第一章　多项式

1.1　集合

定义 1.1.1. **集合**是指具有某种特定性质的具体的或抽象的对象汇总而成的集体, 这些对象称为该集合的**元素**.

- 设 S 为集合, 则记 $x \in S$ 表示 x 为集合 S 的元素; 记 $y \notin S$ 表示 y 不是集合 S 的元素.
- 设 A, B 为集合, 记 $A \subseteq B$ 表示集合 A 中的任意元素都是集合 B 的元素. 如果 $A \subseteq B$ 且 $B \subseteq A$, 那么我们称集合 A 与 B **相等**, 记为 $A = B$.
- 记 $A \cap B := \{x \mid x \in A \text{ 且 } x \in B\}$ 表示集合 A 与集合 B 的**交**. 记 $A \cup B := \{x \mid x \in A \text{ 或 } x \in B\}$ 表示集合 A 与集合 B 的**并**. 类似地, 我们可以定义任意多个集合的交与并.
- 记 $\emptyset$ 表示**空集**, 此集合不包含任意元素.

例 1.1.1. 在数学上, 我们总是用 $\mathbb{N}$ 表示自然数集合 (包括 0); $\mathbb{Z}$ 表示整数集合; $\mathbb{Q}$ 表示有理数集合; $\mathbb{R}$ 表示实数集合; $\mathbb{C}$ 表示复数集合. 显然, 我们有

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

定义 1.1.2 (笛卡尔积)**.** 设 M, N 为集合, 定义集合

$$M \times N := \{(m, n) \mid \forall m \in M, n \in N\}.$$

称集合 $M \times N$ 为集合 M 与集合 N 的**笛卡尔积**. 特别地, 集合 $M \times N$ 的元素为二元有序元素对, 其中第一个分量元素来自集合 M, 第二个分量元素来自集合 N.

注记 1.1.1. 一般地, $M \times N \neq N \times M$.

定义 1.1.3 (映射)**.** 集合 M 到集合 N 的 **映射** 或 **函数** $f : M \longrightarrow N$ 是指笛卡尔积 $M \times N$ 的一个子集 G, 满足对任意的 $m \in M$, 存在唯一的 $n \in N$ 使得 $(m, n) \in G$. 此时我们一般记 $n = f(m)$ 并记映射 f 为

$$\begin{aligned} f : \ M &\longrightarrow N \\ m &\mapsto f(m). \end{aligned}$$

称集合 G 为映射 f 的**图像**.

设 $f : M \longrightarrow N$ 和 $g : M \longrightarrow N$ 为映射.

- 称映射 f 与 g **相等**, 如果对任意的 $m \in M$, $f(m) = g(m)$. 此时记为 $f = g$.
- 称映射 f 为**单射**, 如果对任意的 $m_1, m_2 \in M$ 满足 $f(m_1) = f(m_2)$, 那么有 $m_1 = m_2$ 成立.
- 称映射 f 为**满射**, 如果对任意的 $n \in N$, 存在 $m \in M$ 使得 $f(m) = n$.
- 称映射 f 为**双射**, 如果 f 即是单射又是满射.

例 1.1.2. 设 M 为非空集合. 记

$$\begin{aligned} \mathrm{id}_M : \quad M &\longrightarrow M \\ m &\mapsto m \end{aligned}$$

表示集合 M 上的**恒等映射**. 显然, 恒等映射为双射.

例 1.1.3. 记 $\mathbb{Z}$ 表示整数集合. 利用笛卡尔集及映射我们将 $\mathbb{Z}$ 上的加法 $+$ 与乘法 $\times$ 表示为映射的形式如下:

$$\begin{aligned} + : \quad \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} & \times : \quad \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (m, n) &\longmapsto m + n & (m, n) &\longmapsto mn \end{aligned}$$

一般地, 设 M 为非空集合, 我们称任意的映射 $f : M \times M \longrightarrow M$ 为集合 M 上的一个**运算**.

练习 1.1.1. 设集合 M 只有有限多个元素. 设 $f : M \longrightarrow M$ 为映射. 证明: f 是双射当且仅当 f 是单射当且仅当 f 是满射.

定义 1.1.4 (映射的复合**).** 设 $f : L \longrightarrow M$ 和 $g : M \longrightarrow N$ 为映射, 称映射

$$\begin{aligned} g \circ f : \quad L &\longrightarrow N \\ l &\mapsto g(f(l)) \end{aligned}$$

为映射 f 与 g 的 **复合** 或 **合成**.

命题 1.1.1 (映射复合的结合律**).** 设 $f : X \longrightarrow Y, g : Y \longrightarrow Z, h : Z \longrightarrow W$ 为映射, 则

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

练习 1.1.2. 设 $f : L \longrightarrow M, g : M \longrightarrow N$ 为映射. 证明:

1. 若 $g\circ f$ 为单射, 则 f 为单射;

2. 若 $g\circ f$ 为满射, 则 g 为满射;

3. $f:L\longrightarrow M$ 为双射当且仅当存在映射 $h:M\longrightarrow L$ 使得

$$f\circ h=\mathrm{id}_M \text{ 且 } h\circ f=\mathrm{id}_L.$$

进一步地, h 是唯一的且也是双射, 称为映射 f 的**逆映射**, 记为 $h=f^{-1}$.

练习 1.1.3. 设 $f:M\longrightarrow N, g:N\longrightarrow M$ 为映射. 举例说明

(1) 映射 $g\circ f$ 是单射, 但映射 g 不是单射;

(2) 映射 $g\circ f$ 是满射, 但映射 f 不是满射;

(3) 映射 $g\circ f=\mathrm{id}_M$, 但 f 不是双射.

1.2 整数

我们将从整数的加法与乘法运算的基本性质 (交换律、结合律、分配律、消去律等) 以及整数上存在全序 (任意两个整数可比较大小) 出发, 证明算术基本定理. 我们还需要用到

数学归纳原理. 设 $P(n)$ 是与自然数 n 有关的一个性质. 假设 $P(0)$ 成立, 并假设只要 $P(n)$ 成立, 则 $P(n+1)$ 也成立. 那么对于每个自然数 $m\in\mathbb{N}$, $P(m)$ 都成立.

第二数学归纳法. 设 $Q(n)$ 是与自然数 n 有关的一个性质, m_0 是一个自然数. 假设 $Q(m_0)$ 成立, 并假设只要对每个 $m_0\le m<n$ 都有 $Q(m)$ 成立, 则 $Q(n)$ 也成立. 那么 $Q(m)$ 对于一切自然数 $m\ge m_0$ 都成立.

1.2.1 整除

定义 1.2.1. 设 $a,b\in\mathbb{Z}$, 如果存在 $q\in\mathbb{Z}$ 使得 $a=bq$, 那么称 b **整除** a, 或者 b 为 a 的 **因子**. 记为 $b|a$, 此时我们也称 a 为 b 的**倍数**. 反之则称 b **不整除** a, 记为 $a\nmid b$.

注记 1.2.1. 在经典数论中, 我们一般要求除数 $b\neq 0$.

例 1.2.1. (1) 对任意的 $a\in\mathbb{Z}$, $a|0$;

(2) 对任意的 $a\in\mathbb{Z}$, $\pm1|a, \pm a|a$, 称 ±1 及 $\pm a$ 为整数 a 的**平凡因子**;

(3) 设 $a,b\in\mathbb{Z}$ 且 $a\neq 0$, 若 $b|a$, 则 $|b|\le|a|$;

(4) 设 $a,b,c\in\mathbb{Z}$ 且 $a\mid b, a\mid c$, 则对任意的整数 k,l, $a\mid kb+lc$;

(5) 已知 a,b 为正整数, 则 $a=b$ 当且仅当 $a \mid b$ 且 $b \mid a$.

定义 1.2.2. 设 $a,b,c \in \mathbb{Z}$. 如果 $c|a$ 且 $c|b$, 那么称 c 为 a 与 b 的**公因子**.

设 $a,b \in \mathbb{Z}$ 不全为零, 如果存在 $1 \leq d \in \mathbb{Z}$ 使得 $d|a$ 及 $d|b$ 且满足对任意的 a 与 b 的公因子 c, 都有 $c|d$, 那么称 d 为 a 与 b 的**最大公因子**, 此时记为 $d=\gcd(a,b)=(a,b)$. 我们约定 $(0,0)=0$.

注记 1.2.2. 上述定义并未保证对任意的 $a,b \in \mathbb{Z}$, a 与 b 的最大公因子 (a,b) 一定存在. 但容易证明: 如果 (a,b) 存在则唯一且为 a 与 b 的公因子中的最大数. 另一方面, 对于某些特殊的 a,b, 由上述定义可以直接判断出其最大公因子存在, 如 $(b,0)=|b|$.

