第14次作业.

(P128.3)

1. 群 G. $a,b\in G$ 满足 $ab=ba$ (乘法可交换). $ord(a)=s$. $ord(b)=t$.

若 $\gcd(s,t)=1$ 则 G 中有一个(st)阶的循环子群 $\langle a,b\rangle$ ($=\langle a\cdot b\rangle$)

Pf. 首先证明 $\langle a,b\rangle$ 是循环群 即 $\langle a,b\rangle=\langle a\cdot b\rangle$

显然 $a\cdot b\in\langle a,b\rangle$ $\therefore\ \langle a\cdot b\rangle\subseteq\langle a,b\rangle$

$\because \gcd(s,t)=1$ $\therefore\ \exists\ u,v\in\mathbb{Z}$ s.t. $us+vt=1$ (Bézout's relation)

则 $a=a^{su+tv}=\overset{e}{(a^s)}{}^u\cdot a^{tv}=a^{tv}=a^{tv}\cdot(\overset{e}{b^t})^v=a^{tv}\cdot b^{tv}=(a\cdot b)^{tv}\in\langle a\cdot b\rangle$

同理 $b\in\langle a\cdot b\rangle$ $\therefore\ \langle a,b\rangle\subseteq\langle a\cdot b\rangle$ $\therefore\ \langle a,b\rangle=\langle a\cdot b\rangle$

再证 $|\langle a\cdot b\rangle|=s\cdot t$

$(a\cdot b)^{st}=a^{st}\cdot b^{st}=(a^s)^t\cdot(b^t)^s=e \Rightarrow ord(a\cdot b)\mid st$

$\forall\ m\in\mathbb{N}$ s.t. $(a\cdot b)^m=e \Rightarrow (a\cdot b)^{m\cdot s}=(a^s)^m\cdot b^{m\cdot s}=e \Rightarrow b^{m\cdot s}=e \Rightarrow t\mid m\cdot s$

同理 $s\mid m\cdot t$ $\because \gcd(s,t)=1$ $\therefore\ t\mid m$ 且 $s\mid m \Rightarrow s\cdot t\mid m$

$\therefore\ ord(\overset{a\cdot b}{\cancel{s\cdot t}})=s\cdot t$ 即 $|\langle a\cdot b\rangle|=s\cdot t$.

综上 $\langle a,b\rangle=\langle a\cdot b\rangle$ 是一个(st)阶的循环子群.

(P128.5)

2. 设 G 是幺半群. 若 $\forall\ a,b\in G$ $ax=b$, $ya=b$ 均有唯一解.

则 G 是一个群.

Pf. 设 e为 G中单位元. $\forall\ g\in G$ $gx=e$, $y\cdot g=e$ 均有唯一解 设为 x_0, $y_0\in G$

则 $(y_0 g)x_0=e\cdot x_0=x_0$

$\quad y_0\cdot(g x_0)=y_0\cdot e=y_0$ $\therefore\ x_0=y_0$ $\therefore\ \exists\ x_0\in G$ s.t. $g x_0=x_0 g=e$

则 x_0 为 g 的逆元 由 g 任意性 $\Rightarrow$ G为群.

3. (P128,7) 群 $SL_2(\mathbb{Z})$ 含元素 $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$ 阶分别为 4, 3.

证明 $\langle AB\rangle$ 是无限循环群. 即 群 G 中 两个有限阶元相乘不一定有限阶

这在 Abel 群 中 成立吗?

解. $A\cdot B = \begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}0&1\\-1&-1\end{pmatrix} = \begin{pmatrix}-1&-1\\0&-1\end{pmatrix} = -\begin{pmatrix}1&1\\0&1\end{pmatrix}$

$(AB)^n = \left(-E_2-\begin{pmatrix}0&1\\0&1\end{pmatrix}\right)^n = (-1)^n\cdot\sum_{i=0}^{n}\binom{n}{i}\begin{pmatrix}0&1\\0&0\end{pmatrix}^i = (-1)^n\left[\binom{n}{0}\cdot E_2+\binom{n}{1}\cdot\begin{pmatrix}0&1\\0&0\end{pmatrix}\right]$

$= (-1)^n\cdot\begin{pmatrix}1&n\\0&1\end{pmatrix} \neq E_2$ 对 $\forall\, n\in \cancel{N}\,\mathbb{Z}^+$ $\therefore$ AB 为无穷阶.

