Einführung in die Algebra

Vorlesung im
Sommersemester 2008
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

CHAPTER 5

Moduln und Gitter

5.1. Definition

Es sei R ein Ring. Ein R (Links)-Modul M ist eine Abelsche Gruppe zusammen mit einer Verknüpfung: $\circ : R \times M \rightarrow M$ mit $(rs) \circ m = r \circ (s \circ m)$, $(r + s) \circ m = r \circ m + s \circ m$ und $r \circ (m + n) = r \circ m + r \circ n$ für alle $r, s \in R, m, n \in M$.

M heißt *unitär*, falls R ein Einselement $1 \neq 0$ besitzt und $1 \circ m = m$ für jedes $m \in M$ gilt.

Eine Teilmenge U eines R -Moduls M heißt *Unterm modul* (*Teilmodul*) von M , falls gelten:

- (i) U ist Untergruppe von M ,
- (ii) $RU \subseteq U$.

(Ein Modul ist im Prinzip ein Vektorraum über einem Ring.)

Ist M ein Modul, so ist der Durchschnitt von Teilmoduln von M wieder ein Teilmodul. Also existiert zu jeder Teilmenge $A \subseteq M$ ein kleinster Teilmodul von M der A enthält.

5.2. Definition

Es sei M ein R -Modul. Für $A \subseteq M$ bezeichne $\langle A \rangle$ den kleinsten Teilmodul von M der A enthält.

M heißt *endlich erzeugt*, falls $A \subseteq M$ mit $\#A < \infty$ und $M = \langle A \rangle$ existiert.

Ist M ein unitärer Modul, so gilt

$$\langle A \rangle = \left\{ \sum_{\text{endlich}} r_a a \mid a \in A, r_a \in R \right\}.$$

Für eine Familie $(M_i)_{i \in I}$ von Teilmoduln von M mit

$$M_j \cap \langle M_i \mid i \in I, i \neq j \rangle = \{0\}$$

für jedes $j \in I$ heißt

$$\dot{+}_{i \in I} M_i := \langle M_i \mid i \in I \rangle$$

innere direkte Summe. Für eine beliebige Familie von R -Moduln werden das direkte (äußere) Produkt $\prod_{i \in I} M_i$ und die äußere direkte Summe $\oplus_{i \in I} M_i$ wie üblich definiert.

5.3. Hilfssatz

Unter der Festsetzung $\alpha \circ (x + U) := \alpha \circ x + U$ wird die Faktorgruppe M/U eines R -Moduls M mit Untermodul U zu einem R -Modul (*Faktormodul*).

5.4. Definition

Es seien $M, \tilde{M}$ zwei R -Moduln und $\varphi : M \rightarrow \tilde{M}$ ein Gruppenhomomorphismus. Falls

$$\varphi(\alpha \circ m) = \alpha \circ \varphi(m) \quad \forall \alpha \in R \quad \forall m \in M$$

gilt, so heißt φ *R -Modulhomomorphismus*, wir schreiben $\varphi \in \text{Hom}_R(M, \tilde{M})$.

5.5. Hilfssatz

Es seien $M, \tilde{M}$ zwei R -Moduln und $\varphi : M \rightarrow \tilde{M}$ ein R -Modulhomomorphismus. Dann gelten:

- (i) $\text{Im bild}(\varphi) \cong M / \ker(\varphi)$,
- (ii) $(U + V)/U \cong V/(U \cap V)$ für Teilmoduln U, V von M ,
- (iii) $M/V \cong (M/U)/(V/U)$ für U, V wie in (ii) mit $U \subseteq V$.

Beweis: Wie für Gruppen, Ringe, Vektorräume.

5.6. Definition

Für $A \subseteq M$ ist $\text{ann}(A) := \{r \in R \mid \forall m \in A : rm = 0\}$ der *Annulator* von A . Falls $\text{ann}(M) = \{0\}$ gilt, so heißt M *treu* (englisch: faithful). $m \in M$ heißt *Torsionselement*, falls $\text{ann}(m) \neq 0$ gilt. Wir schreiben $\text{Tor}(M) := \{m \in M \mid \text{ann}(m) \neq 0\}$. M heißt *Torsionsmodul*, falls $\text{Tor}(M) = M$ gilt, M heißt *torsionsfrei*, falls $\text{Tor}(M) = 0$ gilt.

5.7. Hilfssatz

- (i) Für $U \subseteq M$ ist $\text{ann}(U)$ ein Linksideal von R .
- (ii) Ist $M \neq \{0\}$ torsionsfrei, so hat R keine Nullteiler.

Beweis:

- (i) Für $m \in M$ und $\phi_m : R \rightarrow M : r \mapsto rm$ gilt $\ker \phi_m = \text{ann}(m)$. Demnach ist $\text{ann}(U) = \bigcap_{m \in U} \ker \phi_m$, daher ist (U) ann ein (Links-) Ideal.
- (ii) Es seien $r \neq 0 \neq s$ mit $sr = 0$ gegeben. Dann ist $s(rm) = (sr)m = 0$ und $rm \neq 0$ ein Torsionselement. $\square$

Bemerkung $\text{Tor}(M)$ ist im allgemeinen kein Untermodul von M . (Sei etwa $M = R = \mathbb{Z}/6\mathbb{Z} \Rightarrow \text{Tor}(M) = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\} \Rightarrow \text{Tor}(M)$ ist keine Untergruppe von $(M, +)$, also auch kein Untermodul.)

5.8. Hilfssatz

Es sei R ein Integritätsring und M ein R -Modul. Dann ist $\text{Tor}M$ ein Teilmodul, und $M/\text{Tor}M$ ist torsionsfrei.

Beweis: Setze $\tilde{M} := \text{Tor}(M)$. Es seien $x, y \in \tilde{M}$ mit $\alpha, \beta \in R, \alpha \neq 0 \neq \beta$, so dass $\alpha \circ x = \beta \circ y = 0$ gilt. Es folgt

$$\alpha\beta \circ (x - y) = \alpha\beta \circ x - \alpha\beta \circ y = \beta \circ (\alpha \circ x) - \alpha \circ (\beta \circ y) = 0,$$

also $x - y \in \tilde{M}$ wegen $\alpha\beta \neq 0$. Demnach ist $(\tilde{M}, +)$ Untergruppe von $(M, +)$. Für x, α wie oben folgt weiter

$$\alpha \circ (\beta \circ x) = (\alpha\beta) \circ x = \beta \circ (\alpha \circ x) = 0 \quad \forall \beta \in R,$$

also $\beta \circ x \in \tilde{M}$ und damit $R \circ \tilde{M} \subseteq \tilde{M}$. Also ist $\text{Tor}(M)$ Untermodul von M .

Sind nun $x + \tilde{M} \in M/\tilde{M}$ und $\alpha \in R$ mit $\alpha \circ (x + \tilde{M}) = \alpha \circ x + \tilde{M} = \tilde{M}$, so impliziert dies $\alpha \circ x \in \tilde{M}$, es existiert $\beta \in R, \beta \neq 0$, mit $\beta\alpha \circ x = 0$. Für $\alpha \neq 0$ ist dann $\beta\alpha \neq 0$, also $x \in \tilde{M}$ und damit $x + \tilde{M} = \tilde{M}$. Also ist $M/\text{Tor}(M)$ torsionsfrei. $\square$

5.9. Definition

Eine endliche Teilmenge $\{x_1, \dots, x_n\}$ eines R -Moduls M heißt *über R frei* (unabhängig), falls aus $\sum_{i=1}^n \alpha_i x_i = 0$ für $\alpha_1, \dots, \alpha_r \in R$ bereits $\alpha_1 = \dots = \alpha_r = 0$ folgt. Eine beliebige Teilmenge S von M heißt frei, falls jede endliche Teilmenge von S frei ist.

$S \subseteq M$ heißt *Basis* von M , falls S frei ist und $\langle S \rangle = M$ gilt. Ein Modul mit Basis heißt *freier Modul*.

Bemerkung $\emptyset$ ist frei.

M frei impliziert M torsionsfrei. Die Umkehrung ist im Allgemeinen falsch.

5.10. Satz

Es sei $X \subset M$, M ein unitärer R -Modul. Dann sind äquivalent:

- (i) Für jedes $x \in X$ ist die Abbildung $rx \mapsto r$ ein R -Modul-Isomorphismus zwischen Rx und R . Ferner gilt $M = \dot{+}_{x \in X} Rx$.
- (ii) M ist frei mit Basis X .
- (iii) Jedes $m \in M$ besitzt eine eindeutige Darstellung $m = \sum_{\text{fin}} r_x x$.
- (iv) $M \cong \bigoplus_{x \in X} R$, wobei die Isomorphie durch $(r_x)_x \mapsto \sum r_x x$ gegeben ist.

Beweis:

(i) $\Rightarrow$ (ii) $M = \dot{+}_{x \in X} Rx$ impliziert $M = \langle X \rangle$. X ist frei, da andernfalls die Summe nicht direkt ist.

(ii) $\Rightarrow$ (iii) Jedes $m \in M$ hat eine Darstellung in der Form $\sum_{\text{fin}} r_x x$ (Definition der Basis). Für $\sum_{\text{fin}} r_x x = \sum_{\text{fin}} s_x x$ folgt $\sum_{\text{fin}} (r_x - s_x)x = 0$ und daher $r_x = s_x$, da X frei ist.

(iii) $\Rightarrow$ (iv) Da sich jedes $m \in M$ eindeutig in der Form $m = \sum r_x x$ darstellen lässt, sind die Abbildungen $\phi_x : M \rightarrow R : m = \sum r_y y \mapsto r_x$ für jedes $x \in X$ R -linear. Offenbar ist $\Phi : M \rightarrow \bigoplus_{x \in X} R : m \mapsto (\phi_x(m))_x$ daher linear und wohldefiniert. Φ ist injektiv, da die Darstellung eindeutig ist und surjektiv, da $\Psi : \bigoplus_{x \in X} R x \rightarrow M : (r_x x) \mapsto \sum r_x x$ nach Voraussetzung surjektiv ist. Ψ ist offenbar invers zu Φ .

(iv) $\Rightarrow$ (i) Die äußere direkte Summe ist isomorph zur inneren. □

Beispiel Vektorräume besitzen bekanntlich Basen, sind also freie Moduln. Es sei K ein Körper, V ein K -Vektorraum. Dann ist V ein $\text{End}(V)$ -Modul mittels $(\phi, v) \mapsto \phi(v)$.

Gruppen G sind $\mathbb{Z}$ -Moduln ($\mathbb{Z}G$ Gruppenringe).

In einem kommutativen Ring R gilt: Ein Ideal $A \subseteq R$ ist ein freier R -Modul genau dann, wenn A Hauptideal ist. (Es sei X eine Basis von A . Existiert $\{a, b\} \subseteq X$ mit $a \neq b$, so gilt $0 = ab - ba$, und X ist nicht frei.)

Es sei $R \subseteq S$ eine unitäre Ringerweiterung. Dann ist S ein unitärer R -Modul.

Der Durchschnitt aller maximalen Ideale eines Ringes R heißt **Jacobson Radikal** J_R von R . Wir behaupten, dass ein Element $x \in R$ genau dann zu J_R gehört, wenn $1 - xy$ eine Einheit in R für alle $y \in R$ ist. Wenn $1 - xy$ keine Einheit ist, dann liegt es in einem geeigneten maximalen Ideal $\mathfrak{m}$. Für $x \in J_R \subseteq \mathfrak{m}$ erhalten wir $xy \in \mathfrak{m}$, und daher $1 \in \mathfrak{m}$, ein Widerspruch. Wenn x nicht in einem maximalen Ideal, etwa $\mathfrak{m}$, enthalten ist, gilt $\mathfrak{m} + Rx = R$, daher $m + yx = 1$ für geeignete Elemente $m \in \mathfrak{m}$, $y \in R$. Aber dann liegt das Element $1 - yx = m$ ebenfalls in $\mathfrak{m}$ und kann daher keine Einheit sein.

5.11. Lemma (Nakayama)

Es seien M ein endlich erzeugter unitärer R -Modul und $\mathfrak{a}$ ein Ideal von R , welches im Jacobson Radikal von R enthalten ist. Gilt dann $\mathfrak{a}M = M$, so ist der Modul M trivial.

Beweis: Wir nehmen an, dass M nicht Null ist und dass $u_1, \dots, u_n$ eine minimale Anzahl von Erzeugern von M ist. Weil $u_n \in M = \mathfrak{a}M$ gilt, existieren Elemente $a_1, \dots, a_n \in \mathfrak{a}$ mit $u_n = a_1 u_1 + \dots + a_n u_n$. Weil $\mathfrak{a}$ in dem Jacobson Radikal von R enthalten ist, ist das Element $1 - a_n$ eine Einheit von R , und wir erhalten

$$u_n = a_1(1 - a_n)^{-1}u_1 + \dots + a_{n-1}(1 - a_n)^{-1}u_{n-1}$$

entgegen unserer Annahme, dass n minimal ist.

□

5.12. Korollar 1

Es sei R ein lokaler noetherscher Integritätsring und $\mathfrak{a}$ ein maximales Ideal von R . Dann gilt $\mathfrak{a}^{n+1} \subset \mathfrak{a}^n$ für alle natürlichen Zahlen n .

