3.1 Sukzessive Minima und reduzierte Basen: Resultate

In diesem Abschnitt behandeln wir die Existenz von „kurzen Basen“, das sind Basen eines Gitters, deren sämtliche Vektoren zumindest im Mittel „kurz“ sind. Wir wissen aus Abschnitt 1.4, dass man das Minimum eines Gitters L durch seine Determinante abschätzen kann: für einen kürzesten Vektor $v_1 \in \operatorname{Min} L$ gilt

$$\|v_1\|^2 \ \leq \ \gamma_n \, (\det L)^{1/n},$$

wobei γ_n die Hermite-Konstante in Dimension n ist. Ein kürzester Vektor v_1 kann zu einer Basis $v_1, v_2, \ldots, v_n$ von L ergänzt werden, denn er ist primitiv. Dieses hatten wir bereits in Bemerkung 1.3.5 festgestellt.

Eine entsprechende Abschätzung kann man allerdings nicht für alle Vektoren einer Basis erwarten, auch nicht mit einer schlechteren Konstanten als γ_n. Dieses überlegt man sich am Spezialfall der Gitter, die eine Orthogonalbasis $v_1, v_2, \ldots, v_n$ besitzen. Sei die Nummerierung so gewählt, dass $\|v_1\| \leq \|v_2\| \leq \cdots \leq \|v_n\|$ ist. Man überlegt sich, dass dann $\|v_i\| \leq \|w_i\|$ ist für jede Basis $w_1, w_2, \ldots, w_n$ und alle i. Mit anderen Worten, eine Orthogonalbasis (die natürlich in aller Regel nicht existiert) kann bezüglich der Länge der Basisvektoren nicht verbessert werden. Es gilt hier offenbar $\prod_{i=1}^n \|v_i\|^2 = \det L$. Das heißt, dass bei großer Determinante und „kurzen” Vektoren $v_1, \ldots v_{n-1}$ der letzte Basisvektor v_n zwangsweise lang sein muss. Sei konkret $\|v_1\| = \ldots = \|v_{n-1}\| = 1$, dann ist $\|v_n\|^2 = \det L$, was für $\det L \to \infty$ nicht durch eine Konstante mal $(\det L)^{1/n}$ abgeschätzt werden kann.

Auf der positiven Seite sehen wir jedoch, dass zumindest das geometrische Mittel der $\|v_i\|^2$ den Wert $(\det L)^{1/n}$ hat. Dieses ist der Größenordnung nach immer richtig, nicht nur im trivialen Spezialfall der Gitter mir orthogonaler Basis, wie der folgende grundlegende Satz von Hermann Minkowski zeigt.

Theorem 3.1.1 *Für jede Dimension n gibt es eine Konstante C_n derart, dass jedes n-dimensionale Gitter eine Basis $v_1, ..., v_n$ besitzt mit*

$$\prod_{i=1}^{n} \|v_i\|^2 \ \leq \ C_n \cdot \det L.$$

Bevor wir diesen Satz weiter erläutern und beweisen, wollen wir eine wichtige Folgerung ziehen.

Korollar 3.1.2 Zu gegebenem n und d gibt es bis auf Isometrie nur endlich viele ganzzahlige Gitter L auf einem euklidischen Vektorraum mit $\operatorname{rang} L = n$ und $\det L \leq d$.

In der Tat: für die Gram-Matrix bezüglich einer Basis, die der Abschätzung des Theorems genügt, gibt es für die Diagonalelemente und damit für die gesamte (positiv definite!) Matrix nur endlich viele Möglichkeiten.

In der Sprache der quadratischen Formen formuliert besagt das Korollar, dass es bei gegebener Variablenzahl und Determinante nur endlich viele Äquivalenzklassen positiv definiter ganzzahliger quadratischer Formen gibt. Dieses ist ein klassisches Resultat der Zahlentheorie, das für drei Variablen bereits um die Mitte des 19. Jahrhunderts Autoren wie Gauß, Eisenstein und Seeber bekannt war und in beliebiger Dimension von Hermite stammt.

