Блок лекций “Объёмы выпуклых тел”
Лекция 5. Теорема Минковского о решётках

25.03.2023

Теорема 1 (Минковский)**.** *Пусть $K \subset \mathbb{R}^n$ ограничено, выпукло, центрально-симметрично. Тогда*

- *Если $\operatorname{Vol} K > 2^n$, то K содержит ненулевую точку целочисленной решётки, т.е. $K \cap (\mathbb{Z}^n \setminus \{0\}) \neq \varnothing$;*
- *То же справедливо в случае, если K замкнуто и $\operatorname{Vol} K \geqslant 2^n$.*

Доказательство. Выведем из первого утверждения второе. Для любого $\varepsilon > 0$ имеем $\operatorname{Vol}((1+\varepsilon)K) > 2^n$, поэтому $K(1+\varepsilon)$ содержит точку $x_\varepsilon \in \mathbb{Z}^n$; при $\varepsilon \to 0$ можно выделить сходящуюся подпоследовательность и её предел лежит в K.

Итак, пусть $\operatorname{Vol} K > 2^n$. Возьмём $K' = \frac{1}{2}K$ и докажем, что найдётся сдвиг $x \in \mathbb{Z}^n \setminus \{0\}$, такой что $K' \cap (K' + x) \neq \varnothing$. Если это так, то найдётся $v \in K'$, $v - x \in K'$. В силу симметричности, $x - v \in K'$ и $\frac{1}{2}(v + (x - v)) = \frac{1}{2}x \in K'$, то есть $x \in K$.

Предположим противное: все сдвиги $K' + x$, $x \in \mathbb{Z}^n$, не пересекаются. Возьмём большое R и множество сдвигов

$$\{K' + x \colon x \in \mathbb{Z}^n \cap [-R, R]^n\}.$$

Эти множества не пересекаются и лежат в кубе $[-R - r, R + r]^n$, где r — диаметр K'. Сравнивая объёмы, получим

$$(2R + 2r)^n \geqslant (2R + 1)^n \operatorname{Vol} K',$$

откуда $\operatorname{Vol} K' \leqslant ((2R + 2r)/(2R + 1))^n$. Переходя к пределу при $R \to \infty$, получим $\operatorname{Vol} K' \leqslant 1$ — противоречие. □

Решётки. Пусть $z_1, \ldots, z_n$ — базис $\mathbb{R}^n$. Решёткой с базисом $\{z_k\}$ называется множество

$$\Lambda(z_1, \ldots, z_n) = \{\sum_{i=1}^{n} k_i z_i \colon k_i \in \mathbb{Z}\}.$$

Дадим общее определение. Множество $\Lambda \subset \mathbb{R}^n$ называется решёткой, если выполнены условия

- Λ является подгруппой $(\mathbb{R}^n, +)$, т.е. сумма и разность любых элементов Λ лежат в Λ;
- Λ дискретна, т.е. $\inf\limits_{u,v\in\Lambda,\, u\neq v} |u - v| > 0$;
- $\operatorname{span}\Lambda = \mathbb{R}^n$.

Эти определения эквивалентны. (Однако, часто удобно говорить о решётках без уточнения базиса, так же как в линейных пространствах удобно не фиксировать базис.)

Утверждение 1. *Для любой решётки $\Lambda \subset \mathbb{R}^n$ существует базис: $\Lambda = \Lambda(z_1, \ldots, z_n)$.*

Доказательство. Докажем индукцией по j следующее утверждение: найдутся линейно независимые вектора $z_1, \ldots, z_j$, такие что для $F_j := \operatorname{span}\{z_1, \ldots, z_n\}$ все точки $\Lambda \cap F_j$ имеют вид $\sum_{i=1}^{j} k_i z_i$ с целыми k_i.

При $j = n$ мы получим требуемое утверждение.

База индукции: $j = 0$, ничего доказывать не нужно. Для наглядности всё же разберём случай $j = 1$. Возьмём произвольное $w \in \Lambda$, $w \neq 0$. Среди всех точек отрезка $\Lambda \cap \{tw \colon 0 \leqslant t \leqslant 1\}$, возьмём точку z_1 с минимальным ненулевым t. Это и будет нужный вектор. Действительно, если $u = tz_1 \in \Lambda$, то $u' = (t - \lfloor t \rfloor)z_1 \in \Lambda$. Если коэффициент в скобках ненулевой, то получаем противоречие с минимальностью z_1. Значит, коэффициент изначально целый.

Индуктивный переход аналогичен. Пусть построены $z_1, \ldots, z_{j-1}$. Рассматриваем $F_{j-1} := \operatorname{span}\{z_1, \ldots, z_{j-1}\}$, берём произвольно $w \in \Lambda \setminus F_{j-1}$, рассматриваем палаллелепипед

$$\{\sum_{i=1}^{j-1} t_i z_i + t_j w \colon t_i \in [0, 1]\}$$

и в нём точку z_j с минимальным t_j. Аналогично предыдущему доказывается, что она подходит. $\square$

Общий вид теоремы Минковского Пусть Λ — решётка. Она имеет базис $z_1, \ldots, z_n$. Определим $\det \Lambda := |\det Z|$, где Z — матрица со столбцами z_i.

