Lattices and Quadratic Forms (Summer 2024) - Solutions to Problem Set 2

1.

a) Let us start by defining

$$L' := \{x \in L : \, x \cdot v = 0\}.$$

This is a sublattice of L with the symmetric bilinear form inherited from that of L. The only thing to note is that L' is a finitely generated free abelian group since L' is a subgroup of L and any subgroup of a finitely generated free abelian group is also a free abelian group with rank less than or equal to that of the original group.

Furthermore, elements of the sublattice L' are orhtogonal to those of the sublattice $\mathbb{Z}v$ and we have $L' \cap \mathbb{Z}v = \{0\}$. So $L' \perp \mathbb{Z}v$ is a sublattice of L. The only remaining thing to check is to ensure that each elements of L is in $L' \perp \mathbb{Z}v$. For this, we decompose an arbitrary element $\ell \in L$ to its orthogonal projection onto $\mathbb{R}v$ and the plane orthogonal to that:

$$\ell = \left(\ell - \frac{\ell \cdot v}{v \cdot v} v\right) + \frac{\ell \cdot v}{v \cdot v} v.$$

Since L is an integral lattice and since $v \cdot v = \pm 1$, we have $\frac{\ell \cdot v}{v \cdot v} \in \mathbb{Z}$ and hence the second factor is in $\mathbb{Z}v$. Moreover, this shows that $\ell' := \ell - \frac{\ell \cdot v}{v \cdot v} v$ is an element of L that is orthogonal to v so that $\ell' \in L'$.

b) Using part (a), we can recursively remove sublattices generated by norm 1 vectors to write $L = L' \perp \mathbb{Z}^k$ for some k and some sublattice L' that contains no norm 1 vectors (that is possibly trivial). If L' is nontrivial, note that norm 2 vectors of L can not have nontrivial overlap with both L' and $\mathbb{Z}^k$: If ℓ is a norm 2 vector such that $\ell = \ell_1 + \ell_2$ with ℓ_1 and ℓ_2 nonzero vectors that are orthogonal, then both of ℓ_j's should have norm 1, but L' has no norm 1 vectors. Since norm 1 and norm 2 vectors generate L, this in turn means that the integral, positive definite sublattice L' is generated by its norm 2 vectors and hence is a root lattice.

2.

a) L_1 and L_2 are not isometric: Both L_1 and L_2 are integral lattices since the given Gram matrices are integer valued. However L_1 is an even lattice since the diagonal entries are even, whereas L_2 is not.[1]

b) The lattices $\mathbb{Z}\langle 2\rangle \perp \mathbb{Z}\langle -1\rangle$ and $\mathbb{Z}\langle -2\rangle \perp \mathbb{Z}$ are isometric as can be seen from the change of coordinates

$$(n_1, n_2) \mapsto (n_1 + n_2, 2n_1 + n_2).$$

Note that the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right)$ implementing the change of coordinates is in $\mathrm{GL}_2(\mathbb{Z})$ (its determinant is -1) and hence maps $\mathbb{Z}^2$ bijectively to itself. Moreover, it correctly changes the inner product since

$$2n_1^2 - n_2^2 = -2(n_1 + n_2)^2 + (2n_1 + n_2)^2.$$

3.

a) Norm 2 vectors in $\mathbb{Z}^n$ have two entries equal to ± 1 with the rest equal to zero. Since all such vectors have the sum of their coordinates equal to 0 or ± 2, they are all in D_n and hence the roots of D_n are of the form

$$\pm\varepsilon_i \pm \varepsilon_j = (0, \ldots, 0, \pm 1, 0, \ldots, 0, \pm 1, 0, \ldots, 0),$$

where the nonzero entries are at the positions i and j with $1 \leq i \neq j \leq n$.[2] To find the number of roots, note that there are $\binom{n}{2}$ ways to choose the positions i, j with nonzero entries and then there are 4 ways to choose the signs for each i, j pair. So the number of roots in D_n is

$$4\binom{n}{2} = 2n(n-1).$$

[1] One can also check the associated discriminant forms and show that these lattices are not isometric. However, it is a good idea to check easier isometry invariants first!

[2] Here $\varepsilon_i \in \mathbb{Z}^n$ denotes the vector that has all zeros as coordinates except for a '+1' at the i^{th} entry.

