2.5 Benachbarte Gitter nach M. Kneser

Wir stellen in diesem Abschnitt die Kneser'sche Methode der „benachbarten Gitter“ als ein Werkzeug zur Konstruktion von Gittern vor. Mit diesem Verfahren konstruiert man aus einen gegebenen Gitter L neue Gitter, die in demselben quadratischen $\mathbb{Q}$-Vektorraum liegen und die gleiche Determinante haben. Die Vorteile dieser Methode gegenüber klassischen Verfahren zur Auflistung von Gram-Matrizen (Stichwort: Reduktionstheorie) werden in der auch heute noch lesenswerten Einleitung der Original-Publikation von Martin Kneser dargestellt, in der die Nachbarmethode erstmalig entwickelt wurde:

> M. Kneser: *Klassenzahlen definiter quadratischer Formen.* Archiv der Mathematik **8** (1957), Seiten 241 – 250.

Wir stellen im folgenden auch um einige technische Details der Nachbarmethode dar, die für eine effiziente Computer-Implementierung nötig sind. Auf der anderen Seite müssen wir bezüglich der Tragweite der Methode, d.h. zur Beantwortung der Frage, welche Gitter denn nun auf diese Art ausgehend von einem bekannten Gitter konstruiert werden, auf die Literatur über die arithmetische Theorie der quadratischen Formen verweisen. Wir geben lediglich einen einfach zu formulierenden Spezialfall der allgemeinen Resultate an.

Definition 2.5.1 Es sei p eine Primzahl. Zwei Gitter L und L' auf demselben Vektorraum über $\mathbb{Q}$ heißen *p-Nachbarn*, falls

$$[L : L \cap L'] = [L' : L \cap L'] = p.$$

Wenn p aus dem Zusammenhang hervorgeht oder keine Rolle spielt, sprechen wir auch einfach von Nachbarn. Der Fall $p = 2$ hat für Anwendungen eine besondere Bedeutung. Wenn ohne weitere Erläuterung von Nachbarn die Rede ist, so sind immer 2-Nachbarn gemeint.

Beispiel 2.5.2 Das Gitter D_n^+ (vergl. 2.2) ist Nachbar des Standardgitters I_n; das gemeinsame Untergitter vom Index 2 ist D_n.

Wir bemerken, dass p-Nachbarn in einem Vektorraum mit symmetrischer Bilinearform bzw. quadratischer Form notwendig die gleiche Determinante haben.

Hilfssatz 2.5.3 Sei L ein ganzzahliges Gitter in einem quadratischen Vektorraum, p eine Primzahl, die $\det L$ nicht teilt. Wenn $y \in L \setminus pL$ ist mit $b(y, y) \in p^2\mathbb{Z}$, so ist

$$L(y) := L_y + \mathbb{Z}\tfrac{1}{p}y \text{ mit } L_y := \{x \in L \mid b(x, y) \in p\mathbb{Z}\}$$

ein ganzzahliger p-Nachbar von L. Jeder ganzzahlige p-Nachbar ist von dieser Form.

Beweis: Die Abbildung $L \to \mathbb{Q}$, $x \mapsto b(x,y)$ nimmt wegen $y \in L$ ihre Werte in $\mathbb{Z}$ an ($\mathbb{Z}_p$ bezeichnet die p-adischen Zahlen); jedoch ist wegen $y \notin p(\mathbb{Z}_p L)^\# = p\mathbb{Z}_p L$ ihr Bild nicht in $p\mathbb{Z}$ enthalten. Sie induziert also eine Surjektion $L \to \mathbb{Z}/p\mathbb{Z}$, deren Kern definitionsgemäß gleich L_y ist. Also ist $[L : L_y] = p$. Offensichtlich ist $p\frac{1}{p}y = y \in L_y$, wegen $\frac{1}{p}y \notin L$ ist also $[L(y) : L_y] = p$ und weiter $L \cap L(y) = L_y$, also $L(y)$ und L Nachbarn.

