第十六次作业

1.（柯 P61.1）设 $f(x)=x^5+3x^4+x^3+4x^2-3x-1$，$g(x)=x^2+x+1$。用带余除法证明：

在 $\mathbb{Z}[x]$ 中 $g\nmid f$ 但在 $\mathbb{Z}_5[x]$ 中 $g\mid f$。反过来可能吗？

证．带余除法

$$
\begin{array}{r|l}
 & x^3+2x^2-2x+4 \\
\hline
x^2+x+1 & x^5+3x^4+x^3+4x^2-3x-1 \\
 & x^5+x^4+x^3 \\
\hline
 & 2x^4+4x^2-3x-1 \\
 & 2x^4+2x^3+2x^2 \\
\hline
 & -2x^3+2x^2-3x-1 \\
 & -2x^3-2x^2-2x \\
\hline
 & 4x^2-x-1 \\
 & 4x^2+4x+4 \\
\hline
 & -5x-5
\end{array}
$$

设 $q(x)=x^3+2x^2-2x+4$

$r(x)=-5x-5$

则在 $\mathbb{Z}[x]$ 中

$f=q\cdot g+r$ 且 $r\neq 0$

$\therefore g\nmid f$

在 $\mathbb{Z}_5[x]$ 中 $f=q\cdot g+r$

且 $r=\bar{5}(-x-1)=\bar{0}$ $\therefore g\mid f$

反过来即在 $\mathbb{Z}_5[x]$ 中有 $g\nmid f$ 但在 $\mathbb{Z}[x]$ 中 $g\mid f$，不可能。

考虑环同态 $\pi:\mathbb{Z}[x]\longrightarrow\mathbb{Z}_5[x]$

$\sum_{i=0}^{n}a_ix^i\longmapsto\sum_{i=0}^{n}\bar{a}_ix^i$

若在 $\mathbb{Z}[x]$ 中有 $g\mid f$ 即 $\exists\, h\in\mathbb{Z}[x]$ s.t. $f=g\cdot h$ 两边作用环同态 π.

$\pi(f)=\pi(g\cdot h)=\pi(g)\cdot\pi(h)\Rightarrow\pi(g)\mid\pi(f)\Rightarrow$ 在 $\mathbb{Z}_5[x]$ 中 $g\mid f$ 矛盾. □

2. 设 $f(x)=x^2+x-2=(x-1)(x+2)$．矩阵 $A=\begin{pmatrix}1&1&\\&1&1\\&&1\end{pmatrix}$ 求 $f(A)$

解：$f(A)=A^2+A-2E=\begin{pmatrix}1&2&1\\&1&2\\&&1\end{pmatrix}+\begin{pmatrix}1&1&\\&1&1\\&&1\end{pmatrix}-\begin{pmatrix}2&&\\&2&\\&&2\end{pmatrix}=\begin{pmatrix}0&3&1\\&0&3\\&&0\end{pmatrix}$

（另法）考虑环同态（赋值同态）$\rho_A:\mathbb{R}[x]\longrightarrow\mathbb{R}[A]$

$f(x)\longmapsto f(A)$

则 $\rho_A(f)=\rho_A(x-1)\cdot\rho_A(x+2)=(A-E)\cdot(A+2E)=\begin{pmatrix}0&1&\\&0&1\\&&0\end{pmatrix}\cdot\begin{pmatrix}3&1&\\&3&1\\&&3\end{pmatrix}$ □

3. 设域 F，$a,b\in F$ 且 $a\neq 0$．设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in F[x]$ 且 $a_n\neq 0$．

证明 $\deg(f(x))=\deg(f(ax+b))$ 计算 $\mathrm{lc}(f(ax+b))$

证．$f(ax+b)=a_n(ax+b)^n+\cdots+a_1(ax+b)+a_0$

$=a_n\cdot a^nx^n+$ lower terms

$\because a,\ a_n$ 均非零且 F 为域

$\therefore a^na_n\neq 0$ $\therefore\deg$ 不变.