To show that the roots generate all the vectors in D_n, let us start with the roots

$$\alpha_1 = (1,-1,0,\dots,0), \quad \alpha_2 = (0,1,-1,0,\dots,0), \ \dots\ , \alpha_{n-1} = (0,\dots,0,1,-1), \quad \alpha_n = (0,\dots,0,1,1)$$

introduced in part (b) and consider an arbitrary element $(k_1,k_2,\dots,k_n) \in D_n$. Then note that

$$k_1\alpha_1 + (k_1+k_2)\alpha_2 + \ldots + (k_1+\ldots+k_{n-1})\alpha_{n-1} = (k_1,k_2,\dots,k_{n-1},-k_1-k_2-\ldots-k_{n-1})$$

so that we can add $\frac{1}{2}(k_1+\ldots+k_n)(\alpha_n-\alpha_{n-1})$ to correct the last coordinate, where we note

$$\alpha_n - \alpha_{n-1} = (0,\dots,0,2)$$

and $\frac{1}{2}(k_1+\ldots+k_n) \in \mathbb{Z}$ by the definition of D_n. So overall we have

$$\begin{aligned}(k_1,\dots,k_n) = k_1\alpha_1 + (k_1+k_2)\alpha_2 + \ldots + (k_1+\ldots+k_{n-2})\alpha_{n-2}\\ + \frac{k_1+\ldots+k_{n-1}-k_n}{2}\alpha_{n-1} + \frac{k_1+\ldots+k_{n-1}+k_n}{2}\alpha_n.\end{aligned}$$

b) The vectors $\alpha_1,\dots,\alpha_n$ are linearly independent in $\mathbb{R}^n$ and as we have already found in part (a), they span the lattice D_n. So they form a basis for D_n and the only thing we need to check to ensure that they form a fundamental system of roots is to check whether each root in D_n can be decomposed into $\alpha_1,\dots,\alpha_n$ with all nonnegative or all nonpositive coefficients.
In part (a) we found all the roots in D_n as well as the decomposition of an arbitrary element $(k_1,\dots,k_n) \in D_n$ to $\alpha_1,\dots,\alpha_n$. We use these to show that half of the roots can be decomposed into $\alpha_1,\dots,\alpha_n$ with all nonnegative coefficients (so that they would constitute the positive roots and the other half, which consist of their negations, would decompose with all nonpositive coefficients). In particular, we consider the roots $\varepsilon_i \pm \varepsilon_j$ with $1 \le i < j \le n$.

- For $1 \le i < j \le n$ we have
$$\varepsilon_i - \varepsilon_j = \alpha_i + \alpha_{i+1} + \ldots + \alpha_{j-1}.$$
- For $1 \le i < j \le n-2$ we have
$$\varepsilon_i + \varepsilon_j = (\alpha_i + \alpha_{i+1} + \ldots + \alpha_{j-1}) + (2\alpha_j + 2\alpha_{j+1} + \ldots + 2\alpha_{n-2}) + \alpha_{n-1} + \alpha_n.$$
- For $1 \le i < j = n-1$ we have
$$\varepsilon_i + \varepsilon_{n-1} = \alpha_i + \alpha_{i+1} + \ldots + \alpha_{n-2} + \alpha_{n-1} + \alpha_n.$$
- For $1 \le i < j = n$ we have
$$\varepsilon_i + \varepsilon_n = \alpha_i + \alpha_{i+1} + \ldots + \alpha_{n-2} + \alpha_n.$$

c) In class, we found that if L' is a sublattice of a lattice L of the same dimension, then we have

$$\det(L') = |L/L'|^2 \det(L).$$

We would like to apply this with $L = \mathbb{Z}^n$ and $L' = D_n$. First note tat D_n is an index 2 sublattice of $\mathbb{Z}_n$ since we have

$$\mathbb{Z}^n = D_n \cup (e + D_n),$$

where the coset $e + D_n$ with $e := (1,0,\dots,0)$ consists of $\mathbb{Z}^n$ elements whose sum of coordinates is odd. So $|\mathbb{Z}^n/D_n| = 2$ and $\det(\mathbb{Z}^n) = 1$ yields

$$\det(D_n) = 4.$$

d) The discriminant group $D_n^\sharp/D_n$ has $|\det(D_n)| = 4$ elements. For an arbitrary element $k = (k_1, \ldots, k_n) \in D_n \leq \mathbb{Z}^n$, all three of

$$k \cdot v = \frac{k_1 + \ldots + k_n}{2}, \quad k \cdot w = \frac{k_1 + \ldots + k_n}{2} - k_1, \quad k \cdot e = k_1$$

are integers since $k_1 + \ldots + k_n$ is even for elements of D_n. So v, w and e are all elements of the dual lattice $D_n^\sharp$. It is clear that v, w, e are not in D_n so the corresponding cosets

