1.2 Gitter: Grundlegende Konzepte

Es sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum. Auf V sei ein Skalarprodukt gegeben, dessen Werte mit $\langle x, y\rangle \in \mathbb{R}$, dabei $x, y \in V$, bezeichnet werden. Wie üblich heißt $||v|| := \sqrt{\langle v, v\rangle}$ die Länge eines Vektors $v \in V$; die Zahl $\langle v, v\rangle$ wird auch als *Quadratlänge* oder Norm von v bezeichnet.

Definition 1.2.1 Eine Teilmenge $L \subset V$ heißt *Gitter in* V, falls linear unabhängige Vektoren $v_1, \ldots, v_m$ in V existieren mit

$$L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m = \left\{ \sum_{i=1}^{m} x_i v_i \mid x_i \in \mathbb{Z} \right\}.$$

L heißt *Gitter auf* V, falls darüberhinaus $m = n$ ist, d. h. L den Vektorraum V erzeugt. Das m-Tupel $(v_1, \ldots, v_m)$ heißt auch *Basis* des Gitters L.

Die folgende Zeichnung zeigt einen Ausschnitt aus einem typischen Gitter in der Dimension 2. Natürlich soll man sich die gezeichnete Punktmenge als in beide Richtungen periodisch ins Unendliche fortgesetzt vorstellen.

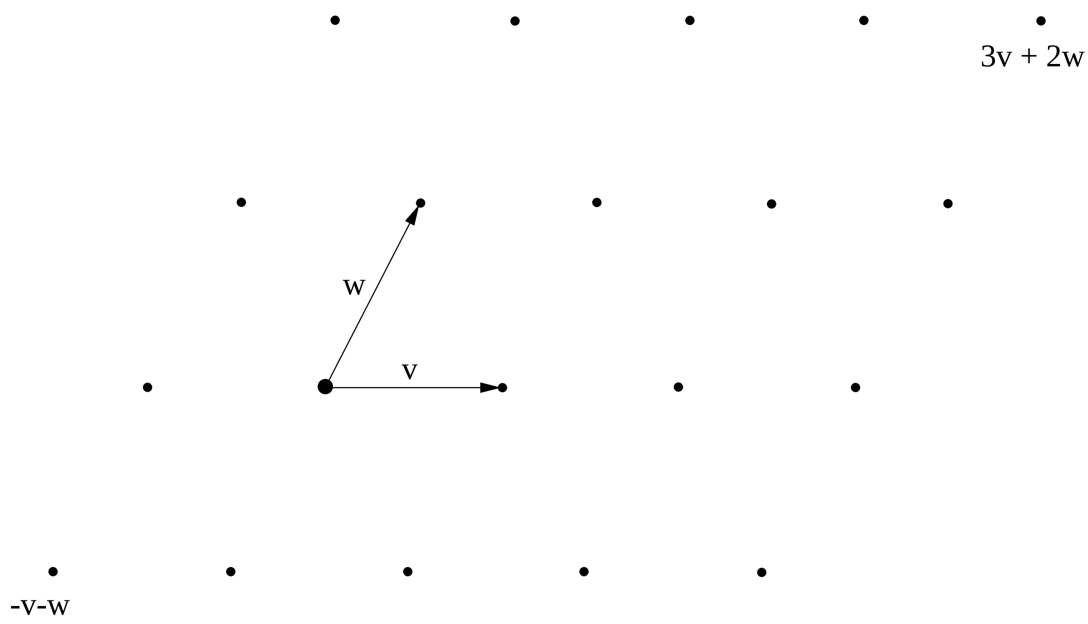

Abb. 1.2.1: Ein Gitter in der Dimension 2

Definition und Bemerkung 1.2.2 Die Matrix

$$G := \Big(\langle v_i, v_j\rangle\Big)_{i,j=1,\ldots,m}$$

heißt *Gram-Matrix* des Gitters L bezüglich der Basis $v_1, \ldots, v_m$. Die Determinante $\det L := \det G$ ist unabhängig von der Wahl der Basis und heißt *Determinante von* L (bezüglich des fixierten Skalarproduktes).

