

DAVENPORT · 圆法 · 高中详解版

数的几何

The geometry of numbers

本章要解决什么 · 读完能掌握什么

这一章和前面"圆法"主线看似无关，其实是为后面"三次型"（第 13 章起）准备的一件**几何工具**。它研究的核心对象叫**格**（lattice）——就是空间里一张"均匀的钉子板"，钉子（格点）按照规则铺满整个空间。我们想回答一个非常具体的问题：

"在一个半径为 R 的球里，这张钉子板上有多少颗钉子？"

这看似简单，但当格被拉得"又长又扁"时，答案会千差万别。本章引入一组数 $R_1 \leq R_2 \leq \dots \leq R_n$ （叫**相继极小**），用它们就能把"球里有几个格点"这件事算清楚（引理 12.4）。最后的引理 12.6 是给三次型问题量身定制的结论：它保证某组不等式的解的个数，当**区间缩小时不会缩小得太快**。

读完你会掌握：① 什么是格、格的基、格的行列式；② 闵可夫斯基（Minkowski）两条基本定理的思想（引理 12.1、12.2）；③ 相继极小如何刻画一个格；④ 伴随格（极格）与 Mahler 定理；⑤ 如何把一组线性不等式翻译成"球里数格点"的问题。沿途所有超出高中的记号（ $\det$ 、矩阵、 $\ll$ 、 $\asymp$ 、向量内积、 n 维球体积……）都从零讲起。

第 0 节 · 先补齐高中没学过的"地基"

本章会反复用到几样东西，高中课本里没有或只讲了一点点。先在这里一次性讲清楚，后面遇到就不再打断。

0.1 n 维空间里的"点"和"向量"

高中里平面上的点写成 (x, y) ，空间里写成 (x, y, z) 。把这个推广：所谓 n 维空间里的一个点，就是 n 个实数排成的一串

$$\mathbf{x} = (x_1, x_2, \dots, x_n).$$

记号 $\mathbf{x}$ (黑体 $\mathbf{x}$) 读作"向量 $\mathbf{x}$ "。它代表 n 个数 $x_1, \dots, x_n$ 的整体。脚标 x_1 读作" $\mathbf{x}$ 下标 1"，是这个点的第 1 个坐标。 n 是空间维数（一个固定的正整数，比如 2、3、6）。把 $\mathbf{x}$ 想成"从原点 $O = (0, \dots, 0)$ 出发指向该点的箭头"也完全可以——本章"点"和"向量"是一回事。

两个向量可以相加 $\mathbf{x} + \mathbf{y} = (x_1 + y_1, \dots, x_n + y_n)$ ，也可以乘一个数 $c\mathbf{x} = (cx_1, \dots, cx_n)$ ，就跟平面向量一样，只是分量更多。

0.2 点到原点的距离 $|\mathbf{x}|$

平面上点 (x_1, x_2) 到原点距离是 $\sqrt{x_1^2 + x_2^2}$ （勾股定理）。 n 维里照搬：

$$|\mathbf{x}| = \sqrt{x_1^2 + x_2^2 + \dots + x_n^2}.$$

记号 $|\mathbf{x}|$ 读作" $\mathbf{x}$ 的模长"或" $\mathbf{x}$ 的长度"，就是点 $\mathbf{x}$ 到原点 O 的直线距离。注意：每个坐标的绝对值一定不超过总长度，即 $|x_k| \leq |\mathbf{x}|$ （因为 $x_k^2 \leq x_1^2 + \dots + x_n^2$ ）。这个小事实后面会用到好幾次。

0.3 线性型、线性组合、线性无关

一个**线性型**（linear form）就是若干变量的"一次齐次"表达式，例如 $3u_1 - 2u_2 + u_3$ ，没有常数项、没有平方项。它无非是"把各变量按固定系数加权求和"。

把若干向量 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(k)}$ 各乘一个数再加起来， $c_1\mathbf{x}^{(1)} + \dots + c_k\mathbf{x}^{(k)}$ ，叫它们的一个**线性组合**。

若一组向量中"谁都不能写成其余几个的线性组合"，就说它们**线性无关**（linearly independent）。直观说： n 个线性无关的向量"撑开"了整个 n 维空间，方向上互不重复。平面里 $(1, 0)$ 与 $(0, 1)$ 线性无关；而 $(1, 0)$ 与 $(2, 0)$ 线性相关（后者是前者 2 倍，方向重复）。

0.4 矩阵与行列式 det

把 n^2 个数排成 n 行 n 列的方阵，叫一个 $n \times n$ **矩阵**，记作 $\Lambda = (\lambda_{ij})$ ， λ_{ij} 是第 i 行第 j 列那个数。

记号 λ_{ij} λ 是希腊字母，读"拉姆达"。 λ_{ij} 读作"拉姆达 i j"，下标 i 是行号、 j 是列号。

每个方阵有一个数叫它的**行列式**，记作 $\det \lambda_{ij}$ 或 $\det \Lambda$ 。它的几何意义是关键：

det 的几何意义（务必记住） 把矩阵的 n 个列向量当成 n 维空间里 n 条棱，它们张成一个"平行体"（二维是平行四边形，三维是平行六面体）。 $|\det|$ 就等于这个平行体的体积。若 $\det = 0$ ，说明这些列向量"压扁了"（线性相关，挤在低维里），体积为 0。所以" $\det \neq 0$ "正是"这 n 个方向真正撑满 n 维、线性无关"的代数说法。

二维例子：列向量 $(a, c), (b, d)$ 组成的矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ，行列式 $= ad - bc$ ，绝对值正是这两个向量张成的平行四边形面积。这个高中选修里见过。

0.5 整数集 $\mathbb{Z}$ 与"整系数"

记号 $\mathbb{Z}$ 读作"整数集", 指 $\dots, -2, -1, 0, 1, 2, \dots$ 全体整数 (来自德语 Zahlen "数")。说变量"取整数值"就是只允许它在 $\mathbb{Z}$ 里跳。本章格点的本质, 就是"系数被限制成整数"。

0.6 数量级记号 $O(\cdot)$ 、 $\ll$ 、 $\gg$ 、 $\asymp$

分析数论里不追求精确常数, 只关心"大约多大"。这套记号是全章的语言, 务必先吃透。

$A \ll B$ (读作"A 远小于等于 B", 即 $A = O(B)$)

意思是: 存在一个常数 $C > 0$ (在本章里这个 C 只许依赖维数 n , 不许依赖别的变量), 使得 $|A| \leq C B$ 永远成立。通俗讲就是"A 至多是 B 的某个固定倍数"。例如 $3x + 5 \ll x$ (当 $x \geq 1$), 因为 $3x + 5 \leq 8x$ 。

$A \gg B$ (读作"A 远大于等于 B")

就是 $B \ll A$ 反过来写: 存在固定常数 $c > 0$ 使 $A \geq c B$ 。即"A 至少是 B 的某个固定倍数"。

$A \asymp B$ (读作"A 与 B 同阶")

同时有 $A \ll B$ 与 $A \gg B$ 。意思是 A/B 被夹在两个正常数之间, A 和 B "差不多大、只差一个有界倍数"。本章正文里临时也写成 $A \asymp B$ (原书用 $\asymp$)。

为什么允许这么"粗" 本章服务于后面三次型的次弧估计, 那里只需要"数量级对、误差被主项压住", 常数 C 具体是 7 还是 700 无所谓。Davenport 在开篇就声明: 依赖 n 的常数对我们的目的不重要。所以全章放心地用 $\ll, \gg, \asymp$ 。

0.7 n 维球的体积 J_n

圆面积 πr^2 、球体积 $\frac{4}{3}\pi r^3$, 都是" r^n 乘一个只跟维数有关的常数"。一般地, n 维空间里半径 ρ 的球, 体积 $= J_n \rho^n$ 。

记号 J_n 表示 n 维空间里半径为 1 的球的体积（一个只依赖 n 的正常数）。比如 $J_2 = \pi$ （单位圆面积）， $J_3 = \frac{4}{3}\pi$ 。把半径放大到 ρ ，体积按比例放大 ρ^n 倍，得 $J_n \rho^n$ ——因为长度放大 ρ 倍， n 维体积就放大 ρ^n 倍。

0.8 历史背景：什么是"数的几何"

"数的几何"（geometry of numbers）这门学科由德国数学家闵可夫斯基（Hermann Minkowski, 1864–1909）在 1896 年前后创立。它的革命性想法是：很多关于**整数解**的纯算术问题（"某个不等式组有没有非零整数解？"），可以翻译成**几何问题**（"某个对称凸区域里是否含有格点？"），从而用体积、对称这类直观工具去解决。闵可夫斯基本人用它在数论、二次型理论里取得了一连串突破。本章只取其中"处理线性不等式"够用的几条，证明也用了对我们够用的简化版本（用球/椭球代替一般凸体）。

第 1 节 · 格、基、行列式

译文 我们现在来证明数的几何中的若干基本结果，仅限于那些有助于处理线性不等式的结果。更完整的论述（例如 Cassels 给出的 [12]）会既更一般又更精确：更一般之处在于把普通的距离换成了某种度量下的距离，更精确之处在于注意到了依赖于 n （维数）的常数。这类常数对我们所要达到的目的而言并不重要。

这段在说什么：开宗明义交代"取舍"。Davenport 告诉你他故意只讲一个简化版。"更一般"指：本章只用普通的欧氏距离 $\sqrt{x_1^2 + \cdots + x_n^2}$ ，而完整理论（Cassels 的专著，方括号 [12] 是书末参考文献编号）允许用别的"距离度量"。"更精确"指：本章对那些只依赖 n 的常数一律用 $\ll, \asymp$ 糊弄过去，不去算它

们到底是多少。最后一句给出理由——后面三次型的应用里，这些常数被吸收入"误差项"里，取值无所谓。这就是 0.6 节那套粗记号的"许可证"。

译文 n 维空间中的一个格 Λ ，是由 n 个变量 $u_1, \dots, u_n$ 的 n 个线性型——当这些变量取整数值时——所给出的所有（实）点 $\mathbf{x} = (x_1, \dots, x_n)$ 构成的集合：

$$\begin{aligned}x_1 &= \lambda_{11}u_1 + \cdots + \lambda_{1n}u_n, \\&\vdots \\x_n &= \lambda_{n1}u_1 + \cdots + \lambda_{nn}u_n,\end{aligned}$$

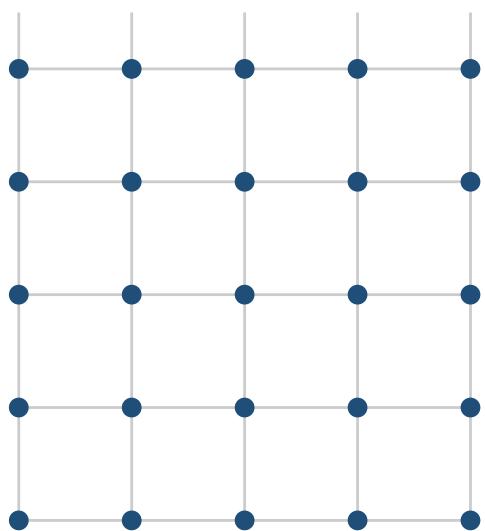
用矩阵记号即 $\mathbf{x} = \Lambda \mathbf{u}$ 。系数 λ_{ij} 是满足 $\det \lambda_{ij} \neq 0$ 的实数。

这段在定义本章的主角"格"。逐字拆开看。我们手里有 n^2 个固定的实数 λ_{ij} （这是"模板"，定好就不动了）。再准备 n 个变量 $u_1, \dots, u_n$ ，规定它们只能取整数。每给一组整数 $(u_1, \dots, u_n)$ ，上面那组式子就算出一个点 $\mathbf{x}$ 。把所有可能的整数组对应的点 $\mathbf{x}$ 收集起来，这一大堆点的集合就叫格 Λ 。

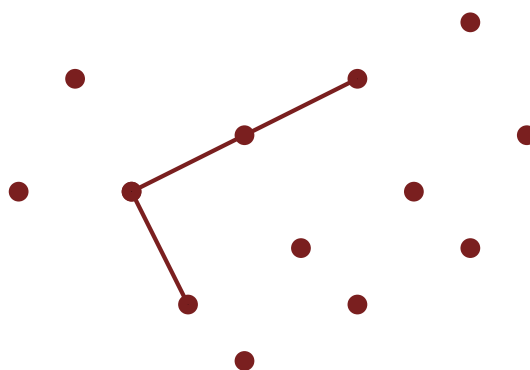
记号 Λ 、 u_j 、 $\mathbf{x} = \Lambda \mathbf{u}$ Λ 是大写希腊字母，读"拉姆达"，既表示这个格，也表示那个系数矩阵 (λ_{ij}) 。 u_j 读"u 下标 j"，是只能取整数的参数。 $\mathbf{x} = \Lambda \mathbf{u}$ 是把上面 n 行式子"打包"成的矩阵乘法写法：把 $\mathbf{u} = (u_1, \dots, u_n)$ 这一竖列乘上矩阵 Λ ，结果就是 $\mathbf{x}$ 。条件 $\det \Lambda \neq 0$ （见 0.4）保证这 n 个线性型"互不重复方向"，格才真正铺满 n 维而不是塌缩到低维。

最简单的例子 取 $n = 2$ ， $\lambda_{11} = \lambda_{22} = 1$ ， $\lambda_{12} = \lambda_{21} = 0$ ，则

$x_1 = u_1$ ， $x_2 = u_2$ 。于是格 Λ 就是所有整数坐标的点 (u_1, u_2) ，即平面上标准的方格钉子板 $\mathbb{Z}^2$ 。一般的 λ_{ij} 无非是把这块方格钉子板"拉伸、剪切、旋转"成一张倾斜的网。



标准格 $\mathbb{Z}^2$ (方网)



一般格 Λ (倾斜网)

格就是一张均匀的"钉子板"。左边是标准方格，右边是被拉斜的格；两条红线是右图的一组"基向量"（见下文）。

译文 对变量 $u_1, \dots, u_n$ 施行一个行列式为 1 的整系数线性代换（么模代换）不改变这个格。该格的点也可以表示为

$$\mathbf{x} = u_1 \mathbf{x}^{(1)} + \dots + u_n \mathbf{x}^{(n)},$$

其中 $\mathbf{x}^{(j)} = (\lambda_{1j}, \dots, \lambda_{nj})$, $j = 1, \dots, n$ 。点 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ 构成该格的一组基，而刚才提到的变量更换正对应于基的更换。

这段引入"基"，并指出格的描述不唯一。先解释第二个式子：把矩阵乘法 $\mathbf{x} = \Lambda \mathbf{u}$ 换种眼光看。 Λ 的第 j 列是向量 $\mathbf{x}^{(j)} = (\lambda_{1j}, \dots, \lambda_{nj})$ 。矩阵乘向量，本质就是"用 u_j 把第 j 列加权再求和"，所以

$$\mathbf{x} = u_1 \mathbf{x}^{(1)} + u_2 \mathbf{x}^{(2)} + \dots + u_n \mathbf{x}^{(n)}.$$

