朱尧辰 著

数的几何引论

An Introduction to the Geometry of Numbers

中国科学技术大学出版社

朱尧辰 著

数的几何引论

An Introduction to the Geometry of Numbers

中国科学技术大学出版社

内 容 简 介

数的几何是数论的一个经典分支.本书给出它的基本结果和一些数论应用.基本结果包括凸体和格的性质,Minkowski 第一和第二凸体定理,Minkowski-Hlawka 容许格定理,Mahler 列紧性定理,二次型的约化理论及堆砌与覆盖等;数论应用有四平方和定理及 Hurwitz 逼近定理等的证明.

本书以大学理工科有关专业高年级学生和研究生为主要对象,也可供有关研究人员参考.

图书在版编目(CIP)数据

数的几何引论/朱尧辰著. —合肥:中国科学技术大学出版社,2019.5
ISBN 978-7-312-04643-8

Ⅰ. 数… Ⅱ. 朱… Ⅲ. 数的几何 Ⅳ. O156.3

中国版本图书馆 CIP 数据核字(2019)第 010928 号

出版 中国科学技术大学出版社
安徽省合肥市金寨路 96 号,230026
http://press.ustc.edu.cn
https://zgkxjsdxcbs.tmall.com
印刷 合肥市宏基印刷有限公司
发行 中国科学技术大学出版社
经销 全国新华书店
开本 710 mm×1000 mm 1/16
印张 15.75
字数 309 千
版次 2019 年 5 月第 1 版
印次 2019 年 5 月第 1 次印刷
定价 45.00 元

前　言

数的几何是应用几何方法研究某些数论问题的一个数论分支, 也称几何数论. 就整体而言, 数的几何的研究对象具有互相关联的两个侧面: 算术侧面和几何侧面. 历史上, 首先出现的是算术的观点. 但早在 17~18 世纪间, J.-H. Lagrange 和 C. F. Gauss 等就已经开始以几何方法研究二次型的算术性质. 直到 1896 年, H. Minkowski 的 *Geometrie der Zahlen* (《数的几何》) 问世, 系统地确立了几何的观点, 建立了关于凸体的两个基本定理, 才奠定了数的几何作为一个独立的数论分支的地位. 我们可以将数的几何的基本问题表述为: 在什么条件下, 一个给定的凸体中含有非零整点? 也可以表述为: 在什么条件下, 对于空间中每个点 $\boldsymbol{z}$, 在一个给定的立体中存在点 $\boldsymbol{x}$, 使得 $\boldsymbol{x}-\boldsymbol{z}$ 是一个整点? 从 Minkowski 的开创性工作开始, 一直到 20 世纪 80 年代, 围绕基本问题的研究, 数的几何积累了丰硕的理论成果, 并且成为研究某些丢番图逼近和代数数论问题的重要数论工具. 它们大体上构成数的几何的经典部分.

目前以数的几何为主题的中文出版物很少. 本书是作者在大学数论专业课程讲稿基础上补充加工而成的, 以 Minkowski 凸体定理为主, 比较系统地给出经典数的几何的基本结果, 为大学理工科有关专业高年级学生和研究生进一步学习或从事研究工作提供一座桥梁, 也适当兼顾有关科研人员的参考需求.

本书含 8 章, 各章内容如下: 第 1 章和第 2 章给出关于 n 维凸体和格的基本概念和一些基本性质, 是全书的预备, 其中包含一些后文并不引用但在数的几何中具有基本意义的结果. 第 3 章研究一个凸体何时含有非零格点的问题. 首先证明 Blichfeldt 定理, 然后由此推出 Minkowski 第一凸体定理 (分别就 $\mathbb{Z}^n$ 情形和一般格的情形加以讨论), 并给出 Minkowski 线性型定理. 这一章其余部分给出 Minkowski 第一凸体定理在某些数论问题研究中的应用, 如格的特征的讨论, 用二次型表示整数问题 (四平方和定理等) 的数的几何解法. 第 4 章考虑一个凸体何时不含有非零格点的问题, 引进容许格和临界行列式的概念, 证明关于容许格

