TECHNISCHE UNIVERSITÄT DORTMUND

Fakultät für Mathematik
Lehrstuhl II - Geometrie
Prof. Dr. Rudolf Scharlau

Vorlesung im Sommersemester 2009

Gitter und Codes

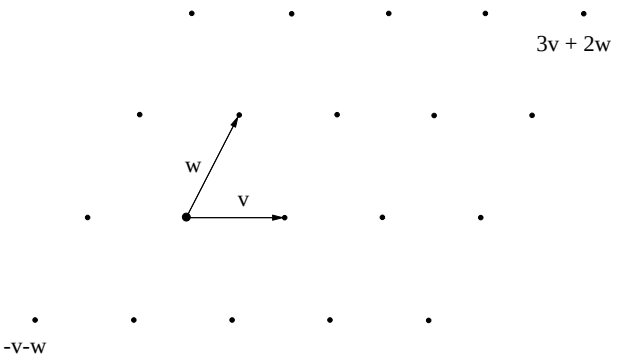
Wahlveranstaltung in den Studiengängen
Mathematik Diplom, Mathematik Promotion,
Informatik Diplom mit Nebenfach Mathematik

Termin :	Montag,	12 – 14 Uhr,	M/1011
	Donnerstag,	12 – 14 Uhr,	M/1011

Beginn der Vorlesung: Mittwoch, 16. April 2009

Inhalt der Vorlesung

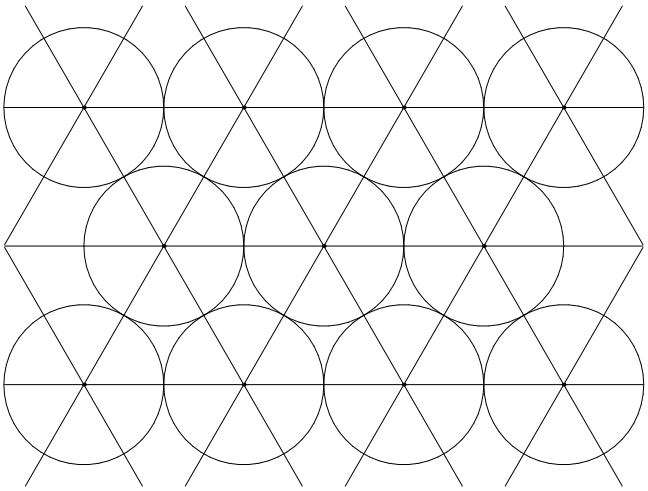
„Gitter und Codes" hat sich in den letzten Jahren als Bezeichung eines Gebietes eingebürgert, das in erster Linie in der Tradition der vor über 100 Jahren von Minkowski und Voronoi begründeten „Geometrie der Zahlen" gehört, aber auch starke Beziehungen zur algebraischen Codierungstheorie, algebraischen Zahlentheorie und zur Gruppentheorie hat (siehe unten). Wir geben eine kurze Beschreibung der Thematik.
Ein Gitter im n-dimensionalen euklidischen Raum $\mathbb{R}^n$ besteht definitionsgemäß aus den ganzzahligen Linearkombinationen einer (frei wählbaren) Basis des $\mathbb{R}^n$, etwa für $n = 2$ aus den Vektoren $x\mathbf{v} + y\mathbf{w}, x, y \in \mathbb{Z}$, für fest gewählte $\mathbf{v}, \mathbf{w} \in \mathbb{R}^2$. Zwei Gitter werden als „im wesentlichen gleich" angesehen, wenn sie kongruent (im Sinne der Geometrie) sind, also durch eine isometrische Abbildung ineinander überführt werden können.



In der Dimension 2 wird ein Gitter durch drei Parameter beschrieben, nämlich die beiden Längen zweier kürzestmöglicher Basisvektoren (in der Zeichnung $\mathbf{v}$ und $\mathbf{w}$) sowie den Winkel zwischen ihnen. Beispiele für Gitter der Dimension 2 liefern die Ringe ganzer Zahlen in quadratischen Zahlkörpern.

Gitter treten in verschiedenen mathematischen Fragestellungen auf: in der mathematischen Kristallographie als Mengen (sogar Gruppen) von Translationsvektoren einer kristallographischen Gruppe, in der Zahlentheorie als geometrische Realisierung von ganzzahligen quadratischen Formen, d.h. Ausdrücken des Typs $\sum a_{ij}x_ix_j$, $x_i \in \mathbb{Z}$, in

der Struktur- und Darstellungstheorie von Lie-Gruppen und Lie-Algebren als sogenannte Wurzelgitter und Gewichts-Gitter, in der diskreten Geometrie im Zusammenhang mit der dichtestmöglichen Packung von Kugeln im $\mathbb{R}^n$.