Докажем корректность определения. Если $w_1, \ldots, w_n$ — другой базис Λ, то есть матрица перехода C. В силу того, что $w_k \in \Lambda(z_1, \ldots, z_n)$, все коэффициенты C целочисленны. Аналогично, коэффициенты C^{-1} целочисленны. Тогда $\det C, \det C^{-1} \in \mathbb{Z}$ и $\det C \cdot \det C^{-1} = 1$, поэтому эти определители равны ± 1.

Теперь мы можем сформулировать теорему Минковского в более общем виде.

Теорема 2. *Пусть $\Lambda \subset \mathbb{R}^n$ решётка; $K \subset \mathbb{R}^n$ ограничено, выпукло, центрально-симметрично. Тогда*

- *Если $\operatorname{Vol} K > 2^n \det \Lambda$, то K содержит ненулевую точку решётки Λ;*
- *То же справедливо в случае, если K замкнуто и $\operatorname{Vol} K \geqslant 2^n \det \Lambda$.*

Для доказательства достаточно рассмотреть линейное отображение, переводящее Λ в $\mathbb{Z}^n$ и применить теорему для стандартной решётки.

Приложения. Первый пример. Пусть $\alpha \in (0, 1)$ и $N \in \mathbb{N}$. Докажем (теорему Дирихле о том), что найдутся $p, q \in \mathbb{N}$, $q \leqslant N$, такие что

$$|\alpha - \frac{p}{q}| < \frac{1}{Nq}.$$

Перепишем неравенство в виде $|\alpha q - p| < 1/N$. Рассмотрим на плоскости множество

$$K = \{(x, y) \colon |\alpha x - y| < 1/N,\ |x| \leqslant N + 1/2.\}$$

Это параллелограмм и его площадь равна $\frac{2}{N} \cdot (2N + 1) > 4$. По теореме Минковского, найдётся ненулевая точка $(q, p) \in K \cap \mathbb{Z}^2$. Ясно, что $q \neq 0$, тогда считаем $q > 0$. Это и будет нужная пара.

Второй пример. Докажем известную теорему о том, что любое простое число p, для которого $p \equiv 1 \bmod 4$, представимо в виде суммы двух квадратов. Покажем, что для таких p число -1 будет квадратичным вычетом, т.е. $-1 \equiv x^2 \bmod p$ для некоторого $x \in \mathbb{Z}/p\mathbb{Z}$. Действительно,

рассмотрим в $\mathbb{Z}/p\mathbb{Z}$ произведение $1 \cdot 2 \cdots (p-1)$. Сомножители разбиваются на пары x и x^{-1}. Исключение составляют числа с $x = x^{-1}$, т.е $x^2 = 1$, т.е. $x = \pm 1$. Отсюда

$$1 \cdot 2 \cdots (p-1) \equiv -1 \bmod p.$$

С другой стороны, если бы -1 был квадратичным невычетом, то есть уравнение $-1 \equiv x^2 \bmod p$ не имело бы решений, то все сомножители разбивались бы на пары x и $-x^{-1}$ и произведение было бы равно $(-1)^{\frac{p-1}{2}}$ по модулю p, противоречие.

Итак, зафиксируем q, такое что $q^2 \equiv -1 \bmod p$. Рассмотрим на плоскости решётку Λ с базисом $z_1 = (1, q)$, $z_2 = (0, p)$. Тогда $\det \Lambda = p$. Положим $K := \{(x, y) \colon x^2 + y^2 \leqslant 2p$. Заметим, что $\operatorname{Vol} K = \pi \cdot 2p > 4\delta\Lambda$ и K содержит ненулевую целую точку $(u, v) = k_1 z_1 + k_2 z_2$, т.е. $u = k_1$, $v = k_1 q + k_2 p$. Далее вычислим по модулю p:

$$u^2 + v^2 = k_1^2 + (k_1 q + k_2 p)^2 \equiv k_1^2 (1 + q^2) \equiv 0 \bmod p.$$

То есть, $u^2 + v^2$ делится на p. Но $0 < u^2 + v^2 < 2p$, поэтому в точности $u^2 + v^2 = p$.

