

# Réseaux Euclidiens

## Définition

- Étant donné  $B = (b_1, \dots, b_n)$  une base de  $\mathbb{R}^n$ , on définit le réseau engendré par  $B$ :

$$L(B) = \{xB \mid x \in \mathbb{Z}^n\} = \left\{ \sum_{i=1}^n x_i b_i \mid x_1, \dots, x_n \in \mathbb{Z} \right\}$$

- Étant donné un point  $v \in L$ , on note sa norme Euclidienne:

$$\|v\| = \sqrt{v_1^2 + \dots + v_n^2}$$

- On note la longueur du plus court vecteur non nul de  $L$

$$\lambda = \min_{v \in L \setminus \{0\}} \|v\|$$

# Réseaux Euclidiens

Exemple:  $\mathbb{Z}^2$

Soit la base  $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

On engendre le réseau:

$$\begin{aligned} L &= \{xB \mid x \in \mathbb{Z}^2\} \\ &= \left\{ x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mid x_1, x_2 \in \mathbb{Z} \right\} \end{aligned}$$

