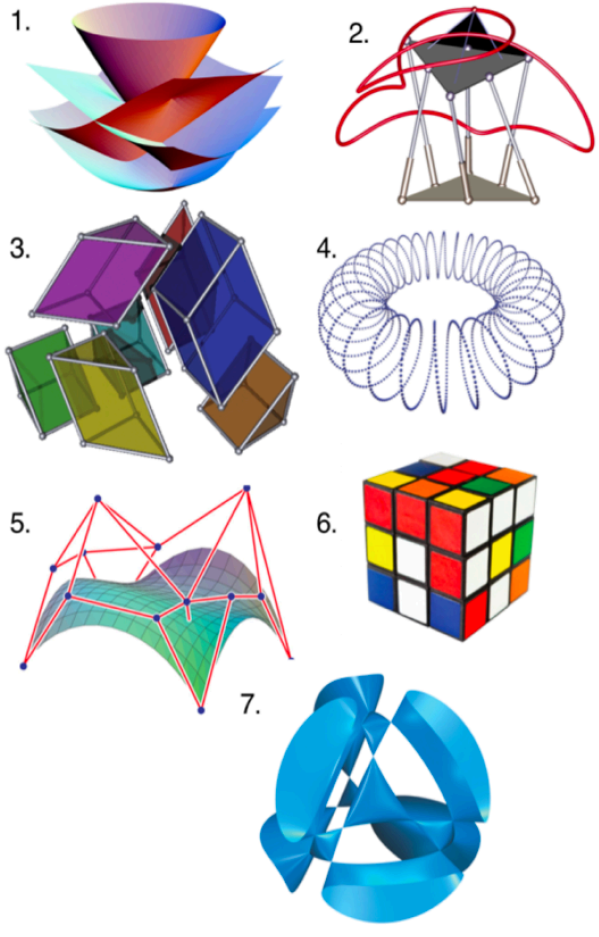
计算机代数



牟晨琪

北航沙河校区E403-7
chenqi.mou@buaa.edu.cn

2020年春

计算机代数：从一个例子开始

JOHN D. COOK
CONSULTING

ABOUT　SERVICES　WRITING　CLIENTS

(832) 422-8646
CONTACT

Solving systems of polynomial equations

Posted on **13 May 2017** by **John**

In a high school algebra class, you learn how to solve polynomial equations in one variable, and systems of linear equations. You might reasonably ask "So when do we combine these and learn to solve systems of polynomial equations?" The answer would be "Maybe years from now, but most likely never." There are systematic ways to solve systems of polynomial equations, but you're unlikely to ever see them unless you study algebraic geometry.

Here's an example from [1]. Suppose you want to find the extreme values of $x^3 + 2xyz - x^2$ on the unit sphere using Lagrange multipliers. This leads to the following system of polynomial equations where λ is the Lagrange multiplier.

$$\begin{aligned} 3x^2 + 2yz - 2x\lambda &= 0 \\ 2xz - 2y\lambda &= 0 \\ 2xy - 2z - 2z\lambda &= 0 \\ x^2 + y^2 + z^2 - 1 &= 0 \end{aligned}$$

Search ...
Search

LET'S TALK

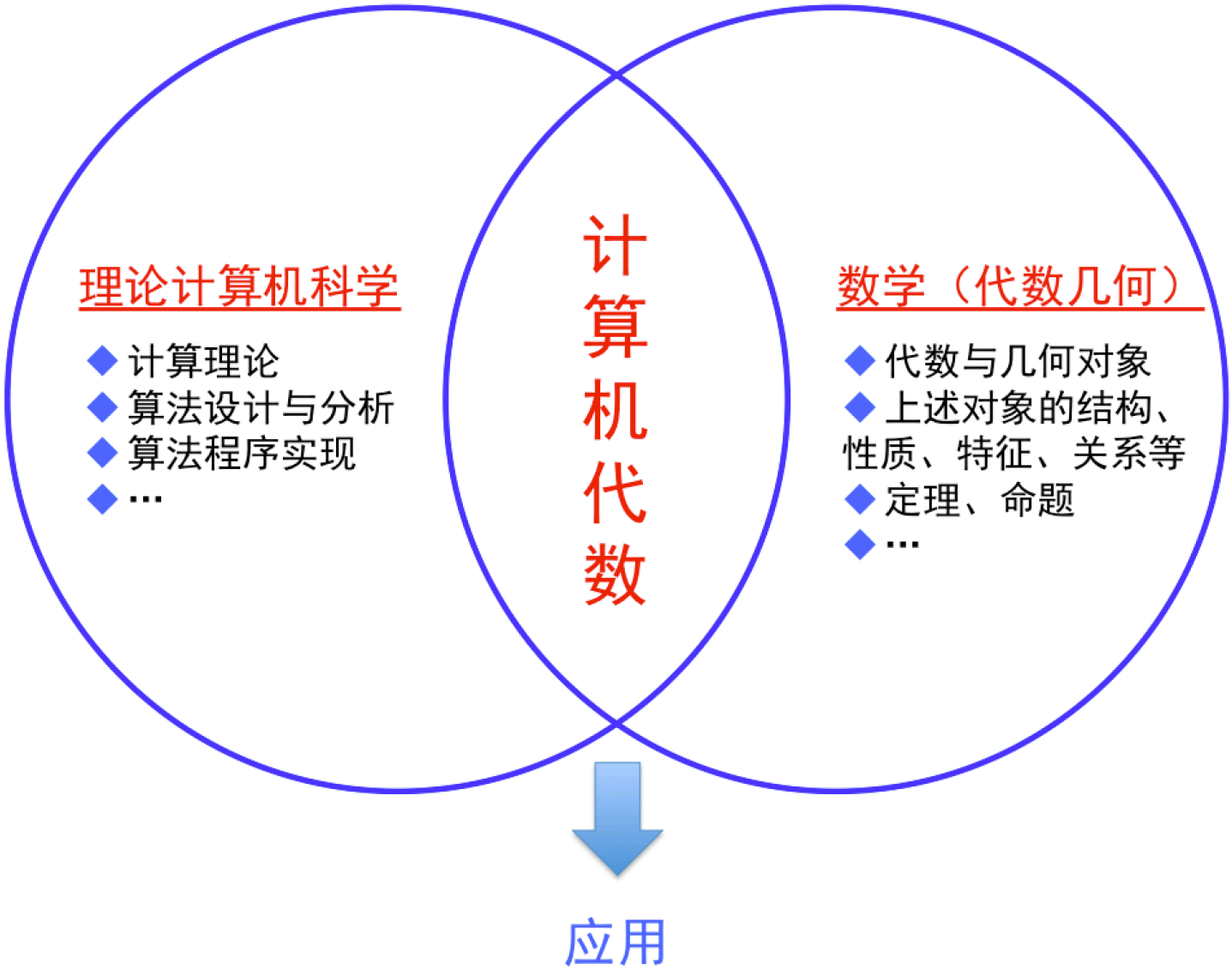
Latest Posts

Discrete example of concentration of measure

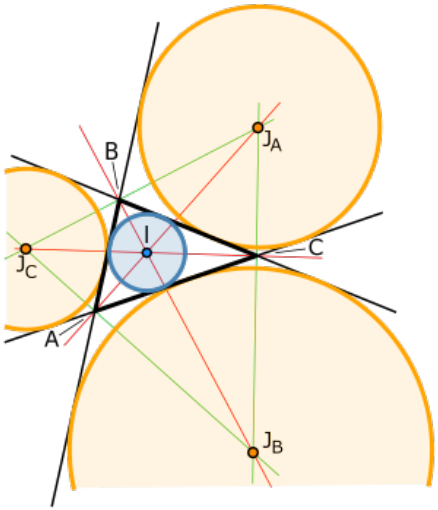
Nearly all the area in a high-dimensional sphere is near the equator

- Maple 例子：上面截图中曲面方程应为 $x^3 + 2xyz - z^2$

计算机代数：交叉学科

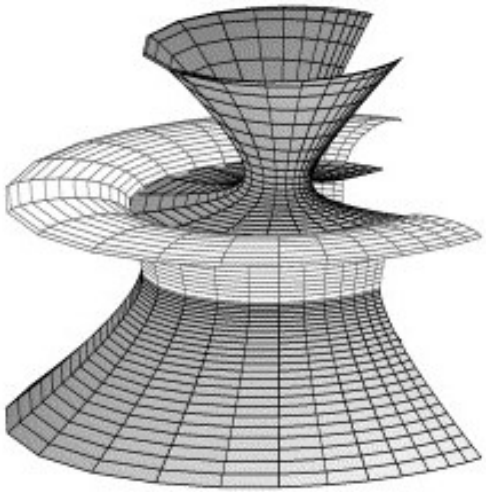

理论计算机科学
计算理论
算法设计与分析
算法程序实现
…
计算机代数
数学（代数几何）
代数与几何对象
上述对象的结构、性质、特征、关系等
定理、命题
…
应用

