Prof. C. P. Schnorr Sommersemester 2016

# Gitter und Kryptographie

Blatt 1, Freitag, 15.04.2016, Abgabe Freitag, 22.04.2016

**Aufgabe 1.** Sei $\mathbf{A} = \mathbf{A}^t = [a_{i,j}] \in \mathbb{R}^{n\times n}$ und die Untermatrizen der ersten $i$ Zeilen unf Spalten von $\mathbf{A}$ seien regulär. Zeige, dass es eine eindeutige Zerlegung $\mathbf{A} = \mathbf{R}^t\mathbf{D}\mathbf{R}$ gibt, derart, dass $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$ eine obere Dreiecksmatrix ist (also $r_{i,j} = 0$ für $i > j$) mit $r_{i,i} > 0$ und $\mathbf{D}$ Diagonalmatrix mit Diagonale $(\sigma_1, \ldots, \sigma_n) \in \{\pm 1\}^n$.

*Hinweis LR*-Zerlegung der Numerik.

**Aufgabe 2.** Zeige für jede Basis $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{Z}^m$ und $D_i := (\det \mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_i))^2$:

1. $D_{i-1}\mathbf{b}_i^* \in \mathbb{Z}^m$, 2. $D_j\, \mu_{i,j} \in \mathbb{Z}$ für $j < i$.

*Hinweis*: Lemma 4.2.3, Skript.

**Aufgabe 3.** Seien $\mathbf{B} = \mathbf{Q}\mathbf{R}$, $\mathbf{Q}'\mathbf{R}' = \mathbf{B}'$ $QR$–Zerlegungen. Zeige, dass folgende Aussagen äquivalent sind:

**1.** $\mathbf{B}, \mathbf{B}'$ sind isometrisch

**2.** $\mathbf{R}, \mathbf{R}'$ sind isometrisch

**3.** $\mathbf{R}^t\mathbf{R} = \mathbf{R}'^t \cdot \mathbf{R}'$

**4.** $\mathbf{R} = \mathbf{R}'$

*Hinweis: Lemma 1.1.3 des Skripts zeigt einen Teil der Aufgabe.*

**Punktzahl 5 fuer Aufgaben 1,2 und 8 fuer Aufgabe 3**