1.5 Duales Gitter und Diskriminantengruppe

Dieser Abschnitt ist im wesentlichen algebraischer Natur: Es spielt keine Rolle, dass unsere Gitter in einem Vektorraum über $\mathbb{R}$ liegen, man könnte auch (mit der gleichen Definition) Gitter in Vektorräumen V über $\mathbb{Q}$ oder irgendeinem anderen Körper $\mathbb{K}$ der Charakteristik Null betrachten. Weiter benötigt man zur Definition der Gram-Matrix und der Determinante (Diskriminante) eines Gitters nicht unbedingt ein Skalarprodukt, es reicht eine nicht-entartete symmetrische Bilinearform $b : V \times V \to \mathbb{K}$. Z.B. kann $\mathbb{K} = \mathbb{Q},\ V = F$ eine endliche Körpererweiterung und b die aus der Algebra bzw. algebraischen Zahlentheorie bekannte Spurform sein, also

$$b(\alpha, \beta) := \mathrm{Tr}_{\mathbb{Q}}^{F}(\alpha\beta),\ \alpha, \beta \in F. \tag{1.5.1}$$

Statt der aus der Körpertheorie bekannten Spurabbildung $\mathrm{Tr}_{\mathbb{Q}}^{F}$ kann man sogar eine völlig beliebige, von null verschiedene Linearform $t : F \to \mathbb{Q}$, allgemeiner $t : F \to \mathbb{K}$ nehmen. Die Bilinearform

$$b_t : F \times F \to \mathbb{K}, \quad (\alpha, \beta) \mapsto t(\alpha\beta), \tag{1.5.2}$$

ist immer nicht-entartet, wie man sofort aus der Existenz von Inversen im Körper F ableitet.

Ein *Teilgitter* oder *Untergitter* eines Gitters L ist eine Teilmenge $K \subseteq L$, die selbst ein Gitter ist. Aus der allgemeinen Theorie freier abelscher Gruppen (der „ganzzahligen linearen Algebra") weiß man, dass jede Untergruppe K von L ein Untergitter ist. D. h., K besitzt eine Basis aus über $\mathbb{Z}$ und dann auch über $\mathbb{R}$ linear unabhängigen Vektoren. Im Augenblick benutzen wir diesen Sachverhalt noch nicht. Jedoch benötigen wir folgende Tatsache, die sich unmittelbar aus dem Elementarteilersatz ergibt.

Proposition 1.5.1 *Es seinen $L \subseteq M$ Gitter vom gleichen Rang n und $S \in \mathbb{Z}^{n\times n}$ die Matrix eines Basiswechsels von einer Basis von M zu einer von L. Dann gilt*

$$[M : L] = |\det S|,$$

wobei $[M : L]$ den Gruppenindex von L in M bezeichnet. Insbesondere ist dieser Index endlich.

Beweis: Klar ist zunächst, dass der Betrag $|\det S|$ unabhängig von den gewählten Basen ist. Denn Basiswechsel innerhalb von L oder M haben jeweils die Determinante ± 1. Wähle nun nach dem Elementarteilersatz eine Basis $v_1, \ldots, v_n$ von M so, dass Skalare $d_1, \ldots, d_n$ derart existieren, dass $d_1 v_1, \ldots, d_n v_n$ eine Basis von L ist. Die Matrix des Basiswechsels ist dann die Diagonalmatrix mit Einträgen $d_1, \ldots d_n$, hat also die Determinante $d = d_1 \cdot d_2 \cdot \cdots \cdot d_n$. Das Urbild von L unter dem zugehörigen Basisisomorphismus $\mathbb{Z}^n \to M$ ist gleich $d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z}$.

