§5.1-5.4

+ 群 × 结合(无逆元) +·× 分配律

⇓

交换环

Polynomial Algebra $\rightsquigarrow$ $F[x]$ is a PID (Principal Ideal Domain)

逆元

分式域 整环

- ✓ Division Theorem, Divisibility
- The (Not A!) Greatest Common Divisor (GCD) and Relatively Prime
- $\rightsquigarrow$ Chinese Reminder Theorem (CRT) $\rightsquigarrow$ Lagrange Interpolation Formula
- $\rightsquigarrow\rightsquigarrow$ (Chapter 7) Jordan-Chevalley Decomposition
- In PID, Irreducible $\Leftrightarrow$ Prime
- (PID $\Rightarrow$ UFD) Unique Factorization
- Repeated Factor $\rightsquigarrow$ $(f(x), f'(x)) = 1$?

Cauchy 乘积 $\sum_{i+j=2p} (-1)^i 1^j x^{2p} = \sum_{i=0}^{2p} (-1)^i = 1.$

Try

令

$$f(x) = \left\{ \sum_{k=0}^{2n} (-1)^k x^k \right\} \left\{ \sum_{k=0}^{2n} x^k \right\}$$

那么其中 x^{2p} 的系数均为 1， x^{2p-1} 的系数均为 0. $(1 \le p \le 2n^2,\ p \in \mathbb{N}^*)$

$\sum_{i=0}^{2p-1} (-1)^i = 0$.

否.

整环

$F[x]$ is an integral domain:

- $f(x), g(x) \in F[x]$, if $f(x), g(x) \neq 0$, then $f(x)g(x) \neq 0$;

  $a_n x^n$, $a_n \neq 0$; $b_m x^m$, $b_m \neq 0$; $a_n b_m x^{n+m}$, $a_n b_m \neq 0$

- $f(x), g(x), h(x) \in F[x]$, if $f(x)h(x) = g(x)h(x)$, $h(x) \neq 0$, then $f(x) = g(x)$. (消去律)

  $(f(x)-g(x))h(x) = 0 \xrightarrow{\text{反证}} f(x) = g(x)$

例 1

If $f(x), g(x), h(x) \in \mathbf{R}[x]$ and we have $xf^2(x) + xg^2(x) = h^2(x)$, then $f(x) = g(x) = h(x) = 0$.

deg 奇 偶

Notes:

- 回顾 $f(x), g(x) \in \mathbf{R}[x]$, $f^2(x) + g^2(x) = 0 \rightsquigarrow f(x) = g(x) = 0$.
  $i^2 + 1^2 = 0.$
- 上述两个结论在 $\mathbf{C}[x]$ 上还成立吗？

待证: 只有 $f=g=h=0$.

pf:

- $f=g=0 \Rightarrow h^2=0 \Rightarrow h=0$
- 不妨 $\deg f > \deg g$ 不妨 $g=0$ 则 $\deg f \geq 0$.

  $\Rightarrow xf^2(x) = h^2(x) \overset{h\neq 0}{\Rightarrow} 1+2\deg f = 2\deg h.$

  $\Rightarrow$ 矛盾!

- 不妨 $\deg f \geq \deg g \geq 0$

  $\boxed{\text{要求 } h \neq 0}$

  $\deg[xf^2(x) + xg^2(x)] = 2\deg f + 1.$ ($\deg f \geq \deg g$)

  同理可证 导出矛盾!

  ★ $(a_n^2 + b_n^2)x^{n+1}$ 首项 $2\deg f+1$ =.

  $a_n, b_n \in \mathbf{R}$. $a_n \neq 0, b_n \neq 0 \Rightarrow a_n^2 + b_n^2 \neq 0.$

$f(x) = i$, $g(x) = 1$. $xf^2(x) + xg^2(x) = 0 = h^2(x)$

例 2

Determine all polynomials $f(x) \in F[x]$ such that $f[f(x)] = f^n(x)$, where $n \in \mathbf{N}^*$ is a given positive integer.