Beweis: $\mathfrak{m}$ bezeichne das maximale Ideal von R . Offenbar ist $\mathfrak{a}$ in $\mathfrak{m} = J_R$ enthalten. Wenn wir $\mathfrak{a}\mathfrak{a}^n = \mathfrak{a}^n$ hätten, würden wir $\mathfrak{a}^n = 0$ gemäß Nakayamas Lemma erhalten. Aber $\mathfrak{a}$ enthält Elemente ungleich 0 und demnach auch $\mathfrak{a}^n$, weil R ein Integritätsring ist. $\square$

5.13. Korollar 2

Es sei R ein noetherscher Integritätsring und $\mathfrak{a}$ ein echtes Ideal von R . Dann gilt $\mathfrak{a}^{n+1} \subset \mathfrak{a}^n$ für alle natürlichen Zahlen n .

Beweis: Wir wenden Lokalisierung an! Es sei $\mathfrak{a}$ enthalten in dem maximalen Ideal $\mathfrak{p}$ von R . Wenn wir $\mathfrak{a}\mathfrak{a}^n = \mathfrak{a}^n$ hätten, würde dasselbe für das Ideal $\tilde{\mathfrak{a}} = \frac{\mathfrak{a}}{R \setminus \mathfrak{p}}$ gelten. Man sieht leicht, dass $\widetilde{\mathfrak{a}^{n+1}} = \tilde{\mathfrak{a}}^n$ gilt, und der Beweis erfolgt durch die Anwendung des vorangehenden Korollars. $\square$

Moduln über Hauptidealringen

Ab jetzt sei R ein kommutativer unitärer Hauptidealring.

5.14. Satz

Es sei M ein freier R -Modul vom Rang n . Dann ist jeder Untermodul U von M frei vom Rang $m \leq n$.

Beweis: Der Beweis erfolgt mittels vollständiger Induktion über die Anzahl n der Erzeuger von $M = Rx_1 \dot{+} \dots \dot{+} Rx_n$.

Induktionsanfang: $n = 0$ (trivial).

Induktionsschritt $n - 1 \Rightarrow n$:

Wir setzen $A_n := \{a_n \in R \mid \exists x \in U : x = \sum_{i=1}^n a_i x_i\}$.

Dann ist A_n offenbar ein Ideal in R . Wir schreiben $A_n = (\alpha_n)$. Hierzu existiert ein $y \in U$ etwa $y = \sum_{i=1}^n \alpha_i x_i$ ($y = 0$ ist möglich!). Wir bilden dann $\tilde{U} := U \cap (Rx_1 \dot{+} \dots \dot{+} Rx_{n-1})$ und zeigen $U = \tilde{U} \dot{+} Ry$. Dazu bemerken wir:

- (i) $\forall x \in U \exists \alpha \in R : x - \alpha y \in U$,
- (ii) $\tilde{U} \cap Ry = \{0\}$, denn $x_1, \dots, x_n$ sind frei.

Nunmehr wenden wir die Induktionsvoraussetzung für $\tilde{U}$ an. $\square$

5.15. Satz

Endlich erzeugte, torsionsfreie Moduln über Hauptidealringen sind frei.

Beweis: Nach Voraussetzung gilt

$$M = \sum_{i=1}^n Rx_i.$$

Unter den Teilmengen von $\{x_1, \dots, x_n\}$ wähle eine freie mit maximal vielen Elementen. Nach eventueller Ummumerierung sei dies $\{x_1, \dots, x_s\}$. Für $n = s$ ist man fertig. Sei also $s < n$. Für jedes $j \in \{s+1, \dots, n\}$ existieren dann $\alpha_j, \alpha_{ji} \in R$ ($1 \leq i \leq s$), $\alpha_j \neq 0$, mit

$$\alpha_j x_j = \sum_{i=1}^s \alpha_{ji} x_i.$$

Hiernach ist $\alpha_j x_j \in F$ für $F = \sum_{i=1}^s Rx_i$.

Für $\alpha = \prod_{j=s+1}^n \alpha_j \neq 0$ ist $\alpha x \in F \forall x \in M$ bzw. $\alpha M \subseteq F \subseteq M$. Gemäß 5.14 ist αM frei vom Rang $\leq s$. Dann ist $\varphi : M \rightarrow \alpha \cdot M : x \mapsto \alpha \cdot x$ ein Modulhomomorphismus, welcher surjektiv und injektiv aufgrund der Torsionsfreiheit von M ist. Es folgt $M \simeq \alpha \cdot M$ also ist M frei vom Rang s . $\square$

Bemerkung $\mathbb{Q}$ ist ein torsionsfreier $\mathbb{Z}$ -Modul, aber nicht frei.

5.16. Satz

Es seien R ein Hauptidealring und M ein endlich erzeugter R -Modul. Dann gilt $M = \text{Tor}(M) \oplus F$ mit einem freien Untermodul $F \simeq M/\text{Tor}(M)$.

Beweis Nach 5.8 und 5.15 ist $M/\text{Tor}(M)$ frei, etwa mit Basis B . Betrachte nun den kanonischen Epimorphismus

$$\varphi : M \rightarrow M/\text{Tor}(M) : x \mapsto x + \text{Tor}(M).$$

Zu jedem $b \in B$ wähle ein festes $m_b \in M$ mit $\varphi(m_b) = b$. Es ist $F := \sum_{b \in B} Rm_b$ ein Untermodul von M . Offensichtlich ist $\{m_b \mid b \in B\}$ eine Basis von F . Wir zeigen: $M = \text{Tor}(M) \oplus F$. Wir haben $F = \tau(M/\text{Tor}(M))$ mit einem Isomorphismus

$$\tau : M/\text{Tor}(M) \rightarrow F : \sum_{b \in B} \alpha_b b + \text{Tor}(M) \mapsto \sum_{b \in B} \alpha_b m_b.$$

Für $m \in M$ gilt $m = \tau(\varphi(m)) + (m - \tau(\varphi(m))) \in F + \text{Tor}(M)$. Ist andererseits $x \in F \cap \text{Tor}(M)$, so gilt $x = \tau(\tilde{m})$ mit $\tilde{m} \in M/\text{Tor}(M)$, also $0 = \varphi(x) = \varphi(\tau(\tilde{m})) = \tilde{m}$, folglich $x = \tau(\tilde{m}) = 0$ und $F \cap \text{Tor}(M) = \{0\}$. $\square$

5.17. Definition

Es seien R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Die invertierbaren Matrizen $U \in R^{n \times n}$ heißen *unimodular*. $\text{GL}(n, R)$ bezeichnet die Menge aller invertierbaren Matrizen.

5.18. Hilfssatz

- (i) Die unimodularen $(n \times n)$ -Matrizen über R bilden eine Gruppe $\text{GL}(n, R)$.
- (ii) $A \in R^{n \times n}$ ist genau dann unimodular, falls $\det(A) \in R^* = U(R)$ ist.

Beweis: Übungsaufgabe.

5.19. Hilfssatz

Es seien R ein kommutativer Ring mit Eins und M ein freier R -Modul vom Rang n . Für zwei Basen $b_1, \dots, b_n$ und $c_1, \dots, c_n$ von M existiert $U \in \text{GL}(n, R)$ mit

$$(b_1, \dots, b_n) = (c_1, \dots, c_n)U.$$

5.20. Hilfssatz

Es seien R ein Hauptidealring und $a_1, \dots, a_n \in R$. Dann existiert eine Matrix $A \in R^{n \times n}$ mit erster Zeile $a_1, \dots, a_n$ und $\det(A) = \text{ggT}(a_1, \dots, a_n)$.

Beweis: Der Induktionsanfang ($n = 1$) ist trivial. Für $n > 1$ existiert nach Induktionsannahme $\tilde{A} = (\tilde{a}_{i,j}) \in R^{(n-1) \times (n-1)}$ mit $\tilde{a}_{1,j} = a_j$ ($1 \leq j \leq n-1$) und $\det(\tilde{A}) = \text{ggT}(a_1, \dots, a_{n-1})$. Sei $c := \text{ggT}(\det(\tilde{A}), a_n)$. Dann existieren $u, v \in R$ mit $c = u \det(\tilde{A}) + va_n$. Setze

$$A := \left(\begin{array}{ccc|c} & & & a_n \\ & & & 0 \\ & & & \vdots \\ & & & 0 \\ \hline b_1 & \cdots & b_{n-1} & u \end{array} \right)$$

mit $b_i = -va_i / \det(\tilde{A})$ ($1 \leq i \leq n-1$) und erhalte $\det(A) = u \det(\tilde{A}) + a_n v = c$. $\square$

Example: Let $R = \mathbb{Z}$ and $a_1 = 30$, $a_2 = 42$, $a_3 = 70$, $a_4 = 105$. By calculating

$$\begin{aligned} d_1 &= 30, \\ d_2 &= 6 = 3 \cdot 30 + (-2) \cdot 42, \\ d_3 &= 2 = 12 \cdot 6 + (-1) \cdot 70, \\ d_4 &= 1 = 53 \cdot 2 + (-1) \cdot 105 \end{aligned}$$

we get

$$A = \begin{pmatrix} 30 & 42 & 70 & 105 \\ 2 & 3 & 0 & 0 \\ 5 & 7 & 12 & 0 \\ 15 & 21 & 35 & 53 \end{pmatrix}.$$

We note that the actual computation of A requires the calculation of a presentation of $d = \gcd(a, b)$ by a and b and is therefore practicable in Euclidean rings only.

5.21. Hilfssatz

Es seien R ein Hauptidealring und $a_1, \dots, a_n \in R$. Dann existiert $U \in \text{GL}(n, R)$ mit $(a_1, \dots, a_n) \cdot U = (c, 0, \dots, 0)$ für $c := \text{ggT}(a_1, \dots, a_n)$.

Beweis: Bilde $A = (a_{ij}) \in R^{n \times n}$ mit $\det(A) = c$ wie in 6.20. Setze $\tilde{A} = (\tilde{a}_{ij}) \in R^{n \times n}$ mittels $\tilde{a}_{ij} := a_{ij}$ ($2 \leq i \leq n, 1 \leq j \leq n$) und $\tilde{a}_{1j} := \frac{a_{1j}}{c}$ ($1 \leq j \leq n$). $\tilde{A}$ ist dann unimodular wegen $\det(\tilde{A}) = 1$, und es gilt $(c, 0, \dots, 0)\tilde{A} = (a_1, \dots, a_n)$. Also erfüllt $\tilde{A}^{-1}$ die Behauptung. $\square$

Für einen kommutativen Ring R mit Eins ist

$$a \sim b : \iff \exists u \in R^* : a = ub$$

eine Äquivalenzrelation auf R . Im folgenden sei $\mathcal{R} \subseteq R$ ein Vertretersystem für die Äquivalenzklassen (für $R = \mathbb{Z}$ etwa $\mathcal{R} = \mathbb{Z}^{\geq 0}$).

5.22. Satz (Hermite Normalform)

Für einen Hauptidealring und eine Matrix $A \in R^{m \times n}$ existiert $U \in \text{GL}(n, R)$, so dass AU eine untere Dreiecksmatrix ist, deren Diagonalelemente in $\mathcal{R}$ liegen. AU heißt *Hermite-Normalform* von A .

Beweis: Der Induktionsanfang ($n = 1$) ist trivial.

Sei nun $n > 1$. Zu $c = \text{ggT}(a_{11}, \dots, a_{1n}) \in \mathcal{R}$ existiert nach 6.21 $U_1 \in \text{GL}(n, R)$ mit

$$AU_1 = \left(\begin{array}{c|ccc} c & 0 & \dots & 0 \\ \hline * & & & \tilde{A} \end{array} \right).$$

Durch Anwendung der Induktionsannahme auf $\tilde{A}$ erhält man eine Matrix der gewünschten Gestalt. $\square$

Bemerkung Es sei G eine Abelsche Gruppe die mit Erzeugern und Relationen definiert ist: $G := \langle x_1, \dots, x_n \mid \sum_{i=1}^n a_{i,j}x_i = 0, 1 \leq j \leq m \rangle$. Dann kann mit Hilfe der HNF die Anzahl der Relationen auf n beschränkt werden. Ferner liefert dies ein Verfahren, um die Endlichkeit von G nachzuweisen.

5.23. Satz (Smith Normalform)

Für einen Hauptidealring R und $A = (a_{ij}) \in R^{m \times n}$ setze $r = \min(m, n)$. Dann existieren $V \in \text{GL}(m, R)$ und $U \in \text{GL}(n, R)$, so dass für $S(A) := (s_{i,j}) := VAU$ gelten:

- (i) $s_{i,j} = 0$ ($1 \leq i \leq m, 1 \leq j \leq n, i \neq j$),
- (ii) $s_{i,i} | s_{j,j}$ ($1 \leq i \leq j \leq r$),
- (iii) $s_{i,i} \in \mathcal{R}$ ($1 \leq i \leq r$).

$S(A)$ ist eindeutig bestimmt und heißt *Smith-Normalform* von A . Die Diagonalelemente in der Smith Normalform heißen *Elementarteiler*.

