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

1.

a) Let start with the orthonormal basis

$$\alpha_1 = (1,0,0\ldots,0,0), \quad \alpha_2 = (0,1,0,\ldots,0,0), \quad \ldots \quad \alpha_n = (0,0,0,\ldots,0,1)$$

for $\mathbb{Z}^n$. Now recall that automorphisms are in bijective correspondence with n-tuples of $\mathbb{Z}^n$ vectors $(\alpha'_1,\ldots,\alpha'_n)$ with the same Gram matrix as that of $(\alpha_1,\ldots,\alpha_n)$; i.e. we are looking for norm 1 vectors that are pairwise orthogonal.

- For α'_1 we have $2n$ candidates with a single nonzero entry (for which there are n possibilities) that is ± 1.
- Given each α'_1, there are $2(n-1)$ candidates for α'_2, again given by a vector with a single ± 1 entry at a position other than that of the nonzero entry of α'_1.
- Going on in this way for each $\alpha'_1,\ldots,\alpha'_r$, there are $2(n-r)$ choices for α'_{r+1}.

This shows that the order of the automorphism group is

$$|\mathrm{Aut}(\mathbb{Z}^n)| = 2^n\, n!.$$

In fact, we can explicitly find $2^n\, n!$ automorphisms by

$$(k_1,k_2,\ldots,k_n) \mapsto (\varepsilon_1 k_{\sigma^{-1}(1)}, \varepsilon_2 k_{\sigma^{-1}(2)}, \ldots, \varepsilon_n k_{\sigma^{-1}(n)}) \quad \text{where } \varepsilon_j \in \{\pm 1\} \text{ and } \sigma \in S_n.$$

So the automorphism group is the semidirect product

$$\mathrm{Aut}(\mathbb{Z}^n) \simeq (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n,$$

where the semidirect product is defined by permutation action of S_n on $(\mathbb{Z}/2\mathbb{Z})^n$ that implements the sign changes.

b) First note that the vectors v_1, v_2, v_3 are linearly independent over the reals and they are all elements of A_3 since summing their coordinates gives zero. Finally, an arbitrary element $(n_1, n_2, n_3, -n_1-n_2-n_3)$ of A_3 can be expanded as $n_1v_1+(n_1+n_2)v_2+(n_1+n_2+n_3)v_3$ with integer coefficients. So $\mathcal{V} = (v_1, v_2, v_3)$ forms a basis for A_3. The corresponding Gram matrix is

$$G(\mathcal{V}) = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}.$$

To find the automorphism group, let us first find the candidates $(v'_1,\ldots,v'_n)$ for the images of (v_1,v_2,v_3) under the automorphism. These are roots with the same inner products as those of (v_1,v_2,v_3).
The roots of A_3 are vectors with two nonzero entries with one equal to $+1$ and one equal to -1. There are 12 such vectors:

$$(+1,-1,0,0), \quad (+1,0,-1,0), \quad (+1,0,0,-1), \quad (0,+1,-1,0,), \quad (0,+1,0,-1), \quad (0,0,+1,-1),$$
$$(-1,+1,0,0), \quad (-1,0,+1,0), \quad (-1,0,0,+1), \quad (0,-1,+1,0,), \quad (0,-1,0,+1), \quad (0,0,-1,+1).$$

So we have 12 candidates for v'_1. Given each v'_1, there are 4 candidates for v'_2:

- The $+1$ entry of v'_2 has the same position as the -1 entry of v'_1 and then the remaining -1 entry of v'_2 is placed in one of the two positions corresponding to the 0 entries of v'_1.
- Alternatively, the -1 entry of v'_2 has the same position as the $+1$ entry of v'_1 and then the remaining $+1$ entry of v'_2 is placed in one of the two positions corresponding to the 0 entries of v'_1.

Finally, given each v_1' and v_2' pair, there is a unique candidate for the vector v_3': Since v_3' is orthogonal to v_1' and since it has inner product -1 with v_2', if v_2' has the nonzero entry ε at the position corresponding to the zero entry of v_1', then the corresponding entry for v_3' has to be $-\varepsilon$ and the position where both v_1' and v_2' have their zero has to have a ε entry for v_3'. For example, if we have

$$v_1' = (0, -1, +1, 0) \quad \text{and} \quad v_2' = (0, +1, 0, -1),$$

then

$$v_3' = (-1, 0, 0, +1).$$

So that yields the order of the automorphism group as

$$|\mathrm{Aut}(A_3)| = 48. \tag{0.1}$$

In fact, we can find 48 different automorphisms given by

$$(k_1, k_2, k_3, k_4) \mapsto \pm(k_{\sigma^{-1}(1)}, k_{\sigma^{-1}(2)}, k_{\sigma^{-1}(3)}, k_{\sigma^{-1}(4)}) \quad \text{where } \sigma \in S_4$$