定理 1.2.1 (带余除法). 对任意的 $a,b \in \mathbb{Z}$ 且 $b \neq 0$, 存在唯一的 $q,r \in \mathbb{Z}$ 且 $0 \leq r < |b|$ 使得

$$a=bq+r,$$

其中 q 称为 a 除以 b 的**商**, r 称为 a 除以 b 的**最小非负剩余项**.

引理 1.2.2. 设 $S \subset \mathbb{Z}$ 且存在 $0<a \in S$, 则存在 $x \in S$ 使得 $0<x$ 且对任意的 $0<b \in S$, 有 $x \leq b$. 特别地, x 为集合 S 中最小的正整数.

定理 1.2.3 (最大公因子的存在性). 设 $a,b \in \mathbb{Z}$ 不全为零, 则 a,b 的最大公因子存在.

推论 1.2.4. 设 $a,b \in \mathbb{Z}$ 不全为零, 则 a 与 b 的最大功因子为集合 $S=\{ma+nb \mid m,n \in Z\}$ 中最小的正整数.

推论 1.2.5. 设 $a,b \in \mathbb{Z}$ 不全为零, $d \in \mathbb{Z}$, 则

$$d=(a,b) \Longleftrightarrow \begin{cases} d>0; \\ d|a, d|b; \\ \text{存在 } u,v \in \mathbb{Z} \text{ 使得 } d=ua+vb. \end{cases}$$

引理 1.2.6 (最大公因子的求解: 辗转相除法). 设 $a,b \in \mathbb{Z}$ 且 $b \neq 0$. 若 $a=bq+r$, 则 $(a,b)=(b,r)$.

例 1.2.2. 求 $(2018,118)$ 及整数 u,v 使得 $(2018,118)=2018u+118v$.

例 1.2.3. 设 $a,k \in \mathbb{Z}$. 证明: $(a,a+k) \mid k$.

注记 1.2.3. 设 $d=(a,b)$, 则存在无穷多组 $u,v \in \mathbb{Z}$ 使得 $d=ua+vb$.

练习 1.2.1. 设 $a_1,\cdots,a_t \in \mathbb{Z}$ 且不全为零. 若整数 $c \in \mathbb{Z}$ 满足 $c \mid a_i, \forall 1 \leq i \leq t$, 则称 c 为 $a_1,\cdots,a_t$ 的**公因子**. 如果存在正整数 d 为 $a_1,\cdots,a_t$ 的公因子且对任意的公因子 c 都有 $c \mid d$, 那么称 d 为 $a_1,\cdots,a_t$ 的**最大公因子**. 记为 $d=(a_1,\cdots,a_t)$.
证明: (1) 整数 $(\cdots((a_1,a_2),a_3),\cdots,a_t)$ 为 $a_1,\cdots,a_t$ 的最大公因子;

(2) d 为 $a_1, \cdots, a_t$ 的最大公因子当且仅当 $\begin{cases} d \geq 1; \\ d \mid a_i, \forall 1 \leq i \leq t; \\ \exists\, u_i \in \mathbb{Z},\ \text{使得}\ d = \sum_{i=1}^{t} u_i a_i. \end{cases}$

定义 1.2.3. 设 $a, b \in \mathbb{Z}$. 若 $(a, b) = 1$, 则称 a 与 b **互素**.

命题 1.2.7. 设 $a, b \in \mathbb{Z}$, 则 $(a, b) = 1$ 当且仅当存在 $u, v \in \mathbb{Z}$ 使得 $1 = ua + vb$.

推论 1.2.8. 设 $a, b, c \in \mathbb{Z}$ 满足 $a \mid bc$ 且 $(a, b) = 1$, 则 $a \mid c$.

练习 1.2.2. 设 $a, b \in \mathbb{Z}$ 不全为零, $u_0, v_0 \in \mathbb{Z}$ 使得 $(a, b) = u_0 a + v_0 b$. 试求所有的 $u, v \in \mathbb{Z}$ 使得 $(a, b) = ua + vb$.

练习 1.2.3. 是否存在整数 x 使得 x 除以 5 的余数为 2, x 除以 7 的余数为 3? 若存在, 试求满足上述条件最小的正整数 x.

1.2.2 素数与算术基本定理

定义 1.2.4. 设 $p \in \mathbb{N}$ 且 $p > 1$. 如果 p 没有非平凡因子, 那么称 p 为**素数**.

引理 1.2.9. 设 $p \in \mathbb{N}$ 为素数.

(1) 对任意的 $a \in \mathbb{Z}$, $p|a$ 或者 $(p, a) = 1$;

(2) 对任意的 $a, b \in \mathbb{Z}$, 若 $p|ab$, 则 $p|a$ 或者 $p|b$;

(3) 对任意的 $a_1, \cdots, a_t \in \mathbb{Z}$, 若 $p|a_1 a_2 \cdots a_t$, 则存在 $1 \leq i \leq t$ 使得 $p|a_i$.

注记 1.2.4. 事实上可以证明上述引理中的 (1) 与 (2) 与 p 是素数等价.

定理 1.2.10 (算术基本定理). 对任意的 $a \in \mathbb{N}$ 且 $a > 1$, 存在素数 $p_1, \cdots, p_t$ 使得

$$a = p_1 p_2 \cdots p_t;$$

若还存在素数 $q_1, q_2, \cdots, q_s$ 也满足 $a = q_1 q_2 \cdots q_s$, 则 $t = s$ 且经过适当的重新编号后有 $p_i = q_i, i = 1, \cdots, t$.

推论 1.2.11. 素数有无穷多个.

注记 1.2.5. 由算术基本定理知, 任意大于 1 的整数 n 存在两两不等的素数 $p_1, \cdots, p_t$ 及一组大于或等于 1 的整数 $r_1, \cdots, r_t$ 使得

$$n = \prod_{i=1}^{t} p_i^{r_i} := p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}.$$

上述表达式称为整数 n 的**标准分解式**.

1.3 数域

1.3.1 复数

作为集合我们有 $\mathbb{C}=\{a+ib \mid a,b\in\mathbb{R}\}$, 其中 i 满足 $i^2=-1$, 称为**虚数单位**. 对任意的复数 $\alpha=a+ib$, 记 $\overline{\alpha}:=a-ib$, 称 $\overline{\alpha}$ 为复数 α 的**共轭**; 称非负实数 $|\alpha|:=\sqrt{a^2+b^2}$ 为复数 α 的**模长**.

引理 1.3.1. 设 $\alpha,\beta\in\mathbb{C}$.

1. $\alpha=0$ 当且仅当 $|\alpha|=0$;
2. $|\alpha|=|\overline{\alpha}|$;
3. $|\alpha\beta|=|\alpha||\beta|$;
4. $|\alpha|^2=\alpha\overline{\alpha}$.

设 $\alpha=a+ib\in\mathbb{C}$, 存在唯一的 $\theta\in[0,2\pi)$ 使得 $\cos\theta=\frac{a}{|\alpha|},\sin\theta=\frac{b}{|\alpha|}$, 称 θ 为复数 α 的**辐角**. 利用乘法可将 α 表示为

$$\alpha=|\alpha|(\cos\theta+i\sin\theta):=|\alpha|e^{i\theta},$$

称上述表达式为复数 α 的**指数形式**.

命题 1.3.2 (De Moivre)**.** 设 $\alpha=r_1e^{i\theta_1},\beta=r_2e^{i\theta_2}\in\mathbb{C}$, 其中 r_1,r_2 为非负实数.

(a) $\alpha\beta=r_1r_2e^{i(\theta_1+\theta_2)}$;

(b) 对任意的正整数 n, $\alpha^n=r_1^ne^{in\theta_1}$.

1.3.2 数域

定义 1.3.1. 设 $\mathbb{F}$ 为复数 $\mathbb{C}$ 的非空子集, 称 $\mathbb{F}$ 为**数域**, 如果 $\mathbb{F}$ 满足下列条件

(a) $1\in\mathbb{F}$;

(b) $\forall\, a,b\in\mathbb{F}, a\pm b\in\mathbb{F}, ab\in\mathbb{F}$;

(c) $\forall\, a,b\in\mathbb{F}$ 且 $b\neq0$, $\frac{a}{b}\in\mathbb{F}$.

例 1.3.1. (1) $\mathbb{Q},\mathbb{R},\mathbb{C}$ 为数域;

(2) $\mathbb{Q}$ 为最小数域, 特别地, 若 $\mathbb{F}$ 为数域, 则 $\mathbb{Q}\subset\mathbb{F}$;

练习 1.3.1. 设 $\mathbb{F}$ 为复数 $\mathbb{C}$ 的非空子集. 记 $(a1)$:$\mathbb{F}$ 中至少有两个不同的元素; $(c1):\forall\, 0\neq b\in\mathbb{F}$, 有 $b^{-1}\in\mathbb{F}$. 证明: $\mathbb{F}$ 为数域当且仅当 $\mathbb{F}$ 满足条件 $(a1)+(b)+(c)$ 当且仅当 $\mathbb{F}$ 满足条件 $(a)+(b)+(c1)$.