Beweis: Wir bestimmen zunächst $\tilde{V} \in \text{GL}(m, R)$ und $\tilde{U} \in \text{GL}(n, R)$, so dass $\tilde{V}A\tilde{U}$ die Bedingung (1) erfüllt. Der Induktionsanfang ($n = 1$) folgt aus 6.21. Es sei nun $n > 1$. Durch Anwenden von 6.22 erreicht man

$$A\tilde{U}_1 = \left(\begin{array}{c|c} c_1 & 0 \\ * & A_1 \end{array} \right),$$

und weiter, falls c_1 nicht alle Elemente der ersten Spalte (Zeilen 2 bis m) teilt,

$$\tilde{V}_2 A \tilde{U}_1 = \left(\begin{array}{c|c} c_2 & * \\ 0 & A_2 \end{array} \right), \quad \tilde{V}_2 A \tilde{U}_1 \tilde{U}_2 = \left(\begin{array}{c|c} c_3 & 0 \\ * & A_3 \end{array} \right), \quad \dots$$

Wegen $c_{i+1} | c_i$ und $c_1 | a_{11}$ terminiert dieser Prozeß, weil a_{11} nur endlich viele Primteiler besitzt. Subtraktionen passender Vielfacher der ersten Zeile oder Spalte liefern

$$\left(\begin{array}{c|c} c_k & 0 \\ 0 & A_k \end{array} \right).$$

Durch Anwendung der Induktionsannahme auf A_k erhält man eine Matrix, welche die Bedingung (1) erfüllt.

Um nun $s_{ii} | s_{jj}$ ($1 \leq i < j \leq r$) zu erreichen, ersetzt man durch passende Spalten- und Zeilenoperationen s_{ii} durch $\text{ggT}(s_{ii}, s_{jj}) \in \mathcal{R}$ und s_{jj} durch $\text{kgV}(s_{ii}, s_{jj}) \in \mathcal{R}$:

Es sei $g := \text{ggT}(s_{ii}, s_{jj}) = rs_{ii} + ts_{jj}$ und $l := s_{ii}s_{jj}/g = \text{kgV}(s_{ii}, s_{jj})$. Dann gilt:

$$\begin{aligned} \left(\begin{array}{cc} s_{ii} & 0 \\ 0 & s_{jj} \end{array} \right) & \cdot \begin{pmatrix} 1 & 0 \\ t & 1 \\ \rightarrow \end{pmatrix} & \left(\begin{array}{cc} s_{ii} & 0 \\ ts_{jj} & s_{jj} \end{array} \right) \\ & \cdot \begin{pmatrix} 1 & 0 \\ r & 1 \\ \rightarrow \end{pmatrix} & \left(\begin{array}{cc} s_{ii} & 0 \\ g & s_{jj} \end{array} \right) \\ & \cdot \begin{pmatrix} 1 & -s_{ii}/g \\ 0 & 1 \\ \rightarrow \end{pmatrix} & \left(\begin{array}{cc} 0 & -s_{ii}s_{jj}/g \\ g & s_{jj} \end{array} \right) \\ & \cdot \begin{pmatrix} 1 & l/s_{ii} \\ 0 & 1 \\ \rightarrow \end{pmatrix} & \left(\begin{array}{cc} 0 & -l \\ g & 0 \end{array} \right) \\ & \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \\ \rightarrow \end{pmatrix} & \left(\begin{array}{cc} g & 0 \\ 0 & l \end{array} \right). \end{aligned}$$

Zum Beweis der Eindeutigkeit sei $d_i(A)$ der ggT aller (i, i) -Minoren von A ($1 \leq i \leq r$). Es gilt $d_{i-1}(A) | d_i(A)$ ($2 \leq i \leq r$). Ferner folgt $d_i(A) | d_i(A \cdot B)$ für $B \in R^{n \times n}$, denn die Spalten von $A \cdot B$ sind Linearkombinationen der Spalten von A , so dass jeder Minor von $A \cdot B$ Produkt eines Minors von A ist. Analog folgt $d_i(A) | d_i(C \cdot A)$ für $C \in R^{m \times m}$. Damit erhält man

$$d_i(A) | d_i(A \cdot U) | d_i(V \cdot A \cdot U) = d_i(S(A)) | d_i(V^{-1} \cdot S(A) \cdot U^{-1}) = d_i(A).$$

Also gilt

$$d_i(A) = d_i(S(A)) = \prod_{j=1}^i s_{jj} \quad (1 \leq i \leq r).$$

Wegen $s_{ii} = d_i(A)/d_{i-1}(A)$ ($1 \leq i \leq r$, $d_0(A) := 1$) ist man fertig. $\square$

Bemerkung Aus der SNF folgt unmittelbar der Hauptsatz über endlich erzeugte Abelsche Gruppen: $G \cong C_{n_1} \times \cdots \times C_{n_n} \times \mathbb{Z}^r$ mit $n_1 | \dots | n_n$ und $r \geq 0$. Unter diesen Bedingungen sind die n_i und das r eindeutig bestimmt.

5.24. Hilfssatz

M sei ein freier Modul mit Basis b_i ($1 \leq i \leq n$). Ferner sei $i \in \{1, \dots, n\}$ und $c_i := \sum_{j=1}^n \gamma_j b_j \in M$. Dann ist $b_1, \dots, b_{i-1}, c_i$ genau dann zu einer Basis von M ergänzbar, wenn $\text{ggT}(\gamma_i, \dots, \gamma_n) = 1$ ist.

Beweis $\text{ggT}(\gamma_i, \dots, \gamma_n) = 1 \iff \exists U \in GL(n+1-i, R) : (\gamma_i, \dots, \gamma_n)U = (1, 0, \dots, 0)$ nach 5.21

$$\iff (b_1, \dots, b_n) \left(\begin{array}{c|ccc} & \gamma_1 & & \\ & \vdots & & 0 \\ I_{i-1} & & & \\ \hline & \gamma_{i-1} & & \\ \hline 0 & & & (U^{-1})^t \end{array} \right) \text{Basis von } M. \quad \square$$

5.25. Gitter - Definition

Es seien $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{R}^n$ linear unabhängig über $\mathbb{R}$. Dann nennt man den $\mathbb{Z}$ -Modul

$$\Lambda := \left\{ \sum_{i=1}^k \lambda_i \mathbf{b}_i \mid \lambda_1, \dots, \lambda_k \in \mathbb{Z} \right\}$$

ein Gitter der Dimension k . $d(\Lambda) := \det(\mathbf{b}_i^t \cdot \mathbf{b}_j)_{1 \leq i, j \leq k}^{1/2}$ heißt *Gitterdiskriminante* von Λ , und

$$\Pi(\Lambda) := \left\{ \mathbf{x} \in \mathbb{R}^n \mid \mathbf{x} = \sum_{i=1}^k \xi_i \mathbf{b}_i, 0 \leq \xi_i < 1 \ (1 \leq i \leq k) \right\}$$

bezeichnet man als das *Fundamentalparallelotop* (*Grundmasche*) von Λ . $\Lambda' \subseteq \Lambda$ heißt Teilgitter von Λ , sofern Λ' selbst ein Gitter im $\mathbb{R}^n$ ist.

Im folgenden sei Λ ein k -dimensionales Gitter im $\mathbb{R}^n$ mit $\mathbb{Z}$ -Basis $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{R}^n$.

5.26. Hilfssatz

- (i) $d(\Lambda) = \text{vol}_k(\Pi(\Lambda))$.
(ii) Ist Λ' ein k -dimensionales Teilgitter von Λ mit einer Gitterbasis $\mathbf{c}_1, \dots, \mathbf{c}_k$, so gilt

$$d(\Lambda') = |\det(U)| d(\Lambda)$$

für $U \in \mathbb{Z}^{k \times k}$ mit $(\mathbf{c}_1, \dots, \mathbf{c}_k) = (\mathbf{b}_1, \dots, \mathbf{b}_k)U$.

Beweis:

- (i) Dies folgt mit dem Orthogonalisierungsverfahren von Gram-Schmidt aus der Tatsache, dass das Volumen eines Quaders gleich dem Produkt der Längen der aufspannenden Kanten ist.
(ii) Trivial. □

5.27. Hilfssatz

Ist Λ' ein k -dimensionales Teilgitter von Λ , so gilt

$$(\Lambda : \Lambda') = \frac{d(\Lambda')}{d(\Lambda)}.$$

Beweis: Es sei $\mathbf{c}_1, \dots, \mathbf{c}_k$ eine $\mathbb{Z}$ -Basis von Λ' . Nach 6.22 können wir annehmen, dass die Transformationsmatrix $U = (u_{ij}) \in \mathbb{Z}^{k \times k}$ mit $(\mathbf{c}_1, \dots, \mathbf{c}_k) = (\mathbf{b}_1, \dots, \mathbf{b}_k)U$ eine untere Dreiecksmatrix ist. Da

$$\mathcal{V} := \left\{ \sum_{i=1}^k m_i \mathbf{b}_i + \Lambda' \mid 0 \leq m_i < u_{ii}, m_i \in \mathbb{Z} (1 \leq i \leq k) \right\}$$

ein komplettes Vertretersystem von Λ/Λ' ist, folgt $\#\mathcal{V} = (\Lambda : \Lambda')$. Andererseits gilt nach 6.26 (ii)

$$\frac{d(\Lambda')}{d(\Lambda)} = |\det(U)| = \prod_{i=1}^k u_{ii} = \#\mathcal{V}. \quad \square$$

5.28. Algorithmus (Quadratische Ergänzung)

Zu $A \in \mathbb{R}^{k \times k}$ positiv definit wird eine obere Dreiecksmatrix $Q \in \mathbb{R}^{k \times k}$ berechnet, so dass

$$\mathbf{x}^t \cdot A \cdot \mathbf{x} = \sum_{i=1}^k q_{ii} \left(x_i + \sum_{j=i+1}^k q_{ij} x_j \right)^2$$

gilt.

- (i) (Initialisierung) Setze $Q \leftarrow A$.
- (ii) Für $i = 1, \dots, k-1$ setze $q_{ji} \leftarrow q_{ij}, q_{ij} \leftarrow \frac{q_{ij}}{q_{ii}}$ ($i+1 \leq j \leq k$) und weiter
 $q_{\mu\nu} \leftarrow q_{\mu\nu} - q_{\mu i} q_{i\nu}$ ($i+1 \leq \mu \leq \nu \leq k$).
- (iii) Setze $q_{ij} \leftarrow 0$ ($1 \leq j < i \leq k$).

Es sei $A \in \mathbb{R}^{k \times k}$ positiv definit mit zugehöriger quadratischer Form $f(\mathbf{x}) = \mathbf{x}^t \cdot A \cdot \mathbf{x}$. Quadratische Ergänzung liefert dann

$$\begin{aligned} f(\mathbf{x}) &= \sum_{i=1}^k q_{ii} (x_i + \sum_{j=i+1}^k q_{ij} x_j)^2 \\ &= q_{11} (x_1 + q_{12} x_2 + \dots + q_{1k} x_k)^2 + \underbrace{\sum_{i=2}^k q_{ii} \left(x_i + \sum_{j=i+1}^k q_{ij} x_j \right)^2}_{=: g(\mathbf{x})}. \end{aligned}$$

Wir betrachten nun die lineare Abbildung $\varphi : \mathbb{R}^k \rightarrow \mathbb{R}^k$ mit zugehöriger Matrix

$$U = \begin{pmatrix} 1 & -q_{12} & \dots & -q_{1k} \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}.$$

Offensichtlich gilt $\det(U) = 1$ und weiter

$$f(U\mathbf{x}) = q_{11} x_1^2 + g(\mathbf{x}) = \mathbf{x}^t (U^t \cdot A \cdot U) \mathbf{x}.$$

g läßt sich als quadratische Form in $k-1$ Variablen (eben $x_2, \dots, x_k$) auffassen. Ist dann $B \in \mathbb{R}^{(k-1) \times (k-1)}$ die zugehörige Matrix, so gilt

$$\det(A) = \det(U^t \cdot A \cdot U) = \det \left(\begin{array}{c|ccc} q_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array} \right) = q_{11} \det(B).$$

Induktiv folgt daraus $\det(A) = \prod_{i=1}^k q_{ii}$.

5.29. Algorithmus (Auszählalgorithmus)

Zu $A \in \mathbb{R}^{k \times k}$ und $C > 0$ bestimmen wir alle $\mathbf{0} \neq \mathbf{x} \in \mathbb{Z}^k$ mit $\mathbf{x}^t \cdot A \cdot \mathbf{x} \leq C$.

- (i) Bestimme $Q \in \mathbb{R}^{k \times k}$ wie in 6.28.
- (ii) (Initialisierung) Setze $i \leftarrow k, T_i \leftarrow C, U_i \leftarrow 0$.
- (iii) (Schranken für x_i) Setze $Z \leftarrow \sqrt{\frac{T_i}{q_{ii}}}, B_i \leftarrow \lfloor Z - U_i \rfloor$ und weiter
 $x_i \leftarrow \lceil -Z - U_i \rceil - 1$.
- (iv) Setze $x_i \leftarrow x_i + 1$. Falls $x_i \leq B_i$, so gehe zu Schritt 6.
- (v) Setze $i \leftarrow i - 1$ und gehe zu Schritt 4.

