

## Gitter und Kryptographie

Blatt 3, 02.11.2007, Abgabe 09.11.2007

**Aufgabe 1.** Sei  $\mathcal{L} \subset \mathbb{R}^m$  Gitter der Dim.  $n$  und  $\mathcal{B}_m(\mathbf{0}, r) \subset \mathbb{R}^m$  die  $m$ -dim. Kugel mit Mittelpunkt  $\mathbf{0}$  und Radius  $r$ . Zeige

$$\lim_{r \rightarrow \infty} |\mathcal{L} \cap \mathcal{B}_m(\mathbf{0}, r)| / \text{vol}(\mathcal{B}_m(\mathbf{0}, r)) = \frac{1}{\det \mathcal{L}(B)}$$

d.h.  $\det \mathcal{L}(B)$  ist der Kehrwert der Dichte der Gitterpunkte.

*Hinweis:* Satz 1.1.2, Skript.

Im Folgenden sei  $B = QR$ ,  $Q = (q_{i,j}) \in \mathbb{R}^{m \times n}$ ,  $R = (r_{i,j}) \in \mathbb{R}^{n \times n}$   $QR$ -Zerlegung der Basis  $B = (\mathbf{b}_1, \dots, \mathbf{b}_n) \in \mathbb{R}^{m \times n}$ .

**Aufgabe 2.** Zeige:

1. Für  $Q_k := (q_{i,j})_{1 \leq i \leq m, 1 \leq j \leq k}$ ,  $R_k := (r_{i,j})_{1 \leq i, j \leq k}$ ,  $B_k := (\mathbf{b}_1, \dots, \mathbf{b}_k)$

ist  $B_k = Q_k R_k$  die  $QR$ -Zerlegung.

2. Zeige die Eindeutigkeit der  $QR$ -Zerlegung, z.B. durch Induktion über  $k$ .

**Aufgabe 3.** Gib ein Verfahren an, welches zu gegebener Basis  $B = (b_{i,j}) \in \mathbb{R}^{m \times n}$  die  $QR$ -Zerlegung  $B = QR$  liefert, mit Operationen  $+$ ,  $\cdot$ ,  $/$ , sqrt. Zähle die Anzahl der Operationen.

**Aufgabe 4.** Zeige: Für  $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{Z}^m$ ,  $D_i := \det \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_i)^2$  gilt:

1.  $D_{i-1} \mathbf{b}_i^* \in \mathbb{Z}^n$ ,

2.  $D_j \mu_{i,j} \in \mathbb{Z}$  für  $j < i$ .

*Hinweis:* Lemma 4.2.3, Skript.