G. Nebe, M. Kirschmer

Gitter und Codes, WS 08/09

Lösung 14

Aufgabe 1.

Sei $(E,q) \cong [1,1,1,1]$ ein quadratischer $\mathbb{Q}_2$-Vektorraum. Angenommen E ist nicht anisotrop. Dann existieren $x_1,\dots,x_4 \in \mathbb{Q}_2$ mit $\sum_{i=1}^n x_i = 0$. Ohne Einschränkung ist $\min\{v_2(x_i) \mid 1 \le i \le 4\} = 0$. Betrachten wir nun diese Gleichung modulo $8\mathbb{Z}_2$. Für $a \in 2\mathbb{Z}$ ist $a^2 \equiv_4 0$ und für $a \in 1+2\mathbb{Z}$ ist $a^2 \equiv_8 1$. Also ist $\sum_{i=1}^4 x_i^2 \in 8\mathbb{Z}_2$ nur möglich, falls alle x_i in $2\mathbb{Z}_2$ liegen. Das widerspricht aber der Wahl der x_i.

Zeigen wir nun, daß (E,q) universell ist. Dazu müssen wir $q(E) = \mathbb{Q}_2$ zeigen. Sicher ist $q(0) = 0$. Ferner ist $q(\lambda e) = \lambda^2 q(e)$ für alle $e \in E$ und $\lambda \in \mathbb{Q}_2^*$. Also genügt es zu zeigen, daß $q(E)$ ein Vertretersystem von $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ enthält. Ein solches ist bekanntlich durch $\{1,3,5,7,2,6,10,14\}$ gegeben. Daß diese Vertreter als Bilder von E unter q vorkommen prüft man leicht nach.

Aufgabe 2.

Ist $v \in L$ und $\lambda \in \mathbb{Z}_p$, so ist auch $\lambda v \in L$. Zeigen wir nun, daß $v,w \in L$ auch $v+w \in L$ impliziert. Seien dazu $v,w \in L - \{0\}$.

Angenommen v,w sind linear abhängig über $\mathbb{Q}_p$. Ohne Einschränkung ist $q(v) \le q(w)$ und $w = \lambda v$ mit $\lambda \in \mathbb{Q}_p$. Wegen $\lambda^2 = q(w)/q(v) \in \mathbb{Z}_p$ ist $\lambda \in \mathbb{Z}_p$ und damit $q(v+w) = (1+\lambda)^2 q(v) \in \mathbb{Z}_p$ also $v+w \in L$.

Seien nun v und w linear unabhängig über $\mathbb{Q}_p$. Wegen $q(v+w) = q(v) + q(w) + b_q(v,w)$ genügt es zu zeigen, daß $b_q(v,w) \in \mathbb{Z}_p$. Angenommen $i := v_p(b_q(v,w)) < 0$. Wir setzen

$$f(X) := p^{-i} \cdot q(v+Xw) = p^{-i} \cdot (X^2 q(w) + X b_q(v,w) + q(v)) \in \mathbb{Z}_p[X]\,.$$

Sei $a_0 := \frac{-q(v)}{b_q(v,w)} \in \mathbb{Z}_p$. Dann ist $v_p(f(a)) = v_p(p^{-i} \cdot a_0^2 \cdot q(v)) \ge -i + 2v_p(a_0) > 0$. Weiter ist $f'(X) = p^{-i}(2Xq(w) + b_q(v,w))$ und somit $v_p(f'(a_0)) = -i + v_p(2a_0 + b_q(v,w)) = -i + i = 0$, da $2a_0 \in \mathbb{Z}_p$ und $b_q(v,q) \notin \mathbb{Z}_p$. Insbesondere liftet die Nullstelle a_0 zu einer Nullstelle $a \in \mathbb{Z}_p$. Da v und w linear unabhängig sind, ist $v + aw \neq 0$ aber $q(v+aw) = 0$ ein Widerspruch zu (E,q) anisotrop.

Bis jetzt haben wir gezeigt, daß L ein $\mathbb{Z}_p$-Modul in E ist. Bleibt zu zeigen, daß L endlich erzeugt ist und eine $\mathbb{Q}_p$-Basis von E enthält. Sei dazu $(b_1,\dots,b_n)$ eine Basis von E.
Dann ist $v_p(q(b_i)) = 2k_i + r_i$ mit $k_i \in \mathbb{Z}$ und $r_i \in \{0,1\}$. Wir setzen $b_i' = p^{-k_i} b_i$. Dann ist $v_p(q(b_i')) \in \{0,1\}$ und $M := \langle b_1',\dots,b_n' \rangle$ ist ein $\mathbb{Z}_p$-Gitter mit $M \subseteq L$.
Sei $v \in L$ beliebig. Dann sind $q(b_i)$ und $q(v)$ in $\mathbb{Z}_p$. Nach dem bereits gezeigten ist dann auch $b_q(v,b_i) \in \mathbb{Z}_p$ und daher $L \subseteq M^\# = \{x \in E \mid b_q(x,y) \in \mathbb{Z}_p \text{ für alle } y \in L\}$. Da b_q regulär ist, ist $M^\#$ ein $\mathbb{Z}_p$-Gitter, also endlich erzeugt. Somit gilt dies auch für L.

Daß L das maximal ganze Gitter ist, ist klar.

Aufgabe 3.

Wir beginnen mit einer kleinen Bemerkung.

Bemerkung: Sei L ein ganzes Gitter in einem Euklidischen Vektorraum (V,b) vom Rang 2.

(a) L besitzt eine Grammatrix $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ mit $a,b,c \in \mathbb{Z}$ und

$$0 < a \le 2\sqrt{\det(L)/3} \qquad a \le c \qquad 0 \le b \le a/2$$

(b) Ist $G = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ eine Grammatrix von L mit dem obigen Eigenschaften, so ist $a = \min(L)$.