若 G 为 Abel 群（交换群） 则 两个有限阶元相乘一定是有限阶.

$\because$ 设 $a,b\in G$ 且 $ord(a)=s$, $ord(b)=t$, $s,t\in \cancel{\mathbb{Z}}\,\mathbb{N}$.

则 $(a\cdot b)^{s\cdot t} \overset{交换}{=} a^{s\cdot t}\cdot b^{s\cdot t} = (a^s)^t\cdot(b^t)^s = e \Rightarrow ord(a\cdot b)\mid s\cdot t \Rightarrow$ 有限 □

4. (P128. 8) 群 G. 若 $|G|=2n$ 为偶数 则 $\exists\, g\in G$ s.t. $g^2=e$ 且 $g\neq e$.

证.(反证) 假设 $\forall\, g\neq e$ 且 $g\in G$, $g^2\neq e$ 则对 $\forall\, g\in G\setminus\{e\}$ $g\neq g^{-1}$

$\therefore$ $|\{g, g^{-1}\}| = 2$ 又 $\because$ ~~若~~ $\forall\, g_1, g_2\in G$. 若 $g_1=g_2$ 或 $g_1=-g_2$ 时

则 $\{g_1, g_1^{-1}\} = \{g_2, g_2^{-1}\}$ $\therefore$ $\{g_1, g_1^{-1}\}\neq\{g_2, g_2^{-1}\} \Rightarrow \{g_1,g_1^{-1}\}\cap\{g_2,g_2^{-1}\}=\emptyset$.

$\therefore$ 可以对 G 作分析(划分) $G=\{e\}\cup\{g_1,g_1^{-1}\}\cup\cdots\{g_s,g_s^{-1}\}$

$\therefore$ $|G|=2s+1$ 为奇数 矛盾. $\therefore$ $\exists\, g\neq e$ 且 $g^2=e$ □.

5. (P128. 14) 设 $A, B\in M_n(\mathbb{R})$. $\exists\, m\in\mathbb{Z}$ s.t. $(AB)^m=E$ 那么必有 $(BA)^m=E$ 吗?

解: 是

$\because$ $\exists\, m\in\mathbb{Z}$ s.t. $(AB)^m=E$ $\therefore$ $|(AB)^m| = |AB|^m = |A|^m\cdot|B|^m = 1 \Rightarrow |A|\neq0$, $|B|\neq0$

$\therefore$ A, B 均可逆.

$\left(\begin{aligned}(BA)^m &= B(AB)^{m-1}A = B\cdot(AB)^m\cdot(AB)^{-1}\cdot A\\ &= B\cdot(AB)^{-1}A = B\cdot B^{-1}\cdot A^{-1}\cdot A = E.\end{aligned}\right)$

若 $m=0$ 则 显然 $(BA)^m=E$

若 $m>0$ 则 $A^{-1}(AB)^mA = A^{-1}EA = A^{-1}A = E$

$$= (A^{-1}A)\underbrace{(BA)(BA)\cdots(BA)(BA)}_{2m个} = (BA)^m$$

若 $m<0$ 则 $B(AB)^mB^{-1}=E= B((AB)^{-1})^{-m}B^{-1} = B(B^{-1}A^{-1})^{-m}B^{-1} = (A^{-1}B^{-1})^{-m} = (BA)^m$

$\therefore$ $(BA)^m=E$ 对 $\forall\, m\in\mathbb{Z}$ 成立 □

6. 证明 (1) 所有四阶群都是 Abel 群.