Also ist M/L isomorph zu $\mathbb{Z}^n/(d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z})$, was wiederum isomorph zu $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$, also von der Ordnung d ist. □

Eine Folgerung von 1.5.1 ist die ständig benutzte, schon bei den obigen Beispielen nützliche

Satz 1.5.2 (Determinanten-Index-Formel) *Es seien $L \subseteq M$ Gitter vom selben Rang in einem (euklidischen) Vektorraum. Dann gilt*

$$\det L = [M : L]^2 \cdot \det M \, .$$

Zum Beweis seien $\mathcal{A}$ und $\mathcal{B}$ Basen von M bzw. L und S die Matrix des Basiswechsels von $\mathcal{A}$ zu $\mathcal{B}$. Für die zu $\mathcal{A}$ und $\mathcal{B}$ gehörigen Gram-Matrizen G bzw. H gilt dann $H = S^tGS$, also $\det L = \det M \cdot (\det S)^2$. Die Behauptung folgt nun aus 1.5.1. □

Die Determinanten-Index-Formel wird auch geometrisch unmittelbar einsichtig, wenn man daran denkt, dass $\sqrt{\det L}$ das Volumen eines Fundamentalbereichs des Gitters ist und noch folgende Überlegung anstellt. Wenn wir kurz $m = [M : L]$ für den Index schreiben, so erhält man einen Fundamentalbereich des kleineren Gitters L als Vereinigung von m kongruenten Kopien, sogar Translaten, eines Fundamentalbereichs des größeren Gitters M. Man nimmt nämlich die Translate $y_j + L$, wobei $y_1, \ldots, y_m$ ein Vertretersystem für die Faktorgruppe M/L ist. Das Volumen ver-m-facht sich also, wie in der Determinanten-Index-Formel behauptet.

Wir notieren noch eine einfache, häufig benutzte Folgerung:

Folgerung 1.5.3 Es seien L, M Gitter mit $L \subseteq M$ und $\det L = \det M$. Dann ist $L = M$.

Anwendungen hierfür haben wir schon gesehen, weitere werden folgen, z.B. beim Beweis von 1.5.6 d).

Wir kommen nun zur Definition des „dualen Gitters" zu einem gegebenen Gitters L. Wie man in der der Linearen Algebra den Dualraum $V^* := \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K})$ eines $\mathbb{K}$-Vektorraumes betrachtet, so kann man für eine endlich erzeugte freie abelsche Gruppe $L \cong \mathbb{Z}^n$ den dualen Modul

$$L^* := \mathrm{Hom}(L, \mathbb{Z}) \quad \textbf{(dualer Modul)} \tag{1.5.3}$$

betrachten. Dieses ist in natürlicher Weise wieder eine abelsche Gruppe, und mit der üblichen Definition „dualer Basen" zeigt man schnell, das L^* wieder frei vom gleichen Rang, also $L^* \cong \mathbb{Z}^n$ ist.

Da unsere Gitter nicht nur abstrakte Gruppen, sondern Untergruppen eines Vektorraumes sind, bietet sich folgende weitere Definition an:

Definition 1.5.4 Es sei L ein Gitter auf V. Dann ist auch

$$L^\# := \{y \in V \mid \langle x, y\rangle \in \mathbb{Z} \text{ für alle } x \in L\}$$

ein Gitter auf V. Es heißt das zu L *duale Gitter* (bezüglich der auf V gegebenen nicht-entarteten Bilinearform).

Beweis: Sei $v_1, \ldots, v_n$ irgendeine Basis von L. Sei $v_1^\#, \ldots, v_n^\#$ die hierzu bezüglich der Bilinearform duale Vektorraumbasis, also $\langle v_i, v_j^\#\rangle = \delta_{ij}$. Man überlegt sich sofort, dass $L^\# = \mathbb{Z}v_1^\# + \ldots + \mathbb{Z}v_n^\#$ gilt. □