且 $\mathrm{lc}=a^n\cdot a_n$.

4. 设域 F, $f,g,h\in F[x]$ 证明 若 $\gcd(f,h)=\gcd(g,h)=1$ 则 $\gcd(fg,h)=1$

Pf. $\because \gcd(f,h)=1$ 且 $\gcd(g,h)=1$ 则 $\exists\ u_1,v_1,u_2,v_2\in F[x]$ s.t.

令 $u_1f+v_1h=1$ 且 $u_2g+v_2h=1$ 则 $u_1f=1-v_1h$. $u_2g=1-v_2h$

$\Rightarrow u_1u_2fg=(1-v_1h)(1-v_2h)=1-v_1h-v_2h+v_1v_2h^2=1-(v_1+v_2-v_1v_2h)\cdot h$

$\therefore u_1u_2fg+(v_1+v_2-v_1v_2h)h=1$ 即 $\exists\ u_3=u_1\cdot u_2$, $v_3=v_1+v_2-v_1v_2h\in F[x]$

s.t. $u_3\cdot fg+v_3\cdot h=1 \Rightarrow \gcd(fg,h)=1$ □.

5. 判断下列多项式在所处环中是否可约 并给出不可约分解.

(1) $\mathbb{Z}_p[x]$ 中 $x^p-\bar{1}$ (p为素数)

$x^{p-1}+\cdots+x+1$ 在 $\mathbb{Q}[x]$ 上不可约
但在 $\mathbb{Z}_p$ 上可约.

若 $p=2$ 则 $x^2-\bar{1}=(x+\bar{1})(x-\bar{1})=(x-\bar{1})^2$

若 p为奇素数 则 $(x-\bar{1})^p=x^p-\bar{1}+\sum_{k=1}^{p-1}\binom{p}{k}x^k(-\bar{1})^{p-k}=x^p-\bar{1}$

(2) $\mathbb{Q}[x]$ 中 $x^4-8x^3+12x^2+2$

Eisenstein 判别法 取素数 $p=2$ 易知 $p\mid 8$, $p\mid 12$, $p\mid 2$ 且 $p^2\nmid 2$ $\therefore$ 不可约.

(3) $\mathbb{Q}[x]$ 中 x^p+px+1. (p是奇素数)

设 $f(x)=x^p+px+1$ 令 $g(x)=f(x-1)=(x-1)^p+p(x-1)+1$

$\Rightarrow g(x)=x^p+\sum_{k=1}^{p-2}(-1)^k\binom{p}{k}x^{p-k}+(-1)^{p-1}\binom{p}{1}x+(-1)^p+px-p+1$

$=x^p+\sum_{k=1}^{p-2}(-1)^k\binom{p}{k}x^{p-k}+2px-p$

$\because p\mid\binom{p}{k}$ $(k=1,\cdots p-2)$ 且 $p\mid 2p$, $p\mid -p$ 但 $p^2\nmid(-p)$ $\therefore$ g不可约 $\Rightarrow$ f不可约.

一元多项式不可约因式分解.

<u>Def</u> 设域 F. 多项式 $f\in F[x]$, 若 $lc(f)=1$ (即 f 首항系数为1) 则称 f 首1.

<u>Thm</u>. 设域 F. $\forall f\in F[x]\setminus F$ $\exists!$ $\lambda\in F$, 两两不相伴的, 非平凡的, 首1的不可约多项式 $p_1,\cdots p_s$ 和正整数 $m_1,\cdots m_s$ s.t.

$$f=\lambda p_1^{m_1}\cdots p_s^{m_s}$$

<u>Pf</u>. 由 Thm 4.4 (讲义十六 P26) $f=\alpha p_1\cdots p_m$ (其中 $\alpha\in F\setminus\{0\}$. $p_1,\cdots p_m$ 非平凡 不可约).

且在适当的顺序和相伴的条件下唯一.

设 $\tilde{p}_i=(lc(p_i))^{-1}\cdot p_i$ $(i=1,2\cdots m)$ 则 $\tilde{p}_i$ 为首一多项式. 非非平凡. 不可约.