Hint: $f(x) \neq 0 \rightsquigarrow \deg f[f(x)] = (\deg f(x))^2$.

Lemma: Hint.

不妨设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \; (a_n \neq 0)$, $\deg f = n$.

$f(f(x))$ $\boxed{首项}$ $\rightsquigarrow a_n (a_n x^n)^n = a_n^{n+1} x^{n^2}$.

$\rightsquigarrow \deg(f(f(x))) = n^2 = (\deg f(x))^2 \rightsquigarrow f(f(x))$ 首项 a_n^{n+1}

$f[f(x)] = f^n(x)$

- $\deg f(x) = -\infty \Rightarrow f(x) = 0$ ✓.

- $f(x) = c \in F$. $\quad c = c^n \Rightarrow c^{n-1} = 1 = (\cos 2k\pi + i\sin 2k\pi)$

$c \neq 0$

Recall: $[\rho(\cos\theta + i\sin\theta)]^n = \rho^n(\cos n\theta + i\sin n\theta)$

$f(x) = c = \cos\frac{2k\pi}{n-1} + i\sin\frac{2k\pi}{n-1}$, $k \in \mathbb{Z}$.

- $\deg f(x) > 0$. $\quad \underbrace{f[f(x)]} = \underbrace{f^n(x)}_{\Delta}$ $\quad \deg f(x) > 0$.

$\Rightarrow$ 比较. $[\deg f(x)]^2 = n \deg \underline{\underline{f(x)}} \Rightarrow \deg f(x) = \underset{\Delta}{n}$.

$\Rightarrow f(x) = a_n x^n + \cdots + a_1 x + a_0$.

$\Rightarrow f[f(x)] = \underline{\underline{a_n}} f^n(x) + \cdots + a_1 f(x) + a_0$.

$= f^n(x)$

两边最高次项. $a_n (x^n)^{(n)} = (x^n)^{(n)} \Rightarrow a_n = 1.$

$\Rightarrow a_{n-1} f^{(n-1)}(x) + \cdots + a_1 f(x) + a_0 = 0$

依次取. $(x^n)^{(n-1)}, (x^n)^{(n-2)} \cdots (x^n)', 1$

则系数 $=0.$ $\leadsto a_{n-1} = \cdots = a_1 = a_0 = 0.$

$\Rightarrow f(x) = x^n.$

$\square$.

$A, B \in M_n(F)$，$A \sim B$ 在 $\mathbb{C}$ 上成立，那么在 F 上是否有 $A \sim B$？

Thm 3

$PA = BP$ $\quad P = (p_{ij})_{n \times n}$ $\quad n^2$

Suppose $f(x), g(x) \in F[x]$ and $g(x) \neq 0$, then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x), \tag{1}$$

在 $K[x]$ 中仍成立

where $\deg r(x) < \deg g(x)$.

唯一性

Notes:

- 若 $r(x) = 0$，那么 $\deg 0 = -\infty < \deg g(x)$ 也成立；
- (带余除法与数域扩大无关) 若 $F \subseteq K$，在 $K[x]$ 中存在 $\tilde{q}(x), \tilde{r}(x) \in K[x]$ 满足

$\Rightarrow \tilde{q}(x), \tilde{r}(x) \in F[x]$

$$f(x) = \tilde{q}(x)g(x) + \tilde{r}(x) \rightsquigarrow \tilde{q}(x) = q(x),\ \tilde{r}(x) = r(x).$$

$= 0$

Thm 3

Suppose $f(x), g(x) \in F[x]$ and $g(x) \neq 0$, then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x), \tag{1}$$

where $\deg r(x) < \deg g(x)$.

deg $f(x)$ $\le n$ 时 成立 ✓.

$= n \rightsquigarrow \deg g(x) \le n.$

$= m$

$\boxed{a_n x^n}$ $(a_n \neq 0)$ $+\,0 \cdot x^{n-1}$?