练习 1.3.2. 设 $\mathbb{F}=\{a+b\sqrt{2}|a,b\in\mathbb{Q}\}$. 证明: $\mathbb{F}$ 为数域.

练习 1.3.3. 设 $R_1=\{a+b\sqrt{2}|a,b\in\mathbb{Q}\}, R_2=\{a+b\sqrt{3}|a,b\in\mathbb{Q}\}$. 求 $\mathbb{C}$ 中包含 $R_1\cup R_2$ 的最小的数域.

练习 1.3.4. 设 $\mathbb{F}$ 为数域且 $\mathbb{R}\subseteq\mathbb{F}\subseteq\mathbb{C}$. 证明: $\mathbb{F}=\mathbb{R}$ 或者 $\mathbb{F}=\mathbb{C}$.

1.4 一元多项式

1.4.1 一元多项式的基本概念

定义 1.4.1. 设 $\mathbb{F}$ 为数域, $n\in\mathbb{N}$, x 为不定元或形式变量. 称形式表达式

$$f(x):=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=\sum_{i=0}^{n}a_ix^i,\ \text{其中 } a_i\in\mathbb{F},$$

为数域 $\mathbb{F}$ 上的**一元多项式**.

称 a_ix^i 为多项式 $f(x)$ 的**第 i 次项**, a_i 为多项式 $f(x)$ 的**第 i 次项系数**.

称 a_0 为多项式 $f(x)$ 的**零次项或常数项**.

若 $a_n\neq0$, 则称 a_nx^n 为多项式 $f(x)$ 的**首项**, a_n 为多项式 $f(x)$ 的**首项系数**. 此时称 $f(x)$ 为 n **次多项式**, 记为 $\deg f(x)=\partial f(x)=n$. 若 $a_n=1$, 则称多项式 $f(x)$ 为**首一的**.

若 $f(x)=c\in\mathbb{F}$, 则称 $f(x)$ 为**常数多项式**. 当 $c\neq0$ 时, $\deg f(x)=0$.

若多项式 $f(x)$ 的所有次项的系数都为零, 则称 $f(x)$ 为**零多项式**, 记为 **0**. 约定 $\deg 0=-\infty$.

设 $f(x),g(x)$ 都是 $\mathbb{F}$ 上的多项式, 称 $f(x)$ 与 $g(x)$ **相等** (记为 $f(x)=g(x)$), 如果除系数为零的次项外, $f(x)$ 与 $g(x)$ 的同次项的系数两两相等.

例 1.4.1. 设 $f(x)=x+1, g(x)=0x^3+0x^2+x+1$, 根据相等的定义有 $f(x)=g(x)$.

注记 1.4.1. 我们约定 $-\infty+(-\infty)=-\infty$; $-\infty+n=-\infty$, 对任意的 $n\in\mathbb{Z}$.

1.4.2 多项式的运算

设 $\mathbb{F}$ 为数域, 记 $\mathbb{F}[x]$ 表示数域 $\mathbb{F}$ 的所有以 x 为形式变量的一元多项式构成的集合. 我们定义 $\mathbb{F}[x]$ 上的**加法**运算如下:

$$\begin{aligned}+:\ \mathbb{F}[x]\times\mathbb{F}[x]\ &\longrightarrow\mathbb{F}[x]\\ (f(x),g(x))\ &\mapsto f(x)+g(x)\end{aligned}$$

若 $f(x)=\sum\limits_{i=0}^{n}a_ix^i,\ g(x)=\sum\limits_{j=0}^{m}b_jx^j\in\mathbb{F}[x]$, 则

$$f(x)+g(x):=\sum_{k=0}^{m}(a_k+b_k)x^k,$$

其中如果 $m \leq n$, 那么我们令 $b_n = b_{n-1} = \cdots = b_{n+1} = 0$.

事实 . 设 $f(x), g(x), h(x)$ 为数域 $\mathbb{F}$ 上的多项式.

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

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

(3) $f(x) + \mathbf{0} = f(x)$;

(4) 若 $f(x) = \sum_{i=0}^{n} a_i x^i$, 令 $-f(x) = \sum_{i=0}^{n} (-a_i) x^i$, 则 $f(x) + (-f(x)) = 0$.

注记 1.4.2. 上述定义的多项式的加法赋予了多项式定义中的形式符号 $+$ 真正的加法意义. 如 $f(x) = 2x^3 + 3x + 1, g(x) = 2x^3, h(x) = 3x, k(x) = 1$, 则 $f(x) = g(x) + h(x) + k(x)$.

我们定义 $\mathbb{F}[x]$ 上的**乘法**运算如下:

$$\begin{aligned} \times : \quad \mathbb{F}[x] \times \mathbb{F}[x] \quad &\longrightarrow \mathbb{F}[x] \\ (f(x), g(x)) \quad &\mapsto f(x) \times g(x) \end{aligned}$$

若 $f(x) = \sum\limits_{i=0}^{n} a_i x^i,\ g(x) = \sum\limits_{j=0}^{m} b_j x^j \in \mathbb{F}[x]$, 则

$$f(x) \times g(x) := \sum_{k=0}^{m+n} c_k x^k,$$

其中 $c_k = \sum_{i+j=k} a_i b_j$ 且 $1 \leq i \leq n, 1 \leq j \leq m$.

事实 . 设 $f(x), g(x), h(x)$ 为数域 $\mathbb{F}$ 上的多项式.

(1) $f(x)g(x) = g(x)f(x)$;

(2) $1 \times f(x) = f(x)$;

(3) $f(x) \times \mathbf{0} = \mathbf{0}$;

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

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

证明. 我们利用 (4) 来证明 (5). 首先证明,

断言 I: 对任意的 $0 \leq i, j \in \mathbb{N}$ 及 $a, b \in \mathbb{F}$, 有 $(ax^i \times bx^j) \times h(x) = ax^i \times (bx^j \times h(x))$.

设 $h(x) = \sum\limits_{k=1}^{l} c_k x^k$. 直接计算可知

$$\begin{aligned} LHS &= abx^{i+j} \times h(x) = abc_l x^{l+i+j} + abc_{l-1} x^{l+i+j-1} + \cdots + abc_1 x^{i+j+1} + abc_0 x^{i+j} \\ &= ax^i (bc_l x^{l+j} + bc_{l-1} x^{l+j-1} + \cdots + bc_1 x^{j+1} + bc_0 x^j) \\ &= RHS. \end{aligned}$$

利用断言 I 及 (4) 可以证明:

断言 II: 对任意的 $0 \leq j \in \mathbb{N}, b \in \mathbb{F}$, 有 $(f(x) \times bx^j) \times h(x) = f(x) \times (bx^j \times h(x))$.

设 $f(x) = \sum_{i=0}^{n} a_i x^i$. 由 (4) 知

$$f(x) \times bx^j = (a_n x^n + \cdots + a_1 x + a_0) \times bx^j = a_n x^n \times bx^j + \cdots a_1 x \times bx^j + a_0 \times bx^j.$$

代入 $(f(x) \times bx^j) \times h(x)$ 并利用 (4) 可得

$$\begin{aligned}
(f(x) \times bx^j) \times h(x) &= (a_n x^n \times bx^j + \cdots a_1 x \times bx^j + a_0 \times bx^j) \times h(x) \\
&= (a_n x^n \times bx^j) \times h(x) + \cdots + (a_0 \times bx^j) \times h(x) \\
&= a_n x^n \times (bx^j \times h(x)) + \cdots + a_0 \times (bx^j \times h(x)) \\
&= (a_n x^n + \cdots + a_1 x + a_0) \times (bx^j \times h(x)) \\
&= f(x) \times (bx^j \times h(x)),
\end{aligned}$$

其中第 $1, 2, 4$ 等式因为分配律 (4) 成立, 第 3 等式因为断言 I 成立.

下面我们证明多项式的乘法具有结合性, *i.e.* 等式 (5) 成立. 设 $g(x) = \sum_{j=0}^{m} b_j x^i$. 运用分配律 (4) 及断言 II, 我们有

$$\begin{aligned}
& (f(x) \times g(x)) \times h(x) \\
= \ & (f(x) \times (b_m x^m + \cdots + b_1 x + b_0)) \times h(x) \\
= \ & (f(x) \times b_m x^m + \cdots + f(x) \times b_1 x + f(x) \times b_0)) \times h(x) \\
= \ & (f(x) \times b_m x^m) \times h(x) + \cdots + (f(x) \times b_1 x) \times h(x) + (f(x) \times b_0) \times h(x) \\
= \ & f(x) \times (b_m x^m \times h(x)) + \cdots f(x) \times (b_1 x \times h(x)) + f(x) \times (b_0 \times h(x)) \\
= \ & f(x) \times (b_m x^m \times h(x) + \cdots b_1 x \times h(x) + b_0 \times h(x)) \\
= \ & f(x) \times ((b_m x^m + \cdots b_1 x + b_0) \times h(x)) \\
= \ & f(x) \times (g(x) \times h(x)),
\end{aligned}$$

其中第 $2, 3, 5, 6$ 等式因为分配律 (4) 成立, 第 (3) 等式因为断言 II 成立. □

推论 1.4.1. 设 $f(x), g(x)$ 为数域 $\mathbb{F}$ 上的多项式.

