回忆：广义分配律

设 R 是环，$a_1, \cdots, a_m, b_1, \cdots, b_n \in R$

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

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

推论 3.1 设 $a, b \in R$，$m, n \in \mathbb{Z}$

$(ma)(nb) = (mn)(ab)$.

证：情形1 $m>0$ 且 $n>0$

由广义分配律直接可得

情形2. $m=0$ 或 $n=0$. 等号约定

情形3. $m<0$ 且 $n>0$

由 $ma = (-m)(-a)$

$(ma)(nb) = [(-m)(-a)](nb]$

$= (-mn)(-ab)$ （情形1）

$= (mn)(ab)$

（等号约定）

情形4 $m>0$ 且 $n<0$

与情形3类似

情形5 $m<0$ 且 $n<0$

$(ma)(nb) = [(-m)(-a)][(-n)(-b)]$

$= [(-m)(-n)][(-a)(-b)]$

$= (mn)(ab)$

注：$(-a)(-b) = (-1)a(-1)b = (-1)(-1)ab$

$= ab$

§3.2 零因子和可逆元

定义：设 R 是环，$a, b \in R \setminus \{0\}$

如果 $ab=0$，则称 a 是 b 的左零因子，b 是 a 的右零因子. 当 R 是交换环时，我们不区分左右零因子.

例：在 $(\mathbb{Z}, +, 0, \cdot, 1)$ 中没有零因子

例：在 $(M_n(\mathbb{R}), +, O, \cdot, E)$ 中

A 是左零因子 $\Leftrightarrow$ $\mathrm{rank}(A) < n$ 且 $A \neq O$

证："$\Rightarrow$" 设 A 是左零因子. 则 $\exists B \in M_n(\mathbb{R})$

$B \neq O$，满足 $AB = O$.

若 $\mathrm{rank}(A) = n$. 则 A 可逆

$\Rightarrow A^{-1}AB = EB = B = O$ →←

于是 $\mathrm{rank}(A) < n$. 类似可知当 A 是右零因子时，$\mathrm{rank}(A) < n$

"$\Leftarrow$" 因为 $\mathrm{rank}(A) < n$. 所以 $V_A \neq \{0\}$

设 $\vec{v} \in V_A \setminus \{0\}$ 且 $B = (\vec{v}, \underbrace{\vec{0}, \cdots \vec{0}}_{n-1})$

则 $AB = O \Rightarrow A$ 是左零因子

类似 A^t 也是左零因子

于是 $\exists C \in M_n(\mathbb{R}) \setminus \{O\}$, $A^tC = O$

$\Rightarrow C^tA = O$ ②

$\Rightarrow A$ 是右零因子. 证

定义：设 R 是环，$a, b \in R$ 如果 $ab = ba = 1$.

则称 a 是可逆元，且 b 是 a 的逆

设 a 由命题2.1，可逆元 a 的逆唯一，记为 a^{-1}

注：可逆元不是零因子

例：整数环 $\mathbb{Z}$ 中的可逆元是 ± 1

例：矩阵环 $M_n(\mathbb{R})$ 中的可逆元是 $GL_n(\mathbb{R})$

命题3.1 设 $\bar{m} \in \mathbb{Z}_n$ 则

(i) $\bar{m}$ 可逆 $\Leftrightarrow \gcd(m, n) = 1$

(ii) $\bar{m}$ 是零因子 $\Leftrightarrow \gcd(m, n) > 1$ 且 $n \nmid m$

证 (i) 命题2.1

(ii) 设 $g = \gcd(m, n)$

"$\Rightarrow$" $\because \bar{m}$ 是零因子 $\therefore \bar{m}$ 不可逆且 $\bar{m} \neq \bar{0}$

$\Rightarrow g > 1$ 且 $n \nmid m$

"⇐" 此时 $g \in \{2,3,\cdots,n-1\}$.

设 $m=kg$, $n=lg$. 则 $\overline{l} \neq \overline{0}$

且 $m = lkg = kn \Rightarrow \overline{l}\,\overline{m} = \overline{l}\,\overline{m} = \overline{0}$

$\Rightarrow \overline{m}$ 是零因子.

