1 Gitter im euklidischen Raum

1.1 Skalarprodukte und quadratische Formen

In diesem einleitenden Abschnitt stellen wir einige Tatsachen über Bilinearformen, Skalarprodukte und quadratische Formen zusammen, die jedoch im Großen und Ganzen als aus der Linearen Algebra bekannt vorausgesetzt werden.

Ein *Skalarprodukt* auf einem reellen Vektorraum V ist eine positiv definite, symmetrische Bilinearform $b : V \times V \to \mathbb{R}$. Für $x, y \in V$ schreiben wir kurz $\langle x, y\rangle := b(x, y)$. Das Paar (V, b) heißt auch *euklidischer Vektorraum*. Wenn V endlich-dimensional ist (im folgenden wird das immer der Fall sein), ist ein Skalarprodukt insbesondere eine *reguläre* Bilinearform, d.h. zu jeder Linearform $f : V \to \mathbb{R}$ gibt es einen eindeutig bestimmten Vektor $y = y_f$ mit $f(x) = \langle x, y_f\rangle$ für alle $x \in V$.

Wenn $v_1, \ldots, v_k$ Vektoren in V sind, so heißt die Matrix

$$G := (\langle v_i, v_j\rangle)_{i,j=1,\ldots,k} \in \mathbb{R}^{k\times k} \tag{1.1.1}$$

die Gram'sche Matrix oder *Gram-Matrix*[1] von $v_1, \ldots, v_k$ (genauer: des k-Tupels $(v_1, \ldots, v_k)$). Eine Gram-Matrix $G = (g_{ij})$ ist immer positiv semidefinit, d.h. $\sum g_{ij}x_ix_j \geq 0$ für alle $(x_1, \ldots, x_k) \in \mathbb{R}^k$. Sie ist positiv definit genau dann, wenn sie invertierbar ist, genau dann, wenn die Vektoren $v_1, \ldots, v_k$ linear unabhängig sind. Wenn das der Fall ist, so ist $\sqrt{\det G}$ zu interpretieren als das k-dimensionale Volumen des von $v_1, \ldots, v_k$ aufgespannten *Quaders*

Beweis?

$$\sqrt{\det G} = \operatorname{vol} Q, \text{ wobei } Q = \left\{ \sum_{i=1}^{k} t_i v_i \mid 0 \leq t_i \leq 1 \right\}; \tag{1.1.2}$$

wir werden das insbesondere für $k = n = \dim V$ benutzen. Eine (mögliche) Begründung für diese Volumenformel geben wir weiter unten in diesem Abschnitt.

Wenn $\mathcal{A} = (v_1, \ldots, v_n)$ und $\mathcal{B} = (w_1, \ldots, w_n)$ zwei Basen von V sind und $G_\mathcal{A}$ bzw. $G_\mathcal{B}$ die zugehörigen Gram-Matrizen, ferner $S \in \mathrm{GL}_n(\mathbb{R})$ die Matrix des Basiswechsels

$$w_j = \sum_{i=1}^{n} s_{ij} v_i\,, \qquad j = 1, \ldots, n \tag{1.1.3}$$

(hierbei bezeichnet $\mathrm{GL}_n(\mathbb{R})$ die allgemeine lineare Gruppe, also die invertierbaren $(n \times n)$-Matrizen über $\mathbb{R}$), so hat man die Formel

$$G_\mathcal{B} = S^t G_\mathcal{A} S\,. \tag{1.1.4}$$

Hierbei ist S^t die transponierte Matrix zu S.

[1] Nach J.P. Gram, 1850–1916

Zwei Vektoren $v, w \in V$ heißten *orthogonal* oder *senkrecht* zueinander, falls $\langle v, w\rangle = 0$ ist, entsprechend für zwei Teilmengen $A, B \subseteq V$. Wenn $A \subset V$ eine beliebige Teilmenge ist, so ist der *Orthogonalraum* von A

$$A^\perp := \{y \in V \mid \langle x, y\rangle = 0 \text{ für alle } x \in A\}$$

in der Tat ein Untervektorraum von V. Falls U ein Unterraum von V ist, heißt $U^\perp$ auch das *orthogonale Komplement* von U; es gilt nämlich $V = U \oplus U^\perp$.

