Prof. C. P. Schnorr Sommersemester 2009

Gitter und Kryptographie

Blatt 7, 03.06.2009, Abgabe Mittwoch, 10.06.2009

Definition. Das *duale* (polare oder reziproke) Gitter $\mathcal{L}^*$ zum Gitter $\mathcal{L}$ ist

$$\mathcal{L}^* = \{x \in \operatorname{span}(\mathcal{L}) \mid \langle x, b\rangle \in \mathbb{Z} \text{ für alle } b \in \mathcal{L}\}.$$

Aufgabe 1: Zeige für $R^{-t} := (R^{-1})^t = (R^t)^{-1}$

1. Für die QR–Zerlegung $B = QR$ der Basis B gilt $\mathcal{L}(B)^* = \mathcal{L}(QR^{-t})$.

2. $\det \mathcal{L}^* = 1/\det \mathcal{L}$.

Hinweis: Kap. 1.2, Skript

Def.: Die Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathcal{L}$ heissen *paarweise reduziert*, wenn

1. $|\langle \mathbf{b}_i, \mathbf{b}_j\rangle| \|\mathbf{b}_j\|^{-2} \leq \frac{1}{2}$ für $1 \leq j < i \leq n$
2. $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \cdots \leq \|\mathbf{b}_n\|$.

Aufgabe 2: Zeige: Es gibt paarweise reduzierte Basen $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \in \mathbb{R}^3$, so dass $\|\mathbf{b}_1\|/\|\mathbf{b}_1 - \mathbf{b}_2 + \mathbf{b}_3\|$ beliebig groß ist.

Hinweis: Wähle $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ so dass $\|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \|\mathbf{b}_3\|$

$$\langle \mathbf{b}_1, \mathbf{b}_2\rangle = \tfrac{1}{2} \approx \langle \mathbf{b}_2, \mathbf{b}_3\rangle,\ \langle \mathbf{b}_1, \mathbf{b}_3\rangle \approx -\tfrac{1}{2}.$$

Aufgabe 3: Beweise

$\prod_{i=1}^n \lambda_i(\mathcal{L}) \leq \gamma_n^{n/2} \det \mathcal{L}$ für Gitter $\mathcal{L}$ der Dimension n.

Sei $\mathcal{L} = \mathcal{L}(B)$ und $R = \mathrm{GNF}(B)$, arbeite mit $R = (r_{i,j})$.

Hinweis: Beweis von Satz 2.3.1, Skript.