记号 $\mathbf{x}^{(j)}$ 与"基" $\mathbf{x}^{(j)}$ 读"x 上标 j"（括号里的 j 不是次方，只是编号），是矩阵 Λ 的第 j 个列向量。这 n 个向量叫格的一组基 (basis)：意思是格里每一个点都能、而且只能用一种方式写成它们的整数系数组合 $\sum u_j \mathbf{x}^{(j)}$ 。在上面右图

里，那两条红线就是一组基；整张红网上的每颗钉子，都是"沿红线 1 走整数步 + 沿红线 2 走整数步"到达的。

"么模代换不改变格"是什么意思？ 同一张钉子板，可以选不同的两条基向量去描述它（就像同一面墙可以用不同的两块地砖去铺）。换基对应于对参数 $(u_1, \dots, u_n)$ 做一个变量替换。能用的替换必须满足两条：(1) 系数是整数（否则会跳到非格点）；(2) 这个替换可逆、且逆也是整系数（否则换过去的"新基"撑不出原来全部的点）。线性代数告诉我们，整系数且整系数可逆 $\iff$ 这个替换矩阵的行列式 $= \pm 1$ 。行列式为 1（或 ± 1 ）的整系数矩阵就叫**么模**（unimodular，"么"指 1）。换一组基，钉子板本身一颗钉子都没动，只是描述它的"坐标系"变了。

么模换基的二维例子 标准格 $\mathbb{Z}^2$ ，原基是 $(1, 0), (0, 1)$ 。换成 $(1, 0), (1, 1)$ ：替换矩阵 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ，行列式 $= 1$ ，是么模的。用新基

$u(1, 0) + v(1, 1) = (u + v, v)$ ，当 u, v 跑遍整数时， $(u + v, v)$ 也跑遍所有整点——还是同一张方格板。但若错用 $(2, 0), (0, 1)$ （行列式 $= 2$ ，非么模），就只能得到横坐标为偶数的点，丢了一半钉子，那是另一张更稀疏的格。

译文 我们用下式定义 Λ 的行列式 $d(\Lambda)$ ： $d(\Lambda) = |\det \lambda_{ij}|$ ；这是一个正数，不受变量的么模更换影响。该格的密度（在显然的意义下）为 $1/d(\Lambda)$ 。任意一组 n 个格点的坐标的行列式都是 $d(\Lambda)$ 的整数倍。为方便起见，我们通常假设 $d(\Lambda) = 1$ 。

这段定义"格的行列式"——格最重要的一个数，并给它几何意义。

记号 $d(\Lambda)$ 读"d of Lambda"，定义为系数矩阵行列式的绝对值 $|\det \lambda_{ij}|$ ，恒为正数（因为 $\det \neq 0$ 且取了绝对值）。由 0.4 的几何意义， $d(\Lambda)$ 正是基向量 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ 张成的那个平行体的体积——也就是钉子板里"一个网格单元（基本胞腔）的体积"。

逐句解释三个论断：

- 1 "不受么模更换影响"：换基相当于把 Λ 右乘一个么模矩阵 U ($\det U = \pm 1$)。由行列式乘法法则 $\det(\Lambda U) = \det \Lambda \cdot \det U = \det \Lambda \cdot (\pm 1)$ ，取绝对值后 $|\det(\Lambda U)| = |\det \Lambda|$ 。所以无论怎么换基， $d(\Lambda)$ 都不变——它是钉子板本身的属性，和你怎么描述它无关。这正对应"同一张网，单元胞腔的体积是定的"。
- 2 "密度为 $1/d(\Lambda)$ "：每个体积为 $d(\Lambda)$ 的胞腔里恰好"摊到一个格点"，所以单位体积里的格点数（密度）= $1/d(\Lambda)$ 。胞腔越大、网越稀、密度越低，符合直觉。这个"显然的意义"在引理 12.1 的证明里会被精确用到（大立方体内格点数 $\approx X^n/d(\Lambda)$ ）。
- 3 "任意 n 个格点坐标的行列式是 $d(\Lambda)$ 的整数倍"：任取格里 n 个点，每个都是基的整系数组合，第 k 个点 = $\sum_j m_{kj} \mathbf{x}^{(j)}$ ($m_{kj} \in \mathbb{Z}$)。把这 n 个点的坐标排成矩阵，等于整数矩阵 (m_{kj}) 乘基矩阵 Λ 。两边取行列式： $\det = \det(m_{kj}) \cdot \det \Lambda$ 。其中 $\det(m_{kj})$ 是整数矩阵的行列式，必为整数。所以这 n 个格点坐标的行列式 = (整数) $\times \det \Lambda$ ，取绝对值就是 $d(\Lambda)$ 的整数倍。这个事实在引理 12.2 里立刻要用。

最后"通常假设 $d(\Lambda) = 1$ "只是为了式子干净：把网格统一缩放，使一个胞腔体积恰为 1。这不损失一般性，因为任何格都能通过整体缩放化到 $d(\Lambda) = 1$ ，结论再缩放回去即可。

译文 空间的一个仿射变换是一个（齐次）线性变换，它从 $x_1, \dots, x_n$ 到 $y_1, \dots, y_n$ ，系数为实数且行列式 $\neq 0$ 。该变换把 x 空间中的格 Λ 映为 y 空间中的格 M ；如果这个变换的行列式为 1，则 $d(\Lambda) = d(M)$ 。

这段引入"仿射变换"——一种把一张钉子的板整体搬成另一张的操作。这里的"仿射/齐次线性变换"就是用一个 $n \times n$ 实矩阵 A 把每个点 $\mathbf{x}$ 换成 $\mathbf{y} = A\mathbf{x}$ (没有平移, 所以"齐次", 原点仍去原点)。要求 $\det A \neq 0$, 保证变换可逆、不把空间压扁。

记号 M (新字体 M) 读"格 M ", 表示把 Λ 经仿射变换后得到的新格 (在新坐标 y 空间里)。

为什么 $\det A = 1$ 时 $d(\Lambda) = d(M)$? 变换 A 把任何体积都放大 $|\det A|$ 倍 (这是 $\det$ 的几何意义)。格的胞腔体积是 $d(\Lambda)$, 变换后变成 $|\det A| \cdot d(\Lambda)$ 。若 $\det A = 1$ ("等积变换", 比如旋转、错切都属此类), 体积不变, 故 $d(M) = d(\Lambda)$ 。这条性质马上在引理 12.1 的证明里用到: "把椭球变成球"用的就是一个 $\det = 1$ 的仿射变换, 既不改变格的行列式、也不改变体积大小关系。

第 2 节 · 引理 12.1: 闵可夫斯基第一定理 (大体积椭球必含格点)

译文 · 引理 12.1 任何以原点 O 为中心、体积 $> 2^n$ 的椭球, 在每一个行列式为 1 的格中都包含一个异于 O 的点。

先把这句翻译成成人话。椭球就是球被各方向不等地拉伸后的形状 (二维是椭圆, 把圆压扁; 三维是橄榄球/铅球那种)。“以原点为中心”指它关于 O 对称。结论是: 只要这个椭球足够大 (体积超过 2^n 这个门槛), 那么不管钉子板 ($d = 1$ 的格) 怎么摆, 椭球里除了正中间的原点之外, 一定还罩住至少一颗钉子。

记号 2^n 与 O 2^n 读"2 的 n 次方", 是维数决定的临界体积 ($n = 2$ 时是 4, $n = 3$ 时是 8……)。 O 是原点 $(0, \dots, 0)$, 本身永远是格点 (取

$u_1 = \cdots = u_n = 0$)。引理要找的是"另一颗"非零格点。

为什么门槛恰是 2^n (动机) 这是闵可夫斯基定理的精髓。想象把椭球缩小一半 (线性尺寸各减半) 得到"半椭球", 它体积是原来的 $1/2^n$, 即 > 1 。一堆体积之和超过 1 的东西若全塞进"一个胞腔"的位置去比对, 必然有重叠——重叠就逼出两颗钉子离得很近, 从而逼出一颗非零近原点的钉子。门槛 2^n 正是为了让"半尺寸体积 $> 1 =$ 单位胞腔体积"。下面的证明就是把这个思想做实。

译文·证明 只需对球证明此结果即可, 因为一个椭球可以通过空间的一个行列式为 1 的仿射变换变为一个球。设 ρ 为球的半径。由于 $d(\Lambda) = 1$, 当 $X \rightarrow \infty$ 时, Λ 在大边长 X 的立方体内的点数渐近于 X^n 。如果我们在每一个这样的格点处放置一个半径为 $\frac{1}{2}\rho$ (因而体积 $V > 1$) 的球, 则它们的总体积渐近于 VX^n 。它们全都包含在边长为 $X + \rho$ 的立方体内。对于大的 X , 我们有 $VX^n > (X + \rho)^n$, 于是这些球必定重叠。因此存在 Λ 的两个相距小于 ρ 的不同点, 从而存在 Λ 的一个异于 O 的点, 它与 O 的距离小于 ρ 。

原文这段是高度浓缩的"鸽笼+体积"论证, 每一步都有省略。下面**一步一步**补全。

1 为何"只需对球证明"。椭球可由一个 $\det = 1$ 的仿射变换 A 拉回成球 (各轴方向反向缩放, 使三条半轴变得一样长; 适当选 A 可让 $\det A = 1$)。由第 1 节末, $\det A = 1$ 的变换既保持格的行列式 ($d = 1$ 仍是 $d = 1$), 又保持"含不含非零格点"这件事 (变换可逆, 格点对格点、椭球内点对球内点一一对应)。还保持体积 ($> 2^n$ 仍 $> 2^n$)。所以"球的情形成立"自动推出"椭球的情形成立"。这就把问题简化成了球。

2 设球半径为 ρ 。球体积 $= J_n \rho^n > 2^n$ (题设)。记半径减半的小球体积 $V = J_n (\frac{1}{2}\rho)^n = \frac{J_n \rho^n}{2^n} > \frac{2^n}{2^n} = 1$ 。这就是关键不等式 $V > 1$ 的来历——它直接来自"体积 $> 2^n$ "这个门槛。

3 大立方体里的格点数 $\approx X^n$ 。取一个边长为 X 的大立方体（中心在原点）。因为 $d(\Lambda) = 1$ ，格的密度是 1（每单位体积一个点，见第 1 节），所以立方体里格点数 $\approx$ （立方体体积） $= X^n$ ，当 X 越来越大时这个近似越来越准（“渐近于 X^n ”就是这个意思）。

4 在每个格点处放一个半径 $\frac{1}{2}\rho$ 的小球。立方体内约 X^n 个格点，每个配一个体积为 V 的小球，小球总体积 $\approx V \cdot X^n$ 。

5 这些小球都装在一个稍大的立方体里。每个小球球心在边长 X 的立方体内，半径 $\frac{1}{2}\rho$ ，所以球面最多探出 $\frac{1}{2}\rho$ ；两侧都探出，整体被边长 $X + \rho$ 的立方体兜住。这个大盒子体积 $= (X + \rho)^n$ 。

6 体积比较逼出重叠（鸽笼原理的体积版）。当 X 足够大时，比较“小球总体积”与“盒子体积”：

$$V X^n \text{ vs } (X + \rho)^n.$$

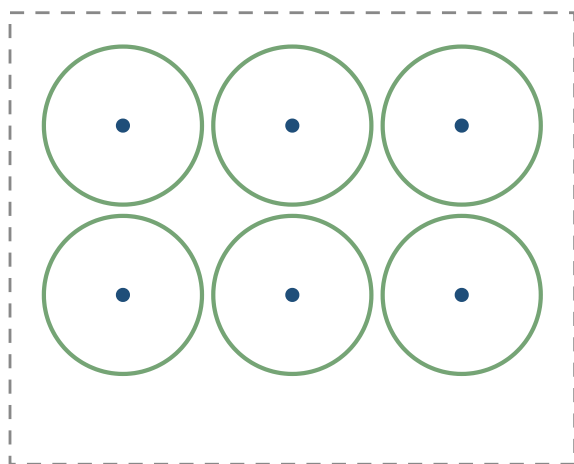
因为 $V > 1$ （第 2 步），而 $\frac{(X + \rho)^n}{X^n} = \left(1 + \frac{\rho}{X}\right)^n \rightarrow 1$ （当 $X \rightarrow \infty$ ，括号里趋于 1）。于是只要 X 大到使 $\left(1 + \frac{\rho}{X}\right)^n > V$ ，即 $(X + \rho)^n > V X^n$ ，即小球总体积 $>$ 装它们的盒子体积。一堆东西总体积超过容器体积，它们**必有重叠**（否则总体积不会超过容器）。

7 重叠 = 两个球心靠得近。两个半径都为 $\frac{1}{2}\rho$ 的小球若重叠，它们的球心（两个不同格点 $\mathbf{p}, \mathbf{q}$ ）距离 $< \frac{1}{2}\rho + \frac{1}{2}\rho = \rho$ 。所以存在两个不同格点相距小于 ρ 。

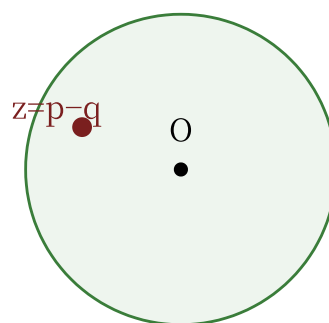
8 平移到原点，得非零近原点格点。格的关键性质：两格点之差仍是格点（因为 $\mathbf{p} = \sum a_j \mathbf{x}^{(j)}$ ， $\mathbf{q} = \sum b_j \mathbf{x}^{(j)}$ ，整系数相减仍整系数，故 $\mathbf{p} - \mathbf{q} = \sum (a_j - b_j) \mathbf{x}^{(j)}$ 是格点）。令 $\mathbf{z} = \mathbf{p} - \mathbf{q}$ ，它非零（因 $\mathbf{p} \neq \mathbf{q}$ ）。

), 且 $|\mathbf{z}| = |\mathbf{p} - \mathbf{q}| < \rho$ 。这正是"一个异于 O 、到 O 距离小于 ρ 的格点"——它落在半径 ρ 的球内。■

边长 X 的立方体 (含 $\approx X^n$ 个格点)



总体积 $V \cdot X^n >$ 盒子体积 $\rightarrow$ 必有两球相交



两近格点之差 = 半径 ρ 球内的非零

左：在每个格点放半径 $\frac{1}{2}\rho$ 的小球，体积一旦超过容器就被迫重叠。右：重叠 $\Rightarrow$ 存在相距 $< \rho$ 的两格点 $\Rightarrow$ 其差是球内非零格点。

