G. Nebe, M. Künzer

Quadratische Formen, WS 05/06

Lösung 13

Aufgabe 46.

Sei (E, b) ein bilinearer $\mathbf{Z}$-Modul mit $\operatorname{rk} E \leq 4$. Sei $\det E = 2$.

(1) Aus der Hermiteschranke (18.1) folgt, daß $\min E \leq (4/3)^{(n-1)/2} \cdot 2^{1/n}$, i.e., daß $\min E \leq 2$ für $\operatorname{rk} E = 1$ und $\min E \leq 1$ für $\operatorname{rk} E \in [2, 4]$.

Wir führen eine Induktion nach $\operatorname{rk} E$. Sei $\operatorname{rk} E = 1$. Nur $\langle 2 \rangle$ hat Determinante 2.

Sei nun $\operatorname{rk} E \in [2, 4]$. Ist $\min E = 1$, so sei $e \in E$ mit $|b(e, e)| = 1$. Dann ist $\langle e \rangle_{\mathbf{Z}}$ scharf primitiv in E, also $E = \langle e \rangle \perp \langle e \rangle^{\perp}$. Nach Induktion ist $\langle e \rangle^{\perp}$ von der behaupteten Gestalt. Da $\langle e \rangle_{\mathbf{Z}} \simeq \langle \pm 1 \rangle$, gilt dies auch für E.

Ist $\min E = 0$, so sei $e \in E$ primitiv mit $b(e, e) = 0$. Sei $b(e, E) =: a\mathbf{Z}$, $a > 0$. Wähle $f \in E$ mit $b(e, f) = a$. Da mit $\tilde{E} := E + \langle a^{-1} e \rangle$ auch $\tilde{E}$ in $\tilde{E}^{\#}$ liegt, und da $a^{-1} e$ wegen der Primitivität von e die Ordnung a in $\tilde{E}/E$ hat, ist $E \overset{a}{\subseteq} \tilde{E} \subseteq \tilde{E}^{\#} \overset{a}{\subseteq} E^{\#}$, und also a^2 ein Teiler von $|E^{\#}/E| = \det E = 2$, und also $a = 1$. Somit ist $\langle e, f \rangle_{\mathbf{Z}} = \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & * \end{smallmatrix} \right\rangle$, und wir können mit einer weiteren Ersetzung von f auch noch $\langle e, f \rangle_{\mathbf{Z}} = \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right\rangle$ oder $\langle e, f \rangle_{\mathbf{Z}} = \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix} \right\rangle$ erreichen. Dieser Teilraum spaltet ab. Da $\langle e, f \rangle_{\mathbf{Z}}^{\perp}$ nach Induktion von der behaupteten Gestalt ist, gilt dies auch für E, sobald wir es für $\langle e, f \rangle_{\mathbf{Z}}$ eingesehen haben. Falls $\langle e, f \rangle_{\mathbf{Z}} = \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right\rangle$, so ist dies unmittelbar der Fall. Falls $\langle e, f \rangle_{\mathbf{Z}} = \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix} \right\rangle$, so spaltet darin $\langle f \rangle \simeq \langle 1 \rangle$ ab, und wir erhalten $\langle e, f \rangle_{\mathbf{Z}} \simeq \langle 1 \rangle \perp \langle -1 \rangle$. Es ist dann übrigens $\langle f \rangle^{\perp} = \langle e - f \rangle_{\mathbf{Z}}$.

(2) Wir bemerken zunächst, daß wir eine Isometrie

$$\begin{array}{rcl} \langle -1 \rangle \perp \langle 2 \rangle & \xrightarrow{\sim} & \langle 1 \rangle \perp \langle -2 \rangle \\ e_1 & \longmapsto & e_1' + e_2' \\ e_2 & \longmapsto & 2e_1' + e_2' \end{array}$$

haben, wobei e_1 Erzeuger von $\langle -1 \rangle$, und e_2 Erzeuger von $\langle 2 \rangle$ sei, und analog auf der rechten Seite.

$\operatorname{rk} E = 1$. Hier gibt es nur $\langle 2 \rangle$.

$\operatorname{rk} E = 2$. Nach (1) sind alle Gitter isometrisch zu einem der folgenden.

$$\langle 1 \rangle \perp \langle 2 \rangle,\ \langle -1 \rangle \perp \langle -2 \rangle\ .$$

Über $\mathbf{R}$ unterscheiden sich deren Signaturen, so daß sie nicht zueinander isometrisch sind. Es liegen also bereits Repräsentanten vor.

