

# Protokoll zur Vorlesung Algorithmische Zahlentheorie

## WS 25/26

W. Bley

16. Dezember 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  $r = \text{rg}(V)$ .
- (2) Sei  $W \subseteq V$  ein Teilmodul. Dann ist  $W$  endlich erzeugt und es gilt  $\text{rg}(W) \leq \text{rg}(V)$ .
- (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  $m = \text{rg}(V)$ . 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  $f: \{r+1, \dots, n\} \rightarrow \{1, \dots, m\}$ ,  $0 \leq r \leq n$  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  $U \in \text{Gl}_n(\mathbb{Z})$  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  $A: \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ . 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:

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

### 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  $(\text{HNF}(dL), d)$ .

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  $D := \text{kgV}(d_1, d_2)$ . 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  $\text{HNF}(W)$  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  $g_1, \dots, g_n$  ein Erzeugendensystem von  $G$ . Dann induziert der Epimorphismus  $\pi: \mathbb{Z}^n \rightarrow G, (x_1, \dots, x_n)^t \mapsto x_1g_1 + \dots + x_ng_n$  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  $U, V \in \text{GL}_n(\mathbb{Z})$ .*

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  $A = (\alpha_1, \dots, \alpha_r)$  mit  $\alpha_i \in \mathcal{A}$  ein Zeilenvektor von Elementen in  $\mathcal{A}$ . Für einen Spaltenvektor  $X = (x_1, \dots, x_r)^t \in \mathbb{Z}^r$  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  $M = (m_{ij}) \in \mathbb{Z}^{r \times n}$

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

**Definition 1.8.1** Sei  $\mathcal{A}$  eine e-e abelsche Gruppe und  $G = (g_1, \dots, g_r)$  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  $GM = (1_{\mathcal{A}}, \dots, 1_{\mathcal{A}})$ . 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  $U, V \in \text{Gl}_n(\mathbb{Z})$ , so dass  $UHV = D'$  in SNF ist. Setze

$$A' = (\alpha_1, \dots, \alpha_m, \alpha_{n+1}, \dots, \alpha_r) := GU^{-1},$$

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  $D := \text{diag}(d_1, \dots, d_m)$ ,  $A := (\alpha_1, \dots, \alpha_m)$ . 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 ein 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  $\alpha$  bezüglich  $A$ .

**Sprechweise:** Sei  $\psi: \mathcal{A} \rightarrow \mathcal{B}$  ein Homomorphismus von effektiv berechneten (endlichen) abelschen Gruppen. Seien  $(A, D_A)$  und  $(B, D_B)$  jeweils Erzeugende und Relationen in SNF. Wir sagen, dass  $\psi$  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

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

eine exakte Sequenz von (endlichen) abelschen Gruppen. Wir setzen voraus, dass  $\mathcal{A}, \mathcal{B}$  effektiv berechnet sind. Zusätzlich brauchen wir, dass  $\psi$  und  $\phi$  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  $\gamma \in \phi(\mathcal{C})$  kann man  $\beta \in \mathcal{B}$  berechnen kann mit  $\phi(\beta) = \gamma$ .

Sei  $\mathcal{C}' := \phi(\mathcal{B})$ . Dann ist  $\mathcal{C}'$  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:

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

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  $\beta$  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  $\gamma$  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  $B'' := B'D_{\mathcal{C}} = (\beta''_1, \dots, \beta''_{|C|})$  und  $A'' = (\alpha''_1, \dots, \alpha''_{|C|})$  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  $\beta - B'Y \in \ker(\phi) = \text{im}(\psi)$ , 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  $\beta$  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  $\psi, \phi$  und  $\pi$ ) 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

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

die Einbettungen  $K \hookrightarrow \mathbb{C}$ . Hierbei bezeichnen  $\sigma_1, \dots, \sigma_{r_1}$  die reellen Einbettungen und  $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$  die Paare komplex-konjugierter Einbettungen.

