Geometry of Numbers

Inoffizielles Skript
zur Vorlesung von Prof. Henk, WS 2017/18

Henning Seidler

Inhaltsverzeichnis

In den letzten 100 Jahren wurden viele Brücken zwischen diversen gebieten der Mathematik geschlagen. So hat man erkannt, dass man gewisse Probleme der Zahlentheorie mit geometrischen Methoden lösen kann. Wir haben viele Verbindungen zu anderen Teilgebieten:

- (Diskrete) Geometrie
- Zahlentheorie
- additive Kombinatorik
- Funktionalanalysis
- Theorie der Bewertungen (engl.: "valuations")
- Optimierung

1 Einführung

Wir beginnen mit der Untersuchung von positiv definiten quadratischen Formen in n Variablen $x = (x_1, \ldots, x_n)$.

1.1 Definition. Eine quadratische Form ist eine Funktion der Form $q(x) = x^T Q x$. Dabei heißt q positiv (semi-) definit, falls Q positiv (semi-)definit ist.

- Das heißt Q ist symmetrisch und alle Eigenwerte sind positiv. Somit können wir Q diagonalisieren in die Form $Q = B^T D B$, wobei $D = (\lambda_1, \ldots, \lambda_n)$ eine Diagonalmatrix ist.
- Alternativ haben wir die Cholesky-Zerlegung $Q = (\sqrt{D}B)^T \cdot (\sqrt{D}B)$.
- Äquivalent dazu: Q ist positiv definit $\Leftrightarrow \forall x \neq 0. x^T Q x > 0$.

1.2 Bemerkung. Aus der Zahlentheorie haben wir nun die Frage: Was ist das Minimum einer positiv definiten quadratischen Form für $x \in \mathbb{Z}^n \setminus \{0\}$.
Dazu wollen wir zeigen: Es gibt eine Funktion $c : Q \mapsto c(Q)$ so, dass für jede p.d.q. Form gilt $\exists x \in \mathbb{Z}^n \setminus \{0\}. q(x) \leq c(Q)$.
Diese Funktion liefert uns eine obere Schranke für das Minimum. Wir werden zeigen, dass $c(Q) = h_n \cdot \sqrt[n]{\det Q}$ ist, wobei h_n die sogenannte Hermite-Konstante ist.

- Lagrange zeigte 1773, dass $h_2 = \frac{2}{\sqrt{3}}$.
- Gauss, 1831: $h_3 = \sqrt[3]{2}$.
- Korleine/Zolotareff, 1872/1877: Werte?
- Hermite, 1850: $h_n \leq \left(\frac{2}{\sqrt{3}}\right)^{n-1}$, aber dies liefert nur eine obere Schranke.

1.3 Beispiel. Nehmen wir die Form q aus der Matrix $Q = \begin{pmatrix} 193 & \frac{217}{2} \\ \frac{217}{2} & 61 \end{pmatrix}$. Dann ist $\frac{2}{\sqrt{3}}\sqrt{\det Q} = 1$.
Nach Lagrange gibt es also ein $z \in \mathbb{Z}^2 \setminus \{0\}$ mit $q(z) = 193z_1^2 + 217z_1z_2 + 61z_2^2 \leq 1$. Und da alles ganzzahlig ist, gilt Gleichheit.
Das Finden dieses Punktes ist im Allgemeinen das Problem eines kürzesten Vektors in einem Gitter und führt zur "Reduktionstheorie"..

1.4 Bemerkung. Was würde passieren, wenn Q nur positiv semidefinit ist? Wir haben also mindestens einen Eigenwert 0. Damit ist auch $\det Q = 0$, beachte $Q \in \mathbb{Q}^{n \times n}$. Dann gibt es eine rationale Lösung $Qv = 0$, mit $v \neq 0$. Damit gibt es auch immer einen ganzzahligen Vektor im Kern.

1.5 Bemerkung (Reduktionstheorie für unser Beispiel). Wir formen q um in $q'(x) = q(Ux) = x^T(U^T Q U)x$ mit $U \in \mathrm{GL}_N(\mathbb{Z})$. Damit ist $\det U = \pm 1$. Daraus folgt $q'(\mathbb{Z}^n) = q(U\mathbb{Z}^n) = q(\mathbb{Z}^n)$.
Idee: Finde eine "bestimmte" "reduzierte" Form q'. Da beide die gleichen Werte annehmen, haben sie insbesondere auch das gleiche Minimum.

1.6 Beispiel (Forsetzung Beispiel 1.3). Wähle $U = \begin{pmatrix} 5 & -9 \\ -9 & 16 \end{pmatrix}$. Dann ist $q'(x) = x_1^2 + x_1x_2 + x_2^2$.
Das hat klar ein Minimum bei $q(e_1) = 1$. Das zugehörige Minimum von q ist dann $Ue_1 = (5, -9)^T$.

In vielen Reduziertheitsbegriffen wird auch verlangt, dass e_1 das Minimum für die reduzierte p.d.q. Form ist.

1.7 Bemerkung (Hermann Minkowski, 1864-1909). Wir schreiben $Q = A^T A$ mit $A \in \mathbb{R}^{n\times n}$. Dann bekommen wir für die Niveaumengen ("sub-level-sets")

$$\begin{aligned}\{x \in \mathbb{R}^n : q(x) \leq \rho\} &= \{x \in \mathbb{R}^n : (Ax)^T(Ax) \leq \rho\} = \{A^{-1}x : x^T x \leq \rho\} \\ &= (\sqrt{\rho}A^{-1})\{x \in \mathbb{R}^n : x^T x \leq 1\} = (\sqrt{\rho}A^{-1})B_n(0)\end{aligned}$$

und dies sind Ellipsiode.

Das Finden des Minimums von $q(x)$ ist also das geometrische Problem, das kleinste ρ zu finden so, dass obiger Ellipsoid einen nicht-trivialen ganzzahligen Punkt enthält.

$$\min\left\{\rho \in \mathbb{R}^n : \sqrt{\rho}A^{-1}B_n \cap (\mathbb{Z}^n \setminus \{0\}) \neq \emptyset\right\}$$

1.8 Beispiel (Forsetzung Beispiel 1.3).

$$U^T Q U = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}^T \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} =: A^T A$$

Minkowski (1889): Für jede kompakte symmetrische Menge K (d.h. $x \in K \Leftrightarrow -x \in K$) mit Volumen mindestens 2^n enthält einen Punkt aus $\mathbb{Z}^n \setminus \{0\}$. Die Grenze 2^n ist scharf, wie man mit $K = (-1,1)^n$ sieht.
Für das Volumen gilt

$$\operatorname{vol}(\sqrt{\rho}B_n) = \sqrt{\rho}^n \cdot (\det A)^{-1} \operatorname{vol}(B_n)$$

Damit erhalten wir die Schranke

$$\rho \geq 4 \cdot \operatorname{vol}(B_n)^{-\frac{2}{n}} \cdot (\det Q)^{\frac{1}{n}} \sim \text{const} \cdot n \cdot \sqrt[n]{\det Q}$$

Das heißt, $h_n \leq c \cdot n$ für eine Konstante c, was deutlich besser ist, als die exponentielle Schranke von Hermite.

Notation. Sei $A \subseteq \mathbb{R}^n$.

- $\operatorname{aff} A$ ist die affine Hülle von A.
- $\operatorname{lin} A$ ist die lineare Hülle, also das Erzeugnis
- Wir schreiben $\dim A := \dim(\operatorname{aff} A)$.

Für $A = \emptyset$ ist $\operatorname{lin} A = \{0\}$ und $\operatorname{aff}(A) = \emptyset$.

1.9 Definition.

- Eine Menge $C \subseteq \mathbb{R}^n$ heißt *konvex*, falls

$$\forall c_1, c_2 \in X. \forall \lambda \in [0,1]. \lambda c_1 + (1-\lambda)c_2 \in C$$

- Ist $K \subseteq \mathbb{R}^n$ konvex und kompakt, dann heißt K *konvexer Körper* (engl. "convex body").
- Gilt zusätzlich, dass $K = -K$, so heißt K *symmetrisch*.
- Wir schreiben $\mathcal{K}^n$ für die Menge aller konvexen Körper in $\mathbb{R}^n$ und $\mathcal{K}_o^n := \{K \in \mathcal{K}^n : K \text{ symmetrisch}\}$.

1.1 Normen

Ist $|\cdot| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ eine Norm, so ist die zugehörige Einheitskugel $B := \{x \in \mathbb{R}^n : |x| \leq 1\}$. Diese ist eine symmetrischer konvexer Körper.
Für $K \in \mathcal{K}_o^n$ mit $\dim K = n$ heißt

$$|\cdot|_K : \mathbb{R}^n \to \mathbb{R}_{\geq 0} \qquad\qquad |x|_K := \min\{\rho \in \mathbb{R}_{\geq 0} : x \in \rho K\}$$

die Distanzfunktion und definiert eine Norm (siehe Übung).
Eine wichtige Klasse sind die p-Normen $|\cdot|_p$ und deren Einheitskugeln B_n^p für $p \in [1, \infty]$

$$|x|_p := \left(\sum_{i=1}^n |x_i|^p\right)^{\frac{1}{p}}$$

mit dem Grenzfall $|x|_\infty = \max\{|x_i| : i = 1, \ldots, n\}$. Wir betrachten nur die Fälle $p \geq 1$, da sonst die Einheitskugel nicht mehr konvex ist.

1.2 Hyperebenen

Sei $a \in \mathbb{R}^n \setminus \{0\}$ und $b \in \mathbb{R}$. Dann definiert dies eine Hyperebene und zwei Halbräume durch

$$\begin{aligned} H(A,b) &:= \{x \in \mathbb{R}^n : \langle a, x\rangle = b\} \\ H(A,b)_\geq &:= \{x \in \mathbb{R}^n : \langle a, x\rangle \geq b\} \\ H(A,b)_\leq &:= \{x \in \mathbb{R}^n : \langle a, x\rangle \leq b\} \end{aligned}$$

1.10 Definition. Sei $K \in \mathcal{K}^n$ und $H = H(a,b)$ mit $H \cap K \neq \emptyset$ und $K \subseteq H_\leq(a,b)$. Dann heißt H *Stützhyperebene* von K.

1.11 Lemma. *Sei $K \in \mathcal{K}^n$ und $a \in \mathbb{R}^n \setminus \{0\}$. Dann existiert eine eindeutige Verschiebung $h_K(a)$ so, dass $H(a, h_K(a))$ eine Stützebene von K ist. Dabei ist $h_K(a) = \max\{\langle a, x\rangle : x \in K\}$. Diese Funktion heißt Stützfunktion (engl.: "support function").*

1.12 Definition. Ist $K \in \mathcal{K}^n$ mit $0 \in \operatorname{int} K$, dann ist $r_K : \mathbb{R}^n \setminus \{0\} \to \mathbb{R}$ via $r_K(x) := \max\{\lambda > 0 : \lambda x \in K\}$ die *Radialfunktion.*

1.3 Polare Mengen

Sei $X \subseteq \mathbb{R}^n$. Dann definieren wir $X^* := \{y \in \mathbb{R}^n : \forall x \in X. \langle x, y\rangle \leq 1\}$.

Abbildung 1: Beispiel für den *-Operator, links X, rechts X^*.

Für $X = B_2^n$ bleibt $X^* = X$.

1.13 Lemma. *X^* ist konvex und abgeschlossen.*
Für konvexes X gilt: X^* ist beschränkt genau dann, wenn $0 \in \operatorname{int}(X)$.

1.4 Volumen

Eine Menge $D \subseteq \mathbb{R}^n$ heißt Peano-Jordan-messbar, falls für

$$\chi_D : \mathbb{R}^n \to \{0,1\} \qquad \chi_D(x) = \begin{cases} 1 & : x \in D \\ 0 & : x \notin D \end{cases}$$

Riemann-integrierbar ist, also $\mathrm{vol}(D) := \int_{\mathbb{R}^n} \chi_D(x)\mathrm{d}x$ existiert.

1.14 Proposition. *Sei $X \subseteq \mathbb{R}^n$ messbar. Dann*

$$\mathrm{vol}(X) = \lim_{m\to\infty} \frac{\#\left(X \cap \frac{1}{m}\mathbb{Z}^n\right)}{m^n}$$

Beweis. Die Formel beschreibt einfach das Ausfüllen von X mit Würfeln der Kantenlänge $\frac{1}{m}$. □

1.15 Lemma. *Für $A \in \mathbb{R}^{n\times n}$ gilt $\mathrm{vol}(AX) = \det A \cdot \mathrm{vol}(X)$. Insbesondere gilt $\mathrm{vol}(\lambda X) = \lambda^n \cdot \mathrm{vol}(X)$. Weiter ist $\mathrm{vol}(X+t) = \mathrm{vol}(X)$ (Translationsinvarianz) und $X \subseteq Y \implies \mathrm{vol}(X) \leq \mathrm{vol}(Y)$ (Monotonie).*

1.16 Definition. Seien $K, L \in \mathcal{K}^n$. Dann definieren wir den *Hausdorff-Abstand*

$$d_H(K,L) := \min\{\rho \in \mathbb{R}_{\geq 0} : K \subseteq L + \rho B_n \wedge L \subseteq K + \rho B_n\}$$

dies definiert eine Metrik auf $\mathcal{K}^n$, und sogar einen vollständigen Raum.

1.17 Theorem (Blaschke selection theorem). *Jede beschränkte Folge in $\mathcal{K}^n$ enthält eine konvergierende Teilfolge.*

1.18 Theorem (Löwer-John). *Für jedes $K \in \mathcal{K}^n$ mit $\dim K = n$ gibt es ein eindeutiges Ellipsoid $a + AB_n$, gegeben durch $A \in \mathrm{GL}_n(\mathbb{R})$ und $a \in \mathbb{R}^n$, welche maximales Volumen hat und es gilt $a + AB_n \subseteq K \subseteq a + nAB_n$. Das heißt, wir geben zwei Schranken an, deren Größenfaktor maximal n ist.*
Wenn K symmetrisch ist, dann ist $a = 0$ und wir können den Faktor n durch $\sqrt{n}$ ersetzen.

1.19 Theorem (Bourgain-Milman). *Es gibt eine positive absolute Konstante C so, dass*

$$\mathrm{vol}(K)\,\mathrm{vol}(K^*) \geq C^n\,\mathrm{vol}(B_n)^2$$

für alle $K \in \mathcal{K}_o^n$ mit $\dim K = n$.

Bemerkung (Mahler-Vermutung). Das Mahler-Volumen $M(K) := \mathrm{vol}(K)\,\mathrm{vol}(K^*)$

paar Minuten fehlen

1.20 Theorem (Brunn-Minkowski). *Seien $K, L \in \mathrm{SL}^n$ und $\lambda \in [0,1]$. Dann ist*

$$\begin{aligned} \overline{vol}\,(\lambda K + (1-\lambda)L)^{\frac{1}{n}} \geq \lambda\,\mathrm{vol}(K)^{\frac{1}{n}} + (1-\lambda)\,\mathrm{vol}(L)^{\frac{1}{n}} \geq \mathrm{vol}(K)^{\frac{\lambda}{n}} \cdot \mathrm{vol}(L)^{\frac{1-\lambda}{n}} \\ \implies \mathrm{vol}(\lambda K + (1-\lambda)L) \geq \mathrm{vol}(K)^{\lambda} \cdot \mathrm{vol}(L)^{1-\lambda} \end{aligned}$$

1.21 Theorem (Caratheodory). *Sei $X \subseteq \mathbb{R}^n$. Dann ist*

$$\mathrm{conv}(X) = \left\{ \sum_{i=0}^{\dim X} \lambda_i x_i : \sum \lambda_i = 1, \lambda_i \geq 0, x_i \in X \right\}$$

1.22 Theorem (Minkowsky-Weil). *C ist ein Polytop genau dann, wenn es ein beschränktes Polyeder ist.*

Bemerkung. Sei $S = \operatorname{conv}(v_0, \dots, v_n)$ ein Simplex. Dann ist

$$\operatorname{vol}(S) = \frac{1}{n!} \cdot \det(v_1 - v_0, \dots, v_n - v_0)$$

Bemerkung. Es ist ein offenes Problem, was die minimale Anzahl an Simplizes zur Triangulierung eines Würfels ist. Da die untere Schranke $n!$ viel zu schnell steigt, ist Triangulierung nicht geeignet, um das Volumen eines Körpers zu berechnen.

Bemerkung. Im 3D-Würfel erhalten wir einen regelmäßigen Tetraeder, indem wir die konvexe Hülle von zwei gegenüber liegenden Diagonalen nehmen. Die Frage ist, in welchen Dimensionen der Würfel $[0,1]^n$ ein regelmäßiges Simplex enthält. Die Vermutung ist, dass es genau die Dimensionen sind, zu denen es Hadamard-Matrizen gibt.

2 Gitter

Sei $S \subseteq \mathbb{R}^n$.Dann bezeichnen wir

$$\operatorname{lin}_{\mathbb{Z}} S := \left\{ \sum_{i=1}^{m} z_i s_i : z_i \in \mathbb{Z}, s_i \in S, m \in \mathbb{N} \right\}$$

2.1 Definition. Seien $b_1, \dots, b_n \in \mathbb{R}^n$ linear unabhängig.

$$\Lambda := \operatorname{lin}_{\mathbb{Z}}\{b_1, \dots, b_n\}$$

heißt n-dimensionales Gitter. Die Menge $\{b_1, \dots, b_n\}$ heißt Basis, ein $b \in \Lambda$ heißt Gitterpunkt. Die Menge aller n-dimensionalen Gitter bezeichnen wir mit $\mathcal{L}^n$.
Wir werden auch schreiben $B = (b_1, \dots, b_n)$ und $\Lambda = B\mathbb{Z}^n$.

Bemerkung. Gitter haben viele Bezüge zur Kryptografie, wo es darum geht, zu einer gegebenen Basis einen kürzesten Vektor zu finden.

2.2 Definition. Eine Matrix $U \in \mathbb{Z}^{n \times n}$ heißt *unimodular* falls $|\det U| = 1$. Die Menge aller unimodularen Matrizen bildet die Gruppe $\mathrm{GL}(n, \mathbb{Z})$.

2.3 Proposition. *Es gilt* $\mathrm{GL}(n, \mathbb{Z}) = \{U \in \mathbb{R}^{n \times n} : U\mathbb{Z}^n = \mathbb{Z}^n\}$.

Beweis. Wir haben die Kette

$$U \in \mathrm{GL}(n, \mathbb{Z}) \Leftrightarrow U, U^{-1} \in \mathbb{Z}^{n \times n} \Leftrightarrow U\mathbb{Z}^n \subseteq \mathbb{Z}^n, U^{-1}\mathbb{Z}^n \subseteq \mathbb{Z}^n \Leftrightarrow U\mathbb{Z}^n = \mathbb{Z}^n$$

Die letzte Rückrichtung folgt, da U vollen Rang haben muss. □

2.4 Lemma. *Sei $\Lambda = B\mathbb{Z}^n \in \mathcal{L}^n$. Dann ist A eine Basis genau dann, wenn ein $U \in \mathrm{GL}(n, \mathbb{Z})$ existiert mit $A = BU$, oder kurz $B^{-1}A \in \mathrm{GL}(n, \mathbb{Z})$.*

Beweis. Wir haben

$$A \text{ Basis} \Leftrightarrow A\mathbb{Z}^n = \Lambda = B\mathbb{Z}^n \Leftrightarrow B^{-1}A\mathbb{Z}^n = \mathbb{Z}^n \overset{\text{Proposition 2.3}}{\Leftrightarrow} B^{-1}A \in \mathrm{GL}(n, \mathbb{Z})$$ □

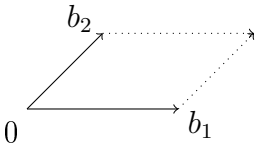


Abbildung 2: Beispiel für eine Fundamentalzelle. Die gepunkteten Linien gehören nicht zu P_B.

2.5 Definition. Sei $\Lambda \in \mathcal{L}^n$ mit Basis B.

- $\det \Lambda := |\det B|$ heißt *Determinante von* Λ (was wohldefiniert ist nach Lemma 2.4).
- $P_B := \{\lambda_1 b_1 + \ldots + \lambda_n b_n : \lambda_i \in [0,1)\} = B[0,1)^n$ heißt *Fundamentalzelle.*

Bemerkung.

- An Rechenregeln haben wir $\operatorname{vol} P_B = |\det \Lambda|$.
- Für $\lambda \geq 0$ gilt $\lambda\Lambda = \{\lambda b : b \in \Lambda\}$ und $\det(\lambda\Lambda) = \lambda^n \det \Lambda$.
- $\operatorname{vol}(P_B - P_B) = 2^n \operatorname{vol}(P_B)$, da wir nun als Bedingung $-1 < \lambda_i < 1$ haben, also je Dimension doppelt so groß.
- $(P_B - P_B) \cap \Lambda = \{0\}$

Bemerkung. Wenn wir $n+1$ Punkte nehmen, im $\mathbb{R}^n$, dann erhalten wir nicht unbedingt ein Gitter. Einfachstes Beispiel ist $\{1, \sqrt{2}\} \subseteq \mathbb{R}$. Wäre $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ ein Gitter, dann wäre $\sqrt{2}$ rational.

2.6 Proposition. *Sei $\Lambda = B\mathbb{Z}^n \in \mathcal{L}^n$. Dann gilt $\mathbb{R}^n = \dot{\bigcup}_{b \in \Lambda}(b + P_B)$.*

Beweis. Angenommen $b, \bar{b} \in \Lambda$ mit $(b + P_B) \cap (\bar{b} + P_B) \neq \emptyset$. Dann ist $b - \bar{b} \in (P_B - P_B) \cap \Lambda = \{0\}$, also $b = \bar{b}$.
Sei $x \in \mathbb{R}^n$ beliebig. Dies hat eine (reelle) Linearkombination $x = \sum \rho_i b_i$. Wähle $b = \sum \lfloor \rho_i \rfloor b_i$. Dann ist $x \in b + P_B$. □

2.7 Lemma. *Sei $S \subset \mathbb{R}^n$ eine diskrete Untergruppe. Seien $F, G \subset S$ mit G endlich,* $\operatorname{lin} F \cap S = \operatorname{lin}_{\mathbb{Z}} G$. *Sei $s \in S \setminus \operatorname{lin} F$. Dann existiert ein $b \in S$ so, dass* $\operatorname{lin}(F \cup s) = \operatorname{lin}_{\mathbb{Z}}(G \cup b)$.