(2) $\forall$ 四阶群 G 要么 $G \cong U = \langle (1234) \rangle$，要么 $G \cong V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$

(V_4 也称为 Klein 群)

(3) $L_1 = \{\pm E_2, \ \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\}$，$L_2 = \{\pm E_2, \ \pm\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}\}$ 均为 $GL_2(\mathbb{R})$ 子群

且并给出同构映射 $U \to L_1$，$V_4 \to L_2$.

证. (1) 设群 G 为 4 阶群 即 $|G| = 4$ 则 $\forall a \in G$ $ord(a) \mid 4 \Rightarrow ord(a) = 1, 2, 4$

若 $\exists a \in G$ s.t. $ord(a) = 4$ 则 G 为循环群 $\langle a \rangle \Rightarrow G$ 交换.

若 G 中无 4 阶元 则 $\forall a \in G$ $a^2 = e$ 由上周作业 G 交换.

(2) 若 $\exists a \in G$ s.t. $G = \langle a \rangle$ $\because$ 任意四阶循环群均同构于 $(\mathbb{Z}_4, +, \bar{0})$

$\therefore G \cong \langle (1234) \rangle$

若 G 中无 4 阶元 则设 $G = \{e, a, b, c\}$ 且 $a^2 = b^2 = c^2 = e$ $ab = c$, $ac = b$, $bc = a$.

($\because$ 若 $ab = a$ 则 $a \cdot a \cdot b = a \cdot a = e \Rightarrow b = e \to \leftarrow$)

构造 φ: $G \longrightarrow V_4$

$e \mapsto e$

$a \mapsto (12)(34)$

$b \mapsto (13)(24)$

$c \mapsto (14)(23)$

显然 $\varphi(a \cdot b) = \varphi(c) = (14)(23)$

$\varphi(a) \cdot \varphi(b) = (12)(34)(13)(24) = (14)(23)$

$\therefore \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ 同理可证 φ 为同态

显然 φ 良定义且为双射 $\therefore \varphi$ 同构.

(3). $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = E_2$ $\left(\pm\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}\right)^2 = E_2$ 易证为子群.

构造 φ_1 $U \longrightarrow L_1$

$\sigma \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$\sigma^2 \mapsto -E_2$

$\sigma^3 \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$e \mapsto E_2$

φ_2 : $V_4 \longrightarrow L_2$.

$e \mapsto E_2$

$(12)(34) \mapsto -E_2$

$(13)(24) \mapsto \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$

$(14)(23) \mapsto \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$

注：Klein 群一般看成 $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$

环

1. 定义：设集合 R 上有 2个运算：$+, \cdot$ 且有2个特别的元素 $0, 1 \in R$

若 1) $(R, +, 0)$ 构成交换群.

2) $(R, \cdot, 1)$ 构成幺半群　(如果交换 则称交换环).

3) 分配律：$\forall a, b, c \in$ ~~中~~ R. $\begin{cases} a\cdot(b+c) = a\cdot b + a\cdot c \\ (b+c)\cdot a = b\cdot a + c\cdot a \end{cases}$

则称 R 为环. 记为 $(R, +, 0, \cdot, 1)$

1'等价定义：设集合 R. 有 2个二元运算 $+, \cdot$　$\exists\, 0, 1 \in R$ s.t. $0 \neq 1$ 且

$\forall a, b, c \in R$　i) $(a+b)+c = a+(b+c)$
$0+a = a+0 = a$
$\exists\, d \in R$ s.t. $a+d = d+a = 0$ (ie $d = -a$)
$a+b = b+a$.
} 关于 + 构成交换群

ii) $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
$1\cdot a = a\cdot 1 = a$
} 关于 · 构成幺半群

iii) $a\cdot(b+c) = a\cdot b + a\cdot c$
$(b+c)\cdot a = b\cdot a + c\cdot a$
} ~~结合~~分配律.

2. 子环：设 R 为环. 集合 $S \subseteq R$ s.t. $0, 1 \in S$ 且 $(S, +, 0, \cdot, 1)$ 构成环.

则称 S 为 R 的子环.