$b_m x^m$ $(b_m \neq 0)$

$$\boxed{f(x) - a_n (b_m)^{-1} x^{n-m} g(x)} = q(x)g(x) + r(x)$$

deg $< n$.

(不一定 $= n-1$) $\rightsquigarrow$ $\boxed{\text{归纳}}$.

例 4

Suppose $f(x), g(x) \in F[x]$ and $g(x) \neq 0$. Let $k \in \mathbf{N}^*$ and assume $k \deg g(x) \leq \deg f(x) < (k+1)\deg g(x)$. Then, there exist unique polynomials $p_i(x) \in F[x]$ $(i = 0, 1, 2, \cdots, k)$ such that

$$f(x) = p_0(x) + p_1(x)g(x) + \cdots + p_k(x)g^k(x), \tag{2}$$

where $\deg p_i(x) < \deg g(x)$.

Hint: We can repeatedly apply the division theorem to the quotient $q(x)$.

Pf:

$f(x) = \boxed{q_0(x)}\, g(x) + r(x)$, $\deg r(x) < \deg g(x)$

$(k-1)\deg g(x) \leq \_ < (k)\deg g(x)$

$q_0(x) = q_1(x)\, g(x) + r_1(x)$.

$\boxed{q_1(x)}\, g^2(x) + r_1(x) g(x) + r(x)$

$k-2$ $\qquad$ $k-1$

$q_2(x)\, g^3(x) + r_2(x)\, g^2(x)$

$q_{k-2}(x) = q_{k-1}(x)\, g(x) + r_{k-1}(x)$

$\boxed{0 \leq \quad < 1 \cdot \deg g(x)}$

$\boxed{q_{k-1}(x)}\, g^k(x) + r_{k-1}(x)\, g^{k-1}(x) + \cdots$

$+ \cdots + r_2(x)\, g^2(x) + r_1(x)\, g(x) + r(x)$

$$f(x) = p_0(x) + p_1(x)g(x) + \cdots + p_k(x)g^k(x).$$

$$= q_0(x) + q_1(x)g(x) + \cdots + q_k(x)g^k(x).$$

$$(p_0 - q_0) + (p_1 - q_1)g + \cdots + (p_k - q_k)g^k = 0.$$

$$\underbrace{(p_0 - q_0)}_{=0} + g\Big[\underbrace{(p_1 - q_1) + (p_2 - q_2)g + \cdots + (p_k - q_k)g^{k-1}}_{=0.}\Big] = 0$$

以此类推

$$p_1 = q_1 \to p_2 = q_2 \to \cdots \to p_k = q_k$$

$\boxed{\text{III}}$.

(1) Find the quotient $q(x)$ and the reminder $r(x)$ when $f(x) = 3x^4 - 4x^3 + 5x - 1$ is divided by $g(x) = x^2 - x + 1$.

$$
\begin{array}{r}
3x^2 - x - 4 \\
x^2 - x + 1 \enclose{longdiv}{3x^4 - 4x^3 + 0x^2 + 5x - 1} \\
3x^4 - 3x^3 + 3x^2 \\
\hline
-x^3 - 3x^2 + 5x - 1 \\
-x^3 + x^2 - x + 0 \\
\hline
-4x^2 + 6x - 1 \\
-4x^2 + 4x - 4 \\
\hline
2x + 3
\end{array}
$$

(2) Prove that when $f(x) \in F[x]$ is divided by $(x-a)(x-b)$, the reminder $r(x)$ is

$$\frac{f(a)-f(b)}{a-b}x + \frac{af(b)-bf(a)}{a-b}.$$

$(a \neq b)$

$$f(x) = g(x) \cdot \underbrace{(x-a)(x-b)}_{\text{二次}} + \underbrace{\boxed{mx+n}}_{\text{一次}}$$