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

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

定义 1.4.2. 称 $(\mathbb{F}[x], +, \times)$ 为数域 $\mathbb{F}$ 上的**一元多项式环**.

命题 1.4.2 (乘法消去律). *(1)* 设 $f(x), g(x) \in \mathbb{F}[x]$. 证明: $f(x)g(x) = 0$ 当且仅当 $f(x) = 0$ 或者 $g(x) = 0$;

(2) 设 $f(x), g(x), h(x) \in \mathbb{F}[x]$ 且 $f(x) \neq 0$. 若 $f(x)g(x) = f(x)h(x)$, 则 $g(x) = h(x)$.

练习 1.4.1. 设 $f(x)$ 为实数 $\mathbb{R}$ 上的非零多项式且存在正整数 $k \in \mathbb{N}$ 使得 $f(f(x)) = f^k(x)$. 试求 $f(x) = ?$

1.4.3 多项式的整除

定义 1.4.3. 设 $f(x), g(x) \in \mathbb{F}[x]$, 若存在 $h(x) \in \mathbb{F}[x]$ 使得 $f(x) = g(x)h(x)$, 则称 $g(x)$ **整除** $f(x)$, 记为 $g(x)|f(x)$. 反之则称 $g(x)$ 不整除 $f(x)$, 记为 $g(x) \nmid f(x)$.

若 $g(x) \mid f(x)$, 则称 $g(x)$ 为 $f(x)$ 的一个**因式**, $f(x)$ 为 $g(x)$ 的一个**倍式**.

例 1.4.2. 设 $f(x) \in \mathbb{F}[x]$, 则 $f(x) \mid 0$. 对任意的非零常数 $a \in \mathbb{F}$, $a \mid f(x), af(x) \mid f(x)$, 统称为多项式 $f(x)$ 的**平凡因式**.

引理 1.4.3. 设 $f(x), g(x), h(x) \in \mathbb{F}[x]$.

(a) $f(x) \mid g(x), g(x) \mid h(x) \Rightarrow f(x) \mid h(x)$;

(b) $f(x) \mid g(x), f(x) \mid h(x) \Rightarrow \forall u(x), v(x) \in \mathbb{F}[x], f(x) \mid u(x)g(x) + v(x)h(x)$;

(c) $f(x) \mid g(x), g(x) \mid f(x) \Leftrightarrow \exists\, 0 \neq c \in \mathbb{F}$ 使得 $f(x) = cg(x)$;

(d) 若 $f(x) \mid g(x)$ 且 $\deg f(x) > \deg g(x)$, 则 $g(x) = 0$.

定理 1.4.4 (带余除法). 设 $f(x), g(x) \in \mathbb{F}[x]$ 且 $g(x) \neq 0$, 则存在唯一的一对多项式 $q(x), r(x) \in \mathbb{F}[x]$, 其中 $\deg r(x) < \deg g(x)$, 使得

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

称 $q(x)$ 为 $g(x)$ 除 $f(x)$ 的**商**, $r(x)$ 为 $g(x)$ 除 $f(x)$ 的**余式**.

推论 1.4.5. 设 $f(x), g(x) \in \mathbb{F}[x]$ 且 $g(x) \neq 0$, 则 $g(x) \mid f(x)$ 当且仅当 $f(x)$ 除以 $g(x)$ 的余式为零.

练习 1.4.2. 设 $f(x) = x^4 + 3x^2 - 4x - 3, g(x) = x^3 + 3x^2 + 2x - 3$. 利用长除法求 $f(x)$ 除以 $g(x)$ 的商及余式.

练习 1.4.3. 设 $d, n \in \mathbb{N}$. 证明: $x^d - 1 \mid x^n - 1$ 当且仅当 $d \mid n$.

问题 1.4.1 (整除与数域扩大的关系). 设 $\mathbb{F} \subseteq \mathbb{K}$ 为数域, $f(x), g(x) \in \mathbb{F}[x]$. 问作为 $\mathbb{F}$ 上的多项式 $f(x) \mid g(x)$ 与作为 $\mathbb{K}$ 上的多项式 $f(x) \mid g(x)$ 是否等价?

1.4.4 最大公因式

定义 1.4.4. 设 $f(x), g(x) \in \mathbb{F}[x]$ 且不全为零, 若 $h(x) \in \mathbb{F}[x]$ 使得 $h(x) \mid f(x)$ 且 $h(x) \mid g(x)$, 则称 $h(x)$ 为 $f(x)$ 与 $g(x)$ 的**公因式**. 如果**首一**多项式 $d(x)$ 为多项式 $f(x), g(x)$ 的公因式且满足对任意的 $f(x)$ 与 $g(x)$ 的公因式 $h(x)$, 有 $h(x) \mid d(x)$, 那么称 $d(x)$ 为多项式 $f(x)$ 与 $g(x)$ 的**最大公因式**. 此时记为 $d(x) = \gcd(f(x), g(x)) = (f(x), g(x))$. 我们约定 $(0, 0) = 0$.

注记 1.4.3. 设 $f(x), g(x) \in \mathbb{F}[x]$ 不全为零. 由最大公因式的定义知, 如果 $f(x)$ 与 $g(x)$ 的最大公因式存在, 那么其一定是唯一的且是 $f(x)$ 与 $g(x)$ 的公因式中次数最大的首一的公因式.

引理 1.4.6. 设 $X \subset \mathbb{F}[x]$ 为非空集合且存在非零多项式 $f(x) \in X$, 则集合 X 中存在次数最小的非零多项式.

定理 1.4.7 (最大公因式的存在性**).** 任意两个不全为零的多项式的最大公因式存在且唯一. 进一步地, 存在多项式 $u(x), v(x) \in \mathbb{F}[x]$ 使得

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

注记 1.4.4. 上述定理中的多项式 $u(x), v(x)$ 不唯一.

推论 1.4.8. 设 $f(x), g(x) \in \mathbb{F}[x]$ 且不全为零, 则

$$d(x) = (f(x), g(x)) \text{ 当且仅当 } \begin{cases} d(x) \text{ 首一} \\ d(x) \mid f(x), d(x) \mid g(x) \\ \exists\, u(x), v(x) \in \mathbb{F}[x], s.t.\ d(x) = u(x)f(x) + v(x)g(x). \end{cases}$$

例 1.4.3. 设 $f(x) = x^4 - x^2 + 5x + 1, g(x) = x^2 + 12x + 5$, 利用辗转相除法求 $(f(x), g(x))$ 及多项式 $u(x), v(x)$ 使得 $(f(x), g(x)) = u(x)f(x) + v(x)g(x)$.

练习 1.4.4. 设 $f_i(x) \in \mathbb{F}[x], i = 1, \cdots, t$ 且不全为零. 若 $h(x) \in \mathbb{F}[x]$ 满足对任意的 $1 \leq i \leq t$, $h(x) \mid f_i(x)$, 则称 $h(x)$ 为 $f_1(x), \cdots, f_t(x)$ 的一个**公因式**. 若存在首一多项式 $d(x)$ 为 $f_1(x), \cdots, f_t(x)$ 的公因式且对任意的公因式 $h(x)$ 有 $h(x) \mid d(x)$, 则称 $d(x)$ 为多项式 $f_1(x), \cdots, f_t(x)$ 的**最大公因式**. 此时记为 $d(x) = (f_1(x), \cdots, f_t(x))$.
证明:(1) $(\cdots((f_1(x), f_2(x)), f_3(x)), \cdots, f_t(x))$ 是 $f_1(x), \cdots, f_t(x)$ 的最大公因式;

$$\text{(2) } d(x) = (f_1(x), \cdots, f_t(x)) \text{ 当且仅当 } \begin{cases} d(x) \text{ 首一} \\ d(x) \mid f_i(x), \forall 1 \leq i \leq t \\ \exists\, u_i(x) \in \mathbb{F}[x],\ s.t.\ d(x) = \sum_{i=1}^{t} u_i(x)f_i(x). \end{cases}$$

定义 1.4.5. 设 $f(x), g(x) \in \mathbb{F}[x]$, 称 $f(x)$ 与 $g(x)$ **互素**, 如果 $(f(x), g(x)) = 1$.

命题 1.4.9. 设 $f(x), g(x) \in \mathbb{F}[x]$, 则 $(f(x), g(x)) = 1$ 当且仅当存在 $u(x), v(x) \in \mathbb{F}[x]$ 使得

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

命题 1.4.10. 设 $f(x), g(x), h(x) \in \mathbb{F}[x]$.