译文·注 这一结果——把椭球换成任何关于 O 有中心对称性的凸体——就是闵可夫斯基第一基本定理。其证明本质上相同。

这条注交代历史与推广。"凸体" (convex body) 指一块鼓鼓的、没有凹陷的立体区域：里面任意两点连线整段都在区域内（圆、椭球、立方体、正多面体都是凸的；月牙形、五角星不是）。"关于 O 中心对称"指 $\mathbf{x}$ 在里面 $\Rightarrow -\mathbf{x}$ 也在里面。闵可夫斯基 1896 年的**第一基本定理**说：体积 $> 2^n$ 的中心对称凸体必含非零格点——这是数的几何的奠基定理。本章为省事只对椭球证（够后面用），但 Davenport 提醒你：换成一般凸体，上面那套"半尺寸小球体积 > 1 必重叠"的证明几乎一字不改照样成立（凸性保证"两点之差落在原凸体内"这一步）。

第 3 节 · 相继极小：用 n 个数刻画一张格

译文 一个格 Λ 的相继极小定义如下。设 R_1 为 Λ 中任一异于 O 的点到 O 的最小距离，并设 $\mathbf{x}^{(1)}$ 为 Λ 中一个处于该距离的点。用 $|\mathbf{x}|$ 表示点 $\mathbf{x}$ 到 O 的距离，则有 $|\mathbf{x}^{(1)}| = R_1$ 。设 R_2 为 Λ 中任一不在直线 $\langle O, \mathbf{x}^{(1)} \rangle$ 上的点到 O 的最小距离，并设 $\mathbf{x}^{(2)}$ 为满足 $|\mathbf{x}^{(2)}| = R_2$ 的这样一个点。设 R_3 为 Λ 中任一不在平面 $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)} \rangle$ 上的点到 O 的最小距离，依此类推。我们得到数 $R_1, \dots, R_n$ 与线性无关的点 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ ，使得

$$0 < R_1 \leq R_2 \leq \dots \leq R_n, \quad |\mathbf{x}^{(\nu)}| = R_\nu.$$

这是全章的核心定义，务必弄懂。动机：一张格可能"各方向疏密悬殊"——某个方向钉子排得很密（最近的非零钉子很近），换个方向却很疏。我们想用一串数把这种"各方向有多密"量化出来。做法是"贪心地一层层往外找最近的新方向"。

记号 R_ν 与 $\langle \dots \rangle$ ν 是希腊字母，读"纽"，当编号用 ($\nu = 1, 2, \dots, n$)。 R_ν 读"R 下标 纽"，是第 ν 个相继极小。记号 $\langle O, \mathbf{x}^{(1)} \rangle$ 表示"由 O 与 $\mathbf{x}^{(1)}$ 张成的直线"； $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)} \rangle$ 表示由这三点张成的平面；一般地 $\langle O, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(k)} \rangle$ 是一个 k 维"子空间"。

定义过程一步步是：

1 R_1 = 全部非零格点里离原点最近的那个距离；取一个达到它的点叫 $\mathbf{x}^{(1)}$ ，于是 $|\mathbf{x}^{(1)}| = R_1$ 。（这刻画了"最密方向有多密"。）

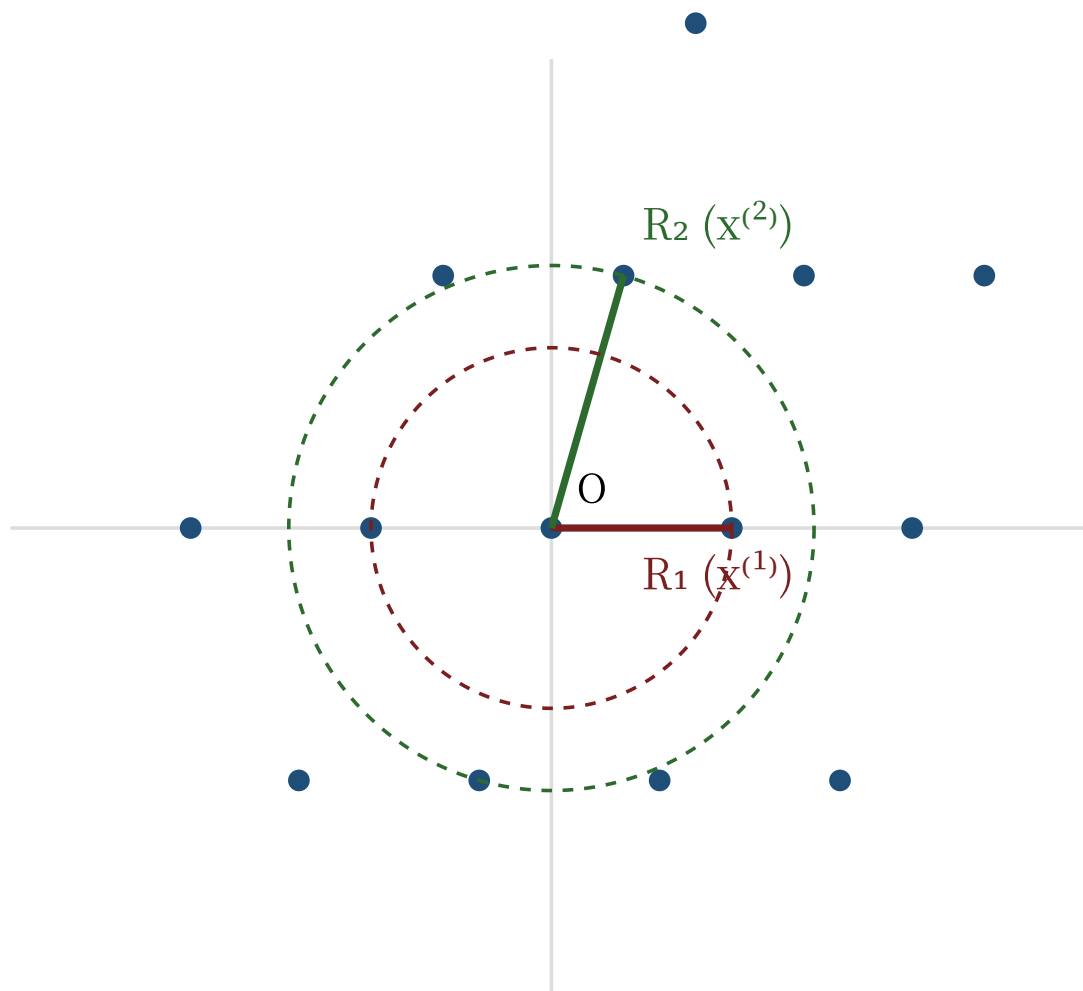
2 R_2 = 在"不躺在 $\mathbf{x}^{(1)}$ 那条直线上"的格点里，离原点最近的距离；取达到它的点叫 $\mathbf{x}^{(2)}$ 。为什么要排除那条直线？因为直线上的点（如 $2\mathbf{x}^{(1)}, 3\mathbf{x}^{(1)}$ ）只是 $\mathbf{x}^{(1)}$ 方向的重复，提供不了"新方向"。我们要的是一个真正新的、线性无关的方向。

3 R_3 = 在"不躺在 $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$ 张成的那张平面上"的格点里，离原点最近的距离；取点 $\mathbf{x}^{(3)}$ 。如此每次都跳出上一层张成的子空间，找一个最近的新方

向。

4 做满 n 步，得到 n 个数 $R_1, \dots, R_n$ 和 n 个点 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ 。由于每步都跳出前面所有方向张成的子空间，这 n 个点必然**线性无关**。

5 为何 $R_1 \leq R_2 \leq \dots \leq R_n$? 因为找 $R_{\nu+1}$ 时的候选点集 ("不在前 ν 个方向张成的子空间里"的格点) 是找 R_ν 时候选集的子集 (限制更严, 排除得更多)。在更小的范围里求最小, 结果只会更大或相等, 所以 $R_{\nu+1} \geq R_\nu$ 。又因为非零格点离原点总有正距离 (格点是离散的, 最近的非零点不会贴在原点), 故 $R_1 > 0$ 。



二维例子: R_1 是最近非零格点的距离 (红, 沿横向); R_2 是"不在那条横线上"的最近格点距离 (绿)。两圈半径就是 $R_1 \leq R_2$ 。

译文 点 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ 可能不止一种选法，但容易看出这不影响数 $R_1, \dots, R_n$ 的唯一性。这些数就是 Λ 的相继极小，而 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ 是 Λ 的一组极小点。这些点不一定构成一组基，尽管在 $n = 2$ 时恰好如此。

这段澄清两个细节。第一，达到最近距离的点可能有好几个（例如对称的格里 $\mathbf{x}^{(1)}$ 和 $-\mathbf{x}^{(1)}$ 距离一样），所以“极小点” $\mathbf{x}^{(\nu)}$ 选法不唯一；但距离值 R_ν 是唯一的——因为 R_ν 被定义成“某个候选集里的最小距离”，最小值这个数不会因为有多多个点达到它而改变。原文说“容易看出”，补全这一句理由即如上。

“极小点” vs “基” 的区别（重要） 极小点 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ 一定线性无关，但不一定能用它们的整系数组合凑出格里每个点（也就是不一定是基）。 $n = 2$ 时恰好它们也是基；但维数 ≥ 5 时可能出现“极小点撑出的整系数格比原格稀疏”的反例。这正是下一节引理 12.3 要解决的麻烦：从极小点出发，调整出一组真正的基 $\mathbf{X}^{(\nu)}$ ，同时让它的长度仍 $\asymp R_\nu$ 。

第 4 节 · 引理 12.2：相继极小之积被夹住（闵可夫斯基第二定理）

译文 · 引理 12.2 若 $d(\Lambda) = 1$ ，则有

$$1 \leq R_1 R_2 \cdots R_n \leq 2^n / J_n, \quad (12.1)$$

其中 J_n 表示 n 维中半径为 1 的球的体积。

这条引理说： n 个相继极小的乘积 $R_1 R_2 \cdots R_n$ ，被牢牢夹在 1 与 $2^n / J_n$ 之间——两端都是只依赖 n 的常数。换言之，对 $d = 1$ 的格， $R_1 \cdots R_n \asymp 1$ 。意义：某个方向特别密（ R_ν 很小）必然以另一个方向特别疏（别的 R 很大）为代

价，疏密"总账守恒"。这与第 1 节"胞腔体积固定为 1"是一回事的精细化。下面分别证下界和上界。

译文·证明（下界） 我们可以绕 O 旋转 n 维空间，直到

$$\mathbf{x}^{(1)} = (x_1^{(1)}, 0, \dots, 0), \mathbf{x}^{(2)} = (x_1^{(2)}, x_2^{(2)}, 0, \dots, 0), \dots, \mathbf{x}^{(n)} = (x_1^{(n)}, \dots, x_n^{(n)}, 0, \dots, 0).$$

由于这 n 个点的行列式是 $d(\Lambda) = 1$ 的整数倍，而它们又线性无关，故

$$|x_1^{(1)} x_2^{(2)} \cdots x_n^{(n)}| \geq 1. \text{ 由于 } R_\nu = |\mathbf{x}^{(\nu)}| \geq |x_\nu^{(\nu)}|, \text{ 我们得到}$$

$$R_1 R_2 \cdots R_n \geq 1.$$

1 旋转坐标系做"三角化"。旋转不改变任何长度和距离（刚体转动），所以不改变 R_ν 、不改变 $d(\Lambda)$ 、不改变是否格点。我们转动坐标轴，使第一个极小点 $\mathbf{x}^{(1)}$ 正好躺在第 1 根坐标轴上（于是它只有第 1 个坐标非零）；再使 $\mathbf{x}^{(2)}$ 落在前两根轴张成的平面里（第 3 个起的坐标为 0）；依此类推。结果坐标矩阵成"下三角"形状（对角线下方可非零、上方全为 0），如译文所列。**为什么能这样转？** 因为 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 张成的是个 ν 维子空间，总能把坐标系转得让这个子空间正好是"前 ν 根轴"张成的那个，这是线性代数里的标准事实（Gram-Schmidt 正交化的几何版）。

2 三角矩阵的行列式 = 对角线之积。对下三角矩阵， $\det =$ 对角元乘积 $= x_1^{(1)} x_2^{(2)} \cdots x_n^{(n)}$ （上三角部分全 0，展开只剩这一项）。

3 这个行列式的绝对值 ≥ 1 。由第 1 节第 3 条：任意 n 个格点坐标的行列式是 $d(\Lambda)$ 的整数倍 $= (\text{整数}) \times 1 = \text{整数}$ 。又这 n 个极小点线性无关，行列式 $\neq 0$ ，所以是个非零整数，绝对值 ≥ 1 。于是 $|x_1^{(1)} x_2^{(2)} \cdots x_n^{(n)}| \geq 1$ 。

4 每个对角元不超过对应点的长度。由 0.2 的小事实 $|x_\nu^{(\nu)}| \leq |\mathbf{x}^{(\nu)}| = R_\nu$ （一个坐标的绝对值不超过整个向量的模长）。

5 连乘得下界。把第 4 步对所有 ν 相乘：

$|x_1^{(1)} x_2^{(2)} \cdots x_n^{(n)}| = \prod_{\nu} |x_{\nu}^{(\nu)}| \leq \prod_{\nu} R_{\nu} = R_1 \cdots R_n$. 结合第 3 步 $1 \leq |x_1^{(1)} \cdots x_n^{(n)}|$, 得 $1 \leq R_1 R_2 \cdots R_n$. 下界证毕。

译文·证明（上界） 为得到 $R_1 R_2 \cdots R_n$ 的上界，我们考虑椭球

$$\frac{x_1^2}{R_1^2} + \cdots + \frac{x_n^2}{R_n^2} < 1.$$

它不包含 Λ 的任何异于 O 的点。事实上，设 Λ 的某点 $\mathbf{x}$ 线性依赖于 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 但不依赖于 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu-1)}$ ，其中 $1 \leq \nu \leq n$ 。则按 R_{ν} 的定义有 $|\mathbf{x}| \geq R_{\nu}$ 。又 $x_{\nu+1} = 0, \dots, x_n = 0$ ；于是

$$\frac{x_1^2}{R_1^2} + \cdots + \frac{x_n^2}{R_n^2} \geq \frac{x_1^2 + \cdots + x_{\nu}^2}{R_{\nu}^2} \geq 1.$$

因此 $\mathbf{x}$ 不在该椭球内。由引理 12.1 可知该椭球的体积 $\leq 2^n$ 。该体积为 $(R_1 R_2 \cdots R_n) J_n$ ，于是所需不等式成立。

这一半要用引理 12.1 反着用："若椭球太大就会含非零格点；现在我造一个恰好不含非零格点的椭球，那它就不能太大，由此把 $R_1 \cdots R_n$ 卡在上面。"逐步补全：

1 构造椭球。取椭球 $E: \frac{x_1^2}{R_1^2} + \cdots + \frac{x_n^2}{R_n^2} < 1$ 。它的 n 条半轴长正是

$R_1, \dots, R_n$ （沿第 k 轴，令其余坐标为 0，边界处 $x_k = R_k$ ）。选这个椭球的动机：把"各方向相继极小 R_{ν} "直接做成各方向的半轴，这样它的体积里就自然含有 $R_1 \cdots R_n$ 。

2 断言： E 内没有非零格点。反证地考察任意非零格点 $\mathbf{x}$ 。设它"恰好用到第 ν 个方向"——即 $\mathbf{x}$ 能写成 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 的组合，但写不成