3. 简单性质：1) $\forall r \in R$　$0\cdot r = r\cdot 0 = 0$

2) $\forall r \in R$.　$-r = (-1)\cdot r = r\cdot(-1)$

3) $(-1)\cdot(-1) = 1$

4) $\forall a, b \in R$. $m, n \in \mathbb{Z}$.　$(\underset{\uparrow\,\text{加法}}{m}a)\cdot(nb) = (\underset{\uparrow\,\text{整数乘法}}{m\cdot n})\cdot(a \underset{\uparrow\,\text{环中乘法}}{\cdot} b)$

4. 零因子和可逆元.

Def 1 设 R 为环，$a, b \in R \setminus \{0\}$ 若 $a \cdot b = 0$ 则称 a 为左零因子. b 为右零因子.

2. 设 R 为环 $a \in R$ 若 $\exists\, b \in R$ s.t. $a \cdot b = b \cdot a = 1$ 则称 a 为可逆元

(同理 b 也为可逆元) 且 b 为 a 的逆 (同理 a 也是 b 的逆).

eg 1. $M_n(\mathbb{R})$ 非交换环 $\operatorname{rank} A < n \iff A$ 既为左零因子又为右零因子.

$\operatorname{rank} A = n \iff A$ 可逆. $(sm + tn = 1 \Rightarrow \bar{m}^{-1} = \bar{s})$

$\mathbb{Z}_n$ 交换环. $\bar{m} \in \mathbb{Z}_n \setminus \{\bar{0}\}$ $\begin{cases} \bar{m} \text{ 可逆} \iff \gcd(m, n) = 1 \\ \bar{m} \text{ 是零因子} \iff \gcd(m, n) > 1 \end{cases}$

eg 2. 设 $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$

(1) 证明 R 为子环且交换 (2). 确定 R 中零因子. 可逆元.

(1) 解. 验证 $(R, +, 0)$ 为交换子~~群~~ 即证 $\forall A, B \in R$ $A - B \in R$ 显然

验证 $(R, \cdot, E_2)$ 为交换幺半~~群~~.

1) 封闭性 $\forall A, B \in R$ 设 $A = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}$, $B = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$

$$A \cdot B = \begin{pmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + a_2 b_1 \\ -(a_2 b_1 + a_1 b_2) & a_1 a_2 - b_1 b_2 \end{pmatrix} \in R$$

2) 结合律和乘法单位元 E_2 显然

3) 交换: $\cancel{AB}$ $BA = \begin{pmatrix} a_1 a_2 - b_1 b_2 & a_2 b_1 + a_1 b_2 \\ -(a_2 b_1 + a_1 b_2) & a_1 a_2 - b_1 b_2 \end{pmatrix} = BA$.

~~验证分配律~~:

$\therefore R \subseteq M_2(\mathbb{R})$ 为交换子环.

(2) $\forall A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in R$ $|A| = a^2 + b^2$ 则 $|A| = 0 \iff A = O$

$\therefore R$ 中无非平凡零因子.

若 $A \neq 0$ 则 $A^{-1} = \frac{1}{|A|} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in R$ $\therefore$ 非零元均为可逆元.

注 R 实际上是域.

eg3. 设环 R. 若 $\forall\, a\in R$ $\exists!\, b\in R$ s.t. $aba=a$ $\Rightarrow$ R 无0因子.

注 非交换环无0因子 即是 既无左零因子 又无右零因子.

证. (反证) 假设 R 有 左零因子. 设为 a 则 $\exists$ $c\in R\setminus\{0\}$ s.t.

$ac=0 \Rightarrow aca=0\cdot a=0$ ① 又 $\because$ $\exists\, b\in R$ s.t. $aba=a$ ②

$\xRightarrow{①+②}$ $aca+aba=a \Rightarrow a(c+b)a=a$ (分配律)

$\because$ $c\neq 0$ $\therefore$ $c+b\neq b$ 即 又存在一个 $c+b$ 满足题意 与唯一性矛盾.

同理可证 R 无右零因子. $\therefore$ R 无0因子 □

5. 整环: 交换环 + 无0因子. (有消去律)

eg. $\mathbb{Z}$. ($F[x]$)

6. 环同态.

