Wolfgang K. Seiler
Tel. 2515

A5, C201

20. Oktober 2011

7. Übungsblatt Computeralgebra

Aufgabe 1: *(5 Punkte)*

$f \in \mathbb{Z}[x]$ sei das Polynom vom Grad vier mit höchstem Koeffizienten eins, das die Nullstellen $\pm\sqrt{2} \pm \sqrt{3}$ hat.

a) Berechnen Sie die Koeffizienten von f ohne Computerhilfe explizit!

b) Faktorisieren Sie $f \bmod 2$ und $f \bmod 3$!

c) $p > 3$ sei eine Primzahl. Zeigen Sie: Falls 2 und 3 Quadrate in $\mathbb{F}_p$ sind, zerfällt $f \bmod p$ in Linearfaktoren, ansonsten in zwei quadratische Faktoren.

d) In $\mathbb{F}_{23}$ ist $5^2 = 2$ und $7^2 = 3$. Faktorisieren Sie $f \bmod 23$!

Aufgabe 2: *(6 Punkte)*

a) Berechnen Sie eine Orthogonalbasis des von $b_1 = \begin{pmatrix} 2 \\ 4 \\ 2 \\ -1 \end{pmatrix}$, $b_2 = \begin{pmatrix} 4 \\ 3 \\ 4 \\ 3 \end{pmatrix}$ und $b_3 = \begin{pmatrix} 5 \\ 3 \\ 3 \\ 3 \end{pmatrix}$ aufgespannten Untervektorraums U von $\mathbb{R}^4$!

b) Ergänzen Sie diese zu einer Orthogonalbasis von $\mathbb{R}^4$!

Aufgabe 3: *(4 Punkte)*

a) Zeigen Sie: Für zwei beliebige teilerfremde ganze Zahlen $p, q \in \mathbb{Z}$ gibt es stets eine Gitterbasis von $\mathbb{Z} \oplus \mathbb{Z}$, die den Vektor $\binom{p}{q}$ enthält.

b) Für jede reelle Zahl λ gibt es eine Gitterbasis von $\mathbb{Z} \oplus \mathbb{Z}$, deren Basisvektoren beide mindestens die Länge λ haben.

c) Ist v, w eine beliebige Gitterbasis von $\mathbb{Z} \oplus \mathbb{Z}$, so hat das von v und w aufgespannte Dreieck die Fläche $\frac{1}{2}$.

Aufgabe 4: *(5 Punkte)*

Das Gitter $\Gamma \subset \mathbb{R}^5$ sei erzeugt von den Vektoren

$$b_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad b_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad b_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad b_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{und} \quad b_5 = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

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

b) Berechnen Sie nach Gram-Schmidt die zugehörige Orthogonalbasis von $\mathbb{R}^5$, und prüfen Sie, ob obige Basis LLL-reduziert ist!

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

d) Bestimmen Sie alle Vektoren der Länge höchstens 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.

Abgabe bis zum Donnerstag, dem 27. Oktober 2011, um 15.30 Uhr