(1) 若 $(f(x), g(x)) = 1$ 且 $f(x) \mid g(x)h(x)$, 则 $f(x) \mid h(x)$;

(2) 若 $(f(x), g(x)) = 1$ 且 $f(x) \mid h(x), g(x) \mid h(x)$, 则 $f(x)g(x) \mid h(x)$;

(3) 若 $(f(x),g(x))=1$, $(f(x),h(x))=1$, 则 $(f(x),g(x)h(x))=1$.

练习 1.4.5. 设 $f(x),g(x)\in\mathbb{F}[x]$ 不全为零, $d(x)=(f(x),g(x))$ 且 $f(x)=d(x)f_1(x), g(x)=d(x)g_1(x)$. 设 $u_0(x),v_0(x)\in\mathbb{F}[x]$ 使得 $d(x)=u_0(x)f(x)+v_0(x)g(x)$. 证明: 若 $u(x),v(x)\in\mathbb{F}[x]$ 也满足 $d(x)=u(x)f(x)+v(x)g(x)$, 则存在 $t(x)\in\mathbb{F}[x]$ 使得

$$u(x)=u_0(x)+g_1(x)t(x) \text{ 及 } v(x)=v_0(x)-f_1(x)t(x).$$

练习 1.4.6. 求次数最低的首一多项式 $f(x)\in\mathbb{Q}[x]$ 使得 $f(x)$ 被 $(x-1)^2$ 除时的余式为 $2x$, 被 $(x-2)^3$ 除时的余式为 $3x$.

练习 1.4.7. 求所有的 $u(x),v(x)\in\mathbb{F}[x]$ 使得

$$x^m u(x)+(x-2)^n v(x)=1.$$

1.5 多项式环的因式分解定理

定义 1.5.1. 设 $p(x)\in\mathbb{F}[x]$ 且 $\deg p(x)\geq 1$. 若 $p(x)$ 只有平凡因式, 则称 $p(x)$ 在**数域 $\mathbb{F}$ 上不可约**. 反之则称 $p(x)$ 在**数域 $\mathbb{F}$ 上可约**.

例 1.5.1. (1) 对任意的 $a\in\mathbb{F}$, 多项式 $x-a$ 为数域 $\mathbb{F}$ 上的不可约多项式. 更一般地, 任意的一次多项式都是不可约的.

(2) 设 $f(x)=x^2+1$. 易知 $f(x)$ 在 $\mathbb{R}$ 上不可约, 但在 $\mathbb{C}$ 上可约.

(3) $p(x)\in\mathbb{F}[x]$ 为不可约多项式当且仅当对任意的非零常数 $a\in\mathbb{F}$, $ap(x)$ 为不可约多项式.

引理 1.5.1. 设 $p(x)\in\mathbb{F}[x]$ 为不可约多项式.

(1) 对任意的多项式 $f(x)\in\mathbb{F}[x]$

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

(2) 若多项式 $f(x)$, $g(x)\in\mathbb{F}[x]$ 使得 $p(x)\mid f(x)g(x)$, 则 $p(x)\mid f(x)$ 或者 $p(x)\mid g(x)$.

定理 1.5.2 (因式分解定理). 对数域 $\mathbb{F}$ 上的任意的次数大于或等于 1 的多项式 $f(x)$, 存在唯一的 *(不计顺序)* 两两不同的首一不可约多项式 $p_1(x),\cdots,p_t(x)$ 及正整数 $r_1,\cdots,r_t$ 使得

$$f(x)=ap_1^{r_1}(x)p_2^{r_2}(x)\cdots p_t^{r_t}(x), \text{ 其中 } a \text{ 为多项式 } f(x) \text{ 的首项系数.}$$

注记 1.5.1. 称上述分解为多项式 $f(x)$ 的**标准分解式**. 需要指出的是对于任意给定的多项式 $f(x)\in\mathbb{F}[x]$, 我们没有方法求其在数域 $\mathbb{F}$ 上的具体的标准分解式. 为了了解多项式 $f(x)$ 的标准分解式的信息, 我们进而考虑如下问题:

1. 能否判断 $f(x)$ 在数域 $\mathbb{F}$ 上是否可约? (不可能!)

2. 在 $f(x)$ 的标准分解式中是否存在 $r_i \geq 2$?

3. 在 $f(x)$ 的标准分解式中是否存在形如 $x-a(a \in \mathbb{F})$ 的不可约因式?

1.6 重因式

定义 1.6.1. 设 $1 \leq k \in \mathbb{Z}$. 设 $f(x) \in \mathbb{F}[x]$, 称 $\mathbb{F}$ 上的不可约多项式 $p(x)$ 为 $f(x)$ 的k-**重因式**, 如果 $p^k(x) \mid f(x)$ 但是 $p^{k+1}(x) \nmid f(x)$. 若 $k=1$, 则称 $p(x)$ 为 $f(x)$ 的**单因式**; 当 $k>1$ 时, 称 $p(x)$ 为 $f(x)$ 的**重因式**.

定义 1.6.2. 设 $f(x)=\sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$. 定义映射

$$\begin{aligned} \mathbb{D}: \quad \mathbb{F}[x] \quad &\longrightarrow \mathbb{F}[x] \\ f(x) \quad &\mapsto f'(x)=\sum_{i=1}^{n} i a_i x^{i-1}. \end{aligned}$$

称 $\mathbb{D}f(x):=f'(x)$ 为多项式 $f(x)$ 的 **(形式) 导数或微商**. 对任意的 $k \geq 2$, 称 $f^{(k)}(x):=\mathbb{D}^k(f(x)):=\mathbb{D}(\mathbb{D}^{k-1}(f(x)))$ 为多项式 $f(x)$ 的k-**阶微商**.

注记 1.6.1. (1) 设 $f(x) \in \mathbb{F}[x]$, 则 $\mathbb{D}(f(x))=0$ 当且仅当 $f(x)=c \in \mathbb{F}$.

(2) 设 $f(x) \in \mathbb{F}[x]$ 且 $\deg f(x)=n \geq 1$, 则 $\deg \mathbb{D}(f(x))=n-1$, $\mathbb{D}^{n+1}(f(x))=0$.

练习 1.6.1. 设 $f(x),\ g(x) \in \mathbb{F}[x], a \in \mathbb{F}, n \geq 2$, 则

(1) $\mathbb{D}(f(x)+g(x))=\mathbb{D}(f(x))+\mathbb{D}(g(x))$;

(2) $\mathbb{D}(af(x))=a\mathbb{D}(f(x))$;

(3) $\mathbb{D}(f(x)g(x))=\mathbb{D}(f(x))g(x)+f(x)\mathbb{D}(g(x))$;

(4) $\mathbb{D}(f^n(x))=nf^{n-1}(x)\mathbb{D}(f(x))$.

命题 1.6.1. 设不可约多项式 $p(x) \in \mathbb{F}[x]$ 为多项式 $f(x) \in \mathbb{F}[x]$ 的 k-重因式, 则 $p(x)$ 为多项式 $\mathbb{D}(f(x))$ 的 $(k-1)$-重因式.

推论 1.6.2. 设 $f(x) \in \mathbb{F}[x]$, 则 $f(x)$ 有重因式当且仅当 $(f(x), \mathbb{D}(f(x))) \neq 1$.

练习 1.6.2. 设 $f(x), p(x) \in \mathbb{F}[x]$ 且 $p(x)$ 为不可约多项式. 证明: $p(x)$ 为 $f(x)$ 的 k-重因式当且仅当 $p(x)$ 为 $f(x), \mathbb{D}(f(x)) \cdots, \mathbb{D}^{k-1}(f(x))$ 的公因式但 $p(x) \nmid \mathbb{D}^k(f(x))$.

1.7 多项式函数与根

定义 1.7.1. 设 $f(x)=\sum\limits_{i=0}^{n}a_ix^i\in\mathbb{F}[x]$. 对任意的 $\alpha\in\mathbb{F}$, 记 $f(\alpha)=\sum\limits_{i=0}^{n}a_i\alpha^i\in\mathbb{F}$. 称 $f(\alpha)$ 为多项式 $f(x)$ 在 $x=\alpha$ 处的**值**, 称

$$\begin{aligned} f(x):\ \mathbb{F}\ &\longrightarrow\mathbb{F}\\ \alpha\ &\mapsto f(\alpha)\end{aligned}$$

为数域 $\mathbb{F}$ 上的由多项式 $f(x)$ 定义的**多项式函数**.

若 $f(\alpha)=0$, 则称 $\alpha\in\mathbb{F}$ 为多项式 $f(x)$ 的一个**根或者零点**.

注记 1.7.1. (a) 设 $f(x),g(x),h(x)\in\mathbb{F}[x]$.

(1) 如果 $f(x)+g(x)=h(x)$, 那么对任意的 $\alpha\in\mathbb{F}$, $f(\alpha)+g(\alpha)=h(\alpha)$;

(2) 如果 $f(x)g(x)=h(x)$, 那么对任意的 $\alpha\in\mathbb{F}$, $f(\alpha)g(\alpha)=h(\alpha)$.

