P(42) 7题

1. 证明：已知 ~~$\mathbb{Z}_3$~~ $M_2(\mathbb{Z}_3)$ 是环（即数域 $\mathbb{Z}_3$ 上的2阶方阵全体）只须证 $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a,b\in\mathbb{Z}_3\right\}$ 是子环 $\triangleq A$

且所有元素都有逆元。

① ∵ $(M_2(\mathbb{Z}_3),+,\begin{pmatrix}\bar0&\bar0\\\bar0&\bar0\end{pmatrix})$ 是环，只须证 $(A,+,\begin{pmatrix}\bar0&\bar0\\\bar0&\bar0\end{pmatrix})$ 子环．即 ~~$\begin{pmatrix}\bar0&\bar0\\\bar0&\bar0\end{pmatrix}\in A$~~ $\forall x,y\in A$.

$x-y\in A$ 且 $xy\in A$.

$x=\begin{pmatrix}\bar a_1 & \bar b_1\\ -\bar b_1 & \bar a_1\end{pmatrix}$ $y=\begin{pmatrix}\bar a_2 & \bar b_2\\ -\bar b_2 & \bar a_2\end{pmatrix}$ $\therefore x-y=\begin{pmatrix}\bar a_1-\bar a_2 & \bar b_1-\bar b_2\\ \bar b_2-\bar b_1 & \bar a_1-\bar a_2\end{pmatrix}=\begin{pmatrix}\overline{a_1-a_2} & \overline{b_1-b_2}\\ -\overline{b_1-b_2} & \overline{a_1-a_2}\end{pmatrix}\in A$

$xy=\begin{pmatrix}\overline{a_1a_2-b_1b_2} & \overline{a_1b_2+b_1a_2}\\ -\overline{b_1a_2+a_1b_2} & \overline{a_1a_2-b_1b_2}\end{pmatrix}=yx$ $\therefore A$ 是交换环

② ~~∴ $(A,+)$ 是~~ $\begin{pmatrix}\bar1&\bar0\\\bar0&\bar1\end{pmatrix}\in A$

③ $\forall x=\begin{pmatrix}\bar a_1 & \bar b_1\\ -\bar b_1 & \bar a_1\end{pmatrix}\in A$ $\begin{pmatrix}\bar a_1 & \bar b_1\\ -\bar b_1 & \bar a_1\end{pmatrix}\cdot\begin{pmatrix}\bar a_1 & -\bar b_1\\ \bar b_1 & \bar a_1\end{pmatrix}\dfrac{\bar1}{\overline{a_1^2+b_1^2}}=\begin{pmatrix}\bar1&\bar0\\\bar0&\bar1\end{pmatrix}$

∵ 在 $\mathbb{Z}_3$ 中所有元素可逆 $\therefore \dfrac{\bar1}{\overline{a_1^2+b_1^2}}\in\mathbb{Z}_3$ $\therefore \begin{pmatrix}\bar a_1 & -\bar b_1\\ \bar b_1 & \bar a_1\end{pmatrix}\dfrac{\bar1}{\overline{a_1^2+b_1^2}}\in M_2(\mathbb{Z}_3)$ 且

$\begin{pmatrix}\bar a_1 & -\bar b_1\\ \bar b_1 & \bar a_1\end{pmatrix}\dfrac{\bar1}{\overline{a_1^2+b_1^2}}\in A$ $\therefore A$ 是域 且 不同的 a,b 组合有 $3\times3=9$ 种 ∴ 是9元域

④ 令 $a=\begin{pmatrix}\bar1&\bar1\\-\bar1&\bar1\end{pmatrix}$ $a^2=\begin{pmatrix}\bar0&\bar2\\-\bar2&\bar0\end{pmatrix}$ $a^3=\begin{pmatrix}-\bar2&\bar2\\-\bar2&-\bar2\end{pmatrix}$ $a^4=\begin{pmatrix}\bar2&\bar0\\\bar0&\bar2\end{pmatrix}$

$a^8=(a^4)^2=\begin{pmatrix}\bar1&\bar0\\\bar0&\bar1\end{pmatrix}$ $\therefore a$ 是8阶元 $\therefore A$ 的乘法群是8阶循环群.

3. 有限整环一定是域.

证明：设 R 是有限整环．则当 $a\neq0$ 时．$ab=ac\Rightarrow b=c$（没有零因子）∴ 若 $b\neq c$ 则 $ab\neq ac$

$\therefore |aR|=|R|$ 且 $aR\subset R$ $\therefore aR=R$ ∵ R 整环 ∴ 有幺元 ∴ $1\in R$ ∴ $\exists b\in R$ 使 $ab=1$

∵ 交换 ∴ $ba=ab=1$ ∴ $b=a^{-1}$ ∴ R 是域.