二次 $\Rightarrow$ 一次

$$\begin{cases} f(a) = ma+n \\ f(b) = mb+n \end{cases}$$

$$A = \begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix} \quad r(A) = 2.$$

$$A \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} f(a) \\ f(b) \end{pmatrix}$$

$$\begin{pmatrix} m \\ n \end{pmatrix} = A^{-1} \begin{pmatrix} f(a) \\ f(b) \end{pmatrix}$$

$$A^{-1} = \frac{1}{\det A} \cdot A^{*} = \frac{1}{a-b} \begin{pmatrix} 1 & -1 \\ -b & a \end{pmatrix} \begin{pmatrix} f(a) \\ f(b) \end{pmatrix}$$

$$\frac{1}{a-b}\begin{pmatrix} f(a)-f(b) \\ -bf(a)+af(b) \end{pmatrix}$$

$$\Rightarrow \quad m = \frac{f(a)-f(b)}{a-b} \qquad n = \frac{af(b)-bf(a)}{a-b}$$ □.

[证] ($\underline{\text{CRT}}$) Chinese Reminder. Theorem.

$f(a) = f(a)$ $\qquad$ $f(x)-f(a)=0$ 有根 $x=a$.

Claim: $\boxed{x-a \mid f(x)-f(a)}$ 商 余数.

$\Rightarrow f(x)-f(a) = q(x)(x-a)+r \Rightarrow \underline{r(x)=0}$.

$\Rightarrow$ $\underline{代入 x=a}$. $\quad 0 = 0 + r \Rightarrow r=0$

$$\underline{m \mid a-b} \iff a \equiv b \pmod{m}$$

$$2 \mid 7-1 \iff 7 \equiv 1 \pmod{2}$$

$$m(x) \mid f(x)-g(x) \iff f(x) \equiv g(x) \pmod{m(x)}$$

$$x-a \mid \underline{f(x)-f(a)} \iff \underline{f(x) \equiv f(a) \pmod{x-a}}$$

$$☆ \begin{cases} f(x) \equiv f(a) \pmod{\underline{\underline{x-a}}} \\ f(x) \equiv f(b) \pmod{\underline{\underline{x-b}}} \end{cases} \qquad \underline{\underline{a \neq b}}$$

找一个解

Δ.

$$\frac{1}{b-a}\,(\underline{\underline{x-a}}) - \frac{1}{b-a}\,(\underline{\underline{x-b}}) = \frac{1}{\Delta}.$$

$$\underline{\frac{1}{b-a}(x-a)} \equiv 1 \pmod{\underline{\underline{x-b}}}$$

$$-\frac{1}{b-a}(x-b) \equiv 1 \pmod{x-a}.$$

$$\begin{cases} f(x) \equiv f(a) \pmod{x-a} \\ f(x) \equiv f(b) \pmod{x-b} \end{cases}$$

$$f(x) = \frac{1}{b-a}(x-a)f(b) + \frac{-1}{b-a}(x-b)f(a) + k(x)(x-a)(x-b).$$

Review of §5.2 Divisibility

Thm 6

Given conditions in Division Theorem, if we have $r(x) = 0$, i.e., $f(x) = q(x)g(x)$, we say that $g(x)$ divides $f(x)$ (or $g(x)$ is a divisor of $f(x)$), and we denote this as $g(x) \mid f(x)$. Otherwise, we write $g(x) \nmid f(x)$.

Notes: $g(x) \mid g(x)$? ✓ $f(x) \mid g(x)$. $g(x) \mid h(x) \Rightarrow f(x) \mid h(x)$ ✓

- 整除有自反性和传递性，以及相伴性(associate)：

$$f(x) \mid g(x), g(x) \mid f(x) \rightsquigarrow \exists\, c \in F, f(x) = cg(x);$$

$f(x) = g(x)h(x)$ $\deg g \le \deg f \Rightarrow \deg g = \deg f$.

- (整除与数域扩大无关) 若 $F \subseteq K$，在 $K[x]$ 中存在 $\tilde{q}(x) \in K[x]$ 满足

$\Rightarrow \deg f \geq \deg g$.