Sei umgekehrt M ein Nachbar von L. Wähle irgendein $y \in pM \smallsetminus pL$. Dann ist $b(L,y) \subsetneqq p\mathbb{Z}$, denn sonst wäre $\frac{1}{p}y \in L^\# \subseteq (\mathbb{Z}_p L)^\# = \mathbb{Z}_p L$ und damit $M = (M \cap L) + \mathbb{Z}\frac{1}{p}y \subseteq \mathbb{Z}_p L$, also $M \subseteq L$. Offensichtlich ist $L \cap M \subseteq L_y$. Insgesamt haben wir also die Inklusionskette $L \cap M \subseteq L_y \subsetneqq L$ mit $[L : L \cap M] = p$, also notwendig $L \cap M = L_y$ und weiter $M = L_y + \mathbb{Z}\frac{1}{p}y = L(y)$. □

Zur Illustration des Hilfssatzes betrachen wir das obige Beispiel: den Nachbarn D_n^+ von I_n erhält man als $D_n^+ = I_n(\mathbf{y})$ mit $\mathbf{y} = (1, \ldots, 1)$.

Im folgenden Hilfssatz beschreiben wir im Detail die Bedingungen an die Vektoren y zur Nachbarbildung sowie die Bedingungen für die Gleichheit zweier Nachbarn $L(y) = L(y')$. U.a. ergibt sich, daß jedes Gitter L nur endlich viele ganzzahlige Nachbarn besitzt. Für $p = 2$ können die Nachbarn sowohl gerade als auch ungerade sein.

Hilfssatz 2.5.4 Die Voraussetzungen seien wie in Hilfssatz 2.5.3.

a) Die Nachbarn $L(y)$ und $L(y')$ mit $y' = y + z$ stimmen überein, wenn $z \in pL$ und $b(y,z) \in p\mathbb{Z}$ ist (also $z \in pL_y$ ist).

b) Für $p \neq 2$ stimmen $L(y)$ und $L(y')$ bereits überein, wenn $y' - y \in pL$ ist. Das gleiche gilt für $p = 2$, wenn $L, L(y)$ und $L(y')$ gerade sind.

c) Wenn $p \neq 2$ und $v \in L$ ein Vektor mit $q(v) = \frac{1}{2}b(v,v) \equiv 0 \pmod{p}$ ist, so gibt es ein $y \in v + pL$ mit $q(y) \equiv 0 \pmod{p^2}$. Das gleiche gilt für $p = 2$ und gerade Gitter.

d) Jedes $\phi \in \mathrm{O}(L)$ induziert eine Isometrie des Nachbarn $L(y)$ auf den Nachbarn $L(\phi y)$.

Beweis: a) Für $z = y' - y \in pL$ gilt offensichtlich $L_y = L_{y'}$ und weiter $L(y') = L_{y'} + \mathbb{Z}\frac{1}{p}y' = L_y + \mathbb{Z}\frac{1}{p}(y+z) = L_y + \mathbb{Z}\frac{1}{p}y$, falls $z \in pL_y$.

b) Nach a) bleibt zu zeigen, dass $z = y' - y$ zwangsläufig in pL_y liegt. Es ist

$$b(y,y') = b(y,y) + 2b(y,z) + b(z,z)\,,$$

also $2b(y,z) \in p^2\mathbb{Z}$ und für $p \neq z$ folglich $b(y,z) \in p^2\mathbb{Z}$, wie behauptet. Für $p = 2$ sind nach Voraussetzung $b(y',y')$, $b(y,y)$, $b(z,z)$ sämtlich durch 8 teilbar, und wir können entsprechend schließen.

c) Wir machen für y den Ansatz $y = v + pz$, $z \in L$ und erhalten die Bedingung

$$q(y) = q(v) + pb(v,z) + p^2 q(z) \equiv 0 \pmod{p^2},$$

also $q(v)/p + b(v,z) \equiv 0 \pmod{p}$, was wegen $p \nmid \det L$ durch ein geeignetes $z \in L$ lösbar ist. Beachte, daß auch für $p = 2$ der Wert $q(z)$ voraussetzungsgemäß in $\mathbb{Z}$ liegt.

