本章主要讲述如下问题

- 环和同态
- 分式域
- 理想
- 多项式环

§10.1 环和同态

- **定义1** 设R是具有两种结合法(通常表示为加法(+)和乘法)的非空集合. R叫做**环**, 如果如下条件成立:

  i) R对于加法构成一个交换群;

  ii) (结合律) $\forall a,\ b,\ c \in R, (ab)c = a(bc)$;

  iii) (分配律) $\forall a,\ b,\ c \in R,$

  $$(a+b)c = ac + bc,\ a(b+c) = ab + ac.$$

- R叫做**交换环**, 如果R还满足

  (iv)(交换律) $\forall a, b \in R, ab = ba.$

- R叫做**有单位元环**, 如果R中有元素$e = 1_R$使得

  (v) $\forall a \in R$, 有 $a1_R = 1_R a = a.$

- **定理1** 设R是一个环. 则

  (i) 对任意$a \in R$, 有

$$0a = a0 = 0;$$

  (ii) 对任意$a, b \in R$, 有

$$(-a)b = a(-b) = -ab;$$

- **证** (i) 因为

$$0a = (0 + 0)a = 0a + 0a,$$

  所以$0a = 0$. 同样, $a0 = 0$.

  (ii) 因为

$$(-a)b + ab = ((-a) + a)b = 0a = 0,$$

$$a(-b) + ab = a((-b) + b) = a0 = 0,$$

  所以$(-a)b = a(-b) = -ab$.

- **定理1**(续) 设R 是一个环. 则

  (iii) 对任意$a, b \in R$, 有

$$(-a)(-b) = ab;$$

  (iv) 对任意$n \in \mathbf{Z}$, 任意$a, b \in R$, 有

$$(na)b = a(nb) = nab;$$

  (v) 对任意$a_i, b_j \in R$, 有

$$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j.$$

- **证** (iii), (iv) 和(v) 可有(i) 和(ii) 得到.

- **定理2** 设R 是有单位元的环. $a, b \in R$.
- (i) 如果$ab = ba$, 则$(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}$.
- **证** (i) 对n 用数学归纳法. 当$n = 1$时, 结论显然. 假设对$n = s$时成立, 即有$(a+b)^s = \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k}$. 则当$n = s+1$时有(注意到$ab = ba$)

$$
\begin{aligned}
& (a+b)^{s+1} \\
= & (a+b)^s (a+b) \\
= & \left(\sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k} \right) (a+b) \\
= & \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k} a + \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k+1} \\
= & \sum_{k=0}^{s-1} \left(\frac{s!}{k!(s-k)!} a^{k+1} b^{s-k} + \frac{s!}{(k+1)!(s-k)!} a^{k+1} b^{s-k} \right) + a^{s+1} + b^{s+1} \\
= & \sum_{k=0}^{s+1} \frac{(s+1)!}{k!(s+1-k)!} a^k b^{s+1-k}
\end{aligned}
$$

即对$n = s+1$结论也成立, 故定理成立.

- **定理2 (续)** (ii) 如果$a_i a_j = a_j a_i,\ 1 \le i, j \le r$, 则

$$(a_1 + \cdots + a_r)^n = \sum_{i_1+\cdots+i_r=n} \frac{n!}{i_1! \cdots i_r!} a_1^{i_1} \cdots a_r^{i_r}.$$

- **证** (ii) 对r用归纳法. 当$r = 2$时即为(i)的结论, 显然成立. 假设$r = m$时结论成立. 当$r = m + 1$时,由(i) 及归纳假设可得

$$(a_1 + \cdots + a_m + a_{m+1})^n = ((a_1 + \cdots + a_m) + a_{m+1})^n$$

$$= \sum_{i_{m+1}=0}^{n} \frac{n!}{i_{m+1}!(n-i_{m+1})!} (a_1 + \cdots + a_m)^{n-i_{m+1}} a_{m+1}^{i_{m+1}}$$

$$= \sum_{i_{m+1}=0}^{n} \frac{n!}{i_{m+1}!(n-i_{m+1})!} \sum_{i_1+\cdots+i_m=n-i_{m+1}} \frac{(n-i_{m+1})!}{i_1! \cdots i_m!} a_1^{i_1} \cdots a_m^{i_m} a_{m+1}^{i_{m+1}}$$

$$= \sum_{i_1+\cdots+i_m+i_{m+1}=n} \frac{n!}{i_1! \cdots i_m! \cdot i_{m+1}!} a_1^{i_1} \cdots a_m^{i_m} a_{m+1}^{i_{m+1}}$$

即得当$r = m + 1$时结论也成立.

- **例1** 整数环$\mathbf{Z}$.
- $\mathbf{Z}$ 对于加法$a+b$ 构成一个交换加群. 零元为0, a 的负元为$-a$.
- $\mathbf{Z}$ 对于乘法$a \cdot b$, 满足结合律和交换律, 有单位元1. 并且有分配律. 因此, $\mathbf{Z}$ 是有单位元的交换环.

- **例2** 设$\mathbf{R}$ 是有单位元的交换环.
- 给定多项式环$\mathbf{R}[X]$ 上两个多项式:

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

  $g(x) = b_n x^n + \cdots + b_1 x + b_0.$
- 在$\mathbf{R}[X]$ 上定义加法:

  $$(f+g)(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0),$$

  则$\mathbf{R}[X]$ 对于该加法构成一个交换加群.
- 零元为0,
- $f(x)$ 的负元为

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

- 设 $f(x)=a_nx^n+\cdots+a_1x+a_0, \quad a_n\neq 0,$
  $g(x)=b_mx^m+\cdots+b_1x+b_0, \quad b_m\neq 0,$
- 在$\mathbf{R}[X]$ 上定义乘法:

  $$(f\cdot g)(x)=c_{n+m}x^{n+m}+\cdots+c_1x+c_0,$$

  其中$c_k=\sum_{i+j=k}a_ib_j, 0\leq k\leq n+m$, 即

  $c_{n+m}=a_nb_m,\ c_{n+m-1}=a_nb_{m-1}+a_{n-1}b_m,\ \ldots,\ c_0=a_0b_0.$
- $\mathbf{R}[X]$ 对于该乘法, 满足结合律和交换律, 有单位元1. 并且有分配律.
- 因此, $\mathbf{R}[X]$ 是有单位元的交换环.

- **定义2** 设a 是环R 中的一个非零元. a 称为**左零因子**(对应地. **右零因子**) , 如果存在非零元$b \in R$ (对应地. $c \in R$) 使得$ab = 0$ (对应地. $ca = 0$), a 称为**零因子**, 如果它同时为左零因子和右零因子.
- **例4** $\mathbf{Z}/6\mathbf{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ 是一个有零因子环环. 因为$\overline{2} \cdot \overline{3} = 0$.

