Einführung in die Algebra

Vorlesung im
Wintersemester 2006-2007
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

Contents

CHAPTER 5

Moduln

5.1. Definition

Es sei R ein Ring. Ein *R(Links)-Modul M* ist eine Abelsche Gruppe zusammen mit einer Verknüpfung: $\circ : R \times M \to M$ 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 *Untermodul* (*Teilmodul*) von M, falls gelten:

(1) U ist Untergruppe von M,
(2) $RU \subseteq U$.

(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

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

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 $\varphi : M \to \tilde{M}$ ein Gruppenhomomorphismus. Falls

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

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

5.5. Hilfssatz

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

(1) Im bild$(\varphi) \cong M/\ker(\varphi)$,
(2) $(U + V)/U \cong V/(U \cap V)$ für Teilmoduln U,V von M,
(3) $M/V \cong (M/U)/(V/U)$ für U,V wie in (ii) mit $U \subseteq V$.

Beweis: Wie für Gruppen, Ringe, Vektorräume.

5.6. Definition

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

5.7. Hilfssatz

(1) Für $U \subseteq M$ ist $\mathrm{ann}(U)$ ein Linksideal von R.
(2) Ist $M \neq \{0\}$ torsionsfrei, so hat R keine Nullteiler.

Beweis:

(1) Für $m \in M$ und $\phi_m : R \to M : r \mapsto rm$ gilt $\ker \phi_m = \mathrm{ann}(m)$. Demnach ist $\mathrm{ann}(U) = \bigcap_{m \in U} \ker \phi_M$, daher ist (U) ann ein (Links-) Ideal.
(2) Es seien $r \neq 0 \neq s$ mit $sr = 0$ gegeben. Dann ist $s(rm) = (sr)m = 0$ und $rm \neq 0$ ein Torsionselement. □

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

5.8. Hilfssatz

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

Beweis: Setze $\tilde{M} := \mathrm{Tor}(M)$. 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

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

also $\beta \circ x \in \tilde{M}$ und damit $R \circ \tilde{M} \subseteq \tilde{M}$. Also ist $\mathrm{Tor}(M)$ 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 $M/\mathrm{Tor}(M)$ torsionsfrei. □

5.9. Definition

Eine endliche Teilmenge $\{x_1, \ldots, x_n\}$ eines R-Moduls M heißt *über R frei* (unabhängig), falls aus $\sum_{i=1}^{r} \alpha_i x_i = 0$ für $\alpha_1, \ldots, \alpha_r \in R$ bereits $\alpha_1 = \ldots = \alpha_r = 0$ 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 Allgmeinen falsch.

5.10. Satz

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

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

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

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

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

(iv)⇒(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 $\mathrm{End}\,(V)$-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 geeigete 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 $u_1, ..., u_n$ eine minimale Anzahl von Erzeugern von M ist. Weil $u_n \in M = \mathfrak{a}M$ gilt, existieren Elemente $a_1, ..., a_n \in \mathfrak{a}$ mit $u_n = a_1 u_1 + ... + a_n u_n$. Weil $\mathfrak{a}$ in dem Jacobson Radikal von R enthalten ist, ist das Element $1 - a_n$ eine Einheit von R, und wir erhalten

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

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. □

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 $\widetilde{\mathfrak{a}^{n+1}} = \tilde{\mathfrak{a}}\widetilde{\mathfrak{a}^n}$ gilt, und der Beweis erfolgt durch die Anwendung des vorangehenden Korollars. □

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 $M = Rx_1 \dot{+} \ldots \dot{+} Rx_n$.
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 $\tilde{U} := U \cap (Rx_1 \dot{+} \ldots \dot{+} Rx_{n-1})$ und zeigen $U = \tilde{U} \dot{+} Ry$. Dazu bemerken wir:

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

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

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

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

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 $\varphi : M \to \alpha \cdot M : x \mapsto \alpha \cdot x$ 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. □

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 $M = \mathrm{Tor}(M) \oplus F$ mit einem freien Untermodul $F \simeq M/\mathrm{Tor}(M)$.

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

$$\varphi : M \to M/\mathrm{Tor}(M) : x \mapsto x + \mathrm{Tor}(M).$$

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 vom M. Offensichtlich ist $\{m_b \mid b \in B\}$ eine Basis von F. Wir zeigen: $M = \mathrm{Tor}(M) \oplus F$. Wir haben $F = \tau(M/\mathrm{Tor}(M))$ mit einem Isomorphismus

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

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

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*. $\mathrm{GL}\,(n, R)$ bezeichnet die Menge aller invertierbaren Matrizen.