4. (1) 证明 作用．由定义．① $\exists L_{\bar0}\in\mathbb{Z}_2$ 使 $\forall(a,b)\in X$. $L_{\bar0}(a,b)=(a,b)$

② $L_{\bar0}\circ L_{\bar1}(a,b)=L_{\bar0}(b,a)=(b,a)=L_{\bar1}(a,b)=L_{\bar0+\bar1}(a,b)=L_{\bar1}\circ L_{\bar0}(a,b)$

$L_{\bar1}\circ L_{\bar1}(a,b)=L_{\bar1}(b,a)=(a,b)=L_{\bar1+\bar1}(a,b)=L_{\bar0}(a,b)$

即 $\forall g_1,g_2\in\mathbb{Z}_2$，$\forall x\in X$ 有 $L_{g_1}\circ L_{g_2}(x)=L_{g_1g_2}(x)$ $(g_1(g_2(x))=g_1g_2(x))$

(2) 即求 $a\in X$，使得 $\forall L_i\in\mathbb{Z}_2\ (i=0,1)$ $L_i(x)=x$.

对 $\forall(a,b)\in X$. 有 $L_0(a,b)=(a,b)$ 故只须考虑某 $(a,b)\in X$. 使得 $L_1(a,b)=(a,b)=(b,a)$ $\therefore a=b$

又 $\because ab=e$ $\therefore a=b^{-1}$ $b=a^{-1}$ 即 $\therefore b=a^{-1}=a$

$\therefore X$ 上的不动点为 $\{(a,a^{-1})\mid a^{-1}=a\in G\}$

(3). 所有 X 上不是不动点的元素即所有的 $\{(a,a^{-1}),(a^{-1},a)\mid$ 其中 $a^{-1}\neq a\in G\}$ 有偶数个.

~~$\therefore X$ 上是不动~~ $\because |G|=2n$ $\therefore |X|=(2n)^{n}$ 也是偶数 $\therefore X$ 上不动点个数有偶数个.

$\because (e,e)$ 是一个不动点 $\therefore$ 不动点个数大于等于2. 故存在非平凡的二阶元.

(4) 定义 $L_0(a_1,\cdots a_p)=(a_1,\cdots,a_p)$

$L_1(a_1,\cdots a_p)=(a_2,\cdots a_p,a_1)$

$L_2(a_1\cdots a_p)=(a_3\cdots a_p,a_1,a_2)$

$\cdots$

$L_p(a_1\cdots a_p)=(a_p,a_1\cdots a_{p-1})$

作用：① $\exists L_0\in\mathbb{Z}_p$. 使 $L_0(a_1,\cdots a_p)=(a_1,\cdots a_p)$ 对 $\forall(a_1,\cdots a_p)\in X$ 成立.

② $\forall L_i,L_j\in\mathbb{Z}_p$. $L_i(L_j(a_1\cdots a_p))=L_i(a_{j+1},\cdots a_p,a_1\cdots a_j)=(a_{i+j+1},\cdots a_p,a_1\cdots a_{i+j})$

$=L_{i+j}(a_1\cdots a_p)$ （即 $\forall g_1,g_2\in\mathbb{Z}_p.\ \forall x\in X\ g_1(g_2(x))=g_1g_2(x)$）

(5) $|O_x|=\dfrac{|\mathbb{Z}_p|}{|H_x|}$ $|X|=\sum_{x\in\Omega}|O_x|$ （Ω 是不同轨道的代表

$\because |\mathbb{Z}_p|=p$ 是素数 $\therefore$ 只有 $|O_x|=p$ 或 1 当 $|O_x|=1$ 时. 即 $O_x=\{x\mid\forall g\in\mathbb{Z}_p.\ g(x)=x\}$

$=\{g(x)\mid\forall g\in\mathbb{Z}_p\}$

即 x 是不动点 $\therefore |X|=kp+m\cdot 1$ （m 即为 X 中不动点的个数）

$\therefore |X|-m\cdot 1=kp\equiv 0\bmod p$

若 $|G|$ 被 p 整除，设 $=np$ 则 $|X|=(np)^{n}\equiv 0\bmod p$ $\therefore m\equiv 0\bmod p$

X 中所有不动点 $(a_1\cdots a_p)$ 满足 $\forall L_i\in\mathbb{Z}_p$. $L_i(a_1\cdots a_p)=(a_1,\cdots a_p)=(a_{i+1},\cdots a_p,a_1\cdots a_i)$

$\therefore a_1=a_2=\cdots=a_p$ 又 $\because a_1\cdot a_2\cdots a_p=(a_1)^p=e$ $\therefore a_1$ 是 p 阶元或 e，显然 $(e,\cdots,e)$ 是一个不动点，（且 p 是素数）

$\therefore m\geq 1$ 又 $\because m\equiv 0\bmod p$ $\therefore m\geq p$ 且 $m\equiv 0\bmod p$ 至少有 $p-1$ 个 p 阶元在 G 中.

