Prof. C. P. Schnorr Wintersemester 2005/06

Gitter und Kryptographie

Blatt 4, 18.11.2005, Abgabe 25.11.2005

Die Gitter $A_n := \{\mathbf{x} \in \mathbf{Z}^{n+1} | \langle \mathbf{x}, \mathbf{1} \rangle = 0\}$, $D_n := \{\mathbf{x} \in \mathbf{Z}^n | \langle \mathbf{x}, \mathbf{1} \rangle = 0 \bmod 2\}$ und die geschichteten (laminated) Gitter $\mathcal{L}^{(n)} = \mathcal{L}(R_n)$ für $n = 1, \ldots, 8$ haben Basen nach Kap. 2.1 und 3.2 (Seiten 7, 24, 25) des Vorlesungskripts.

Aufgabe 1. Konstruiere Basen von A_n und D_n mit Beweis.

Aufgabe 2. Zeige, dass A_3 und D_3 isometrisch sind. Transformiere die gegebenen Basen in isometrische Basen.

Aufgabe 3. Zeige, dass A_3 und $\mathcal{L}^{(3)}$ isometrisch sind. Transformiere die gegebenen Basen in isometrische Basen.

Aufgabe 4. Zeige, dass D_4 und $\mathcal{L}^{(4)}$ isometrisch sind. Transformiere die gegebenen Basen in isometrische Basen.