第十五次作业

1. 证明：任意有限整环 R 是一个域.

Pf. 即证 $\forall a \in R\setminus\{0\}$ $\exists b \in R\setminus\{0\}$ s.t. $ab=ba=1$ (交换律自然满足).

若 $a=1$ 则 $b=1$ 为 a 逆.

若 $a\neq 1$ 由环中乘法封闭性可知 $a, a^2, \cdots a^n \cdots \in R$

$\because R$ 为有限整环 $\therefore \exists i,j \in \mathbb{Z}^+$ s.t. $i\neq j$ 且 $a^i = a^j$，不妨设 $i<j$

则 $a^i(1-a^{j-i}) = 0$ $\because R$ 是整环且 $a\neq 0$ (有消去律)

$\therefore 1 = a^{j-i}$ 若 $j-i=1$ 则 $a=1$ 与 $a\neq 1$ 矛盾

$\therefore j-i>1$ 则 $a^{j-i-1}\cdot a = 1$ 令 $b = a^{j-i-1}$ 即满足 $ab=ba=1$. □.

设 $R=\{r_1,\cdots r_n\}$

$\forall r_i \in R\setminus\{0\}, r_i\cdot r_j \neq r_i\cdot r_j$ 对于 $i\neq j$

$\therefore |\{r_1r_i, \cdots r_nr_i\}| = n$ 且已含于 R

$\therefore R = \{r_1r_i,\cdots r_nr_i\} \Rightarrow \exists j\in\{1,\cdots n\}$ s.t. $r_ir_j = 1\cdot a$.

2. 素数 p. 交换幺环 R，若 $\forall x\in R$ 均有 $px=0$ 则 $(x+y)^{p^m} = x^{p^m} + y^{p^m}$

对 $\forall m\in\mathbb{Z}^+$ 和 $x,y\in R$ 成立.

Pf 对 m 用归纳法：$m=1$ 时 $(x+y)^p = x^p + y^p + \sum_{i=1}^{p-1}\binom{p}{i}x^i y^{p-i}$ (有交换律)

$\because p \mid \binom{p}{i}$ 对 $\forall i=1,2\cdots p-1$ 均成立 ($\binom{p}{i} = \frac{p}{p-i}\cdot\binom{p-1}{i}$) $\therefore px \mid \binom{p}{i}x^i y^{p-i}$

$\therefore (x+y)^p = x^p + y^p$ (或直接利用 Freshmen's dream)

假设 $m-1$ 时等式成立 则 $(x+y)^{p^m} = \left((x+y)^{p^{m-1}}\right)^p = \left(x^{p^{m-1}} + y^{p^{m-1}}\right)^p$

$= (x^{p^{m-1}})^p + (y^{p^{m-1}})^p = x^{p^m} + y^{p^m}$ □

$\left(p^m \mid \binom{p^m}{k}\right)$

3. 环 R，非零 $x\in R$ 称为幂零元. 若 $\exists n\in\mathbb{N}$ s.t. $x^n = 0$

证明 (1) 若 x 是幂零元，则 $1-x$ 是可逆元.

(2) 环 $\mathbb{Z}_m$ 中含有幂零元 $\Leftrightarrow$ 存在整数 $s>1$ s.t. $s^2 \mid m$.

Pf. (1) 若 $x=0$ 则 1 是可逆元显然 (一般幂零元不为零 0)

若 $x\neq 0$ 且 x 是幂零元 则 $\exists n\in\mathbb{N}$ s.t. $x^n=0$ 且 $\because x\neq 0$ $\therefore n>1$.

则 $1-x^n = 1 = (1-x)(1+x+\cdots+x^{n-1}) = (1+x+\cdots+x^{n-1})(1-x)$

$\therefore 1-x$ 可逆.

(2) (⇐) 不妨设 $m = s^2 \cdot t$ $(m>1, t\in\mathbb{Z}^+)$ ∵ $st < m$ ∴ 在环 $\mathbb{Z}_m$ 中

$\bar{st} \neq \bar{0}$ 但 $(\bar{st})^2 = \bar{s}^2\bar{t}^2 = \bar{m}\cdot\bar{t} = \bar{0}$ ∴ $\bar{st}$ 为 $\mathbb{Z}_m$ 中幂零元.

