О лемме Минковского

Михаил Михайлов

Октябрь 2020

Содержание

Решетки. Простейшие свойства решеток

Определение. Пусть $\{\vec{b_1}, \dots \vec{b_n}\}$ — базис в $\mathbb{R}^n$.
Решетка в $\mathbb{R}^n$ — множество

$$L = \{\sum_{i=1}^{n} k_i \vec{b_i} \mid k_i \in \mathbb{Z}\}.$$

Фундаментальная область (ячейка) — множество

$$P = \{\sum_{i=1}^{n} x_i \vec{b_i} \mid x_i \in [0;1)\}.$$

Лемма 1.1. *Для любой точки* $\mathbf{x} \in \mathbb{R}^n$ *существует единственная* $\mathbf{y} \in P$*, такая что* $\mathbf{x} - \mathbf{y} \in L$.

Следствие. *Определено отображение* $p : \mathbb{R}^n \to P$.

Лемма 1.2. *Отображение* p *локально сохраняет объем: если* $E \subset \mathbb{R}^n$ *измеримо, и для любых* $\mathbf{x}, \mathbf{y} \in E : p(\mathbf{x}) \neq p(\mathbf{y})$*, то:*

$$\operatorname{vol} p(E) = \operatorname{vol} E$$

Доказательство. Представим E в следующем виде

$$E = \bigcup_{\mathbf{u} \in L} (E \cap P_u) = \bigcup_{\mathbf{u} \in L} E_u$$

Где P_u — P параллельно перенесенная на $\mathbf{u}$. Тогда, из инъективности p на E_u получаем что образы $p(E_u)$ не пересекаются. Тогда

$$\operatorname{vol} p(E) = \sum_{\mathbf{u} \in L} \operatorname{vol} p(E_u) = \sum_{\mathbf{u} \in L} \operatorname{vol} E_u = \operatorname{vol} E$$

□

Пример. Рассмотрим в $\mathbb{R}^2$ решетку точек с целочисленными координатами. D — круг радиуса $\frac{1}{3}$ с центром в $\mathbf{A} = (2, 1)$. Его образ изображен на рисунке 1

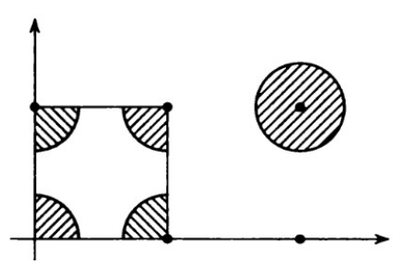

Рис. 1: Пример к лемме 1.2

Лемма Минковского

Определение. $F \subset \mathbb{R}^n$ выпукло, если для любых $\mathbf{x}, \mathbf{y} \in F : \{ t\mathbf{x} + (1-t)\mathbf{y} \mid t \in [0;1] \} \subset F$

Теорема 2.1 (Лемма Минковского)**.** *Пусть K — выпуклое и центрально-симметричное относительно начала координат подмножество $\mathbb{R}^n$, L — решетка в этом пространстве, P — ее фундаментальная область. Тогда если $\operatorname{vol} K > 2^n \operatorname{vol} P$, то K содержит хотя бы одну ненулевую точку из L.*

Доказательство. $\mathcal{F}$ — гомотетия с коэффициентом $\frac{1}{2}$, $K' = \mathcal{F}(K)$. Имеем

$$\operatorname{vol} K' = 2^{-n} \operatorname{vol} K > \operatorname{vol} P \Rightarrow p|_{K'} \text{ не инъективно}$$

Тогда существуют две различные точки $\mathbf{x}, \mathbf{y} \in K'$, такие что $p(\mathbf{x}) = p(\mathbf{y}) \Leftrightarrow \mathbf{x} - \mathbf{y} \in L$. Имеем $2\mathbf{x}, 2\mathbf{y} \in K$. Тогда, в силу центральной симметрии множества K $-2\mathbf{y} \in K$ и середина отрезка соединяющего $\mathbf{x}, \mathbf{y}$ лежит в K в силу выпуклости:

$$\mathbf{z} = \frac{1}{2}(2\mathbf{x} + 2(-\mathbf{y})) \in K$$

Заметим, что если $\mathbf{x} = -\mathbf{y}$, то в силу того что $p(\mathbf{x}) = p(\mathbf{y})$, получаем, что:

$$\mathbf{x} = \sum_{i=1}^{n} \pm \frac{\vec{b_i}}{2}$$
$$\mathbf{y} = \sum_{i=1}^{n} \mp \frac{\vec{b_i}}{2}$$

Но тогда очевидно, $2\mathbf{x}, 2\mathbf{y} \in L$ □

Следствие. *Пусть L — решетка в $\mathbb{R}^n$ с объемом ячейки v. Существует отличная от 0 точка $\mathbf{x_0}$ такая что:*

$$|\mathbf{x_0}| \leqslant 2^n \sqrt{\frac{v}{\omega_n}} = r,$$

где ω_n — объем единичного n-мерного шара.

