G. Nebe, M. Künzer

Gitter und Codes, SS 07

Lösung 1

Aufgabe 1.

Allzuviel Topologie wird in der Vorlesung nicht auftreten. Diese Aufgabe ist insofern untypisch.

Schreibe $B = (b_1, \ldots, b_n)$.

(i) Wir wollen zeigen, daß $\mathcal{P}(B) = \{\sum_{i=1}^n a_i b_i \;:\; a_i \in [0,1]\}$ eine abgeschlossene Teilmenge des $\mathbf{R}^n$ ist.

Es ist $(-, b_j^*) : \mathbf{R}^n \longrightarrow \mathbf{R}$ stetig für alle $1 \leq j \leq n$. Sei A_j das Urbild von $[0,1] \subseteq \mathbf{R}$ unter dieser Abbildung. Als Urbild einer abgeschlossenen Menge ist A_j abgeschlossen.

Da $\sum_{i=1}^n a_i b_i$ unter $(-, b_j^*)$ auf a_j abgebildet wird, ist $\mathcal{P}(B) = \bigcap_{i=1}^n A_j$, und somit als Schnitt abgeschlossener Mengen abgeschlossen.

Bestimmen wir noch gleich den Rand $\partial\mathcal{P}(B)$ von $\mathcal{P}(B)$. Sei U_j das Urbild von $(0,1) \subseteq \mathbf{R}$ unter $(-, b_j^*) : \mathbf{R}^n \longrightarrow \mathbf{R}$. Als Urbild einer offenen Menge ist A_j offen. Sei $\mathcal{P}^0(B) := \bigcap_{i=1}^n U_j \subseteq \mathcal{P}(B)$. Es ist $\mathcal{P}^0(B) \subseteq \mathbf{R}^n$ offen als Schnitt offener Mengen.

Um zu zeigen, daß $\partial\mathcal{P}(B) = \mathcal{P}(B) \smallsetminus \mathcal{P}^0(B)$, müssen wir zeigen, daß $\mathcal{P}^0(B)$ der offene Kern von $\mathcal{P}(B)$ ist, daß also jeder innere Punkt von $\mathcal{P}(B)$ bereits in $\mathcal{P}^0(B)$ liegt.

In anderen Worten, wir müssen zeigen, daß für ein gegebenes Element $x \in \mathcal{P}(B) \smallsetminus \mathcal{P}^0(B)$ und ein gegebenes $\varepsilon > 0$ die offene Kugel $\mathrm{B}_\varepsilon(x)$ keine Teilmenge von $\mathcal{P}(B)$ ist.

Sei $x = \sum_{i=1}^n a_i b_i$ mit $a_i \in [0,1]$. Es ist für ein i der Koeffizient a_i in $\{0,1\}$. Sei ohne (wesentliche) Einschränkung $a_1 = 0$. Schreibe $\delta := \varepsilon|b_1|^{-1}/2 > 0$. Sei $x' := -\delta b_1 + \sum_{i=2}^n a_i b_i$ definiert. Es ist $x' \notin \mathcal{P}(B)$. Es ist $|x - x'| = \delta|b_1| = \varepsilon/2 < \varepsilon$, und somit $x' \in \mathrm{B}_\varepsilon(x)$. Also ist $\mathrm{B}_\varepsilon(x) \not\subseteq \mathcal{P}(B)$.

Ausgeschrieben wird also

$$\partial\mathcal{P}(B) \;=\; \{\sum_{i=1}^n a_i b_i \;:\; a_i \in [0,1],\text{ es gibt ein } 1 \leq i \leq n \text{ mit } a_i \in \{0,1\}\}\,.$$

(ii) Sei $x \in V$. Schreibe $x = \sum_{i=1}^n a_i b_i$ mit $a_i \in \mathbf{R}$. Für $a \in \mathbf{R}$ schreiben wir $\lfloor a \rfloor := \max(\mathbf{Z} \cap (-\infty, a])$. Es ist $\ell := \sum_{i=1}^n \lfloor a_i \rfloor b_i \in \langle B \rangle_{\mathbf{Z}} = L$, und zugleich $x - \ell = \sum_{i=1}^n (a_i - \lfloor a_i \rfloor)\, b_i \in \mathcal{P}(B)$, da ja $a_i - \lfloor a_i \rfloor \in [0,1) \subseteq [0,1]$ stets.

