Prof. Dr. H. Brenner **Osnabrück SS 2008**

Zahlentheorie

Vorlesung 26

Hermann Minkowski (1864-1909)

Unser Ziel ist es, zu zeigen, dass die Klassengruppe eines quadratischen Zahlbereichs endlich ist. Zu dem Beweis benötigt man Methoden aus der konvexen Geometrie und einige topologische Begriffe, die im folgenden aufgeführt werden. Man spricht in diesem Zusammenhang von der Geometrie der Zahlen, die mit dem Namen von Minkowski verbunden ist. Der grundlegende Satz ist der Gitterpunktsatz von Minkowski, den wir in diesem Abschnitt vorstellen und beweisen wollen. Im Fall eines quadratischen Zahlbereichs bilden die ganzen Zahlen ein zweidimensionales Gitter, nämlich $\mathbb{Z} \oplus \mathbb{Z}\omega$, das wir in einem zweidimensionalen reellen Vektorraum auffassen werden. Der Gitterpunktsatz macht eine Aussage darüber, dass gewisse Teilmengen mit hinreichend großem Flächeninhalt (oder allgemeiner Volumen) mindestens zwei Gitterpunkte enthalten müssen.

Wir erinnern zunächst an einige Grundbegriffe aus der konvexen Geometrie, der Topologie und der Maßtheorie.

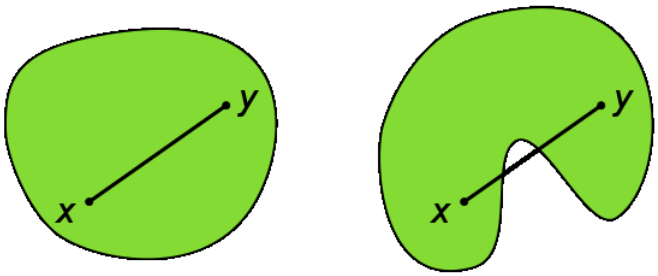
Definition 26.1. Seien $v_1, \ldots, v_n$ linear unabhängige Vektoren im $\mathbb{R}^n$. Dann heißt die Untergruppe $\mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$ ein *Gitter* im $\mathbb{R}^n$.

Manchmal spricht man auch von einem vollständigen Gitter.

Definition 26.2. Eine Teilmenge $T \subseteq \mathbb{R}^n$ heißt *konvex*, wenn mit je zwei Punkten $P, Q \in T$ auch jeder Punkt der Verbindungsstrecke, also jeder Punkt der Form

$$rP + (1-r)Q \text{ mit } r \in [0,1]\,,$$

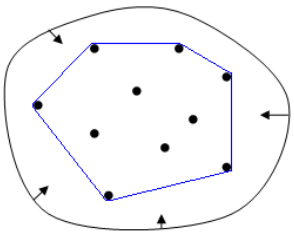
ebenfalls zu T gehört.



Der Durchschnitt von konvexen Teilmengen ist wieder konvex (Aufgabe 26.3). Daher kann man definieren:

DEFINITION 26.3. Zu einer Teilmenge $U \subseteq \mathbb{R}^n$ heißt die kleinste konvexe Teilmenge T, die U umfasst, die *konvexe Hülle* von T.

Die konvexe Hülle ist einfach der Durchschnitt von allen konvexen Teilmengen, die U umfassen.



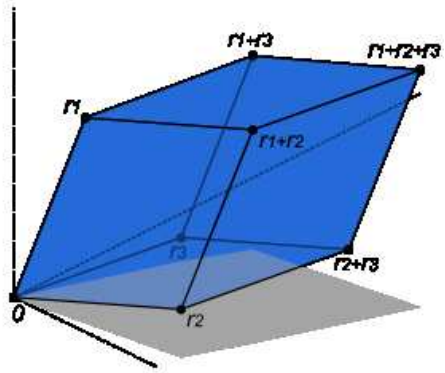
Im zweidimensionalen kann man sich die konvexe Hülle so vorstellen, dass man eine Schnur um die fixierten Punkte aus U legt und die Schnur dann zusammen zieht.