定义：设 R 是环. 如果 R 中没有左和右零因子，则 R 是无零因子环. 无零因子的交换环. 称为整环 (domain)

定理 3.2 设 R 是无零因子环.

则 $\forall a,b,c \in D$, $a \neq 0$

$ab = ac \Rightarrow b = c$ (左消去律)

$ba = ca \Rightarrow b = c$ (右消去律)

证： $ab = ac \Rightarrow a(b-c) = 0$

$\Rightarrow b-c = 0$ ($\because a \neq 0$ 且 a 不是零因子)

$\Rightarrow b = c$

左消去律的证明类似 ☒

环 { 交换环 { 整环 $\mathbb{Z}$, $\mathbb{Z}_p$ p 是素数; 非整环, $\mathbb{Z}_n$. n 是合数 }; 非交换环 { 无零因子环 ☒ ?; 有零因子环, $M_n(\mathbb{R})$ } }

§3.3 子环

定义：设 $(R,+,0,\cdot,1)$ 是环. 如果 $S \subset R$ 且 $(S,+,0,\cdot,1)$ 也是环，则称 S 是 R 的子环 (subring).

例：$\mathbb{Z}$ 是 $\mathbb{Q}$ 的子环.

例：设 R 是环，

$$C_R = \{ c \in R \mid \forall r \in R,\ cr = rc \}$$

C_R 称为 R 的中心，它是一个子环

证：先证：$(C_R, +, 0)$ 是 $(R, +, 0)$ 的子群。设 $a, b \in C_R$.

$\forall r \in R$ $\quad r(a-b) = ra - rb$

$= ar - br = (a-b)r$

$\Rightarrow a-b \in C_R$

$\Rightarrow (C_R, +, 0)$ 是 $(R, +, 0)$ 的子群. [5] 例2.4

$\forall r \in R$ $\quad r(ab) = arb = (ab)r$

$\Rightarrow ab \in C_R$

$1 \in C_R \Rightarrow (C_R, \cdot, 1)$ 是幺半群

分配律由 R 中的分配律得证

$\Rightarrow C_R$ 是 R 的子环

例：~~Hadmilton~~ Hamilton 四元数 ④

设 $i^2 = -1$.

设 $H = \left\{ \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$

则 H 是 $M_2(\mathbb{C})$ 中的子环，

H 非交换且 H 中每个非零元都可逆.

（期末考虑数）

§3.4 环同态

定义：设 $(R, +, 0_R, \cdot, 1_S)$ 和

$(S, +, 0_S, \cdot, 1_S)$ 是两个环.

$\varphi: R \to S$ 称为 R 到 S 的环同态

如果 $\forall x, y \in R$

$\varphi(x+y) = \varphi(x) + \varphi(y)$

$\varphi(xy) = \varphi(x)\varphi(y)$

$\varphi(1_R) = 1_S$.

类似地有单同态，满同态和环同构.

例: $\pi_n: \mathbb{Z} \longrightarrow \mathbb{Z}_n$ 是环同态

$\pi_n(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \pi_n(a) + \pi_n(b)$

$\pi_n(ab) = \overline{ab} = \bar{a}\,\bar{b} = \pi_n(a)\,\pi_n(b)$

$\pi_n(1) = \bar{1}$.

定义: 设 $\varphi: R \to S$ 是环同态.

$$\ker(\varphi) := \{ r \in R \mid \varphi(r) = 0_S \}$$

命题 3.2 设 $\varphi: R \to S$ 是环同态

则 φ 是单射 $\Leftrightarrow \ker(\varphi) = \{0_R\}$

证: $\Rightarrow$ 由 $\varphi(0_R) = 0_S$ 可得

"$\Leftarrow$" 设 $a, b \in R$, $\varphi(a) = \varphi(b)$

则 $\varphi(a) - \varphi(b) = 0_S$

$\Rightarrow \varphi(a-b) = 0_S \Rightarrow a - b = 0_R$

$\Rightarrow a = b$ ∎

注: 设 R 是环，其中 $0 = 1$.

