

数的几何

The geometry of numbers

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。

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：

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

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。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（幺模代换）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。

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 $d(\Lambda) = 1$ 。

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 $d(\Lambda) = d(M)$ 。

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。

证. 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 。 ■

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。

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

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

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。

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。

证. 我们可以绕 O 旋转 n 维空间, 直到

$$\begin{aligned} \mathbf{x}^{(1)} &= (x_1^{(1)}, 0, 0, \dots, 0), \\ \mathbf{x}^{(2)} &= (x_1^{(2)}, x_2^{(2)}, 0, \dots, 0), \\ &\vdots \\ \mathbf{x}^{(n)} &= (x_1^{(n)}, x_2^{(n)}, x_3^{(n)}, \dots, x_n^{(n)}). \end{aligned}$$

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

$$|x_1^{(1)} x_2^{(2)} \cdots x_n^{(n)}| \geq 1.$$

由于 $R_\nu = |\mathbf{x}^{(\nu)}| \geq |x_\nu^{(\nu)}|$, 我们得到 $R_1 R_2 \cdots R_n \geq 1$ 。

为得到 $R_1 R_2 \cdots R_n$ 的上界, 我们考虑椭圆

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

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。 ■

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。

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。

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 $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(n)}$ ：

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

其中

$$|\mathbf{X}^{(\nu)}| \asymp R_\nu \quad \text{且} \quad |X_\nu^{(\nu)}| \asymp R_\nu, \quad (12.2)$$

对 $\nu = 1, \dots, n$ 成立。

证. 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

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

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，它与 $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}$ 一起整数地生成 Λ 在该空间内的所有点。 $\mathbf{X}^{(3)}$ 的选取在可加上 $\mathbf{X}^{(1)}, \mathbf{X}^{(2)}$ 的任意倍数这一意义上是任意的。基于与前面相同的理由，我们有

$$N\mathbf{X}^{(3)} = u_1\mathbf{x}^{(1)} + u_2\mathbf{x}^{(2)} + u_3\mathbf{x}^{(3)}$$

对某些整数 $N > 0, u_1, u_2, u_3$ 成立。这一次我们不能断言 $u_3 = 1$ ，但可以断言 u_3 整除 N ，因为 $\mathbf{x}^{(3)}$ 可表为

$$\mathbf{x}^{(3)} = v_1\mathbf{X}^{(1)} + v_2\mathbf{X}^{(2)} + v_3\mathbf{X}^{(3)},$$

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

$$|\mathbf{X}^{(\nu)}| \leq \frac{\nu+1}{2}R_\nu \ll R_\nu, \quad (1 \leq \nu \leq n).$$

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 $|\mathbf{X}^{(\nu)}| \gg R_\nu$ 。或者，最后这个不等式也可由数 $R_1, \dots, R_n$ 的定义得出。 ■

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。

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 $R_\nu \leq R < R_{\nu+1}$ 中的 R_{n+1} 应略去。

证. 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

$$|u_j| \leq \frac{1}{\nu} \frac{R}{|\mathbf{X}^{(j)}|}, \quad (1 \leq j \leq \nu)$$

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

$$\gg \prod_{j=1}^{\nu} \frac{R}{|\mathbf{X}^{(j)}|} \gg \frac{R^\nu}{R_1 R_2 \cdots R_\nu},$$

这里用到了引理 12.3。

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

$$\mathbf{x} = v_1 \mathbf{X}^{(1)} + \cdots + v_\nu \mathbf{X}^{(\nu)}$$

其中 $v_1, \dots, v_\nu$ 为整数。对这样的点，我们有

$$\begin{aligned} x_\nu &= v_\nu X_\nu^{(\nu)}, \\ x_{\nu-1} &= v_\nu X_{\nu-1}^{(\nu)} + v_{\nu-1} X_{\nu-1}^{(\nu-1)}, \end{aligned}$$