- **定义3** 设a 是有单位元1_R 的环R 中的一个元. a 称为**左逆元**(对应地. **右逆元**) , 如果存在元$b \in R$ (对应地. $c \in R$) 使得$ab = 1_R$ (对应地. $ca = 1_R$). 这时, b (对应地. c) 叫做a 的**右逆**(对应地. **左逆**). a 称为**逆元**, 如果它同时为左逆元和右逆元.

- **例5** 设整数D 无平方因子. 则

$$\mathbf{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbf{Z}\}$$

对于如下的加法和乘法构成有单位元的交换环.

加法:

$$(a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}.$$

乘法:

$$(a + b\sqrt{D}) \cdot (c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}.$$

$u = a + b\sqrt{D}$ 为可逆元的充要条件是

$$a^2 - b^2 D = \pm 1.$$

- **定义4** 设R 是一个交换环. 我们称R 为**整环**, 如果R 中有单位元, 但没有零因子.
- **例6** 整数环$\mathbf{Z}$ 是一个整环.
- **例7** 整数的多项式环$\mathbf{Z}[x]$ 是一个整环.
- **定义5** 我们称交换环R 为一个**域**, 如果R 中有单位元, 且每个非零元都是可逆元.

  即R 对于加法构成一个交换群,

  $R^* = R \setminus \{0\}$ 对于乘法构成一个交换群.
- **例8** 实数集$\mathbf{R}$ 是一个域.
- **例9** 设p 是一个素数. 则$\mathbf{F}_p$ 是一个域.

- **定义6** 设R 是一个交换环, $a,\ b \in R,\ b \neq 0$. 如果一个元素$c \in R$ 使得$a = bc$, 就称b **整除** a 或者a 被b 整除, 记作$b|a$. 这时, 把b叫做a 的**因子**, 把a 叫做b 的**倍元**.
- 如果$b,\ c$ 都不是单位元, 就b 称为a 的**真因子**.
- R 中的元素p 称为不可约元或素元, 如果p 不是单位元, 且没有真因子. 也就是说, 如果有元素$b,\ c \in R$ 使得$p = bc$, 则b 或c 一定是单位元.
- R 中的两个元素$a,\ b$ 称为**相伴**的, 如果存在可逆元$u \in R$ 使得$a = bu$.

- **定义7** 设$R,\ R'$ 是两个环. 我们称映射$f : R \longrightarrow R'$ 为**环同态**, 如果f 满足如下条件:

  (i) 对任意的$a,\ b \in I$, 都有$f(a+b) = f(a) + f(b)$;

  (ii) 对任意的$a,\ b \in I$, 都有$f(ab) = f(a)f(b)$.

  如果f 是一对一的, 则称f 为**单同态**; 如果f 是满的, 则称f 为**满同态**; 如果f 是一一对应的, 则称f 为**同构**.

- **定义8** 设$R,\ R'$ 是两个环. 我们称R 与R' 同构, 如果存在一个R 到R' 的同构.

- **定义9** 设R是一个环. 如果存在一个最小正整数p使得对任意$a \in R$, 都有

$$pa = \underbrace{a + \cdots + a}_{p\text{个}a} = 0,$$

则称环R的**特征**为p. 如果不存在这样的正整数, 则称环R的特征为0.

- **定理3** 如果域K的特征不为零, 则其特征比为素数.
- **证** 设域K的特征为p. 如果p不是素数, 则存在整数$1 < p_1,\ p_2 < p$, 使得$p = p_1 p_2$. 从而,

$$(p_1 1_{\mathbf{K}})(p_2 1_{\mathbf{K}}) = (p_1 p_2) 1_{\mathbf{K}} = 0.$$

因为域**K**无零因子, 所以$(p_1 1_{\mathbf{K}}) = 0$或$(p_2 1_{\mathbf{K}}) = 0$. 这与特征p的最小性矛盾. 证毕.

- **定理4** 设R 是有单位元的交换环. 如果环R 的特征是素数p, 则对任意$a,\ b \in R$, 有

$$(a+b)^p = a^p + b^p.$$

- **证** 根据定理2, 我们有

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k b^{p-k} + b^p.$$

对于$1 \leq k \leq p-1$, 有$(p,\ k!(p-k)!) = 1$, 从而$p \mid p\dfrac{(p-1)!}{k!(p-k)!}$. 这样, 由$R$ 的特征是素数p, 得到$\dfrac{p!}{k!(p-k)!} a^k b^{p-k} = 0$. 因此, 定理成立. 证毕.

- **定理5** 设p是一个素数. 设$f(x) = a_n x^n + \cdots + a_1 x + a_0$是整系数多项式. 则

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

- **证** 在域$\mathbf{F}_p$上的多项式环$\mathbf{F}_p[x]$上, 应用定理4, 有

$$\begin{aligned} f(x)^p &= (a_n x^n)^p + \cdots + (a_1 x)^p + a_0^p \\ &= a_n (x^p)^n + \cdots + a_1 (x^p) + a_0 \\ &= f(x^p). \end{aligned}$$

也就是,

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

§10.2 分式域

- 设A 是一个整环. 令$E = A \times A^*$.
- 在E 上定义关系R:

  $(a,b)R(c,d)$ 如果$ad = bc$.

  则R 是E 上的等价关系, 即有

  (i) 自反性: 对任意$(a,b) \in E$, 有$(a,b)R(a,b)$.

  (ii) 对称性: 如果$(a,b)R(c,d)$, 则$(c,d)R(a,b)$.

  (iii) 传递性: 如果$(a,b)R(c,d)$ 和$(c,d)R(e,f)$, 则$(a,b)R(e,f)$.

- 记 $\frac{a}{b} = C_{(a,b)} = \{(e,f) \mid \in E, (a,b)R(c,d)\}$ 为(a,b)的等价类.
- 在商集E/R 上定义加法和乘法如下:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

(这里需要说明上述定义的合理性)

- 则E/R 关于加法构成一个交换群,
  零元为$\frac{0}{b}$, $\frac{a}{b}$ 的负元为$\frac{-a}{b}$.
- $(E/R)^* = E/R \setminus \{\frac{0}{b}\}$ 关于乘法构成一个交换群,
  单位元为$\frac{b}{b}$, $\frac{a}{b}$ 的逆元为$\frac{b}{a}$.
  因此, E/R 构成一个域. 叫做A 的**分式域**.