的存在性的 Minkowski-Hlawka 定理. 第 5 章的主题是 Minkowski 第二凸体定理. 首先比较一般地讨论距离函数, 然后简明地给出商空间 $\mathbb{R}^n/\Lambda$ (其中 Λ 是一个格) 上的测度概念, 进而引入相继极小的概念, 并证明 Minkowski 第二凸体定理, 最后给出上述基本结果到对偶凸集情形的扩充, 并且介绍 Mahler 复合体, 以及近些年来 W. M. Schmidt 和 L. Summerer 提出的“参数数的几何”. 第 6 章引进格序列收敛性概念, 证明 Mahler 列紧性定理 (或称 Mahler 选择定理). 第 7 章的主题通常称为二次型的约化理论, 首先讨论格与型的一般关系, 然后给出关于正定二次型的约化的基本定理, 并用于正定二次型绝对值的极小问题, 最后给出不定二元二次型情形的一些方法和结果, 并用来给出 Hurwitz 逼近定理的一种证明. 第 8 章是关于堆砌与覆盖的简明引论, 包括一些一般性的结果, 以及关于球格堆砌和球格覆盖的某些基本结果. 各章末附习题. 正文之后集中给出部分习题的解答或提示, 供读者参考.

从现有文献看, 数的几何的某些部分如覆盖与堆砌的当代发展 (包括在编码理论中的应用等) 突破了它的经典框架, 通常归于离散几何、计算几何以及凸几何 (甚至有时数的几何本身也被视作凸几何的一个组成部分), 所有这些都超出本书的预设目标. 对此我们只在参考文献中列出若干有关专著.

限于作者的水平, 书中存在谬误和不妥在所难免, 欢迎读者和同行批评指正.

朱尧辰

2018 年 6 月于北京

主要符号说明

1° $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$　依次为正整数集, 整数集, 有理数集, 实数集, 复数集.

$\mathbb{N}_0$　等于 $\mathbb{N}\cup\{0\}$.

$|S|$　有限集 S 所含元素的个数.

2° $[a]$ $(\lfloor a\rfloor)$　实数 a 的整数部分, 即不超过 a 的最大整数.

$\{a\}$　实数 a 的分数部分, 也称小数部分, 即 $\{a\}=a-[a]$.

$\lceil a\rceil$　大于或等于 a 的最小整数.

$\gcd(a_1,\cdots,a_n)$　整数 $a_1,\cdots,a_n$ 的最大公因子.

δ_{ij}　Kronecker 符号, 即当 $i=j$ 时其值为 1, 否则为 0.

$\operatorname{sgn}(a)$　实数 a 的符号函数 (其值等于 $+1$(若 $a>0$), -1(若 $a<0$), 或 0(若 $a=0$)).

3° $\log_b a$　实数 $a>0$ 的以 b 为底的对数.

$\log a$ (与 $\ln a$ 同义)　实数 $a>0$ 的自然对数.

$\exp(x)$　指数函数 e^x.

$\Gamma(x)$　伽马函数.

4° $(x_1,\cdots,x_n)^{\mathrm{T}}$　向量 $(x_1,\cdots,x_n)$ 的转置.

$\boldsymbol{x}\cdot\boldsymbol{y}$　向量 $\boldsymbol{x}=(x_1,\cdots,x_n),\boldsymbol{y}=(y_1,\cdots,y_n)\in\mathbb{R}^n$ 的内积 (数量积), 即 $x_1y_1+\cdots+x_ny_n$.

$|\boldsymbol{x}|$　向量 $\boldsymbol{x}=(x_1,\cdots,x_n)$ 的长, 即 $|\boldsymbol{x}|=(\boldsymbol{x}\cdot\boldsymbol{x})^{1/2}=(x_1^2+\cdots+x_n^2)^{1/2}$.

$(a_{ij})_{m\times n}$　第 i 行、第 j 列元素为 a_{ij} 的 $m\times n$ 矩阵.

$(a_{ij})_n$　第 i 行、第 j 列元素为 a_{ij} 的 n 阶方阵, 不引起混淆时可记为 (a_{ij}).

$\boldsymbol{I}_n$　n 阶单位方阵, 不引起混淆时可记为 $\boldsymbol{I}$.

$\boldsymbol{O}_n$　n 阶零方阵, 不引起混淆时可记为 $\boldsymbol{O}$.

$\operatorname{diag}(a_{11},a_{22},\cdots,a_{nn})$　n 阶对角方阵.