(b) 由定义知相同的多项式定义的多项式函数相等.

定理 1.7.1 (余数定理)**.** 设 $f(x)\in\mathbb{F}[x],\alpha\in\mathbb{F}$, 则存在唯一的多项式 $q(x)\in\mathbb{F}[x]$ 使得

$$f(x)=(x-\alpha)q(x)+f(\alpha).$$

推论 1.7.2.

$$x-\alpha|f(x)\Longleftrightarrow f(\alpha)=0.$$

练习 1.7.1. 设 $a\neq b\in\mathbb{F}$. 求多项式 $f(x)\in\mathbb{F}[x]$ 除以 $(x-a)(x-b)$ 的余式.

定义 1.7.2. 称 $\alpha\in\mathbb{F}$ 称为多项式 $f(x)\in\mathbb{F}[x]$ 的 k-**重根**, 如果 $x-\alpha$ 为 $f(x)$ 的 k-重因式.

当 $k=1$ 时, 称 α 为 $f(x)$ 的**单根**; 当 $k>1$ 时, 称 α 为 $f(x)$ 的**重根.**

推论 1.7.3. $\alpha\in\mathbb{F}$ 为多项式 $f(x)\in\mathbb{F}[x]$ 的重根当且仅当 $f(\alpha)=f'(\alpha)=0$.

练习 1.7.2. 设 $p(x)\in\mathbb{F}[x]$ 为 $\mathbb{F}$ 上的不可约多项式. 证明: $p(x)$ 在 $\mathbb{C}$ 上没有重根.

练习 1.7.3. 设 $p(x)\in\mathbb{F}[x]$ 为 $\mathbb{F}$ 上的不可约多项式, $\alpha\in\mathbb{C}$ 为 $p(x)$ 在 $\mathbb{C}$ 上的根. 令 $\mathbb{K}:=\{f(\alpha)|f(x)\in\mathbb{F}[x]\}\subseteq\mathbb{C}$. 证明: $\mathbb{K}$ 为数域.

定理 1.7.4. 设 $f(x)\in\mathbb{F}[x]$ 且 $\deg f(x)=n\geq 1$, 则 $f(x)$ 在 $\mathbb{F}$ 上至多有 n 个根 *(根按重数计算).*

注记 1.7.2. $f(x)$ 可能在 $\mathbb{F}$ 上没有根. 如 $f(x)=x^2+1\in\mathbb{Q}[x]$, $f(x)$ 在 $\mathbb{Q}$ 上无根, 但在 $\mathbb{C}$ 上有根.

推论 1.7.5. 设 $f(x), g(x) \in \mathbb{F}[x]$ 不全为零且 $\deg f(x) \leq n, \deg g(x) \leq n$. 若存在 $n+1$ 个不同的数 $\alpha_1, \cdots, \alpha_{n+1} \in \mathbb{F}$ 使得 $f(\alpha_i) = g(\alpha_i), i = 1, \cdots, n+1$, 则 $f(x) = g(x)$.

推论 1.7.6. 设 $f(x), g(x) \in \mathbb{F}[x]$, 则 $f(x) = g(x)$ *(*作为多项式相等*)* 当且仅当 $f(x)$ 与 $g(x)$ 定义的多项式函数相等.

练习 1.7.4. 设 $f(x) \in \mathbb{C}[x]$. 对任意的 $a \in \mathbb{R}$, $f(a) \in \mathbb{R}$. 证明: $f(x) \in \mathbb{R}[x]$.

1.8 复/实系数多项式

定理 1.8.1 (代数学基本定理)**.** 每个次数大于或等于 1 的复系数多项式在 $\mathbb{C}$ 中有根.

定理 1.8.2 (代数学基本定理)**.** 设 $f(x) \in \mathbb{C}[x]$ 且 $\deg f(x) = n \geq 1$, 则 $f(x)$ 在 $\mathbb{C}$ 中恰有 n 个根 *(*计重数*)*.

推论 1.8.3. *(1)* $\mathbb{C}[x]$ 中的首一不可约多项式恰为 $\{x - c \mid c \in \mathbb{C}\}$;

(2) 设 $f(x) \in \mathbb{C}[x]$ 且 $\deg f(x) = n \geq 1$, 则存在两两不相等的 $\alpha_1, \cdots, \alpha_s \in \mathbb{C}$ 及正整数 $r_1, \cdots, r_s$ 使得

$$f(x) = a(x - \alpha_1)^{r_1}(x - \alpha_2)^{r_2} \cdots (x - \alpha_s)^{r_s},$$

其中 a 为 $f(x)$ 的首项系数, $\sum_{i=1}^{s} r_i = n$.

练习 1.8.1. 设 $f(x), p(x) \in \mathbb{F}[x]$ 且 $p(x)$ 为 $\mathbb{F}$ 上的不可约多项式. 若 $p(x)$ 与 $f(x)$ 在 $\mathbb{C}$ 上有公共根 α, 则 $p(x)|f(x)$.

练习 1.8.2. 设 $f(x) = x^2 + x + 1, g(x) = x^{3n} + x^{3m+1} + x^{3p+2}$, 其中 m, n, p 为自然数. 证明: $f(x)|g(x)$.

定理 1.8.4. $\mathbb{R}$ 上的首一不可约多项式恰为

$$\{x - a \mid a \in \mathbb{R}\} \cup \{x^2 + bx + c \mid b, c \in \mathbb{R}, b^2 - 4c < 0\}.$$

推论 1.8.5. 设 $f(x) \in \mathbb{R}[x]$ 且 $\deg f(x) = n \geq 1$, 则存在两两互素的一次多项式 $x - c_i \in \mathbb{R}[x], i = 1, \ldots, s$ 与两两互素的不可约二次多项式 $x^2 + p_j x + q_j \in \mathbb{R}[x], j = 1, \ldots, t$ 使得

$$f(x) = a(x - c_1)^{k_1}(x - c_2)^{k_2} \cdots (x - c_s)^{k_s}(x^2 + p_1 x + q_1)^{l_1} \cdots (x^2 + p_t x + q_t)^{l_t},$$

其中 a 为 $f(x)$ 的首项系数, $k_1, \cdots, k_s, l_1, \cdots, l_t$ 为正整数且满足 $\sum_{i=1}^{s} k_i + \sum_{j=1}^{t} 2l_j = n$.

例 1.8.1. 求多项式 $x^n - 1$ 在复数 $\mathbb{C}$ 及实数 $\mathbb{R}$ 上的标准分解.

练习 1.8.3. 设 $f(x), g(x) \in \mathbb{C}[x]$ 满足 $f^{-1}(0) = g^{-1}(0)$ 且 $f^{-1}(1) = g^{-1}(1)$. 证明: $f(x) = g(x)$.

练习 1.8.4. 设 $f(x) \in \mathbb{F}[x]$. 证明: $f(x)$ 在数域 $\mathbb{F}$ 上无重因式当且仅当 $f(x)$ 在 $\mathbb{C}$ 上无重根.

练习 1.8.5. 设 $f(x) \in \mathbb{F}[x]$ 在 $\mathbb{F}$ 上不可约, $\alpha, \frac{1}{\alpha} \in \mathbb{C}$ 为 $f(x)$ 的复根. 证明: 若 $b \in \mathbb{C}$ 是 $f(x)$ 在 $\mathbb{C}$ 上的根, 则 $\frac{1}{b}$ 也是 $f(x)$ 的复根.

1.9 有理多项式

定义 1.9.1. 设 $f(x) \in \mathbb{Q}[x]$, 若 $\alpha \in \mathbb{Q}$ 使得 $f(\alpha) = 0$, 则称 α 为 $f(x)$ 的**有理根**.

引理 1.9.1. 设 $f(x) \in \mathbb{Q}[x]$ 且 $\deg f(x) \geq 2$. 若 $f(x)$ 有有理根, 则 $f(x)$ 在 $\mathbb{Q}$ 上可约.

注记 1.9.1. 若 $f(x) \in \mathbb{Q}[x]$ 无有理根, $f(x)$ 在 $\mathbb{Q}$ 上也可能可约. 如 $f(x) = (x^2+1)^2$.

注记 1.9.2. 设 $f(x) \in \mathbb{Q}[x]$, 则总存在非零整数 c 使得 $cf(x) \in \mathbb{Z}[x]$. 显然 $f(x)$ 与 $cf(x)$ 具有相同的有理根, 并且 $f(x)$ 在 $\mathbb{Q}$ 上不可约当且仅当 $cf(x)$ 在 $\mathbb{Q}$ 上不可约. 因此研究有理数域上的多项式是否可约, 我们只需要研究系数都是整数的多项式即可.

定义 1.9.2. 设 $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$. 若 $a_i \in \mathbb{Z}, i = 0, \cdots, n$, 则称 $f(x)$ 为**整系数多项式**. 记 $\mathbb{Z}[x]$ 表示整系数多项式环 (对多项式的加法及乘法封闭).