$\operatorname{rk} E = 3$. Nach (1) und der Vorbemerkung sind alle Gitter isometrisch zu einem der folgenden.

$$\langle 1 \rangle \perp \langle 1 \rangle \perp \langle 2 \rangle,\ \langle -1 \rangle \perp \langle -1 \rangle \perp \langle 2 \rangle,\ \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right\rangle \perp \langle -2 \rangle\ .$$

Über $\mathbf{R}$ hat ersteres Signatur 3, das zweite und das dritte hingegen Signatur -2. Das dritte Gitter ist jedoch im Gegensatz zum zweiten ein gerades Gitter. Also ist dies bereits eine Liste von Repräsentanten von Isometrieklassen für den Rang 3.

$\operatorname{rk} E = 4$. Nach (1) und der Vorbemerkung sind alle Gitter isometrisch zu einem der folgenden.

$$\langle 1 \rangle \perp \langle 1 \rangle \perp \langle 1 \rangle \perp \langle 2 \rangle,\ \langle 1 \rangle \perp \langle -1 \rangle \perp \langle -1 \rangle \perp \langle 2 \rangle,\ \langle -1 \rangle \perp \langle -1 \rangle \perp \langle -1 \rangle \perp \langle -2 \rangle,\ \langle 1 \rangle \perp \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right\rangle \perp \langle -2 \rangle\ .$$

Ersteres hat Signatur 4, zweiteres und vierteres Signatur 0, und dritteres Signatur -4.

Wenn wir die Standardbasis des zweiten mit (e, f, g, h) bezeichnen, so wird etwa $\langle f + g + h,\, e - f \rangle_{\mathbf{Z}} = \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right\rangle$. Dieser Teilraum spaltet ab, und $\langle f + g + h,\, e - f \rangle_{\mathbf{Z}}^{\perp} = \langle -e + f - g,\, 2f + g \rangle_{\mathbf{Z}}$. Da $\langle -e + f - g \rangle_{\mathbf{Z}} = \langle 1 \rangle$, spaltet dieser Teilraum ab, und wegen der Determinante ist sein Komplement isometrisch zu $\langle -2\rangle$. Dies zeigt, daß das das zweite isometrisch zum vierten ist. Somit erhalten wir z.B. Repräsentanten

$$\langle 1\rangle \perp \langle 1\rangle \perp \langle 1\rangle \perp \langle 2\rangle,\ \langle -1\rangle \perp \langle -1\rangle \perp \langle -1\rangle \perp \langle -2\rangle,\ \langle 1\rangle \perp \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right\rangle \perp \langle -2\rangle\ .$$

Aufgabe 47.

(1) (i) Zu zeigen ist hierzu, daß

$$ax^2 + 2cxy + by^2 \ \overset{!}{\geq}\ a$$

für $(x, y) \in \mathbf{Z}^2 \smallsetminus \{0\}$. Quadratisch ergänzt bedeutet dies gerade

$$\left(x + \frac{c}{a}\, y\right)^2 + \left(\frac{b}{a} - \frac{c^2}{a^2}\right) y^2 \ \overset{!}{\geq}\ 1$$

Beachte, daß $\frac{b}{a} \geq 1$, $\frac{c}{a} \leq \frac{1}{2}$ und $\frac{c^2}{a^2} \leq \frac{1}{4}$. Ist $y = 0$, so ist $|x| \geq 1$, und also bereits der erste Summand ≥ 1. Ist $|y| = 1$ und $x = 0$, so steht insgesamt $\frac{b}{a} \geq 1$ auf der linken Seite. Ist $|y| = 1$ und $|x| \geq 1$, so ist der erste Summand $\geq \frac{1}{4}$, und der zweite $\geq \frac{3}{4}$. Ist $|y| \geq 2$, so ist der zweite Summand ≥ 3.

(ii) Mit $a = 2$, $b = 2$ und $c = 1$ erhalten wir nach (i) als Minimum 2. Und auch die Hermite-Schranke ergibt sich zu

$$(4/3)^{(n-1)/2} |\det(E)|^{1/2} \ =\ (4/3)^{1/2} \cdot 3^{1/2} \ =\ 2\ .$$

(2) (i) Es ist

$$\mathrm{v}_p(b(f, f')) \ =\ \mathrm{v}_p(2b(f, f')) \ =\ \mathrm{v}_p(b(f + f', f + f') - b(f, f) - b(f', f')) \ \geq\ i\ .$$

Insbesondere ist $(L, p^{-i}b)$ ein bilinearer $\mathbf{Z}_p$-Modul. Wegen $p^{-i}b(e, e) \in \mathbf{Z}_p^*$ ist $\langle e\rangle_{\mathbf{Z}_p}$ scharf primitiv. Also können wir $L = \langle e\rangle_{\mathbf{Z}_p} \perp \langle e\rangle_{\mathbf{Z}_p}^{\perp}$ zerlegen.