$(\boldsymbol{a}_1\ \ \boldsymbol{a}_2\ \ \cdots\ \ \boldsymbol{a}_n)$　由 n 维列向量 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n$ 组成的 n 阶方阵.

$\begin{pmatrix}\boldsymbol{a}_1\\ \vdots\\ \boldsymbol{a}_n\end{pmatrix}$ 由 n 维行向量 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n$ 组成的 n 阶方阵.

$\boldsymbol{A}^{\mathrm{T}},(a_{ij})^{\mathrm{T}}$ 方阵 $\boldsymbol{A}$ 和 (a_{ij}) 的转置.

$\det\boldsymbol{A},\det(\boldsymbol{A}),\det(a_{ij}),|\boldsymbol{A}|$ 方阵 $\boldsymbol{A}$ 或 (a_{ij}) 的行列式.

$\|\boldsymbol{\tau}\|$ $\mathbb{R}^n$ 中线性变换 $\boldsymbol{\tau}$ 的范数 (模), 若 $\boldsymbol{\tau}$ 对应的系数矩阵是 (τ_{ij}), 则 $\|\boldsymbol{\tau}\|=n\max\limits_{1\leqslant i,j\leqslant n}|\tau_{ij}|$.

5° $D(f)$ 二次型 f 的判别式 (行列式).

$M(f)$ 定义见 7.6 节的式 (10), 即 $M(f)=\inf\limits_{\boldsymbol{x}\in\mathbb{Z}^n\setminus\{\boldsymbol{0}\}}f(\boldsymbol{x})$.

6° $\mathcal{L},\mathcal{L}_n$ 所有 n 维格的集合.

$\Lambda_0,\Lambda_0^{(n)}$ 所有 n 维整点形成的格, 等同于 $\mathbb{Z}^n$.

$d(\Lambda)$ 格 Λ 的行列式, 定义见 2.1 节的式 (6).

$\Delta(\mathscr{S})$ 点集 $\mathscr{S}$ 的临界行列式 (格常数), 定义见 4.1 节的式 (1).

$F(\Lambda)$ 定义见 5.3 节的式 (1), 即 $F(\Lambda)=\inf\limits_{\boldsymbol{a}}F(\boldsymbol{a})$, 其中 F 是距离函数, $\boldsymbol{a}$ 遍历格 Λ 的所有非零格点.

$|\Lambda|$ 定义见 5.3 节的式(2), 即 $|\Lambda|=\inf\limits_{\boldsymbol{a}}|\boldsymbol{a}|$, 其中 $\boldsymbol{a}$ 遍历格 Λ 的所有非零格点.

$\delta(F)$ 定义见 5.3 节的式 (4), 即 $\delta(F)=\sup\limits_{\Lambda\in\mathcal{L}_n}\big(F(\Lambda)\big)^n/d(\Lambda)$.

$\widehat{\delta}(\mathscr{S},\mathcal{C}),\widehat{\delta}(\mathscr{S})$ 有界凸集 $\mathscr{S}$ 的 (平移) 堆砌 $\mathcal{C}$ 的密度.

$\delta(\mathscr{S})$ 有界凸集 $\mathscr{S}$ 的最密 (平移) 堆砌密度.

$\widehat{\delta}^*(\mathscr{S},\Lambda),\widehat{\delta}^*(\mathscr{S})$ 有界凸集 $\mathscr{S}$ 的格堆砌密度.

$\delta^*(\mathscr{S})$ 有界凸集 $\mathscr{S}$ 的最密格堆砌密度.

$\delta_n=\delta(\mathscr{S}_n)$ 最密球堆砌密度 ($\mathscr{S}_n$ 表示 n 维单位球).

$\delta_n^*=\delta^*(\mathscr{S}_n)$ 最密球格堆砌密度.

$\widehat{\vartheta}(\mathscr{S},\mathcal{C}),\widehat{\vartheta}(\mathscr{S})$ 有界凸集 $\mathscr{S}$ 的 (平移) 覆盖 $\mathcal{C}$ 的密度.

$\vartheta(\mathscr{S})$ 有界凸集 $\mathscr{S}$ 的最稀 (平移) 覆盖密度.

$\widehat{\vartheta}^*(\mathscr{S},\Lambda),\widehat{\vartheta}^*(\mathscr{S})$ 有界凸集 $\mathscr{S}$ 的格覆盖密度.