DEFINITION 26.4. Zu einem durch linear unabhängige Vektoren $v_1, \ldots, v_n$ gegebenen Gitter bezeichnet man die konvexe Hülle der Vektoren $e_1v_1 + \ldots + e_nv_n$ mit $e_i \in \{0, 1\}$ als die *Grundmasche* (oder *Fundamentalmasche*) des Gitters.

Die in der vorstehenden Definition auftauchenden Vektoren sind die Eckpunkte des von den Basisvektoren $v_1, \ldots, v_n$ erzeugten Parallelotops. Die Elemente der Grundmasche selbst sind alle Vektoren der Form

$$r_1v_1 + \ldots + r_nv_n \text{ mit } r_i \in [0, 1]$$

Wir werden die Grundmasche häufig mit $\mathfrak{M}$ bezeichnen. Zu einem Gitterpunkt P nennt man die Menge $P+\mathfrak{M}$ eine *Masche* des Gitters. Ein beliebiger Punkt $Q \in \mathbb{R}^n$ hat eine eindeutige Darstellung $Q = t_1v_1+\ldots+t_nv_n$ und damit ist $Q = (\lfloor t_1 \rfloor v_1 + \ldots + \lfloor t_n \rfloor v_n) + ((t_1 - \lfloor t_1 \rfloor)v_1 + \ldots + (t_n - \lfloor t_n \rfloor)v_n)$, wobei der erste Summand zum Gitter gehört und der zweite Summand zur Grundmasche. Insbesondere haben zwei verschiedene Maschen nur Randpunkte, aber keine inneren Punkte gemeinsam.



DEFINITION 26.5. Eine Teilmenge $T \subseteq \mathbb{R}^n$ heißt *zentralsymmetrisch*, wenn mit jedem Punkt $P \in T$ auch der Punkt $-P$ zu T gehört.

Der Begriff der Kompaktheit sollte aus den Anfängervorlesungen bekannt sein.

DEFINITION 26.6. Ein topologischer Raum X heißt *kompakt*, wenn es zu jeder offenen Überdeckung

$$X = \bigcup_{i \in I} U_i \quad \text{mit } U_i \text{ offen und einer beliebigen Indexmenge}$$

eine endliche Teilmenge $J \subseteq I$ gibt derart, dass

$$X = \bigcup_{i \in J} U_i$$

ist.

Für eine Teilmenge im $\mathbb{R}^n$ ist eine Teilmenge T genau dann kompakt, wenn sie abgeschlossen und beschränkt ist.

Die endliche Vereinigung von kompakten Mengen ist kompakt. Abgeschlossene Teilmengen von kompakten Mengen sind wieder kompakt. Zu zwei disjunkten kompakten Mengen X und Y in einem metrischen Raum Z gibt es einen Minimalabstand d. D.h. zu jede zwei Punkten $x \in X$ und $y \in Y$ ist $d(x, y) \geq d$.

Wir stellen einige Grundbegriffe aus der Maßtheorie zusammen.

Nicht jeder Teilmenge des $\mathbb{R}^n$ kann man sinnvollerweise ein Maß zuordnen. In der Maßtheorie werden die sogenannten Borelmengen eingeführt, und diesen Borelmengen kann ein Maß, das sogenannte Borel-Lebesque Maß λ zugeordnet werden. Die Borelmengen umfassen unter anderem alle offenen Mengen, alle abgeschlossenen Mengen (insbesondere alle kompakten Mengen). Borelmengen sind unter abzählbarer Vereinigung und abzählbaren Durchschnitten abgeschlossen, und mit einer Borelmenge ist auch deren Komplement eine Borelmenge.

Das Borel-Lebesque Maß λ hat seine Werte in $\overline{\mathbb{R}}_{\geq 0} = \mathbb{R}_{\geq 0} \cup \{\infty\}$ und ist durch folgende Eigenschaften charakterisiert (der Nachweis der Existenz erfordert einigen Aufwand):

(1) Für einen Quader Q mit den Seitenlängen $s_1, \ldots, s_n$ ist $\lambda(Q) = s_1 \cdot s_2 \cdots s_n$.
(2) Für eine abzählbare Familie von disjunkten Borelmengen T_i, $i \in I$, ist $\lambda(\bigcup_{i \in I} T_i) = \sum_{i \in I} \lambda(T_i)$.
(3) Das Borel-Lebesque Maß λ ist translationsinvariant, d.h. für eine Borelmenge T und einen Vektor $v \in \mathbb{R}^n$ ist auch die um v verschobene Menge $v + T$ eine Borelmenge mit $\lambda(v + T) = \lambda(T)$.