d) ist offensichtlich. □

Der letzte Hilfssatz zeigt insbesondere, dass die Nachbarbildung eine Angelegenheit modulo p ist, das heißt, die Restklasse modulo pL eines Vektors $y \in L$ entscheidet, ob y zur Bildung des Nachbarn $L(y)$ geeignet ist, und der Nachbar hängt nur von dieser Klasse ab. Dieses gilt für gerade Gitter auch im Fall $p = 2$. Ferner kann man die Restklasse $\bar{y} = y + pL$ bis auf Vielfache aus dem zugehörigen Nachbarn $L(y)$ zurückgewinnen: für die auf $\bar{L} := L/pL$ induzierte, nach Voraussetzung reguläre Bilinearform, steht $\bar{y}$ auf dem Bild von $L(y)$ in $\bar{L}$ senkrecht, muß also aus Dimensionsgründen gleich dem Orthogonalraum dieses Bildes sein. Der folgende Satz fasst die Diskussion zusammen.

Satz 2.5.5 *Es sei p eine Primzahl und L ein ganzzahliges, im Falle $p = 2$ sogar gerades Gitter auf einem quadratischen $\mathbb{Q}$-Vektorraum, p sei kein Teiler der Determinante von L. Die ganzzahligen und im Fall $p = 2$ geraden p-Nachbarn M von L entsprechen vermöge $M \mapsto ((L \cap M)/pL)^{\perp} \subset L/pL$ bijektiv und kanonisch den isotropen Geraden im quadratischen $\mathbb{F}_p$-Vektorraum L/pL.*

Als Beispiel für die Anwendung der letzten Sätze bestimmen wir alle Nachbarn des Gitters I_n mit Orthonormalbasis.

Beispiel 2.5.6 Die ganzzahligen 2-Nachbarn von I_n sind bis auf Isometrie genau die Gitter $\widetilde{D}_m \perp I_{n-m}$ mit $m \equiv 0 \pmod 4$, $0 \leq m \leq n$, $m \neq 4$ (vergl. auch Beispiel 2.5.2).

Beweis: Wir betrachten Nachbarn $I_n(\mathbf{y})$ mit $\mathbf{y} = \sum y_i \mathbf{e}_i, y_i \in \mathbb{Z}$, und schränken die Vektoren $\mathbf{y}$ gemäß Hilfssatz 1 ein. Falls ein $y_i \in 2\mathbb{Z}$ ist, so ersetze man $\mathbf{y}$ durch $\mathbf{y}' = \mathbf{y} - y_i \mathbf{e}_i$. Man kann also $y_i = 0$ erreichen. Ist $y_j = 4z_j \pm 1$, so ersetze man $\mathbf{y}$ durch $\mathbf{y}' = \mathbf{y} - 4z_j \mathbf{e}_i$. Man kann also $y_j = \pm 1$ erreichen. Nach Hilfssatz 2.5.4 d) kann man noch die $\mathbf{e}_j$ mit ± 1 multiplizieren und dadurch $y_j = 1$ erreichen. Nach Permutation der $\mathbf{e}_i$ bleibt für $\mathbf{y} = \mathbf{y}_m$ nur noch die Möglichkeit $y_i = 1$ für $i = 1, \ldots, m$, $y_i = 0$ für $i = m+1, \ldots, n$. Es ist $b(\mathbf{y}, \mathbf{y}) = m$; da dieser Wert in $4\mathbb{Z}$ liegen soll, muß $m \equiv 0 \pmod 4$ sein. Den Nachbarn $\widetilde{D}_4 \perp I_{n-4}$ führen wir nicht auf, da er isometrisch zu I_n ist. □

Es stellt sich nun die Frage, welche Gitter man, ausgehend von einem gegebenen Gitter, durch iterierte Bildung von p-Nachbarn erreichen kann. Dabei ist die Primzahl p als fixiert anzusehen. Die allgemeine Antwort erfordert kompliziertere Begriffe aus der arithmetischen Theorie der Quadratischen Formen, nämlich sogenannte Geschlechter und Spinorgeschlechter. Dieses würde den Rahmen dieser Vorlesung sprengen. Wir wollen lediglich ein Resultat angeben, das zumindest in

der Formulierung diese Begriffe nicht benutzt. Die Eigenschaft eines ganzzahligen Gitters, gerade bzw. ungerade zu sein, wollen wir, um leichter formulieren zu können, im folgenden manchmal als *Parität* des Gitters bezeichnen.