$\vartheta^*(\mathscr{S})$ 有界凸集 $\mathscr{S}$ 的最稀格覆盖密度.

$\vartheta_n=\vartheta(\mathscr{S}_n)$ 最稀球覆盖密度 ($\mathscr{S}_n$ 表示 n 维单位球).

$\vartheta_n^*=\vartheta^*(\mathscr{S}_n)$ 最稀球格覆盖密度.

$\Gamma(\mathscr{S})$ 点集 $\mathscr{S}$ 的覆盖常数, 定义见 8.2 节.

$\mu(\mathscr{S},\Lambda)$ 点集 $\mathscr{S}$ 对于格 Λ 的非齐次极小, 定义见 8.2 节.

$\mu_0(\mathscr{S})$ 点集 $\mathscr{S}$ 的下绝对非齐次极小, 定义见 8.2 节.

目　录

第 1 章　n 维点集

本章是全书的预备, 给出 n 维欧氏空间中整点和凸体及其他有关概念.

1.1　整　　点

我们将 $\mathbb{R}^n$ 中的点 $(x_1,\cdots,x_n)$ 等同于向量 $\boldsymbol{x}=(x_1,\cdots,x_n)$. 若 $(x_1,\cdots,x_n)\in\mathbb{R}^n$ 的所有分量都是整数, 则称它为一个整点, $\boldsymbol{x}$ 称为整向量. 若整数 $x_1,\cdots,x_n$ 不同时为零, 则 $(x_1,\cdots,x_n)$ 称为非零整点. 若非零整点 $\boldsymbol{x}=(x_1,\cdots,x_n)$ 的所有分量的最大公因子等于 1, 也就是说, 它不能表示为 $u\boldsymbol{x}'$ 的形式 (其中 u 是大于 1 的整数, $\boldsymbol{x}'$ 是非零整点), 则称它为本原整点 (简称本原点). 记 n 维向量

$$\boldsymbol{e}_1=(1,0,\cdots,0),\quad \boldsymbol{e}_2=(0,1,0,\cdots,0),\quad \cdots,\quad \boldsymbol{e}_n=(0,\cdots,0,1),$$

那么 $\boldsymbol{x}=(x_1,\cdots,x_n)$ 是一个整点, 当且仅当

$$\boldsymbol{x}=\sum_{i=1}^{n}x_i\boldsymbol{e}_i\quad (x_1,\cdots,x_n\in\mathbb{Z}).$$

$\mathbb{Z}^n$ 也记作 Λ_0.

设点集 $\mathscr{M}\subset\mathbb{R}^n$. 若对于任何 $\boldsymbol{x},\boldsymbol{y}\in\mathscr{M}$, 总有 $\boldsymbol{x}\pm\boldsymbol{y}\in\mathscr{M}$, 则称 $\mathscr{M}$ 是一个模. 因此, 若 $\mathscr{M}$ 是一个模, 则它含有点 $\boldsymbol{0}$, 并且 $\mathscr{M}$ 中任意有限多个点的整系数线性组合也在 $\mathscr{M}$ 中. 如果 $\boldsymbol{x}^{(i)}\,(i=1,2,\cdots,m)$ 是模 $\mathscr{M}$ 中的 m 个向量, 具有性质:

(i) 每个 $\boldsymbol{x}\in\mathscr{M}$ 可表示为 $\boldsymbol{x}=\sum\limits_{i=1}^{m}a_i\boldsymbol{x}^{(i)}$, $a_i\in\mathbb{Z}\,(i=1,\cdots,m)$,

(ii) 诸 $\boldsymbol{x}^{(i)}$ 在 $\mathbb{Q}$ 上线性无关, 即 $\sum_{i=1}^{m} a_i \boldsymbol{x}^{(i)} = \boldsymbol{0}, a_i \in \mathbb{Z}(i=1,\cdots,m) \Leftrightarrow a_i = 0$ $(i=1,\cdots,m)$,

则称 $\boldsymbol{x}^{(i)}(i=1,2,\cdots,m)$ 是模 $\mathscr{M}$ 的一组基.