则 $\exists\lambda\in F\setminus\{0\}$ s.t. $f=\lambda\tilde{p}_1\cdots\tilde{p}_m$

不失一般性, 不妨设 $\tilde{p}_1\cdots\tilde{p}_s$ 两两不相伴 而 $\tilde{p}_j\overset{\text{相伴}}{\sim_F}\tilde{p}_i$ $(\forall j\in\{s+1,\cdots m\},\ \exists i\in\{1,\cdots s\})$

$\because$ $\tilde{p}_j\sim_F\tilde{p}_i$ 且 $\tilde{p}_i,\tilde{p}_j$ 均首一 $\therefore$ $\tilde{p}_j=\tilde{p}_i$

$\therefore$ $\exists$ $m_1,\cdots m_s\in\mathbb{Z}^+$ s.t. $f=\lambda\tilde{p}_1^{m_1}\cdots\tilde{p}_s^{m_s}$

其中 $\tilde{p}_1,\cdots\tilde{p}_s$ 两两不相伴, 非平凡, 首一, 不可约. $\lambda\in F\setminus\{0\}$, $m_1\cdots m_s\in\mathbb{Z}^+$.

唯一性由 Thm 4.4 易知. □.

注: 一般 $\mathbb{Q}[x]$ 上的不可约因式分解是可以算法化给出的.

(Berlekamp 算法 + Hensel lifting 算法)

eg. 求 x^3-3x+2 在 $\mathbb{Q}[x]$ 上的不可约分解.

解: 若 $f(x)=x^3-3x+2$ 可约 则 $f(x)=0$ 一根在 $\mathbb{Q}$ 中

设 $f(\alpha)=0$ 则若 f 首1 ~~两~~ 且 $f\in\mathbb{Z}[x]$ 则 $\alpha\mid 2$

即 $\alpha=\pm1$ or ±2. 易知 $f(1)=0$ $\Rightarrow$ $x-1\mid f(x)$

$\Rightarrow f(x)=(x-1)(x^2+x-2)=(x-1)(x-1)(x+2)$

$\therefore f(x)=(x-1)^2(x+2)$

eg2. 求证 $f(x)=x^{n-1}+\cdots+x+1$ 在 $\mathbb{Q}[x]$ 中不可约 $\Longleftrightarrow$ n 为素数.

Pf ($\Leftarrow$) 考虑环同态 $\varphi: \mathbb{Q}[x]\longrightarrow \mathbb{Q}[x]$ s.t. ~~$\varphi(f(x))=f(x+1)$~~ $\varphi(g(x))=g(x+1)$.

(已证)

则 $\varphi(f(x))=\varphi\left(\frac{x^n-1}{x-1}\right)=\frac{(x+1)^n-1}{(x+1)-1}=\frac{x^n+\binom{n}{1}x^{n-1}+\cdots+\binom{n}{n-1}x+1-1}{x}$

$$=x^{n-1}+\binom{n}{1}x^{n-2}+\cdots+\binom{n}{n-1}$$

若 n 为素数 则 $n\mid\binom{n}{k}$ 对 $\forall\ k=1,2\cdots n-1$ 而 $\binom{n}{n-1}=n$ $\therefore n^2\nmid\binom{n}{n-1}$

由 Eisenstein 判别法 可知 $\varphi(f(x))$ 不可约 $\therefore f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

($\Rightarrow$). (反证) 假设 n 为合数 设 $n=m\cdot d$ $(1<m<n,\ 1<d<n)$

则 $f(x)=\frac{x^n-1}{x-1}=\frac{(x^m)^d-1}{x-1}=\frac{(x^m)^d-1}{x^m-1}\cdot\frac{x^m-1}{x-1}$

$$=(y^{d-1}+\cdots+y+1)\cdot(x^{m-1}+\cdots+x+1) \quad (其中\ y=x^m)$$

令 $g(x)=x^{m(d-1)}+\cdots+x^m+1$ $\quad h(x)=x^{m-1}+\cdots+x+1$.