5.18. Hilfssatz

(1) Die unimodularen $(n \times n)$–Matrizen über R bilden eine Gruppe $\mathrm{GL}(n, R)$.
(2) $A \in R^{n \times n}$ 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 $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ von M existiert $U \in \mathrm{GL}(n, R)$ mit

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

5.20. Hilfssatz

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

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 $\det(\tilde{A}) = \mathrm{ggT}(a_1, \ldots, a_{n-1})$. Sei $c := \mathrm{ggT}(\det(\tilde{A}), a_n)$. Dann existieren $u, v \in R$ mit $c = u \det(\tilde{A}) + v a_n$. Setze

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

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

5.21. Hilfssatz

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

Beweis: Bilde $A = (a_{ij}) \in R^{n \times n}$ mit $\det(A) = c$ wie in 5.20. 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 $(c, 0, \ldots, 0)\tilde{A} = (a_1, \ldots, a_n)$. Also erfüllt $\tilde{A}^{-1}$ die Behauptung.

□

Für einen kommutativen Ring R mit Eins ist

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

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 $U \in \mathrm{GL}(n, R)$, 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 $c = \mathrm{ggT}(a_{11}, \ldots, a_{1n}) \in \mathcal{R}$ existiert nach 5.21 $U_1 \in \mathrm{GL}(n, R)$ mit

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

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

Bemerkung Es sei G eine Abelsche Gruppe die mit Erzeugern und Relationen definiert ist: $G := \langle x_1, \ldots, x_n \mid \sum_{i=1}^n a_{i,j}x_i = 0, \quad 1 \leq j \leq m\rangle$. 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 $V \in \mathrm{GL}(m, R)$ und $U \in \mathrm{GL}(n, R)$, so dass für $S(A) := (s_{i,j}) := VAU$ gelten:

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

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

Beweis: Wir bestimmen zunächst $\tilde{V} \in \mathrm{GL}(m, R)$ und $\tilde{U} \in \mathrm{GL}(n, R)$, so dass $\tilde{V}A\tilde{U}$ die Bedingung (1) erfüllt. Der Induktionsanfang ($n = 1$) folgt aus 5.21. Es sei nun $n > 1$. Durch Anwenden von 5.22 erreicht man

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

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

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

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

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

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

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

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

$$\begin{array}{ll} \begin{pmatrix} s_{ii} & 0 \\ 0 & s_{jj} \end{pmatrix} & \cdot\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \\ & \quad\longrightarrow \\ & \begin{pmatrix} s_{ii} & 0 \\ ts_{jj} & s_{jj} \end{pmatrix} \\ & \cdot\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \\ & \quad\longrightarrow \\ & \begin{pmatrix} s_{ii} & 0 \\ g & s_{jj} \end{pmatrix} \\ & \cdot\begin{pmatrix} 1 & -s_{ii}/g \\ 0 & 1 \end{pmatrix} \\ & \quad\longrightarrow \\ & \begin{pmatrix} 0 & -s_{ii}s_{jj}/g \\ g & s_{jj} \end{pmatrix} \\ & \cdot\begin{pmatrix} 1 & l/s_{ii} \\ 0 & 1 \end{pmatrix} \\ & \quad\longrightarrow \\ & \begin{pmatrix} 0 & -l \\ g & 0 \end{pmatrix} \\ & \cdot\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ & \quad\longrightarrow \\ & \begin{pmatrix} g & 0 \\ 0 & l \end{pmatrix}. \end{array}$$

Zum Beweis der Eindeutigkeit sei $d_i(A)$ der ggT aller (i,i)–Minoren von A $(1 \le i \le r)$. Es gilt $d_{i-1}(A)|d_i(A)$ $(2 \le i \le r)$. 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

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

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 $n_1 | \ldots | n_n$ 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 $i \in \{1, \ldots, n\}$ und $c_i := \sum_{j=1}^{n} \gamma_j b_j \in M$. Dann ist $b_1, \ldots, b_{i-1}, c_i$ genau dann zu einer Basis von M ergänzbar, wenn $\mathrm{ggT}(\gamma_i, \ldots, \gamma_n) = 1$ ist.

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

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

5.25. Gitter - Definition

Es seien $\mathbf{b_1}, \ldots, \mathbf{b_k} \in \mathbb{R}^n$ linear unabhängig über $\mathbb{R}$. Dann nennt man den $\mathbb{Z}$–Modul

$$\Lambda := \left\{ \sum_{i=1}^{k} \lambda_i \mathbf{b_i} \;\mid\; \lambda_1, \ldots, \lambda_k \in \mathbb{Z} \right\}$$

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

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

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 $\mathbf{b_i}, \ldots, \mathbf{b_k} \in \mathbb{R}^n$.

5.26. Hilfssatz

(1) $d(\Lambda) = \mathrm{vol}_k(\Pi(\Lambda))$.