Beweis. Sei $Z = \left\{\sum_{g \in G} \alpha_G \cdot g + \alpha_s \cdot s : 0 \leq \alpha_g, \alpha_s \leq 1\right\}$ (heißt Zonotop). Da S diskret und Z beschränkt, ist $S \cap Z$ endlich. Weil $s \notin \operatorname{lin} F$ gibt es ein $b \in Z$ mit minimalem Abstand zu $\operatorname{lin} F$. Das heißt $b = \sum_{g \in G} \overline{\alpha}_g g + \overline{\alpha}_s s$ mit $\overline{\alpha}_s$ minimal. Dann ist $\operatorname{lin}(F \cup s) = \operatorname{lin}(G \cup b)$ und $\operatorname{lin}_{\mathbb{Z}}(G \cup b) \subseteq \operatorname{lin}(F - \cup s)$.

$$v \in \operatorname{lin}(F \cup s) \cap S \implies v = \sum_{g \in G} \beta_g g + \beta_b b$$

Es ist zu zeigen, dass die Skalare β ganzzahlig gewählt werden können.

$$v - \sum_{g \in G} \lfloor \beta_g \rfloor g - \lfloor \beta_b \rfloor b = \sum_{g \in G} \left(\underbrace{\beta_g - \lfloor \beta_g \rfloor + \overline{\alpha}_s(\beta_b - \lfloor \beta_b \rfloor)}_{=:\mu_g} \right) g + \underbrace{\overline{\alpha}_s(\beta_b - \lfloor \beta_b \rfloor)}_{=:\Gamma_s} s$$

$$\implies v - \sum_{g \in G} \lfloor \beta_g \rfloor g - \lfloor \beta_b \rfloor b - \sum_{g \in G} \lfloor \Gamma_g \rfloor g = \sum_{g \in G} (\mu_g - \lfloor \mu_g \rfloor) g + \Gamma_s s \in \mathbb{Z}$$

$$\overset{\Gamma_s < \overline{\alpha}_s}{\implies} \Gamma_s = 0 \implies \beta_b \in \mathbb{Z} \implies v - \beta_b b = \sum_{g \in G} \beta_g g \operatorname{lin} F \cap S = \operatorname{lin}_{\mathbb{Z}} G$$ □

2.8 Korollar. *Sei $S \subset \mathbb{R}^n$ eine diskrete Untergruppe und seien $s_1, \dots, s_m \in S$ linear unabhängig. Dann existieren $b_1, \dots, b_m \in S$ so, dass $\operatorname{lin}\{s_1, \dots, s_i\} \cap S = \operatorname{lin}_{\mathbb{Z}}\{b_1, \dots, b_i\}$ füri $= 1, \dots, m$.*

Beweis. Wir beginnen mit $F = G = \{0\}$ und $s = s_1$. Nach Lemma 2.7 existiert ein $b_1 \in S$ mit $S \cap \operatorname{lin}\{s_1\} = \operatorname{lin}_{\mathbb{Z}}\{b_1\}$. Wir fahren fort mit

Stück fehlt

□

2.9 Satz. *$S \subset \mathbb{R}^n$ ist ein Gitter genau dann, wenn S eine diskrete Untergruppe ist, die n linear unabhängig Vektoren enthält.*

Beweis. **$\Leftarrow$:** Korollar 2.8 mit $m = n$ und $s_1, \dots, s_m$ die linear unabhängigen Vektoren aus S. Dies liefert $b_1, \dots, b_m$ so, dass

$$S = \operatorname{lin}\{s_1, \dots, s_n\} \cap S = \operatorname{lin}_{\mathbb{Z}}\{b_1, \dots, b_n\}$$

$\Rightarrow$: Sei $b_1, \dots, b_n$ eine Basis von S. Ganzzahlige Linearkombinationen sind bilden eine Untergruppe. Um die Diskretheit zu zeigen, reicht, dass wir die für 0 zeigen (da wir Untergruppe bereits haben). Es gilt

$$\min_{z \in \mathbb{Z}^n \setminus \{0\}} |Bz| \geq \min_{z \in \mathbb{Z}^n \setminus \{0\}} \frac{|Bz|}{|z|} = \|B\| > \varepsilon$$

für ein $\varepsilon > 0$, da B vollen Rang hat. □

2.10 Definition. Seien $b_1, \dots, b_k \in \Lambda \in \mathcal{L}^n$, b_i linear unabhängig. Dann heißt $\{b_1, \dots, b_k\}$ *primitive Menge* von Gittervektoren, falls

$$\operatorname{lin}\{b_1, \dots, b_k\} \cap \Lambda = \operatorname{lin}_{\mathbb{Z}}\{b_1, \dots, b_k\}$$

2.11 Lemma.

1. *Jede Teilmenge einer Basis eines Gitters ist primitiv.*
2. *Jede primitive Menge kann zu einer Basis eines Gitters ergänzt werden.*

Beweis.

1. Sei $b_1, \dots, b_n \in \Lambda$ eine Basis. Jeder Vektor $b \in \mathbb{R}^n$ hat eine eindeutige Darstellung, insbesondere jedes $b \in \Lambda$. Und dies sind genau die, mit ganzzahligen Koeffizienten.
2. Sei $F = \{b_1, \dots, b_k\} \subseteq \Lambda$ primitiv, $k < n = \dim \Lambda$. Dann existiert ein $s \in \Lambda \setminus \operatorname{lin} F$. Mit Lemma 2.7 gibt es ein b_{k+1}, welche die primitive Menge vergrößert. Iteration liefert dann eine Basis. □

2.12 Satz. *Seien $A = (a_1, \dots, a_n)$ linear unabhängige Vektoren eines Gitters $\Lambda \in \mathcal{L}^n$. Dann gibt es eine Basis $B = (b_1, \dots, b_n)$ so, dass für $H := B^{-1}A$ gilt:*

1. *H ist eine nichtnegative ganzzahlige obere Dreiecksmatrix*
2. *in jeder Spalte ist das Diagonalelement maximal: $0 \leq h_{ik} < h_{kk}$ für $q \leq i < k \leq n$.*

Dabei ist B (und somit H) eindeutig bestimmt durch A.

Beweis. Nach Korollar 2.8 gibt es eine Basis $b_1, \dots, b_n$ von Λ mit

$$a_k = \sum_{i=1}^{k} \overline{h_{i,k}} b_i \qquad \overline{h}_{i,k} \in \mathbb{Z}$$

Falls $\overline{h}_{1,1} < 0$, ersetze b_1 durch $-b_1$. Dann sind die Bedingungen erfüllt.
Wir nehmen nun also an, dass $\overline{h}_{i,k}$ die Bedingungen erfüllen für $i < k \leq l < n$. Für $\gamma_i \in \mathbb{Z}$ mit $\gamma_{l+1} \in \{-1, 1\}$ bilden wir die Vektoren

$$b_1, \ldots, b_l, \sum_{i=1}^{l+1} \gamma_i b_i, b_{l+2}, \ldots, b_n$$

eine Basis von Λ.
Für die Eindeutigkeit nehmen wir an B' ist eine andere Basis von Λ mit $B'^{-1}A = H'$ und H' hat ebenfalls die gesuchte Eigenschaft. Dan xistiert ein $U \in \mathrm{GL}(n, \mathbb{Z})$ mit $B' = BU$. Daraus folgt $H = UH'$, bzw $H^T = (H')^T U^T$. Damit erzeugen die Zeilen von H und H' das gleich Gitter, aber $H \neq H'$. Wähle einen Zeilenindex k und dann ein minimales l so, dass oBdA $H_{kl} > H'_{kl}$. Sei $g := H_{k*} - H'_{k*}$ die Differenz der beiden Zeilen. Dann ist $g_i = 0$ für $i < l$ und $g_l > 0$. Wir wissen, dass g im Gitter liegt, das von den Zeilen von H erzeugt wird. Dazu müssen aber die Koeffizienten von H_{i*} für $i < l$ auf 0 gesetzt werden, da die Einträge aus der Diagonalen sich nicht mehr wegheben können. Hintere Zeilen tragen aber nicht mehr zum l-ten Eintrag ein. Damit gilt $g_l \mid H_{ll}$. Dies widerspricht jedoch der Maximalität von H_{ll}. □

Beispiel.

$$A = \begin{pmatrix} 2 & 3 & 4 \\ 4 & 9 & 16 \\ 8 & 27 & 64 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 1 \\ 4 & 9 & 6 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 4 \\ 0 & 3 & 0 \\ 0 & 0 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 7 & 18 & 24 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 & 4 \\ 1 & 3 & 6 \\ -1 & -2 & -3 \end{pmatrix}$$

2.13 Definition. Sei $\Lambda \in \mathcal{L}^n$ und $a_1, \ldots, a_n \in \Lambda$ linear unabhängig. Dann ist $\Lambda_0 := \mathrm{lin}_{\mathbb{Z}}\{a_1, \ldots, a_n\}$ ein *Untergitter*. Die Anzahl der Nebenklassen $|\Lambda/\Lambda_0|$ heißt *Index*.

2.14 Lemma. *Sei* $\Lambda_0 \leq \Lambda \in \mathcal{L}^n$.

1. $|\Lambda/\Lambda_0| = |P_A \cap \Lambda|$ *wobei* A *eine Basis von* Λ_0.
2. $|\Lambda/\Lambda_0| = \frac{\det \Lambda_0}{\det \Lambda}$

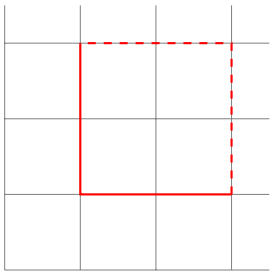


Abbildung 3: Fundamentalzelle: Der Index von $2\mathbb{Z}^2$ in $\mathbb{Z}^2$ ist 4.

2.15 Korollar. *Sei* $A = (a_1, \ldots, a_n) \in \mathbb{Z}^{n \times n}$ *mit* $\det A \neq 0$ *und sei* $P_A = A[0,1)^n$. *Dann ist* $|P_A \cap \mathbb{Z}^n| = |\det A| = \mathrm{vol}(P_A)$.

Beweis. Siehe Lemma 2.14 mit $\Lambda_0 = \langle A \rangle$ und $\Lambda = \mathbb{Z}^n$.

$$|P_A \cap \mathbb{Z}^n| = |\mathbb{Z}^n/\Lambda_0| = \frac{\det \Lambda_0}{\det \mathbb{Z}^n} = \det \Lambda_0 = |\det A|$$ □

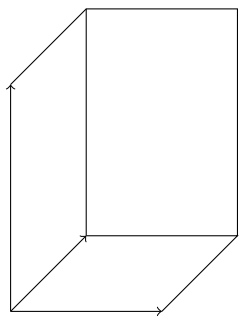


Abbildung 4: Beispiel für eine Zerlegung in Parallelepipede, in $\mathbb{Z}^2$

Beispiel. Betrachte das Gitter $Z = \langle (1,1),(2,0),(0,3)\rangle$, siehe Abbildung 4. Dann ist $|Z \cap \mathbb{Z}^2| = |\det(a_1,a_2)| + |\det(a_1,a_3)| + |\det(a_2,a_3)|$.

2.16 Korollar. *Seien $u_1,\dots,u_m \in \mathbb{Z}^n$ und seien $k_i \in \mathbb{N}$. Dann ist*

$$\Lambda := \{z \in \mathbb{Z}^n : \langle u_i, z\rangle \equiv 0 \mod k_i, i = 1,\dots,m\}$$

ein Untergitter von $\mathbb{Z}^n$ mit $\det \Lambda_0 \leq \prod k_i$.

Beweis. Da $\Lambda \leq \mathbb{Z}^n$ ist es diskret. Setze $K := \prod k_i$. Dann ist $K \cdot e_i \in \Lambda$, also haben wir n unabhängige Vektoren in Λ. Nach Satz 2.9 ist Λ ein n-dimensionales Gitter.
Betrachte die Restklassen von $\mathbb{Z}^n$ modulo Λ. Dann ist $[z_1] \neq [z_2] \Leftrightarrow z_1 - z_2 \notin \Lambda$. Das heißt es gibt ein $i \leq m$ mit $\langle u_i, z_1 - z_2\rangle \not\equiv 0 \mod k_i$. Also gehören $\langle u_i, z_1\rangle$ und $\langle u_i, z_2\rangle$ zu verschiedenen Restklassen modulo k_i. Für jedes u_i gibt es maximal k_i verschiedene Restklassen. Insgesamt ist also die Anzahl der Restklassen beschränkt durch $k_1 \cdot \ldots \cdot k_m$. □

Bemerkung. Sei $A = (a_1,\dots,a_n)$ mit $a_i \in \Lambda \in \mathcal{L}^n$ und a_i linear unabhängig. Dann gilt

$$A \text{ eine Basis von } \Lambda \Leftrightarrow |\Lambda / A\mathbb{Z}^n| = 1 \Leftrightarrow |P_A \cap \Lambda| = \{0\}$$

2.17 Proposition. *Sei $\Lambda \in \mathcal{L}^2$ und seien $a_1, a_2 \in \Lambda$ linear unabhängig. Dann ist a_1, a_2 eine Basis von Λ genau dann, wenn*

$$\operatorname{conv}(0, a_1, a_2) \cap \Lambda = \{0, a_1, a_2\}$$

Beweis. $\Rightarrow$ Wenn es eine Basis ist, enthält die Fundamentalzelle nur die 0. Für das Dreieck kommen noch a_1, a_2 hinzu.

$\Leftarrow$ Setze $T_A := \operatorname{conv}\{0, a_1, a_2\}$ Wir nutzen

$$P_A = T_A \setminus \{a_1, a_2\} \cup ((a_1 + a_2) - \operatorname{int} T_A)$$

Angenommen, es gäbe noch einen Punkt a in der Fundamentalzelle. Dann liegt $a_1 + a_2 - a$ im Inneren des Dreiecks, was der Annahme widerspricht. □

Leider gilt dies nicht mehr in Dimension 3.

Vorlesung fehlt

Sei $L \subseteq \mathbb{R}^n$ linear und $L^\perp = \{y \in \mathbb{R}^n : \langle x, y\rangle = 0\}$. Für $S \in \mathbb{R}^n$ ist $S \mid L^\perp$ die orthogonale Projektion. Wenn $A \in \mathbb{R}^{n\times k}$ eine Basis von L ist, dann ist

$$S|L = A(A^TA)^{-1}A^TS$$

2.18 Lemma. *Sei $\Lambda \in \mathcal{L}^n$ und $1 < k \leq n-1$.*

1. $L \in \mathcal{L}(k, \Lambda) \Leftrightarrow L^\perp \mathcal{L}(n-k, \Lambda^*)$
2. *Wenn $L \in \mathcal{L}(k, \Lambda)$, dann ist $\Lambda | L^\perp$ ein $(n-k)$-dimensionales Gitter und es ist $(\Lambda \mid L^\perp)^* = L^\perp \cap \Lambda^*$*
3. *Wenn $L \in \mathcal{L}(k, \Lambda)$ dann gilt*

$$\det \Lambda = \det(\Lambda \mid L^\perp) \cdot \det(L \cap \Lambda)$$
$$\det(L \cap \Lambda) = \det \Lambda \cdot \det(L^\perp \cap \Lambda^*)$$

Beweis. 1. ✓, siehe letztes Mal

2. Sei $b_1, \ldots, b_n$ eine Basis von Λ so, dass $b_1, \ldots, b_l$ eine Basis von $\Lambda \cap L$ ist. Die zugehörige polare Basis sei $b_1^*, \ldots, b_n^*$. Betrachten wir die Projektionen $\overline{b_i} b_i \mid L^\perp$ für $i = k+1, \ldots, n$. Sei $b = \sum_{i=1}^n \tau_i b_i \in \Lambda$. Dann gilt

$$b \mid L^\perp = \sum_{i=1}^n \tau_i (b_i \mid L^\perp) = \sum_{i=k+1}^n \tau_i \overline{b_i}$$

daraus folgt $\Lambda \mid L^\perp$ ist ein $(n-k)$-dimensionales Gitter mit Basis $\overline{b_{k+1}}, \ldots, \overline{b_n}$. Betrachten wir nun $b_j^* \in L^\perp$ für $j > k$, so erhalten wir

$$\langle b_{k+i}^*, \overline{b_{k+j}} \rangle = \langle b_{k+i}^*, b_{k+j} \rangle = \delta_{ij}$$

und dies ergibt die Aussage.

3. Sei $B_k = (b_1, \ldots, b_k)$ und $\overline{B}_{n-k} = (\overline{b}_{k+1}, \ldots, \overline{b}_n)$. Dann erhalten wir

$$\begin{aligned}
\det \Lambda &= |\det(b_1, \ldots, b_n)| = |\det(B_k, \overline{B}_{n-k})| = \sqrt{\det(B_k, \overline{B}_{n-k})(B_k, \overline{B}_{n-k})^T} \\
&= \left(\det \begin{pmatrix} B_k^T B_k & 0 \\ 0 & \overline{B}_{n-k}^T \overline{B}_{n-k} \end{pmatrix} \right)^{\frac{1}{2}} = \sqrt{\det(B_k^T B_k)} \cdot \sqrt{\det(\overline{B}_{n-k}^T \overline{B}_{n-k})} \\
&= \det(L \cap \Lambda) \cdot \det(L^\perp \cap \Lambda^*)
\end{aligned}$$

□

Beispiel. Wir definieren das Gitter

$$A_n = \{z \in \mathbb{Z}^{n+1} : z_1, \ldots, z_{n+1} = 0\}$$

Bekanntermaßen ist $\det(\mathbb{Z}^{n+1}) = 1$. Der Normalenvektor von A_n ist $\mathbf{1}$. Damit ist $\det A_n = \sqrt{n+1}$.

Sei $f : \mathbb{R} \to \mathbb{C}$ eine Funktion mit Periode T. Nach Fourier können wir die schreiben als

$$f(y) = \sum_{k=-\infty}^{\infty} \widehat{f}(k) e^{\frac{2\pi i}{T} ky}$$
$$\widehat{f}(k) = \frac{1}{T} \int_0^T f(x) x^{-\frac{2\pi i}{T} ikx} \mathrm{d}x$$

Für nicht-periodische Funktionen nehmen wir $T = \infty$ und erhalten für eine beliebige Funktion anstatt der Fourier-Reihe die Fourier-Transformierte

$$\widehat{f}(y) = \int_{\mathbb{R}} f(x) e^{-2\pi i x y} \mathrm{d}x$$

Beispiel. Nehmen wir $f(x) = e^{-\pi\left(\frac{x}{t}\right)^2}$. Dann ist $\widehat{f}(y) = te^{-\pi(yt)^2}$. Für $t = 1$ ist dann $f = \widehat{f}$.

2.19 Satz. *Seien $f, \widehat{f} : \mathbb{R} \to \mathbb{C}$ gutartig. Dann gilt*

$$f(x) = \int_{\mathbb{R}} \widehat{f}(y) e^{2\pi i x y} \mathrm{d}y$$

2.20 Satz (Poisson-Summenformel Teil 1). *Seien $f, \widehat{f} : \mathbb{R} \to \mathbb{C}$ gutartig. Dann gilt*

$$\sum_{l=-\infty}^{\infty} f(l) = \sum_{l=-\infty}^{\infty} \widehat{f}(l)$$

Beweis. Wir definieren die periodische Funktion

$$g(x) = \sum_{l=-\infty}^{\infty} f(x+l)$$

Damit hat $g : \mathbb{R} \to \mathbb{C}$ die Periode 1. Für die Fourier-Transformierte gilt

$$\begin{aligned}\widehat{g}(k) &= \int_0^1 g(y) e^{2\pi i k y} \mathrm{d}y = \int_0^1 \sum_{l=-\infty}^{\infty} f(y+l) e^{2\pi i k y} \mathrm{d}y \\ &\overset{\text{gutartig}}{=} \sum_{l=-\infty}^{\infty} \int_0^1 f(y+l) e^{2\pi i k (y+l)} \mathrm{d}y = \int_{\mathbb{R}} f(x) e^{2\pi i k x} \mathrm{d}x = \widehat{f}(k)\end{aligned}$$

Damit haben wir

$$\sum_{l=-\infty}^{\infty} = g(0) = \sum_{l=-\infty}^{\infty} \widehat{g}(l) = \sum_{l=-\infty}^{\infty} \widehat{f}(l)$$

□

Definition. Jetzt heben wir das ganze in höhere Dimension. Sei $f : \mathbb{R}^n \to \mathbb{C}$ gutartig. Dann ist die Fourier-Transformierte gegeben durch

$$\widehat{f}(y) = \int_{\mathbb{R}^n} f(x) e^{2\pi i \langle x, y \rangle} \mathrm{d}x$$

2.21 Bemerkung.

1. Können wir $f : \mathbb{R}^n \to \mathbb{C}$ zerlegen als $f(x) = \prod g(x_i)$ für ein $g : \mathbb{R} \to \mathbb{C}$, dann gilt

$$\widehat{f}(y) = \prod \widehat{g}(y_i)$$

2. Für $f(x) = e^{-\pi\left|\frac{x}{t}\right|^2}$ gilt $\widehat{f}(y) = t^n e^{-\pi |ty|^2}$.

2.22 Satz. *Seien $f, \widehat{f}$ gutartig. Dann ist*

$$f(x) = \int_{\mathbb{R}^n} \widehat{f}(y) e^{2\pi i \langle x, y \rangle} \mathrm{d}y$$

Für Fourier-Reihen verlangen wir nun Periode $f(x+b) = f(x)$ für alle $b \in \Lambda$. Für $\Lambda = \mathbb{Z}^n$ ergibt sich

$$f(x) = \sum_{y \in \mathbb{Z}^n} \widehat{f}(y) e^{2\pi i \langle x, y \rangle}$$

$$\widehat{f}(y) = \int_{[0,1)^n} f(x) e^{-2\pi i \langle x, y \rangle} \mathrm{d}x$$

Wenn $\Lambda = B\mathbb{Z}^n$, und f eine Λ-periodische Funktion ist, so ist die transformation $g(x) = f(Bx)$ nun $\mathbb{Z}$-periodisch.

2.1 Algebraische Zahlkörper und Gitter

Sei L eine endliche Körpererweiterung von $\mathbb{Q}$ vom Grad n und es gibt ein $\alpha \in L$ mit

$$L = \mathbb{Q}(\alpha) = \left\{ \sum_{i=0}^{n-1} q_i \alpha^i : q_i \in \mathbb{Q} \right\}$$

Seien $\alpha = \alpha^{(1)}, \ldots, \alpha^{(n)}$ die Nullstellen des Minimalpolynoms. Für $\beta = \sum q_i \alpha^i \in L$ sind $\beta^{(j)} := \sum q_i \left(\alpha^{(j)}\right)^i$ die *Körperkonjugierten.*
Ist $\deg \beta = k \mid n$, dann enthalten die Körperkonjugierten $\frac{n}{k}$ Kopien der algebraisch Konjugierten.
Sei $\beta \in L$. Dann setze

$$\operatorname{norm}(\beta) = \prod_{i=1}^{n} \beta^{(i)} \qquad \operatorname{trace}(\beta) = \sum_{i=1}^{n} \beta^{(i)}$$

Falls $f_\beta = \sum p_i x^i \in \mathbb{Z}[x]$, so gilt

$$\operatorname{norm}(\beta) = \left((-1)^k \cdot \frac{p_0}{p_k} \right)^{\frac{n}{k}} \operatorname{norm}(\beta) \qquad = \left(-\frac{p_0}{p_k} \right)^{\frac{n}{k}}$$

Beispiel. Sei $d \in \mathbb{Z}$ quadratfrei. Dann ist $L := \mathbb{Q}(\sqrt{d}) = \{q_0 + q_1\sqrt{d} : q_i \in \mathbb{Q}\}$. Das Minimalpolynom ist $f(x) = x^2 - d$ mit den Nullstellen $\pm\sqrt{d}$.

Eine Zahl $\gamma \in L$ heißt *ganze algebraische Zahl*, falls sie Nullstelle eines normierten ganzzahligen Polynoms ist. Die zugehörige Menge wird mit $\mathbb{Z}_L$ bezeichnet.