$\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu-1)}$ 的组合（每个非零格点都有这样一个确定的"最高层级 ν "）。

3 它的长度 $\geq R_\nu$ 。因为 $\mathbf{x}$ 不在 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu-1)}$ 张成的子空间里（第 2 步），按 R_ν 的定义（"不在前 $\nu - 1$ 个方向子空间里的最近距离"），有 $|\mathbf{x}| \geq R_\nu$ 。

4 它的高位坐标全为 0。在第 1 步那套三角化坐标里， $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 的第 $\nu + 1$ 个及以后坐标都是 0； $\mathbf{x}$ 是它们的组合，所以 $\mathbf{x}$ 也满足 $x_{\nu+1} = \dots = x_n = 0$ 。

5 代入椭球表达式，证明 ≥ 1 。

$$\frac{x_1^2}{R_1^2} + \dots + \frac{x_n^2}{R_n^2} \stackrel{(a)}{=} \frac{x_1^2}{R_1^2} + \dots + \frac{x_\nu^2}{R_\nu^2} \stackrel{(b)}{\geq} \frac{x_1^2 + \dots + x_\nu^2}{R_\nu^2} \stackrel{(c)}{=} \frac{|\mathbf{x}|^2}{R_\nu^2} \stackrel{(d)}{\geq} 1$$

其中 (a) 用第 4 步把 ν 之后的项扔掉（它们是 0）；(b) 因为

$R_1 \leq R_2 \leq \dots \leq R_\nu$ ，所以分母 $R_1, \dots, R_\nu$ 都 $\leq R_\nu$ ，把前面各项的分母统一放大到 R_ν^2 ，每项只会变小，整体 $\geq$ ；(c) 因为

$x_{\nu+1}, \dots, x_n = 0$ ， $x_1^2 + \dots + x_\nu^2 = x_1^2 + \dots + x_n^2 = |\mathbf{x}|^2$ ；(d) 用第 3 步 $|\mathbf{x}| \geq R_\nu$ ，故 $|\mathbf{x}|^2/R_\nu^2 \geq 1$ 。

6 结论：该值 ≥ 1 ，所以 $\mathbf{x}$ 不满足 " < 1 "，即 $\mathbf{x} \notin E$ 。因此 E 里除原点外没有格点。

7 用引理 12.1 反推体积上界。引理 12.1 说"体积 $> 2^n$ 的中心椭球必含非零格点"。 E 恰恰不含非零格点，所以它的体积不能 $> 2^n$ ，即 $\text{vol}(E) \leq 2^n$ 。

8 算出 E 的体积并收尾。椭球 E 由单位球各轴拉伸 $R_1, \dots, R_n$ 倍得到，
 体积 = 单位球体积 $\times$ 各轴拉伸倍数之积 = $J_n \cdot R_1 R_2 \cdots R_n$ 。代入上一步： $(R_1 R_2 \cdots R_n) J_n \leq 2^n$ ，即

$$R_1 R_2 \cdots R_n \leq \frac{2^n}{J_n}.$$

上界证毕。合并下界，(12.1) 全部成立。■

译文·注 引理 12.2 以及关于相继极小的定义，同样可以推广到以 O 为中心的任意凸体。在这种更一般的形式下，引理 12.2 就是闵可夫斯基第二基本定理；不过它的证明要困难得多。注意引理 12.2 蕴含 $J_n R_1^n \leq 2^n$ ，这正是引理 12.1 的结果。

历史定位：这条注告诉你引理 12.2 的"豪华版"叫闵可夫斯基第二基本定理（把球/椭球换成一般中心对称凸体，相继极小也按那个凸体来定义）。它比第一定理深得多，闵可夫斯基本人的完整证明相当费力。Davenport 这里用椭球的版本是"够用就好"的取舍。

"蕴含引理 12.1"的验证：由 $R_1 \leq R_2 \leq \cdots \leq R_n$ ，把乘积里每个因子都缩小到最小的 R_1 ： $R_1^n = R_1 \cdot R_1 \cdots R_1 \leq R_1 R_2 \cdots R_n \leq 2^n / J_n$ ，即 $J_n R_1^n \leq 2^n$ 。而 $J_n R_1^n$ 正是半径 R_1 的球体积。它 $\leq 2^n$ 等价于说："若一个中心球体积 $> 2^n$ ，就不可能 $R_1 \geq$ 该球半径，也就是 $R_1 <$ 半径，即存在距离 $<$ 半径的非零格点"——这正是引理 12.1。可见第二定理确实把第一定理当特例包含了。

第 5 节·同阶记号 $\asymp$ 与引理 12.3：把极小点修成一组好基

译文 我们暂时引入记号 $A \asymp B$ 来表示同时有 $A \ll B$ 与 $A \gg B$ ；换言之，表明 A/B 在上下两端都被仅依赖于 n 的数所界住。

这就是 0.6 节已经预讲过的 $\asymp$ 。Davenport 在这里正式登场使用它： $A \asymp B$ 读“A 与 B 同阶”，意思是存在只依赖 n 的常数 $c, C > 0$ 使 $cB \leq A \leq CB$ ，即 A, B 互相被对方的常数倍夹住。后面引理 12.3、12.4、12.5、12.6 全靠这个记号简洁陈述。“暂时”指它只在本章好用。

译文·引理 12.3 经过空间的适当旋转后，任何行列式为 1 的格都有一组形如下式的基 $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(n)}$ ：

$$\mathbf{X}^{(1)} = (X_1^{(1)}, 0, \dots, 0), \quad \mathbf{X}^{(2)} = (X_1^{(2)}, X_2^{(2)}, 0, \dots, 0), \quad \dots$$

其中 $|\mathbf{X}^{(\nu)}| \asymp R_\nu$ 且 $|X_\nu^{(\nu)}| \asymp R_\nu$ ，(12.2) 对 $\nu = 1, \dots, n$ 成立。

这条引理解决第 3 节末提出的麻烦：极小点不一定是基。引理 12.3 说：可以找到一组真正的基 $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(n)}$ （整系数能凑出格里每个点），并且这组基有两条好性质：(1) 坐标呈下三角（ $\mathbf{X}^{(\nu)}$ 只有前 ν 个坐标非零）；(2) 每个基向量的长度、以及它的“对角坐标” $X_\nu^{(\nu)}$ ，都与相继极小 R_ν 同阶。这样一来，这组基既好用（是基）、又“诚实地反映各方向的疏密”（长度 $\asymp R_\nu$ ）。

记号 $\mathbf{X}^{(\nu)}$ 、 $X_\nu^{(\nu)}$ 大写黑体 $\mathbf{X}^{(\nu)}$ 是修出来的第 ν 个基向量（区别于小写极小点 $\mathbf{x}^{(\nu)}$ ）。 $X_\nu^{(\nu)}$ 是它的第 ν 个坐标（“对角元”），即在下三角形里位于对角线上的那个分量。(12.2) 里 $|\mathbf{X}^{(\nu)}| \asymp R_\nu$ 说“长度同阶”， $|X_\nu^{(\nu)}| \asymp R_\nu$ 说“对角坐标也同阶”。

译文·证明（构造基，上界部分）我们由引理 12.2 证明中的极小点 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ 出发，通过一个调整过程来得到这组基点。取 $\mathbf{X}^{(1)}$ 为 $\mathbf{x}^{(1)}$ 。取 $\mathbf{X}^{(2)}$ 为 Λ 在平面 $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)} \rangle$ 内的一个点，它与 $\mathbf{X}^{(1)}$ 一起整数地生成 Λ 在该平面内的所有点；这样的点的存在在几何上是直观的。它在可加上 $\mathbf{x}^{(1)}$ 的任意倍数这一意义上是任意的。由于 $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$ 有理地（虽然也许不是整数地）生成 Λ 在平面 $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)} \rangle$ 内的所有点，故有

$$N\mathbf{X}^{(2)} = u_1\mathbf{x}^{(1)} + u_2\mathbf{x}^{(2)}$$

对某些整数 $N > 0, u_1, u_2$ 成立。由于 $\mathbf{x}^{(2)}$ 是 $\mathbf{X}^{(2)}$ 与 $\mathbf{X}^{(1)} = \mathbf{x}^{(1)}$ 的整系数线性组合，故必有 $u_2 = 1$ 。通过向 $\mathbf{X}^{(2)}$ 加上 $\mathbf{x}^{(1)}$ 的适当整数倍，我们可以设 $|u_1| \leq \frac{1}{2}N$ 。于是

$$|\mathbf{X}^{(2)}| \leq \frac{|u_1|}{N} |\mathbf{x}^{(1)}| + \frac{1}{N} |\mathbf{x}^{(2)}| \leq \frac{1}{2}R_1 + R_2 \leq \frac{3}{2}R_2.$$

这是个"逐层修基"的归纳构造。先把 $\mathbf{X}^{(2)}$ 这一层讲透，更高层完全类比。

1 第1层照搬。 令 $\mathbf{X}^{(1)} = \mathbf{x}^{(1)}$ 。一维里极小点自己就是基，没问题，且 $|\mathbf{X}^{(1)}| = R_1$ 。

2 第2层要修。 问题： $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$ 也许不能整系数生成它们所在平面里全部格点（这正是极小点不一定是基的毛病）。但几何上一定存在一个点 $\mathbf{X}^{(2)}$ ，使得 $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}$ 整系数恰好生成该平面内全部格点（"平面内的格是二维格，二维格一定有基"，这是直观且可证的）。 $\mathbf{X}^{(2)}$ 可以加上 $\mathbf{x}^{(1)}$ 的任意整数倍而仍是合法选择（沿已有方向平移不影响"生成"）——这个自由度待会儿用来压短它。

3 把 $\mathbf{X}^{(2)}$ 用极小点表示。 $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$ 至少能有理系数生成该平面所有格点（因为它们是平面里两个线性无关向量，张成整个平面，任何点都是它们的实组合；而格点用它们表示时系数是有理数）。所以 $\mathbf{X}^{(2)}$ 乘上某个正整数 N 后能变成整系数： $N\mathbf{X}^{(2)} = u_1\mathbf{x}^{(1)} + u_2\mathbf{x}^{(2)}$ ，
 $N, u_1, u_2 \in \mathbb{Z}, N > 0$ （通分清分母即得 N ）。

4 推出 $u_2 = 1$ 。 反过来， $\mathbf{x}^{(2)}$ 在平面格里，故能被基 $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}$ 整系数表示： $\mathbf{x}^{(2)} = a\mathbf{X}^{(1)} + b\mathbf{X}^{(2)}$ 。把第3步的式子和这个式子联立（都在以 $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$ 为坐标的平面里比较 $\mathbf{x}^{(2)}$ 的系数），可得
 $b \cdot u_2 = N \cdot (\text{某整数关系})$ 最终强制 $u_2 = 1$ 。直观说： $\mathbf{X}^{(2)}$ 与 $\mathbf{X}^{(1)}$ 整系数生成 $\mathbf{x}^{(2)}$ ，意味着 $\mathbf{x}^{(2)}$ 在 $\mathbf{X}^{(2)}$ 方向上的"格距"恰是一格，对应

$u_2 = 1$ 。(这一步原文只丢结论，这里点明它来自" $\mathbf{x}^{(2)}$ 是 $\mathbf{X}$ 的整组合"。)
于是 $N\mathbf{X}^{(2)} = u_1\mathbf{x}^{(1)} + \mathbf{x}^{(2)}$ 。

- 5 用自由度把 u_1 压进半格。第 2 步说 $\mathbf{X}^{(2)}$ 可加 $\mathbf{x}^{(1)}$ 的整数倍；加一次 $\mathbf{x}^{(1)}$ 会使 u_1 改变 N （因为两边乘了 N ）。于是总能调到 $|u_1| \leq \frac{1}{2}N$ （把 u_1 对 N 取"最接近的余数"，余数绝对值不超过 $N/2$ ）。

- 6 估长度。由第 4、5 步， $\mathbf{X}^{(2)} = \frac{u_1}{N}\mathbf{x}^{(1)} + \frac{1}{N}\mathbf{x}^{(2)}$ 。用三角不等式（ $|\mathbf{a} + \mathbf{b}| \leq |\mathbf{a}| + |\mathbf{b}|$ ）：

$$|\mathbf{X}^{(2)}| \leq \frac{|u_1|}{N}|\mathbf{x}^{(1)}| + \frac{1}{N}|\mathbf{x}^{(2)}| \leq \frac{N/2}{N}R_1 + \frac{1}{N}R_2 \leq \frac{1}{2}R_1 + R_2.$$

（用了 $|u_1|/N \leq \frac{1}{2}$ 、 $1/N \leq 1$ 、 $|\mathbf{x}^{(1)}| = R_1$ 、 $|\mathbf{x}^{(2)}| = R_2$ 。）再因 $R_1 \leq R_2$ ，得 $\frac{1}{2}R_1 + R_2 \leq \frac{1}{2}R_2 + R_2 = \frac{3}{2}R_2$ 。所以 $|\mathbf{X}^{(2)}| \leq \frac{3}{2}R_2$ 。

译文·证明（第 3 层及一般层） 接下来取 $\mathbf{X}^{(3)}$ 为 Λ 在空间 $\langle O, \mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \mathbf{x}^{(3)} \rangle$ 内的一个点……我们有 $N\mathbf{X}^{(3)} = u_1\mathbf{x}^{(1)} + u_2\mathbf{x}^{(2)} + u_3\mathbf{x}^{(3)}$ ……这一次我们不能断言 $u_3 = 1$ ，但可以断言 u_3 整除 N ，因为 $\mathbf{x}^{(3)} = v_1\mathbf{X}^{(1)} + v_2\mathbf{X}^{(2)} + v_3\mathbf{X}^{(3)}$ ，且我们必有 $N = u_3v_3$ 。与前面一样，我们可以确保 $|u_1| \leq \frac{1}{2}N$ 且 $|u_2| \leq \frac{1}{2}N$ 。于是

$$|\mathbf{X}^{(3)}| \leq \frac{1}{2}|\mathbf{x}^{(1)}| + \frac{1}{2}|\mathbf{x}^{(2)}| + |\mathbf{x}^{(3)}| \leq \frac{1}{2}R_1 + \frac{1}{2}R_2 + R_3 \leq 2R_3.$$

这样继续下去，我们得到 Λ 的一组整数基，满足 $|\mathbf{X}^{(\nu)}| \leq \frac{\nu+1}{2}R_\nu \ll R_\nu$ ， $(1 \leq \nu \leq n)$ 。

- 1 第 3 层同样修。取 $\mathbf{X}^{(3)}$ 使 $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}, \mathbf{X}^{(3)}$ 整系数生成三维子空间里全部格点。同理 $N\mathbf{X}^{(3)} = u_1\mathbf{x}^{(1)} + u_2\mathbf{x}^{(2)} + u_3\mathbf{x}^{(3)}$ 。