- (vi) Falls $i = 1$, so gehe zu Schritt 7, sonst setze $i \leftarrow i - 1, U_i \leftarrow \sum_{j=i+1}^k q_{ij}x_j, T_i \leftarrow T_{i+1} - q_{i+1,i+1}(x_{i+1} + U_{i+1})^2$ und gehe zu 2.
- (vii) Für $\mathbf{x} = 0$ terminiere, sonst gebe $\mathbf{x}$ sowie $-\mathbf{x}$ aus und gehe zu Schritt 4.

5.30. Satz (Diskretheit von Gittern)

Zu $\mathbf{x} \in \mathbb{R}^n$ und $C > 0$ gibt es nur endlich viele $\mathbf{y} \in \Lambda$ mit $\|\mathbf{x} - \mathbf{y}\| \leq C$.
Beweis: Konsequenz aus dem Auszählalgorithmus. $\square$

5.31. Korollar

Es existiert $\delta > 0$ mit $\|\mathbf{x} - \mathbf{y}\| > \delta \quad \forall \mathbf{x}, \mathbf{y} \in \Lambda, \mathbf{x} \neq \mathbf{y}$.

Beweis: Angenommen für alle $n \in \mathbb{N}$ existieren $\mathbf{x}_n, \mathbf{y}_n \in \Lambda, \mathbf{x}_n \neq \mathbf{y}_n$, mit $\|\mathbf{x}_n - \mathbf{y}_n\| \leq \frac{1}{n}$. Dann folgt $\#\{\mathbf{z} \in \Lambda \mid \|\mathbf{z}\| \leq 1\} = \infty$ im Widerspruch zu 6.30. $\square$

5.32. Korollar

Es sei $(\mathbf{x}_n)_{n \in \mathbb{N}}$ eine Folge in Λ . Konvergiert $(\mathbf{x}_n)_{n \in \mathbb{N}}$ gegen $\mathbf{x} \in \mathbb{R}^n$, so gilt $\mathbf{x} \in \Lambda$.

Beweis: Λ ist nach 6.31 abgeschlossen im $\mathbb{R}^n$. $\square$

5.33. Satz

Es sei $k = n$. Ist $C \subseteq \mathbb{R}^n$ konvex und ursprungssymmetrisch, so enthält C einen nicht-trivialen Gitterpunkt ($\mathbf{x} \neq \mathbf{0}$), falls eine der beiden folgenden Bedingungen erfüllt ist:

- (i) $\text{vol}(C) > 2^n d(\Lambda)$;
- (ii) $\text{vol}(C) \geq 2^n d(\Lambda)$ und C kompakt.

Beweis:

- (i) Für das Fundamentalparallelotop $\Pi(\Lambda)$ gilt

$$\mathbb{R}^n = \bigcup_{\mathbf{y} \in \Lambda} \Pi(\Lambda) + \mathbf{y}.$$

Damit folgt

$$\frac{1}{2}C = \frac{1}{2}C \cap \mathbb{R}^n = \bigcup_{\mathbf{y} \in \Lambda} \left(\frac{1}{2}C \cap (\mathbf{y} + \Pi(\Lambda)) \right)$$

und weiter

$$\begin{aligned}
\text{vol}(\Pi(\Lambda)) &= d(\Lambda) < \frac{1}{2^n} \text{vol}(C) = \text{vol}\left(\frac{1}{2}C\right) \\
&= \text{vol}\left(\bigcup_{\mathbf{y} \in \Lambda} \left(\frac{1}{2}C \cap (\mathbf{y} + \Pi(\Lambda))\right)\right) \\
&= \sum_{\mathbf{y} \in \Lambda} \text{vol}\left(\frac{1}{2}C \cap (\mathbf{y} + \Pi(\Lambda))\right) \\
&= \sum_{\mathbf{y} \in \Lambda} \text{vol}\left(\left(\frac{1}{2}C - \mathbf{y}\right) \cap \Pi(\Lambda)\right).
\end{aligned}$$

Angenommen $(\frac{1}{2}C - \mathbf{u}) \cap (\frac{1}{2}C - \mathbf{v}) = \emptyset \forall \mathbf{u}, \mathbf{v} \in \Lambda, \mathbf{u} \neq \mathbf{v}$, so folgt

$$\begin{aligned}
\sum_{\mathbf{y} \in \Lambda} \text{vol}\left(\left(\frac{1}{2}C - \mathbf{y}\right) \cap \Pi(\Lambda)\right) &= \text{vol}\left(\left(\bigcup_{\mathbf{y} \in \Lambda} \left(\frac{1}{2}C - \mathbf{y}\right)\right) \cap \Pi(\Lambda)\right) \\
&\leq \text{vol}(\Pi(\Lambda)),
\end{aligned}$$

offensichtlich ein Widerspruch. Also existieren $\mathbf{y}, \mathbf{z} \in \Lambda, \mathbf{y} \neq \mathbf{z}$, mit $(\frac{1}{2}C - \mathbf{y}) \cap (\frac{1}{2}C - \mathbf{z}) \neq \emptyset$. Für $\mathbf{c}_1, \mathbf{c}_2 \in C$ mit $\frac{1}{2}\mathbf{c}_1 - \mathbf{y} = \frac{1}{2}\mathbf{c}_2 - \mathbf{z}$ folgt dann

$$0 \neq \mathbf{y} - \mathbf{z} = \frac{1}{2}\mathbf{c}_1 - \frac{1}{2}\mathbf{c}_2 = \frac{1}{2}\mathbf{c}_1 + \frac{1}{2}(-\mathbf{c}_2) \in C.$$

- (ii) Wähle zunächst eine monotone Nullfolge $(e_n)_{n \in \mathbb{N}}$ in $\mathbb{R}^{>0}$ und bilde

$$C_n := (1 + e_n)C \quad (n \in \mathbb{N}).$$

C_n ist offensichtlich für jedes $n \in \mathbb{N}$ konvex sowie ursprungssymmetrisch, und es gilt $\text{vol}(C_n) > 2^n d(\Lambda)$. Zu jedem $n \in \mathbb{N}$ existiert nach (a) also $\mathbf{x}_n \in C_n \cap \Lambda \setminus \{0\}$. Da C_1 kompakt ist, besitzt $(\mathbf{x}_n)_{n \in \mathbb{N}}$ eine konvergente Teilfolge $(\mathbf{x}_{n_j})_{j \in \mathbb{N}}$ mit $\mathbf{x} := \lim_{j \rightarrow \infty} \mathbf{x}_{n_j} \in C$, also $\mathbf{x} \in \Lambda$ nach 6.32. $\square$

Sukzessive Minima

5.34. Definition

Für $i \in \{1, \dots, k\}$ heißt

$$M_i := \min\{\gamma > 0 \mid \exists x_1, \dots, x_i \in \Lambda \text{ linear unabhängig mit } \|x_\nu\|^2 \leq \gamma \ (1 \leq \nu \leq i)\}$$

i -tes sukzessives Minimum des Gitters Λ .

5.35. Hilfssatz

- (i) Es existieren $\mathbf{y}_1, \dots, \mathbf{y}_k \in \Lambda$ linear unabhängig mit $\|\mathbf{y}_i\|^2 = M_i$ ($1 \leq i \leq k$).
- (ii) $\mathbf{v} \in \Lambda$ mit $\|\mathbf{v}\|^2 = M_1$ lässt sich zu einer Basis von Λ ergänzen.

Beweis:

- (i) Trivialerweise existiert $\mathbf{y}_1 \in \Lambda$ mit $\|\mathbf{y}_1\|^2 = M_1$. Sind nun $\mathbf{y}_1, \dots, \mathbf{y}_{j-1} \in \Lambda$ gefunden mit $\|\mathbf{y}_i\|^2 = M_i$ ($1 \leq i < j$), so existieren nach Definition $\mathbf{x}_1, \dots, \mathbf{x}_j \in \Lambda$ linear unabhängig mit $\|\mathbf{x}_i\|^2 \leq M_j$ ($1 \leq i \leq j$). Insbesondere existiert $m \in \{1, \dots, j\}$, so dass $\mathbf{y}_1, \dots, \mathbf{y}_{j-1}, \mathbf{x}_m$ linear unabhängig sind. O.B.d.A. können wir $m = j$ und $M_1 < M_j$ annehmen. Würde nun $\|\mathbf{x}_j\|^2 < M_j$ gelten, so existierte ein $r \in \{0, \dots, j-2\}$ mit

$$M_{j-r-1} < M_{j-r} = \dots = M_j$$

und $\mathbf{y}_1, \dots, \mathbf{y}_{j-r-1}, \mathbf{x}_j$ linear unabhängig im Widerspruch zur Definition von M_{j-r} . Also folgt $\|\mathbf{x}_j\|^2 = M_j$.

- (ii) Konsequenz aus (5.20). $\square$

5.36. Satz

Es existiert eine nur von k abhängige Konstante $\gamma_k \in \mathbb{R}$ (Hermitesche-Konstante), welche

$$M_1^k \leq \gamma_k^k d(\Lambda)^2$$

für alle k -dimensionalen Gitter Λ leistet und minimal mit dieser Eigenschaft ist.

Beweis: Wir zeigen $M_1^k \leq C_k d(\Lambda)^2$ für

$$C_k := \left(\frac{4}{3}\right)^{\frac{1}{2}k(k-1)}.$$

Der Induktionsanfang ($k = 1$) ist trivial. Sei also nun $k > 1$. Nach 6.35 können wir $\|\mathbf{b}_1\|^2 = M_1$ annehmen. Bilde

$$f(\mathbf{x}) = \sum_{i,j=1}^k x_i x_j b_i^t b_j \quad (\mathbf{x} = \sum_{\nu=1}^k x_\nu \mathbf{b}_\nu).$$

Dann gilt

$$f(\mathbf{x}) = M_1(x_1 + \sum_{j=2}^k q_{1j}x_j)^2 + g(x_2, \dots, x_k)$$

mit $\det(A) = d(\Lambda)^2$ und

$$\det(B) = \frac{d(\Lambda)^2}{M_1},$$

sofern A bzw. B die zugehörigen Matrizen zu den quadratischen Formen f bzw. g sind. Seien nun $y_2, \dots, y_k \in \mathbb{Z}$ mit

$$g(y_2, \dots, y_k) = \min\{g(x_2, \dots, x_k) \mid x_2, \dots, x_k \in \mathbb{Z}, |x_2| + \dots + |x_k| > 0\}.$$

Nach Induktionsannahme folgt

$$g(y_2, \dots, y_k)^{k-1} \leq C_{k-1} \frac{d(\Lambda)^2}{M_1}.$$

Wähle $y_1 \in \mathbb{Z}$ mit

$$\left| y_1 + \sum_{j=2}^k q_{1j}y_j \right| \leq \frac{1}{2}.$$

Für $\mathbf{y} := y_1 \mathbf{b}_1 + \dots + y_k \mathbf{b}_k \in \Lambda \setminus \{0\}$ folgt dann

$$M_1 \leq f(\mathbf{y}) \leq \frac{1}{4}M_1 + \left(C_{k-1} \frac{d(\Lambda)^2}{M_1} \right)^{\frac{1}{k-1}}.$$

Damit folgt

$$M_1 \leq \frac{4}{3} \left(C_{k-1} \frac{d(\Lambda)^2}{M_1} \right)^{\frac{1}{k-1}},$$

und weiter

$$\begin{aligned} M_1^k &\leq \left(\frac{4}{3} \right)^{k-1} C_{k-1} d(\Lambda)^2 = \left(\frac{4}{3} \right)^{k-1} \left(\frac{4}{3} \right)^{\frac{1}{2}(k-2)(k-1)} d(\Lambda)^2 \\ &= \left(\frac{4}{3} \right)^{\frac{1}{2}k(k-1)} d(\Lambda)^2 = C_k d(\Lambda)^2. \end{aligned}$$

□

5.37. Satz

Es gilt $M_1 \cdot \dots \cdot M_k \leq \gamma_k^k d(\Lambda)^2$.