则 $\deg(g(x))=m(d-1)$ 满足 $1<m(d-1)<n$

$\deg(h(x))=m-1$ 满足 $1\le m-1<n$

$\therefore f=g\cdot h$ 可分解为2个次数大于0的多项式之积, $\therefore f$ 可约. $\rightarrow\leftarrow$ □.

eg3. 求 $f(x)=x^6-\bar{1}\in\mathbb{Z}_6[x]$ 的不可约分解.

解 $f(x)=(x^3)^2-\bar{1}=(x^3-\bar{1})(x^3+\bar{1})=(x-\bar{1})(x^2+x+\bar{1})(x+1)(x^2-x+\bar{1})$

现证 $x^2+x+\bar{1}$ 在 $\mathbb{Z}_6$ 上不可约.

假设可约. 则可分成2个一次因子. $\therefore\exists\ \bar{m}\in\mathbb{Z}_6$ s.t. $\bar{m}^2+\bar{m}+\bar{1}=\bar{0}$

经验证 $\forall\ \bar{m}\in\mathbb{Z}_6$ $\bar{m}^2+\bar{m}+\bar{1}\neq\bar{0}$ $\therefore$ 不可约.

同理. $x^2-x+\bar{1}$ 也不可约 $\therefore$ 上式即为不可约分解. □.

期末复习

一. 线性映射.

设 $\varphi: \mathbb{R}^n \longrightarrow \mathbb{R}^m$ 为线性映射 即 $\forall\ \vec{x}, \vec{y} \in \mathbb{R}^n,\ \alpha, \beta \in \mathbb{R}$ $\varphi(\alpha\vec{x} + \beta\vec{y}) = \alpha\varphi(\vec{x}) + \beta\varphi(\vec{y})$.

则 $A = (\varphi(\vec{e}_1), \varphi(\vec{e}_2), \cdots \varphi(\vec{e}_n))$ 为 φ 在标准基下的矩阵 ($\vec{e}_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ ← i行)

(实际上, 线性映射与矩阵一一对应).

$\ker\varphi := \{\vec{x} \in \mathbb{R}^n \mid \varphi(\vec{x}) = \vec{0}\} \subseteq \mathbb{R}^n$ 是线性子空间

$= \{\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n \mid \sum_{i=1}^n x_i \cdot \varphi(\vec{e}_i) = \vec{0}\} = \{\vec{x} \in \mathbb{R}^n \mid A\vec{x} = \vec{0}\} = V_A$

$\mathrm{im}\,\varphi := \{\varphi(\vec{x}) \mid \vec{x} \in \mathbb{R}^n\} \subseteq \mathbb{R}^m$ 为线性子空间.

$= \{\sum_{i=1}^n x_i\, \varphi(\vec{e}_i) \mid x_i \in \mathbb{R},\ i = 1, 2, \cdots n\} = V_c(A)$ (列空间)

二. 矩阵乘法.

$A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{s\times n}$ $\Longrightarrow$ $A\cdot B = (c_{ij}) \in \mathbb{R}^{m\times n}$ 且 $c_{ij} = \sum_{k=1}^{s} a_{ik} b_{kj}$

$$\begin{tikzcd} \mathbb{R}^n \arrow[r, "\varphi_B"] \arrow[dr, "\varphi_A \circ \varphi_B"'] & \mathbb{R}^s \arrow[d, "\varphi_A"] \\ & \mathbb{R}^m \end{tikzcd}$$

$A\cdot B$ 即为复合映射 $\varphi_A \circ \varphi_B$ 在标准基下的矩阵.

Prop 1) $(AB)C = A(BC)$ 结合律

2) $(AB)^t = B^t A^t$

3) 交换律, 消去律 均不成立.

三. 矩阵运算时的秩:

1. 设 $A \in \mathbb{R}^{m\times n}$

$\mathrm{rank}(A) \leq \min(m, n)$

$\mathrm{rank}(A^t) = \mathrm{rank}(A)$

$\dim V_A + \mathrm{rank}\, A = n$

$\dim(\ker\varphi_A) + \dim(\mathrm{im}\,\varphi_A) = n$.

