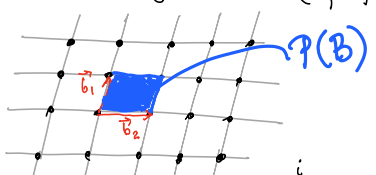
I. Определения

Опр-ие 1 Пусть $\{b_i\}_{i \le d}$ – лин. независ. вектора в $\mathbb{R}^n$ $(d \le n)$.
Решётка, порождённая $\{b_i\}_{i \le d}$ – мн-во вида

$$L(\{b_i\}_{i\le d}) = \sum_i \mathbb{Z}\cdot b_i = \{\sum x_i b_i,\ x_i \in \mathbb{Z}\}$$

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



Примеры: 1) $\mathbb{Z}^n$, $n \ge 1$ $\{b_i = e_i\}$; $\frac{1}{2}\mathbb{Z}^n$
$e_i = (0..0,\overset{i}{1},0..0)$

2) $\forall$ подгруппа $\mathbb{Z}^n$, например, $2\mathbb{Z}^n$;

3) $a\mathbb{Z} + b\mathbb{Z}$, $a, b \in \mathbb{Q}$

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

Опр-ие 2 Пусть $L = L(\{b_i\})$ для лин. независ. $b_i \in \mathbb{R}^n$. Тогда $\{b_i\}$ – базис L. $B = \begin{bmatrix} | & & | \\ b_1 & \dots & b_d \\ | & & | \end{bmatrix} \in \mathbb{R}^{n\times d}$, $L(B)$ – решётка, порождённая $\{b_i\}_{i\le d}$

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

$L(\{b_i\}_{i\le d}) = L(\{b_i'\}_{i\le d'}) \iff$
- $d = d'$ – унимодулярные $d\times d$ матрицы, $\det(U) = \pm 1$
- $\exists\ U \in GL_d(\mathbb{Z})$ т.ч. $B = B' \cdot U$, где

$$B = \begin{bmatrix} | & & | \\ b_1 & \dots & b_d \\ | & & | \end{bmatrix},\quad B' = \begin{bmatrix} | & & | \\ b_1' & \dots & b_d' \\ | & & | \end{bmatrix}.$$

◀ "$\Leftarrow$" (см. упражнения)

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

оболочка $= \sum_i \mathbb{R}\cdot b_i$

2) $b_1' \in L(\{b_i\})$
$\Rightarrow b_1' = \sum_{j=1}^d u_{j1} b_i$
$b_2' \in L(\{b_i\})$
$\Rightarrow b_2' = \sum_{j=1}^d u_{j2} b_i$
$\vdots$
$b_d' = \dots$

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

$B = B'\cdot V = B\cdot U\cdot V \iff B(\underline{Id - U\cdot V}) = 0$
$\Rightarrow$ т.к. B сост. из лин. независ. векторов $\Rightarrow U\cdot V = Id$
$\underset{\in\mathbb{Z}}{\det(U)}\cdot\underset{\in\mathbb{Z}}{\det(V)} = 1$ ▶

Замечание: Для $d \ge 2$, $\forall$ фиксированная решётка имеет ∞ много различных базисов.

"Простые" задачи на решётках:

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

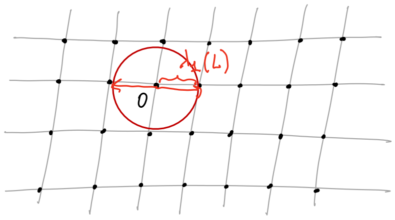
② Определить, задают ли B, B' одну и ту же решётку.

II Инварианты решётки

Опр-ие 3 (Первый) минимум решётки L:

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

Здесь $\|\cdot\|$ - Евклидова (ℓ_2)-норма $\quad \|x\| = \sqrt{\sum x_i^2}$; $\quad \|x\|_\infty = \max_i |x_i|$



Лемма 2 λ_1 достигается не менее 2х раз и не более 3^d раз.

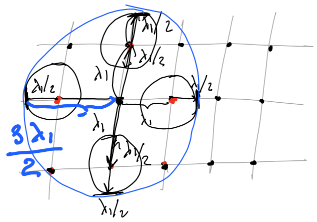
◄ 1) $\|b_1\| = \lambda_1 \Rightarrow \|-b_1\| = \lambda_1$

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

Эти шары не пересекаются (иначе, противоречие λ_1).

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

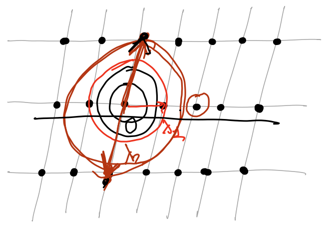
$$\Rightarrow \#\text{ шаров} \le \frac{\mathrm{Vol}\, B(0, \frac{3\lambda_1}{2})}{\mathrm{Vol}(B(0, \lambda_1/2))} = \frac{(3\lambda_1/2)^d \cdot \mathrm{Vol}(B(0,1))}{(\lambda_1/2)^d \cdot \mathrm{Vol}(B(0,1))} = 3^d.$$

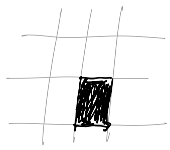


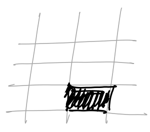
►

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

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







Лемма 3 $\forall L \quad \exists c_1, \dots, c_d \in L$ - лин. независ., т.ч. $\|c_i\| = \lambda_i(L) \quad \forall i \le d$

(λ_i достигаются $\forall L$)

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

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

$(2\,2\,2\,2\,2) - (2\,0\,0\,0\,0) - (0\,2\,0\,0\,0) - (0\,0\,2\,0\,0) - (0\,0\,0\,2\,0) = (0\,0\,0\,0\,2)$.

Опр-ие 5 Пусть $B \in \mathbb{R}^{n\times d}$ - базисная матрица решётки L (т.е. столбцы B образуют базис L).

Определитель L, $\det(L)$, - это

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

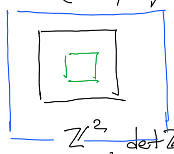
Для $B \in \mathbb{R}^{d\times d}$, $\det(L) = |\det B| \quad \left(\det(L) = \sqrt{\det(B^T)\cdot\det(B)} = \sqrt{\det(B)^2} = |\det B|\right)$.

Лемма 4 Если B, B' – два базиса одной и той же решётки, то

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

$\Big(B = B' \cdot U$ (лемма 1) $\Rightarrow \det(B^T \cdot B) = \det((B' \cdot U)^T \cdot B' \cdot U)$
$= \det U^T \cdot \det B'^T \cdot \det B' \cdot \det U$
$= \det(B'^T B'). \Big)$

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



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

$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$

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

$2\mathbb{Z}^2$, $\det(2\mathbb{Z}^2) = 4$

Опр-ие 6 $P(\{b_i\}_{i \le d}) = \{ \sum y_i b_i,\ y_i \in [0,1)\}$ – фундаментальный параллелепипед L.

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

III Теоремы Минковского

Теорема

1) $\lambda_1(L) \le \sqrt{d} \cdot (\det L)^{\frac{1}{d}}$

2) $\lambda_1^\infty(L) \le (\det L)^{\frac{1}{d}}$

$\mathbb{Z}^d$, $\lambda_1^\infty(\mathbb{Z}^d) = 1$

$(1\,0\,0 \ldots 0)$
$(0\,1\,0 \ldots 0)$
$\det \mathbb{Z}^d = 1$

$\Rightarrow$ граница Минковского для λ_1^∞ достигается $\mathbb{Z}^d$.