(iii) Seien $x = \sum_{i=1}^n a_i b_i$ und $x' = \sum_{i=1}^n a_i' b_i$ in $\mathcal{P}(B)$, und sei $x - x'$ in L. In anderen Worten, stets seien a_i und a_i' in $[0,1]$, und stets sei $a_i - a_i' \in \mathbf{Z}$. Für ein festes i ist also

$$\text{entweder} \quad a_i = a_i' \quad \text{oder} \quad (a_i' = 0 \text{ und } a_i = 1) \quad \text{oder} \quad (a_i' = 1 \text{ und } a_i = 0).$$

Wegen $x \neq x'$ kann nun nicht für alle i der Fall $a_i = a_i'$ eintreten. Somit gibt es ein i mit $a_i,\, a_i' \in \{0,1\}$. Gemäß der Bestimmung von $\partial\mathcal{P}(B)$ aus (i) sind also $x,\, x' \in \partial\mathcal{P}(B)$.

Aufgabe 2.

(1) Sei (b_1, b_2) eine Gitterbasis von L, bezüglich derer G die Grammatrix von L ist.

(i) Für $x = (\,1\;0\,)$ ist $(x,x) = xGx^{\mathrm{t}} = 2$. Wir behaupten, daß $m = 2$. Dafür haben wir zu zeigen, daß $(y,y) \geq 2$ für alle $y \in L \smallsetminus \{0\}$. Schreibe $y = a_1 b_1 + a_2 b_2$. Es ist $(y,y) = 2a_1^2 + 2a_2^2 + 2a_1 a_2 \equiv_2 0$. Da $(y,y) \geq 0$, folgt $(y,y) \geq 2$.

Bestimmen wir $\{y \in L \;:\; (y,y) = 2\}$. Schreiben wir wieder $y = a_1 b_1 + a_2 b_2$ mit $a_i \in \mathbf{Z}$, so haben wir $(y,y) = 2a_1^2 + 2a_2^2 + 2a_1 a_2 = 2$ zu lösen, oder aber

$$1 \;\overset{!}{=}\; a_1^2 + a_2^2 + a_1 a_2 \;=\; (a_1 + \frac{1}{2}a_2)^2 + \frac{3}{4}a_2^2\,.$$

Wir wollen folgendermaßen vorgehen. Zunächst zeigen wir, daß (a_1, a_2) aus einer gewissen endlichen Menge stammen müssen. Dann ermitteln wir die Lösungen durch Testen all dieser endlich vielen Elemente.

Sicher haben $|a_1 + \frac{1}{2}a_2| \leq 1$ und $|a_2| \leq 2 \cdot 3^{-1/2}$ zu sein. Wegen der geforderten Ganzzahligkeit ist also auch $|a_2| \leq 1$. Somit müssen alle Lösungen (a_1, a_2) im Parallelogramm mit den Ecken $(\frac{1}{2}, 1)$, $(-\frac{3}{2}, 1)$, $(-\frac{1}{2}, -1)$, $(\frac{3}{2}, -1)$ liegen. Durchprobieren der darin liegenden Punkte mit ganzzahligen Koordinaten liefert die sechselementige Lösungsmenge

$$K \;:=\; \{y \in L \;:\; (y,y) = 2\} \;=\; \{\pm b_1,\, \pm b_2,\, \pm(b_1 - b_2)\}\;.$$

(ii) Wir bestimmen zunächst alle Elemente von $\mathrm{Aut}(L)$. Ein solches Element schreiben wir als Matrix B' bezüglich der Basis (b_1, b_2). In den Zeilen dieser Matrix haben Vektoren b'_1 und b'_2 so zu stehen, daß $b'_i G {b'_j}^{\mathrm{t}} = g_{i,j}$ stets, wobei $G = (g_{i,j})_{i,j}$; i.e. $B'GB'^{\mathrm{t}} = G$. Insbesondere sind b'_1 und b'_2 aus der Menge K aus (i). Berechnen der Skalarprodukte je zweier verschiedener Elemente aus K liefert

$$\begin{array}{rcl} \mathrm{Aut}(L) & = & \Big\{ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&0\\1&-1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&-1\\1&0\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&-1\\0&-1\end{smallmatrix}\right), \\ & & \left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}-1&0\\-1&1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}0&1\\-1&1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}0&-1\\-1&0\end{smallmatrix}\right),\, \left(\begin{smallmatrix}-1&1\\-1&0\end{smallmatrix}\right),\, \left(\begin{smallmatrix}-1&1\\0&1\end{smallmatrix}\right) \Big\} \\ & \leq & \mathrm{GL}_2(\mathbf{Z})\;. \end{array}$$

Insbesondere ist $|\,\mathrm{Aut}(L)| = 12$. Eine (echte) Teilmenge von $\mathrm{Aut}(L)$, die die ganze Gruppe erzeugt, ist e.g. gegeben durch $\Big\{ \left(\begin{smallmatrix}0&1\\-1&1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right) \Big\}$.

Mittels dieser Erzeuger erkennt man, daß $\mathrm{Aut}(L) \simeq D_{12} := \langle a, b \;:\; a^6,\, a^b a\rangle$.

