Лекция №1
Евклидовы решётки

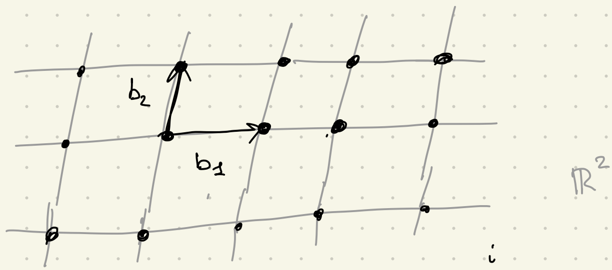
I. Опр-ия

$\boxed{\text{Опр-е 1}}$ Пусть $\{b_i\}_{i\le d}$ – лин. незав-ие вектора в $\mathbb{R}^n$ $(d \le n)$

Решётка, порождённая $\{b_i\}$ – это мн-во вида

$$\mathcal{L}(\{b_i\}_{i\le d}) = \sum_i \mathbb{Z} b_i = \{\sum_{i=1}^{d} x_i b_i \quad x_i \in \mathbb{Z}\}$$

Альтернативное опр-ие Решётка – это дискретная, конечно-порождённая, аддитивная подгруппа в $(\mathbb{R}^n, +)$.



Примеры

1) $\mathbb{Z}^n$, $n \geq 1$ $\quad \{b_i = e_i\}$, $e_i = (0, 0, .., \overset{i}{1}, 0, .. 0)$
2) $\forall$ подгруппа $\mathbb{Z}^n$, например $2\mathbb{Z}^n$
3) $a\mathbb{Z} + b\mathbb{Z}$, $\quad a, b \in \mathbb{Q}$

$\mathbb{Z} + \sqrt{2}\mathbb{Z}$ не является решёткой! (см. упр-ия).

$\boxed{\text{Опр-ие 2}}$ Пусть $\mathcal{L} = \mathcal{L}(\{b_i\})$ – решётка для лин. незав-ие $\{b_i\}$, $b_i \in \mathbb{R}^n$.

Тогда $\{b_i\}$ является базисом $\mathcal{L}$.

$$B = \begin{bmatrix} | & & | \\ b_1 & \dots & b_d \\ | & & | \end{bmatrix} \in \mathbb{R}^{n\times d},$$

$\mathcal{L}(B)$ – решётка, порождённая векторами-столбцами в B

$\boxed{\text{Лемма 1}}$ Пусть $\{b_i\}_{i\le d}$ и $\{b_i'\}_{i\le d'}$ — два мн-ва лин. независ. векторов в $\mathbb{R}^d$. Тогда,

$\mathcal{L}(\{b_i\}) = \mathcal{L}\{b_i'\} \Leftrightarrow$
- $d = d'$ унимодулярная ($\det U = \pm 1$)
- $\exists U \in GL_d(\mathbb{Z})$, т.ч. $B = B' \cdot U$

$\triangleleft$ 1) "$\Leftarrow$" см. упражнения

2) "$\Rightarrow$" 1) $d = \dim \operatorname{Span}_{\mathbb{R}} (\{b_i\}_{i\le d}) = \dim \operatorname{Span}_{\mathbb{R}} (\{b_i'\}) = d'$

$$\operatorname{Span}_{\mathbb{R}}(\{b_i\}) = \sum \mathbb{R} b_i$$

2) $$\left.\begin{aligned} &b_1' \in \mathcal{L}(\{b_i\}) \Rightarrow b_1' = \sum_{j=1}^{d} u_{j1} b_j \\ &b_2' \in \mathcal{L}(\{b_i\}) \Rightarrow b_2' = \sum_{j=1}^{d} u_{j2} b_j \\ &\vdots \\ &b_d' = \ldots \end{aligned}\right\} \Rightarrow B' = B \cdot U$$

В итоге, $B' = B \cdot U$

Аналогично (выражая b_i через b_j'), имеем $B = B' \cdot V$

$U, V \in \mathbb{Z}^{d\times d} \Rightarrow \underline{B} = B' \cdot V = \underline{B \cdot U \cdot V}$

$$B - B \cdot U \cdot V = 0$$

$$B(Id - U \cdot V) = 0$$

$$\Updownarrow$$

$$U \cdot V = Id$$

$$\Downarrow$$

$$\underbrace{\det(U)}_{\in\mathbb{Z}} \cdot \underbrace{\det(V)}_{\in\mathbb{Z}} = \det(Id) = 1 \Rightarrow \det U, \det V \in \{\pm 1\}$$

$\Rightarrow U, V$ — унимодулярные. $\blacktriangleright$

Замечание Для $d \geq 2$, $\forall$ фиксированная решётка имеет ∞ много базисов.