$$[v] = v + D_n, \quad [w] = w + D_n, \quad \text{and} \quad [e] = e + D_n$$

are nontrivial elements of $D_n^\sharp/D_n$. Moreover, all these three cosets are different and hence give the three nontrivial elements of $D_n^\sharp/D_n$ since none of

$$v - w = (1, 0, \ldots, 0), \quad v - e = \left(-\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right), \quad \text{and} \quad w - e = \left(-\frac{3}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right)$$

are in D_n. This finally confirms that

$$D_n^\sharp/D_n = \{[0], [v], [e], [w]\}.$$

To identify this group in more detail, note that there are two groups of order 4 up to isomorphism, namely $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Since $2e \in D_n$, the coset $[e]$ has order two in $D_n^\sharp/D_n$. However

$$2v = (1, 1, \ldots, 1) \quad \text{and} \quad 2w = (-1, 1, \ldots, 1)$$

are in D_n if and only if n is even.

- So if n is even, all three of $[v], [e], [w]$ have order two and we have

$$D_n^\sharp/D_n \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

- If n is odd, on the other hand, $2[v]$ and $2[w]$ are not trivial, so $[v]$ and $[w]$ have order four instead (in fact is easy to see that $4v$ and $4w$ are in D_n) and either one of them generates $D_n^\sharp/D_n$ as a cyclic group:

$$D_n^\sharp/D_n \simeq \mathbb{Z}/4\mathbb{Z}.$$

To find the discriminant form, we compute the inner products

$$v \cdot v = \frac{n}{4}, \qquad w \cdot w = \frac{n}{4}, \qquad e \cdot e = 1$$

and

$$v \cdot w = \frac{n-2}{4}, \qquad v \cdot e = \frac{1}{2}, \qquad w \cdot e = -\frac{1}{2}$$

Reducing these modulo 1, we find the following possibilities for

$$\begin{pmatrix} ([0],[0]) & ([0],[v]) & ([0],[e]) & ([0],[w]) \\ ([v],[0]) & ([v],[v]) & ([v],[e]) & ([v],[w]) \\ ([e],[0]) & ([e],[v]) & ([e],[e]) & ([e],[w]) \\ ([w],[0]) & ([w],[v]) & ([w],[e]) & ([w],[w]) \end{pmatrix}:$$

- If n is even and hence $D_n^\sharp/D_n \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, the discriminant form is

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix} \text{ if } n \equiv 0 \bmod 4 \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \text{ if } n \equiv 2 \bmod 4.$$

- If n is odd and hence $D_n^\sharp/D_n \simeq \mathbb{Z}/4\mathbb{Z}$, the discriminant form is

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{4} & \frac{1}{2} & \frac{3}{4} \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{3}{4} & \frac{1}{2} & \frac{1}{4} \end{pmatrix} \text{ if } n \equiv 1 \bmod 4 \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{3}{4} & \frac{1}{2} & \frac{1}{4} \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{1}{4} & \frac{1}{2} & \frac{3}{4} \end{pmatrix} \text{ if } n \equiv 3 \bmod 4.$$

e) The linear mapping

$$f : (k_1, k_2, \dots, k_n) \mapsto (-k_1, k_2, \dots, k_n)$$

is an involution that bijectively maps D_n to itself (note that the mapping preserves $k_1 + \dots k_n \bmod 2$) while preserving the underlying Euclidean norm on $\mathbb{Z}^n$. So this is an automorphism of D_n that maps v to w and hence $[v]$ to $[w]$.

f) Firstly, since n is even we have $2v \in D_n$ so that $D_n^+ := D_n \cup (v + D_n)$ is a subgroup and hence a sublattice of $D_n^\sharp$.

- All elements of D_n have even norm. Similarly, for any $w \in D_n$ we have

$$(v + w)^2 = v^2 + 2v \cdot w + w^2 \in 2\mathbb{Z}$$

since $v^2 = \frac{n}{4} \in 2\mathbb{Z}$ and $v \cdot w \in \mathbb{Z}$ because $v \in D_n^\sharp$. Therefore, every element of $v + D_n$ and hence of D_n^+ has even norm. In other words, D_n^+ is an even lattice.

