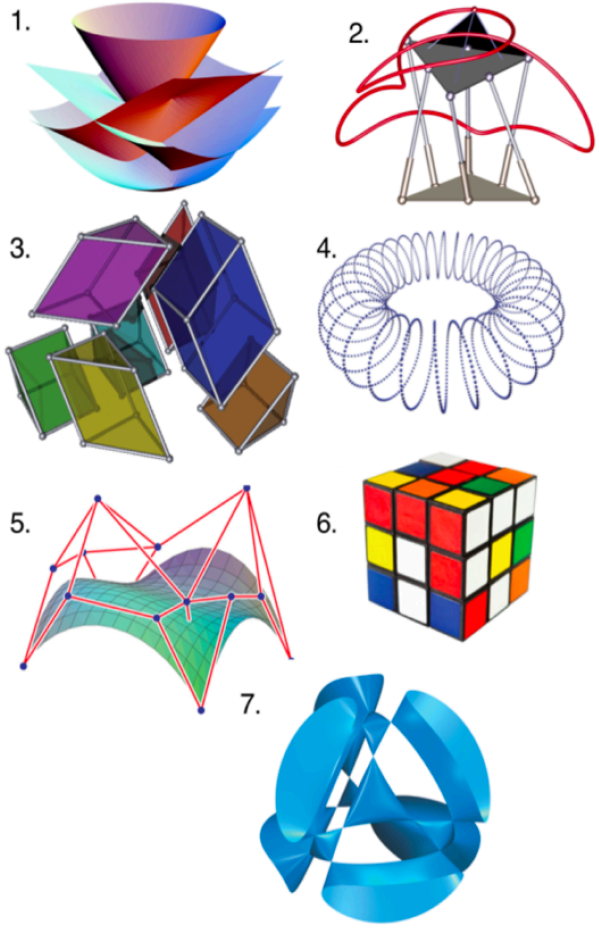
计算机代数



牟晨琪

北航沙河校区E403-7
chenqi.mou@buaa.edu.cn

2020年春

第三章

计算交换代数与代数几何

代数 VS 几何

L'algèbre n'est qu'une géométrie écrite;
la géométrie n'est qu'une algèbre figurée.
(Algebra is nothing but written geometry;
Geometry is nothing but pictured algebra.)

Sophie Germain (1776-1831)

代数簇

代数簇

设 $\mathcal{F}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 的任意非空子集 (可以为无限集). $\mathcal{F}$ 中全体多项式在仿射空间 $\mathcal{K}^n$ 中的公共零点构成的集合

$$\mathsf{V}(\mathcal{F}) := \{\boldsymbol{v} \in \mathcal{K}^n : \ F(\boldsymbol{v}) = 0, \forall\, F \in \mathcal{F}\}$$

称为 $\mathcal{F}$ 的仿射代数簇 (affine algebraic variety). 我们规定 $\mathsf{V}(\emptyset) := \mathcal{K}^n$. 若 $\mathcal{F} = \{F_1, \ldots, F_t\}$, 则 $\mathcal{F}$ 的仿射代数簇简记为 $\mathsf{V}(F_1, \ldots, F_t)$.

Example

设 $F = y - x^2 \in \mathbb{R}[x, y]$, 则集合 $\mathsf{V}(F) \setminus \{(2, 4)\}$ 不为 $\mathbb{R}^2$ 中的代数簇.

- 证明 $\mathsf{V}(\mathcal{F}) = \mathsf{V}(\langle \mathcal{F} \rangle) \to$ 理想的代数簇.

对应理想

对应理想

设 Z 为仿射空间 $\mathcal{K}^n$ 的任意子集, 记 $\mathsf{I}(Z)$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中所有在 Z 上为零的多项式构成的集合, 即

$$\mathsf{I}(Z) := \{F \in \mathcal{K}[\boldsymbol{x}] : \ F(\boldsymbol{v}) = 0, \forall\, \boldsymbol{v} \in Z\}.$$

$\mathsf{I}(Z)$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的理想, 称为 Z 的对应理想 (corresponding ideal). 我们将单点集 $\{\boldsymbol{v}\}$ 的对应理想简记为 $\mathsf{I}(\boldsymbol{v})$.

命题 (反向包含, 证明)

1. 若 $\mathcal{F}_1 \subseteq \mathcal{F}_2$, 则 $\mathsf{V}(\mathcal{F}_1) \supseteq \mathsf{V}(\mathcal{F}_2)$;
2. 若 $Z_1 \subseteq Z_2$, 则 $\mathsf{I}(Z_1) \supseteq \mathsf{I}(Z_2)$.

