Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 12

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, January 26th, at 12:05 pm.

1. Let Γ be an additive subgroup of $\mathbb{R}^m$; i. e., Γ is a subgroup of $(\mathbb{R}^m, +)$. Prove that the following four properties of Γ are equivalent.

(a) For every $v \in \Gamma$, there is a constant $\varepsilon_v > 0$ such that
$$\Gamma \cap \{a \in \mathbb{R}^m \mid \|a - v\| < \varepsilon_v\} = \{v\}\,.$$

(b) There is a constant $\delta > 0$ such that $\{v \in \Gamma \mid \|v\| < \delta\} = \{\mathbf{0}\}$, where $\mathbf{0}$ is the zero vector of $\mathbb{R}^m$.

(c) There is a constant $\varepsilon > 0$ such that for every $v \in \Gamma$
$$\Gamma \cap \{a \in \mathbb{R}^m \mid \|a - v\| < \varepsilon\} = \{v\}\,.$$

(d) For every constant $r > 0$, the set $\{v \in \Gamma \mid \|v\| \leq r\}$ is finite.

A subgroup Γ of $\mathbb{R}^m$ satisfying any of the above properties is called *discrete.*

2. Let L be a subset of $\mathbb{R}^n$. Prove that the following two properties of L are equivalent:

(a) There is a basis $\{v_1, v_2, \ldots, v_n\}$ of $\mathbb{R}^n$ so that
$$L = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \mid \alpha_1, \alpha_2, \ldots \alpha_n \in \mathbb{Z}\}\,.$$

(b) L is a discrete subgroup of $\mathbb{R}^n$ and $\operatorname{Span}(L) = \mathbb{R}^n$.

Remark. So any of the above two properties could be taken as a definition of a *lattice* of dimension n in $\mathbb{R}^n$.

3. Let L be the lattice given by the basis
$$\mathcal{B} = \{(3, 1, -2), (1, -3, 5), (4, 2, 1)\}\,.$$
Which of the following sets of vectors are also bases for L? For those that are, express the new basis in terms of the basis $\mathcal{B}$, that is, find the change of basis matrix.

(a) $\mathcal{B}_1 = \{(4, -2, 3), (3, 3, -3), (-2, -4, 7)\}$.

(b) $\mathcal{B}_2 = \{(4, -2, 3), (6, 6, -6), (7, -1, 1)\}$.

(c) $\mathcal{B}_3 = \{(5, 13, -13), (0, -4, 2), (7, -13, 18)\}$.

4. Let $\{v_1, \ldots, v_n\}$ be a basis for a lattice $L \subset \mathbb{R}^m$, $n \leq m$. The *Gram matrix* of $v_1, \ldots, v_n$ is the following matrix of dot products (= scalar products):
$$\operatorname{Gram}(v_1, \ldots, v_n) = \begin{pmatrix} v_1 \cdot v_1 & \cdots & v_1 \cdot v_n \\ \cdots & \cdots & \cdots \\ v_n \cdot v_1 & \cdots & v_n \cdot v_n \end{pmatrix}.$$

(a) Prove that
$$\det\bigl(\operatorname{Gram}(v_1, \ldots, v_n)\bigr) = \bigl(\det(L)\bigr)^2.$$

(b) Let $L \subset \mathbb{R}^4$ be the 3-dimensional lattice with basis
$$v_1 = (1, 0, 1, -1), \qquad v_2 = (1, 2, 0, 4), \qquad v_3 = (1, -1, 2, 1).$$
Compute the Gram matrix of this basis and use it to compute $\det(L)$.