(⇒) 设 $\bar{x}\in\mathbb{Z}_m$ 为幂零元 且 $\bar{x}^n = \bar{0}$ $(n\in\mathbb{N})$ 即 $m\nmid x$ 且 $m\mid x^n$.

下证 m 可被一个大于1的整数平方整除.

(反证) 假设 m 无平方因子. 考虑 m 的素分解 $m = p_1 p_2 \cdots p_s$

其中 $p_i \neq p_j$ 如果 $i\neq j$ ∵ $m\mid x^n$ ∴ 对 $\forall i=1,2\cdots s$ 均有 $p_i \mid x^n$

又∵ p_i 为素数 ∴ $p_i \mid x$ 则 $\mathrm{lcm}(x_1,\cdots x_s)\mid x$ ⇒ $m\mid x$ ⇒ $\bar{x}=\bar{0}$ →←

4. 环 R. 若 $\forall x\in R$ 均有 $x^2 = x$ 证明 R 为交换环.

($2=1+1=(1+1)^2=4$ ⇒ $2=0$ 即 $1=-1$)

证. $\forall x\in R$ $(x+x)^2 = x+x = 2x$ ⇒ $2x=0$ ⇒ $x=-x$

$(x+x)^2 = 4x^2 = 4x$

又 $\forall x,y\in R$ $(x+y)^2 = x+y = x^2+xy+yx+y^2 = x+y+xy+yx$

⇒ $xy = -yx = yx$ ∴ R 为交换环.

5. 环 R. $a,b\in R$. 证明: 若 $1-ab$ 可逆 则 $1-ba$ 可逆. (提示: 逆为 $1+bca$ 其中 $c=(1-ab)^{-1}$)

证. 要证 $1-ba$ 可逆 即 求 $x\in R$ s.t. $\begin{cases}(1-ba)x=1\\ x(1-ba)=1\end{cases}$

∵ $1-ab$ 可逆. 不妨设逆为 c 即 $(1-ab)c = c(1-ab)=1$.

若 $(1-ba)x=1$ ⇒ $a(1-ba)x = a$ ⇒ $(a-aba)x=a$ ⇒ $(1-ab)ax=a$

∵ $1-ab$ 的逆为 c 两边左乘 c 得 $ax = ca$

再两边右乘 b 得 $bax = bca$ ⇒ $x - bax = x - bca$ ⇒ $x = 1+bca$

$(1-ba)x = 1$

∴ $1+bca$ 为 $1-ba$ 的左逆. 同理可证 也为右逆 ∴ $(1-ba)^{-1} = 1+bca$. □

6. $f = \bar{2}x^2 + x + \bar{4}$. $g = \bar{3}x^3 + \bar{5}x$, $h = x+\bar{3}\in\mathbb{Z}_6[x]$. 求 fg, gh 的次数.

解 $fg = \bar{6}x^5 + (\bar{10}+\bar{15})x^3 + (\bar{12}+\bar{5})x^2 + \bar{20}x = \bar{3}x^4 + \bar{4}x^3 + \bar{5}x^2 + \bar{2}x$

$gh = \bar{3}x^4 + \bar{9}x^3 + (\bar{5}+\bar{15})x^2 + \bar{15}x = \bar{3}x^4 + \bar{3}x^3 + \bar{5}x^2 + \bar{3}x$

∴ $4 = \deg(fg) < \deg(f)+\deg(g) = 5$ $3 = \deg(gh) = \deg(g)+\deg(h) = 3$ □.

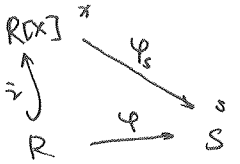
§1 多项式的赋值同态

Thm1 赋值同态定理

设交换环 R, S，环同态 $\varphi: R \to S$ 和元素 $s \in S$，则

$\exists!$ 环同态 $\varphi_s: R[x] \to S$ 满足 $\varphi_s|_R = \varphi$ 和 $\varphi_s(x) = s$

注：



$$\varphi_s\left(\sum_{i=0}^{d} f_i x^i\right) = \sum_{i=0}^{d} \varphi(f_i)\cdot s^i$$

Cor 1. $\pi_{\bar{m}}: \mathbb{Z}[x] \to \mathbb{Z}_n$ 是环同态.

