第一章　多项式

张彪

天津师范大学

数学科学学院

zhang@tjnu.edu.cn

目录

- 在讨论问题时，应首先明确所考虑的数的范围；不同范围内同一问题的答案可能不同. 例如方程 $x^2+1=0$ 在实数域 $\mathbb{R}$ 与复数域 $\mathbb{C}$ 中的解集不同.
- 常见的数集：$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$.
- 这些数集的共同代数性质：对加、减、乘、除（除数不为 0）运算封闭.
- 为统一具有这些代数性质的集合，引入一个抽象的数学对象——数域（Field）.

- 在讨论问题时，应首先明确所考虑的数的范围；不同范围内同一问题的答案可能不同. 例如方程 $x^2+1=0$ 在实数域 $\mathbb{R}$ 与复数域 $\mathbb{C}$ 中的解集不同.
- 常见的数集：$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$.
- 这些数集的共同代数性质：对加、减、乘、除（除数不为 0）运算封闭.
- 为统一具有这些代数性质的集合，引入一个抽象的数学对象——数域（Field）.

定义 (数域)

设 P 是复数集的一个子集，且 $0,1\in P$. 若对任意 $a,b\in P$ 有：

$$a+b,\ a-b,\ ab\in P, \qquad \text{且在} b\neq 0 \text{ 时} \frac{a}{b}\in P,$$

则称 P 为一个数域.

(1) 简而言之：在加、减、乘、除（除数不为 0）运算下封闭并包含 0、1 的集合称为数域.

(2) 因此任何数域都包含 0 与 1.

例子

有理数集 $\mathbb{Q}$、实数集 $\mathbb{R}$、复数集 $\mathbb{C}$ 都是数域；而整数集 $\mathbb{Z}$、自然数集 $\mathbb{N}$ 都不是数域.

数集的封闭性举例

问题 1

所有奇数组成的数集，对于加、减、乘、除四种运算，哪些是封闭的？

问题 2

某个数的整倍数所组成的数集，对于加、减、乘、除四种运算，哪些是封闭的？

数集的封闭性举例

问题 1

所有奇数组成的数集，对于加、减、乘、除四种运算，哪些是封闭的？

问题 2

某个数的整倍数所组成的数集，对于加、减、乘、除四种运算，哪些是封闭的？

解答 1

所有奇数组成的数集

- 乘法封闭，例如 $3 \times 5 = 15$；
- 加法不封闭，例如 $3 + 5 = 8$；
- 减法不封闭，例如 $9 - 5 = 4$；
- 除法不封闭，例如 $3 \div 5 = \frac{3}{5}$.

解答 2

某个数的整倍数组成的数集（如所有 3 的倍数）

- 加法封闭，例如 $3 + 6 = 9$；
- 减法封闭，例如 $9 - 6 = 3$；
- 乘法封闭，例如 $3 \times 6 = 18$；
- 除法不封闭，例如 $6 \div 3 = 2$.

数集的封闭性举例

问题 1

所有奇数组成的数集，对于加、减、乘、除四种运算，哪些是封闭的？

问题 2

某个数的整倍数所组成的数集，对于加、减、乘、除四种运算，哪些是封闭的？

解答 1

所有奇数组成的数集

- 乘法封闭，例如 $3 \times 5 = 15$；
- 加法不封闭，例如 $3 + 5 = 8$；
- 减法不封闭，例如 $9 - 5 = 4$；
- 除法不封闭，例如 $3 \div 5 = \frac{3}{5}$.

解答 2

某个数的整倍数组成的数集（如所有 3 的倍数）

- 加法封闭，例如 $3 + 6 = 9$；
- 减法封闭，例如 $9 - 6 = 3$；
- 乘法封闭，例如 $3 \times 6 = 18$；
- 除法不封闭，例如 $6 \div 3 = 2$.

这两个数集都不是数域，因为它们对四种基本运算都不封闭.

例 1

所有形如 $a + b\sqrt{2}$ (a, b 为有理数) 的数构成的集合, 记为 $\mathbb{Q}(\sqrt{2})$, 是一个数域.

例 1

所有形如 $a+b\sqrt{2}$ (a, b 为有理数) 的数构成的集合，记为 $\mathbb{Q}(\sqrt{2})$，是一个数域.

证明 加法单位元 $0=0+0\sqrt{2}$ 和乘法单位元 $1=1+0\sqrt{2}$ 均在集合内.

设 $\alpha=a+b\sqrt{2}$ 和 $\beta=c+d\sqrt{2}$ 是 $\mathbb{Q}(\sqrt{2})$ 中的任意两个元素.

1. **加减与乘法封闭性**：
$$\alpha \pm \beta=(a \pm c)+(b \pm d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$
$$\alpha \cdot \beta=(ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

2. **除法封闭性**：若 $\alpha=a+b\sqrt{2} \neq 0$，则其有理数共轭 $a-b\sqrt{2}$ 也非零，且它们的乘积 $a^2-2b^2 \neq 0$ (因为 $\sqrt{2}$ 是无理数).
$$\frac{\beta}{\alpha}=\frac{c+d\sqrt{2}}{a+b\sqrt{2}}=\frac{(c+d\sqrt{2})(a-b\sqrt{2})}{(a+b\sqrt{2})(a-b\sqrt{2})}=\underbrace{\frac{ac-2bd}{a^2-2b^2}}_{\in\mathbb{Q}}+\underbrace{\frac{ad-bc}{a^2-2b^2}}_{\in\mathbb{Q}}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

因此，$\mathbb{Q}(\sqrt{2})$ 是一个数域. ∎

例 1

所有形如 $a+b\sqrt{2}$ (a, b 为有理数) 的数构成的集合，记为 $\mathbb{Q}(\sqrt{2})$，是一个数域.

思考：下列集合是否构成数域？

情况一：系数扩展为复数 $\mathbb{C}$

$$S_1 = \{a + b\sqrt{2} \mid a, b \in \mathbb{C}\}$$

情况二：系数限缩为整数 $\mathbb{Z}$

$$S_2 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

例 1

所有形如 $a+b\sqrt{2}$ (a, b 为有理数) 的数构成的集合，记为 $\mathbb{Q}(\sqrt{2})$，是一个数域.

思考：下列集合是否构成数域？

情况一：系数扩展为复数 $\mathbb{C}$

$$S_1=\{a+b\sqrt{2}\mid a, b\in\mathbb{C}\}$$

情况二：系数限缩为整数 $\mathbb{Z}$

$$S_2=\{a+b\sqrt{2}\mid a, b\in\mathbb{Z}\}$$

答案与解析

是数域

- 该集合 S_1 就是复数域 $\mathbb{C}$ 本身.
- 因为对于任意复数 $z\in\mathbb{C}$，总可以取 $a=z, b=0$ 来表示，所以 $S_1=\mathbb{C}$.

不是数域

- 该集合 S_2 对除法运算不封闭.
- **反例**：$2\in S_2$ (当 $a=2, b=0$ 时)，但它的乘法逆元 $\frac{1}{2}$ 无法写成 a, b 均为整数的形式.

性质

任何数域包含有理数域作为它的一部分.

性质

任何数域包含有理数域作为它的一部分.

证明　设 P 为一个数域.

- 由定义知 $1 \in P$,
- 又 P 对加法封闭知: $1+1=2, 1+2=3, \cdots$, P 包含所有自然数;
- 由 $0 \in P$ 及 P 对减法的封闭性知: P 包含所有负整数, 因而 P 包含所有整数;
- 任何一个有理数都可以表为两个整数的商, 由 P 对除法的封闭性知: P 包含所有有理数.
  即任何数域都包含有理数域作为它的一部分.

§2 一元多项式

多项式理论是高等代数的重要组成部分.

- 它不仅涵盖了初等代数中的基本内容, 一次多项式 $ax+b$, 二次多项式 x^2+ax+b 等,
- 更为高等代数中的核心概念与理论提供了坚实的基础.
- 多项式理论中的一些重要定理与方法, 在后续数学理论的学习以及实际问题的求解中具有广泛而深远的应用. 例如,
  - 在数学分析中, 著名的魏尔斯特拉斯逼近定理指出: 任意闭区间上的连续函数都可以用多项式函数一致逼近;
  - 在常微分方程中, 线性微分方程的求解往往依赖于其对应的特征多项式;
  - 在代数几何中, 多项式方程组的零点集（即解集）构成了该领域的基本研究对象;
  - 在理论计算机科学中, “多项式时间算法”是衡量算法效率的重要标准之一. . .

本章介绍一元多项式的基本理论.

一、一元多项式的有关概念

设 P 是一个数域，x 是未定元，n 为非负整数. 形式表达式

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

其中 $a_0, a_1, \ldots, a_n \in P$，称为系数在数域 P 中的一元多项式，简称为数域 P 上的一元多项式.

- 符号 x 可以是为未知数，也可以是其它待定事物.
- 习惯上记为 $f(x), g(x), \ldots$ 或 $f, g, \ldots$
- 上述形式表达式可写为 $f(x) = \sum_{i=0}^{n} a_i x^i$.
- 这里 $a_i x^i$ 称为 i 次项，a_i 称为 i 次项系数.

- 多项式相等 ——$f(x) = g(x) \Leftrightarrow$ 同次项的系数全相等（系数为零的项除外）
- 零多项式 ——系数全为 0 的多项式

- 若 $a_n \neq 0$, 则称 $a_n x^n$ 为 首项（或 最高次项）.
  若 $a_n = 1$, 则称 $f(x)$ 为 首一多项式.
- 多项式 $f(x)$ 的 次数 定义为它的最高次项对应的幂次, 记作 $\deg f(x)$.
- 零多项式不定义次数.
- $\dfrac{1}{x}$ 是多项式吗？

二、多项式的运算

设 $f(x), g(x)$ 为数域 P 上的一元多项式，不妨令

$$f(x)=\sum_{i=0}^{n} a_i x^i,\ g(x)=\sum_{j=0}^{m} b_j x^j$$

- **加法**：$f(x) \pm g(x)=\sum_{i=0}^{n}\left(a_i \pm b_i\right) x^i$，若 $n \geq m$
- **乘法**：

$$\begin{aligned} f(x)g(x) &= a_n b_m x^{n+m}+\left(a_n b_{m-1}+a_{n-1} b_m\right) x^{n+m-1}+\cdots+a_0 b_0 \\ &= \sum_{k=0}^{n+m}\left(a_0 b_k+a_1 b_{k-1}+\cdots+a_k b_0\right) x^k=\sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k \end{aligned}$$

由此可得：数域 P 上的多项式经过加、减、乘运算后，所得结果仍然是数域 P 上的多项式.

例 $f(x)=2x^2+3x-1, g(x)=x^3+2x^2-3x+2,$

例 $f(x) = 2x^2 + 3x - 1, g(x) = x^3 + 2x^2 - 3x + 2$, 则

例 $f(x)=2x^2+3x-1, g(x)=x^3+2x^2-3x+2$, 则

$$f(x)+g(x)=\left(2x^2+3x-1\right)+\left(x^3+2x^2-3x+2\right)=x^3+4x^2+1$$

$$f(x)-g(x)=\left(2x^2+3x-1\right)-\left(x^3+2x^2-3x+2\right)=-x^3+6x-3$$

$$\begin{aligned} f(x)g(x) &= \left(2x^2+3x-1\right)\left(x^3+2x^2-3x+2\right) \\ &= 2x^5+7x^4-x^3-7x^2+9x-2 \end{aligned}$$

三、多项式运算后的次数关系及次数定理

设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0,$$

且 $a_n \neq 0, b_m \neq 0$.

$\nVdash$. 对于多项式的和与差，当 $f(x) \pm g(x) \neq 0$ 时，运算后的次数关系为

$$\deg f(x) \pm g(x) \leq \max\{\deg f(x), \deg g(x)\}.$$

$\nvDash$. 对于多项式的乘法，若 $f(x) \neq 0$, $g(x) \neq 0$, 则 $f(x)g(x) \neq 0$, 并且

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

此外，乘积的首项系数等于因子首项系数的乘积，即 $a_n b_m x^{n+m}$ 是 $f(x)g(x)$ 的首项.

四、多项式的运算规律

设 $f(x), g(x), h(x)$ 为数域 P 上的一元多项式，则

(1) 加法交换律：

$$f(x)+g(x)=g(x)+f(x)$$

(2) 加法结合律：

$$(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$$

(3) 乘法交换律：

$$f(x)g(x)=g(x)f(x)$$

(4) 乘法结合律：

$$(f(x)g(x))h(x)=f(x)(g(x)h(x))$$

(5) 乘法对加法的分配律：

$$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$$

(6) 乘法消去律：若 $f(x)g(x)=f(x)h(x)$ 且 $f(x)\neq 0$，则 $g(x)=h(x)$.

(6) 乘法消去律：若 $f(x)g(x)=f(x)h(x)$ 且 $f(x)\neq 0$，则 $g(x)=h(x)$.

证明 因为 $f(x)g(x)=f(x)h(x)$，故由分配律可得 $f(x)[g(x)-h(x)]=0$.

由于 $f(x)\neq 0$，那么 $g(x)-h(x)=0$，即 $g(x)=h(x)$. ∎

从上述性质可以看出，多项式与整数有很多相似之处：

- 都有加法、减法和乘法三种运算，
- 加法和乘法也满足交换律、结合律和分配律等.

定义

数域 P 上的一元多项式的全体，称为**数域 P 上的一元多项式环**，记作 $P[x]$，P 称为 $P[x]$ 的**系数域**.

§3 整除的概念

与整数的运算一样, 我们要讨论多项式的除法问题.

考虑这一问题是为了进一步讨论多项式的因式分解.

自本节开始, 我们总是在某一固定数域 P 上讨论多项式.

- 在多项式理论中, 两个多项式可以作加、减、乘等运算, 是否有除法?

§3 整除的概念

与整数的运算一样，我们要讨论多项式的除法问题.

考虑这一问题是为了进一步讨论多项式的因式分解.

自本节开始，我们总是在某一固定数域 P 上讨论多项式.

- 在多项式理论中，两个多项式可以作加、减、乘等运算，是否有除法?

除法运算并不是普遍可以作的，如 $\frac{x+1}{x}$ 不是多项式，即 $\frac{x+1}{x} \notin P[x]$.

回忆在整数中，除法也并非处处可行.

具体来说，任意两个整数 a, b 不一定有 b 整除 a，但在整数中当 $b \neq 0$ 时，存在唯一的整数 q, r，使得

$$a = bq + r, \quad 0 \leq r < |b|.$$

- 在多项式理论中，两个多项式是否有带余除法?

回忆在整数中，除法也并非处处可行.

具体来说，任意两个整数 a, b 不一定有 b 整除 a，但在整数中当 $b \neq 0$ 时，存在唯一的整数 q, r，使得

$$a = bq + r, \quad 0 \leq r < |b|.$$

- 在多项式理论中，两个多项式是否有带余除法?