- **例1** 取$A = \mathbf{Z}$, 则$\mathbf{Z}$ 是一个整环, 从而有分式域, 叫做$\mathbf{Z}$ 的**有理数域**, 记为$\mathbf{Q}$.

  例2 取$A = \mathbf{Z}/p\mathbf{Z}$, 其中$p$ 为素数. 则A 是一个整环, 从而有分式域, 叫做$\mathbf{Z}/p\mathbf{Z}$ 的$p-$ **元域**, 记为$\mathbf{F}_p$ 或$GF(p)$..

  例3 设K 是一个域. 则$A = \mathbf{K}[X]$ 是一个整环, 从而有分式域, 叫做$\mathbf{K}[X]$ 的**多项式分式域**, 记为$\mathbf{K}(X)$. 即

$$\mathbf{K}(X) = \left\{ \frac{f(X)}{g(X)} \mid f(X),\ g(X) \in \mathbf{K}[X],\ g(X) \neq 0 \right\}.$$

§10.3 理想

- **定义1** 设R是一个环, I是R的子环.
- I称为R的**左理想**, 如果对任意的$r \in R$和对任意的$a \in I$, 都有$ra \in I$.
- I称为R的**右理想**, 如果对任意的$r \in R$和对任意的$a \in I$, 都有$ar \in I$.
- I称为R的**理想**, 如果R同时为左理想和右理想.
- **例1** $\{0\}$和R都是R的理想, 叫做R的**平凡理想**.

- **定理1** 环R 的非空子集I 是左(对应地. 右)理想的充要条件是:

  (i) 对任意的$a, b \in I$, 都有$a - b \in I$;

  (ii) 对任意的$r \in R$ 和对任意的$a \in I$, 都有$ra \in I$. (对应地. $ar \in I$.)

- **证** 必要性是显然的. 我们证明充分性. 由(i) 和(ii) 立即知道I 是R 的子环.

- **推论** 设$\{A_i\}_{i\in I}$ 是环R 中的一族(左)理想. 则$\cap_{i\in I} A_i$ 也是一个(左)理想.

- **定义2** 设X 是环R 的一个子集. 设$\{A_i\}_{i\in I}$ 是环R 中包含X 的所有(左)理想. 则

$$\bigcap_{i\in I} A_i$$

  称为由X**生成的(左)理想**. 记为(X).

- X 中的元素叫做理想(X) 的**生成元**.
- 如果$X = \{a_1, \ldots, a_n\}$, 则理想(X) 记为$(a_1, \ldots, a_n)$, 称为**有限生成的**.
- 由一个元素生成的理想(a) 叫做**主理想**.

- **定理2** 设R 是交换环, $a \in R,\ X \subset R$. 则

  (i) 主理想(a) 为

$$(a) = \{ra + ar' + na + \sum_{i=1}^{m} r_i a s_i \mid r,\ s,\ r_i,\ s_i \in R,\ m \in \mathbf{N},\ n \in \mathbf{Z}\}.$$

  证 (i) 根据理想的定义, 易知

$$I = \{ra + ar' + na + \sum_{i=1}^{m} r_i a s_i \mid r,\ s,\ r_i,\ s_i \in R,\ m \in \mathbf{N},\ n \in \mathbf{Z}\}$$

  是一个包含a 的理想.

  同时, 包含a 的任一理想一定包含I, 所以$I = (a)$.

- **定理2** (续1) 设R 是交换环, $a \in R,\ X \subset R$. 则

(ii) 如果R 有单位元1_R 时, 则

$$(a) = \{ \sum_{i=1}^{m} r_i a s_i \mid r_i,\ s_i \in R,\ m \in \mathbf{N}, \}.$$

(iii) 如果a 在R 的中心, 则

$$(a) = \{ra + na \mid r \in R,\ n \in \mathbf{Z}\}.$$

证 (ii) 如果R 有单位元1_R , 则有

$$ra = ra1_R, \quad ar' = 1_R ar', \quad na = (n1_R)a.$$

因此, (ii) 成立.

(iii) 如果a 在R 的中心, 则有

$$ar' = r'a, \quad \sum_{i=1}^{m} r_i a s_i = (\sum_{i=1}^{m} r_i s_i)a.$$

因此, (iii) 成立.

- **定理2** (续2) 设R 是交换环, $a \in R,\ X \subset R$. 则
  (iv) $Ra = \{ra \mid r \in R\}$ 是R 中的的左理想.
  $aR = \{ar \mid r \in R\}$ 是R 中的的右理想.
  如果R 有单位元, 则$a \in Ra,\ a \in aR$.
  证 由(ii) 和(iii) 即可得到(iv). 证毕.
- 环R 叫做**主理想环**, 如果R 的所有理想都是主理想.

- **例2** $\mathbf{Z}$ 是主理想环.

  证 设I 是$\mathbf{Z}$ 中的一个非零理想. 当$a \in I$ 时, 有
  $0 = 0a \in I$ 及$-a = (-1)a \in I$.
  因此, I 中有正整数存在. 设d 是I 中的最小正整数, 则$I = (d)$. 事实上, 对任意$a \in I$, 存在整数q, r 使得

$$a = dq + r, \quad 0 \leq r < d.$$

  这样, 由$a \in I$ 及$dq \in I$, 得到

$$r = a - dq \in I.$$

  但$r < d$ 以及d 是I 中的最小正整数. 因此,
  $r = 0$, $a = dq \in (d)$. 从而$I \subset (d)$.
  又显然有$(d) \subset I$. 故$I = (d)$. 故$\mathbf{Z}$ 是主理想环.

- **例3** $\mathbf{Z}[X]$ 是主理想环.
- **例4** $\mathbf{Z}[\sqrt{-5}]$ 不是主理想环.

- **定理3** 设$A_1, A_2, \ldots, A_n$ 是环R 的(左)理想. 则
  (i) $A_1 + A_2 + \cdots + A_n$ 和$A_1A_2 \cdots A_n$ 是(左)理想.
- **证** (i) 对n用数学归纳法. 当$n = 1$时定理显然成立. 当$n = 2$时, $A_1 + A_2$ 是R的子加群, 对于$r \in R$, 及

$$x = x_1 + x_2 \in A_1 + A_2, \quad x_i \in A_i,$$

由于A_1, A_2是R的(左)理想, 故

$$rx = r(x_1+x_2) = rx_1+rx_2, \quad xr = (x_1+x_2)r = x_1r+x_2r$$

都属于$A_1 + A_2$, 从而$A_1 + A_2$是R的(左)理想.
假设对$n - 1$定理成立, 则由于

$$A_1+A_2+\cdots+A_{n-1}+A_n = (A_1+A_2+\cdots+A_{n-1})+A_n$$

故易知定理对n也成立.

