i, z.B. $0 \leq x_i < d_i$. $(x_1, \ldots, x_n)^t$ heißt diskreter Logarithmus von α bezüglich A.

Beispiel 1.20. Sei (A, M) eine Präsentation von $\mathcal{A} = \langle g_1, g_2, g_3 \rangle_{\mathbb{Z}}$, wobei $A = (g_1, g_2, g_3)$ und

$$M = \begin{pmatrix} 3 & -6 & 9 \\ 3 & 5 & 9 \\ 1 & 4 & 4 \end{pmatrix}.$$

Man berechnet die Smith-Normalform als

$$UHV = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 4 & -3 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, U^{-1} = \begin{pmatrix} 1 & 3 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 4 & 0 & -3 \\ 0 & 1 & 0 \\ -1 & 1 & 1 \end{pmatrix}$$

Wir haben also neue Relationen

$$MV = \begin{pmatrix} 3 & 3 & 0 \\ 3 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

entsprechend $g_1^3 g_2^3 = 1 = g_1^3 g_2^4 = g_3$, und neue Erzeugende

$$A' = GU^{-1} = (g_1 g_2, g_1^3 g_2^4), g_3) = (g_1 g_2, 1, 1),$$

also ist unsere neue Präsentation $A = (g_1 g_2)$, $D = (3)$ und $U_a = (4, -3, 0)$. Wir überprüfen $AU_a = ((g_1 g_2)^4, (g_1 g_2)^{-3}, 1) = (g_1, g_2, g_3) = G$.

1.5 Effektive Berechenbarkeit von endlichen abelschen Gruppen in exakten Sequenzen

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

(a) wir für $\mathcal{A}$ eine SNF (A, D) haben, und

(b) wir einen effektiven Algorithmus zur Lösung des Diskreten Logarithmus-Problems haben, d.h. zu $\alpha \in \mathcal{A}$ berechne $X \in \mathbb{Z}^{|A|}$ mit $\alpha = AX$.

Sei $\psi : \mathcal{A} \to \mathcal{B}$ ein Homomorphismus von endlichen abelschen Gruppen mit Präsentationen $(A, D_{\mathcal{A}})$, $(B, D_{\mathcal{B}})$. Dann heißt ψ *effektiv berechnet*, wenn

(a) Zu $\alpha \in \mathcal{A}$ kann $\psi(\alpha)$ in der Form $\psi(\alpha) = BY$ mit effektiv berechenbarem $Y \in \mathbb{Z}^{|B|}$ geschrieben werden, und

(b) Zu $\beta \in \psi(\mathcal{A})$ kann $\alpha \in \mathcal{A}$ mit $\psi(\alpha) = \beta$ effektiv berechnet werden.

Wir brauchen noch einen Algorithmus zur Berechnung von Quotienten: Sei

$$\mathcal{A} \xrightarrow{\psi} \mathcal{B} \xrightarrow{\varphi} \mathcal{C} \to 1$$

exakt, wobei $\mathcal{A}, \mathcal{B}$, ψ und φ effektiv berechnet seien. Ziel ist es, eine SNF $(C, D_{\mathcal{C}})$ von $\mathcal{C}$ zu bestimmen.

Algorithm 3: Effektive Berechnung von Quotienten

Input: effektiv berechenbare $\mathcal{A}, \mathcal{B}, \varphi, \psi$ wie oben
Output: Effektive Berechenbarkeit von $\mathcal{C}$

1 Sei $B' = \varphi(B)$. Dann ist B' ein Erzeugendensystem für C.

2 Sei $V \in \mathbb{Z}^{B'}$ eine Relation, d.h. $B'V = 1_{\mathcal{C}}$. Es gilt

$$\begin{aligned} B'V = 1_{\mathcal{C}} &\iff 1_{\mathcal{C}} = \varphi(B)V = \varphi(BV) \iff BV \in \ker(\varphi) = \operatorname{im}(\psi) \\ &\iff BV = \psi(A)X \quad \text{für ein } X \in \mathbb{Z}^{|A|}. \end{aligned}$$

Da ψ effektiv berechnet ist, kann man $P \in \mathbb{Z}^{|B|\times|A|}$ mit $\psi(A) = BP$. Also $B'V = 1_{\mathcal{C}} \iff V - PX \in \operatorname{im}(D_{\mathcal{B}}) \iff V \in \operatorname{im}(P \mid D_{\mathcal{B}})$. Also ist $(B', (P \mid D_{\mathcal{B}}))$ ein System von Erzeugern und Relationen von C.

3 Berechne davon die SNF $(C, D_{\mathcal{C}})$ und erhalte von Algorithmus 2 die Matrix U_a. Damit lässt sich das DL-Problem lösen.

