Lattices

Def: Let Q be a nondegenerate symmetric bilinear form on $\mathbb{Z}^n$. Then $(\mathbb{Z}^n, Q)$ is called a lattice (of rank n)

Note: If a matrix is given for Q, it is understood that the standard basis has been chosen.

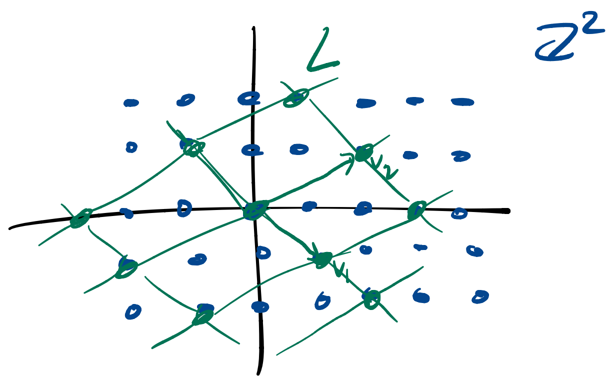
Ex:
- $(\mathbb{Z}^n, I)$ is the standard positive definite lattice
- $(\mathbb{Z}^n, -I)$ is the standard negative definite lattice

Def: Let $\{v_1, \dots, v_k\} \subset \mathbb{Z}^n$ be a linearly independent set of vectors. Let $L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \dots, v_k\}$. Then (L, Q) is called a sublattice of $(\mathbb{Z}^n, Q)$ of rank k. If $k = n$, (L, Q) is called a full rank sublattice

Ex: $v_1 = e_1 - e_2$

$v_2 = 2e_1 + e_2$

$L = \mathrm{Span}_{\mathbb{Z}}\{v_1, v_2\}$



Def: Let $(\mathbb{Z}^n, Q_1)$ and $(\mathbb{Z}^n, Q_2)$ be lattices

A lattice embedding $(\mathbb{Z}^n, Q_1) \to (\mathbb{Z}^n, Q_2)$ is a map $\varphi: \mathbb{Z}^n \to \mathbb{Z}^n$ satisfying:

(i) $\varphi(v+w) = \varphi(v) + \varphi(w) \quad \forall\ v, w \in \mathbb{Z}^n$ (φ is a group homomorphism)

(ii) $Q_1(v,w) = Q_2(\varphi(v), \varphi(w)) \quad \forall\ v, w \in \mathbb{Z}^n$

We usually write $\varphi: (\mathbb{Z}^n, Q_1) \to (\mathbb{Z}^n, Q_2)$

Note: If (i) is true, we need only check that (ii) is true on basis $\{e_1, \dots, e_n\}$ for $\mathbb{Z}^n$. Since $Q_1(e_i, e_j) = (i,j)$-th entry of Q_1, we need to check $Q_2(\varphi(e_i), \varphi(e_j)) = (i,j)$-th entry of Q_1

Note: $(\mathrm{Im}\,\varphi, Q_2)$ is a sublattice of $(\mathbb{Z}^n, Q_2)$

Note: Lattice embeddings are injective

Ex: Let $Q_1 = \begin{bmatrix} -5 & 1 \\ 1 & -2 \end{bmatrix}$ and $Q_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I$

Find a lattice embedding $\varphi: (\mathbb{Z}^2, Q_1) \to (\mathbb{Z}^2, Q_2)$

Let $\{f_1, f_2\}$ denote the standard basis for the domain

Let $\{e_1, e_2\}$ denote the standard basis for the codomain

Then
$$\varphi(f_1) = x_1 e_1 + x_2 e_2 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$
$$\varphi(f_2) = y_1 e_1 + y_2 e_2 = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

• $-5 = Q_1(f_1,f_1) = Q_2(\varphi(f_1),\varphi(f_1)) = -x_1^2 - x_2^2 \Rightarrow (x_1,x_2) \in \{(\pm 2,\pm 1),(\pm 1,\pm 2)\}$

Choose $x_1 = -2$, $x_2 = 1$. Note: Choosing another possibility corresponds to change of basis.

