

4.2 Perfekte und eutaktische Formen

Die sogenannte Perfektheit ist eine Bedingung an ganzzahlige quadratische Formen bzw. Gitter, die –wie wir unten in Satz 4.2.12 sehen werden– von allen Extremformen erfüllt wird, und die leicht zu überprüfen ist. Für $\mathbf{x} \in \mathbb{R}^n = \mathbb{R}^{n \times 1}$ definieren wir

$$Q_{\mathbf{x}} := \mathbf{x}\mathbf{x}^t \in \mathcal{S}_{\geq 0}. \quad (4.2.1)$$

Die symmetrische Matrix $Q_{\mathbf{x}} = (x_i x_j)_{ij}$ ist tatsächlich positiv semidefinit und vom Rang 1, sobald $\mathbf{x} \neq \mathbf{0}$. Jede positiv semidefinite Matrix vom Rang 1 ist kongruent zu einer Matrix $Q_{\mathbf{x}}$. Diese Matrizen erzeugen den Vektorraum $\mathcal{S}$. Genauer gilt sogar:

Bemerkung 4.2.1 Die Matrizen $Q_{\mathbf{x}}$, $\mathbf{x} \in \{\mathbf{e}_i, \mathbf{e}_i + \mathbf{e}_j \mid i, j = 1, \dots, n, i < j\}$ bilden eine Basis von $\mathcal{S}$, ebenso für $\mathbf{x} \in \{\mathbf{e}_i, \mathbf{e}_i - \mathbf{e}_j \mid i, j = 1, \dots, n, i < j\}$.

Die Betrachtung von “perfekten” quadratischen Formen geht erstaunlicherweise schon in das 19. Jahrhundert zurück. Die folgende Definition ist in der modernen Literatur üblich; für die klassische Definition siehe den Satz 4.2.8 unten.

Definition und Bemerkung 4.2.2 (Perfekte Formen und Gitter)

- a) Eine Menge von Vektoren $M \subset \mathbb{R}^n$ heißt *perfekt*, wenn die Matrizen $Q_{\mathbf{z}}$, $\mathbf{z} \in M$, den Vektorraum $\mathcal{S}$ aller symmetrischen Matrizen erzeugen.
- b) Wenn M perfekt ist und $S \in \mathrm{GL}_n(\mathbb{R})$, dann ist auch SM perfekt.
- c) Eine positiv definite quadratische Form $F \in \mathcal{S}_{>0}$ heißt *perfekt*, wenn die Menge ihrer Minimalvektoren $\mathrm{Min} F \subset \mathbb{Z}^n$ perfekt ist.
- d) Wenn eine quadratische Form perfekt ist, dann ist es auch jede hierzu äquivalente quadratische Form.
- e) Ein Gitter in einem euklidischen Vektorraum heißt *perfekt*, wenn eine und damit jede seiner Gram-Matrizen perfekt ist.
- f) Eine Teilmenge $M \subseteq V$ eines reellen Vektorraumes heißt *perfekt*, wenn für einen und damit jeden Isomorphismus $\varphi : V \rightarrow \mathbb{R}^n$ die Menge $\varphi(M) \subseteq \mathbb{R}^n$ perfekt ist.
- g) Ein Gitter in einem euklidischen Vektorraum ist genau dann perfekt, wenn die Menge seiner Minimalvektoren perfekt ist.

Beispiel 4.2.3 Die unzerlegbaren Wurzelgitter A_n , $n \geq 1$ und D_n , $n \geq 3$, E_6 , E_7 , E_8 sind perfekt.

Für D_n ergibt sich der Beweis unmittelbar aus Bemerkung 4.2.1, indem man die $\mathbf{e}_i + \mathbf{e}_j$ und $\mathbf{e}_i - \mathbf{e}_j$ gemeinsam benutzt. Für A_n könnte man die folgende Bemerkung benutzen, und E_7 und E_8 sind Obergitter von A_7 bzw. D_8 mit gleichem Minimum, also einer größeren Menge von Minimalvektoren, und somit erst recht perfekt. Unten werden wir mittels Lemma 4.2.9 einen gemeinsamen Beweis für alle Fälle geben, der nur die Definition und einfache Eigenschaften, aber nicht die Klassifikation der Wurzelgitter benutzt.