- 根据$A_1A_2\cdots A_n$的定义,

$$A_1A_2\cdots A_n=\{\sum_{i=1}^{s}a_{1,i}a_{2,i}\cdots a_{n,i}\mid a_{1,i}\in A_1,\cdots,a_{n,i}\in A_n\},$$

易验证$A_1A_2\cdots A_n$满足(左)理想的两个条件, 即$A_1A_2\cdots A_n$也是(左)理想.

- **定理3**(续) 设$A, A_1, A_2, \ldots, A_n, B$ 和C 是环R 的(左)理想. 则

(ii) $(A+B)+C=A+(B+C)$.

(iii) $(AB)C=ABC=A(BC)$.

(iv) $B(A_1+A_2+\cdots+A_n)=BA_1+BA_2+\cdots+BA_n$,
$(A_1+A_2+\cdots+A_n)C=A_1C+A_2C+\cdots+A_nC$.

证 (ii),(iii),(iv)由理想的定义得到.

商环

- 设R 是一个环. I 是R 的一个理想.
- I 是$(R,+)$ 的一个正规子群. 因此, 对于加法运算

$$(a+I)+(b+I)=(a+b)+I,$$

商群R/I 存在.

- 在R/I 上可定义乘法运算: $(a+I)(b+I)=ab+I$. 事实上, 当$a+I=a'+I,\ b+I=b'+I$ 时, 有

$$a=a'+r_1,\ \ b=b'+r_2,\quad r_1,\ r_2\in I.$$

因为I 是理想, 所以$r_1b',\ a'r_2,\quad r_1r_2\in I$. 从而,

$$ab+I=(a'+r_1)(b'+r_2)+I=a'b'+r_1b'+a'r_2+r_1r_2+I=a'b'+I.$$

- 此外, R/I 中有结合律和分配律. 事实上, $\forall a+I$, $b+I$, $c+I \in R/I$, 有

$$\begin{aligned}(a+I)((b+I)(c+I)) &= (a+I)((bc)+I)\\ &= a(bc)+I\\ &= (ab)c+I\\ &= ((a+I)(b+I))(c+I)\end{aligned}$$

以及

$$\begin{aligned}((a+I)+(b+I))(c+I) &= ((a+b)+I)(c+I)\\ &= (a+b)c+I\\ &= (ac+I)+(bc+I)\\ &= (a+I)(c+I)+(b+I)(c+I),\end{aligned}$$

$$(a+I)((b+I)+(c+I)) = (a+I)(b+I)+(a+I)(c+I).$$

- **定理4** 设R 是一个环. I 是R 的一个理想. 则R/I 对于加法运算

$$(a+I)+(b+I)=(a+b)+I,$$

和乘法运算

$$(a+I)(b+I)=ab+I,$$

构成一个环. 当R 是交换环或有单位元时, R/I 也是交换环或有单位元.

证 当R是交换环时, 有

$$(a+I)(b+I)=ab+I=ba+I=(b+I)(a+I).$$

当R 有单位元e时,

$$(a+I)(e+I)=a+I.$$

因此, R/I 是交换环或有单位元. 证毕.

- **定理5** 设f 是环R 到环R' 的同态, 则f 的核$\ker(f)$是R 的理想. 反过来, 如果I 是环R 的理想, 则映射

$$\begin{aligned} s : R &\longrightarrow R/I \\ r &\longmapsto r+I \end{aligned}$$

是核为I 的同态.

- **证** 设f 是环R 到环R' 的同态, 则$\forall a \in R,\ b \in \ker(f)$, 有

$$f(a \cdot b) = f(a) \times f(b) = 0,$$

从而$a \cdot b \in \ker(f)$.

- 同理可得$b \cdot a \in \ker(f)$.
- 因此, $\ker(f)$是R 的理想.

- 反过来, 作映射$s : R \longrightarrow R/I,\ a \longmapsto a + I$. 则$s$ 是同态. 事实上, $\forall a, b \in R$, 有

$$s(a+b) = (a+b)+I = (a+I)+(b+I) = s(a)+s(b),$$

$$s(a\,b) = ab + I = (a+I)(b+I) = s(a)s(b).$$

对于$\forall (a+I) \in R/I$,有原像为a,故s为R到R/I的满同态. 进一步,

$$\ker(s) = \{a \mid a + I = I,\ a \in R\} = \{a \mid a \in I\} = I.$$

证毕.

映射$s : R \longrightarrow R/I$ 称为R 到R/I 自然同态.

- **定理6** 设f 是环R 到环R' 的同态, 则存在惟一的$R/\ker(f)$ 到像子环$f(R)$ 的同构$\overline{f} : a + \ker(f) \longmapsto f(a)$ 使得$f = i \circ \overline{f} \circ s$, 其中$s$ 是环R 到商环$R/\ker(f)$ 的自然同态, $i : c \longmapsto c$ 是$f(R)$ 到R' 的恒等同态. 即有如下的交换图:

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \mathbf{s}\downarrow & & \uparrow\mathbf{i} \\ R/\ker(f) & \xrightarrow{\overline{f}} & f(R) \end{array}$$

- 证 根据定理5, $\ker(f)$ 是环R 的理想, 所以存在商环$R/\ker(f)$. 现在要证明: $\overline{f} : a+\ker(f) \longmapsto f(a)$ 是$R/\ker(f)$ 到像子环$f(R)$ 的同构.
- 首先, $\overline{f}$ 是$R/\ker(f)$ 到像子环$f(R)$ 的同态. 事实上, 对任意的$a+\ker(f),\ b+\ker(f) \in R/\ker(f)$,

$$\begin{aligned}\overline{f}((a+\ker(f))(b+\ker(f)) &= \overline{f}((ab)+\ker(f)) = f(ab) = f(a)f(b)\\ &= \overline{f}(a+\ker(f))\overline{f}(b+\ker(f)).\end{aligned}$$

- 其次, $\overline{f}$ 是一对一.
- 最后, $\overline{f}$ 是满同态.
- 因此, $\overline{f}$ 是同构, 并且有$f = i \circ \overline{f} \circ s$.
- 此外, $\overline{f}$ 是惟一的. 若还有同构$g : R/\ker(f) \longrightarrow f(R)$ 使得$f = i \circ g \circ s$, 则对任意$a+\ker(f) \in R/\ker(f)$, 有

$$g(a+\ker(f)) = i(g(s(a))) = (i \circ g \circ s)(a) = f(a) = \overline{f}(a+\ker(f)).$$

因此, $g = \overline{f}$. 证毕.

