理想、簇与算法

Ideals, Varieties, and Algorithms

原书第四版

原著作者 David Cox, John Little, Donal O'Shea

中文翻译 临江仙

更新发布 https://afdian.com/a/solitairemiya

更新日期 2026 年 4 月 7 日

惊鸿舟数海，一笔临江仙。

目录

第一章
几何、代数与算法

第 1 节　多项式与仿射空间

为建立代数与几何之间的联系，我们将研究域上的多项式. 虽然我们都知道什么是多项式，但**域**这个术语可能不太熟悉. 基本的直观理解是，域是一个在其中可以定义加法、减法、乘法和除法且具有通常性质的集合. 标准例子是实数 $\mathbb{R}$ 和复数 $\mathbb{C}$，而整数 $\mathbb{Z}$ 不是域，因为除法不成立（3 和 2 是整数，但它们的商 3/2 不是）. 域的正式定义可在附录 A 中找到.

域之所以重要，原因之一是线性代数在任何域上都成立. 因此，即使你的线性代数课程将标量限制在 $\mathbb{R}$ 或 $\mathbb{C}$ 中，你所学到的大多数定理和技术都适用于任意域 k. 在本书中，我们将为不同目的使用不同的域. 最常用的域是：

有理数 $\mathbb{Q}$：我们大多数计算机示例所用的域.

实数 $\mathbb{R}$：用于绘制曲线和曲面图像的域.

复数 $\mathbb{C}$：用于证明许多定理的域.

偶尔会遇到其他域，如有理函数域（将在后面定义）. 有限域也有一个很有趣的理论——见习题中一个较简单的例子.

现在可以定义多项式了. 读者当然熟悉单变量和双变量的多项式，但此处需要讨论 n 个变量 $x_1, \ldots, x_n$ 且系数在任意域 k 中的多项式. 首先定义**单项式**.

定义 1. $x_1, \ldots, x_n$ 中的**单项式**是指形如

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

的乘积，其中所有指数 $\alpha_1, \ldots, \alpha_n$ 都是非负整数. 该单项式的**总次数**是和 $\alpha_1 + \cdots + \alpha_n$.

可如下简化单项式的记号：记 $\alpha=(\alpha_1,\dots,\alpha_n)$ 为非负整数的 n 元组，并设

$$x^\alpha = x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdots x_n^{\alpha_n}.$$

当 $\alpha=(0,\dots,0)$ 时，注意 $x^\alpha=1$. 我们还用 $|\alpha|=\alpha_1+\cdots+\alpha_n$ 表示单项式 x^α 的总次数.

定义 2. $x_1,\dots,x_n$ 中系数在域 k 中的**多项式** f 是单项式的有限线性组合（系数在 k 中）. 我们将多项式 f 写成如下形式

$$f=\sum_\alpha a_\alpha x^\alpha,\quad a_\alpha\in k,$$

其中求和是对有限个 n 元组 $\alpha=(\alpha_1,\dots,\alpha_n)$ 进行的. $x_1,\dots,x_n$ 中系数在 k 中的所有多项式组成的集合记为 $k[x_1,\dots,x_n]$.

处理变量个数较少的多项式时，通常省略下标. 因此，单变量、双变量和多变量的多项式分别属于 $k[x]$、$k[x,y]$ 和 $k[x,y,z]$. 例如，

$$f=2x^3y^2z+\frac{3}{2}y^3z^3-3xyz+y^2$$

是 $\mathbb{Q}[x,y,z]$ 中的一个多项式. 通常用字母 f,g,h,p,q,r 来指代多项式.

处理多项式时，将使用以下术语.

定义 3. 设 $f=\sum_\alpha a_\alpha x^\alpha$ 是 $k[x_1,\dots,x_n]$ 中的一个多项式.

(i) 称 a_α 为单项式 x^α 的**系数**.

(ii) 如果 $a_\alpha\neq 0$，则称 $a_\alpha x^\alpha$ 为 f 的一个**项**.

(iii) $f\neq 0$ 的**总次数**，记为 $\deg(f)$，是使得系数 a_α 非零的最大的 $|\alpha|$. 零多项式的总次数未定义.

作为例子，上面给出的多项式 $f=2x^3y^2z+\frac{3}{2}y^3z^3-3xyz+y^2$ 有四项，总次数为六. 注意有两项具有最大的总次数，这在单变量多项式中是不可能发生的. 在第 2 章中，我们将研究如何对多项式的项进行排序.

两个多项式的和与积仍然是多项式. 若存在某个多项式 $h\in k[x_1,\dots,x_n]$ 使得 $g=fh$，则称多项式 f 整除多项式 g.

可以证明，在加法和乘法下，$k[x_1,\dots,x_n]$ 满足除乘法逆元存在性外的所有域公理（因为例如 $1/x_1$ 不是多项式）. 这样的数学结构称为**交换环**（完整定义见附录 A），因此我们将 $k[x_1,\dots,x_n]$ 称为**多项式环**.

下一个要考虑的主题是仿射空间.

定义 4. 给定域 k 和正整数 n，定义 k 上的 n 维**仿射空间**为集合

$$k^n=\{(a_1,\dots,a_n)\mid a_1,\dots,a_n\in k\}.$$

作为仿射空间的例子，考虑 $k = \mathbb{R}$ 的情况. 这里得到微积分和线性代数中熟悉的 $\mathbb{R}^n$ 空间. 一般地，称 $k^1 = k$ 为**仿射直线**，k^2 为**仿射平面**.

下面来看多项式与仿射空间的关系. 关键思想是，多项式 $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ 给出一个函数

$$f : k^n \longrightarrow k$$

定义如下：给定 $(a_1, \ldots, a_n) \in k^n$，在 f 的表达式中将每个 x_i 替换为 a_i. 由于所有系数也在 k 中，这一运算给出元素 $f(a_1, \ldots, a_n) \in k$. 能够将多项式视为函数，这使得建立代数与几何之间的联系成为可能.

多项式的这种双重性质有一些出人意料的后果. 例如，问题 "$f = 0$ 吗？" 现在有两种可能的含义：f 是零多项式吗？这意味着它的所有系数 a_α 都为零；还是 f 是零函数吗？这意味着对所有 $(a_1, \ldots, a_n) \in k^n$ 都有 $f(a_1, \ldots, a_n) = 0$. 令人惊讶的事实是，这两个命题在一般情况下并不等价. 关于它们如何可能不同的例子，考虑由 0 和 1 两个元素组成的集合. 在习题中，将看到这可以构成一个域，其中 $1 + 1 = 0$. 这个域通常称为 $\mathbb{F}_2$. 现在考虑多项式 $x^2 - x = x(x - 1) \in \mathbb{F}_2[x]$. 由于这个多项式在 0 和 1 处都为零，找到了一个非零多项式，它在仿射空间 $\mathbb{F}_2^1$ 上给出零函数. 其他例子将在习题中讨论.

然而，只要 k 是无限的，就没有问题.

命题 5. *设 k 是无限域，且 $f \in k[x_1, \ldots, x_n]$. 则 $f = 0$ 在 $k[x_1, \ldots, x_n]$ 中当且仅当 $f : k^n \to k$ 是零函数.*

证明. 证明的一个方向是显然的，因为零多项式显然给出零函数. 为证明逆命题，需证明若 $f(a_1, \ldots, a_n) = 0$ 对所有 $(a_1, \ldots, a_n) \in k^n$ 成立，则 f 是零多项式. 对变量个数 n 使用归纳法.

当 $n = 1$ 时，众所周知，$k[x]$ 中次数为 m 的非零多项式至多有 m 个不同的根（将在 §5 的推论 3 中证明这一事实）. 对于特定的 $f \in k[x]$，假设对所有 $a \in k$ 都有 $f(a) = 0$. 由于 k 是无限的，这意味着 f 有无穷多个根，因此 f 必须是零多项式.

现在假设逆命题对 $n - 1$ 成立，并设 $f \in k[x_1, \ldots, x_n]$ 是在 k^n 的所有点处都为零的多项式. 通过收集 x_n 的各次幂，可将 f 写成如下形式

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^i,$$

其中 $g_i \in k[x_1, \ldots, x_{n-1}]$. 将证明每个 g_i 都是 $n-1$ 个变量的零多项式，这将迫使 f 成为 $k[x_1, \ldots, x_n]$ 中的零多项式.

若固定 $(a_1, \ldots, a_{n-1}) \in k^{n-1}$，得到多项式 $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$. 根据对 f 的假设，这对每个 $a_n \in k$ 都为零. 从 $n = 1$ 的情况可知 $f(a_1, \ldots, a_{n-1}, x_n)$ 是 $k[x_n]$ 中的零多项式. 使用上面 f 的公式，看到 $f(a_1, \ldots, a_{n-1}, x_n)$ 的系数是 $g_i(a_1, \ldots, a_{n-1})$，因此对所有 i 都有 $g_i(a_1, \ldots, a_{n-1}) = 0$. 由于 $(a_1, \ldots, a_{n-1})$ 是在 k^{n-1} 中任意选取的，因此每个 $g_i \in k[x_1, \ldots, x_{n-1}]$ 在 k^{n-1} 上给出零函数.

归纳假设推出每个 g_i 都是 $k[x_1,\ldots,x_{n-1}]$ 中的零多项式. 这迫使 f 成为 $k[x_1,\ldots,x_n]$ 中的零多项式，从而完成了命题的证明. □

注意，在命题 5 的陈述中，断言 "$f=0$ 在 $k[x_1,\ldots,x_n]$ 中" 意味着 f 是零多项式，即 f 的每个系数都为零. 因此，用同一个符号 "0" 来表示 k 的零元素和 $k[x_1,\ldots,x_n]$ 中的零多项式. 上下文将清楚地表明指的是哪一个.

作为推论，两个无限域上的多项式相等，当且仅当它们在仿射空间上给出相同的函数.

推论 6. *设 k 是无限域，且 $f,g\in k[x_1,\ldots,x_n]$. 则 $f=g$ 在 $k[x_1,\ldots,x_n]$ 中当且仅当 $f:k^n\to k$ 和 $g:k^n\to k$ 是相同的函数.*

证明. 为证明非平凡的方向，假设 $f,g\in k[x_1,\ldots,x_n]$ 在 k^n 上给出相同的函数. 根据假设，多项式 $f-g$ 在 k^n 的所有点处都为零. 命题 5 推出 $f-g$ 是零多项式. 这证明了 $f=g$ 在 $k[x_1,\ldots,x_n]$ 中. □

最后，需要记录复数域 $\mathbb{C}$ 上多项式的一个特殊性质.

定理 7（代数基本定理）. *每个非常数多项式 $f\in\mathbb{C}[x]$ 在 $\mathbb{C}$ 中都有根.*

证明. 这就是代数基本定理，证明可在大多数复分析的入门教材中找到（尽管还有许多其他证明是已知的）. □

若域 k 上的每个非常数多项式在 $k[x]$ 中都有根，则称 k 是**代数闭的**. 因此 $\mathbb{R}$ 不是代数闭的（x^2+1 的根是什么?），而上述定理断言 $\mathbb{C}$ 是代数闭的. 在第 4 章中，将证明定理 7 的一个强有力的推广，称为 Hilbert 零点定理.

1.1.1 习题

(1) 设 $\mathbb{F}_2=\{0,1\}$，并定义加法和乘法为 $0+0=1+1=0$，$0+1=1+0=1$，$0\cdot 0=0\cdot 1=1\cdot 0=0$ 和 $1\cdot 1=1$. 解释为什么 $\mathbb{F}_2$ 是一个域.（你不必验证结合律和分配律，但应该验证单位元和逆元的存在性，包括加法和乘法的）.

(2) 设 $\mathbb{F}_2$ 是习题 1 中的域.

  (a) 考虑多项式 $g(x,y)=x^2y+y^2x\in\mathbb{F}_2[x,y]$. 证明对所有 $(x,y)\in\mathbb{F}_2^2$ 都有 $g(x,y)=0$，并解释为什么这不与命题 5 矛盾.

  (b) 在 $\mathbb{F}_2[x,y,z]$ 中找到一个在每一点 $\mathbb{F}_2^3$ 处都为零的非零多项式. 试着找一个包含所有三个变量的.

  (c) 在 $\mathbb{F}_2[x_1,\ldots,x_n]$ 中找到一个在每一点 $\mathbb{F}_2^n$ 处都为零的非零多项式. 你能找一个包含所有 $x_1,\ldots,x_n$ 的吗?

(3)（需要抽象代数）. 设 p 是素数. 模 p 的整数环是有 p 个元素的域，记为 $\mathbb{F}_p$.

(a) 解释为什么 $\mathbb{F}_p \setminus \{0\}$ 在乘法下是一个群.
(b) 使用 Lagrange 定理证明对所有 $a \in \mathbb{F}_p \setminus \{0\}$ 都有 $a^{p-1} = 1$.
(c) 证明对所有 $a \in \mathbb{F}_p$ 都有 $a^p = a$. 提示：分别处理 $a = 0$ 和 $a \neq 0$ 的情况.
(d) 在 $\mathbb{F}_p[x]$ 中找到一个在每一点 $\mathbb{F}_p$ 处都为零的非零多项式. 提示：使用 (c) 部分.

(4)（需要抽象代数）. 设 F 是有 q 个元素的有限域. 改写习题 3 的论证，证明 $x^q - x$ 是 $F[x]$ 中在每一点 F 处都为零的非零多项式. 这表明命题 5 对所有有限域都不成立.

(5) 在命题 5 的证明中，取 $f \in k[x_1, \ldots, x_n]$ 并将其写成系数在 $k[x_1, \ldots, x_{n-1}]$ 中关于 x_n 的多项式. 为看看这在具体情况下是什么样子，考虑多项式

$$f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3.$$

(a) 将 f 写成系数在 $k[y, z]$ 中关于 x 的多项式.
(b) 将 f 写成系数在 $k[x, z]$ 中关于 y 的多项式.
(c) 将 f 写成系数在 $k[x, y]$ 中关于 z 的多项式.

(6) 在 $\mathbb{C}^n$ 中，有子集 $\mathbb{Z}^n$，它由所有整数坐标的点组成.
(a) 证明若 $f \in \mathbb{C}[x_1, \ldots, x_n]$ 在每一点 $\mathbb{Z}^n$ 处都为零，则 f 是零多项式. 提示：改写命题 5 的证明.
(b) 设 $f \in \mathbb{C}[x_1, \ldots, x_n]$，并设 M 是 f 中出现的任何变量的最大幂次. 设 $\mathbb{Z}^n_{M+1}$ 是 $\mathbb{Z}^n$ 中所有坐标都在 1 到 $M + 1$ 之间（含）的点组成的集合. 证明若 f 在每一点 $\mathbb{Z}^n_{M+1}$ 处都为零，则 f 是零多项式.

第 2 节　仿射簇

现在可以定义本书研究的基本几何对象.

定义 1.. 设 k 是一个域，$f_1, \ldots, f_s$ 是 $k[x_1, \ldots, x_n]$ 中的多项式. 定义

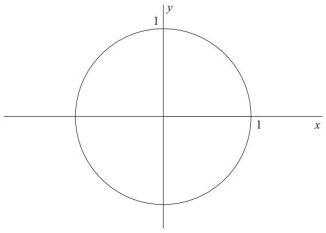
$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ 对所有} 1 \leqslant i \leqslant s\}.$$

称 $\mathbf{V}(f_1, \ldots, f_s)$ 为由 $f_1, \ldots, f_s$ 定义的**仿射簇**.

于是，仿射簇 $\mathbf{V}(f_1, \ldots, f_s) \subseteq k^n$ 就是方程组

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$$

的所有解的集合. 用字母 V, W 等来表示仿射簇. 本节的主要目的是向读者介绍大量例子，有些是新的，有些是熟悉的. 使用 $k = \mathbb{R}$ 以便能够画图.

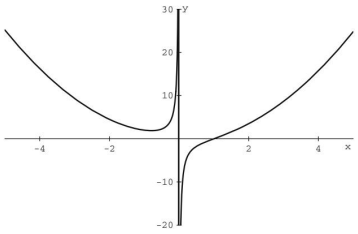


从平面 $\mathbb{R}^2$ 中的仿射簇 $\mathbf{V}(x^2+y^2-1)$ 开始，它是以原点为中心、半径为 1 的圆：

在学校学习的**圆锥曲线** (圆、椭圆、抛物线和双曲线) 都是仿射簇. 同样地，多项式函数的图像也是仿射簇 [函数 $y=f(x)$ 的图像是 $\mathbf{V}(y-f(x))$]. 虽然不那么显然，但有理函数的图像也是仿射簇. 例如，考虑函数

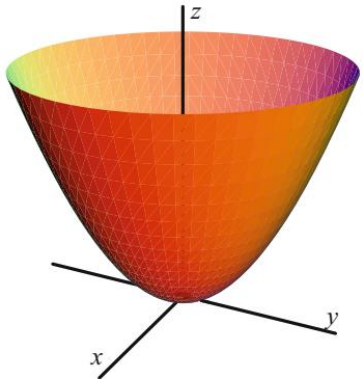
$$y=\frac{x^3-1}{x}$$

的图像：



容易验证这就是仿射簇 $\mathbf{V}(xy-x^3+1)$.

接下来，看看三维空间 $\mathbb{R}^3$. 一个很好的仿射簇是由旋转抛物面 $\mathbf{V}(z-x^2-y^2)$ 给出的，它是将抛物线 $z=x^2$ 绕 z 轴旋转得到的 (可用极坐标来验证这一点). 这提供了下图：

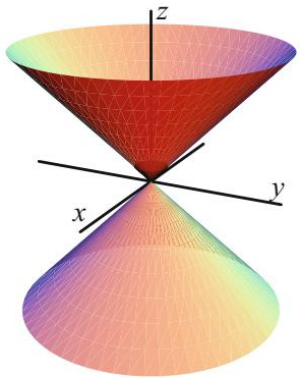


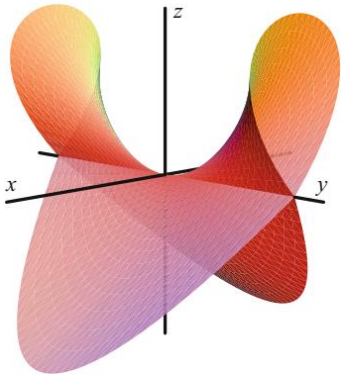
你可能也熟悉锥面 $\mathbf{V}(z^2-x^2-y^2)$：

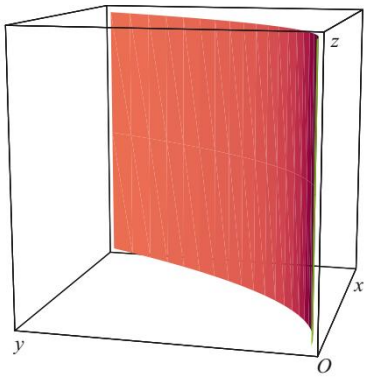
一个复杂得多的曲面由 $\mathbf{V}(x^2-y^2z^2+z^3)$ 给出：

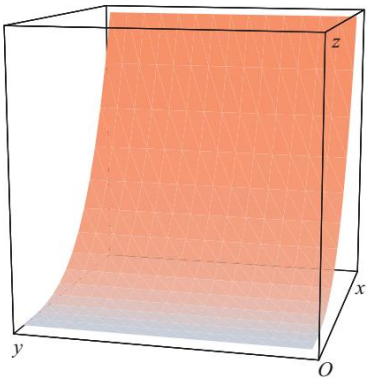
在最后这两个例子中，曲面并非处处光滑：锥面在原点有一个尖点，最后一个例子沿整个 y 轴自相交. 这些是**奇点**的例子，将在本书后面进行研究.