带余除法

对于数域 P 上的任意两个多项式 $f(x)$ 与 $g(x)$，只要 $g(x) \neq 0$，一定有 $P[x]$ 中的多项式 $q(x)$，$r(x)$ 存在，使得

$$f(x) = q(x)g(x) + r(x) \qquad (1)$$

成立，其中 $\deg r(x) < \deg g(x)$ 或者 $r(x) = 0$，并且这样的 $q(x)$，$r(x)$ 是唯一的.

注

(1) 带余除法 *(1)* 中的

- $q(x)$ 称为 $g(x)$ 除 $f(x)$ 所得的商式，
- $r(x)$ 称为 $g(x)$ 除 $f(x)$ 所得的余式.

(2) 此法实际上是“首项除首项”的方法.

证明　(存在性) 若 $f(x)=0$, 取 $q(x)=r(x)=0$ 即可.

以下设 $f(x)\neq 0$. $\deg f(x))=n$, $\deg g(x)=m$.

对 $f(x)$ 的次数 n 作数学归纳法.

当 $n<m$ 时, 取 $q(x)=0, r(x)=f(x)$, 有 $f(x)=q(x)g(x)+r(x)$, 结论成立.

当 $n\geq m$ 时, 假设次数小于 n 时结论成立.

以下证明次数为 n 时结论也成立.

设 $f(x), g(x)$ 的首项分别为 $a_n x^n$ 及 $b_m x^m$. 令

$$f_1(x)=f(x)-b_m^{-1}a_n x^{n-m}g(x)$$

注意到 $b_m^{-1}a_n x^{n-m}g(x)$ 与 $f(x)$ 有相同的首项, 可知 $\deg f_1(x)<n$ 或 $f_1(x)=0$.

对于后者, 取 $q(x)=b_m^{-1}a_n x^{n-m}$, $r(x)=0$.

对于前者, 由归纳假设及 (1), 对于 $f_1(x), g(x)$, 必有 $q_1(x), r_1(x)$ 存在, 使得

$$f_1(x) = q_1(x)g(x) + r_1(x),$$

其中 $\deg r_1(x) < \deg g(x)$ 或者 $r_1(x) = 0$.

于是

$$f(x) = f_1(x) + b_m^{-1}a_nx^{n-m}g(x) = [q_1(x) + b_m^{-1}a_nx^{n-m}]g(x) + r_1(x),$$

故可取 $q(x) = q_1(x) + b_m^{-1}a_nx^{n-m}$, $r(x) = r_1(x)$, 就能使得

$$f(x) = q(x)g(x) + r(x),$$

其中 $\deg r(x) < \deg g(x)$ 或 $r(x) = 0$.

由第二数学归纳法原理, 存在性得证.

(唯一性) 若还有 $q'(x), r'(x) \in P[x]$, 使

$$f(x) = q'(x)g(x) + r'(x),$$

其中 $\deg r'(x) < \deg g(x)$ 或 $r'(x) = 0$.

则

$$q(x)g(x) + r(x) = q'(x)g(x) + r'(x),$$

即

$$\left(q(x) - q'(x)\right) g(x) = r'(x) - r(x).$$

（反证）假设 $q(x) \neq q'(x)$. 由假设 $g(x) \neq 0$ 可知 $r'(x) - r(x) \neq 0$ 且

$$\deg\left(q(x) - q'(x)\right) + \deg g(x) = \deg\left(r'(x) - r(x)\right),$$

但与 $\deg g(x) > \deg\left(r'(x) - r(x)\right)$ 矛盾.

因此, $q(x) = q'(x), r'(x) = r(x)$. ∎

例 1

设 $f(x) = 3x^3 + 4x^2 - 5x + 6$, $g(x) = x^2 - 3x + 1$, 求 $g(x)$ 除 $f(x)$ 所得的商式和余式.

例 1

设 $f(x)=3x^3+4x^2-5x+6$, $g(x)=x^2-3x+1$, 求 $g(x)$ 除 $f(x)$ 所得的商式和余式.

解

$$
\begin{array}{r|rrrr|l}
x^2-3x+1 & 3x^3 & +4x^2 & -5x & +6 & 3x+13 \\
 & 3x^3 & -9x^2 & +3x & & \\
\hline
 & & 13x^2 & -8x & +6 & \\
 & & 13x^2 & -39x & +13 & \\
\hline
 & & & 31x & -7 &
\end{array}
$$

$$f(x)=q(x)g(x)+r(x)$$

- 回顾正整数的带余除法, 我们只需会计算, 而很少有人会怀疑计算过程的合理性, 也并不知道或者没有想过为什么计算结果一定是唯一的!
- 这些理论性的问题在数学研究中是必不可少的, 我们经常会遇到一些研究对象的存在唯一性问题 (如最大公因式), 需要给出严格的理论证明从而使下一步的研究建立在一个坚实的基础上.

二、整除的概念

定义 (整除)

- 设 $f(x), g(x) \in P[x]$，如果存在多项式 $h(x) \in P[x]$，使
$$f(x) = h(x)g(x)$$
则称 $g(x)$ 整除 $f(x)$，记为 $g(x) \mid f(x)$.
- 当 $g(x) \mid f(x)$ 时，称 $g(x)$ 为 $f(x)$ 的因式，$f(x)$ 为 $g(x)$ 的倍式.
- 当 $g(x)$ 不能整除 $f(x)$ 时，记为 $g(x) \nmid f(x)$.

注

(1) 任意多项式 $f(x)$ 能整除其自身及零多项式.

(2) 若 $0 \mid f(x)$，则必有 $f(x) = 0$.

(3) 零次多项式 $a\ (\neq 0)$ 能整除任意多项式 $f(x)$，这是因为 $f(x) = a(a^{-1}f(x))$.

(4) 当 $g(x) \neq 0$ 且 $g(x) \mid f(x)$ 时，$g(x)$ 除 $f(x)$ 所得商有时可记为
$$\frac{f(x)}{g(x)}.$$

定理 1 (整除的判别)

设 $f(x), g(x) \in P[x]$, $g(x) \neq 0$, 则 $g(x) \mid f(x) \Leftrightarrow g(x)$ 除 $f(x)$ 的余式为零.

定理 1 (整除的判别)

设 $f(x), g(x) \in P[x]$, $g(x) \neq 0$, 则 $g(x) \mid f(x) \Leftrightarrow g(x)$ 除 $f(x)$ 的余式为零.

证明 $\Leftarrow$ 若余式 $r(x) = 0$, 则

$$f(x) = q(x)g(x),$$

即 $g(x) \mid f(x)$.

$\Rightarrow$ 若 $g(x) \mid f(x)$, 则

$$f(x) = q(x)g(x) = q(x)g(x) + 0$$

即 $r(x) = 0$. ∎

三、整除的性质

性质 1

$f(x) \mid g(x)$ 且 $g(x) \mid f(x) \Leftrightarrow f(x) = c\, g(x)$, 其中 c 为数域 P 中的一个非零常数.

由此可得:

$f(x)$ 与其任一非零常数倍 $cf(x)$ 有完全相同的因式及倍式, 故在讨论中必要时可互相替代.

性质 2

若 $f(x) \mid g(x), g(x) \mid h(x)$, 则 $f(x) \mid h(x)$. (传递性)

性质 3

如果 $f(x) \mid g_i(x), i=1,2,\cdots,r$ ，那么

$$f(x) \mid \left(u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_r(x)g_r(x)\right),$$

其中 $u_i(x)$ 是数域 P 上任意的多项式.

性质 3

如果 $f(x) \mid g_i(x), i = 1, 2, \cdots, r$，那么

$$f(x) \mid (u_1(x)g_1(x) + u_2(x)g_2(x) + \cdots + u_r(x)g_r(x)),$$

其中 $u_i(x)$ 是数域 P 上任意的多项式.

证明 由 $g_i(x) = h_i(x)f(x), i = 1, 2, \cdots, r$，即得

$$\begin{aligned} & u_1(x)g_1(x) + u_2(x)g_2(x) + \cdots + u_r(x)g_r(x) \\ = & (u_1(x)h_1(x) + u_2(x)h_2(x) + \cdots + u_r(x)h_r(x)) f(x). \end{aligned}$$

∎

通常，$u_1(x)g_1(x) + u_2(x)g_2(x) + \cdots + u_r(x)g_r(x)$ 称为多项式 $g_1(x), g_2(x), \cdots, g_r(x)$ 的一个组合.

由于我们会考虑不同的数域，而一些数域之间有包含关系，因此，一些多项式可以看作不同数域上的多项式，比如有理多项式可以看作任意其他数域上的多项式.

那么自然就有一个问题：我们之前以及之后考虑的很多问题，如整除、带余除法以及后文的最大公因式、因式分解等是否与数域有关？这是我们随时需要关注的.

现在，从带余除法的过程可以得到如下命题.

性质 4：两个多项式的整除关系在数域的扩大下保持不变

设 $P, \overline{P}$ 都是数域，且 $P \subseteq \overline{P}$. 又设 $f(x), g(x) \in P[x] \subseteq \overline{P}[x]$, $g(x) \neq 0$, 则作为 $P[x]$ 和 $\overline{P}[x]$ 中的多项式，$g(x)$ 除 $f(x)$ 的商与余式是一样的.

特别地，在 $P|x|$ 中 $g(x) \mid f(x) \Leftrightarrow$ 在 $\overline{P}[x]$ 中 $g(x) \mid f(x)$.

§4 最大公因式

- 对于多项式的研究与整数的研究是类似的，适当进行比较是有益的.
- 有兴趣的同学不妨尝试一下补充整数中类似结论的理论证明.
- 这样的类比工作有助于找到一些研究对象的共性，从而在统一的层面上理解它们并予以推广.

定义

设 $f(x), g(x) \in P[x]$, 若有 $d(x) \in P[x]$, 使 $d(x)|f(x), d(x)|g(x)$,
则称 $d(x)$ 为 $f(x)$ 与 $g(x)$ 的一个**公因式**.

由于任意两个多项式总有公因式 (非 0 常数), 因此公因式中占有重要地位的 – 最大公因式.

定义

设 $f(x), g(x) \in P[x]$. 若有 $d(x) \in P[x]$ 满足:

- $d(x)$ 是 $f(x), g(x)$ 的公因式;
- $f(x), g(x)$ 的公因式全是 $d(x)$ 的因式.

则称 $d(x)$ 为 $f(x)$ 与 $g(x)$ 的一个最大公因式.

由于任意两个多项式总有公因式 (非 0 常数), 因此公因式中占有重要地位的 – 最大公因式.

定义

设 $f(x), g(x) \in P[x]$. 若有 $d(x) \in P[x]$ 满足:

- $d(x)$ 是 $f(x), g(x)$ 的公因式;
- $f(x), g(x)$ 的公因式全是 $d(x)$ 的因式.

则称 $d(x)$ 为 $f(x)$ 与 $g(x)$ 的一个最大公因式.

- 若将 "最大公因式" 定义为 $f(x), g(x)$ 中次数最大的公因式, 则其存在性是显然的, 但唯一性并不直观, 并且它与其他因式之间的关系仍需进一步探讨.
- 事实上, 这两种定义是等价的 (思考题).

规定 两个零多项式的最大公因式是零多项式.

性质 1 ——整除情形

若 $g(x) \mid f(x)$, 则 $g(x)$ 即为 $f(x)$ 与 $g(x)$ 的一个最大公因式.

- 任意多项式 $f(x)$ 是 $f(x)$ 与 0 的一个最大公因式.
- 任意多项式 $f(x)$ 与 1 的最大公因式为零次多项式.

性质 2 ——带余除法（核心）

设 $f(x), g(x) \in P[x]$. 如果等式

$$f(x) = q(x)g(x) + r(x), \qquad (*)$$

成立, 则

- $f(x), g(x)$ 和 $g(x), r(x)$ 有相同的公因式.
- 若 $d(x)$ 是 $g(x), r(x)$ 的一个最大公因式, 则 $d(x)$ 也是 $f(x), g(x)$ 的最大公因式.

证明 由 $(*)$ 知, $f(x)$ 是 $g(x)$ 与 $r(x)$ 的一个组合, 故若 $\varphi(x)|g(x), \varphi(x)|r(x)$, 必有 $\varphi(x) \mid f(x)$, 此即 $g(x), r(x)$ 的公因式都是 $f(x), g(x)$ 的公因式; 又由 $(*)$, 有 $r(x) = f(x) - q(x)g(x)$

故若 $\varphi(x)|f(x), \varphi(x)|g(x)$, 必有 $\varphi(x)$ 整除 $f(x)$ 与 $g(x)$ 的组合 $r(x)$,

此即 $f(x), g(x)$ 的公因式都是 $g(x), r(x)$ 的公因式.

综上所述, $f(x), g(x)$ 和 $g(x), r(x)$ 有相同的公因式. ∎

定理 2 (最大公因式存在性定理)

对于 $P[x]$ 中的两个多项式 $f(x), g(x)$，在 $P[x]$ 中存在一个最大公因式 $d(x)$ 且存在 $u(x), v(x) \in P[x]$ 使

$$d(x) = u(x)f(x) + v(x)g(x) \text{ (贝祖等式)}$$

说明

等式 $d(x) = u(x)f(x) + v(x)g(x)$ 成立，$d(x)$ 未必就是 $f(x)$ 与 $g(x)$ 的最大公因式.
例如 $f(x) = x^2 + 1, g(x) = x, u(x) = x, v(x) = x + 1$，$d(x) = 2x\left(x^2 + 1\right)$. 有

$$d(x) = u(x)f(x) + v(x)g(x)$$

但 $f(x)$ 与 $g(x)$ 无公因式，故 $d(x)$ 不是 $f(x)$ 与 $g(x)$ 的最大公因式.