Beweis: Es seien $\mathbf{y}_1, \dots, \mathbf{y}_k \in \Lambda$ linear unabhängig mit $\|\mathbf{y}_i\|^2 = M_i$ ($1 \leq i \leq k$). Ferner sei $Q \in \mathbb{Q}^{k \times k}$ mit

$$(\mathbf{b}_1, \dots, \mathbf{b}_k) = (\mathbf{y}_1, \dots, \mathbf{y}_k) \cdot Q.$$

Bilde $Y := (\mathbf{y}_i^t \mathbf{y}_j)_{1 \leq i, j \leq k}$ sowie $B := (\mathbf{b}_i^t \mathbf{b}_j)_{1 \leq i, j \leq k}$. Für $\mathbf{x} \in \Lambda$ mit

$$\mathbf{x} = \sum_{i=1}^k x_{b_i} \mathbf{b}_i = \sum_{i=1}^k x_{y_i} \mathbf{y}_i \quad (x_{b_1}, \dots, x_{b_k} \in \mathbb{Z}, y_{b_1}, \dots, y_{b_k} \in \mathbb{Q})$$

gilt dann

$$\begin{aligned}\|\mathbf{x}\|^2 &= (x_{b_1}, \dots, x_{b_k}) \cdot B \cdot (x_{b_1}, \dots, x_{b_k})^t \\ &= (x_{b_1}, \dots, x_{b_k}) \cdot Q^t \cdot Y \cdot Q \cdot (x_{b_1}, \dots, x_{b_k})^t \\ &= (x_{y_1}, \dots, x_{y_k}) \cdot Y \cdot (x_{y_1}, \dots, x_{y_k})^t.\end{aligned}$$

Sei f die zu Y gehörige quadratische Form. Quadratische Ergänzung liefert dann

$$\begin{aligned}(z_1, \dots, z_k) \cdot Y \cdot (z_1, \dots, z_k)^t &= f(z_1, \dots, z_k) \\ &= \sum_{i=1}^k q_{ii} \underbrace{\left(z_i + \sum_{j=i+1}^k q_{ij} z_j \right)^2}_{=: g_i(z_1, \dots, z_k)}.\end{aligned}$$

Damit bildet man eine neue quadratische Form

$$h(z_1, \dots, z_k) := \sum_{i=1}^k \frac{1}{M_i} g_i(z_1, \dots, z_k).$$

Ist C die zugehörige Matrix von h , so gilt

$$\det(Q^t \cdot C \cdot Q) = \det(Q)^2 \cdot \det(C) = \det(Q)^2 \frac{\det(Y)}{M_1 \cdot \dots \cdot M_k} = \frac{d(\Lambda)^2}{M_1 \cdot \dots \cdot M_k}.$$

Also erhält man aus 6.36

$$\begin{aligned}\min\{(z_1, \dots, z_k) \cdot Q^t \cdot C \cdot Q \cdot (z_1, \dots, z_k)^t \mid z_1, \dots, z_k \in \mathbf{Z}, |z_1| + \dots + |z_k| > 0\}^k \\ \leq \gamma_k^k \frac{d(\Lambda)^2}{M_1 \cdot \dots \cdot M_k}.\end{aligned}$$

Es sei nun $\mathbf{x} \in \Lambda \setminus \{0\}$ beliebig. Für m maximal mit $x_{y_m} \neq 0$ folgt

$$\begin{aligned}(x_{b_1}, \dots, x_{b_k}) \cdot Q^t \cdot C \cdot Q \cdot (x_{b_1}, \dots, x_{b_k})^t \\ &= h(x_{y_1}, \dots, x_{y_k}) \\ &= \sum_{i=1}^m \frac{1}{M_i} g_i(x_{y_1}, \dots, x_{y_k}) \geq \frac{1}{M_m} \sum_{i=1}^m g_i(x_{y_1}, \dots, x_{y_k}) \\ &= \frac{1}{M_m} f(x_{y_1}, \dots, x_{y_k}) = \frac{1}{M_m} \|\mathbf{x}\|^2 \geq 1,\end{aligned}$$

denn $\mathbf{x}$ ist linear unabhängig von $\mathbf{y}_1, \dots, \mathbf{y}_{m-1}$, weswegen $\|\mathbf{x}\|^2 \geq M_m$ gilt. $\square$

Zu $\mathbf{b}_1, \dots, \mathbf{b}_k$ sei nun $\mathbf{b}_1^*, \dots, \mathbf{b}_k^* \in \mathbb{R}^n$ die Orthogonalbasis von $\mathbb{R}\mathbf{b}_1 + \dots + \mathbb{R}\mathbf{b}_n$, welche man mit dem Verfahren von E. Schmidt berechnet, also

$$\begin{aligned}\mathbf{b}_i^* &:= \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^* \quad (1 \leq i \leq k), \\ \mu_{ij} &:= \frac{\mathbf{b}_i^t \mathbf{b}_j^*}{\mathbf{b}_j^{*t} \mathbf{b}_j^*} \quad (1 \leq j < i \leq k).\end{aligned}$$

5.38. Satz (Hadamard)

Es gilt

$$d(\Lambda) \leq \prod_{i=1}^k \|\mathbf{b}_i\|.$$

Beweis: Nach Konstruktion gilt

$$(\mathbf{b}_1^*, \dots, \mathbf{b}_k^*) = (\mathbf{b}_1, \dots, \mathbf{b}_k) \cdot Q$$

für $Q \in \mathbb{R}^{k \times k}$ mit $\det(Q) = 1$, also

$$\det(\mathbf{b}_i^t \cdot \mathbf{b}_j)^{1/2}_{1 \leq i, j \leq k} = \det(\mathbf{b}_i^{*t} \cdot \mathbf{b}_j^*)^{1/2}_{1 \leq i, j \leq k}.$$

Ferner gilt $\|\mathbf{b}_i^*\| \leq \|\mathbf{b}_i\|$ ($1 \leq i \leq k$) wegen

$$\|\mathbf{b}_i\|^2 = \|\mathbf{b}_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 \|\mathbf{b}_j^*\|^2 \geq \|\mathbf{b}_i^*\|^2 \quad (1 \leq i \leq k).$$

Damit folgt

$$d(\Lambda) = \det(\mathbf{b}_i^{*t} \cdot \mathbf{b}_j^*)^{1/2}_{1 \leq i, j \leq k} = \prod_{i=1}^k \|\mathbf{b}_i^*\| \leq \prod_{i=1}^k \|\mathbf{b}_i\|.$$

□

5.39. Korollar

Es gilt $d(\Lambda)^2 \leq M_1 \cdot \dots \cdot M_k$.

Beweis: Es seien $\mathbf{y}_1, \dots, \mathbf{y}_k \in \Lambda$ linear unabhängig mit $\|\mathbf{y}_i\|^2 = M_i$ ($1 \leq i \leq k$). Dann ist $\Lambda' := \mathbb{Z}\mathbf{y}_1 + \dots + \mathbb{Z}\mathbf{y}_k$ ein Teilgitter von Λ , und wir erhalten

$$d(\Lambda)^2 \leq d(\Lambda')^2 \leq \prod_{i=1}^k \|\mathbf{y}_i\|^2 = M_1 \cdot \dots \cdot M_k.$$

□

LLL–reduzierte Basen

5.40. Definition

Wir nennen eine Gitterbasis $\mathbf{b}_1, \dots, \mathbf{b}_k$ LLL–reduziert, falls für sie die Bedingungen gelten:

- (i) $|\mu_{ij}| \leq \frac{1}{2}$ ($1 \leq j < i \leq k$),
- (ii) $\|\mathbf{b}_i^* + \mu_{i,i-1} \mathbf{b}_{i-1}^*\|^2 \geq \frac{3}{4} \|\mathbf{b}_{i-1}^*\|^2$ ($1 < i \leq k$).

5.41. Satz

Ist die Basis $\mathbf{b}_1, \dots, \mathbf{b}_k$ LLL-reduziert, so gelten:

- (i) $\|\mathbf{b}_j\|^2 \leq 2^{i-1} \|\mathbf{b}_i^*\|^2$ ($1 \leq j < i \leq k$),
- (ii) $d(\Lambda) = \prod_{i=1}^k \|\mathbf{b}_i^*\| \leq \prod_{i=1}^k \|\mathbf{b}_i\| \leq 2^{\frac{1}{4}k(k-1)} d(\Lambda)$,
- (iii) $\|\mathbf{b}_1\| \leq 2^{\frac{1}{4}(k-1)} d(\Lambda)^{\frac{1}{k}}$,
- (iv) $\|\mathbf{b}_1\|^2 \leq 2^{k-1} \|\mathbf{x}\|^2 \forall \mathbf{x} \in \Lambda \setminus \{0\}$,
- (v) Für $\mathbf{x}_1, \dots, \mathbf{x}_t \in \Lambda$ linear unabhängig gilt

$$\|\mathbf{b}_j\|^2 \leq 2^{k-1} \max\{\|\mathbf{x}_1\|^2, \dots, \|\mathbf{x}_t\|^2\} \quad (1 \leq j \leq t).$$

Beweis:

(i) Zunächst gilt

$$\|\mathbf{b}_i^* + \mu_{i,i-1} \mathbf{b}_{i-1}^*\|^2 = \|\mathbf{b}_i^*\|^2 + \mu_{i,i-1}^2 \|\mathbf{b}_{i-1}^*\|^2 \quad (1 < i \leq k).$$

Also

$$\|\mathbf{b}_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|\mathbf{b}_{i-1}^*\|^2 \geq \frac{1}{2} \|\mathbf{b}_{i-1}^*\|^2 \quad (1 < i \leq k).$$

Daraus folgt induktiv zunächst

$$\|\mathbf{b}_j^*\|^2 \leq 2^{i-j} \|\mathbf{b}_i^*\|^2 \quad (1 \leq j \leq i \leq k)$$

und für $i \in \{1, \dots, k\}$ hiermit

$$\begin{aligned} \|\mathbf{b}_i\|^2 &= \|\mathbf{b}_i^* + \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^*\|^2 \leq \|\mathbf{b}_i^*\|^2 + \frac{1}{4} \sum_{j=1}^{i-1} \|\mathbf{b}_j^*\|^2 \\ &\leq \|\mathbf{b}_i^*\|^2 + \frac{1}{4} \|\mathbf{b}_i^*\|^2 \sum_{j=1}^{i-1} 2^{i-j} = \|\mathbf{b}_i^*\|^2 + \frac{1}{4} \|\mathbf{b}_i^*\|^2 \sum_{j=1}^{i-1} 2^j \\ &= \|\mathbf{b}_i^*\|^2 + \frac{1}{4} \|\mathbf{b}_i^*\|^2 (2^i - 2) = \|\mathbf{b}_i^*\|^2 \left(1 + \frac{1}{2} (2^{i-1} - 1)\right) \\ &= \|\mathbf{b}_i^*\|^2 \left(2^{i-2} + \frac{1}{2}\right) \leq 2^{i-1} \|\mathbf{b}_i^*\|^2. \end{aligned}$$

Damit ergibt sich $\|\mathbf{b}_j\|^2 \leq 2^{j-1} \|\mathbf{b}_j^*\|^2 \leq 2^{i-1} \|\mathbf{b}_i^*\|^2$ ($1 \leq j < i \leq k$).

(ii) Aus (i) folgt zunächst

$$\prod_{i=1}^k \|\mathbf{b}_i\| \leq \prod_{i=1}^k 2^{\frac{1}{2}(i-1)} \|\mathbf{b}_i^*\| = d(\Lambda) \prod_{i=1}^k 2^{\frac{1}{2}(i-1)} = 2^{\frac{1}{4}k(k-1)} d(\Lambda).$$

Die restliche Behauptung erhält man aus dem Beweis zu 6.38.

(iii) Aus (i) folgt

$$\|\mathbf{b}_1\|^{2k} = \prod_{i=1}^k \|\mathbf{b}_1\|^2 \leq \prod_{i=1}^k 2^{i-1} \|\mathbf{b}_i^*\|^2 = 2^{\frac{1}{2}k(k-1)} d(\Lambda)^2.$$

(iv) Sei $\mathbf{x} \in \Lambda \setminus \{0\}$ mit Darstellungen

$$\mathbf{x} = \sum_{i=1}^k x_i \mathbf{b}_i = \sum_{i=1}^k x_i^* \mathbf{b}_i^* \quad (x_1, \dots, x_k \in \mathbb{Z}, x_1^*, \dots, x_k^* \in \mathbb{R}).$$

Ist m der größte Index mit $x_m \neq 0$, so gilt gemäß Konstruktion $x_m = x_m^*$, also

$$\|\mathbf{x}\|^2 \geq x_m^2 \|\mathbf{b}_m^*\|^2 \geq \|\mathbf{b}_m^*\|^2.$$

Damit folgt aus (i)

$$\|\mathbf{b}_1\|^2 \leq 2^{m-1} \|\mathbf{b}_m^*\|^2 \leq 2^{m-1} \|\mathbf{x}\|^2.$$

(v) Für

$$\mathbf{x}_j = \sum_{i=1}^k x_{ij} \mathbf{b}_i \quad (x_{ij} \in \mathbb{Z}, 1 \leq i \leq k, 1 \leq j \leq t)$$

sei jeweils i_j der maximale Index mit $x_{i_j, j} \neq 0$. Wie in (d) folgt dann

$$\|\mathbf{x}_j\|^2 \geq x_{i_j, j}^2 \|\mathbf{b}_{i_j}^*\|^2 \geq \|\mathbf{b}_{i_j}^*\|^2 \quad (1 \leq j \leq t).$$

O.B.d.A. gelte nun $i_1 \leq \dots \leq i_t$, also $i_1 < \dots < i_t$, denn $\mathbf{x}_1, \dots, \mathbf{x}_t$ sind linear unabhängig, so folgt $i_j \geq j$ ($1 \leq j \leq t$) und damit aus (i)

$$\|\mathbf{b}_j\|^2 \leq 2^{i_j-1} \|\mathbf{b}_{i_j}^*\|^2 \leq 2^{k-1} \|\mathbf{b}_{i_j}^*\|^2 \leq 2^{k-1} \|\mathbf{x}_j\|^2 \quad (1 \leq j \leq t). \quad \square$$

5.42. LLL-Algorithmus

Aus einer Basis $\mathbf{b}_1, \dots, \mathbf{b}_k$ wird eine LLL-reduzierte Basis $\mathbf{c}_1, \dots, \mathbf{c}_k$ von Λ berechnet.