代数簇与对应理想

命题 (只证 (1), (3))

设 $\mathcal{F} \subseteq \mathcal{K}[\boldsymbol{x}]$, $Z \subseteq \mathcal{K}^n$, 则

a. $\mathsf{VI}(Z) \supseteq Z$;
b. $\mathsf{IV}(\mathcal{F}) \supseteq \langle \mathcal{F} \rangle$;
c. $\mathsf{IVI}(Z) = \mathsf{I}(Z)$;
d. $\mathsf{VIV}(\mathcal{F}) = \mathsf{V}(\mathcal{F})$.

推论

对任意代数簇 $V \subseteq \mathcal{K}^n$ 都有 $\mathsf{VI}(V) = V$.

问：代数簇与理想之间是否有对应关系？

- 理想 $\langle x \rangle, \langle x^2 \rangle \subseteq \mathbb{C}[x, y]$ 对应于相同的代数簇, 即 $\mathsf{V}(\langle x \rangle) = \mathsf{V}(\langle x^2 \rangle) = \{(0, u) : u \in \mathbb{C}\}$.

Hilbert 弱零点定理

是否有解的判定问题

给定一组多项式方程

$$\begin{cases} F_1(x_1, \ldots, x_n) = 0, \\ \cdots\cdots \\ F_s(x_1, \ldots, x_n) = 0, \end{cases}$$

如何判定其是否有解.

任意全次数为 d 的多项式 $F \in \mathcal{K}[\boldsymbol{x}]$ 都能唯一表示为 $F = \sum_{i=0}^{d} F_{(i)}$, 其中 $F_{(i)}$ 为 i 次齐次多项式. 我们称 $\sum_{i=0}^{d} F_{(i)}$ 为 F 的齐次分解 (homogeneous decomposition), 而 $F_{(i)}$ 为 F 的 i 次齐次分量 (homogeneous component).

Hilbert 弱零点定理

引理

设 $F \in \mathcal{K}[x_1, \ldots, x_k]$ 为非常数多项式, 即 $\mathrm{tdeg}(F) = d > 0$. 考虑变元替换

$$\begin{aligned} x_k &= \tilde{x}_k, \\ x_{k-1} &= \tilde{x}_{k-1} + a_{k-1}\tilde{x}_k, \\ &\cdots\cdots \\ x_1 &= \tilde{x}_1 + a_1\tilde{x}_k, \end{aligned} \tag{1}$$

其中 $a_1, \ldots, a_{k-1}$ 为未定元, 并将其代入 F 可得

$$\begin{aligned} F(x_1, \ldots, x_k) &= F(\tilde{x}_1 + a_1\tilde{x}_k, \ldots, \tilde{x}_{k-1} + a_{k-1}\tilde{x}_k, \tilde{x}_k) \\ &= c(a_1, \ldots, a_{k-1})\,\tilde{x}_k^d + T, \end{aligned}$$

这里 $\deg(T, \tilde{x}_k) < d$. 我们断言 $c(a_1, \ldots, a_{k-1})$ 为关于 $a_1, \ldots, a_{k-1}$ 的非零多项式.

Hilbert 弱零点定理

定理 (Hilbert 弱零点定理)

设 $\mathcal{K}$ 为代数闭域, $\mathfrak{a}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中理想, 则 $\mathsf{V}(\mathfrak{a}) = \emptyset$ 当且仅当 $1 \in \mathfrak{a}$.

证明: ($\Longleftarrow$) 显然. ($\Longrightarrow$) 对变元个数 n 归纳证明

1. $n = 1$: 主理想, 代数闭域
2. 归纳假设: 现假设变元个数 $n = k - 1$ 时定理成立,
3. $n = k$: F_1 不为常数, 对其进行引理中的变量替换, 考察以此定义的环同构; 由考虑 a 转而考虑同态像 $\tilde{a}$; 利用扩张定理把 $n = k$ 中性质转化为 $n = k - 1$，使用归纳假设.

代数闭域的必要性

方程 $x^2 + y^2 = -1$ 在 $\mathbb{R}^2$ 中无解, 即 $\mathsf{V}(x^2 + y^2 + 1) = \emptyset$. 但是 $1 \notin \langle x^2 + y^2 - 1 \rangle$; 否则存在多项式 $F \in \mathbb{R}[x, y]$ 使得 $1 = (x^2 + y^2 - 1)F$,

扩张定理推论：复习

扩张定理推论

设 $\mathfrak{a} = \langle F_1, \ldots, F_s \rangle \subseteq \mathbb{C}[\boldsymbol{x}]$ 为理想，且存在 i $(1 \leqslant i \leqslant s)$，使得 F_i 有如下形式:

$$F_i = c\, x_n^N + H_i,$$

其中 $N > 0$，c 为常数，且 $\deg(H_i, x_n) < N$. 若 $\mathfrak{a}_{n-1}$ 是 $\mathfrak{a}$ 的第 $n-1$ 个消去理想，且 $(c_1, \ldots, c_{n-1}) \in \mathsf{Z}(\mathfrak{a}_{n-1})$ 为部分解，则存在 $c_n \in \mathbb{C}$ 使得 $(c_1, \ldots, c_{n-1}, c_n) \in \mathsf{Z}(a)$.