Die Funktion $V \to \mathbb{R}_{\geq 0}$, $x \mapsto \sqrt{\langle x, x\rangle} =: \|x\|$ ist eine Norm (im Sinne der Analysis) auf V, die *euklidische Norm* bezüglich des fixierten Skalarproduktes. Insbesondere gilt für diese Norm und die zugehörige Abstandsfunktion $d(x, y) := \|x - y\|$ die Dreiecksungleichung; diese zeigt man mit Hilfe der Cauchy-Schwarz'schen Ungleichung $|\langle x, y\rangle| \leq \sqrt{\langle x, x\rangle}\sqrt{\langle y, y\rangle}$. In der Geometrie der Zahlen wird allerdings oft die Zahl $\langle x, x\rangle = \|x\|^2$ als Norm von x bezeichnet; wir werden der Deutlichkeit halber dann von der *Quadratlänge* von x sprechen.

Sei speziell $V = \mathbb{R}^n$ und b das Standardskalarprodukt $\mathbf{x} \cdot \mathbf{y} := \sum x_i y_i$, dabei $\mathbf{x} = (x_1, x_2, \ldots, x_n)^t$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)^t$ Spaltenvektoren. Dann ist ein System $(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ von n Elementen von V, d.h. von Spaltenvektoren, dasselbe wie eine $n \times n$-Matrix A. Die zugehörige Gram-Matrix G_A ist dann gleich $A^t A$. Zum Beweis schreibe man das Skalarprodukt als das Matrizenprodukt einer Zeile mit einer Spalte, d.h. einer $(1 \times n)$-matrix mit einer $(n \times 1)$-Matrix: $\mathbf{x} \cdot \mathbf{y} = \mathbf{x}^t \mathbf{y}$.

Bekanntlich ist $|\det A|$ das Volumen des von $a_1, \ldots, a_n$ aufgespannten Quaders Q im $\mathbb{R}^n$. Wegen $\det G_A = (\det A)^2$ ergibt sich die frühere Formel $\sqrt{\det G}$ für das Volumen von Q.

Die Menge

$$\mathrm{O}(V) = \mathrm{O}(V, b) := \{\psi \in \mathrm{GL}(V) \mid \forall x, y \in V : \langle \psi(x), \psi(y)\rangle = \langle x, y\rangle\}$$

aller orthogonalen Vektorraum-Automorphismen von V heißt auch die *orthogonale Gruppe* des euklidischen Vektorraumes (V, b). Dieses ist in der Tat eine Gruppe, nämlich eine Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}(V)$ aller Vektorraum-Automorphismen von V. Eine orthogonale Abbildung ist nämlich automatisch injektiv, also wegen der Endlich-Dimensionalität bijektiv. Ferner ist die Verkettung von zwei orthogonalen Abbildungen wieder orthogonal, ebenso die Inverse einer orthogonalen Abbildung.

Eine ergänzende Bemerkung: Eine lineare Abbildung ψ ist orthogonal genau dann, wenn sie eine *Isometrie* ist, d.h. abstandserhaltend: $d(\psi(x), \psi(y)) = d(x, y)$ für alle $x, y \in V$. Bemerkenswerterweise gilt dieses auch ohne die Voraussetzung der Linearität; man braucht lediglich die (offensichtlich notwendige) Voraussetzung $\psi(0) = 0$ und kann dann zeigen, dass eine bijektive Isometrie automatisch linear ist.

Im Hinblick auf die zahlentheoretischen Aspekte dieser Vorlesung wollen wir schließlich noch den Begriff einer *quadratischen Form* einführen. Klassisch ist eine quadratische Form ein homogenes Polynom vom Grad 2 in einer gewissen Anzahl n von Variablen

$$f = f(X_1, \ldots, X_n) = \sum_{i,j} f_{ij} X_i X_j \,. \tag{1.1.5}$$

Man beachte, dass in dieser Darstellung für $i \neq j$ das Monom $X_i X_j$ zwei mal vorkommt, das Polynom selbst bestimmt lediglich die Summe $f_{ij} + f_{ji}$, nicht die beiden Summanden. Wir fordern zusätzlich $f_{ij} = f_{ji}$ für alle i, j und erhalten so eine eindeutige symmetrische Matrix $F = (f_{ij})$, die immer noch 1.1.5 erfüllt. Die beschriebene bijektive Korrespondenz zwischen quadratischen Formen und symmetrischen Matrizen gilt offenbar über jedem Ring, in dem 2 eine Einheit ist, insbesondere über den reellen Zahlen, allgemeiner über allen Körpern der Charakteristik $\neq 2$ (aber nicht über $\mathbb{Z}$).

Die zu einer quadratischen Form gehörige Funktion $\mathbb{Z}^n \to \mathbb{R}$ oder $\mathbb{R}^n \to \mathbb{R}$, $(x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n)$ wird ebenfalls als quadratische Form bezeichnet.

