EXERCISES FOR LATTICES

MICHAEL E. POHST

1. Multiple choice

1. Let $\mathbf{b}_1, ..., \mathbf{b}_k \in \mathbb{R}^n$ be independent. What is the dimension of the lattice $\Lambda = \mathbb{Z}\mathbf{b}_1 + ... + \mathbb{Z}\mathbf{b}_k$?
a) n, b) k, c) other.
2. Let $m \in \mathbb{Z}$ with $m \geq 2$ and $(b_1, ..., b_n)^{\text{tr}} \in \mathbb{Z}^n$.
Is $\Lambda = \{\mathbf{a} = (a_1, ..., a_n)^{\text{tr}} \in \mathbb{Z}^n \mid \sum_{i=1}^n b_i a_i \equiv 0 \bmod m\}$ a lattice?
a) yes, no.
3. Let $M_1, ..., M_k$ be the successive minima of a k–dimensional lattice Λ in $\mathbb{R}^n$. Does there always exist a basis $\mathbf{b}_1, ..., \mathbf{b}_k$ of Λ subject to $\|\mathbf{b}_i\|^2 = M_i \ \ (1 \leq i \leq k)$?
a) yes, b) no.
4. Let Λ be a lattice and $\mathbf{b} \in \Lambda$ subject to $\|\mathbf{b}\|^2 = M_1$. Can $\mathbf{b}$ be extended to a basis of Λ?
a) yes, no.
5. Let $B_1, B_2 \in \mathbb{R}^{n \times n}$ be matrices such that the columns of both generate the same n–dimensional lattice Λ. What can we say about their determinants?
a) $\det(B_1) = \det(B_2)$, $b)\det(B_1) = \pm\det(B_2)$, other.
6. Let $\Lambda = \mathbb{Z}\mathbf{b}_1 + ... + \mathbb{Z}\mathbf{b}_k$ be a k–dimensional lattice. Let $\mathbf{b} = \beta_1\mathbf{b}_1 + ... + \beta_k\mathbf{b}_k \in \Lambda$ with $\|\mathbf{b}\|^2 = M_1$. Then one of the coefficients β_i is odd.
a) yes, b) no.

2. Computations

1. Compute the Gram Schmidt orthogonal basis for

$$\mathbf{b}_1 = (4, 0, 0)^{\text{tr}}, \mathbf{b}_2 = 2, 9, 0)^{\text{tr}}, \mathbf{b}_3 = (1, -3, 1)^{\text{tr}} \ .$$

2. Compute a basis for the lattice

$$\Lambda = \{(b_1, b_2, b_3)^{\text{tr}} \in \mathbb{Z}^3 \mid b_1 + 4b_2 - b_3 \equiv 0 \bmod 10\} \ .$$

3. Compute all shortest vectors in a lattice Λ with Gram matrix

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} \ .$$

3. Proofs

1. Let $f(x) \in \mathbb{Z}[x]$ be a monic n-th degree polynomial. Consider $R = \mathbb{Z}[x]/(f)$. Each residue class $g + (f)$ has a unique representative $g(x) \in \mathbb{Z}[x]$ of degree $< n$. Hence, each residue class can be uniquely represented by the coefficient vector of g in $\mathbb{Z}^n$:

$$\varphi : g_0 + g_1 x + ... + g_{n-1}x^{n-1} \mapsto (g_0, ..., g_{n-1}) \ .$$

Let I be an ideal of R. Show that $\varphi(I)$ is a lattice. What is the dimension of $\varphi(I)$?
2. Show that $\mathbb{Z}(1,1)^{\mathrm{tr}} + \mathbb{Z}(\sqrt{2}, -\sqrt{2})^{\mathrm{tr}}$ is a 2–dimensional lattice, but $\mathbb{Z}1 + \mathbb{Z}\sqrt{2}$ is not a lattice.
3. Let $\Lambda = \mathbb{Z}\mathbf{b}_1 + \ldots + \mathbb{Z}\mathbf{b}_k$ be a k–dimensional lattice in $\mathbb{R}^n$ with $n > k$. Develop an algorithm which for given $\mathbf{a} \in \mathbb{R}^n$ determines $\mathbf{b} \in \Lambda$ satisfying

$$\|\mathbf{b} - \mathbf{a}\| = \min\{\|\mathbf{c} - \mathbf{a}\| \mid \mathbf{c} \in \Lambda\} \ .$$

4. Prove that $\gamma_2^2 = \frac{4}{3}$.