Beispiel. Es gilt

$$\mathbb{Z}_{\mathbb{Q}(\sqrt{d})} = \left\{ z_1 + z_2\sqrt{d} : z_i \in \mathbb{Z} \right\} \qquad \text{falls } d \equiv 2, 3 \mod 4$$

Für $d \equiv 1 \mod 4$, gilt hingegen

$$\mathbb{Z}_{\mathbb{Q}(\sqrt{d})} = \left\{ z_1 + z_2 \left(\frac{1+\sqrt{d}}{2} \right) : z_i \in \mathbb{Z} \right\}$$

2.23 Bemerkung. $\mathbb{Z}_L$ ist ein Ring.

2.24 Bemerkung. $\mathbb{Z}_L$ enthält n rational unabhängige algebraische Zahlen.

Beweis. Sei $\beta \in L$ mit $\deg \beta = n$ und $g(x) = \sum_{i=0}^{n} g_i x^i$ mit $g_i \in \mathbb{Z}$ und $g(\beta) = 0$.

$$0 = g_n^{n-1} g(\beta) = \sum_{i=0}^{n} g_i g_n^{n-1} \beta^i = \sum_{i=0}^{n} g_i g_n^{n-i-1} (g_n \beta)^i$$

Damit ist $g_n \beta \in \mathbb{Z}_L$. □

Das zeigt ferner, es existiert ein $c \in \mathbb{N}$ (welches nur von α abhängt) so, dass

$$1 = (c\alpha)^0, (c\alpha)^1, \ldots, (c\alpha)^{n-1} \in \mathbb{Z}_L$$

eine Basis ist. Das heißt

$$\forall \gamma \in \mathbb{Z}_L . \exists q_i \in \mathbb{Q} . \gamma = \sum_{i=0}^{n-1} q_i (c\alpha)^i$$

Damit haben wir

$$\begin{aligned} \gamma (c\alpha)^k &= \sum_{i=0}^{n-1} q_i (c\alpha)^k (c\alpha)^i \\ \implies \operatorname{trace}(\gamma (c\alpha)^k) &= \sum_{i=0}^{n-1} q_i \operatorname{trace}((c\alpha)^k (c\alpha)^i) \qquad k = 1, \dots, n \end{aligned}$$

2.25 Bemerkung. Sei $\gamma \in \mathbb{Z}_L$. Dann können wir die schreiben als

$$\gamma = \frac{1}{k(\alpha)} \cdot \sum_{i=0}^{n-1} z_i \alpha^i$$

für $z_i \in \mathbb{Z}$ und $k(\alpha) \in \mathbb{Z}$.

Betrachte die Abbildung

$$\Phi : \mathbb{Z}_L \to \mathbb{R}^n \qquad \gamma = \sum_{i=0}^{n-1} q_i \alpha^i \mapsto (q_0, \dots, q_{n-1})$$

Mit den vorigen Bemerkungen folgt

- $\Phi(\mathbb{Z}_L)$ ist ein n-dimensionales Untergitter von $\frac{1}{k(\alpha)} \mathbb{Z}^n$.
- $\Phi(\mathbb{Z}_L) = \operatorname{lin}_{\mathbb{Z}}(b_1, \dots, b_n)$
- Sei $w_i = \Phi^{-1}(b_i)$, dann ist $\mathbb{Z}_L = \{\sum z_i w_i : z_i \in \mathbb{Z}\}$.

Definition. Der Ausdruck $\Delta_L = \det((w_1, \dots, w_n)^2)$ heißt Diskriminante von $L/\mathbb{Q}$. Diese ist unabhängig von der gewählten Basis, $\Delta_L \neq 0$.

Beispiel. Sei $d \equiv 2, 3 \mod$ und $L = \mathbb{Z}(\sqrt{d})$. Dann ist

$$\Delta_L = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = (-2\sqrt{d})^2 = 4d$$

Ist hingegen $d \equiv 1 \mod 4$, so gilt $\Delta_L = d$.

Sei $\alpha^{(1)}, \dots, \alpha^{(k)} \in \mathbb{R}$ die reellen Nullstellen, und $\alpha^{(k+l)}, \alpha^{(k+l+s)}$ die komplexen Nullstellen mit $\overline{\alpha^{(k+l)}} = \alpha^{(k+l+s)}$. Dabei ist $n = k + 2s$.

2.26 Proposition. *Die Menge von Punkten*

$$\Lambda = \left\{ \gamma^{(1)}, \dots, \gamma^{(k)}, \operatorname{Re} \gamma^{(k+1)}, \operatorname{Im} \gamma^{(k+1)}, \dots : \gamma \in \mathbb{Z}_L \right\} \subseteq \mathbb{R}^n$$

ein Gitter mit Determinante $\det \Lambda = 2^{-s} \sqrt{|\Delta_L|}$.

Beweis. Sei $\omega_1, \dots, \omega_n$ eine $\mathbb{Z}$-Basis von $\mathbb{Z}_L$.

$$\omega_j^{(k+q)} = \underbrace{\delta_j^{(q)}}_{\text{Re}} + i \underbrace{\theta_s^{(q)}}_{\text{Im}} \qquad q = 1, \dots, s; j = 1, \dots, n$$

Nehmen wir eine Zahl

$$\gamma = \sum_{j=1}^{n} z_j \omega_j \qquad \gamma^{(l)} = \sum_{j=1}^{n} z_j \omega_j^{(l)}$$

Die n Vektoren

$$(\omega_j^{(1)}, \dots, \omega_j^{(k)}, \delta_j^{(1)}, \theta_j^{(1)}, \dots, \delta_j^{(s)}, \theta_j^{(s)})$$

für $j = 1, \dots, n$ bilden eine Basis von Λ. Für jedes komplex konjugierte Paar erhalten wir damit einen Faktor $\frac{1}{2}$. Damit ist

$$\det \Lambda = \left(\frac{1}{2}\right)^s \sqrt{|\Delta_L|}$$ □

3 Minkowskis sukzessives Minima

3.1 Lemma. *Sei $X \subset \mathbb{R}^n$ beschränkt, Jordan-messbar. Sei $\Lambda \in \mathcal{L}^n$.*

1. *Angenommen $(b_1 + X) \cap (b_2 + x) = \emptyset$ für alle $b_i \in \Lambda$, $b_1 \neq b_2$. Dann ist* $\operatorname{vol}(X) \leq \det \Lambda$.
2. *Wenn $\Lambda + X = \mathbb{R}^n$, so ist* $\operatorname{vol}(X) \det \Lambda$.

Beweis. Sei P die Fundamentalzelle. Dann gilt $\Lambda + P = \mathbb{R}^n$. Weiter ist

$$\operatorname{vol}(X) = \operatorname{vol}((\Lambda + P) \cap X) = \sum_{b \in \Lambda} \operatorname{vol}((b + P) \cap X) = \sum_{b \in \Lambda} (P \cap (X - b))$$

Damit arbeiten wir nun weiter:

1. $$\sum_{b \in \Lambda} (P \cap (X - b)) = \operatorname{vol}\left(\bigcup_{b \in \Lambda} (P \cap (X - b))\right) \leq \operatorname{vol}(P) = \det \Lambda$$

2. $$\sum_{b \in \Lambda} (P \cap (X - b)) \geq \operatorname{vol}\left(\bigcup_{b \in \Lambda} (P \cap (X - b))\right) \leq \operatorname{vol}(P) = \det \Lambda$$ □

3.2 Korollar. *Sei $X \subset \mathbb{R}^n$ mit* $\operatorname{vol}(X) > \det \Lambda$ *für $\Lambda \in \mathcal{L}^n$. Dann ist $(X - X) \cap (\Lambda \setminus \{0\}) \neq \emptyset$.*

Beweis. Nach Lemma 3.1 existieren $b_1, b_2 \in \Lambda$ mit $b_1 \neq b_2$ und $x \in (X + b_1) \cap (X + b_2)$. Damit ist $x - b_1, x - b_2 \in X$, also $b_1 - b_2 \in (X - X) \cap (\Lambda \setminus \{0\})$. □

Äquivalent dazu können wir auch schreiben

$$\exists t \in \mathbb{R}^n . |(t + X) \cap \Lambda| \geq 2$$

3.3 Theorem (Minkowski). *Sei $K \in \mathcal{K}_0^n$ (also $K = -K$), und $\Lambda \in \mathcal{L}^n$. Ist* $\operatorname{vol}(K) \geq 2^n \det(L)$, *so ist $K \cap (\Lambda \setminus \{0\})$.*

Beweis. Wir können K schreiben als $K = \frac{1}{2}K - \frac{1}{2}K$.

(a) Ist $\operatorname{vol}(K) > 2^n \det L$, haben wir $\operatorname{vol}\left(\frac{1}{2}K\right) = \det L$. Nach Korollar 3.2 haben wir ein $b \in \Lambda \setminus \{0\}$ mit $b \in \frac{1}{2}K - \frac{1}{2}K = K$.

(b) Angenommen $\operatorname{vol}(K) = 2^n \det L$. Da K kompakt und Λ abgeschlossen existiert ein $\lambda > 1$ mit $\lambda K \cap L = K \cap L$ (wähle $\lambda = \operatorname{dist}(\Lambda \setminus K, K)$). Dann haben wir aber $\operatorname{vol}(\lambda K) > 2^n \det L$ und wir haben wieder obigen Fall. □

Bemerkung. Es hätte auch gereicht, diese Aussage für das Standardgitter $\mathbb{Z}^n$ zu zeigen, da wir alle anderen Gitter daraus durch lineare Transformation erhalten.

Bemerkung. Die Schranke in Theorem 3.3 ist scharf, wie man am Beispiel Würfel sieht. Aber es gibt noch andere Beispiele. Im zweidimensionalen gibt es ein Rechteck, im dreidimensionalen 5 und die Anzahlen steigen immer weiter. Alle ergeben Parkettierungen des Raums.

3.4 Theorem. *Sei $K \in \mathcal{K}_0^n$ und $\Lambda \in \mathcal{L}^n$ mit $\overline{int}(K) \cap \Lambda = \{0\}$. Dann ist*

$$2^n \det L = \operatorname{vol}(K) + \frac{4^n}{\operatorname{vol}(K)} \cdot \sum_{a \in \Lambda^* \setminus \{0\}} \left| \widehat{1}_{\frac{1}{2}K}(a) \right|^2$$

Beweis. Es gilt

$$\operatorname{int}(K) \cap \Lambda = \{0\} \Leftrightarrow \forall b \in \Lambda \setminus \{0\}. \operatorname{int}\left(\frac{1}{2}K\right) \cap \left(\operatorname{int}\left(\frac{1}{2}K\right) + b\right) = \emptyset$$

Definiere Funktion f als Faltung $f(x) := \left(1_{\frac{1}{2}K} * 1_{-\frac{1}{2}K}\right)(x)$. Für Faltungen gilt

$$(f * g)(y) = \int_{\mathbb{R}^n} f(x) g(y - x) \mathrm{d}x \qquad \widehat{f * g} = \widehat{f} \cdot \widehat{g}$$

Nach **??** gilt somit

$$\sum_{b \in \Lambda} f(b) = \det \Lambda^* \sum_{a \in \Lambda^*} \widehat{f}(a)$$

Die linke Seite formen wir um

$$\begin{aligned}
\sum_{b \in \Lambda} f(b) &= \sum_{b \in \Lambda} \int_{\mathbb{R}^n} 1_{\frac{1}{2}K}(x) \cdot 1_{-\frac{1}{2}K}(b - x) \mathrm{d}x = \int_{\mathbb{R}^n} 1_{\frac{1}{2}K}(x) \cdot 1_{-\frac{1}{2}K}(-x) \mathrm{d}x = \int_{\mathbb{R}^n} 1_{\frac{1}{2}K}(x)^2 \mathrm{d}x \\
&= \int_{\mathbb{R}^n} 1_{\frac{1}{2}K}(x) \mathrm{d}x = \operatorname{vol}\left(\frac{1}{2}K\right) = \frac{1}{2^n} \operatorname{vol}(K)
\end{aligned}$$

denn für $b \neq 0$ integrieren wir nur über über einen $n-1$-dimensionalen Unterraum, also Maß 0. Für die rechte Seite haben wir

$$\begin{aligned}
\sum_{a \in \Lambda^*} \widehat{f}(a) &= \sum_{a \in \Lambda^*} \widehat{1}_{\frac{1}{2}K}(a) \cdot \widehat{1}_{-\frac{1}{2}K}(a) = \sum_{a \in \Lambda^*} \left(\int_{\mathbb{R}^n} 1_{\frac{1}{2}K} e^{-2\pi i \langle x, a \rangle} \mathrm{d}x \right) \left(\int_{\mathbb{R}^n} 1_{-\frac{1}{2}K} e^{-2\pi i \langle x, a \rangle} \mathrm{d}x \right) \\
&= \sum_{a \in \Lambda^*} \left(\int_{\mathbb{R}^n} 1_{\frac{1}{2}K} e^{-2\pi i \langle x, a \rangle} \mathrm{d}x \right) \left(\int_{\mathbb{R}^n} 1_{\frac{1}{2}K} e^{2\pi i \langle x, a \rangle} \mathrm{d}x \right) \\
&= \sum_{a \in \Lambda^*} \widehat{1}_{\frac{1}{2}K}(a) \overline{\widehat{1}_{\frac{1}{2}K}(a)} = \sum_{a \in \Lambda^*} \left| \widehat{1}_{\frac{1}{2}K}(a) \right|^2
\end{aligned}$$

Für den Fall $a = 0$ haben wir

$$\left|\widehat{1}_{\frac{1}{2}K}(0)\right|^2 = \left(\int_{\mathbb{R}^n} 1_{\frac{1}{2}K}(x)\mathrm{d}x\right)^2 = \left(\frac{\mathrm{vol}(K)}{2^n}\right)^2$$

Damit ist die rechte Seite

$$\left(\frac{\mathrm{vol}(K)}{2^n}\right)^2 + \sum_{a\in\Lambda^*}\left|\widehat{1}_{\frac{1}{2}K}(a)\right|^2$$

□

3.5 Korollar. *1. Sei $A \in \mathrm{GL}(n,\mathbb{R})$ und $q(x) = x^T A^T A x$. Dann existiert ein $0 \neq z \in \mathbb{Z}^n$ mit*

$$q(z) \leq 4\left(\frac{(\det A)^2}{\mathrm{vol}(B^n)^2}\right)^{\frac{1}{n}} \leq C \cdot n|\det A|^{\frac{2}{n}}$$

2. Sei $\Lambda \in \mathcal{L}^n$. Dann existiert ein $0 \neq a \in \Lambda$ mit $\|a\| \leq C \cdot \sqrt{n} \cdot (\det \Lambda)^{\frac{1}{n}}$.

Beweis. 1. Für gegebenes τ betrachte die Menge

$$E(\tau) = \left\{x \in \mathbb{R}^n : x^T A^T A x \leq \tau\right\} = \{x \in \mathbb{R}^n : \|Ax\| \leq \sqrt{\tau}\} = \sqrt{\tau}A^{-1}B^n$$

und dies beschreibt einen Ellipsoid (affines Bild einer Kugel) mit

$$\mathrm{vol}(E(\tau)) = \left(\sqrt{\tau}\right)^n |\det A^{-1}| \,\mathrm{vol}(B^n)$$

Damit haben wir

$$\mathrm{vol}(E(\tau)) \geq 2^n \Leftrightarrow \tau \geq \left(\frac{2^n|\det A|}{\mathrm{vol}(B^n)}\right)^{\frac{2}{n}}$$

2. Sei $\Lambda = A\mathbb{Z}^n$. Dann ist $0 \neq a \in \Lambda$ genau dann, wenn $a = Az$ mit $0 \neq z \in \mathbb{Z}^n$. Damit ist $\|a\|^2 = z^T A^T A z$. Mit dem ersten Teil folgt die Behauptung. □

3.6 Korollar. *Sei $l_1(x), \ldots, l_n(x)$ n homogene Linearformen, das heißt*

$$\forall a_i \in \mathbb{R}^n . l_i(x) = \langle a_i, x\rangle$$

Sei A die Matrix mit Zeilen a_i^T und sei $A \in \mathrm{GL}(n,\mathbb{R})$. Seien $\tau_1, \ldots, \tau_n \in \mathbb{R}_{>0}$ mit $\prod \tau_i \geq \det A$. Dann existiert ein $0 \neq z \in \mathbb{Z}^n$ mit $|l_i(z)| \leq \tau$.
Das heißt unter diesen Bedingungen hat das System von Ungleichungen eine nicht-triviale ganzzahlige Lösung.

Beweis. Nutze Minkowski. Sei

$$\begin{aligned} P &= \{x \in \mathbb{R}^n : \forall i. |l_i|(x) \leq \tau_i\} = \{x \in \mathbb{R}^n : \forall i. |\langle a_i, x\rangle| \leq \tau_i\} = \{x \in \mathbb{R}^n : |Ax| \leq \tau\} \\ &= A^{-1}\{x \in \mathbb{R}^n : |x_i| \leq \tau_i\} \end{aligned}$$

Nun gilt $\mathrm{vol}(P) = 2^n \prod \tau_i \cdot (\det A)^{-1} \geq 2^n$. Damit haben wir ein $0 \neq z \in \mathbb{Z}^n$ mit $z \in P$ als Lösung. □

Nun betrachten wir die Modifikation $\prod |l_i(z)| \leq$ klein für ein $0 \neq z \in \mathbb{Z}^n$. Mit der AM-GM-Ungleichung erhalten wir als Bedingung

$$\prod |l_i(x)| \leq \left(\frac{1}{n}\sum |l_i(x)|\right)^n \overset{\exists 0\neq z\in\mathbb{Z}^n}{\leq} \left(\frac{1}{n}\sum |\det A|^{\frac{1}{n}}\right)^n = \det A$$

Dies führt zur

Behauptung (Minkowski-Vermutung). *Seien $t_1, \dots, t_n \in \mathbb{R}$. Dann existiert ein $z \in \mathbb{Z}^n$ mit*

$$\prod_{i=1}^{n} |l_i(x) - t_i| \leq \frac{\det A}{2^n}$$

Bisher ist es bewiesen für $n \leq 9$.

3.7 Korollar. *Seien $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ und sei $0 < \varepsilon < 1$. Dann existieren $p_1, \dots, p_n, 1 \in \mathbb{Z}$ mit $1 \leq 1 \leq \varepsilon^{-n}$ mit*

$$\left| \alpha_i - \frac{p_i}{q} \right| \leq \frac{\varepsilon}{q} < \frac{1}{q^{1+\frac{1}{n}}}$$

Beweis. Sei $l_i(x) = \alpha_i x_{n+1} - x_i$ für $1 \leq i \leq n$ und $l_{n+1}(x) = x_{n+1}$. Die zugehörige Matrix A hat $\det A = 1$. Nach Korollar 3.6 existiert für alle $\tau > 0$ ein Vektor $0 \neq z = (p_1, \dots, p_n, q) \in \mathbb{Z}^{n+1}$ mit

$$|l_i(z)| = |\alpha_i q - p_i| \leq \tau^{-\frac{1}{n}} \qquad\qquad |l_{n+1})z)| = |q| \leq \tau$$

Wähle $\tau > \varepsilon^{-n}$ und $\lfloor \tau \rfloor \leq \varepsilon^{-n}$. Daraus folgt $|\alpha_i q - p_i| < \varepsilon$ und $|q| \leq \lfloor \tau \rfloor \leq \varepsilon^{-n}$. Wäre $q = 0$, so folgt $|p_i| < \varepsilon$, also $p_i = 0$ für alle i, was ausgeschlossen ist. □

3.8 Proposition. *Sei $t > 0$ und $k, s \in \mathbb{N}$ mit $k + 2s = n$. Sei*

$$C_{k,s}^n(t) := \left\{ x \in \mathbb{R}^n : \sum_{i=1}^{k} |x_i| + 2 \sum_{i=1}^{s} \sqrt{x_{k+2i-1}^2 + x_{k+2i}^2} \leq t \right\}$$

Dann ist

$$\operatorname{vol}\left(C_{k,s}^n(t)\right) = t^n \frac{2^k}{n!} \left(\frac{\pi}{2}\right)^s$$

Beweis. Induktion über s:

IA $s = 0$ liefert das Volumen vom Standard-Simplex

$$\operatorname{vol}\left(C_{n,0}^n(t)\right) = \operatorname{vol}\left\{ x : \sum |x_i| \leq t \right\} = t^n \frac{2^n}{n!}$$

IS Definiere $D_t = \{(x_{n-1}, x_n) \in \mathbb{R}^2 : 2\sqrt{x_{n-1}^2 + x_n^2} \leq t\}$. Mit Fubini, Induktion und Polarkoordinaten erhalten wir

$$\begin{aligned}
\operatorname{vol}\left(C_{k,s}^n\right) &= \int_{D_t} \operatorname{vol}_{n-2}\left(C_{k,s-1}^{n-2}\left(t - 2\sqrt{x_{n-1}^2 + x_n^2} \right) \right) \mathrm{d}x_{n-1}x_n \\
&= \frac{2^k}{(n-2)!} \left(\frac{\pi}{2}\right)^{s-1} \int_{D_t} \left(t - 2\sqrt{x_{n-1}^2 + x_n^2} \right)^{n-2} \mathrm{d}x_{n-1}x_n \\
&= \frac{2^k}{(n-2)!} \left(\frac{\pi}{2}\right)^{s-1} \int_0^{\frac{t}{2}} \int_0^{2\pi} (t - 2r)^{n-2} r \mathrm{d}\varphi \mathrm{d}r \\
&= \frac{2^k}{(n-2)!} \left(\frac{\pi}{2}\right)^{s-1} 2\pi \int_0^{\frac{t}{2}} (t - 2r)^{n-2} r \mathrm{d}r \\
&= \frac{2^k}{(n-2)!} \left(\frac{\pi}{2}\right)^{s} \int_0^{t} (t - x)^{n-2} x \mathrm{d}x \\
&= \frac{2^k}{(n-2)!} \left(\frac{\pi}{2}\right)^{s} \left[-\frac{(t-x)^{n-1}(nx + t - x)}{(n-1)n} \right]_0^t = \frac{2^k}{n!} \left(\frac{\pi}{2}\right)^{s} t^n
\end{aligned}$$

□

3.9 Satz (Minkowski). *Sei L ein Zahlkörper vom Grad n. Dann gilt*

$$|\Delta_L| \geq \left(\left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}\right)^2 \geq 1$$

Beweis. Sei $L = \mathbb{Q}(\alpha)$ und seien $\alpha^{(1)}, \ldots, \alpha^{(n)} \in L$ die Konjugierten mit $\alpha^{(i)} \in \mathbb{R}$ für $i \leq k$. Weiter sei $\alpha^{(k+i)} = \overline{\alpha^{(k+i+s)}}$ für $1 \leq i \leq s$ und damit $k+2s = n$. Nach Proposition 2.26 sei $\omega_1, \ldots, \omega_n \in \mathbb{Z}_L$ eine $\mathbb{Z}$-Basis von $\mathbb{Z}_L$. Zerlege in Real- und Imaginärteil $\omega_j^{k+l} = \delta_j^{(l)} + i\Theta^{(l)}$. Weiter sei

$$w_j = (\omega_j^{(1)}, \ldots, \omega_j^{(k)}, \delta_j^{(1)}, \Theta_j^{(1)}, \ldots, \delta_j^{(s)}, \Theta_j^{(s)})^T$$

die entsprechende Basis des Gitters Λ_L mit $\det \Lambda_L = 2^{-s}\sqrt{|\Delta_L|}$. Wähle

$$\bar{t} = \left(\left(\frac{4}{\pi}\right)^s n!\sqrt{|\Delta_L|}\right)^{\frac{1}{n}}$$

Damit erhalten wir

$$\operatorname{vol}\left(C_{k,s}^n(\bar{t})\right) = \frac{2^k}{n!}\left(\frac{\pi}{2}\right)^s \left(\left(\frac{4}{\pi}\right)^s n!\sqrt{|\Delta_L|}\right) = 2^n 2^{-s}\sqrt{|\Delta_L|} = 2^n \det \Delta_L$$

Nach Theorem 3.3 existiert ein $0 \neq u \in \mathbb{Z}^n$ so, dass $v = \sum u_i w_i \in C_{k,s}^n(\bar{t})$. Sei $\gamma^{(j)} = \sum u_i w_i^{(j)}$ für$1 \leq j \leq n$. Damit gilt

$$\gamma^{(j)} = \begin{cases} v_j & : j = 1, \ldots, k \\ v_k + 2(j-k) - 1 + i \cdot v_k + 2(j-k) & : j = k+1, \ldots, k+s \\ \gamma^{(j-s)} = v_k + 2(j-k-s) - 1 + i \cdot v_k + 2(j-k-s) & : j = k+s+1, \ldots, n \end{cases}$$