- **定义3** 设P 是环R 的理想. P 称为R 的**素理想**, 如果$P \neq R$, 且对任意的理想$A, B,\ AB \subset P$, 有$A \subset P$ 或$B \subset P$.
- **定理7** 设P 是环R 的理想. 如果$P \neq R$, 且对任意的$a, b \in R$, 当$ab \in P$时, 有$a \in P$ 或$b \in P$, 则P 是素理想. 反过来, 如果P 是素理想, 且R 是交换环, 则上述结论也成立.

  证 必要性. 如果理想$A,\ B$ 使得$AB \subset P,\ A \not\subset P$, 则存在元素$a \in A,\ a \notin P$. 对任意元素$b \in B$, 根据假设, 从$ab \in AB \subset P$ 及$a \notin P$ 可得到$b \in P$. 这说明, $B \subset P$. 因此, P 是素理想.

  反过来, 设P 是素理想, 且R 是交换环, 则对任意的$a, b \in R$, 满足$ab \in P$, 有$(a)(b) = (ab) \subset P$. 根据素理想的定义, 我们有$(a) \subset P$ 或$(b) \subset P$. 由此得到, $a \in P$ 或$b \in P$. 证毕.

- **例5** 任意整环的零理想是素理想.
- **例6** 设p 是素数. 则$P = (p) = p\mathbf{Z}$ 是$\mathbf{Z}$ 的素理想.
- **证** 对任意的整数$a,\ b$, 若$ab \in P = (p)$, 则$p|ab$. 根据§1.4 定理2, 有$p|a$ 或$p|b$. 由此得到, $a \in P$ 或$b \in P$. 根据定理7, $P = (p) = p\mathbf{Z}$ 是$\mathbf{Z}$ 的素理想.

- **定理8** 在有单位元$1_R \neq 0$ 的交换环R 中, 理想P 是素理想的充要条件是商环R/P 是整环.
- **证** 因为环R 有单位元$1_R \neq 0$, 所以R/P 有单位元$1_R + P$ 和零元$0_R + P = P$. 又因为P 是素理想, 所以$1_R + P \neq P$. 现在说明R/P 无零因子. 事实上, 若$(a + P)(b + P) = P$, 则$ab + P = P$. 因此, $ab \in P$. 但P 是交换环R 的素理想, 根据定理7, 得到$a \in P$ 或$b \in P$, 即$a + P = P$ 或$b + P = P$ 是R/P 的零因子. 故商环R/P 是整环.

  反过来, 对任意的$a, b \in R$, 满足$ab \in P$, 有

$$(a + P)(b + P) = ab + P = P.$$

  因为商环R/P 是整环, 没有零因子, 所以$a + P = P$ 或$b + P = P$. 由此得到, $a \in P$ 或$b \in P$. 根据定理7, 理想P 是素理想. 证毕.

- **定义4** 设M 是环R 的(左)理想. M 称为R 的**最大(左)理想**, 如果$M \neq R$, 且对任意的理想N, 使得$M \subset N \subset R$, 有$N = M$ 或$N = R$.
- **定理9** 在有单位元的非零环R 中, 最大(左)理想总是存在的. 事实上, R 的每个(左)理想($\neq R$)都包含在一个最大(左)理想中.
- **定理10** 设R 是一个理想. 如果$R^2 = R$, (特别地, 如果R 有单位元), 则R 的每个最大理想是素理想.

  证 设$ab \in M$, 但$a \notin M$, $b \notin M$.

  因为$(a) + M$ 和$(b) + M$ 都是严格包含M 的理想, 所以$(a) + M = (b) + M$.

- **定理11** 设R是一个有单位元$1_R \neq 0$的环, M是R的一个理想.

  (i) 如果M是最大理想, 且R是交换环, 则商环R/M是一个域;

  (ii) 如果商环R/M是一个除子环, 则M是一个极大理想.

- **定理12** 设R是一个有单位元$1_R \neq 0$的交换环, 则如下条件等价:

  (i) R是的一个域.

  (ii) R没有真理想.

  (iii) 0是R的最大理想.

  (iv) 每个非零环同态$R \to R'$是单同态.

§10.4 多项式环

- 我们考虑整环R 上的全体多项式组成的集合$R[X]$.
  首先, 定义$R[X]$ 上的加法. 设

  $$f(x)=a_nx^n+\cdots+a_1x+a_0,\quad g(x)=b_nx^n+\cdots+b_1x+b_0,$$

  定义$f(x)$ 和$g(x)$ 的加法为

  $$(f+g)(x)=(a_n+b_n)x^n+\cdots+(a_1+b_1)x+(a_0+b_0),$$

  则$R[X]$ 中的零元为0,
  $f(x)$ 的负元为

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

- 其次, 定义$R[X]$ 上的乘法.

  设$f(x) = a_n x^n + \cdots + a_1 x + a_0,\ a_n \neq 0,$

  $g(x) = b_m x^m + \cdots + b_1 x + b_0,\ b_m \neq 0,$

  定义$f(x)$ 和$g(x)$ 的乘法为

  $$(f \cdot g)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0,$$

  其中$c_k = \sum_{i+j=k} a_i b_j, 0 \leq k \leq n+m,$ 即

  $c_{n+m} = a_n b_m,\ c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m,\ \ldots,\ c_0 = a_0 b_0,$

  则$R[X]$ 中的单位元为1.

  $R[X]$ 对于上述加法运算和乘法运算构成一个整环.

- **例1** 设$f(x)=x^6+x^4+x^2+x+1,\ g(x)=x^7+x+1\in \mathbf{F}_2[x]$, 则

$$f(x)+g(x)=x^7+x^6+x^4+x^2,$$

$$f(x)g(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1.$$

事实上 $(x^6+x^4+x^2+x+1)\cdot(x^7+x+1)$

$$\begin{aligned}&= x^{13}+x^{11}+x^9+x^8+x^7+x^7+x^5+x^3+x^2+x\\ &\quad +x^6+x^4+x^2+x+1\\ &= x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1\end{aligned}$$

- 设$f(x)=a_nx^n+\cdots+a_1x+a_0,\ a_n\neq 0$, 则称多项式$f(x)$ 的**次数**为n, 记为$\deg f=n$.
- **例2** $\mathbf{Z}[X]$ 中的$2x+3$ 的次数为1, x^2+2x+3 的次数为2, x^4+1 的次数为4, $x^8+x^4+x^3+x+1$ 的次数为8.