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

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

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

$$(R_1, 0, 0, \dots, 0), (0, R_2, 0, \dots, 0), \dots, (0, 0, 0, \dots, R_n)$$

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。

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

$$x_1 y_1 + \dots + x_n y_n = u_1 v_1 + \dots + u_n v_n \quad (12.3)$$

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。

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

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

证. 设 $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ 为 Λ 的极小点（不一定是一组基），并设 $\mathbf{y}^{(1)}, \dots, \mathbf{y}^{(n)}$ 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¹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 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

$$R_\nu S_{n-\nu+1} \geq 1, \quad (1 \leq \nu \leq n). \quad (12.4)$$

相反方向的不等式由比较乘积得出。由于

$$R_1 \cdots R_n S_1 \cdots S_n \leq \left(\frac{2^n}{J_n} \right)^2$$

(由引理 12.2), 由 (12.4) 可得

$$R_\mu S_{n-\mu+1} \ll \left(\frac{2^n}{J_n} \right)^2, \quad (1 \leq \mu \leq n).$$

这就证明了引理 12.5。 ■

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。

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:

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

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

$$\mathbf{M} = (\Lambda^T)^{-1} = \begin{pmatrix} aI_n & -a\gamma^T \\ 0 & a^{-1}I_n \end{pmatrix}.$$

如果 $\gamma^T = \gamma$, 也就是说如果

$$\gamma_{ij} = \gamma_{ji} \quad \text{对所有 } i, j, \quad (12.5)$$

那么格 $\mathbf{M}$ 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 $y_{n+1}, \dots, y_{2n}$.

因此, 在条件 (12.5) 之下, $\mathbf{M}$ 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

$$R_n \ll 1 \ll R_{n+1}.$$

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。

引理 12.6. 设 $L_1, \dots, L_n$ 为线性型:

$$L_i = \gamma_{i1}u_1 + \dots + \gamma_{in}u_n, \quad (1 \leq i \leq n),$$

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

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

证. 这些不等式等价于

$$|x_1| < Z, \dots, |x_n| < Z, \quad |x_{n+1}| < Z, \dots, |x_{2n}| < Z$$

(对上面定义的 $2n$ 维格 Λ 的一般点 $(x_1, \dots, x_{2n})$)。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

$$N_0(Z) \leq N(Z) \leq N_0(\sqrt{2n} Z).$$

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

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll \left(\frac{Z_2}{Z_1} \right)^n, \quad (12.8)$$

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)。

设 $R_1, \dots, R_{2n}$ 表示 Λ 的相继极小。我们已经看到

$$R_n \ll 1 \ll R_{n+1}.$$

用下式定义 ν 与 μ :

$$R_\nu \leq Z_1 < R_{\nu+1}, \quad R_\mu \leq Z_2 < R_{\mu+1},$$

从而 $\nu \leq \mu$ 。由引理 12.4,

$$N_0(Z_1) \gg \frac{Z_1^\nu}{R_1 \cdots R_\nu} \quad \text{且} \quad N_0(Z_2) \ll \frac{Z_2^\mu}{R_1 \cdots R_\mu},$$

从而

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll \frac{Z_2^\mu}{Z_1^\nu R_{\nu+1} \cdots R_\mu}.$$

若 $\mu \leq n$, 则 (12.8) 成立, 因为右端

$$\leq \frac{Z_2^\mu}{Z_1^\mu} \leq \left(\frac{Z_2}{Z_1} \right)^\mu.$$

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

$$\frac{N_0(Z_2)}{N_0(Z_1)} \ll \frac{Z_2^\mu}{Z_1^\nu} \ll 1 \ll \left(\frac{Z_2}{Z_1} \right)^\mu.$$

这就证明了引理 12.6。 ■

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 $u_1 = \cdots = u_{2n} = 0$, 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 $2n - 1$ 。

1. 我们当然是指：从 O 到 $\mathbf{x}$ 的向量垂直于从 O 到 $\mathbf{y}$ 的向量。↵