(ii) Iteriert man die Zerlegung aus (i), so erhält man eine Orthogonalbasis $(e_1, \ldots, e_n)$ von E, mit $\mathrm{v}_p(b(e_i, e_i))$ monoton wachsend. Setzt man nun

$$L_k \ :=\ \langle e_i \ :\ \mathrm{v}_p(b(e_i, e_i)) = k\rangle_{\mathbf{Z}_p}$$

für $k \geq 0$, und $b_k := p^{-k} b|_{L_k \times L_k}$, so erhält man eine Zerlegung wie gewünscht.

Wir bemerken noch, daß $L_j^{\#} = p^{-j} L_j$ für $j \geq 0$ bezüglich $(L_j, p^j b_j)$, wie man e.g. unter Zuhilfenahme einer Zerlegung gemäß der Orthogonalbasis erkennt.

(iii) Allgemein vertauscht $(-)^{\#}$ mit der orthogonalen Summe; vgl. die Lösung zu Aufgabe 41 (3). Also genügt es, zum einen für $j \geq k+1$ zu zeigen, daß $L_j/(L_j \cap p^{k+1} L_j^{\#}) = 0$, i.e. daß $L_j \subseteq p^{k+1} L_j^{\#}$. Dies folgt aber aus $L_j^{\#} = p^{-j} L_j$ wegen $j \geq k+1$. Zum anderen ist zu zeigen, daß

$$\begin{array}{rcl} L_k/pL_k & \longrightarrow & L_k/(L_k \cap p^{k+1} L_k^{\#}) \\ x + pL_k & \longmapsto & x + (L_k \cap p^{k+1} L_k^{\#}) \end{array}$$

wohldefiniert und bijektiv ist. Daß es eine Isometrie ist, folgt dann aus der Tatsache, daß jeweils die induzierten Bilinearformen betrachtet werden.

Bleibt also zu zeigen, daß $pL_k = L_k \cap p^{k+1} L_k^{\#}$. Dies folgt aber aus $L_k^{\#} = p^{-k} L_k$, wie man unter Zuhilfenahme einer Zerlegung gemäß der Orthogonalbasis erkennt.

(iv) Wir führen eine Induktion über den Rang. Sei $k \geq 0$ minimal mit $L_k \neq 0$ oder $\tilde{L}_k \neq 0$. Mit (iii) verschwinden dann beide nicht, und sind zueinander isometrisch, wie man mittels (13.6) aus der Vorlesung erkennt.

Bleibt zu zeigen, daß $L_k^{\perp} \simeq \tilde{L}_k^{\perp}$.

Wir bemerken zunächst, daß $(L_k, p^{-k}b)$ und $(\tilde{L}_k, p^{-k}b)$ als reguläre orthogonale Summanden scharf primitiv sind.

Wir dürfen nun die uns unbekannte Tatsache aus Kneser (4.4) verwenden (Satz von Witt für lokale Ringe), daß es eine Isometrie $L \xrightarrow[\sim]{f} L$ mit $f(L_k) = \tilde{L}_k$, und entsprechend dann auch $f^{-1}(\tilde{L}_k) = L_k$ gibt. Insbesondere ist für $x \in L_k^\perp$ auch

$$b(f(x), \tilde{L}_k) \;=\; b(f(x), f(L_k)) \;=\; b(x, L_k) \;=\; 0\;,$$

woraus wir $f(x) \in \tilde{L}_k^\perp$ ersehen, und somit $f(L_k^\perp) \subseteq \tilde{L}_k^\perp$. Genauso $f^{-1}(\tilde{L}_k^\perp) \subseteq L_k^\perp$. Also ist in der Tat $L_k^\perp$ zu $\tilde{L}_k^\perp$ isometrisch.

(3) (i) Nach (1.i) ist das Minimum von E gleich 2, und das Minimum von F gleich 8. Das Minimum ist aber eine Invariante unter Isometrie. Also sind E und F nicht isometrisch.