可以证明 (参见文献 [9]): 如果 $\mathscr{M} \subseteq \mathbb{Z}^n$ 是一个模, 并且至少含有一个非零点, 则它必有一组下列形式的由 $m(\leqslant n)$ 个向量组成的基:

$$\boldsymbol{x}^{(i)} = (0,\cdots,0,x_{ii},\cdots,x_{in}), \quad x_{ii} \neq 0 \quad (i=1,\cdots,m).$$

显然 $\mathbb{Z}^n$ 本身是一个模, $\boldsymbol{e}_1,\cdots,\boldsymbol{e}_n$ 是它的一组基.

我们下面给出关于 2 维情形 (即平面整点) 的一些结果.

引理 1.1.1 设 $0 \leqslant a < b, y = f(x)$ 是 $[a,b]$ 上的连续函数, 那么在曲线 $y = f(x)$ 和区间 $[a,b]$ 以及直线 $x = a$ 和 $x = b$ 所围成的曲边梯形 T 内部和曲线边界上的整点个数为

$$N(T) = \sum_{n \in \mathbb{Z} \cap (a,b)} [f(n)].$$

证 设整数 $n \in (a,b)$, 记 $A = (n,0), B = (n,f(n))$, 那么线段 AB 上的整点个数为 $[f(n)]+1$(包括 A), 因此推出结论. □

例 1.1.1 设 $p,q > 2$ 是两个不相等的素数, 则

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{l=1}^{(q-1)/2} \left[\frac{lp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

证 考虑直角坐标平面上以 $O(0,0), A(p/2,0), B(p/2,q/2)$ 和 $C(0,q/2)$ 为顶点的矩形 Π 内部 (即不含边界) 的整点个数. 矩形对角线 OB 所在的直线方程是 $qx - py = 0$. 若整点 (ξ,η) 在此直线上, 则 $q\xi = p\eta$, 因为 p,q 互素, 所以 $p \mid \xi, q \mid \eta$, 于是 $\xi \geqslant p, \eta \geqslant q$, 从而 (ξ,η) 在矩形 Π 外部. 因此在 Π 的对角线 OB 上没有整点. 于是依引理 1.1.1, $\triangle OAB$ 内部的整点个数为

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right];$$

因为 $\triangle OCB$ 与 $\triangle OAB$ 全等, 所以 $\triangle OCB$ 内部的整点个数为

$$\sum_{l=1}^{(q-1)/2} \left[\frac{lp}{q}\right].$$

注意矩形 Π 内部的整点个数也等于

$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

于是得到结论.

例 1.1.2　设整数 $n \geqslant 1$, 则

$$\sum_{k=1}^{n}\left[\frac{n}{k}\right]=2\sum_{k=1}^{[\sqrt{n}]}\left[\frac{n}{k}\right]-[\sqrt{n}]^2.$$

证　应用引理 1.1.1 的证明的思路. 我们用不同方法计算满足 $xy \leqslant n$ 的正整数对 (x,y) 的个数 N.

一方面, 由 $xy \leqslant n$ 可知 $x,y \in \{1,2,\cdots,n\}$. 不等式 $xy \leqslant n$ 等价于 $x \leqslant n/y$. 当 $y=k(1 \leqslant k \leqslant n)$ 时, x 取 $[n/k]$ 个正整数值, 所以得到 $[n/k]$ 组正整数解 (x,y), 因此

$$N=\sum_{k=1}^{n}\left[\frac{n}{k}\right]. \tag{1}$$

另一方面, 换一种算法, 曲线 $xy=n$ 被点 $(\sqrt{n},\sqrt{n})$ 分为两部分. 当 $1 \leqslant x \leqslant \sqrt{n}$ 时得到满足 $xy \leqslant n$ 的正整数解 (x,y) 的组数等于

$$\sum_{x=1}^{[\sqrt{n}]}\left[\frac{n}{x}\right]. \tag{2}$$

当 $1 \leqslant y \leqslant \sqrt{n}$ 时得到满足 $xy \leqslant n$ 的正整数解 (x,y) 的组数等于

$$\sum_{y=1}^{[\sqrt{n}]}\left[\frac{n}{y}\right]. \tag{3}$$

式 (2) 和式 (3) 显然相等, 但都将以 $(1,1),(1,\sqrt{n}),(\sqrt{n},\sqrt{n}),(\sqrt{n},1)$ 为顶点的正方形 (包括边界) 中的整点算入, 它们总共有 $[\sqrt{n}]^2$ 个, 所以

$$N=2\sum_{k=1}^{[\sqrt{n}]}\left[\frac{n}{k}\right]-[\sqrt{n}]^2. \tag{4}$$

由式 (1) 和式 (4) 立得所要证的等式.