计算机代数：应用



几何定理的机器证明

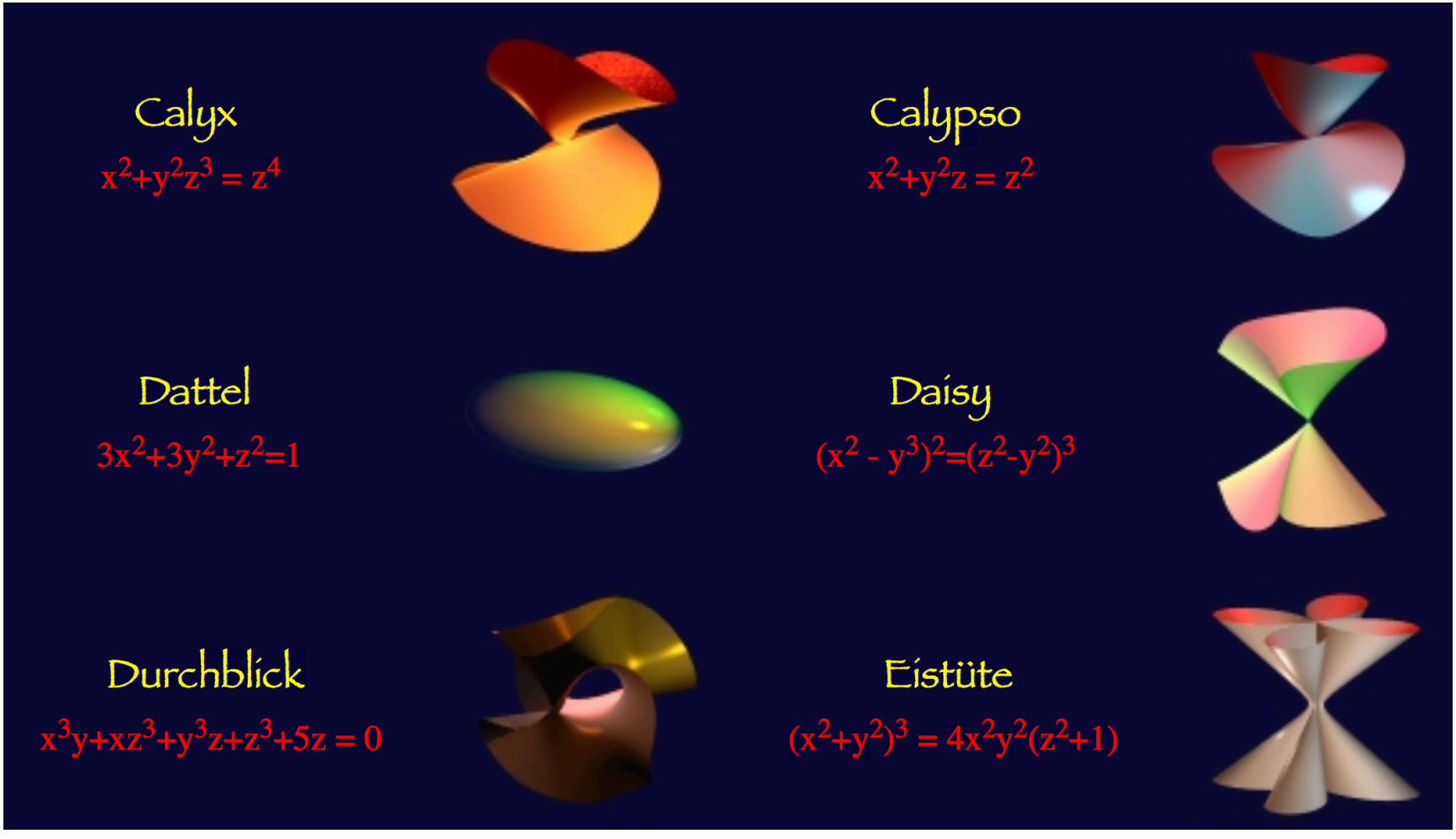
机器人运动学



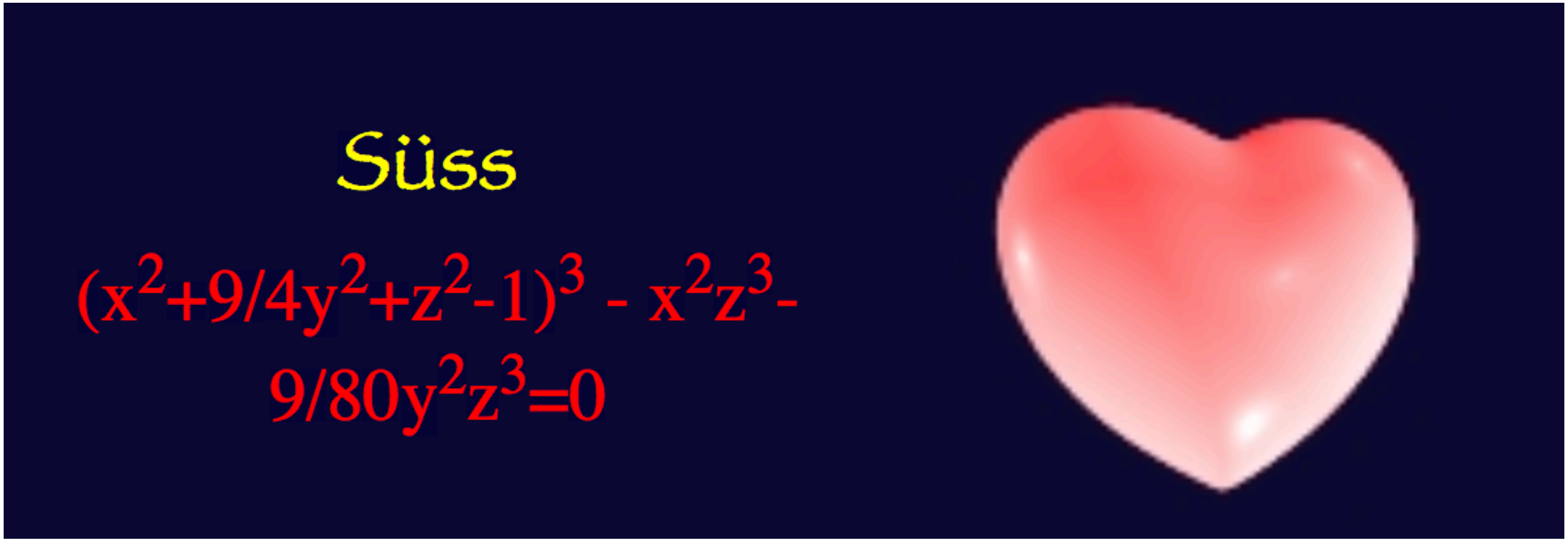
曲线与曲面的计算

密码学

代数曲面


Calyx
$x^2+y^2z^3 = z^4$
Calypso
$x^2+y^2z = z^2$
Dattel
$3x^2+3y^2+z^2=1$
Daisy
$(x^2 - y^3)^2=(z^2-y^2)^3$
Durchblick
$x^3y+xz^3+y^3z+z^3+5z = 0$
Eistüte
$(x^2+y^2)^3 = 4x^2y^2(z^2+1)$

代数曲面



- 多项式 VS 曲面 $\Longrightarrow$ 代数表达式 VS 几何表示
- 隐式表示 VS 显示表示

更多代数曲面：`http://homepage.univie.ac.at/herwig.hauser/bildergalerie/gallery.html`

多项式代数

学科	线性代数 $\rightsquigarrow$线性	多项式代数 $\rightsquigarrow$非线性
	$\Downarrow$	$\Downarrow$
核心	求解线性方程组	求解多项式方程组
	$\Downarrow$	$\Downarrow$
代数对象	线性空间/矩阵	理想/代数簇
工具与方法	高斯消去法	三角列/Gröbner 基
软件与实施	Matlab/LinBox	Maple/Mathematica

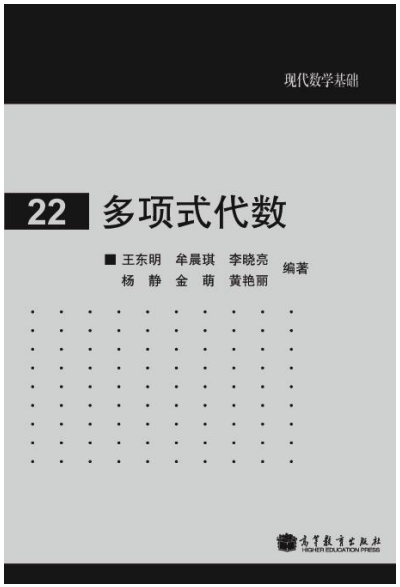
符号计算 (VS 数值计算)

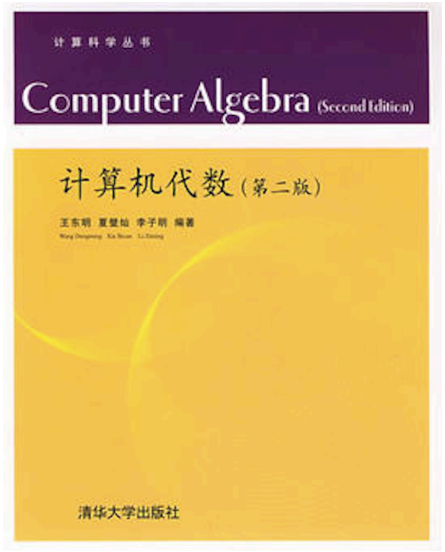
计算机代数又称符号计算，主要处理具有含义的抽象符号，主要研究如何进行这些符号之间的精确运算，因而没有误差。

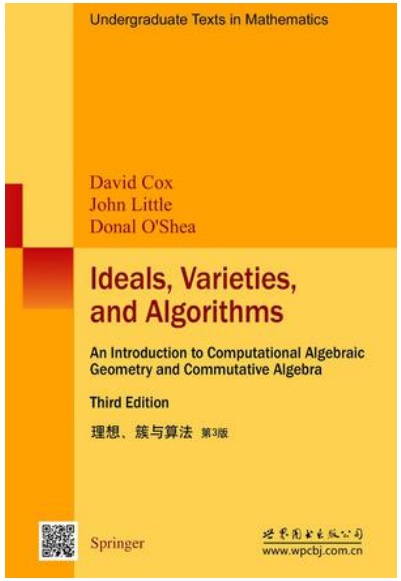
- 数值计算：有误差、数值稳定性、收敛速度、计算效率
- （理论）数学中的运算都是符号运算：如高斯消去法

课程基本信息

- 本科生 48 学时, 研究生 32 学时 (!!?)
- 教材: 《多项式代数》. 王东明, 牟晨琪等, 高等教育出版社.