则 $\forall r \in R$, $r \cdot 0 = r \cdot 1 \Rightarrow 0 = r$

于是 $R = \{0\}$. 为了排除这一平凡情形

以此我们约定在环 R 中 $0 \neq 1$.

定义: 设 R 是环，如果 1 在群 $(R, +, 0)$ 中的阶是无限，则称 R 的特征为 0

否则 称 R 的特征为 $\mathrm{ord}(1)$，记特征为 $\mathrm{char}(R)$

例: $\mathrm{char}(\mathbb{Z}) = 0$, $\mathrm{char}(\mathbb{Z}_n) = n$

命题 3.3 设 R 是环且 $\mathrm{char}(R)$ 是合数

则 R 中有零因子

证: 设 $\mathrm{char}(R) = mn$, $m, n \in \mathbb{Z}^+ \setminus \{1\}$

$0 = (mn)1 = (m1)(n1)$ [推论3.1]

$\because m1 \neq 0$, $n1 \neq 0$ $\therefore$ 命题成立

引理3.1 设环 R 的特征为 $m>0$，$n\in\mathbb{Z}$ 且 $m\mid n$. 则 $\forall r\in R$

$$nr=0_R$$

证：设 $n=km$. $nr=kmr$

$$=k(mr)=k(\underbrace{r+\cdots+r}_{m})=k(\underbrace{1+\cdots+1}_{m})r$$

$$=k(0_R\cdot r)=k\cdot 0_R=0_R$$

注：设 $\varphi: R\to S$ 为环同态，$r_1,\cdots,r_k\in R$

则 $\varphi(r_1+\cdots+r_k)=\varphi(r_1)+\cdots+\varphi(r_k)$

$\varphi(r_1\cdots r_k)=\varphi(r_1)\cdots\varphi(r_k)$

直接对 k 归纳证明即可

例：设 R,S 为环. $\mathrm{char}(R)=m>0$

若 $\mathrm{char}(S)=0$ 或 $\mathrm{char}(S)>m$

则不存在环同态 $R\to S$

证：假设 $\varphi: R\to S$ 为环同态

$$0_S=\varphi(0_R)=\varphi(m\cdot 1_R)=\varphi(\underbrace{1_R+\cdots+1_R}_{m})$$

$$=\underbrace{\varphi(1_R)+\cdots+\varphi(1_R)}_{m}=\underbrace{1_S+\cdots+1_S}_{m}$$

$$=m\,1_S\Rightarrow \mathrm{char}(S)\le m$$

又 $\mathrm{char}(S)\neq 0$ $\to\leftarrow$ ∎

§3.5 特殊的环和子环

命题3.4. 设 $A\in M_n(\mathbb{R})$. 令

$$\mathbb{R}[A]=\{a_0E+a_1A+\cdots+a_mA^m \mid a_0,a_1,\cdots a_m\in\mathbb{R},\ m\in\mathbb{N}\}$$

则 $\mathbb{R}[A]$ 为交换环

证：设 $B,C\in\mathbb{R}[A]$ 则 $\exists\, b_0,\cdots b_k, c_0,\cdots c_\ell\in\mathbb{R}$

使得 $B=b_0E+b_1A+\cdots+b_kA^k$ 和 $C=c_0E+c_1A+\cdots+c_\ell A^\ell$

不妨设 $k\ge\ell$

$$B-C=(b_0-c_0)E+\cdots+(b_\ell-c_\ell)A^\ell+b_{\ell+1}A^{\ell+1}+\cdots+b_kA^k$$

$$\in\mathbb{R}[A]\Rightarrow(\mathbb{R}[A],+,0)\text{ 为交换群}$$

$$BC=\left(\sum_{i=0}^{k}b_iA^i\right)\left(\sum_{j=0}^{\ell}c_jA^j\right)=\sum_{i=0}^{k}\sum_{j=0}^{\ell}b_iA^ic_jA^j$$

$$=\sum_{i=0}^{k}\sum_{j=0}^{\ell}b_ic_jA^{i+j}=\sum_{j=0}^{\ell}\sum_{i=0}^{k}c_jA^jb_iA^i=CB$$

又 $BC\in\mathbb{R}[A]$. 于是 $(\mathbb{R}[A],\cdot,E)$ 为交换幺半群. 分配律自然成立 ∎

于是 $(\mathbb{R}[A]_{n\times n}, \cdot, E)$ 关于乘法的含幺半群.