$\Rightarrow \tilde{q}(x) \in F[x]$ ①

$$f(x) = \tilde{q}(x)g(x) \rightsquigarrow \tilde{q}(x) = q(x).$$

②

例 7

(1) $f(x), g(x) \in F[x]$, $f(x^2) \mid g(x^2) \Rightarrow f(x) \mid g(x)$;

(2) $f(x), g(x) \in F[x]$, $f^2(x) \mid g^2(x) \Rightarrow f(x) \mid g(x)$;

(3) Given $a \neq 0, d, n \in \mathbf{N}^*$, $x^m - a^m \mid x^n - a^n \Leftrightarrow m \mid n$.

(1) 設:$g(x) = q(x)f(x) + r(x)$, $\deg r < \deg f$.

$f(x^2) \mid g(x^2) = \boxed{q(x^2)f(x^2)} + r(x^2)$ $\quad \deg r(x^2) < \deg f(x^2)$

$f(x^2) \mid f(x^2) \Rightarrow f(x^2) \mid r(x^2) \Rightarrow r(x^2) = 0 \Rightarrow r(x) = 0$.

Note: $f(x^n) \mid g(x^n) \Rightarrow f(x) \mid g(x)$

(2) $x \mid f(x) \Longleftrightarrow x^2 \mid f^2(x)$.

$\Leftarrow$: $f(x) = x\,q(x) + r$. $\quad x^2 \mid f^2(x) = x^2 q^2(x) + x \cdot 2r\,q(x) + r^2$.

$$\Rightarrow x^2 \mid x(2r\,g(x)) + r^2.$$

$$\Rightarrow x \mid x^2 \mid \underline{2rx\,g(x)} + r^2.$$

$$\Rightarrow \underline{\underline{x \mid r^2}} \Rightarrow \deg r^2 = 0. \Rightarrow r^2 = 0.$$

<deg>

(3). $x^m - a^m \mid x^n - a^n \iff m \mid n.$

1) $\boxed{m \mid n} \Rightarrow n = km$

$$x^n - a^n = x^{km} - a^{km} = (x^m)^k - (a^m)^k.$$

$$= (x^m - a^m)\left[\underbrace{(x^m)^{k-1} + (x^m)^{k-2}a + \cdots}\right] \checkmark.$$

zt.

2) $\boxed{n = km + r}$, $0 \le r < m$

$$x^m - a^m \mid x^n - a^n = x^{km+r} - a^{km+r}$$

$$- x^r a^{km} + x^r a^{km}$$

$$= (x^{km} - a^{km})x^r + a^{km}(x^r - a^r).$$

$\Rightarrow x^m - a^m \mid x^r - a^r$

$\boxed{r < m}$, $\Rightarrow x^r - a^r = 0$

$\Rightarrow r = 0$!

Examples

Slogan: $g(x) \mid f_k(x) \rightsquigarrow g(x) \,\Big|\, \sum_k h_k(x) f_k(x)$, For all $h_k(x) \in F[x]$.

例 8

(1) $x^2 + x + 1 \mid x^{3n} + x^{3m+1} + x^{3p+2}$, For all $n, m, p \in \mathbb{N}^*$;

(2) If $m, n, p \in \mathbb{N}^*$ have the same parity, prove that $x^2 - x + 1 \mid x^{3n} - x^{3m+1} + x^{3p+2}$. Check the converse of this proposition is also true.

Notes: $f(\omega_i) = 0 \Rightarrow x - \omega_i \mid f(x)$ $\quad \underline{\omega_1 \neq \omega_2}$ $\quad (x-\omega_1, x-\omega_2) = 1$

- (§5.5 Polynomial Functions) Alternative: $x^2 + x + 1 = (x - \omega_1)(x - \omega_2) = 0$, $\omega_i^3 = 1, \omega_i \neq 1 \rightsquigarrow \omega_i^{3n} + \omega_i^{3m+1} + \omega_i^{3p+2} = 1 + \omega_i^1 + \omega_i^2 = 0$.