Der klassische Beweis des Theorems 3.1.1 nach Minkowski zerfällt in zwei deutlich getrennte Schritte. Der erste Schritt benötigt die folgende Definition:

Definition 3.1.3 Die *sukzessiven Minima* $\min_k L$, $k = 1, ..., n$, eines Gitters L sind definiert als

$$\min_k L = \min\{\alpha \in \mathbb{R}_+ \mid \operatorname{rang} L_{(\leq\alpha)} \geq k\}, \text{ wobei}$$
$$L_{(\leq\alpha)} := \{v \in L \mid \langle v, v\rangle \leq \alpha\}.$$

Unter dem Rang einer Menge von Vektoren ist hier natürlich die Dimension ihrer linearen Hülle im Vektorraum zu verstehen. Das k-te sukzessive Minimum ist also die kleinste Zahl α derart, dass k linear unabhängige Gittervektoren der Quadratlänge $\leq \alpha$ existieren. Offensichtlich gilt

$$\min L = \min_1 L \leq \min_2 L \leq ... \leq \min_{n-1} L \leq \min_n L. \tag{3.1.1}$$

Vektoren $v_1, ..., v_n$ heißen *sukzessive Minimalvektoren*, wenn sie linear unahbhängig sind und

$$\|v_k\|^2 = \min_k L \text{ für } k = 1, ..., n \tag{3.1.2}$$

gilt. Wenn solche Vektoren sogar eine Basis bilden würden, könnte man diese Basis als „kurz“ (so kurz wie möglich) oder „reduziert“ bezeichnen. Eine solche Basis muss allerdings gar nicht existieren, wie wir unten an einem relativ einfachen Beispiel sehen werden. Wenn $v_1, ..., v_n$ eine Basis ist und weiter (nach eventueller Umnummerierung) $\|v_1\| \leq \|v_2\| \leq ... \leq \|v_n\|$, dann gilt offenbar lediglich

$$\|v_k\|^2 \geq \min_k L \text{ für } k = 1, ..., n\ . \tag{3.1.3}$$

Trotz dieses „Basis-Problems” sind die sukzessiven Minima sehr nützlich, denn sie können gemäß dem folgenden Satz durch die Determinante beschränkt werden:

Satz 3.1.4 *Für jedes n-dimensionale Gitter L gilt:*

$$\min_1 L \cdot \min_2 L \cdot ... \cdot \min_n L \leq \gamma_n^n \cdot \det L,$$

wobei γ_n die Hermite-Konstante zur Dimension n ist.

Für die sukzessiven Minima an Stelle der Längen der Vektoren einer „kurzen“ Basis gilt also eine Abschätzung des im Theorem 3.1.1 gewünschten Typs, und zwar mit $C_n = \gamma_n^n$. Aus der nächsten Bemerkung folgt, dass die Konstante im Satz nicht verkleinert werden kann.

Bemerkung 3.1.5 a) Die Abschätzung aus Satz 3.1.4 ist trivial für Gitter, deren sämtliche sukzessiven Minima übereinstimmen.

b) Sei L ein n-dimensionales Gitter mit $\gamma(L) = \gamma_n$, also mit größtmöglicher Packungsdichte in Dimension n. Dann stimmen alle sukzessiven Minima von L überein, und die Abschätzung aus Satz 3.1.4 gilt mit Gleichheit.

BEWEIS: In der Situation von a) reduziert sich die Ungleichung des Satzes auf $(\min L)^n \leq \gamma_n^n \cdot \det L$, was einfach nach Definition der Hermite-Konstante γ_n gilt. Allgemein gilt

$$(\min L)^n \leq \min_1 L \cdot \min_2 L \cdot ... \cdot \min_n L \leq \gamma_n^n \cdot \det L.$$

In der Situation von b) stimmen der linke und der rechte Term überein, also auch mit dem mittleren, und es muss $\min L = \min_k L$ für alle $k = 1, \ldots, n$ sein. Man beachte, dass wir für Teil b) den Satz bereits benutzen. □

Aus Teil a) der Bemerkung ergibt sich auch die Beweisstrategie im allgemeinen Fall: Durch eine geschickte Abänderung des Skalarproduktes zieht man sich auf eine Situation zurück, in der nur das erste Minimum des Gitters betrachtet werden muss. Die Durchführung dieser Idee geben wir im folgenden Abschnitt.

Wir bringen nun das oben angekündigte Beispiel dafür, dass eine Gitterbasis mit $\|v_k\|^2 = \min_k L$ für $k = 1, \ldots, n$ im allgemeinen nicht existiert.

