第十二次习题课

一、作业分析及需要注意的问题

1. 设A为一n阶方阵，用rank(A)表示rank($A^\vee$).

对rank(A)分类讨论

① 若rank(A)=n，$A^\vee=|A|\cdot A^{-1}$ [满秩可逆，才有此式子]

$\text{rank}A^{-1}=\text{rank}(A)=n.$

② 若rank(A)=n-1，则A存在n-1阶非零子式

i.e. $\exists i,j$ s.t. $A_{ij}\neq 0 \implies \text{rank}(A^\vee)\geq 1.$

又$\because A\cdot A^\vee=|A|\cdot E=0$ 由Sylvester不等式

$\text{rank}(A\cdot A^\vee)\geq \text{rank}(A)+\text{rank}(A^\vee)-n$

$\implies \text{rank}(A^\vee)\leq 1$

综上：$\text{rank}(A^\vee)=1.$

③ 若rank(A)<n-1，则A所有n-1阶子式均为0.

$\implies \text{rank}(A^\vee)=0.$

注：1. 由子式定义矩阵的秩的理解.

2. 伴随矩阵的定义

hw2. 证：$\det(A)\neq 0$，$\text{rank}(A)=n$，A可逆

$$\begin{pmatrix} A & B \\ C & D\end{pmatrix}\begin{pmatrix} E_n & -A^{-1}B \\ 0 & E_n\end{pmatrix}=\begin{pmatrix} A & 0 \\ C & D-CA^{-1}B\end{pmatrix}$$ 两边取行列式

$$\det\begin{pmatrix} A & B \\ C & D\end{pmatrix}\cdot\det\begin{pmatrix} E_n & -A^{-1}B \\ 0 & E_n\end{pmatrix}=(-1)^{2n^2}\det\begin{pmatrix} D-CA^{-1}B & C \\ 0 & A\end{pmatrix}$$

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix}\cdot\det(E_n)\cdot\det(E_n) = 1\cdot\det(D-CA^{-1}B)\cdot\det(A)$$

即 $$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD-ACA^{-1}B)$$
$$=\det(A)\cdot\det(D-CA^{-1}B)$$

验证：$AC=CA$时，
$$\det(AD-ACA^{-1}B)=\det(AD-CAA^{-1}B)$$
$$=\det(AD-CB)$$

$AB=BA$时，
$$\det(A(D-CA^{-1}B))=\det[(D-CA^{-1}B)A]$$
$$=\det(DA-CA^{-1}BA)=\det(DA-CA^{-1}AB)$$
$$=\det(DA-CB)$$

二、 二元运算（结合律） 半群

单位元 含幺半群

逆元 群

注：i) 左逆、右逆与消去律

ii) 交换群

hw3. ① 证明半群

Step 1. 新定义的运算封闭

若 $A=(a_{ij})_{n\times n}$，$B=(b_{ij})_{n\times n}$ $\quad A, B\in M_n^0(\mathbb{R})$

则 $A\cdot B=C=(c_{ij})_{n\times n}$

$$\sum_j c_{ij}=\sum_j\sum_k a_{ik}b_{kj}=\sum_k\sum_j a_{ik}b_{kj}=0$$

$$\Longrightarrow A\cdot B\in M_n^0(\mathbb{R})$$

Step2. 结合律

$(A\cdot B)\cdot C = A\cdot(B\cdot C)$ [由矩阵乘法可知]

$\therefore$ $M_n^0(\mathbb{R})$为半群.

假设有单位元 $e=(e_{ij})_{n\times n}$ s.t. $eA=Ae=A$.

此时由矩阵乘法知 $e=E_n$.

又 $E_n \notin M_n^0(\mathbb{R})$

$\therefore$ $(M_n^0(\mathbb{R}),\cdot)$ 无单位元.

三、群的乘法表与同余运算

hw4.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{1}$	$\bar{2}$	$\bar{1}$

×	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

通过行列清晰的看出左乘与右乘

通过表格看群的结构

验证: $\mathbb{Z}_3^\times := \mathbb{Z}_3\setminus\{\bar{0}\}$ 为群.

Step1. 封闭

Step2. 结合

Step3. $\bar{1}\cdot\bar{1}=\bar{1}$, $\bar{1}\cdot\bar{2}=\bar{2}\cdot\bar{1}=\bar{2}$, $\bar{1}$ 为单位元

Step4. $\bar{2}\cdot\bar{2}=\bar{1}$, $\bar{2}^{-1}=\bar{2}$. 逆元.

$\mathbb{Z}_3^*=\{\bar{2},\bar{2}^2\}$ 为二阶循环群.