代数簇与理想的对应

$\mathsf{V}(\langle x \rangle) = \mathsf{V}(\langle x^2 \rangle)$

根理想

设 $\mathfrak{a}$ 为环 $\mathcal{R}$ 中理想. 定义 $\mathfrak{a}$ 的根 (radical) 为

$$\sqrt{\mathfrak{a}} := \{F \in \mathcal{R} : \ F^m \in \mathfrak{a}, \exists\, m \in \mathbb{N}\}.$$

若 $\mathfrak{a} = \sqrt{\mathfrak{a}}$, 则称 $\mathfrak{a}$ 为根理想 (radical ideal).

Hilbert 强零点定理 (Nullstellesatz, 证明)

设 $\mathcal{K}$ 为代数闭域, 则对任意理想 $\mathfrak{a} \subset \mathcal{K}[\boldsymbol{x}]$ 都有 $\mathsf{IV}(\mathfrak{a}) = \sqrt{\mathfrak{a}}$.

证明: 转而考虑 $\mathcal{K}[x_1, \ldots, x_n, y]$ 中理想 $\mathfrak{a}^+ = \langle F_1, \ldots, F_s, 1 - yF \rangle$, 证明 $\mathsf{V}(\mathfrak{a}^+) = \emptyset$, 从而利用 Hilbert 弱零点定理.

根理想与代数簇的对应关系

- 代数闭域的必要性：设 $F \in \mathcal{K}[x]$ 在 $\mathcal{K}$ 中无根，则 $\mathsf{V}(\langle F\rangle) = \emptyset$，此时 $\mathsf{I}(\mathsf{V}(\langle F\rangle)) = \mathcal{K}[\boldsymbol{x}] \neq \sqrt{\langle F\rangle}$.

对应关系

设 $\mathcal{K}$ 为代数闭域，则 I 和 V 建立了 $\mathcal{K}^n$ 中代数簇与 $\mathcal{K}[\boldsymbol{x}]$ 中根理想之间的反序一一对应关系. 这里反序的意思是:

a. 若代数簇 $V_1 \subseteq V_2$，则 $\mathsf{I}(V_1) \supseteq \mathsf{I}(V_2)$;

b. 若理想 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$，则 $\mathsf{V}(\mathfrak{a}_1) \supseteq \mathsf{V}(\mathfrak{a}_2)$.

- 根理想 $\longleftrightarrow$ 代数簇;

素理想与不可约代数簇的对应关系

素理想

称 $\mathcal{R}$ 中理想 $\mathfrak{p}$ 为素理想 (prime ideal), 如果 $FG \in \mathfrak{p}$ 蕴涵着 $F \in \mathfrak{p}$ 或 $G \in \mathfrak{p}$.

- 素理想均为根理想
- 以 $\mathfrak{p} = \langle H \rangle$ 为例
- 素理想 VS 素数

命题 (不证明)

(a) 设 $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ 为 $\mathcal{R}$ 中素理想, 而理想 $\mathfrak{a} \subseteq \bigcup_{i=1}^{m} \mathfrak{p}_i$, 则存在 i $(1 \leqslant i \leqslant m)$ 使得 $\mathfrak{a} \subseteq \mathfrak{p}_i$.
(b) 设 $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ 为 $\mathcal{R}$ 中理想, 而素理想 $\mathfrak{p} \supseteq \bigcap_{i=1}^{m} \mathfrak{a}_i$, 则存在 i $(1 \leqslant i \leqslant m)$ 使得 $\mathfrak{p} \supseteq \mathfrak{a}_i$. 进一步, 若 $\mathfrak{p} = \bigcap_{i=1}^{m} \mathfrak{a}_i$, 则存在 i $(1 \leqslant i \leqslant m)$ 使得 $\mathfrak{p} = \mathfrak{a}_i$.

素理想与不可约代数簇的对应关系

不可约代数簇

称代数簇 $W \subseteq \mathcal{K}^n$ 不可约 (irreducible), 如果 W 不能写成两个真子代数簇的并, 即 $W = V_1 \cup V_2$ 蕴涵着 $W = V_1$ 或 $W = V_2$.

对应关系 (证明)

设 $\mathcal{K}$ 为代数闭域, 而 $W \subseteq \mathcal{K}^n$ 为代数簇, 则 W 不可约当且仅当 $\mathsf{I}(W)$ 为素理想.