Beweis: Es sei $w_1, \dots, w_m$ eine weitere Basis von L und $S = (s_{ij})$ die Matrix des Basiswechsels:

$$w_j = \sum_{j=1}^{m} s_{ij} v_i.$$

Dann hat zunächst einmal S ganzzahlige Koeffizienten. Die Matrix S^{-1} drückt umgekehrt die Gittervektoren v_i durch die Gitterbasis w_j aus, hat also ebenfalls ganzzahlige Koeffizienten. Insbesondere sind die Determinanten $\det S$ und $\det S^{-1}$ ganze Zahlen. Wegen $\det S \cdot \det S^{-1} = 1$ folgt $\det S = \pm 1$. Ferner gilt $H = S^t G S$ für die Gram-Matrix H bezüglich $w_1, \dots, w_m$ (siehe Formel 1.1.4), womit $\det G = \det H$ sofort folgt. □

Wir schließen an den letzten Beweis an und bemerken noch folgendes: Wenn S eine beliebige ganzahlige quadratische Matrix mit $\det S = \pm 1$ ist, dann ist S invertierbar, und die bekannte, sich aus der Cramer'schen Regel für lineare Gleichungssysteme ergebende Formel für die inverse Matrix zeigt, daß S^{-1} ebenfalls ganze Koeffizienten hat. Wir haben insgesamt folgendes gesehen:

Bemerkung 1.2.3 Die Gruppe aller invertierbaren ganzahligen Matrizen mit ganzzahliger Inverser kann folgt beschrieben werden:

$$\mathrm{GL}_m(\mathbb{Z}) := \{S \in \mathbb{Z}^{m \times m} \mid \det S = \pm 1\}.$$

Isometrie von Gittern. Wir klären in diesem Unterabschnitt, wann zwei Gitter „isomorph", man sagt „isometrisch", sind.

Definition 1.2.4 Eine *Isometrie* eines Gitters K in ein Gitter L ist ein Homomorphismus $\varphi : K \to L$ mit

$$\langle \varphi x, \varphi y \rangle = \langle x, y \rangle \text{ für alle } x, y \in K\,.$$

Zwei Gitter K und L heißen *isometrisch,* in Zeichen $K \cong L$, falls eine bijektive Isometrie $\varphi : K \to L$ existiert.

Beachte, dass eine Isometrie automatisch injektiv ist. Wie üblich ist „Isometrie" im Sinne von „isometrisch-sein" eine Äquivalenzrelation auf den Gittern. Die betrachteten Gitter liegen definitionsgemäß in euklidischen Vektorräumen, nennen wir sie U bzw. V. Eine Isometrie $\varphi : K \to L$ setzt sich eindeutig zu einer linearen Isometrie (orthogonalen Abbildung) $\widetilde{\varphi} : \langle K \rangle_{\mathbb{R}} \to \langle L \rangle_{\mathbb{R}}$ zwischen den erzeugten Vektorräumen $\langle K \rangle_{\mathbb{R}} \subseteq U$ und $\langle L \rangle_{\mathbb{R}} \subseteq V$ fort. Im Fall der Gleicheit kann man also eine Isometrie von zwei Gittern K, L <u>auf</u> euklidischen Vektorräumen U bzw. V auch definieren als eine isometrische lineare Abbildung $\psi : U \to V$ mit $\psi(K) \subseteq L$. Insbesondere gilt:

Bemerkung 1.2.5 Zwei Gitter L, M auf demselben euklidischen Vektorraum V sind isometrisch genau dann, wenn ein Element $\varphi \in \mathrm{O}(V)$ der orthogonalen Gruppe von V existiert mit $\varphi(L) = M$.

Das ist der übliche Begriff von Isometrie oder „Kongruenz" für Punktmengen im euklidischen Raum V.

Ein handhabbares Kriterium für Isometrie ergibt sich aus folgendem einfachen Resultat:

Proposition 1.2.6 *a) Zwei Gitter L und M sind isometrisch genau dann, wenn es Basen von L und M gibt, die dieselbe Gram-Matrix liefern.*

b) Zwei Gitter L und M seien gegeben durch Gram-Matrizen G bzw. H bezüglich irgendwelcher Basen. Dann sind L und M isometrisch genau dann, wenn eine Matrix $S \in \mathrm{GL}_n(\mathbb{Z})$ existiert mit $S^tGS = H$.

Die Isometrie-Klassen von n-dimensionalen Gittern entsprechen somit bijektiv den Äquivalenzklassen positiv-definiter reeller symmetrischer $n \times n$-Matrizen mit der gerade unter b) beschriebenen Äquivalenzrelation. Diese Relation ist genau die in Abschnitt 1.1 im Zusammenhang mit quadratischen Formen beschriebene ganzzahlige Kongruenz. Ganzzahlige Gitter entsprechen dabei den Kongruenzklassen ganzzahliger Matrizen. Wir werden später noch sehen, wie das zunächst nur prinzipielle Kriterium 1.2.6 b) angewendet wird, mit anderen Worten, „wo" man die Matrix S suchen muss und wie man sie findet, oder auch nicht. Es handelt sich hier um ein subtiles Problem der algorithmischen Algebra, das auch zu aktuellen Forschungsfragen Anlass gibt.