Demnach haben wir

$$v \in C_{k,s}^n(\bar{t}) \implies \sum_{j=1}^n |\gamma^{(j)}| \leq \bar{t}$$

Für die Norm gilt nun

$$1 \leq |\operatorname{norm}(\gamma)| = \prod_{j=1}^n |\gamma^{(j)}| \leq \left(\frac{1}{n}\sum_{j=1}^n |\gamma^{(j)}|\right)^n \leq \left(\frac{\bar{t}}{n}\right)^n = \frac{1}{n^n}\left(\frac{4^s}{\pi^s} n!\sqrt{|\Delta_L|}\right)^n \qquad \square$$

3.10 Korollar. *Sei $p \in \mathbb{P}$ mit $p \equiv 1 \mod 4$. Dann existieren $m_1, m-2 \in \mathbb{Z}$ mit $p = m_1^2 + m_2^2$.*

Beweis. Wir wissen (aus Elementare Zahlentheorie), dass ein $u \in \mathbb{Z}$ existiert mit $u^2 \equiv -1 \mod p$. Sei nun $\Lambda \subset \mathbb{R}^2$ das Gitter mit Basis

$$B = \begin{pmatrix} 1 & 0 \\ u & p \end{pmatrix} \qquad \det \Lambda = p$$

Betrachte den konvexen Körper

$$K = \sqrt{\frac{3}{2}} B_2 = \left\{(x_1, x_2) : x_1^2 + x_2^2 \leq \frac{3}{2}p\right\}$$

Für diesen gilt $\mathrm{vol}(K) = \frac{3}{2}p\pi \geq 4p = 2^2 \det \Lambda$. Nach Theorem 3.3 existiert also ein $0 \neq z \in \mathbb{Z}^2$ mit $m := Bz \in K \cap \Lambda \setminus \{0\}$. Wir erhalten die Schranken

$$0 < m_1^2 + m_2^2 = z_1^2 + (t_1 u + z_2 p)^2 \leq \frac{3}{2}p$$

Rechnen wir modulo p ergibt sich

$$z_1^2 + (z_1 u + z_2 p)^2 \equiv z_1^2(1 + u^2) \equiv 0 \mod p$$

Also gilt $p \mid m_1^2 + m_2^2$, also $p = m_1^2 + m_2^2$. □

3.11 Satz. *Sei $\Lambda \in \mathcal{L}^n$, $k \in \mathbb{N}$ und $X \subset \mathbb{R}^n$ Jordan-messbar mit $\mathrm{vol}(X) > k \det \Lambda$. Dann existieren $x_1, \ldots, x_{k+1} \in X$, $x_i \neq x_j$ mit $x_i - x_j \in \Lambda$ für alle $i \neq j$.*
Dies ist äquivalent zu

$$\exists t \in \mathbb{R}^n. \, |(z + X) \cap \mathbb{Z}^n| \geq k + 1$$

Beweis A. Wegen der Jordan-Messbarkeit gilt

$$k \det \Lambda < \mathrm{vol}(X) = \lim_{m \to \infty} \left| X \cap \frac{1}{m}\Lambda \right| \cdot \frac{\det \Lambda}{m^n}$$

Also gilt diese Ungleichung für ein hinreichend großes $\overline{m}$. Es gilt also $\#\left(X \cap \frac{1}{\overline{m}}\Lambda\right) > \overline{m}^n k$. Wegen $\left|\frac{1}{\overline{m}}\Lambda : \Lambda\right| = \overline{m}^n$ gibt es nach Schubfachprinzip eine Nebenklasse mit mehr als k Elementen. □

Beweis B. OBdA sei $\Lambda = \mathbb{Z}^n$, also $\det \Lambda = 1$, da wir das Volumen hin und her transformieren können. Damit haben wir Fundamentatlzelle $P = [0, 1)^n$. Sei 1_X die charakteristische Funktion von X. Für $x \in \mathbb{R}^n$ sei

$$\phi(x) = \sum_{z \in \mathbb{Z}^n} 1_X(x + z) = \#((-x + X) \cap \mathbb{Z}^n)$$

Wir beschränken uns auf eine beschränkte Teilmenge von X, welche die Bedingungen erfüllt, damit dies endlich ist. Dann haben wir

$$k < \mathrm{vol}(X) = \int_{\mathbb{R}^n} 1_X \mathrm{d}x = \sum_{z \in \mathbb{Z}^n} \int_P 1_X(x + z) \mathrm{d}x = \int_P \phi(x) \mathrm{d}x$$

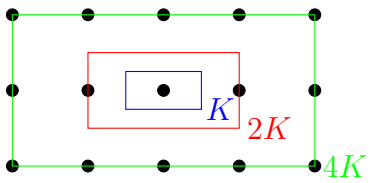
Nach Mittelwertsatz existiert ein $t \in P$ mit $\phi(t) > k$. Also ist $\#((-t + X) \cap \mathbb{Z}^n) \geq k + 1$. □

3.12 Korollar. *Seien $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$ mit $\mathrm{vol}(K) \geq 2^n k \det \Lambda$. Dann ist $\#(K \cap \Lambda) \geq 2k + 1$.*

Beweis. OBdA $\Lambda = \mathbb{Z}^n$ und $\mathrm{vol}(K) > 2^n k$ (wie bei Minkowski Theorem 3.3). Nach Satz 3.11 existieren $x_1, \ldots, x_{k+1} \in \frac{1}{2}K$ mit $x_i \neq n_j$ und $x_i - x_j \in \mathbb{Z}^n \cap K$ für $i \neq j$. Sei x_1 das Element maximaler Norm. Setzen wir $z_i := x_{i+1} - x_1$, so erhalten wir k neue Elemente, da diese unterhalb der Hyperebene $\langle x_1, x \rangle = 0$ liegen, während die bisherigen Punkte darüber liegen. Es gilt nämlich

$$\langle x_1, z_i \rangle = \langle x_1, x_{i+1} \rangle - \langle x_1, x_1 \rangle \leq |x_1| \cdot |x_{i+1}| - |x_1| \cdot |x_1| \leq 0$$

und Gleichheit kann nur eintreten, wenn $x_1 \parallel x_{i+1}$ und $|x_1| = |x_{i+1}|$, also $x_1 = x_{i+1}$ (was nicht sein kann). Damit haben wir $2k + 1$ verschiedene Punkte. □



3.13 Definition. Sei $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$. Für $1 \leq i \leq n$ heißt

$$\lambda_i(K, \Lambda) := \min \{\lambda > 0 : \dim(\lambda K \cap \Lambda) \geq i\}$$

das i-te sukzessive Minimum.

Beispiel. Betrachte folgende Figur. Das heißt $\lambda_1(K, \mathbb{Z}^2) = 2$ und $\lambda_2(K, \mathbb{Z}^2) = 4$.

3.14 Bemerkung. Es gelten folgende Beziehungen

1. $\lambda_i(K, \Lambda) \geq \lambda_{i-1}(K, \Lambda)$
2. $\lambda_i(K, \Lambda) = \lambda_i(AK, A\Lambda)$ für $A \in \mathrm{GL}(n, \mathbb{R})$
3. $\lambda_i(\mu K, \Lambda) = \frac{1}{\mu}\lambda_i(K, \Lambda) = \lambda_i\left(K, \frac{1}{\mu}\Lambda\right)$
4. $\lambda_1(K, \Lambda) \geq 1 \Leftrightarrow \mathrm{int}(K \cap \Lambda \setminus \{0\}) = \emptyset$.
5. $\lambda_1(K, \Lambda) = \min\{|b|_K : b \in \Lambda \setminus \{0\}\}$

3.15 Proposition. *Sei $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$ und seien $a_1, \ldots, a_n \in \Lambda$ linear unabhängig mit $a_i \in \lambda_i(K, \Lambda) \cdot K$. Dann gilt*

$$\mathrm{int}\left(\lambda_i(K, \Lambda) \cdot K\right) \cap \Lambda \subseteq \mathrm{lin}\{a_1, \ldots, a_{i-1}\}$$

Beweis. Schreibe $\lambda_i := \lambda_i(K, \Lambda)$ und sei $k \leq i$ der minimale Index mit $\lambda_k = \lambda_i$. Nach Definition enthält $\mathrm{int}\, \lambda_k \cdot K$ höchstens $k-1$ linear unabhängige Gitterpunkte (sonst könnten wir es verkleinern). Und nach Wahl sind $a_1, \ldots, a_{k-1} \in \mathrm{int}(\lambda_k K) \cap \Lambda$. Also ist $\mathrm{int}(\lambda_k K) \cap \Lambda \subseteq \mathrm{lin}\{a_1, \ldots, a_{k-1}\}$. □

3.16 Theorem. *Sei $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$. Dann ist*

$$\lambda_1(K, \Lambda)^n \,\mathrm{vol}(K) \leq 2^n \det \Lambda$$

Beweis. Definition kann $\lambda_1(K, \Lambda) \cdot K$ keinen inneren Punkt enthalten außer 0. Aber nach Theorem 3.3 ist

$$2^n \det L \geq \mathrm{vol}\left(\lambda_1(K, \Lambda) K\right) = \lambda_1(K, \Lambda)^n \,\mathrm{vol}(K)$$ □

Bemerkung. Genau genommen ist Theorem 3.16 äquivalent zu Theorem 3.3. Es gilt

$$\begin{aligned} \mathrm{vol}(K) \geq 2^n \det \Lambda &\implies 2^n \det L \lambda_1(K, \Lambda)^n \leq \lambda_1(K, \Lambda)^n \,\mathrm{vol}(K) \leq 2^n \det \Lambda \\ &\implies \lambda_1(K, \Lambda) \leq 1 \implies K \cap \Lambda \setminus \{0\} \neq \emptyset \end{aligned}$$

3.17 Theorem. *Sei $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$. Dann ist*

$$\frac{2^n}{n!} \det \Lambda \leq \prod_{i=1}^{n} \lambda_i(K, \Lambda) \cdot \mathrm{vol}(K) \leq 2^n \det \Lambda$$

Beweis. OBdA sei $\Lambda = \mathbb{Z}^n$, und wir schreiben $\lambda_i := \lambda_i(K, \mathbb{Z}^n)$. Seien $z_1, .., z_n \in \mathbb{Z}^n$ linear unabhängig mit $z_i \in \lambda_i K \cap \mathbb{Z}^n$. Sei $L_i := \{x \in \mathbb{R}^n : x_{i+1} = \ldots = x_n = 0\} = \langle e_1, \ldots, e_i \rangle$. Mit einer Matrix $U \in \mathrm{GL}(n, \mathbb{Z})$ können wir erreichen $Uz_i \in L_i$ (siehe Satz 2.12). Diese Matrix ändert Volumen und Dimension nicht. Damit können wir annehmen $z_i \in L_i$.
Wir betrachten nun neue Körper $K_i := \frac{\lambda_i}{2} K$. Für $q \in \mathbb{N}$ sei weiter

$$M_q^n = \{p \in \mathbb{Z}^n : |p_i| \leq q\} \qquad M_q^j = M_q^n \cap L_j \qquad \overline{M}_q^j = M_q^n \cap L_j^\perp$$

Dann ist $\#M_q^n = (2q+1)^n$.

(1) Da K beschränkt, existiert ein $\gamma > 0$ mit $\mathrm{vol}\left(M_q^n + K_n\right) \leq (2q + 2\gamma)^n$.

(2) Nach Definition von λ_1 gilt

$$z + \mathrm{int}(K_1) \cap \overline{z} + \mathrm{int}(K) = \emptyset$$

für alle $z, \overline{z} \in \mathbb{Z}^n$ mit $z \neq \overline{z}$. Damit gilt

$$z - \overline{z} \in \mathrm{int}(K_1) - \mathrm{int}(K_1) = \mathrm{int}(K_1 - K_1) = \mathrm{int}\left(\frac{\lambda_1}{2} K + \frac{\lambda_1}{2} K\right) = \mathrm{int}(\lambda_1 K)$$

Damit ist

$$\mathrm{vol}(M_q^n + K_1) = (2q+1)^n \,\mathrm{vol}(K_1) = (2q+1)^n \left(\frac{\lambda_1}{2}\right)^n \mathrm{vol}(K)$$

(3) Im folgenden zeigen wir

$$\mathrm{vol}\left(M_g^n + K_{i+1}\right) \geq \left(\frac{\lambda_{i+1}}{\lambda_i}\right)^{n-1} \mathrm{vol}\left(M_g^n + K_i\right)$$

Es gilt $\lambda_{i+1} > \lambda_i$. Seien $z, \overline{z} \in M_q^n$, $z \neq \overline{z}$ und $a, \overline{a} \in M_q^i$. Dann ist

$$(z + \mathrm{int}(a + K_{i+1})) \cap (\overline{z} + \mathrm{int}(\overline{a} + K_{i+1})) = \emptyset$$

sonst wäre

$$z - \overline{z} - (a - \overline{a}) \in \mathrm{int}(\lambda_{i+1} K) \cap \mathbb{Z}^n \overset{\textit{Definition 3.13}}{\subseteq} \mathrm{lin}\{z_1, \ldots, z_i\} \subset L_i \quad \lightning$$

da $z - \overline{z} \in L_i^\perp$. Also gilt

$$\mathrm{vol}(M_q^i + K_{i+1}) = (2q+1)^{n-i} \,\mathrm{vol}\left(M_q^i + K_{i+1}\right)$$
$$\mathrm{vol}(M_q^i + K_i) = (2q+1)^{n-i} \,\mathrm{vol}\left(M_q^i + K_i\right)$$

Zeile fehlt

Definiere Abbildungen $f_1, f_2 : \mathbb{R}^n \to \mathbb{R}^n$ mit

$$f_1(x) = \left(\frac{\lambda_{i+1}}{\lambda_i} x_1, \ldots, \frac{\lambda_{i+1}}{\lambda_i} x_i, x_{i+1}, \ldots, x_n\right)^T$$
$$f_2(x) = \left(\frac{x_1, \ldots, x_i, x_{i+1}, \ldots, \frac{\lambda_{i+1}}{\lambda_i} \lambda_{i+1}}{\lambda_i} x_n\right)^T$$

Daraus folgt

$$M_q^i + K_{i+1} = f_2(M_q^i + f_1(K_i)) \implies \mathrm{vol}(M_q^i + K_{i+1}) = \left(\frac{\lambda_{i+1}}{\lambda_i}\right)^{n-i} \mathrm{vol}(M_q^i + f_1(K_i))$$

Es reicht zu zeigen

$$\mathrm{vol}(M_q^i + f_1(K_i)) \geq \mathrm{vol}(M_q^i + K_i)$$

Für $x \in L_i$ gibt es einen Translationsvektor $t(x) \in L_i$ mit

$$\begin{aligned} &K_i \cap (x + L_i) \subseteq (f_1(K_i) \cap (x + L_i)) + t(x) \\ \implies &(M_q^i + K_i) \cap (x + L_i) \subseteq \left[(M_q^i + f_1(K_i) \cap (x + L_i))\right] + t(x) \end{aligned}$$

Nach Fubini folgt nun

$$\begin{aligned} \mathrm{vol}(M_q^i + K_i) &= \int_{x \in L_i^\perp} \mathrm{vol}\left((M_q^i + K_i) \cap (x + L_i)\right) \mathrm{d}x \\ &\leq \mathrm{vol}(M_q^i + f_1(K_i)) = \int_{x \in L_i^\perp} \mathrm{vol}\left((M_q^i + K_i) \cap (x + L_i)\right) \mathrm{d}x = \mathrm{vol}(M_q^i + f_1(K_i)) \end{aligned}$$

Für die untere Schranke betrachte $\pm\frac{z_i}{2} \in K$. Damit enthält ihre Konvexe Hülle das Kreuzpolytop.

Formel

Aus (1),(2) und (3) folgt dann die Behauptung.

$$\begin{aligned} (2g + 2\gamma)^n &\overset{item\ 1}{\geq} \mathrm{vol}\left(M_g^n + K_n\right) \overset{item\ 3}{\geq} \left(\frac{\lambda_n}{\lambda_{n-1}}\right) \mathrm{vol}\left(M_g^n + K_{n-1}\right) \\ &\overset{item\ 3}{\geq} \prod_{i=1}^{n} \left(\frac{\lambda_{n-i+1}}{\lambda_{n-i}}\right)^i \cdot \mathrm{vol}\left(M_g^n + K_1\right) \overset{item\ 2}{\geq} \prod \lambda_i \cdot \frac{\mathrm{vol}(K)}{2^n}(2q+1)^n \end{aligned}$$

□

3.18 Proposition. *Sei $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$. Dann gilt*

$$\#(K \cap \Lambda) \leq [\![\frac{2}{\lambda_1(K, \Lambda)} + 1]\!]^n$$

Das bedeutet

$$\mathrm{int}(K cap \Lambda) = \{0\} \implies \lambda_1(K, \Lambda) \geq 1 \implies \#(K \cap \Lambda) \leq 3^n$$

Beweis. OBdA sei $\Lambda = \mathbb{Z}^n$, und wir schreiben $\lambda_i := \lambda_i(K, \mathbb{Z}^n)$. Setze $k := [\![\frac{2}{\lambda_1} + 1]\!]$. Angenommen, es gilt $z, \overline{z} \in \mathbb{Z}^n \cap K$ mit $z \equiv \overline{z} \mod k$. Dann gilt

$$\mathbb{Z}^n \ni \frac{1}{k}(z - \overline{z}) = \frac{2}{k}\left(\frac{1}{2}z - \frac{1}{2}\overline{z}\right) \in \frac{2}{k} \subset \mathrm{int}(\lambda_1 K) \implies z = \overline{z}$$

Zwei verschiedene Gitterpunkte von K liegen in verschiedenen Restklassen modulo k. Also ist $\#(K \cap \mathbb{Z}^n) \leq k^n$. □

Wir haben quasi eine diskrete Version von Minkowskis erstem Satz. Die Frage nach einem Analogon für den zweiten Satz ist offen. Die diskrete Version impliziert die Aussage für das Volumen, da wir Jordan-messbar voraus setzen.

Formel

Vorlesung fehlt

3.19 Lemma. *1.*

2. $b_1, \dots, b_n \in \Lambda$ *ist eine HKZ-Basis genau dann, wenn*

$$\overline{b}_k = b_k | L_{k-1}^{\perp} \qquad\qquad L_i = \operatorname{lin}\{b_1, \dots, b_i\}$$

sind kürzeste Gittervektoren in $\Lambda | L_{k-1}^{\perp}$ *und* $|\mu_{ij}| \leq \frac{1}{2}$

Beweis. 1.

2. Induktion, $n = 1$ ist klar. Nach Definition is $b_1, \dots, b_n$ HKZ-reduziert genau dann, wenn

   (a) b_1 kürzester Gittervektor in Λ

   (b) $v_2 = b_2 - \mu_{21} b_1, \dots, v_n = b_n - \mu_{n1} b_1$ ist HKZ von $\Lambda_{n-1} = \Lambda | \operatorname{lin}\{b_1\}^{\perp}$.

   (c) $|\mu_{i1}| \leq \frac{1}{2}$

   Nach Induktion ist $v_2, \dots, v_n$ HKZ genau dann, wenn

   (a) $\overline{v}_k = v_k | \widetilde{L}_{k-2}^{\perp}$ ist kürzester Gittervektor von $\Lambda_{n-1} | \widetilde{L}_{k-2}^{\perp}$ für $k = 2, \dots, n$.

   (b) $\left| \frac{\langle v_i, \overline{v}_j \rangle}{\|\overline{v}_j\|^2} \right| \leq \frac{1}{2}$ für $2 \leq j < i \leq n$.

   Nun ist $L_{k-1} = \widetilde{L}_{k-2}^{\perp} \oplus \operatorname{lin}\{b_1\}$. Damit ist $x | L_{k-1}^{\perp} = \left(x | \operatorname{lin}\{b_1\}^{\perp}\right) | \widetilde{L}_{k-2}$ und

   $$\overline{b}_k = b_k | l_{k-1}^{\perp} = v_k | \widetilde{L}_{k-2}^{\perp} = \overline{v}_k \qquad\qquad k = 2, \dots, n$$

   Damit erhalten wir

   $$|\mu_{ij}| = \left| \frac{\langle b_i, \overline{b}_j \rangle}{|\overline{b}_j|^2} \right| = \left| \frac{\langle b_i, \overline{v}_j \rangle}{|\overline{v}_j|^2} \right| = \left| \frac{\langle v_i, \overline{v}_j \rangle}{|\overline{v}_j|^2} \right| \leq \frac{1}{2}$$

□

3.20 Satz. *Sei* $b_1, \dots, b_n$ *HKZ von* $\Lambda \in \mathcal{L}^n$. *Dann ist*

$$\frac{2}{\sqrt{i+3}} \lambda_i(B_n, \Lambda) \leq |b_i| \leq \frac{\sqrt{i+3}}{2} \lambda_i(B_n, \Lambda) \qquad\qquad i = 1, \dots, n$$

Beweis. Setze $\lambda_i := \lambda_i(B_n, \Lambda)$. Sei $\overline{b}_1, \dots, \overline{b}_n$ die zugehörige GSO-Basis. Dann gilt

$$|b_i|^2 = \left| \overline{b}_i + \sum_{j=1}^{i-1} \mu_{ij} \overline{b}_j \right|^2 = \left|\overline{b}_i\right|^2 + \sum_{j=1}^{i-1} |\mu_{ij}|^2 \left|\overline{b}_j\right|^2 \leq \left|\overline{b}_i\right|^2 + \frac{1}{4} \sum_{j=1}^{i-1} \left|\overline{b}_j\right|^2 \tag{1}$$

obere Schranke Seien $a_1, \dots, a_n \in \Lambda$ linear unabhängig mit $|a_j| = \lambda_j$. Für $j \leq n$ wähle k so, dass $a_k | \operatorname{lin}\{b_1, \dots, b_{j-1}\}^{\perp} \neq 0$. Nach Lemma 3.19.item 2 gilt für $j \leq n$

$$|\overline{b}_j| \leq \left| a_k | \operatorname{lin}\{b_1, \dots, b_{j-1}\}^{\perp} \right| \leq a_k \leq \lambda_j$$

Nach (1) ergibt sich

$$|b_i|^2 \leq \lambda_i^2 + \frac{1}{4}\sum_{j=1}^{i-1}\lambda_i^2 = \lambda_i^2\left(1+\frac{i-1}{4}\right)$$
$$\Longrightarrow |b_i| \leq \frac{i+3}{2}\lambda_i$$

untere Schranke Wir haben

$$\left|\bar{b}_i\right| \leq \left|b_k|\operatorname{lin}\{b_1,\ldots,b_{i-1}\}^{\perp}\right| \leq |b_k|$$
$$\overset{(1)}{\Longrightarrow} |b_i|^2 \leq \left|\bar{b}_i\right|^2 + \frac{1}{4}\sum_{j=1}^{i-1}\left|\bar{b}_j\right|^2 = \left(\frac{i+3}{4}\right)|b_k|^2$$

Für festes k folgt dann

$$\lambda_k^2 \leq \max\{|b_i|^2 : i \leq k\} \leq \frac{k+3}{4}|b_k|^2$$

wobei die erste Ungleichung aus der Definition der sukzessiven Minima folgt. Damit haben wir die untere Schranke. □

3.21 Korollar. *Sei $\Lambda \in \mathcal{L}^n$. Es gibt eine Basis $b_1,\ldots,b_n$ von Λ mit*

$$\left(\frac{|b_1|\cdot\ldots\cdot|b_n|}{\det\Lambda}\right)^{\frac{1}{n}} \leq cn$$

wobei c eine absolute Konstante ist.