- 素理想 $\longleftrightarrow$ 不可约代数簇;

极大理想与单点集的对应关系

极大理想

称 $\mathcal{R}$ 中理想 $\mathfrak{m}$ 为极大理想 (maximal ideal), 如果

1. $\mathfrak{m} \neq \mathcal{R}$;
2. 不存在真包含 $\mathfrak{m}$ 的真理想, 即 $\mathfrak{m} \subseteq \mathfrak{a} \subseteq \mathcal{R}$ 蕴涵着 $\mathfrak{a} = \mathfrak{m}$ 或 $\mathfrak{a} = \mathcal{R}$.

- 极大理想为素理想.

命题 (证明)

设 $\boldsymbol{v} = (a_1, \ldots, a_n) \in \mathcal{K}^n$, 则 $\mathsf{I}(\boldsymbol{v})$ 为极大理想. 反之, 若 $\mathcal{K}$ 为代数闭域, 则对任意极大理想 $\mathfrak{m} \subseteq \mathcal{K}[\boldsymbol{x}]$, 都存在点 $\boldsymbol{v} \in \mathcal{K}^n$ 使得 $\mathfrak{m} = \mathsf{I}(\boldsymbol{v})$.

- 极大理想 $\longleftrightarrow$ 单点集.

理想的和

对于 $\mathcal{R}$ 中任意理想 $\mathfrak{a}, \mathfrak{b}$, 定义 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的和 (sum) 为

$$\mathfrak{a}+\mathfrak{b} := \{F+G:\ F\in\mathfrak{a} \text{ 且 } G\in\mathfrak{b}\}.$$

容易证明 $\mathfrak{a}+\mathfrak{b}$ 为包含 $\mathfrak{a}, \mathfrak{b}$ 的最小理想.

命题：代数簇语言 (证明)

设理想 $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{K}[\boldsymbol{x}]$, 则 $\mathsf{V}(\mathfrak{a}+\mathfrak{b}) = \mathsf{V}(\mathfrak{a}) \cap \mathsf{V}(\mathfrak{b})$.

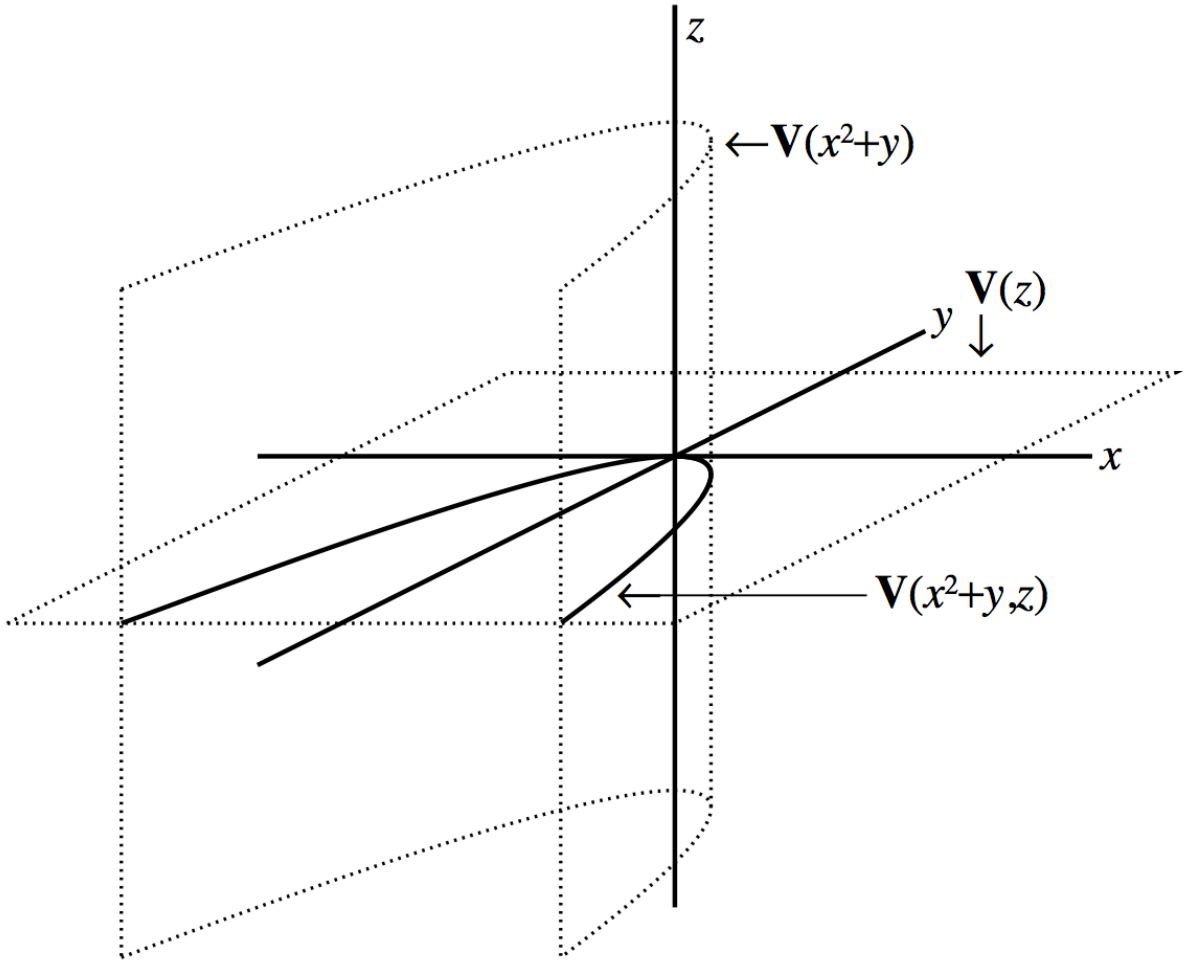
定理：理想语言 (证明)