分配律由 $M_n(\mathbb{R})$ 中的分配律可得 □

定理3.3 设 R 是环. $U_R = \{u \in R \mid u$ 可逆$\}$

则 $(U_R, \cdot, 1)$ 是群.

证: 乘法封闭 设 $u, v \in U_R$

$$(uv)v^{-1}u^{-1} = 1 \quad = v^{-1}u^{-1}(uv) = 1$$

于是 $uv \in U_R$. 即 "$\cdot$" 是 U_R 上的二元运算.

结合律自然满足. $1 \in U_R$

$\forall u \in U_R$, $u^{-1} \in U_R$ □

推论3.2. 设 p 是素数 则

$$U_{\mathbb{Z}_p} = \mathbb{Z}_p \setminus \{0\}$$

证: 由命题3.1 (1) 直接可得

推论3.3 Fermat Little Theorem ⑦

设 p 是素数, $m \in \mathbb{Z}$ 且 $p \nmid m$

则 $m^{p-1} \equiv 1 \mod p$

证: 设 $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. 由推论3.2

$(\mathbb{Z}_p^*, \cdot, 1)$ 是群且 $\mathrm{card}(\mathbb{Z}_p^*) = p-1$

由推论1: $\mathrm{ord}(\bar{m}) \mid (p-1)$

由引理2.5: $\bar{m}^{p-1} = \bar{1}$. 即 $\overline{m^{p-1}} = \bar{1}$

$\Rightarrow m^{p-1} \equiv 1 \mod p$ □

§4. 域 (Field)

定义: 设 $(F, +, 0, \cdot, 1)$ 是交换环, $0 \neq 1$

如果 F 中的任何非零元都可逆. 则称

F 是域.

注: F 是域 $\Leftrightarrow F \setminus \{0\} = U_F$

注: 域必是整环.

例：$\mathbb{Q}$，$\mathbb{R}$ 是域，$\mathbb{Z}_p$ 是域（推论3.2）

§4.1 分式域

设 D 是整环，$D^* = D\setminus\{0\}$. 在 $D\times D^*$ 上定义如下等价关系. 设 $(a,b),(c,d)\in D\times D^*$

如果 $\underline{ad=bc}$，则 $(a,b)\sim(c,d)$

"$\frac{a}{b}=\frac{c}{d}$"

验证：$\sim$ 是等价关系.

自反：设 $(a,b)\in D\times D^*$ $ab=ab\Rightarrow(a,b)\sim(a,b)$

对称：设 $(a,b)\sim(c,d)$ $ad=bc\Rightarrow bc=ad$

$\Rightarrow(c,d)\sim(a,b)$

传递：设 $(a_1,b_1)\sim(a_2,b_2)$，$(a_2,b_2)\sim(a_3,b_3)$

$$a_1b_2=b_1a_2 \qquad a_2b_3=b_2a_3 \quad (*)$$

$$a_1a_2b_2b_3=b_1a_2b_2a_3$$

$$(a_1b_3-a_3b_1)(a_2b_2)=0$$

若 $a_2\neq 0$，则 $a_2b_2\neq 0$（$\because D$ 是整环）

$a_1b_3=a_3b_1$（消去律）

若 $a_2=0$ 由 $(*)$，$a_1b_2=0$，$a_3b_2=0$

$\because b_2\neq 0$ $\therefore a_1=a_3=0$

$\Rightarrow a_1b_3=a_3b_1$.

综上 $(a_1,b_1)\sim(a_3,b_3)$

设 $F=(D\times D^*)/\sim$. (a,b) 等价类

记为 $\frac{a}{b}$.