- Since D_n^+ is an even and hence integral lattice, it is a sublattice of its dual lattice $(D_n^+)^\sharp$. Our next goal is to compute the size of the discriminant group $(D_n^+)^\sharp/D_n^+$ by computing $\det(D_n^+)$. For this purpose, we use the relation (for L' a sublattice of L of the same rank)

$$\det(L') = |L/L'|^2 \det(L)$$

with $L' = D_n$ and $L = D_n^+$. Since $|D_n^+/D_n| = 2$ and $\det(D_n) = 4$, this relation yields

$$\det(D_n^+) = 1.$$

So the discriminant group is trivial and we have $(D_n^+)^\sharp = D_n^+$, i.e. D_n^+ is self-dual.

g) The smallest norm possible in the cosets $[v]$ and $[w]$ come from elements which have all of their entries equal to $\pm\frac{1}{2}$ like v and w. So the minimal norm in $[v]$ and $[w]$ is $\frac{n}{4}$ (which are realized by 2^{n-1} vectors in each coset). In the coset $[e]$ however, the smallest possible norm come from vectors which have a single ± 1 entry with the rest equal to zero like e (so there are $2n$ such vectors).

- For $n > 4$, the fact that the minimum norms are different implies that there can not be a D_n automorphism mapping $[v]$ or $[w]$ to $[e]$.
- This argument fails for $n = 4$, since the minimal norm in $[v]$, $[w]$, and $[e]$ are all 1. In fact even the numbers of the vectors realizing this minimal norm are the same since both 2^{n-1} and $2n$ are equal to 8 in this case.

h) First let us check that the linear transformations U and V bijectively map D_4 to itself (so they are isomorphisms of the underlying abelian group). For this, we first check that they map D_4 into D_4:

- This is obvious in the case of V, which maps

$$(k_1, k_2, k_3, k_4) \mapsto (k_1, k_2, k_3, -k_4),$$

since $k_1 + k_2 + k_3 + k_4$ and $k_1 + k_2 + k_3 - k_4$ are equal modulo 2.

- In the case of U, which maps

$$k := (k_1, k_2, k_3, k_4) \mapsto$$
$$k' := \left(\frac{k_1 + k_2 + k_3 + k_4}{2}, \frac{k_1 + k_2 - k_3 - k_4}{2}, \frac{k_1 - k_2 + k_3 - k_4}{2}, \frac{-k_1 + k_2 + k_3 - k_4}{2} \right),$$

first note that $k' \in \mathbb{Z}^4$ since $k_1 + k_2 + k_3 + k_4$ is even for $k \in D_4$ and consequently so are $k_1 + k_2 - k_3 - k_4$, $k_1 - k_2 + k_3 - k_4$, and $-k_1 + k_2 + k_3 - k_4$. Moreover, we have

$$k_1' + k_2' + k_3' + k_4' = k_1 + k_2 + k_3 - k_4$$

equal to $k_1 + k_2 + k_3 + k_4$ modulo 2, i.e. it is even. So k' is also in D_4.

Since $U^3 = I_4$ and $V^2 = I_4$, these transformations have orders 3 and 2, respectively. This, in turn, shows that U and V map $D_4 \to D_4$ bijectively. Moreover, we have $U^T U = I_4$ and $V^T V = I_4$, so both U and V are orthogonal transformations on $\mathbb{R}^4$ preserving the underlying Euclidean inner product. Consequently, these are both automorphisms of D_4.

Since U has order three, V has order two, and $UV = VU^2$, an arbitrary element of the subgroup G of $\mathrm{Aut}(D_4)$ generated by U and V can be written of the form

$$V^j U^k \quad \text{with } j \in \{0,1\} \text{ and } k \in \{0,1,2\}.$$

Moreover, we can compute all these six possibilities and see that they lead to different matrices. So the subgroup in question has order six.

In fact, we can see this more explicitly and also identify the group along the way: For this purpose, consider that the group action of G on the set $\{[v],[w],[e]\}$ (note that the cosets $[v]$, $[w]$, and $[e]$ can not be mapped to the trivial coset $[0] = D_4$). Since

$$Uv \equiv e \pmod{D_4}, \qquad Uw \equiv v \pmod{D_4}, \qquad Ue \equiv w \pmod{D_4},$$

and

$$Vv \equiv w \pmod{D_4}, \qquad Vw \equiv v \pmod{D_4}, \qquad Ve \equiv e \pmod{D_4},$$

labeling $[v], [w], [e]$ as μ_1, μ_2, μ_3, respectively we find that

$$U : \mu_j \mapsto \mu_{\sigma(j)} \text{ with } \sigma := (132) \in S_3 \quad \text{ and } \quad V : \mu_j \mapsto \mu_{\sigma'(j)} \text{ with } \sigma' := (12) \in S_3.$$

Since (12) and (132) generate the symmetric group S_3, these results show that G is isomorphic to S_3 and it permutes the cosets $[v], [w], [e]$.