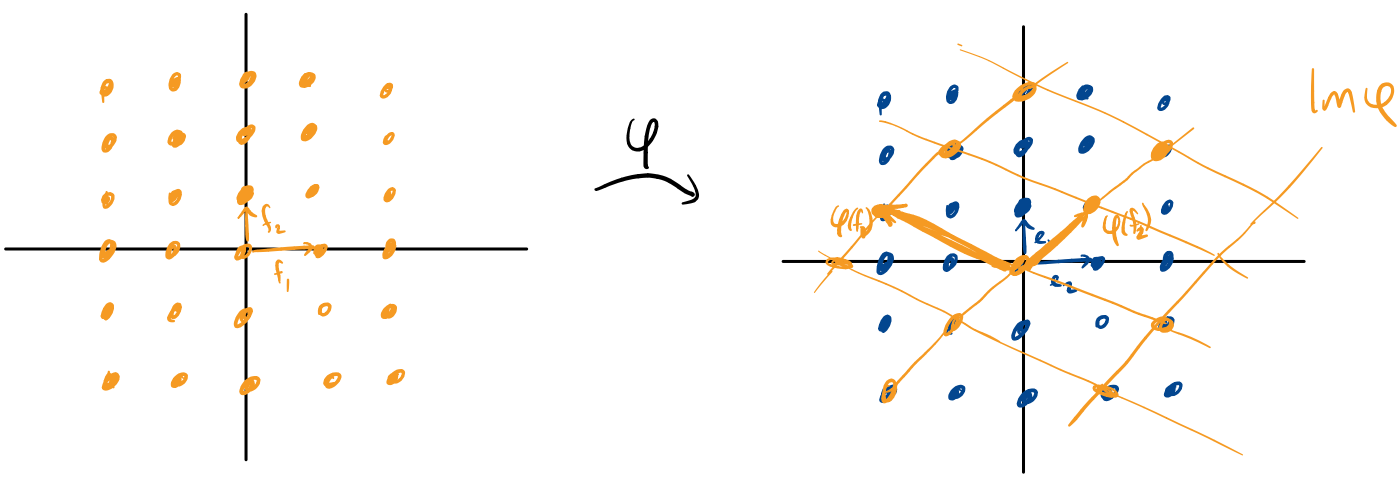
• $-2 = Q_1(f_2,f_2) = Q_2(\varphi(f_2),\varphi(f_2)) = -y_1^2 - y_2^2 \Rightarrow (y_1,y_2) = (\pm 1,\pm 1)$

• $1 = Q_1(f_1,f_2) = Q_2(\varphi(f_1),\varphi(f_2)) = -x_1y_1 - x_2y_2 = 2y_1 - y_2$

$\Rightarrow y_1 = y_2 = 1.$

So $\varphi(f_1) = -2e_1 + e_2$

$\varphi(f_2) = e_1 + e_2$



Since $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$, we can express it as the matrix $A = \begin{bmatrix} 1 & -2 \\ 1 & 1 \end{bmatrix}$

since $\varphi(f_1) = A\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\1\end{bmatrix} = e_1 + e_2$

$\varphi(f_2) = A\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}-2\\1\end{bmatrix} = -2e_1 + e_2$

In general, given bases for $(\mathbb{Z}^n, Q_1)$ and $(\mathbb{Z}^n, Q_2)$, a lattice embedding $\varphi: (\mathbb{Z}^n, Q_1) \to (\mathbb{Z}^n, Q_2)$ can be expressed as multiplication by a matrix P

i.e. $\varphi(v) = Pv \quad \forall \; v \in \mathbb{Z}^n$

Moreover, since $Q_1(v,w) = Q_2(\varphi(v), \varphi(w))$

we have that $Q_1(v,w) = Q_2(Pv, Pw)$.

If Q_1 and Q_2 are also matrix representations for Q_1 and Q_2, we have $v^T Q_1 w = v^T (P^T Q_2 P) w$

$\Rightarrow Q_1 = P^T Q_2 P$

Hence $\det Q_1 = \det P^T \det Q_2 \det P = (\det P)^2 \cdot \det Q_2$.

Upshot: If $\exists$ lattice embedding $\varphi: (\mathbb{Z}^n, Q_1) \to (\mathbb{Z}^n, Q_2)$, then $\dfrac{\det Q_1}{\det Q_2}$ is a perfect square.

Ex: Let $Q_1 = \begin{bmatrix} -2 & 1 \\ 1 & -2 \end{bmatrix}$, $Q_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

Show $\nexists$ lattice embedding $\varphi : (\mathbb{Z}^2, Q_1) \to (\mathbb{Z}^2, Q_2)$

Method 1: $\dfrac{\det Q_1}{\det Q_2} = \dfrac{3}{1} = 3$ is not a perfect square

(This does not always work, so we'll also prove this using a method that always works)

Method 2:

Assume $\exists$ an embedding φ.

Then $\varphi(f_1) = x_1 e_1 + x_2 e_2$

$\varphi(f_2) = y_1 e_1 + y_2 e_2$

- $-2 = Q_1(e_1, e_1) = Q_2(\varphi(f_1), \varphi(f_1)) = -x_1^2 - x_2^2$

  $\Rightarrow x_1, x_2 \in \{\pm 1\}$

- $-2 = Q_1(e_2, e_2) = Q_2(\varphi(f_2), \varphi(f_2)) = -y_1^2 - y_2^2$

  $\Rightarrow y_1, y_2 \in \{\pm 1\}$

But then $Q_2(\varphi(f_1), \varphi(f_2)) = -x_1 y_1 - x_2 y_2 \in \{0, \pm 2\}$

while $Q_1(f_1, f_2) = 1$

Thus we have reached a contradiction

$\Rightarrow \nexists$ a lattice embedding