- (i) (Initialisierung) Setze $\mathbf{c}_i \leftarrow \mathbf{b}_i, C_i \leftarrow \|\mathbf{c}_i^*\|^2$ ($1 \leq i \leq k$) und $m \leftarrow 2$.
- (ii) Setze $l \leftarrow m - 1$.
- (iii) Falls $|\mu_{ml}| > \frac{1}{2}$, so setze

$$r \leftarrow \lfloor \mu_{ml} + \frac{1}{2} \rfloor, \quad \mathbf{c}_m \leftarrow \mathbf{c}_m - r \mathbf{c}_l,$$

$$\mu_{mj} \leftarrow \mu_{mj} - r \mu_{lj} \quad (1 \leq j \leq l - 1), \quad \mu_{ml} \leftarrow \mu_{ml} - r.$$

Für $l < m - 1$, gehe zu Schritt 5.

- (iv) Falls $C_m < (\frac{3}{4} - \mu_{m, m-1}^2) C_{m-1}$ gilt, so gehe zu Schritt 6.
- (v) Setze $l \leftarrow l - 1$. Für $l > 0$ gehe zu Schritt 3. Für $m = k$, terminiere, sonst setze $m \leftarrow m + 1$ und gehe zu Schritt 2.
- (vi) (Vertausche $\mathbf{c}_{m-1}$ und $\mathbf{c}_m$) Setze $\mu \leftarrow \mu_{m, m-1}, C \leftarrow C_m + \mu^2 C_{m-1}$ sowie $\mu_{m, m-1} \leftarrow \mu \frac{C_{m-1}}{C}, C_m \leftarrow \frac{C_{m-1} C_m}{C}, C_{m-1} \leftarrow C$. Dann setze

$$\begin{pmatrix} \mathbf{c}_{m-1} \\ \mathbf{c}_m \end{pmatrix} \leftarrow \begin{pmatrix} \mathbf{c}_m \\ \mathbf{c}_{m-1} \end{pmatrix}.$$

Ferner setze

$$\begin{pmatrix} \mu_{m-1, j} \\ \mu_{mj} \end{pmatrix} \leftarrow \begin{pmatrix} \mu_{mj} \\ \mu_{m-1, j} \end{pmatrix} \quad (1 \leq j \leq m - 2),$$

und für $i = m + 1, \dots, k$ schließlich

$$\begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix} \leftarrow \begin{pmatrix} 1 & \mu_{m,m-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix}.$$

Falls $m > 2$ ist, so setze $m \leftarrow m - 1$. Gehe zu Schritt 2.

Um zu zeigen, dass der obige Algorithmus terminiert, setzen wir

$$\Lambda_i := \sum_{j=1}^i \mathbb{Z} \cdot \mathbf{c}_j \quad (1 \leq i \leq k).$$

Für $D_i := d(\Lambda_i)^2$ ($1 \leq i \leq k$) gilt dann

$$D_i = \det(\mathbf{c}_\mu^{*t} \cdot \mathbf{c}_\nu^*)_{1 \leq \mu, \nu \leq i} = \prod_{\nu=1}^i C_\nu.$$

Nach 6.36 folgt $M_1^i \leq \gamma_i^i \cdot D_i$ ($1 \leq i \leq k$), wobei M_1 die Länge des kürzesten Gittervektors in Λ bezeichnet. Nach jedem Durchlauf von Schritt 6 des Algorithmus ist der neue Wert von C_{m-1} um einen Faktor $< \frac{3}{4}$ kleiner als der alte Wert von C_{m-1} und damit ebenso der neue Wert von D_{m-1} . Andererseits bleiben die übrigen D_i unverändert, weil die zugehörigen Gitter Λ_i sich nicht ändern. Also terminiert der Algorithmus.

5.43. MLLL-Algorithmus

Es seien $\mathbf{c}_1, \dots, \mathbf{c}_k \in \Lambda$ linear unabhängig. Zu $\mathbf{c}_{k+1} \in \Lambda$ beliebig berechnen wir $m_1, \dots, m_{k+1} \in \mathbb{Z}$ mit

$$\sum_{i=1}^{k+1} m_i \mathbf{b}_i = 0 \quad (|m_1| + \dots + |m_{k+1}| > 0).$$

Ferner bestimmen wir $\mathbf{c}'_1, \dots, \mathbf{c}'_k \in \Lambda$ mit

$$\sum_{i=1}^{k+1} \mathbb{Z} \cdot \mathbf{c}_i = \sum_{i=1}^k \mathbb{Z} \cdot \mathbf{c}'_i.$$

- (i) (Initialisierung) Setze $C_i \leftarrow \|\mathbf{c}_i^*\|^2$, $\mathbf{c}'_i \leftarrow \mathbf{c}_i$ ($1 \leq i \leq k + 1$).
Ferner setze $H = (\mathbf{h}_1, \dots, \mathbf{h}_{k+1}) \leftarrow I_{k+1}$ und $m \leftarrow 2$.
- (ii) Setze $l \leftarrow m - 1$.
- (iii) Für $|\mu_{ml}| > \frac{1}{2}$ setze

$$r \leftarrow \lfloor \mu_{ml} + \frac{1}{2} \rfloor, \quad \mathbf{c}'_m \leftarrow \mathbf{c}'_m - r \mathbf{c}'_l, \quad \mathbf{h}_m \leftarrow \mathbf{h}_m - r \mathbf{h}_l,$$

$$\mu_{mj} \leftarrow \mu_{mj} - r \mu_{lj} \quad (1 \leq j \leq l - 1), \quad \mu_{ml} \leftarrow \mu_{ml} - r.$$

Für $\mathbf{c}'_m = 0$ setze $\mathbf{c}'_i \leftarrow \mathbf{c}'_{i+1}$ ($m \leq i \leq k$), $(m_1, \dots, m_{k+1})^t \leftarrow \mathbf{h}_m$ und terminiere. Falls $l < m - 1$ ist, so gehe zu Schritt 5.

- (iv) Falls $C_m < (\frac{3}{4} - \mu_{m,m-1}^2) C_{m-1}$ ist, so gehe zu Schritt 6.

- (v) Setze $l \leftarrow l - 1$. Für $l > 0$ gehe zu Schritt 3, sonst setze $m \leftarrow m + 1$ und gehe zu Schritt 2.
- (vi) Setze $\mu \leftarrow \mu_{m,m-1}, C \leftarrow C_m + \mu^2 C_{m-1}$. Falls $C = 0$ ist, so gehe zu Schritt 7. Sonst setze $\mu_{m,m-1} \leftarrow \mu C_{m-1}/C$ sowie $C_m \leftarrow C_{m-1} C_m / C$ und für $i = m + 1, \dots, k$ ferner

$$\begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix} \leftarrow \begin{pmatrix} 1 & \mu_{m,m-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix}.$$

- (vii) (Vertausche $\mathbf{c}'_{m-1}$ und $\mathbf{c}'_m$) Setze $C_{m-1} \leftarrow C$,

$$\begin{pmatrix} \mathbf{h}_{m-1} \\ \mathbf{h}_m \end{pmatrix} \leftarrow \begin{pmatrix} \mathbf{h}_m \\ \mathbf{h}_{m-1} \end{pmatrix}, \quad \begin{pmatrix} \mathbf{c}'_{m-1} \\ \mathbf{c}'_m \end{pmatrix} \leftarrow \begin{pmatrix} \mathbf{c}'_m \\ \mathbf{c}'_{m-1} \end{pmatrix},$$

$$\begin{pmatrix} \mu_{m-1,j} \\ \mu_{mj} \end{pmatrix} \leftarrow \begin{pmatrix} \mu_{mj} \\ \mu_{m-1,j} \end{pmatrix} \quad (1 \leq j \leq m-2).$$

Für $m > 2$ setze $m \leftarrow m - 1$. Gehe zu Schritt 2.

Wir zeigen nun, dass der obige Algorithmus terminiert. Nach der Initialisierung gilt zunächst $C_{k+1} = 0$. Wie in 6.42 schließt man nun, dass in Schritt 6 der Wert C nur endlich oft $\neq 0$ sein kann, da in diesem Fall der neue Wert von C_{m-1} um einen Faktor $< \frac{1}{4}$ kleiner als der alte Wert von C_{m-1} ist. Also erreicht man nach endlich vielen Schritten $\mu_{k+1,k} = 0$, der Vektor $\mathbf{c}'_{k+1}$ ist linear abhängig von $\mathbf{c}'_1, \dots, \mathbf{c}'_{k-1}$. Nach Voraussetzung existieren $m_1, \dots, m_{k+1} \in \mathbb{Z}, |m_1| + \dots + |m_{k+1}| > 0$, mit

$$\sum_{i=1}^{k+1} m_i \mathbf{c}'_i = 0.$$

Da $\mathbf{c}'_{k+1}$ von $\mathbf{c}'_1, \dots, \mathbf{c}'_{k-1}$ linear abhängig ist, können wir dabei $m_k = 0$ annehmen. Also ist

$$\Lambda' := \mathbb{Z}\mathbf{c}'_1 + \dots + \mathbb{Z}\mathbf{c}'_{k-1} + \mathbb{Z}\mathbf{c}'_{k+1}$$

ein $(k-1)$ -dimensionales Teilgitter von Λ . Der Algorithmus wird nun auf diesem Teilgitter fortgesetzt. Sofern er nicht vorher terminiert, liefert er schließlich zwei linear abhängige Vektoren $\mathbf{c}'_1, \mathbf{c}'_2 \in \Lambda$. Nach endlich vielen weiteren Schritten gilt dann $\mu_{12} = 0$, also $\mathbf{c}'_2 = 0$. Damit spätestens terminiert der Algorithmus.

5.44. Polynomfaktorisierung über $\mathbb{Q}$

Dies ist eine interessante Anwendung des LLL-Algorithmus. Lenstra, Lenstra und Lovasz zeigten 1983 damit, dass die Faktorisierung von Polynomen über $\mathbb{Q}$ "polynomial time" in den Eingabedaten (Grad, Stellenzahl der Koeffizienten) ist. Interessanterweise ist kein Verfahren bekannt, mit dem man die Faktorisierung einer natürlichen Zahl n in

ihre Primfaktoren in polynomieller Zeit in der Stellenzahl von n erreichen kann.

Es sei $g(t) \in \mathbb{Q}[t]$ mit $m = \deg(g) > 1$ vorgegeben. Es genügt dann (!), einen echten Faktor von g zu berechnen und das Verfahren zu iterieren. Wie in den Kapiteln über Ringe und Körper gesehen, können wir uns auf Polynome $g(t) \in \mathbb{Z}[t]$ beschränken. Ebenso können wir $g(t)$ als normiert annehmen: $g(t) = \sum_{i=0}^m g_i t^{m-i}$ ($g_i \in \mathbb{Z}$, $g_0 = 1$). Ferner dürfen wir annehmen, dass $g(t)$ quadratfrei ist.

Der Faktorisierungsalgorithmus erläutert dann so:

- (i) Bestimme $p \in \mathcal{P}$ geeignet und faktorisiere $g(t) \bmod p\mathbb{Z}[t]$ in Primfaktoren.
- (ii) Lifte die Faktorisierung $\bmod p\mathbb{Z}[t]$ zu einer $\bmod p^\kappa\mathbb{Z}[t]$ für $\kappa \in \mathbb{N}$ passend.
- (iii) Gewinne aus der Faktorisierung von $g(t) \bmod p^\kappa\mathbb{Z}[t]$ die in $\mathbb{Z}[t]$ zurück.

Wir diskutieren die 3 Schritte im folgenden etwas detaillierter. Nur im 3. Schritt wird der LLL-Algorithmus gebraucht.

Ad (i) $p \in \mathcal{P}$ ist so zu wählen, dass p nicht den Leitkoeffizienten von g teilt (hier automatisch erfüllt, vgl. Ausführungen zum Reduktionalgorithmus im Abschnitt über Polynome im Ringkapitel) und dass p nicht die Diskriminante von g teilt. Denn aus dem Resultantenabschnitt wissen wir:

$$p \mid d(g) \iff g(t) \bmod p\mathbb{Z}[t] \text{ besitzt Primteiler und Multiplizität } > 1.$$

Die Faktorisierung $\bmod p\mathbb{Z}[t]$ erfolgt dann mit dem Berlekamp Algorithmus. (Der ist zwar nicht polynomial in $\log p$, doch können wir hier p stets "klein" im Verhältnis zu den Eingabedaten wählen.)

Ad (ii) Das Liften erfolgt mit dem sogenannten Hensel Lifting. Da dieser Algorithmus über beliebigen Integritätsringen funktioniert, halten wir die Darstellung entsprechend allgemein.

