1. Recall that a subgroup $S$ is a \textit{discrete subgroup} of $\mathbb{R}^n$, provided that there exists $\epsilon > 0$ such that the ball $B(0, \epsilon)$ centered at 0 with radius $\epsilon$ does not contain any non zero elements from $S$, i.e. $B(0, \epsilon) \cap S = \{0\}$.

a) Prove that for any point $y \in S$, $B(y, \epsilon) \cap S = \{y\}$, i.e. the ball centered at $y$ with radius $\epsilon$ contains only $y$ from $S$.

b) Use part a) to show that a bounded set $\Pi \subseteq \mathbb{R}^n$ contains only finitely many points from $S$.

c) Consider a set $\{a_1, \ldots, a_n\}$ of linearly independent vectors in $\mathbb{R}^n$. Show that the set
\[
\Lambda = \{\mu_1 a_1 + \ldots + \mu_m a_m \mid \mu_1, \ldots, \mu_m \in \mathbb{Z}\}
\]
is a discrete subgroup (and hence a lattice). Hint: Construct an invertible linear transformation $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ such that $T(\mathbb{Z}^n) = \Lambda$. You can use, without proof, the fact that invertible linear transformations in $\mathbb{R}^n$ map open sets to open sets.

2. Consider a lattice $\Lambda$ of $\mathbb{R}^n$. A \textit{lattice subspace} is defined as a subspace $L \subseteq \mathbb{R}^n$ such that $L$ has a basis contained in $\Lambda$. Show that the projection of $\Lambda$ onto the orthogonal complement of $L$ is a discrete subgroup when $L$ is a lattice subspace.

3. Recall that the \textit{orthogonality defect} $\gamma$ for a basis $B$ of a lattice is defined by
\[
\gamma = \left(\prod_{i=1}^k \|b_i\|/|\det(B)|\right),
\]
where $b_i$’s are the columns of $B$. Prove that $\gamma = 1$ if and only if $B$ is orthogonal, i.e. all the $b_i$’s are mutually orthogonal vectors.

4. **Hermite Normal Form**

Consider the following \textit{elementary column operations} for a matrix $A$.

i. exchanging two columns.

ii. multiplying a column by -1.

iii. adding an integral multiple of one column to another column.

Recall that any integral matrix $A$ with full row rank can be converted into the form $[B, 0]$ using only the above elementary column operations, such that $B$ is a nonsingular, lower triangular matrix with non-zero entries on the main diagonal. (This is Lemma 4.1 from your notes in IP)

a) Show that, in fact, one can further enforce both of the following properties for $B$.

- $B$ has only nonnegative entries.

- In each row of $B$ there is a unique maximum element, which sits on the main diagonal of $B$.

This strengthening of the Hermite Normal Form will be referred to as s-HNF below (for strengthened-HNF).

b) Let $A$ be an $m \times n$ integral matrix with $[B, 0]$ as its s-HNF. Let $a_i$ denote the columns of $A$ and $b_i$ denote the columns of $B$. Show that
\{\mu_1 a_1 + \ldots + \mu_m a_m \mid \mu_1, \ldots, \mu_m \in \mathbb{Z}\} = \{\lambda_1 b_1 + \ldots + \lambda_n b_n \mid \lambda_1, \ldots, \lambda_n \in \mathbb{Z}\}

c) Let $U$ be a unimodular matrix (recall this means that $U$ is an integral $n \times n$ matrix and has determinant $\pm 1$). Show that the s-HNF of $U$ is the identity matrix. Conclude that the lattice generated by the columns of a unimodular matrix is $\mathbb{Z}^n$.

5. Consider a lattice $\Lambda$ of $\mathbb{R}^n$. Let $y \in \Lambda$ be a lattice point and $r \in \mathbb{R}^n$ be any vector. Show that given any $\epsilon$, there exists a $\lambda > 0$ and a lattice point $p \in \Lambda$ such that $\|p - (y + \lambda r)\| \leq \epsilon$. In other words, for any $\epsilon$, there exists a lattice point (other than $y$) that has distance at most $\epsilon$ from the half-line $\{y + \lambda r \mid \lambda \geq 0\}$.

Hint: You may find Dirichlet’s approximation result useful:

Given real numbers $\alpha_1, \ldots, \alpha_n, \varepsilon$ with $0 < \varepsilon < 1$, there exist integers $p_1, \ldots, p_n$ and $q$ such that

$$\left| \alpha_i - \frac{p_i}{q} \right| < \frac{\varepsilon}{q}, \text{ for } i = 1, \ldots, n, \text{ and } 1 \leq q \leq \varepsilon^{-1}. \quad (1)$$

6. **Norms and Lattices**
   a) Show that if a lattice is generated by an orthogonal basis, then the shortest lattice vector is one of the basis vectors.

   b) Show that a lattice $\Lambda$ has a non-zero point $v$ such that $\|v\|_{\infty} \leq \sqrt[\det(\Lambda)]{\varepsilon}$.

7. **Basis Reduction and Integer Programming**
   a) Consider a lattice $\Lambda$ of $\mathbb{R}^n$ generated by a basis $\{b_1, \ldots, b_n\}$ and any point $p \in \mathbb{R}^n$. Show that there exists a $z \in \Lambda$ such that $\|z - p\| \leq \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \|b_i\|^2$.

   b) Let $B$ be an $n \times n$ matrix with entries from $\mathbb{R}$. Prove that $|\det(B)| \leq (\sqrt{n}M)^n$, where $M$ is the absolute value of the largest entry in $B$. (This bound was needed for bounding the running time for the LLL algorithm)