(2) Ist Λ' ein k–dimensionales Teilgitter von Λ mit einer Gitterbasis $\mathbf{c_1}, \ldots, \mathbf{c_k}$, so gilt

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

für $U \in \mathbb{Z}^{k\times k}$ mit $(\mathbf{c_1}, \ldots, \mathbf{c_k}) = (\mathbf{b_1}, \ldots, \mathbf{b_k})U$.

Beweis:

(1) 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.
(2) Trivial. □

5.27. Hilfssatz

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

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

Beweis: Es sei $\mathbf{c_1}, \ldots, \mathbf{c_k}$ eine $\mathbb{Z}$–Basis von Λ'. Nach 5.22 können wir annehmen, dass die Transformationsmatrix $U = (u_{ij}) \in \mathbb{Z}^{k\times k}$ mit $(\mathbf{c_1}, \ldots, \mathbf{c_k}) = (\mathbf{b_1}, \ldots, \mathbf{b_k})U$ eine untere Dreiecksmatrix ist. Da

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

ein komplettes Vertretersystem von Λ/Λ' ist, folgt $\#\mathcal{V} = (\Lambda : \Lambda')$. Andererseits gilt nach 5.26 (ii)

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

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.

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

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

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

Wir betrachten nun die lineare Abbildung $\varphi : \mathbb{R}^k \to \mathbb{R}^k$ 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 $\mathbf{x}^t \cdot A \cdot \mathbf{x} \leq C$.

(1) Bestimme $Q \in \mathbb{R}^{k\times k}$ wie in 5.28.
(2) (Initialisierung) Setze $i \leftarrow k, T_i \leftarrow C, U_i \leftarrow 0$.
(3) (Schranken für x_i) Setze $Z \leftarrow \sqrt{\frac{T_i}{q_{ii}}}, B_i \leftarrow \lfloor Z - U_i \rfloor$ und weiter $x_i \leftarrow \lceil -Z - U_i \rceil - 1$.
(4) Setze $x_i \leftarrow x_i + 1$. Falls $x_i \leq B_i$, so gehe zu Schritt 6.
(5) Setze $i \leftarrow i + 1$ und gehe zu Schritt 4.
(6) 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.
(7) 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. □

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 5.30. □

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 5.31 abgeschlossen im $\mathbb{R}^n$. □

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:

(1) $\mathrm{vol}(C) > 2^n d(\Lambda)$;
(2) $\mathrm{vol}(C) \geq 2^n d(\Lambda)$ und C kompakt.

Beweis:

(1) Für das Fundamentalparallelotop $\Pi(\Lambda)$ gilt

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

Damit folgt

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

und weiter

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

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

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

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

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

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

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

C_n ist offensichtlich für jedes $n \in \mathbb{N}$ konvex sowie ursprungssymmetrisch, und es gilt $\mathrm{vol}(C_n) > 2^n d(\Lambda)$. 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 $\mathbf{x} := \lim_{j \to \infty} \mathbf{x}_{n_j} \; \in C$, also $\mathbf{x} \in \Lambda$ nach 5.32. $\square$

Sukzessive Minima

5.34. Definition

Für $i \in \{1, \ldots, k\}$ heiß t

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

i-tes sukzessives Minimum des Gitters Λ.

5.35. Hilfssatz

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

Beweis:

(1) Trivialerweise existiert $\mathbf{y}_1 \in \Lambda$ mit $\|\mathbf{y}_1\|^2 = M_1$. Sind nun $\mathbf{y}_1, \ldots, \mathbf{y}_{j-1} \in \Lambda$ gefunden mit $\|\mathbf{y}_i\|^2 = M_i \ (1 \leq i < j)$, so existieren nach Definition $\mathbf{x}_1, \ldots, \mathbf{x}_j \in \Lambda$ linear unabhängig mit $\|\mathbf{x}_i\|^2 \leq M_j \ (1 \leq i \leq j)$. Insbesondere existiert $m \in \{1, \ldots, j\}$, so dass $\mathbf{y}_1, \ldots, \mathbf{y}_{j-1}, \mathbf{x}_m$ 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 $r \in \{0, \ldots, j-2\}$ mit

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

und $\mathbf{y}_1, \ldots, \mathbf{y}_{j-r-1}, \mathbf{x}_j$ linear unabhängig im Widerspruch zur Definition von M_{j-r}. Also folgt $\|\mathbf{x}_j\|^2 = M_j$.
(2) Konsequenz aus (5.20). □

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 5.35 können wir $\|\mathbf{b}_1\|^2 = M_1$ annehmen. Bilde

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

Dann gilt

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

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 $y_2, \ldots, y_k \in \mathbb{Z}$ mit

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

Nach Induktionsannahme folgt

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

Wähle $y_1 \in \mathbb{Z}$ mit

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

Für $\mathbf{y} := y_1\mathbf{b}_1 + \cdots + y_k\mathbf{b}_k \in \Lambda \setminus \{0\}$ 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 $M_1 \cdot \ldots \cdot M_k \leq \gamma_k^k d(\Lambda)^2$.