参考书目

- 《计算机代数》. 王东明, 夏壁灿, 李子明, 清华大学出版社, 2007
- 《Ideals, Varieties, and Algorithms》 (3rd Edition). D. Cox, J. Little, D. O'shea. Springer, 2007 (已引进,《理想、簇与算法》)

课程基本内容：共计六部分

1. 多项式基础（10 课时, 本研）
   - 多项式基础、域论初步、结式、最大公因子的计算
2. 多项式消元与方程求解（12 课时，本研）
   - Groebner 基方法、三角化方法、多项式方程组求解
3. 计算实代数几何（8 课时，本研）
   - 实闭域、实根隔离、柱形代数分解
4. 计算机代数系统（2 课时，本研）
5. 计算交换代数与代数几何（8 课时，本）
   - 理想与代数簇、理想的基本运算、理想与代数簇的分解
6. 应用（8 课时，本）
   - 几何定理的机器证明、曲线与曲面的计算、微分系统的定性分析

考核方式

预计留4/3 道大作业，以 4/3 次大作业综合得分作为考试成绩

第一章

多项式—概念及基本运算

1.1 多项式基础

多项式

设 $\mathcal{R}$ 为带单位元的交换环, $x_1, \ldots, x_n$ 为 $\mathcal{R}$ 上的未定元.

称形式幂积 $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ $(\alpha_i \geqslant 0)$ 为关于 $x_1, \ldots, x_n$ 的项 (term), 简记为 $\boldsymbol{x}^{\boldsymbol{\alpha}}$, 其中 $\boldsymbol{x}$ 和 $\boldsymbol{\alpha}$ 分别表示向量 $(x_1, \ldots, x_n)$ 和 $(\alpha_1, \ldots, \alpha_n)$.

- α_i 为 $\boldsymbol{x}^{\boldsymbol{\alpha}}$ 关于变元 x_i 的次数 (degree), 记为 $\deg(\boldsymbol{x}^{\boldsymbol{\alpha}}, x_i)$
- $\alpha_1 + \cdots + \alpha_n$ 为 $\boldsymbol{x}^{\boldsymbol{\alpha}}$ 的全次数 (total degree), 记为 $\mathrm{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}})$.

称有限和 $F = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$ $(c_{\boldsymbol{\alpha}} \in \mathcal{R})$ 为 $\mathcal{R}$ 上关于 $x_1, \ldots, x_n$ 的多项式 (polynomial)

- $c_{\boldsymbol{\alpha}}$ 为 F 关于项 $\boldsymbol{x}^{\boldsymbol{\alpha}}$ 的系数 (coefficient), 记为 $\mathrm{coef}(F, \boldsymbol{x}^{\boldsymbol{\alpha}})$
- 若 $c_{\boldsymbol{\alpha}} \neq 0$, 则称 $c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$ 为 F 的 单项式 (monomial).
- F 关于变元 x_i 的次数 (degree)

$$\deg(F, x_i) := \max\{\deg(\boldsymbol{x}^{\boldsymbol{\alpha}}, x_i) : \mathrm{coef}(F, \boldsymbol{x}^{\boldsymbol{\alpha}}) \neq 0\}$$

- F 的全次数 (total degree)

$$\mathrm{tdeg}(F) := \max\{\mathrm{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) : \mathrm{coef}(F, \boldsymbol{x}^{\boldsymbol{\alpha}}) \neq 0\}$$

多项式环

对于 $\mathcal{R}$ 上关于 $x_1, \ldots, x_n$ 的任意多项式 $F = \sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$, $G = \sum_{\boldsymbol{\alpha}} b_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$, 定义加法和乘法如下:

$$F + G := \sum_{\boldsymbol{\alpha}} (a_{\boldsymbol{\alpha}} + b_{\boldsymbol{\alpha}}) \boldsymbol{x}^{\boldsymbol{\alpha}}, \quad F \cdot G := \sum_{\boldsymbol{\gamma}} c_{\boldsymbol{\gamma}} \boldsymbol{x}^{\boldsymbol{\gamma}},$$

其中 $c_{\boldsymbol{\gamma}} = \sum_{\boldsymbol{\alpha}+\boldsymbol{\beta}=\boldsymbol{\gamma}} a_{\boldsymbol{\alpha}} b_{\boldsymbol{\beta}}$.

按上述定义的加法和乘法, $\mathcal{R}$ 上关于 $x_1, \ldots, x_n$ 的所有多项式组成的集合构成带单位元的交换环, 称为 $\mathcal{R}$ 上关于 $x_1, \ldots, x_n$ 的多项式环 (polynomial ring), 记为 $\mathcal{R}[x_1, \ldots, x_n]$ 或 $\mathcal{R}[\boldsymbol{x}]$.

- 当 $n = 1$ 时, 称为一元多项式环 (univariate polynomial ring);
- 当 $n > 1$ 时, $\mathcal{R}[\boldsymbol{x}]$ 称为多元多项式环 (multivariate polynomial ring).

多项式：从项的角度，项序

变元 $x_1, \ldots, x_n$ 的所有项组成的集合记为 $\mathfrak{T}(\boldsymbol{x})$: $x_1 < \cdots < x_n$

集合 $\mathfrak{T}(\boldsymbol{x})$ 上的全序关系 $<$ 称为项序 (term ordering), 如果:

1. 对任意 $\mu_1, \mu_2, \mu \in \mathfrak{T}(\boldsymbol{x})$, 若 $\mu_1 < \mu_2$, 则 $\mu\mu_1 < \mu\mu_2$;
2. $<$ 为良序, 即 $\mathfrak{T}(\boldsymbol{x})$ 中任意非空子集关于 $<$ 都有最小元.

常见的全序

设 $\boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $\boldsymbol{x}^{\boldsymbol{\beta}} = x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathfrak{T}(\boldsymbol{x})$

1. 字典序 (lexicographical order): $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}} \Leftrightarrow$
   存在 $i\,(1 \leqslant i \leqslant n), \alpha_j = \beta_j \ \ (i+1 \leqslant j \leqslant n)$ 且 $\alpha_i < \beta_i$
2. 分次字典序 (graded lexicographical order): $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\text{grlex}} \boldsymbol{x}^{\boldsymbol{\beta}} \Leftrightarrow$
   $\text{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) < \text{tdeg}(\boldsymbol{x}^{\boldsymbol{\beta}})$, 或者 $\text{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \text{tdeg}(\boldsymbol{x}^{\boldsymbol{\beta}})$ 且 $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}}$
3. 分次逆字典序 (graded reverse lexicographical order):
   $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\text{grevlex}} \boldsymbol{x}^{\boldsymbol{\beta}} \Leftrightarrow$
   $\text{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) < \text{tdeg}(\boldsymbol{x}^{\boldsymbol{\beta}})$, 或者 $\text{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \text{tdeg}(\boldsymbol{x}^{\boldsymbol{\beta}})$ 且 $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\text{rlex}} \boldsymbol{x}^{\boldsymbol{\beta}}$.

项序

Example

设变元序为 $x < y < z$. 多项式

$$x^2yz + 2\,x^3yz + 3\,xy^3 + 4\,y^2z^2 \in \mathbb{Z}[x, y, z]$$

可按字典序、分次字典序和分次逆字典序从大到小排列:

- 字典序: $4\,y^2z^2 + 2\,x^3yz + x^2yz + 3\,xy^3$;
- 分次字典序: $2\,x^3yz + 4\,y^2z^2 + x^2yz + 3\,xy^3$;
- 分次逆字典序: $2\,x^3yz + 4\,y^2z^2 + 3\,xy^3 + x^2yz$.

设 $F = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}}\,\boldsymbol{x}^{\boldsymbol{\alpha}}$ 为 $\mathcal{R}[\boldsymbol{x}]$ 中的非零多项式, $<$ 为 $\mathcal{R}[\boldsymbol{x}]$ 上的项序, 则 F 关于 $<$ 的

- 首项 (head term): $\mathrm{ht}_<(F) := \max_<\{\mu : \mu \in \mathfrak{T}(F)\}$
- 首项系数 (head coefficient): $\mathrm{hc}_<(F) := \mathrm{coef}(F, \mathrm{ht}_<(F))$
- 首单项式 (head monomial): $\mathrm{hm}_<(F) := \mathrm{hc}_<(F) \cdot \mathrm{ht}_<(F)$

在不引起混淆的情况下, 分别简写为 $\mathrm{ht}(F)$, $\mathrm{hc}(F)$ 和 $\mathrm{hm}(F)$.

项序

引理 1.1.5

设 $<$ 为 $\mathfrak{T}(\boldsymbol{x})$ 上的全序关系, 则 $<$ 为良序当且仅当 $\mathfrak{T}(\boldsymbol{x})$ 中任意严格递减序列都终止.

- 证明: 不存在不终止的严格递减序列.
- 上述引理常常用来证明多项式算法的终止性.

定理 1.1.6

全序关系 $<_{\text{lex}}, <_{\text{grlex}}$ 和 $<_{\text{grevlex}}$ 均为项序.

- 下面仅证明字典序 $<_{\text{lex}}$ 的情形: 利用上述引理
- 逆字典序不是项序.

多项式：从变元的角度

所有 $k\,(1 \leqslant k \leqslant n)$ 都有 $\mathcal{R}[\boldsymbol{x}] = \mathcal{R}[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n][x_k]$，$F \in \mathcal{R}[\boldsymbol{x}]$ 可以写成下面的形式

$$F = \sum_{i=0}^{d_k} C_i\, x_k^i$$

其中 $C_i \in \mathcal{R}[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$，$d_k = \deg(F, x_k)$，且 $C_{d_k} \neq 0$.

- 称 C_{d_k} 为 F 关于变元 x_k 的导系数 (leading coefficient)，记为 $\mathrm{lc}(F, x_k)$.