$\mathbb{R}^3$ 中曲线的一个有趣例子是三**次扭曲线**，即仿射簇 $\mathbf{V}(y-x^2,z-x^3)$. 为简单起见，只考虑位于第一卦限的部分. 首先，分别画出曲面 $y=x^2$ 和 $z=x^3$：

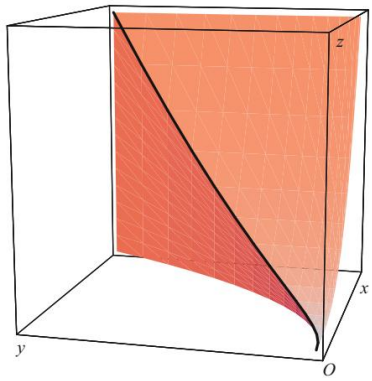

z
y
x


z
x
y

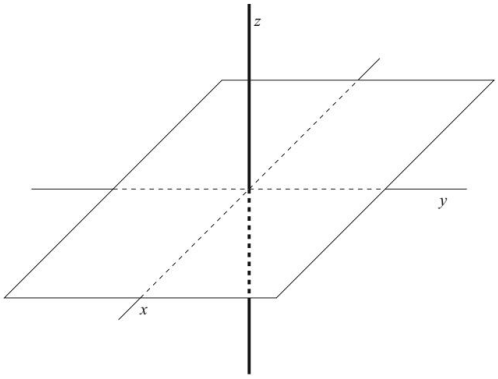

z
x
y
O


z
x
y
O

然后它们的交线就给出了三次扭曲线：



注意，当在 $\mathbb{R}^2$ 中有一个方程时，得到一条曲线，这是一个 1 维对象. 在 $\mathbb{R}^3$ 中也有类似的情况：$\mathbb{R}^3$ 中的一个方程通常给出一个曲面，其维数为 2. 同样，维数下降了 1. 但现在考虑三次扭曲线：这里 $\mathbb{R}^3$ 中的两个方程给出一条曲线，所以维数下降了 2. 由于每个方程都施加了一个额外的约束，直觉告诉我们每个方程使维数下降 1. 因此，如果从 $\mathbb{R}^4$ 开始，会希望由两个方程定义的仿射簇是一个曲面. 不幸的是，维数的概念比上述例子所暗示的更加微妙. 为说明这一点，考虑仿射簇 $\mathbf{V}(xz, yz)$. 容易验证方程 $xz = yz = 0$ 定义了 (x, y) 平面和 z 轴的并：



因此，这个仿射簇由两个具有不同维数的部分组成，其中一个部分 (平面) 按照上述直觉具有“错误” 的维数.

下面给出一些高维空间中仿射簇的例子. 一个熟悉的例子来自线性代数. 即固定一个域 k，考虑一个具有 k 中系数的 m 个线性方程、n 个未知数 $x_1, \ldots, x_n$ 的方程组：

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1, \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m. \end{aligned} \tag{1}$$

这些方程的解构成 k^n 中的一个仿射簇，称之为**线性簇**. 因此，直线和平面都是线性簇，还有任意大维数的例子. 在线性代数中，学习了行约化方法 (也称为 **Gauss 消元法**)，它给出了求解这种

方程组的算法. 在第 2 章中，将研究这种算法的一个推广，它适用于多项式方程组.

线性簇与关于维数的讨论密切相关. 即若 $V \subseteq k^n$ 是由 (1) 定义的线性簇，则 V 的维数不必是 $n-m$，尽管 V 由 m 个方程定义. 事实上，当 V 非空时，线性代数告诉我们 V 的维数是 $n-r$，其中 r 是矩阵 (a_{ij}) 的秩. 因此对于线性簇，维数由独立方程的个数决定. 这种直觉适用于更一般的仿射簇，只是 "独立" 的概念更加微妙.

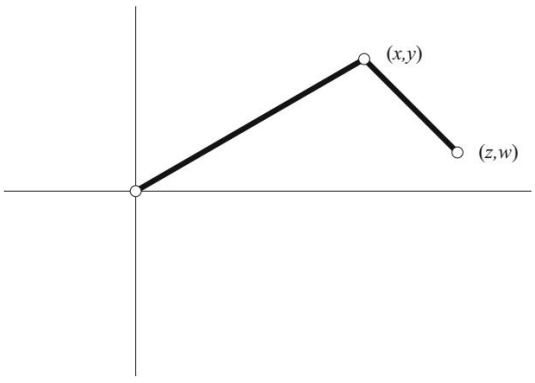
微积分中也有一些高维的复杂例子. 例如，假设想求函数 $f(x,y,z) = x^3 + 2xyz - z^2$ 在约束条件 $g(x,y,z) = x^2 + y^2 + z^2 = 1$ 下的最小值和最大值. **Lagrange 乘子**法指出，在局部极小值或极大值处有 $\nabla f = \lambda \nabla g$[回忆 f 的梯度是偏导数向量 $\nabla f = (f_x, f_y, f_z)$]. 这给出了以下关于四个未知数 x, y, z, λ 的四个方程的方程组：

$$\begin{aligned} 3x^2 + 2yz &= 2x\lambda, \\ 2xz &= 2y\lambda, \\ 2xy - 2z &= 2z\lambda, \\ x^2 + y^2 + z^2 &= 1. \end{aligned} \tag{2}$$

这些方程定义了 $\mathbb{R}^4$ 中的一个仿射簇，关于维数的直觉使希望它由有限多个点 (维数为 0) 组成，因为它由四个方程定义. 学生们常常觉得 Lagrange 乘子法很难，因为方程太难解了. 第 2 章的算法将为解决这类问题提供强大的工具. 特别是，将找到上述方程的所有解.

还应提到仿射簇可以是空集. 例如，当 $k = \mathbb{R}$ 时，显然 $\mathbf{V}(x^2 + y^2 + 1) = \emptyset$，因为 $x^2 + y^2 = -1$ 没有实数解 (尽管当 $k = \mathbb{C}$ 时有解). 另一个例子是 $\mathbf{V}(xy, xy - 1)$，无论域是什么它都是空的，因为给定的 x 和 y 不能同时满足 $xy = 0$ 和 $xy = 1$. 在第 4 章中，将研究一种确定 $\mathbb{C}$ 上仿射簇何时非空的方法.

为说明仿射簇的一些应用，考虑一个来自机器人学的简单例子. 假设在平面上有一个机器人手臂，由两根长度分别为 1 和 2 的连杆组成，较长的连杆固定在原点：



手臂的 "状态" 完全由图中标出的坐标 (x,y) 和 (z,w) 描述. 因此状态可以看作是一个 4 元组 $(x,y,z,w) \in \mathbb{R}^4$. 然而，并非所有 4 元组都能作为手臂的状态出现. 事实上，容易看出可能状态的

子集是 $\mathbb{R}^4$ 中由以下方程定义的仿射簇：

$$x^2 + y^2 = 4,$$

$$(x - z)^2 + (y - w)^2 = 1.$$

注意即使更大的维数也很容易进入：若考虑同一手臂在三维空间中的情况，则状态的仿射簇将由 $\mathbb{R}^6$ 中的两个方程定义. 本书将要发展的技术在机器人学理论中有一些重要的应用.

到目前为止，所有的图都是在 $\mathbb{R}$ 上的. 在本书后面，将考虑 $\mathbb{C}$ 上的仿射簇. 在这里，要获得这种仿射簇的几何直观更加困难 (但并非不可能).

最后，记录仿射簇的一些基本性质.

引理 2.. *若 $V, W \subseteq k^n$ 是仿射簇，则 $V \cup W$ 和 $V \cap W$ 也是仿射簇.*

证明. 假设 $V = \mathbf{V}(f_1, \ldots, f_s)$ 且 $W = \mathbf{V}(g_1, \ldots, g_t)$. 断言

$$V \cap W = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t),$$

$$V \cup W = \mathbf{V}(f_i g_j \mid 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t).$$

第一个等式很容易证明：在 $V \cap W$ 中意味着 $f_1, \ldots, f_s$ 和 $g_1, \ldots, g_t$ 都消失，这与 $f_1, \ldots, f_s, g_1, \ldots, g_t$ 都消失是一样的.

第二个等式需要多做一点工作. 若 $(a_1, \ldots, a_n) \in V$，则所有的 f_i 在这点消失，这意味着所有的 $f_i g_j$ 也在这点 $(a_1, \ldots, a_n)$ 消失. 于是 $V \subseteq \mathbf{V}(f_i g_j)$，类似地有 $W \subseteq \mathbf{V}(f_i g_j)$. 这证明了 $V \cup W \subseteq \mathbf{V}(f_i g_j)$. 反过来，选择 $(a_1, \ldots, a_n) \in \mathbf{V}(f_i g_j)$. 若这点在 V 中，则完成了，若不在，则存在某个 i_0 使得 $f_{i_0}(a_1, \ldots, a_n) \neq 0$. 由于 $f_{i_0} g_j$ 对所有 j 都在 $(a_1, \ldots, a_n)$ 处消失，g_j 必须在这点消失，证明了 $(a_1, \ldots, a_n) \in W$. 这表明 $\mathbf{V}(f_i g_j) \subseteq V \cup W$. □

这个引理意味着仿射簇的有限交和有限并仍然是仿射簇. 结果表明已经见过并和交的例子. 关于并，考虑仿射 3 空间中 (x, y) 平面和 z 轴的并. 根据上面的公式，有

$$\mathbf{V}(z) \cup \mathbf{V}(x, y) = \mathbf{V}(zx, zy).$$

这当然就是本节前面讨论的例子之一. 至于交，注意三次扭曲线是作为两个曲面的交给出的.

本节给出的例子引出了一些关于仿射簇的有趣问题. 假设有 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. 则：

- (相容性) 能否确定 $\mathbf{V}(f_1, \ldots, f_s) \neq \emptyset$，即方程 $f_1 = \cdots = f_s = 0$ 是否有公共解?
- (有限性) 能否确定 $\mathbf{V}(f_1, \ldots, f_s)$ 是否有限，若是，能否显式地找出所有解?
- (维数) 能否确定 $\mathbf{V}(f_1, \ldots, f_s)$ 的 “维数”?

这些问题的答案是肯定的，尽管在选择工作的域 k 时必须小心. 最难的是关于维数的问题，因为它涉及一些复杂的概念. 尽管如此，将对所有三个问题给出完整的解答.

1.2.1 习题

(1) 在 $\mathbb{R}^2$ 中画出下列仿射簇的草图：
   (a) $\mathbf{V}(x^2+4y^2+2x-16y+1)$
   (b) $\mathbf{V}(x^2-y^2)$
   (c) $\mathbf{V}(2x+y-1, 3x-y+2)$
   在每种情况下，该仿射簇是否具有你直观上期望的维数?

(2) 在 $\mathbb{R}^2$ 中，画出 $\mathbf{V}(y^2-x(x-1)(x-2))$ 的草图. 提示：对于哪些 x 可以解出 y? 每个 x 对应几个 y? 该曲线具有什么对称性?

(3) 在平面 $\mathbb{R}^2$ 中，画图说明

$$\mathbf{V}(x^2+y^2-4)\cap\mathbf{V}(xy-1)=\mathbf{V}(x^2+y^2-4, xy-1),$$

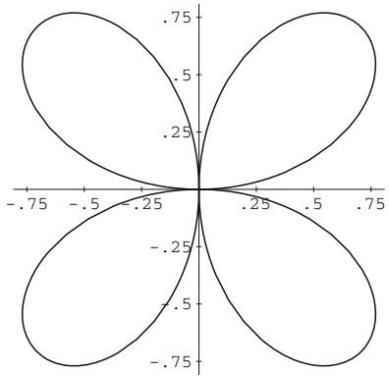
   并确定交点. 注意这是引理 2 的一个特例.

(4) 在 $\mathbb{R}^3$ 中画出下列仿射簇的草图：
   (a) $\mathbf{V}(x^2+y^2+z^2-1)$
   (b) $\mathbf{V}(x^2+y^2-1)$
   (c) $\mathbf{V}(x+2, y-1.5, z)$
   (d) $\mathbf{V}(xz^2-xy)$. 提示：将 xz^2-xy 因式分解
   (e) $\mathbf{V}(x^4-zx, x^3-yx)$
   (f) $\mathbf{V}(x^2+y^2+z^2-1, x^2+y^2+(z-1)^2-1)$
   在每种情况下，该仿射簇是否具有你直观上期望的维数?

(5) 使用引理 2 的证明，在 $\mathbb{R}^3$ 中画出 $\mathbf{V}((x-2)(x^2-y), y(x^2-y), (z+1)(x^2-y))$ 的草图. 提示：这是哪两个仿射簇的并?

(6) 证明 k^n 的所有有限子集都是仿射簇.
   (a) 证明单点 $(a_1, \ldots, a_n)\in k^n$ 是一个仿射簇.
   (b) 证明 k^n 的每个有限子集都是仿射簇. 提示：引理 2 会有用.

(7) 极坐标中最漂亮的例子之一是四叶玫瑰线
   这条曲线由极坐标方程 $r=\sin(2\theta)$ 定义. 将证明这条曲线是一个仿射簇.
   (a) 利用 $r^2=x^2+y^2$，$x=r\cos(\theta)$ 和 $y=r\sin(\theta)$，证明四叶玫瑰线包含在仿射簇 $\mathbf{V}((x^2+y^2)^3-4x^2y^2)$ 中. 提示：使用 $\sin(2\theta)$ 的一个恒等式.
   (b) 现在仔细论证 $\mathbf{V}((x^2+y^2)^3-4x^2y^2)$ 包含在四叶玫瑰线中. 这比看起来要棘手，因为在 $r=\sin(2\theta)$ 中 r 可以是负的.



结合 (a) 和 (b) 两部分，证明了四叶玫瑰线就是仿射簇 $\mathbf{V}((x^2+y^2)^3-4x^2y^2)$.

(8) 证明某物不是仿射簇可能需要一些工作. 例如，考虑集合

$$X=\{(x,x)\mid x\in\mathbb{R},x\neq 1\}\subseteq\mathbb{R}^2,$$

它是直线 $x=y$ 去掉点 $(1,1)$. 为证明 X 不是仿射簇，假设 $X=\mathbf{V}(f_1,\ldots,f_s)$. 则每个 f_i 在 X 上消失，若能证明 f_i 在 $(1,1)$ 也消失，就能得到所需的矛盾. 因此，要证明的是：若 $f\in\mathbb{R}[x,y]$ 在 X 上消失，则 $f(1,1)=0$. 提示：令 $g(t)=f(t,t)$，它是 $\mathbb{R}[t]$ 中的多项式. 现在应用 §1 中命题 5 的证明.

(9) 设 $R=\{(x,y)\in\mathbb{R}^2\mid y>0\}$ 是上半平面. 证明 R 不是仿射簇.

(10) 设 $\mathbb{Z}^n\subseteq\mathbb{C}^n$ 由具有整数坐标的点组成. 证明 $\mathbb{Z}^n$ 不是仿射簇. 提示：参见 §1 的练习题 6.

(11) 到目前为止，讨论了 $\mathbb{R}$ 或 $\mathbb{C}$ 上的仿射簇. 也可以考虑域 $\mathbb{Q}$ 上的仿射簇，尽管这里的问题往往要困难得多. 例如，设 n 是一个正整数，考虑由

$$x^n+y^n=1$$

定义的 $\mathbb{Q}^2$ 中的仿射簇 $F_n\subseteq\mathbb{Q}^2$. 注意当 x 或 y 为零时有一些明显的解. 称这些为平凡解. 一个有趣的问题是是否存在非平凡解.

(a) 证明若 n 是奇数，则 F_n 有两个平凡解；若 n 是偶数，则 F_n 有四个平凡解.

(b) 证明 F_n 对某个 $n\geqslant 3$ 有非平凡解当且仅当 Fermat 大定理是错误的.

Fermat 大定理指出，对于 $n\geqslant 3$，方程

$$x^n+y^n=z^n$$

没有 x,y,z 都是非零整数的解. 这个猜想的一般情形由 Andrew Wiles 于 1994 年使用一些非常复杂的数论方法证明. 这个证明极其困难.

(12) 找一本微积分书中的 Lagrange 乘子问题，并写下相应的方程组. 务必使用一个想要找到多项

式函数在多项式约束下的最小值或最大值的例子. 这样方程就定义了一个仿射簇，尽量找一个导致复杂方程的问题. 稍后将使用 Gröbner 基方法来解这些方程.

(13) 考虑 $\mathbb{R}^2$ 中的一个机器人手臂，它由长度分别为 3、2 和 1 的三根连杆组成. 长度为 3 的连杆固定在原点，长度为 2 的连杆连接在长度为 3 的连杆的自由端，长度为 1 的连杆连接在长度为 2 的连杆的自由端. 机器人手臂的 “手” 连接在长度为 1 的连杆的末端.
   (a) 画出机器人手臂的示意图.
   (b) 确定手臂的 “状态” 需要多少个变量?
   (c) 给出可能状态的仿射簇的方程.
   (d) 利用本节讨论的关于维数的直观概念，猜测状态仿射簇的维数应该是多少.

(14) 这个练习将研究练习题 13 中描述的机器人手臂的可能 “手” 位置.
   (a) 若 (u, v) 是手的位置，解释为什么 $u^2 + v^2 \leqslant 36$.
   (b) 假设将长度为 3 和长度为 2 的连杆之间的关节 “锁定” 形成直角，但允许另一个关节自由移动. 画图说明在这些构型中，(u, v) 可以是环形区域 $16 \leqslant u^2 + v^2 \leqslant 36$ 中的任意点.
   (c) 画图说明 (u, v) 可以是圆盘 $u^2 + v^2 \leqslant 36$ 中的任意点. 提示：分别考虑 $16 \leqslant u^2 + v^2 \leqslant 36$，$4 \leqslant u^2 + v^2 \leqslant 16$ 和 $u^2 + v^2 \leqslant 4$.

(15) 在引理 2 中，证明了若 V 和 W 是仿射簇，则它们的并 $V \cup W$ 和交 $V \cap W$ 也是仿射簇. 在这个练习中，将研究其他集合运算如何影响仿射簇.
   (a) 证明仿射簇的有限并和有限交仍然是仿射簇. 提示：归纳法.
   (b) 举例说明仿射簇的无限并不必是仿射簇. 提示：根据练习题 8–10，知道一些 k^n 的不是仿射簇的子集. 令人惊讶的是，仿射簇的无限交仍然是仿射簇. 这是 Hilbert 基定理的推论，将在第 2 章和第 4 章中讨论.
   (c) 举例说明两个仿射簇的集合差 $V \setminus W$ 不必是仿射簇.
   (d) 设 $V \subseteq k^n$ 和 $W \subseteq k^m$ 是两个仿射簇，令

$$V \times W = \{(x_1, \ldots, x_n, y_1, \ldots, y_m) \in k^{n+m} \mid (x_1, \ldots, x_n) \in V, (y_1, \ldots, y_m) \in W\}$$

   是它们的笛卡尔积. 证明 $V \times W$ 是 k^{n+m} 中的仿射簇. 提示：若 V 由 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ 定义，则可以将 $f_1, \ldots, f_s$ 看作 $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ 中的多项式，W 的情况类似. 证明这给出了笛卡尔积的定义方程.

第 3 节　仿射簇的参数化

本节讨论描述仿射簇 $\mathbf{V}(f_1, \ldots, f_s)$ 的点的问题. 这归结为是否存在一种方法 “写下” 多项式方程组 $f_1 = \cdots = f_s = 0$ 的解. 当解有限时，目标就是简单地把它们全部列出. 但如果有无穷多个解时，该怎么办呢? 将看到，这个问题引出了仿射簇参数化的概念.

先从一个线性代数的例子开始. 设域为 $\mathbb{R}$，考虑方程组

$$x + y + z = 1, \tag{1}$$

$$x + 2y - z = 3.$$

从几何上看，这表示 $\mathbb{R}^3$ 中的一条直线，它是平面 $x + y + z = 1$ 和 $x + 2y - z = 3$ 的交线. 由此可见有无穷多解. 为描述这些解，对 (1) 式进行行变换，得到等价方程

$$x + 3z = -1,$$

$$y - 2z = 2.$$

记 $z = t$，其中 t 是任意的，这意味着 (1) 的所有解由

$$x = -1 - 3t,$$

$$y = 2 + 2t, \tag{2}$$

$$z = t$$

给出，其中 t 取遍 $\mathbb{R}$. 称 t 为参数，因此 (2) 就是 (1) 的解的参数化.
为看看参数化解的想法是否可以应用于其他仿射簇，来看单位圆的例子

$$x^2 + y^2 = 1. \tag{3}$$

参数化圆的一种常用方法是使用三角函数：

$$x = \cos(t),$$

$$y = \sin(t).$$

还有一种更代数化的方法来参数化这个圆：

$$x = \frac{1 - t^2}{1 + t^2},$$

$$y = \frac{2t}{1 + t^2}. \tag{4}$$

读者应该验证由这些方程定义的点在圆 (3) 上. 有趣的是，这种参数化并不能描述整个圆：由于 $x = \frac{1-t^2}{1+t^2}$ 永远不可能等于 -1，点 $(-1, 0)$ 没有被覆盖到. 在本节末尾，将解释如何得到这种参数

化.