Beweis. Sei $b_1,\ldots,b_n$ eine HKZ-Basis von Λ.

$$\left(\frac{|b_1|\cdot\ldots\cdot|b_n|}{\det\Lambda}\right)^{\frac{1}{n}} \overset{\text{Satz 3.20}}{\leq} \left(\prod_{i=1}^{n}\frac{\sqrt{i+3}}{2}\right)^{\frac{1}{n}}\cdot\left(\frac{\prod_{i=1}^{n}\lambda_i(B_n,\Lambda)}{\det\Lambda}\right)^{\frac{1}{n}}$$
$$\overset{\text{Theorem 3.17}}{\leq} \sqrt{n}\cdot\left(\frac{2^n}{\operatorname{vol}(B_n)}\right)^{\frac{1}{n}} = 2\sqrt{n}\cdot\left(\frac{\Gamma\left(\frac{n}{2}+1\right)}{\pi^{\frac{n}{2}}}\right)^{\frac{1}{n}} \leq cn$$

wobei wir nutzen $\Gamma(\frac{n}{2}+1) \approx \left(\frac{n}{2}\right)! \leq \left(\frac{n}{2}\right)^{\frac{n}{2}}$. □

Beispiel. Im 2-dimensionalen, sei b_1 ein kleinster Gittervektor. Dann haben wir $|b_2|^2 \geq |b_1|^2$ und damit $|b_2|^2 \leq \frac{1}{1-\mu^2}|\bar{b}_2|^2$. Daraus erhalten wir

$$\frac{|b_1|\cdot|b_2|}{\det\Lambda} = \frac{|b_1||b_2|}{|b_1||\bar{b}_2|} = \frac{|b_2|}{|\bar{b}_2|} \leq \sqrt{\frac{1}{1-\mu^2}} \leq \frac{2}{\sqrt{3}} \approx 1.1547$$

Dieser Wert ist optimal, wie das Hexagonalgitter zeigt.

3.22 Proposition. *Sei $B = (b_1,\ldots,b_n)$ eine HKZ-Basis von $\Lambda \in \mathcal{L}^n$. und sei $q_B(x) = x^T B^T B x$ für $x \in \mathbb{R}^n$. Dann gilt*

$$q_B(x) = \sum_{i=1}^{n}\left(|\bar{b}_i|^2\left(x_i + \sum_{j=i+1}^{n}\mu_{ji}x_j\right)^2\right)$$

mit

$$|\mu_{ji}| \leq \frac{1}{2}$$

$$|b_k|^2 = \min\left\{\sum_{i=k}^{n}\left(|b_i|^2\left(z_i + \sum_{j=i+1}^{n}\mu_{ij}z_j\right)^2\right) : 0 \neq (z_k, \ldots, z_n \in \mathbb{Z}^{n-k+1}\right\}$$

Beweis. Sei $\overline{B} = (\bar{b}_1, \ldots, \bar{b}_n)$ die GSO. Schreibe $B = \overline{B} \cdot M$ wobei M eine obere Dreiecksmatrix ist, mit 1 auf Diagonale und μ_{ij} oberhalb. Dann ist

$$q_B(x) = x^T M^T \overline{B}^T \overline{B} M x = x^T M^T \begin{pmatrix} |\bar{b}_1|^2 & \ldots & \\ & \ddots & \\ & \ldots & |\bar{b}_n|^2 \end{pmatrix} M x$$

Weiter ist $q_B(z) = z^T B^T B z = |Bz|^2$ und

$$\min\{q_B(z) : 0 \neq z \in \mathbb{Z}^n\} = \min\left\{|Bz|^2 : 0 \neq z \in \mathbb{Z}^n\right\} = \min\left\{|b|^2 : 0 \neq b \in \Lambda\right\} = |b_1|^2 \qquad \square$$

3.23 Definition. Sei A positiv definit. Die Form

$$q_A(x) := x^T A x = \sum_{i=1}^{n} a_i \cdot \left(x_i + \sum_{j=i+1}^{n} a_{ji} x_j\right)^2$$

heißt HKZ-reduziert, falls die positiven äußeren Koeffizienten

Rest der Vorlesung fehlt

Lücke

3.24 Satz. *Sei $b_1, \ldots, b_n \in \Lambda$ eine LLL-reduzierte Basis von $\Lambda \in \mathcal{L}^n$. Dann gilt*

$$|\bar{b}_i|^2 \leq 2^{j-i}|\bar{b}_j|^2$$

weiter

3.25 Satz. *Sei $\Lambda \in \mathcal{L}^n$ und $b_1, \ldots, b_n$ eine LLL-reduzierte Basis.*

1. $|b_1| \leq 2^{\frac{n-1}{2}}\lambda_1(B_n, \Lambda)$
2. $|b_1| \leq 2^{\frac{n-1}{4}}(\det\Lambda)^{\frac{1}{n}}$
3. $\left(\frac{|b_1|\cdot\ldots\cdot|b_n|}{\det\Lambda}\right)^{\frac{1}{n}}$

Beweis. Nach Satz 3.24 gilt

$$|\bar{b}_k|^2 \geq \left(\frac{1}{2}\right)^{k-i}|\bar{b}_i|^2 \text{ für} k \geq i$$

$$\overset{i=1}{\Longrightarrow} |\bar{b}_k|^2 \geq \left(\frac{1}{2}\right)^{k-i}|b_1|^2$$

$$\overset{??}{\Longrightarrow} \lambda_1(B_n, \Lambda) \geq \min\{|\bar{b}_1|, \ldots, |\bar{b}_n|\} \geq \left(\frac{1}{2}\right)^{\frac{n-1}{2}}|b_1|$$

Weiterhin ist

$$(\det\Lambda)^2 = \prod_{k=1}^{n} |\bar{b}_k|^2 \geq \prod_{k=1}^{n} \frac{1}{2^{k-1}} |b_1|^2 = \frac{1}{2^{\binom{n}{2}}} |b_1|^{2n}$$

$$|b_k|^2 = \left| \bar{b}_k + \sum_{i=1}^{k-1} \mu_{k,i} \bar{b}_i \right|^2 \leq |\bar{b}_k|^2 + \frac{1}{4} \sum_{i=1}^{k-1} |\bar{b}_i|^2 \leq |\bar{b}_k|^2 + \left(\frac{1}{4} \sum_{i=1}^{k-1} 2^{k-i} \right) |\bar{b}_k|^2 \leq 2^{k-1} |\bar{b}_k|^2$$

Damit haben wir

$$\prod_{k=1}^{n} |b_k|^2 \leq \prod_{k=1}^{n} |\bar{b}_k|^2 \prod_{k=1}^{n} 2^{k-1} = (\det\Lambda)^2 \cdot 2^{\binom{n}{2}} \qquad \square$$

3.26 Bemerkung (Babai, 1986). Sei $\Lambda \subseteq \mathbb{Q}^n$ eine Gitter und sei $w \in \mathbb{Q}^n$. Dann existiert ein polynomieller Algorithmus, der ein $a \in \Lambda$ berechnet mit $|w - a| \leq 2^{\frac{n}{2}} \min\{|w - b| : b \in \Lambda\}$.

Beweis. Sei $b_1, \ldots, b_n$ eine LLL-reduzierte Basis. Zunächst bestimmen wir einen Punkt $a \in \Lambda$ mit

$$w - a = \sum_{i=1}^{n} \sigma_i \bar{b}_i \qquad\qquad |\sigma_i| \leq \frac{1}{2}$$

Sei $w = \sum_{i=1}^{n} \sigma_{i,n} \bar{b}_i$ mit $\sigma_{i,n} \in \mathbb{Q}$. Dann haben wir

$$w - [\sigma_{n,n}] b_n = \sum_{i=1}^{n} \sigma_{i,n-1} \bar{b}_i + (\sigma_{n,n} - [\sigma_{n,n}]) \bar{b}_n$$

Im nächsten Schritt ziehen wir $[\sigma_{n-1,n-1}] b_{n-1}$ von der linken Seite ab usw. Sei $a = \sum_{i=1}^{n} [\sigma_{i,i}] b_i \in \Lambda$. Sei $c \in \Lambda$ mit $|w - c| = \min\{|w - b| : b \in \Lambda\}$ und schreibe $w - c = \sum \mu_i \bar{b}_i$. Angenommen $c \neq a$. Setze $\rho_k := \sigma_{k,k} - [\sigma_{k,k}]$. Dann ist $w - a = \sum \rho_i \bar{b}_i$. Sei k der größte Index mit $\mu_k \neq \rho_k$. Dann ist

oder so

$$\Lambda \cap \mathrm{lin}\{\mathrm{b}_1, \ldots, \mathrm{b}_\mathrm{k}\} \ni c - a = (w - a) - (w - c) = \sum_{i=1}^{k} (\rho_i - \mu_i) \bar{b}_i = \sum_{i=1}^{k-1} \tau_i \bar{b}_i + \underbrace{(\rho_k - \mu_k)}_{\neq 0, \in \mathbb{Z}} b_k$$

(wähle τ_i so, dass dies gilt). Der letzte Koeffizient ist ganzzahlig, da es sich um einen Gittervektor handelt. Damit haben wir $|\rho_k - \mu_k| \geq 1$, also $|\mu_k| \geq \frac{1}{2}$. Dies ergibt

$$\begin{aligned} |w - a|^2 &\leq \frac{1}{4} \sum_{i=1}^{k} |\bar{b}_i|^2 + \sum_{i=1}^{k+1} \rho_i^2 |\bar{b}_i|^2 \overset{\text{Satz 3.24}}{\leq} \frac{1}{4} \sum_{i=1}^{k} 2^{k-i} |\bar{b}_k|^2 + \sum_{i=1}^{k+1} \rho_i^2 |\bar{b}_i|^2 \\ &< 2^k \left(\frac{1}{4} |\bar{b}_k|^2 + \sum_{i=k+1}^{n} \mu_i^2 |\bar{b}_i|^2 \right) \leq 2^k \left(\sum_{i=k}^{n} \mu_i^2 |\bar{b}_i|^2 \right) \leq 2^k |w - c|^2 \end{aligned} \qquad \square$$

3.31 Satz. *Sei $k \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$. Dann existiert eine Basis $b_1, \ldots, b_n$ von Λ so, dass $|b_i|_K \leq \max\left\{1, \frac{i}{2}\right\} \cdot \lambda_i(K, \Lambda)$.*

Beweis. seien $a_1, \ldots, a_n \in \Lambda$ linear unabhängig mit $a_i \in \lambda_i(K, \Lambda) K$. Nach Satz 2.12 existiert eine Basis $C := (c_1, \ldots, c_n)$ von Λ und eine obere Dreiecksmatrix $H \in \mathbb{Z}^{n \times n}$ mit nicht-negativen Einträgen und $h_{k,k} > h_{i,k}$ für alle $i < k$ so, dass $A := (a_1, \ldots, a_n) = C \cdot H$. Sei $\overline{H} := H^{-1} = (\bar{h}_{ij})$. Dann ist $\overline{H}$ eine obere Dreiecksmatrix mit $\bar{h}_{ii} = h_{ii}^{-1}$. Sei $V \in \mathbb{Z}^{n \times n}$ eine andere obere Dreiecksmatrix mit Nullen auf der Diagonalen so, dass $|\bar{h}_{ij} + v_{ij}| \leq \frac{1}{2}$ für alle $i < j$. Setze

$$B := (b_1, \ldots, b_n) = A(\overline{H} + V) = C + AV$$

Dann ist $b_i \in \Lambda$ und

$$\det B = \det A \cdot \det\left(\overline{H} + V\right) = \frac{\det A}{\det H} = \det C \neq 0$$

Damit ist B eine Basis des Gitters.

$$\begin{aligned}
|b_k|_K &= \left|\sum_{s=1}^{k-1} \left(\overline{h}_{jk} + v_{jk}\right) a_j + \frac{1}{h_{kk}} a_k\right|_K \leq \sum_{s=1}^{k-1} \left|\overline{h}_{jk} + v_{jk}\right| |a_j|_K + \frac{1}{h_{kk}} |a_k|_K \\
&\leq \frac{k-1}{2}\lambda_k(K,\Lambda) + \frac{1}{h_{kk}}\lambda_k(K,\Lambda) \leq \begin{cases} \frac{k}{2}\lambda_k(K,\Lambda) & : h_{kk} \geq 2 \\ \lambda_k(K,\Lambda) & : h_{kk} = 1 \end{cases}
\end{aligned}$$

denn, wenn $h_{kk} = 1$, dann gilt $h_{ik} = 0$ für $i < k$, also $\overline{h}_{ik} = v_{ik} = 0$. □

3.32 Korollar. *Sei $K \in \mathcal{K}_0^n$ und $\Lambda \in \mathcal{L}^n$. Es gibt eine Basis $b_1, \ldots, b_n$ von Λ mit*

$$\overline{c} \cdot \frac{1}{n}\left(\frac{|b_1|_K \cdot \ldots \cdot |b_n|_K}{\det \Lambda} \cdot \mathrm{vol}(K)\right)^{\frac{1}{n}} \leq cn$$

für absolute Konstanten $c, \overline{c}$ und es gilt

$$|b_i|_K \leq \left(\frac{4n!}{\mathrm{vol}(K)} \cdot \frac{\det L}{\lambda_1(K,\Lambda)^{i-1}}\right)^{\frac{1}{n-i+1}}$$

Beweis. Nach Theorem 3.17 gilt

$$\frac{2^n}{n!}\det\Lambda \leq \mathrm{vol}(K)\prod_{i=1}^{n}\lambda_i(K,\Lambda) \leq 2^n \det\Lambda$$

Mit Satz 3.31 erhalten wir zudem

$$\prod_{i=1}^{n}|b_i|_K \cdot \frac{2^{n-1}}{n!} \leq \prod_{i=1}^{n}\lambda_i(K,\Lambda) \leq \prod_{i=1}^{n}|b_i|_K$$

Einsetzen liefert die obere Schranke.
Für die untere Schranke betrachte

$$\lambda_1^{i-1}\lambda_i \ldots \lambda_n \leq \lambda_1 \ldots \lambda_n \,\mathrm{vol}(K) \leq 2^n \det\Lambda$$

Damit haben wir

$$\begin{aligned}
\frac{2^{n-i+1}}{n!}\mathrm{vol}(K)\min\left\{|b_j|_K : i \leq j \leq n\right\}^{n-i+1} &\leq \mathrm{vol}(K)\frac{2^{n-i+1}}{n!}|b_i|_K \ldots |b_n|_K \\
&\leq \lambda_i \ldots \lambda_n \,\mathrm{vol}(K) \leq 2^n \frac{\det L}{\lambda_1^{i-1}}
\end{aligned}$$

□

3.33 Definition. Für $Kin\mathcal{K}_0^n$ mit $\Lambda \in \mathcal{L}^n$ heißt eine Basis *Minkowski-reduziert*, falls für $1 \leq i \leq n$ gilt

$$|b_i|_K = \min\left\{|b|_K : b \in \Lambda, \{b_1, \ldots, b_{i-1}, b\} \text{ primitiv}\right\}$$

3.34 Proposition. *Sei $K \in \mathcal{K}_0^n$ und $\Lambda \in \mathcal{L}^n$. Dann ist $b_1, \ldots, b_n$ Minkowski-reduziert, genau dann, wenn*

$$|b_i|_K \leq \left| \sum_{j=1}^{n} z_j b_j \right|$$

für alle $z \in \mathbb{Z}^n$ mit $\mathrm{ggT}(z_i, \ldots, z_n) = 1$.

3.35 Satz. *Sei $K \in \mathcal{K}_0^n$ und $\Lambda \in \mathcal{L}^n$ und seien $b_1, \ldots b_n$ Minkowski-reduziert. Dann gilt*

$$\lambda_i(K, \Lambda) \leq \max\{|b_j|_K : j \leq i\}$$

sowie

$$|b_i|_K \leq \left(\frac{3}{2}\right)^{i-1} \lambda_i(K, \Lambda)$$

Beweis. Die untere Schranke ist klar.
Obere Schranke mit Induktion. $i = 1$ ist klar. Seien $a_1, \ldots, a_i$ linear uabängig mit $|a_j|_K \leq \lambda_i(K, \Lambda)$ für $1 \leq j \leq i$. Betrachte $b_1, \ldots, b_{i-1}, a_i$ und sei $b \in \mathrm{lin}\{b_1, \ldots, b_{i-1}, a_i\} \cap \Lambda$ so, dass $b_1, \ldots, b_{i-1}, b$ eine Basis von $\mathrm{lin}\{b_1, \ldots, b_{i-1}, a_i\} \cap \Lambda$ ist. Dann lässt b sich schreiben als

$$b = \sum_{k=1}^{i-1} \rho_j b_j + \rho_i a_i \qquad \text{mit } \rho_j \in \mathbb{R}$$

Dann gilt $\frac{1}{\rho_i} \in \mathbb{Z}$. Weiterhin können wir annehmen, dass $|\rho_i| \leq \frac{1}{2}$ für $1 \leq i \leq j-1$, denn ansonsten ersetzte b durch $b - \sum \lfloor \rho_j \rfloor b_j$. Daraus folgt

$$\begin{aligned} |b_i|_K \leq |b|_K \leq \left| \sum_{j=1}^{i-1} \rho_j b_j + \rho_i a_i \right|_K &\leq \sum_{j=1}^{i-1} \frac{1}{2} |b_j|_K + |a_i|_K \\ &\leq \left(\sum_{j=1}^{i-1} \frac{1}{2} \left(\frac{3}{2}\right)^{j-1} + 1 \right) \lambda_i(K, \Lambda) \leq \left(\frac{3}{2}\right)^{i-1} \lambda_1(K, \Lambda) \end{aligned}$$

□

Mit mehr Aufwand kann man den Faktor $\frac{3}{2}$ ersetzen durch $\frac{5}{4}$. Es ist offen, ob es polynomiell (möglichst linear) geht.

4 Übertragungssätze

4.1 Bemerkung. Sei Λ eine Gitter mit Basis $\alpha_i e_i$ mit $\alpha_1 \geq \ldots \geq \alpha_n$. Λ^* ist ein Gitter mit Basis $\alpha_i^{-1} e_i$. Dann gilt

$$\lambda_i(B_n, \Lambda) = \alpha_{n+1-i} \qquad \lambda_i(B_n, \Lambda^*) = \alpha_i^{-1}$$

Für das Produkt ergibt sich dann

$$\lambda_i(B_n, \Lambda) \lambda_j(B_n, \Lambda^*) = \frac{\alpha_{n+1-i}}{\alpha_j}$$

Dafür wollen wir Schranken angeben. Doch eine obere Schranke ist nur möglich für $j \leq n+1-i$ und eine untere Schranke existiert nur für $j \geq n+1-i$.

4.2 Lemma. *Sei $K \in \mathcal{K}_0^n$ und $\Lambda \in \mathcal{L}^n$. Dann existiert eine absolute Konstante c mit*

$$\lambda_1(K,\Lambda)\lambda_1(K^*,\Lambda^*) \leq cn$$

Beweis. Aus Theorem 3.16 folgt

$$\lambda_1(K,\Lambda) \leq \frac{2\sqrt[n]{\det \Lambda}}{\sqrt[n]{\mathrm{vol}(K)}} \qquad \lambda_1(K^*,\Lambda^*) \leq \frac{2\sqrt[n]{\det \Lambda^*}}{\sqrt[n]{\mathrm{vol}(K^*)}}$$

Damit erhalten wir

$$\lambda_1(K,\Lambda)\lambda_1(K^*,\Lambda^*) \leq \frac{4}{\sqrt[n]{\mathrm{vol}(K)\,\mathrm{vol}(K^*)}} \overset{1.6}{\leq} cn$$

□

4.3 Satz. *Für jedes n gibt es ei Gitter $\Lambda \in \mathcal{L}^n$ mit $\Lambda = \Lambda^*$ und*

$$\lambda_1(B_n,\Lambda)\lambda_1(B_n,\Lambda^*) = \lambda_1(B_n,\Lambda)^2 \geq c'n$$

Damit ist eine lineare Schranke das beste, was möglich ist.

4.4 Satz. *Sei $\Lambda \in \mathcal{L}^n$. Dann existiert eine Konstante c mit*

$$\lambda_i(B_n,\Lambda)\lambda_{n+1-i}(B_n,\Lambda^*) \leq cn^2$$

Beweis. Sei $b_1,\ldots,b_n$ eine HKZ-reduzierte Basis mit GSO $\overline{b_1},\ldots,\overline{b_n}$. Sei $L_i = \langle b_1,\ldots,b_{i-1}\rangle$ und $\Lambda_{n+1-i} := \Lambda \mid L_i^\perp$. Nach Lemma 2.18 ist $[\Lambda_{n+1-i}]^* = L_i^\perp \cap \Lambda^* \subseteq \Lambda^*$.
Schreibe verkürzt

$$\lambda_{j,n+1-i} = \lambda_j(B_n \cap L_i^\perp, \Lambda_{n+1-i}) \qquad \lambda^*_{j,n+1-i} = \lambda_j(B_n \cap L_i^\perp, [\Lambda_{n+1-i}]^*)$$

Weiterhin ist

$$|b_i|^2 = \left|\overline{b}_i + \sum_{j=1}^{i-1}\mu_{ij}\overline{b}_j\right|^2 \leq \left|\overline{b}_i\right| + \frac{1}{4}\sum_{j=1}^{i-1}\left|\overline{b}_j\right|^2 = \lambda^2_{1,n+1-i} + \frac{1}{4}\sum_{j=1}^{i-1}\lambda^2_{1,n+1-j}$$

Daraus ergibt sich

$$\begin{aligned}
|b_i|^2\left(\lambda^*_{1,n}\right)^2 &\leq \lambda^2_{1,n+1-i}\left(\lambda^*_{1,n}\right)^2 + \frac{1}{4}\sum_{j=1}^{i-1}\lambda^2_{1,n+1-j}\left(\lambda^*_{1,n}\right)^2 \\
&\leq \lambda^2_{1,n+1-i}\left(\lambda^*_{1,n+1-i}\right)^2 + \frac{1}{4}\sum_{j=1}^{i-1}\lambda^2_{1,n+1-j}\left(\lambda^*_{1,n+1-j}\right)^2 \\
&\leq c\cdot\left((n+1-i)^2 + \frac{1}{4}\sum_{j=1}^{i-1}(n+1-j)^2\right) \leq c\cdot\frac{i+3}{4}n^2
\end{aligned}$$

Da $\lambda_{k,n} \leq \max\{|b_1|,\ldots,|b_k|\}$, erhalten wir

$$\lambda_{i,n}\lambda^*_{1,n} \leq c\sqrt{\frac{i+3}{4}}\cdot n \tag{2}$$

Nun betrachten wir

$$
\begin{aligned}
|b_i|^2 \left(\lambda^*_{1,n+1-i}\right)^2 &\leq \lambda^2_{1,n+1-i} \left(\lambda^*_{n+1-i,n}\right)^2 + \frac{1}{4}\sum_{j=1}^{i-1} \lambda^2_{1,n+1-j} \left(\lambda^*_{n+1-i,n}\right)^2 \\
&\leq \lambda^2_{1,n+1-i} \left(\lambda^*_{n+1-i,n+1-i}\right)^2 + \frac{1}{4}\sum_{j=1}^{i-1} \lambda^2_{1,n+1-j} \left(\lambda^*_{n+1-i,n+1-j}\right)^2 \\
&\overset{(2)}{\leq} c \cdot \left(\frac{n-i+4}{4}(n+1-i)^2 + \frac{1}{4}\sum_{j=1}^{i-1} \frac{n-i+4}{4}(n+1-j)^2 \right) \leq c \cdot \frac{n-i+4}{4}\frac{i+3}{4} n^2 \leq cn^4
\end{aligned}
$$

Zusammen ergibt dies

$$\lambda^2_{i,n} \left(\lambda^*_{n+1-i,n}\right)^2 \leq cn^4$$

□

4.5 Satz. *Sei $K \in \mathcal{K}^n_0$ und $\Lambda \in \mathcal{L}^n$. Dann ist*

$$1 \leq \lambda_i(K,\Lambda)\lambda_{,+1-i}(K^*,\Lambda^*) \leq cn^{\frac{5}{2}}$$

Beweis. Nach Bemerkung 1.5 existiert ein $A \in \mathbb{R}^{n\times n}$ so, dass $B_n \subseteq AK$ □

Stück fehlt

4.6 Bemerkung.

1. $\mu(K,\Lambda) \geq (\det\Lambda/\operatorname{vol}(K))^{\frac{1}{n}}$
2. Für $t \in \mathbb{R}^n$, $\lambda > 0$ gilt
$$\begin{aligned}\mu(t+K,\Lambda) &= \mu(K,\Lambda) \\ \mu(K,\lambda\Lambda) &= \lambda\mu(K,\Lambda)\end{aligned}$$
3. Wenn $K \cap \Lambda = \emptyset$, dann ist $\mu(K,\Lambda) > 1$
4. $\mu(B_n,\mathbb{Z}^n) = \frac{1}{2}\sqrt{n}$, man muss nur den Punkt $\left(\frac{1}{2},\ldots,\frac{1}{2}\right)$ betrachten.