Mit den symmetrischen (Gram-)Matrizen als Bindeglied ergibt sich aus Proposition 1.2.6 der folgende grundlegende Zusammenhang zwischen Gittern (im euklidischen Raum) und (positiv definiten) quadratischen Formen:

Proposition 1.2.7 *Es gibt eine bijektive Korrespondenz zwischen den Isometrieklassen von n-dimensionalen Gittern in euklidischen Vektorräumen und den Äquivalenzklassen von positiv definiten quadratischen Formen in n Unbestimmten.*

In der Diskreten Geometrie interessiert man sich für geometrische (auch topologische oder analytische) Eigenschaften diskreter Punktmengen, von denen Gitter eine wichtige Teilklasse sind. In der Zahlentheorie interessiert man sich für die Lösbarkeit, die Lösungsanzahlen und die Größe der Lösungen von diophantischen Gleichungen. Die Proposition 1.2.7 erklärt (zumindest für quadratische Gleichungen), wieso diese beiden Problemfelder eng miteinander zu tun haben.

Geometrische Interpretation der Determinante eines Gitters. Es sei L ein Gitter, $v_1, \ldots, v_n$ eine Basis von L und Q wie früher der von dieser Basis aufgespannte Quader (siehe 1.1.2). Sei $x \in V$ ein beliebiger Vektor. Schreibe $x = \sum x_i v_i$, $x_i \in \mathbb{R}$ und weiter $x_i = m_i + t_i$, $m_i \in \mathbb{Z}$, $0 \le t_i < 1$. Setze $v := \sum m_i v_i$ und $y = \sum t_i v_i$. Dann gilt

$$x = v + y \text{ mit } v \in L \text{ und } y \in Q.$$

Anders aufgefaßt, V ist die Vereinigung aller Mengen $v + Q$, $v \in L$, also aller Translate von Q um Gittervektoren. Eine kleine Weiterführung dieser Überlegung zeigt, dass Q ein Fundamentalbereich für L im Sinne der folgenden Definition ist.

Definition 1.2.8 Eine Teilmenge $F \subset V$ heißt *Fundamentalbereich* für ein Gitter L, falls folgendes gilt:

(F1) $V = \bigcup_{v \in L} v + F$,

(F2) F ist meßbar,

(F3) $\operatorname{vol}(F \cap (v + F)) = 0$ für $v \in L \setminus \{0\}$.

Hierbei bezeichnet $\operatorname{vol} X$ das Volumen oder Maß einer meßbaren Teilmenge $X \subseteq V$. Die Gültigkeit von (F3) für Quader folgt daraus, dass $F \cap (v+F)$ im Rand von F enthalten ist, also in einer Hyperebene von V, und deshalb eine Nullmenge. Es ist anschaulich plausibel und auch nicht allzu schwer zu beweisen, dass je zwei Fundamentalbereiche dasselbe Volumen haben. Dieses verallgemeinert die obige, bei der Definition von $\det L$ gemachte Feststellung, dass die Determinanten von je zwei Gram-Matrizen übereinstimmen, denn dieses sind ja die Volumina der von den beiden zugehörigen Basen aufgespannten Fundamentalquader, Beweis?

Dieses Volumen nennt man übrigens auch das *Covolumen* von L; es ist das „natürliche" Volumen von V/L, einer kompakten, n-dimensionalen Mannigfaltigkeit, die gleichzeitig Gruppe ist.

Kurze Vektoren in Gittern Das folgende Lemma beinhaltet eine grundlegende, zumindest in der Dimension 2 übrigens anschaulich völlig einsichtige geometrische (genauer: topologische) Eigenschaft von Gittern, nämlich deren Diskretheit. Mehr dazu in Abschnitt 1.4.

Lemma 1.2.9 Es sei L ein Gitter und α eine reelle Konstante. Dann existieren nur endlich viele $v \in L$ mit Quadratlänge $\langle v, v\rangle \le \alpha$.

Beweis: Wähle irgendeine Basis $v_1, \ldots, v_n$ von L und V, und betrachte die zugehörige Maximumsnorm $\|v\| = \max_{i=1,\ldots,n} |x_i|$, wobei $v = \sum x_i v_i \in V$, $x_i \in \mathbb{R}$. Da bekanntlich je zwei Normen auf V äquivalent sind, gibt es ein C mit $\|v\| \le C\sqrt{\langle v, v\rangle}$ für alle $v \in V$. Für $v \in L$, $v = \sum z_i v_i$, $z_i \in \mathbb{Z}$ mit $\langle v, v\rangle \le \alpha$ gilt also $|z_i| \le C\sqrt{\alpha}$. Also existieren höchstens $(2C\sqrt{\alpha + 1})^n$ solcher Gittervektoren v. □

Eine effektive Version dieses Lemmas, die zur expliziten Bestimmung aller v beschränkter Quadratlänge führt, geben wir später an; siehe auch schon das folgende Beispiel 1.3.1.