注意方程 (4) 涉及多项式的商. 这些是**有理函数**的例子，在说明什么是簇的参数化之前，需要先定义有理函数的一般概念.

定义 1.. 设 k 是一个域. k 上以 $t_1,\dots,t_m$ 为变元的**有理函数**是两个多项式 $f,g\in k[t_1,\dots,t_m]$ 的商 f/g，其中 g 不是零多项式. 此外，两个有理函数 f/g 和 f'/g' 相等当且仅当 $g'f=gf'$ 在 $k[t_1,\dots,t_m]$ 中成立. 最后，所有 k 上以 $t_1,\dots,t_m$ 为变元的有理函数的集合记为 $k(t_1,\dots,t_m)$.

不难证明有理函数的加法和乘法是良定义的，且 $k(t_1,\dots,t_m)$ 是一个域. 将不加证明地承认这些事实.

现在假设给定一个簇 $V=\mathbf{V}(f_1,\dots,f_s)\subseteq k^n$. 则 V 的一个**有理参数表示**由有理函数 $r_1,\dots,r_n\in k(t_1,\dots,t_m)$ 组成，使得由

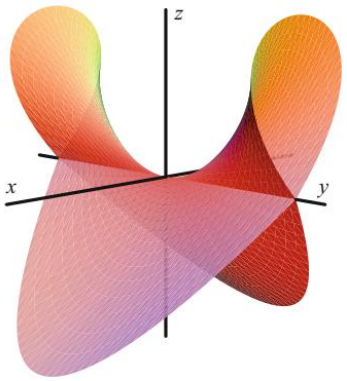
$$\begin{aligned} x_1&=r_1(t_1,\dots,t_m),\\ x_2&=r_2(t_1,\dots,t_m),\\ &\vdots\\ &\vdots\\ x_n&=r_n(t_1,\dots,t_m) \end{aligned}$$

给出的点落在 V 中. 还要求 V 是包含这些点的 “最小” 簇. 如圆的例子所示，参数化可能无法覆盖 V 的所有点. 在第 3 章中，将对 “最小” 的含义给出更精确的定义.

在许多情况下，有簇 V 的参数化，其中 $r_1,\dots,r_n$ 是多项式而不是有理函数. 这就是 V 的**多项式参数表示**.

相比之下，V 的原始定义方程 $f_1=\cdots=f_s=0$ 称为 V 的**隐式表示**. 在前面的例子中，注意 (1) 和 (3) 是簇的隐式表示，而 (2) 和 (4) 是参数表示.

参数表示曲线或曲面的一个主要优点是便于在计算机上绘制. 给定参数化的公式，计算机对参数的各种取值进行计算，然后绘制出得到的点. 例如，在 §2 中观察过曲面 $\mathbf{V}(x^2-y^2z^2+z^3)$:



这幅图不是使用隐式表示 $x^2 - y^2z^2 + z^3 = 0$ 绘制的. 相反，使用了由下式给出的参数表示

$$\begin{aligned} x &= t(u^2 - t^2), \\ y &= u, \\ z &= u^2 - t^2. \end{aligned} \tag{5}$$

由于描述的是一个曲面，所以有两个参数 t 和 u，上面的图是使用范围 $-1 \leqslant t, u \leqslant 1$ 绘制的. 在习题中，将推导这个参数化并验证它覆盖了整个曲面 $\mathbf{V}(x^2 - y^2z^2 + z^3)$.

同时，拥有簇的隐式表示往往也是有用的. 例如，假设想知道点 $(1, 2, -1)$ 是否在上面提到的曲面上. 若只有参数化 (5)，则要回答这个问题，就需要求解方程组

$$\begin{aligned} 1 &= t(u^2 - t^2), \\ 2 &= u, \\ -1 &= u^2 - t^2 \end{aligned} \tag{6}$$

关于 t 和 u. 另一方面，若有隐式表示 $x^2 - y^2z^2 + z^3 = 0$，则只需代入这个方程即可. 由于

$$1^2 - 2^2(-1)^2 + (-1)^3 = 1 - 4 - 1 = -4 \neq 0,$$

可知 $(1, 2, -1)$ 不在该曲面上 [因此方程组 (6) 无解].

拥有这两种表示法的愿望引出了以下两个问题：

(参数化) 是否每个仿射簇都有有理参数表示?

(隐式化) 给定仿射簇的参数表示，能否找到定义方程（即能否找到隐式表示)?

第一个问题的答案是否定的. 事实上，大多数仿射簇都不能用这里描述的方法进行参数化. 那些可以参数化的称为**单有理的**簇. 一般来说，判断给定的簇是否是单有理的是很困难的. 第二个问题的情况要好得多. 在第 3 章中，将看到答案总是肯定的：给定参数表示，总能找到定义方程.

来看一个隐式化如何工作的例子. 考虑参数表示

$$\begin{aligned} x &= 1 + t, \\ y &= 1 + t^2. \end{aligned} \tag{7}$$

这描述了平面上的一条曲线，但目前还不能确定它是否位于某个仿射簇上. 为找到要找的方程，注意可以从第一个方程解出 t，得到

$$t = x - 1.$$

代入第二个方程得到

$$y = 1 + (x-1)^2 = x^2 - 2x + 2.$$

因此参数方程 (7) 描述了仿射簇 $\mathbf{V}(y - x^2 + 2x - 2)$.

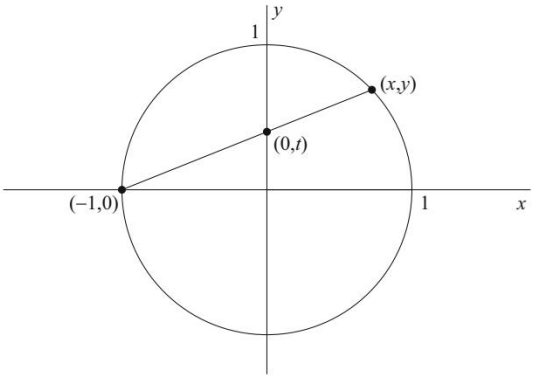
在上面的例子中，注意基本策略是消去变量 t，使只剩下一个只涉及 x 和 y 的方程. 这说明了**消元理论**所起的作用，将在第 3 章中更详细地研究这一理论.

接下来将讨论两个如何用几何方法参数化簇的例子. 从单位圆 $x^2 + y^2 = 1$ 开始，它通过 (4) 被参数化为

$$x = \frac{1-t^2}{1+t^2},$$

$$y = \frac{2t}{1+t^2}.$$

为看看这个参数化从何而来，注意每条过点 $(-1,0)$ 的非垂直直线将与圆交于唯一点 (x,y):



每条非垂直直线也与 y 轴相交，在上图中这就是点 $(0,t)$.

这给出了圆的一个几何参数化：给定 t，画一条连接 $(-1,0)$ 和 $(0,t)$ 的直线，令 (x,y) 为这条直线与 $x^2+y^2=1$ 的交点. 注意前面这句话确实给出了一个参数化：当 t 在纵轴上从 $-\infty$ 变到 $+\infty$ 时，对应的点 (x,y) 遍历整个圆，除了点 $(-1,0)$.

现在需要找到用 t 表示 x 和 y 的显式公式. 为此，考虑上图中直线的斜率. 可以用两种方式计算斜率，使用点 $(-1,0)$ 和 $(0,t)$，或者点 $(-1,0)$ 和 (x,y). 这给出了方程

$$\frac{t-0}{0-(-1)} = \frac{y-0}{x-(-1)},$$

化简为

$$t = \frac{y}{x+1}.$$

因此，$y = t(x+1)$. 若代入 $x^2+y^2=1$，得到

$$x^2 + t^2(x+1)^2 = 1,$$

这给出了二次方程

$$(1+t^2)x^2+2t^2x+t^2-1=0. \tag{8}$$

这个方程给出了直线与圆的交点的 x 坐标，它是二次的，因为有两个交点. 其中一个点是 -1，所以 $x+1$ 是 (8) 的一个因式. 现在很容易找到另一个因式，可以将 (8) 改写为

$$(x+1)\left((1+t^2)x-(1-t^2)\right)=0.$$

由于想要的 x 坐标由第二个因式给出，得到

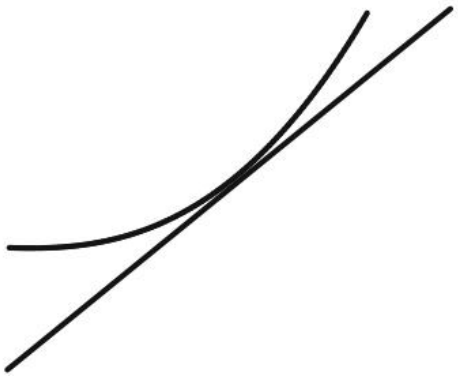
$$x=\frac{1-t^2}{1+t^2}.$$

此外，$y=t(x+1)$ 很容易导出

$$y=\frac{2t}{1+t^2}$$

(读者应该验证这一点)，这样就推导出了前面给出的参数化. 注意几何方法如何准确地告诉我们圆被覆盖的部分.

对于第二个例子，考虑来自 §2 的三次扭曲线 $\mathbf{V}(y-x^2,z-x^3)$. 这是三维空间中的一条曲线，通过观察曲线的切线，将得到一个有趣的曲面. 思路如下. 给定曲线上的一个点，可以画出该点的切线：



现在想象取三次扭曲线所有点处的切线. 这给出了如下曲面：

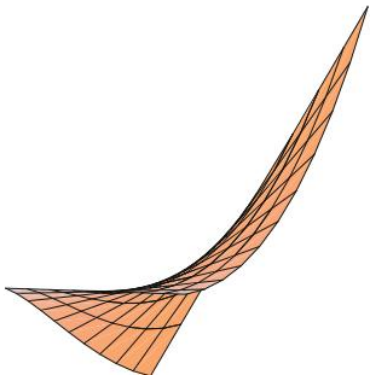
这幅图显示了几条切线. 上面的曲面称为三次扭曲线的**切曲面**.

为将这个几何描述转化为更代数化的形式，注意在 $y-x^2=z-x^3=0$ 中令 $x=t$ 得到三次扭曲线的一个参数化

$$x=t,$$

$$y=t^2,$$

$$z=t^3.$$



将这写成 $\mathbf{r}(t) = (t, t^2, t^3)$. 现在固定一个特定的 t 值，这给出曲线上的一个点. 由微积分可知，曲线在 $\mathbf{r}(t)$ 给出的点处的切向量是 $\mathbf{r}'(t) = (1, 2t, 3t^2)$. 由此可知切线被参数化为

$$\mathbf{r}(t) + u\mathbf{r}'(t) = (t, t^2, t^3) + u(1, 2t, 3t^2) = (t + u, t^2 + 2tu, t^3 + 3t^2u),$$

其中 u 是沿切线移动的参数. 如果现在让 t 变化，就可以通过

$$x = t + u,$$

$$y = t^2 + 2tu,$$

$$z = t^3 + 3t^2u$$

来参数化整个切曲面. 参数 t 和 u 有如下解释：t 告诉我们位于曲线上的哪个位置，而 u 告诉我们位于切线上的哪个位置. 这个参数化被用来绘制前面呈现的切曲面图.

最后一个问题涉及切曲面的隐式表示：如何找到它的定义方程？这是前面提到的隐式化问题的特例，等价于从上面的参数方程中消去 t 和 u. 在第 2 章和第 3 章中，将看到有一个算法可以做到这一点，特别是将证明三次扭曲线的切曲面由方程

$$x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2 = 0$$

定义.

将以计算机辅助几何设计（CAGD）中的一个例子来结束本节. 在设计汽车引擎盖或飞机机翼等复杂形状时，设计工程师需要形状多样、易于描述且绘制迅速的曲线和曲面. 涉及多项式和有理函数的参数方程满足这些要求；关于这个主题有大量文献.

为简单起见，假设一位设计工程师想要描述平面上的一条曲线. 复杂曲线通常是通过连接较简单的片段来创建的，为了使片段光滑连接，切线方向必须在端点处匹配. 因此，对于每个片段，设计师需要控制以下几何数据：

曲线的起点和终点；
起点和终点处的切线方向.

由雷诺汽车设计师 P. Bézier 引入的 **Bézier 三次曲线**特别适合这一目的. Bézier 三次曲线由方程

$$\begin{aligned} x &= (1-t)^3x_0 + 3t(1-t)^2x_1 + 3t^2(1-t)x_2 + t^3x_3, \\ y &= (1-t)^3y_0 + 3t(1-t)^2y_1 + 3t^2(1-t)y_2 + t^3y_3 \end{aligned} \tag{9}$$

参数化给出，其中 $0 \leqslant t \leqslant 1$，而 $x_0, y_0, x_1, y_1, x_2, y_2, x_3, y_3$ 是由设计工程师指定的常数. 看看这些常数如何与上述几何数据相对应.

如果在 $t = 0$ 和 $t = 1$ 处计算上面的公式，得到

$$(x(0), y(0)) = (x_0, y_0),$$

$$(x(1), y(1)) = (x_3, y_3).$$

当 t 从 0 变到 1 时，方程 (9) 描述了一条从 (x_0, y_0) 开始、到 (x_3, y_3) 结束的曲线. 这给出了所需数据的一半. 接下来将用微积分来求 $t = 0$ 和 $t = 1$ 处的切线方向. 知道 $t = 0$ 时 (9) 的切向量是 $(x'(0), y'(0))$. 为计算 $x'(0)$，对 (9) 的第一式求导得到

$$x' = -3(1-t)^2x_0 + 3((1-t)^2 - 2t(1-t))x_1 + 3(2t(1-t) - t^2)x_2 + 3t^2x_3.$$

代入 $t = 0$ 得到

$$x'(0) = -3x_0 + 3x_1 = 3(x_1 - x_0),$$

从这里开始，直接可得

$$(x'(0), y'(0)) = 3(x_1 - x_0, y_1 - y_0), \tag{10}$$

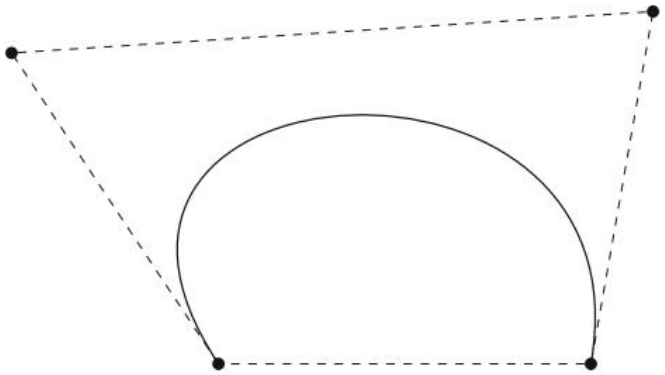
$$(x'(1), y'(1)) = 3(x_3 - x_2, y_3 - y_2).$$

由于 $(x_1 - x_0, y_1 - y_0) = (x_1, y_1) - (x_0, y_0)$，可知 $(x'(0), y'(0))$ 是从 (x_0, y_0) 到 (x_1, y_1) 的向量的三倍. 因此，通过放置 (x_1, y_1)，设计师可以控制曲线起点处的切线方向. 类似地，(x_2, y_2) 的放置控制了曲线终点处的切线方向.

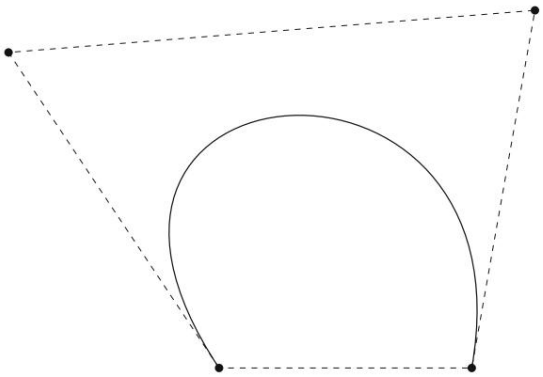
点 $(x_0, y_0), (x_1, y_1), (x_2, y_2)$ 和 (x_3, y_3) 称为 Bézier 三次曲线的**控制点**. 它们通常记为 P_0, P_1, P_2 和 P_3，它们确定的凸四边形称为**控制多边形**. 下面是一幅 Bézier 曲线及其控制多边形的图片：

在习题中，将证明 Bézier 三次曲线总是位于其控制多边形内部.

因此，确定 Bézier 三次曲线的数据易于指定且具有强烈的几何意义. 到目前为止尚未解决的一个问题是切向量 $(x'(0), y'(0))$ 和 $(x'(1), y'(1))$ 的长度. 根据 (10)，可以在不改变切线方向的情况下



改变点 (x_1, y_1) 和 (x_2, y_2). 例如，如果保持与前一幅图相同的方向，但增加切向量的长度，则得到如下曲线：



因此，增加端点处的速度会使曲线在更长的一段距离上保持接近切线. 通过练习和经验，设计师可以熟练使用 Bézier 三次曲线创建各种曲线. 有趣的是，设计师可能永远不知道用于描述曲线的方程 (9).

除了 CAGD，还应提到 Bézier 三次曲线也用于页面描述语言 PostScript 中. PostScript 中的 curveto 命令以控制点的坐标作为输入，输出 Bézier 三次曲线. 上面的 Bézier 三次曲线就是这样绘制的——每条曲线都在 PostScript 文件中通过单个 curveto 指令指定.

1.3.1 习题

(1) 参数化线性方程

$$x + 2y - 2z + w = -1,$$

$$x + y + z - w = 2$$

的所有解.

(2) 使用三角恒等式证明

$$x = \cos(t),$$

$$y = \cos(2t)$$

参数化了抛物线的一部分. 指明具体覆盖了抛物线的哪一部分.

(3) 给定 $f \in k[x]$，求 $\mathbf{V}(y - f(x))$ 的一个参数化.

(4) 考虑参数表示

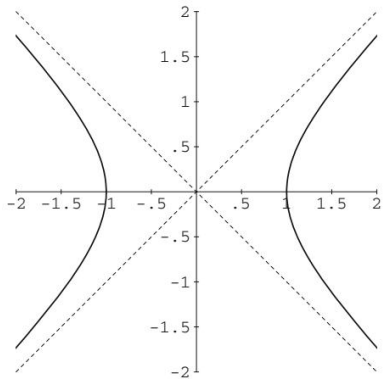
$$x = \frac{t}{1+t},$$

$$y = 1 - \frac{1}{t^2}.$$

(a) 求由上述参数方程确定的仿射簇的方程.

(b) 证明上述方程参数化了第 (a) 部分中找到的簇的所有点，除了点 $(1, 1)$.

(5) 本题研究双曲线 $x^2 - y^2 = 1$.



(a) 正如三角函数用于参数化圆一样，双曲函数用于参数化双曲线. 证明点

$$x = \cosh(t),$$

$$y = \sinh(t)$$

总是在 $x^2 - y^2 = 1$ 上. 覆盖了双曲线的哪一部分?

(b) 证明一条直线与双曲线相交于 0、1 或 2 个点，并用图说明你的答案. 提示：分别考虑 $x = a$ 和 $y = mx + b$ 的情况.

(c) 仿照用于圆 $x^2 + y^2 = 1$ 的论证，推导双曲线的参数化. 提示：考虑过双曲线上点 $(-1, 0)$ 的非垂直线.

(d) 你在第 (c) 部分找到的参数化对两个 t 值无定义. 解释这与双曲线的渐近线有何关系.

(6) 本题的目标是证明三维空间中的球面 $x^2 + y^2 + z^2 = 1$ 可以被参数化为

$$x = \frac{2u}{u^2 + v^2 + 1},$$

$$y = \frac{2v}{u^2+v^2+1},$$
$$z = \frac{u^2+v^2-1}{u^2+v^2+1}.$$

思路是将用于圆 $x^2+y^2=1$ 的论证推广到三维空间.

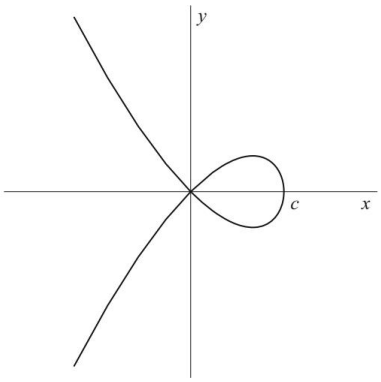
(a) 给定 (x,y) 平面上一点 $(u,v,0)$，从该点画一条直线到球面的“北极” $(0,0,1)$，令 (x,y,z) 为直线与球面的另一个交点. 画一幅图说明这一点，并从几何上论证将 (u,v) 映射到 (x,y,z) 给出了球面去掉北极的参数化.