当p为素数时, $\mathbb{Z}_p^*=\{\bar{1},\cdots,\overline{p-1}\}$

$\forall \bar{a} \in \mathbb{Z}_p^*$, $(a, p)=1$ 故 $\exists k, l$ s.t. $ak+pl=1$.

$\therefore \bar{a}\bar{k}+\bar{p}\bar{l}=\bar{1} \implies \bar{a}\cdot\bar{k}=\bar{1}$

由此可知 满足群的定义.

$\therefore$ $\mathbb{Z}_p^*$ 为乘法群.

eg1. 在乘法幺半群 M 中选出任意一个元素 t, 并引入一个新的运算 $*$: $x*y=xty$. 证明 $(M,*)$ 是一个半群, 且 $(M,*)$ 成为一个幺半群, 当且仅当所选的元素 t 是可逆的, 这时它的单位元为 t^{-1}.

证: step1. 封闭 $\forall x, y \in M$ $\because t \in M$ 且 M 对乘法封闭

$\therefore xty \in M \implies x*y \in M$.

step2. 结合律: $\forall x, y, z \in M$.

$$(x*y)*z=(xty)tz=xt(ytz)=x*(y*z)$$

$\therefore$ $(M,*)$ 构成半群.

"$\implies$" 设 e 为乘法单位元, ε 为 $(M,*)$ 的幺元.

则 $e=e*\varepsilon=et\varepsilon=t\varepsilon$

$e=\varepsilon*e=\varepsilon te=\varepsilon t$

$\implies t\varepsilon=\varepsilon t=e \implies t$ 可逆且 $\varepsilon=t^{-1}$.

"$\impliedby$" $\forall x \in M$, $t^{-1}*x=(t^{-1}t)x=ex=x$.

$x*t^{-1}=x(tt^{-1})=x$ $\therefore t^{-1}$ 为 $*$ 单位元.

$\therefore$ $(M,*)$ 构成幺半群.

eg2. 证明集合 $\mathbb{Z}$ 关于运算 $\circ$ 构成一个交换幺半群, 其中 $\circ$:

$n\circ m=n+m+nm=(1+n)\times(1+m)-1$, 什么是 $(\mathbb{Z},\circ)$ 的单位元? 找出 $(\mathbb{Z},\circ)$ 的全部可逆元。

解: 封闭, 结合律满足, 可自行验证.

单位元：$\forall n\in\mathbb{Z}$，$n\circ 0=0\circ n=n \Rightarrow 0$ 为 $(\mathbb{Z},\circ)$ 单位元。

交换：$\forall n,m\in\mathbb{Z}$，$n\circ m=(1+n)(1+m)-1$

$=(1+m)(1+n)-1=m\circ n$.

可逆元：设 $n\in\mathbb{Z}$ 可逆 即 $m\in\mathbb{Z}$ s.t. $n\circ m=0$

$\Rightarrow (1+m)(1+n)=1$

$\Rightarrow 1+n=1$ or $1+n=-1 \Rightarrow n=0$ or $n=-2$.

$0^{-1}=0$，$(-2)^{-1}=-2$.

可逆元为 $\{0,-2\}$.

eg3. $\mathbb{Z}_{30}$ 的所有可逆元，并证明 $\mathbb{Z}_{30}$ 的所有可逆元关于乘法构成一个群。

证：1) $\bar{n}\in\mathbb{Z}_{30}$ 可逆 $\Longleftrightarrow \gcd(n,30)=1$.

($\bar{n}$ 可逆 $\Longleftrightarrow \exists\, \bar{m}\in\mathbb{Z}_{30}$ s.t. $\bar{n}\cdot\bar{m}=\bar{1}$

$\Longleftrightarrow \overline{m\cdot n-1}=\bar{0}$

$\Longleftrightarrow m\cdot n-1=30k \quad (k\in\mathbb{Z})$

$\Longleftrightarrow m\cdot n+(-k)\cdot 30=1$

$\Longleftrightarrow \gcd(n,30)=1$)

$\therefore$ $\mathbb{Z}_{30}$ 的全部可逆元为 $S=\{\bar{1},\bar{7},\overline{11},\overline{13},\overline{17},\overline{19},\overline{23},\overline{29}\}$

2) 证明 S 为群.

封闭，$\forall \bar{m},\bar{n}\in\mathbb{Z}_{30}$ 可逆 $\Rightarrow \bar{m}\cdot\bar{n}$ 可逆

结合律成立.

$\bar{1}$ 为 S 单位元

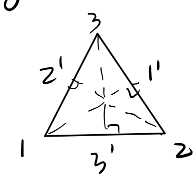
$\forall \bar{m}\in S$，$\because \bar{m}$ 可逆 $\Rightarrow \exists\, \bar{n}\in\mathbb{Z}_{30}$ s.t $\bar{m}\cdot\bar{n}=\bar{1}$

$\Rightarrow \bar{n}$ 可逆 $\Rightarrow \bar{n}\in S$.

