

## Gitter und Kryptographie

Blatt 2, 22.04.2016, Abgabe 29.04.2016

**Aufgabe 1.** Zeige: das Gitter  $\mathcal{L}(\mathbf{B})$  mit Basis  $\mathbf{B} = \begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{3/4} \end{bmatrix}$  ist kritisch,  $\Delta(\mathcal{L}) = \Delta_2$ , und  $\gamma_2 = 2/\sqrt{3}$ .

*Hinweis* : Abb. 3.2.1 Skript Seite 26.

**Aufgabe 2.** Seien  $\mathcal{L}' \subset \mathcal{L}$  Gitter,  $\dim \mathcal{L}' < \dim \mathcal{L}$ . Zeige die Äquivalenz folgender Aussagen:

1.  $\text{span}(\mathcal{L}') \cap \mathcal{L} = \mathcal{L}'$ .
2. Jede Basis von  $\mathcal{L}'$  ist zu einer Basis von  $\mathcal{L}$  erweiterbar.

*Hinweis* : Beweis von Satz 1.3.2, Kap. 1.3 Skript.

**Aufgabe 3.** Zeige, dass die Gitter  $\mathbb{A}_3, \mathbb{D}_3$  auf Seite 7 des Skripts äquivalent zum Apfelsinen-Gitter mit Radius  $1/\sqrt{2}$  sind.

**Punktzahl pro Aufgabe: 5**