G. Nebe, M. Kirschmer

Gitter und Codes, WS 08/09

Lösung 1

Aufgabe 1.

(a) Es sei $B = (b_1, b_2)$ eine Basis von L mit $\mathcal{G}(B) = G$. Weiter sei $x = a_1 b_1 + a_2 b_2 \in L$ (also $a_i \in \mathbb{Z}$).

- Für $x \neq 0$ ist $0 < (x, x) = 2(a_1^2 + a_1 a_2 + a_2^2) \in 2\mathbb{Z}$. Wegen $(b_1, b_1) = 2$ folgt $\min(L) = 2$.
- Es ist $x \in S(L) \iff (x, x) = \min(L) = 2$. Dies ist äquivalent zu $a_1^2 + a_1 a_2 + a_2^2 - 1 = 0$. Fassen wir dies als quadratische Gleichung in a_1 auf, so hat diese genau dann eine Lösung, falls $D := a_2^2 - 4(a_2^2 - 1) = 4 - 3a_2^2$ nicht negativ ist. Dies ist nur für $a_2 \in \{-1, 0, 1\}$ der Fall. Einsetzen dieser Werte für a_2 liefert
$$S(L) = \{\pm b_1, \pm b_2, \pm(b_1 - b_2)\}\ .$$
- Ein Element $\varphi \in \mathrm{End}(V)$ identifizieren wir mit seiner Matrixdarstellung ${}_B\varphi_B$ bezüglich der $\mathbb{Q}$-Basis B von V. Dann ist $\varphi \in \mathrm{Aut}(L)$ genau dann wenn ${}_B\varphi_B \in \mathrm{GL}_2(\mathbb{Z})$ und $({}_B\varphi_B) G ({}_B\varphi_B)^{\mathrm{tr}} = G$ gelten.
Also ist $\varphi \in \mathrm{Aut}(L)$ genau dann, wenn $b_1\varphi \in S(L)$, $b_2\varphi \in S(L) \setminus \{\pm(b_1\varphi)\}$ und $(b_1\varphi, b_2\varphi) = 1$ gelten. Explizites Nachrechnen liefert:
$$A := \{{}_B\varphi_B \mid \varphi \in \mathrm{Aut}(L)\} = \left\{ \begin{array}{cccc} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), & \left(\begin{smallmatrix} 1 & 0 \\ 1 & -1 \end{smallmatrix}\right), & \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), & \left(\begin{smallmatrix} -1 & 0 \\ -1 & 1 \end{smallmatrix}\right), \\ \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), & \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right), & \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right), & \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right), \\ \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right), & \left(\begin{smallmatrix} 1 & -1 \\ 0 & -1 \end{smallmatrix}\right), & \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right), & \left(\begin{smallmatrix} -1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \end{array} \right\}$$
Damit ist $|\mathrm{Aut}(L)| = 12$.
Seien nun $a := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ und $b := \left(\begin{smallmatrix} -1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in A. Dann haben a und b Ordnung 2 und ab hat Ordnung 6. Also erzeugen die beiden Elemente a und b eine Untergruppe von A welche isomorph zu D_{12} ist. Also ist $A = \langle a, b \rangle \cong D_{12}$.

(b) Siehe (c).

(c) Es sei $B = (b_1, \ldots, b_n)$ eine Basis von L mit $\mathcal{G}(B) = G$. Weiter sei $x = \sum_{i=1}^n a_i b_i \in L$.

