WOLFGANG K. SEILER
Tel. 2515

A5, C201

23. Oktober 2008

7. Übungsblatt Computeralgebra

Aufgabe 1: (*5 Punkte*)
Das Gitter $\Gamma \subset \mathbb{R}^5$ sei erzeugt von den Vektoren

$$\vec{b}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{b}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{b}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{b}_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{und} \quad \vec{b}_5 = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

a) Was ist $d(\Gamma)$?

b) Berechnen Sie nach GRAM-SCHMIDT die zugehörige Orthogonalbasis von $\mathbb{R}^5$, und zeigen Sie, daß obige Basis LLL-reduziert ist!

c) Zeigen Sie: Γ enthält fünf linear unabhängige Vektoren der Länge eins.

d) Bestimmen Sie alle Vektoren der Länge eins in Γ und zeigen Sie, daß es keine Gitterbasis aus Vektoren der Länge eins gibt!

e) Zeigen Sie: Das Gitter Γ hat keine Orthogonalbasis.

Aufgabe 2: (*5 Punkte*)
$\Gamma = \mathbb{Z}\vec{v} \oplus \mathbb{Z}\vec{w}$ sei ein Gitter in $\mathbb{R}^2$. Wir reduzieren diese Basis mit folgendem Algorithmus à la EUKLID:
1. Schritt: Wähle $k \in \mathbb{Z}$ so, daß $-\frac{1}{2}|\vec{v}|^2 < (\vec{w} - k\vec{v}) \cdot \vec{v} \leq \frac{1}{2}|\vec{w}|^2$ ist.
2. Schritt: Ersetze $\vec{w}$ durch $\vec{w} - k\vec{v}$.
3. Schritt: Falls $|\vec{v}| \leq |\vec{w}|$ endet der Algorithmus; andernfalls werden $\vec{v}$ und $\vec{w}$ vertauscht und wir gehen zurück zum ersten Schritt.

a) Führen Sie diesen Algorithmus durch für die Gitter $\mathbb{Z}\binom{1}{0} \oplus \mathbb{Z}\binom{\sqrt{2}}{1}$ und $\mathbb{Z}\binom{17}{19} \oplus \mathbb{Z}\binom{8}{9}$!

b) Zeigen Sie allgemein: Der Algorithmus endet nach endlich vielen Iterationen. Am Ende ist $\vec{v}$ ein kürzester Vektor aus Γ und $\vec{w}$ ein kürzester Vektor aus $\Gamma \setminus \mathbb{R}\vec{v}$.

c) Die Gitterbasis $\vec{v}, \vec{w}$, die der Algorithmus liefert, ist LLL-reduziert.

Aufgabe 3: (*10 Punkte*)
Finden Sie eine LLL-reduzierte Basis des von

$$\vec{b}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \vec{b}_2 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \quad \text{und} \quad \vec{b}_3 = \begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix}$$

aufgespannten Gitters $\Gamma \subset \mathbb{R}^3$!

Abgabe bis zum Donnerstag, dem 30. Oktober 2008, um 15.30 Uhr