### 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

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

von  $f$ . Diese entsprechen den Einbettungen  $K \hookrightarrow \mathbb{C}$  und werden entsprechend wie oben nummeriert. Es gilt:

$$\mathbb{Q}[X]/(f(X)) \simeq \mathbb{Q}(\alpha) \text{ induziert von } g(X) \mapsto g(\alpha).$$

Diese Darstellung nennen wir die Standarddarstellung. Die Rechenoperationen finden in  $\mathbb{Q}[X]/(f(X))$  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  $\theta_1, \dots, \theta_n$  gegeben ist. Zum Beispiel ist für  $K = \mathbb{Q}[X]/(f(X)) = \mathbb{Q}(\alpha)$  eine solche Basis durch  $1, \alpha, \dots, \alpha^{n-1}$  gegeben. 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  $\theta_1, \dots, \theta_n$  eine  $\mathbb{Q}$ -Basis von  $K$  und  $\beta \in K$ . Dann ist die Multiplikation mit  $\beta$  ein Endomorphismus von  $K$ ,

$$\mu_\beta: K \longrightarrow K, \quad \xi \mapsto \beta\xi.$$

Sei  $M_\beta \in \mathbb{Q}^{n \times n}$  die Darstellungsmatrix bezüglich der fixierten Basis  $\theta_1, \dots, \theta_n$ . 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

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

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 imaginär-quadratischen 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 charakteristisches Polynom

**Definition 2.2.1** (a) Sei  $\beta \in K$ . Dann heit

$$\chi_\beta(X) := \prod_{i=1}^n (X - \sigma_i(\beta))$$

charakteristisches Polynom von  $\beta$ .

(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  $\beta$ .

Es gilt:  $\text{Tr}_{K/\mathbb{Q}}(\beta) = s_1(\beta)$ ,  $N_{K/\mathbb{Q}}(\beta) = s_n(\beta)$ .

Die approximative Berechnung von  $\chi_\beta$  ist leicht, wenn  $\beta$  als Konjugiertenvektor gegeben ist. Es gilt ferner:

$$\chi_\beta(X) = \det(XE - M_\beta).$$

Insbesondere sind Norm und Spur von  $\beta$  durch die Determinante und Spur von  $M_\beta$  gegeben.

**Satz 2.2.2** Sei  $\beta = \sum_{i=0}^{n-1} a_i \alpha^i \in K = \mathbb{Q}(\alpha)$ . Sei  $A(X) := \sum_{i=0}^{n-1} a_i X^i$ . Dann gilt:

$$\chi_\beta(X) = \text{Res}_Y(f(Y), X - A(Y)).$$

Insbesondere gilt fr die Norm

$$N_{K/\mathbb{Q}}(\beta) = \text{Res}_Y(f(Y), A(Y)).$$

Hierbei bezeichnet  $\text{Res}_Y$  die Resultante bezglich  $Y$  ber 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  $K$  enthlt.

Sei  $R$  eine Ordnung und  $I \subseteq R$  ein Ideal. Dann ist  $R/I$  stets endlich und wir definieren

$$N(I) := |R/I|.$$

**Definition 2.3.2** Sei  $R \subseteq K$  eine Ordnung.

(a) Eine nicht-leere Teilmenge  $(0) \neq I \subseteq K$  heit gebrochenes Ideal von  $R$ , falls es ein  $d \in \mathbb{Z}$  gibt, so dass  $dI \subseteq R$  ein Ideal ist.

(b) Ein gebrochenes Ideal heit 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:

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

## 2.4 Darstellung von Moduln und Idealen

**Definition 2.4.1** Sei  $R \subseteq K$  eine Ordnung und sei  $\omega_1, \dots, \omega_n$  eine  $\mathbb{Z}$ -Basis von  $R$ . Sei  $M \subseteq K$  ein voller  $\mathbb{Z}$ -Teilmodul. Dann gibt es eine eindeutig bestimmte  $\mathbb{Z}$ -Basis  $\mu_1, \dots, \mu_n$  von  $M$  mit

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

so dass  $d, w_{ij}$  die folgenden Eigenschaften erfllen:

- (1)  $d, w_{ij} \in \mathbb{Z}, d > 0, \text{ggT}(d, w_{ij}, \forall i, j) = 1$ ,
- (2) Die Matrix  $W = (w_{ij})$  ist in HNF.

Dann heit das Paar  $(W, d)$  HNF von  $M$  bezglich  $R$ , genauer bezglich der fixierten Basis  $\omega_1, \dots, \omega_n$  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  $\mathfrak{d} := \mathfrak{a}\mathfrak{a} + \mathfrak{b}\mathfrak{b}$ . 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  $\beta$  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  $\omega_1, \dots, \omega_n \in V$  und  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \in I_R$ , so dass

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

Falls  $M = \mathfrak{a}'_1\omega'_1 \oplus \dots \oplus \mathfrak{a}'_n\omega'_n$ , 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  $\text{cl}_R$  überein.