(b) 证明连接 $(0,0,1)$ 和 $(u,v,0)$ 的直线被参数化为 $(tu,tv,1-t)$，其中 t 是沿直线移动的参数.

(c) 将 $x=tu, y=tv$ 和 $z=1-t$ 代入球面方程 $x^2+y^2+z^2=1$. 利用它推导问题开头给出的公式.

(7) 将上一题的论证加以改进，以参数化 n 维仿射空间中的“球面” $x_1^2+\cdots+x_n^2=1$. 提示：将有 $n-1$ 个参数.

(8) 考虑由 $y^2=cx^2-x^3$ 定义的曲线，其中 c 是某个常数. 当 $c>0$ 时，曲线的图像如下：



目标是参数化这条曲线.

(a) 证明一条直线与这条曲线相交于 0、1、2 或 3 个点. 用图说明你的答案. 提示：设直线方程为 $x=a$ 或 $y=mx+b$.

(b) 证明当 $m^2 \neq c$ 时，过原点的一条非垂直线与曲线恰好在另一个点相交. 画一幅图说明这一点，看看能否给出一个直观的解释为什么会发生这种情况.

(c) 现在画垂直线 $x=1$. 给定该直线上一点 $(1,t)$，画一条连接 $(1,t)$ 与原点的直线. 这条直线将与曲线交于一点 (x,y). 画一幅图说明这一点，并从几何上论证这给出了整条曲线的一个参数化.

(d) 证明第 (c) 部分的几何描述导致参数化

$$x = c - t^2,$$

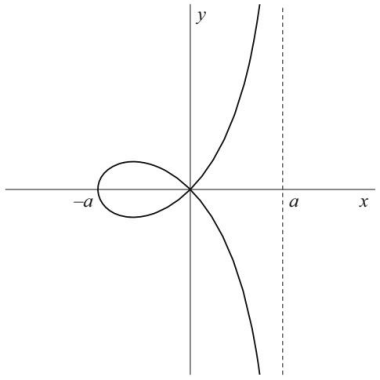
$$y = t(c - t^2).$$

(9) 环索线是一条曾被多位数学家研究过的曲线，包括 Isaac Barrow（1630–1677）、Jean Bernoulli（1667–1748）和 Maria Agnesi（1718–1799）. 它的一个三角参数化是

$$x = a\sin(t),$$

$$y = a\tan(t)(1 + \sin(t))$$

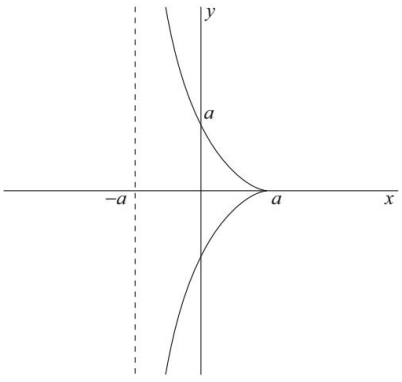
其中 a 是常数. 如果让 t 在范围 $-4.5 \leqslant t \leqslant 1.5$ 内变化，得到这里显示的图像.



(a) 求用 x 和 y 描述环索线的方程. 提示：如果不够仔细，会得到方程 $(a^2-x^2)y^2 = x^2(a+x)^2$. 要知道为什么这不完全正确，看看当 $x = -a$ 时会发生什么.

(b) 求环索线的一个代数参数化.

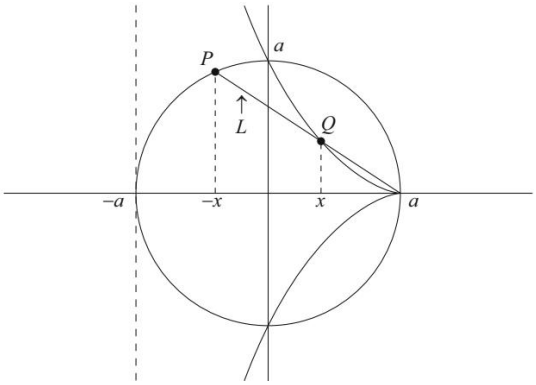
(10) 大约公元前 180 年，Diocles 写了一本书《论燃烧镜》. 他考虑的曲线之一是蔓叶线，并用它来解决倍立方问题 [见第 (c) 部分 below]. 蔓叶线的方程是 $y^2(a + x) = (a - x)^3$，其中 a 是常数. 这给出了平面上如下的曲线：



(a) 求蔓叶线的一个代数参数化.

(b) Diocles 用如下几何构造描述了蔓叶线. 给定一个半径为 a 的圆（取圆心在原点），在 a 和 $-a$ 之间选取 x，并画一条连接 $(a, 0)$ 和圆上点 $P = (-x, \sqrt{a^2 - x^2})$ 的直线 L. 这确定

了 L 上一点 $Q=(x,y)$：



证明蔓叶线是所有这样的点 Q 的轨迹.

(c) 倍立方问题是古希腊的经典问题，试图仅用尺规作图构造 $\sqrt[3]{2}$. 已知仅用尺规这是不可能的. Diocles 证明了如果额外允许使用蔓叶线，那么就可以构造 $\sqrt[3]{2}$. 方法如下. 画一条连接 $(-a,0)$ 和 $(0,a/2)$ 的直线. 这条直线将与蔓叶线交于一点 (x,y). 然后证明

$$2=\left(\frac{a-x}{y}\right)^3,$$

这说明如何用尺规和蔓叶线构造 $\sqrt[3]{2}$.

(11) 在本题中，将推导曲面 $x^2-y^2z^2+z^3=0$ 的参数化

$$x=t(u^2-t^2),$$

$$y=u,$$

$$z=u^2-t^2.$$

(a) 将习题 8 第 (d) 部分的公式加以改进，证明曲线 $x^2=cz^2-z^3$ 被参数化为

$$z=c-t^2,$$

$$x=t(c-t^2).$$

(b) 现在将第 (a) 部分的 c 替换为 y^2，并解释这如何导出 $x^2-y^2z^2+z^3=0$ 的上述参数化.

(c) 解释为什么这个参数化覆盖了整个曲面 $\mathbf{V}(x^2-y^2z^2+z^3)$. 提示：见习题 8 第 (c) 部分.

(12) 考虑簇 $V=\mathbf{V}(y-x^2,z-x^4)\subseteq\mathbb{R}^3$.

(a) 画一幅 V 的图像.

(b) 以类似于对三次扭曲线所做的方法参数化 V.

(c) 参数化 V 的切曲面.

(13) 求参数化曲面的方程这一一般问题将在第 2 章和第 3 章中研究. 然而，当曲面是平面时，可以使用微积分或线性代数的方法. 例如，考虑由

$$\begin{aligned} x &= 1 + u - v, \\ y &= u + 2v, \\ z &= -1 - u + v \end{aligned}$$

参数化的 $\mathbb{R}^3$ 中的平面. 求用这种方法确定的平面的方程. 提示：设平面方程为 $ax+by+cz=d$. 然后将上述参数化代入，得到关于 a, b, c, d 的方程组. 解决这个问题的另一种方法是将参数化写成向量形式 $(1,0,-1)+u(1,1,-1)+v(-1,2,1)$. 然后可以用叉乘快速求解.

(14) 本题讨论凸集，将在下一题中用来证明 Bézier 三次曲线位于其控制多边形内. 子集 $C \subseteq \mathbb{R}^2$ 是**凸的**，如果对所有 $P, Q \in C$，连接 P 和 Q 的线段也位于 C 中.

(a) 如果 $P = \begin{pmatrix} x \\ y \end{pmatrix}$ 和 $Q = \begin{pmatrix} z \\ w \end{pmatrix}$ 位于凸集 C 中，证明当 $0 \leqslant t \leqslant 1$ 时，

$$t \begin{pmatrix} x \\ y \end{pmatrix} + (1-t) \begin{pmatrix} z \\ w \end{pmatrix} \in C.$$

(b) 如果 $P_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix}$ 对于 $1 \leqslant i \leqslant n$ 位于凸集 C 中，证明当 $t_1, \ldots, t_n$ 是非负数且 $\sum_{i=1}^{n} t_i = 1$ 时，

$$\sum_{i=1}^{n} t_i \begin{pmatrix} x_i \\ y_i \end{pmatrix} \in C.$$

提示：对 n 用归纳法.

(15) 设一条 Bézier 三次曲线由

$$\begin{aligned} x &= (1-t)^3 x_0 + 3t(1-t)^2 x_1 + 3t^2(1-t)x_2 + t^3 x_3, \\ y &= (1-t)^3 y_0 + 3t(1-t)^2 y_1 + 3t^2(1-t)y_2 + t^3 y_3 \end{aligned}$$

给出.

(a) 证明上述方程可以写成向量形式

$$\begin{pmatrix} x \\ y \end{pmatrix} = (1-t)^3 \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + 3t(1-t)^2 \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + 3t^2(1-t) \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} + t^3 \begin{pmatrix} x_3 \\ y_3 \end{pmatrix}.$$

(b) 利用上一题证明 Bézier 三次曲线总是位于其控制多边形内部. 提示：在上述方程中，系数的和是多少?

(16) Bézier 三次曲线的一个缺点是圆和双曲线等曲线无法被三次曲线精确描述. 在本题中，将讨论一种类似于例子 (4) 的方法来参数化圆锥曲线. 处理基于 BALL（1987）[另见 GOLDMAN（2003），第 5.7 节].

圆锥曲线是平面上由二次方程 $ax^2 + bxy + cy^2 + dx + ey + f = 0$ 定义的曲线. 圆锥曲线包括圆、椭圆、抛物线和双曲线等熟悉的例子. 现在考虑由

$$x = \frac{(1-t)^2 x_1 + 2t(1-t)wx_2 + t^2 x_3}{(1-t)^2 + 2t(1-t)w + t^2},$$

$$y = \frac{(1-t)^2 y_1 + 2t(1-t)wy_2 + t^2 y_3}{(1-t)^2 + 2t(1-t)w + t^2}$$

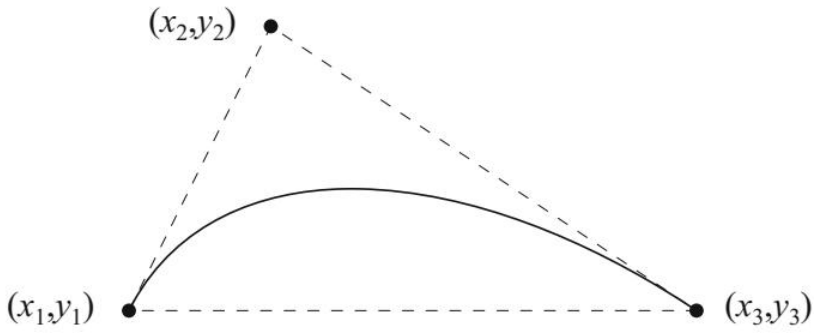
参数化的曲线，其中 $0 \leqslant t \leqslant 1$. 常数 $w, x_1, y_1, x_2, y_2, x_3, y_3$ 由设计工程师指定，假设 $w \geqslant 0$. 在第 3 章中，将证明这些方程参数化了一条圆锥曲线. 本题的目标是为量 $w, x_1, y_1, x_2, y_2, x_3, y_3$ 给出几何解释.

(a) 证明假设 $w \geqslant 0$ 意味着上述公式中的分母永不为零.

(b) 在 $t = 0$ 和 $t = 1$ 处计算上述公式. 这将告诉你 x_1, y_1, x_3, y_3 的含义.

(c) 现在计算 $(x'(0), y'(0))$ 和 $(x'(1), y'(1))$. 利用它证明 (x_2, y_2) 是曲线起点和终点处切线的交点. 解释为什么 $(x_1, y_1), (x_2, y_2)$ 和 (x_3, y_3) 称为曲线的控制点.

(d) 定义控制多边形（在本题中实际上是一个三角形），并证明由上述方程定义的曲线总是位于其控制多边形内部. 提示：改进上一题的论证. 这给出如下图像：

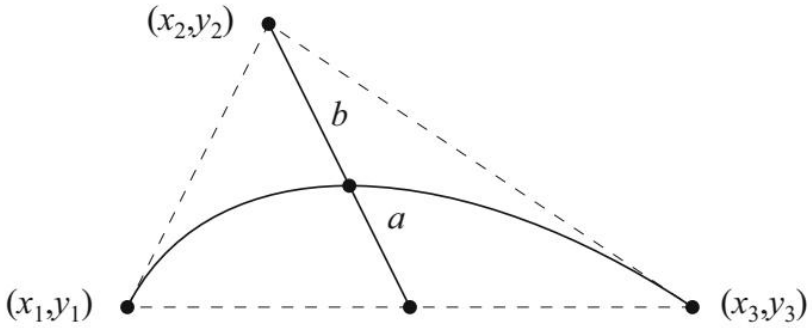


现在剩下要解释常数 w，它称为形状因子. 从第 (c) 部分的答案中应该得到提示，因为注意 w 出现在 $t = 0$ 和 $t = 1$ 时切向量的公式中. 所以 w 以某种方式控制着“速度”，较大的 w 应该迫使曲线更靠近 (x_2, y_2). 在问题的最后两部分，将确定 w 的确切作用.

(e) 证明

$$\begin{pmatrix} x(1/2) \\ y(1/2) \end{pmatrix} = \frac{1}{1+w}\left(\frac{1}{2}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} x_3 \\ y_3 \end{pmatrix}\right) + \frac{w}{1+w}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

利用这个公式证明 $(x(1/2), y(1/2))$ 位于连接 (x_2, y_2) 与 (x_1, y_1) 和 (x_3, y_3) 连线中点的线段上.



第 4 节　理想

接下来定义本书研究的基本代数对象.

定义 1. 子集 $I \subseteq k[x_1,\ldots,x_n]$ 称为**理想**，如果它满足以下条件：

(i) $0 \in I$.

(ii) 若 $f, g \in I$，则 $f+g \in I$.

(iii) 若 $f \in I$ 且 $h \in k[x_1,\ldots,x_n]$，则 $hf \in I$.

本节的目标是向读者介绍一些自然出现的理想，并展示理想如何与仿射簇相关联. 理想的真正重要性在于它们为我们提供了一种用于计算仿射簇的语言.

第一个自然的理想例子是由有限个多项式生成的理想.

定义 2. 设 $f_1,\ldots,f_s$ 是 $k[x_1,\ldots,x_n]$ 中的多项式. 定义

$$\langle f_1,\ldots,f_s\rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1,\ldots,h_s \in k[x_1,\ldots,x_n] \right\}.$$

关键事实是 $\langle f_1,\ldots,f_s\rangle$ 是一个理想.

引理 3. 若 $f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$，则 $\langle f_1,\ldots,f_s\rangle$ 是 $k[x_1,\ldots,x_n]$ 的一个理想. 称 $\langle f_1,\ldots,f_s\rangle$ 为由 $f_1,\ldots,f_s$ **生成**的理想.

证明. 首先，$0 \in \langle f_1,\ldots,f_s\rangle$，因为 $0 = \sum_{i=1}^{s} 0 \cdot f_i$. 其次，假设 $f = \sum_{i=1}^{s} p_i f_i$ 且 $g = \sum_{i=1}^{s} q_i f_i$，并设 $h \in k[x_1,\ldots,x_n]$. 则由以下等式

$$f+g = \sum_{i=1}^{s} (p_i+q_i) f_i,$$
$$hf = \sum_{i=1}^{s} (hp_i) f_i$$

即可完成 $\langle f_1,\ldots,f_s\rangle$ 是理想的证明. □

理想 $\langle f_1, \ldots, f_s \rangle$ 在多项式方程方面有很好的解释. 给定 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$，得到方程组

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ &\vdots \\ &\vdots \\ f_s &= 0. \end{aligned}$$

从这些方程出发，可以通过代数方法推导出其他方程. 例如，如果将第一个方程乘以 $h_1 \in k[x_1, \ldots, x_n]$，第二个乘以 $h_2 \in k[x_1, \ldots, x_n]$，等等，然后将所得的方程相加，得到

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0,$$

这是原方程组的一个推论. 注意到这个方程的左边正是理想 $\langle f_1, \ldots, f_s \rangle$ 中的一个元素. 因此，可以将 $\langle f_1, \ldots, f_s \rangle$ 看作由方程 $f_1 = f_2 = \cdots = f_s = 0$ 导出的所有 “多项式推论” 的集合.

为理解这在实践中的含义，考虑 §3 中的例子，在那里取

$$x = 1 + t,$$

$$y = 1 + t^2$$

并消去 t 得到

$$y = x^2 - 2x + 2$$

[见 §3 中方程 (7) 后面的讨论]. 用上述思想重新做这个例子. 首先将方程写成

$$\begin{aligned} x - 1 - t &= 0, \\ y - 1 - t^2 &= 0. \end{aligned} \tag{1}$$

为消去含 t 的项，将第一个方程乘以 $x - 1 + t$，第二个乘以 -1:

$$(x-1)^2 - t^2 = 0,$$

$$-y + 1 + t^2 = 0,$$

然后相加得到

$$(x-1)^2 - y + 1 = x^2 - 2x + 2 - y = 0.$$

用由方程 (1) 生成的理想来表示，可以写成

$$\begin{aligned} &x^2-2x+2-y=(x-1+t)(x-1-t)+(-1)(y-1-t^2)\\ &\in\langle x-1-t,y-1-t^2\rangle. \end{aligned}$$

类似地，(1) 的任何其他 “多项式推论” 都导出该理想中的一个元素.

若存在 $f_1,\dots,f_s\in k[x_1,\dots,x_n]$ 使得 $I=\langle f_1,\dots,f_s\rangle$，则称理想 I 是**有限生成**的，并称 $f_1,\dots,f_s$ 是 I 的一个**基**. 在第 2 章中，将证明一个惊人的事实：$k[x_1,\dots,x_n]$ 的每个理想都是有限生成的（这就是著名的 Hilbert 基定理）. 注意，一个给定的理想可能有多个不同的基. 在第 2 章中，将展示可以选择一种特别有用的基，称为 Gröbner 基.

这里有一个与线性代数的有趣类比. 理想的定义类似于子空间的定义：两者都必须在加法和乘法下封闭，但对于子空间，乘以标量，而对于理想，乘以多项式. 此外，注意到由多项式 $f_1,\dots,f_s$ 生成的理想类似于有限个向量 $v_1,\dots,v_s$ 的张成. 在每种情况下，都取线性组合，对于张成使用域系数，对于理想使用多项式系数. 与线性代数的进一步联系在习题 6 中探讨.

理想的另一个重要作用体现在以下命题中，该命题表明簇仅依赖于其定义方程所生成的理想.

命题 4. *若 $f_1,\dots,f_s$ 和 $g_1,\dots,g_t$ 是 $k[x_1,\dots,x_n]$ 中同一理想的基，即 $\langle f_1,\dots,f_s\rangle=\langle g_1,\dots,g_t\rangle$，则有 $\mathbf{V}(f_1,\dots,f_s)=\mathbf{V}(g_1,\dots,g_t)$.*

证明. 证明非常直接，留作习题. □

例如，考虑簇 $\mathbf{V}(2x^2+3y^2-11,x^2-y^2-3)$. 容易证明 $\langle 2x^2+3y^2-11,x^2-y^2-3\rangle=\langle x^2-4,y^2-1\rangle$（见习题 3），因此由上述命题

$$\mathbf{V}(2x^2+3y^2-11,x^2-y^2-3)=\mathbf{V}(x^2-4,y^2-1)=\{(\pm2,\pm1)\}$$

于是，通过改变理想的基，更容易确定簇.

改变基而不影响簇的能力非常重要. 在本书后面，这将导致如下观察：仿射簇由理想决定，而不是由方程决定.（事实上，理想与簇的对应是第 4 章的主题.）从更实际的角度看，还将看到命题 4 与上面提到的 Gröbner 基结合，为理解仿射簇提供了强大的工具.