Die folgende Bemerkung klärt, wie man in einem euklidischen Vektorraum Perfektheit einer Menge von Vektoren direkt definieren kann, ohne den Umweg über die Bemerkung 4.2.2 b). Hierzu benötigt man ein Analogon, bzw. eine Verallgemeinerung der Abbildung $\mathbf{x} \mapsto \mathbf{x}\mathbf{x}^t$, $\mathbb{R}^n \rightarrow \mathcal{S} \subset \mathbb{R}^{n \times n}$.

Bemerkung 4.2.4 Für einen beliebigen Vektorraum V bezeichne $\mathcal{S}_V$ den Vektorraum der symmetrischen Bilinearformen auf V . Für einen euklidischen Vektorraum (V, b) definiere die Abbildung

$$V \rightarrow \mathcal{S}_V, z \mapsto b_z, \text{ wobei } b_z(x, y) := b(x, z)b(y, z).$$

Eine Teilmenge $M \subseteq V$ ist genau dann perfekt, wenn die Menge der b_z , $z \in M$, den Vektorraum $\mathcal{S}_V$ erzeugt.

Zum Beweis bemerkt man, dass für $V = \mathbb{R}^n$ und b das Standardskalarprodukt die Matrix von $b_{\mathbf{z}}$ bezüglich der Standardbasis genau die obige Matrix $Q_{\mathbf{z}}$ ist.

Proposition 4.2.5 *Es sei M eine perfekte Teilmenge eines n -dimensionalen Vektorraumes V . Dann gilt:*

- a) $|M| \geq \frac{1}{2}n(n+1)$
- b) M erzeugt V .
- c) Für jedes Skalarprodukt auf V ist M orthogonal unzerlegbar.

Korollar 4.2.6 Es sei L ein perfektes Gitter der Dimension n auf einem euklidischen Vektorraum.

- a) L besitzt mindestens $\frac{1}{2}n(n+1)$ Paare $\pm v$ von Minimalvektoren.
- b) Alle sukzessiven Minima von L stimmen überein:

$$\min_1 L = \min_2 L = \dots = \min_n L.$$

- c) L ist unzerlegbar.

BEWEIS von c): Angenommen, L ist zerlegbar als $L = L_1 \perp L_2$ mit nicht-trivalem L_1 und L_2 . Wir zeigen, dass dann auch $\text{Min } L$ zerlegbar ist, in Widerspruch zu Proposition 4.2.5.c). Jedenfalls liegt jeder kürzeste Vektor $v \in L$ in L_1 oder in L_2 , denn in einer Summe $v = v_1 + v_2$, $v_i \in L_i \setminus 0$ wäre $\|v\| = \|v_1\| + \|v_2\|$ und deshalb $0 < \|v_1\| \leq \|v\|$ und deshalb v kein kürzester Vektor. Weiter sind $\text{Min } L \cap L_1$ und $\text{Min } L \cap L_2$ beide nicht leer, weil sonst $\text{Min } L \subset L_2$ bzw. $\text{Min } L \subset L_1$ wäre, im Widerspruch zu Teil b). $\square$

Bemerkung: Die Aussage 4.2.5.c) ist tatsächlich stärker als 4.2.6.c), d.h. in einem unzerlegbaren Gitter kann die Menge der Minimalvektoren zerlegbar sein. Ein Beispiel ist das Gitter $D_n^\#$ für $n \geq 5$ mit den Minimalvektoren $\{\pm \mathbf{e}_1, \dots, \pm \mathbf{e}_n\}$. Dieses ist allerdings nur möglich, wenn das Gitter nicht von seinen Minimalvektoren erzeugt wird.