Weitere wichtige Eigenschaften sind:

- Für $U \subseteq T$ ist $\lambda(U) \leq \lambda(T)$.
- Teilmengen, die in einem echten linearen Unterraum des $\mathbb{R}^n$ liegen, haben das Maß 0.
- Ein einzelner Punkt und damit auch jede abzählbare Ansammlung von Punkten hat das Maß 0.
- Unter einer linearen Abbildung $L : \mathbb{R}^n \to \mathbb{R}^n$ verhält sich das Borel-Lebesque Maß so: zu einer Borelmenge T ist auch das Bild $L(T)$ eine Borelmenge mit $\lambda(L(T)) = |\det(L)| \cdot \lambda(T)$.

Eine Basis $v_1, \ldots, v_n$ von $\mathbb{R}^n$ liefert ein Gitter $\Gamma \subset \mathbb{R}^n$ zusammen mit der Grundmasche $\mathfrak{M}$, nämlich das durch die v_i aufgespannte Parallelotop. Dessen Volumen (also dessen Borel-Lebesgue-Maß) wird im Folgenden eine Rolle spielen. Das Volumen berechnet sich wie folgt: man schreibt die Vektoren v_i (die ja jeweils n Einträge haben) als Spalten einer quadratischen $n \times n$-Matrix M. Dann ist

$$\mathrm{Vol}(\mathfrak{M}) = |\det(M)| .$$

Dies folgt aus (bzw. ist äquivalent mit) der oben zitierten Aussage, wie sich das Borel-Lebesgue-Maß unter linearen Abbildung verhält, wenn man sie auf die lineare Abbildung anwendet, die die Einheitsvektoren e_i auf v_i schickt.

Zu einem Gitter $\Gamma \subset \mathbb{R}^n$ gibt es keine eindeutig definierte Gitterbasis und damit auch keine eindeutig definierte Grundmasche. Wenn bspw. v_1, v_2 eine Basis eines zweidimensionalen Gitters bilden, so ist auch $v_1, v_2 + tv_1$ ($t \in \mathbb{Z}$) eine Basis desselben Gitters. Wenn man also von einer Grundmasche eines Gitters spricht, so meint man in Wirklichkeit die Grundmasche zu einer fixierten Basis eines Gitters. Wichtig ist dabei, dass das Volumen einer Grundmasche nur vom Gitter selbst abhängt, nicht aber von der Gitterbasis!

Sei nämlich $w_1, \ldots, w_n$ eine weitere Gitterbasis. Dann gibt es zunächst eine quadratische invertierbare reellwertige Matrix A, die den Basiswechsel beschreibt, also $w = Av$. Da die w_i zum Gitter gehören muss diese Matrix ganzzahlig sein. Aus dem gleichen Grund muss die inverse Matrix ganzzahlig sein. Damit muss die Determinante von $A¿$ aber entweder 1 oder -1 sein.

Nach der Formel für das Maß unter linearen Abbildungen haben also die Parallelotope zur Basis v und zur Basis w das gleiche Volumen. Man spricht daher auch vom Volumen (oder Kovolumen) des Gitters.

SATZ 26.7. *(Gitterpunktsatz von Minkowski) Sei Γ ein Gitter im $\mathbb{R}^n$ mit Grundmasche $\mathfrak{M}$. Es sei T eine konvexe, kompakte, zentralsymmetrische Teilmenge in $\mathbb{R}^n$, die zusätzlich die Volumenbedingung*

$$\operatorname{Vol}(T) \geq 2^n \operatorname{Vol}(\mathfrak{M})$$

erfülle. Dann enthält T mindestens einen von null verschiedenen Gitterpunkt.