Zum DL in $\mathcal{C}$: Da φ effektiv ist, kann man zu $\gamma \in \mathcal{C}$ ein $\beta \in \mathcal{B}$ mit $\varphi(\beta) = \gamma$ berechnen. Weiter ist $\mathcal{B}$ effektiv berechenbar, also können wir $X \in \mathbb{Z}^{|B|}$ mit $\beta = BX$ berechnen. Dann folgt

$$\gamma = \varphi(\beta) = \varphi(BX) = \varphi(B)X = (CU_a)X = C(U_aX),$$

also ist U_aX der DL von $\gamma \in \mathcal{C}$.

Umgekehrt wollen wir auch Gruppenerweiterungen effektiv berechnen. Sei also $1 \to \mathcal{A} \xrightarrow{\psi} \mathcal{B} \xrightarrow{\varphi} \mathcal{C} \to 1$ kurz exakt, und $\mathcal{A} = (A, D_{\mathcal{A}})$, $\mathcal{C} = (C, D_{\mathcal{C}})$ sowie ψ und φ effektiv berechenbar. Dann berechne B' mit $\varphi(B') = C$, sodass $B = (\psi(A) \mid B')$ ein Erzeugendensystem von $\mathcal{B}$ ist.

Sei $\beta \in B$ und $\varphi(\beta) = CY$. Dann ist $\varphi(\beta) = CY = \varphi(B'Y)$, also $\beta - B'Y \in \ker\varphi = \operatorname{im}\psi$, also gibt es $X \in \mathbb{Z}^{|A|}$ mit $\beta - B'Y = \psi(AX) = \psi(A)X$. Insgesamt ist nun

$$\beta = B'Y + \psi(A)X = (\psi(A) \mid B') \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Sei $R = \left(\frac{X}{Y}\right)$ eine Relation, d.h. $(\psi(A) \mid B')\left(\frac{X}{Y}\right) =!_{\mathcal{B}}$. Anwenden von φ gibt $CY = \varphi(B')Y = 1_{\mathcal{C}}$, also $Y \in \operatorname{im}(D_{\mathcal{C}})$. Schreibe $Y = D_{\mathcal{C}}Y_1$ für ein passendes $Y_1 \in \mathbb{Z}^{|C|}$. Setze $B'' := B'D_{\mathcal{C}} = (\beta_1, \ldots, \beta_{|C|}$, dann gilt $\varphi(B'') = CD_{\mathcal{C}} = 1_{\mathcal{C}}$, also sind die $\beta_i \in \ker\varphi = \operatorname{im}\psi$ von der Form $\beta_i = \psi(\alpha_i)$ für $(\alpha_1, \ldots, \alpha_{|C|} = AP$ mit $P \in \mathbb{Z}^{|A|\times|C|}$ berechenbar; und $B'' = \psi(A)P$.

Insgesamt haben wir die Relation $AX + BY = 1_{\mathcal{B}}$ umgeschrieben zu $\psi(A)X + \psi(A)PY_1 = 1_{\mathcal{B}}$. Wegen der Injektivität von ψ ist das äquivalent zu $A(X + PY_1) = 1_{\mathcal{A}}$, also zu $X + PY_1 \in \operatorname{im}(D_{\mathcal{A}})$. Setze $X + PY_1 = D_{\mathcal{A}}T$ für $T \in \mathbb{Z}^{|A|}$, dann ist

$$R = \begin{pmatrix} X \\ Y \end{pmatrix} = \underbrace{\begin{pmatrix} D_{\mathcal{A}} & -P \\ 0 & D_{\mathcal{C}} \end{pmatrix}}_{=:D} \begin{pmatrix} T \\ Y_1 \end{pmatrix},$$

d.h. D beschreibt alle Relationen in $\mathcal{B}$.

Algorithm 4: Effektive Berechnung von Erweiterungen

Input: effektiv berechenbare $\mathcal{A}, \mathcal{C}, \varphi, \psi$ wie oben
Output: Effektive Berechenbarkeit von $\mathcal{B}$

1 Berechne B' mit $\varphi(B') = C$, sowie $\psi(A)$.
2 Setze $B'' := B'D_{\mathcal{C}}$ und berechne A'' mit $\psi(A'') = B''$. Mithilfe des DL-Algorithmus in $\mathcal{A}$ berechne P mit $A'' = AP$.
3 Setze $G = (\psi(A) \mid B')$ und $M = \begin{pmatrix} D_{\mathcal{A}} & -P \\ 0 & D_{\mathcal{C}} \end{pmatrix}$. Berechne die SNF von (G, M) und gib diese (sowie die dabei berechnete Matrix U_a) aus.

Zum DL-Problem in $\mathcal{B}$: Sei $\beta \in B$. Löse zunächst $\varphi(\beta) = CY$, dann gilt $\varphi(\beta - B'Y) \in \ker\varphi = \operatorname{im}\psi$, berechne also $\alpha \in \mathcal{A}$ mit $\psi(\alpha) = \beta - B'Y$ und löse $\alpha = AX$ in $\mathcal{A}$. Dann gilt $\beta = \psi(A)X + B'Y$.