4.7 Satz. *Sei $\Lambda \in \mathcal{L}^n$.*

1. *Für $K \in \mathcal{K}^n$ gilt*
$$\mu(K,\Lambda) \leq \lambda_1(K-K,\Lambda) + \ldots + \lambda_n(K-K,\Lambda)$$
2. *Für $K \in \mathcal{K}^n_0$ gilt*
$$\mu(K,\Lambda) \geq \frac{1}{2}\lambda_n(K,\Lambda)$$

Beweis. Schreibe $\mu := \mu(K,\Lambda)$ und $\lambda_i = \lambda_i(K-K,\Lambda)$. Seien $a_1,\ldots,a_n \in \Lambda$ linear unabhängig mit $a_i \in \lambda_i(K-K)$. Dann existieren $v_i, v_i' \in K$ mit $a_i = \lambda_i(v_i - v_i')$. Sei $w_i := \lambda_i v_0'$. Damit gilt $w_i, w_i + a_i \in \lambda_i K$. Sei $x \in \mathbb{R}^n$ beliebig und schreibe $x - \sum w_i = \sum \rho_i a_i$ für Koeffizienten $\rho_i \in \mathbb{R}$.

$$
\begin{aligned}
x &= \sum_{i=1}^n \lfloor\rho_i\rfloor a_i + \sum_{i=1}^n w_i + \sum_{i=1}^n \left(\rho_i - \lfloor\rho_i\rfloor\right) a_i \\
&= \sum_{i=1}^n \lfloor\rho_i\rfloor a_i + \sum_{i=1}^n \left(1 - \rho_i + \lfloor\rho_i\rfloor\right) w_i + \sum_{i=1}^n \left(\rho_i - \lfloor\rho_i\rfloor\right)(w_i + a_i) \in \Lambda + \sum_{i=1}^n \lambda_i K
\end{aligned}
$$

Daraus folgt $\mu \leq \sum \lambda_i$.
Sei $a_i \in \lambda_i(K,\Lambda)K$. Angenommen, es gibt ein $b \in \Lambda$ mit $\left|b - \frac{1}{2}a_n\right|_K < \frac{1}{2}\lambda_n$. Nach Dreiecksungleichung gilt

$$|b|_K \leq \left|b - \frac{1}{2}a_n\right|_K + \left|\frac{1}{2}a_n\right|_K < \frac{1}{2}\lambda_n + \frac{1}{2}\lambda_n = \lambda_n$$

Doch dasselbe wenden wir an auf $b - a_n$ und erhalten

$$|b - a_n|_K \leq \left|b - \frac{1}{2}a_n\right|_K + \left|\frac{1}{2}a_n\right|_K < \frac{1}{2}\lambda_n + \frac{1}{2}\lambda_n = \lambda_n$$

Damit gilt

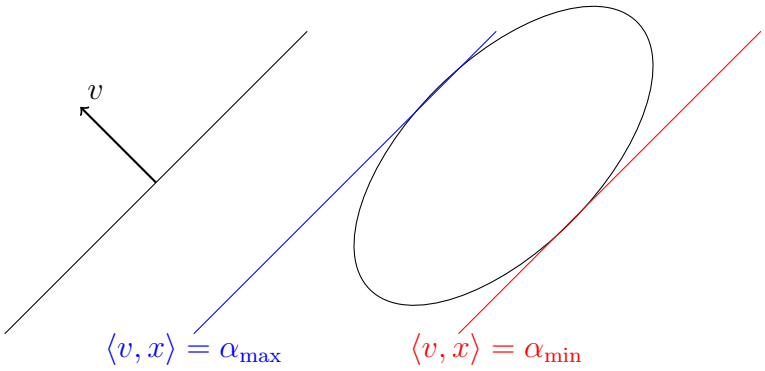
$$b, b - a_n \in \Lambda \cap \operatorname{int}(\lambda_n K) \subseteq \operatorname{lin}\{a_1, \ldots, a_{n-1}\}$$

was ein Widerspruch zur linearen Unabhängigkeit ist. □

4.8 Definition (Gitterdicke). Sei $\Lambda \in \mathcal{L}^n$, $K \in \mathcal{K}^n$.

$$W_\Lambda(K) := \min_{0 \neq b \in \Lambda^*} \left(\max_{x \in K} \langle b, x \rangle - \min_{y \in K} \langle b, y \rangle \right)$$

heißt *Gitterdicke* von K bezüglich Λ.



Das heißt, wir zählen zwischen unseren beiden Schranken die Anzahl der parallelen Gitter-Hyperebenen.
Sei $b \in \Lambda^*$ primitiv, ergänze dies zu einer Basis $b, b_2, \ldots, b_n$ von Λ^*. Wähle $\widetilde{b}, \widetilde{b}_2, \ldots, \widetilde{b}_n$ als zugehörige polare Basis von Λ. Dann gilt

$$\langle b, \widetilde{b} \rangle = 1 \qquad\qquad \langle b, \widetilde{b}_i \rangle = 0$$

Das heißt, gemessen am Ergebnis der Skalarprodukte haben alle Hyperebenen Abstand 1.

4.9 Proposition. *Sei $K \in \mathcal{K}^n$, $\Lambda \in \mathcal{L}^n$.*

$$W_\Lambda(K) = \lambda_1((K - K)^*, \Lambda^*)$$
$$\mu(K,\Lambda) W_\Lambda(K) \leq c \cdot n^{\frac{7}{2}}$$

Beweis. Angenommen,$L \in \mathcal{K}_0^n$, dann ist $y \in \rho L \Leftrightarrow \forall x \in L. \langle y, x \rangle \leq \rho$.
Sei b beliebig. Setze $\rho := \max\{\langle b, v \rangle : v \in K - K\}$. Dann ist $b \in \rho(K - K)^*$, also $|b|_{(K-K)^*} \leq \rho$.

Weiterhin ist

$$|b|_{(K-K)^*} = \rho \implies b \in \rho(K-K)^* \implies \forall v \in K-K. \langle b, v\rangle \leq \rho \implies \max_{v\in K-K} \langle b, v\rangle \leq \rho$$

Somit ist

$$W_\Lambda(K) = \min_{0\neq b\in\Lambda^*} \max_{v\in K-K} \langle b, v\rangle = \min_{0\neq b\in\Lambda^*} |b|_{(K-K)^*} = \lambda_1((K-K)^*, \Lambda^*)$$

(Beachte, dass das $\max - \min$ aus der Definition einfließt in $K-K$, da wir beide Teile separat optimieren.)

$$\begin{aligned}
\mu(K,\Lambda)W_\Lambda(K) = \mu(K,\Lambda)\lambda_1((K-K)^*,\Lambda^*) &\overset{4.4}{\leq} \left(\sum_{i=1}^n \lambda_i(K-K,\Lambda)\right)\lambda_1((K-K)^*,\Lambda^*) \\
&= \sum_{i=1}^n \lambda_i(K-K,\Lambda)\lambda_1((K-K)^*,\Lambda^*) \leq n\lambda_n(K-K,\Lambda)\lambda_1((K-K)^*,\Lambda^*) \\
&\overset{4.5}{\leq} cn\cdot n^{\frac{5}{2}}
\end{aligned}$$

□

4.10 Korollar (Flatness Theorem). *Sei $K \in \mathcal{K}^n$, $\Lambda \in \mathcal{L}^n$ mit $K \cap \Lambda = \emptyset$. Dann ist $W_\Lambda(K) \leq c\cdot n^{\frac{7}{2}}$.*

Beweis. Wegen $K\cap\Lambda = \emptyset$ ist $\mu(K,\Lambda) > 1$ und wir sind fertig mit Proposition 4.9. □

4.11 Notation. Sei $\rho_t : \mathbb{R}^n \to \mathbb{R}$ gegeben durch $\rho_t(x) = e^{-\pi\left(\frac{x}{t}\right)^2}$ Sei $v \in \mathbb{R}^n$. Für Teilmengen $\subseteq v+\Lambda$ setze $\rho_t(S) := \sum_{x\in S}\rho_t(x)$.

4.12 Lemma. *Sei $\Lambda \in \mathcal{L}^n$ und $u \in \mathbb{R}^n$.*

1. $\rho_t(\Lambda) = \det\Lambda^* t^n \rho_{1/t}(\Lambda^*)$.
2. $\rho_t(\Lambda) \leq t^n\rho_1(\Lambda)$ *für* $t \geq 1$.
3. $\rho_t(u+\Lambda) = \det\Lambda^* t^n \sum_{y\in\Lambda^*}\rho_{1/t}(y)e^{2\pi i\langle y,u\rangle}$
4. $\rho_t(u+\Lambda) \leq \rho_t(\Lambda)$

Beweis. Nach **??** ist

$$\sum_{x\in\Lambda} f(x) = \det\Lambda^* \sum_{y\in\Lambda^*}\widehat{f}(y)$$

Nach Bemerkung 2.21 ist $\widehat{\rho}_t(y) = t^n\rho_{1/t}(y)$ und mit **??** folgt item 1.
Mit item 1 haben wir nun

$$\rho_t(\Lambda) = \det\Lambda^* t^n\rho_{1/t}(\Lambda^*) \overset{t\geq 1}{\leq} \det\Lambda^* t^n\rho_1(\Lambda^*) \overset{1}{=} \det\Lambda^* t^n \det\Lambda\rho_1(\Lambda) = t^n\rho_1(\Lambda)$$

Sei $g(x) = \rho_t(x+u)$. Dann ist

$$\widehat{g}(y) = \int_{\mathbb{R}^n} e^{-\pi\left|\frac{1}{t}(x+u)\right|^2} e^{-2\pi i\langle x,y\rangle}\mathrm{d}x = e^{2\pi i\langle u,y\rangle}\cdot\int_{\mathbb{R}^n} e^{-\pi\left|\frac{1}{t}(x+u)\right|^2} e^{-2\pi i\langle x+u,y\rangle}\mathrm{d}x = e^{2\pi i\langle u,y\rangle}\widehat{\rho}_t(y)$$

Mit **??** erhalten wir daraus

$$\rho_t(u+\Lambda) = \sum_{x\in\Lambda} g(x) = \det\Lambda^* \sum_{y\in\Lambda^*} \widehat{g}(y) = \det\Lambda^* t^n \sum_{y\in\Lambda^*} e^{2\pi i\langle u,y\rangle}\rho_{1/t}(y)$$

Für den letzten Teil nehmen wir die Dreiecksungleichung

$$\rho_t(u+\Lambda) \le \det\Lambda^* t^n \sum_{y\in\Lambda^*} \left|e^{2\pi i\langle u,y\rangle}\right| \cdot \left|\rho_{1/t}(y)\right| = \det\Lambda^* t^n \sum_{y\in\Lambda^*} \rho_{1/t}(y) \overset{1}{=} \rho_t(\Lambda)$$

□

4.13 Lemma. *Sei $u \in \mathbb{R}^n$. dann gilt*

$$\rho_1\left(\left\{v \in u+\Lambda : |v| > \sqrt{n}\right\}\right) \le 2^{-n}\rho_1(\Lambda)$$

Beweis.

$$2^n\rho_1(\Lambda) \ge \rho_2(u+\Lambda) \ge \rho_2\left(\left\{v \in u+\Lambda : |v| > \sqrt{n}\right\}\right) = \sum_{v\in u+\Lambda, |v|>\sqrt{n}} e^{-\pi\frac{|v|^2}{4}} = \sum_{v\in u+\Lambda, |v|>\sqrt{n}} e^{-\pi|v|^2} e^{\frac{3}{4}\pi|v|^2} \ge e^{\frac{3}{4}\pi n}$$

□

4.14 Korollar. *Sei $\Lambda \in \mathcal{L}^n$ mit $\lambda_1(B_n,\Lambda) > \sqrt{n}$. Dann gilt*

$$\forall u \in \mathbb{R}^n. \left|\frac{\rho_1(u+\Lambda^*)}{\det\Lambda} - 1\right| \le 2^{-n+1}$$

Das heißt, die Funktion (in Abhängigkeit von u) ist nahezu konstant. Insbesondere ist

$$\frac{\rho_1(\Lambda^*)}{\rho_1(u+\Lambda^*)} \le \frac{1+2^{-n+1}}{1-2^{-n+1}} \le 3$$

Beweis. Es ist $\Lambda \setminus \{0\} = \{v \in L : |v| > \sqrt{n}\}$. Nach Lemma 4.13 mit $u = 0$ folgt

$$\rho_1(\Lambda\setminus\{0\}) \le 2^{-n}\rho_1(\Lambda) = 2^{-n}\left(1+\rho_1(\Lambda\setminus\{0\})\right) \le 2^{-n} + \frac{1}{2}\rho_1(\Lambda\setminus\{0\})$$

und damit $\rho_1(\Lambda\setminus\{0\}) \le 2^{-n+1}$. Daraus folgt

$$\rho_1(\Lambda^*) \overset{3}{=} \det\Lambda \sum_{y\in\Lambda} \rho_1(y)e^{2\pi i\langle y,u\rangle} = \det\Lambda\left(1 + \sum_{y\in\Lambda\setminus\{0\}} \rho_1(y)e^{2\pi i\langle y,u\rangle}\right) \implies \left|\frac{\rho_1(u+\Lambda^*)}{\det\Lambda}\right|$$

Stück fehlt, zu schnell abgewischt

□

4.15 Satz. *Sei $\Lambda \in \mathcal{L}^n$. Dann ist $\lambda_1(B_n,\Lambda)\mu(B_n,\Lambda^*) \le n$.*

Beweis. Schreibe kurz $\lambda_1 = \lambda_1(B_n,\Lambda)$ und $\mu^* = \mu(B_n,\Lambda^*)$. Angenommen $\lambda_1\mu > n$. Durch Skalierung können wir oBdA annehmen $\lambda_1, \mu^* > \sqrt{n}$. Damit existiert ein $v \in \mathbb{R}^n$ mit $\forall b^* \in \Lambda^*. |b^* - v| > \sqrt{n}$. Daraus folgt

$$\rho_1(-v+\Lambda^*) = \rho_1\left(\left\{u \in -v+\Lambda^* : |u| \ge \sqrt{n}\right\}\right) \overset{4.13}{\le} 2^n\rho_1(\Lambda^*) \overset{4.14}{\le} 2^n \cdot 3\rho_1(-v+\Lambda^*) \overset{n\ge 2}{<} \rho_1(-v+\Lambda^*) \quad ↯$$

□

4.16 Korollar. *Sei $\Lambda \in \mathcal{L}^n$ und $K \in \mathcal{K}_0^n$.*

1. $\lambda_1(B_n, \Lambda)\lambda_n(B_n, \Lambda^*) \leq 2n$
2. $\lambda_1(K, \Lambda)\mu(K^*, \Lambda^*) \leq 2n^{\frac{3}{2}}$
3. $\lambda_1(K, \Lambda)\lambda_n(K^*, \Lambda^*) \leq 4n^{\frac{3}{2}}$
4. *Sei $L \in \mathcal{K}^n$ mit $L \cap \Lambda = \emptyset$. Dann ist $w_\Lambda(L) \leq 2n^2$.*

Anmerkung: Die beste bekannte Schranke ist $n^{\frac{4}{3}} \cdot (\log n)^c$, vermutet wird n (was eine untere Schranke ist).

5 Packungen

5.1 Definition. $D \subseteq \mathbb{R}^n$ heißt *Packung* von $K \in \mathcal{K}^n$,falls $\forall x, y \in D.(x+\mathrm{int}(K)) \cap (y+\mathrm{int}(K)) = \emptyset$. Die Menge aller Packungen ist $\mathcal{P}(K)$.

Rest fehlt

5.2 Proposition. *Sei $K \in \mathcal{K}^n$.*

1. $0 < \delta(K) \leq 1$.
2. $\delta(t + AK) = \delta(K)$ *für beliebige $A \in \mathrm{GL}(n, \mathbb{R})$ und $t \in \mathbb{R}^n$. Das heißt, die Packungsdichte ist affin invariant.*
3. *Sei $K \in \mathcal{K}_0^n$. Dann ist*
$$D \in \mathcal{P}(K) \Leftrightarrow \forall x, y \in D.|x - y|_K \geq 2 \Leftrightarrow \forall x, y \in D.(x + \mathrm{int}(K)) \cap (y + \mathrm{int}(K)) = \emptyset$$
4. *Sei $D \in \mathcal{P}(K)$. Dann ist*
$$\delta(D, K) = \limsup_{\lambda \to \infty} \frac{\mathrm{vol}(K) \cdot \#(D \cap \lambda[-1, 1]^n)}{\mathrm{vol}(\lambda[-1, 1]^n)}$$
5. $\mathcal{P}(K) = \mathcal{P}\left(\frac{1}{2}(K - K)\right)$ *und für $D \in \mathcal{P}(K)$ gilt*
$$\delta(D, K) = \delta\left(\frac{1}{2}(K - K), D\right) \cdot \frac{\mathrm{vol}(K)}{\mathrm{vol}\left(\frac{1}{2}(K - K)\right)} \implies \delta(K) = \delta\left(\frac{1}{2}(K - K)\right) \frac{\mathrm{vol}(K)}{\mathrm{vol}\left(\frac{1}{2}(K - K)\right)}$$

Beweis. Teil (i)-(iii) klar. Setze $C_n := [-1, 1]^n$ (für „cube“).

4. Nach Definition ist
$$\delta(D, K) = \limsup_{\lambda \to \infty} \mathrm{vol}(K) \frac{\#\{x \in D : x + K \subset \lambda C_n\}}{\mathrm{vol}(\lambda C_n)}$$
Sei $\gamma > 0$, $K, K - K \subset \gamma C_n$ und für $\lambda > \gamma$ sei
$$m_1(\lambda) := \#\{X \in D : x + K \subset \lambda C_n\} \qquad m_1(\lambda) := \#\{X \in D : x \subset \lambda C_n\}$$

Sei $x \in D$ mit $x + K \subset \lambda C_n$, aber $x \notin \lambda C_n$. Dann gilt $x + K \subset \lambda C_n \setminus (\lambda - \gamma)C_n$, weil

$(x + K) \cap (\lambda - \gamma)C_n \neq \emptyset \implies \exists v \in K. x + v \in (\lambda - \gamma)C_n \implies x \in -v + (\lambda - \gamma)C_n \subset \gamma C_n + (\lambda - \gamma$

Daraus folgt

$\operatorname{vol}(K)m_1(\lambda) \leq m_2(\lambda)\operatorname{vol}(K) + (\lambda^n - (\lambda - \gamma)^n)\operatorname{vol}(C_n) \leq \operatorname{vol}(K)m_2(\lambda) + \lambda^{n-1}\overline{c}(n,\gamma)\operatorname{vol}(C_n)$

Im Grenzwert verschwindet der zweite Summand.
Angenommen $x \in D \cap \lambda C_n$, aber $x + K \nsubseteq \lambda C_n$. Dann gilt $x + K \subset (\lambda + \gamma)C_n \setminus (\lambda - \gamma)C_n$.

$\operatorname{vol}(K)m_2(\lambda) \leq m_1(\lambda)\operatorname{vol}(K) + ((\lambda + \gamma)^n - (\lambda - \gamma)^n)\operatorname{vol}(C_n) \leq \operatorname{vol}(K)m_1(\lambda) + \lambda^{n-1}\widetilde{c}(n,\gamma)\operatorname{vol}(C_n)$

Erneut ist der zweite Summand im Grenzwert irrelevant.
Zusammen ergeben beide Ungleichungen

$$-\frac{\widetilde{c}(n,\gamma)}{\lambda}\frac{\operatorname{vol}(K)m_1(\lambda)}{\operatorname{vol}(\lambda C_n)} - \frac{\operatorname{vol}(K)m_2(\lambda)}{\operatorname{vol}(\lambda C_n)} \leq \frac{\overline{c}(n,\gamma)}{\lambda}$$

Für $\lambda \to \infty$ ergibt sich Gleichheit.