Die nebenstehende Zeichnung zeigt die bestmögliche Packung von Kreisen in der Ebene: etwa 90 % der Ebene sind durch die Vereinigung der Kreisscheiben überdeckt. Die Mittelpunkte bilden ein Gitter, das sogenannte hexagonale Gitter, identisch mit dem Wurzelgitter vom Typ A_2. Zahlentheoretisch kann dieses Gitter auch als der Ring $\mathbb{Z}[\zeta_3] \subset \mathbb{C}$ aufgefasst werden. Die zugehörige quadratische Form ist $x^2 + xy + y^2$.

Gewisse Gitter existieren in unendlichen Serien wachsender Dimension, also $L_n \subset \mathbb{R}^n$, $n = 1, 2, 3, \ldots$; so etwa das Standardgitter $\mathbb{Z}^n \subset \mathbb{R}^n$, oder die erwähnten Wurzelgitter A_n und D_n. Andere Gitter sind „Einzelstücke", sporadische Phänomene, die nur in wenigen oder sogar nur einer einzigen Dimension n auftreten.

Die Gitter in den Dimensionen 2, 3 und 4 sind sind unter geometrischem Aspekt in der mathematischen Kristallographie intensiv untersucht worden (Stichwort: Bravaisklassen); unter zahlentheoretischem Blickwinkel besteht ein enger, in der Literatur gut belegter Zusammenhang mit quadratischen Zahlkörpern und Quaternionenalgebren.

Ein besonders wichtiges sporadisches Gitter ist das exzeptionelle Wurzelgitter E_8 in Dimension 8, dieses hat u.a. mit dem aus der Codierungstheorie bekannten erweiterten Hamming-Code der Blocklänge 8 zu tun, aber auch mit Modulformen: Seine Thetareihe (siehe unten) stimmt mit der Eisensteinreihe von Gewicht 4 überein. Seine Automorphismengruppe ist die größte endliche Gruppe aus 8×8-Matrizen. Es liefert die dichteste gitterförmige Kugelpackung in Dimension 8.

Das unumstritten spektakulärste sporadische Gitter ist das Leech-Gitter in der Dimension $n = 24$. Die zugehörige Kugelpackung hat eine außerordentlich hohe Dichte, die sehr nahe an den theoretischen Schranken liegt und für Gitter beweisbar bestmöglich ist. Seine Automorphismengruppe ist (modulo $\pm\mathrm{Id}$) eine 26 sporadischen einfachen endlichen Gruppen, nämlich die Conway-Gruppe Co_1.

Verbindungen zu anderen mathematischen Gebieten

- *Diskrete Geometrie:* dichteste Packungen und Überdeckungen des n-dimensionalen euklidischen Raumes durch Kugeln
- *Zahlentheorie*: ganzzahlige quadratische Formen, insbesondere explizite Konstruktionen und Automorphismengruppen

- *algebraische Codierungstheorie:* das Problem optimaler fehlerkorrigierender Codes in endlichen Vektorräumen als Analogon des euklidischen Packungsproblems; explizite Konstruktion von Gittern mittels Codes
- *Algebra (Gruppentheorie):* Permutationsgruppen und ihre geometrische Realisierung, sporadische einfache Gruppen (Mathieu-Gruppen, Conway-Gruppen)
- *Kombinatorik:* Designs und Steiner-Systeme
- *Algebra (Lie-Algebren und Darstellungstheorie):* Wurzelsysteme und Spiegelungsgruppen; diese treten als Invarianten diverser algebraischer Strukturen auf
- *Funktionentheorie (Modulformen)*: die Transformationseigenschaften und die Fourierentwicklung von Thetareihen sind ein Mittel zur Abzählung von Gitterpunkten; Anzahlformeln für klassische Probleme der Zahlentheorie.

gewünschte Vorkenntnisse

Gute Kenntnisse der Grundvorlesungen Lineare Algebra und Analysis;
Algebrakenntnisse im Rahmen einer Vorlesung *Algebra I*;
Theorie der freien abelschen Gruppen, insbesondere der Elementarteilersatz (dieses ggf aus Algebra II).
Grundkenntnisse aus der algebraischen Codierungstheorie kann man sich nebenbei aneignen (Skript, Kapitel 2). Kenntnisse in (algebraischer) Zahlentheorie sowie über Modulformen sind an einigen Stellen nützlich, aber nicht notwendig.

Literatur

- W. Ebeling: *Lattices and Codes*, 2. Auflage Vieweg-Verlag 2002
- J.H. Conway, N.J.A. Sloane: *Sphere Packings, Lattices and Groups*, 3rd ed., Springer-Verlag 1999
- J. Martinet: *Perfect Lattices in Euclidean Spaces*, Springer-Verlag 2003

gez. R. Scharlau