2 这次不一定 $u_3 = 1$, 但 $u_3 \mid N$ (u_3 整除 N)。理由: $\mathbf{x}^{(3)}$ 能被新基整系数表示 $\mathbf{x}^{(3)} = v_1 \mathbf{X}^{(1)} + v_2 \mathbf{X}^{(2)} + v_3 \mathbf{X}^{(3)}$ 。比较 $\mathbf{X}^{(3)}$ 方向 (即第 3 层的"新方向") 的系数: 第一个式子给该方向系数为 u_3/N (把式子除以 N), 第二个式子给整数 v_3 。但 $\mathbf{x}^{(3)}$ 是同一个点, 沿 $\mathbf{X}^{(3)}$ 方向的系数唯一, 所以 $u_3/N = v_3$, 即 $N = u_3 v_3$, v_3 是整数, 故 u_3 整除 N 。含义: 虽然 u_3 不必是 1, 但 u_3 是 N 的因子, 这一步对长度上界其实不直接需要数值, 只需后面 $|u_1|, |u_2| \leq \frac{1}{2}N$ 即可; 写出 $u_3 \mid N$ 是为了确认 $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}, \mathbf{X}^{(3)}$ 确实构成子空间格的基 (生成性正确)。

3 同样把 u_1, u_2 压到 $\leq \frac{1}{2}N$ 。利用 $\mathbf{X}^{(3)}$ 可加 $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}$ (从而可加 $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$) 整数倍的自由度, 把 u_1, u_2 都调进半格。注意第 3 个系数是 u_3/N , 而 $N = u_3 v_3$ 给 $u_3/N = 1/v_3$, 其绝对值 ≤ 1 。

4 估长度。 $\mathbf{X}^{(3)} = \frac{u_1}{N} \mathbf{x}^{(1)} + \frac{u_2}{N} \mathbf{x}^{(2)} + \frac{u_3}{N} \mathbf{x}^{(3)}$, 三角不等式给

$$|\mathbf{X}^{(3)}| \leq \frac{1}{2}R_1 + \frac{1}{2}R_2 + 1 \cdot R_3 \leq \frac{1}{2}R_3 + \frac{1}{2}R_3 + R_3 = 2R_3$$

(用 $R_1, R_2 \leq R_3$ 把前两项放大)。

5 一般第 ν 层。完全类比, 前 $\nu - 1$ 个系数各 $\leq \frac{1}{2}$ 、第 ν 个 ≤ 1 , 得

$$|\mathbf{X}^{(\nu)}| \leq \underbrace{\frac{1}{2}R_1 + \cdots + \frac{1}{2}R_{\nu-1}}_{\nu-1 \text{ 项}} + R_\nu \leq \frac{\nu-1}{2}R_\nu + R_\nu = \frac{\nu+1}{2}R_\nu.$$

(每个 $R_j \leq R_\nu$ 。) 由于 $\frac{\nu+1}{2} \leq \frac{n+1}{2}$ 是只依赖 n 的常数, 故 $|\mathbf{X}^{(\nu)}| \ll R_\nu$ 。这就给出 (12.2) 中 $|\mathbf{X}^{(\nu)}|$ 的上界。

译文·证明 (下界 + 对角坐标) 由于 $\mathbf{X}^{(\nu)}$ 是 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 的线性组合, 其最后 $n - \nu$ 个坐标为 0。我们有 $|X_\nu^{(\nu)}| \leq |\mathbf{X}^{(\nu)}| \ll R_\nu$, 于是 (12.2) 中的两个上界都成立。下界则由行列式的比较以及 (12.1) 得出。由于 $d(\Lambda) = 1$, 我们

有 $|X_1^{(1)} \cdots X_n^{(n)}| = 1$, 从而 $R_1 \cdots R_{\nu-1} |X_\nu^{(\nu)}| R_{\nu+1} \cdots R_n \gg 1$, 而 (12.1) 的右半部分给出 $|X_\nu^{(\nu)}| \gg R_\nu$. 由此更有 $|\mathbf{X}^{(\nu)}| \gg R_\nu$.

1 对角坐标的上界。 $\mathbf{X}^{(\nu)}$ 是 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 的组合, 而这些极小点在三角化坐标里第 $\nu + 1$ 起的坐标都为 0, 故 $\mathbf{X}^{(\nu)}$ 也满足"最后 $n - \nu$ 个坐标为 0", 即它确实是下三角形状。再由 0.2 的小事实, 对角坐标 $|X_\nu^{(\nu)}| \leq |\mathbf{X}^{(\nu)}| \ll R_\nu$. 两个上界 (向量长度、对角坐标) 齐了。

2 基矩阵行列式 = 1。因 $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(n)}$ 是 $d(\Lambda) = 1$ 的格的基, 其坐标矩阵的行列式绝对值 = $d(\Lambda) = 1$ 。又它是下三角矩阵, 行列式 = 对角元之积, 故 $|X_1^{(1)} X_2^{(2)} \cdots X_n^{(n)}| = 1$ 。

3 把这个 1 拆开, 孤立出 $X_\nu^{(\nu)}$ 。对每个 $j \neq \nu$, 已证上界 $|X_j^{(j)}| \leq |\mathbf{X}^{(j)}| \ll R_j$, 即 $|X_j^{(j)}| \leq CR_j$ 。把第 2 步的等式两边除以这些:

$$1 = \prod_j |X_j^{(j)}| = |X_\nu^{(\nu)}| \prod_{j \neq \nu} |X_j^{(j)}| \leq |X_\nu^{(\nu)}| \cdot C' \prod_{j \neq \nu} R_j,$$

所以 $|X_\nu^{(\nu)}| \cdot R_1 \cdots R_{\nu-1} R_{\nu+1} \cdots R_n \gg 1$, 即 $|X_\nu^{(\nu)}| \gg \frac{1}{\prod_{j \neq \nu} R_j}$ 。

4 用 (12.1) 右半把分母换成 R_ν 。(12.1) 说 $R_1 R_2 \cdots R_n \leq 2^n / J_n \ll 1$, 所以 $\prod_{j \neq \nu} R_j = \frac{R_1 \cdots R_n}{R_\nu} \ll \frac{1}{R_\nu}$ 。代入上一步:
 $|X_\nu^{(\nu)}| \gg \frac{1}{\prod_{j \neq \nu} R_j} \gg R_\nu$ 。对角坐标的下界 $|X_\nu^{(\nu)}| \gg R_\nu$ 得证。

5 向量长度的下界。由 $|\mathbf{X}^{(\nu)}| \geq |X_\nu^{(\nu)}| \gg R_\nu$ (向量长度不小于它任一坐标的绝对值), 自动得到 $|\mathbf{X}^{(\nu)}| \gg R_\nu$ 。或者更直接: $\mathbf{X}^{(\nu)}$ 不在

$\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu-1)}$ 的子空间里, 由 R_ν 定义 $|\mathbf{X}^{(\nu)}| \geq R_\nu$ 。两条上界两条下界全部到手, (12.2) 完全成立。■

译文·注 如有需要, 引理 12.3 中找到的这组整数基还可以进一步"规范化"。通过向 $\mathbf{X}^{(\nu)}$ 加上 $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(\nu-1)}$ 的适当倍数, 我们可以确保 $|X_\mu^{(\nu)}| \leq \frac{1}{2}|X_\mu^{(\mu)}|$ 对所有满足 $\mu < \nu$ 的 μ, ν 成立。

这条注说基还能"擦干净"。下三角矩阵对角线下方那些非对角元 $X_\mu^{(\nu)}$ ($\mu < \nu$), 可以通过给 $\mathbf{X}^{(\nu)}$ 减去低层基向量的整数倍而压到很小——不超过对应对角元 $|X_\mu^{(\mu)}|$ 的一半。这就像解线性方程组里的"回代消元": 每加一个 $\mathbf{X}^{(\mu)}$ 的整数倍, $X_\mu^{(\nu)}$ 就改变 $X_\mu^{(\mu)}$ 的整数倍, 于是能把它对 $X_\mu^{(\mu)}$ 取最接近余数压进半格。这步在本章后文不是必需, 故称"如有需要", 但它让基更标准、更便于显式计算。

第 6 节·引理 12.4: 球里到底有多少格点

译文·引理 12.4 设 $d(\Lambda) = 1$ 。设 $N(R)$ 表示 Λ 中满足 $|\mathbf{x}| \leq R$ 的 $\mathbf{x}$ (含原点) 的个数。则当 $R < R_1$ 时 $N(R) = 1$, 而若 $R_\nu \leq R < R_{\nu+1}$ 则
$$N(R) \asymp \frac{R^\nu}{R_1 R_2 \cdots R_\nu}.$$
 (注: 若 $\nu = n$, 则条件中的 R_{n+1} 应略去。)

这是本章的"主力公式", 回答本章开头那个问题: 半径 R 的球里有几个格点。答案完全由相继极小决定。

记号 $N(R)$ 读"N of R", 表示落在以原点为心、半径 R 的闭球内的格点个数 (包含原点本身)。注意它是阶梯函数: R 连续增大, 但只有当球面扫过新格点时 $N(R)$ 才跳一下。

公式怎么读: 当 $\backslash(R$

译文·证明（平凡情形 + 下界） 所陈述的第一个结果是显然的；满足 $|\mathbf{x}| < R_1$ 的 Λ 的唯一一点就是原点。为在一般情形得到 $N(R)$ 的下界，我们考虑所有形如 $\mathbf{x} = u_1 \mathbf{X}^{(1)} + \cdots + u_\nu \mathbf{X}^{(\nu)}$ 的点，其中 $u_1, \dots, u_\nu$ 取一切满足 $|u_j| \leq \frac{1}{\nu} \frac{R}{|\mathbf{X}^{(j)}|}$, ($1 \leq j \leq \nu$) 的整数值。所有这些点都满足 $|\mathbf{x}| \leq R$ 。

$u_1, \dots, u_\nu$ 的选取数目（因为允许取零值）为

$$\gg \prod_{j=1}^{\nu} \frac{R}{|\mathbf{X}^{(j)}|} \gg \frac{R^\nu}{R_1 R_2 \cdots R_\nu}, \text{ 这里用到了引理 12.3.}$$

1 平凡情形。 $\backslash(R$

2 下界：造一批保证在球内的格点。用引理 12.3 修出的好基

$\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(\nu)}$ 。考虑所有 $\mathbf{x} = \sum_{j=1}^{\nu} u_j \mathbf{X}^{(j)}$ ，其中整数 u_j 受限 $|u_j| \leq \frac{1}{\nu} \cdot \frac{R}{|\mathbf{X}^{(j)}|}$ 。

3 验证它们都在球内。三角不等式：

$$|\mathbf{x}| \leq \sum_{j=1}^{\nu} |u_j| |\mathbf{X}^{(j)}| \leq \sum_{j=1}^{\nu} \frac{1}{\nu} \frac{R}{|\mathbf{X}^{(j)}|} \cdot |\mathbf{X}^{(j)}| = \sum_{j=1}^{\nu} \frac{R}{\nu} = \nu \cdot \frac{R}{\nu} = R$$

每一项的 $|\mathbf{X}^{(j)}|$ 约掉，正好凑成 R 。所以这些点确实都满足 $|\mathbf{x}| \leq R$ ，是合格的被计数对象。（除以 ν 这个因子正是为了让 ν 项加起来不超过 R 。）

4 数有多少种 $(u_1, \dots, u_\nu)$ 。每个 u_j 在区间 $[-\frac{1}{\nu} \frac{R}{|\mathbf{X}^{(j)}|}, \frac{1}{\nu} \frac{R}{|\mathbf{X}^{(j)}|}]$ 里取整数，含 0。一个长度为 $2t$ 的区间里整数个数 $\geq t$ （且当 $t \geq$ 某常数时 $\asymp t$ ）。所以 u_j 的取法数 $\gg \frac{R}{\nu |\mathbf{X}^{(j)}|} \gg \frac{R}{|\mathbf{X}^{(j)}|}$ （ $\nu \leq n$ 是常数，吸收进 $\gg$ ）。各 u_j 独立选取，相乘：取法总数 $\gg \prod_{j=1}^{\nu} \frac{R}{|\mathbf{X}^{(j)}|}$ 。

5 不同 (u_j) 给不同点。因为 $\mathbf{X}^{(j)}$ 是基，整系数表示唯一，所以不同的系数组对应不同格点，没有重复计数。故 $N(R) \geq \text{取法数} \gg \prod_{j \leq \nu} \frac{R}{|\mathbf{X}^{(j)}|}$ 。

6 换成 R_j 。由引理 12.3 的 $|\mathbf{X}^{(j)}| \asymp R_j$ ，有 $\frac{R}{|\mathbf{X}^{(j)}|} \asymp \frac{R}{R_j}$ ，连乘得

$$N(R) \gg \prod_{j=1}^{\nu} \frac{R}{R_j} = \frac{R^{\nu}}{R_1 R_2 \cdots R_{\nu}}.$$

下界证毕。

译文·证明（上界） 关于上界，我们首先注意到， Λ 中满足 $|\mathbf{x}| \leq R$ 的所有点 $\mathbf{x}$ 必定线性依赖于 $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(\nu)}$ ，因为 $R < R_{\nu+1}$ 。因此它们可表为 $\mathbf{x} = v_1 \mathbf{X}^{(1)} + \cdots + v_{\nu} \mathbf{X}^{(\nu)}$ ， v_j 为整数。对这样的点，我们有 $x_{\nu} = v_{\nu} X_{\nu}^{(\nu)}$ ， $x_{\nu-1} = v_{\nu} X_{\nu-1}^{(\nu)} + v_{\nu-1} X_{\nu-1}^{(\nu-1)}$ ，依此类推。由于 $\mathbf{x}$ 的每个坐标绝对值 $\leq R$ ，故 v_{ν} 的可能数目为 $\ll R/|X_{\nu}^{(\nu)}|$ ；一旦 v_{ν} 选定， $v_{\nu-1}$ 的可能数目为 $\ll R/|X_{\nu-1}^{(\nu-1)}|$ ，依此类推。（注意所有这些数都 $\gg 1$ ，否则该论证就不成立。）因此，再次利用引理 12.3，我们断定点 $\mathbf{x}$ 的数目为

$$\ll \frac{R^{\nu}}{|X_1^{(1)}| \cdots |X_{\nu}^{(\nu)}|} \ll \frac{R^{\nu}}{R_1 R_2 \cdots R_{\nu}}.$$

1 球内格点只用得到前 ν 个方向。任何 $(\|\mathbf{x}\| \leq R)$ ，矛盾。所以 $\mathbf{x} = \sum_{j=1}^{\nu} v_j \mathbf{X}^{(j)}$ ，整系数 v_j 。

2 从最高坐标往下"逐个锁定" v_j （回代）。因为基是下三角，坐标关系是：

$$x_{\nu} = v_{\nu} X_{\nu}^{(\nu)}, \quad x_{\nu-1} = v_{\nu} X_{\nu-1}^{(\nu)} + v_{\nu-1} X_{\nu-1}^{(\nu-1)}, \quad \dots$$