Beispiel 3.1.6 Es sei $n \geq 5$, Betrachte das Gitter

$$D_n^\# = \mathbb{Z}^n + \mathbb{Z}\mathbf{u} \text{ dabei } \mathbf{u} = (\tfrac{1}{2}, \tfrac{1}{2}, \ldots, \tfrac{1}{2})$$

mit dem Standard-Skalarprodukt. Hierfür gilt

$$\min_k D_n^\# = 1 \text{ für } k = 1, \ldots, n,$$

es gibt jedoch keine Basis aus Vektoren der Länge 1.

BEWEIS: (Es handelt sich hier in der Tat um das duale Gitter des Wurzelgitters $D_n \subset \mathbb{Z}^n$.) Wegen $\det D_n = 4$ hat $\mathbb{Z}^n$ in $D_n^\#$ den Index 2, es gilt also $D_n^\# = \mathbb{Z}^n \cup (\mathbf{u} + \mathbb{Z}^n)$. Für jeden Vektor in der Nebenklasse $\mathbf{u} + \mathbb{Z}^n$ sind alle Einträge halbzahlig, insbesondere $\neq 0$, er hat also mindestens die Quadratlänge $\frac{n}{4} \geq \frac{5}{4}$. Somit ist $\min D_n^\# = 1$. Da es n linear unabhängige Gittervektoren der Länge 1 gibt, z.B. $\mathbf{e}_1, ..., \mathbf{e}_n$, folgt weiter $\min_k D_n^\# = 1$ für $k = 1, \ldots, n$. Eine Basis aus Vektoren der Länge 1 kann es nicht geben, weil alle diese Vektoren (nämlich die $2n$ Vektoren $\pm\mathbf{e}_i$) im echten Teilgitter $\mathbb{Z}^n$ liegen. □

Das eben angegebene Beispiel in Dimension $n = 5$ ist das „kleinste“ Beispiel seiner Art. Genauer gilt, dass in den Dimensionen ≤ 3 sukzessive Minimalvektoren immer eine Basis bilden, in der Dimension 4 findet man zumindest eine Basis aus sukzessiven Minimalvektoren (siehe das Theorem 3.1.10 unten).

Eine Basis aus (in einem geeigneten Sinn) kurzen Vektoren nennt man *reduzierte Basis*. Wir entscheiden uns nun für eine von mehreren möglichen Definitionen hierfür; siehe auch den späteren Abschnitt 3.3.

Definition 3.1.7 (Minkowski-reduzierte Basis) Eine Basis $v_1, \ldots, v_n$ eines Gitters L in einem euklidischen Vektorraum heißt *reduziert* (im Sinne von Minkowski), falls für $k = 1, \ldots, n$ gilt

$$(\mathrm{MR}_k) \quad \begin{array}{l} \|v\| \geq \|v_k\| \text{ für jedes } v \in L \text{ derart, dass} \\ (v_1, \ldots, v_{k-1}, v) \text{ sich zu einer Basis ergänzen läßt.} \end{array}$$

Wir wollen im Augenblick kurz von „reduziert" statt „Minkowski-reduziert" sprechen; entsprechend auch später, wenn sich die Präzisierung aus dem Kontext ergibt.

Beispiel 3.1.8 Die Vektoren $\mathbf{e}_1\mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \mathbf{u} = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ bilden eine reduzierte Basis von $D_5^{\#}$.

Man beachte, dass die Bedingung an den k-ten Vektor einer reduzierten Basis von den vorher gewählten Vektoren (nicht nur ihren Normen) abhängt. Dieses macht es prinzipiell schwierig, über die Normen der Vektoren einer reduzierten Basis exakte Aussagen zu machen. Folgendes ist jedoch leicht zu sehen:

Proposition 3.1.9 Jedes Gitter besitzt eine Minkowski-reduzierte Basis. Für eine solche gilt

a) $\|v_1\| = \min L$,

b) $\|v_1\| \leq \|v_2\| \leq \ldots \leq \|v_n\|$,

c) $\|v_k\|^2 \geq \min_k L$ für $k = 1 \ldots, n$.