$\therefore$ S 构成群。

四、同态与同构及其性质

eg4. 考虑将等边三角形变到自身的所有变换



旋转变换 $\begin{cases} \varphi_0 \longleftrightarrow e & (\text{旋转 } 0^\circ) \\ \varphi_1 \longleftrightarrow (132) & (\text{旋转 } 120^\circ) \\ \varphi_2 \longleftrightarrow (123) & (\text{旋转 } 240^\circ) \end{cases}$

对称变换 $\begin{cases} \psi_1 \longleftrightarrow (23) \\ \psi_2 \longleftrightarrow (13) \\ \psi_3 \longleftrightarrow (12) \end{cases}$ 轴对称变换 (反射)

$G = \{\varphi_0, \varphi_1, \varphi_2, \psi_1, \psi_2, \psi_3\}$

则 $G \cong S_3$ (3个元素的置换群)

$(\varphi_1\psi_1 = \psi_2 \longleftrightarrow (132)(23) = (13))$.

i) 比较群 G 与 G' 的方法: 同构. $\begin{cases} f(a*b) = f(a)\circ f(b) \\ \text{双射.} \end{cases}$ $f\ (\exists)$.

ii) 同构的性质: 单→单, 逆→逆, 逆映射.

Thm1. 任意两个同阶的循环群是同构的(特别地,任意两个无限循环群是同构的).

证: ① 若 $\langle g\rangle$ 是无限循环群, 则所有 g 的方幂 g^n 彼此不同.

令 $g^n \longmapsto f(g^n) = n$. 同构: $f: \langle g \rangle \longrightarrow (\mathbb{Z}, +)$

$$f(g^m g^n) = f(g^m) f(g^n)$$

f 双射.

②. $G = \{e, g, \cdots, g^{q-1}\}$, $G' = \{e', g', \cdots, (g')^{q-1}\}$

是两个 q 阶循环群

$$f: g^k \longrightarrow (g')^k \qquad k = 0, 1, \cdots, q-1.$$

任取 $n,m=0,1,\cdots,g-1$. 设 $n+m=lg+r \quad 0\le r\le g-1$.

$$f(g^{n+m})=f(g^r)=(g')^r=(g')^{n+m}$$
$$=(g')^n(g')^m=f(g^n)f(g^m). \quad \square$$

iii> 同态映射

既不要求 f 单，又不要求 f 满.

$$f: G \longrightarrow G'$$

$Im f \subset G'$ 是 G' 的一个子群.

$\begin{cases} ker f \le G \\ im f \le G' \end{cases}$

同态与同构的区别主要在于非平凡核 $ker f$ 的存在.

$ker f=\{g\in G \mid f(g)=e', e'$ 是 G' 单位元$\}$.

eg5. 对一般线性群 $(GL_n(\mathbb{R}), \cdot, E_n)$，其中

$GL_n(\mathbb{R})=\{A\in\mathbb{R}^{n\times n} \mid det(A)\neq 0\}$. 定义映射

$$\phi: GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$$

s.t. $\phi(A)=(A^{-1})^t$. 证明 ϕ 是同构映射。

证: Step 1. 群同态:

$\forall A,B\in GL_n(\mathbb{R})$

$$\varphi(A\cdot B)=((AB)^{-1})^t=(B^{-1}A^{-1})^t=(A^{-1})^t(B^{-1})^t$$
$$=\varphi(A)\cdot\varphi(B).$$

Step 2. 单射:

$$(A^{-1})^t=E_n \Longrightarrow A^{-1}=E_n \Longrightarrow A=E_n \Longrightarrow \text{单}.$$

$(\varphi$ 单射 $\Longleftrightarrow ker\varphi=\{E_n\})$.

Step 3. 满射

$\forall A\in GL_n(\mathbb{R}) \quad \because |A|\neq 0$

$\therefore A$ 可逆 令 $B=(A^t)^{-1}$

则 $\varphi(B)=(((A^t)^{-1})^{-1})^t=A$.

五、子群.

i) $H\subset G$ 且 H 为群, $\forall h_1,h_2\in H$, $h_1h_2^{-1}\in H \Rightarrow H$ 为 G 的子群.

ii) 设G是有限群，$H \leq G$ 则 $card(H) \mid card(G)$.

Cor1：设G是有限群，$\forall a \in G$，$ord(a) \mid card(G)$.

Cor2. 设G是有限群. $\forall a \in G$，$a^{card(G)} = e$.