2. 设 $A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{s\times n}$.

$\mathrm{rank}(AB) \leq \min(\mathrm{rank}A, \mathrm{rank}B)$

$\mathrm{rank}(AB) \geq \mathrm{rank}(A) + \mathrm{rank}(B) - s$

(Sylvester's 不等式)

四 矩阵相抵

<u>Lemma</u>（打洞引理）

$\forall\ A \in \mathbb{R}^{m\times n}$. $\exists$ 可逆矩阵 $P \in M_m(\mathbb{R})$. $Q \in M_n(\mathbb{R})$ s.t.

$$PAQ = \begin{pmatrix} E_r & \\ & O_{n-r} \end{pmatrix}$$ 其中 $r = \operatorname{rank} A$.

<u>Def</u> 相抵.

设 $A, B \in \mathbb{R}^{m\times n}$. 若 $\exists$ 可逆矩阵 $P \in M_m(\mathbb{R})$. $Q \in M_n(\mathbb{R})$ s.t.

$PAQ = B$ 则称 A 与 B 相抵（初等等价） 记为 $A \sim_s B$（等价关系）.

<u>Thm</u> 设 $A, B \in \mathbb{R}^{m\times n}$. $A \sim_s B \iff \operatorname{rank} A = \operatorname{rank} B$.

五 矩阵求逆.

设 $A \in M_n(\mathbb{R})$ 可逆（即 $\operatorname{rank} A = n$） 则 $(A\ E_n) \xrightarrow{\text{初等行变换}} (E_n\ A^{-1})$

<u>Prop</u>. 1) $(AB)^{-1} = B^{-1}A^{-1}$

2) $\forall\ A \in \mathbb{R}^{m\times n}$ $B \in M_m(\mathbb{R})$. $C \in M_n(\mathbb{R})$

若 $\operatorname{rank} B = m$ 则 $\operatorname{rank}(BA) = \operatorname{rank} A$

若 $\operatorname{rank} C = n$ 则 $\operatorname{rank}(AC) = \operatorname{rank} A$.

3) $(A^t)^{-1} = (A^{-1})^t$

六 行列式（n重线性斜对称函数 且 $\det(\vec{e}_1, \cdots \vec{e}_n) = 1$）

$$\det(A) = |A| = \sum_{\sigma \in S_n} \varepsilon_\sigma\, a_{\sigma(1),1}\, a_{\sigma(2),2} \cdots a_{\sigma(n),n}$$

<u>Prop</u> 1) $\det(A) = \det(A^t)$

2) 若 A 中有一行（列）为 $\vec{0}$ 或两行（列）相同 则 $|A| = 0$

3) $\det(F_{ij}(A)) = -\det(A)$

$\det(F_{ij}(\lambda)(A)) = \det(A)$

$\det(F_i(\lambda)(A)) = \lambda \det(A)$

4) 若 A 为三角阵 则 $\det(A) = \prod_{i=1}^{n} a_{ii}$

5) $\det(A) = \sum_{j=1}^{n} a_{ij} A_{ij} = \sum_{i=1}^{n} a_{ij} A_{ij}$

其中 $A_{ij} = (-1)^{i+j} M_{ij}$ — 代数余子式.

$M_{ij} = |A$ 去掉 i 行 j 列$|$（按行/列展开）

6) $|AB| = |A| \cdot |B|$.

七 行列式应用

1. 伴随矩阵 $A^{\vee} = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}$ 其中 A_{ji} 为代数余子式.

