Q $\mathbb{Z}\{v_1, v_2, v_3\} \overset{?}{=} \mathbb{Z}\{w_1, w_2, w_3\}$.

$$(v_1\ v_2\ v_3) = (w_1\ w_2\ w_3)\,A$$

$$\begin{pmatrix} 1 & 1 & 4 \\ 2 & -1 & 2 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} A$$

$$A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 & 4 \\ 2 & -1 & 2 \\ 1 & 1 & 3 \end{pmatrix}$$

$$= \frac{1}{3}\begin{pmatrix} 1 & 1 & 0 \\ -1 & 2 & 0 \\ -1 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 & 4 \\ 2 & -1 & 2 \\ 1 & 1 & 3 \end{pmatrix}$$

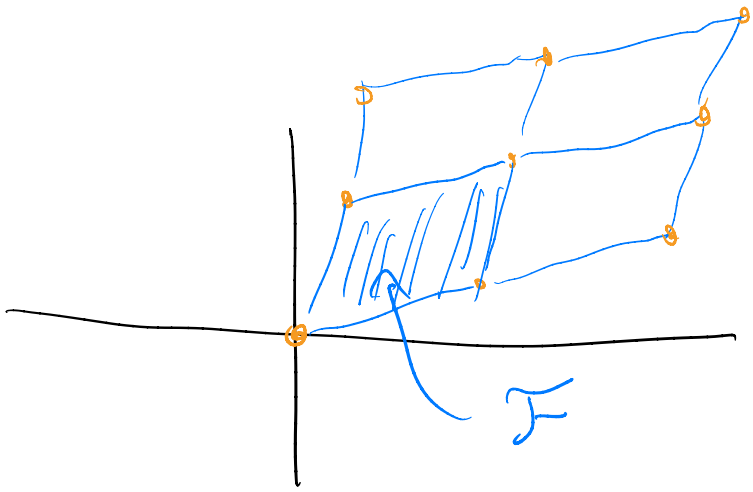
$$= \begin{pmatrix} 1 & 0 & 2 \\ 1 & -1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$\det(A) = -1 + 2 = 1 \in \mathbb{Z}^\times \Rightarrow A \in Gl_n(\mathbb{Z})$.

$\Rightarrow \mathbb{Z}\{v_1, v_2, v_3\} = \mathbb{Z}\{w_1, w_2, w_3\}$.

Def The fundamental domain F of L wrt a basis $\{v_1, \dots, v_n\}$ is

$$\left\{ x = t_1 v_1 + \cdots + t_n v_n \;:\; 0 \le t_i < 1 \right\}$$



Rmk If $n = m$ then $\mathbb{R}^m = F + L$.
In other words, $\mathbb{R}^m$ is perfectly covered by translates of F.

Prop If L has rk m, then

$$\mathrm{vol}(F) = \left| \det(v_1 \cdots v_n) \right|.$$

More generally, if n not nec. equal to m,

$$\mathrm{vol}(\mathcal{F}) = \left(\det(\langle v_i, v_j \rangle)\right)^{1/2}.$$

So if v_i have integer entries, $\mathrm{vol}(\mathcal{F})$ is the square root of an integer.

Ex (1) $L_2 = \mathbb{Z}\left\{\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1/2\\1\end{pmatrix}\right\}$

$$\Rightarrow \mathrm{vol} = \left|\det\begin{pmatrix}0 & 1/2\\ 1 & 1\end{pmatrix}\right| = |-1/2| = 1/2.$$

(2) $L_1 = \mathbb{Z}\left\{\begin{pmatrix}1\\1\end{pmatrix}\right\}$

$$\mathrm{vol} = \sqrt{2} = \sqrt{\det\left\langle \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right\rangle}$$

Proof

General Case $\Rightarrow$ n=m formula

$$\det(\langle v_i, v_j \rangle) = \det\left[\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} (v_1 \cdots v_n)\right]$$

$$= \det\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \det(v_1 \cdots v_n)$$

$$= \det(v_1 \cdots v_n)^2.$$

General case $\Rightarrow$ $\mathrm{vol}(F) = |\det(v_1 \cdots v_n)|$.