Wir wissen aus der Reduktionstheorie und aus der bisherigen Behandlung des Problems dichtester Gitter, dass man den Ausdruck $F[\mathbf{z}]$ für $F \in \mathcal{S}$ und $\mathbf{z} \in \mathbb{Z}^n$ oft als Funktion zweier gleichberechtigter Variablen betrachtet, der quadratischen Form F und des Vektors $\mathbf{z}$. Dieser Aspekt ist auch für die Behandlung perfekter Formen nützlich. Hierzu liefert das folgende Lemma ein interessantes neues Werkzeug: auf dem Vektorraum $\mathcal{S}$ wird ein Skalarprodukt eingeführt, mit dessen Hilfe man $F[\mathbf{x}]$ “universell” ausdrücken kann. Mit $\text{tr } A$ wird wie üblich die Spur einer Matrix $A \in \mathbb{R}^{n \times n}$ bezeichnet:

Lemma 4.2.7 a) Durch $\langle A, B \rangle := \text{tr}(A^t B)$ wird auf $\mathbb{R}^{n \times n}$ ein Skalarprodukt definiert.

b) Für $F \in \mathcal{S}$, $\mathbf{x} \in \mathbb{R}^n$ gilt $F[\mathbf{x}] = \langle F, Q_{\mathbf{x}} \rangle$.

Der Beweis ergibt sich durch einfaches Nachrechnen; man beachte, dass mit $A = (a_{ij})$, $B = (b_{ij})$ gilt $\langle A, B \rangle = \sum_{i,j=1}^n a_{ij} b_{ij}$. Wenn wir $\mathbb{R}^{n \times n}$ mit $\mathbb{R}^{n^2}$ identifizieren, haben wir also das Standard-Skalarprodukt.

Nach diesen Vorbereitungen ist der folgende Satz sehr schnell zu beweisen; die dortige Beschreibung der perfekten Formen ist in der klassischen Literatur die Definition: Grob gesprochen ist eine Form perfekt, wenn sie bestimmt wird durch die Menge ihrer Minimalvektoren und deren Länge.

Satz 4.2.8 Eine positiv definite Form F ist genau dann perfekt, wenn folgendes gilt: Wenn $G \in \mathcal{S}$ ist und $G[\mathbf{z}] = F[\mathbf{z}]$ für alle $\mathbf{z} \in \text{Min } F$, dann ist $G = F$.

BEWEIS: Bei gegebener Menge $M = \text{Min } F$ von Minimalvektoren ist die Eigenschaft aus dem Satz eine lineare Bedingung: Wenn wir $F - G =: C$ setzen und für jedes $\mathbf{z} \in M$ die Linearform $C \mapsto C[\mathbf{z}]$ auf $\mathcal{S}$ betrachten, so soll der Schnitt der Kerne aller dieser Linearformen gleich Null sein. Nach Lemma 4.2.7.b) ist der Kern einer solchen Linearform genau der Orthogonalraum von $Q_{\mathbf{z}}$ in $\mathcal{S}$. Der

Schnitt dieser Orthogonalräume ist genau dann Null, wenn die $Q_{\mathbf{z}}$ ganz $\mathcal{S}$ erzeugen. $\square$

Wenn man Lemma 4.2.7.b) nicht speziell auf die Menge der Minimalvektoren einer quadratischen Form, sondern auf irgendeine Vektormenge anwendet, und außerdem die Situation auf beliebige Vektorräume statt des $\mathbb{R}^n$ verallgemeinert, erhält man folgendes:

Lemma 4.2.9 Eine Teilmenge $M \subset V$ eines Vektorraumes ist genau dann perfekt, wenn folgendes gilt: Jede symmetrische Bilinearform c auf V mit $c(v, v) = 0$ für alle $v \in M$ ist identisch Null.

Die perfekten Teilmengen von V sind also genau die “Testmengen” für quadratische Formen (beliebiger Signatur) auf V . Anders ausgedrückt, M ist “nicht quadratisch”, d.h. darf in keiner Quadrik $\{x \in V \mid c(x, x) = 0\}$ enthalten sein. (Konsequenterweise sollte man in der letzten Formulierung M und die Quadrik durch ihr jeweiliges Bild im projektiven Raum $\mathbb{P}(V) = V/\mathbb{R}^*$ ersetzen.)