对 $F \in \mathcal{R}[\boldsymbol{x}] \setminus \mathcal{R}$，定义 F 的：

- 类 (class)：F 所含变元的最大下标

$$\mathrm{cls}(F) := \max\{k :\ \deg(F, x_k) > 0, 1 \leqslant k \leqslant n\};$$

- 导元 (leading variable)：$\mathrm{lv}(F) := x_{\mathrm{cls}(F)}$
- 导次数 (leading degree)：$\mathrm{ldeg}(F) := \deg(F, \mathrm{lv}(F))$
- 初式 (initial)：$\mathrm{ini}(F) := \mathrm{lc}(F, \mathrm{lv}(F))$

多项式：从变元的角度

Example

考虑 $\mathbb{Z}[x_1, \ldots, x_3]$ 中多项式

$$F = 4\,x_1 x_2^2 x_3 + 4\,x_3^3 - 5\,x_1^3 - 3\,x_1 x_2^2 x_3^3 + 7\,x_1^2 x_3^2.$$

对变元序 $x_1 < x_2 < x_3$ 以及项序 $<_{\text{lex}}$, 容易看出

$$\begin{aligned} &\operatorname{ht}(F) = x_1 x_2^2 x_3^3, \quad \operatorname{hc}(F) = -3, \quad \operatorname{hm}(F) = -3\,x_1 x_2^2 x_3^3, \\ &\operatorname{cls}(F) = 3, \ \operatorname{lv}(F) = x_3, \ \operatorname{ldeg}(F) = 3, \ \operatorname{ini}(F) = -3\,x_1 x_2^2 + 4 \end{aligned}$$

域上的一元多项式

设 $\mathcal{K}$ 为域, $F \in \mathcal{K}[x]$, 将 $\deg(F, x)$ 和 $\mathrm{lc}(F, x)$ 简记为 $\deg(F)$ 和 $\mathrm{lc}(F)$.

定理 (不证明)

设 $\mathcal{K}$ 为域, G 为 $\mathcal{K}[x]$ 中的非常数多项式, 则对任意 $F \in \mathcal{K}[x]$, 存在唯一的 $Q, R \in \mathcal{K}[x]$ 使得

$$F = QG + R, \tag{1}$$

其中 $\deg(R) < \deg(G)$.

若上述定理中的条件满足, 则称 (1) 式为 F 关于 G 的带余除法公式 (division formula), 而 Q 和 R 分别为 F 关于 G 的商 (quotient) 和余式 (remainder).

带余除法算法

算法 2　带余除法 $(Q, R) := \mathsf{Rem}(F, G)$

输入: 多项式 $F, G \in \mathcal{K}[x]$.

输出: F 关于 G 的商 Q 和余式 R.

$Q := 0; R := F; l := \deg(G);$

while $\deg(R) \geqslant l$ **do**

$r := \deg(R);$

$R := R - (\mathrm{lc}(R)/\mathrm{lc}(G))x^{r-l}G;$

$Q := Q + (\mathrm{lc}(R)/\mathrm{lc}(G))x^{r-l};$

end

return (Q, R);

例: $x^3 + 2x + 1$ 除以 $2x + 3 \in \mathbb{Q}[x]$

带余除法算法

算法 2　带余除法 $(Q, R) := \mathsf{Rem}(F, G)$

输入: 多项式 $F, G \in \mathcal{K}[x]$.

输出: F 关于 G 的商 Q 和余式 R.

$Q := 0; R := F; l := \deg(G);$

while $\deg(R) \geqslant l$ **do**

$r := \deg(R);$

$R := R - (\mathrm{lc}(R)/\mathrm{lc}(G))x^{r-l}G;$

$Q := Q + (\mathrm{lc}(R)/\mathrm{lc}(G))x^{r-l};$

end

return (Q, R);

例: $x^3 + 2x + 1$ 除以 $2x + 3 \in \mathbb{Q}[x]$

问: $x^3 + 2x + 1$ 除以 $2x + 3 \in \mathbb{Z}[x]$?

多元多项式的伪除

命题 (伪除, 证明)

设 $F, G \in \mathcal{R}[\boldsymbol{x}]$, x_k 为一变元, 且 $l = \deg(G, x_k)$, $m = \deg(F, x_k)$. 若 $l > 0$, 则存在 $Q, R \in \mathcal{R}[\boldsymbol{x}]$ 以及整数 $0 \leqslant s \leqslant m - l + 1$ 使得

$$\mathrm{lc}(G, x_k)^s F = QG + R, \quad \text{且} \quad \deg(R, x_k) < l. \tag{2}$$

若固定 s, 则 Q, R 唯一确定.

- 表达式 (2) 为 F 关于 G 的伪余公式 (pseudo-remainder formula)
- Q: F 对 G 关于 x_k 的伪商 (pseudo-quotient), $\mathrm{pquo}(F, G, x_k)$
- R 为 F 对 G 关于 x_k 的伪余式 (pseudo-remainder), $\mathrm{prem}(F, G, x_k)$
- 称 F 关于 G 是约化的 (reduced): $\deg(F, \mathrm{lv}(G)) < \mathrm{ldeg}(G)$, 显然 $\mathrm{prem}(F, G)$ 关于 G 是约化的

多元多项式的伪除

算法 1　伪除 $(Q, R, s) := \mathsf{Prem}(F, G, x_k)$

输入: 多项式 $F, G \in \mathcal{R}[\boldsymbol{x}]$, 变元 x_k 使得 $\deg(G, x_k) > 0$.

输出: F 对 G 关于 x_k 的伪商 Q 和伪余式 R, 以及整数 s 使得 (1.4) 式成立.

$R := F; Q := 0; l := \deg(G, x_k); s := 0;$

while $\deg(R, x_k) \geqslant l$ **do**

$r := \deg(R, x_k);$

$R := \mathrm{lc}(G, x_k)R - \mathrm{lc}(R, x_k)x_k^{r-l}G;$

$Q := \mathrm{lc}(G, x_k)Q + \mathrm{lc}(R, x_k)x_k^{r-l};$

$s := s + 1;$

end

return $(Q, R, s);$

Example

考虑多项式 $F = 2y^3 - y^2 + x^2y$, $G = xy^2 + 1$. 由伪除算法可得 F 对 G 关于 y 的伪余公式为

$$x^2F = (2xy - x)G + x^4y - 2xy + x.$$

特别有,

$$\mathrm{pquo}(F, G, y) = 2xy - x,$$

$$\mathrm{prem}(F, G, y) = x^4y - 2xy + x.$$

1.2 域论初步

多项式的零点

本节中 $\mathcal{F}$, $\mathcal{K}$ 和 $\mathcal{L}$ 皆为域.

定义

若 $\mathcal{F} \subseteq \mathcal{K}$, 则称 $\mathcal{K}$ 为 $\mathcal{F}$ 的扩域 (extension field), 而 $\mathcal{F}$ 为基域 (base field).

赋值同态

设 $\mathcal{K}$ 为 $\mathcal{F}$ 的扩域. 对任意 $F = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}} \in \mathcal{F}[\boldsymbol{x}]$ 及 $\boldsymbol{a} \in \mathcal{K}^n$, 定义在 $\boldsymbol{a}$ 处的赋值同态 $\mathrm{ev}_{\boldsymbol{a}}\colon \mathcal{F}[\boldsymbol{x}] \longrightarrow \mathcal{K}$ 为

$$\mathrm{ev}_{\boldsymbol{a}}(F) := \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \boldsymbol{a}^{\boldsymbol{\alpha}}.$$

也将 $\mathrm{ev}_{\boldsymbol{a}}(F)$ 记为 $F(\boldsymbol{a})$ 或 $F|_{\boldsymbol{x}=\boldsymbol{a}}$.

- 若 $F(\boldsymbol{a}) = 0$, 则称 $\boldsymbol{a}$ 为 F 在 $\mathcal{K}^n$ 中的零点 (zero).
- 当 F 为一元多项式时, 其零点 $a \in \mathcal{K}$ 通常称为 F 在 $\mathcal{K}$ 中的根 (root).

若 $\mathcal{K}$ 未明确给出, 则 F 的根意指在 $\mathcal{F}$ 的某个扩域中.

根的重数

重根

设 $F \in \mathcal{F}[x]$, 而 $\mathcal{K}$ 为 $\mathcal{F}$ 的扩域. 对 F 在 $\mathcal{K}$ 中的根 a, 若 $(x-a)^r \mid F$, 而 $(x-a)^{r+1} \nmid F$, 则称 r 为 a 的重数 (multiplicity), 而 a 为 F 的 r 重根. 当 $r=1$ 时, a 称为 F 的单根 (simple root); 当 $r>1$ 时, a 称为 F 的重根 (multiple root).

- 如何判断重根并计算其重数?

形式导数

设 $F = \sum_{i=0}^{m} c_i x^i \in \mathcal{F}[x]$. 定义 F 的形式导数 (formal derivation) 为

$$F' := \sum_{i=1}^{m} i c_i x^{i-1}.$$

- 定义 $F^{(r)} := (F^{(r-1)})'$ / 导数运算的基本性质

域的特征

形式导数的计算与域的特征有密切的关系

- $F = x^3 + 1 \in \mathbb{F}_3[x]$, 则 $F' = ?$

域的特征

对任意 $a \in \mathcal{F}$, 使得 $sa = 0$ 成立的最小正整数 s 称为 $\mathcal{F}$ 的特征 (characteristic), 记为 $\mathrm{char}(\mathcal{F})$.

- 如不存在这样的整数, 则称 $\mathrm{char}(\mathcal{F}) = 0$.
- 对任意域 $\mathcal{F}$, 要么 $\mathrm{char}(\mathcal{F}) = 0$, 要么 $\mathrm{char}(\mathcal{F}) = p > 0$, 其中 p 为素数.

命题 (不证明)

设 $F \in \mathcal{F}[x]$, 则下列结论成立:

1. 若 $\mathrm{char}(\mathcal{F}) = 0$, 则 $F' = 0$ 当且仅当 $F \in \mathcal{F}$;
2. 若 $\mathrm{char}(\mathcal{F}) = p > 0$, 则 $F' = 0$ 当且仅当存在 $G \in \mathcal{F}[x]$, 使得 $F = G(x^p)$, 即 $F \in \mathcal{F}[x^p]$.