General Case

Apply Gram Schmidt process to $v_1, \ldots, v_n$.

to get $w_1, \ldots, w_n$ $\blacksquare$!

$$w_1 = v_1$$

$$w_2 = v_2 - \frac{\langle v_2, w_1 \rangle}{\langle w_1, w_1 \rangle} w_1$$

$$w_3 = v_3 - \frac{\langle v_3, w_1 \rangle}{\langle w_1, w_1 \rangle} w_1 - \frac{\langle v_3, w_2 \rangle}{\langle w_2, w_2 \rangle} w_2$$

$$\vdots$$

$$(\mathrm{Vol}(\mathcal{F}))^2 = \|w_1\|^2 \cdots \|w_n\|^2$$

$$= \det \begin{pmatrix} \|w_1\|^2 & & \\ & \ddots & \\ & & \|w_n\|^2 \end{pmatrix}$$

$$= \det \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} (w_1 \cdots w_n)$$

$$= \det S^t \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} (v_1 \cdots v_n) S$$

$$= \det \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} (v_1 \cdots v_n)$$

□

S an $n \times n$ change of basis

$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ upper triangular $\Rightarrow \det(S) = 1$

Cor $\mathrm{Vol}(\mathcal{F})$ does not depend on choice of basis of L.

Def $\det(L) = \mathrm{Vol}(\mathcal{F})$.

Pf If $(w_1 \cdots w_n) = (v_1 \cdots v_n) A$ w/ $A \in GL_n(\mathbb{Z})$.

then $\mathrm{Vol}(\mathcal{F}')^2 = \det \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} (w_1 \cdots w_n)$

$$= \det A^t \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} (w_1 \cdots w_n) A$$

$$= \det(A^t)\det(A)\det\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} (w_1 - w_n)$$

$$= (\pm 1)^2 \operatorname{vol}(\mathcal{F})^2$$

$$= \operatorname{vol}(\mathcal{F})^2. \qquad \square$$

Prop (Hadamard inequality)

$\det(L) \leq \|v_1\| \cdots \|v_n\|$ w/ equality iff

$v_1, \ldots, v_n$ orthogonal.

Defn Given $\{v_1, \ldots, v_n\}$ the **Hadamard ratio**

$$H(v_1, \ldots, v_n) = \left(\frac{\det(L)}{\|v_1\| \cdots \|v_n\|} \right)^{1/n} \leq 1.$$

$H \in (0, 1]$ measures orthogonality.

Hard Problems

Shortest vector problem (SVP):

Find $v \in L$ a nonzero vector w/ minimal $\|\vec{v}\|$

Closest vector problem (CVP):

Given $w \in \mathbb{R}^n$, find $v \in L$ minimizing $\|v - w\|$.

How to solve SVP/CVP

Observation: easy if $v_1, \dots, v_n$ an orthogonal basis of L.

SVP: $v = a_1 v_1 + \dots + a_n v_n \quad a_i \in \mathbb{Z}$

$$\|v\|^2 = a_1^2 \|v_1\|^2 + \dots + a_n^2 \|v_n\|^2.$$

$\Rightarrow v_{shortest} = v_i$ where v_i shortest among $v_1, \dots, v_n$.

CVP Write $w = t_1 v_1 + \cdots + t_n v_n \quad t_i \in \mathbb{R}$

Then $\|v - w\|^2 = (a_1 - t_1)^2 \|v_1\|^2 + \cdots + (a_n - t_n)^2 \|v_n\|^2$

$\Rightarrow v_{closest} = \text{round}(t_1) v_1 + \cdots + \text{round}(t_n) v_n$.

Not every lattice has an orthogonal basis, but these algorithms work if we have a basis that is almost orthogonal $\mathcal{H} \sim 1$.