Лекция №1
Евклидовы решётки

I Определения

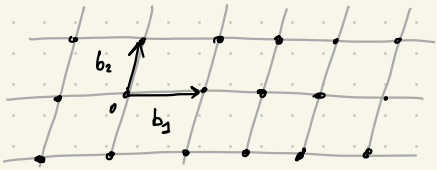
Опр-ие 1 Пусть $\{b_i\}_{i\le d}$ – лин. независимые вектора в $\mathbb{R}^n$ $(d \le n)$

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

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

При этом d называет размерностью / рангом решётки.

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



$\mathbb{R}^2$

Примеры

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

$\mathbb{Z} + \sqrt{2}\mathbb{Z}$ НЕ является решёткой! (см. упражнения)

Опр-ие 2 Пусть $\mathcal{L}(\{b_i\})$ – решётка, порождённая лин. независимыми $\{b_i\}$, $b_i \in \mathbb{R}^n$. Тогда $\{b_i\} \subset \mathbb{R}^n$ является базисом $\mathcal{L}$.

$$B = \begin{bmatrix} | & & | \\ b_1 & \dots & b_d \\ | & & | \end{bmatrix} \in \mathbb{R}^{n \times d}; \quad \mathcal{L}(B) - \text{решётка, порождённая столбцами } B.$$

Лемма 1 Пусть $\{b_i\}_{i\le d}$ и $\{b_i'\}_{i\le d'}$ — два ни-ва линейно независимых векторов. Тогда

$$\mathcal{L}(\{b_i\}) = \mathcal{L}(\{b_i'\}) \Leftrightarrow \begin{cases} \bullet\ d = d' \\ \bullet\ \exists U \in GL_d(\mathbb{Z}), \text{ т.ч. } B = B'\cdot U \end{cases}$$

U - унимодулярная ($\det U = \pm 1$).

◀ "$\Leftarrow$" см. упражнения

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

2) $b_1' \in \mathcal{L}(\{b_i\}) \Rightarrow b_1' = \sum_{j=1}^{d} u_{j1} b_j$

$b_2' \in \mathcal{L}(\{b_i\}) \Rightarrow b_2' = \sum_{j=1}^{d} u_{j2} b_j$

$\vdots$

$b_d' \in \mathcal{L}(\{b_i\}) \Rightarrow b_d' = \sum_{j=1}^{d} u_{jd} b_j$

$$\left(\begin{array}{ccc} | & & | \\ b_1' & \dots & b_d' \\ | & & | \end{array}\right) = B' \Rightarrow B' = B \cdot U$$

В итоге, $B' = B \cdot U$

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

$U, V \in \mathbb{Z}^{d\times d}$

$$B = B' \cdot V = B \cdot U \cdot V$$

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

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

$$U \cdot V = \mathrm{Id}$$

$$\Downarrow$$

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

$\Rightarrow \det(U), \det(V) \in \{\pm 1\} \Rightarrow U, V$ - унимодулярные. ▶

Замечание Для $d \ge 2$, ∀ фиксированная решётка имеет ∞ много базисов.

"Простые" задачи на решётках:

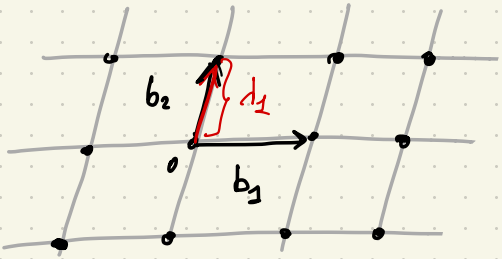
1. Для $v \in \mathbb{R}^n$ и $\mathcal{L}(B) \subset \mathbb{R}^n$, определить $v \in \mathcal{L}(B)$? $\quad v = B \cdot x$
2. Определить по B, B', задают ли они одну и ту же решётку

II Инварианты решётки.