Insgesamt können wir nun also in einer kurzen exakten Sequenz, bei der zwei Gruppen und beide Morphismen effektiv berechenbar sind, die dritte Gruppe effektiv berechnen (Für Kerne, die wir als Untergruppen betrachten können, ist das klar). Mit diesen Werkzeugen kann man auch in langen exakten Sequenzen arbeiten, indem man diese in mehrere kurze exakte Sequenzen aufteilt. Sei beispielsweise

$$\mathcal{A} \to \mathcal{B} \to \mathcal{C} \xrightarrow{\gamma} \mathcal{D} \to 1$$

exakt, und wir wollen $\mathcal{C}$ aus den restlichen Daten bestimmen. Setze $W := \ker\gamma$, dann sind $\mathcal{A} \to \mathcal{B} \to W \to 1$ und $1 \to W \to \mathcal{C} \to \mathcal{D} \to 1$ exakt, mittels der obigen Algorithmen können wir also zuerst W und dann $\mathcal{C}$ effektiv berechnen.

2 Zahlkörper

Sei $K = \mathbb{Q}(\alpha)/\mathbb{Q}$ ein Zahlkörper, o.E. fixieren wir einen algebraischen Abschluss $\mathbb{Q}^c \subseteq \mathbb{C}$. Sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von α über $\mathbb{Q}$, dann ist die von $X \mapsto \alpha$ induzierte Abbildung $\mathbb{Q}[X]/(f(X)) \to \mathbb{Q}(\alpha)$ ein Körperisomorphismus

Definition 2.1. Sei $f \in \mathbb{Q}[X]$ normiert und irreduzibel. Dann ist $\mathbb{Q}[X]/f(X)$ ein *algebraischer Zahlkörper in Standarddarstellung*.

In dieser Standarddarstellung lassen sich z.B. leicht Inverse berechnen, dann dazu löst man für $\overline{g} \in \mathbb{Q}[X]/(f)$ die Gleichung $gh + fk = 1$ mittels des erweiterten Euklidischen Algorithmus, um $\overline{g}^{-1} = \overline{h}$ zu erhalten.

Seien $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ die Konjugierten von α, d.h. die Nullstellen von f in $\mathbb{C}$. Dann sind $\sigma_i : K \to \mathbb{C}, \alpha \mapsto \alpha_i$ genau die $\mathbb{Q}$-linearen Einbettungen $K \to \mathbb{C}$.

Algebraische Zahlen als Wurzeln der Minimalgleichung Sei $f \in \mathbb{Q}[x]$ normiert und irreduzibel. Dann ist $K = \mathbb{Q}[x]/(f(x))$ ein Körper. Seien $\alpha = \alpha_1, \ldots, \alpha_n \in \mathbb{C}$ die (paarweise verschiedenen) Nullstellen von f. Oft braucht oder hat man "guteÄpproximationen an die Konjugierten α_i. Aus solchen Approximationen $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n$ lässt sich f zurückgewinnen, falls $d \in \mathbb{Z}$ bekannt ist mit $df \in \mathbb{Z}[x]$. Es gilt $df = d\prod_i (X - \widetilde{\alpha}_i) \in \mathbb{Z}[x]$, und man kann die Koeffizienten runden. Division

Weitere Darstellungen Voraussetzung: K ist gegeben durch eine $\mathbb{Q}$-Basis $\theta_1, \ldots, \theta_n$, zum Beispiel $\theta_i = \alpha^{i-1}$. Berechne a^j für $j = n, n+1, \ldots, 2n-2$ rekursiv mittles $f(x)$, oder allgemeiner $\theta_i\theta_j$ als Linearkombination der θ_k. Dafür müssen $\frac{n^2+n}{2}$ Koeffizienten gespeichert werden.

Matrixdarstellung: Betrachte $\mu_\alpha : K \to K, \beta \mapsto \alpha\beta$. Sei $M_\alpha \in M_n(\mathbb{Q})$ die darstellende Matrix von μ_α. Dann ist $K \to M_n(\mathbb{Q})$, $\alpha \mapsto M_\alpha$ ein injektiver $\mathbb{Q}$-Algebrenhomomorphismus. Es gilt $\alpha(\theta_1, \ldots, \theta_n)^t = M_\alpha(\theta_1, \ldots, \theta_n)^t$. Diese Darstellung hat die Vorteile, dass Multiplikation und Division einfach ausführbar sind, sowie $\chi_\alpha, \mathrm{Tr}(\alpha)$ etc. einfach zu berechnen sind.