定义：$+:F\times F\longrightarrow F$

$$\left(\frac{a}{b},\frac{c}{d}\right)\mapsto\frac{ad+bc}{bd}$$

$\cdot\ F\times F\longrightarrow F$

$$\left(\frac{a}{b},\frac{c}{d}\right)\mapsto\frac{ac}{bd}$$

良定义 设 $\frac{a}{b}=\frac{a'}{b'}$, $\frac{c}{d}=\frac{c'}{d'}$

即 $(a,b)\sim(a',b')$, $(c,d)\sim(c',d')$

即 $ab'=ba'$ $cd'=dc'$ $(**)$

要验证: $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$

$\Leftrightarrow \frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$

$\Leftrightarrow b'd'(ad+bc)=bd(a'd'+b'c')$

$\Leftrightarrow b'd'ad+b'd'bc=bda'd'+bdb'c'$

$\Leftrightarrow b'd'ad-bda'd'=bdb'c'-b'd'bc$

$\Leftrightarrow d'd(b'a-a'b)=bb'(dc'-d'c)$

$\Leftrightarrow 0=0$ $(**)$

要验证: $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}$

$\Leftrightarrow \frac{ac}{bd}=\frac{a'c'}{b'd'}$

$\Leftrightarrow acb'd'=a'c'bd$

$\Leftrightarrow acb'd'-a'c'bd=0$

$\Leftrightarrow ba'cd'-a'cbd=0$ $(**)$

$\Leftrightarrow ba'cd'-a'bcd'=0$ $(**)$

$\Leftrightarrow 0=0$

验证: $(F,+,\frac{0}{1})$ 是交换群

验证: 注: $\frac{0}{b}=\frac{0}{1}$ $\forall b\in D^*$

$\frac{ac}{bc}=\frac{a}{b}$ $\forall c\in D^*$

交换: $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{c}{d}+\frac{a}{b}$

结合

$$\left(\frac{a_1}{b_1}+\frac{a_2}{b_2}\right)+\frac{a_3}{b_3}=\frac{a_1b_2+b_1a_2}{b_1b_2}+\frac{a_3}{b_3}=\frac{a_1b_2b_3+a_3b_1b_2+a_3b_1b_2}{b_1b_2b_3}$$

$$=\frac{a_1}{b_1}+\left(\frac{a_2}{b_2}+\frac{a_3}{b_3}\right)$$

$\frac{a}{b}+\frac{0}{1}=\frac{a\cdot1+b0}{b\cdot1}=\frac{a}{b}$

$\frac{a}{b}+\frac{(-a)}{b}=\frac{ab-ab}{b^2}=\frac{0}{b^2}=\frac{0}{1}$

✓

验证：$(F, \cdot, \frac{1}{1})$ 关于乘法构成群.

交换

交换：$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}=\frac{c}{d}\cdot\frac{a}{b}$

结合：$\left(\frac{a_1}{b_1}\cdot\frac{a_2}{b_2}\right)\cdot\left(\frac{a_3}{b_3}\right)=\frac{(a_1a_2)}{(b_1b_2)}\cdot\frac{a_3}{b_3}$

$$=\frac{(a_1a_2)a_3}{(b_1b_2)b_3}=\frac{a_1a_2a_3}{b_1b_2b_3}$$

$$=\left(\frac{a_1}{b_1}\right)\left(\frac{a_2}{b_2}\cdot\frac{a_3}{b_3}\right).$$

单位：$\frac{a}{b}\cdot\frac{1}{1}=\frac{a\cdot1}{b\cdot1}=\frac{a}{b}$

分配：

$$\frac{a_1}{b_1}\left(\frac{a_2}{b_2}+\frac{a_3}{b_3}\right)=\frac{a_1}{b_1}\frac{a_2b_3+b_2a_3}{b_2b_3}$$

$$=\frac{a_1a_2b_3+a_1a_3b_2}{b_1b_2b_3}$$

$$\frac{a_1}{b_1}\frac{a_2}{b_2}+\frac{a_1}{b_1}\cdot\frac{a_3}{b_3}=\frac{a_1a_2}{b_1b_2}+\frac{a_1a_3}{b_1b_3}$$

$$=\frac{a_1a_2b_1b_3+a_1a_3b_1b_2}{b_1^2b_2b_3}\xrightarrow{\text{约分}}\frac{a_1a_2b_3+a_1a_3b_1}{b_1b_2b_3}$$