Beweis: Wir überlegen uns, dass der erste Vektor v_1 einer reduzieren Basis ein Minimalvektor sein muss, und zeigen induktiv, dass jeder Minimalvektor $v_1 \in \operatorname{Min} L$ zu einer reduzierten Basis ergänzt werden kann; das zeigt dann auch a).

In der Bedingung (MR_1) sind als Vergleichsvektoren v alle Vektoren zu betrachten, die zu einer Basis ergänzt werden können, also alle primitiven Vektoren. Insbesondere können wir irgendeinen Vektor $v \in \operatorname{Min} L$ nehmen, und wegen (MR_1) muss dann auch $v_1 \in \operatorname{Min} L$ sein. Umgekehrt sei v_1 ein beliebiger Minimalvektor und bereits ein primitives System $v_1, \ldots, v_k$ (dabei $1 < k < n$) gefunden, das $(\mathrm{MR}_1), \ldots, (\mathrm{MR}_k)$ erfüllt. Es sei $M(v_1, \ldots, v_k)$ die Menge aller Vektoren $w \in L$ derart, dass $v_1, \ldots, v_k, w$ ein primitives System ist; diese Menge ist jedenfalls nicht leer; es sei weiter $M_0(v_1, \ldots, v_k) \subset M(v_1, \ldots, v_k)$ die Menge der kürzesten Vektoren in $M(v_1, \ldots, v_k)$. Diese Menge ist endlich und kann (zumindest im Prinzip) explizit bestimmt werden. Wenn nun $v_{k+1} \in M_0(v_1, \ldots, v_k)$ beiliebig gewählt wird, so erfüllen die Vektoren $v_1, \ldots, v_k, v_{k+1}$ die Bedingungen

$(\mathrm{MR}_1), \ldots, (\mathrm{MR}_{k+1})$. Durch $k-1$-malige Anwendung dieses Schrittes, beginnend mit einem beliebigen Minimalvektor $v_1 \in \operatorname{Min} L$ erhält man also eine reduzierte Basis. (In der Tat liefert das beschriebene Verfahren offenbar alle reduzierten Basen, wenn man in jedem Schritt alle Vektoren aus $M_0(v_1, \ldots, v_k)$ berücksichtigt.)

Teil b) folgt schnell aus der Definition: Angenommen, es existiert ein $k < n$ mit $\|v_{k+1}\| < \|v_k\|$. Dann liegt der Vektor v_{k+1} in der Menge $M(v_1, \ldots, v_{k-1})$ und ist kürzer als v_k, d.h. die Bedingung (MR_k) ist für v_k nicht erfüllt, Widerspruch.

Teil c) folgt aus der Definition der sukzessiven Minima zusammen mit b), denn die Vektoren $v_1, \ldots, v_k$ aus einer reduzierten Basis $v_1, \ldots, v_n$ sind insbesondere linear unabhängig. □

Der folgende grundlegende Satz sagt, dass man für Basisvektoren zwar im Allgemeinen keine Gleichheit, jedoch eine Abschätzung $\|v_k\|^2 \leq C_k \min_k L$ mit einer Konstanten C_k (die nur von k, aber nicht noch weiter von n abhängt) erreichen kann:

Theorem 3.1.10 (Remak) *Es sei L ein beliebiges Gitter in einem euklidischen Vektorraum und $\min_k L$, $k = 1, ..., n$ seine sukzessiven Minima. Dann gelten für jede Minkowski-reduzierte Basis $v_1, ..., v_n$ von L die Abschätzungen*

$$\|v_k\| \leq \delta_k \min_k L \text{ für } k = 1, \ldots, n, \text{ wobei}$$
$$\delta_1 = \delta_2 = \delta_3 = \delta_4 = 1 \text{ und } \delta_k = \left(\tfrac{5}{4}\right)^{k-4} \text{ für } k > 4.$$

Den Beweis geben wir im nächsten Abschnitt. Die Konstante $\delta_5 = \frac{5}{4}$ dieses Satzes kann nicht verbessert werden, wie wiederum das Beispiel des Gitters $D_5^{\#}$ zeigt.

Als Folgerung des Theorems 3.1.10 und des obigen Satzes 3.1.4 ergibt sich, dass das ankgekündigte Theorem 3.1.1 richtig ist mit der Konstanten $C_n = (\frac{5}{4})^{(n-4)(n-3)/2} \cdot \gamma_n^n$.