4.2.10 Beweis zu Beispiel 4.2.3: Es sei L ein unzerlegbares Wurzelgitter und $a_1, a_2, \dots, a_n$ eine Wurzelbasis von L , also $\langle a_i, a_i \rangle = 2$ und $\langle a_i, a_j \rangle \in \{0, -1\}$ für $i \neq j$. Es sei Γ der zugehörige Orthogonalitätsgraph mit Knotenmenge $I = \{1, 2, \dots, n\}$ (das Coxeter-Diagramm von L). Weil L unzerlegbar ist, ist Γ zusammenhängend. Weiter ist Γ ein Baum (enthält keine Kreise).

Der Beweis dieser Tatsache ergibt sich sofort aus der Klassifikation der Wurzelgitter, bzw. ihrer Coxeter-Diagramme, benötigt diese aber nicht. Vielmehr handelt es sich um ein einfaches Lemma, das man sich innerhalb des Beweises des Klassifikationssatzes überlegt: ein Kreis im Coxeter-Graphen würde zu einem isotropen Vektor führen.

Für jede Teilmenge $J \subseteq I$ setze nun $a_J := \sum_{j \in J} a_j$. Mit Induktion über $|J|$ zeigt man leicht:

$$\langle a_J, a_J \rangle = 2 \text{ für jede zusammenhängende Teilmenge } J \subseteq I. \quad (4.2.2)$$

Wir wenden nun das Kriterium aus Lemma 4.2.9 an: Es sei c eine symmetrische Bilinearform mit $c(a, a) = 0$ für alle $a \in \text{Min } L = L_{(2)}$, insbesondere $c(a_i, a_i) = 0$ für alle $i \in I$. Wir zeigen durch Induktion über den Abstand $d(i, j)$ von i und j in Γ , dass $c_{ij} := c(a_i, a_j) = 0$ für alle Paare (i, j) . Sei also $i \neq j$ und $J \supseteq \{i, j\}$ die Menge der Knoten, die in dem eindeutig bestimmten Weg von i nach j in Γ vorkommen. Nach Voraussetzung und (4.2.2) gilt

$$0 = c(a_J, a_J) = \sum_{k, l \in J} c_{kl} = 2c_{ij} + \sum_{\{k, l\} \neq \{i, j\}} c_{kl}. \quad (4.2.3)$$

In der letzten Summe sind nach Induktionsannahme alle $c_{kl} = 0$, weil immer $d(k, l) < d(i, j)$ ist. $\square$

Wir wenden uns nun wieder dem Problem der gitterförmigen dichtesten Kugelpackungen und damit dem Studium der Hermite-Funktion $\gamma : \mathcal{S}_{>0} \rightarrow \mathbb{R}$ zu.

Lemma 4.2.11 Zu jeder quadratischen Form $A \in \mathcal{S}_{>0}$ gibt es eine Umgebung $\mathcal{U}$ von A in $\mathcal{S}_{>0}$ derart, dass $\text{Min } A' \subseteq \text{Min } A$ für alle $A' \in \mathcal{U}$.

BEWEIS(SKIZZE): Es sei $\mathbf{z} \in \text{Min } F$ und $\mathbf{w} \in \mathbb{Z}^n \setminus \text{Min } F$. Dann gilt $A[\mathbf{z}] < A[\mathbf{w}]$, und die gleiche Ungleichung gilt auch für alle A' aus einer geeigneten Umgebung $\mathcal{U}_{\mathbf{z},\mathbf{w}}$ von A . D.h. $\mathbf{w}$ ist auch für alle diese A' kein Minimalvektor. Für quadratische Formen A' , die nahe bei A liegen, kann sich das Minimum $m' := \min A'$ nur wenig von $\min A$ unterscheiden; weiter sind wegen der Äquivalenz aller Normen auf $\mathbb{R}^n$ die Komponenten eines Vektors $\mathbf{x} \in \mathbb{R}^n$ mit $A'[\mathbf{x}] = m'$ nicht beliebig groß, sondern beschränkt durch eine Schranke C , die für alle in Frage kommenden m' und A' gleich gewählt werden kann. D.h. als neue Minimalvektoren für ein A' nahe bei A kommen überhaupt nur endlich viele $\mathbf{w} \in \mathbb{Z}^n$ in Frage. Für diese endlich vielen $\mathbf{w}$ und die endlich vielen $\mathbf{z} \in \text{Min } A$ können wir den Durchschnitt der obigen Umgebungen $\mathcal{U}_{\mathbf{z},\mathbf{w}}$ bilden und erhalten so in der Tat eine Umgebung $\mathcal{U}$ derart, dass $A'[\mathbf{z}] < A'[\mathbf{w}]$ gilt für alle $\mathbf{z} \in \text{Min } A$, $\mathbf{w} \in \mathbb{Z}^n \setminus \text{Min } A$, $A' \in \mathcal{U}$. $\square$