设 $\mathcal{K}[\boldsymbol{x}]$ 中的理想 $\mathfrak{a} = \langle F_1, \ldots, F_s\rangle, \mathfrak{b} = \langle G_1, \ldots, G_t\rangle$, 则

$$\mathfrak{a}+\mathfrak{b} = \langle F_1, \ldots, F_s, G_1, \ldots, G_t\rangle.$$

几何示例

设 $\mathfrak{a} = \langle x^2 + y \rangle, \mathfrak{b} = \langle z \rangle$ 为 $\mathbb{R}^3[x, y, z]$ 中的理想，现考虑 $\mathrm{V}(\mathfrak{a} + \mathfrak{b})$:



理想的积

对于 $\mathcal{R}$ 中任意理想 $\mathfrak{a}, \mathfrak{b}$, 定义 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的积 (product) 为

$$\mathfrak{ab} := \{FG : F \in \mathfrak{a} \text{ 且 } G \in \mathfrak{b}\}.$$

容易证明 $\mathfrak{ab}$ 也是 $\mathcal{R}$ 中理想.

命题: 代数簇语言 (证明)

设理想 $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{K}[\boldsymbol{x}]$, 则 $\mathsf{V}(\mathfrak{ab}) = \mathsf{V}(\mathfrak{a}) \cup \mathsf{V}(\mathfrak{b})$.

定理: 理想语言 (证明)

设 $\mathcal{K}[\boldsymbol{x}]$ 中的理想 $\mathfrak{a} = \langle F_1, \ldots, F_s \rangle$, $\mathfrak{b} = \langle G_1, \ldots, G_t \rangle$, 则

$$\mathfrak{ab} = \langle F_i G_j : 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t \rangle.$$

理想的交

设 $\mathfrak{a}, \mathfrak{b}$ 为 $\mathcal{R}$ 中理想, $\mathfrak{a}$ 与 $\mathfrak{b}$ 的交 (intersection) 定义为 $\mathfrak{a}$, $\mathfrak{b}$ 作为集合的交, 记为 $\mathfrak{a} \cap \mathfrak{b}$. 容易验证 $\mathfrak{a} \cap \mathfrak{b}$ 为包含于 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的最大理想.

命题：代数簇语言 (证明)

设理想 $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{K}[\boldsymbol{x}]$, 则 $\mathsf{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathsf{V}(\mathfrak{a}) \cup \mathsf{V}(\mathfrak{b})$.

- $\mathfrak{a} \cap \mathfrak{b}$ 与 $\mathfrak{ab}$ 之间有什么关系, 是否为同一理想?

Example (反例)

易知 $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{ab}$. 而反向包含关系 $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab}$ 是否成立呢? 一般来说, 答案是否定的. 例如, 令 $\mathfrak{a} = \langle x \rangle$, $\mathfrak{b} = \langle x^2 \rangle$, 则 $\mathfrak{a} \cap \mathfrak{b} = \langle x^2 \rangle$, 而 $\mathfrak{ab} = \langle x^3 \rangle$, 于是 $\mathfrak{a} \cap \mathfrak{b} \nsubseteq \mathfrak{ab}$.

理想的交

定理 (证明)

设理想 $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{K}[\boldsymbol{x}]$, 则 $\mathfrak{a} \cap \mathfrak{b} = (y\mathfrak{a} + (1-y)\mathfrak{b}) \cap \mathcal{K}[\boldsymbol{x}]$, 其中 y 为引入的新变元.

算法 20 理想的交 $\mathcal{H} := \mathsf{Intsec}(\mathcal{F}, \mathcal{G})$

输入: 多项式集合 $\mathcal{F}, \mathcal{G}$.

输出: $\langle \mathcal{F} \rangle \cap \langle \mathcal{G} \rangle$ 的 Gröbner 基.