于是 $(F, +, \frac{0}{1}, \cdot\frac{1}{1})$ 是域 ⑩

注：在 F 中 $\frac{a}{1}$ 记为 a

于是 $\mathbb{D}$ 可以看作 F 的子集

例如：$\mathbb{Z}\subset\mathbb{Q}$

§4.2 域同态和域特征

设 F, K 是两个域，$\varphi: F\to K$ 是环同态

则称 φ 是域同态

命题 4.4：设 F, K 是两个域，$\varphi: F\to K$ 是同态，则 φ 是单射

证：由命题 3.2，只需证：$\ker(\varphi)=\{0_F\}$

设 $a\in F$ 使得 $\varphi(a)=0_K$ 且 $a\neq0$

$$1_K=\varphi(1_F)=\varphi(a^{-1}a)=\varphi(a^{-1})\varphi(a)$$

$$=\varphi(a^{-1})0_K=0_K$$

$\Rightarrow 1_K=0_K$ →← ☒

注：由命题3.3 设 F 是域，则

$\mathrm{char}(F)=0$ 或素数。

~~由引理4.1 设 F 是域~~

命题4.2 (Freshmen's dream)

设 F 是域，$\mathrm{char}(F)=p>0$

则 $\forall\, x,y\in F$，$(x+y)^p=x^p+y^p$

证：$(x+y)^p=\underbrace{(x+y)\cdots\cdots(x+y)}_{p}$

$=x^p+\binom{p}{1}x^{p-1}y+\binom{p}{2}x^{p-2}y^2+\cdots+\binom{p}{p-1}xy^{p-1}+y^p$

由第一章最后一个例子（讲义-5. page4）

$p\mid\binom{p}{k}$，$k\in\{1,2,\cdots p-1\}$

由引理3.1 $\binom{p}{k}x^{p-k}y^k=\overline{0}$

$\Rightarrow (x+y)^p=x^p+y^p$ ☒

注：在第二、三章中，$\mathbb{R}$ 除了若干例子所有的定义，定理等结论对任何域都成立

例外：设 $A\in M_n(\mathbb{R})$ $\mathrm{rank}(A)=\mathrm{rank}(A^tA)$

（$\because\ x_1^2+\cdots+x_n^2=0\Rightarrow x_1=\cdots=x_n=0$）

~~等数所学对称的行列式推广~~

（多项式≠0）

记号：设 F 是域，F^n 记以 F 为基域的坐标空间。

$M_n(F)=\{(a_{ij})_{n\times n}\mid a_{ij}\in F\}$

例：设 $A=\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{2}&\bar{4}\\ \bar{1}&\bar{4}&\bar{2}\end{pmatrix}\in M_3(\mathbb{Z}_5)$

计算 V_A 的维数和一组基

$$A \to \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{2} & \bar{4} \\ \bar{0} & \bar{2} & \bar{4} \end{pmatrix} \to \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{2} & \bar{4} \\ 0 & 0 & 0 \end{pmatrix}$$

$\text{rank}(A)=2 \Rightarrow \dim_{\mathbb{Z}_5} V_A = 1$

$$\begin{cases} x_1 + \bar{2}x_2 + \bar{3}x_3 = 0 \\ \bar{2}x_2 + \bar{4}x_3 = 0 \end{cases}$$

$\Rightarrow x_2 = -\bar{2}^{-1}\bar{4}x_3 = \bar{3}\bar{4}x_3 = \bar{3}x_3$

$x_1 + \bar{6}x_3 + \bar{3}x_3 = 0 \Rightarrow x_1 + \bar{9}x_3 = 0$

$x_1 + \bar{4}x_3 = 0 \quad x_1 = -\bar{4}x_3$

$x_1 = \bar{1}\cdot x_3$

$$V_A = \left\langle \begin{pmatrix} \bar{1} \\ \bar{3} \\ \bar{1} \end{pmatrix} \right\rangle = \left\{ \alpha \begin{pmatrix} \bar{1} \\ \bar{3} \\ \bar{1} \end{pmatrix} \mid \alpha \in \mathbb{Z}_5 \right\}$$

例 证明 $\left(\mathbb{Z}_2^3, +, \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix}\right)$ 不可能