Satz 4.2.12 (Korkine und Zolotareff) Jede Extremform ist perfekt.

BEWEIS: Es sei $A \in \mathcal{S}_{>0}$ nicht perfekt und $B \in \mathcal{S}$ so, dass $B[\mathbf{z}] = 0$ für alle $\mathbf{z} \in \text{Min } A$, aber $B \neq 0$. Wir betrachten nun die Schar von Formen $A_t := A + tB$. Nach Lemma 4.2.11 gibt es ein $\varepsilon > 0$ so, dass für $|t| < \varepsilon$ gilt $\min A_t = \min A$ (und auch $\text{Min } A_t = \text{Min } A$). Wir zeigen nun, dass für genügend kleines positives oder negatives t gilt $\det A_t < \det A$. Für diese t folgt weiter $\gamma(A_t) > \gamma(A)$, das heißt, A ist nicht extrem. Es reicht, diese Behauptung für $\log \det A_t$ statt $\det A_t$ zu zeigen. Mit anderen Worten behaupten wir, dass die Funktion $\log \det A_t$ in $t = 0$ kein lokales Minimum hat. Wir gehen hierzu ähnlich vor wie beim Beweis von Lemma 4.1.3: die Matrizen A und B können simultan diagonalisiert werden, und es ergibt sich $\det(A_t) = \prod_{i=1}^n (a_i + b_i t)$ mit $a_i > 0$ und weiter

$$\frac{d}{dt} \log \det A_t = \sum \frac{d}{dt} \log(a_i + b_i t) = \sum \frac{b_i}{a_i + b_i t}, \quad (4.2.4)$$

$$\frac{d^2}{dt^2} \log \det A_t = - \sum \frac{b_i^2}{(a_i + b_i t)^2}. \quad (4.2.5)$$

D.h. die zweite Ableitung von $\log \det A_t$ bei $t = 0$ ist strikt negativ, die Funktion könnte dort zwar evtl. eine Extremstelle, aber jedenfalls kein lokales Minimum haben. (Geometrisch: die Funktion ist auf einer Umgebung von $t = 0$ strikt konvex, was ebenfalls der Existenz eines Tiefpunktes auf dem Funktionsgraphen widerspricht.) $\square$

Wir kommen nun zu einer zweiten Bedingung, die alle Extremformen erfüllen müssen:

Definition 4.2.13 Ein Gitter (L, b) heißt *eutaktisch*, wenn sein Skalarprodukt sich schreiben läßt als

$$b(x, y) = \sum_{v \in \text{Min } L} \rho_v b(x, v) b(y, v) \text{ mit } \rho_v \in \mathbb{R}_{>0}. \quad (4.2.6)$$

bzw. mit der Bezeichnung von 4.2.4

$$b = \sum_{v \in \text{Min } L} \rho_v b_v \text{ mit } \rho_v \in \mathbb{R}_{>0}. \quad (4.2.7)$$