第 ν 个坐标只含 v_{ν} （因为只有 $\mathbf{X}^{(\nu)}$ 在第 ν 坐标上非零），所以 $v_{\nu} = x_{\nu} / X_{\nu}^{(\nu)}$ 。

3 数 v_ν 的可能数目。 $|x_\nu| \leq |\mathbf{x}| \leq R$ ，而 $v_\nu = x_\nu / X_\nu^{(\nu)}$ 是整数，所以 $|v_\nu| \leq R / |X_\nu^{(\nu)}|$ ，可能取值个数 $\ll R / |X_\nu^{(\nu)}|$ 。

4 逐层往下。 v_ν 定了后，第 $\nu - 1$ 坐标式中 $v_\nu X_{\nu-1}^{(\nu)}$ 已知，于是 $v_{\nu-1} = (x_{\nu-1} - v_\nu X_{\nu-1}^{(\nu)}) / X_{\nu-1}^{(\nu-1)}$ ；同样 $|x_{\nu-1}| \leq R$ ，可能数目 $\ll R / |X_{\nu-1}^{(\nu-1)}|$ 。如此一层层回代到 v_1 ，第 j 层可能数目 $\ll R / |X_j^{(j)}|$ 。

5 括号里的提醒"这些数都 $\gg 1$ "。这一步逻辑很关键：用"可能数目 $\ll R / |X_j^{(j)}|$ "去相乘，前提是每个 $R / |X_j^{(j)}| \gg 1$ （即至少有一种取法、量级是真的"多"），否则把一堆 < 1 的数相乘会得出荒谬的小上界。这里 $R \geq R_\nu \geq R_j \asymp |X_j^{(j)}|$ （对 $j \leq \nu$ ），所以确实 $R / |X_j^{(j)}| \gg 1$ ，论证成立。

6 相乘得上界。把各层可能数目相乘（这是计数的乘法原理：先选 v_ν ，再选 $v_{\nu-1}$ ，……）：

$$N(R) \ll \prod_{j=1}^{\nu} \frac{R}{|X_j^{(j)}|} = \frac{R^\nu}{|X_1^{(1)}| \cdots |X_\nu^{(\nu)}|} \ll \frac{R^\nu}{R_1 R_2 \cdots R_\nu},$$

末一步又用引理 12.3 的 $|X_j^{(j)}| \asymp R_j$ 。上界证毕。上下界同阶，引理 12.4 成立。■

译文·注 引理 12.4 的一般含义是：就计数球（或其它固定形状的凸体）内的格点而言，每一个格的表现都与由

$(R_1, 0, \dots, 0), (0, R_2, 0, \dots, 0), \dots, (0, 0, \dots, R_n)$ 所生成的矩形格相同，相差一个仅依赖于 n 的常数。因此对许多目的而言，我们可以借助这 n 个正数 $R_1, \dots, R_n$ 来充分描述一个格。

这条注点出引理 12.4 的"灵魂"。它说：任何一张可能歪七扭八的格，在"球里数格点"这件事上，都和一张方方正正的矩形格——各坐标轴方向间距分别为

$R_1, R_2, \dots, R_n$ 的那张——表现一致（只差常数倍）。对矩形格，半径 R 球里格点数显然约是 $\prod_j (2R/R_j + 1)$ 这种乘积，正对应公式 $R^\nu / (R_1 \cdots R_\nu)$ 。于是结论：研究格点计数时，可以把任意格"等效替换"成只由 n 个数 $R_1, \dots, R_n$ 描述的矩形格，复杂的 n^2 个系数 λ_{ij} 全部浓缩成 n 个相继极小。这正是相继极小作为"格的指纹"的威力，也是引理 12.6 能成立的基础。

第 7 节 · 伴随格（极格）与 (12.3)

译文 x 空间中的格 Λ 与 y 空间中的格 M ，若它们的基可以选取得使 $\Lambda^T M = I$ ，则称为**伴随的**，或**极的**，其中 T 表示矩阵的转置。如果两个格分别由 $\mathbf{x} = \Lambda \mathbf{u}$ 与 $\mathbf{y} = M \mathbf{v}$ 给出，其中 $\mathbf{u}$ 与 $\mathbf{v}$ 为整向量，则该条件意味着 $x_1 y_1 + \cdots + x_n y_n = u_1 v_1 + \cdots + u_n v_n$ (12.3) 恒成立。注意 $d(\Lambda)d(M) = 1$ 。 Λ 与 M 之间的关系是对称的。但该关系在 x 空间的任意线性变换下不是不变的；若 $\mathbf{x} = A\mathbf{x}'$ 且 $\mathbf{y} = B\mathbf{y}'$ ，则该关系仅在 $A^T B = I$ 时才得以保持。

这段引入"伴随格"，是为下一条 Mahler 定理做准备。先补两个记号。

记号 Λ^T （转置）与 I （单位阵） 转置 Λ^T 读"Lambda 转置"，就是把矩阵沿主对角线翻折：原来第 i 行第 j 列的数，挪到第 j 行第 i 列。单位阵 I 是对角线全 1、其余全 0 的矩阵，乘任何矩阵都不改变它（相当于数里的 1）。

记号 $\sum x_k y_k$ （内积/点积） $x_1 y_1 + \cdots + x_n y_n$ 叫向量 $\mathbf{x}$ 与 $\mathbf{y}$ 的**内积**（也叫点积、数量积），高中学过二维三维版本。它有个关键几何意义：**内积 = 0 当且仅当两向量垂直**；而内积 = $|\mathbf{x}||\mathbf{y}| \cos \theta$ ， θ 是夹角。下面会反复用它。

"伴随/极"的定义：两张格 Λ （在 x 空间）、 M （在 y 空间）若能选基使 $\Lambda^T M = I$ ，就叫一对伴随格（adjoint）/ 极格（polar）。下面解释这个矩阵条件等价于内积

关系 (12.3)。

- 1 **展开内积。** 设 $\mathbf{x} = \Lambda \mathbf{u}$, $\mathbf{y} = \mathbf{M} \mathbf{v}$ ($\mathbf{u}, \mathbf{v}$ 整向量)。把内积写成矩阵语言: $x_1 y_1 + \cdots + x_n y_n = \mathbf{x}^T \mathbf{y}$ (一行乘一列正好是对应分量相乘求和)。
- 2 **代入。** $\mathbf{x}^T \mathbf{y} = (\Lambda \mathbf{u})^T (\mathbf{M} \mathbf{v}) = \mathbf{u}^T \Lambda^T \mathbf{M} \mathbf{v}$ (转置法则 $(\Lambda \mathbf{u})^T = \mathbf{u}^T \Lambda^T$)。
- 3 **用条件。** 若 $\Lambda^T \mathbf{M} = I$, 则 $\mathbf{u}^T \Lambda^T \mathbf{M} \mathbf{v} = \mathbf{u}^T I \mathbf{v} = \mathbf{u}^T \mathbf{v} = u_1 v_1 + \cdots + u_n v_n$ 。所以 $\sum x_k y_k = \sum u_k v_k$ 恒成立, 这就是 (12.3)。反之这个恒等式对一切整 $\mathbf{u}, \mathbf{v}$ 成立也能逼出 $\Lambda^T \mathbf{M} = I$ 。两种说法等价。
- 4 $d(\Lambda)d(\mathbf{M}) = 1$ 。对 $\Lambda^T \mathbf{M} = I$ 取行列式: $\det(\Lambda^T) \det(\mathbf{M}) = \det I = 1$ 。而 $\det \Lambda^T = \det \Lambda$ (转置不改变行列式), 取绝对值得 $|\det \Lambda| |\det \mathbf{M}| = 1$, 即 $d(\Lambda)d(\mathbf{M}) = 1$ 。所以一张格的胞腔越大, 它伴随格的胞腔就越小, 互成倒数。
- 5 **关系是对称的。** 由 $\Lambda^T \mathbf{M} = I$ 可推 $\mathbf{M}^T \Lambda = I$ (两边转置: $(\Lambda^T \mathbf{M})^T = \mathbf{M}^T \Lambda = I^T = I$), 所以" $\mathbf{M}$ 是 Λ 的伴随" 与 " Λ 是 $\mathbf{M}$ 的伴随" 是一回事。
- 6 **为何不在任意线性变换下不变。** 若在 x 空间作变换 $\mathbf{x} = A \mathbf{x}'$ 、 y 空间作 $\mathbf{y} = B \mathbf{y}'$, 要让内积关系 (12.3) 保持, 需要 $\mathbf{x}^T \mathbf{y} = \mathbf{x}'^T A^T B \mathbf{y}' = \mathbf{x}'^T \mathbf{y}'$ 对一切成立, 即 $A^T B = I$ 。一般的 A, B 不满足这条, 所以伴随关系会被破坏——它依赖于两个空间用互相配套 ($A^T B = I$) 的坐标。这点提醒我们: 伴随关系是"带着内积结构"的, 不能随便换坐标。

"极/伴随"的动机 为什么要造伴随格？因为很多问题里，" $\mathbf{x}$ 满足某些线性条件"会自然地对应到" $\mathbf{y}$ 在伴随格里的尺寸"。Mahler 定理（下条）会揭示：一张格某方向"密"，它伴随格的**对偶**方向就"疏"，两者相继极小成倒数关系。这种"对偶"思想让我们能在 Λ 和 M 之间来回倒换，挑容易处理的一边算。

第 8 节 · 引理 12.5 (Mahler)：伴随格的相继极小成倒数

译文 · 引理 12.5 (Mahler) 若 Λ, M 为行列式皆为 1 的伴随格，相继极小分别为 $R_1, \dots, R_n$ 与 $S_1, \dots, S_n$ ，则

$$R_1 \asymp \frac{1}{S_n}, R_2 \asymp \frac{1}{S_{n-1}}, \dots, R_n \asymp \frac{1}{S_1}.$$

这是 Mahler 的漂亮定理。 $S_1, \dots, S_n$ 是伴随格 M 的相继极小（与 Λ 的 $R_1, \dots, R_n$ 平行定义）。结论：把 M 的相继极小**倒过来排**取倒数，就与 Λ 的相继极小一一对应同阶。统一写成 $R_\mu S_{n-\mu+1} \asymp 1$ 。直观： Λ 在某方向最密（ R_1 小），对应 M 在对偶方向最疏（ S_n 大），乘积 $\asymp 1$ 。这把"格"和"它的对偶格"的疏密信息完全绑在一起。德国数学家 Kurt Mahler (1903–1988) 在 1930 年代证明了这个对偶定理。下面证明分两半：先证下界 $R_\nu S_{n-\nu+1} \geq 1$ ，再用乘积比较得反向。

译文 · 证明（一半： $R_\nu S_{n-\nu+1} \geq 1$ ） 设 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 为 Λ 的极小点， $\mathbf{y}^{(1)}, \dots, \mathbf{y}^{(n-\nu+1)}$ 为 M 的极小点。恒等式 (12.3) 表明，对 Λ, M 的任意点 $\mathbf{x}, \mathbf{y}$ ，要么 $\mathbf{x}$ 垂直于 $\mathbf{y}$ ，要么 $|x_1 y_1 + \dots + x_n y_n| \geq 1$ ，从而 $|\mathbf{x}| |\mathbf{y}| \geq 1$ 。垂直于每一个 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 的那些 $\mathbf{y}$ 构成一个 $(n - \nu)$ 维线性空间。它不能包含多于 $n - \nu$ 个线性无关的 $\mathbf{y}$ 空间的点，因而不能包含 $\mathbf{y}^{(1)}, \dots, \mathbf{y}^{(n-\nu+1)}$ 的全部。故存在 $r \leq \nu$ 与 $s \leq n - \nu + 1$ ，使得 $|\mathbf{x}^{(r)}| |\mathbf{y}^{(s)}| \geq 1$ 。又

$|\mathbf{x}^{(r)}| \leq R_\nu$ 且 $|\mathbf{y}^{(s)}| \leq S_{n-\nu+1}$ 。由此推出 $R_\nu S_{n-\nu+1} \geq 1$, ($1 \leq \nu \leq n$)。
(12.4)

1 关键二分法。取 Λ 的格点 $\mathbf{x}$ (非零) 和 $\mathbf{M}$ 的格点 $\mathbf{y}$ (非零)。由 (12.3), 内积 $\sum x_k y_k = \sum u_k v_k$ 是整数 (整向量内积)。一个整数要么是 0, 要么绝对值 ≥ 1 。所以: 要么 $\sum x_k y_k = 0$ (即 $\mathbf{x} \perp \mathbf{y}$, 垂直), 要么 $|\sum x_k y_k| \geq 1$ 。后者结合 $|\sum x_k y_k| \leq |\mathbf{x}||\mathbf{y}|$ (柯西不等式 $|\mathbf{x} \cdot \mathbf{y}| \leq |\mathbf{x}||\mathbf{y}|$) 得 $|\mathbf{x}||\mathbf{y}| \geq 1$ 。所以两个非零、不垂直的格点 (一边一个), 长度乘积必 ≥ 1 。

2 找一对不垂直的极小点。考虑"同时垂直于 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$ 的所有 $\mathbf{y}$ "。垂直于 ν 个线性无关向量, 是 ν 个线性方程的解集, 构成一个 $(n - \nu)$ 维子空间。这个子空间最多容纳 $n - \nu$ 个线性无关向量。

3 鸽笼: $n - \nu + 1$ 个极小点装不进去。 $\mathbf{M}$ 的极小点 $\mathbf{y}^{(1)}, \dots, \mathbf{y}^{(n-\nu+1)}$ 共 $n - \nu + 1$ 个、且线性无关。但上面子空间只能放 $n - \nu$ 个线性无关向量。所以这 $n - \nu + 1$ 个 $\mathbf{y}$ 不可能全部落在该子空间里——必有某个 $\mathbf{y}^{(s)}$ ($s \leq n - \nu + 1$) 不垂直于全部 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(\nu)}$, 即存在某个 $\mathbf{x}^{(r)}$ ($r \leq \nu$) 与它不垂直。

4 对这对用第 1 步。 $\mathbf{x}^{(r)}, \mathbf{y}^{(s)}$ 不垂直, 故 $|\mathbf{x}^{(r)}||\mathbf{y}^{(s)}| \geq 1$ 。

5 放大成 $R_\nu, S_{n-\nu+1}$ 。因 $r \leq \nu$, 相继极小递增, $|\mathbf{x}^{(r)}| = R_r \leq R_\nu$; 同理 $|\mathbf{y}^{(s)}| = S_s \leq S_{n-\nu+1}$ 。代入: $1 \leq |\mathbf{x}^{(r)}||\mathbf{y}^{(s)}| \leq R_\nu S_{n-\nu+1}$ 。得 (12.4): $R_\nu S_{n-\nu+1} \geq 1$ 。

译文·证明 (另一半: 上界) 相反方向的不等式由比较乘积得出。由于

$$R_1 \cdots R_n S_1 \cdots S_n \leq \left(\frac{2^n}{J_n} \right)^2 \quad (\text{由引理 12.2}), \text{ 由 (12.4) 可得}$$

$$R_\mu S_{n-\mu+1} \ll \left(\frac{2^n}{J_n} \right)^2, \quad (1 \leq \mu \leq n). \text{ 这就证明了引理 12.5.}$$