5. Wir haben

$$(x + \operatorname{int}(K)) \cap (y + \operatorname{int}(K)) \neq \emptyset \Leftrightarrow x - y \in \operatorname{int} K - \operatorname{int} K = \operatorname{int}(K - K) = \frac{1}{2}\operatorname{int}(K - K) - \frac{1}{2}\operatorname{int}(K$$
$$\Leftrightarrow \left(x + \frac{1}{2}\operatorname{int}(K - K)\right) \cap \left(y + \frac{1}{2}\operatorname{int}(K - K)\right) \neq \emptyset \implies$$

Damit erhalten wir

$$\delta(K, D) \stackrel{1}{=} \limsup_{\lambda \to \infty} \frac{\operatorname{vol}(K)\#(\cap \lambda C_n)}{\operatorname{vol}(\lambda C_n)} = \frac{\operatorname{vol}(K)}{\operatorname{vol}\left(\frac{1}{2}(K - K)\right)} \limsup_{j \to \infty} \frac{\operatorname{vol}\left(\frac{1}{2}(K - K)\right)\#(D \cap \lambda C_n)}{\operatorname{vol}(\lambda C_n)} = \frac{\operatorname{vo}}{\operatorname{vol}\left(\frac{1}{2}(\right.}$$

□

5.3 Lemma. *Sei $S \subset \mathbb{R}^n$ beschränkt, messbar und $\operatorname{vol}(S) > 0$. Sei $D \in \mathcal{P}(K)$. Dann existieren $v, w \in \mathbb{R}^n$ mit*

$$\frac{\operatorname{vol}(K)\#((w + S) \cap D)}{\operatorname{vol}(S)} \leq \delta(K, D) \leq \frac{\operatorname{vol}(K)\#((v + S) \cap D)}{\operatorname{vol}(S)}$$

Beweis. Betrachte die obere Schranke, die untere folgt analog. Sei $\gamma > 0$ mit $S \subset \gamma C_n$ und sei $\varepsilon(\lambda) \in \mathbb{R}$ mit $\varepsilon(\lambda) \to 0$ für $\lambda \to \infty$ und

$$\varepsilon(\lambda) + \frac{\delta(K,)}{\operatorname{vol}(K)} = \frac{\#(D \cap \lambda C_n)}{\operatorname{vol}(\lambda C_n)}$$

Sei $x \in D \cap \lambda C_n$. Dann ist

$$-\{v \in \mathbb{R}^n : x \in v + S\} - x - S \subset (\lambda + \gamma)C_n$$
$$\implies \int_{(\lambda+\gamma)C_n} \#\left((v + S) \cap (D \cap \lambda C_n)\right) \mathrm{d}v = \operatorname{vol}(S)\#(C \cap \lambda C_n)$$

Die letzte Gleichheit erhalten wir, indem wir die charakteristische Funktion $\chi_x(v+S)$ betrachten und dann

$$\int_{(\lambda+\gamma)C_n} \left(\sum_{x \in D \cap \lambda C_n} \chi_x(v+S) \right) \mathrm{d}v = \sum_{x \in D \cap \lambda C_n} \left(\int_{(\lambda+\gamma)C_n} \chi_x(v+S) \mathrm{d}v \right) = \sum_{X \in D \cap \lambda C_n} \mathrm{vol}(x-S)$$

Daraus folgt, ex existiert ein $v_\lambda \in \mathbb{R}^n$ mit

$$\#\left((v_\lambda + S) \cap (D \cap \lambda C_n)\right) \geq \frac{\mathrm{vol}(S)\#(D \cap \lambda C_n)}{\mathrm{vol}((\lambda+\gamma)C_n)} \mathrm{vol}(S) \frac{\#(D \cap \lambda C_n)}{\mathrm{vol}(\lambda C_n)} \left(\frac{\lambda}{\lambda+\gamma} \right)^n$$

Mit item 5 eralten wir

$$\#\left((v_\lambda + S) \cap D \cap \lambda C_n\right) \geq \frac{\delta(K,D)\,\mathrm{vol}(S)}{\mathrm{vol}(K)} + \varepsilon(\lambda)\,\mathrm{vol}(S) + \left(1 - \frac{\gamma}{\lambda+\gamma}\right)^n = \frac{\delta(K,D)\,\mathrm{vol}(S)}{\mathrm{vol}(K)} + \widetilde{\varepsilon}(\lambda)$$

mit $\widetilde{\varepsilon}(\lambda) \to 0$ für $\lambda \to \infty$. Da $\#\left((v_\lambda + S) \cap D \cap \lambda C_n\right) \in \mathbb{N}$, gibt es ein $\overline{\lambda} \in \mathbb{R}$ mit

$$\#\left((v_{\overline{\lambda}} + S) \cap D \cap \overline{\lambda} C_n\right) \geq \frac{\delta(K,D)\,\mathrm{vol}(S)}{\mathrm{vol}(K)}$$

□

5.4 Bemerkung. Sei $K \in \mathcal{K}^n$. Der Wert

$$R(K) = \min\{R > 0 : \exists x \in \mathbb{R}^n . K \subseteq x + RB_n\}$$

heißt Umkugelradius. Der zugehörige Wert $t \in \mathbb{R}^n$ mit $K \subseteq t + R(K)B_n$ heißt Umkugelmitelpunkt. Analog für die Inkugel.
Es existiert ein $k \in \{1, \ldots, n+1\}$ und $x_1, \ldots, x_{k+1} \in \mathrm{bd}(K) \cap (t + R(K) \cdot \mathrm{bd}(B_n))$ (Kontaktpunkte von Körper und Kugel) und $\lambda_i > 0$ mit

$$t = \dim_{i=1}^{k+1} \lambda_i x_i \qquad\qquad \sum \lambda_i = 1$$

Das heißt, wir haben Kontaktpunkte, die einen Simplex bilden und der Mittelpunkt ist eine konvexe Kombination dieser Kontaktpunkte.

5.5 Satz. *1. Für $K \in \mathcal{K}_0^n$ ist $\delta(K) \geq 2^{-n}$.*

2. $\delta(B_n) \leq (n+1)\sqrt{2}^{-n}$. (Die beste bekannte Schranke liegt bei $2^{-(0.5991+o(1))n}$.)

Beweis. 1. Sei D_S eine Packungsmenge so, dass für alle $x \in \mathbb{R}^n$ gilt $(x+K) \cap (D_S + K) \neq \emptyset$. (Diese Packung heißt saturiert, es passt nichts mehr dazu.) Damit haben wir

$$\forall x \in \mathbb{R}^n . (x + (K-K)) \cap D_S \neq \emptyset \Leftrightarrow \forall x \in \mathbb{R}^n . (x + 2K) \cap D_S \neq \emptyset$$

Nun nutzen wir Lemma 5.3 mit $S = 2K$ und $D = D_S$. Dann existiert ein $w \in \mathbb{R}^n$ mit

$$\delta(K, D_S) \geq \frac{\mathrm{vol}(K)\#\left((w+2K) \cap D_S\right)}{\mathrm{vol}(2K)} \geq \frac{\mathrm{vol}(K)}{\mathrm{vol}(2K)} = 2^{-n}$$

da wir die Mächtigkeit des Schnitts mit 1 abschätzen können.

2. Für $r > 0$ sei $f(r,n) = \max\{\#(D \cap \mathrm{int}(rB_n)) : D \in \mathcal{P}(B_n)\}$.

□

Bemerkung. Der Umkugelradius vom regelmäßigen Simplex ist $\sqrt{2} \cdot \sqrt{\frac{n}{n+1}}$.

Vorlesung fehlt

5.6 Satz (Auswahlsatz von Mahler). *Seien $\Lambda_m \in \mathcal{L}^n$ für $m \in \mathbb{N}$ und seien $p_1, p_2 \in B_0$ mit $\det \Lambda_m \leq p_1$ und $\lambda_1(B_n, \Lambda_m) \geq p_2$. Dann gibt es eine Teilfolge $(\Lambda_{m_i})_{i \in \mathbb{N}}$, die konvergiert.*

Beweis. Nach Korollar 3.21 hat Λ_m eine Basis $b_1^{(m)}, \ldots, b_n^{(m)}$ mit $\prod |b_i|^{m)}| \leq c_n \det \Lambda_m$, wobei c_n eine Konstante ist, die nur von m abhängt. Ordne $|b_j^{(m)}| \leq |b_{j+1}^{(m)}|$. Dann gilt

$$\lambda_1(B_n, \Lambda_m)^{i-1} |b_i^{(m)}|^{n-i+1} \leq c_m \det \Lambda_m \implies |b_i^{(m)}| \leq \widetilde{c}_n \det \Lambda_m \leq \widetilde{c}_n$$

Nach Bolzano-Weierstraß (eine beschränkte Folge hat eine konvergente Teilfolge), haben wir nun Grenzwerte $b_i^{(m_j)} \to b_i \in \mathbb{R}^n$ für $j \to \infty$. Sei $\Lambda = \operatorname{lin}_{\mathbb{Z}}\{b_1, \ldots, b_n\}$. Damit gilt

$$\left| \left(b_1^{(m_j)}, \ldots, b_n^{(m_j)} \right) - (b_1, \ldots, b_n) \right|_1 \xrightarrow{j \to \infty} 0$$

evtl. fehlt ein Stück

Wegen $\det \Lambda_{m_j} \xrightarrow{j \to \infty} |\det(b_1, \ldots, b_n)|$ folgt $|\det(b_1, \ldots, b_n)| > 0$, also $\Lambda \in \mathcal{L}^n$ mit $\Lambda_m \to \Lambda$. $\square$

5.7 Definition. sei $K \in \mathcal{K}_0^n$. Ein Gitter $\Lambda \in \mathcal{L}^n$ heißt $k$zulässig, falls $\operatorname{int}(K) \cap \Lambda = \{0\}$. Schreibe $\delta(K) := \inf\{\det \Lambda : \Lambda \text{ ist } K\text{-zulässig}\}$ heißt kritische Determinante von K.

Es gilt Λ is K-zulässig, genau dann, wenn $2\Lambda \in \mathcal{P}(K)$. Um dies zu sehen:

$$(2a + \operatorname{int}(K)) \cap (2\overline{a} + \operatorname{int}(K)) = \emptyset \Leftrightarrow 2(a - \overline{a}) \in \operatorname{int}(2K) \Leftrightarrow (a - \overline{a}) \in \operatorname{int}(K) \overset{\operatorname{int}(K) \cap \Lambda = 0}{\Leftrightarrow} a = \overline{a}$$

5.8 Proposition. *sei $K \in \mathcal{K}_0^n$. Es gibt ein K-zulässiges Gitter Λ_K mit $\det \Lambda_K = \Delta(K)$. (Dieses Λ_K heißt kritisches Gitter.)*

Beweis. Sei Λ K-zulässig mit $\det \Lambda = p_1$. Weiterhin sei $p_2 B_n \subseteq K$. Dann folgt $\lambda_1(B_n, \Lambda) \geq p_2$ für Λ K zulässig. Damit ist

$$\Delta(K) = \inf\{\det \Lambda : \Lambda \text{ ist } K\text{-zulässig}, \lambda_1(B_n, \Lambda) \geq p_2, \det \Lambda \leq p_1\}$$

Nach Satz 5.6 existiert eine konvergente Folge $(\Lambda_m)_{m \in \mathbb{N}}$ von K-zulässigen Gittern mit $\Lambda_m \to \Lambda_K$ und $\det \Lambda_m \to, \Delta(K)$,also $\det \Lambda_K = \delta(K)$. $\square$

5.9 Proposition. *Sei $K \in \mathcal{K}_0^n$. Dann gilt*

1. $\delta_y(K) = \frac{\operatorname{vol}(K)}{2^n \Delta(K)}$
2. $\operatorname{vol}(K) \leq 2^n \Delta(K)$.
3. *Für $\Lambda \in \mathcal{L}^n$ gilt $\lambda_1(K, \Lambda)^n \Delta(K) \leq \det \Lambda$ Dies ist äquivalent zu:*

Beweis. 1. klar

2. Nach Theorem 3.16 gilt $\lambda_1(K, \Lambda_K)^n \operatorname{vol}(K) \leq 2^n \det \Lambda_K$.

3. Dies ist äquivalent zu $\Delta(K) \leq \det\left(\frac{1}{\lambda_1(K,\Lambda)}\Lambda\right)$ und dies ist ein K-zulässiges Gitter. Weiterhin ist $\lambda_1(K, \frac{1}{\lambda_1}\Lambda) = 1$.

$\square$

5.10 Bemerkung (Vermutung von Davenport). Aus Proposition 5.9 erhalten wir

$$\lambda_1(K,\lambda)^n \operatorname{vol}(K) \leq \delta_Y(K) 2^n \det \Lambda$$

Dies führt zur Vermutung von Davenport:

$$\lambda_1(K,\Lambda) \cdot \ldots \cdot \lambda_n(K,\Lambda)\Delta(K) \leq \det \Lambda$$

5.12 Satz (Minkowski-Hlavka,1943). *Sei $S \subseteq \mathbb{R}^n$ eine beschränkte Jordan-messbare Menge mit $\operatorname{vol}(S) < 1$. Dann existiert ein $\Lambda \in \mathcal{L}^n$ mit $\det \Lambda = 1$ und $S \cap \Lambda \setminus \{0\} = \emptyset$.*

Beweis. Es existiert eine Primzahl p mit

1. $\frac{1}{p^{n-1}} \# \left(S \cap \frac{1}{p^{\frac{n-1}{n}}\mathbb{Z}^n}\right) < 1$
2. $S \subset \{x \in \mathbb{R}^n : \forall i. |x_i| < \sqrt[n]{p}\}$

Das erste sagt einfach, dass wir ein hinreichend feines Würfelgitter in S nehmen (wie bei der Volumenbestimmung).
Angenommen, es gibt p^{n-1} Untergitter Λ_i von $\mathbb{Z}^n$ mit $\det \Lambda_i = p^{n-1}$ so, dass 0 der einzige paarweise gemeinsame Punkt ist. Nach item 1 gilt nun

$$p^{n-1} > \# \left(S \cap \frac{1}{p^{\frac{n-1}{n}}\mathbb{Z}^n} \setminus \{0\}\right) \geq \sum_{i=1}^{p^{n-1}} \# \left(S \cap \underbrace{\frac{1}{p^{\frac{n-1}{n}}}\Lambda_i}_{\det=1} \setminus \{0\}\right)$$

Nach Mittelwertsatz existiert ein Λ_i mit $\# \left(S \cap \frac{1}{p^{\frac{n-1}{n}}}\Lambda_i \setminus \{0\}\right) = 0$.
Nun müssen wir noch Gitter mit der obigen Eigenschaft finden. Sei

$$U_p = \{u \in \mathbb{Z}^n : u_1 = 1, \forall 2 \leq i \leq n. 0 \leq u_i < p\}$$

Für$u \in U_p$ sei

$$\Lambda(u) = \operatorname{lin}_{\mathbb{Z}}\{u, pe_2, \ldots, pe_n\}$$

Damit ist $\det \Lambda(u) = p^{n-1}$. Da $u_1 = 1$, gilt

$$z \in \Lambda(u) \Leftrightarrow \forall i = 2, \ldots, m. z_i \equiv z_i u_i \mod p$$

sowie

$$\Lambda(u) \ni m_1 u + \sum_{i=2}^{n} m_i p e_i = z \Leftrightarrow z_1 = m_1, \forall i \geq 2. z_i = z_1 u_i + m_i p$$

Behauptung. *Seien $u, \overline{u} \in U : p$ mit $u \neq \overline{u}$. Dann gilt*

$$\Lambda(u) \cap \Lambda(\overline{u}) \subset \{0\} \cup \{x \in \mathbb{R}^n : \exists x_i. |x_i| \geq p\}$$

Beweis. Sei $z \in \Lambda(u) \cap \Lambda(\overline{u})$. Dann gilt $z_1(u_i - \overline{u}_i) \equiv 0 \mod p$. Wegen $-(p-1) \leq u_i - \overline{u}_i \leq p-1$, und $u_i \neq \overline{u}_i$ muss also $z_1 \equiv 0 \mod p$. Mit $z_i \neq 0$ folgt $|z_i| \geq p$ und wir sind fertig. Andernfalls ist z_0 und somit $z_i = m_i p$ also $z \equiv \mathbf{0} \mod p$. Damit ist $z = \mathbf{0}$ oder $\exists i.|z_i| \geq p$. □

Das heißt, die Mengen $S \cap \frac{1}{p^{\frac{n-1}{n}}}\Lambda(u) \setminus \{0\}$ für $u \in U_p$ sind paarweise disjunkt. Daraus folgt

$$p^{n-1} > \#\left(S \cap \frac{1}{p^{\frac{n-1}{n}}}\mathbb{Z}^n\right) \geq \sum_{u \in U_p} \#\left(S \cap \Lambda(u) \setminus \{0\}\right)$$

Somit existiert ein $\widetilde{u} \in U_p$ mit

$$\#\left(S \cap \frac{1}{p^{\frac{n-1}{n}}}\Lambda(\widetilde{u}) \setminus \{0\}\right) = 0$$

□

Als Konsequenz aus dem Satz haben wir $\delta_Y(K) \geq \zeta(n) \cdot 2^{-(n-1)}$.

5.13 Definition. 1. Für $s > 1$ setze $\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$.

2. Sei $m \in \mathbb{N}$. Die Möbius-Funktion ist

$$\mu(m) = \begin{cases} 0 & : \exists a.a^2 \mid m \\ 1 & : m = 1 \\ (-1)^k & : m = p_1 \cdot \ldots \cdot p_k, p_i \in \mathbb{P} \end{cases}$$

5.14 Proposition. *1. Für $k \in \mathbb{N}_+$ gilt*

$$\sum_{m|k} \mu(m) = \begin{cases} 0 & : k > 1 \\ 1 & : k = 1 \end{cases}$$

2. Für $n \geq q2$ gilt

$$\sum_{m=1}^{\infty} \frac{\mu(m)}{m^n} = \frac{1}{\zeta(n)}$$

Beweis. 1. Sei $k = \prod_{i=1}^{l} p_i^{n_i} \geq 2$ die Primfaktorzerlegung. Dann ist

$$\sum_{m|k} \mu(m) = 1 + \sum_{i=1}^{l} \mu(p_i) + \sum_{1 \leq i < j \leq l} \mu(p_i p_j) + \ldots + \mu(p_1 \ldots p_l) = \binom{l}{0} - \binom{l}{1} + \ldots \pm \binom{l}{l} = (0-0)^l =$$

2. Multipliziere mit $\zeta(n)$, dann haben wir

$$\zeta(n) \sum_{m=1}^{\infty} \frac{\mu(m)}{m^n} = \sum_{k=1}^{\infty} \frac{1}{k^n} \sum_{m=1}^{\infty} \frac{\mu(m)}{m^n} = \sum_{k,m=1}^{\infty} \frac{\mu(m)}{(km)^n} = \sum_{l=1}^{\infty} \frac{1}{l^n} \sum_{j|k} \mu(j) \stackrel{1}{=} 1$$

□

5.15 Notation. Sei $\Lambda \in \mathcal{L}^n$. Setze

$$\Lambda^0 := \{b \in \Lambda \setminus \{0\} : [0, b] \cap \Lambda = \{0, b\}\}$$

die Menge der primitiven Gitterpunkte.

5.16 Proposition. *Sei $\Lambda \in \mathcal{L}^n$ und $f : \mathbb{R}^n \to \mathbb{R}$ mit $f(x) = 0$ für $|x| \geq R$ (das heißt, außerhalb eines gewissen bereichs verschwindet die unktion). Dann gilt*

$$\sum_{b \in \Lambda^0} f(b) = \sum_{m=1}^{\infty} \mu(m) \sum_{b \in \Lambda \setminus \{0\}} f(mb)$$

Beweis. Es gilt

$$\begin{aligned}
\sum_{b \in \Lambda^0} f(b) &\overset{1}{=} \sum_{b \in \Lambda^0} \sum_{k=1}^{\infty} \sum_{m|k} \mu(m) \\
&= \sum_{b \in \Lambda^0} \left(\sum_{m=1}^{\infty} \mu(m) \sum_{l=1}^{\infty} f(mlb) \right) \\
&= \sum_{m=1}^{\infty} \mu(m) \sum_{b \in \Lambda^0} \sum_{l=1}^{\infty} f(mlb) \\
&= \sum_{m=1}^{\infty} \mu(m) \sum_{b \in \Lambda^0 \setminus \{0\}} f(mb)
\end{aligned}$$

□

5.17 Lemma. *Sei $\Lambda \in \mathcal{L}^n$, $n \geq 2$ und sei $f : \mathbb{R}^n \to \mathbb{R}$ Riemann-integrierbar mit $f(x) = 0$ für $|x| \geq R$. dann gilt*

$$\lim_{m \to \infty} \frac{\det \Lambda}{m^n} \sum_{b \in \frac{1}{m}\Lambda^0} f(b) = \frac{1}{\zeta(n)} \int_{\mathbb{R}^n} f(x) \mathrm{d}x$$

Beweis. Nach Proposition 5.16 und item 2 gilt

$$\begin{aligned}
\frac{\det \Lambda}{m^n} \sum_{b \in \frac{1}{m}\Lambda^0} f(b) &= \sum_{k=1}^{\infty} \mu(k) \sum_{b \in \frac{1}{m}\Lambda \setminus \{0\}} \frac{\det \Lambda}{m^n} f(bk) \\
&= \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \sum_{b \in \Lambda \setminus \{0\}} \det \Lambda \left(\frac{k}{m}\right)^n f\left(\frac{k}{m} b\right) \\
&= \sum_{k=1}^{\infty} \frac{\mu(k)}{k^n} \left(\int_{\mathbb{R}^n} f(x) \mathrm{d}x + \varepsilon(k,m) \right) && \varepsilon \text{ - Fehler}
\end{aligned}$$

$$\frac{1}{\zeta(n)} \int_{\mathbb{R}^n} f(x) \mathrm{d}x + \sum_{k=1}^{\infty} \frac{\mu(k)}{k^n} \varepsilon(k,m)$$

mit $\varepsilon(k,m) \to 0$ für $\frac{k}{m} \to 0$. Nach Voraussetzungen (f verschwindet für große Argument) gibt es eine Konstante c mit $|\varepsilon(k,m)| \leq c$ für alle $k, m \in \mathbb{N}$. Sei $\varepsilon > 0$ und $k(\varepsilon) \in \mathbb{N}$ mit

$$\sum_{k=k(\varepsilon)}^{\infty} \frac{1}{k^n} < \frac{\varepsilon}{c}$$

und sei $m(\varepsilon) \in \mathbb{N}$ so, dass

$$\forall k \leq k(\varepsilon). \forall m \geq m(\varepsilon). \, |\varepsilon(k,m)| \leq \frac{\varepsilon}{k(\varepsilon)}$$

Daraus erhalten wir

$$\left|\frac{\det\Lambda}{m^n}\sum_{b\in\frac{1}{m}\Lambda^0} f(b) - \frac{1}{\zeta(n)}\int_{\mathbb{R}^n} f(x)\mathrm{d}x\right| = \left|\sum_{k=1}^{\infty}\frac{\mu(k)}{k^n}\varepsilon(k,m)\right| \leq \left|\sum_{k=1}^{k(\varepsilon)}\frac{\mu(k)}{k^n}\varepsilon(k,m)\right| + \varepsilon \leq 2\varepsilon$$

□

5.18 Definition. Sei $\emptyset \neq S \subseteq \mathbb{R}^n$.

1. S heißt Strahlenmenge, falls $\lambda x \in S$ für alle $x \in S$, $\lambda \in [0,1]$.
2. S heißt Strahlenkörper falls S eine 0-symmetrische abgeschlossene Strahlenmenge ist und $\lambda x \in \operatorname{int} S$ für alle $x \in S$, $\lambda \in [0,1)$. (Insbesondere muss S volldimensional sein.)

5.19 Korollar. *Sei S eine beschränkte Jordan-messbare Menge.*

1. *Ist S eine Strahlenmenge mit* $\operatorname{vol}(S) < \zeta(n)$ *oder*
2. $S = -S$ *mit* $\operatorname{vol}(S) > 2$ *oder*
3. *S ist Sternkörper mit* $\operatorname{vol}(S) < 2\zeta(n)$

Dann existiert ein $\Lambda \in \mathcal{L}^n$ mit $\det\Lambda = 1$ *und* $S \cap \Lambda \setminus \{0\} = \emptyset$.

Beweis. 1. Für Strahlenmengen S gilt

$$S \cap \Lambda \setminus \{0\} = \emptyset \Leftrightarrow S \cap \Lambda^0 = \emptyset$$

Mit Lemma 5.17 folgt die Existenz einer Primzahl p mit

$$\lim_{m\to\infty}\frac{1}{p^{m-1}}\#\left(S \cap \frac{1}{p^{\frac{m-1}{m}}}(\mathbb{Z}^n)^0\right) < 1$$

Rest analog zu Beweis von Satz 5.12

2. Wende Satz 5.12 mit $\overline{S} = S \cap \{x \in \mathbb{R}^n : x_1 \geq 0\}$ an. Das ergibt

$$\operatorname{vol}(\overline{S}) = \frac{\operatorname{vol}(S)}{2} \leq 1 \overset{5.12}{\Longrightarrow} \exists\Lambda \in \mathcal{L}^n.\, \det\Lambda = 1 \wedge \overline{S} \cap \Lambda \setminus \{0\} = \emptyset$$

Und damit ist $S \cap \Lambda \setminus \{0\} = \emptyset$.