证明 (存在性) (i) 如果 $f(x), g(x)$ 有一个为零多项式, 比如 $g(x) = 0$, 则 $f(x)$ 就是 $f(x), g(x)$ 一个最大公因式, 即 $d(x) = f(x)$, 且

$$f(x) = 1 \cdot f(x) + 1 \cdot 0 = 1 \cdot f(x) + 1 \cdot g(x).$$

(ii) 一般情形：不妨设 $g(x) \neq 0$. 由带余除法, 用 $g(x)$ 除 $f(x)$, 得到商 $q_1(x)$, 余式 $r_1(x)$; 即

$$f(x) = q_1(x)g(x) + r_1(x)$$

若 $r_1(x) = 0$, 则 $g(x)$ 为 $f(x), g(x)$ 的一个最大公因式;

若 $r_1(x) \neq 0$, 再用 $r_1(x)$ 除 $g(x)$, 得到商 $q_2(x)$, 余式 $r_2(x)$;

又若 $r_2(x) \neq 0$, 就用 $r_2(x)$ 除 $r_1(x)$, 得出商 $q_3(x)$, 余式 $r_3(x)$;

如此辗转相除下去, 则所得余式的次数不断降低, 即

$$\deg g(x) > \deg r_1(x) > \deg r_2(x) \quad > \cdots ..$$

经有限次之后, 必有余式为零 (因次数有限).

$$
\begin{aligned}
f(x) &= q_1(x)g(x) + r_1(x) \\
g(x) &= q_2(x)r_1(x) + r_2(x) \\
&\cdots\cdots \\
r_{i-2}(x) &= q_i(x)r_{i-1}(x) + r_i(x) \\
&\cdots\cdots \\
r_{s-3}(x) &= q_{s-1}(x)r_{s-2}(x) + r_{s-1}(x) \\
r_{s-2}(x) &= q_s(x)r_{s-1}(x) + r_s(x) \\
r_{s-1}(x) &= q_{s+1}(x)r_s(x) + 0
\end{aligned}
$$

$$
\begin{aligned}
f(x) &= q_1(x)g(x) + r_1(x) \\
g(x) &= q_2(x)r_1(x) + r_2(x) \\
&\cdots\cdots \\
r_{i-2}(x) &= q_i(x)r_{i-1}(x) + r_i(x) \\
&\cdots\cdots \\
r_{s-3}(x) &= q_{s-1}(x)r_{s-2}(x) + r_{s-1}(x) \\
r_{s-2}(x) &= q_s(x)r_{s-1}(x) + r_s(x) \\
r_{s-1}(x) &= q_{s+1}(x)r_s(x) + 0
\end{aligned}
$$

由最后一个等式可知, $r_s(x)$ **是** $r_s(x)$ **与** $r_{s-1}(x)$ **的一个最大公因式**.

由引理知, $r_s(x)$ **也是** $r_{s-1}(x)$ **与** $r_{s-2}(x)$ **的一个最大公因式**.

以此逐步上推 $\cdots\cdots$

$r_s(x)$ **就是** $f(x)$ **与** $g(x)$ **的一个最大公因式**.

为得到定理结论中的等式, 由上面的倒数第二个等式, 我们有

$$r_s(x) = r_{s-2}(x) - q_s(x) r_{s-1}(x)$$

而由倒数第三式, 有

$$r_{s-1}(x) = r_{s-3}(x) - q_{s-1}(x) r_{s-2}(x)$$

带入上式, 消去 $r_{s-1}(x)$, 得到

$$r_s(x) = (1 + q_s(x) q_{s-1}(x)) \, r_{s-2}(x) - q_s(x) r_{s-3}(x)$$

以同样的方法逐个消去 $r_{s-2}(x), \cdots\cdots, r_1(x)$, 并项后, 得到

$$r_s(x) = u(x) f(x) + v(x) g(x)$$

唯一性：设 $d_1(x), d_2(x)$ 均为 $f(x)$ 与 $g(x)$ 的一个最大公因式，下证 $d_1(x)$ 与 $d_2(x)$ 之间只相差一个非零常因子.

因为 $d_1(x)$ 与 $d_2(x)$ 都是 $f(x), g(x)$ 的最大公因式，故有 $d_2(x) \mid d_1(x)$ 且 $d_1(x) \mid d_2(x)$

从而 $d_1(x) = cd_2(x), c \neq 0$. ∎

说明

- 定理中求最大公因式的方法称为**辗转相除法**或**欧几里得算法**(Euclidean Algorithm).
- 最大公因式在相差一个非零常数的意义下是唯一确定的.
- $(f(x), g(x))$ 是指 $f(x)$ 与 $g(x)$ 首项系数为 1 的最大公因式.

例 1

$$f(x) = x^4 + 3x^3 - x^2 - 4x - 3$$
$$g(x) = 3x^3 + 10x^2 + 2x - 3$$

求 $(f(x), g(x))$, **并求** $u(x), v(x)$ **使**

$$(f(x), g(x)) = u(x)f(x) + v(x)g(x)$$

例 1

$$f(x) = x^4 + 3x^3 - x^2 - 4x - 3$$
$$g(x) = 3x^3 + 10x^2 + 2x - 3$$

求 $(f(x), g(x))$, 并求 $u(x), v(x)$ 使

$$(f(x), g(x)) = u(x)f(x) + v(x)g(x)$$

辗转相除法可按下面的格式来作:

$$
\begin{array}{r|r|l}
3x^3 + 10x^2 + 2x - 3 & x^4 + 3x^3 - x^2 - 4x - 3 & \frac{1}{3}x - \frac{1}{9} \\
 & x^4 + \frac{10}{3}x^3 + \frac{2}{3}x^2 - x & = q_1(x) \\
\hline
 & -\frac{1}{3}x^3 - \frac{5}{3}x^2 - 3x - 3 & \\
 & -\frac{1}{3}x^3 - \frac{10}{9}x^2 - \frac{2}{9}x + \frac{1}{3} & \\
\hline
 & r_1(x) = -\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3} &
\end{array}
$$

$$f(x) = q_1(x)g(x) + r_1(x)$$

$-\frac{27}{5}x+9$	$3x^3+10x^2+2x-3$	$x^4+3x^3-x^2-4x-3$	$\frac{1}{3}x-\frac{1}{9}$
$=q_2(x)$	$3x^3+15x^2+18x$	$x^4+\frac{10}{3}x^3+\frac{2}{3}x^2-x$	$=q_1(x)$
	$-5x^2-16x-3$	$-\frac{1}{3}x^3-\frac{5}{3}x^2-3x-3$	
	$-5x^2-25x-30$	$-\frac{1}{3}x^3-\frac{10}{9}x^2-\frac{2}{9}x+\frac{1}{3}$	
	$r_2(x)=9x+27$	$r_1(x)=-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}$	

$$f(x)=q_1(x)g(x)+r_1(x)$$

$$g(x)=q_2(x)r_1(x)+r_2(x)$$

$$
\begin{array}{r|r|r|l}
-\frac{27}{5}x+9 & 3x^3+10x^2+2x-3 & x^4+3x^3-x^2-4x-3 & \frac{1}{3}x-\frac{1}{9} \\
=q_2(x) & 3x^3+15x^2+18x & x^4+\frac{10}{3}x^3+\frac{2}{3}x^2-x & =q_1(x) \\
\cline{2-3}
 & -5x^2-16x-3 & -\frac{1}{3}x^3-\frac{5}{3}x^2-3x-3 & \\
 & -5x^2-25x-30 & -\frac{1}{3}x^3-\frac{10}{9}x^2-\frac{2}{9}x+\frac{1}{3} & \\
\cline{2-3}
 & r_2(x)=9x+27 & r_1(x)=-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3} & -\frac{5}{81}x-\frac{10}{81} \\
 & & -\frac{5}{9}x^2-\frac{5}{3}x & =q_3(x) \\
\cline{3-3}
 & & -\frac{10}{9}x-\frac{10}{3} & \\
 & & -\frac{10}{9}x-\frac{10}{3} & \\
\cline{3-3}
 & & 0 &
\end{array}
$$

$$f(x) = q_1(x)g(x) + r_1(x)$$

$$g(x) = q_2(x)r_1(x) + r_2(x)$$

$$r_1(x) = q_3(x)r_2(x)$$

因此

$$(f(x), g(x)) = \frac{1}{9} r_2(x) = x + 3$$

由

$$\begin{aligned} f(x) &= q_1(x) g(x) + r_1(x) \\ g(x) &= q_2(x) r_1(x) + r_2(x) \\ r_1(x) &= q_3(x) r_2(x) \end{aligned}$$

可知

$$\begin{aligned} r_2(x) &= g(x) - q_2(x) r_1(x) \\ &= g(x) - q_2(x) \left(f(x) - q_1(x) g(x)\right) \\ &= -q_2(x) f(x) + \left(1 + q_1(x) q_2(x)\right) g(x) \\ &= \left(\frac{27}{5} x - 9\right) f(x) + \left(-\frac{9}{5} x^2 + \frac{18}{5} x\right) g(x) \end{aligned}$$

于是，令

$$\begin{aligned} u(x) &= -\frac{1}{9} q_2(x) = \frac{3}{5} x - 1, \\ v(x) &= \frac{1}{9} \left(1 + q_1(x) q_2(x)\right) = -\frac{1}{5} x^2 + \frac{2}{5} x, \end{aligned}$$

就有

$$(f(x), g(x)) = u(x) f(x) + v(x) g(x).$$

二、互素多项式

已知零次多项式是任意两个多项式的公因式.

现在讨论两个多项式 $f(x)$ 与 $g(x)$ 的公因式只有零次多项式时, $f(x)$ 与 $g(x)$ 的关系.

定义 (互素)

设 $f(x)$ 与 $g(x)$ 是数域 P 上两个多项式. 如果 $(f(x), g(x)) = 1$, 则称 $f(x)$ 与 $g(x)$ 互素.

互素的情况非常普遍且重要.

定理 3 (多项式互素的判定定理)

$F[x]$ 中两个多项式 $f(x)$ 与 $g(x)$ 互素 $\Leftrightarrow$ 存在 $u(x), v(x)$, 使得

$$u(x)f(x) + v(x)g(x) = 1.$$

定理 3 (多项式互素的判定定理)

$F[x]$ 中两个多项式 $f(x)$ 与 $g(x)$ 互素 $\Leftrightarrow$ 存在 $u(x), v(x)$, 使得

$$u(x)f(x) + v(x)g(x) = 1.$$

证明 $\Rightarrow$ 因为 $f(x)$ 与 $g(x)$ 互素, 即 $(f(x), g(x)) = 1$, 故由定理 3 得, 存在 $u(x), v(x)$, 使得

$$u(x)f(x) + v(x)g(x) = 1.$$

$\Leftarrow$ 因为 1 是 $f(x), g(x)$ 的一个公因式, 且 $u(x)f(x) + v(x)g(x) = 1$,

故对于任意的 $h(x)$, 只要 $h(x) \mid f(x), h(x) \mid g(x)$, 就可得出 $h(x) \mid 1$, 那么 $(f(x), g(x)) = 1$, 亦即 $f(x)$ 与 $g(x)$ 互素. ∎

互素的条件就转化为易于操作的等式, 为我们处理问题提供了方便.

例 2

判断 $f(x) = x^3 + x^2 + 2x + 2$ 与 $g(x) = x^2 - 2x + 2$ 是否互素.

例 2

判断 $f(x)=x^3+x^2+2x+2$ 与 $g(x)=x^2-2x+2$ 是否互素.

解 因为

$$f(x)=(x+3)g(x)+6x-4,$$
$$g(x)=(\frac{1}{6}x-\frac{2}{9})(6x-4)+\frac{10}{9},$$

所以 $(f(x),g(x))=1$.

定理 4

如果 $(f(x), g(x)) = 1$, 且 $f(x) \mid g(x)h(x)$, 那么

$$f(x) \mid h(x)$$

三、多项式互素的性质

定理 4

如果 $(f(x), g(x)) = 1$，且 $f(x) \mid g(x)h(x)$，那么

$$f(x) \mid h(x).$$

定理 4

如果 $(f(x), g(x)) = 1$ ，且 $f(x) \mid g(x)h(x)$ ，那么

$$f(x) \mid h(x).$$

证明 由 $(f(x), g(x)) = 1$ 可知，有 $u(x), v(x)$ 使

$$u(x)f(x) + v(x)g(x) = 1$$

等式两边乘 $h(x)$ ，得

$$u(x)f(x)h(x) + v(x)g(x)h(x) = h(x)$$

因为 $f(x) \mid g(x)h(x)$ ，所以 $f(x)$ 整除等式左端，从而

$$f(x) \mid h(x).$$

推论

如果 $f_1(x)\,|g(x), f_2(x)|\,g(x)$ **，且** $(f_1(x), f_2(x)) = 1$ **，那么**

$$f_1(x)f_2(x) \mid g(x)$$

推论

如果 $f_1(x)\,|g(x), f_2(x)|\,g(x)$，且 $(f_1(x), f_2(x)) = 1$，那么

$$f_1(x)f_2(x) \mid g(x)$$

证明 由 $f_1(x) \mid g(x)$ 有

$$g(x) = f_1(x)h_1(x).$$

因为 $f_2(x) \mid f_1(x)h_1(x)$, 且 $(f_1(x), f_2(x)) = 1$，所以根据定理 4, 有 $f_2(x) \mid h_1(x)$，即

$$h_1(x) = f_2(x)h_2(x)$$

代人上式即得

$$g(x) = f_1(x)f_2(x)h_2(x)$$

这就是说,

$$f_1(x)f_2(x) \mid g(x).$$

简而言之, 辗转相除法就是持续使用带余除法.

而带余除法的过程与数域无关, 因此辗转相除法的过程也与数域无关.

于是我们有

性质

设 $f(x), g(x) \in \mathbb{F}[x] \subseteq \overline{\mathbb{F}}[x]$, 则 $f(x)$ 与 $g(x)$ 在 $\mathbb{F}[x]$ 和 $\overline{\mathbb{F}}[x]$ 中的最大公因式相等.

说明

需要注意的是最大公因式与数域无关, 并不意味着公因式也与数域无关.
例如, x^2+1 与 $(x^2+1)^2$ 的最大公因式是 x^2+1 ,
但 $x+\sqrt{-1}$ 是它们在复数域上的公因式, 而不是它们在有理数域上的公因式.

多个多项式的最大公因式

定义

如果多项式 $d(x)$ 满足以下两条:

(1) $d(x) \mid f_i(x), i = 1, 2, \cdots, s,$

(2) 若 $\varphi(x) \mid f_i(x), i = 1, 2, \cdots, s,$ 则 $\varphi(x) \mid d(x),$

那么称 $d(x)$ 为 $f_1(x), f_2(x), \cdots, f_s(x)$ 的一个最大公因式.

设 $d_0(x)$ 为 $f_1(x), f_2(x), \cdots, f_{s-1}(x)$ 的一个最大公因式,

则 $(d_0(x), f_s(x))$ 即为 $f_1(x)$, $f_2(x)$, $\cdots$, $f_{s-1}(x)$, $f_s(x)$ 的最大公因式,

亦即可逐次利用辗转相除法来求出多个多项式的最大公因式. 由上所述,

性质

任意 s $(s \geq 2)$ 个多项式的最大公因式必定存在, 且能表示成该 s 个多项式的组合,

即存在 $u_1(x), u_2(x), \cdots, u_s(x)$, 使得 $\sum_{i=1}^{s} u_i(x) f_i(x) = d(x)$.

定义

若 $(f_1(x), f_2(x), \cdots, f_s(x)) = 1$，则称 $f_1(x), f_2(x), \cdots, f_s(x)$ 互素.