Wir tragen noch nach, warum die „duale Basis bezüglich einer Bilinearform" existiert (und tatsächlich wieder eine Basis ist): Wenn b eine nicht-entartete Bilinearform auf V ist, dann ist die Abbildung

$$\widehat{b} : V \to V^*,\ y \mapsto b(-, y) \tag{1.5.4}$$

ein Vektorraumisomorphismus. Die behauptete Basis $v_1^\#, \ldots, v_n^\#$ von V ist einfach das Urbild der üblichen dualen Basis $v_1^*, \ldots, v_n^*$ von V^* unter diesem Isomorphismus. Aus dem Isomorphismus $\widehat{b}$ kann man weiter noch folgendes ablesen:

Bemerkung 1.5.5 Es sei L ein Gitter auf einem $\mathbb{K}$-Vektorraum V mit nicht entarteter Bilinearform b. Dann ist die Abbildung

$$\widehat{b}_L : L^\# \to L^*,\ y \mapsto b(-, y) \tag{1.5.5}$$

ein Isomorphismus abelscher Gruppen.

Jeder Homomorphismus $L \to \mathbb{Z}$ kann nämlich (mittels einer Basis) eindeutig zu einer $\mathbb{K}$-linearen Abbildung $V \to \mathbb{K}$ fortgesetzt werden, und der diese Abbildung darstellende Vektor (gemäß 1.5.4) liegt dann definitionsgemäß in $L^\#$. □

Die beiden verschiedenen Duale eines Gitters sind also kanonisch isomorph.

Wir notieren erste Eigenschaften des dualen Gitters. Man beachte, dass die Teile a) und b) der folgenden Proposition von dualen Basen und nicht wirklich von Gittern handeln.

Proposition 1.5.6 *a) Sei $\mathcal{B} = (v_1, \ldots, v_n)$ eine beliebige Vektorraumbasis und $\mathcal{B}^\# = (v_1^\#, \ldots, v_n^\#)$ die bezüglich des Skalarporduktes duale Basis. Dann ist die Gram-Matrix $G = G_\mathcal{B}$ die Matrix des Basiswechsels von $\mathcal{B}^\#$ zu $\mathcal{B}$.*

b) Die Gram-Matrix von $\mathcal{B}^\#$ ist gleich G^{-1}.

c) Für jedes Gitter L gilt $\det L^\# = (\det L)^{-1}$.

d) Ein Gitter L ist genau dann ganzzahlig, wenn $L \subseteq L^\#$ ist.

e) Wenn L ein ganzzahliges Gitter ist, so ist $[L^\# : L] = |\det L|$

Beweis:

a) Formelmäßig bedeutet die Behauptung:

$$\sum_{i=1}^{n} g_{ij} v_i^\# = v_j \text{ für } j = 1, \ldots, n.$$

Es reicht zu sehen, dass beide Seiten das gleiche Skalarprodukt mit einem belebigem v_k haben. Dieses folgt unmittelbar aus den Definitionen.

b) folgt aus a) und der allgemeinen Transformationsformel für Gram-Matrizen bei Basiswechsel: die Gram-Matrix bzgl. der dualen Basis ist $(G^{-1})^t \, G \, G^{-1} = G^{-1} G G^{-1} = G^{-1}$.

c) ergibt sich unmittelbar aus b).

d) ist klar.

e) ergibt sich aus a) und der Determinanten-Index-Formel, angewendet auf $L \subseteq L^\#$. □

Das duale Gitter eines ganzzahligen Gitters L ist unter anderem nützlich, um ganzzahlige Obergitter $M \supset L$ zu bestimmen. Für solche M gilt wegen $b(M, L) \subseteq b(M, M) \subseteq \mathbb{Z}$ nämlich, dass $M \subseteq L^\#$ ist. Weiter ist M bei fixiertem L eindeutig durch die endliche Gruppe M/L bestimmt. In der folgenden Bemerkung klären wir, wie die zusätzliche Bedingung an M/L aussieht, damit das Urbild M wirklich ganzzahlig ist.