Die folgende Aussage ist eine unmittelbare Konsequenz des Lemmas 1.2.9.

Proposition 1.2.10 *Jedes Gitter L besitzt kürzeste Vektoren, d.h. die Menge aller Quadratlängen $\{\langle v, v\rangle \mid v \in L \setminus \{0\}\}$ besitzt ein kleinstes Element.*

Die Länge eines kürzesten Gittervektors und die Konfiguration aller kürzesten Vektoren, insbesondere ihre Anzahl, sind wichtige, intensiv studierte Invarianten eines Gitters. Deswegen gibt es hierfür eigene Bezeichnungen:

Bezeichnung 1.2.11

$$\begin{aligned} \min L &:= \min\{\langle v, v\rangle \mid v \in L \setminus \{0\}\} \\ \operatorname{Min} L &:= \{v \in L \mid \langle v, v\rangle = \min L\} \end{aligned}$$

Die Zahl $\min L$ heißt auch das *Minimum von* L. Die Elemente von $\operatorname{Min} L$ heißen *Minimalvektoren*. Die Anzahl $s(L) := |\operatorname{Min} L|$ der Minimalvektoren heißt die *Kontaktzahl* von L.

Der Grund für die Bezeichnung „Kontaktzahl“ wird im Abschnitt 1.4 näher erklärt: in der zum Gitter gehörigen Kugelpackung ist es die Anzahl der Kugeln, die eine gegebenen Kugel berühren.

Wir wollen schließlich noch festhalten, dass die frühere Proposition 1.2.6 zusammen mit Lemma 1.2.9 zumindest im Prinzip eine effektives Verfahren für das Testen von Gittern auf Isometrie liefert:

Bemerkung 1.2.12 (Prinzipieller Isometrietest) Gegeben seien zwei Gitter L und M der gleichen Dimension n und G die Gram-Matrix von L bezüglich einer Basis $v_1, \ldots, v_n$. Es sei λ das Maximum der Werte $g_{ii} = \langle v_i, v_i\rangle,\ i = 1, \ldots, n$, also das größte Diagonalelement von G. Bestimme in M die endliche Menge M_0 aller Vektoren $w \in M$ mit $\langle w, w\rangle \leq \lambda$. Überprüfe für alle n-Tupel $(w_1, \ldots, w_n)$ mit $\langle w_i, w_i\rangle = g_{ii},\ i = 1, \ldots, n$, ob auch $\langle w_i, w_j\rangle = g_{ij}$ ist für alle $i < j$. Wenn ein Tupel $(w_1, \ldots, w_n)$ dieses erfüllt, so wird durch $v_i \mapsto w_i,\ i = 1, \ldots, n$ eine Isometrie von L auf M definiert. Wenn kein solches Tupel existiert, so sind L und M nicht isometrisch.

Schließlich noch eine naheliegende Definition, die die zahlentheoretisch relevanten Gitter hervorhebt:

Definition 1.2.13 Ein Gitter L heißt *ganzzahlig*, falls $\langle x, y\rangle \in \mathbb{Z}$ für alle $x, y \in L$. Es heißt *gerade*, falls $\langle x, x\rangle \in 2\mathbb{Z}$ für alle $x \in L$.

Wegen

$$\langle x, y\rangle = \frac{1}{2}(\langle x + y, x + y\rangle - \langle x, x\rangle - \langle y, y\rangle)$$

gilt: jedes gerade Gitter ist ganzzahlig. Man überlegt sich leicht, daß ein Gitter genau dann ganzzahlig ist, wenn die Gram-Matrix bzgl. einer beliebigen Basis ganze Einträge hat und gerade, wenn zusätzlich die Diagonaleinträge gerade Zahlen sind. (Wenn dieses für eine Gram-Matrix gilt, dann auch für alle anderen.) Die ganzzahligen symmetrischen Matrizen mit gerader Diagonale sind uns bereits aus dem Schluss von Abschnitt 1.1 bekannt; gemäß Formel 1.1.10 entsprechen sie bijektiv den ganzzahligen quadratischen Formen. Proposition 1.2.7 liefert also eine bijektive Korrespondenz zwischen den Äquivalenzklassen ganzzahliger quadratischer Formen und den Isometrieklassen gerader Gitter.