- **定义1** 设$f(x),\ g(x)$ 是整环R 上的任意两个多项式, 其中$g(x) \neq 0$. 如果存在一个多项式$q(x)$ 使得等式

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

成立, 就称$g(x)$ **整除** $f(x)$ 或者$f(x)$ 被$g(x)$ 整除, 记作$g(x)|f(x)$. 这时, 把$g(x)$叫做$f(x)$ 的**因式**, 把$f(x)$叫做$g(x)$ 的**倍式**. 否则, 就称$g(x)$ 不能整除$f(x)$ 或者$f(x)$ 不能被$g(x)$ 整除,记作$g(x) \nmid f(x)$.

- **例3** $\mathbf{Z}[X]$ 中的$2x+3 \mid 2x^2+3x$, $x^2+1 \mid x^4-1$.
- **定义2** 设$f(x)$ 是整环R 上的非常数多项式. 如果除了显然因式1 和$f(x)$ 外, $f(x)$ 没有其它因式, 那么, $f(x)$ 叫做**不可约多项式**, 否则, $f(x)$ 叫做**合式**.

多项式是否可约与所在的环或域相关.

- **例4** 多项式x^2+1 在$\mathbf{Z}[x]$ 中是不可约的, 但在$\mathbf{F}_2[x]$ 中是可约的.
- **例5** $\mathbf{F}_2[x]$ 中
- 一次不可约多项式为$x,\ x+1.$
- 二次不可约多项式为$x^2+x+1,$
- 可约多项式为$x^2,\ x^2+1=(x+1)^2,\ x^2+x=x(x+1).$
- 三次不可约多项式为$x^3+x+1,\ x^3+x^2+1,$
- 可约多项式为

  $x^3,\ x^3+x,\ x^3+x^2,\ x^3+x^2+x,$

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

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

- **定理1** 设$f(x)=a_nx^n+\cdots+a_0,\ g(x)=x^m+\cdots+b_0$是整环$R$上的多项式, 则存在$q(x)$和$r(x)$使得

$$f(x)=g(x)q(x)+r(x),\quad \deg r<\deg g.$$

- **定义3** (2) 式中的$q(x)$叫做$f(x)$被$g(x)$除所得的**不完全商**, $r(x)$叫做$f(x)$被$g(x)$除所得的**余式**.
- 定理1叫做**多项式欧几里得除法**.
- **定理1之证明** 对次数$\deg f=n$作归纳法.

  (i) 设$\deg f<\deg g$, 取$q(x)=0,\ r(x)=f(x)$. 成立.
- (ii) 设$\deg f\geq\deg g$. 假设结论对$\deg f<n$的多项式成立.

- (ii) 设$\deg f \geq \deg g$. 假设结论对$\deg f < n$ 的多项式成立. 对于$\deg f = n \geq \deg g$, 有

$$\begin{aligned} & f(x) - a_n x^{n-m} \cdot g(x) \\ = \ & (a_{n-1} - a_n b_{m-1}) x^{n-1} + \cdots + (a_{n-m} - a_n b_0) x^{n-m} \\ & + a_{n-m-1} x^{n-m-1} + \cdots + a_0. \end{aligned}$$

这说明$f(x) - a_n x^{n-m} \cdot g(x)$ 是次数$\leq n-1$ 的多项式. 对其运用归纳假设或情形(I), 存在整系数多项式$q_1(x)$ 和$r_1(x)$ 使得

$$f(x) - a_n x^{n-m} \cdot g(x) = g(x) q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x).$$

因此, $q(x) = a_n x^{n-m} + g_1(x)$, $r(x) = r_1(x)$ 为所求. 根据数学归纳法原理, 结论是成立的. 证毕.

- **推论1** 设$f(x)$ 是整环R 上的多项式, $a \in R$, 则存在多项式$q(x)$ 和常数$c = f(a)$ 使得

$$f(x) = (x - a)q(x) + f(a).$$

- **证** 根据定理1, 对于$f(x), g(x) = x - a \in R[x]$, 存在多项式$q(x), r(x)$ 使得

$$f(x) = g(x)q(x) + r(x), \quad \deg r < \deg g.$$

因为$\deg g = 1,\ \deg r < \deg g$, 所以$\deg r = 0,\ r(x) = c \in R$. 即有

$$f(x) = (x - a)q(x) + c.$$

特别, 取$x = a$, 有$c = f(a)$. 证毕.

- **推论2** 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$是整环$R$上的多项式, $a\in R$, 则$x-a|f(x)$的充要条件是$f(a)=0$.
- **证** 根据推论1, 存在$q(x)\in R[x]$, 使得

$$f(x)=(x-a)q(x)+f(a).$$

因此, $x-a|f(x)$的充要条件是$f(a)=0$. 证毕.

- **例6** 设$f(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$, $g(x)=x^8+x^4+x^3+x+1\in\mathbf{F}_2[x]$, 求$q_1(x)$和$r_1(x)$使得

$$f(x)=g(x)q_1(x)+r_1(x),\quad \deg r_1<\deg g_1.$$

- **解** 逐次消除最高次项,

$$\begin{aligned}&x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1\\&-x^5(x^8+x^4+x^3+x+1)\\=\ &x^{11}+x^4+x^3+1,\\&x^{11}+x^4+x^3+1-x^3(x^8+x^4+x^3+x+1)\\=\ &x^7+x^6+1.\end{aligned}$$

因此, $q_1(x)=x^5+x^3$, $r_1(x)=x^7+x^6+1$.

- 类似于整数中的最大公因数和最小公倍数, 我们可以给出多项式环$R[x]$ 中的最大公因式和最小公倍式.
- 设$f(x),\ g(x) \in R[x]$. $d(x) \in R[x]$ 叫做$f(x),\ g(x)$ 的**最大公因式**, 如果

  (1) $d(x)|f(x),\ d(x)|g(x)$.

  (2) 若$h(x)|f(x),\ h(x)|g(x)$, 则$h(x)|d(x)$.

  $f(x),\ g(x)$ 的最大公因式记作$(f(x), g(x))$.
- 当考虑域**K** 上的最大公因式时, 约定其最高次项系数为1, 则最大公因式是惟一的.

- 设$f(x),\ g(x) \in R[x]$. $D(x) \in R[x]$ 叫做$f(x),\ g(x)$ 的**最小公倍式**, 如果

  (1) $f(x)|D(x),\ g(x)|D(x)$.

  (2) 若$f(x)|h(x),\ g(x)|D(x)$, 则$D(x)|h(x)$.

  $f(x),\ g(x)$ 的最小公倍式记作$[f(x), g(x)]$.

  当考虑域$\mathbf{K}$ 上的最小公倍式时, 约定其最高次项系数为1, 则最小公倍式是惟一的.