引理 1.1.2　在 2 维平面上, 若直线 $y=kx$ 的斜率是无理数, 则对于任何 $\varepsilon>0$, 该直线两边总存在整点与该直线的距离小于 ε.

证　直线方程是 $l: y=kx$, 其中 k 是无理数. 显然任何整点都不可能在 l 上. 设 (q,p) 是任意整点, 则它与 l 的距离

$$d=\frac{|kq-p|}{\sqrt{1+k^2}}>0.$$

由注 3.4.1 的 2° 知, 存在无穷多组整数 $(p,q)(q>0)$ 满足

$$|kq-p| \leqslant \frac{1}{q}.$$

对于给定的 $\varepsilon>0$, 存在 $(p,q)(q>0)$ 满足上述不等式并且 $q>1/\varepsilon\sqrt{1+k^2}$, 于是整点 $\pm(q,p)$ 与 l 的距离 $d<\varepsilon$. □

设 $O(0,0)$ 是坐标原点, $A(\xi,\eta)$ 是一个 (平面) 整点, 如果线段 OA 内部没有任何整点, 则称 A 是 (关于点 O 的) 可见点, 不然称 A 是隐藏点.

引理 1.1.3 (平面) 整点 $A(\xi,\eta)$ 是可见点, 当且仅当 ξ,η 互素.

证 我们不妨考虑第一象限. 若整点 $A(\xi,\eta)$ 的坐标不互素, 即 $k=\gcd(\xi,\eta)>1$, 则可设 $\xi=ka,\eta=kb$, 其中 $a,b\in\mathbb{N}$. 于是 $a<\xi,b<\eta,a/b=\xi/\eta$, 这表明点 (a,b) 在线段 OA 上, 从而 $A(\xi,\eta)$ 是隐藏点. 因此, 若 $A(\xi,\eta)$ 是可见点, 则 ξ,η 互素.

反之, 我们来证明: 若 ξ,η 互素, 则 $A(\xi,\eta)$ 是可见点. 用反证法. 设点 $A(\xi,\eta)$ 是隐藏点, 那么在线段 OA 上必然有一个可见点 (a,b). 于是依刚才所证, a,b 互素. 又由相似三角形性质可知

$$\frac{a}{b}=\frac{\xi}{\eta}, \tag{5}$$

并且

$$0<a<\xi,\quad 0<b<\eta. \tag{6}$$

由 $b\xi=a\eta$ 以及 a,b 互素推出 $a|\xi,b|\eta$. 于是有 $\xi=aa',\eta=bb'$, 其中 $a'>1,b'>1$ 是正整数, 从而由式 (5) 得到

$$\frac{a}{b}=\frac{\xi}{\eta}=\frac{aa'}{bb'},$$

因此 $a'=b'$. 进而由 $\xi=aa',\eta=bb'$ 及 a,b 互素推出 $\gcd(\xi,\eta)=a'>1$. 我们得到矛盾.

或者: 由 a,b 互素可知, 存在整数 m,n 满足

$$am+bn=1. \tag{7}$$

由式 (5) 解出 $a=b\xi/\eta$, 代入式 (7) 得到

$$b(\xi m+\eta n)=\eta. \tag{8}$$

类似地得到

$$a(\xi m+\eta n)=\xi. \tag{9}$$

因为 ξ,η 互素, 所以由式 (8) 和式 (9) 可知 $\xi m+\eta n=1$, 从而 $\xi=a,\eta=b$. 这与式 (6) 矛盾. □

注 1.1.1 关于 2 维平面中整点与任意闭曲线之间的关系, 有一些有趣的结果. 例如, 如果 C 是长度为 l 的封闭不自交的曲线, 它所围的区域 R 的面积为 A,R 内部的整点个数为 M, 以这些整点为顶点形成的完全被 C 包围的单位正方形的个数为 N, 那么:

(a) 若 $l \geqslant 1$, 则 $|A-N| < l$(Jarnik 定理, 见文献 [4]).

(b) 存在常数 $\beta > 0$, 使得 $0 \leqslant A-N \leqslant \beta l$. 若 α 表示满足此不等式的 β 的下确界, 则有

$$\frac{\pi+4}{2\pi} \leqslant \alpha \leqslant 3+\frac{2}{\gamma},$$

其中

$$\gamma = 6\pi\left(1+\sqrt{1+\frac{2}{9\pi}}\right)$$

(见文献 [54]).