性质

$f_1(x), f_2(x), \cdots, f_s(x)$ 互素 $\Leftrightarrow$ 存在 $u_1(x), u_2(x), \cdots, u_s(x)$，使得

$$\sum_{i=1}^{s} u_i(x) f_i(x) = 1.$$

多个多项式互素时，其中的多项式未必两两互素．如下面的三个多项式：

$$f_1(x) = x^2 + 3x + 2 = (x+2)(x+1),$$

$$f_2(x) = x^2 - x - 2 = (x-2)(x+1),$$

$$f_3(x) = x^2 - 4 = (x-2)(x+2).$$

最小公倍式

定义

多项式 $m(x)$ 称为多项式 $f(x), g(x)$ 的一个**最小公倍式**, 如果
(1) $f(x)|m(x), g(x)|m(x)$,
(2) $f(x), g(x)$ 的任一公倍式都是 $m(x)$ 的倍式.

我们以 $[f(x), g(x)]$ 表示首项系数是 1 的那个最小公倍式.

最小公倍式与最大公因式密切相关.

性质

如果 $f(x), g(x)$ 的首项系数都是 1, 那么 $[f(x), g(x)] = \frac{f(x)g(x)}{(f(x),g(x))}$. (补充题)

§5 因式分解定理

多项式理论中的一个重要问题是因式分解：将多项式表示为不可再分的因式的乘积.

因式分解不仅是代数运算的基础，也是研究多项式结构的重要工具.

在中学阶段，我们已掌握一些简单的因式分解方法，例如提公因式、平方差公式等.

但对于高次多项式，是否可以进一步分解，取决于其系数所在的数域 P. 例如：

$$\begin{aligned} x^4-4 &\overset{\mathbb{Q}}{=} (x^2-2)(x^2+2) && \text{（有理数域中）} \\ &\overset{\mathbb{R}}{=} (x-\sqrt{2})(x+\sqrt{2})(x^2+2) && \text{（实数域中）} \\ &\overset{\mathbb{C}}{=} (x-\sqrt{2})(x+\sqrt{2})(x+\sqrt{2}i)(x-\sqrt{2}i) && \text{（复数域中）} \end{aligned}$$

由此可见：

- 因式分解的结果依赖于系数所在的数域；
- “不可再分”的含义必须明确系数域后才能确定；
- 理解数域的作用，有助于更深入地研究多项式结构与代数性质.

一、不可约多项式

在数学发展史中，一个常用的思想方法是通过这些研究对象的相似性来推广已知的理论.

正如前文所述，多项式和整数有很多类似之处，正整数由素数、合数和 1 组成，

由算术基本定理每个大于 1 的正整数都可以唯一分解为素数的乘积 (如何证明?).

那么多项式理论中是否也有类似的概念和结论呢?

一、不可约多项式

在数学发展史中，一个常用的思想方法是通过这些研究对象的相似性来推广已知的理论.

正如前文所述，多项式和整数有很多类似之处，正整数由素数、合数和 1 组成，

由算术基本定理每个大于 1 的正整数都可以唯一分解为素数的乘积 (如何证明?).

那么多项式理论中是否也有类似的概念和结论呢?

类似于素数的概念，我们有

定义

- 数域 P 上一个次数 ≥ 1 的多项式 $p(x)$ 称为 P 上的一个**不可约多项式**，如果它不能表示成数域 P 上的两个次数均比它低的多项式的乘积;
- 否则，即

$$p(x) = p_1(x)p_2(x),$$

其中 $\deg p_i(x) < \deg p(x), p_i(x) \in P[x], i = 1, 2$, 则称 $p(x)$ 为数域 P 上的一个**可约多项式**.

例 1

在有理数域 $\mathbb{Q}$ 上 x^2-2 可约, 在实数域 $\mathbb{R}$ 上不可约.

注

(1) 多项式是否可约与所讨论的数域 P 有关.

(2) 在任意数域上一次多项式总是不可约的, 如 $x, x+c$ 等.

(3) 零次多项式与 0 多项式不定义可约与不可约.

(4) 不可约多项式的因式只有两种:

- 非零常数,
- 自身的非零常数倍,

这两种因式称为平凡因式, 即不可约多项式只有平凡因式, 反之, 亦然.

下面讨论不可约多项式的性质.

性质 1

设 $p(x)$ 为数域 P 上的一个不可约多项式, 则 $p(x)$ 与任意多项式 $f(x) \in P[x]$ 只有两种关系:

$$p(x) \mid f(x) \text{ 或者 } (p(x), f(x)) = 1.$$

下面讨论不可约多项式的性质.

性质 1

设 $p(x)$ 为数域 P 上的一个不可约多项式, 则 $p(x)$ 与任意多项式 $f(x)\in P[x]$ 只有两种关系:

$$p(x)\mid f(x) \text{ 或者 } (p(x),f(x))=1.$$

定理 5

若不可约多项式 $p(x)\mid f(x)g(x)$, 则 $p(x)\mid f(x)$ 或者 $p(x)\mid g(x)$.

推论

若不可约多项式 $p(x)\mid f_1(x)f_2(x)\cdots f_s(x)$, 则 $p(x)$ 必能整除 $f_1(x), f_2(x), \cdots, f_s(x)$ 中的某一个.

二、因式分解定理

因式分解及唯一性定理

- 数域 P 上任意一个次数 ≥ 1 的多项式 $f(x)$ 都可以唯一地分解成数域 P 上一些不可约多项式的乘积(也包括只有一个不可约因式的情况).
- 所谓唯一性是说，如果有两个分解式

$$f(x) = p_1(x) \cdots p_s(x) = q_1(x) \cdots q_t(x),$$

那么必有 $s = t$，并且适当排列因式的次序后，有

$$p_i(x) = c_i q_i(x), i = 1, 2, \cdots, s,$$

其中 $c_i (i = 1, 2, \cdots, s)$ 是 P 中一些非零常数.

此定理在理论上是非常重要的，它是代数基本定理的基础.

证明 先证明分解式的存在性. 对 $\deg f(x)$ 用第二数学归纳法.

若 $\deg(f(x)) = 1$, 则 $f(x)$ 为不可约的, 故 $f(x) = f(x)$ 即为所求.

假设结论对于次数 $< n$ 的多项式是成立的, 下证 $\deg(f(x)) = n$ 时结论也成立:

若 $f(x)$ 不可约, 则 $f(x) = f(x)$, 结论成立.

若 $f(x)$ 可约, 则 $f(x)$ 可以分解成两个次数都比它低的多项式的乘积, 即

$$f(x) = f_1(x)f_2(x), \deg(f_i(x)) < n, i = 1, 2,$$

由归纳假设, $f_1(x), f_2(x)$ 都可以分解成一些不可约多项式的乘积, 即

$$f_1(x) = p_1(x) \cdots p_k(x), f_2(x) = p_{k+1}(x) \cdots p_s(x),$$

那么 $f(x) = f_1(x)f_2(x)$ 就可以分解成

$$f(x) = p_1(x) \cdots p_k(x)p_{k+1}(x) \cdots p_s(x),$$

其中 $p_i(x)$ $(1 \leq i \leq s)$ 均为不可约多项式. 由第二数学归纳法原理, 存在性得证.

唯一性：设 $f(x)=p_1(x)\cdots p_s(x)=q_1(x)\cdots q_t(x)$，其中 $p_i(x),q_j(x)$ 均为不可约多项式，下证 $s=t$，且适当排列因式的次序之后，有 $q_i(x)=c_ip_i(x),1\le i\le s$.

对第一个分解式中因式的个数用第一数学归纳法.

当 $s=1$ 时，$f(x)=p_1(x)=q_1(x)\cdots q_t(x)$，而 $p_1(x)$ 不可约，故 $t=1$ 且 $p_1(x)=q_1(x)$ 成立.

假设 $s=k-1$ 时，结论成立，则 $s=k$ 时，有 $f(x)=p_1(x)\cdots p_k(x)=q_1(x)\cdots q_t(x)$.

因为 $p_1(x)\mid q_1(x)\cdots q_t(x)$，由不可约多项式性质 (4) 得知，存在 $1\le i\le t$，不妨设 $i=1$，使得 $p_1(x)\mid q_1(x)$，那么 $q_1(x)=p_1(x)h(x)$.

因为 $q_1(x)$ 不可约，故 $h(x)=c_1\in F$，即 $q_1(x)=c_1p_1(x)$，从而 $p_1(x)p_2(x)\cdots p_k(x)=c_1p_1(x)q_2(x)\cdots q_t(x)$. 由消去律可得 $p_2(x)\cdots p_k(x)=c_1q_2(x)\cdots q_t(x)$. 由归纳假设 $t-1=k-1$，且 $c_1q_2(x)=c_2'p_2(x),q_i(x)=c_ip_i(x),2<i\le k$. 令 $c_1^{-1}c_2'=c_2$，则有 $t=k$，且 $q_i(x)=c_ip_i(x),i=1,2,\cdots,k$. 由数学归纳法原理，唯一性得证. ∎

注意：实际上，对于一般的情况，不存在一个因式分解的普遍可行的方法.

三、标准分解式

- 根据因式分解定理，任意次数大于零的多项式 $f(x)$ 都可以唯一分解为若干不可约多项式的乘积. 将 $f(x)$ 的首项系数提出，使每个因式的首项系数均为 1，可表示为

$$f(x) = a\, p_1(x) \cdots p_s(x),$$

其中 a 为首项系数，$p_i(x)$ 为首项系数为 1 的不可约多项式. 进一步将相同的不可约因式合并，可得到

$$f(x) = a\, p_1^{k_1}(x) \cdots p_t^{k_t}(x),$$

其中 $p_1(x), \ldots, p_t(x)$ 互不相同，首项系数均为 1，k_i 为相应指数.

- 这种形式称为 $f(x)$ 的 标准分解式.
- **例子**：考虑多项式 $f(x) = 2x^4 - 8x^3 + 8x^2$. 首先提出首项系数 2：

$$f(x) = 2(x^4 - 4x^3 + 4x^2) = 2x^2(x^2 - 4x + 4) = 2x^2(x-2)^2.$$

于是 $f(x)$ 的标准分解式为

$$f(x) = 2 \cdot x^2 \cdot (x-2)^2,$$

其中 x 与 $(x-2)$ 为首项系数为 1 的不可约多项式.

- 若 $f(x)$ 的标准分解式为

$$f(x) = a_0 p_1^{m_1}(x) p_2^{m_2}(x) \cdots p_r^{m_r}(x),$$

则 $g(x)$ 为 $f(x)$ 的因式 $\Leftrightarrow$

$$g(x) = b_0 p_1^{n_1}(x) p_2^{n_2}(x) \cdots p_r^{n_r}(x),$$

其中 b_0 为 $g(x)$ 的首项系数, $0 \le n_i \le m_i$, $i = 1, 2, \cdots, r$.

- 若两个多项式 $f(x), g(x)$ 均已化为标准分解式, 则其最大公因式就很容易求了. 设

$$f(x) = a p_1^{k_1}(x) \cdots p_r^{k_r}(x) q_{r+1}^{k_{r+1}}(x) \cdots q_s^{k_s}(x),$$

$$g(x) = b p_1^{l_1}(x) \cdots p_r^{l_r}(x) h_{r+1}^{l_{r+1}}(x) \cdots h_t^{l_t}(x),$$

其中 $p_i(x)$ $(1 \le i \le r)$, $q_j(x)$ $(r+1 \le j \le s)$, $h_u(x)$ $(r+1 \le u \le t)$ 均为首项系数为 1 的、互不相同的不可约多项式, 那么

$$(f(x), g(x)) = p_1^{m_1}(x) \cdots p_r^{m_r}(x),$$

其中 $m_i = min\{k_i, l_i\}$, $i = 1, 2, \cdots, r$.

§6 重因式

定义

设 $p(x)$ 是数域 P 上的一个不可约多项式, $f(x) \in P[x], k$ 为非负整数.
若 $p^k(x) \mid f(x)$, 但是 $p^{k+1}(x) \nmid f(x)$, 则称 $p(x)$ 是 $f(x)$ 的一个k 重因式.

- $k = 0$ 时, $p(x)$ 不是 $f(x)$ 的因式;
- $k = 1$ 时, $p(x)$ 是 $f(x)$ 的一个单因式;
- $k > 1$ 时, $p(x)$ 称为 $f(x)$ 的一个重因式.

性质

- 不可约多项式 $p(x)$ 为 $f(x)$ 的 k 重因式 $\Leftrightarrow f(x) = p^k(x)g(x)$, 其中 $(p(x), g(x)) = 1$.
- 若 $f(x)$ 的标准分解式为

$$f(x) = cp_1^{k_1}(x) \cdots p_s^{k_s}(x),$$

  则 $p_i(x)$ 是 $f(x)$ 的 k_i 重因式, $i = 1, 2, \cdots, s$, 其中 $k_i > 1$ 的那些不可约因式 $p_i(x)$ 为 $f(x)$ 的重因式.

一、多项式的导数

定义

设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 是数域 P 上的一个多项式，则

- 称

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$$

  为 $f(x)$ 的一阶导数.

- $f'(x)$ 的一阶导数称为 $f(x)$ 的二阶导数，记为 $f''(x)$，

  $\cdots\cdots$

- $(f^{(k-1)}(x))'$ 称为 $f(x)$ 的k 阶导数，记为 $f^{(k)}(x)$.

- 若 $\deg f(x) = n \ (n \geq 1)$，则

$$\deg f'(x) = n-1, \deg f''(x) = n-2, \cdots\cdots, \deg f^{(n)}(x) = 0, f^{(n+1)}(x) = 0.$$

  如 $f(x) = 3x^3 - 2x^2 + x - 5$ 的各阶导数分别为

$$f'(x) = 9x^2 - 4x + 1, f''(x) = 18x - 4, f'''(x) = 18, f^{(4)}(x) = 0.$$

导数的基本公式

(1) $(f(x)+g(x))' = f'(x)+g'(x)$,

(2) $(c\cdot f(x))' = c\cdot f'(x)$,

(3) $(f(x)g(x))' = f'(x)g(x)+f(x)g'(x)$,

(4) $(f^m(x))' = mf^{m-1}(x)f'(x)$.

例

设 $f(x) = p^k(x)g(x)$, 求 $f'(x)$

导数的基本公式

(1) $(f(x)+g(x))' = f'(x)+g'(x)$,

(2) $(c \cdot f(x))' = c \cdot f'(x)$,

(3) $(f(x)g(x))' = f'(x)g(x)+f(x)g'(x)$,

(4) $(f^m(x))' = mf^{m-1}(x)f'(x)$.