$f(x) \mapsto f(\bar{m})$

2. $\rho_A: F[x] \to F[A]$ 是环同态.

$f(x) \mapsto f(A)$

例1 设域 F，$a, b \in F$ 且 $a \neq 0$ 定义映射 $\varphi_{ab}: F[x] \to F[x]$，$f(x) \mapsto f(ax+b)$ $\forall f \in F[x]$.

(且 $\varphi_{ab}|_F = id_F$)，证明 φ_{ab} 是自同构.

Pf: 考虑环同态 $i: F \to F[x]$ (嵌入) 和元素 $ax+b \in F[x]$

$f \mapsto f$

由 Thm1 可知 $\exists!$ 环同态 $\varphi: F[x] \to F[x]$ 满足 $\varphi|_F = i = id_F$

和 $\varphi(x) = ax+b$ 由题设和唯一性可知 $\varphi = \varphi_{ab}$ 是个环同态.

下面证双射：单：设 $f = \sum_{i=0}^{d} f_i x^i \in \ker(\varphi_{ab})$ 即 $\sum_{i=0}^{d} f_i (ax+b)^i = 0$

则首项系数为 $f_d \cdot a^d = 0$ $\because a \neq 0$ $\therefore f_d = 0 \Rightarrow f = 0$ $\therefore$ 单.

满：$\forall g(x) \in F[x]$ 设 $g(x) = \sum_{i=0}^{l} g_i x^i$ 令 $f(x) = \sum_{i=0}^{l} g_i (a^{-1}(x-b))^i$

则 $\varphi_{ab}(f) = \sum_{i=0}^{l} g_i [a(a^{-1}(x-b))+b]^i = \sum_{i=0}^{l} g_i x^i = g$ $\therefore$ 满.

综上 φ_{ab} 是自同构. □

注：$\forall f, g \in F[x]$. $\varphi_{ab}(f+g) = (f+g)(ax+b) = f(ax+b) + g(ax+b) = \varphi_{ab}(f) + \varphi_{ab}(g)$

$$\varphi_{ab}(f\cdot g) = \varphi_{ab}\left(\sum_{i=0}^{d} f_i x^i \cdot g(x)\right) = \sum_{i=0}^{d} \varphi_{ab}(f_i x^i \cdot g) = \sum_{i=0}^{d} \varphi_{ab}\left(f_i x^i \cdot \sum_{j=0}^{l} g_j x^j\right)$$

$$= \sum_{i=0}^{d} \varphi_{ab}\left(\sum_{j=0}^{l} f_i g_j x^{i+j}\right) = \sum_{i=0}^{d}\sum_{j=0}^{l} \varphi_{ab}(f_i g_j x^{i+j}) = \sum_{i=0}^{d}\sum_{j=0}^{l} f_i g_j (ax+b)^{i+j}$$

$= \varphi_{ab}(f)\cdot\varphi_{ab}(g)$ 且 $\varphi_{ab}(1) = 1$ $\therefore$ φ_{ab} 是环同态.

例2. 矩阵 $A, B \in M_n(\mathbb{R})$ 求证 $(AB)^\vee = B^\vee A^\vee$.

证. 利用赋值同态:

对 $\forall\ A \in M_n(\mathbb{R})$, 引入未定元 t. 考虑为矩阵 $A+tE \in M_n(\mathbb{R}(t))$

其中 $\mathbb{R}(t)$ 为关于 t 的有理函数域 (也可看成多项式环 $\mathbb{R}[x]$ 的分式域)

且 $\mathbb{R}(t) := \{ \frac{a(t)}{b(t)} \mid a, b \in \mathbb{R}[t] \text{ 且 } b \neq 0 \}$

令 $C = A+tE = (c_{ij})_{n\times n}$ 则 $|C| = \sum_{\sigma \in S_n} \varepsilon_\sigma \cdot c_{\sigma(1),1} \cdots c_{\sigma(n),n}$

$\therefore |C| = c_{11}\cdots c_{nn} + \sum_{\substack{\sigma\in S_n \\ \sigma \neq id}} \varepsilon_\sigma \cdot c_{\sigma(1),1}\cdots c_{\sigma(n),n}$

$= \prod_{i=1}^{n}(a_{ii}+t) + \sum_{\sigma\neq id} \varepsilon_\sigma c_{\sigma(1),1}\cdots c_{\sigma(n),n}$

若 $\sigma \neq id$ 则 $c_{\sigma(1),1}, \cdots$ 每 $c_{\sigma(n),n}$ 中至多有 $n-2$ 个含 t 项相乘.