设环 R_1, R_2 若映射 $\varphi: (R_1,+,0,\cdot,e_1)\longrightarrow(R_2,+,0,\cdot,e_2)$ 满足.

$\forall\, a,b\in R_1$. $\begin{cases}\varphi(a+b)=\varphi(a)+\varphi(b)\\ \varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)\\ \varphi(e_1)=e_2\end{cases}$ 则称 φ 为环同态.

(注 $\because$ 有加法消去律 $\therefore$ $\varphi(0)=0$
但乘法一般无消去律 需定义 $\varphi(e_1)=e_2$.)

eg. $\varphi: \mathbb{Z}\longrightarrow\mathbb{Z}_n$ 为环同态.

$m \mapsto \overline{m}=\{m+kn \mid k\in\mathbb{Z}\}$

eg4. 求 $\mathbb{Z}_{24}$ 的零因子 和 可逆元. (可不讲)

可逆元 $\overline{1}$. $\overline{5}$ $\overline{7}$ $\overline{11}$ $\overline{13}$ $\overline{17}$ $\overline{19}$ $\overline{23}$

零因子 $\overline{2}$ $\overline{3}$ $\overline{4}$ $\overline{6}$ $\overline{8}$ $\overline{9}$ $\overline{10}$ $\overline{12}$ $\overline{14}$ $\overline{15}$ $\overline{16}$ $\overline{18}$ $\overline{20}$ $\overline{21}$ $\overline{22}$

求 $\overline{17}$ 的逆 求 $17s+24t=1$ 利用扩展 Euclidean 算法 $s=-7$. $t=5$.

$\therefore$ $\overline{17}$ 的逆为 $\overline{-7}=\overline{24-7}=\overline{17}$ $\therefore$ $\overline{17}\cdot\overline{17}=\overline{1}$.

域

1. 定义：设 F 是整环（交换 + 无0因子）且 F 中任意非0元可逆，则称 F 为域

eg. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$（p为素数）

2. 域的特征　考虑域 $(F, +, 0, \cdot, 1)$

域 F, $\begin{cases} 若不存在\ m \in \mathbb{Z}^+\ s.t.\ \overbrace{1+\cdots+1}^{m个} = 0 & 则称域F特征为0. \\ 若\ \exists\ p \in \mathbb{Z}^+\ s.t.\ \overbrace{1+\cdots+1}^{p个} = 0\ 且\ p为素数（最小正整数） & 则称F特征为p. \end{cases}$

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

且 $\mathbb{Z}_p$ 为 char = p 的最小域

eg. $\mathrm{char}(\mathbb{Q}) = 0$,　$\mathrm{char}(\mathbb{Z}_p) = p$　（p为素数）

Prop 1 (1) Freshmen's dream：
设域 F　$\mathrm{char}(F) = p > 0$　则 $\forall x, y \in F$　$(x+y)^p = x^p + y^p$.

(2) Fermat's little thm：
设域 F, $\mathrm{char}(F) = p > 0$　则 $\forall x \in F$　$x^p = x$　$(p \nmid m \Rightarrow m^p \equiv m \mod p)$

3. 域上的线性代数.

考虑 $F_p = (\mathbb{Z}_p, +, \bar{0}, \cdot, \bar{1})$ 上的线性代数.

$$F_p^n = \left\{ \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_n \end{pmatrix} \middle| \ \bar{x}_i \in \mathbb{Z}_p \right\}$$

加法　$\vec{x} + \vec{y} = \begin{pmatrix} \overline{x_1 + y_1} \\ \vdots \\ \overline{x_n + y_n} \end{pmatrix}$

数乘：$\bar{\alpha} \cdot \vec{x} = \begin{pmatrix} \overline{\alpha x_1} \\ \vdots \\ \overline{\alpha x_n} \end{pmatrix}$

线性相关/无关：称 $\vec{w}_1, \cdots \vec{w}_\ell \in F_p^n$ 线性相关，如果 $\exists$ 不全为 $\bar{0}$ 的
$\bar{r}_1, \cdots \bar{r}_\ell \in \mathbb{Z}_p$ s.t. $\bar{r}_1 \cdot \vec{w}_1 + \cdots + \bar{r}_\ell \cdot \vec{w}_\ell = \vec{0} = \begin{pmatrix} \bar{0} \\ \vdots \\ \bar{0} \end{pmatrix}$

否则 称 线性无关.