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

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

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

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

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

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

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  $(\eta_1, \dots, \eta_n) = (\omega_1, \dots, \omega_n)U$  mit einer Matrix  $U \in \text{Gl}_n(K)$ . 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  $\mathfrak{b}_1, \dots, \mathfrak{b}_n \in I_R$  und  $U \in \text{Gl}_n(K)$  gegeben. Es gelte  $\mathfrak{a} = \det(U)\mathfrak{b}$  und  $u_{ij} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$ . Definiert man dann  $\eta_1, \dots, \eta_n$  durch  $(\eta_1, \dots, \eta_n) = (\omega_1, \dots, \omega_n)U$ , 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  $I = (\mathfrak{a}_1, \dots, \mathfrak{a}_k), \mathfrak{a}_j \in I_R$ .

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

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

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

1.  $u_{ij} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$ ,  $\forall 1 \leq i, j \leq k$ .
2.  $\mathfrak{a} = \det(U) \mathfrak{b}$ , wobei  $\mathfrak{a} := \mathfrak{a}_1 \cdots \mathfrak{a}_k$  und  $\mathfrak{b} := \mathfrak{b}_1 \cdots \mathfrak{b}_k$ .

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

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

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

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

5.  $(U_j, \mathfrak{b}_j)_{1 \leq j \leq k-n}$  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  $e = 0, 1, \dots$  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  $\mathfrak{a} \mathfrak{p} \subseteq \mathcal{O}_K$ . Für jedes solche  $a$  gilt:

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

Es gilt dann:

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

### 3.4 Berechnung der Differenten und Idealinversion

Wir erinnern an die Spurform

$$K \times K \longrightarrow \mathbb{Q}, \quad (\alpha, \beta) \mapsto \text{Tr}_{K/\mathbb{Q}}(\alpha\beta).$$

Die Spurform ist eine nicht-ausgeartete symmetrische Bilinearform auf dem  $\mathbb{Q}$ -Vektorraum  $K$ . Für einen vollen  $\mathbb{Z}$ -Teilmodul  $M \subseteq K$  sei

$$M^* := \{\alpha \in K \mid \text{Tr}_{K/\mathbb{Q}}(\alpha M) \subseteq \mathbb{Z}\}.$$

Falls  $M = \langle \gamma_1, \dots, \gamma_n \rangle_{\mathbb{Z}}$ , so ist

$$M^* = \langle \gamma_1^*, \dots, \gamma_n^* \rangle_{\mathbb{Z}}$$

mit der Dualbasis (bez. der Spurform)  $\gamma_1^*, \dots, \gamma_n^*$  definiert durch  $\text{Tr}_{K/\mathbb{Q}}(\gamma_i \gamma_j^*) = \delta_{ij}$  (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 Dualen 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 Differenten oder Kodifferenten.

## 4 Berechnung der Maximalordnung

### 4.1 Die Sätze von Pohst-Zassenhaus

Sei  $K = \mathbb{Q}(\theta)$ ,  $\theta$  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)  $I_p := \sqrt{p\mathcal{O}} = \{\alpha \in \mathcal{O} \mid \exists m \in \mathbb{Z}_{>0} : \alpha^m \in p\mathcal{O}\}$  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  $\mathfrak{p}_1, \dots, \mathfrak{p}_g$  die paarweise verschiedenen Primideale 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  $K = \mathbb{Q}(\theta)$ ,  $\theta$  ganz, und  $m(x) \in \mathbb{Z}[x]$  das Minimalpolynom von  $\theta$ . 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

$$f(x) := \frac{1}{p} (g(x)h(x) - m(x)).$$

Dann ist  $f(x) \in \mathbb{Z}[x]$  und es gilt

$$\mathcal{O} = \mathbb{Z}[\theta] \text{ ist } p\text{-maximal} \iff (\bar{f}, \bar{g}, \bar{h}) = 1 \text{ in } \mathbb{F}_p[x].$$

- 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

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

Den Beweis des Dedekindkriteriums werden wir zumindest teilweise im neuen Jahr erbringen.