Beweis. Wir betrachten das verdoppelte Gitter 2Γ. Ist $v_1, \ldots, v_n$ eine Basis für Γ, so ist $2v_1, \ldots, 2v_n$ eine Basis für 2Γ, und für das Volumen gilt $\operatorname{Vol}(2\Gamma) = 2^n \operatorname{Vol}(\Gamma)$. Wir bezeichnen die Grundmasche von 2Γ mit $\mathfrak{N}$. Zu jeder Masche $\mathfrak{N}_Q = Q + \mathfrak{N}$, $Q \in 2\Gamma$, betrachten wir den Durchschnitt $T_Q = T \cap \mathfrak{N}_Q$. Da T kompakt und insbesondere beschränkt ist, gibt es nur endlich viele Maschen derart, dass dieser Durchschnitt nicht leer ist. Seien diese Maschen (bzw. ihre Ausgangspunkte) mit $\mathfrak{N}_i$ (bzw. Q_i), $i \in I$, bezeichnet (da der Nullpunkt aufgrund der Konvexität und der Zentralsymmetrie zu T gehört, umfasst I zumindest 2^n Elemente). Die in die Grundmasche $\mathfrak{N}$ verschobenen Durchschnitte bezeichnen wir mit

$$\tilde{T_i} := T_i - Q_i \,.$$

Wir behaupten zunächst, dass die $\tilde{T_i}$ nicht paarweise disjunkt sind. Sei also angenommen, sie wären paarweise disjunkt. Mindestens eines der T_i hat positives Volumen, sagen wir für $i = 1$. Wegen der angenommenen Disjunktheit sind insbesondere

$$X := \tilde{T_1} \text{ und } Y := \bigcup_{i \in I, i \neq 1} \tilde{T_i}$$

disjunkt zueinander. Wir haben also zwei disjunkte kompakte Teilmengen, und diese besitzen einen Minimalabstand d (d.h. zu jedem Punkt aus X liegen in einer d-Umgebung keine Punkte aus Y).

Sei $x \in X$ ein innerer Punkt (den es gibt, da X positives Volumen besitzt) und sei $y \in Y$. Mit S sei die Verbindungstrecke von x nach y bezeichnet, die ganz in $\mathfrak{N}$ verläuft. Wir wählen einen Punkt $s \in S$, der weder zu Xnoch zu Y gehört (solche Punkte gibt es wegen des Minimalabstandes). Da s sowohl zu X als auch zu Y einen Minimalabstand besitzt, gibt es eine ϵ-Umgebung B von s, die disjunkt zu X und Y ist. Wir können ferner annehmen, dass B ganz innerhalb von $\mathfrak{N}$ liegt (wegen der Wahl von x). Als eine Ballumgebung hat B ein positives Volumen, was zu folgendem Widerpruch führt.

$$\begin{aligned} \operatorname{Vol}(\mathfrak{N}) &\geq \operatorname{Vol}(X \cup Y \cup B) \\ &= \operatorname{Vol}(\bigcup_{i \in I} \tilde{T_i}) + \operatorname{Vol}(B) \\ &> \sum_{i \in I} \operatorname{Vol}(\tilde{T_i}) \end{aligned}$$

$$\begin{aligned} &= \sum_{i\in I} \mathrm{Vol}(T_i) \\ &= \mathrm{Vol}(T) \\ &\geq 2^n \,\mathrm{Vol}(\mathfrak{M}) \\ &= \mathrm{Vol}(\mathfrak{N}). \end{aligned}$$

Es gibt also Indizes $i \neq j$ und einen Punkt $z \in \tilde{T}_i \cap \tilde{T}_j$ (z muss selbst nicht zu T gehören). Sei

$$z_i := z + Q_i \in T_i \text{ und } z_j := z + Q_j \in T_j \,.$$

Wegen $Q_i, Q_j \in 2\Gamma$ ist auch $Q_i - Q_j \in 2\Gamma$ und daher

$$0 \neq \frac{Q_i - Q_j}{2} \in \Gamma \,.$$

Aus $z_i \in T$ folgt (wegen der Zentralsymmetrie) auch $-z_i \in T$ und wegen der Konvexität von T ergibt sich

$$\begin{aligned} \frac{Q_i - Q_j}{2} &= \frac{1}{2}(z - z_i) - \frac{1}{2}(z - z_j) \\ &= -\frac{1}{2} z_i + \frac{1}{2} z_j \\ &\in T. \end{aligned}$$

Wir haben also einen von null verschiedenen Gitterpunkt in T gefunden. $\square$

Abbildungsverzeichnis