判断根的重数

命题 (证明)

设 $\mathrm{char}(\mathcal{F}) = 0$, 而 $F \in \mathcal{F}[x]$, 则下列结论成立:

1. a 是 F 的 r 重根当且仅当对所有 $i\ (0 \leqslant i < r), F^{(i)}(a) = 0$ 且 $F^{(r)}(a) \neq 0$;
2. a 是 F 的 r 重根当且仅当 a 是 $\gcd(F, F')$ 的 $r-1$ 重根.

Example

令 $F = (x-1)^3(x-2)^2 \in \mathbb{Q}[x]$, 则

$$F' = 3(x-1)^2(x-2)^2 + 2(x-1)^3(x-2)$$

$$F'' = 6(x-1)(x-2)^2 + 12(x-1)^2(x-2) + 2(x-1)^3$$

$$F''' = 6(x-2)^2 + 36(x-1)(x-2) + 18(x-1)^2$$

- $F'(2) = 0, F''(2) = 2, F'(1) = F''(1) = 0, F'''(1) = 6.$
- $\gcd(F, F') = (x-1)^2(x-2) \Longrightarrow$ 无平方因子?

有限生成扩域

定义

设 $\mathcal{K}$ 为 $\mathcal{F}$ 的扩域, 而集合 $S \subseteq \mathcal{K}$. 称

- $\mathcal{K}$ 中包含 $\mathcal{F}$ 和 S 的最小环为由 $\mathcal{F}$ 和 S 生成的环, 记为 $\mathcal{F}[S]$.
- 称 $\mathcal{K}$ 中包含 $\mathcal{F}$ 和 S 的最小域为由 $\mathcal{F}$ 和 S 生成的域, 记为 $\mathcal{F}(S)$.
- 若 $S = \{a_1, \ldots, a_n\}$, 则记 $\mathcal{F}[S] = \mathcal{F}[a_1, \ldots, a_n]$, $\mathcal{F}(S) = \mathcal{F}(a_1, \ldots, a_n)$, 而称 $\mathcal{F}(S)$ 为 $\mathcal{F}$ 的有限生成扩域 (finitely generated extension).

命题 (不证明)

设 $\mathcal{K}$ 为 $\mathcal{F}$ 的扩域, 而 $a_1, \ldots, a_n \in \mathcal{K}$, 则

$$\mathcal{F}[a_1, \ldots, a_n] = \{F(a_1, \ldots, a_n) : F \in \mathcal{F}[\boldsymbol{x}]\},$$

$$\mathcal{F}(a_1, \ldots, a_n) = \left\{ \frac{F(a_1, \ldots, a_n)}{G(a_1, \ldots, a_n)} : F, G \in \mathcal{F}[\boldsymbol{x}], G(a_1, \ldots, a_n) \neq 0 \right\}.$$

代数元与极小多项式

代数元、超越元

设 $\mathcal{K}$ 为 $\mathcal{F}$ 的扩域, 而 $a \in \mathcal{K}$. 若存在非零多项式 $F \in \mathcal{F}[x]$, 使得 $F(a) = 0$, 则称 a 为 $\mathcal{F}$ 上的代数元 (algebraic element); 否则称 a 为 $\mathcal{F}$ 上的超越元 (transcendental element).

- 代数扩域 (algebraic extension): 若 $\mathcal{K}$ 中每个元都是 $\mathcal{F}$ 上的代数元; 否则称为超越扩域 (transcendental extension).

设 $r \in \mathbb{Q}$, 则 $\sqrt[m]{r}$ 为 $\mathbb{Q}$ 上的代数元, 因为它是 $x^m - r \in \mathbb{Q}[x]$ 的根. 而 e 和 π 都是 $\mathbb{Q}$ 上的超越元 (证明很繁琐、化圆为方).

极小多项式

设 a 是 $\mathcal{F}$ 上的代数元, 称 $\mathcal{F}[x]$ 中满足 $P(a) = 0$ 的次数最低的首一多项式 P 为 a 在 $\mathcal{F}$ 上的极小多项式 (minimal polynomial), 记作 $\min(\mathcal{F}, a)$.

极小多项式的性质

若基域不同, 代数元的极小多项式也有可能不同.

- i 是 $\mathbb{Q}$, $\mathbb{R}$ 和 $\mathbb{C}$ 上的代数元, 易知 $\min(\mathbb{Q}, \mathrm{i}) = \min(\mathbb{R}, \mathrm{i}) = x^2 + 1$, 而 $\min(\mathbb{C}, \mathrm{i}) = x - \mathrm{i}$.

命题 (证明)

设 $\mathcal{K}$ 为 $\mathcal{F}$ 的扩域, $a \in \mathcal{K}$ 为 $\mathcal{F}$ 上的代数元. 令 $P = \min(\mathcal{F}, a)$, $m = \deg(P)$, 则下列结论成立:

1. P 在 $\mathcal{F}$ 上不可约;
2. 设 $G \in \mathcal{F}[x]$, 则 $G(a) = 0$ 当且仅当 $P \mid G$;
3. $\mathcal{F}(a) \cong \mathcal{F}[x]/\langle P \rangle$, 从而 $\mathcal{F}(a)$ 中每个元均可唯一表为 $\sum_{i=0}^{m-1} c_i a^i$, 其中 $c_i \in \mathcal{F}$;
4. $1, a, \ldots, a^{m-1}$ 是 $\mathcal{F}$ 向量空间 $\mathcal{F}(a)$ 的一组基.

1.4 结式

结式：用根定义

$$F = \sum_{i=0}^{m} a_i x^i, \quad G = \sum_{j=0}^{l} b_j x^j \in \mathcal{R}[x]$$

其中 $a_m, b_l \neq 0$, 且 $m, l > 0$.

一元结式

$F, G \in \mathcal{R}[x]$ 关于 x 的结式 (resultant) 定义为

$$\mathrm{Res}(F, G, x) := a_m^l b_l^m \prod_{i=1}^{m} \prod_{j=1}^{l} (\alpha_i - \beta_j),$$

其中 α_i $(1 \leqslant i \leqslant m)$ 和 β_j $(1 \leqslant j \leqslant l)$ 分别为 F 和 G 的根.

- $\mathrm{Res}(F, G, x) = 0$ 当且仅当 F 和 G 有公共根, 且容易验证

$$\mathrm{Res}(F, G, x) = a_m^l \prod_{i=1}^{m} G(\alpha_i) = (-1)^{ml} b_l^m \prod_{j=1}^{l} F(\beta_j).$$

Sylvester 结式

Sylvester 矩阵

称 $m+l$ 阶方阵

$$\begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & a_m & a_{m-1} & \cdots & a_0 \\ b_l & b_{l-1} & \cdots & b_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & b_l & b_{l-1} & \cdots & b_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} l \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \end{matrix}$$

为 F 和 G 关于 x 的Sylvester (西尔维斯特) 矩阵, 记作 $\mathrm{Syl}(F, G, x)$.

- $\mathrm{Syl}(F, G, x)$ 的前 l 行: $x^{l-1}F, \ldots, xF, F$ 的系数 (后面行)

Sylvester 结式

称矩阵 $\mathrm{Syl}(F, G, x)$ 的行列式为 F 和 G 关于 x 的 Sylvester 结式, 记作 $\mathrm{res}(F, G, x) \Longrightarrow \in$ 哪里?

Sylvester 结式

$$\operatorname{res}(G, F, x) = (-1)^{ml} \det(\operatorname{Syl}(F, G, x)) = (-1)^{ml} \operatorname{res}(F, G, x)$$

Example

$F = x^3 + 3x - 1,\ G = F' = 3x^2 + 3$, 则

$$\operatorname{res}(F, G, x) = \det \begin{pmatrix} 1 & 0 & 3 & -1 & 0 \\ 0 & 1 & 0 & 3 & -1 \\ 3 & 0 & 3 & 0 & 0 \\ 0 & 3 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 & 3 \end{pmatrix} = 135,$$

且 $\operatorname{res}(G, F, x) = (-1)^6 \operatorname{res}(F, G, x) = 135.$

- $\operatorname{res}(F, G, x)$ VS $\operatorname{Res}(F, G, x)$?

结式的性质 I

命题 (证明)

设 $F,\ G \in \mathcal{R}[x]$ 如前所示, 则存在 $A, B \in \mathcal{R}[x]$, 使得 $AF + BG = \mathrm{res}(F, G, x)$, 且 $\deg(A) < l, \deg(B) < m$.

将 Sylvester 矩阵的第 i 列乘以 x^{m+l-i} 然后加到最后一列, 变为

$$\left.\begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & & x^{l-1}F \\ & \ddots & \ddots & \ddots & \ddots & \\ & & a_m & a_{m-1} & \cdots & F \\ b_l & b_{l-1} & \cdots & b_0 & & x^{m-1}G \\ & \ddots & \ddots & \ddots & \ddots & \\ & & b_l & b_{l-1} & \cdots & G \end{pmatrix}\right\} \begin{matrix} l \\ \\ \\ m \\ \\ \end{matrix}$$

将上述矩阵的行列式按最后一列展开即证.

- 矩阵的第 3 类初等变换，不改变行列式

结式的性质 II

命题 (证明)

设 $F,\ G \in \mathcal{R}[x]$ 如前文所示, 则下列条件等价:

1. $\mathrm{res}(F, G, x) = 0$;
2. 存在非零多项式 $A, B \in \mathcal{R}[x]$, 使得 $AF + BG = 0$, 且 $\deg(A) < l, \deg(B) < m$.

- 线性方程组是否有非零解

推论 (证明、结式的重要性质)

设 $F,\ G \in \mathcal{R}[x]$ 如前文所示, 则 $\mathrm{res}(F, G, x) = 0$ 当且仅当 F 和 G 有非常数公因子.

- VS $\mathrm{Res}(F, G, x)$ ($= 0$ 当且仅当有公共根)?