$A \cdot E$, 若A可逆 则 $A^{-1} = \frac{A^{\vee}}{|A|}$

Prop 1) $A \cdot A^{\vee} = A^{\vee} \cdot A = |A| \cdot E$

2) $\operatorname{rank}(A^{\vee}) = \begin{cases} n & (\operatorname{rank} A = n) \\ 1 & (\operatorname{rank} A = n-1) \\ 0 & (\operatorname{rank} A < n-1) \end{cases}$

3) $|A^{\vee}| = |A|^{n-1}$, $(AB)^{\vee} = B^{\vee}A^{\vee}$ $(A^{t})^{\vee} = (A^{\vee})^{t}$

$(\lambda A)^{\vee} = \lambda^{n-1} \cdot A^{\vee}$, $(A^{\vee})^{\vee} = |A|^{n-2} \cdot A$

2. Cramer 法则

设 $A \in M_n(\mathbb{R})$ $\vec{b} \in \mathbb{R}^n$ $\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ 则 $A\vec{x} = \vec{b}$ 确定 $\Leftrightarrow$ A可逆

此时 $x_i = \frac{\det(\vec{A}^{(1)} \cdots \vec{A}^{(i-1)}\ \vec{b}\ \vec{A}^{(i+1)} \cdots \vec{A}^{(n)})}{\det(A)}$ $(i=1,2\cdots n)$

3. 行列式与秩. 设 $A \in \mathbb{R}^{m \times n}$

Def k阶子式: 设 $i_1, \cdots i_k \in \{1, \cdots m\}$. $j_1, \cdots j_k \in \{1, \cdots n\}$

则称行列式 $M_A\begin{pmatrix} i_1 \cdots i_k \\ j_1 \cdots j_k \end{pmatrix} = \begin{vmatrix} a_{i_1 j_1} & \cdots & a_{i_1 j_k} \\ \vdots & & \vdots \\ a_{i_k j_1} & \cdots & a_{i_k j_k} \end{vmatrix}$ 为A的一个k阶子式.

即A的某k行, k行交叉的元素. 加边子式为 $M_A\begin{pmatrix} i_1 \cdots i_k\ s \\ j_1 \cdots j_k\ t \end{pmatrix}$ $s \in \{1, \cdots m\}$, $t \in \{1, \cdots n\}$

Thm $\operatorname{rank} A = r$ $\Leftrightarrow$ ∃ r阶子式非0 且 ∀ 大于r阶子式均为0

$\Leftrightarrow$ ∃ r阶子式非0 且 ∀ r+1阶子式均为0

$\Leftrightarrow$ ∃ r阶子式非0 且 该子式所有加边子式为0.

$\Leftrightarrow$ ∃ r阶子式非0 且

卷八群

1. 定义：非空集合 G. G上的二元运算 $\cdot: G\times G \longrightarrow G$.

封闭：G 关于 $\cdot$ 封闭

结合律：$\forall\, a,b,c\in G$. ~~ab~~ $(ab)c=a(bc)$

单位元(幺元)：$\exists\, e\in G$ s.t. $\forall\, a\in G$ $ae=ea=a$.

逆元：$\forall\, a\in G$ $\exists\, b\in G$ s.t. $ab=ba=e$

（封闭、结合律）半群；（加单位元）幺半群；（加逆元）群.

2. 群同态：设群 $(G_1,\cdot,e_1)$ 和 $(G_2,*,e_2)$ 之间的映射

$\varphi: G_1 \longrightarrow G_2$ 满足 $\forall\, a_1,b_1\in G_1$ 均有.

$\varphi(a_1\cdot b_1) = \varphi(a_1) * \varphi(b_1)$ $(\Rightarrow \varphi(e_1)=e_2,\ \varphi(a^{-1})=(\varphi(a))^{-1})$.

群同构 = 群同态 + 双射(单+满)

3. 子群 $H\leq G$ 若 $\forall\, a,b\in H$ 均有 $ab^{-1}\in H$. (必考)

卷九环与域.

1. 环定义：非空集合 R. 及 R上两个二元运算 $+,\ \cdot$ 且 $\exists\, 0,1\in R$

$$\begin{cases} (R,+,0) \text{ 构成交换群.} \\ (R,\cdot,1) \text{ 构成幺半群.} \\ \forall\, a,b,c\in R \quad \begin{cases} (a+b)c = ac+bc \\ c(a+b) = ca+cb \end{cases} \text{ (满足分配律)} \end{cases}$$

2. 可逆元与零因子.