例

设 $f(x) = p^k(x)g(x)$, 求 $f'(x)$

解

$$\begin{aligned} f'(x) &= (p^k(x))'g(x) + p^k(x)g'(x) \\ &= kp^{k-1}(x)p'(x)g(x) + p^k(x)g'(x) \\ &= p^{k-1}(x)(kp'(x)g(x) + p(x)g'(x)). \end{aligned}$$

定理 6

- 如果不可约多项式 $p(x)$ 是 $f(x)$ 的一个 k 重因式 $(k \geq 1)$，则 $p(x)$ 是 $f'(x)$ 的一个 $k-1$ 重因式.
- 特别地，$f(x)$ 的单因式不是 $f'(x)$ 的因式.

定理 6

- 如果不可约多项式 $p(x)$ 是 $f(x)$ 的一个 k 重因式 $(k \geq 1)$, 则 $p(x)$ 是 $f'(x)$ 的一个 $k-1$ 重因式.
- 特别地, $f(x)$ 的单因式不是 $f'(x)$ 的因式.

证明 只需证明 $p^{k-1}(x) \mid f'(x)$, 但 $p^k(x) \nmid f'(x)$. 因为 $p(x)$ 是 $f(x)$ 的一个 k 重因式, 所以

$$f(x) = p^k(x)g(x), \qquad \text{其中}(p(x), g(x)) = 1.$$

于是

$$\begin{aligned} f'(x) &= [p^k(x)]'g(x) + p^k(x)g'(x) \\ &= kp^{k-1}(x)p'(x)g(x) + p^k(x)g'(x) \\ &= p^{k-1}(x)[kp'(x)g(x) + p(x)g'(x)]. \end{aligned}$$

所以, $p^{k-1}(x) \mid f'(x)$, 但 $p(x) \nmid [kp'(x)g(x) + p(x)g'(x)]$(为什么？), 故 $p^k(x) \nmid f'(x)$.

因此, $p(x)$ 为 $f'(x)$ 的 $k-1$ 重因式.

特别地, $f(x)$ 的单因式是 $f'(x)$ 的 0 重因式, 因此它不是 $f'(x)$ 的因式. ∎

二、重因式的性质

定理 6

- 如果不可约多项式 $p(x)$ 是 $f(x)$ 的一个 k 重因式 $(k \geq 1)$，则 $p(x)$ 是 $f'(x)$ 的一个 $k-1$ 重因式.
- 特别地，$f(x)$ 的单因式不是 $f'(x)$ 的因式.

说明

定理的逆命题不成立：例如 $f(x) = x^3 - 1$，则 $f'(x) = 3x^2$.
显然 x 是 $f'(x)$ 的二重因式，但它不是 $f(x)$ 的三重因式.

若加强条件，则逆命题成立：

性质

若不可约多项式 $p(x)$ 是 $f'(x)$ 的 $(k-1)$ 重因式，且是 $f(x)$ 的一个因式，则它是 $f(x)$ 的 k 重因式.

证明　设 $p(x)$ 在 $f(x)$ 中的重数为 r，则 $p(x)$ 在 $f'(x)$ 中的重数为 $r-1$（当 $r \geq 1$ 时）. 若 $p(x)$ 在 $f'(x)$ 中恰好是 $(k-1)$ 重因式，且仍为 $f(x)$ 的因式，则 $r-1 = k-1$，从而 $r = k$. ∎

二、重因式的性质

定理 6

- 如果不可约多项式 $p(x)$ 是 $f(x)$ 的一个 k 重因式 $(k \geq 1)$，则 $p(x)$ 是 $f'(x)$ 的一个 $k-1$ 重因式.
- 特别地，$f(x)$ 的单因式不是 $f'(x)$ 的因式.

推论 1

不可约多项式 $p(x)$ 是 $f(x)$ 的一个 $k(\geq 1)$ 重因式
$\Leftrightarrow$ $p(x)$ 是 $f(x), f'(x), \ldots, f^{(k-1)}(x)$ 的因式，但不是 $f^{(k)}(x)$ 的因式.

二、重因式的性质

定理 6

- 如果不可约多项式 $p(x)$ 是 $f(x)$ 的一个 k 重因式 $(k \geq 1)$，则 $p(x)$ 是 $f'(x)$ 的一个 $k-1$ 重因式.
- 特别地，$f(x)$ 的单因式不是 $f'(x)$ 的因式.

推论 1

不可约多项式 $p(x)$ 是 $f(x)$ 的一个 $k(\geq 1)$ 重因式
$\Leftrightarrow$ $p(x)$ 是 $f(x), f'(x), \ldots, f^{(k-1)}(x)$ 的因式，但不是 $f^{(k)}(x)$ 的因式.

证明 因为 $p(x)$ 是 $f(x)$ 的一个 k 重因式，故由定理 6，$p(x)$ 是 $f'(x)$ 的一个 $k-1$ 重因式，$\cdots$，是 $f^{(k-2)}(x)$ 的一个 2 重因式，也是 $f^{(k-1)}(x)$ 的一个单因式，进而它不是 $[f^{(k-1)}(x)]' = f^{(k)}(x)$ 的因式.

反之，因为 $p(x)$ 是 $f(x)$ 的因式，不妨设为 l 重因式.

由前所述，$p(x)$ 为 $f'(x), f''(x), \cdots, f^{(l-1)}(x)$ 的因式，但不是 $f^{(k)}(x)$ 的因式，那么 $k > l-1$，即 $k \geq l$.

又因为 $p(x)$ 是 $f'(x), f''(x), \cdots, f^{(k-1)}(x)$ 的因式，但不是 $f^{(l)}(x)$ 的因式，所以 $l \geq k$. 从而 $l = k$. ∎

推论 2

不可约多项式 $p(x)$ 是 $f(x)$ 的一个重因式 $\Leftrightarrow$ $p(x)$ 是 $f(x)$ 与 $f'(x)$ 的一个公因式.

推论 3

多项式 $f(x)$ 无重因式 $\Leftrightarrow$ $f(x)$ 与 $f'(x)$ 互素.

推论 2

不可约多项式 $p(x)$ 是 $f(x)$ 的一个重因式 $\Leftrightarrow$ $p(x)$ 是 $f(x)$ 与 $f'(x)$ 的一个公因式.

证明 $\Rightarrow$ 因为 $p(x)$ 是 $f(x)$ 的一个重因式，不妨设为 k 重因式，则 $k \geq 2$. 由定理 6 , $p(x)$ 为 $f'(x)$ 的一个 $k-1$ 重因式 $(k-1 \geq 1)$，故它是 $f'(x)$ 的一个因式. 那么 $p(x)$ 是 $f(x)$ 与 $f'(x)$ 的一个公因式.

$\Leftarrow$ 已知 $p(x)$ 是 $f(x)$ 与 $f'(x)$ 的一个公因式. 下证 $p(x)$ 是 $f(x)$ 的一个重因式：否则，$p(x)$ 为 $f(x)$ 的一个单因式，由定理 6 , $p(x)$ 不是 $f'(x)$ 的因式，从而不是 $f(x)$ 与 $f'(x)$ 的公因式，矛盾. 所以 $p(x)$ 是 $f(x)$ 的一个重因式. ∎

推论 3

多项式 $f(x)$ 无重因式 $\Leftrightarrow$ $f(x)$ 与 $f'(x)$ 互素.

证明 $\Rightarrow$ 反证法. 假设不可约多项式 $p(x)$ 是 $f(x)$ 与 $f'(x)$ 的一个公因式，则由推论 2 知,$p(x)$ 是 $f(x)$ 的一个重因式. 与 $f(x)$ 无重因式矛盾. 故 $(f(x), f'(x)) = 1$.

$\Leftarrow$ 设 $(f(x), f'(x)) = 1$，假若 $f(x)$ 有一个重因式 $p(x)$，则由推论 2 知，$p(x)$ 是 $f(x)$ 与 $f'(x)$ 的公因式，故 $p(x) \mid 1$，这与 $p(x)$ 是不可约多项式矛盾. 从而 $f(x)$ 无重因式. ∎

三、分离重因式

下面介绍一个去掉重因式的有效方法，称为分离重因式法.

命题

设 $f(x)$ 的标准分解式为

$$f(x)=ap_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x),\ r_i>0,\ i=1,2,\cdots,s,$$

则

$$\frac{f(x)}{(f(x),f'(x))}=ap_1(x)\cdots p_s(x).$$

证明　由定理 6 可知，p_i 是 $f(x)$ 的 r_i-1 重因式. 因此，$(f(x),f'(x))$ 的标准分解式为

$$p_1^{r_1-1}(x)\cdots p_s^{r_s-1}(x).$$

∎

这个多项式每个不可约因式只出现一次，故无重因式，但与 $f(x)$ 有完全相同的不可约因式.

分离重因式法有助于分解因式.

例 1

求出 $f(x) = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$ 的标准分解式.

分离重因式法有助于分解因式.

例 1

求出 $f(x)=x^5-x^4-2x^3+2x^2+x-1$ 的标准分解式.

解 因为 $f'(x)=5x^4-4x^3-6x^2+4x+1$, 所以

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

$$g(x)=\frac{f(x)}{(f(x),f'(x))}=(x-1)(x+1)=x^2-1.$$

因此, $x-1,x+1$ 分别为 $f(x)$ 的 3 重和 2 重因式.

从而 $f(x)=(x-1)^3(x+1)^2$.

例 2

a, b 应该满足什么条件, 才使得 $f(x) = x^3 + 3ax + b$ 有重因式?

例 2

a, b 应该满足什么条件，才使得 $f(x) = x^3 + 3ax + b$ 有重因式？

解 因为 $f'(x) = 3x^2 + 3a$，用 $f'(x)$ 除 $f(x)$ 所得余式为 $r_1(x) = 2ax + b$.

若 $a = 0$，则 $f(x)$ 有重因式 $\Leftrightarrow$ $r_1(x) = 0$，即 $a = b = 0$. 此时 $f(x) = x^3$ 有重因式 x.

若 $a \neq 0$，则 $r_1(x)$ 是一个 1 次多项式，用 $r_1(x)$ 除 $f'(x)$，得余式 $r_2(x) = 3a + \frac{3b^2}{4a^2}$.

则此时 $f(x)$ 有重因式 $\Leftrightarrow$ $r_2(x) = 0$，即 $4a^3 + b^2 = 0$.

综上所述，$f(x)$ 有重因式 $\Leftrightarrow$ $4a^3 + b^2 = 0$.

例 3

设 $f(x) \in P[x]$ 且 $\deg(f(x)) = n \geqslant 1$，则 $f'(x) \mid f(x) \Leftrightarrow$ 存在 $a, b \in P$ 使得 $f(x) = a(x-b)^n$.

例 3

设 $f(x)\in P[x]$ 且 $\deg(f(x))=n\geqslant 1$，则 $f'(x)\mid f(x)\Leftrightarrow$ 存在 $a,b\in P$ 使得 $f(x)=a(x-b)^n$.

证明 充分性 因为 $f(x)=a(x-b)^n$ ，所以 $f'(x)=na(x-b)^{n-1}$. 故 $f'(x)\mid f(x)$.

必要性 因为 $f'(x)\mid f(x)$ ，所以可设 $f(x)=\frac{1}{n}f'(x)(x-b)$ ，其中 $b\in P$.

于是 $(f(x),f'(x))=\frac{1}{na}f'(x)$，其中 $a\in P$ 是 $f(x)$ 的首项系数. 因此,

$$\frac{f(x)}{(f(x),f'(x))}=a(x-b).$$

因为 $f(x)$ 与 $\frac{f(x)}{(f(x),f'(x))}$ 有完全相同的不可约因式，且 $\deg f(x)=n$，故 $f(x)=a(x-b)^n$.

§7 多项式函数

从不同的角度去理解同一数学对象，这在数学研究中是相当重要的，

因为它不仅可以开阔思路，更重要的是有可能发掘出表面不同的数学对象之间的本质联系.

这一节，我们将考虑多项式的取值问题，即利用函数的观点理解多项式.

设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in P[x]$，用 $c \in P$ 代替 x 得 $f(c) = a_n c^n + \cdots + a_1 c + a_0$.

从而对于任意的 $c \in P$，P 中存在唯一的数 $f(c)$ 与之对应，即得 P 到自身的一个映射.

定义

由 $P[x]$ 中一个多项式 $f(x)$ 确定的 P 到 P 的映射： $c \longmapsto f(c)$ 称为数域 P 上的一个**多项式函数**.

设 $f(x), g(x) \in P[x], c \in P$，由多项式的相等及加法、乘法定义可得

- 若 $f(x) = g(x)$，则 $f(c) = g(c)$.
- 若 $h_1(x) = f(x) \pm g(x), h_2(x) = f(x)g(x)$，则 $h_1(c) = f(c) \pm g(c), h_2(c) = f(c)g(c)$.

定理 7 (余数定理)

用一次式 $x-c$ 去除 $f(x)$ 所得的余数等于 $f(x)$ 在 $x=c$ 处的函数值 $f(c)$.

证明 由带余除法定理, 用 $x-c$ 去除 $f(x)$ 所得余式为常数 r, 商式设为 $q(x)$, 则 $f(x)=(x-c)q(x)+r$. 取 $x=c$, 得 $f(c)=(c-c)q(c)+r=r$. ∎

- 那么如何求 $x-c$ 除 $f(x)$ 所得的商式 $q(x)$ 呢?

现设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

$$q(x)=b_{n-1}x^{n-1}+\cdots+b_1x+b_0,$$

则由

$$f(x)=q(x)(x-c)+r=(b_{n-1}x^{n-1}+\cdots+b_1x+b_0)(x-c)+r$$

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 =$$

$$b_{n-1}x^n + (b_{n-2} - cb_{n-1})x^{n-1} + \cdots + (b_1 - cb_2)x^2 + (b_0 - cb_1)x + r - b_0 c.$$

比较两端同次项系数可得

$$\begin{cases} a_n = b_{n-1}, \\ a_{n-1} = b_{n-2} - cb_{n-1}, \\ \vdots \\ a_k = b_{k-1} - cb_k, \\ \vdots \\ a_1 = b_0 - cb_1, \\ a_0 = r - cb_0, \end{cases} \Rightarrow \begin{cases} b_{n-1} = a_n, \\ b_{n-2} = a_{n-1} + cb_{n-1}, \\ \vdots \\ b_{k-1} = a_k + cb_k, \\ \vdots \\ b_0 = a_1 + cb_1, \\ r = a_0 + cb_0. \end{cases}$$

这样, **欲求系数** b_{k-1}, **只需前一个系数** b_k **乘** c **再加上** a_k **即可**.