$\therefore |C| = t^n + \text{Lowerterms}$. 是一个 n 次多项式 $\therefore |C| \neq 0$ (在 $\mathbb{R}(t)$ 中).

$\therefore A+tE$ 在 $M_n(\mathbb{R}(t))$ 中可逆. 同理 $B+tE$ 也可逆.

$\therefore (A+tE)\cdot(B+tE)$ 可逆. 对于可逆矩阵, 我们有 $C^\vee = |C|\cdot C^{-1}$

$\therefore ((A+tE)(B+tE))^\vee = |(A+tE)\cdot(B+tE)| \cdot ((A+tE)(B+tE))^{-1}$

$= |A+tE|\cdot|B+tE|\cdot(B+tE)^{-1}\cdot(A+tE)^{-1}$

$= (B+tE)^\vee \cdot (A+tE)^\vee$ (直接令 $t=0$ 有 $(AB)^\vee = B^\vee A^\vee$).

设 $X = (A+tE)(B+tE)$ $Y = B+tE$, $Z = A+tE$.

X_{ij} 为 $X^\vee$ 第 i 行 j 列的元素 由伴随矩阵定义. $X_{ij} \in \mathbb{R}[t]$, Y_{ik}, Z_{kj} 同理.

由上述等式可知 $X_{ij} = \sum_{k=1}^{n} Y_{ik}\cdot Z_{kj}$ 考虑赋值同态 $\varphi_0: \mathbb{R}[t] \to \mathbb{R}$, $t \mapsto 0$

$\varphi_0(X_{ij}) = \sum_{k=1}^{n} \varphi_0(Y_{ik})\cdot\varphi_0(Z_{kj})$

而 $\varphi_0(X_{ij}) = (AB)^\vee$ 的 i 行 j 列元素. $\varphi_0(Y_{ik}) = B^\vee$ 的 k 列元素.

$\varphi_0(Z_{kj}) = A^\vee$ k 行 j 列元素. $\therefore (AB)^\vee = B^\vee\cdot A^\vee$ 口.

§2 域上多项式的因式分解.

Def1 设域 F. $f, g \in F[x]$ 且 $f \neq 0$ 若 $\exists\, h \in F[x]$ s.t. $g = hf$ 则称 f 是 g 的 因子, g 是 f 的 倍式. 记 $f \mid g$

Def2 设 $f, g \in F[x]$ 若 $\exists\, \alpha \in F \setminus \{0\}$ s.t. $f = \alpha g$ 则称 f, g 相伴.

易验证 相伴是等价关系 且 f, g 相伴 $\Leftrightarrow$ $f \mid g$ 且 $g \mid f$.

Def3 设 $f \in F[x] \setminus F$. 若 f 不能分成 $F[x]$ 中两个次数大于 0 的多项式之积, 则称 f 为 F 上 ($F[x]$ 中) 的不可约多项式.

注: 若 f 不可约 且 $f \sim g$ (相伴) 则 g 不可约.

若 f 不可约 且 $g \mid f$ 则 g 不可约.

若 f 不可约 且 $f \mid gh$ 则 $f \mid g$ 或 $f \mid h$.

$\forall f \in F[x]$ 可分解成若干不可约因式之积 (某种形式下唯一)

Def4 设 $f, g \in F[x]$. $h \in F[x] \setminus \{0\}$ 若 $h \mid f$ 且 $h \mid g$ 则称 h 为 f, g 公因子.

设 h 为 f, g 公因子. 若 $\forall$ 公因子 p 均有 $p \mid h$ 则称最大公因子, 记 gcd.

Thm2 1) 设 $f, g \in F[x]$ 且 $g \neq 0$ 则 $\exists\, u, v \in F[x]$ s.t.

$$uf + vg = \gcd(f, g) \quad \text{(Bézout 关系)}$$

注: 若 $\gcd(f, g) = 1$ 则称 f, g 互素.