取 $<$ 为满足 $y > x_i$ $(1 \leqslant i \leqslant n)$ 的字典序;

$\mathcal{H} := \mathsf{GröbnerBasis}(y\mathcal{F} \cup (1-y)\mathcal{G}, <)$;

$\mathcal{H} := \mathcal{H} \cap \mathcal{K}[\boldsymbol{x}]$;

return $\mathcal{H}$;

计算理想的交

理想的交

Example

设 $V_1 = \mathsf{V}(\mathfrak{a}), V_2 = \mathsf{V}(\mathfrak{b}) \subseteq \mathbb{C}^3$, 其中

$$\mathfrak{a} = \langle (x_2 - x_1^2)x_2 \rangle, \quad \mathfrak{b} = \langle (x_2 - x_1^2)(x_3 - x_1) \rangle \subseteq \mathbb{C}[x_1, x_2, x_3].$$

下面计算 $V_1 \cup V_2$ 的对应理想 $\mathsf{I}(V_1 \cup V_2)$.
容易验证 $\mathsf{I}(V_1) = \mathfrak{a}$, $\mathsf{I}(V_2) = \mathfrak{b}$ (根理想). 理想

$$y\mathfrak{a} + (1-y)\mathfrak{b} = \langle yx_2(x_2 - x_1^2), (1-y)(x_2 - x_1^2)(x_3 - x_1) \rangle$$

在字典序 $y > x_1 > x_2 > x_3$ 下的 Gröbner 基为

$$[x_2(x_1^2 - x_2)(x_3 - x_1), yx_2(x_1^2 - x_2), (1-y)(x_1^2 - x_2)(x_3 - x_1)].$$

选取其中不含 y 的多项式, 得到 $\mathfrak{a} \cap \mathfrak{b}$ 的基 $\{x_2(x_1^2 - x_2)(x_3 - x_1)\}$.
易证, 其即为 $\mathsf{I}(V_1 \cup V_2)$ 的基.

理想的商

对于 $\mathcal{R}$ 中任意理想 $\mathfrak{a}$ 和 $\mathfrak{b}$, 定义 $\mathfrak{a}$ 关于 $\mathfrak{b}$ 的商 (quotient) 为

$$\mathfrak{a} : \mathfrak{b} := \{F \in \mathcal{R} : \ FG \in \mathfrak{a}, \forall\, G \in \mathfrak{b}\}.$$

若 $\mathfrak{b} = \langle H \rangle$, 则 $\mathfrak{a}$ 关于 $\mathfrak{b}$ 的商简记为 $\mathfrak{a} : H$.

- 设理想 $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{R}$, 则 $\mathfrak{a} : \mathfrak{b}$ 为 $\mathcal{R}$ 中理想.

命题 (证明)

设理想 $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{a}_i, \mathfrak{b}_i \subseteq \mathcal{R}$, $i \in \theta$, 其中 θ 为任意指标集, 则

1. $\mathfrak{a} \subseteq \mathfrak{a} : \mathfrak{b}$;
2. $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$;
3. $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : \mathfrak{b}\mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}$;
4. $(\bigcap_{i\in\theta} \mathfrak{a}_i) : \mathfrak{b} = \bigcap_{i\in\theta}(\mathfrak{a}_i : \mathfrak{b})$;
5. $\mathfrak{a} : (\sum_{i\in\theta} \mathfrak{b}_i) = \bigcap_{i\in\theta}(\mathfrak{a} : \mathfrak{b}_i)$.

理想的商

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{a} : \langle G_1, \ldots, G_t \rangle = \mathfrak{a} : \left(\sum_{i=1}^{t} \langle G_i \rangle \right) = \bigcap_{i=1}^{t} (\mathfrak{a} : \langle G_i \rangle).$$

- 如何计算 $\mathfrak{a} : \langle G_i \rangle$

定理 (证明)

设理想 $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{x}]$, 多项式 $G \in \mathcal{K}[\boldsymbol{x}]$. 若 $\{F_1, \ldots, F_m\}$ 为 $\mathfrak{a} \cap \langle G \rangle$ 的一组基, 则 G 整除 $F_1, \ldots, F_m$, 并且 $\{F_1/G, \ldots, F_m/G\}$ 为 $\mathfrak{a} : \langle G \rangle$ 的一组基.

算法 21 理想的商 $\mathcal{B} := \mathsf{Quot}(\mathcal{F}, \mathcal{G})$

输入: $\mathcal{K}[\boldsymbol{x}]$ 中多项式集 $\mathcal{F}, \mathcal{G}$.
输出: $\langle \mathcal{F} \rangle : \langle \mathcal{G} \rangle$ 的基.

