Due in class on April 18, 2024

Lattices and Quadratic Forms (Summer 2024) - Problem Set 1

1. In class we have found that positive definite lattices have finite automorphism groups. In this problem, we will study examples from lattices in $\mathbb{R}^n$.
   a) What is the the automorphism group of $\mathbb{Z}^n$?
   b) Let us define the A_3 lattice as a sublattice of $\mathbb{Z}^4$ defined by

$$A_3 := \{n \in \mathbb{Z}^4 : n_1 + n_2 + n_3 + n_4 = 0\}.$$

   Show that the vectors

$$v_1 := \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 := \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \quad v_3 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$$

   form a basis for this lattice. What is the corresponding Gram matrix? What is the automorphism group?
2. Let L be a lattice and $\mathcal{V} = \begin{pmatrix} v_1 & v_2 & v_3 \end{pmatrix}$ be a basis with Gram matrix

$$G(\mathcal{V}) = \begin{pmatrix} 3 & -4 & 3 \\ -4 & 2 & -2 \\ 3 & -2 & 3 \end{pmatrix}.$$

   Give a basis for the dual lattice $L^{\#}$. What is the discriminant group $L^{\#}/L$?
3. Consider the lattice L in $\mathbb{R}^3$ spanned by

$$v_1 = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \quad v_2 = \begin{pmatrix} -1 \\ 2 \\ 5 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 3 \\ 4 \\ 12 \end{pmatrix}.$$

   What is the shortest possible length for nonzero vectors in this lattice? Give an example vector in L that has this length. *Hint:* Reduce the problem to a finite number of possibilities and try these computationally.

   Note: The problem we are solving here is called the *shortest vector problem* and there is no known efficient algorithm that would solve it in arbitrary dimensions. Remarkably, however, there is an efficient algorithm for an approximate version of this problem. See the so-called *LLL algorithm* developed by Lenstra, Lenstra and Lovász for more details.
4. Let V be a real vector space of dimension n that is equipped with a symmetric bilinear form $B : V \times V \to \mathbb{R}$. Recall that we defined a lattice L in V as a subgroup of the form

$$L = \langle v_1, \ldots, v_m \rangle_{\mathbb{Z}},$$

   where the vectors $v_1, \ldots, v_m \in V$ are linearly independent over real numbers and where we equip L with a symmetric bilinear form by restricting B. A more intrinsic alternative is to define a lattice in V to be a discrete subgroup of V (again equipped with the restriction of B). Prove the equivalence of these two definitions.

Note: You may use computational tools to help with your solutions, but describe your steps.