LEMMA 5.1. *Es seien R Integritätsring mit echtem Ideal $\mathfrak{b}$, sowie normierte nicht-konstante Polynome $g, h, k \in R[t]$, die den Bedingungen*

- (i) $g(t) \equiv h(t)k(t) \bmod \mathfrak{b}[t]$ sowie
- (ii) $u(t)h(t) + v(t)k(t) \equiv 1 \bmod \mathfrak{b}[t]$ mit Polynomen $u, v \in R[t]$, $\deg(u) < \deg(k)$, $\deg(v) < \deg(h)$ genügen.

Dann existieren Polynome $\tilde{h}, \tilde{k}, \tilde{u}, \tilde{v} \in R[t]$ mit $\deg(\tilde{u}) < \deg(\tilde{k})$, $\deg(\tilde{v}) < \deg(\tilde{h})$, $\tilde{h}, \tilde{k}$ normiert mit

- (i') $g(t) = \tilde{h}(t) \tilde{k}(t) \bmod \mathfrak{b}^2[t]$,
- (ii') $\tilde{u}(t) \tilde{h}(t) + \tilde{v}(t) \tilde{k}(t) \equiv 1 \bmod \mathfrak{b}^2[t]$,
- (iii') $h(t) \equiv \tilde{h}(t) \bmod \mathfrak{b}[t]$, $k(t) \equiv \tilde{k}(t) \bmod \mathfrak{b}[t]$.

Beweis: Zum Beweis setzen wir

$$\begin{aligned} a(t) &:= g(t) - h(t)k(t) \in \mathfrak{b}[t], \deg(a) < \deg(g); \\ b(t) &:= 1 - u(t)h(t) - v(t)k(t) \in \mathfrak{b}[t], \deg(b) < \deg(g). \end{aligned}$$

Für $\hat{d} := au$, $\hat{c} := av$ und $\hat{h} := h + \hat{c}$, $\hat{k} := k + \hat{d}$ folgt dann unmittelbar:

$$\begin{aligned} g - \hat{h}\hat{k} &= g - hk - h\hat{d} - k\hat{c} - \hat{c}\hat{d} \\ &= a - auh - avk - \hat{c}\hat{d} \\ &= ab - \hat{c}\hat{d} \in \mathfrak{b}^2[t] \end{aligned}$$

Allerdings wollen wir noch $\deg(h) = \deg(\tilde{h})$, $\deg(k) = \deg(\tilde{k})$ erreichen. Hierzu schreiben wir mittels Division mit Rest

$$\begin{aligned} \hat{c} &= Q_1h + c, \deg(c) < \deg(h), \deg(d) < \deg(k) \\ \hat{d} &= Q_2k + d \end{aligned}$$

Da h, k normiert sind, folgt aus $\hat{c}, \hat{d} \in \mathfrak{b}[t]$ zunächst $Q_1, Q_2 \in \mathfrak{b}[t]$ und sodann $c, d \in \mathfrak{b}[t]$.

Schließlich setzen wir $\tilde{h} = h + c$, $\tilde{k} = k + d$, so dass (iii') erfüllt bleibt.

Es folgt

$$\begin{aligned} g - \tilde{h}\tilde{k} &= g - hk - hd - kc - cd \\ &= a - h(\hat{d} - Q_2k) - k(\hat{c} - Q_1h) - cd \\ &= a - \hat{d} - k\hat{c} + hk(Q_1 + Q_2) - cd. \end{aligned}$$

Wegen $\deg(g - \tilde{h}\tilde{k}) < \deg(g) = \deg(hk)$ muss hierin $Q_1 + Q_2 \in \mathfrak{b}^2[t]$ gelten, also auch $g - \tilde{h}\tilde{k} \in \mathfrak{b}^2[t]$.

Nun müssen $\hat{u} := u + \hat{e}$, $\hat{v} + \hat{f}$ mit $\hat{e}, \hat{f} \in \mathfrak{b}[t]$ so bestimmt werden, dass $\hat{u}\tilde{h} + \hat{v}\tilde{k} \equiv 1 \bmod \mathfrak{b}^2[t]$ gilt.

Wir erhalten

$$\begin{aligned} \hat{y} := 1 - \hat{u}\tilde{h} - \hat{v}\tilde{k} &= 1 - (u + \hat{e})(h + c) - (v + \hat{f})(k + d) \\ &= 1 - uh - vk - uc - \hat{e}h - \hat{e}c - vd - \hat{f}k - \hat{f}d \\ &= b - \hat{e}h - \hat{f}k - uc - vd - \hat{e}c - \hat{f}d. \end{aligned}$$

Der Ansatz $\tilde{b} := b - uc - vd \in \mathfrak{b}[t]$ sowie $\hat{e} := \tilde{b}u$, $\hat{f} := \tilde{b}v \in \mathfrak{b}[t]$ liefert:

$$\hat{y} = \tilde{b} - \tilde{b}uh - \tilde{b}vk - \hat{e}c - \hat{f}d \in \mathfrak{b}^2[t].$$

Schließlich setzen wir noch (Division mit Rest)

$$\begin{aligned} \hat{e} &= Q_3k + e, \\ \hat{f} &= Q_4h + f, \deg(e) < \deg(k), \deg(f) < \deg(h). \end{aligned}$$

Wie zuvor sind mit $\hat{e}, \hat{f}$ auch Q_3, Q_4, e, f in $\mathfrak{b}[t]$.

Wir behaupten, dass dann $\tilde{u} := u + e, \tilde{v} := v + f$ auch (ii') erfüllen.

Dazu betrachten wir:

$$\begin{aligned} y &:= 1 - \tilde{u}\tilde{h} - \tilde{v}\tilde{k} \\ &= 1 - (u + e)(h + c) - (v + f)(k + d) \\ &= 1 - uh - vk - uc - eh - ec - vd - fk - fd \\ &= b - uc - vd - (\hat{e} - Q_3k)h - (\hat{f} - Q_4h)k - ec - fd \\ &= \tilde{b} - \hat{e}h - \hat{f}k + kh(Q_3 + Q_4) - ec - fd. \end{aligned}$$

Erneut wissen wir:

$\deg(y) < \deg(g) = \deg(h) + \deg(k), \tilde{b} - \hat{e}h - \hat{f}k, ec, fd \in \mathfrak{b}^2[t]$. Da h, k normiert sind, muss auch $Q_3 + Q_4 \in \mathfrak{b}_2[t]$ gelten, also auch $y \in \mathfrak{b}_2[t]$. $\square$

Hensel Lifting

Input An integral domain R with a proper ideal $\mathfrak{b}$
and monic non-constant polynomials
 $g(t), h(t), k(t) \in R[t]$ subject to

$$\begin{aligned} g(t) &\equiv h(t)k(t) \pmod{\mathfrak{b}[t]}, \\ u(t)h(t) + v(t)k(t) &\equiv 1 \pmod{\mathfrak{b}[t]} \end{aligned}$$

for suitable $u(t), v(t) \in R[t]$.

Output Monic polynomials $\tilde{h}(t), \tilde{k}(t) \in R[t]$ satisfying

$$\begin{aligned} g(t) &\equiv \tilde{h}(t)\tilde{k}(t) \pmod{\mathfrak{b}^2[t]}, \\ h(t) &\equiv \tilde{h}(t) \pmod{\mathfrak{b}[t]}, \\ k(t) &\equiv \tilde{k}(t) \pmod{\mathfrak{b}[t]}, \\ \tilde{u}(t)\tilde{h}(t) + \tilde{v}(t)\tilde{k}(t) &\equiv 1 \pmod{\mathfrak{b}^2[t]} \end{aligned}$$

with $\tilde{u}(t), \tilde{v}(t) \in R[t]$ and $\deg(\tilde{u}) < \deg(\tilde{k}),$
 $\deg(\tilde{v}) < \deg(\tilde{h})$.

Step 1 Set

$$a(t) := g(t) - h(t)k(t), \quad b(t) := 1 - u(t)h(t) - v(t)k(t).$$

Step 2 Set

$$\begin{aligned} c(t) &:= \mathbf{Rem}(v(t)a(t), h(t)), & \tilde{h}(t) &:= h(t) + c(t), \\ d(t) &:= \mathbf{Rem}(u(t)a(t), k(t)), & \tilde{k}(t) &:= k(t) + d(t). \end{aligned}$$

Step 3 Set $e(t) := b(t) + u(t)c(t) + v(t)d(t)$ and

$$\tilde{u}(t) := \mathbf{Rem}(u(t)(1 - e(t)), k(t)), \quad \tilde{v}(t) := \mathbf{Rem}(v(t)(1 - e(t)), h(t)).$$

We note that each lifting procedure requires only 4 long divisions by monic polynomials and 9 multiplications.

Beispiel:

$$x^4 + 1 \equiv (x^2 + 2)(x^2 - 2) \pmod{5}$$

$$\begin{array}{ccc} & h & k \\ -1(x^2 + 2) + 1(x^2 - 2) & = & -4 \equiv 1 \pmod{5} \\ u & & v \end{array}$$

1. $a = g - hk = x^4 + 1 - (x^4 - 4) = 5$,
 $b = 1 + x^2 + 2 - x^2 + 2 = 5$
2. $\tilde{h} = h + c = x^2 + 7$, $c = 5$ $\tilde{k} = x - 7$, $d = -5$
3. $e = 5 + 5 + 5 = 15$
 $\tilde{u} = -16$ $\tilde{v} = 16$
 $-16(x^2 + 7) + 16(x^2 - 7) = -112 - 2 \equiv 1 \pmod{25}$

Bemerkung:

- (i) Das Liften von $\mathfrak{b}$ nach $\mathfrak{b}^2$ lässt sich ohne weiteres auf $\mathfrak{b}^{2^k}$ ($k \in \mathbb{N}$) fortführen.
- (ii) Hat $g(t) \pmod{\mathfrak{b}[t]}$ mehr als zwei Faktoren, ist das Liften entsprechend mehrfach durchzuführen.

Damit ist erreicht, dass wir die Ausgangsfaktorisierung aus dem Berlekamp Verfahren (also $\pmod{p\mathbb{Z}[t]}$ zu einer Faktorisierung von $g(t) \pmod{p^{2^k}\mathbb{Z}[t]}$ ($k \in \mathbb{N}$) liften können. Wir müssen uns allerdings noch darüber klar werden, welcher Exponent k für unsere Zwecke ausreicht.

Nach dem Durchlaufen der ersten drei Schritte des Faktorisierungsalgorithmus befinden wir uns in folgender Situation. Wir haben eine Primzahl p sowie normierte Polynome $h, k \in \mathbb{Z}[t]$ mit den Eigenschaften

- (i) $h(t)$ ist irreduzibel in $\mathbb{Z}/p\mathbb{Z}[t]$,
- (ii) $g(t) \equiv h(t)k(t) \pmod{p^r\mathbb{Z}[t]}$
- (iii) $h(t) \nmid k(t)$ in $\mathbb{Z}/p\mathbb{Z}[t]$.

Es sei $l := \deg(h)$. Das nachfolgende Lemma ist grundlegend für alles weitere.

LEMMA 1. *Das Polynom g besitzt einen normierten irreduziblen Faktor $h_0(t) \in \mathbb{Z}[t]$ vom Grad r , $l \leq r \leq m$, so dass $h_0(t)$ von $h(t)$ in $\mathbb{Z}/p\mathbb{Z}[t]$ geteilt wird. Dann sind für $d(t) \in \mathbb{Z}[t]$ normiert mit $d(t) \mid g(t)$ äquivalent:*

- (i) $h(t)$ teilt $d(t)$ in $\mathbb{Z}/p\mathbb{Z}[t]$;
- (ii) $h(t)$ teilt $d(t)$ in $\mathbb{Z}/p^x\mathbb{Z}[t]$;
- (iii) $h_0(t)$ teilt $d(t)$ in $\mathbb{Z}[t]$;

BEWEIS. Die 1. Behauptung ist trivial.

(1) $\implies$ (2) Per Hensel Lifting, da $h(t)$ und $k(t)$ modulo $p\mathbb{Z}[t]$ koprim sind.

(2) $\implies$ (1) Trivial.

(3) $\implies$ (1) Trivial.

(1) $\implies$ (3) $g(t)$ hat genau einen irreduziblen Faktor in $\mathbb{Z}[t]$, der in $\mathbb{Z}/p\mathbb{Z}[t]$ von $h(t)$ geteilt wird. Division mit Rest von d und h_0 liefert die Behauptung. $\square$

Zunächst testen wir $h(t) \mid f(t)$ in $\mathbb{Z}[t]$.

Falls dies nicht gilt, versuchen wir, einen irreduziblen Teiler h_0 von g in $\mathbb{Z}[t]$ zu bestimmen, für den $h \mid h_0$ in $\mathbb{Z}/p\mathbb{Z}[t]$ gilt. Wir müssen also für $r := \deg(h_0)$ die Werte $r := l + 1, l + 2, \dots, \deg g - 1$ testen. Dazu bilden wir Polynome von beschränktem Grad mit Koeffizienten in $\mathbb{Z}$ auf Gittervektoren ab:

$$\varphi_r : \{u(t) \in \mathbb{Z}[t] \mid \deg(u) \leq r\} \longrightarrow \mathbb{Z}^{r+1} : \sum_{i=0}^r u_i t^i \mapsto (u_0, \dots, u_r).$$

(Hierbei ist $r \in \mathbb{Z}^{\geq 0}$ natürlich beliebig.) Offenbar ist φ_r ein $\mathbb{Z}$ -Modul-Isomorphismus. Speziell betrachten wir das $(r+1)$ -dimensionale Gitter Λ mit der Basis

$$B = \{\varphi_r(p^x t^i) \mid 0 \leq i < l\} \cup \{\varphi_r(h(t)t^j) \mid 0 \leq j \leq r - l\}$$

es hat die Diskriminante $d(\Lambda) = p^{\kappa l}$.