and hence the automorphism group is given by the direct product

$$\mathrm{Aut}(A_3) \simeq (\mathbb{Z}/2\mathbb{Z}) \times S_4.$$

2. A basis $\mathcal{V}^\# = (v_1^\# \, v_2^\# \, v_3^\#)$ for $L^\#$ is given by $\mathcal{V}^\# = \mathcal{V}\, G(\mathcal{V})^{-1}$ (the basis dual to $\mathcal{V}$), which yields

$$v_1^\# = -\frac{v_1 + 3v_2 + v_3}{6}, \qquad v_2^\# = \frac{v_3 - v_1}{2}, \qquad v_3^\# = \frac{5v_3 + 3v_2 - v_1}{6}.$$

To compute the discriminant group, we find the Smith normal form of the given Gram matrix and find that

$$S\, G(\mathcal{V})\, T = D \quad \text{where } S := \begin{pmatrix} -1 & 2 & 4 \\ -1 & 0 & 1 \\ -1 & 3 & 5 \end{pmatrix}, \; T := \begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z}) \text{ and } D := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}.$$

This shows that we can change bases to $\mathcal{W}^\# = \mathcal{V}^\# S^{-1}$ for $L^\#$ and $\mathcal{W} = \mathcal{V}T$ for L to find them related by $\mathcal{W}^\# D = \mathcal{W}$. This yields the discriminant group as

$$L^\#/L \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}).$$

3. There are many ways to solve this problem. Here is one that employs some of the facts we proved in the lectures (and that is not so efficient): The Gram matrix corresponding to the basis $\mathcal{V} = (v_1\, v_2\, v_3)$ is

$$G(\mathcal{V}) = \begin{pmatrix} 5 & 12 & 28 \\ 12 & 30 & 65 \\ 28 & 65 & 169 \end{pmatrix}.$$

In particular, we see that the vector v_1 has norm 5 (in the squared length sense we have been using in this course) and hence the shortest nonzero norm possible within L can be at most 5. So denoting the coordinates of a lattice element with respect to $\mathcal{V}$ with the integer column vector $n \in \mathbb{Z}^3$, lattice elements with norm shorter than 5 are found by the solutions of the inequality

$$n^T\, G(\mathcal{V})\, n \leq 5.$$

Now we can easily check that $G(\mathcal{V}) - \frac{1}{20} I_3$ is a positive definite matrix so that

$$\frac{1}{20}(n_1^2 + n_2^2 + n_3^2) \leq n^T\, G(\mathcal{V})\, n.$$

So solutions of $n^T G(\mathcal{V})\, n \le 5$ necessarily satisfy $n_1^2 + n_2^2 + n_3^2 \le 100$ and hence $|n_j| \le 10$ for all j. We can then computationally check these finitely many possibilities to find that the smallest nonzero norm in this lattice is 2 and only two vectors have this norm, namely $\pm(2v_1 - v_2)$.

Remark: In fact, since the finite set above contains all the vectors with norm ≤ 5, the same computation shows that the norm 3 vectors in L are $\pm(3v_1 - v_2)$, there are no norm 4 vectors, and the norm 5 vectors are $\pm v_1$ and $\pm(5v_1 - 2v_2)$.

4. The symmetric bilinear form B plays no role in this problem. Moreover, to discuss the topology on V, we pick a basis to identify V with $\mathbb{R}^n$ and then equip $\mathbb{R}^n$ with the Euclidean metric (which induces the topology on V). So when we discuss distances below, we will be referring to this Euclidean metric instead of B. Moreover, we note that both statements trivially hold if $L = \{0\}$ or $n = 0$, so we assume below that L is nontrivial and $n > 0$.

   - First assume that there are linearly independent vectors $v_1, \ldots, v_m \in \mathbb{R}^n$ such that $L = \langle v_1, \ldots, v_m \rangle_{\mathbb{Z}}$. Then as we discussed in class, given any real number $r > 0$, the number of vectors in L with Euclidean square-norm less than r^2 is finite. If necessary, by making r smaller to exclude these finitely many nonzero vectors we can ensure that the only lattice element in the open ball $B_r(0)$ with radius r and center at zero is the point $0 \in L$. So the origin is an isolated point of L. Furthermore, given any other lattice point $v \in L$, if there were any lattice point $w \ne v$ within the open ball $B_r(v)$ centered at v, then $w - v \in L$ would be a nonzero lattice point in $B_r(0)$. So no such w exists and hence all the lattice points are isolated. This means that the subspace $L \subset \mathbb{R}^n$ is discrete.
   - Conversely, assume that the subgroup L is a discrete subspace of $\mathbb{R}^n$. Let us first prove that L is a closed set in $\mathbb{R}^n$. If not, L would have a limit point $p \notin L$. Then for any $r > 0$, there is a lattice element $v \in L$ with $v \in B_r(p)$. We can also find a lattice element $w \in L$ in the smaller neighborhood $B_{r'}(p)$ with $r' < |p - v| < r$. Since $v \ne w$, we then have a nonzero lattice point $v - w \in L$ in the open ball $B_{2r}(0)$ around the origin. Since this is true for any $r > 0$, the origin would not be an isolated point, contradicting the fact that L is a discrete subspace.