2) 设 $f, g \in F[x] \setminus \{0\}$. 则 f, g 互素 $\Leftrightarrow$ $\exists\, u, v \in F[x]$ s.t. $uf + vg = 1$.

注. 带余除法:

设交换环 R, $f, g \in R[x]$ 且 $lc(g)$ 可逆 则 $\exists!\, q, r \in R[x]$ s.t.

$f = qg + r$, 其中 $\deg(r) < \deg(g)$

Cor 域 F. $f, g \in F[x]$. $g \neq 0$ 则 $\exists!\, q, r \in F[x]$ s.t. $f = qg + r$, $\deg(r) < \deg(g)$.

※ 可利用多次带余除法 (辗转相除、扩展欧几里德算法) 求 gcd.

Def 5 设 $f \in \mathbb{Z}[x] \setminus \{0\}$ 形如 $f = f_d x^d + \cdots + f_1 x + f_0$，其中 $f_0, \cdots f_d \in \mathbb{Z}$ 且 $f_d \neq 0$.

称 $\gcd(f_0, f_1, \cdots f_d)$ 为 f 的容度 记为 $\mathrm{cont}(f)$

若 $\mathrm{cont}(f) = 1$ 则称 f 为本原多项式.

Lemma 1 设 p 为素数 则

(1) $\varphi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ 是环同态.

$\sum_{i=0}^{d} f_i x^i \mapsto \sum_{i=0}^{d} \overline{f_i} x^i$

(2) 若 $g \in \mathbb{Z}[x]$ 是本原的，则 $\varphi_p(g) \neq 0$.

注：1) $\forall f \in \mathbb{Z}[x]$，若 $\varphi_p(f)$ 不可约 则 f 不可约.（判断不可约的一个方法）

2) 一个非零多项式可能是个零映射.

eg $\mathbb{Z}_p[x]$ 中多项式 $f(x) = x^p - x$ 显然 $f \neq 0$

考虑映射 $f: \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ 由 Fermat's little lemma

$\overline{x} \longmapsto \overline{x}^p - \overline{x}$ $\forall \overline{x} \in \mathbb{Z}_p$ $f(\overline{x}) = \overline{0} \Rightarrow f = \overline{0}$.

Lemma 2 (Guass 引理) 设 $f, g \in \mathbb{Z}[x]$ 本原，则 $f \cdot g$ 也本原.

Thm 3 * 设 $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$ 则 f 在 $\mathbb{Z}$ 上不可约 $\Longleftrightarrow$ f 在 $\mathbb{Q}$ 上不可约.

Thm 4 (Eisenstein 判别法) 设 $n > 1$ $f = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0 \in \mathbb{Z}[x]$，素数 p.

若 $p \mid f_{n-1}, \cdots p \mid f_1, p \mid f_0$ 且 $p^2 \nmid f_0$ 则 $f(x)$ 在 $\mathbb{Q}$ 上不可约

eg. 判断 $f(x) = x^3 + 3x + 2$ 是否在 $\mathbb{Z}$ 上可约.

解. [法一] Eisenstein 判别法. 考虑 环同态 $\varphi: \mathbb{Z}[x] \to \mathbb{Z}[x]$ $(g(x) \mapsto g(x+1))$

则 $\varphi(f(x)) = f(x+1) = (x+1)^3 + 3(x+1) + 2 = x^3 + 3x^2 + 6x + 6$

对素数 $p=3$ 有 p 整除 所有系数（不含首项）且 $p^2 \nmid 6$（尾项） $\Rightarrow \varphi(f)$ 不可约.

$\therefore f$ 不可约.

[法二] 模 p 法. 取 $p=5$ 考虑 环同态 $\varphi_p: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$

则 $\varphi_p(f) = x^3 + 3x + 2 = g$ 假设 $\varphi_p(f)$ 可约 则 有一次因子

但 $\forall \overline{m} \in \mathbb{Z}_5$, $g(\overline{m}) \neq \overline{0}$ 无根值. $\therefore \varphi(f)$ 在 $\mathbb{Z}_5$ 上不可约 $\Rightarrow f$ 在 $\mathbb{Z}$ 上不可约.