Konjugiertenvektor Sei $\xi = \sum a_i\alpha^i \in K$. Stelle ξ als Konjugiertenvektor

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

da. Dies ist berechenbar, wenn z.B. die Konjugierten von α approximativ gegeben sind. Problematisch ist aber, dass $|\alpha^i|$ sehr groß werden kann, was präzise Berechnungen erschwert. Gegeben einen Konjugiertenvektor, so gilt $\sigma_j(\xi) = \sum_i a_i\sigma_j(\alpha^i)$, also löst $(a_0, \ldots, a_{n-1})^t$ das Lineare Gleichungssystem $(\sigma_i(\alpha^j)x = (\sigma_i(\xi))$. So kommt man also von einem Konjugiertenvektor wieder zur Basisdarstellung zurück.

Beispiel 2.2. Sei K ein Zahlkörper und $K(1)$ sein Hilbertsher Zahlkörper, also die maximale abelsche unverzweigte Erweiterung von K. Dann ist $K(1)$ ebenfalls ein Zahlkörper, und es gilt ("Kroneckers Jugendtraum") $[K(1) : K] = h_K$ und $\mathrm{Gal}(K(1)/K) \cong \mathrm{cl}_K$.

Sei nun $K = \mathbb{Q}(\sqrt{d})$, $d < 0$ ein imaginär-quadratischer Zahlkörper, und sei $L \subseteq K$ ein $\mathbb{Z}$-Gitter, nimm z.B. $L = \mathcal{O}_K$. Definiere $s_{2k}(L) = \sum_{0 \neq w \in L} \frac{1}{w^{2k}}$ sowie $g_2 = 60s_4$, $g_3 = 140s_6$, $\Delta = 4g_2^3 - 27g_3^2$ und $j = 1728g_2^3/\Delta$. $j(\mathcal{O}_K)$ ist berechenbar, und es gilt $K(1) = K(j(\mathcal{O}_K))$.

Die Konjugierten von $j(\mathcal{O}_K)$ sind gegeben durch $j(\mathfrak{a})$, wobei $[\mathfrak{a}]$ durch cl_K läuft. D.h. $(j(\mathfrak{a}))_{[\mathfrak{a}] \in \mathrm{cl}_K}$ ist ein Konjugiertenvektor für $K(1)/K$.

2.1 Ordnungen und Ideale

Definition 2.3. Eine Ordnung R in einem Zahlkörper K ist ein Teilring der als $\mathbb{Z}$-Modul endlich erzeugt ist und Rang $n = [K : \mathbb{Q}]$ hat.

Beispiel 2.4. (i) Für $K = \mathbb{Q}(\alpha)$ mit $\alpha \in \mathcal{O}_K$ ist $\mathbb{Z}[\alpha]$ eine Ordnung von K. Gegenüber dem Ganzheitsring hat diese den Vorteil, dass sie leichter zu berehnen ist.

(ii) Seien $L/K/\mathbb{Q}$ Zahlkörper, und $\mathfrak{a} \subseteq \mathcal{O}_L$. Dann ist $R = \mathcal{O}_K + \mathfrak{a}$ eine Ordnung in L.

(iii) Die Ordnungen in einem quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ sind genau von der Form $\mathbb{Z}[f\omega]$ mit $f \in \mathbb{Z}$ und $\omega = \sqrt{d}$ oder $\frac{1+\sqrt{d}}{2}$ der kanonische Erzeuger.

Proposition 2.5. *Sei $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ ein Ideal. Dann ist $|R/\mathfrak{a}| < \infty$*

Beweis. Sei $0 \neq a \in \mathfrak{a}$. Dann sind R und aR abelsche Gruppen vom gleichen Rang, also ist $\infty > |R/aR| > |R/\mathfrak{a}|$. □

Definition 2.6. $\mathrm{N}(\mathfrak{a}) := |R/\mathfrak{a}| \in \mathbb{N}$ ist die Norm eines Ideals $\mathfrak{a}$

Achtung: Die Idealnorm ist nicht multiplikativ, außer wenn $R = \mathcal{O}_K$.

Definition 2.7. $0 \neq \mathfrak{a} \subseteq K$ heißt gebrochenes Ideal, falls es $d \in \mathbb{Z}$ gibt, sodass $d\mathfrak{a} \subseteq R$ ein Ideal ist. Schreibe $I(R)$ oder I_R für die Menge aller gebrochenen Ideale.
Sei $\mathfrak{a} \in I_R$. Dann heißt $\mathfrak{a}$ invertierbar, falls es $\mathfrak{b} \in I_R$ mit $\mathfrak{ab} = R$ gibt.

Im Gegensatz zu $\mathcal{O}_K$ sind in allgemeinen Ordnungen nicht alle Ideale invertierbar. Zum Beispiel gilt in $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Q}(\sqrt{-3})$, dass (2) nicht invertierbar ist.