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 =$$
$$b_{n-1}x^n + (b_{n-2} - cb_{n-1})x^{n-1} + \cdots + (b_1 - cb_2)x^2 + (b_0 - cb_1)x + r - b_0c.$$

比较两端同次项系数可得

$$\begin{cases} a_n = b_{n-1}, \\ a_{n-1} = b_{n-2} - cb_{n-1}, \\ \vdots \\ a_k = b_{k-1} - cb_k, \\ \vdots \\ a_1 = b_0 - cb_1, \\ a_0 = r - cb_0, \end{cases} \Rightarrow \begin{cases} b_{n-1} = a_n, \\ b_{n-2} = a_{n-1} + cb_{n-1}, \\ \vdots \\ b_{k-1} = a_k + cb_k, \\ \vdots \\ b_0 = a_1 + cb_1, \\ r = a_0 + cb_0. \end{cases}$$

这样, 欲求系数 b_{k-1}, 只需前一个系数 b_k 乘 c 再加上 a_k 即可. 可由下表容易地求出

$$\begin{array}{c|cccccc} c & a_n & a_{n-1} & \cdots & a_2 & a_1 & a_0 \\ & & cb_{n-1} & \cdots & cb_2 & cb_1 & cb_0 \\ \hline & b_{n-1} & b_{n-2} & \cdots & b_1 & b_0 & r \end{array}$$

此法称为**综合除法**.

例 1

求 $x+3$ 除 $f(x)=x^4+x^2+4x-9$ 所得商式及余数.

例 1

求 $x+3$ 除 $f(x)=x^4+x^2+4x-9$ 所得商式及余数.

解 用综合除法:

$$
\begin{array}{r|rrrrr}
-3 & 1 & 0 & 1 & 4 & -9 \\
 & & -3 & 9 & -30 & 78 \\
\hline
 & 1 & -3 & 10 & -26 & 69
\end{array}
$$

故商式 $q(x)=x^3-3x^2+10x-26$, 余数 $r=69$.

例 2

将 $f(x) = x^4 + x^2 + 4x - 9$ 表示成 $x + 3$ 的方幂和的形式.

例 2

将 $f(x)=x^4+x^2+4x-9$ 表示成 $x+3$ 的方幂和的形式.

解

$$
\begin{array}{r|rrrrr}
-3 & 1 & 0 & 1 & 4 & -9 \\
 & & -3 & 9 & -30 & 78 \\
\hline
 & 1 & -3 & 10 & -26 & 69 \\
 & & -3 & 18 & -84 & \\
\cline{2-5}
 & 1 & -6 & 28 & -110 & \\
 & & -3 & 27 & & \\
\cline{2-4}
 & 1 & -9 & 55 & & \\
 & & -3 & & & \\
\cline{2-3}
 & 1 & -12 & & &
\end{array}
$$

$$f(x)=(x+3)^4-12(x+3)^3+55(x+3)^2-110(x+3)+69.$$

定义

设 $f(x)$ 是 $F[x]$ 中的一个多项式, 而 c 为数域 P 中的一个数.
若 $x=c$ 时, $f(x)$ 的值 $f(c)$ 等于 0, 那么 c 就叫做 $f(x)$ 在 P 中的一个根.

以下结论将一次因式与根紧密地联系起来.

推论

c 为 $f(x)$ 的一个根 $\Leftrightarrow$ $(x-c)\mid f(x)$.

证明 $\Rightarrow$ 因为 c 是 $f(x)$ 的一个根, 故 $f(c)=0$. 但由余数定理, $f(c)$ 为 $x-c$ 除 $f(x)$ 所得的余数 r, 故 $r=0$. 从而 $(x-c)\mid f(x)$.

$\Leftarrow$ 因为 $(x-c)\mid f(x)$, 所以 $f(x)=(x-c)q(x)+0$, 故 $f(c)=0$, 即 c 为 $f(x)$ 的一个根. ∎

定义

若 $x-c$ 是 $f(x)$ 的一个 k 重因式, 则称 c 是 $f(x)$ 的一个 k 重根 $(k \geq 1)$.

- $k=1$ 时, c 为 $f(x)$ 的一个 单根;
- $k>1$ 时, c 为 $f(x)$ 的一个 重根.

由定理 6 可知

性质

- 若 c 为 $f(x)$ 的一个 k 重根, 其中 $k>1$, 则 c 必为 $f'(x)$ 的一个 $k-1$ 重根.
- c 是 $f(x)$ 的 k 重根的充要条件是 $f(c)=f'(c)=\cdots=f^{(k-1)}(c)=0$, 而 $f^{(k)}(c)\neq 0$.

思考

如果 α 是 $f'(x)$ 的 m 重根, 那么 α 是不是 $f(x)$ 的 $m+1$ 重根 ?

定理 8

数域 P 上 n 次多项式 $f(x)$ 在 P 中最多有 n 个根（k 重根按 k 个计算）.

证明 $n=0$ 时, $f(x)$ 是零次多项式, 它在 P 上根的个数为 0, 命题成立.

$n>0$ 时, $f(x)$ 为一个次数 >0 的多项式, 由因式分解定理, $f(x)$ 可以分解为 P 上一些不可约多项式的乘积. 令 $(x-c_1),(x-c_2),\cdots,(x-c_s)$ 是出现在 $f(x)$ 的标准分解式中所有互不相同的一次式, 并设它们的重数分别为 $k_1,k_2,\cdots,k_s$, 则

$$f(x)=(x-c_1)^{k_1}(x-c_2)^{k_2}\cdots(x-c_s)^{k_s}g(x),$$

其中 $g(x)$ 无一次因式.

因此 $f(x)$ 在 P 中的根只能是 $c_1,c_2,\cdots,c_s$, 它们的重数分别为 $k_1, k_2, \cdots, k_s$. 故由 (1) 式得

$$\sum_{i=1}^{s} k_i \le n = \deg f(x).$$

∎

由上可知，每个多项式函数都可由一个多项式来定义.

那么不同的多项式会不会定义出相同的函数呢?

下面的定理给出了一个否定的回答.

定理 9

设 $f(x), g(x)$ 的次数不超过 n，而它们对于 P 中 $n+1$ 个互不相同的数 $c_1, c_2, \cdots, c_{n+1}$ 都有相同的函数值，即 $f(c_i)=g(c_i), 1 \leq i \leq n+1$，那么 $f(x)=g(x)$.

证明 令 $u(x)=f(x)-g(x)$，欲证 $f(x)=g(x)$，只要证明 $u(x)=0$. 因为

$$u(c_i)=f(c_i)-g(c_i)=0, 1 \leq i \leq n+1,$$

故 $u(x)$ 在 P 中至少有 $n+1$ 个根. 若 $f(x) \neq g(x)$，则 $u(x)=f(x)-g(x) \neq 0$，那么由次数定理及

$$\max\{\deg f(x), \deg g(x)\} \leq n$$

得 $\deg u(x) \leq n$，即 $u(x)$ 是一个次数不超过 n 的多项式，但它在 P 中至少有 $n+1$ 个根，与定理 8 矛盾. 从而必有 $u(x)=0$，即 $f(x)=g(x)$. ∎

由上可知，每个多项式函数都可由一个多项式来定义.

那么不同的多项式会不会定义出相同的函数呢?

下面的定理给出了一个否定的回答.

定理 9

设 $f(x), g(x)$ 的次数不超过 n，而它们对于 P 中 $n+1$ 个互不相同的数 $c_1, c_2, \cdots, c_{n+1}$ 都有相同的函数值，即 $f(c_i) = g(c_i), 1 \le i \le n+1$，那么 $f(x) = g(x)$.

推论

设 P 是数域，$f(x), g(x) \in P[x]$ ，则
$f(x) = g(x) \Leftrightarrow f = g$，即对任意 $\alpha \in F$ ，都有 $f(\alpha) = g(\alpha)$.

注记

设 $\mathbb{F} = \{0, 1\}$ 是二元域. 类似于数域的情形，可以定义 $\mathbb{F}$ 上的一元多项式环 $\mathbb{F}[x]$.
此时，上面的命题不成立. 例如，设 $f(x) = x + 1, g(x) = x^2 + 1 \in \mathbb{F}[x]$.
显然 $f(x) \neq g(x)$，但是 $f = g$.

§8 复系数与实系数多项式的因式分解

我们先来看一个具体例子，感受一下同一个多项式在不同数域上分解的差异：

$$
\begin{aligned}
x^4-4 &\overset{\mathbb{Q}}{=} (x^2-2)(x^2+2)\\
&\overset{\mathbb{R}}{=} (x-\sqrt{2})(x+\sqrt{2})(x^2+2)\\
&\overset{\mathbb{C}}{=} (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}i)(x+\sqrt{2}i)
\end{aligned}
$$

- 在有理数域 $\mathbb{Q}$ 中，我们只能“看见”平方差分解；
- 进入实数域 $\mathbb{R}$，平方项又可以继续分解，得到两个实根；
- 而到了复数域 $\mathbb{C}$，连 x^2+2 也不再“顽固”，它终于能彻底分解成一次因式.

由此可以直观体会到：多项式的分解形式取决于我们所处的数域.

- 在任意数域 P 上，多项式的根与因式之间的关系依然成立；
- 次数为 n 的多项式最多有 n 个根，但这些根能否“出现”，要看数域是否足够“宽”；
- 实数域与复数域各自拥有特殊的代数结构，因此值得我们单独研究.

一、复系数多项式的因式分解

在复数域 $\mathbb{C}$ 上，有一个极其重要的结论——

代数基本定理

任意次数 ≥ 1 的复系数多项式在复数域 $\mathbb{C}$ 上至少有一个根.

- 这个定理最早由德国数学家高斯（Carl Friedrich Gauss, 1777–1855）严格证明.
- 他在 1797 年的博士论文中首次给出了证明思路，后来又多次改进，提供了不同的证明版本.
- 高斯被称为“数学王子”，他的工作不仅影响了代数学，也为整个数学体系奠定了严谨的基础.
- 在今后学习复变函数时，我们还会看到用更简洁、更优雅的方法证明这一深刻的结论.

我们知道，根与一次因式一一对应. 因此，代数基本定理也可以换一种等价而更直观的表述：

命题

任意次数 ≥ 1 的复系数多项式在复数域 $\mathbb{C}$ 上必定可以分解出一个一次因式.

复系数多项式因式分解定理

每一个次数 ≥ 1 的复系数多项式在复数域上都能分解成一次多项式的乘积.

证明　只要证明在复数域上次数 ≥ 2 的多项式全是可约的. 设 $\deg f(x) \geq 2$, 由代数基本定理, $f(x)$ 在复数域 $\mathbb{C}$ 中至少有一个根, 设 c 为其一个根, 即 $f(c) = 0$. 由根与一次式的关系可得 $(x-c) \mid f(x)$. 故有 $q(x)$, 使得 $f(x) = (x-c)q(x)$, 即 $f(x)$ 在复数域 $\mathbb{C}$ 上可约. 从而在复数域 $\mathbb{C}$ 上只有一次式才是不可约多项式, 故任一次数 ≥ 1 的复系数多项式都可分解成一次多项式的乘积. ∎

复系数多项式因式分解定理

每一个次数 ≥ 1 的复系数多项式在复数域上都能分解成一次多项式的乘积.

性质

复系数多项式 $f(x)$ 的标准分解式:

$$f(x) = a(x - c_1)^{k_1}(x - c_2)^{k_2} \cdots (x - c_s)^{k_s},$$

其中 $c_1, c_2, \cdots, c_s$ 为复数, $k_1, k_2, \cdots, k_s$ 为正整数.

设 $\deg f(x) = n$. 当 $n \geq 1$ 时, 由 $f(x)$ 的标准分解式及根与一次式的关系知, c_i 为 $f(x)$ 的 k_i 重根, 且 $\sum_{i=1}^{s} k_i = n$. 因此,

命题

n 次多项式 $f(x)$ 在复数域 $\mathbb{C}$ 上恰有 n 个根.

下面讨论根与系数的关系. 在中学里有著名的韦达定理, 现在也来讨论此类问题.

设

$$
\begin{aligned}
f(x) &= a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \\
&= a_0(x^n + \frac{a_1}{a_0}x^{n-1} + \cdots + \frac{a_{n-1}}{a_0}x + \frac{a_n}{a_0}) \\
&= a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),
\end{aligned}
$$

其中 $a_0 \neq 0$, 而 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 为 $f(x)$ 的 n 个根. 比较两端系数, 得

$$
\begin{cases}
\frac{a_1}{a_0} = -\sum\limits_{i=1}^{n} \alpha_i, \\
\frac{a_2}{a_0} = \sum\limits_{1\le i<j\le n} \alpha_i\alpha_j, \\
\qquad\vdots \\
\frac{a_k}{a_0} = (-1)^k \sum\limits_{1\le i_1<i_2<\cdots<i_k\le n} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k} \\
\qquad\vdots \\
\frac{a_n}{a_0} = (-1)^n\alpha_1\cdots\alpha_n.
\end{cases}
$$

它称为韦达公式.

二、实系数多项式

虚根成对定理

如果实系数多项式 $f(x)$ 有虚根 α, 则 α 的共轭数 $\overline{\alpha}$ 必定是 $f(x)$ 的一个根, 且 α 与 $\overline{\alpha}$ 有相同的重数.

证明 设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. 因为 α 是 $f(x)$ 的一个根, 故 $f(\alpha) = 0$, 即

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

两边取共轭, 得

$$\overline{a_n}\ \overline{\alpha}^n + \overline{a_{n-1}}\ \overline{\alpha}^{n-1} + \cdots + \overline{a_1}\ \overline{\alpha} + \overline{a_0} = 0.$$

又因为 $a_i \in \mathbb{R}$, 所以 $\overline{a_i} = a_i$, $0 \le i \le n$. 故有

$$a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \cdots + a_1\overline{\alpha} + a_0 = 0,$$

即 $f(\overline{\alpha}) = 0$, 亦即 $\overline{\alpha}$ 为 $f(x)$ 的一个根, 从而

$$(x-\alpha), (x-\overline{\alpha}) \mid f(x).$$

又 $\alpha \neq \overline{\alpha}$, 故 $(x-\alpha, x-\overline{\alpha}) = 1$, 那么 $f(x)$ 可被 $g(x) = (x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha}$ 整除. 由共轭数的性质易知, $g(x)$ 的系数均为实数. 故存在 $h(x) \in \mathbb{R}[x]$, 使得 $f(x) = g(x)h(x)$. ∎

实系数多项式的因式分解定理

每一个次数 ≥ 1 的实系数多项式在实数域 $\mathbb{R}$ 上，都能唯一地分解成一次式与若干二次不可约多项式的乘积.

证明　对多项式的次数用数学归纳法. 对于一次多项式，结论显然成立.

假设结论对所有次数 $< n$ 的多项式成立，现对 n 次多项式 $f(x)$ 讨论.

由代数基本定理，$f(x)$ 在复数域 $\mathbb{C}$ 上至少有一个根 α.