定理 1.9.2 (有理根存在必要条件). 设 $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, $\alpha = \frac{c}{d}$ 为 $f(x)$ 的有理根, 其中 $d, c \in \mathbb{Z}, (d, c) = 1$, 则 $d | a_n, c | a_0$.

练习 1.9.1. 判断 $f(x) = 2x^5 + 3x^2 + 4x + 9$ 是否有有理根?

定义 1.9.3. 设 $f(x) = \sum\limits_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. 若 $a_0, a_1, \cdots, a_n$ 的最大公因子为 1, 则称 $f(x)$ 为**本原多项式**.

注记 1.9.3.

- 设 $f(x), g(x)$ 为本原多项式, $a \in \mathbb{Q}$ 使得 $f(x) = ag(x)$, 则 $a = \pm 1$.
- 设 $f(x) \in \mathbb{Q}[x]$, 则存在本原多项式 $g(x)$ 及有理数 $c \in \mathbb{Q}$ 使得 $f(x) = cg(x)$.

引理 1.9.3 (Gauss 引理). 两个本原多项式的乘积为本原多项式.

定理 1.9.4. 设 $f(x) \in \mathbb{Z}[x]$, 则 $f(x)$ 在有理数域 $\mathbb{Q}$ 上可约当且仅当存在 $g(x), h(x) \in \mathbb{Z}[x]$ 满足 $\deg g(x) < \deg f(x), \deg h(x) < \deg f(x)$ 使得 $f(x) = g(x)h(x)$.

练习 1.9.2. 设 $a_1, \cdots, a_n$ 为 n 个互不相同的整数. 证明:

(1) $f(x) = (x - a_1) \cdots (x - a_n) - 1$ 在 $\mathbb{Q}$ 上不可约;

(2) $g(x)=(x-a_1)^2\cdots(x-a_n)^2+1$ 在 $\mathbb{Q}$ 上不可约.

定理 1.9.5 (Eisenstein 判别法). 设 $f(x)=\sum\limits_{i=0}^{n}a_ix^i\in\mathbb{Z}[x]$. 若存在素数 p 使得 $p|a_i,i=0,\cdots,n-1$, $p\nmid a_n$ 且 $p^2\nmid a_0$, 则 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

推论 1.9.6. 对任意的 $n\geq 1$, 存在 $f(x)\in\mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上不可约且 $\deg f(x)=n$.

引理 1.9.7. 设 $f(x)\in\mathbb{Q}[x],0\neq a\in\mathbb{Q},b\in\mathbb{Q}$, 令 $g(x)=f(ax+b)\in\mathbb{Q}[x]$, 则 $f(x)$ 不可约当且仅当 $g(x)$ 不可约.

例 1.9.1. 判断 $f(x)=x^6-x^3+1$ 在 $\mathbb{Q}$ 上是否可约.

练习 1.9.3. 设 p 为素数. 证明: $f(x)=\sum\limits_{i=0}^{p-1}x^i$ 在 $\mathbb{Q}$ 上不可约.

练习 1.9.4. 设 $f(x)=\sum\limits_{i=0}^{n-1}x^i$. 证明: $f(x)$ 在 $\mathbb{Q}$ 上不可约当且仅当 n 为素数.

练习 1.9.5. 设 $f(x)$ 是次数大于零的首一整系数多项式. 证明: 若 $f(0),f(1)$ 都是奇数, 则 $f(x)$ 没有整数根.

1.10 多元多项式与对称多项式

1.10.1 多元多项式的基本概念

设 $\mathbb{F}$ 为数域, $x_1,\cdots,x_n$ 为 n 个不定元 (或形式变量). 记

$$\mathbb{N}^n:=\{(m_1,\cdots,m_n)|m_i\in\mathbb{N},i=1,2,\cdots,n\}.$$

定义 1.10.1. 称形式表达式

$$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},\ \text{其中}\ a\in\mathbb{F},k_1,\cdots,k_n\in\mathbb{N}$$

为数域 $\mathbb{F}$ 上一个n **元单项式** (monomial).

称 a 为该单项式的**系数**.

若 $a\neq 0$, 则称 $k_1+k_2+\cdots+k_n\in\mathbb{N}$ 为该单项式的**次数**.

称两个单项式 $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 与 $bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$ 为**同类项** (similar term), 如果 $k_1=l_1,\cdots,k_n=l_n$.

定义 1.10.2. 设 M 为 $\mathbb{N}^n$ 的任意的非空有限子集. 称形式表达式

$$f(x_1,\cdots,x_n):=\sum_{(k_1,\cdots,k_n)\in M}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},\ \text{其中}\ a_{k_1k_2\cdots k_n}\in\mathbb{F},$$

为数域 $\mathbb{F}$ 上的一个 n **元多项式**. 特别地, n 元多项式为有限多个 n 元单项式的形式和.

定义 1.10.3. 设 $f(x_1,\cdots,x_n)$ 与 $g(x_1,\cdots,x_n)$ 为数域 $\mathbb{F}$ 上的 n 元多项式.

称 $f(x_1,\cdots,x_n)$ 与 $g(x_1,\cdots,x_n)$ **相等**, 如果他们含有完全相同的系数非零的单项式.

如果数域 $\mathbb{F}$ 上的一个 n 元多项式的所有的单项式的系数都为 0, 那么称它为**零多项式**, 记为 0.

设 $f(x_1,\cdots,x_n)$ 为数域 $\mathbb{F}$ 上的 n 元多项式, 它的所有的系数非零的单项式的次数的最大值称为 $f(x_1,\cdots,x_n)$ 的**次数**, 记为 $\deg f(x_1,\cdots,x_n)$ 或者 $\partial f(x_1,\cdots,x_n)$. 约定零多项式的次数为 $-\infty$.

注记 1.10.1. 具有次数最大的单项式可能不唯一.

定义 1.10.4 (字典排序法). 设 $(i_1,i_2,\cdots,i_n)$ 及 $(j_1,j_2,\cdots,j_n)\in\mathbb{N}^n$. 称 $(i_1,\cdots,i_n)$ **先于** $(j_1,\cdots,j_n)$, 如果存在 $1\leq s\leq n$ 使得 $i_1=j_1,\cdots,i_{s-1}=j_{s-1},i_s>j_s$. 此时记为 $(i_1,\cdots,i_n)>(j_1,\cdots,j_n)$.

称单项式 $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ **先于** $bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$ 如果 $(k_1,\cdots,k_n)>(l_1,\cdots,l_n)$.

定义 1.10.5. 设 $f(x_1,\cdots,x_n)$ 为 $\mathbb{F}$ 上的 n 元多项式. 将 $f(x_1,\cdots,x_n)$ 的单项式按字典排序法写出来的第一个非零单项式 (最大的) 称为 $f(x_1,\cdots,x_n)$ 的**首项**.

注记 1.10.2. 多元多项式的首项不一定具有最大的次数.

1.10.2 多元多项式的运算

记 $\mathbb{F}[x_1,\cdots,x_n]$ 表示数域 $\mathbb{F}$ 上的 n 元多项式全体. 设 $f(x_1,\cdots,x_n),g(x_1,\cdots,x_n)\in\mathbb{F}[x_1,\cdots,x_n]$, 则存在 $\mathbb{N}^n$ 的非空有限子集 M_1,M_2 使得

$$f(x_1,\cdots,x_n)=\sum_{(k_1,\cdots,k_n)\in M_1}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

$$g(x_1,\cdots,x_n)=\sum_{(l_1,\cdots,l_n)\in M_2}b_{l_1l_2\cdots l_n}x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}.$$

定义**多元多项式的加法** $+$:

$$f(x_1,\cdots,x_n)+g(x_1,\cdots,x_n):=\sum_{(t_1,\cdots,t_n)\in M_1\cup M_2}(a_{t_1t_2\cdots t_n}+b_{t_1t_2\cdots t_n})x_1^{t_1}x_2^{t_2}\cdots x_n^{t_n},$$

其中约定当 $(t_1,\cdots,t_n)\in M_1\diagdown M_2$ 时记 $b_{t_1\cdots t_n}=0$, 当 $(t_1,\cdots,t_n)\in M_2\diagdown M_1$ 时记 $a_{t_1\cdots t_n}=0$.

定义**多元多项式的乘法** $\times$:

$$f(x_1,\cdots,x_n)\times g(x_1,\cdots,x_n):=\sum_{(t_1,\cdots,t_n)\in M}c_{t_1t_2\cdots t_n}x_1^{t_1}x_2^{t_2}\cdots x_n^{t_n},$$

其中

$$M := \{(m_1, \cdots, m_n) \in \mathbb{N}^n | \exists (k_1, \cdots, k_n) \in M_1, (l_1, \cdots, l_n) \in M_2 \text{ 使得 } m_i = k_i + l_i, i = 1, \cdots, n\},$$

$$c_{t_1 t_2 \cdots t_n} = \sum_{\substack{(k_1, \cdots, k_n) \in M_1 \\ (l_1, \cdots, l_n) \in M_2 \\ k_i + l_i = t_i, i = 1, \cdots, n}} a_{k_1 k_2 \cdots k_n} b_{l_1 l_2 \cdots l_n}.$$

练习 1.10.1. 验证 $\mathbb{F}[x_1, \cdots, x_n]$ 在上述加法与乘法意义下为交换环. 称 $(\mathbb{F}[x_1, \cdots, x_n], +, \times)$ 为数域 $\mathbb{F}$ 上的 n 元多项式环.