$a\in R$ 若 $\exists\, b\in R$ s.t. $ab=ba=1$ 则称 a为可逆元. b为a的逆.

$a\in R\setminus\{0\}$ 若 $\exists\, b\in R\setminus\{0\}$ s.t. $ab=0$ $(ba=0)$ 则称 a为左零因子(右).

整环 = 交换环 + 无零因子. (有消去律).

3. 环同态：环 $(R_1, +, 0, \cdot, e_1)$ 和 $(R_2, +, 0, \cdot, e_2)$ 之间一映射

$\varphi: R_1 \longrightarrow R_2$ 满足 $\forall a, b \in R_1$ 均有

$$\begin{cases} \varphi(a+b) = \varphi(a) + \varphi(b) \\ \varphi(ab) = \varphi(a) \cdot \varphi(b) \\ \varphi(e_1) = e_2 \end{cases}$$

4. 域 = 整环 + 非 0 元可逆.

域特征 $\mathrm{char}(F) = \begin{cases} 0 & (\forall m \in \mathbb{Z}^+ \quad m \cdot 1 \neq 0) \\ p & (\exists \text{ 素数 } p \text{ s.t. } p \cdot 1 = 0) \end{cases}$ eg $\mathbb{Z}_p$

十. 一元多项式.

$F[x] := \{ \sum_{i=0}^{d} a_i x^i \mid a_i \in F, d \in \mathbb{N} \}$ 构成环

Prop 1). $\forall f, g \in F[x]$. $\deg(f+g) \leq \max(\deg(f), \deg(g))$

$\deg(f \cdot g) = \deg(f) + \deg(g)$ （注：一般环上多项式是 $\leq$）

2) 赋值同态定理.

3) 因式分解（Eisenstein 判别法）

4) 带余除法.

环 R 若 $\forall x\in R$ 均有 $x^3=x$ 则 R 为交换环.

Pf. $\forall\ x\in R$ $(x+x)^3=(2x)^3=8x^3=8x=2x \Rightarrow 3x=-3x$.

$(x+1)^3=x^3+3x^2+3x+1=x+1+3x^2+3x=x+1 \Rightarrow 3(x^2+x)=0$.

$\forall\ x,y\in R$ $(x+y)^3=x^3+x^2y+xyx+xy^2+yx^2+yxy+y^2x+y^3=x^3+y^3=x+y$

$\Rightarrow x^2y+xyx+xy^2+yx^2+yxy+y^2x=0$ ①

$(x-y)^3=x^3-x^2y-xyx+xy^2-yx^2+yxy+y^2x-y^3=x^3-y^3=x-y$

$\Rightarrow -x^2y-xyx+xy^2-yx^2+yxy+y^2x=0$ ②

①+②得 $2(xy^2+yxy+y^2x)=0$ ③

③式左乘y得 $2(yxy^2+y^2xy+y^3x)=0 \Rightarrow 2(yxy^2+y^2xy+yx)=0$ ④

③式右乘y得 $2(xy^3+yxy^2+y^2xy)=0 \Rightarrow 2(xy+yxy^2+y^2xy)=0$ ⑤

④-⑤得 $2(yx-xy)=0$ ⑥

又 $\because \forall x\in R$ $3(x^2+x)=0$ 则 $\forall\ x,y\in R$ $3((x+y)^2+(x+y))=0$

$\Rightarrow 3(x^2+xy+yx+y^2+x+y)=0$

$\Rightarrow 3(x^2+x)+3(y^2+y)+3(xy+yx)=0 \Rightarrow 3(xy+yx)=0$

又 $\because$ $3x=-3x$ 对 $\forall x\in R$ 成立 $\therefore 3xy=-3yx=3yx$

$\therefore 3(yx-xy)=0$ ⑦ ~~⑦~~ ⑥-⑦得 $xy-yx=0$

□.

由 x, y 任意性. 可知 R 是交换环.