     In particular, $\mathbb{R}^n \setminus L$ is open and therefore any point in $\mathbb{R}^n \setminus L$ has an open neighborhood with no points from L. Together with discreteness of L, this means that every point in $\mathbb{R}^n$ has an open neighborhood with at most one point from L. So given any $R > 0$, the closed ball $\overline{B}_R(0)$ can be covered with such neighborhoods. The compactness of $\overline{B}_R(0)$ means that there is a finite subcover and hence $\overline{B}_R(0)$ contains finitely many points from L.

     We are finally ready to prove the converse statement and we will do this with induction over n.

     – For $n = 1$, let v_0 be a nonzero element of L, which exists because L is nontrivial. So letting $R := \sqrt{v_0 \cdot v_0}$, the closed ball $\overline{B}_R(0)$ contains finitely many points from L with at least one that is nonzero (namely v_0). Then among all the nonzero lattice vectors in $\overline{B}_R(0)$ pick one with minimal length, say $v \in L$. So we have $\mathbb{Z}v \subset L$. Moreover, if $w \in L$ is an arbitrary lattice element, then we can write $w = (n + r)v$ with $n \in \mathbb{Z}$ and $-\frac{1}{2} \le r < \frac{1}{2}$. Since $rv = w - nv \in L$, it is then required that $r = 0$ as otherwise we would have a nonzero vector in L with length smaller than that of v. This then completes the proof that $L = \langle v \rangle_{\mathbb{Z}}$.

     – Now suppose that $n > 1$ and the statement holds in dimensions $1, \ldots, n - 1$. As in the $n = 1$, case pick a nonzero vector v_1 in L with minimal length. Then as above we can argue that $L \cap \mathbb{R}v_1$ is equal to $\mathbb{Z}v_1$, otherwise we would obtain a shorter vector. If $L = \mathbb{Z}v_1$, we are done. If not, consider the orthogonal projection π of L to the subspace U orthogonal to v_1. This is a nontrivial subgroup of the additive group U isomorphic to $\mathbb{R}^{n-1}$.

       Now let λ be an arbitrary element of $L \setminus \mathbb{Z}v_1$ and write it as $\lambda = \pi(\lambda) + cv_1$ for some $c \in \mathbb{R}$. Writing $c = n + r$ with $n \in \mathbb{Z}$ and $-\frac{1}{2} \le r < \frac{1}{2}$, we find that $\pi(\lambda) + rv_1 = \lambda - nv_1 \in L$. Since any nonzero element of L has length at least $|v_1|$, we find

$$|\pi(\lambda)| \ge |\lambda - nv_1| - |rv_1| \ge \frac{1}{2}|v_1|.$$

This implies that the subgroup $\pi(L)$ is a discrete subspace of U. Then the inductive hypothesis yields linearly independent vectors $w_2, \ldots, w_m \in U$ with $\pi(L) = \langle w_2, \ldots, w_m \rangle_{\mathbb{Z}}$. Letting $v_j \in L$ be such that $\pi(v_j) = w_j$ for $2 \leq j \leq m$, the vectors $v_1, \ldots, v_m$ are linearly independent in $\mathbb{R}^n$ (as can be seen by applying π to a potential linear dependence and noting that $\pi(v_1) = 0$). Moreover, if $u \in L$ is an arbitrary element, then we know that

$$\pi(u) = n_2 w_2 + \ldots + n_m w_m$$

for some integers $n_2, \ldots, n_m$. So $u - n_2 v_2 - \ldots - n_m v_m \in L$ is in the kernel of the homomorphism $\pi : L \to U$, which is nothing but $L \cap \mathbb{R} v_1 = \mathbb{Z} v_1$. So we have

$$u - n_2 v_2 - \ldots - n_m v_m = n_1 v_1$$

for some $n_1 \in \mathbb{Z}$ and hence $L = \langle v_1, \ldots, v_m \rangle_{\mathbb{Z}}$.