群、环、域知识梳理：

半群：①集合G；②运算"+"：$G\times G\to G$；③结合律加法：$(g_1+g_2)+g_3=g_1+(g_2+g_3)$

幺半群：①②③④含有幺元：$\exists e\in G$, s.t. $\forall g\in G$, 都有 $e+g=g+e=g$ （可简化为 $e+g=g$）单位元(幺元)是唯一的

群：①②③④⑤每个元素 $g\in G$, $\exists g'\in G$ s.t. $g+g'=g'+g=e$ （可简化为 $g+g'=e$）g'称为g的逆元是唯一的，写作g^{-1}

交换群(Abel群)：①②③④⑤⑥ 对 $\forall g_1,g_2\in G$, $g_1+g_2=g_2+g_1$

子群：G是一个群，H是G的子群，即：H关于G中运算形成群，写作$H<G$.

证明步骤：方法一：1) $e\in H$；2) $\forall h\in H$, $h^{-1}\in H$ 3)$\forall h_1,h_2\in H$, $h_1+h_2\in H$

法二：2) $\forall h_1,h_2\in H$, $h_1+h_2^{-1}\in H$

正规子群：G是一个群，H是G的正规子群，即：①H是G的子群；②$\forall g\in G$, $gH=Hg$ $gHg^{-1}=H+g$（左陪集=右陪集）

环：①②③④⑤⑥⑦运算"·"：$G\times G\to G$；⑧乘法结合律 $\forall g_1g_2g_3\in G$, $(g_1g_2)g_3=g_1(g_2g_3)$；

⑨两个分配律：$\forall g_1,g_2,g_3\in G$, $g_1(g_2+g_3)=g_1g_2+g_1g_3$；$(g_1+g_2)g_3=g_1g_3+g_2g_3$；

[注：此时，关于"+"的g的逆元，称作g的负元，写作$-g$；关于"+"的单位元(幺元)，称作零元，写作0]

幺环：①②③④⑤⑥⑦⑧⑨⑩含有关于"·"的单位元(幺元)：$\exists e\in G$, s.t. $\forall g\in G$, $eg=ge=g$（可简化为$eg=g$，乘法单位元是唯一的）将e写作1.

[注：所有的设L是幺环，若对于$a,b\in L$，使得 $ab=1$，则称b为a的右逆，a为b的左逆。若a的左逆和右逆都存在且相等，则称a为L的一个可逆元素，叫做单位，L的全体单位构成的集合对乘法成一群，称为L的单位群]

零因子：L是环，$a\in L$, $a\neq 0$. 若$\exists b\in L$, s.t. $ab=0$ 则a称为一个左零因子.

[注：若在环L中消去律成立$\Leftrightarrow$没有零因子]

子环：L是环，S是L的子环，即：S关于L中的"+"、"·"运算形成环。

证明步骤：法一：1) S关于"+"构成L的子群；2) S关于"·"封闭，$\forall s_1,s_2\in S$, $s_1s_2\in S$

交换环：①②③④⑤⑥⑦⑧⑨⑪ 对L是一个环，$\forall a,b\in L$, $ab=ba$ 乘法交换

整环：①②③④⑤⑥⑦⑧⑨⑩⑪⑫ 没有零因子.

域：①②③④⑤⑥⑦⑧⑨⑩⑪⑫⑬全体非零元素都有关于"·"的逆，即都是可逆元素.

~~反证~~证明：法一：1)关于加法是群；2)关于加法交换；3)若下是域，则$1\in F$；4)全体非零都是可逆元素

[注：实际上⑬即暗含⑫]

除环：(体) ① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑫ ⑬ ：(没有乘法交换的域)

分式环(商域)：R为整环，包含R的最小的域，称为R的商域。

分式域 ⇔ 若F是R的商域，则：1) R是F的子环；

2) F的每个元素 $a\in F$，可写成R的两个元素 $b,c\in R$ 的商，即 $a=\frac{b}{c}$，$c\neq 0$

群同态：G,G' 是两个群，称映射 φ 是群同态，则：即：$\varphi: G\to G'$ 满足 $\varphi(g_1g_2)=\varphi(g_1)\cdot\varphi(g_2)$ 对 $\forall g_1,g_2\in G$ 成立

其中等式右边的"·"是G中乘法运算，右边的"·"是G'中乘法运算。

环同态：L,L' 是两个环，称 ψ 是环的同态，即：$\psi: L\to L'$ 满足 1) $\psi(g_1+g_2)=\psi(g_1)+\psi(g_2)$，对 $\forall g_1,g_2\in GL$

2) $\psi(g_1g_2)=\psi(g_1)\cdot\psi(g_2)$，对 $\forall g_1,g_2\in GL$

问题：设 $f: R\to R'$ 是一个满的环同态，而且将R的单位元1映射到R'的单位元$1'$。指出下列命题的正确和错误。

i) 若 $a\in R$ 是幂零(幂等)元，则 $f(a)$ 也是R'的幂零(幂等)元 (如果环的元素a，有$a^2=a$，则a叫做幂零元)

ii) 若 $a\in R$ 是零因子，则 $f(a)$ 也是R'的零因子

iii) 若R为整环，则 $f(R)=R'$ 也是整环

iv) 若 $f(R)=R'$ 为整环，则R也是整环

v) 若 $u\in R$ 为单位，则 $f(u)$ 也是R'的单位

vi) 若 $f(u)$ 是R'的单位，则u也是R的单位。