

**Gitter und Kryptographie**

Blatt 6, 23.11.2007, Abgabe 30.11.2007

**Aufgabe 1.** Zeige:

Die LLL-Reduktion, Alg. 3, transformiert linear abhängige Eingabevektoren  $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{Z}^m$  in  $(\mathbf{b}_1, \dots, \mathbf{b}_n)T = (\mathbf{0}^i, \mathbf{b}'_{i+1}, \dots, \mathbf{b}'_n)$  so dass  $\mathbf{b}'_{i+1}, \dots, \mathbf{b}'_n \in \mathbb{Z}^m$  linear unabhängig sind.

**Aufgabe 2.** Sei  $(\mathbf{b}_1, \dots, \mathbf{b}_n) = QR \in \mathbb{R}^{m \times n}$  Gitterbasis. Wie ändert die Vertauschung von  $\mathbf{b}_{k-1}, \mathbf{b}_k$  die  $r_{i,k-1}, r_{i,k}$  ?

Zeige für  $i = 1, \dots, k-2$ :  $r_{i,k-1}^{\text{neu}} = r_{i,k}^{\text{alt}}, r_{i,k}^{\text{neu}} = r_{i,k-1}^{\text{alt}}$ .

**Aufgabe 3.** Zeige, dass die Gitter

$$A_n = \{\mathbf{x} \in \mathbb{Z}^{n+1} \mid \langle \mathbf{x}, \mathbf{1} \rangle = 0\}$$

$$D_n = \{\mathbf{x} \in \mathbb{Z}^n \mid \langle \mathbf{x}, \mathbf{1} \rangle = 0 \pmod{2}\}$$

für  $n = 3$  isometrisch sind. Transformiere die gegebenen Basen im Skript, Seite 7, in isometrische Basen.

**Aufgabe 4.** Zeige:

Jedes Gitter  $\mathcal{L} \subset \mathbb{Z}^n$  hat eine Basis  $B = (b_{i,j})$  in oberer Dreiecksform,

d.h.  $b_{i,j} = 0$  für  $i < j$ .