"Простые" задачи на решётках

1. Для $v \in \mathbb{R}^n$ и $L = L(B)$, определить $v \in L(B)$? $v = B \cdot x$

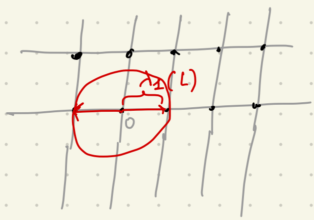
2. Определить, задают ли B и B' одну и ту же решётку.

II Инварианты решётки.

$\boxed{\text{Опр-ие 3}}$ (Первый) минимум решётки L:

$$\lambda_1(L) = \min \{ r : \exists b \in L \setminus \{0\} : \|b\| \le r \}$$

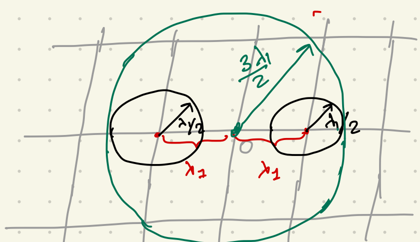
Евклидова норма (ℓ_2-норма: $\sqrt{\sum x_i^2}$)



$\boxed{\text{Лемма 2}}$ λ_1 достигается как min. дважды, и не более 3^d раз.

△ 1) $\|b_1\| = \lambda_1$, то $\|-b_1\| = \lambda_1$

2) $\forall b \in L$, т.ч. $\|b\| = \lambda_1$, нарисуем $B(b, \frac{\lambda_1}{2})$ (центр, радиус.)



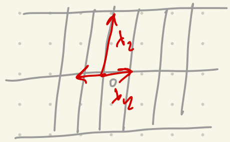
Эти шары не пересекаются. С другой стороны, эти шары лежат в $B(0, \frac{3\lambda_1}{2})$

$$\Rightarrow \#\text{шаров} \le \frac{\operatorname{Vol} B(0, \frac{3\lambda_1}{2})}{\operatorname{Vol} B(0, \frac{\lambda_1}{2})} = \frac{\left(\frac{3\lambda_1}{2}\right)^d \cdot \operatorname{Vol} B(0,1)}{\left(\frac{\lambda_1}{2}\right)^d \cdot \operatorname{Vol} B(0,1)} = 3^d$$

▶

$\boxed{\text{Опр-ие 4}}$ Последовательные минимумы решётки: для $i \le d$:

$$\lambda_i = \min\{r : \dim(B(0,r) \cap L \ge i\}.$$



$\boxed{\text{Лемма 3}}$ $\forall L$, $\exists c_1 \ldots c_d \in L$, т.ч. $\|c_i\| = \lambda_i(L)$ $\forall i \in L$.

(!) $\exists$ решётки, для которых $\nexists$ базиса, вектора которого достигают λ_i одновременно.

Например, $B = \begin{bmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ $\lambda_1 = 2$ $\lambda_2 = 2$ $\lambda_3 = 2$ $\lambda_4 = 2$ $\lambda_5 = 2$ (т.к.

$(2,2,2,2,2) - (2,0,0,0,0) - (0,2,0,0,0) - (0,0,2,0,0) - (0,0,0,2,0)$

$= (0,0,0,0,2)$))

$\boxed{\text{Опр-ие 5}}$ Пусть $B \in \mathbb{R}^{n \times d}$ - базисная матрица решётки L.

Опр-ль L, $\det(L)$ - это

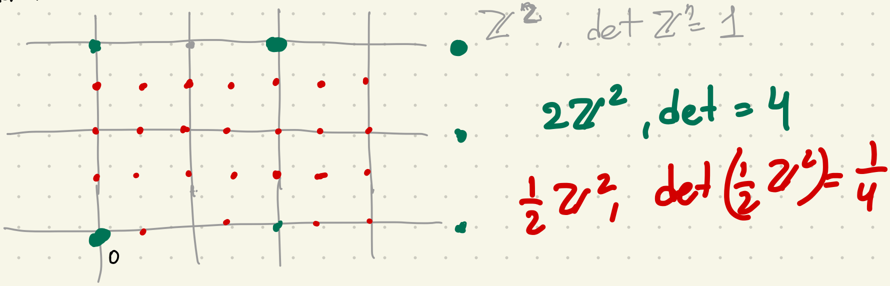
$$\det(L) = \sqrt{\det(B^T \cdot B)}$$

Для $B \in \mathbb{R}^{d \times d}$, $\det(L) = \sqrt{\det(B^T \cdot B)} = \sqrt{\det B^T \cdot \det B} = \sqrt{\det B^2} = |\det B|$.

$\boxed{\text{Лемма 4}}$ Если B, B' - два базиса одной и той же решётки, то

$$\det(B^T \cdot B) = \det(B'^T \cdot B')$$

Определитель решётки задаёт ее "плотность": чем меньше опр-ль, тем "плотнее" решётка.



$\boxed{\text{Опр-ие 6}}$ $P(\{b_i\}) = \left\{\sum y_i b_i,\ y_i \in [0,1)\right\}$ – фундаментальный параллелепипед L

$\det L = vol\,(P\{b_i\})$.