(ii) Sei zunächst $p \geq 3$. Wir vergleichen die Jordanzerlegungen. Deren Konstruktion folgt (2.i). Mit $e := (\begin{smallmatrix} 1 & 0 \end{smallmatrix})$ ist $\mathrm{v}_p(b(e,e)) = \mathrm{v}_p(2) = 0$. Ferner ist $\langle e\rangle_{\mathbf{Z}_p}^\perp = \langle e'\rangle_{\mathbf{Z}_p}$, wobei $e' := (\begin{smallmatrix} -1 & 2 \end{smallmatrix})$, und somit $E_p = \langle e\rangle_{\mathbf{Z}_p} \perp \langle e'\rangle_{\mathbf{Z}_p} \simeq \langle 2, 2\cdot 63\rangle$ jordanzerlegt.
Mit $f := (\begin{smallmatrix} 1 & 0 \end{smallmatrix})$ ist $\mathrm{v}_p(b(f,f)) = \mathrm{v}_p(8) = 0$. Ferner ist $\langle f\rangle_{\mathbf{Z}_p}^\perp = \langle f'\rangle_{\mathbf{Z}_p}$, wobei $f' := (\begin{smallmatrix} -1 & 8 \end{smallmatrix})$, und somit $F_p = \langle f\rangle_{\mathbf{Z}_p} \perp \langle f'\rangle_{\mathbf{Z}_p} \simeq \langle 8, 8\cdot 63\rangle$ jordanzerlegt.
Wir erkennen, daß $E_p \simeq \langle 2, 2\cdot 63\rangle \simeq \langle 8, 8\cdot 63\rangle \simeq F_p$, da 4 ein Quadrat in $\mathbf{Z}_p$ ist.
Sei nun $p = 2$. Es sind E_2 und F_2 regulär. Es ist ist $E/2E \simeq \left\langle\begin{smallmatrix} 2 & 1 \\ 1 & 32 \end{smallmatrix}\right\rangle = \left[\begin{smallmatrix} 1 & 1 \\ & 0 \end{smallmatrix}\right]$ isometrisch zu einer hyperbolischen Ebene. Ferner ist $E/2E \simeq \left\langle\begin{smallmatrix} 8 & 1 \\ 1 & 8 \end{smallmatrix}\right\rangle = \left[\begin{smallmatrix} 0 & 1 \\ & 0 \end{smallmatrix}\right]$ eine hyperbolischen Ebene. Aus $E/2E \simeq F/2F$ folgt nun mit (13.6), daß $E_2 \simeq F_2$.
Schließlich ist auch die Signatur beidmalig gleich 2.

(4) Sei $p \geq 3$ prim. Es genügt, die Jordanzerlegungen zu vergleichen. Deren Konstruktion folgt (2.i). Mit $e := (\begin{smallmatrix} 1 & 0 \end{smallmatrix})$ ist $\mathrm{v}_p(b(e,e)) = \mathrm{v}_p(2) = 0$. Ferner ist $\langle e\rangle_{\mathbf{Z}_p}^\perp = \langle e'\rangle_{\mathbf{Z}_p}$, wobei $e' := (\begin{smallmatrix} -1 & 2 \end{smallmatrix})$, und somit

$$E_p \;=\; \langle e\rangle_{\mathbf{Z}_p} \perp \langle e'\rangle_{\mathbf{Z}_p} \;\simeq\; \langle 2, 2\cdot 15\rangle$$

jordanzerlegt; wobei genau dann zwei Jordansummanden $E_{p,i}$ nicht verschwinden, wenn $p \in \{3,5\}$.
Mit $f := (\begin{smallmatrix} 1 & 0 \end{smallmatrix})$ ist $\mathrm{v}_p(b(f,f)) = \mathrm{v}_p(4) = 0$. Ferner ist $\langle f\rangle_{\mathbf{Z}_p}^\perp = \langle f'\rangle_{\mathbf{Z}_p}$, wobei $f' := (\begin{smallmatrix} -1 & 4 \end{smallmatrix})$, und somit

$$F_p \;=\; \langle f\rangle_{\mathbf{Z}_p} \perp \langle f'\rangle_{\mathbf{Z}_p} \;\simeq\; \langle 4, 4\cdot 15\rangle$$

jordanzerlegt; wobei wiederum genau dann zwei Jordansummanden $F_{p,i}$ nicht verschwinden, wenn $p \in \{3,5\}$.

Sei nun $p \in \{3,5\}$. Dann ist der jeweilige Jordansummand $E_{p,0} = \langle 2\rangle$ resp. $F_{p,0} = \langle 4\rangle$. Reduzieren wir modulo p, so erkennen wir, daß $E_{p,0}/pE_{p,0}$ und $F_{p,0}/pF_{p,0}$ nicht isometrisch sind, da $4/2 = 2$ kein Quadrat in $\mathbf{F}_p$ ist. Also sind auch $E_{p,0}$ und $F_{p,0}$ nicht isometrisch. Mit (2.iv) sind nun E_p und F_p nicht isometrisch, da eine solche Isometrie eine Jordanzerlegung von E_p auf eine Jordanzerlegung von F_p abbilden würde.