其他有关结果可见文献 [43, 67].

1.2 列 紧 集

对于 $\mathbb{R}^n$ 中任意向量 $\boldsymbol{x} = (x_1, \cdots, x_n)$, 定义它的长为

$$|\boldsymbol{x}| = (\boldsymbol{x}\cdot\boldsymbol{x})^{1/2} = (x_1^2+\cdots+x_n^2)^{1/2}.$$

并定义两点 $\boldsymbol{x} = (x_1, \cdots, x_n), \boldsymbol{y} = (y_1, \cdots, y_n)$ 之间的 (欧氏) 距离为

$$|\boldsymbol{x}-\boldsymbol{y}| = \left((x_1-y_1)^2+\cdots+(x_n-y_n)^2\right)^{1/2}.$$

特别地, 有 $|\boldsymbol{x}| = |\boldsymbol{x}-\boldsymbol{0}|$. 有下列 "三角形不等式" 成立:

$$|\boldsymbol{x}+\boldsymbol{y}| \leqslant |\boldsymbol{x}|+|\boldsymbol{y}|.$$

设 $\boldsymbol{x} = (x_1, \cdots, x_n), \boldsymbol{y} = (y_1, \cdots, y_n) \in \mathbb{R}^n$,

$$y_i = \sum_{j=1}^{n} \alpha_{ij} x_j \quad (i = 1, \cdots, n) \tag{1}$$

是一个可逆实线性变换, 即 $\det(\alpha_{ij}) \neq 0$. 由 Cauchy 不等式推出

$$\begin{aligned} |\boldsymbol{y}|^2 &= \sum_{i=1}^{n}\left(\sum_{j=1}^{n}\alpha_{ij}x_j\right)^2 \leqslant \sum_{i=1}^{n}\left(\sum_{k=1}^{n}\alpha_{ik}^2\right)\left(\sum_{j=1}^{n}x_j^2\right) \\ &\leqslant n^2A^2\sum_{j=1}^{n}x_j^2 = n^2A^2|\boldsymbol{x}|^2, \end{aligned}$$

其中

$$A=\max_{1\leqslant i,j\leqslant n}|\alpha_{ij}|.$$

由变换的可逆性解出

$$x_i=\sum_{j=1}^{n}\beta_{ij}y_j\quad(i=1,\cdots,n).\tag{2}$$

于是, 类似地有

$$|\boldsymbol{x}|^2\leqslant n^2B^2|\boldsymbol{y}|^2,$$

其中

$$B=\max_{1\leqslant i,j\leqslant n}|\beta_{ij}|.$$

因而得到:

引理 1.2.1 设 $\boldsymbol{x},\boldsymbol{y}$ 如式 (1) 或式 (2) 给出, 则存在与 $\boldsymbol{x},\boldsymbol{y}$ 无关的常数 $c_1,c_2>0$, 使得

$$c_1|\boldsymbol{y}|\leqslant|\boldsymbol{x}|\leqslant c_2|\boldsymbol{y}|,$$

特别是当 $\boldsymbol{y}\neq\boldsymbol{0}$ 时,

$$c_1\leqslant\frac{|\boldsymbol{x}|}{|\boldsymbol{y}|}\leqslant c_2.$$

设 $\mathscr{R}\subset\mathbb{R}^n$. 若存在常数 C, 使得对于任意 $\boldsymbol{x}=(x_1,\cdots,x_n)\in\mathscr{R}$, 都有

$$|x_i|\leqslant C\quad(i=1,\cdots,n),$$

则称 $\mathscr{R}$ 是有界集, 否则是无界集.