$W \subseteq F_p^n$ 为子空间 如果 W 对 加法 数乘 封闭.

4. 域同态

设 $\varphi: (E, +, 0_E, \cdot, 1_E) \longrightarrow (F, +, 0_F, \cdot, 1_F)$ 为环同态.

则 φ 为域同态.

注 $\varphi(0_E) = 0_F$. $\varphi(1_E) = 1_F$. $\varphi(-a) = -\varphi(a)$. $\varphi(a^{-1}) = (\varphi(a))^{-1}$ $(\forall a \neq 0_E)$.

<u>Prop1.</u> 若 $\varphi: E \longrightarrow F$ 为域同态 则 φ 为单射.

<u>Prop2</u> 设域 E, F 若 $\mathrm{char}(E) \neq \mathrm{char}(F)$ 则 E, F 之间不可能有同态.

<u>Pf</u>. 假设 $\exists$ 域同态 $\varphi: E \longrightarrow F$.

1) 若 $\mathrm{char}(E) = 0$ $\mathrm{char}(F) = p > 0$

$$\varphi(\underbrace{1_E + \cdots + 1_E}_{p\text{个}}) = \varphi(1_E) + \cdots + \varphi(1_E) = \underbrace{1_F + \cdots + 1_F}_{p\text{个}} = 0_F$$

$\because \varphi$ 为单射 $\therefore \underbrace{1_E + \cdots + 1_E}_{p} = 0_E$ 与 $\mathrm{char}(E) = 0$ 矛盾.

2) 若 $\mathrm{char}(E) = p > 0$ $\mathrm{char}(F) = 0$.

$$\varphi(\underbrace{1_E + \cdots + 1_E}_{p}) = \varphi(0_E) = 0_F = \underbrace{1_F + \cdots + 1_F}_{p}$$ 与 $\mathrm{char}(F) = 0$ 矛盾.

3) 若 $\mathrm{char}(E) = p > 0$ $\mathrm{char}(F) = q > 0$

$$\varphi(\underbrace{1_E + \cdots + 1_E}_{p}) = 0_F = \underbrace{1_F + \cdots + 1_F}_{p} \Rightarrow \because \mathrm{char}(F) = q \ \therefore q \mid p$$

又 $\because p$ 为素数 $\therefore p = q$ 矛盾. 综上 不存在域同态 □.

eg1. 设 $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ 求解 $\begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{2} & \bar{1} & \bar{2} \\ \bar{1} & \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix}$

$$A \longrightarrow \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & \overline{-3} & \bar{0} \\ \bar{0} & \overline{-2} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \end{pmatrix} \Rightarrow \begin{cases} x_1 + x_3 = \bar{0} \\ x_2 = \bar{0} \end{cases}$$

$\therefore$ 非零解为 $\begin{pmatrix} \bar{1} \\ \bar{0} \\ \overline{-1} \end{pmatrix} = \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{2} \end{pmatrix}$

$\therefore$ 解空间维数是 1. $V_A = \left\{ \lambda \cdot \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{2} \end{pmatrix} \mid \lambda \in \mathbb{Z}_3 \right\} = \left\{ \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{2} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{0} \\ \bar{1} \end{pmatrix} \right\}$.

eg2. 设 $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ 求 $\begin{pmatrix} \bar{1} & \bar{2} \\ \bar{0} & \bar{1} \end{pmatrix}^n$ $(n \in \mathbb{N})$

$$\begin{pmatrix} \bar{1} & \bar{2} \\ 0 & \bar{1} \end{pmatrix}^n = \left[\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} - \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{0} \end{pmatrix} \right]^n = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} - n \cdot \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & -\bar{n} \\ 0 & \bar{1} \end{pmatrix}$$