- 1 两格相继极小乘积都 $\ll 1$ 。对 Λ 用引理 12.2: $R_1 \cdots R_n \leq 2^n/J_n$; 对 M (也是 $d=1$): $S_1 \cdots S_n \leq 2^n/J_n$ 。相乘:
 $R_1 \cdots R_n S_1 \cdots S_n \leq (2^n/J_n)^2$ 。

- 2 把它配成 n 个"配对乘积"。注意 $\{R_\nu S_{n-\nu+1} : \nu = 1, \dots, n\}$ 恰好把全部 R 和全部 S 各用一次配对 (R_1 配 S_n , R_2 配 S_{n-1} , $\dots$), 所以

$$\prod_{\nu=1}^n (R_\nu S_{n-\nu+1}) = (R_1 \cdots R_n) (S_1 \cdots S_n) \leq (2^n/J_n)^2.$$

- 3 每个配对都被压住。对某个固定 μ , 把上式里除了 $R_\mu S_{n-\mu+1}$ 以外的配对都用第一半 (12.4) 的下界 ≥ 1 替掉:

$$R_\mu S_{n-\mu+1} \cdot \underbrace{\prod_{\nu \neq \mu} R_\nu S_{n-\nu+1}}_{\geq 1} \leq (2^n/J_n)^2.$$

既然后面那一大坨 ≥ 1 , 必有 $R_\mu S_{n-\mu+1} \leq (2^n/J_n)^2 \ll 1$ 。这就是上界 $R_\mu S_{n-\mu+1} \ll 1$ 。

- 4 合并。下界 $R_\mu S_{n-\mu+1} \geq 1$ 与上界 $R_\mu S_{n-\mu+1} \ll 1$ 一起给出
 $R_\mu S_{n-\mu+1} \asymp 1$, 即 $R_\mu \asymp 1/S_{n-\mu+1}$, 正是引理 12.5。■

译文·注 引理 12.5 中的条件 $d(\Lambda) = 1$ 并非必要, 但它并不损失一般性。当引理 12.5 被推广到关于任意凸体 (关于原点中心对称) 的相继极小时, 必须在 x 空间用一个凸体、而在 y 空间用一个关于单位球与之互极的凸体。

这条注的两点。第一， $d(\Lambda) = 1$ 只是为了证明里直接套用引理 12.2 的干净形式；任何格缩放一下就能化到 $d = 1$ ，所以不损失一般性。第二，若要把 Mahler 定理升级到"用一般凸体量距离"的版本，必须让 x 空间用的凸体 K 与 y 空间用的凸体是一对"极体" (polar body，关于单位球互极： K 越往某方向胖，它的极体在该方向就越瘦)。这呼应第 7 节"伴随关系依赖配套内积结构"的提醒。本章只用球，故无需操心这层推广。

第 9 节 · 一类自伴随的 $2n$ 维格

译文 在 $2n$ 维空间中有一类特殊的格，它本质上是自伴随的。设 Λ 表示由下式给出的 $2n$ 维格：

$$\begin{aligned} ax_1 &= u_1, \dots, ax_n = u_n, \\ a^{-1}x_{n+1} &= \gamma_{11}u_1 + \dots + \gamma_{1n}u_n + u_{n+1}, \dots, \\ a^{-1}x_{2n} &= \gamma_{n1}u_1 + \dots + \gamma_{nn}u_n + u_{2n}, \end{aligned}$$

其中 $a \neq 0$ 且数 γ_{ij} 为实数。它具有形如下式的矩阵

$$\Lambda = \begin{pmatrix} a^{-1}I_n & 0 \\ a\gamma & aI_n \end{pmatrix}.$$

其伴随格具有矩阵 $M = (\Lambda^T)^{-1} = \begin{pmatrix} aI_n & -a\gamma^T \\ 0 & a^{-1}I_n \end{pmatrix}$ 。

这段造出后面三次型要用的具体格。它生活在 $2n$ 维空间（坐标分成两半：前 n 个 $x_1, \dots, x_n$ ，后 n 个 $x_{n+1}, \dots, x_{2n}$ ）。设计动机：把" n 个线性型 $L_i = \sum_j \gamma_{ij}u_j$ 接近整数"这件事，编码成一张 $2n$ 维格的几何。

记号 a 、 γ_{ij} 、 I_n 、分块矩阵 $a > 0$ （后面取 $a > 1$ ）是一个缩放参数：前 n 个坐标被乘 $1/a$ （压扁），后 n 个被乘 a （拉长），用来调节"哪半边密、哪半边疏"。 γ_{ij} 是线性型的系数。 I_n 是 $n \times n$ 单位阵。矩阵写成 2×2 的"分块"形

式：每个块是 $n \times n$ 小矩阵， $\begin{pmatrix} a^{-1}I_n & 0 \\ a\gamma & aI_n \end{pmatrix}$ 表示左上块 $a^{-1}I_n$ 、左下块 $a\gamma$ 、右上块 0、右下块 aI_n 。

怎么从方程读出矩阵。前 n 行 $ax_i = u_i$ 即 $x_i = a^{-1}u_i$ ：前 n 个坐标只依赖前 n 个参数，系数 a^{-1} ，对应左上块 $a^{-1}I_n$ 、右上块 0。后 n 行 $a^{-1}x_{n+i} = \sum_j \gamma_{ij}u_j + u_{n+i}$ 即 $x_{n+i} = a \sum_j \gamma_{ij}u_j + au_{n+i}$ ：依赖前 n 个参数（系数 $a\gamma$ ）和后 n 个参数（系数 aI_n ），对应左下块 $a\gamma$ 、右下块 aI_n 。这就拼出了 Λ 。

1 算伴随格矩阵 $M = (\Lambda^T)^{-1}$ 。由第 7 节，伴随条件 $\Lambda^T M = I$ 即 $M = (\Lambda^T)^{-1}$ 。先转置： $\Lambda^T = \begin{pmatrix} a^{-1}I_n & a\gamma^T \\ 0 & aI_n \end{pmatrix}$ （左下块 $a\gamma$ 转到右上变 $a\gamma^T$ ；右上块 0 转到左下变 0）。

2 求逆。对上三角分块阵 $\begin{pmatrix} P & Q \\ 0 & S \end{pmatrix}$ ，逆是 $\begin{pmatrix} P^{-1} & -P^{-1}QS^{-1} \\ 0 & S^{-1} \end{pmatrix}$ 。这里 $P = a^{-1}I_n, Q = a\gamma^T, S = aI_n$ ，于是 $P^{-1} = aI_n, S^{-1} = a^{-1}I_n, -P^{-1}QS^{-1} = -(aI_n)(a\gamma^T)(a^{-1}I_n) = -a\gamma^T$ 。得

$$M = \begin{pmatrix} aI_n & -a\gamma^T \\ 0 & a^{-1}I_n \end{pmatrix},$$

与译文一致。

译文 如果 $\gamma^T = \gamma$ ，也就是说如果 $\gamma_{ij} = \gamma_{ji}$ （对所有 i, j ）(12.5)，那么格 M 可以通过下述操作变为格 Λ ：(i) 改变 $v_{n+1}, \dots, v_{2n}$ 的符号，(ii) 改变 $y_{n+1}, \dots, y_{2n}$ 的符号，(iii) 互换 $v_1, \dots, v_n$ 与 $v_{n+1}, \dots, v_{2n}$ ，(iv) 互换 $y_1, \dots, y_n$ 与 $y_{n+1}, \dots, y_{2n}$ 。

关键转折：对称条件 (12.5) 让 M 和 Λ 长得一样。

对称条件 $\gamma_{ij} = \gamma_{ji}$ 即系数矩阵 γ 关于主对角线对称（转置等于自己， $\gamma^T = \gamma$ ）。这在三次型应用里自然成立（来自三次型的某种对称二阶结构）。这条件是引理 12.6 里指数能取到 n 而非 $2n - 1$ 的根本原因（见本节末注）。

若 $\gamma^T = \gamma$ ，则 $M = \begin{pmatrix} aI_n & -a\gamma \\ 0 & a^{-1}I_n \end{pmatrix}$ 。译文里那串“改符号、互换上下半”的操作，是在对 M 的坐标 (y, v) 做么模 + 旋转/反射的整理：交换前后两半、给后半变号，本质是用一个行列式 ± 1 的正交置换把 M 的矩阵“洗”成 Λ 的矩阵。结果是：在 γ 对称时， M 与 Λ 是同一张格（只差坐标重排与符号），即 Λ “本质上自伴随”。我们不必逐一核对四步操作（它们只是把分块 $\begin{pmatrix} aI & -a\gamma \\ 0 & a^{-1}I \end{pmatrix}$ 经行列对调与变号还原成 $\begin{pmatrix} a^{-1}I & 0 \\ a\gamma & aI \end{pmatrix}$ 的同构），重点是结论。

译文 因此，在条件 (12.5) 之下， M 的相继极小与 Λ 的相同。由上一个引理，可得 $R_1 R_{2n} \asymp 1, \dots, R_n R_{n+1} \asymp 1$ 。特别地，我们有 $R_n \ll 1 \ll R_{n+1}$ 。

1 两格相继极小相同。因为 M 与 Λ 是同一张格（自伴随），它们的相继极小逐个相等： $S_k = R_k$ 。

2 代入 Mahler 定理。引理 12.5 对这对伴随格（维数是 $2n$ ）给 $R_\mu S_{2n-\mu+1} \asymp 1$ 。把 $S_k = R_k$ 代入： $R_\mu R_{2n-\mu+1} \asymp 1$ 。取 $\mu = 1, \dots, n$ 得 $R_1 R_{2n} \asymp 1, R_2 R_{2n-1} \asymp 1, \dots, R_n R_{n+1} \asymp 1$ 。

3 挑出最中间那对，得 $R_n \ll 1 \ll R_{n+1}$ 。由 $R_n R_{n+1} \asymp 1$ ：因 $R_n \leq R_{n+1}$ （相继极小递增），两数乘积 $\asymp 1$ 而前者不大于后者，故 $R_n^2 \leq R_n R_{n+1} \asymp 1$ 给出 $R_n \ll 1$ ，而 $R_{n+1}^2 \geq R_n R_{n+1} \asymp 1$ 给出 $R_{n+1} \gg 1$ 。所以 $R_n \ll 1 \ll R_{n+1}$ 。这条“ R_n 不超过常数、 R_{n+1} 不小于常数”的分界，正是引理 12.6 证明里反复用的支点：前 n 个方向“密”（极小 $\ll 1$ ），后 n 个方向“疏”（极小 $\gg 1$ ）。

译文 我们现在可以证明后续关于三次型的工作所需的主要结果。

一句过渡：前面所有铺垫（格、相继极小、引理 12.4 的计数、Mahler 定理、自伴随格的 $R_n \ll 1 \ll R_{n+1}$ ）都是为了下面这条引理 12.6——它是第 13 章起处理三次型时真正要调用的工具。

第 10 节 · 引理 12.6：解数随区间缩小而不会掉太快

译文 · 引理 12.6 设 $L_1, \dots, L_n$ 为线性型 $L_i = \gamma_{i1}u_1 + \dots + \gamma_{in}u_n$, $(1 \leq i \leq n)$, 满足对称条件 $\gamma_{ij} = \gamma_{ji}$ 。设 $a > 1$ 为实数, 并设 $N(Z)$ 表示满足

$$\begin{cases} |u_1| < aZ, \dots, |u_n| < aZ, \\ |L_1 - u_{n+1}| < a^{-1}Z, \dots, |L_n - u_{2n}| < a^{-1}Z \end{cases} \quad (12.6)$$

的整数组 $u_1, \dots, u_{2n}$ (含 0) 的个数。则当 $0 < Z_1 \leq Z_2 \leq 1$ 时, 有

$$\frac{N(Z_2)}{N(Z_1)} \ll \left(\frac{Z_2}{Z_1} \right)^n. \quad (12.7)$$

先把这条引理"翻译成普通话"。我们有 n 个对称线性型 L_i 。给定一个"尺度" Z , $N(Z)$ 数的是这样的整数组 $(u_1, \dots, u_{2n})$: 前 n 个整数 $u_1, \dots, u_n$ 各自绝对值 \ (非常接近某个整数 u_{n+i} (误差 \ (

记号 $N(Z), Z_1, Z_2$ $N(Z)$ 是尺度 Z 下满足 (12.6) 的解数 (含全零解)。

$Z_1 \leq Z_2$ 是两个尺度, $Z_2/Z_1 \geq 1$ 是放大倍数。

结论 (12.7) 的含义：把尺度从 Z_1 放大到 Z_2 , 解数 N 增长不会超过 $(Z_2/Z_1)^n$ 倍。反过来读 (这才是真正要用的方向)：把尺度缩小, 解数减少得不会比

$(Z_1/Z_2)^n$ 更狠——解不会"突然全没了"。这正是后面三次型次弧估计需要的"稳健性"：缩小盒子时还能保住足够多的解。

译文·证明（化成球内格点计数） 这些不等式等价于 $|x_1| < Z, \dots, |x_{2n}| < Z$ （对上面定义的 $2n$ 维格 Λ 的一般点）。因此这些不等式蕴含 $|\mathbf{x}| < \sqrt{2n} Z$ 。另一方面，它们被 $|\mathbf{x}| < Z$ 所蕴含。于是，若 $N_0(Z)$ 表示满足 $|\mathbf{x}| < Z$ 的 Λ 的点（含原点）的个数，则有 $N_0(Z) \leq N(Z) \leq N_0(\sqrt{2n} Z)$ 。

1 把不等式组翻译成格 Λ 的坐标。回到第 9 节那张 $2n$ 维格： $x_i = a^{-1}u_i$ ($i \leq n$), $x_{n+i} = a(L_i + u_{n+i})$ 这里 $L_i = \sum_j \gamma_{ij}u_j$, 所以 $a^{-1}x_{n+i} = L_i + u_{n+i}$, 即 $x_{n+i} = a(L_i - (-u_{n+i}))$ 。把 (12.6) 的 u_{n+i} 理解成这第 $n+i$ 个整数参数（符号无所谓），则：
· $\setminus(|u_i| \cdot \setminus(|L_i - u_{n+i}|)$ 所以 (12.6) 恰好等价于"格点 $\mathbf{x}$ 的全部 $2n$ 个坐标都 $\setminus$ (

2 立方体夹在两个球之间。若每个 $\setminus(|x_k|$

3 夹逼 $N(Z)$ 。记 $N_0(Z) =$ (半径 Z 球内格点数)。由上面的包含关系： $N_0(Z) \leq N(Z) \leq N_0(\sqrt{2n} Z)$ 。这样就把"数不等式解"彻底转化成"数球内格点"，可以套引理 12.4 了。