$\square$

LEMMA 2. Falls $\mathbf{b} \in \Lambda$ der Ungleichung $\|\mathbf{b}\|^m \|\varphi_m(g)\|^r < d(\Lambda)$ genügt, wird das Polynom $b(t) := \varphi_r^{-1}(\mathbf{b})$ von h_0 in $\mathbb{Z}[t]$ geteilt. Speziell gilt: $a(t) := \gcd(b, g) \neq 1$.

BEWEIS. Für $\mathbf{b}(t) = \mathbf{0}$ ist nichts zu zeigen. Also nehmen wir $\mathbf{b} \neq \mathbf{0}$ an und setzen $a(t) := \gcd(g(t), b(t))$ mit $b(t) = \varphi_r^{-1}(\mathbf{b})$. Nach dem vorangehenden Lemma genügt es zu zeigen, dass $a(t)$ von $h(t)$ in $\mathbb{Z}/p\mathbb{Z}[t]$ geteilt wird.

Dabei benutzen wir

$$l = \deg(h), \quad m = \deg(g), \quad r = \deg(h_0)$$

und setzen

$$s_1 = \deg(a), \quad s_2 := \deg(b) = \deg(\varphi_r^{-1}\mathbf{b}).$$

Offenbar gilt dann

$$0 \leq s_1 \leq s_2 \leq r = \dim(\Lambda) - 1.$$

Wir nehmen jetzt an, dass $a(t)$ in $\mathbb{Z}/p\mathbb{Z}[t]$ nicht von $h(t)$ geteilt wird und führen dies zum Widerspruch.

Unter jener Annahme existieren $\alpha(t), \beta(t) \in \mathbb{Z}[t]$, $\delta \in p\mathbb{Z}[t]$ mit

$$(*) \quad \alpha(t) h(t) + \beta(t) a(t) = 1 - \delta(t).$$

Nunmehr betrachten wir

$$\mathcal{S} := \{\lambda(t) g(t) + \mu(t) b(t) \in \mathbb{Z}[t] \mid \deg(\lambda) < s_2 - s_1, \deg(\mu) < m - s_1\},$$

□

Wir bekommen den gewünschten Widerspruch in 3 Schritten:

$$(I) \quad T := \{\varphi_{m+s_2-s_1}(g(t)t^i) \mid 0 \leq i < s_2 - s_1\} \cup \{\varphi_{m+s_2-s_1}(b(t)t^j) \mid 0 \leq j < m - s_1\}$$

bildet die Basis eines $(m + s_2 - 2s_1)$ -dimensionalen $\mathbb{Z}$ -Gitters $\tilde{\Lambda}$. (Aufgrund der gemachten Voraussetzungen erhalten wir dann für die Gitterdiskriminante:

$$(**) \quad d(\tilde{\Lambda}) \leq \|b\|^{m-s_1} \|g\|^{s_2-s_1} \leq \|b\|^m \|g\|^r < p^{\kappa l}.)$$

Wir haben zu zeigen, dass T linear unabhängig ist. Dazu genügt der Nachweis, dass für Polynome $\lambda(t), \mu(t) \in \mathbb{Z}[t]$ mit $\deg(\lambda) < s_2 - s_1$, $\deg(\mu) < m - s_1$ aus $\deg(\lambda g + \mu b) < s_1$ bereits $\lambda(t) = \mu(t) = 0$ folgt. Wegen $\deg(a) = s_1$ und $a \mid (\lambda g + \mu b)$ muss stets $\lambda g + \mu b = 0$ gelten. Es folgt $\lambda \frac{g}{a} = -\mu \frac{b}{a}$ mit $\gcd\left(\frac{g}{a}, \frac{b}{a}\right) = 1$, also $\left(\frac{g}{a}\right) \mid \mu$. Wegen $\deg\left(\frac{g}{a}\right) = m - s_1 > \deg(\mu)$ gilt $\mu = 0$ und damit auch $\lambda = 0$. (Damit haben wir zudem $T \subset \mathbb{Z}t^{s_1} + \dots + \mathbb{Z}t^{m+s_1-s_2-1}$ gezeigt!)

$$(II) \quad \{\gamma = \lambda g + \mu b \in S \mid \deg(\gamma) < s_1 + l\} \subseteq p^\kappa \mathbb{Z}[t].$$

Wegen $a \mid \gamma$ erhalten wir aus (*) die Gleichung

$$\alpha h \frac{\gamma}{a} + \beta a \frac{\gamma}{a} = \frac{\gamma}{a} (1 - \delta).$$

Wir multiplizieren diese mit $1 + \delta + \dots + \delta^{\kappa-1}$ und bekommen $\tilde{\alpha} h + \tilde{\beta} \gamma = \frac{\gamma}{a} (1 - \delta^\kappa)$.

Nach Annahme teilt h sowohl g als auch b in $\mathbb{Z}/p^\kappa \mathbb{Z}[t]$, daher auch γ und somit auch $\frac{\gamma}{a}$.

Wegen $\deg(h) = l = s_1 + l - s_1 > \deg\left(\frac{\gamma}{a}\right)$ muss folglich $\frac{\gamma}{a}$ (und damit γ selbst) in $p^\kappa \mathbb{Z}[t]$ liegen.

(III) Widerspruch.

Wir wählen eine Basis $\mathbf{b}_{s_1}, \dots, \mathbf{b}_{m+s_2-s_1-1}$ von $\tilde{\Lambda}$, so dass die Matrix mit jenen Spalten in Hermite Normalform ist. Die Leitkoeffizienten der zugehörigen $\mathbf{b}_j$ liegen dann in $p^\kappa \mathbb{Z}$ ($s_1 \leq j < s_1 + l$) wegen (II). (Wir merken dazu an, dass wegen der Annahme $h \nmid a$ in $\mathbb{Z}/p^\kappa \mathbb{Z}[t]$ hier $s_1 \leq m - l$ gelten muss, also auch $s_1 + l \leq m + s_2 - s_1$.) Aber dies impliziert $d(\tilde{\Lambda}) \geq p^{\kappa l}$ im Widerspruch zu (**). □

KOROLLAR 3. In $\mathbb{Z}[t]$ besitzt $f[t]$ einen Teiler $h_0(t)$ vom Grad $\leq r$ mit $h(t)$ teilt $h_0(t)$ in $\mathbb{Z}/p^\kappa \mathbb{Z}[t] \iff \|b_1\| < (p^{\kappa l} / \|f\|^r)^{1/n}$ für den ersten Basisvektor b_1 einer LLL-reduzierten Basis von Λ .

Dies ist eine qualitative Lösung unseres Problems. Für eine quantitative ist n hinreichend groß zu machen, einmal

für das Hensel Lifting, zum anderen damit ein Teilerpolynom $d(t)$ von $f(t)$ in $\mathbb{Z}[t]$ vom Grad r der Abschätzung aus Korollar 3 genügt.

Für den ersten Vektor $\underline{b}_1$ einer LLL-reduzierten Basis von Λ gilt:

$$\| \underline{b}_1 \| \leq 2^{r/2} \| h_0 \| .$$

Mittels der Abschätzung von Mignotte für h_0 : $\| h_0 \| \leq \binom{2r}{r}^{1/2} \| f \|$ genügt es demnach, κ so groß zu machen, dass

$$(2^{r/2} \binom{2r}{r}^{1/2} \| f \|^n) < \frac{p^{\kappa l}}{\| f \|^r}$$
 erfüllt ist.

Abschätzung der Nullstellen eines normierten Polynoms $f(t) \in \mathbb{C}[t]$ mit Mitteln der Linearen Algebra

Es sei $f(t) = t^n + a_1 t^{n-1} + \dots + a_n \in \mathbb{C}[t]$ gegeben. Hierzu gehört die sogenannte **Begleitmatrix** (companion matrix)

$$A_f := \begin{pmatrix} 0 & \cdot & \cdot & \cdot & \cdot & 0 & -a_n \\ 1 & 0 & \cdot & \cdot & \cdot & 0 & -a_{n-1} \\ 0 & 1 & 0 & \cdot & \cdot & 0 & -a_{n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & 0 & -a_2 \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & -a_1 \end{pmatrix} .$$

I.

Wir zeigen, dass das zugehörige charakteristische Polynom $\det(t\mathcal{I}_n - A_f)$ gerade $f(t)$ ist.

Hierzu entwickeln wir die entsprechende(n) Determinante(n) nach der letzten Zeile:

$$\begin{vmatrix} t & 0 & \cdot & \cdot & \cdot & \cdot & 0 & a_n \\ -1 & t & 0 & \cdot & \cdot & \cdot & 0 & a_{n-1} \\ 0 & -1 & t & \cdot & \cdot & \cdot & \cdot & a_{n-2} \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1 & t & a_2 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & -1 & t + a_1 \end{vmatrix}$$

$$= (t+a_1) \begin{vmatrix} t & 0 & \cdot & \cdot & \cdot & 0 \\ -1 & t & 0 & \cdot & \cdot & \cdot \\ 0 & -1 & t & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 & \cdot \\ 0 & \cdot & \cdot & 0 & -1 & t \end{vmatrix} + \begin{vmatrix} t & 0 & \cdot & \cdot & \cdot & 0 & a_n \\ -1 & t & 0 & \cdot & \cdot & \cdot & a_{n-1} \\ 0 & -1 & t & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 & t & a_3 \\ 0 & \cdot & \cdot & \cdot & 0 & -1 & a_2 \end{vmatrix}$$

$$= t^n + a_1 t^{n-1} + a_2 t^{n-2} + \begin{vmatrix} t & 0 & \cdot & \cdot & \cdot & 0 & a_n \\ -1 & t & 0 & \cdot & \cdot & \cdot & a_{n-1} \\ 0 & -1 & t & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 & t & a_4 \\ 0 & \cdot & \cdot & \cdot & 0 & -1 & a_3 \end{vmatrix},$$

woraus man die Behauptung leicht einsieht.

II.

Für die Maximumsnorm und die Zeilensummennorm gilt:

$$\| A\underline{x} \| \leq \| A \| \| \underline{x} \|;$$

denn für $A = (a_{ij}) \in \mathbb{C}^{n \times n}$, $\underline{x} = (x_1, \dots, x_n)^{tr} \in \mathbb{C}^{n \times 1}$ gilt:

$$\| A \| = \max_{1 \leq i \leq n} \left(\sum_{j=1}^n | a_{ij} | \right), \quad \| \underline{x} \| = \max_{1 \leq i \leq n} | x_i |$$

und somit

$$\begin{aligned} \| A\underline{x} \| &= \max_{1 \leq i \leq n} \left(\sum_{j=1}^n | a_{ij} x_j | \right) \leq \max_{1 \leq i \leq n} \| \underline{x} \| \left(\sum_{j=1}^n | a_{ij} | \right) \\ &= \| \underline{x} \| \| A \|. \end{aligned}$$

Ist also $\underline{x} \neq \underline{0}$ und $\lambda \in \mathbb{C}$ Eigenwert zu $\underline{x}$, so folgt:

$$| \lambda | \| \underline{x} \| = \| \lambda \underline{x} \| = \| A\underline{x} \| \leq \| A \| \| \underline{x} \|,$$

also $| \lambda | \leq \| A \|$.

Ist $\lambda \in \mathbb{C}$ Nullstelle von $f(t)$, so ist nach I. λ Eigenwert von A_f . Wir erhalten somit:

$$| \lambda | \leq \| A_f \| = \max\{ | a_n |, 1 + | a_i | \mid 1 \leq i \leq n-1 \}.$$

Beispiel Es sei $f(t) = t^4 + 1$. Alle Nullstellen hiervon sind 4-te Einheitswurzeln, haben also den Betrag 1. Die obige Abschätzung ist in diesem Fall bestmöglich.

Bibliography

- [1] Bewersdorff, Jörg, *Algebra für Einsteiger*, Vieweg, 2002.
- [2] Birkhoff, Bartee, *Modern Applied Algebra*.
- [3] S. Bosch, *Algebra*, Springer, 1993.
- [4] N. Bourbaki, *Algebre*, Hermann, Paris 1962.
- [5] J. H. Davenport, Y. Siret, E. Tournier, *Computer algebra*, Acad. Press, 1989.
- [6] G. Fischer, *Lehrbuch der Algebra*, Vieweg 2008.
- [7] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
- [8] Th. W. Hungerford, *Algebra*, 1974.
- [9] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
- [10] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
- [11] S. Lang, *Algebra*, Addison-Wesley, 1971.
- [12] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
- [13] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
- [14] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
- [15] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
- [16] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
- [17] G. Stroth, *Algebra*, de Gruyter, 1998.
- [18] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
- [19] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.