$\mathcal{B} := \mathcal{K}[\boldsymbol{x}]$;
for $G \in \mathcal{G}$ **do**
  $\mathcal{T} := \mathsf{Intsec}(\mathcal{F}, \{G\})$;
  $\mathcal{A} := \{T/G : T \in \mathcal{T}\}$;
  $\mathcal{B} := \mathsf{Intsec}(\mathcal{B}, \mathcal{A})$;
end
return $\mathcal{B}$;

总结

ALGEBRA		GEOMETRY
radical ideals		varieties
I	$\longrightarrow$	$\mathbf{V}(I)$
$\mathbf{I}(V)$	$\longleftarrow$	V
addition of ideals		intersection of varieties
$I + J$	$\longrightarrow$	$\mathbf{V}(I) \cap \mathbf{V}(J)$
$\sqrt{\mathbf{I}(V) + \mathbf{I}(W)}$	$\longleftarrow$	$V \cap W$
product of ideals		union of varieties
IJ	$\longrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$
$\sqrt{\mathbf{I}(V)\mathbf{I}(W)}$	$\longleftarrow$	$V \cup W$
intersection of ideals		union of varieties
$I \cap J$	$\longrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$
$\mathbf{I}(V) \cap \mathbf{I}(W)$	$\longleftarrow$	$V \cup W$
quotient of ideals		difference of varieties
$I : J$	$\longrightarrow$	$\overline{\mathbf{V}(I) - \mathbf{V}(J)}$
$\mathbf{I}(V) : \mathbf{I}(W)$	$\longleftarrow$	$\overline{V - W}$
elimination of variables		projection of varieties
$\sqrt{I \cap k[x_{l+1}, \ldots, x_n]}$	$\longleftrightarrow$	$\overline{\pi_i(\mathbf{V}(I))}$
prime ideal		irreducible variety
maximal ideal		point of affine space
ascending chain condition		descending chain condition

第四次大作业

1. 给定多项式组 $\mathcal{F},\mathcal{G}\subset\mathbb{Q}[\boldsymbol{x}]$, 编写程序计算理想的交 $\langle\mathcal{F}\rangle\cap\langle\mathcal{G}\rangle$ 和 理想的商 $\langle\mathcal{F}\rangle:\langle\mathcal{G}\rangle$.
2. 定义理想 $\mathfrak{a}\subset\mathcal{K}[\boldsymbol{x}]$ 关于 $H\in\mathcal{K}[\boldsymbol{x}]$ 的饱和 (记作 $\mathfrak{a}:H^\infty$) 为

$$\mathfrak{a}:H^\infty:=\{G:\ H^sG\in\mathfrak{a},\exists\, s\ (s\geqslant 0)\}.$$

   则 $\mathfrak{a}:H^\infty$ 有如下性质：存在非负整数 s 使得 $\mathfrak{a}:H^s=\mathfrak{a}:H^{s+1}=\mathfrak{a}:H^\infty$. 给定多项式组 $\mathcal{F}\subset\mathbb{Q}[\boldsymbol{x}]$ 和 $H\in\mathbb{Q}[\boldsymbol{x}]$, 设计算法并编写程序计算饱和理想 $\langle\mathcal{F}\rangle:H^\infty$.
3. 令

$$\begin{aligned}F_1&=x_2x_4x_5-x_1x_3x_6,\\F_2&=4x_4^2x_5+3x_3^2x_6,\\F_3&=175x_1x_2^2x_4x_5+192x_2^3x_3x_5-108x_1^3x_4x_6,\end{aligned}$$

   而 $H=4x_1x_4+3x_2x_3$. 计算 $\langle F_1,F_2,F_3\rangle:H^\infty$.

第四次大作业

格式与时间要求

- 上交作业为电子版，需包含源程序和简单的解决方式描述（例如主要步骤及其计算结果等），后者鼓励用 Latex 写.
- 截止时间为 5 月 22 日，请将作业打包.zip文件以“计算机代数 4–姓名–学号”命名，以同样名称为邮件名发送至 zjwang@buaa.edu.cn.

1. 建议用 Maple 软件写，因为已经有常见的与多项式理想运算有关的函数 (例如 Saturate)
2. 利用 Maple 软件完成作业时的提示
   - PolynomialIdeals 软件包包含与多项式理想运算有关的常用指令：with(PolynomialIdeals), 之后可以调用下面的命令
   - 判断两个理想 A 和 B 相等：IdealContainment(A, B, A)
   - 两个理想 A 和 B 相乘：Multiply(A, B)
   - Maple 中记号 I 似乎被占用了，不要用 I 作为变量名
   - 第 3 问中的使得 $\langle F_1, F_2, F_3\rangle : H^s = \langle F_1, F_2, F_3\rangle : H^{s+1}$ 的 s 很小，最后饱和理想的结果也很简单

代数簇与根理想的分解

代数簇的降链条件 (DCC)

对 $\mathcal{K}^n$ 中的任意代数簇降链 $V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$, 均存在 $N \geqslant 1$ 使得 $\mathcal{V}_N = \mathcal{V}_{N+1} = \mathcal{V}_{N+2} = \cdots$.