Третий пример. Рассмотрим симметричную положительно-определённую квадратичную форму

$$q(x) = \sum_{i,j=1}^{n} a_{i,j} x_i x_j.$$

Тогда следующее неравенство имеет нетривиальное целочисленное решение:

$$q(u) \leqslant 4 \left(\frac{\det(a_{i,j})}{\operatorname{Vol}(B_2^n)^2} \right)^{\frac{1}{n}}.$$

Рассмотрим множество вида $E_\lambda := \{x \colon q(x) \leqslant \lambda\}$. Это эллипсоид. Действительно, $q(x) = \langle Ax, x \rangle = \langle Bx, Bx \rangle$, где $BB^t = A$ и множество $\{x \colon q(x) \leqslant \lambda\}$ получается из стандартного шара $\{y \colon \langle y, y \rangle \leqslant \lambda\}$ заменой $y = Bx$. Отсюда

$$\operatorname{Vol} E_\lambda = \frac{\operatorname{Vol} \lambda^{n/2} B_2^n}{\det B} = \frac{\operatorname{Vol} \lambda^{n/2} B_2^n}{(\det A)^{1/2}}.$$

Остаётся подобрать λ, при котором $\operatorname{Vol} E_\lambda \geqslant 2^n$.

Четвёртый пример. Пусть $l_1(x), \ldots, l_n(x)$ — линейные формы в $\mathbb{R}^n$, и $|\det l_i| = \delta > 0$. Для любых чисел $\tau_1, \ldots, \tau_n$, таких что $\tau_1 \cdots \tau_n \geqslant \delta$,

следующая система неравенств имеет нетривиальное целочисленное решение:

$$|l_1(x)| \leqslant \tau_1, \ldots, |l_n(x)| \leqslant \tau_n.$$

Для доказательства нужно рассмотреть, очевидно, множество $K := \{x \in \mathbb{R}^n \colon |l_i(x)| \leqslant \tau_i,\ i = 1, \ldots, n\}$.

Разное Полезно следующее обобщение теоремы Минковского: если $K \subset \mathbb{R}^n$ выпукло, ограничено, симметрично и $\operatorname{Vol} K > k2^n$, то K содержит не менее k ненулевых точек целочисленной решётки.

Доказательство. Для доказательства вместо непересекающихся сдвигов $K' + x$, $x \in [-R, R]^n \cap \mathbb{Z}^n$ мы рассматриваем функцию

$$f(z) := \sum_{x \in [-R,R]^n \cap \mathbb{Z}^n} \mathbf{1}_{K'+x}.$$

Наша цель: доказать, что в некоторой точке $f(z_0) > k$. Тогда для некоторых $x_1, \ldots, x_{k+1}$ имеем $K' + x_i \ni z_0$. Тогда для $i = 2, \ldots, k+1$, имеем: $z_0 - x_1 \in K'$, $z_0 - x_i \in K'$, откуда $x_i - x_1 \in K$.

Если $f \leqslant k$, то $\int_{\mathbb{R}^n} f(z)\,dz = (2R+1)^n \operatorname{Vol}(K')$, с другой стороны, $\int_{\mathbb{R}^n} f(z)\,dz \leqslant k(2R+2r)^n$, отсюда в пределе $\operatorname{Vol}(K) \leqslant k$, противоречие. □

Ещё одна полезная теорема:

Теорема 3 (Ваалер)**.** *Любое сечение куба $[-\frac{1}{2}, \frac{1}{2}]^n$ линейным k-мерным пространством ($0 < k < n$) имеет объём не меньше единицы:*

$$\operatorname{Vol}_k([-\frac{1}{2}, \frac{1}{2}] \cap E_k) \geqslant 1.$$

Мы не доказываем эту теорему в данном курсе.

Приведём утверждение из работы Б.С. Кашина 1985 года.

Утверждение 2. *Существует такая абсолютная постоянная $C > 0$, такая что для любого набора векторов $\{e_j\}_{j=1}^m \subset \mathbb{R}^n$, $|e_j| = 1$, найдётся вектор $z = (z_1, \ldots, z_n)$ с координатами $z_i \in \{-1, 0, 1\}$, такой что $\|z\|_1 \geqslant n/6$ и*

$$\max_j |\langle z, e_j \rangle| \leqslant C\sqrt{m/n}, \quad j = 1, \ldots, m.$$

Этот результат может использоваться для построение многочленов со специальными свойствами.

Для доказательства рассматривается множество

$$K_\lambda := \{z\colon |z_i| \leqslant 1.99,\ |\lambda\langle z, e_j\rangle| \leqslant 1.99,\ j = 1, \dots, m\}.$$

Заметим, что K_λ это сечение куба $1.99B_\infty^{n+m}$ плоскостью

$$E := \{w \in \mathbb{R}^{n+m}\colon w_{n+j} = \sum_{i=1}^{n} \lambda w_i e_{j,i},\ j = 1, \dots, m.\}$$

С помощью теоремы Ваалера проверяется, что при нужном λ имеем $\operatorname{Vol} K_\lambda \geqslant 2^n \cdot 1.9^n$. Значит, K содержит не менее 1.9^n целочисленных точек. Все эти точки лежат в $\{-1, 0, 1\}$ и их много, поэтому среди них найдутся z с $\|z\|_1 \geqslant n/6$, что и требовалось.

Список литературы

[1] P.M. Gruber, *Convex and Discrete Geometry*. Springer, 2007.