- Für $x \neq 0$ ist $0 < (x, x) = \sum_{i=1}^n a_i^2 \in \mathbb{Z}$ und $(b_1, b_1) = 1$. Also ist $\min(L) = 1$.
- Es ist $S(L) = \{x \in L \mid (x, x) = 1\} = \{\pm b_i \mid 1 \leq i \leq n\}$.
- Jedes $\varphi \in \mathrm{Aut}(L)$ permutiert die Elemente in $S(L)$. Da B eine Basis von L ist, legen die Bilder $b_1\varphi, \ldots, b_n\varphi \in S(L)$ den Automorphismus φ eindeutig fest.
Insbesondere gilt $b_i\varphi \in S(L) \setminus \{\pm(b_j\varphi) \mid 1 \leq j < i\}$ stets. Damit ist $|\mathrm{Aut}(L)|$ nach oben beschränkt durch $N := \prod_{i=1}^n (|S(L)| - 2(i-1)) = \prod_{k=0}^{n-1} (2n - 2k) = 2^n \cdot n!\ .$
Wir behaupten, es gilt $|\mathrm{Aut}(L)| = N$. Dazu bestimmen wir einige Automorphismen, die eine Gruppen der Ordnung N erzeugen. Sei wieder $A := \{{}_B\varphi_B \mid \varphi \in \mathrm{Aut}(L)\}$.
Ist $n = 1$ so ist sicher $A = \langle (-1) \rangle$. Sei daher nun $n \geq 2$ angenommen. Wir setzen $X_i := \mathrm{Diag}(1, \ldots, 1, -1, 1, \ldots, 1) \in \mathrm{GL}_n(\mathbb{Z})$ mit -1 an der i-ten Stelle. Für $\sigma \in S_n$ bezeichne Y_σ die zu σ gehörende Permutationsmatrix. Dann ist $Y_\sigma G Y_\sigma^{\mathrm{tr}} = Y_\sigma Y_\sigma^{-1} = G$. Also sind $X := \langle X_1, \ldots, X_n \rangle$ und $Y := \langle Y_\sigma \mid \sigma \in S_n \rangle = \langle Y_{(1,2)}, Y_{(1,\ldots,n)} \rangle$ Untergruppen von A. Weiter ist X ein Normalteiler in $\langle X, Y \rangle$ denn es gilt $Y_\sigma^{-1} X_i Y_\sigma = Y_{\sigma^{-1}} X_i Y_\sigma = X_{\sigma(i)}$.
Da alle Elemente in $X \setminus \{I_n\}$ einen negativen Eintrag haben, folgt $X \cap Y = \{I_n\}$. Mit dem Homomorphiesatz folgt $|\langle X, Y \rangle| = |X| \cdot |Y| = 2^n \cdot n!$ und somit $A = \langle X, Y \rangle$.
Insbesondere läßt sich A im Fall $n \geq 2$ durch die zwei- bzw. dreielementige Menge $\{X_1, Y_{(1,2)}, Y_{(1,\ldots,n)}\}$ erzeugen.

Bemerkung: Es ist also $\mathrm{Aut}(L)$ isomorph zum semidirekten Produkt von $C_2 \times \cdots \times C_2$ (n Kopien) und S_n, wobei die symmetrische Gruppe S_n auf den Kopien der C_2 durch Permutation operiert. Dies wird auch *Kranzprodukt* (engl. *wreath product*) genannt.

Aufgabe 2.
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 3.
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 G 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 $\mathbb{Z}$-linearen Elementarteiler von G; es ergibt sich $(1, 4, 4)$. Somit ist $L^{\#}/L \cong \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \cong C_4 \times C_4$.

Aufgabe 4.
Sei $B = (b_1, \ldots, b_n)$. Für $a \in \mathbb{R}$ schreiben wir $\lfloor a \rfloor := \max(\mathbb{Z} \cap (-\infty, a])$.

(i) Wir wollen zeigen, daß $\mathcal{P}(B) = \{\sum_{i=1}^n a_i b_i \mid a_i \in [0,1]\}$ eine abgeschlossene Teilmenge von $(V, (-,=))$ ist.

Aus dem Gram-Schmidt-Verfahren (oder der Tatsache, daß je zwei Normen auf V äquivalent sind) folgt, daß $(-, b_j^*) : V \to \mathbb{R}$, $\sum_{i=1}^n a_i b_i \mapsto a_j$ stetig ist für alle $1 \leq j \leq n$. Sei A_j das Urbild von $[0,1] \subset \mathbb{R}$ 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 $(0,1) \subset \mathbb{R}$ unter $(-, b_j^*) : V \to \mathbb{R}$. Als Urbild einer offenen Menge ist A_j offen. Sei $\mathcal{P}^0(B) := \bigcap_{i=1}^n U_j \subset \mathcal{P}(B)$. Es ist $\mathcal{P}^0(B) \subset V$ offen als Schnitt offener Mengen.

Um zu zeigen, daß $\partial\mathcal{P}(B) = \mathcal{P}(B) \setminus \mathcal{P}^0(B)$, 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 $x \in \mathcal{P}(B) \setminus \mathcal{P}^0(B)$ 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 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

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

(ii) Sei $x \in V$. Schreibe $x = \sum_{i=1}^n a_i b_i$ mit $a_i \in \mathbb{R}$. Dann ist $\ell := \sum_{i=1}^n \lfloor a_i \rfloor b_i \in \langle B \rangle_{\mathbb{Z}} = L$ und $x - \ell = \sum_{i=1}^n (a_i - \lfloor a_i \rfloor)\, b_i \in \mathcal{P}(B)$, da ja $a_i - \lfloor a_i \rfloor \in [0,1)$ 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 $a_i - a'_i \in \mathbb{Z}$. 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 $x,\, x' \in \partial\mathcal{P}(B)$.