结式的应用: 解多项式方程组

圆与椭圆的交点问题

$$\begin{cases} P_1 = x_1^2 + x_2^2 - 2 = 0 \\ P_2 = x_1^2 + 6x_2^2 - 3 = 0 \end{cases}$$

1. 计算 P_1 与 P_2 关于 x_1 的结式

$$R = \mathrm{res}(P_1, P_2, x_1) = (5x_2^2 - 1)^2. \quad \text{有公共根等价于?}$$

2. 计算 R 关于 x_2 的解得 $x_2 = \pm\frac{1}{\sqrt{5}}$.
3. 分别代入 $P_1 = 0$ 与 $P_2 = 0$, 则两式均变为 $x_1^2 - \frac{9}{5} = 0$, 解得 $x_1 = \pm\frac{3}{\sqrt{5}}$.

所有解

$$\left(\frac{3}{\sqrt{5}}, \frac{1}{\sqrt{5}}\right), \left(\frac{3}{\sqrt{5}}, -\frac{1}{\sqrt{5}}\right), \left(-\frac{3}{\sqrt{5}}, \frac{1}{\sqrt{5}}\right), \left(-\frac{3}{\sqrt{5}}, -\frac{1}{\sqrt{5}}\right)$$

结式的应用：参数曲线的隐式化

椭圆的参数方程

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

其中 t 为参数. 计算椭圆关于 x 和 y 的隐式方程 ($\Longrightarrow$ 消去参数 t)

1. 引入多项式 $P_1 = (t^2+1)x - t$, $P_2 = (t^2+1)y - 2$
2. 计算 P_1 与 P_2 关于 t 的结式

$$R = \mathrm{res}(P_1, P_2, t) = 4x^2 + y^2 - 2y$$

3. $R = 0$ 即为所求的椭圆隐式方程 (Why?)

第一次大作业

1. 编写程序计算环上两个一元多项式关于某个变元的 Sylvester 结式：输入为 $F, G \in \mathcal{R}[x]$ 和 x, 输出为 $\mathrm{res}(F, G, x)$.

- 可以利用下式验证结果

$$\mathrm{res}((t^2+1)x - t, (t^2+1)y - 2, t) = 4x^2 + y^2 - 2y$$

2. 利用上述程序解决如下曲面的隐式化问题, 即计算满足下述参数方程的仅含 x, y, z 的隐式多项式.

$$x = \frac{t^3}{2}, \quad y = \frac{(s^2-1)t^2}{s^2+1}, \quad z = \frac{2st^2}{s^2+1}$$

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 3 月 27 日，请将作业打包.zip文件以“计算机代数 1–姓名–学号”命名，以同样名称为邮件名发送至 zjwang@buaa.edu.cn.

几点提示

1. 建议用 Maple 软件写，因为已经有常见的处理矩阵和多项式的函数 (和计算结式的函数 resultant(F, G, x)...)
2. 利用 Maple 软件完成作业时可能需要用到的函数
   - degree(F, x): 返回多项式 F 关于变元 x 的次数
   - coeff(F, x, n): 返回多项式 F 关于 x^n 的系数
   - Matrix(n): 构造一个 $n \times n$ 的全零矩阵
   - factor(F): 返回多项式 F 的因式分解
   - 矩阵赋值可以在帮助文件中搜索Matrix Assignment
   - LinearAlgebra[Determinant](M)：返回矩阵 M 的行列式
   - 基本 for 循环等命令自己查帮助文件
3. 第 2 问需要消去两个变元 s 和 t, 但是结式一次只能消去一个变元，因此...
4. 源程序需包含适量的注释

1.5 最大公因子的计算

最大公因子

定义

设 $F_1, \ldots, F_s \in \mathcal{R}[\boldsymbol{x}]$ 不全为零. 如果存在多项式 $H \in \mathcal{R}[\boldsymbol{x}]$, 使得

1. 对所有 $i\,(1 \leqslant i \leqslant s)$, $H \mid F_i$,
2. 对任意 $P \in \mathcal{R}[\boldsymbol{x}]$, 若 $P \mid F_i\,(1 \leqslant i \leqslant s)$, 则 $P \mid H$,

那么称 H 为 $F_1, \ldots, F_s$ 的最大公因子 (greatest common divisor), 记为 $\gcd(F_1, \ldots, F_s)$.

- 不一定存在 $\Longrightarrow$ $\mathcal{R}$ 限定为唯一析因整环则一定存在
- 不一定唯一, 它们一般相差单位元 $\Longrightarrow$ $2\,x, x, (1/2)x$ 都是 $x, x^2 \in \mathbb{Q}[x]$ 的最大公因子
- $\gcd(F_1, \ldots, F_s) = G$: G 为 $F_1, \ldots, F_s$ 的一个最大公因子

本原多项式

定义

$\mathcal{R}$ 为唯一析因整环, $F \in \mathcal{R}[\boldsymbol{x}]$ 看作关于变元 x_k 的一元多项式

$$F = \sum_{i=0}^{d_k} C_i \, x_k^i,$$

其中 $C_i \in \mathcal{R}[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n]$, 则

- 系数 $C_0, \ldots, C_{d_k}$ 的最大公因子称为 F 关于 x_k 的容度 (content), 记为 $\operatorname{cont}(F, x_k)$.
- 若 $\operatorname{cont}(F, x_k)$ 为单位元, 则称 F 关于 x_k 为本原的 (primitive).
- 称 $F/\operatorname{cont}(F, x_k)$ 为 F 关于 x_k 的本原部分 (primitive part), 记作 $\operatorname{pp}(F, x_k)$

Gauss 引理 (不证明)

设 $\mathcal{R}$ 为唯一析因整环. 若 $F, G \in \mathcal{R}[\boldsymbol{x}]$ 关于 x_k 是本原的, 则 FG 关于 x_k 也是本原的.

Euclid 算法：域上的一元多项式

算法 3　Euclid 算法 $(H, A, B) := \mathsf{Euclid}(F, G)$

输入: 多项式 $F, G \in \mathcal{K}[x]$.

输出: F 和 G 的最大公因子 H, 以及 A 和 B, 使得 $H = AF + BG$.

```
1 H := F; L := G; U := 0; V := 1; A := 1; B := 0;
2 while L ≠ 0 do
3     (Q, R) := Rem(H, L);
4     H := L; L := R;
5     C := A; D := B;
6     A := U; B := V;
7     U := C − QU; V := D − QV;
8 end
9 return (H, A, B);
```

- 扩展的 Euclid 算法: 同时输出 $A, B \in \mathcal{K}[x]$ 使得 $H = AF+BG$
- 证明: 终止性 / 输出 H 是最大公因子
- 问题：域 $\mathcal{K} \Longrightarrow$ 环 $\mathcal{R}$??

多项式余式序列

多项式 $A, B \in \mathcal{R}[x]$ 称为相似的 (similar), 记作 $A \sim B$, 如果存在 $a, b \in \mathcal{R}$ 且 $ab \neq 0$, 使得 $aA = bB$. 称 a 和 b 为 A 与 B 的相似系数 (coefficients of similarity).

多项式余式序列

设 $F, G \in \mathcal{R}[\boldsymbol{x}]$ 且 $\deg(F, x_k) \geqslant \deg(G, x_k)$. 称非零多项式序列 $P_1 = F, P_2 = G, P_3, \ldots, P_r$ 为 F 和 G 关于 x_k 的多项式余式序列 (polynomial remainder sequence), 如果下列条件成立:

1. 对所有 i $(3 \leqslant i \leqslant r)$, $P_i \sim \operatorname{prem}(P_{i-2}, P_{i-1}, x_k) \neq 0$;
2. $\operatorname{prem}(P_{r-1}, P_r, x_k) = 0$.

- Euclid 多项式余式序列: $P_i = \operatorname{prem}(P_{i-2}, P_{i-1}, x_k) \neq 0$
- 本原多项式余式序列: $P_i = \operatorname{pp}(\operatorname{prem}(P_{i-2}, P_{i-1}, x_k)) \neq 0$

多项式余式序列计算最大公因子

命题 (证明)

设 $F, G \in \mathcal{R}[\boldsymbol{x}]$ 为关于 x_k 的本原多项式, 而 $P_1 = F, P_2 = G, P_3, \ldots, P_r$ 为 F 和 G 关于 x_k 的多项式余式序列, 则