Beweis:

(a) Sei $a = \min(L)$ und $v \in L$ mit $b(v,v) = a$. Dann ist $0 < a \leq 2 \cdot \sqrt{\det(L)/3}$ nach Lemma 11.5. Sei nun (b_1, b_2) irgendeine Basis von L. Dann ist $v = x_1 b_1 + x_2 b_2$ mit $x_i \in \mathbb{Z}$. Wäre $g := \gcd(x_1, x_2) \notin \mathbb{Z}^*$, so wäre $g^{-1} \cdot v \in L$ kürzer als v, was der Wahl von a widerspricht. Also ist $g \in \mathbb{Z}^*$ und somit existiert nach dem Elementarteilersatz eine Basis (v, w) von L.

Für jedes $k \in \mathbb{Z}$ ist dann auch $(v, w + kv)$ eine Basis von L. Insbesondere findet man ein k mit $b := b(v, w + vk) = b(v,w) + ka$ im Intervall $[-a/2, a/2]$. Nach eventuellem Multiplizieren dieses Vektors mit -1 ist $b \geq 0$ und wir haben eine Grammatrix mit den gewünschten Eigenschaften konstruiert.

(b) Sei $B := (e_1, e_2)$ eine Basis von L mit $\mathcal{G}(B) = G$. Für $x := x_1 e_1 + x_2 e_2 \in L - \{0\}$ ist

$$\begin{aligned} b(x,x) &= x_1^2 a + x_2^2 c + 2x_1 x_2 b \geq (x_1^2 + x_2^2)a - 2|x_1 x_2| b \geq a \cdot (x_1^2 - |x_1 x_2| + x_2^2) \\ &= a \cdot ((|x_1| - |x_2|)^2 + |x_1 x_2|) \\ &\geq a \quad \text{da } x \neq 0\,. \end{aligned}$$

Jetzt zur Aufgabe:

(a) Jedes Gitter mit Determinante 15 besitzt eine Grammatrix $G = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ wie oben mit $1 \leq a \leq 4$.

Mit der obigen Bemerkung findet man durch Ausprobieren aller Möglichkeiten die folgenden 4 Grammatrizen:

$$G_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 15 \end{smallmatrix}\right) \qquad G_2 = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 8 \end{smallmatrix}\right) \qquad G_3 = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 5 \end{smallmatrix}\right) \qquad G_4 = \left(\begin{smallmatrix} 4 & 1 \\ 1 & 4 \end{smallmatrix}\right)$$

Die zugehörigen Gitter L_1, L_2, L_3 und L_4 sind nicht isometrisch, da sie nach der obigen Bemerkung verschiedene Minima haben.

Wir behaupten, daß all diese Gitter in verschiedenen Geschlechtern liegen. Da L_1 und L_3 ungerade sind, die anderen aber gerade, können höchstens L_1 und L_3 bzw. L_2 und L_4 im selben Geschlecht liegen.

Betrachten wir L_1 und L_3 tensoriert mit $\mathbb{Z}_3$. Die zugehörigen Jordanzerlegungen sind $\mathrm{Diag}(1, 15)$ und $\mathrm{Diag}(5, 3)$. Da 5 kein Quadrat in $\mathbb{Z}_3^*$ ist, können die Gitter über $\mathbb{Z}_3$ nicht isometrisch sein (Jordanzerlegungen sind eindeutig bis auf Isometrie).

Betrachten wir nun L_2 und L_4 tensoriert mit $\mathbb{Z}_3$. Die zugehörigen Jordanzerlegungen liefern die Grammatrizen $\mathrm{Diag}(2, d_2)$ und $\mathrm{Diag}(4, d_2)$ mit $d_i \in 3\mathbb{Z}_3$. Da 2 kein Quadrat in $\mathbb{Z}_3^*$ ist, sind die Gitter über $\mathbb{Z}_3$ nicht isometrisch.

(b) Jedes Gitter mit Determinante 11 besitzt eine Grammatrix $G = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ wie oben mit $1 \leq a \leq 3$.

$$G_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 11 \end{smallmatrix}\right) \qquad G_2 = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 6 \end{smallmatrix}\right) \qquad G_3 = \left(\begin{smallmatrix} 3 & 1 \\ 1 & 4 \end{smallmatrix}\right)$$

Die zugehörigen Gitter L_1, L_2 und L_3 sind wieder nicht isometrisch, da sie verschiedene Minima haben. Weiter ist L_2 gerade und somit nicht im Geschlecht der ungeraden Gitter L_1 und L_3.

Wir behaupten, daß L_1 und L_3 im selben Geschlecht sind. Sei p eine ungerade Primzahl. Das Gitter $L_3 \otimes \mathbb{Z}_p$ besitzt einen Vektor der Länge 4 und somit einen der Länge 1. Dieser spaltet orthogonal ab. Über $\mathbb{Z}_2$ existiert auch so eine Zerlegung: Sei $B = (e, f)$ eine Basis von L_3 mit Grammatrix $\mathcal{G}(B) = G_3$. Dann ist $b(e + f, e + f) = 9$. Also besitzt $L_2 \otimes \mathbb{Z}_2$ der Länge 1 und dieser spaltet orthogonal ab.

Für jede Primzahl p hat $L_3 \otimes \mathbb{Z}_p$ daher eine Grammatrix $\mathrm{Diag}(1, d)$ mit $d \in \mathbb{Z}_p$ und $d \equiv 11 \bmod (\mathbb{Z}_p^*)^2$. Also sind $L_1 \otimes \mathbb{Z}_p$ und $L_3 \otimes \mathbb{Z}_p$ isometrisch.