译文·证明（化简目标 (12.8)） 因此，若 $0 < Z_1 \leq Z_2 < 1$ ，则

$\frac{N(Z_2)}{N(Z_1)} \leq \frac{N_0(\sqrt{2n} Z_2)}{N_0(Z_1)}$ 。如果我们证明对应于 (12.7) 的结果，即 $\frac{N_0(Z_2)}{N_0(Z_1)} \ll \left(\frac{Z_2}{Z_1}\right)^n$ (12.8)，在较弱的条件 $Z_2 \ll 1$ （而非 $Z_2 \leq 1$ ）下成立，那么我们就可以把它用于把 Z_2 换成 $\sqrt{2n} Z_2$ 的情形，从而推出 (12.7)。

1 用夹逼把比值换成 N_0 。 $\frac{N(Z_2)}{N(Z_1)} \leq \frac{N_0(\sqrt{2n}Z_2)}{N_0(Z_1)}$ (上面用 $N(Z_2) \leq N_0(\sqrt{2n}Z_2)$ 、 $N(Z_1) \geq N_0(Z_1)$)。

2 把要证的目标改写为 (12.8)。只要能证 $\frac{N_0(Z_2)}{N_0(Z_1)} \ll (Z_2/Z_1)^n$ ，且这个对 N_0 的结论在放宽条件 $Z_2 \ll 1$ (允许 Z_2 是个不超过常数的数，不必 ≤ 1) 下成立，那么把里头的 Z_2 替换成 $\sqrt{2n}Z_2$ (它仍 $\ll 1$ ，因为 $Z_2 \leq 1$ 时 $\sqrt{2n}Z_2 \leq \sqrt{2n} \ll 1$) 即得

$$\frac{N_0(\sqrt{2n}Z_2)}{N_0(Z_1)} \ll \left(\frac{\sqrt{2n}Z_2}{Z_1} \right)^n = (2n)^{n/2} \left(\frac{Z_2}{Z_1} \right)^n \ll \left(\frac{Z_2}{Z_1} \right)^n,$$

常数 $(2n)^{n/2}$ 只依赖 n ，吸收进 $\ll$ 。结合第 1 步即得 (12.7)。所以剩下任务就是证 (12.8) (条件放宽到 $Z_2 \ll 1$)。

译文·证明 (核心：用引理 12.4 证 (12.8)) 设 $R_1, \dots, R_{2n}$ 表示 Λ 的相继极小。我们已经看到 $R_n \ll 1 \ll R_{n+1}$ 。用 $R_\nu \leq Z_1 < R_{\nu+1}$, $R_\mu \leq Z_2 < R_{\mu+1}$ 定义 ν 与 μ ，从而 $\nu \leq \mu$ 。由引理 12.4, $N_0(Z_1) \gg \frac{Z_1^\nu}{R_1 \cdots R_\nu}$ 且 $N_0(Z_2) \ll \frac{Z_2^\mu}{R_1 \cdots R_\mu}$ ，从而 $\frac{N_0(Z_2)}{N_0(Z_1)} \ll \frac{Z_2^\mu}{Z_1^\nu R_{\nu+1} \cdots R_\mu}$ 。

1 给 Z_1, Z_2 各定"档位" ν, μ 。相继极小 $R_1 \leq \cdots \leq R_{2n}$ 把数轴切成若干档。 Z_1 落在第 ν 档 ($R_\nu \leq Z_1 < R_{\nu+1}$)。

2 套引理 12.4。该引理给 $N_0(Z) \asymp Z^k / (R_1 \cdots R_k)$ (k 是 Z 所在档)。取下界用在分母 $N_0(Z_1) \gg Z_1^\nu / (R_1 \cdots R_\nu)$ ，取上界用在分子 $N_0(Z_2) \ll Z_2^\mu / (R_1 \cdots R_\mu)$ 。

3 相除化简。

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll \frac{Z_2^\mu / (R_1 \cdots R_\mu)}{Z_1^\nu / (R_1 \cdots R_\nu)} = \frac{Z_2^\mu}{Z_1^\nu} \cdot \frac{R_1 \cdots R_\nu}{R_1 \cdots R_\mu} = \frac{Z_2^\mu}{Z_1^\nu R_{\nu+1} \cdots R_\mu}$$

(分子分母的 $R_1 \cdots R_\nu$ 约掉, 分母剩 $R_{\nu+1} \cdots R_\mu$ 。) 这是后面要分情况估的核心表达式。

译文·证明 (三种情况讨论) 若 $\mu \leq n$, 则 (12.8) 成立, 因为右端

$\leq \frac{Z_2^\mu}{Z_1^\mu} \leq \left(\frac{Z_2}{Z_1}\right)^n$ 。若 $\mu > n$ 且 $\nu \leq n$, 我们把该表达式写成

$\frac{Z_2^n}{Z_1^\nu R_{\nu+1} \cdots R_n} \cdot \frac{Z_2^{\mu-n}}{R_{n+1} \cdots R_\mu}$, 由于 $Z_2 \ll 1$ 且 $R_{n+1} \gg 1$, 结果同样成立。最后, 可能 $\nu > n$ 仅当 $Z_1 \gg 1$ 时出现, 此时

$\frac{N_0(Z_2)}{N_0(Z_1)} \ll \frac{Z_2^\mu}{Z_1^\nu} \ll 1 \ll \left(\frac{Z_2}{Z_1}\right)^n$ 。这就证明了引理 12.6。

核心表达式 $\frac{Z_2^\mu}{Z_1^\nu R_{\nu+1} \cdots R_\mu}$ 要分三种情况压到 $\ll (Z_2/Z_1)^n$ 。关键武器是 $R_n \ll 1 \ll R_{n+1}$ (前 n 个极小小、后 n 个大) 和 $Z_2 \ll 1$ 。

1 情况一: $\mu \leq n$ (两个尺度都落在"密"的前半档)。要把核心表达式从上方压住, 需把分母 $R_{\nu+1} \cdots R_\mu$ 从下方估。对每个 j ($\nu < j \leq \mu$), 又相继极小递增, 故 $R_j \geq R_{\nu+1} > Z_1$ 。于是分母含 $\mu - \nu$ 个都 $> Z_1$ 的因子, $R_{\nu+1} \cdots R_\mu > Z_1^{\mu-\nu}$ 。代入:

$$\frac{Z_2^\mu}{Z_1^\nu R_{\nu+1} \cdots R_\mu} < \frac{Z_2^\mu}{Z_1^\nu Z_1^{\mu-\nu}} = \frac{Z_2^\mu}{Z_1^\mu} = \left(\frac{Z_2}{Z_1}\right)^\mu \leq \left(\frac{Z_2}{Z_1}\right)^n.$$

未一步因 $Z_2/Z_1 \geq 1$ 且 $\mu \leq n$, 把指数从 μ 放大到 n 只会更大。**情况一成立。**

- 2 情况二： $\mu > n$ 且 $\nu \leq n$ (Z_1 在前半、 Z_2 跨到了后半)。把核心表达式拆成两段，在 n 处断开：

$$\frac{Z_2^\mu}{Z_1^\nu R_{\nu+1} \cdots R_\mu} = \underbrace{\frac{Z_2^n}{Z_1^\nu R_{\nu+1} \cdots R_n}}_{(A)} \cdot \underbrace{\frac{Z_2^{\mu-n}}{R_{n+1} \cdots R_\mu}}_{(B)}.$$

· 段 (A)：分母 $R_{\nu+1} \cdots R_n$ 用 $R_j > Z_1$ ($j > \nu$) 得 $\geq Z_1^{n-\nu}$ ，故

$$(A) \leq \frac{Z_2^n}{Z_1^\nu Z_1^{n-\nu}} = \frac{Z_2^n}{Z_1^n} = (Z_2/Z_1)^n.$$

· 段 (B)：分母 $R_{n+1} \cdots R_\mu$ 里每个 $R_j \geq R_{n+1} \gg 1$ (后半档全是大极小)，所以分母 $\gg 1$ ；分子 $Z_2^{\mu-n}$ 里 $Z_2 \ll 1$ 、指数 $\mu - n \geq 1$ ，所以 $Z_2^{\mu-n} \ll 1$ 。于是 $(B) \ll 1$ 。

两段相乘： $(A)(B) \ll (Z_2/Z_1)^n \cdot 1 = (Z_2/Z_1)^n$ 。情况二成立。这一步正是 " $R_{n+1} \gg 1$ 与 $Z_2 \ll 1$ " 的用武之地——它保证跨进后半档的那些方向"贡献 $\ll 1$ "，不会把比值撑爆。

- 3 情况三： $\nu > n$ (连 Z_1 都落在后半档)。这只能当

$Z_1 \geq R_\nu \geq R_{n+1} \gg 1$ ，即 $Z_1 \gg 1$ 。但我们处理的是 $Z_1 \leq Z_2 \ll 1$ (小尺度)——所以 $Z_1 \gg 1$ 与 $Z_2 \ll 1$ 同时成立只能挤在

$Z_1 \asymp Z_2 \asymp 1$ 的边界附近。此时直接放缩：

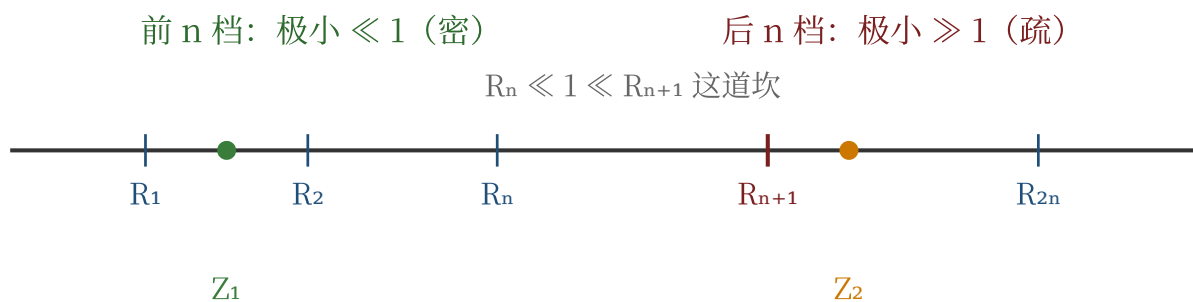
$N_0(Z_2) \ll Z_2^\mu / (R_1 \cdots R_\mu)$ 、 $N_0(Z_1) \gg Z_1^\nu / (R_1 \cdots R_\nu)$ ，但更简单

地， Z_1, Z_2 都 $\asymp 1$ ，故 $N_0(Z_1), N_0(Z_2)$ 都是有界的常数量级，比值

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll 1. \text{ 又因 } Z_2/Z_1 \geq 1 \text{ 给 } (Z_2/Z_1)^n \geq 1, \text{ 所以}$$

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll 1 \leq (Z_2/Z_1)^n. \text{ 情况三成立。}$$

- 4 三种情况穷尽了 (ν, μ) 的所有可能 (因 $\nu \leq \mu$ ，要么 $\mu \leq n$ 、要么 $\mu > n \geq \nu$ 、要么 $\nu > n$)，故 (12.8) 在 $Z_2 \ll 1$ 下成立。回到第二轮的化简，即得 (12.7)。引理 12.6 证毕。■



把 $R_1 \leq \dots \leq R_{2n}$ 标在数轴上分档。 Z_1, Z_2 各落在某档 (定 ν, μ)。坎 $R_n \ll 1 \ll R_{n+1}$ 把"密的前半"与"疏的后半"分开, 正是三种情况讨论的依据。

译文·注 引理 12.6 的意义在于: 不等式组 (12.6) 的解的个数当 Z 减小时不会减小得过快。该结果只有在 aZ 很大时才有意义, 因为若 $aZ < 1$, 则这些不等式蕴含 $u_1 = \dots = u_{2n} = 0$, 且 $N(Z) = 1$ 。看来, 若没有关于线性型 $L_1, \dots, L_n$ 中系数 γ_{ij} 的对称条件, 则只能断言一个较弱的结果, 其中指数 n 要换成 $2n - 1$ 。

这条收尾注点明引理 12.6 的用途、适用范围与对称条件的代价。

- 1 "意义": 解数不会掉太快。(12.7) 反过来读就是 $N(Z_1) \gg (Z_1/Z_2)^n N(Z_2)$: 缩小尺度时解数最多按 n 次幂衰减。后面三次型用圆法时, 需要保证某尺度下解仍然"够多", 这条引理正提供这个下保。
- 2 "只有 aZ 大才有意义"。若 $aZ < 1$, 则首行条件 $\backslash(|u_i| \leq 1)$ 时 $\backslash(a^{-1}Z$
- 3 对称条件的代价。最后一句是 Davenport 的诚实交代: 对称 $\gamma_{ij} = \gamma_{ji}$ 是把指数做到漂亮的 n 的关键。如果 γ 不对称, 第 9 节那张格就不再自伴随, $R_n \ll 1 \ll R_{n+1}$ 这道干净的"中点坎"消失, 三种情况的讨论失效, 只能证出更弱的、指数为 $2n - 1$ 的版本。这解释了为什么前面要费力强调对称性——它不是装饰, 而是把结论从 $2n - 1$ 改进到 n 的命根子。

全章脉络回顾（一页纸记住）

- 1 格、基、行列式 $d(\Lambda)$ ：均匀钉子板，胞腔体积 $= d(\Lambda)$ ，密度 $= 1/d(\Lambda)$ ，换基用么模矩阵不改变格。
- 2 引理 12.1（闵可夫斯基一）：体积 $> 2^n$ 的中心椭球必含非零格点。
证法 = 半尺寸小球体积 > 1 必重叠 $\Rightarrow$ 近原点格点。
- 3 相继极小 $R_1 \leq \dots \leq R_n$ ：逐层往外找最近的新方向，是格的"指纹"。
- 4 引理 12.2（闵可夫斯基二）： $1 \leq R_1 \cdots R_n \leq 2^n/J_n$ ，即乘积 $\asymp 1$ （疏密守恒）。
- 5 引理 12.3：把极小点修成真正的下三角好基 $\mathbf{X}^{(\nu)}$ ，长度仍 $\asymp R_\nu$ 。
- 6 引理 12.4（主力）：半径 R 球内格点数 $\asymp R^\nu/(R_1 \cdots R_\nu)$ ；任意格在计数上等效于矩形格。
- 7 伴随格 + 引理 12.5（Mahler）： $R_\mu S_{n-\mu+1} \asymp 1$ ，格与对偶格疏密成倒数。
- 8 自伴随 $2n$ 维格（对称 γ ）：推出 $R_n \ll 1 \ll R_{n+1}$ 。
- 9 引理 12.6（终点）：解数 $N(Z)$ 随尺度缩小不会掉得比 $(Z_1/Z_2)^n$ 更快——三次型工作的直接工具。

脚注：原文中" $\mathbf{x}$ 垂直于 $\mathbf{y}$ "指从原点 O 到点 $\mathbf{x}$ 的向量垂直于从 O 到点 $\mathbf{y}$ 的向量，即内积 $x_1y_1 + \cdots + x_ny_n = 0$ 。

返回 [全书目录](#)