注记 1.10.3. 对任意的多项式 $f(x_1, \cdots, x_n), g(x_1, \cdots, x_n) \in \mathbb{F}[x_1, \cdots, x_n]$, 显然有

$$\deg f(x_1, \cdots, x_n) + g(x_1, \cdots, x_n) \leq \max\{\deg f(x_1, \cdots, x_n), \deg g(x_1, \cdots, x_n)\}.$$

引理 1.10.1. 设 $f(x_1, \cdots, x_n)$, $g(x_1, \cdots, x_n)$ 为数域 $\mathbb{F}$ 上的非零 n 元多项式, 则 $f(x_1, \cdots, x_n)$ 与 $g(x_1, \cdots, x_n)$ 的乘积的首项为 $f(x_1, \cdots, x_n)$ 的首项与 $g(x_1, \cdots, x_n)$ 的首项的乘积.

定理 1.10.2 (乘法消去律). 设 $f(x_1, \cdots, x_n), g(x_1, \cdots, x_n), h(x_1, \cdots, x_n) \in \mathbb{F}[x_1, \cdots, x_n]$.

(1) 若 $f(x_1, \cdots, x_n)g(x_1, \cdots, x_n) = 0$, 则 $f(x_1, \cdots, x_n) = 0$ 或者 $g(x_1, \cdots, x_n) = 0$;

(2) 若 $f(x_1, \cdots, x_n)g(x_1, \cdots, x_n) = f(x_1, \cdots, x_n)h(x_1, \cdots, x_n)$ 且 $f(x_1, \cdots, x_n)$ 为非零多项式, 则 $g(x_1, \cdots, x_n) = h(x_1, \cdots, x_n)$.

定义 1.10.6. 设 $f(x_1, \cdots, x_n) \in \mathbb{F}[x_1, \cdots, x_n]$, 称 $f(x_1, \cdots, x_n)$ 为 m **次齐次多项式**, 如果它的每个系数非零的单项式都是 m 次的. 约定零多项式可以看作任意次数的齐次多项式.

命题 1.10.3. *(1)* 设 $f(x_1, \cdots, x_n)$ 与 $g(x_1, \cdots, x_n)$ 为非零齐次多项式, 则 $f(x_1, \cdots, x_n)$ 与 $g(x_1, \cdots, x_n)$ 的乘积也是齐次多项式且 $\deg fg = \deg f + \deg g$;

(2) 对任意的多元多项式 $f(x_1, \cdots, x_n) \in \mathbb{F}[x_1, \cdots, x_n]$, 存在唯一的 i 次齐次多项式 $f_i(x_1, \cdots, x_n), i = 0, 1, \cdots, \deg f(x_1, \cdots, x_n)$ 使得

$$f(x_1, \cdots, x_n) = \sum_{i=0}^{\deg f} f_i(x_1, \cdots, x_n);$$

(3) 对任意的 $f(x_1, \cdots, x_n), g(x_1, \cdots, x_n) \in \mathbb{F}[x_1, \cdots, x_n]$, 有

$$\deg f(x_1, \cdots, x_n)g(x_1, \cdots, x_n) = \deg f(x_1, \cdots, x_n) + \deg g(x_1, \cdots, x_n).$$

练习 1.10.2. 设 $f(x_1, \cdots, x_n), g(x_1, \cdots, x_n) \in \mathbb{F}[x_1, \cdots, x_n]$. 若 $f(x_1, \cdots, x_n)g(x_1, \cdots, x_n)$ 为齐次多项式且 $f(x_1, \cdots, x_n) \neq 0 \neq g(x_1, \cdots, x_n)$. 证明: $f(x_1, \cdots, x_n)$ 与 $g(x_1, \cdots, x_n)$ 都是齐次多项式.

定义 1.10.7. 设 $f(x_1,\cdots,x_n)=\sum_{(k_1,\cdots,k_n)\in M}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\in\mathbb{F}[x_1,\cdots,x_n]$. 设 $c_1,\cdots,c_n\in\mathbb{F}$, 称

$$f(c_1,\cdots,c_n):=f(x_1,\cdots,x_n)|_{x_1=c_1,\ldots,x_n=c_n}:=\sum_{(k_1,\cdots,k_n)\in M}a_{k_1k_2\cdots k_n}c_1^{k_1}c_2^{k_2}\cdots c_n^{k_n}\in\mathbb{F}$$

为 $f(x_1,\cdots,x_n)$ 在 $x_1=c_1,\cdots,x_n=c_n$ 处的**取值**.

定理 1.10.4. 设 $f(x_1,\cdots,x_n)$ 为数域 $\mathbb{F}$ 上的非零多项式, 则存在 $c_1,\cdots,c_n\in\mathbb{F}$ 使得 $f(c_1,\cdots,c_n)\neq 0$.

1.10.3 对称多项式

定义 1.10.8. 设 $f(x_1,\cdots,x_n)\in\mathbb{F}[x_1,\cdots,x_n]$, 如果对任意的 $1\leq i\neq j\leq n$,

$$\begin{aligned}&f(x_1,\cdots,x_{i-1},x_i,x_{i+1},\cdots,x_{j-1},x_j,x_{j+1},\cdots,x_n)\\=\;&f(x_1,\cdots,x_{i-1},x_j,x_{i+1},\cdots,x_{j-1},x_i,x_{j+1},\cdots,x_n),\end{aligned}$$

即交换 x_i 与 x_j 的位置后 $f(x_1,\cdots,x_n)$ 不变, 那么称 $f(x_1,\cdots,x_n)$ 为 $\mathbb{F}$ 上的一个 n **元对称多项式**.

例 1.10.1. $\sigma_1(x_1,\cdots,x_n)=x_1+x_2+\cdots+x_n=\sum_{i=1}^n x_i$;

$\sigma_2(x_1,\cdots,x_n)=\sum_{1\leq i<j\leq n}x_ix_j$;

$\cdots$;

$\sigma_k(x_1,\cdots,x_n)=\sum_{1\leq j_1<j_2\cdots<j_k\leq n}x_{j_1}x_{j_2}\cdots x_{j_k}$;

$\cdots$;

$\sigma_n=x_1x_2\cdots x_n$,

为 n 元对称多项式, 称为 n **元初等对称多项式**.

例 1.10.2 (Vieta 定理)**.** 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{F}[x]$ 在 $\mathbb{F}$ 中有 n 个根 $c_1,\cdots,c_n$, 则

$$\begin{aligned}&\sigma_1(c_1,\cdots,x_n)=\sum_{i=1}^n c_i=(-1)^1a_{n-1};\\&\sigma_2(c_1,\cdots,c_n)=\sum_{1\leq i<j\leq n}c_ic_j=(-1)^2a_{n-2};\\&\vdots\\&\sigma_n(c_1,\cdots,x_n)=c_1c_2\cdots c_n=(-1)^na_0.\end{aligned}$$

事实. (1) 对称多项式的和与乘积仍为对称多项式;

(2) 对称多项式的多项式为对称多项式. 特别地, 若 $f_1(x_1,\cdots,x_n),\cdots,f_t(x_1,\cdots,x_n)$ 为对称多项式, 则对任意的 t 元多项式 $g(y_1,\cdots,y_t)\in\mathbb{F}[y_1,\cdots,y_t]$, $g(f_1,f_2,\cdots,f_t)$ 为 $x_1,\cdots,x_n$ 的对称多项式.

定理 1.10.5 (对称多项式基本定理). 设 $f(x_1,\cdots,x_n)\in\mathbb{F}[x_1,\cdots,x_n]$ 为对称多项式, 则存在唯一的多项式 $g(x_1,\cdots,x_n)\in\mathbb{F}[x_1,\cdots,x_n]$ 使得

$$f(x_1,\cdots,x_n)=g(\sigma_1(x_1,\cdots,x_n),\cdots,\sigma_n(x_1,\cdots,x_n)).$$

例 1.10.3. 利用待定系数法将对称多项式 $f(x_1,x_2,x_3)=x_1^3+x_2^3+x_3^3+x_1x_2+x_1x_3+x_2x_3$ 表示为初等对称多项式的多项式.

练习 1.10.3. 设 $x_1,\cdots,x_n$ 为多项式 $x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 的复根. 证明: 关于 $x_2,\cdots,x_n$ 的对称多项式可以表示为 $x_1,a_1,\cdots,a_{n-1}$ 的多项式.