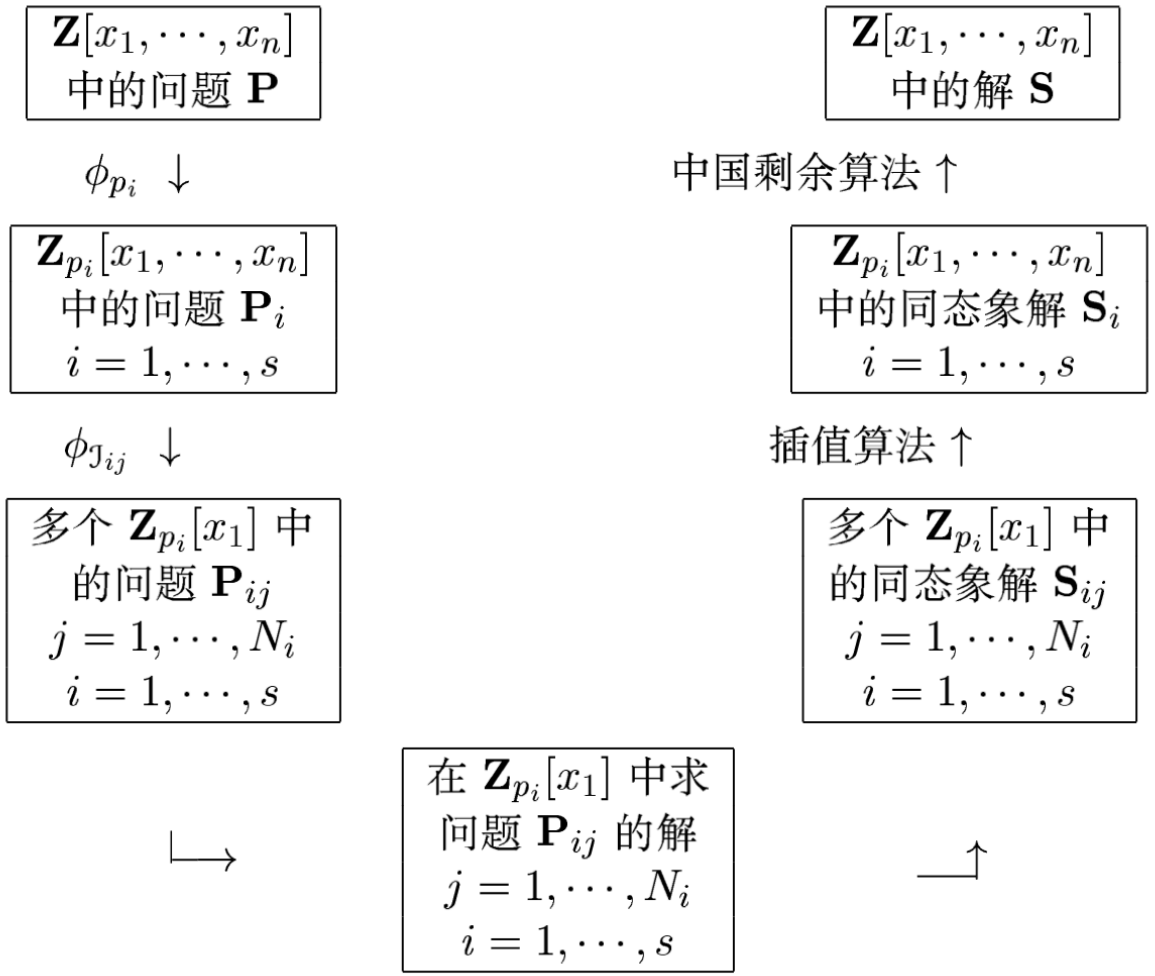
$$\gcd(F, G) = \mathrm{pp}(P_r, x_k).$$

Example

$$F = y^6 + xy^5 + x^3y - xy + x^4 - x^2,$$
$$G = xy^5 - 2\,y^5 + x^2y^4 - 2\,xy^4 + xy^2 + x^2y.$$

- Maple 程序
- 注意: 结果是 $x + y$, 但中间出现的系数达几十万: 中间膨胀 $\Longrightarrow$ 模 11 不就不膨胀了吗!?

模方法：路线图



模方法求解的路线图

模方法：映射

同态映射 $\mathbb{Z} \to \mathbb{Z}_m$

对给定整数 $m \in \mathbb{Z}$, 定义同态映射 $\phi_m : \mathbb{Z}[\boldsymbol{x}] \longrightarrow \mathbb{Z}_m[\boldsymbol{x}]$ 为

$$\phi_m\Big(\sum_{\boldsymbol{\alpha}} c_{\alpha}\boldsymbol{x}^{\boldsymbol{\alpha}}\Big) = \sum_{\boldsymbol{\alpha}} \tilde{c}_{\alpha}\boldsymbol{x}^{\boldsymbol{\alpha}},$$

其中 $\tilde{c}_{\alpha} \in \mathbb{Z}_m$ 满足 $\tilde{c}_{\alpha} \equiv c_{\alpha} \mod m$.

- 当多项式变元的个数为零时, ϕ_m 将 $\mathbb{Z}$ 投影到 $\mathbb{Z}_m$.

对于一个变元的赋值映射

对某一特定未定元 x_i 和固定元素 $a \in \mathcal{R}$, 定义赋值同态 $\mathrm{ev}_{x_i - a}$: $\mathcal{R}[\boldsymbol{x}] \longrightarrow \mathcal{R}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ 为对未定元 x_i 赋值 a.

- 从除法角度看, 这相当于将 $F \in \mathcal{R}[\boldsymbol{x}]$ 映射到 F 除以 $x_i - a$ 的余式.

模方法：插值

命题 (不证明)

设 $u_0, \ldots, u_s \in \mathcal{K}$, 而 $a_0, \ldots, a_s \in \mathcal{K}$ 两两互异, 则存在 $U \in \mathcal{K}[x]$:

1. $\deg(U) \leqslant s$;
2. $U(a_i) = u_i \ (0 \leqslant i \leqslant s)$.

算法 4　Newton 插值算法 $U := \mathsf{NewtonIntp}(a_0, \ldots, a_s; u_0, \ldots, u_s)$

输入: 域 $\mathcal{K}$ 中 $s+1$ 个插值点 $a_0, \ldots, a_s$ 及 $u_0, \ldots, u_s$.

输出: $U \in \mathcal{K}[x]$, 满足 $U(a_i) = u_i \ (0 \leqslant i \leqslant s)$.

$w_0 := u_0; U_0(x) := w_0;$

for $k = 1$ **to** s **do**

$v_k := \prod_{i=0}^{k-1}(a_k - a_i);$

$w_k := (u_k - U_{k-1}(a_k))/v_k;$

$U_k(x) := U_{k-1}(x) + w_k \prod_{i=0}^{k-1}(x - a_i);$

end

$U := U_s(x);$

return U;

牛顿插值

模方法：中国剩余定理

定理：整数情形的中国剩余定理 (证明)

设 $m_1, \ldots, m_s \in \mathbb{Z}\backslash\{0\}$ 两两互素, 而 $r_1, \ldots, r_s \in \mathbb{Z}$, 则存在 $r \in \mathbb{Z}$,

$$r \equiv r_i \mod m_i \quad (1 \leqslant i \leqslant s),$$

并且 r 在满足 $0 \leqslant r < m_1 \cdots m_s$ 的条件下是唯一的.

算法 5　整数情形的中国剩余算法 $r := \mathsf{CRemInt}_s(r_1, \ldots, r_s; m_1, \ldots, m_s)$

输入: $r_1, \ldots, r_s \in \mathbb{Z}$ 和 $m_1, \ldots, m_s \in \mathbb{Z}\backslash\{0\}$, 其中 m_i 两两互素.
输出: $r \in \mathbb{Z}$, 使得 $r \equiv r_i \mod m_i$ $(1 \leqslant i \leqslant s)$.

$M := m_1$; $r := r_1 \mod m_1$;
for $k = 2$ **to** s **do**
　$c := M^{-1} \mod m_k$;
　$r' := r \mod M$;
　$\sigma := (r_k - r')c \mod m_k$;
　$r := r' + \sigma M$;
　$M := M m_k$;
end
return r;

整数情形的中国剩余定理算法

模方法：中国剩余定理 II

定理：多项式情形的中国剩余定理

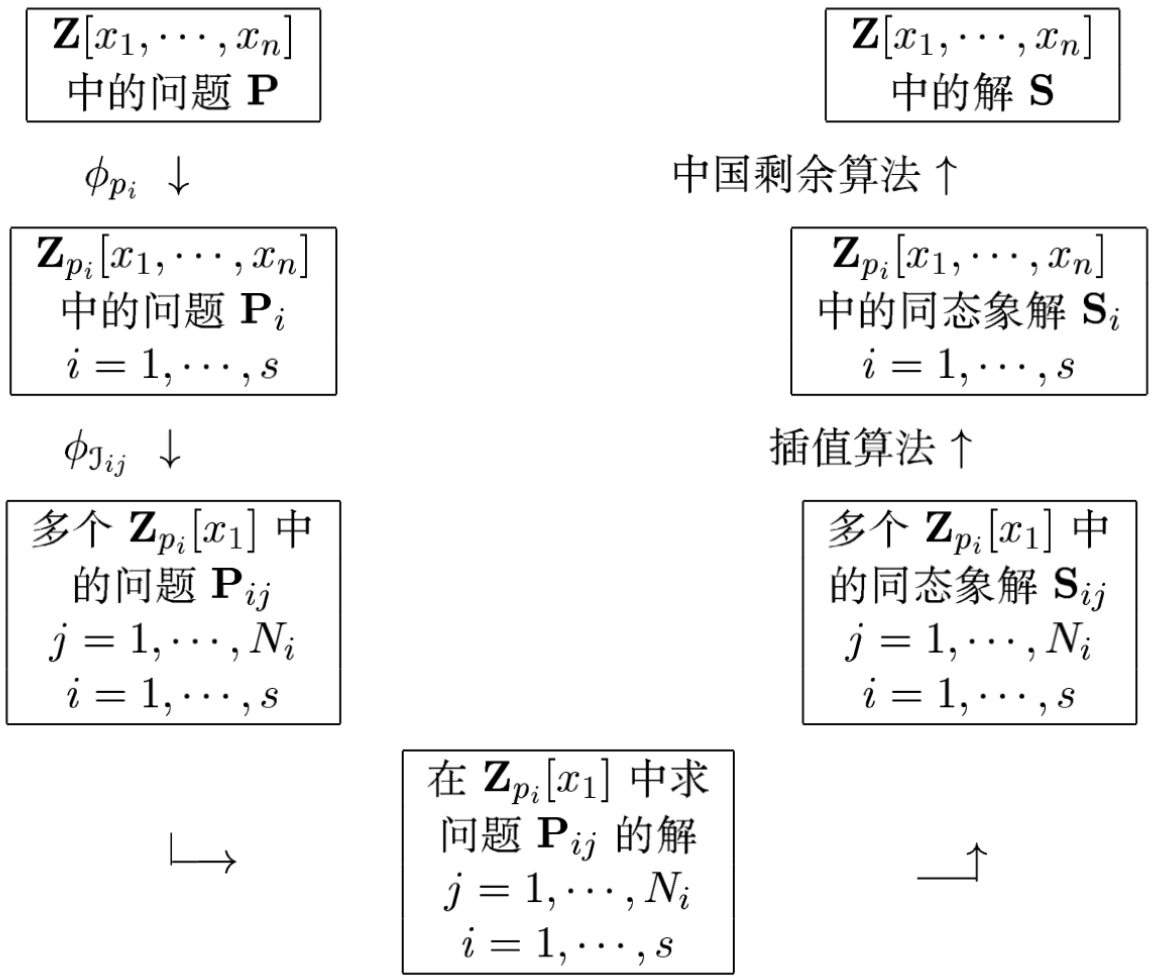
设 $P_1, \ldots, P_s \in \mathcal{K}[x]$ 两两互素. 记 $P = \prod_{j=1}^{s} P_j$, $Q_i = P/P_i$, 而 U_i 为 Q_i 模 P_i 的逆, 即 $U_i Q_i \equiv 1 \mod P_i$. 对任意 $R_1, \ldots, R_s \in \mathcal{K}[x]$, 令 $H = \sum_{j=1}^{s} Q_j U_j R_j$, 则 $H \in \mathcal{K}[x]$ 为

$$H \equiv R_i \mod P_i \ (1 \leqslant i \leqslant s)$$

的解, 且 H 在满足 $\deg(H) < \sum_{i=1}^{s} \deg(P_i)$ 的条件下是唯一的.