Eine wichtige Notation für quadratische Formen bzw. symmetrische Matrizen ist die folgende: Sei F eine symmetrische $n \times n$-Matrix, und S eine $n \times k$-Matrix für ein $k \geq 1$. Schreibe

$$F[S] := S^t F S \quad \text{(eine symmetrische } k \times k\text{-Matrix)} \,. \tag{1.1.6}$$

Zwei Spezialfälle sind besonders wichtig:

- $k = 1$: Dann ist $S = \mathbf{x} = (x_1, \ldots, x_n)^t \in \mathbb{R}^n$ ein Spaltenvektor und

$$F[\mathbf{x}] := \mathbf{x}^t F \mathbf{x} = \sum f_{ij} x_i x_j \ \in \mathbb{R} \tag{1.1.7}$$

  der Wert von F (aufgefaßt als Polynom) auf dem Tupel $x_1, \ldots, x_n$. Unter Verwendung von Gleichung 1.1.5 ist also $F[\mathbf{x}] = f(x_1, x_2, \ldots, x_n)$.

- $k = n$: In diesem Fall kann man S auf die Teilmenge (sogar Untergruppe) der ganzzahligen und über $\mathbb{Z}$ invertierbaren Matrizen $\mathrm{GL}_n(\mathbb{Z})$ einschränken. Bei gegebenem F sind die quadratischen Formen der Gestalt

$$G = F[S] = S^t F S \ , S \in \mathrm{GL}_n(Z) \tag{1.1.8}$$

  definitionsgemäß die zu F *äquivalenten* quadratischen Formen.

Auf der Ebene der Matrizen würde man diese Relation als *ganzzahlige Kongruenz* bezeichnen: zwei symmetrische Matrizen F und G heißen ganzzahlig kongruent, wenn eine Matrix $S \in \mathrm{GL}_n(\mathbb{Z})$ existiert so, dass 1.1.8 gilt.

Für den modernen Begriff einer quadratischen Form betrachtet man nicht primär Polynome. Vielmehr ist eine quadratische Form eine Funktion auf einem

Vektorraum V, allgemeiner einem Modul L über einem Ring R, die von der Gestalt $x \mapsto f(x) := b(x,x)$ ist, wobei b eine Bilinearform auf L ist. Ähnlich wie oben gilt, dass b als symmetrisch angenommen werden kann, wenn 2 eine Einheit in R ist:

$$b(x,x) = \frac{1}{2}(b(x,y) + b(y,x)).$$

Wenn speziell $L = R^n$ ist, ist offenbar jede Bilinearform b auf L von der Gestalt

$$b_F(\mathbf{x},\mathbf{y}) := \mathbf{x}^t F \mathbf{y} = \sum_{i,j} f_{ij} x_i y_j \tag{1.1.9}$$

für eine eindeutig bestimmte Matrix $F \in R^{n\times n}$, und b_F ist symmetrisch genau dann wenn F es ist. Insofern ist der oben betrachtete klassische Begriff einer quadratischen Form in dem jetzt betrachteten enthalten (das gilt übrigens auch, wenn 2 keine Einheit ist). Mit dem offensichtlichen Begriff von Isomorphie von quadratischen Formen, genauer, von „quadratischen Vektorräumen" bzw. „quadratischen Moduln" (L, f), man spricht wiederum von *Isometrie*, sind tatsächlich zwei quadratische Moduln $(R^n, f_1))$ und (R^n, f_2) isometrisch genau dann, wenn f_1 und f_2 äquivalente quadratische Formen im Sinne von 1.1.8 sind. Ferner ist jede quadratische Form auf einem freien Modul, insbesondere einem Vektorraum, isometrisch zu einer „klassischen" quadratischen Form, d.h. einem homogenen Polynom von Grad 2. Beweis?

Zahlentheoretisch interessant sind insbesondere die *ganzzahligen quadratischen Formen*, was bedeutet, dass die Koeffizienten f_{ii} unf $2f_{ij}, i \neq j$ des Polynoms ganze Zahlen sind, d.h. die Elemente außerhalb der Diagonalen von F sind halbganz. Oft arbeitet man lieber mit der ganzzahligen Matrix $H = 2F$ (dieses ist die Hesse-Matrix des Polynoms f) und schreibt

$$f(\mathbf{x}) := \tfrac{1}{2}\mathbf{x}^t H \mathbf{x}. \tag{1.1.10}$$

Auf diese Weise entsprechen die ganzzahligen (positiv definiten) quadratischen Formen bijektiv den (positiv definiten) ganzzahligen symmetrischen Matrizen mit geraden Diagonalelementen. Diese Konvention ist oft (zum Beispiel im Zusammenhang mit Modulformen) praktischer als die aus Formel 1.1.7.