Доказательство. Рассмотрим последовательность n-мерных шаров $\{ D_k \}_{k=1}^{\infty}$с центрами в начале координат радиуса $r_k = r + \frac{1}{k}$. В каждом из шаров, по лемме Минковского найдется отличная от нуля точка $\mathbf{x_k} \in D_k$. Заметим, что так как в каждом из шаров содержится лишь конечное число точек любой решетки, то всегда можно выбрать точки так, чтобы последовательность $\{ \mathbf{x_k} \}_{k=1}^{\infty}$ стабилизировалась. Обозначим за $\mathbf{x_0}$ стабилизруемый элемент, тогда заметим, что в предельном переходе:

$$|\mathbf{x_k}| \leqslant r_k \Rightarrow |\mathbf{x_0}| \leqslant r$$

. □

Теорема Валена о рациональных приближениях

Теорема 3.1. *Для любого действительного α существует такая дробь $\frac{k}{n}$ со сколь угодно большим знаменателем, что:*

$$\left|\alpha - \frac{k}{n}\right| \leqslant \frac{1}{n^2}$$

Доказательство. Не теряя общности, будем считать α иррациональным числом в интервале $(0;1)$. Рассмотрим решетку

$$L(\varepsilon) = \{\,(x,y) \mid x = \frac{n\alpha - k}{\varepsilon},\ y = n\varepsilon,\ n,k \in \mathbb{Z}\,\},\varepsilon > 0$$

И квадрат A с вершинами в $(1,1),(1,-1),(-1,-1),(-1,1)$. Площадь ячейки $L(\varepsilon)$ равна 1. (См рис 3).

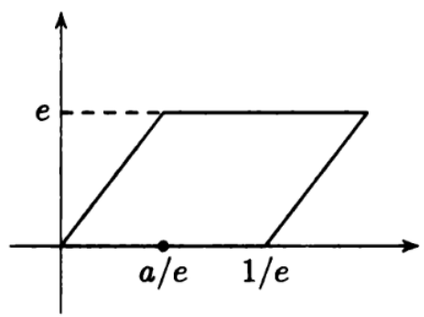

Рис. 2: Решетка $L(e)$

По лемме Минковского внутри квадрата будет ненулевая точка ячейки, тогда найдутся такие $k_0, n_0 \in \mathbb{Z}$, такие что

$$\left|\frac{n_0\alpha - k_0}{\varepsilon}\right| \leqslant 1 \wedge |n_0\varepsilon| \leqslant 1$$

Получаем, что:

$$\left|\alpha - \frac{k_0}{n_0}\right| \leqslant \frac{\varepsilon}{|n_0|} \leqslant \frac{1}{n_0^2}$$

□

Теорема Эйлера о сумме двух квадратов

Теорема 4.1 (Эйлер)**.** *Если $p \in \mathbb{P}$ и $p \equiv 1 \bmod 4$, то найдутся такие $a, b \in \mathbb{Z}$, что $a^2 + b^2 = p$*

Доказательство. Из теории чисел известно, что если $p \in \mathbb{P}$ и $p \equiv 1 \bmod 4$, то уравнение $x^2 + 1 = 0 \bmod p$ имеет корень. Обозначим его за u и рассмотрим решетку

$$L = \{ (a, b) \mid a, b \in \mathbb{Z}, b = ua \bmod p \}$$

Нетрудно видеть, что базисом это решетки являются вектора $\vec{b_1} = (1, u)$ и $\vec{b_2} = (0, p)$, а норма любого вектора всегда кратна p.

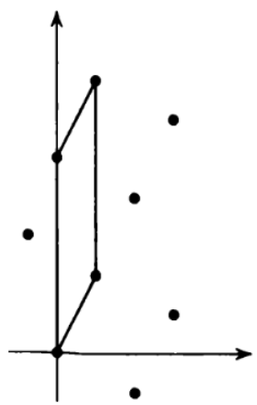

Рис. 3: Пример для $p = 5$

Площадь ячейки у такой решетки будет p. Так как $\omega_2 = \pi$, то по следствию из леммы Минковского найдется такой ненулевой вектор $(a, b) \in \mathbb{Z}^2$, что

$$a^2 + b^2 \leqslant 4\frac{p}{\pi} < 2p$$

Но тогда, так как норма кратна p, то $a^2 + b^2 = p$. □