接下来讨论仿射簇如何产生一类有趣的理想. 假设有一个仿射簇 $V=\mathbf{V}(f_1,\dots,f_s)\subseteq k^n$，由 $f_1,\dots,f_s\in k[x_1,\dots,x_n]$ 定义. 知道 $f_1,\dots,f_s$ 在 V 上为零，但它们是否是唯一的？是否还有其他多项式在 V 上为零？例如，考虑 §2 中研究的三次扭曲线. 这条曲线由 $y-x^2$ 和 $z-x^3$ 的零点定义. 由 §3 中讨论的参数化 (t,t^2,t^3) 可知，$z-xy$ 和 y^2-xz 是在三次扭转线上为零的另外两个多项式. 还有其他这样的多项式吗？如何找到它们全部？

为研究这个问题，将考虑在给定簇上为零的所有多项式的集合.

定义 5. 设 $V \subseteq k^n$ 是一个仿射簇. 定义

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ 对所有} (a_1, \ldots, a_n) \in V\}.$$

关键的观察是 $\mathbf{I}(V)$ 是一个理想.

引理 6. 若 $V \subseteq k^n$ 是一个仿射簇，则 $\mathbf{I}(V) \subseteq k[x_1, \ldots, x_n]$ 是一个理想. 称 $\mathbf{I}(V)$ 为 V 的**理想**.

证明. 显然 $0 \in \mathbf{I}(V)$，因为零多项式在整个 k^n 上为零，因此特别地在 V 上为零. 其次，假设 $f, g \in \mathbf{I}(V)$ 且 $h \in k[x_1, \ldots, x_n]$.

设 $(a_1, \ldots, a_n)$ 是 V 的任意一点. 则

$$\begin{aligned} f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) &= 0 + 0 = 0, \\ h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) &= h(a_1, \ldots, a_n) \cdot 0 = 0, \end{aligned}$$

由此可知 $\mathbf{I}(V)$ 是一个理想. □

作为簇的理想的一个例子，考虑由 k^2 中原点组成的簇 $\{(0,0)\}$. 则其理想 $\mathbf{I}(\{(0,0)\})$ 由在原点处为零的所有多项式组成，断言

$$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle.$$

证明的一个方向是平凡的，因为任何形式为 $A(x,y)x + B(x,y)y$ 的多项式显然在原点处为零. 反过来，假设 $f = \sum_{i,j} a_{ij} x^i y^j$ 在原点处为零. 则 $a_{00} = f(0,0) = 0$，因此

$$\begin{aligned} f &= a_{00} + \sum_{i,j \neq 0,0} a_{ij} x^i y^j \\ &= 0 + \left(\sum_{\substack{i,j \\ i>0}} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \in \langle x, y \rangle. \end{aligned}$$

断言得证.

另一个例子，考虑 V 是整个 k^n 的情形. 则 $\mathbf{I}(k^n)$ 由处处为零的多项式组成，因此由 §1 的命题 5，当 k 无限时有

$$\mathbf{I}(k^n) = \{0\} \quad \text{当} k \text{ 无限时}.$$

（这里 $\{0\}$ 表示 $k[x_1, \ldots, x_n]$ 中的零多项式.）注意 §1 的命题 5 等价于上述陈述. 在习题中，将讨论当 k 是有限域时会发生什么.

一个更有趣的例子由 $\mathbb{R}^3$ 中的三次扭曲线 $V = \mathbf{V}(y - x^2, z - x^3)$ 给出. 断言

$$\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle.$$

为证明这一点，首先证明对于给定的多项式 $f \in \mathbb{R}[x,y,z]$，可以将 f 写成如下形式

$$f = h_1(y - x^2) + h_2(z - x^3) + r, \tag{2}$$

其中 $h_1, h_2 \in \mathbb{R}[x,y,z]$ 且 r 是仅含变量 x 的多项式. 首先，考虑 f 是单项式 $x^\alpha y^\beta z^\gamma$ 的情形. 则由二项式定理

$$\begin{aligned} x^\alpha y^\beta z^\gamma &= x^\alpha \left(x^2 + (y - x^2)\right)^\beta \left(x^3 + (z - x^3)\right)^\gamma \\ &= x^\alpha \left(x^{2\beta} + \text{含} y - x^2 \text{ 的项}\right) \left(x^{3\gamma} + \text{含} z - x^3 \text{ 的项}\right), \end{aligned}$$

展开后表明

$$x^\alpha y^\beta z^\gamma = h_1(y - x^2) + h_2(z - x^3) + x^{\alpha+2\beta+3\gamma}$$

对某些多项式 $h_1, h_2 \in \mathbb{R}[x,y,z]$ 成立. 因此，(2) 在此情形成立. 由于任意 $f \in \mathbb{R}[x,y,z]$ 是单项式的 $\mathbb{R}$-线性组合，可知 (2) 一般成立.

现在可以证明 $\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$. 首先，由三次扭曲线 V 的定义，有 $y - x^2, z - x^3 \in \mathbf{I}(V)$，且由于 $\mathbf{I}(V)$ 是理想，可知 $h_1(y - x^2) + h_2(z - x^3) \in \mathbf{I}(V)$. 这证明了 $\langle y - x^2, z - x^3 \rangle \subseteq \mathbf{I}(V)$. 为证明相反的包含关系，设 $f \in \mathbf{I}(V)$ 并令

$$f = h_1(y - x^2) + h_2(z - x^3) + r$$

为 (2) 给出的表达式. 为证明 r 为零，将使用三次扭转线的参数化 (t, t^2, t^3). 由于 f 在 V 上为零，得到

$$0 = f(t, t^2, t^3) = 0 + 0 + r(t)$$

（回忆 r 是仅含 x 的多项式）. 由于 t 可以是任意实数，由 §1 的命题 5 可知 $r \in \mathbb{R}[x]$ 必须是零多项式. 但 $r = 0$ 表明 f 具有所需的形式，从而证明了 $\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$.

在 (2) 中所做的类似于多项式的除法，只不过除以两个多项式而不是一个. 事实上，(2) 是第 2 章将要研究的广义除法算法的特例.

上述例子的一个很好的推论是，对于给定的多项式 $f \in \mathbb{R}[x,y,z]$，有 $f \in \langle y - x^2, z - x^3 \rangle$ 当且仅当 $f(t, t^2, t^3)$ 恒为零. 这为我们提供了一个判断多项式是否属于该理想的算法. 然而，这种方法依赖于参数化 (t, t^2, t^3). 是否存在一种不使用参数化来判断 $f \in \langle y - x^2, z - x^3 \rangle$ 的方法？在第 2 章中，将使用 Gröbner 基和广义除法算法肯定地回答这个问题.

三次扭转线的例子很有启发性. 从多项式 $y - x^2$ 和 $z - x^3$ 出发，用它们定义一个仿射簇，取在簇上为零的所有函数，然后得到由这两个多项式生成的理想. 自然会想这是否在一般情况下成立.

因此取 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. 这给出

$$\begin{array}{ccccc} \text{多项式} & & \text{簇} & & \text{理想} \\ f_1, \ldots, f_s & \longrightarrow & \mathbf{V}(f_1, \ldots, f_s) & \longrightarrow & \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)), \end{array}$$

自然要问的问题是

$$\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$$

是否成立. 不幸的是，答案并不总是肯定的. 以下是目前能给出的最佳答案.

引理 7. 设 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. 则 $\langle f_1, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$，尽管等式不一定成立.

证明. 设 $f \in \langle f_1, \ldots, f_s \rangle$，这意味着 $f = \sum_{i=1}^{s} h_i f_i$ 对某些多项式 $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$ 成立. 由于 $f_1, \ldots, f_s$ 在 $\mathbf{V}(f_1, \ldots, f_s)$ 上为零，所以 $\sum_{i=1}^{s} h_i f_i$ 亦然. 因此，f 在 $\mathbf{V}(f_1, \ldots, f_s)$ 上为零，这证明了 $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$.

对于引理的第二部分，需要一个 $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ 严格大于 $\langle f_1, \ldots, f_s \rangle$ 的例子. 将证明包含关系

$$\langle x^2, y^2 \rangle \subseteq \mathbf{I}(\mathbf{V}(x^2, y^2))$$

不是等式. 首先计算 $\mathbf{I}(\mathbf{V}(x^2, y^2))$. 方程 $x^2 = y^2 = 0$ 意味着 $\mathbf{V}(x^2, y^2) = \{(0, 0)\}$. 但前面的例子表明 $\{(0, 0)\}$ 的理想是 $\langle x, y \rangle$，因此 $\mathbf{I}(\mathbf{V}(x^2, y^2)) = \langle x, y \rangle$. 为看出这严格大于 $\langle x^2, y^2 \rangle$，注意 $x \notin \langle x^2, y^2 \rangle$，因为对于形如 $h_1(x, y)x^2 + h_2(x, y)y^2$ 的多项式，每个单项式的总次数至少为 2. □

对于任意域，$\langle f_1, \ldots, f_s \rangle$ 与 $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ 之间的关系可能相当微妙（见习题中的一些例子）. 然而，在代数闭域如 $\mathbb{C}$ 上，这些理想之间有直接的关系. 这将在第 4 章证明零点定理时加以解释.

虽然对于一般域，$\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ 可能不等于 $\langle f_1, \ldots, f_s \rangle$，但簇的理想总是包含足够的信息来唯一确定簇.

命题 8. 设 V 和 W 是 k^n 中的仿射簇. 则：

(i) $V \subseteq W$ 当且仅当 $\mathbf{I}(V) \supseteq \mathbf{I}(W)$.

(ii) $V = W$ 当且仅当 $\mathbf{I}(V) = \mathbf{I}(W)$.

证明. 留作习题，证明 (ii) 是 (i) 的直接推论. 为证明 (i)，首先假设 $V \subseteq W$. 则在 W 上为零的任何多项式必在 V 上为零，这证明了 $\mathbf{I}(W) \subseteq \mathbf{I}(V)$. 其次，假设 $\mathbf{I}(W) \subseteq \mathbf{I}(V)$. 知道 W 是由某些多项式 $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ 定义的簇. 则 $g_1, \ldots, g_t \in \mathbf{I}(W) \subseteq \mathbf{I}(V)$，因此 g_i 在 V 上为零. 由于 W 由 g_i 的所有公共零点组成，可知 $V \subseteq W$. □

理想与仿射簇之间有丰富的关系；目前为止介绍的内容只是冰山一角. 将在第 4 章进一步探讨这一关系. 特别地，将看到关于理想证明的定理具有强烈的几何含义. 现在，列出关于 $k[x_1, \ldots, x_n]$ 中理想的三个问题：

（理想的描述）是否每个理想 $I \subseteq k[x_1, \ldots, x_n]$ 都能写成 $\langle f_1, \ldots, f_s \rangle$ 的形式，其中 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$?

（理想的成员判定）若 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$，是否存在一个算法来判断给定的 $f \in k[x_1, \ldots, x_n]$ 是否属于 $\langle f_1, \ldots, f_s \rangle$?

（零点定理）给定 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$，$\langle f_1, \ldots, f_s \rangle$ 与 $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ 之间的确切关系是什么?

在接下来的章节中，将完全解决这些问题（还将解释零点定理这一名称的由来），尽管需要注意在哪个域上工作.

1.4.1 习题

1. 考虑方程
$$x^2 + y^2 - 1 = 0,$$
$$xy - 1 = 0$$
它们描述了一个圆与一条双曲线的交.
   (a) 用代数方法从上述方程中消去 y.
   (b) 说明 (a) 部分找到的多项式如何属于 $\langle x^2 + y^2 - 1, xy - 1 \rangle$. 你的答案应该类似于我们在 (1) 中所做的. 提示：将第二个方程乘以 $xy + 1$.
2. 设 $I \subseteq k[x_1, \ldots, x_n]$ 是一个理想，且 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. 证明以下陈述等价：
   (i) $f_1, \ldots, f_s \in I$.
   (ii) $\langle f_1, \ldots, f_s \rangle \subseteq I$.
   这一事实在你想要证明一个理想包含于另一个理想时很有用.
3. 利用上一习题证明 $\mathbb{Q}[x, y]$ 中以下理想的相等性：
   (a) $\langle x + y, x - y \rangle = \langle x, y \rangle$.
   (b) $\langle x + xy, y + xy, x^2, y^2 \rangle = \langle x, y \rangle$.
   (c) $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$.
   这说明了同一个理想可以有多个不同的基，且不同的基可能含有不同数量的元素.
4. 证明命题 4.
5. 证明 $\mathbf{V}(x + xy, y + xy, x^2, y^2) = \mathbf{V}(x, y)$. 提示：见习题 3.
6. “基”这个词在数学中有多种用法. 在本习题中，将看到“理想的基”（如本节所定义的）与“子空间的基”（在线性代数中研究的）相当不同.
   (a) 首先，考虑理想 $I = \langle x \rangle \subseteq k[x]$. 作为理想，$I$ 有一个由单个元素 x 组成的基. 但 I 也可以看作 $k[x]$ 的子空间，而 $k[x]$ 是 k 上的向量空间. 证明 I 在 k 上的任何向量空间基都是无限的. 提示：只需找到一个无限基即可. 因此，允许 x 被 $k[x]$ 中的元素而不仅仅是 k 中的元素乘，才使得 $\langle x \rangle$ 能有有限基.

(b) 在线性代数中，基必须张成且在 k 上线性无关，而对于理想，基只涉及张成——没有任何独立性的提及. 原因是一旦允许多项式系数，独立性就不可能了. 为看出这一点，考虑理想 $\langle x, y\rangle \subseteq k[x, y]$. 证明零可以写成 y 和 x 的具有非零多项式系数的线性组合.

(c) 更一般地，假设 $f_1, \ldots, f_s$ 是理想 $I \subseteq k[x_1, \ldots, x_n]$ 的基. 若 $s \geqslant 2$ 且对所有 i 有 $f_i \neq 0$，则证明对于任意 i 和 j，零可以写成 f_i 和 f_j 的具有非零多项式系数的线性组合.

(d) 缺乏独立性的一个后果是，当把元素 $f \in \langle f_1, \ldots, f_s\rangle$ 写成 $f = \sum_{i=1}^{s} h_i f_i$ 时，系数 h_i 不是唯一的. 例如，考虑 $f = x^2 + xy + y^2 \in \langle x, y\rangle$. 用两种不同的方式将 f 表示为 x 和 y 的线性组合.（即使 h_i 不唯一，也可以度量它们的不唯一程度. 这引出了有趣的合系话题.）

(e) 理想 I 的基 $f_1, \ldots, f_s$ 称为**极小的**，如果 $f_1, \ldots, f_s$ 的任何真子集都不是 I 的基. 例如，x, x^2 是一个理想的基，但不是极小基，因为 x 生成了同一个理想. 不幸的是，一个理想可以有由不同数量元素组成的极小基. 为看出这一点，证明 x 和 $x + x^2, x^2$ 是 $k[x]$ 中同一理想的极小基. 解释这与线性代数中的情形如何形成对比.

7. 证明对于任意正整数 n 和 m，有 $\mathbf{I}(\mathbf{V}(x^n, y^m)) = \langle x, y\rangle$.

8. 簇的理想 $\mathbf{I}(V)$ 具有一个并非所有理想都有的特殊性质. 具体而言，定义理想 I 是**根理想的**，如果每当多项式 f 的某个幂 f^m 在 I 中时，f 本身也在 I 中. 更简洁地说，当 $f \in I$ 当且仅当对某个正整数 m 有 $f^m \in I$ 时，I 是根理想的.

   (a) 证明 $\mathbf{I}(V)$ 总是根理想的.

   (b) 证明 $\langle x^2, y^2\rangle$ 不是根理想的. 这意味着对任何簇 $V \subseteq k^2$，都有 $\langle x^2, y^2\rangle \neq \mathbf{I}(V)$.

   根理想将在第 4 章中起重要作用. 特别地，零点定理将意味着 $\mathbb{C}^n$ 中的簇与 $\mathbb{C}[x_1, \ldots, x_n]$ 中的根理想之间存在一一对应.

9. 设 $V = \mathbf{V}(y - x^2, z - x^3)$ 是三次扭曲线. 在正文中，证明了 $\mathbf{I}(V) = \langle y - x^2, z - x^3\rangle$.

   (a) 利用三次扭转线的参数化证明 $y^2 - xz \in \mathbf{I}(V)$.

   (b) 用正文中给出的论证方法将 $y^2 - xz$ 表示为 $y - x^2$ 和 $z - x^3$ 的组合.

10. 利用正文中关于三次扭转线的讨论所用的论证方法证明 $\mathbf{I}(\mathbf{V}(x - y)) = \langle x - y\rangle$. 你的论证应对任意无限域 k 有效.

11. 设 $V \subseteq \mathbb{R}^3$ 是由 (t, t^3, t^4) 参数化的曲线.

   (a) 证明 V 是一个仿射簇.

   (b) 改编三次扭曲线情形中使用的方法来确定 $\mathbf{I}(V)$.

12. 设 $V \subseteq \mathbb{R}^3$ 是由 (t^2, t^3, t^4) 参数化的曲线.

   (a) 证明 V 是一个仿射簇.

   (b) 确定 $\mathbf{I}(V)$.

   这个问题比前一个难得多——找出方程 (2) 的恰当类比并不容易. 一旦在第 2 章学习了除法算法，这个习题将变得容易得多.

13. 在 §1 的习题 2 中，证明了 $x^2y + y^2x$ 在 $\mathbb{F}_2^2$ 的所有点处为零. 更一般地，设 $I \subseteq \mathbb{F}_2[x, y]$ 是在 $\mathbb{F}_2^2$ 的所有点处为零的所有多项式构成的理想. 本习题的目标是证明 $I = \langle x^2 - x, y^2 - y\rangle$.

(a) 证明 $\langle x^2-x, y^2-y\rangle \subseteq I$.

(b) 证明每个 $f \in \mathbb{F}_2[x,y]$ 都可以写成 $f = A(x^2-x)+B(y^2-y)+axy+bx+cy+d$，其中 $A, B \in \mathbb{F}_2[x,y]$ 且 $a,b,c,d \in \mathbb{F}_2$. 提示：将 f 写成 $\sum_i p_i(x)y^i$ 的形式，并用除法算法（§5 的命题 2）将每个 p_i 除以 x^2-x. 由此，可以写成 $f = A(x^2-x)+q_1(y)x+q_2(y)$. 现在将 q_1 和 q_2 除以 y^2-y. 同样，一旦知道第 2 章的除法算法，这个论证将变得非常简单.

(c) 证明 $axy+bx+cy+d \in I$ 当且仅当 $a=b=c=d=0$.

(d) 利用 (b) 和 (c) 完成 $I = \langle x^2-x, y^2-y\rangle$ 的证明.

(e) 将 x^2y+y^2x 表示为 x^2-x 和 y^2-y 的组合. 提示：记住在 $\mathbb{F}_2$ 中 $2 = 1+1 = 0$.

14. 本习题涉及命题 8.

(a) 证明命题的 (ii) 部分由 (i) 部分推出.

(b) 证明命题的以下推论：若 V 和 W 是 k^n 中的仿射簇，则 $V \subsetneq W$ 当且仅当 $\mathbf{I}(V) \supsetneq \mathbf{I}(W)$.

15. 在正文中，为簇 $V \subseteq k^n$ 定义了 $\mathbf{I}(V)$. 可以将其推广如下：若 $S \subseteq k^n$ 是任意子集，则定义

$$\mathbf{I}(S) = \{f \in k[x_1,\ldots,x_n] \mid f(a_1,\ldots,a_n) = 0 \text{ 对所有} (a_1,\ldots,a_n) \in S\}.$$

(a) 证明 $\mathbf{I}(S)$ 是一个理想.

(b) 设 $X = \{(a,a) \in \mathbb{R}^2 \mid a \neq 1\}$. 由 §2 的习题 8，知道 X 不是仿射簇. 确定 $\mathbf{I}(X)$. 提示：你在 §2 的习题 8 中证明的内容将很有用. 另见本节的习题 10.

(c) 设 $\mathbb{Z}^n$ 是 $\mathbb{C}^n$ 中具有整数坐标的点集. 确定 $\mathbf{I}(\mathbb{Z}^n)$. 提示：见 §1 的习题 6.

16. 这里是关于理想的更多练习. 设 I 是 $k[x_1,\ldots,x_n]$ 中的理想.

(a) 证明 $1 \in I$ 当且仅当 $I = k[x_1,\ldots,x_n]$.

(b) 更一般地，证明 I 包含非零常数当且仅当 $I = k[x_1,\ldots,x_n]$.

(c) 假设 $f, g \in k[x_1,\ldots,x_n]$ 满足 $f^2, g^2 \in I$. 证明 $(f+g)^3 \in I$. 提示：用二项式定理展开 $(f+g)^3$.