- **引理1** 设$f(x),\ g(x),\ h(x)$ 是域$\mathbf{K}$ 上的三个非零多项式. 如果$f(x)=q(x)g(x)+h(x)$, 其中$q(x)$ 是域$\mathbf{K}$ 上的多项式, 则$(f(x),g(x))=(g(x),h(x))$.

  证 设$d(x)=(f(x),g(x)),\ d'(x)=(g(x),h(x))$, 则$d(x)|f(x),\ d(x)|g(x)$. 进而

$$d(x)|f(x)+(-q(x))g(x)=h(x),$$

  因此, $d(x)$ 是$g(x),\ h(x)$ 的公因式, $d(x)|d'(x)$.

  同理, $d'(x)$ 是$f(x),\ g(x)$ 的公因式, $d'(x)|d(x)$.

  因此, $d(x)=d'(x)$. 于是, 引理1 成立.

- **多项式广义欧几里得除法** 设$f(x),\ g(x)$ 是域**K** 上多项式, $\deg g \geq 1$. 记$r_{-2}(x) = f(x),\ r_{-1}(x) = g(x)$. 反复运用多项式欧几里得除法, 有

$$
\begin{aligned}
r_{-2}(x) &= q_0(x)r_{-1}(x) + r_0(x), && 0 \leq \deg r_0 < \deg r_{-1},\\
r_{-1}(x) &= q_1(x)r_0(x) + r_1(x), && 0 \leq \deg r_1 < \deg r_0,\\
r_0(x) &= q_2(x)r_1(x) + r_2(x), && 0 \leq \deg r_2 < \deg r_1,\\
r_1(x) &= r_2(x)q_2(x) + r_3(x), && 0 \leq \deg r_3 < \deg r_2,\\
&\cdots\cdots\\
r_{k-4}(x) &= q_{k-2}(x)r_{k-3}(x) + r_{k-2}(x), && 0 \leq \deg r_{k-2} < \deg r_{k-3},\\
r_{k-3}(x) &= q_{k-1}(x)r_{k-2}(x) + r_{k-1}(x), && 0 \leq \deg r_{k-1} < \deg r_{k-2},\\
r_{k-2}(x) &= q_k(x)r_{k-1}(x) + r_k(x), && r_k(x) = 0.
\end{aligned}
$$

经过有限步骤, 必然存在k 使得$r_k(x) = 0$, 这是因为

$$0 \leq \deg r_{k-1} < \deg r_{k-2} < \ldots < \deg r_1 < \deg r_0 < \deg r_{-}$$

且$\deg g$是有限正整数.

- **定 理2** 设$f(x),\ g(x) \in \mathbf{K}[x]$，$\deg g \geq 1$, 则$(f(x), g(x)) = r_k(x)$, 其中$r_k(x)$ 是多项式广义欧几里得除法中最后一个非零余式.
- **证** 应用引理1, 有

$$\begin{aligned}(f(x), g(x)) &= (r_{-2}(x), r_{-1}(x)) \\ &= (r_{-1}(x), r_0(x)) \\ &= (r_0(x), r_1(x)) \\ &= \quad \cdots \\ &= (r_{k-2}(x), r_{k-1}(x)) \\ &= (r_{k-1}(x), 0). \\ &= r_{k-1}(x).\end{aligned}$$

证毕.

- **定理3** 设$f(x),\ g(x) \in \mathbf{K}[x]$,则存在$s(x),\ t(x) \in \mathbf{K}[x]$使得

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

- **证**

$$r_0(x) = r_1(x)q_1(x) + r_2(x) \tag{1}$$

$$r_1(x) = r_2(x)q_2(x) + r_3(x) \tag{2}$$

由(1.2)得

$$\begin{aligned} r_0(x)q_2(x) &= r_1(x)q_1(x)q_2(x) + r_2(x)q_2(x) \\ &= r_1(x)q_1(x)q_2(x) + r_1(x) - r_3(x) \end{aligned} \tag{3}$$

即存在$r_0(x)$和$r_1(x)$的组合,使得$r_0(x)f_1(x) + r_1(x)g_1(x) = r_3(x)$,用归纳法,假设$r_4(x), r_5(x), \cdots, r_{k-1}(x)$都可以由$r_0(x)$和$r_1(x)$的上述形式组合得到,则由$r_{k-2}(x) = r_{k-1}(x)q_{k-1}(x) + r_k(x)$得

- **例7** 设$f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1,\ g(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbf{F}_2[x]$, 求多项式$s(x),\ t(x)$ 使得

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

- **解** 运用广义多项式欧几里得除法, 我们有

$$\begin{aligned}
&f(x) = g(x)q_1(x) + r_1(x), && q_1(x) = x^5 + x^3, && r_1(x) = x^7 \\
&g(x) = r_1(x)q_2(x) + r_2(x), && q_2(x) = x + 1, && r_2(x) = x^6 \\
&r_1(x) = r_2(x)q_3(x) + r_3(x), && q_3(x) = x + 1, && r_3(x) = x^5 \\
&r_2(x) = r_3(x)q_4(x) + r_4(x), && q_4(x) = x, && r_4(x) = x^3 \\
&r_3(x) = r_4(x)q_5(x) + r_5(x), && q_5(x) = x^2, && r_5(x) = 1.
\end{aligned}$$

- 从而,

$$\begin{aligned} r_5(x) &= r_3(x) + q_5(x)(r_2(x) + r_3(x)q_4(x)) \\ &= -q_5(x)r_2(x) + (x^3+1)(r_1(x) + r_2(x)q_3(x)) \\ &= (x^3+1)r_1(x) + (x^4+x^3+x^2+x+1)(g(x)+r \\ &= (x^4+x^3+x^2+x+1)g(x) + (x^5+x^3)(f(x)+g \\ &= (x^5+x^3)f(x) + (x^{10}+x^6+x^4+x^3+x^2+x+ \end{aligned}$$

因此, $s(x) = x^5 + x^3$, $t(x) = x^{10} + x^6 + x^4 + x^3 + x^2 + x + 1$.