3. Ist Kombination der beiden vorigen Fälle.

□

5.20 Korollar. *Sei $K \in \mathcal{K}_0^n$. Dann gilt*

$$\delta_y(K) \geq \zeta(n)\left(\frac{1}{2}\right)^{n-1} \Leftrightarrow \Delta(K) \leq \frac{\operatorname{vol}(K)}{2\zeta(n)}$$

Beweis. OBdA sei $\operatorname{vol}(K) = 2\zeta(n) - \varepsilon$ für ein $\varepsilon > 0$. Nach Korollar 5.19 existiert ein $\Lambda_\varepsilon \in \mathcal{L}^n$ mit $\det\Lambda_\varepsilon = 1$ und $K \cap \Lambda_\varepsilon = \{0\}$. Damit ist

$$2\Lambda_\varepsilon \in \mathcal{P}(K)$$

Damit ist

$$\delta_{\mathcal{L}}(K) \geq \frac{\operatorname{vol}(K)}{2^n\det\Lambda_\varepsilon} = 2^{-(n-1)}\zeta(n) - \frac{\varepsilon}{2^n}$$

Da ε beliebig,folgt die Behauptung. □

5.21 Satz. *Sei $K \in \mathcal{K}_0^n$ und sei $\Lambda_K \in \mathcal{L}^n$ ein kritisches Gitter. Dann gilt*

$$\#\left(K \cap \Lambda_K \setminus \{0\}\right) \geq n(n+1)$$

Beweis. Sei $B = (b_1, \ldots, b_n)$ eine Basis von Λ_K, sei $\{\pm a_1, \ldots, \pm a_k\} = \Lambda_K \setminus \{0\} \cap K$. Angenommen $k < \frac{n(n+1)}{2}$. Für $T \in \mathbb{R}^{n \times n}$ mit Einträgen $t_{l,m}$ und für $\rho \in \mathbb{R}$ sei $B_{\rho,T} = B(I_n + \rho T)$. Sei $a_i = Bz_i$ für $z_i \in \mathbb{Z}^n$. Sei H_i eine Stützebene von K in a_i, gegeben durch $H_i = \{x \in \mathbb{R}^n : \langle u_i, x\rangle \leq 1\}$. Das heißt $\langle u_i, a_i\rangle = 1$ und $\forall x \in K. \langle u_i, x\rangle \leq 1$. Sei $a_{i,\rho,T} = B_{\rho,T} z_i$ für $i = 1, \ldots, k$. Dann gilt

$$a_{i,\rho,T} \in H_i \Leftrightarrow \langle u_i, B_{\rho,T} z_i\rangle = 1 \Leftrightarrow \langle u_i, BTzi\rangle = 0 \Leftrightarrow \sum_{l,m=1}^{n} c_{l,m,i} t_{l,m} = 0$$

für geeignete $c_{,m,i} \in \mathbb{R}$. Wir betrachten nun das homogene Gleichungssystem

$$\begin{aligned} 0 &= t_{l,m} - t_{m,l} && 1 \leq l < m \leq n \\ 0 &= \sum_{l,m=1}^{n} c_{l,m,i} t_{l,m} && 1 \leq i \leq k \end{aligned}$$

Die Anzahl der Gleichungen dabei ist

$$\frac{n^2 - n}{2} + k < \frac{n^2 - n}{2} + \frac{n^2 + n}{2} = n^2$$

Daher gibt es eine nicht-triviale Lösung $\overline{T} = \left(\overline{t}_{l,m}\right)$.
Es gibt nun ein $\overline{\rho}$ so, dass $\Lambda_{\rho,\overline{T}} = B_{\rho,\overline{T}} \mathbb{Z}^n$ zulässig ist für K und alle ρ mit $|\rho| \leq \overline{\rho}$. Angenommen, dies wäre nicht so, dann gibt es eine Folge $\rho_i \to 0$ so, dass

$$\forall i \in \mathbb{N}. \exists v_{\rho_i,\overline{T}} \in \Lambda_{\rho_i,\overline{T}} \setminus \{0\} \cap \operatorname{int} K$$

Weiterhin folgt aus der Konvergenz aber auch $\Lambda_{\rho_i,\overline{T}} \to \Lambda_K$ und oBdA gilt $v_{\rho_i,\overline{T}} \to a_1$. Da aber auch $a_{1,\rho_i,\overline{T}} \to a_1$ folgt $v_{\rho_i,\overline{T}} - a_{1,\rho_i,\overline{T}} \to 0$. Da beides Gitterpunkte sind, haben wir Gleichheit für großes i. Dann haben wir mit $a_{1,\rho_i,\overline{T}} \in H_i \cap \operatorname{int}(K)$ einen Widerspruch. (Stützebenen schneiden das Innere nicht.)
Nun wissen wir $\Lambda_{\rho,\overline{T}}$ ist zulässig für beliebiges $|\rho| \leq \overline{\rho}$. Das bedeutet

$$|\det B(I_n + \rho\overline{T})| \geq |\det B| \Leftrightarrow \det\left(I_n + \rho\overline{T}\right) \geq 1 \Leftrightarrow 1 + \tau_1\rho + \tau_2\rho^2 + \ldots + \tau_n\rho^n \geq 1$$

für hinreichende kleines ρ. Für die Koeffizienten ergibt sich

$$\tau_1 = \operatorname{trace}\left(\overline{T}\right) = \sum_{j=1}^{n} \overline{t}_{j,j} \qquad \tau_2 = \sum_{i<j} \overline{t}_{i,i}\overline{t}_{j,j} - \overline{t}_{i,j}\overline{t}_{j,i}$$

Damit obige Ungleichung für alle ρ gilt, muss gelten $\tau_1 = 0$ und $\tau_2 \geq 0$. Daraus folgt

$$0 \leq 2\tau_2 - (\tau_1)^2 = -\sum_{i=1}^{n} \overline{t}_{i,i}^2 - 2\sum_{i<j} \overline{t}_{i,j}^2$$

Somit ist $\overline{T} = 0$, was unsere Annahme widerspricht, dass $\overline{T}$ nicht-trivial ist. $\square$

Bemerkung. Als obere Schranke für die Kusszahl haben wir $3^n - 1$, was wir auch erreichen durch Würfel. Um diese Schranke zu sehen, seien x_i die Mittelpunkte der Translate mit $x_0 = 0$. Das heißt $(x_i + K) \cap (x_j + K) \cap \emptyset$ für $i \neq j$. Dann ist $x_i + K \subseteq 3K$ für alle i. Also ist

$$\operatorname{vol}\left(\bigcap_i (x_i + K)\right) \leq \operatorname{vol}(3K) = 3^n \operatorname{vol}(K)$$

5.22 Lemma (Mordell, 1944). *Sei $n \geq 2$. Dann ist $\Delta(B_n)^{n-2} \geq \Delta(B_{n-1})^n$. Diese untere Schranke für die kritische Determinante ergibt eine obere Schranke für die Packungsdichte.*

Beweis. Sei $\overline{\Lambda}$ ein Gitter mit $\det \overline{L} = \delta(B_n)$. Sei $b^* \in \overline{\Lambda}^*$ mit $\lambda_1(B_n, \overline{\Lambda}^*) = |b^*|$ und sei $\Lambda_{n-1} \subset \overline{\Lambda}$ das $(n-1)$-dimensionale Gitter mit

$$\operatorname{lin} \Lambda_{n-1} = \{x \in \mathbb{R}^n : \langle b^*, x \rangle = 0\} \overset{2.18}{\Longrightarrow} |b^*| \Delta(B_n) = \det \Lambda_{n-1} \geq \Delta(B_{n-1})$$

Beachte es gilt $\lambda_1^(K, \Lambda)^n \Delta(K) \leq \det \Lambda$ und $\frac{1}{\lambda_1(K,\Lambda)} \Lambda$ ist K-zulässig. Mit Proposition 5.9 erhalten wir

$$|b^*|^n \delta(B_n) \leq \det \overline{\Lambda}^* = \frac{1}{\Delta(B_n)} \implies |b^*| \leq \Delta(B_n)^{\frac{2}{n}} \overset{??}{\Longrightarrow} \Delta(B_n)^{1-\frac{2}{n}} \geq \Delta(B_{n-1})$$

□

5.23 Notation.

- Betrachte das Gitter $A_n = \{z \in \mathbb{Z}^{n+1} : \sum z_i = 0\}$. Für dieses Gitter gilt $\lambda_1(B_n, A_n) = \sqrt{2}$, $\det(A_n) = \sqrt{n+1}$. Für die Packugsdichte beachte $\frac{2}{\lambda_1(K,\Lambda)} \in \mathcal{P}(K)$, das ergibt hier

$$\delta\left(B_n, \frac{2}{\sqrt{2}} A_n\right) = \frac{\operatorname{vol}(B_n)}{\sqrt{2}^n \sqrt{n+1}}$$

- Setze $D_n = \{z \in \mathbb{Z}^n : \sum z_i \equiv 0 \mod 2\}$. Für dieses Gitter gilt nun $\lambda_1(B_n, D_n) = \sqrt{2}$ und $\det D_n = 2$. Daraus folgt $\delta(B_n, \sqrt{2} D_n) = \frac{\operatorname{vol}(B_n)}{\sqrt{2}^n \cdot 2}$. Das heißt für $n = 3$ erhalten wir die selbe Dichte, danach ist D_n besser.

- Setze

$$E_8 = \left\{ z \in \mathbb{Z}^8, \cup \left(\frac{1}{2}\mathbf{1} + \mathbb{Z}^8\right) : \sum z_i \equiv 0 \mod 2 \right\}$$

  Wir fügen zu jedem 8-dimensionalen Würfel den Mittelpunkt hinzu, verlieren aber die Hälfte der Elemente. Damit ist $\det E_8 = 1$. Weiter gilt $\lambda_1(B_m, E_8) = \sqrt{2}$. Die Packungsdichte ist $\delta(B_n, \sqrt{2} E_8) = \frac{\pi^4}{384}$, was die optimale Kugelpackung ist.

- Setze $E_7 := \{z \in E_8 : \sum z_i = 0\}$. Hier gilt $\lambda_1(B_7, E_7) = \sqrt{2} = \det E_7$ und $\delta(B_7, \sqrt{2} E_7) = \frac{\pi^3}{105}$.

- Setze $E_6 = \{z \in E_8 : z_6 = z_7 = z_8\}$. Hie gilt $\lambda_1(B_6, E_6) = \sqrt{2}$, $\det E_6 = \sqrt{3}$ und $\delta(B_6, \sqrt{2} E_6) = \frac{\pi^3}{48\sqrt{3}}$.

5.24 Satz (Lagrange, 1773). $\delta_{\mathcal{L}}(B_2) = \delta(B_2, \sqrt{2} A_2) = \frac{\pi}{\sqrt{12}}$.

Beweis. Sei Λ ein beliebiges Packungsgitter vom Kreis B_2. Sei b_1, b_2 eine HKZ-Basis mit GSO-Basis $\bar{b}_1, \bar{b}_2$. Dann ist $|\bar{b}_1| = |b_1| \geq 2$. Nach Proposition 3.22 und **??** ist

$$(\det \Lambda)^2 = \left|\bar{b}_1\right| \cdot |b_1|^2 \geq \frac{3}{4}\left|\bar{b}_1\right| \geq 12$$

Damit ist $\det \Lambda \geq \sqrt{12}$, also $\delta(B_2, \Lambda) \leq \frac{\pi}{\sqrt{12}}$. □

5.25 Satz (Thue, 1890,1910). $\delta(B_2) = \delta_{\mathcal{L}}(B_2)$ *(hier ohne Beweis).*

5.26 Satz (Gauß, 1840). *Im dreidimensionalen gilt*

$$\delta_{\mathcal{L}}(B_3) = \delta(B_3, \sqrt{2}A_3) = \delta(B_3, \sqrt{2}D_3) = \frac{\pi}{3\sqrt{2}} \left(\iff \Delta(B_3) = \frac{1}{\sqrt{2}} \right)$$

Beweis. Sei b_1, b_2, b_3 eine Minkowskli-reduzierte Basis. Dann gilt insbesondere $|b_i \pm b_j|^2 > |b_i|$ für $i \neq j$. Setze $\beta_{i,j} = \langle b_i, b_j \rangle$. Dann gilt $2|\beta_{i,j}| \leq \beta_{j,j}$ und es ist

$$(\det \Lambda)^2 = \beta_{11}\beta_{22}\beta_{33} - \beta_{11}\beta_{23}^2 - \beta_{22}\beta_{13}^2 - \beta_{33} - \beta_{12}^2 + 2\beta_{12}\beta_{13}\beta_{23}$$

Wir können annehmen, dass entweder $\forall i < j.\beta_{ij} \geq 0$ oder $\forall i < j.\beta_{ij} \leq 0$, da wir bei Bedarf b_i durch $-b_i$ ersetzen können. Wir betrachten nur den ersten Fall, der zweite ist analog. Die schreiben wir um zu

$$2\,(\det \Lambda)^2 = \beta_{11}\beta_{22}\beta_{33} + \beta_{11}\beta_{23}(\beta_{22} - 2\beta_{33}) + \beta_{22}\beta_{13}(\beta_{33} - 2\beta_{13}) + \beta_{33}\beta_{12}(\beta_{11} - 2\beta_{12}) + \beta_{23}(\beta_{11} - 2\beta_{13})(\beta_{22}$$

und somit ist $\det \Lambda \geq 4\sqrt{2}$. Daraus folgt

$$\delta(B_3, \Lambda) \leq \frac{\frac{4}{3}\pi}{4\sqrt{2}} = \frac{\pi}{3\sqrt{2}}$$

Im anderen Fall haben wir $|b_1 + b_2 + b_3|^2 \geq |b_i|^2$ und somit

$$\alpha_{ij} := \beta_{ii} + \beta_{jj} + 2\beta_{12} + 2\beta_{13} + 2\beta_{23} \geq 0 \qquad \gamma_{ij} := 2\beta_{ij} + \beta_{jj} \geq 0$$

Damit erhalten wir für die Determinante

$$8(\det \Lambda)^2 = 4\beta_{11}\beta_{22}\beta_{33} - 2\beta_{11}\beta_{23}(\gamma_{13} + \alpha_{23}) - 2\beta_{22}\beta_{13}(\gamma_{!3} + \alpha_{13}) - 4\beta_{33}\beta_{12}\alpha_{12} + (\beta_{33} + \gamma_{13})\gamma_{23}\gamma_{13} + (\beta_{33} + \gamma$$

und somit $\det \Lambda \geq 4\sqrt{2}$. □

Bemerkung. Man könnte dies auch mit einer HKZ-Basis zeigen, analog zum 2-dimensionalen.

5.27 Satz. *In Dimension 4 gilt*

$$\delta_{\mathcal{L}}(B_4) = \delta(B_4, \sqrt{2}D_4) = \frac{\pi^2}{16} \left(\Leftrightarrow \Delta(B_4) = \frac{1}{2} \right)$$

Beweis. Als obere Schranke haben wir

$$\delta(B_4.\sqrt{2}D_4) = \frac{\pi^2}{16} \implies \Delta(B_4) \leq \frac{1}{2}$$

Aus Lemma 5.22 hingegen folgt

$$\Delta(B_4)^2 \geq \Delta(B_3)^4 = \frac{1}{4} \implies \Delta(B_4) \geq \frac{1}{2}$$

□

5.29 Satz (Colin & Elkies, 2003). *Sei $f : \mathbb{R}^n to \mathbb{R}$ eine multivariate Funktion mit*

$$\forall x \in \mathbb{R}^n . |f(x)|, |\widehat{f}(x)| \leq \frac{c}{(1+|x|)^{n+\delta}}$$

für Konstanten c und δ. Angenommen

1. *$f(x) \leq 0$ für $|c| \geq 1$*
2. *$\widehat{f}(y) \geq 0$ für alle $y \in \mathbb{R}^n$*

Dann gilt

$$\delta(B_n) \leq \mathrm{vol}(B_n) \frac{1}{2^n} \cdot \frac{f(0)}{\widehat{f}(0)}$$

Beweis. Sei $\varepsilon > 0$ und sei $D := \bigcup_{i=1}^m (t_i + \Lambda)$ für ein $\Lambda \in \mathcal{L}^n$ eine periodische Packung von $\frac{1}{2}B_n$ mit $\delta\left(\frac{1}{2}B_n\right) \leq \delta\left(\frac{1}{2}B_n, D\right) + \varepsilon$. Wenn f und $\widehat{f}$ „nice“ sind, folgt aus **??**, dass

$$\forall v \in \mathbb{R}^n . \sum_{b \in \Lambda} f(b+v) = \frac{1}{\det \Lambda} \sum_{b^* \in \Lambda^*} \widehat{f}(b^*) e^{2\pi i \langle v, b^* \rangle}$$

Und daraus folgt

$$\begin{aligned}
\sum_{k,j=1}^m \sum_{b \in \Lambda} f(b + t_k - t_j) &= \sum_{k,j=1}^m \frac{1}{\det \Lambda} \sum_{b^* \in \Lambda^*} \widehat{f}(b^*) e^{2\pi i \langle t_k - t_j, b^* \rangle} \\
&= \frac{1}{\det \Lambda} \sum_{b^* \in \Lambda^*} \widehat{f}(b^*) \sum_{k,j=1}^m e^{2\pi i \langle t_k - t_j, b^* \rangle} \\
&= \frac{1}{\det \Lambda} \sum_{b^* \in \Lambda^*} \widehat{f}(b^*) \left| \sum_{j=1}^m e^{2\pi i \langle t_j, b^* \rangle} \right|^2 \\
&\overset{1}{\geq} \frac{1}{\det \Lambda} \widehat{f}(0) m^2
\end{aligned}$$

Es gilt $b + t_i, t_j \in D$, also $|b + t_i - t_j| \geq 1$ bis auf den Fall $b = 0$ und $t_i = t_j$. Daraus folgt

$$\sum_{i,j=1}^m \sum_{b \in \Lambda} f(b + t_i - t_j) \overset{1}{\leq} m f(0)$$

Somit ist

$$\frac{f(0)}{\widehat{f}(0)} \geq \frac{m}{\det \Lambda} = \frac{\delta\left(\frac{1}{2}B_n, D\right)}{\mathrm{vol}\left(\frac{1}{2}B_n\right)} \geq \frac{\delta(B_n) - \varepsilon}{\mathrm{vol}\left(\frac{1}{2}B_n\right)}$$

und für $\varepsilon \to 0$ ergibt sich die Behauptung. □

5.30 Satz (Cohn & Kumar, 2004). *Das Leech-lattice ist die optimal Gitterpackung der Kugel in Dimension 24.*

5.31 Satz. *Um die Lücke zu schließen haben wir*

1. *Viazoska, 2016/17: $\delta(B_8) = \delta_{\mathcal{L}}(B_8)$*

2. *alle zusammen, 2017:* $\delta(B_{24}) = \delta_{\mathcal{L}}(B_{24})$.

5.32 Satz. *Sei* $K \in \mathcal{K}_0^2$, $\operatorname{vol}(K) > 0$.

1. *Seien* $b_1, b_2, b_2 - b_1 \in \partial K$. *Dann ist* $\Lambda = (b_1, b_2)\mathbb{Z}^2$ *zulässig für* K.
2. *Sei* $\Lambda \in \mathcal{L}^2$ *kritisch für* K. *Dann existieren* $b_1, b_2 \in \Lambda$ *mit* $b_1, b_2, b_2 - b_1 \in \partial K$.

Beweis. 1. Nach Voraussetzung ist

$$\operatorname{int} K \cap \{z_1 b_1 + z_2 b_2 : z_2 \in \{0, \pm 1\}, z_1 \in \mathbb{Z}\} = \{0\}$$

Wäre auf der Linie durch b_1 noch ein Gitterpunkt aus K, dann wäre $b_1 \in \operatorname{int} K$. Dann wäre K eine Linie, also $\operatorname{vol}(K) = 0$. Analog für b_2. Angenommen, wir haben ein $b = z_1 b_1 + z_2 b_2 \in \operatorname{int} K$ mit $z_2 \geq 2$. Da es im Inneren liegt, wähle ε mit $b \pm \varepsilon b_1 \in \operatorname{int} K$. Damit ist $P := \operatorname{conv}\{\pm b_1, b \pm \varepsilon b_1\} \subseteq K$. Daraus folgt

$$\begin{aligned} & \operatorname{vol}_1(P \cap \operatorname{lin}\{b_1\}) = 2|b_1| \wedge \operatorname{vol}_1\left(P \cap (\operatorname{lin}\{b_1\} + z_2 b_2)\right) = 2\varepsilon|b_1| \\ \implies & \end{aligned}$$

unvollständig

2. Da $\det \Lambda = \Delta(K)$, existieren zwei linear unabhängige Pukte $b_1 2, b_2 \in \Lambda \cap \partial K$. Nach **??** bilden b_1, b_2 oBdA eine Basis von Λ. Seien $\alpha_1, \alpha_2 \in \mathbb{R}_{>0}$ maxiaml mit $b_2 - \alpha_1 b_1 \in \partial K$ und $b_2 + \alpha_2 b_1 \in \partial K$. (Wir schauen also in dieser ebene, wie weit wir nach links/rechts gehen können, bis wir auf den Rand treffen. Da K konvex, sind α_i eindeutig.) Ist $\alpha_1 \geq 1$, so ist $b_2 - b_1 \in \partial K$ und wir sind fertig. Für $\alpha_2 \geq 1$ ist $b_1 + b_2 \in \partial K$, also nehmen wir die drei Vektoren $(b_1 + b_2), b_1, (b_1 + b_2) - b_1 \in \partial K$.

   Sei nun also $\alpha_1, \alpha_2 < 1$. Haben wir zudem $\alpha_1, \alpha_2 > 0$, so ist $\pm b_2 + \operatorname{lin}\{b_1\}$ eine Stützgerade von K. Daraus folgt $K \setminus \{0\} \cap \Lambda = \{\pm b_1, \pm b_2\}$, was ein Widerspruch ist zu Satz 5.21.

   Also ist oBdA $\alpha_2 = 0$.

$$\begin{tikzcd} & b_2 \\ 0 \arrow[ur] \arrow[r] & b_1 \\ & u \arrow[ul] \end{tikzcd}$$

Bild unvollständig

   Dann existiert ein $\lambda \in (0, 1)$ mit $\operatorname{vol}_1(K \cap (\lambda b_2 + \operatorname{lin}\{b_1\})) = |b_1|$. Seien u, v die entsprechenden Randpunkte. Dann gilt $v = u - b_1$. Nach **??** ist $(b_1, u)\mathbb{Z}^2$ zulässig mit $|\det(b_1, u)| = \lambda |\det(b_1, b_2)| < \det \Lambda$, was ein Widerspruch ist, da Λ kritisch ist.

□

5.33 Korollar. *Sei* $K \in \mathcal{K}_0^2$, *mit* $\operatorname{vol}(K) > 0$ *und sei* H_K *das affine reguläre Sechseck mit Ecken auf dem rand von* K *und minimalem Volumen. Dann ist* $\delta_{\mathcal{L}} = \frac{3}{4} \cdot \frac{\operatorname{vol}(K)}{\operatorname{vol}(H_K)}$, *was bedeutet* $\Delta(K) = \frac{1}{3} \operatorname{vol}(H_K)$.

Bemerkung. Das affine reguläre Sechseck ist gegeben durch die Eckpunkte $\pm b_1, \pm b_2, b_2 \pm b_1$, mit Volumen $3\det(b_1, b_2)$.

5.34 Satz (Fejes Tódt, 1950, Royes, 1951). *Sei $K \in \mathcal{K}^2$. Dann ist $\delta(K) = \delta_{\mathcal{L}}(K)$.*

5.35 Satz (Hales, 1998,2005,2014). *Es gilt $\delta(B_3) = \delta_{\mathcal{L}}(B_3)$.*

Bemerkung. Wir könnten noch über endliche Paackungen reden. Hier ist ein Problem, dass wir für m Kugeln B_n eine endliche Packung D suchen so, dass $\mathrm{vol}(\mathrm{conv}(D + B_n))$ minimal wird.

Behauptung (Wurstvermutung). *Für $n \geq 5$ ist es optimal, die Kugeln in einer Linie („Wurst") anzuordnen. Bewiesen wurde es für $n \geq 42$.*

In Dimension 3 ist es bis $m = 55$ optimal, die Wurst zu nehmen. Aber für $m = 56$ gibt es eine bessere (volldimensionale) Anordnung, „Wurstkatastrophe".