- Q_i 模 P_i 的逆怎么算?

模方法



模方法求解的路线图

模方法：一个例子

求 F 和 G 的最大公因子 (取变元序 $z < y < x$.)

$$
\begin{aligned}
F = {} & x^5 + 2\,x^4yz + 13\,x^3yz^2 - 21\,x^3y^3z + 3\,x^3 + 26\,x^2y^2z^3 - 42\,x^2y^4z^2 \\
& + 2\,x^2 + 39\,xyz^2 - 63\,xy^3z + 4\,xyz + 6, \\
G = {} & x^6 + 13\,x^4yz^2 - 21\,x^4y^3z + x^4z + x^4y + 3\,x^3 + 13\,x^2yz^3 + 13\,x^2y^2z^2 \\
& - 21\,x^2y^3z^2 - 21\,x^2y^4z + 13\,xyz^2 - 21\,xy^3z + 2\,xz + 2\,xy + 2.
\end{aligned}
$$

第一步: 取素数 $p_1 = 11$, 求 $\gcd(F_{11}, G_{11})$, 这时

$$
\begin{aligned}
F_{11} = {} & x^5 + 2\,x^4yz + 2\,x^3yz^2 + x^3y^3z + 3\,x^3 + 4\,x^2y^2z^3 + 2\,x^2y^4z^2 + 2\,x^2 \\
& - 5\,xyz^2 + 3\,xy^3z + 4\,xyz - 5, \\
G_{11} = {} & x^6 + 2\,x^4yz^2 + x^4y^3z + x^4z + x^4y + 3\,x^3 + 2\,x^2yz^3 + 2\,x^2y^2z^2 \\
& + x^2y^3z^2 + x^2y^4z + 2\,xyz^2 + y^3xz + 2\,xz + 2\,xy + 2.
\end{aligned}
$$

模方法：一个例子 II

(1) 因为 $\deg(H,z)\leqslant 3, \deg(H,y)\leqslant 4$, 所以在 $\mathbb{Z}_{11}$ 中选取 z 的四个赋值点 $2,-5,-3,5$, 并分别计算 $z_i=2,-5,-3,5$ 时的最大公因子 $H_{11}=\gcd(F_{11}(x,y,z_i),G_{11}(x,y,z_i))$.

(a) 在 $z_1=2$ 时,

$$\begin{aligned}F_{11}(x,y,2)&=2x^5-4x^4y+5x^3y+4x^3y^3-3x^3+x^2y^2\\&\quad+3x^2y^4+4x^2+xy+5xy^3-6,\\G_{11}(x,y,2)&=5x^6-5x^4y-x^4y^3-2x^4-2x^3-5x^2y\\&\quad+3x^2y^2-4x^2y^3-2x^2y^4+xy-2xy^3-4x-2.\end{aligned}$$

又在 $\mathbb{Z}_{11}$ 中随机选取 y 的 5 个赋值点: $1,3,5,-4,4$, 并用 Euclid 算法分别计算 $H_{11}(x,y_j,2)=\gcd(F_{11}(x,y_j,2),G_{11}(x,y_j,2))$

$$\begin{aligned}H_{11}(x,1,2)&\equiv x^3-x+2 \mod 11,\\H_{11}(x,3,2)&\equiv x^3+x+2 \mod 11,\\H_{11}(x,5,2)&\equiv x^3+4x+2 \mod 11,\\H_{11}(x,-4,2)&\equiv x^3+5x+2 \mod 11,\\H_{11}(x,4,2)&\equiv x^3-5x+2 \mod 11.\end{aligned}$$

模方法：一个例子 III

(b) 用插值算法计算 $H_{11}(x, y, z_1)$. 令 $P_i(y) = \prod_{j\neq i}(y - y_j)$, 其中 $1 \leqslant i, j \leqslant 5$. 由 Lagrange 插值公式可得

$$\begin{aligned} H_{11}(x, y, 2) &= \sum_{i=1}^{5} H_{11}(x, y_i, 2) P_i(y) P_i(y_i)^{-1} \\ &\equiv x^3 + 2\,xy^3 - 3\,xy + 2 \mod 11. \end{aligned}$$

(2) 同理, 关于 z 的另外三个赋值点有

$$\begin{aligned} H_{11}(x, y, -5) &\equiv x^3 - 5\,xy^3 - 5\,xy + 2 \mod 11, \\ H_{11}(x, y, -3) &\equiv x^3 - 3\,xy^3 - 4\,xy + 2 \mod 11, \\ H_{11}(x, y, 5) &\equiv x^3 + 5\,xy^3 - 5\,xy + 2 \mod 11. \end{aligned}$$

(3) 由插值公式计算得

$$H_{11}(x, y, z) = \gcd(F_{11}, G_{11}) \equiv x^3 + xy^3z + 2\,xyz^2 + 2 \mod 11.$$

模方法：一个例子 IV

第二步: 取 $p_2 = 17$, 采用第一步中的方法得

$$H_{17}(x, y, z) = \gcd(F_{17}, G_{17}) \equiv x^3 - 4\,xy^3z - 4\,xyz^2 + 2 \mod 17.$$

第三步: 因为 H_{11} 和 H_{17} 关于 x 的方次相同, 用中国剩余定理将其结合起来可得 $H = x^3 - 21\,xy^3z + 13\,xyz^2 + 2 \in \mathbb{Z}[x, y, z]$. 经检验, 其恰为欲求的最大公因子.

- 素数的选取: unlucky prime numbers
- 插值：稀疏插值

多项式的无平方分解

设 $\mathcal{R}$ 为唯一析因整环

无平方多项式

若非常数多项式 F 无重因子, 即不存在 $G \in \mathcal{R}[x] \setminus \mathcal{R}$ 使得 $G^2 \mid F$, 则称 $F \in \mathcal{R}[x]$ 无平方因子, 简称 F 无平方 (squarefree).

命题 (证明)

设 $\mathcal{K}$ 为域, 而 $F \in \mathcal{F}[x]$. 若 $\gcd(F, F') = 1$, 则 F 无平方.

无平方分解

定义 $F \in \mathcal{R}[x]$ 的无平方分解为 $F = \prod_{i=1}^{k} F_i^i$, 其中每个 $F_i \in \mathcal{R}[x]$ 都无平方, 并且当 $i \neq j$ 时, $\gcd(F_i, F_j) = 1$. 称多项式 $\operatorname{sqfr}(F) := \prod_{i=1}^{k} F_i$ 为 F 的无平方伴随 (squarefree associate).

- 因式分解: 首先无平方分解, 假设输入多项式无平方

多项式的无平方分解

- 仅考虑 $\mathrm{char}(\mathcal{K}) = 0$ 的情形

命题 (证明)

设 $F \in \mathcal{K}[x] \setminus \mathcal{K}$, 其中 $\mathrm{char}(\mathcal{K}) = 0$. 令

$$P = \gcd(F, F'), \quad Q = F/P, \quad S = \gcd(P, Q), \quad T = Q/S,$$

则 $Q = \mathrm{sqfr}(F)$, $S = \mathrm{sqfr}(P) = P/\gcd(P, P')$, 而 T 是 F 的不可约因子的乘积.

$$\begin{array}{rcccccccc}
F & = & & F_1 & F_2^2 & F_3^3 & \cdots & F_i^i & \cdots, \\
F' & = & G & & F_2 & F_3^2 & \cdots & F_i^{i-1} & \cdots, \\
P & = & & & F_2 & F_3^2 & \cdots & F_i^{i-1} & \cdots, \\
Q & = & & F_1 & F_2 & F_3 & \cdots & F_i & \cdots, \\
S & = & & & F_2 & F_3 & \cdots & F_i & \cdots, \\
P/S & = & & & & F_3 & \cdots & F_i^{i-2} & \cdots.
\end{array}$$

多项式的无平方分解

算法 6　无平方分解 $\prod_{i=1}^{s} F_i^i := \mathsf{Sqfree}(F)$

输入: 多项式 $F \in \mathcal{K}[x]$.

输出: F 的无平方分解 $F = \prod_{i=1}^{s} F_i^i$.

$i := 1; L := 1; S := F;$

$P := \gcd(F, F'); Q := F/P;$

while $\deg(S) > 0$ **do**

　$S := \gcd(P, Q); T := Q/S; L := LT^i;$

　$Q := S; P := P/S; i := i + 1;$

end

return L;

Example

计算多项式 $F = x^5 - x^3 \in \mathbb{Q}[x]$ 的无平方分解.

- 思考: $\mathrm{char}(\mathcal{K}) = p$ 有什么不同？例如 $F = x^p \in \mathbb{F}_p[x]$

第一章总结

- 多项式基础：项与变元的角度看多元多项式、伪除
- 域论初步：根的重数 (形式导数)
- 结式：结式的意义、Sylvester 结式的构造和性质、应用举例
- 最大公因子：多项式余式序列、模方法
- 无平方分解：算法