代数簇的分解

设 $V \subseteq \mathcal{K}^n$ 为非空代数簇, 则存在有限个不可约代数簇 $V_1, \ldots, V_s \subseteq \mathcal{K}^n$ 使得 $V = V_1 \cup \cdots \cup V_r$, 且对任意 $i \neq j$ 都有 $V_i \not\supseteq V_j$.

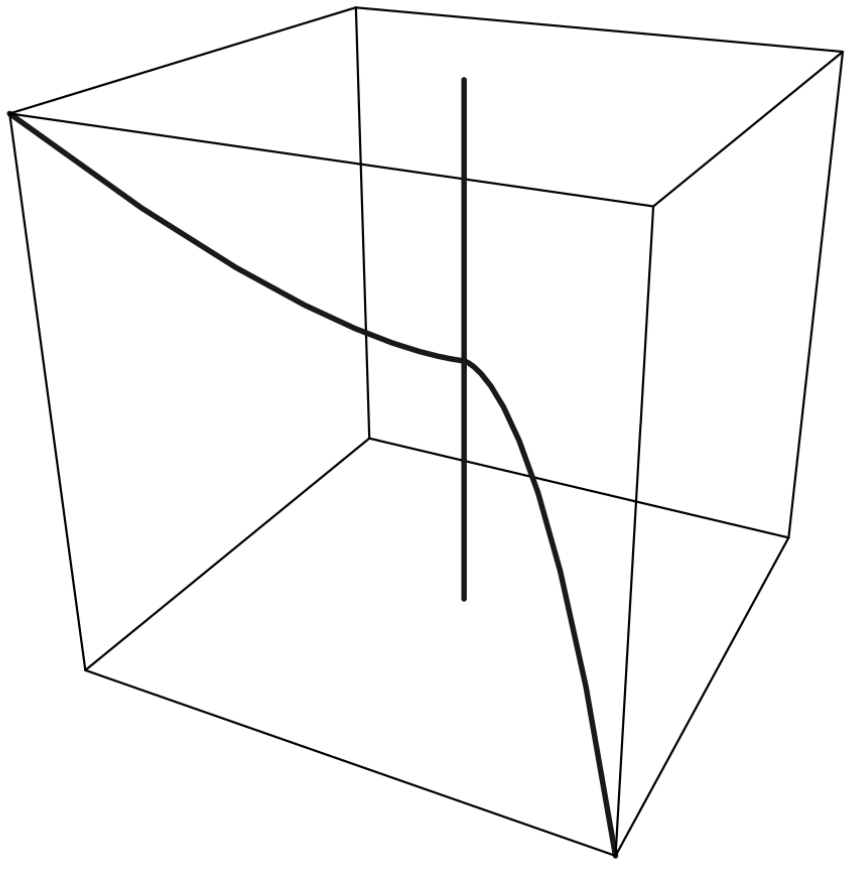
根理想的分解

设 $\mathcal{K}$ 为代数闭域, 而 $\mathfrak{a}$ 为 $\mathcal{K}[\boldsymbol{x}]$ 中的理想, 则存在素理想 $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{K}[\boldsymbol{x}]$ 使得 $\sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$, 且对任意 $i \neq j$ 都有 $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$.

- 代数簇 V 或根理想 $\sqrt{\mathfrak{a}}$ 的极小分解 (minimal decomposition), 存在惟一

示例

考虑代数簇 $V = \mathsf{V}(xz - y^2, x^3 - yz)$



$$V = \mathsf{V}(x, y) \cup \mathsf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$$

一般理想的分解

定义

理想 $q \subseteq \mathcal{R}$ 称为准素理想 (primary ideal), 如果

$$FG \in q \implies F \in q \text{ 或者 } G^m \in q, \exists\, m \in \mathbb{N}.$$

容易验证，上述条件与下述任一条件等价：

- 若 $FG \in q$ 且 $F \notin q$, 则 $G \in \sqrt{q}$;
- 若 $FG \in q$ 且 $F \notin \sqrt{q}$, 则 $G \in q$.

准素分解

Lasker–Noether 准素分解定理: 存在性

设 $\mathcal{R}$ 为 Noether 环, $\mathfrak{a}$ 为 $\mathcal{R}$ 中理想, 则存在有限个准素理想 $\mathfrak{q}_1, \ldots, \mathfrak{q}_m \subseteq \mathcal{R}$ 使得下列条件成立:

a. $\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i$;
b. 对任意 $i \neq j$, 都有 $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$;
c. 对任意 $i\,(1 \leqslant i \leqslant m)$, 都有 $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$.

设理想 $\mathfrak{a} \subseteq \mathcal{R}$, 准素理想 $\mathfrak{q}_1, \ldots, \mathfrak{q}_m \subseteq \mathcal{R}$. 若上述定理中的三个条件成立, 我们称 $\bigcap_{i=1}^{m} \mathfrak{q}_i$ 为理想 $\mathfrak{a}$ 的极小准素分解 (minimal primary decomposition).