(2) Sei (b_1, b_2, b_3) eine Gitterbasis von L, bezüglich derer G die Grammatrix von L ist.

(i) Für $x = (\,1\;0\;0\,)$ ist $(x,x) = xGx^{\mathrm{t}} = 1$. Da $m \in \mathbf{Z}_{\geq 1}$ von vornherein bekannt ist, ist $m = 1$. Bestimmen wir $\{y \in L \;:\; (y,y) = 2\}$. Schreiben wir $y = a_1 b_1 + a_2 b_2 + a_3 b_3$ mit $a_i \in \mathbf{Z}$, so haben wir $(y,y) = a_1^2 + a_2^2 + a_3^2 = 1$ zu lösen. Wir erhalten

$$K \;:=\; \{y \in L \;:\; (y,y) = 1\} \;:=\; \{\pm b_1,\; \pm b_2,\; \pm b_3\}\;.$$

(ii) Wir bestimmen zunächst $\mathrm{Aut}(L)$. Ein Element darin schreiben wir als Matrix B' bezüglich der Basis (b_1, b_2, b_3). In den Zeilen dieser Matrix haben Vektoren b'_1, b'_2 und b'_3 so zu stehen, daß $b'_i G {b'_j}^{\mathrm{t}} = g_{i,j}$ stets, wobei $G = (g_{i,j})_{i,j}$; i.e. $B'GB'^{\mathrm{t}} = G$. Insbesondere sind b'_1, b'_2 und b'_3 aus der Menge K aus (i). Sei $\mathcal{S}_3 \leq \mathrm{GL}_3(\mathbf{Z})$ die Untergruppe der Permutationsmatrizen. Berechnen der Skalarprodukte je zweier Elemente aus K liefert

$$\mathrm{Aut}(L) \;=\; \big\{DS \;:\; S \in \mathcal{S}_3,\; D = \mathrm{diag}(\varepsilon_1, \varepsilon_2, \varepsilon_3),\; \varepsilon_i \in \{\pm 1\}\big\}\;.$$

Insbesondere ist $|\,\mathrm{Aut}(L)| = 8 \cdot 6 = 48$.

Eine (echte) Teilmenge von $\mathrm{Aut}(L)$, die die ganze Gruppe erzeugt, ist e.g. gegeben durch $\Big\{ \left(\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&0&0\\0&0&1\\0&1&0\end{smallmatrix}\right),\, \left(\begin{smallmatrix}-1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right) \Big\}$.

Es ist $\mathrm{Aut}(L)$ isomorph zum semidirekten Produkt von $C_2 \times C_2 \times C_2$ und $\mathcal{S}_3$, wobei letztere Gruppe auf ersterer vermöge Permutation der Einträge operiert. Dies wird auch als Kranzprodukt (wreath product) bezeichnet, $\mathrm{Aut}(L) \simeq C_2 \wr \mathcal{S}_3$.

Aufgabe 3.

Dem Algorithmus entnehmen wir, daß

$$b_i \;=\; b'_i \;+\; \sum_{j=1}^{i-1} \frac{(b_i, b'_j)}{(b'_j, b'_j)}\, b'_j\;.$$

Wegen der Orthogonalität von $(b'_1, \ldots, b'_i)$ folgt, daß

$$(b_i, b_i) \;=\; (b'_i, b'_i) \;+\; \sum_{j=1}^{i-1} \frac{(b_i, b'_j)^2}{(b'_j, b'_j)^2}\, (b'_j, b'_j) \;\geq\; (b'_i, b'_i)\;.$$

Aufgabe 4 (3 Punkte).

Sei (b_1, b_2, b_3) eine Gitterbasis von L, bezüglich derer die angegebene Grammatrix $G = (g_{i,j})_{i,j} := \left(\begin{smallmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{smallmatrix}\right)$ angenommen wird.

Die (im vorliegenden Fall ganzzahlige) Grammatrix beschreibt die Einbettung $L \subseteq L^\#$ bezüglich der Basen (b_1, b_2, b_3) von L und (b_1^*, b_2^*, b_3^*) von $L^\#$. Denn es ist $b_j = \sum_{i=1}^3 g_{i,j} b_i^*$ stets, wie eine Anwendung von $(-, b_k)$ zeigt.

Um $L^\#/L$ zu berechnen, bestimmen wir also die $\mathbf{Z}$-linearen Elementarteiler von G; es ergibt sich $(1, 4, 4)$. Somit ist $L^\#/L \simeq \mathbf{Z}/1 \oplus \mathbf{Z}/4 \oplus \mathbf{Z}/4 \simeq \mathbf{Z}/4 \oplus \mathbf{Z}/4 \simeq C_4 \times C_4$.