- 若 α 为实数，则 $f(x) = (x-\alpha)f_1(x)$，且 $\deg f_1(x) < n$.
  由归纳假设，$f_1(x)$ 可分解为一次与二次不可约因式的乘积，因此 $f(x)$ 亦然.
- 若 α 为虚数，则其共轭 $\overline{\alpha}$ 也是 $f(x)$ 的根，且 $\alpha \neq \overline{\alpha}$. 于是

$$f(x) = (x-\alpha)(x-\overline{\alpha})f_2(x) = [x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha}]f_2(x),$$

  其中 $g(x) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha} \in \mathbb{R}[x]$，且 $g(x)$ 在 $\mathbb{R}$ 上不可约.
  由归纳假设，$f_2(x)$ 可分解为一次与二次不可约因式的乘积，因此 $f(x)$ 亦然.

由数学归纳法原理，结论得证. ∎

实系数多项式的因式分解定理

每一个次数 ≥ 1 的实系数多项式在实数域 $\mathbb{R}$ 上, 都能唯一地分解成一次式与若干二次不可约多项式的乘积.

说明

设 $f(x) = x^2 + px + q \in \mathbb{R}[x]$, 则 $f(x)$ 在实数域 $\mathbb{R}$ 上不可约的充要条件是 $p^2 - 4q < 0$.

性质

实系数多项式 $f(x)$ 的标准分解式为:

$$f(x) = a(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_s)^{k_s}(x^2+p_1x+q_1)^{l_1}\cdots(x^2+p_rx+q_r)^{l_r},$$

其中 $\alpha_i, p_j, q_j \in \mathbb{R}$, k_i, l_j 为正整数, 且 $p_j^2 - 4q_j < 0$.

- 满足 $\omega^n = 1$ 的复数 ω 称为一个 n 次**单位根**，它共有 n 个：

$$\omega_k = e^{\frac{2k\pi}{n}\mathrm{i}} = \cos\frac{2k\pi}{n} + \mathrm{i}\,\sin\frac{2k\pi}{n}, k = 0, 1, \cdots, n-1.$$

- 因为任意 n 次单位根 ω 的模都是 1，所以 $\omega \cdot \overline{\omega} = 1$.

例 1

求 $x^n - 1$ 分别在实数域 $\mathbb{R}$ 和复数域 $\mathbb{C}$ 上的分解式.

- 满足 $\omega^n = 1$ 的复数 ω 称为一个 n 次**单位根**, 它共有 n 个:

$$\omega_k = e^{\frac{2k\pi}{n}\mathrm{i}} = \cos\frac{2k\pi}{n} + \mathrm{i}\,\sin\frac{2k\pi}{n}, k = 0, 1, \cdots, n-1.$$

- 因为任意 n 次单位根 ω 的模都是 1, 所以 $\omega \cdot \overline{\omega} = 1$.

例 1

求 $x^n - 1$ 分别在实数域 $\mathbb{R}$ 和复数域 $\mathbb{C}$ 上的分解式.

解 令 $\omega = \cos\frac{2\pi}{n} + \mathrm{i}\,\sin\frac{2\pi}{n}$ 是一个 n 次单位原根, 则 $\omega^0, \omega^1, \cdots, \omega^{n-1}$ 为全部的 n 次单位根.

在复数域 $\mathbb{R}$ 上,

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}).$$

因为

$$\overline{\omega^k} = \cos\frac{2k\pi}{n} - \mathrm{i}\,\sin\frac{2k\pi}{n} = \cos\frac{2(n-k)\pi}{n} + \mathrm{i}\,\sin\frac{2(n-k)\pi}{n} = \omega^{n-k},$$

所以

$$(x-\omega^k)(x-\omega^{n-k}) = x^2 - 2x\cos\frac{2k\pi}{n} + 1$$

故在实数域 $\mathbb{R}$ 上, 当 n 为奇数时,

$$\begin{aligned} x^n - 1 &= (x-1)[(x-\omega)(x-\omega^{n-1})]\cdot[(x-\omega^2)(x-\omega^{n-2})]\cdots[(x-\omega^{\frac{n-1}{2}})(x-\omega^{\frac{n+1}{2}})] \\ &= (x-1)(x^2-2x\cos\frac{2\pi}{n}+1)(x^2-2x\cos\frac{4\pi}{n}+1)\cdots\cdot(x^2-2x\cos\frac{n-1}{n}\pi+1). \end{aligned}$$

当 n 为偶数时, 因为 $\omega^{\frac{n}{2}}\omega^{\frac{n}{2}} = \omega^{\frac{n}{2}}\overline{\omega^{\frac{n}{2}}} = 1$. 所以, 有 $\omega^{\frac{n}{2}} = \overline{\omega^{\frac{n}{2}}}$. 那么

$$\omega^{\frac{n}{2}} = (\cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n})^{\frac{n}{2}} = -1.$$

从而

$$x^n - 1 = (x-1)(x+1)(x^2-2x\cos\frac{2\pi}{n}+1)(x^2-2x\cos\frac{4\pi}{n}+1)\cdots(x^2-2x\cos\frac{n-2}{n}\pi+1).$$

有理系数多项式的因式分解定理

每一个次数 ≥ 1 的有理系数多项式，都可以在有理数域 $\mathbb{Q}$ 上唯一地分解为若干不可约多项式的乘积.

思考：在有理数域 $\mathbb{Q}$ 上，什么样的多项式才是不可约的？

回答这个问题并不容易. 这一点与实数域和复数域的情形不同：

- 在复数域 $\mathbb{C}$ 上，只有一次式是不可约的；
- 在实数域 $\mathbb{R}$ 上，只有一次式和某些二次式不可约；
- 而在有理数域 $\mathbb{Q}$ 上，不可约多项式的判定更为复杂.

为了研究有理系数多项式的不可约性，我们可以先将其因式分解问题转化为整系数多项式的因式分解问题.

一、本原多项式

定义

若一个非零的整系数多项式

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

的系数 $b_n, b_{n-1}, \cdots, b_1, b_0$ 没有异于 ± 1 的公因数，即它们互素，则称 $g(x)$ 为一个本原多项式.

如 $2x^4 + 3x^3 + 4x^2 + 6x + 8$ 是一个本原多项式，$4x^2 + 6x + 8$ 不是本原多项式. 由定义可得

性质

在有理数域上任意一个非零多项式 $f(x)$ 都可以表示成一个有理数与一个本原多项式的乘积，且在相差一个 $\pm$ 号的意义下表示法唯一.

例如

$$\frac{4}{5}x^2 - 2x + \frac{2}{3} = \frac{2}{15}\left(6x^2 - 15x + 5\right).$$

性质

在有理数域上任意一个非零多项式 $f(x)$ 都可以表示成一个有理数与一个本原多项式的乘积，且在相差一个 $\pm$ 号的意义下表示法唯一.

证明 (存在性) 将 $f(x)$ 的所有系数都写成既约分数，并设 c 是 $f(x)$ 的所有系数的分母的最小公倍数，d 是 $cf(x)$ 的系数的最大公因数. 则

$$f(x) = \frac{1}{c}[cf(x)] = \frac{d}{c}\varphi(x),$$

其中 $g(x) = cf(x)$ 是一个整系数多项式，而 $\varphi(x)$ 是一个本原多项式.

(唯一性) 假设 $f(x) = r\varphi(x) = r_1\varphi_1(x)$，其中 $r, r_1 \in \mathbb{Q}$，$\varphi(x), \varphi_1(x)$ 都是本原多项式.

设 $r = \frac{d}{c}, r_1 = \frac{d_1}{c_1}$ 都是既约分数，其中 c, d, c_1, d_1 均为非零整数.

由 $\frac{d}{c}\varphi(x) = \frac{d_1}{c_1}\varphi_1(x)$，即得 $$c_1 d\varphi(x) = cd_1\varphi_1(x) \triangleq f_1(x),$$

那么 $f_1(x)$ 是一个整系数多项式. 由于 $\varphi(x)$ 与 $\varphi_1(x)$ 均为本原多项式，故 $c_1 d, cd_1$ 均可看作 $f_1(x)$ 的所有系数的最大公因数，从而 $c_1 d = \pm cd_1$，即 $\frac{d}{c} = \pm\frac{d_1}{c_1}$，亦即 $r = \pm r_1$，那么 $\varphi(x) = \pm\varphi_1(x)$. ∎

综上所述，我们将有理系数多项式的因式分解问题转化为整系数多项式的因式分解问题.

定理 10 (Gauss 引理)

两个本原多项式的乘积还是本原多项式，即若

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 = \sum_{j=0}^{m} b_j x^j$$

都是本原多项式，则 $h(x) = f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k$ 也是一个本原多项式，其中 $c_k = \sum_{i+j=k} a_i b_j$.

证明　用反证法. 假设 $h(x)$ 不是本原的，即 $h(x)$ 的各项系数的最大公因数 $d > 1$，

那么一定存在一个素数 $p \mid d$，即 p 为 $h(x)$ 的各项系数的一个公因数.

由 $f(x)$ 是本原多项式，知 p 不能整除 $f(x)$ 的所有系数，即 $f(x)$ 至少有一个系数不能被 p 整除.

假设 a_i 是序列 $a_0, a_1, \cdots, a_n$ 中第一个不能被 p 整除的系数，即 $p \mid a_0, p \mid a_1, \cdots, p \mid a_{i-1}$，但 $p \nmid a_i$.

又由 $g(x)$ 也是本原多项式，故 p 不能整除 $g(x)$ 的所有系数，即 $g(x)$ 至少有一个系数不能被 p 整除.

证明 用反证法. 假设 $h(x)$ 不是本原的, 即 $h(x)$ 的各项系数的最大公因数 $d > 1$,

那么一定存在一个素数 $p \mid d$, 即 p 为 $h(x)$ 的各项系数的一个公因数.

由 $f(x)$ 是本原多项式, 知 p 不能整除 $f(x)$ 的所有系数, 即 $f(x)$ 至少有一个系数不能被 p 整除.

假设 a_i 是数列 $a_0, a_1, \cdots, a_n$ 中第一个不能被 p 整除的系数, 即 $p \mid a_0, p \mid a_1, \cdots, p \mid a_{i-1}$, 但 $p \nmid a_i$.

又由 $g(x)$ 也是本原多项式, 故 p 不能整除 $g(x)$ 的所有系数, 即 $g(x)$ 至少有一个系数不能被 p 整除.

设 b_j 是数列 $b_0, b_1, \cdots, b_m$ 中第一个不能被 p 整除的系数, 即 $p \mid b_0, p \mid b_1, \cdots, p \mid b_{j-1}$, 但 $p \nmid b_j$.

证明 用反证法. 假设 $h(x)$ 不是本原的, 即 $h(x)$ 的各项系数的最大公因数 $d > 1$,

那么一定存在一个素数 $p \mid d$, 即 p 为 $h(x)$ 的各项系数的一个公因数.

由 $f(x)$ 是本原多项式, 知 p 不能整除 $f(x)$ 的所有系数, 即 $f(x)$ 至少有一个系数不能被 p 整除.

假设 a_i 是数列 $a_0, a_1, \cdots, a_n$ 中第一个不能被 p 整除的系数, 即 $p \mid a_0, p \mid a_1, \cdots, p \mid a_{i-1}$, 但 $p \nmid a_i$.

又由 $g(x)$ 也是本原多项式, 故 p 不能整除 $g(x)$ 的所有系数, 即 $g(x)$ 至少有一个系数不能被 p 整除.

设 b_j 是数列 $b_0, b_1, \cdots, b_m$ 中第一个不能被 p 整除的系数, 即 $p \mid b_0, p \mid b_1, \cdots, p \mid b_{j-1}$, 但 $p \nmid b_j$.

现在考虑 $h(x)$ 中 $i+j$ 次项系数

$$c_{i+j} = \sum_{s+t=i+j} a_s b_t = a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0.$$

因为 $p \mid c_{i+j}, p \mid a_0, a_1, \cdots, a_{i-1}, b_0, b_1, \cdots, b_{j-1}$, 所以 $p \mid a_i b_j$.

又 p 是一个素数, 故 $p \mid a_i$ 或 $p \mid b_j$, 矛盾. 从而 $h(x)$ 是一个本原多项式. ∎

定理 11

一个非零整系数多项式能分解成两个次数较低的有理系数多项式的乘积
$\Leftrightarrow$ 它能分解成两个次数较低的整系数多项式的乘积.

证明 $\Leftarrow$ 显然. $\Rightarrow$ 设 $f(x)$ 是一个非零整系数多项式, $f(x) = g(x)h(x)$, 其中 $g(x), h(x) \in \mathbb{Q}[x]$, 并且 $\max\{\deg g(x), \deg h(x)\} < \deg f(x)$. 令

$$f(x) = af_1(x), g(x) = sg_1(x), h(x) = rh_1(x),$$

其中 $a \in \mathbb{Z}, s, r \in \mathbb{Q}, f_1(x), g_1(x), h_1(x)$ 均为本原多项式. 则

$$f(x) = af_1(x) = srg_1(x)h_1(x),$$

即 $\frac{a}{sr}f_1(x) = g_1(x)h_1(x)$. 因为 $f_1(x), g_1(x), h_1(x)$ 都是本原多项式, 由 Gauss 引理, $g_1(x)h_1(x)$ 也是一个本原多项式, 所以 $\frac{a}{sr} = \pm 1$, 即 $sr = \pm a$, 故 sr 是一个非零整数. 从而

$$f(x) = srg_1(x)h_1(x) = [srg_1(x)]h_1(x),$$

即 $f(x)$ 可以分解为两个次数都比它低的的整系数多项式的乘积. ∎

此定理的证明过程中充分体现了 Gauss 引理的重要性.

定理 11

一个非零整系数多项式能分解成两个次数较低的有理系数多项式的乘积
$\Leftrightarrow$ 它能分解成两个次数较低的整系数多项式的乘积.

若某整系数多项式能分解为两个低次数的有理系数多项式的乘积，则其分解式的系数可全取整数.

由此可得, 非零整系数多项式 $f(x)$ 在有理数域 $\mathbb{Q}$ 上可约 $\Leftrightarrow f(x)$ 在整数环 $\mathbb{Z}$ 上可约.

推论

如果非零整系数多项式 $f(x) = g(x)h(x)$, 其中 $g(x)$ 是一个本原多项式, 那么 $h(x)$ 一定是一个整系数多项式.

证明　因为 $g(x)$ 是一个本原多项式, 故在定理 11 的证明过程中, $s = \pm 1$. 那么 $r = \pm a$ 是一个非零整数.

从而 $h(x) = rh_1(x) = \pm ah_1(x)$ 是一个整系数多项式. ∎

定理 12

- 如果有理数 $\frac{r}{s}$ (其中 s, r 互素) 是整系数多项式
$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
的一个有理根，则必有 $s \mid a_n, r \mid a_0$.
- 特别地，当 $a_n = 1$ 时，有理根一定是整数根.

证明 因为有理数 $\frac{r}{s}$ 是 $f(x)$ 的一个有理根且 $(r, s) = 1$.