Proposition 1.5.7 Es sei (V, b) ein Vektorraum mit nicht-ausgearteter Bilinearform $L \subset V$ ein ganzzahliges Gitter auf V.

a) Die Faktorgruppe $T(L) := L^\#/L$ bezeichnet man als *Diskriminantengruppe* von L, genauer von (L, b). Die Bilinearform induziert eine bilineare Abbildung

$$\bar{b} : T(L) \times T(L) \to \mathbb{Q}/\mathbb{Z},$$

die sogenannte *Diskriminantenform* von (L, b).

b) Die Zuordung $M \mapsto M/L$ induziert eine Bijektion zwischen der Menge aller ganzzahligen Obergitter M von L und der Menge aller bezüglich $\bar{b}$ total-isotropen Untergruppen $\mathcal{M} \subseteq T(L)$.

"Total-isotrop" bedeutet wie bei Bilinearformen üblich: $\bar{b}(\mathcal{M}, \mathcal{M}) = 0$. Teil b) der letzten Proposition liefert den allgemeinen Rahmen für diverse Beziehungen zwischen Gittern und Codes, ebenso für die (von Conway und Sloane) so genannte "Gluing-Theorie". Um tatsächlich die angesprochenen Gruppen $\mathcal{M}$ sinnvoll als Codes betrachten zu können, muss allerdings auf $T(L)$ noch eine Metrik eingeführt werden. Dieses geschieht später in dieser Vorlesung. Z.B. wird in Kapitel 2.3 der übliche binäre Hamming-Raum der Codierungstheorie als Spezialfall einer Metrik auf einer Diskriminantengruppe auftauchen.

Wir notieren noch, wie die dualen Gitter der Wurzelgitter A_n und D_n aussehen.

Proposition 1.5.8

$$A_n^\# = A_n + \mathbb{Z}\tfrac{1}{n+1}(-n, 1, 1, \ldots, 1)$$

$$T(A_n) \cong \mathbb{Z}/(n+1)\mathbb{Z}$$

$$D_n^\# = \mathbb{Z}^n + \mathbb{Z}(\tfrac{1}{2}, \tfrac{1}{2}, \ldots, \tfrac{1}{2}) = D_n + \mathbb{Z}e_1 + \mathbb{Z}(\tfrac{1}{2}, \tfrac{1}{2}, \ldots, \tfrac{1}{2})$$

$$T(D_n) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \text{ falls } n \text{ gerade} \\ \mathbb{Z}/4\mathbb{Z}, \text{ falls } n \text{ ungerade.} \end{cases}$$

Zum Beweis rechnet man nach, dass das angegebene Gitter, nennen wir es L', jedenfalls in $L^\#$ enthalten ist und dass ferner der Index von L' über L gleich $\det L$ ist. Dann folgt die gewünschte Gleichheit $L' = L^\#$ aus 1.5.3. Weiter ergibt sich mittels der angegebenen Erzeuger leicht die behauptete Struktur von $L^\#$.

Übungsaufgaben zu Abschnitt 1.5

Aufgabe 1.5.1
Wir betrachten den $\mathbb{R}^3$ mit dem Standardskalarprodukt. Es sei W ein Würfel, dessen sämtliche Ecken $\mathbb{Z}^3$ liegen. Zeige, dass die Kantenlänge von W eine ganze Zahl ist.

Hinweis: O.B.d.A. sei ein Eckpunkt von W der Nullpunkt. Betrachte das von den Ecken erzeugte Gitter.

Aufgabe 1.5.2
Bestimme alle ganzzahligen Obergitter der folgenden Gitter:

a) $A_2 \perp A_2$

b) $A_4 \perp \mathbb{Z}w$, wobei $\langle w, w\rangle = 45$.

c) $A_4 \perp \mathbb{Z}z$, wobei $\langle z, z\rangle = 10$.

d) $A_2 \perp A_2 \perp A_2$

e) $D_4 \perp D_4$.