有两个元素生成

证：假设 $\mathbb{Z}_2^3$ 可由 $\vec{v_1}, \vec{v_2}$ 生成

则 $\mathbb{Z}_2^3$ 作为 $\mathbb{Z}_2$ 上的线性空间

也由 $\vec{v_1}, \vec{v_2}$ 生成

$\Rightarrow \dim \mathbb{Z}_2^3 \leq 2 \to\leftarrow$

注：$\because \text{card}(\mathbb{Z}_2^3) = 8$

$\therefore \left(\mathbb{Z}_2^3, +, \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix}\right)$ 同构于 S_8 的某个子群

$\Rightarrow S_8$ 中有子群的生成元个数 ≥ 3 囧

命题 4.3 设 F, K 是域 R 是 F 的子环

$\varphi: R \to K$ 是同态

$A \in M_n(R)$. 令 $A = (a_{ij})$, $\varphi(A) = (\varphi(a_{ij}))$

则 $\varphi(\det(A)) = \det(\varphi(A))$

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

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

$$= \det(\varphi(A))$$

注：若 $\varphi(A)$ 满秩 $\Rightarrow A$ 必然满秩

例：设 $A=\begin{pmatrix} 2 & 7 & 6 & 4 \\ 5 & 8 & 11 & 9 \\ 3 & 1 & 1 & 0 \\ 0 & 3 & 1 & 1 \end{pmatrix} \in M_4(\mathbb{Z}) \subset M_4(\mathbb{Q})$

判断 A 是否满秩

$$\pi_2 : \mathbb{Z} \to \mathbb{Z}_2$$

$$\pi_2(A) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{1} \\ \overline{1} & \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} & \overline{1} \end{pmatrix}$$

$$\det(\pi_2(A)) = \begin{vmatrix} \overline{1} & \overline{1} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \end{vmatrix} = \begin{vmatrix} \overline{0} & \overline{0} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \end{vmatrix}$$

$$= \begin{vmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{vmatrix} \neq \overline{0}$$

$\Rightarrow$ $\operatorname{rank}(A) = 4$ ✓

第五章 多项式和有数

§2 一元多项式

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

在半群中 $(R, +, 0, \cdot, 1)$ 是交换环

§2.1 一元多项式环的构造

设 $\tilde{R} = \{(a_0, a_1, a_2 \cdots), \mid a_0, a_1, a_2 \cdots \in R$ 有限个非零$\}$

记号 设 $\tilde{a} \in \tilde{R}$. $\tilde{a}_k$ 为 $\tilde{a}$ 中第 k 个坐标,

其中 $k = 0, 1, 2, \cdots$

特别地. $\tilde{0} = (0, 0, 0, \cdots)$, $\tilde{1} = (1, 0, 0, \cdots)$

注: $\forall \tilde{a} \in \tilde{R}$, $\exists l \in \mathbb{N}$, 使得

$a_l = 0$, $a_{l+1} = 0$, $\cdots$

$$+: \tilde{R} \times \tilde{R} \longrightarrow \tilde{R}$$
$$(\tilde{a}, \tilde{b}) \mapsto (\cdots \tilde{a}_k + \tilde{b}_k \cdots)$$

再依据 $(R, +, 0)$ 是交换加法群.

可知 $(\tilde{R}, +, \tilde{0})$ 也是交换加法群.

定义: $\cdot: \tilde{R} \times \tilde{R} \longrightarrow \tilde{R}$
$$(\tilde{a}, \tilde{b}) \mapsto \tilde{c}$$

其中 $\tilde{c}_k = \sum_{i+j=k} \tilde{a}_i \tilde{b}_j$, ~~对于~~ $k \in \mathbb{N}$

阶数

设 $p(x) = a_0 + a_1 x + \cdots + a_m x^m$

$q(x) = b_0 + b_1 x + \cdots + b_n x^n$.

pq 中 x^k 的系数是什么?

$$pq = \left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right)$$

$$= \sum_{i=0}^{m} \sum_{j=0}^{n} (a_i x^i)(b_j x^j)$$

$$= \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j} \overset{m+n}{\underset{k=0}{=}} \left(\sum_{i+j=k} a_i b_j\right) x^k$$