Опр-е 3 (Первый) минимум решётки $\mathcal{L}$:

$$\lambda_1(L) = \min_{r \in \mathbb{R}} \{ r : \exists\, b \in \mathcal{L} \setminus \{0\} : \|b\| \le r \}$$

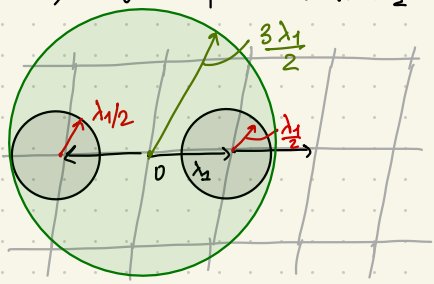
$\|\cdot\|$ — евклидова (B_2) норма



Лемма 2 λ_1 достигается как min. дважды, и не более, чем 3^d раз

△ 1) $v \in \mathcal{L}$ и $\|v\| = \lambda_1$, то $\|-v\| = \lambda_1$

2) $\forall v \in \mathcal{L}$, т.ч. $\|v\| = \lambda_1$ нарисуем $\mathcal{B} = (v, \frac{\lambda_1}{2})$. Эти шары не



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

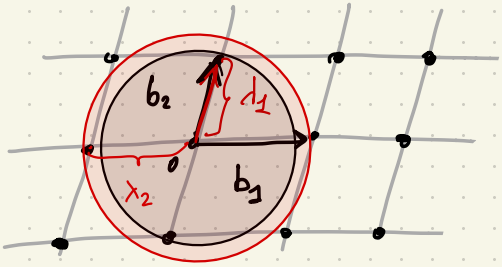
$$\Rightarrow \#\text{шаров} \le \frac{\mathrm{Vol}\, B(0, \frac{3\lambda_1}{2})}{\mathrm{Vol}\, B(0, \frac{\lambda_1}{2})} =$$

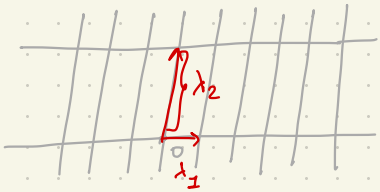
$$= \frac{\left(\frac{3\lambda_1}{2}\right)^d \cdot \mathrm{Vol}\, B(0,1)}{\left(\frac{\lambda_1}{2}\right)^d \cdot \mathrm{Vol}\, B(0,1)} = 3^d$$

▶

Опр-ие 4 Последовательные минимумы решётки для $i \le d$:

$$\lambda_i = \min_{r \in \mathbb{R}} \{ r \cdot \dim (B(0,r) \cap \mathcal{L}) \ge i \}.$$





Лемма 3 $\forall \mathcal{L}$ $\exists$ $v_1 \dots v_d \in \mathcal{L}$, т.ч. $\|v_i\| = \lambda_i(\mathcal{L})$.

$\exists$ 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. $(2,2,2,2,2)$ –
$(0,0,0,2,0)$ –
$(0,0,2,0,0)$ –
$(0,2,0,0,0)$ –
$(2,0,0,0,0)$ =
$(0,0,0,0,2)$.

Опр-ие 5 Пусть $B \in \mathbb{R}^{n \times d}$ – базисная матрица $\mathcal{L}$

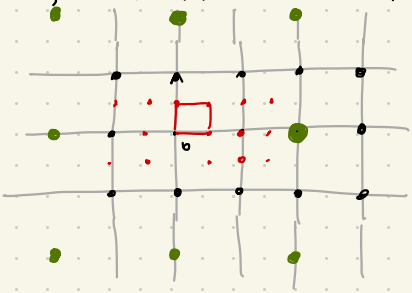
Определитель $\mathcal{L}$, $\det(\mathcal{L})$ – это

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

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

Следствие Если B, B' – два базиса одной и той же решётки, то $\det (B^T \cdot B) = \det (B'^T \cdot B')$

Определитель решётки задаёт её "плотность": чем меньше определитель, тем "плотнее" решётка.



$\mathbb{Z}^2$, $\det \mathbb{Z}^2 = 1$

$2\mathbb{Z}^2$ $\det 2\mathbb{Z}^2 = 4$

$\frac{1}{2}\mathbb{Z}^2$ $\det \frac{1}{2}\mathbb{Z}^2 = \frac{1}{4}$

Опр-ие 6 $\mathcal{P}(\{b_i\}) = \{ \sum y_i b_i \,,\ y_i \in [0,1) \}$ — фунд. параллелепипед

$\det \mathcal{L} = \mathrm{Vol}(\mathcal{P}(\{b_i\}))$