(d) 现在假设 $f, g \in k[x_1,\ldots,x_n]$ 满足 $f^r, g^s \in I$. 证明 $(f+g)^{r+s-1} \in I$.

17. 在引理 7 的证明中，证明了在 $k[x,y]$ 中 $x \notin \langle x^2, y^2\rangle$.

(a) 证明 $xy \notin \langle x^2, y^2\rangle$.

(b) 证明 $1, x, y, xy$ 是不含于 $\langle x^2, y^2\rangle$ 的仅有的单项式.

18. 在正文中，证明了在 $k[x,y]$ 中 $\mathbf{I}(\{(0,0)\}) = \langle x, y\rangle$.

(a) 将其推广，证明原点 $0 = (0,\ldots,0) \in k^n$ 满足在 $k[x_1,\ldots,x_n]$ 中 $\mathbf{I}(\{0\}) = \langle x_1,\ldots,x_n\rangle$.

(b) (a) 部分关于 $k[x_1,\ldots,x_n]$ 中常数项为零的多项式说了什么?

19. 本节的一个关键思想是，方程组 $f_1 = \cdots = f_s = 0$ 给出了多项式推论的理想 $I = \langle f_1,\ldots,f_s\rangle$. 现在假设方程组有一个形如 $f = g$ 的推论，将两边取 m 次幂得到 $f^m = g^m$. 用理想 I 的语言来说，这意味着 $f-g \in I$ 应该蕴含 $f^m - g^m \in I$. 通过对 $f^m - g^m$ 进行因式分解来证明这一点.

第 5 节 一元多项式

本节讨论一元多项式，并研究高中代数中的除法算法. 这个简单的算法有一些令人惊讶的深刻推论——例如，将用它来确定 $k[x]$ 的理想的结构，并探讨最大公因子的概念. 所发展的理论将使我们能够在 $k[x]$ 中多项式的特殊情形下，解决前几节提出的多数问题. 还将开始理解算法所扮演的重要角色.

到此为止，大多数学生在他们的数学学习中已经见过各种算法，尽管可能没有使用 “算法” 这个词. 非正式地说，算法是对符号或数值数据进行操作的特定指令集. 例子包括微积分中的微分公式和线性代数中的行约化方法. 算法有输入（算法使用的对象）和输出（算法的结果）. 在执行的每个阶段，算法必须准确指定下一步将是什么.

在研究算法时，通常用 “伪代码” 来呈现它，这将使其形式结构更易于理解. 伪代码类似于许多常见的计算机语言，附录 B 中给出了简要讨论. 使用伪代码的另一个原因是它表明了如何在计算机上编程实现该算法. 还应提到，本书中的大多数算法都在 Maple、Mathematica 和许多其他计算机代数系统中实现. 附录 C 有关于这些程序的更多细节.

首先讨论 $k[x]$ 中多项式的除法算法. 该算法的一个关键组成部分是 “首项” 的概念. 精确定义如下.

定义 1. 给定非零多项式 $f \in k[x]$，设

$$f = c_0x^m + c_1x^{m-1} + \cdots + c_m,$$

其中 $c_i \in k$ 且 $c_0 \neq 0$[因此 $m = \deg(f)$]. 则称 c_0x^m 为 f 的**首项**，记作 $\mathrm{LT}(f) = c_0x^m$.

例如，若 $f = 2x^3 - 4x + 3$，则 $\mathrm{LT}(f) = 2x^3$. 还注意到若 f 和 g 是非零多项式，则

$$\deg(f) \leqslant \deg(g) \Longleftrightarrow \mathrm{LT}(f) \text{ 整除 } \mathrm{LT}(g). \tag{1}$$

现在可以描述除法算法.

命题 2（除法算法）. 设 k 是域，g 是 $k[x]$ 中的非零多项式. 则每个 $f \in k[x]$ 都可写成

$$f = qg + r,$$

其中 $q, r \in k[x]$，且要么 $r = 0$，要么 $\deg(r) < \deg(g)$. 此外，q 和 r 是唯一的，并且存在求 q 和 r 的算法.

证明. 以下是求 q 和 r 的算法，用伪代码表示：

$$q := 0; \quad r := f$$

WHILE $r \neq 0$ 且 $\mathrm{LT}(g)$ 整除 $\mathrm{LT}(r)$ DO

$$q := q + \mathrm{LT}(r)/\mathrm{LT}(g)$$

$$r := r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$$

RETURN q, r

WHILE...DO 语句表示执行缩进的操作，直到 WHILE 和 DO 之间的表达式变为假. 语句 $q := \ldots$ 和 $r := \ldots$ 表示正在定义或重新定义 q 和 r 的值. 在此算法中，q 和 r 都是变量——它们在每一步都会改变值. 需要证明算法会终止，并且 q 和 r 的最终值具有所需的性质.（关于伪代码的更详细讨论，见附录 B.）

为理解该算法为何有效，首先注意到 $f = qg + r$ 对 q 和 r 的初始值成立，并且每当重新定义 q 和 r 时，等式 $f = qg + r$ 仍然成立. 这是因为恒等式

$$f = qg + r = (q + \mathrm{LT}(r)/\mathrm{LT}(g))g + (r - (\mathrm{LT}(r)/\mathrm{LT}(g))g).$$

其次，注意到 WHILE...DO 语句在 "$r \neq 0$ 且 $\mathrm{LT}(g)$ 整除 $\mathrm{LT}(r)$" 为假时终止，即当要么 $r = 0$，要么 $\mathrm{LT}(g)$ 不整除 $\mathrm{LT}(r)$ 时. 根据 (1)，最后一个命题等价于 $\deg(r) < \deg(g)$. 因此，当算法终止时，它产生的 q 和 r 具有所需的性质.

还没有完成；仍然需要证明算法会终止，即 WHILE 和 DO 之间的表达式最终会变为假（否则，将陷入无限循环）. 关键观察是 $r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$ 要么为 0，要么次数比 r 小. 原因如下，设

$$r = c_0x^m + \cdots + c_m, \quad \mathrm{LT}(r) = c_0x^m,$$

$$g = d_0x^\ell + \cdots + d_\ell, \quad \mathrm{LT}(g) = d_0x^\ell,$$

并设 $m \geqslant \ell$. 则

$$r - (\mathrm{LT}(r)/\mathrm{LT}(g))g = (c_0x^m + \ldots) - (c_0/d_0)x^{m-\ell}(d_0x^\ell + \ldots),$$

由此可见 r 的次数必定下降（或者整个表达式可能消失）. 由于次数是有限的，它最多只能下降有限次，这证明了算法会终止.

为理解该算法如何对应于高中学到的过程，考虑以下部分完成的除法：

$$\begin{array}{r} \\ 2x+1\overline{)\,x^3+2x^2+x+1} \\ x^3+\frac{1}{2}x^2 \\ \hline \frac{3}{2}x^2+x+1 \end{array}$$

这里，f 和 g 分别由 $f = x^3 + 2x^2 + x + 1$ 和 $g = 2x + 1$ 给出，更重要的是，q 和 r 的当前（但不是最终）值是 $q = \frac{1}{2}x^2$ 和 $r = \frac{3}{2}x^2 + x + 1$. 现在注意到 WHILE...DO 循环中的语句

$$q := q + \mathrm{LT}(r)/\mathrm{LT}(g),$$
$$r := r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$$

恰好对应于上述除法的下一步.

证明命题的最后一步是证明 q 和 r 的唯一性. 假设 $f = qg + r = q'g + r'$，其中 r 和 r' 的次数都小于 g（除非其中一个或两者都为 0）. 如果 $r \neq r'$，则 $\deg(r' - r) < \deg(g)$. 另一方面，由于

$$(q - q')g = r' - r, \tag{2}$$

会有 $q - q' \neq 0$，从而

$$\deg(r' - r) = \deg((q - q')g) = \deg(q - q') + \deg(g) \geqslant \deg(g).$$

这个矛盾迫使 $\boldsymbol{r = r'}$，然后由 (2) 可知 $q = q'$. 这完成了命题的证明. □

大多数计算机代数系统都实现了上述算法 [有一些修改——见 VON ZUR GATHEN 和 GERHARD (2013)] 用于多项式除法.

除法算法的一个有用推论涉及一元多项式的根的个数.

推论 3. *若 k 是域且 $f \in k[x]$ 是非零多项式，则 f 在 k 中至多有 $\deg(f)$ 个根.*

证明. 对 $m = \deg(f)$ 使用归纳法. 当 $m = 0$ 时，f 是非零常数，推论显然成立. 现在假设推论对所有次数为 $m - 1$ 的多项式成立，设 f 的次数为 m. 如果 f 在 k 中没有根，则证毕. 因此假设 a 是 k 中的一个根. 如果用 $x - a$ 除 f，则命题 2 告诉我们 $f = q(x - a) + r$，其中 $r \in k$，因为 $x - a$ 的次数为 1. 为确定 r，在 $x = a$ 处求两边的值，得到 $0 = f(a) = q(a)(a - a) + r = r$. 由此可见 $f = q(x - a)$. 还注意到 q 的次数为 $m - 1$.

断言 f 的任何不同于 a 的根也是 q 的根. 为说明这一点，设 $b \neq a$ 是 f 的一个根. 则 $0 = f(b) = q(b)(b - a)$ 意味着 $q(b) = 0$，因为 k 是域. 根据归纳假设，q 至多有 $m - 1$ 个根，因此 f 在 k 中至多有 m 个根. 这完成了证明. □

推论 3 曾被用来证明 §1 中的命题 5，该命题指出当 k 是无限域时 $\mathbf{I}(k^n) = \{0\}$. 这是几何事实可以是算法推论的一个例子.

还可以用命题 2 来确定 $k[x]$ 的所有理想的结构.

推论 4. *若 k 是域，则 $k[x]$ 的每个理想都可写成 $\langle f \rangle$ 的形式，其中 $f \in k[x]$. 此外，f 在乘以 k 中的非零常数后是唯一的.*

证明. 取理想 $I \subseteq k[x]$. 如果 $I = \{0\}$，则证毕，因为 $I = \langle 0 \rangle$. 否则，设 f 是 I 中包含的次数最小的非零多项式. 断言 $\langle f \rangle = I$. 包含关系 $\langle f \rangle \subseteq I$ 是显然的，因为 I 是理想. 反过来，取 $g \in I$. 由除法算法（命题 2），有 $g = qf + r$，其中要么 $r = 0$，要么 $\deg(r) < \deg(f)$. 由于 I 是理想，$qf \in I$，从而 $r = g - qf \in I$. 如果 $r \neq 0$，则 $\deg(r) < \deg(f)$，这与对 f 的选择矛盾. 因此 $r = 0$，从而 $g = qf \in \langle f \rangle$. 这证明了 $I = \langle f \rangle$.

为研究唯一性，假设 $\langle f \rangle = \langle g \rangle$. 则 $f \in \langle g \rangle$ 意味着 $f = hg$ 对某个多项式 h 成立. 因此

$$\deg(f) = \deg(h) + \deg(g), \tag{3}$$

从而 $\deg(f) \geqslant \deg(g)$. 交换 f 和 g 的同样论证表明 $\deg(f) \leqslant \deg(g)$，由此可见 $\deg(f) = \deg(g)$. 然后由 (3) 得 $\deg(h) = 0$，即 h 是非零常数. □

一般地，由一个元素生成的理想称为**主理想**. 鉴于推论 4，称 $k[x]$ 是**主理想整环**，简记为 PID.

推论 4 的证明告诉我们，$k[x]$ 中理想的生成元是该理想中包含的次数最小的非零多项式. 这个描述在实践中并不实用，因为它要求我们检查理想中所有多项式（有无穷多个）的次数. 有没有更好的方法来找到生成元？例如，如何找到理想

$$\langle x^4 - 1, x^6 - 1 \rangle \subseteq k[x]$$

的一个生成元?

解决这个问题的工具是最大公因子.

定义 5. *多项式 $f, g \in k[x]$ 的***最大公因子***是一个多项式 h，满足：*

(i) *h 整除 f 和 g*

(ii) *若 p 是另一个整除 f 和 g 的多项式，则 p 整除 h*

当 h 具有这些性质时，记 $h = \gcd(f, g)$.

以下是最大公因子的主要性质.

命题 6. *设 $f, g \in k[x]$. 则：*

(i) *$\gcd(f, g)$ 存在且在乘以 k 中的非零常数后唯一.*

(ii) *$\gcd(f, g)$ 是理想 $\langle f, g \rangle$ 的一个生成元.*

(iii) *存在求 $\gcd(f, g)$ 的算法.*

证明. 考虑理想 $\langle f, g \rangle$. 由于 $k[x]$ 的每个理想都是主理想（推论 4），存在 $h \in k[x]$ 使得 $\langle f, g \rangle = \langle h \rangle$. 断言 h 是 f, g 的最大公因子. 为说明这一点，首先注意到 h 整除 f 和 g，因为 $f, g \in \langle h \rangle$. 因此，定义 5 的第一部分被满足. 其次，假设 $p \in k[x]$ 整除 f 和 g. 这意味着 $f = Cp$ 且 $g = Dp$ 对某个 $C, D \in k[x]$ 成立. 由于 $h \in \langle f, g \rangle$，存在 A, B 使得 $Af + Bg = h$. 代入得

$$h = Af + Bg = ACp + BDp = (AC + BD)p,$$

这表明 p 整除 h. 因此，$h = \gcd(f, g)$.

这证明了最大公因子的存在性. 为证明唯一性，假设 h' 是 f 和 g 的另一个最大公因子. 则根据定义 5 的第二部分，h 和 h' 将互相整除. 这容易推出 h 是 h' 的非零常数倍. 因此，推论的 (i) 得证，而 (ii) 由在上一段中找到 h 的方式推出.

刚才给出的存在性证明在实践中并不有用. 它依赖于找到 $\langle f, g\rangle$ 的生成元的能力. 正如在推论 4 后的讨论中指出的，这涉及检查无穷多个多项式的次数. 幸运的是，有一个经典算法，称为 **Euclid 算法**，计算 $k[x]$ 中两个多项式的最大公因子. 这就是命题的 (iii) 部分的内容.

需要以下记号. 设 $f, g \in k[x]$，其中 $g \neq 0$，写 $f = qg + r$，其中 q 和 r 如命题 2 中所述. 则令 $r = \text{remainder}(f, g)$. 现在可以陈述求 $\gcd(f, g)$ 的 Euclid 算法：

输入: f, g

输出: $h = \gcd(f, g)$

$h := f$

$s := g$

WHILE $s \neq 0$ DO

$rem := \text{remainder}(h, s)$

$h := s$

$s := rem$

为理解该算法为何计算最大公因子，写 $f = qg + r$ 如命题 2 中所述. 断言

$$\gcd(f, g) = \gcd(f - qg, g) = \gcd(r, g). \tag{4}$$

为证明这一点，根据命题的 (ii) 部分，只需证明理想 $\langle f, g\rangle$ 和 $\langle f - qg, g\rangle$ 相等. 将这个简单的论证留作练习.

可以将 (4) 写成形式

$$\gcd(f, g) = \gcd(g, r).$$

注意到 $\deg(g) > \deg(r)$ 或 $r = 0$. 如果 $r \neq 0$，可以通过重复这个过程使问题更小. 因此，写 $g = q'r + r'$ 如命题 2 中所述，并如上论证，得到

$$\gcd(g, r) = \gcd(r, r'),$$

其中 $\deg(r) > \deg(r')$ 或 $r' = 0$. 继续这样做，得到

$$\gcd(f, g) = \gcd(g, r) = \gcd(r, r') = \gcd(r', r'') = \ldots, \tag{5}$$

其中次数下降

$$\deg(g) > \deg(r) > \deg(r') > \deg(r'') > \ldots,$$

或者当 $r, r', r'', \ldots$ 中有一个变为 0 时过程终止.

现在可以解释 Euclid 算法如何工作. 该算法有变量 h 和 s，可以在方程 (5) 中看到这些变量：h 的值是每个最大公因子中的第一个多项式，s 的值是第二个. 你应该验证在 (5) 中，从一个最大公因子到下一个恰好是算法中 WHILE...DO 循环所做的. 因此，在算法的每个阶段，$\gcd(h, s) = \gcd(f, g)$.

该算法必定会终止，因为 s 的次数不断下降，所以在某个阶段 $s = 0$. 当这种情况发生时，有 $\gcd(h, 0) = \gcd(f, g)$，并且由于 $\langle h, 0\rangle$ 显然等于 $\langle h\rangle$，有 $\gcd(h, 0) = h$. 结合这最后两个方程，当 $s = 0$ 时 $h = \gcd(f, g)$. 这证明了当算法终止时 h 是 f 和 g 的最大公因子，命题 6 的证明现在完成了. □

应该提到，也存在一个求两个整数最大公因子的 Euclid 算法版本. 大多数计算机代数系统都有一个求两个多项式（或整数）最大公因子的命令，它使用 Euclid 算法的修改形式 [更多细节见 VON ZUR GATHEN 和 GERHARD (2013)].

作为 Euclid 算法如何工作的例子，计算 $x^4 - 1$ 和 $x^6 - 1$ 的最大公因子. 首先，使用除法算法：

$$\begin{aligned} x^4 - 1 &= 0 \cdot (x^6 - 1) + x^4 - 1, \\ x^6 - 1 &= x^2(x^4 - 1) + x^2 - 1, \\ x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0. \end{aligned}$$

然后，由方程 (5)，有

$$\begin{aligned} \gcd(x^4 - 1, x^6 - 1) &= \gcd(x^6 - 1, x^4 - 1) \\ &= \gcd(x^4 - 1, x^2 - 1) = \gcd(x^2 - 1, 0) = x^2 - 1. \end{aligned}$$

注意到这个最大公因子计算回答了先前关于寻找理想 $\langle x^4 - 1, x^6 - 1\rangle$ 的生成元的问题. 即，命题 6 和 $\gcd(x^4 - 1, x^6 - 1) = x^2 - 1$ 意味着

$$\langle x^4 - 1, x^6 - 1\rangle = \langle x^2 - 1\rangle.$$

此时，很自然地会问由三个或更多多项式生成的理想会发生什么. 在这种情况下如何找到生成元？想法是将最大公因子的定义扩展到两个以上的多项式.

定义 7. 多项式 $f_1, \ldots, f_s \in k[x]$ 的**最大公因子**是一个多项式 h，满足：

(i) h 整除 $f_1, \ldots, f_s$

(ii) 若 p 是另一个整除 $f_1, \ldots, f_s$ 的多项式，则 p 整除 h

当 h 具有这些性质时，记 $h = \gcd(f_1, \ldots, f_s)$.

以下是这些最大公因子的主要性质.

命题 8. 设 $f_1, \ldots, f_s \in k[x]$，其中 $s \geqslant 2$. 则：

(i) $\gcd(f_1, \ldots, f_s)$ 存在且在乘以 k 中的非零常数后唯一.

(ii) $\gcd(f_1, \ldots, f_s)$ 是理想 $\langle f_1, \ldots, f_s \rangle$ 的一个生成元.

(iii) 若 $s \geqslant 3$，则 $\gcd(f_1, \ldots, f_s) = \gcd(f_1, \gcd(f_2, \ldots, f_s))$.

(iv) 存在求 $\gcd(f_1, \ldots, f_s)$ 的算法.

证明. (i) 和 (ii) 的证明类似于命题 6 中给出的证明，此处省略. 为证明 (iii)，设 $h = \gcd(f_2, \ldots, f_s)$. 将其留作练习来证明

$$\langle f_1, h \rangle = \langle f_1, f_2, \ldots, f_s \rangle.$$

由该命题的 (ii) 部分，看到

$$\langle \gcd(f_1, h) \rangle = \langle \gcd(f_1, \ldots, f_s) \rangle.$$

然后 $\gcd(f_1, h) = \gcd(f_1, \ldots, f_s)$ 由推论 4 的唯一性部分得出，这证明了要证明的结论.