Man beachte, dass alle Koeffizienten strikt positiv sein sollen. Üblicherweise kennt man diese Definition in folgender Form: Eine positiv definite quadratische Form F heißt *eutaktisch*, falls positive Zahlen $\rho_{\mathbf{z}} > 0$, $\mathbf{z} \in M := \text{Min } F$, existieren mit

$$F^{-1} = \sum_{\mathbf{z} \in M} \rho_{\mathbf{z}} \mathbf{z} \mathbf{z}^t = \sum_{\mathbf{z} \in M} \rho_{\mathbf{z}} Q_{\mathbf{z}}. \quad (4.2.8)$$

Dieses ist äquivalent zu

$$F = \sum_{\mathbf{z} \in M} \rho_{\mathbf{z}} (F\mathbf{z})(F\mathbf{z})^t = \sum_{\mathbf{z} \in M} \rho_{\mathbf{z}} Q_{F\mathbf{z}}, \quad (4.2.9)$$

was genau der Gleichung (4.2.7) aus der Definition entspricht.

Die Überprüfung der Eutaxie eines Gitters wird oft dadurch erleichtert (etwa bei Wurzelgittern), dass die orthogonale Gruppe (Isometriegruppe) $O(L)$ von L transitiv auf $\text{Min } L$ operiert und somit alle Koeffizienten ρ_v einander gleich gewählt werden können (z. T. sogar gleich sein müssen). In der Tat gilt folgendes Lemma:

Lemma 4.2.14 Es sei L ein perfektes Gitter, dessen orthogonale Gruppe $O(L)$ transitiv auf der Menge der Minimalvektoren $\text{Min } L$ operiert. Dann ist L eutaktisch.

BEWEIS: Wir wenden die Perfektheit in Form von Bemerkung 4.2.4 an, und zwar auf das zu L gehörige Skalarprodukt b selbst: es gibt Skalare $\rho_v \in \mathbb{R}$, $v \in M := \text{Min } L$ mit

$$b = \sum_{v \in M} \rho_v b_v. \quad (4.2.10)$$

Nun wenden wir die Operation der endlichen Gruppe $G := O(L, b)$ an, um diese Darstellung so zu modifizieren, dass alle ρ_v gleich einem festen ρ sind. Da b positiv definit ist und die b_v positiv semidefinit sind, kann dann nur $\rho > 0$ sein. Die Gruppe $\text{GL}(V)$ des unterliegenden Vektorraumes operiert auf dem Vektorraum $\mathcal{S}_V$ aller symmetrischen Bilinearformen von rechts durch $c^g(x, y) := c(gx, gy)$ für alle $g \in \text{GL}(V)$, $x, y \in V$. Der Stabilisator von $b \in \mathcal{S}_V$ ist definitionsgemäß

die (volle) orthogonale Gruppe $O(b) = O(V, b)$. Die Menge der speziellen Bilinearformen b_x ist invariant (aber nicht fix) unter $O(b)$: für $x \in V$ und $g \in O(b)$ gilt $(b_x)^g = b_{g^{-1}x}$. Die Gruppe G operiert auf der Menge $M = \text{Min } L$, und zwar nach Voraussetzung transitiv, entsprechend auch auf der Menge der b_v , $v \in M$. Nun wenden wir auf beiden Seiten der Gleichung (4.2.12) den Operator $\frac{1}{|G|} \sum_{g \in G} g$ an (formal steht hier ein Element der Gruppenalgebra $\mathbb{R}[G]$); dabei bleibt die linke Seite fest, und es ergibt sich

$$b = \frac{1}{|G|} \sum_{g \in G} \sum_{v \in M} \rho_v b_{g^{-1}v} = \sum_{v \in M} \left(\frac{1}{|G|} \sum_{g \in G} \rho_{gv} \right) b_v. \quad (4.2.11)$$

Wir erhalten eine Gleichung der gewünschten Form:

$$b = \rho \sum_{v \in M} b_v \text{ mit } \rho := \frac{1}{|G|} \sum_{g \in G} \rho_{gv}. \quad (4.2.12)$$

□

Korollar 4.2.15 Die irreduziblen Wurzelgitter A_n , D_n , $n \geq 4$, E_6, E_7, E_8 sind eutaktisch.

Nach dem schon angekündigten Satz von Voronoi sind diese Gitter dann extrem.