由根与一次因式的关系知，在有理数域 $\mathbb{Q}$ 上，$(x - \frac{r}{s}) \mid f(x)$，那么 $(sx - r) \mid f(x)$.

故存在 $g(x) \in \mathbb{Q}[x], f(x) = (sx - r)g(x)$，但 $sx - r$ 是一个本原多项式，

那么由定理 11 的推论得知，$g(x)$ 是一个整系数多项式.

定理 12

- 如果有理数 $\frac{r}{s}$ (其中 s, r 互素) 是整系数多项式
$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
的一个有理根，则必有 $s \mid a_n, r \mid a_0$.
- 特别地，当 $a_n = 1$ 时，有理根一定是整数根.

设
$$g(x) = b_{n-1} x^{n-1} + \cdots + b_1 x + b_0,$$
其中 $b_i \in \mathbb{Z}, i = 0, 1, \ldots, n-1$, 则
$$f(x) = (sx - r)(b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) = s b_{n-1} x^n + \cdots - r b_0.$$
比较首项与常数项的系数，可得 $a_n = s b_{n-1}, a_0 = -r b_0$，从而 $s \mid a_n, r \mid a_0$.

又
$$f(x) = (sx - r) g(x) = (x - \frac{r}{s})[s \cdot g(x)] = (x - \frac{r}{s}) f_1(x),$$
因此，$f_1(x)$ 是一个整系数多项式. ∎

推论

首项系数为 1 的整系数多项式 $f(x)$ 若有有理根，则必为整数根.

设整系数多项式 $f(x)$ 有有理根 $\frac{r}{s}$ (其中 $(r,s)=1$). 因为 $s \mid 1$, 所以 $s=\pm 1$. 故 $\frac{r}{s}=\pm r \in \mathbb{Z}$.

推论

整系数多项式的整数根必为常数项的因数.

例 1

证明多项式 $f(x)=x^3-x+2$ 在有理数域上不可约.

推论

首项系数为 1 的整系数多项式 $f(x)$ 若有有理根, 则必为整数根.

设整系数多项式 $f(x)$ 有有理根 $\frac{r}{s}$ (其中 $(r,s)=1$). 因为 $s \mid 1$, 所以 $s=\pm 1$. 故 $\frac{r}{s}=\pm r \in \mathbb{Z}$.

推论

整系数多项式的整数根必为常数项的因数.

例 1

证明多项式 $f(x)=x^3-x+2$ 在有理数域上不可约.

证明 若 $f(x)$ 在有理数域上可约，则它至少有一个一次因式，也就是说，$f(x)$ 有一个有理根.

但是，$f(x)$ 的有理根只可能是 $\pm 1, \pm 2$. 直接验算可知，$\pm 1, \pm 2$ 都不是 $f(x)$ 的根.

故 $f(x)$ 在有理数域上不可约. ∎

注记

设 $f(x)$ 是有理系数多项式.

(1) 当 $\deg f(x)=1$ 时，$f(x)$ 在有理数域上不可约，但是 $f(x)$ 有有理根.

(2) 若 $2\leqslant \deg f(x)\leqslant 3$ ，则 $f(x)$ 在有理数域上不可约 $\Leftrightarrow$ $f(x)$ 没有有理根.

(3) 当 $\deg f(x)>3$ 时，如果 $f(x)$ 在有理数域上不可约，那么 $f(x)$ 没有有理根.

反之不然.

注记

设 $f(x)$ 是有理系数多项式.

(1) 当 $\deg f(x)=1$ 时，$f(x)$ 在有理数域上不可约，但是 $f(x)$ 有有理根.

(2) 若 $2 \leqslant \deg f(x) \leqslant 3$ ，则 $f(x)$ 在有理数域上不可约 $\Leftrightarrow$ $f(x)$ 没有有理根.

(3) 当 $\deg f(x)>3$ 时，如果 $f(x)$ 在有理数域上不可约，那么 $f(x)$ 没有有理根.

反之不然. 这是因为 $f(x)$ 没有有理根，只能说 $f(x)$ 没有一次因式，但是 $f(x)$ 可能有次数大于 1 的因式，$f(x)$ 可能是可约的. 例如，$\left(x^2+1\right)^2$ 没有有理根，但是它在有理数域上是可约的!

例 2

求多项式 $f(x) = 2x^4 - 2x^3 - 9x^2 - 8x - 3$ 的有理根.

例 2

求多项式 $f(x)=2x^4-2x^3-9x^2-8x-3$ 的有理根.

解 因为 2 的所有因数为 $\pm1,\pm2$, 且 -3 的所有因数为 $\pm1,\pm3$, 那么 $f(x)$ 的有理根必在

$$\{\pm1,\pm3,\pm\frac{1}{2},\pm\frac{3}{2}\}.$$

经检验, -1 和 3 是 $f(x)$ 的有理根, 且

$$f(x)=(x+1)(x-3)(2x^2+2x+1).$$

例 3

求多项式 $f(x)=6x^3-22x^2+16x+8$ 的有理根.

例 2

求多项式 $f(x) = 2x^4 - 2x^3 - 9x^2 - 8x - 3$ 的有理根.

解 因为 2 的所有因数为 $\pm1, \pm2$, 且 -3 的所有因数为 $\pm1, \pm3$, 那么 $f(x)$ 的有理根必在

$$\{\pm1, \pm3, \pm\frac{1}{2}, \pm\frac{3}{2}\}.$$

经检验, -1 和 3 是 $f(x)$ 的有理根, 且

$$f(x) = (x+1)(x-3)(2x^2+2x+1).$$

例 3

求多项式 $f(x) = 6x^3 - 22x^2 + 16x + 8$ 的有理根.

解 $f(x) = 2(3x^3 - 11x^2 + 8x + 4)$. 因为 3 的所有因数为 $\pm1, \pm3$, 且 4 的所有因数为 $\pm1, \pm2, \pm4$, 那么 $f(x)$ 的有理根必在

$$\{\pm1, \pm2, \pm4, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}\}.$$

经检验, -1 和 3 是 $f(x)$ 的有理根, 且 $f(x) = 2(3x+1)(x-2)^2$. 因此, $f(x)$ 所有的有理根为 $-\frac{1}{3}, 2, 2$.

例 2

求多项式 $f(x) = 2x^4 - 2x^3 - 9x^2 - 8x - 3$ 的有理根.

解 因为 2 的所有因数为 $\pm1, \pm2$, 且 -3 的所有因数为 $\pm1, \pm3$, 那么 $f(x)$ 的有理根必在

$$\{\pm1, \pm3, \pm\frac{1}{2}, \pm\frac{3}{2}\}.$$

经检验, -1 和 3 是 $f(x)$ 的有理根, 且

$$f(x) = (x+1)(x-3)(2x^2+2x+1).$$

例 3

求多项式 $f(x) = 6x^3 - 22x^2 + 16x + 8$ 的有理根.

解 $f(x) = 2(3x^3 - 11x^2 + 8x + 4)$. 因为 3 的所有因数为 $\pm1, \pm3$, 且 4 的所有因数为 $\pm1, \pm2, \pm4$, 那么 $f(x)$ 的有理根必在

$$\{\pm1, \pm2, \pm4, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}\}.$$

经检验, -1 和 3 是 $f(x)$ 的有理根, 且 $f(x) = 2(3x+1)(x-2)^2$. 因此, $f(x)$ 所有的有理根为 $-\frac{1}{3}, 2, 2$.

例 4

设 p 是一个奇素数，证明多项式 $f(x) = x^3 - px + 1$ 在有理数域上不可约.

例 4

设 p 是一个奇素数，证明多项式 $f(x)=x^3-px+1$ 在有理数域上不可约.

证明 用反证法. 假若 $f(x)=x^3+px+1$ 在有理数域 $\mathbb{Q}$ 上可约，则 $f(x)$ 必能分解成一个一次式与一个二次式的乘积，从而 $f(x)$ 有有理根，那么 $f(x)$ 的有理根只能在 $\{\pm 1\}$ 中，但

$$f(1)=2+p\neq 0, f(-1)=p\neq 0,$$

矛盾. 故 $f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约. ∎

思考

当 b 取何值时，整系数多项式 $f(x)=x^3+bx+1$ 在 $\mathbb{Q}$ 上可约?

例 4

设 p 是一个奇素数，证明多项式 $f(x) = x^3 - px + 1$ 在有理数域上不可约.

证明 用反证法. 假若 $f(x) = x^3 + px + 1$ 在有理数域 $\mathbb{Q}$ 上可约，则 $f(x)$ 必能分解成一个一次式与一个二次式的乘积，从而 $f(x)$ 有有理根，那么 $f(x)$ 的有理根只能在 $\{\pm 1\}$ 中，但

$$f(1) = 2 + p \neq 0, f(-1) = p \neq 0,$$

矛盾. 故 $f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约. ∎

思考

当 b 取何值时，整系数多项式 $f(x) = x^3 + bx + 1$ 在 $\mathbb{Q}$ 上可约?

因为 $f(1) = 2 + b$, $f(-1) = -b$,

所以只有当 $b = -2$ 或 $b = 0$ 时，$f(x) = x^3 - bx + 1$ 在有理数域上才可约.

三、有理系数多项式不可约判别法

定理 13 (Eisenstein 判别法)

对于一个非零整系数多项式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

如果存在一个素数 p，使得

(1) $p \nmid a_n$，(2) $p \mid a_{n-1}, a_{n-2}, \cdots, a_1, a_0$，(3) $p^2 \nmid a_0$，

则 $f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约.

证明 用反证法. 假设 $f(x)$ 在有理数域 $\mathbb{Q}$ 上可约. 于是，$f(x)$ 可分解成两个次数较低的整系数多项式的乘积：$f(x) = g(x)h(x)$，其中 $g(x), h(x) \in \mathbb{Z}[x]$，且

$$\max\{\deg g(x), \deg h(x)\} < \deg f(x).$$

设
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0,$$
$$h(x)=c_lx^l+c_{l-1}x^{l-1}+\cdots+c_1x+c_0,$$
则
$$f(x)=(b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0)(c_lx^l+c_{l-1}x^{l-1}+\cdots+c_1x+c_0).$$

那么 $a_n=b_mc_l, a_0=b_0c_0$. 因为 $p\mid a_0$, 即 $p\mid b_0c_0$, 而 p 是一个素数, 故 $p\mid b_0$ 或 $p\mid c_0$.

但 $p^2\nmid a_0$, 从而 p 不能同时整除 b_0 和 c_0. 设 $p\mid b_0$, 但 $p\nmid c_0$.

又因为 $p\nmid a_n$, 即 $p\nmid b_mc_l$, 所以 $p\nmid b_m$, 从而 p 不能同时整除 $g(x)$ 的各项系数.

假设 b_k 是 $b_0,b_1,\cdots,b_m$ 中第一个不能被 p 整除的系数,

即 $p\mid b_0,b_1,\cdots,b_{k-1}$, 但 $p\nmid b_k$ (显然 $k\le m$).

考察 $f(x)$ 的 k 次项系数
$$a_k=b_0c_k+b_1c_{k-1}+\cdots+b_kc_0,$$

由 $p\mid a_k, p\mid b_0,b_1,\cdots,b_{k-1}$, 那么 $p\mid b_kc_0$. 而 p 为一个素数, 故 $p\mid b_k$ 或 $p\mid c_0$, 矛盾.

从而 $f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约. ∎

Eisenstein 判别法

对于一个非零整系数多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

如果存在一个素数 p, 使得

$(1)\ p \nmid a_n,\ (2)\ p \mid a_{n-1}, a_{n-2}, \cdots, a_1, a_0,\ (3)\ p^2 \nmid a_0,$

则 $f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约.

说明

- 由 Eisenstein 判别法可知, 在有理数域 $\mathbb{Q}$ 上存在任意次数的不可约多项式.
  如 $x^n + 2$, 取 $p = 2$, 由 Eisenstein 判别法, 它在有理数域 $\mathbb{Q}$ 上不可约.
- Eisenstein 判别法的局限性: 此法并非对一切整系数多项式都适用, 因为满足定理的素数 p 不总是存在. 若找不到适当的素数 p, 则 $f(x)$ 的可约性就无法确定. 如 $x^2 + 3x + 2$, $x^2 + 1$ 都找不到满足条件的素数 p, 但前者在有理数域 $\mathbb{Q}$ 上可约, 后者不可约. 故它的逆不真.
- 对于有些多项式 $f(x)$ 来说, 有时它不能直接应用 Eisenstein 判别法, 但适当变形后就可以应用 Eisenstein 判别法. 此时一般是作一次变换.

例 5

设 p 是一个素数，则本原多项式

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

在有理数域 $\mathbb{Q}$ 上不可约.

例 5

设 p 是一个素数，则本原多项式

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

在有理数域 $\mathbb{Q}$ 上不可约.

证明 令 $x = y + 1$. 因为 $f(x) = \frac{x^p - 1}{x - 1}$，所以

$$g(y) = f(y+1) = \frac{(y+1)^p - 1}{y} = \frac{y^p + C_p^1 y^{p-1} + \cdots + C_p^{p-1} y}{y} = y^{p-1} + C_p^1 y^{p-2} + \cdots + C_p^{p-1}.$$

对素数 p 用 Eisenstein 判别法，因为

(1) $p \nmid 1$，(2) $C_p^i = \frac{p(p-1)\cdots(p-i+1)}{i!}$ 可被 p 整除，$i = 1, 2, \cdots, p-1$，(3) $p^2 \nmid C_p^{p-1} = p$，

故 $g(y)$ 在有理数域 $\mathbb{Q}$ 上不可约. 那么 $f(x)$ 在有理数域 $\mathbb{Q}$ 上也不可约.

否则，存在 $h_1(x), h_2(x) \in Q[x]$，使得

$$f(x) = h_1(x)h_2(x), \deg h_i(x) < \deg f(x), i = 1, 2,$$

那么 $g(y) = f(y+1) = h_1(y+1)h_2(y+1)$，故 $g(y)$ 在有理数域 $\mathbb{Q}$ 上可约，矛盾.

Eisenstein 判别法是针对整系数多项式的，那么如何判断有理系数多项式的可约性呢?

——首先把 $f(x)$ 写成一个有理数与一个本原多项式的乘积 $f(x)=a\varphi(x)$，再判断 $\varphi(x)$ 的可约性.

例 6

$f(x)=2x^4+\frac{8}{3}x^3+\frac{4}{3}x^2+\frac{16}{15}x-\frac{4}{5}=\frac{2}{15}(15x^4+20x^3+10x^2+8x-6)=\frac{2}{15}\varphi(x)$,

取 $p=2$，则 (1) $p\nmid 15$，(2) $p\mid 20,10,8,(-6)$，(3) $p^2\nmid(-6)$,

故由 *Eisenstein* 判别法可知，$f(x)$ 在有理数域 $\mathbb{Q}$ 上不可约.