最后，需要证明存在求 $\gcd(f_1, \ldots, f_s)$ 的算法. 基本思想是将 (iii) 部分与 Euclid 算法结合. 例如，假设要计算四个多项式 f_1, f_2, f_3, f_4 的最大公因子. 使用该命题的 (iii) 部分两次，得到

$$\begin{aligned} \gcd(f_1, f_2, f_3, f_4) &= \gcd(f_1, \gcd(f_2, f_3, f_4)) \\ &= \gcd(f_1, \gcd(f_2, \gcd(f_3, f_4))). \end{aligned} \tag{6}$$

然后如果使用 Euclid 算法三次 [对 (6) 中第二行的每个最大公因子各一次]，就得到 f_1, f_2, f_3, f_4 的最大公因子. 在练习中，你将被要求为一个对任意多个多项式实现这一思想的算法编写伪代码. 命题 8 得证. □

大多数计算机代数系统中的最大公因子命令一次只能处理两个多项式. 因此，要处理两个以上的多项式，你需要使用命题 8 的证明中描述的方法. 例如，考虑理想

$$\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle \subseteq k[x].$$

知道 $\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$ 是一个生成元. 此外，可以验证

$$\begin{aligned} \gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= \gcd(x^3 - 3x + 2, \gcd(x^4 - 1, x^6 - 1)) \\ &= \gcd(x^3 - 3x + 2, x^2 - 1) = x - 1. \end{aligned}$$

由此可见

$$\langle x^3-3x+2, x^4-1, x^6-1\rangle = \langle x-1\rangle.$$

更一般地，给定 $f_1,\dots,f_s \in k[x]$，显然现在有了求 $\langle f_1,\dots,f_s\rangle$ 的生成元的算法.

作为这里开发的算法的另一个应用，考虑来自 §4 的理想成员问题：给定 $f_1,\dots,f_s \in k[x]$，是否存在一个算法来判断给定多项式 $f \in k[x]$ 是否属于理想 $\langle f_1,\dots,f_s\rangle$？答案是肯定的，算法很容易描述. 第一步是使用最大公因子来找到 $\langle f_1,\dots,f_s\rangle$ 的生成元 h. 然后，由于 $f \in \langle f_1,\dots,f_s\rangle$ 等价于 $f \in \langle h\rangle$，只需使用除法算法写 $f = qh + r$，其中 $\deg(r) < \deg(h)$. 由此可见 f 在理想中当且仅当 $r = 0$. 例如，假设想知道

$$x^3+4x^2+3x-7 \in \langle x^3-3x+2, x^4-1, x^6-1\rangle.$$

在上面看到 $x-1$ 是这个理想的生成元，因此问题可以重新表述为

$$x^3+4x^2+3x-7 \in \langle x-1\rangle.$$

除法给出

$$x^3+4x^2+3x-7 = (x^2+5x+8)(x-1)+1.$$

因此 x^3+4x^2+3x-7 不在理想 $\langle x^3-3x+2, x^4-1, x^6-1\rangle$ 中. 在第 2 章中，将使用类似的策略来解决 $k[x_1,\dots,x_n]$ 中多项式的理想成员问题. 首先找到理想的一个好基（称为 Gröbner 基），然后使用一个推广的除法算法来确定一个多项式是否在理想中.

在练习中，将看到在一元情形下，前几节提出的其他问题可以使用这里讨论的方法算法地解决.

1.5.1 习题

(1) 在复数域 $\mathbb{C}$ 上，推论 3 可以被表述为更强的形式. 即，证明若 $f \in \mathbb{C}[x]$ 是次数 $n > 0$ 的多项式，则 f 可写成形式 $f = c(x-a_1)\cdots(x-a_n)$，其中 $c, a_1,\dots,a_n \in \mathbb{C}$ 且 $c \neq 0$. 提示：使用 §1 的定理 7. 注意这个结果对任何代数闭域都成立.

(2) 尽管推论 3 很容易证明，但它有一些很好的推论. 例如，考虑域 k 中由 $a_1,\dots,a_n$ 确定的 $n \times n$ **Vandermonde 行列式**：

$$\det\begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix}.$$

证明当 a_i 互不相同时，该行列式非零. 提示：若行列式为零，则列线性相关. 证明线性关系的

系数确定了一个次数 $\leqslant n-1$ 的多项式，它有 n 个根. 然后使用推论 3.

(3) $k[x]$ 的每个理想都是主理想（由一个元素生成）这一事实是一元多项式情形的特殊性质. 在本练习中将看到原因. 即，考虑理想 $I=\langle x,y\rangle \subseteq k[x,y]$. 证明 I 不是主理想. 提示：若 $x=fg$，其中 $f,g\in k[x,y]$，则证明 f 或 g 是常数. 由此可见本节给出的最大公因子处理方法只适用于一元多项式. 可以计算 $\geqslant 2$ 个变量多项式的最大公因子，但涉及的理论更复杂 [见 VON ZUR GATHEN 和 GERHARD (2013)，第 6 章].

(4) 若 h 是 $f,g\in k[x]$ 的最大公因子，则证明存在 $A,B\in k[x]$ 使得 $Af+Bg=h$.

(5) 若 $f,g\in k[x]$，则证明对任何 $q\in k[x]$ 有 $\langle f-qg,g\rangle=\langle f,g\rangle$. 这将证明正文中的方程 (4).

(6) 给定 $f_1,\dots,f_s\in k[x]$，设 $h=\gcd(f_2,\dots,f_s)$. 则使用等式 $\langle h\rangle=\langle f_2,\dots,f_s\rangle$ 证明 $\langle f_1,h\rangle=\langle f_1,f_2,\dots,f_s\rangle$. 这个等式用于命题 8 的 (iii) 的证明中.

(7) 若你一次只能计算两个多项式的最大公因子（这对某些计算机代数系统成立），给出计算多项式 $f_1,\dots,f_s\in k[x]$（其中 $s>2$）最大公因子的算法的伪代码. 证明你的算法有效. 提示：见 (6). 这将完成命题 8 的 (iv) 的证明.

(8) 使用计算机代数系统计算下列最大公因子：

(a) $\gcd(x^4+x^2+1,x^4-x^2-2x-1,x^3-1)$.

(b) $\gcd(x^3+2x^2-x-2,x^3-2x^2-x+2,x^3-x^2-4x+4)$.

(9) 使用正文描述的方法判断 x^2-4 是否属于理想 $\langle x^3+x^2-4x-4,x^3-x^2-4x+4,x^3-2x^2-x+2\rangle$.

(10) 给出具有输入 $f,g\in k[x]$ 和输出 $h,A,B\in k[x]$ 的算法的伪代码，其中 $h=\gcd(f,g)$ 且 $Af+Bg=h$. 提示：想法是向算法添加变量 A,B,C,D，使得 $Af+Bg=h$ 和 $Cf+Dg=s$ 在算法的每一步都保持成立. 注意 A,B,C,D 的初始值分别是 $1,0,0,1$. 你可能发现让 $\operatorname{quotient}(f,g)$ 表示 f 除以 g 的商是有用的，即，如果除法算法给出 $f=qg+r$，则 $q=\operatorname{quotient}(f,g)$.

(11) 在本练习中，将研究来自 §2 的相容性问题的单变量情形. 给定 $f_1,\dots,f_s\in k[x]$，这询问是否存在一个算法来判断 $\mathbf{V}(f_1,\dots,f_s)$ 是否非空. 将看到当 $k=\mathbb{C}$ 时答案是肯定的.

(a) 设 $f\in\mathbb{C}[x]$ 是非零多项式. 则使用 §1 的定理 7 证明 $\mathbf{V}(f)=\emptyset$ 当且仅当 f 是常数.

(b) 若 $f_1,\dots,f_s\in\mathbb{C}[x]$，证明 $\mathbf{V}(f_1,\dots,f_s)=\emptyset$ 当且仅当 $\gcd(f_1,\dots,f_s)=1$.

(c) 用文字描述（而非伪代码）一个确定 $\mathbf{V}(f_1,\dots,f_s)$ 是否非空的算法.

当 $k=\mathbb{R}$ 时，相容性问题困难得多. 它需要一个算法来判断多项式 $f\in\mathbb{R}[x]$ 是否有实根.

(12) 本练习将研究来自 §4 的零点定理问题的单变量情形，它询问当 $f_1,\dots,f_s\in\mathbb{C}[x]$ 时，$\mathbf{I}(\mathbf{V}(f_1,\dots,f_s))$ 与 $\langle f_1,\dots,f_s\rangle$ 之间的关系. 通过使用最大公因子，可以约化到单个生成元的情形. 因此，在本问题中，当 $f\in\mathbb{C}[x]$ 是非常数多项式时，将显式确定 $\mathbf{I}(\mathbf{V}(f))$. 由于在复数上工作，由练习 1 知道 f 完全分解，即

$$f=c(x-a_1)^{r_1}\cdots(x-a_l)^{r_l},$$

其中 $a_1,\dots,a_l\in\mathbb{C}$ 互不相同，$c\in\mathbb{C}\setminus\{0\}$. 定义多项式

$$f_{\text{red}}=c(x-a_1)\cdots(x-a_l).$$

多项式 f 和 f_{red} 有相同的根，但它们的重数可能不同. 特别地，f_{red} 的所有根的重数都是 1. 称 f_{red} 为 f 的**约化**或**无平方部分**. 后一个名称承认 f_{red} 是 f 的次数最大的无平方因子.

(a) 证明 $\mathbf{V}(f) = \{a_1, \ldots, a_l\}$.

(b) 证明 $\mathbf{I}(\mathbf{V}(f)) = \langle f_{\text{red}} \rangle$.

虽然 (b) 部分描述了 $\mathbf{I}(\mathbf{V}(f))$，但答案并不完全令人满意，因为需要完全分解 f 才能找到 f_{red}. 在练习 13、14 和 15 中，将展示如何在不进行任何分解的情况下确定 f_{red}.

(13) 将研究 $f = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n \in \mathbb{C}[x]$ 的形式导数. 形式导数由微积分中的常用公式定义：

$$f' = nc_0x^{n-1} + (n-1)c_1x^{n-2} + \cdots + c_{n-1} + 0.$$

证明下列微分法则适用：

$$\begin{aligned}(af)' &= af' \quad \text{当} a \in \mathbb{C},\\ (f+g)' &= f' + g',\\ (fg)' &= f'g + fg'.\end{aligned}$$

(14) 在本练习中，将使用练习 13 的微分性质来计算 $f \in \mathbb{C}[x]$ 时的 $\gcd(f, f')$.

(a) 假设 $f = (x-a)^r h$ 在 $\mathbb{C}[x]$ 中，其中 $r \geqslant 1$ 且 $h(a) \neq 0$. 则证明 $f' = (x-a)^{r-1}h_1$，其中 $h_1 \in \mathbb{C}[x]$ 在 a 处不消失. 提示：使用乘积法则.

(b) 设 $f = c(x-a_1)^{r_1} \cdots (x-a_l)^{r_l}$ 是 f 的分解，其中 $a_1, \ldots, a_l$ 互不相同. 证明 f' 是乘积 $f' = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}H$，其中 $H \in \mathbb{C}[x]$ 是在 $a_1, \ldots, a_l$ 处都不消失的多项式.

(c) 证明 $\gcd(f, f') = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}$.

(15) 考虑练习 12 中定义的 $f \in \mathbb{C}[x]$ 的无平方部分 f_{red}.

(a) 使用练习 14 证明 f_{red} 由公式

$$f_{\text{red}} = \frac{f}{\gcd(f, f')}$$

给出. 这个公式的优点在于它允许我们找到无平方部分而无需分解 f. 这使得计算更快.

(b) 使用计算机代数系统找到多项式

$$x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1$$

的无平方部分.

(16) 使用练习 12 和 15 用文字描述（而非伪代码）一个算法，其输入由多项式 $f_1, \ldots, f_s \in \mathbb{C}[x]$ 组成，输出由 $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ 的基组成. 处理多于一个变量的多项式时，构造这样的算法更困难.

(17) 找到理想 $\mathbf{I}(\mathbf{V}(x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1))$ 的一个基.

第二章
Gröbner 基

在第一章中，我们已经看到多项式环 $k[x_1,\ldots,x_n]$ 的代数结构与仿射代数簇的几何结构是如何联系在一起的. 本章将研究 Gröbner 基的方法，它能够以算法或计算的方式来解决关于多项式理想的问题. Gröbner 基的方法也被用于多个强大的计算机代数系统中，以研究应用中出现的特定多项式理想. 在第一章中，我们提出了许多关于多项式理想之代数与仿射簇之几何的问题. 本章及下一章将关注其中四个问题.

第 1 节　§1 引言

2.1.1　问题

(a) **理想描述问题**：是否每个理想 $I \subseteq k[x_1,\ldots,x_n]$ 都有有限基？换句话说，我们能否将 I 写成 $I = \langle f_1,\ldots,f_s\rangle$ 的形式，其中 $f_i \in k[x_1,\ldots,x_n]$?

(b) **理想成员问题**：给定 $f \in k[x_1,\ldots,x_n]$ 和一个理想 $I = \langle f_1,\ldots,f_s\rangle$，判断 f 是否属于 I. 从几何上看，这与判断 $\mathbf{V}(f_1,\ldots,f_s)$ 是否落在簇 $\mathbf{V}(f)$ 上的问题密切相关.

(c) **多项式方程求解问题**：求多项式方程组

$$f_1(x_1,\ldots,x_n) = \cdots = f_s(x_1,\ldots,x_n) = 0$$

在 k^n 中的所有公共解. 这等价于求仿射簇 $\mathbf{V}(f_1,\ldots,f_s)$ 中的点.

(d) **隐式化问题**：设 $V \subseteq k^n$ 以参数形式给出为

$$
\begin{aligned}
x_1 &= g_1(t_1, \ldots, t_m),\\
&\bullet\\
&\vdots\\
&\bullet\\
x_n &= g_n(t_1, \ldots, t_m).
\end{aligned}
$$

若 g_i 是变量 t_j 的多项式（或有理函数），则 V 将是一个仿射簇或其中的一部分. 求定义该簇的关于 x_i 的多项式方程组.

需要做一些说明. 问题（a）询问是否每个多项式理想都有通过生成元给出的有限描述. 到目前为止，见过的许多理想确实具有这样的描述——事实上，研究过的大多数理想都是通过给出有限生成集来指定的. 然而，还有其他构造理想的方式并不直接导致这种描述. 我们见过的主要例子是簇的理想 $\mathbf{I}(V)$. 知道这些理想也具有有限描述将是有用的. 另一方面，在习题中，我们将看到如果允许无限多个变量出现在多项式中，那么问题（a）的答案是否定的.

注意，问题（c）和（d）可以说是互逆的问题. 在问题（c）中，我们要求给定多项式方程组的解集. 而在问题（d）中，给出了解集，问题是要找到一个具有这些解的方程组.

为开始研究 Gröbner 基，下面考虑一些特殊情况，在这些情况中读者已经见过解决上述问题的算法技术.

例 1. 当 $n = 1$ 时，我们在第一章的 *§5* 中解决了理想描述问题. 即，给定理想 $I \subseteq k[x]$，我们证明了 $I = \langle g \rangle$ 对某个 $g \in k[x]$ 成立（见第一章 *§5* 的推论 *4*）. 因此，在这种情况下理想具有特别简单的描述.

我们也在第一章的 *§5* 中看到，理想成员问题的解很容易从除法算法得出：给定 $f \in k[x]$，要检查 f 是否属于 $I = \langle g \rangle$，用 g 除 f：

$$f = q \cdot g + r,$$

其中 $q, r \in k[x]$ 且 $r = 0$ 或 $\deg(r) < \deg(g)$. 然后我们证明了 $f \in I$ 当且仅当 $r = 0$. 因此，在 $n = 1$ 的情况下，存在一个算法测试来判断理想成员.

例 2. 其次，设 n（变量个数）任意，考虑求解多项式方程组的问题：

$$a_{11}x_1 + \cdots + a_{1n}x_n + b_1 = 0,$$

$$a_{m1}x_1 + \cdots + a_{mn}x_n + b_m = 0,$$

其中每个多项式都是线性的（总次数为 1）.

第 2 节 §2 $k[x_1,\dots,x_n]$ 中单项式的序

如果我们仔细考察 $k[x]$ 中的除法算法以及用于线性方程组（或矩阵）的行约化（Gauss 消元法）算法，就会发现多项式中项的排序概念是两者的关键要素（尽管这一点并不常被强调）. 例如，在使用标准方法将 $f(x)=x^5-3x^2+1$ 除以 $g(x)=x^2-4x+7$ 时，我们会：

将多项式中的项按 x 的次数降序排列

在第一步，f 的首项（次数最高的项）是 $x^5=x^3\cdot x^2=x^3$（g 的首项）. 因此，我们从 f 中减去 $x^3\cdot g(x)$ 以消去首项，得到 $4x^4-7x^3-3x^2+1$.

然后，我们对 $f(x)-x^3\cdot g(x)$ 重复相同的过程，以此类推，直到得到一个次数小于 2 的多项式.

对于单变量多项式的除法算法，我们处理的是单变量单项式的次数序：

$$\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1. \tag{1}$$

该算法的成功取决于系统地处理 f 和 g 的首项，而不是使用 g 中的任意项从 f 中“随机”消去项.

类似地，在矩阵的行约化算法中，对于每一行，我们首先系统地处理左侧的项——首项是行中最左侧的非零项. 在线性方程的层面，这通过如下方式对变量 $x_1,\dots,x_n$ 排序来表达：

$$x_1 > x_2 > \cdots > x_n. \tag{2}$$

我们将方程中的项按降序排列. 此外，在阶梯形系统中，方程按其首项的降序排列.（事实上，阶梯形系统的精确定义可以用这种排序来给出——见习题 8.）

从上述证据来看，我们可以推测，将除法和行约化推广到多变元任意多项式的任何扩展的一个主要组成部分将是 $k[x_1,\dots,x_n]$ 中多项式项的排序. 在本节中，我们将讨论这种排序应该具有的理想性质，并构造几个满足我们要求的不同例子. 这些排序中的每一个在不同的上下文中都非常有用.

首先，我们注意到可以从 n 元指数组 $\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{Z}^n_{\geqslant 0}$ 重构单项式 $x^\alpha=x_1^{\alpha_1}\cdots x_n^{\alpha_n}$. 这个观察建立了 $k[x_1,\dots,x_n]$ 中的单项式与 $\mathbb{Z}^n_{\geqslant 0}$ 之间的一一对应关系. 此外，我们在空间 $\mathbb{Z}^n_{\geqslant 0}$ 上建立的任何排序 $>$ 都会给我们一个单项式的排序：如果根据这种排序 $\alpha>\beta$，我们也将说 $x^\alpha>x^\beta$.

在 $\mathbb{Z}^n_{\geqslant 0}$ 上定义排序有很多不同的方法. 然而，对于我们的目的，这些方法中的大多数都不适用，因为我们希望我们的排序与多项式环的代数结构相容.

首先，由于多项式是单项式的和，我们希望能够将多项式中的项按降序（或升序）无歧义地排列. 为此，我们必须能够比较每一对单项式以确定它们的正确相对位置. 因此，我们将要求我们的排序是线性或全序. 这意味着对于每一对单项式 x^α 和 x^β，以下三个陈述中恰好有一个应该为真：

$$x^\alpha > x^\beta, \qquad x^\alpha = x^\beta, \qquad x^\beta > x^\alpha$$

全序还要求传递性，即 $x^\alpha > x^\beta$ 和 $x^\beta > x^\gamma$ 总是蕴含 $x^\alpha > x^\gamma$.

接下来，我们必须考虑和与积运算对多项式的影响. 当我们相加多项式时，合并同类项后，我们可以简单地将存在的项重新排列为适当的顺序，因此加法不会带来困难. 然而，乘积更为微妙. 由于多项式环中的乘法对加法满足分配律，只需考虑当我们将单项式乘以多项式时会发生什么. 如果这样做改变了项的相对顺序，那么在任何类似于 $k[x]$ 中除法算法的过程中都可能出现重大问题，因为在此过程中我们必须识别多项式的首项. 原因是乘积中的首项可能与该单项式和原多项式首项的乘积不同.

因此，我们将要求所有单项式序具有以下附加性质. 如果 $x^\alpha > x^\beta$ 且 x^γ 是任意单项式，那么我们要求 $x^\alpha x^\gamma > x^\beta x^\gamma$. 用指数向量来说，这个性质意味着如果我们在 $\mathbb{Z}^n_{\geqslant 0}$ 上的排序中有 $\alpha > \beta$，那么对于所有 $\gamma \in \mathbb{Z}^n_{\geqslant 0}$，都有 $\alpha + \gamma > \beta + \gamma$.

考虑到这些因素，下面给出定义.