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

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

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

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

gilt dann

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

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

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

Damit bildet man eine neue quadratische Form

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

Ist C die zugehörige Matrix von h, so gilt

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

Also erhält man aus 5.36

$$\begin{aligned}&\min\{(z_1,\ldots,z_k)\cdot Q^t\cdot C\cdot Q\cdot(z_1,\ldots,z_k)^t \mid z_1,\ldots,z_k\in\mathbb{Z},|z_1|+\cdots+|z_k|>0\}^k\\ &\qquad\le\gamma_k^k\frac{d(\Lambda)^2}{M_1\cdot\ldots\cdot M_k}.\end{aligned}$$

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

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

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

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

$$\mathbf{b}_i^*:=\mathbf{b}_i-\sum_{j=1}^{i-1}\mu_{ij}\mathbf{b}_j^*\qquad(1\le i\le k),$$

$$\mu_{ij} := \frac{\mathbf{b}_i^t \mathbf{b}_j^*}{\mathbf{b}_j^{*t} \mathbf{b}_j^*} \qquad (1 \le j < i \le k).$$

5.38. Satz (Hadamard)

Es gilt

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

Beweis: Nach Konstruktion gilt

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

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

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

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

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

Damit folgt

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

□

5.39. Korollar

Es gilt $d(\Lambda)^2 \le M_1 \cdot \ldots \cdot M_k$.

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

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

□

LLL–reduzierte Basen

5.40. Definition

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

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

5.41. Satz

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

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

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

Beweis:

(1) Zunächst gilt

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

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

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

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

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

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

(2) 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 5.38.

(3) Aus (i) folgt

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

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

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

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)

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

(5) Für

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

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

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

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

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

5.42. LLL–Algorithmus

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

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

$$r \leftarrow \lfloor \mu_{ml} + \frac{1}{2} \rfloor, \quad c_m \leftarrow c_m - rc_l,$$

$\mu_{mj} \leftarrow \mu_{mj} - r\mu_{lj} \quad (1 \leq j \leq l-1), \quad \mu_{ml} \leftarrow \mu_{ml} - r.$
Für $l < m-1$, gehe zu Schritt 5.
(4) Falls $C_m < (\frac{3}{4} - \mu_{m,m-1}^2)C_{m-1}$ gilt, so gehe zu Schritt 6.
(5) 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.
(6) (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 $i = m+1, \ldots, k$ 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

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

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

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

Nach 5.36 folgt $M_1^i \le \gamma_i^i \cdot D_i$ $(1 \le i \le k)$, 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 $\mathbf{c}_1, \ldots, \mathbf{c}_k \in \Lambda$ linear unabhängig. Zu $\mathbf{c}_{k+1} \in \Lambda$ beliebig berechnen wir $m_1, \ldots, m_{k+1} \in \mathbb{Z}$ mit

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

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

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

(1) (Initialisierung) Setze $C_i \leftarrow \|\mathbf{c}_i^*\|^2, \mathbf{c}_i' \leftarrow \mathbf{c}_i$ $(1 \le i \le k+1)$. Ferner setze $H = (\mathbf{h}_1, \ldots, \mathbf{h}_{k+1}) \leftarrow I_{k+1}$ und $m \leftarrow 2$.

(2) Setze $l \leftarrow m-1$.

(3) Für $|\mu_{ml}| > \frac{1}{2}$ setze

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

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

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

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

(5) Setze $l \leftarrow l-1$. Für $l > 0$ gehe zu Schritt 3, sonst setze $m \leftarrow m+1$ und gehe zu Schritt 2.

(6) 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 $i = m+1, \ldots, k$ ferner

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

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

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

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

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 5.42 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 $\mathbf{c}'_1, \ldots, \mathbf{c}'_{k-1}$. Nach Voraussetzung existieren $m_1, \ldots, m_{k+1} \in \mathbb{Z}, |m_1| + \cdots + |m_{k+1}| > 0$, mit

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

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

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

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.

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] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
[7] Th. W. Hungerford, *Algebra*, 1974.
[8] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[9] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
[10] S. Lang, *Algebra*, Addison-Wesley, 1971.
[11] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
[12] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
[13] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[14] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
[15] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
[16] G. Stroth, *Algebra*, de Gruyter, 1998.
[17] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
[18] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.