- **定义4** 给定$R[X]$中一个首一多项式$m(x)$. 两个多项式$f(x)$, $g(x)$叫做 模$m(x)$ **同余**, 如果$m(x) \mid f(x) - g(x)$. 记作$f(x) \equiv g(x) \pmod{m(x)}$. 否则, 叫做模$m(x)$ **不同余**. 记作$f(x) \not\equiv g(x) \pmod{m(x)}$.
- 根据定理1, 任一多项式$f(x)$ 都与其被$m(x)$ 除的余式$r(x)$ 模$m(x)$ 同余, 该余式$r(x)$ 叫做$f(x)$ 模$m(x)$ 的**最小余式**, 记为$(f(x) \pmod{m(x)})$.
- 设$p(x)$ 是$R[X]$ 中的多项式, 则$(p(x)) = \{f(x) \mid p(x)|f(x)\}$ 是$R[X]$ 中的理想. 由此得到商环$R/(p(x))$. 该商环上的运算法则为:

  加法:

$$f(x) + g(x) = ((f+g)(x) \pmod{p(x)}),$$

  乘法:

$$f(x)g(x) = ((fg)(x) \pmod{p(x)}).$$

- **例8** 设$n \geq 1$, S 是有单位元环R 的子集. 设$p(x) \in R[x]$, 满足$p(x)|p(x^n)$. 如果在$R[x]$ 中, 对$\forall b \in S$, 有$(x+b)^n \equiv x^n + b \pmod{p(x)}$. 则对任意整数$k \geq 0$, 有$(x+b)^{n^k} \equiv x^{n^k} + b \pmod{p(x)}$.
- **证** 对k 作数学归纳法. $k = 0$ 时, 结论显然成立.
  $k = 1$ 时, 就是假设条件$(x+b)^n \equiv x^n + b \pmod{p(x)}$. 结论成立.

  假设k 时, 结论成立, 即$(x+b)^{n^k} \equiv x^{n^k} + b \pmod{p(x)}$.
  两端作n 次方, 有$(x+b)^{n^{k+1}} \equiv (x^{n^k} + b)^n \pmod{p(x)}$.
  根据假设,
  用x^{n^k} 代替x, 有$(x^{n^k} + b)^n \equiv (x^{n^k})^n + b \equiv x^{n^{k+1}} + b \pmod{p(x^{n^k})}$.
  但由假设, 有$p(x)|p(x^n)$, 进而$p(x^n)|p(x^{n^2}), \ldots, p(x^{n^{k-1}})|p$
  因此, $p(x)|p(x^{n^k})$, $(x^{n^k} + b)^n \equiv (x^{n^k})^n + b \equiv x^{n^{k+1}} + b \pmod{p(x)}$.
  故$(x+b)^{n^{k+1}} \equiv (x^{n^k})^n + b \equiv x^{n^{k+1}} + b \pmod{p(x)}$.
  即对于$k+1$ 结论成立. 根据归纳法原理, 结论对任

- **例9** 设$n, r \geq 2$是整数, S是环$R = \mathbf{Z}/n\mathbf{Z}$的子集. 如果在多项式环$R[x]$中, 对所有的$b \in S$, 都有

$$(x+b)^n \equiv x^n + b \,(\mathrm{mod}\, x^r - 1).$$

则对任意整数$k \geq 0$, 有

$$(x+b)^{n^k} \equiv x^{n^k} + b \,(\mathrm{mod}\, x^r - 1).$$

证 在例8中取$p(x) = x^r - 1$即得结论.

- **例10** 设$n, m, r \geq 2$是整数. 如果$m \equiv n \pmod{r}$, 则对任意多项式$g(x)$, 有

$$g(x^m) \equiv g(x^n) \pmod{x^r - 1}.$$

- **证** 不妨设$m \geq n$. 因为$m \equiv n \pmod{r}$, 所以存在整数$k \geq 0$使得$m = kr + n$.

  $k = 0$时, 结论显然成立. $k \geq 1$时, 设$g(x) = \sum_{i=0}^{N} b_i x^i$, 则

$$g(x^m) - g(x^n) = \sum_{i=0}^{N} b_i x^{in}((x^r)^{ik} - 1)$$

$$= (x^r - 1)\sum_{i=0}^{N} b_i x^{in}((x^r)^{ik-1} + \cdots + x^r + 1).$$

  因此, 结论成立.

- **定理4** 设$\mathbf{K}$ 是一个域. $p(x)$ 是$\mathbf{K}[X]$ 中的不可约多项式. 则商环$\mathbf{K}[X]/(p(x))$ 对于上述运算法则构成一个域.
- **证** 我们只需证明$\mathbf{K}[X]/(p(x))$ 中的非零元$f(x) \pmod{p(x)}$ 为可逆元. 事实上, 对于满足$f(x) \not\equiv 0 \pmod{p(x)}$ 的多项式$f(x)$, 有$(f(x), p(x)) = 1$. 根据定理3 , 存在多项式$s(x)$, $t(x)$ 使得

$$s(x)f(x) + t(x)p(x) = 1.$$

从而,

$$s(x)f(x) \equiv 1 \pmod{p(x)}.$$

这说明$f(x) \pmod{p(x)}$ 为可逆元, $s(x) \pmod{p(x)}$ 为其逆元.

- **例11** 设$\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$ 是一个有限域, 其中p 是素数. 设$p(x)$ 是$\mathbf{K}[X]$ 中的n 次不可约多项式, 则

$$\mathbf{K}[X]/(p(x)) = \{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in \mathbf{K}\}.$$

记为$\mathbf{F}_{p^n}$. 这个域的元素个数为p^n.

$\mathbf{F}_{p^n}$ 中的加法和乘法是:

$$f(x) + g(x) = ((f+g)(x) \pmod{p(x)}),$$

$$f(x)g(x) = ((fg)(x) \pmod{p(x)}).$$

- **例12** 设$\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. 则$p(x) = x^8 + x^4 + x^3 + x + 1$ 是$\mathbf{F}_2[X]$ 中的8 次不可约多项式. 事实上, 我们有

  $$\mathbf{F}_{2^8} = \mathbf{F}_2[X]/(x^8+x^4+x^3+x+1) = \{a_7x^7+\cdots+a_1x+a_0 \mid a$$

  $\mathbf{F}_{2^8}$ 中的加法和乘法是:

  $$f(x)+g(x) = ((f+g)(x) \pmod{x^8+x^4+x^3+x+1}),$$

  $$f(x)g(x) = ((fg)(x) \pmod{x^8+x^4+x^3+x+1}).$$

习题

- 1. **例12** 设$\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. 则$p(x) = x^8 + x^4 + x^3 + x + 1$是$\mathbf{F}_2[X]$ 中的8 次不可约多项式. 事实上, 我们有

  $$\mathbf{F}_{2^8} = \mathbf{F}_2[X]/(x^8+x^4+x^3+x+1) = \{a_7x^7+\cdots+a_1x+a_0 \mid a$$

  $\mathbf{F}_{2^8}$ 中的加法和乘法是:

  $$f(x)+g(x) = ((f+g)(x) \pmod{x^8+x^4+x^3+x+1}),$$

  $$f(x)g(x) = ((fg)(x) \pmod{x^8+x^4+x^3+x+1}).$$