  $(x-\omega_1)(x-\omega_2) \mid f(x)$

- When we have $x^2 + x + 1 \,\Big|\, \sum_i x^{a_i} \; (a_i \in \mathbb{N}^*)$?

(1) $x^2+x+1 \mid x^{3n}+x^{3m+1}+x^{3p+2}$, For all $n, m, p \in \mathbb{N}^*$;

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

$x^2+x+1 \mid x^3-1 \mid x^{3n}+x^{3m+1}+x^{3p+2}$? $+(x^2+x+1)$

$-1 \qquad -x \qquad -x^2$

$\boxed{x^{3m}-1^{3m}}$

$=(x^{3n}-1)+x(x^{3m}-1)+x^2(x^{3p}-1)+1(x^2+x+1)$

- When we have $\boxed{x^2+x+1} \mid \sum_i x^{a_i}$ $(a_i \in \mathbb{N}^*)$?

$\boxed{a_i \text{ 除3余 } 0, 1, 2 \text{ 个数相等.}}$

反之不等. a_i 除 0, 1, 2 个数为 m, n, p.

$\sum x^{a_i}$ $(a_i \geq 3)$ $=\sum(x^{3k_i+1}-x)+\sum(x^{3p_i+2}-x^2)+\sum(x^{3q_i}-1)$

$0 \leq a_i \leq 2$ $\quad + \; m\cdot 1+n\cdot x+p x^2.$

$$\Rightarrow \quad x^2+x+1 \mid m+nx+px^2.$$

$$\deg(x^2+x+1) = \deg(m+nx+px^2) = 2.$$

$$\Rightarrow (x^2+x+1) \sim (m+nx+px^2)$$

$$\Rightarrow c(x^2+x+1) = m+nx+px^2. \Rightarrow m=n=p=c.$$

matches 得证.

(2) If $m, n, p \in \mathbb{N}^*$ have the same parity, prove that $x^2 - x + 1 \mid x^{3n} - x^{3m+1} + x^{3p+2}$. Check the converse of this proposition is also true.

$x^2 - x + 1 \mid x^3 + 1 \mid x^{3k} + 1$ (k. ~~even~~ odd)

$\Rightarrow$

n.m.p 偶

$x^{3n} - x^3 - (x^{3m+1} - x^4) + (x^{3p+2} - x^5)$ $\underline{+x^3 - x^4 + x^5}$

$x^3(1 - x + x^2)$

$= x^3[x^{3(n-1)} - 1] - x^4[x^{3(m-1)} - 1] + x^5[x^{3(p-1)} - 1]$

$+x^3(1 - x + x^2)$

n.m.p 奇 显然.

$$x^2 - x + 1 \mid x^{3n} - x^{3m+1} + x^{3p+2}.$$

$\boxed{x^3 = -1}$ 5pδ -1

$$\underbrace{x^{3n} - x^{3m+1} + x^{3p+2}}_{f_1(x)} = \underbrace{(\underbrace{x^2 - x + 1}_{=0}) \cdot g(x)}_{f_2(x)}.$$

$\boxed{\text{在}\mathbb{C}\text{上}}$ $\omega_1.\ \omega_2.$ $\boxed{\omega_i^3 = -1}$ $\omega_i \neq 1$

$\boxed{\omega_i = \frac{1}{2} \pm \frac{\sqrt{3}}{2} i}$

$$\underset{\triangle}{\omega_i^{3n} - \omega_i^{3m+1} + \omega_i^{3p+2} = 0.}$$

$$\boxed{(-1)^n - (-1)^m \cdot \omega_i + (-1)^p \cdot \omega_i^2 = 0.}$$

若 n.m.p 不同奇偶性. $\Rightarrow \begin{cases} -1 - \omega_i + \omega_i^2 = 0. \\ \boxed{1 + \omega_i + \omega_i^2 = 0} \Rightarrow \omega_i^3 = 1. \ \times \\ 1 - \omega_i - \omega_i^2 = 0 \end{cases}$ 不成立.