Theorem 2.5.7 *Es sei p eine Primzahl und L ein Gitter der Dimension ≥ 3 bzw. ≥ 5, falls $p = 2$. Weiter sei $\ell L^{\#} \subseteq L$ für eine Primzahl $\ell \neq p$ oder $\ell = 1$. Dann erhält man durch wiederholte Bildung von p-Nachbarn aus L alle Gitter der gleichen Dimension, Determinante und für $\ell \neq 2$ gleichen Parität wie L.*

Die angegebene Bedingung besagt, dass die Diskriminantengruppe $L^{\#}/L$ von L ℓ-elementar, also ein direktes Produkt von lauter Gruppen $\mathbb{Z}/\ell\mathbb{Z}$ ist; insbesondere ist $\det L$ eine Potenz von ℓ. Die Dimensionsbedingung im Satz ist eine hinreichende Bedingung für eine andere, technisch komplizierte Bedingung; sie kann insbesondere für $p = 2$ in aller Regel durch eine schwächere Bedingung ersetzt werden, die auch in den Dimensionen 3 und 4 anwendbar ist. In der Dimension 2 ist die Nachbarmethode „oft“ nicht anwendbar, wird allerdings auch nicht benötigt, da mit der Reduktionstheorie eine einfachere und in diesem Fall effizientere Methode zur Konstruktion von Gittern zur Verfügung steht.

Wir schließen mit einer (von vielen möglichen) Anwendungen des (nicht bewiesenen) Theorems 2.5.7. Wie schon erwähnt, heißt ein Gitter *unimodular*, wenn es ganzzahlig ist und die Determinante 1 hat.

Satz 2.5.8 *Die einzigen unimodularen Gitter in den Dimensionen $n \leq 8$ sind I_n und E_8.*

Beweis: Für $n \leq 7$ sind nach Beispiel 2.5.6 alle Nachbarn von I_n zu I_n isometrisch. Für $n = 5, 6, 7$ folgt damit die Behauptung direkt aus dem Theorem. Wegen der eindeutigen Zerlegbarkeit eines Gitters ind Unzerlegbare folgen die Fälle $n \leq 4$, sogar alle Fälle $n < 7$ sofort aus dem Fall $n = 7$. Einen einfacheren Beweis für $n \leq 5$, der das Theorem nicht benutzt, führt man mittels der Hermite-Abschätzung aus Satz 1.4.7: ein solches Gitter enthält einen Vektor der Quadratlänge 1, der automatisch orthogonal abspaltet; mehrfache Anwendung liefert die Existenz einer Orthonormalbasis.

Es bleibt der Beweis im (essentiellen) Fall $n = 8$ zu führen. In dem Beispiel 2.5.6 haben wir bereits gesehen, dass jeder Nachbar von I_8 isometrisch zu I_8 oder E_8 ist. Mit ähnlichen Überlegungen zeigt man das gleiche für E_8, Die Details überlassen wir als Übungsaufgabe. □

Historische Anmerkung. M. Kneser hat mit der dargestellten Methode bereits 1957 alle unimodularen Gitter bis zur Dimension 16 klassifiziert. Gerade unimodulare Gitter existieren nur in durch 8 teilbaren Dimensionen.1968 hat H.V. Niemeier (ein Doktorand von Kneser) die 24-dimensionalen geraden unimodularen Gitter klassifiziert (es gibt 24 Stück, darunter das Leech-Gitter). In den 80er Jahren hat R.E. Borcherds auch die (wesentlich zahlreicheren) ungeraden unimodularen Gitter in Dimension 24 klassifiziert.