定义 1. $k[x_1, \ldots, x_n]$ 上的一个单项式序 $>$ 是 $\mathbb{Z}^n_{\geqslant 0}$ 上的一个关系 $>$，或者等价地，是单项式集合 $\{x^\alpha \mid \alpha \in \mathbb{Z}^n_{\geqslant 0}\}$ 上的一个关系，满足：

(i) $>$ 是 $\mathbb{Z}^n_{\geqslant 0}$ 上的一个全序（或线性序）

(ii) 如果 $\alpha > \beta$ 且 $\gamma \in \mathbb{Z}^n_{\geqslant 0}$，则 $\alpha + \gamma > \beta + \gamma$

(iii) $>$ 是 $\mathbb{Z}^n_{\geqslant 0}$ 上的一个良序. 这意味着 $\mathbb{Z}^n_{\geqslant 0}$ 的每个非空子集在 $>$ 下都有最小元. 换句话说，如果 $A \subseteq \mathbb{Z}^n_{\geqslant 0}$ 非空，则存在 $\alpha \in A$ 使得对于 A 中每个 $\beta \neq \alpha$ 都有 $\beta > \alpha$.

给定一个单项式序 $>$，当 $\alpha > \beta$ 或 $\alpha = \beta$ 时，我们说 $\alpha \geqslant \beta$.

以下引理将帮助我们理解定义中第（iii）部分的良序条件的含义.

引理 2. $\mathbb{Z}^n_{\geqslant 0}$ 上的序关系 $>$ 是良序当且仅当 $\mathbb{Z}^n_{\geqslant 0}$ 中的每个严格递减序列

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots$$

最终终止.

证明. 我们以其逆否命题的形式证明：$>$ 不是良序当且仅当 $\mathbb{Z}^n_{\geqslant 0}$ 中存在无限严格递减序列.

如果 $>$ 不是良序，那么某个非空子集 $S \subseteq \mathbb{Z}^n_{\geqslant 0}$ 没有最小元. 现在取 $\alpha(1) \in S$. 由于 $\alpha(1)$ 不是最小元，我们可以在 S 中找到 $\alpha(1) > \alpha(2)$. 那么 $\alpha(2)$ 也不是最小元，因此在 S 中存在 $\alpha(2) > \alpha(3)$. 继续这样做，我们得到一个无限严格递减序列

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots.$$

反之，给定这样一个无限序列，则 $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ 是 $\mathbb{Z}^n_{\geqslant 0}$ 的一个没有最小元的非空子集，因此 $>$ 不是良序. □

这个引理的重要性将在后面显现出来. 它将用于证明各种算法必须终止，因为在算法的每一步某个项都严格递减（相对于固定的单项式序）.

在 §4 中，我们将看到，给定定义 1 中的第（i）和（ii）部分，第（iii）部分的良序条件等价于对所有 $\alpha \in \mathbb{Z}^n_{\geqslant 0}$ 都有 $\alpha \geqslant 0$.

作为单项式序的一个简单例子，注意 $\mathbb{Z}_{\geqslant 0}$ 上通常的数值序

$$\cdots > m+1 > m > \cdots > 3 > 2 > 1 > 0$$

满足定义 1 的三个条件. 因此，$k[x]$ 上的次数序（1）是一个单项式序，由习题 13 可知它是唯一的.

我们对 n 元组排序的第一个例子将是字典序（或简称字典序）.

定义 3（字典序）. 设 $\alpha = (\alpha_1, \ldots, \alpha_n)$ 和 $\beta = (\beta_1, \ldots, \beta_n)$ 属于 $\mathbb{Z}^n_{\geqslant 0}$. 如果向量差 $\alpha - \beta \in \mathbb{Z}^n$ 的最左边非零项为正，则我们说 $\alpha >_{lex} \beta$. 如果 $\alpha >_{lex} \beta$，我们将写 $x^\alpha >_{lex} x^\beta$.

以下是一些例子：

(a) $(1,2,0) >_{lex} (0,3,4)$，因为 $\alpha - \beta = (1,-1,-4)$.

(b) $(3,2,4) >_{lex} (3,2,1)$，因为 $\alpha - \beta = (0,0,3)$.

(c) 变量 $x_1, \ldots, x_n$ 按字典序以通常的方式排序（见（2））：

$$(1,0,\ldots,0) >_{lex} (0,1,0,\ldots,0) >_{lex} \cdots >_{lex} (0,\ldots,0,1).$$

因此$x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$.

在实践中，当我们处理两个或三个变量的多项式时，我们将变量称为 x, y, z 而不是 x_1, x_2, x_3. 我们还将假设，除非明确说明，否则变量上的字母顺序 $x > y > z$ 用于定义字典序.

字典序类似于字典中使用的词的排序（因此得名）. 我们可以将 n 元组 $\alpha \in \mathbb{Z}^n_{\geqslant 0}$ 的项看作词中字母的类比. 字母按字母顺序排列：

$$\mathrm{a} > \mathrm{b} > \cdots > \mathrm{y} > \mathrm{z}.$$

那么，例如

$$\text{arrow} >_{lex} \text{arson}$$

因为 “arson” 的第三个字母在字母顺序中排在 “arrow” 的第三个字母之后，而前两个字母在两者中是相同的. 由于所有元素 $\alpha \in \mathbb{Z}^n_{\geqslant 0}$ 的长度都是 n，这个类比仅适用于固定字母数的词.

为了完整性，我们必须检查字典序是否满足定义 1 的三个条件.

命题 4. $\mathbb{Z}^n_{\geqslant 0}$ 上的字典序是一个单项式序.

证明. （i）$>_{lex}$ 是全序直接从定义和 $\mathbb{Z}_{\geqslant 0}$ 上通常的数值序是全序这一事实得出.

(ii) 如果 $\alpha >_{lex} \beta$，则我们有向量差 $\alpha - \beta$ 中最左边的非零项，比如 $\alpha_i - \beta_i$，是正的. 但是 $x^\alpha x^\gamma = x^{\alpha+\gamma}$ 且 $x^\beta x^\gamma = x^{\beta+\gamma}$. 那么在 $(\alpha+\gamma)-(\beta+\gamma) = \alpha - \beta$ 中，最左边的非零项又是 $\alpha_i - \beta_i > 0$.

(iii) 假设 $>_{lex}$ 不是良序. 那么根据引理 2，将存在 $\mathbb{Z}^n_{\geqslant 0}$ 的元素的一个无限严格递减序列

$$\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \dots$$

我们将证明这导致矛盾.

考虑向量 $\alpha(i) \in \mathbb{Z}^n_{\geqslant 0}$ 的第一项. 根据字典序的定义，这些第一项形成一个非负整数的非增序列. 由于 $\mathbb{Z}_{\geqslant 0}$ 是良序的，$\alpha(i)$ 的第一项最终必须 “稳定”. 换句话说，存在一个 ℓ 使得所有 $i \geqslant \ell$ 的 $\alpha(i)$ 的第一项都相等.

从 $\alpha(\ell)$ 开始，第二项及以后的项在确定字典序时开始发挥作用.$\alpha(\ell), \alpha(\ell+1), \dots$ 的第二项形成一个非增序列. 根据与之前相同的推理，第二项最终也会 “稳定”. 继续同样的方式，我们看到对于某个 m，$\alpha(m), \alpha(m+1), \dots$ 都相等. 这与 $\alpha(m) >_{lex} \alpha(m+1)$ 的事实矛盾. □

重要的是要认识到有许多字典序，对应于变量的不同排序方式. 到目前为止，我们使用了 $x_1 > x_2 > \cdots > x_n$ 的字典序. 但是给定变量的任何排序 $x_1, \dots, x_n$，都有一个相应的字典序. 例如，如果变量是 x 和 y，那么当 $x > y$ 时我们得到一个字典序，当 $y > x$ 时我们得到另一个. 在一般的 n 变量情况下，有 $n!$ 个字典序. 在下文中，“字典序” 一词将指 $x_1 > \cdots > x_n$ 的那个，除非另有说明.

在字典序中，注意一个变量支配任何只涉及更小变量的单项式，无论其总次数如何. 因此，对于 $x > y > z$ 的字典序，我们有 $x >_{lex} y^5 z^3$. 对于某些目的，我们可能还想考虑单项式的总次数并首先排序总次数较大的单项式. 一种方法是分次字典序（或分次字典序）.

定义 5（分次字典序）. 设 $\alpha, \beta \in \mathbb{Z}^n_{\geqslant 0}$. 如果

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i, \quad \text{或} \quad |\alpha| = |\beta| \text{ 且} \alpha >_{lex} \beta.$$

则我们说 $\alpha >_{grlex} \beta$.

我们看到分次字典序首先按总次数排序，然后使用字典序 “打破平局”. 以下是一些例子：

(a) $(1,2,3) >_{grlex} (3,2,0)$，因为 $|(1,2,3)| = 6 > |(3,2,0)| = 5$.

(b) $(1,2,4) >_{grlex} (1,1,5)$，因为 $|(1,2,4)| = |(1,1,5)|$ 且 $(1,2,4) >_{lex} (1,1,5)$.

(c) 变量按字典序排序，即 $x_1 >_{grlex} \cdots >_{grlex} x_n$.

我们将把它作为习题，证明分次字典序满足定义 1 的三个条件. 与字典序的情况一样，根据变量的排序方式，n 个变量上有 $n!$ 个分次字典序.

单项式的另一种（某种程度上不太直观的）序是分次反字典序（或 grevlex 序）. 尽管这种排序 “需要一些时间来适应”，但已经证明对于某些运算，grevlex 排序是计算中最有效的.

定义 6（分次反字典序）. 设 $\alpha, \beta \in \mathbb{Z}^n_{\geqslant 0}$. 如果

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i,$$

或 $|\alpha| = |\beta|$ 且 $\alpha - \beta \in \mathbb{Z}^n$ 的最右边非零项为负，则我们说 $\alpha >_{grevlex} \beta$.

与分次字典序一样，grevlex 按总次数排序，但它以不同的方式 “打破平局”. 例如：

(a) $(4,7,1) >_{grevlex} (4,2,3)$，因为 $|(4,7,1)| = 12 > |(4,2,3)| = 9$.

(b) $(1,5,2) >_{grevlex} (4,1,3)$，因为 $|(1,5,2)| = |(4,1,3)|$ 且 $(1,5,2) - (4,1,3) = (-3,4,-1)$.

你将在习题中证明 grevlex 排序给出一个单项式序. 还要注意，字典序和 grevlex 在变量上给出相同的排序. 即

$$(1,0,\ldots,0) >_{grevlex} (0,1,\ldots,0) >_{grevlex} \cdots >_{grevlex} (0,\ldots,0,1)$$

或

$$x_1 >_{grevlex} x_2 >_{grevlex} \cdots >_{grevlex} x_n$$

因此，grevlex 确实与变量重新排列后的分次字典序不同（人们可能会从名称中误以为如此）.

为了解释分次字典序和 grevlex 之间的关系，注意两者都以相同的方式使用总次数. 为了打破平局，分次字典序使用字典序，因此它查看最左边（或最大）的变量并倾向于较大的幂. 相反，当 grevlex 发现相同的总次数时，它查看最右边（或最小）的变量并倾向于较小的幂. 在习题中，你将验证这相当于对字典序的 “双重反转”. 例如，

$$x^5yz >_{grlex} x^4yz^2,$$

因为两个单项式的总次数都是 7 且 $x^5yz >_{lex} x^4yz^2$. 在这种情况下，我们也有

$$x^5yz >_{grevlex} x^4yz^2,$$

但原因不同：x^5yz 更大是因为较小的变量 z 出现的幂次较小.

与字典序和分次字典序一样，根据 n 个变量的排序方式，有 $n!$ 个 grevlex 序.

除了这里考虑的序之外，还有许多其他单项式序. 其中一些将在 §4 的习题中探讨. 大多数计算机代数系统实现字典序，大多数还允许其他序，如分次字典序和 grevlex. 一旦选择了这样的序，这些系统允许用户指定变量的 $n!$ 种排序中的任何一种. 正如我们将在本章 §8 和以后的章节中看到的，当研究各种问题时，这种工具非常有用.

我们将以讨论单项式序如何应用于多项式来结束本节. 如果 $f = \sum_\alpha a_\alpha x^\alpha$ 是 $k[x_1,\ldots,x_n]$ 中的

一个非零多项式，并且我们选择了一个单项式序 $>$，那么我们可以根据 $>$ 无歧义地将 f 的单项式排序. 例如，考虑多项式 $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x, y, z]$. 那么：

对于字典序，我们将 f 的项按降序重新排列为

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2.$$

对于分次字典序，我们将有

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2.$$

• 对于 grevlex 序，我们将有

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2.$$

我们将使用以下术语.

定义 7. 设 $f = \sum_\alpha a_\alpha x^\alpha$ 是 $k[x_1, \ldots, x_n]$ 中的一个非零多项式，并设 $>$ 是一个单项式序.

(i) f 的多重次数是

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geqslant 0} \mid a_\alpha \neq 0)$$

（最大值是相对于 $>$ 取的）.

(ii) f 的首项系数是

$$\text{LC}(f) = a_{\text{multideg}(f)} \in k.$$

(iii) f 的首项单项式是

$$\text{LM}(f) = x^{\text{multideg}(f)}$$

（系数为 *1*）.

(iv) f 的首项是

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

为了说明，设 $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ 如前，并设 $>$ 表示字典序. 则

$$\begin{aligned}
&\text{multideg}(f) = (3, 0, 0),\\
&\text{LC}(f) = -5,\\
&\text{LM}(f) = x^3,\\
&\text{LT}(f) = -5x^3.
\end{aligned}$$

在习题中，你将证明多重次数具有以下有用的性质.

引理 8. 设 $f, g \in k[x_1, \ldots, x_n]$ 是非零多项式. 则:

(i) $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$

(ii) 如果 $f+g \neq 0$, 则 $\text{multideg}(f+g) \leqslant \max(\text{multideg}(f), \text{multideg}(g))$. 此外, 如果 $\text{multideg}(f) \neq \text{multideg}(g)$, 则等式成立.

一些书籍使用不同的术语. 在 EISENBUD（1999）中, 首项 $\text{LT}(f)$ 变成初始项 $\text{in}_>(f)$. 在 BECKER 和 WEISPFENNING（1993）中出现了更实质性的差异, 其中 "单项式" 和 "项" 的含义互换. 对他们来说, 首项 $\text{LT}(f)$ 是首单项式 $\text{HM}(f)$, 而首项单项式 $\text{LM}(f)$ 是首项 $\text{HT}(f)$. KREUZER 和 ROBBIANO（2000）的第 10 页总结了不同书籍中使用的术语. 我们建议阅读其他文本时仔细检查定义.

第 3 节 §3 $k[x_1, \ldots, x_n]$ 中的除法算法

在 §1 中, 我们看到除法算法如何用于解决单变量多项式的理想成员问题. 为研究多变元时的这个问题, 我们将为 $k[x_1, \ldots, x_n]$ 中的多项式制定一个除法算法, 它扩展了 $k[x]$ 的算法. 在一般情况下, 目标是将 $f \in k[x_1, \ldots, x_n]$ 除以 $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. 正如我们将看到的, 这意味着将 f 表示为形式

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

其中 "商"$q_1, \ldots, q_s$ 和余式 r 属于 $k[x_1, \ldots, x_n]$. 在决定如何刻画余式时需要一些小心. 这就是我们将使用 §2 中引入的单项式序的地方. 然后我们将看到除法算法如何应用于理想成员问题.

该算法的基本思想与单变量情况相同: 我们希望通过将某个 f_i 乘以适当的单项式并相减来消去 f 的首项（相对于固定的单项式序）. 那么这个单项式就成为相应的 q_i 中的一项. 与其一般地陈述算法, 不如先通过一些例子来观察涉及的内容.

示例 1. 我们将首先用 $f_1 = xy + 1$ 和 $f_2 = y + 1$ 除 $f = xy^2 + 1$, 使用 $x > y$ 的字典序. 我们想采用与单变量多项式除法相同的方案, 区别是现在有几个除数和商. 将除数 f_1, f_2 和商 q_1, q_2 垂直列出, 我们有以下设置:

$$\begin{array}{l} q_1: \\ q_2: \\ \left.\begin{array}{l} xy+1 \\ y+1 \end{array}\right) \overline{xy^2+1} \end{array}$$

首项 $\text{LT}(f_1) = xy$ 和 $\text{LT}(f_2) = y$ 都整除首项 $\text{LT}(f) = xy^2$. 由于 f_1 首先列出, 我们将使用它.

因此，我们将 xy 除入 xy^2，得到 y，然后从 f 中减去 $y \cdot f_1$：

$$\begin{array}{l} q_1: \quad y \\ q_2: \\ \begin{array}{r} xy+1 \\ y+1 \\ \underline{xy^2+y} \\ -y+1 \end{array} \overline{\begin{array}{l} \\ \\ xy^2+1 \end{array}} \end{array}$$

现在我们对 $-y+1$ 重复相同的过程. 这次我们必须使用 f_2，因为 $\mathrm{LT}(f_1) = xy$ 不整除 $\mathrm{LT}(-y+1) = -y$. 我们得到：

$$\begin{array}{c} q_1: \quad y \\ q_2: -1 \\ \begin{array}{r} xy+1 \\ y+1 \\ \underline{-y+1} \\ \underline{-y-1} \\ 2 \end{array} \overline{\begin{array}{l} \\ \\ )xy^2+1 \end{array}} \end{array}$$

由于 $\mathrm{LT}(f_1)$ 和 $\mathrm{LT}(f_2)$ 都不整除 *2*，余式是 $r = 2$，我们完成了. 因此，我们将 $f = xy^2 + 1$ 写成形式

$$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2.$$

术语表

外文术语	中文术语
affine space	仿射空间.
affine variety	仿射簇.
algebraically closed	代数闭的.
algorithm	算法.
Ascending Chain Condition	升链条件.
basis	基.
Bézier cubic	Bézier 三次曲线.
Buchberger’s Algorithm	Buchberger 算法.
Buchberger’s Criterion	Buchberger 判别法.
coefficient	系数.
commutative ring	交换环.
conic section	圆锥曲线.
control point	控制点.
control polygon	控制多边形.
convex	凸的.
deg	deg.
degree	次数.
Dickson’s Lemma	Dickson 引理.
Division Algorithm	除法算法.
elimination theory	消元理论.
Euclidean Algorithm	Euclid 算法.
field	域.
finite field	有限域.
Fundamental Theorem of Algebra	代数基本定理.
Gaussian elimination	Gauss 消元法.

外文术语	中文术语
generated by	由……生成.
graded lexicographic order	分次字典序.
graded reverse lexicographic order	分次反字典序.
greatest common divisor	最大公因子.
Gröbner basis	Gröbner 基.
Hilbert Basis Theorem	Hilbert 基定理.
Hilbert Nullstellensatz	Hilbert 零点定理.
homogeneous syzygy	齐次合冲.
I	$\{I\}$.
ideal	理想.
Ideal Description Problem	理想描述问题.
Ideal Membership Problem	理想成员问题.
ideal of a variety	簇的理想.
implicit representation	隐式表示.
implicitization	隐式化.
lcm representation	最小公倍表示.
leading coefficient	首项系数.
leading monomial	首项单项式.
leading term	首项.
leading term of an ideal	理想的首项.
least common multiple	最小公倍式.
lexicographic order	字典序.
linear variety	线性簇.
minimal basis	极小基.
monomial	单项式.
monomial ideal	单项式理想.
monomial ordering	单项式序.
multidegree	多重次数.
normal form	范式.
normal selection strategy	正常选择策略.
Nullstellensatz	零点定理.
polynomial	多项式.
polynomial parametric representation	多项式参数表示.
polynomial ring	多项式环.
principal ideal	主理想.
principal ideal domain	主理想整环.
pseudocode	伪代码.
radical	根理想的.

外文术语	中文术语
rational function	有理函数.
rational parametric representation	有理参数表示.
reduced Gröbner basis	约化 Gröbner 基.
remainder	余式.
row reduction	行约化.
singular point	奇点.
S-polynomial	S-多项式.
square-free part	无平方部分.
standard basis	标准基.
standard representation	标准表示.
syzygy	合冲.
tangent surface	切曲面.
term	项.
total degree	总次数.
total ordering	全序.
twisted cubic	三次扭曲线.
unirational	单有理的.
V	$\{V\}$.
Vandermonde determinant	Vandermonde 行列式.
variety	簇.
well-ordering	良序.