我们称 $\mathbb{R}^n$ 中无穷点列 $\boldsymbol{x}_k(k=1,2,\cdots)$ 收敛于点 $\boldsymbol{x}$(极限点), 如果按通常意义 (见数学分析教程), 有

$$\lim_{k\to\infty}|\boldsymbol{x}_k-\boldsymbol{x}|=0.$$

显然, 对于任何 $\boldsymbol{a}=(a_1,\cdots,a_n)\in\mathbb{R}^n$, 有

$$\max_{1\leqslant j\leqslant n}|a_j|\leqslant|\boldsymbol{a}|\leqslant\sqrt{n}\max_{1\leqslant j\leqslant n}|a_j|.$$

将此不等式应用于点列 $\boldsymbol{x}_k-\boldsymbol{x}$, 可知: 点列 $\boldsymbol{x}_k(k=1,2,\cdots)$ 收敛于 $\boldsymbol{x}$, 当且仅当 $\boldsymbol{x}_k$ 的各个分量分别收敛于 $\boldsymbol{x}$ 的相应分量.

若 $\mathscr{R}$ 中任意一个无穷点列 $\boldsymbol{x}_n(n=1,2,\cdots)$ 的极限点也在 $\mathscr{R}$ 中, 则称 $\mathscr{R}$ 是闭集.

如果 $\mathscr{R}$ 中每个无穷点列 $\boldsymbol{x}_k(k=1,2,\cdots)$ 总含有一个在 $\mathscr{R}$ 中收敛的子列 $\boldsymbol{y}_{s_r}(s_1<s_2<\cdots)$:

$$\lim_{r\to\infty}\boldsymbol{y}_{s_r}=\boldsymbol{y}\in\mathscr{R},$$

那么称 $\mathscr{R}$ 为列紧集. 经典的 Weierstrass 列紧性定理表明: $\mathbb{R}^n$ 中的点集 $\mathscr{R}$ 是列紧的, 当且仅当它是有界闭集.

1.3 对称凸体

设点集 $\mathscr{R}\subseteq\mathbb{R}^n$. 若对于任意两点 $\boldsymbol{x},\boldsymbol{y}\in\mathscr{R}$ 及任何满足 $\lambda+\mu=1$ 的实数 $\lambda,\mu>0$, 都有

$$\lambda\boldsymbol{x}+\mu\boldsymbol{y}\in\mathscr{R},$$

即对于 $\mathscr{R}$ 中任意两点 $\boldsymbol{x},\boldsymbol{y}$, 连接此两点的线段

$$t\boldsymbol{x}+(1-t)\boldsymbol{y}\quad(0<t<1)$$

整个在 $\mathscr{R}$ 中, 则称 $\mathscr{R}$ 为 n 维凸集 (凸体). 此外, 如果对于位于 $\mathscr{R}$ 中或边界上的任何两点 $\boldsymbol{x},\boldsymbol{y}$, 上述线段上的点都是 $\mathscr{R}$ 的内点, 则称 $\mathscr{R}$ 是严格凸的.

首先给出凸集的一些简单性质:

1° 若 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_s$ 是凸集 $\mathscr{R}$ 的任意 $s(\geqslant 2)$ 个点, 并且

$$t_j\geqslant 0,\quad\sum_{j=1}^{s}t_j=1,$$

那么 $\sum\limits_{j=1}^{s}t_j\boldsymbol{x}_j\in\mathscr{R}$.

证　对 s 用数学归纳法. 对于 $s=2$, 当 $(t_1,t_2)=(1,0)$ 及 $(t_1,t_2)=(0,1)$ 时分别得到点 $\boldsymbol{x}_1$ 及 $\boldsymbol{x}_2$, 所以由定义可知 $s=2$ 时命题成立. 设当 $s=r(>2)$ 时命题成立. 若 $t_1+\cdots+t_{r+1}=1,t_j\geqslant 0$, 则 $t_j(1\leqslant j\leqslant r+1)$ 中有一个 (不妨设是) $t_1\neq 1$. 于是

$$t_1\boldsymbol{x}_1+\cdots+t_{r+1}\boldsymbol{x}_{r+1}=t_1\boldsymbol{x}_1+(1-t_1)\boldsymbol{y},$$

其中

$$\boldsymbol{y}=\frac{t_2}{1-t_1}\boldsymbol{x}_2+\cdots+\frac{t_{r+1}}{1-t_1}\boldsymbol{x}_{r+1}.$$

依归纳假设, $\boldsymbol{y}\in\mathscr{R}$. 因此 $t_1\boldsymbol{x}_1+(1-t_1)\boldsymbol{y}\in\mathscr{R}$, 即 $t_1\boldsymbol{x}_1+\cdots+t_{r+1}\boldsymbol{x}_{r+1}\in\mathscr{R}$. 于是完成归纳证明. □