注：一般Lagrange定理的逆命题不成立. 即对$|G|$的一个因子d，不一定有一个子群H s.t $|H| = d$. 但G循环且有限成立。

hw5.

i) $\forall g_1, g_2 \in ker(\varphi)$ 要证 $g_1 g_2^{-1} \in ker(\varphi)$

$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H \cdot e_H = e_H$

$\Longrightarrow g_1 g_2^{-1} \in ker(\varphi)$ ∴ $ker(\varphi)$为G的子群

ii) $g\, ker(\varphi) = ker(\varphi) \cdot g$

a. $\forall g \cdot g' \in g\, ker(\varphi)$ $g' \in ker(\varphi)$

$\varphi(g g' g^{-1}) = \varphi(g)\varphi(g')\varphi(g)^{-1} = e_H \cdot e_H \cdot e_H = e_H$

∴ $g g' g^{-1} \in ker(\varphi)$ $\underset{\displaystyle gg'}{\underset{\|}{g g' g^{-1} g}} \in ker(\varphi) \cdot g$

b. $g' g \in ker(\varphi)\, g$ 考虑 $g^{-1} g' g \in ker(\varphi)$.

$\underset{\displaystyle g'g}{\underset{\|}{g g^{-1} g' g}} \in g\, ker(\varphi)$

iii) "$\Longrightarrow$" φ为单射，$\varphi(e_G) = e_H$

故 $ker(\varphi) = \{e_G\}$.

"$\Longleftarrow$" 若 $ker(\varphi) = \{e_G\}$ 设 $\varphi(g_1) = \varphi(g_2)$.

则 $\varphi(g_1 g_2^{-1}) = \varphi(g_1) \cdot \varphi(g_2)^{-1} = e_H$

$\Longrightarrow g_1 g_2^{-1} \in ker(\varphi) \Longrightarrow g_1 g_2^{-1} = e_G \Rightarrow g_1 = g_2$

$\Longrightarrow \varphi$为单射。

hw6. 方法一：(反证法)

假设G中无二阶元 即 $\forall g \in G$, $g \neq e$, $g^2 \neq e$

$\Longrightarrow g \neq g^{-1}$.

设 $G=\{e, g_1, g_2, \cdots, g_{2n-1}\}=\{e\} \cup \{g_1, g_1^{-1}\} \cup \{g_2, g_2^{-1}\}$

$\cup \cdots \cup \{g_{2n-1}, g_{2n-1}^{-1}\}$

其中对 $i \neq j$，有 $\{g_i, g_i^{-1}\} \cap \{g_j, g_j^{-1}\} = \phi$

或 $\{g_i, g_i^{-1}\} = \{g_j, g_j^{-1}\}$ 此时 $g_i = g_j^{-1}$

最终：$G=\{e\} \cup \{g_{i_1}, g_{i_1}^{-1}\} \cup \cdots \cup \{g_{i_s}, g_{i_s}^{-1}\}$

$\Longrightarrow |G| = 2s+1$. 矛盾.

方法二：$\forall g \in G$. $ord(g) = ord(g^{-1})$.

G中一阶元只有1个：e

G中m阶元 $(m \geqslant 3)$ 是成对出现的

有偶数个（$\because$ 当 $ord(g) \geqslant 3$ 时，$g \neq g^{-1}$

$ord(g) = ord(g^{-1})$）.

$\because |G|$ 是偶数

$\therefore$ G中2阶元有奇数个（至少有一个）.

eg6. 给出 $(\mathbb{Z}_{12}, +, \bar{0})$ 的所有子群. 求 $\bar{5}$, $\bar{8}$ 的阶.

解：设 $H \leq \mathbb{Z}_{12} = \langle \bar{1} \rangle$ 则 $|H| \mid 12$，$|H|$ 可能是 1, 2, 3, 4, 6, 12

若 $|H|=1$ 则 $H=\{e\}$　　$|H|=4$ 则 $H=\langle \bar{3} \rangle$

$|H|=2$ 则 $H=\langle \bar{6} \rangle$　　$|H|=6$ 则 $H=\langle \bar{2} \rangle$

$|H|=3$ 则 $H=\langle \bar{4} \rangle$　　$|H|=12$ 则 $H=\langle \bar{1} \rangle$

设 $ord(\bar{5}) = d_1$，则 $d_1 \cdot \bar{5} = \overline{d_1 \cdot 5} = \bar{0} \Longrightarrow 12 \mid d_1 \cdot 5$

$\Longrightarrow 12 \mid d_1$ 且 $d_1 \mid 12$

$ord(\bar{5}) = 12$.

设 $ord(\bar{8})=d_2$. 则 $d_2\cdot\bar{8}=\overline{d_2\cdot 8}=\bar{0}$ $\Longrightarrow 12\mid d_2\cdot 8$

$\Longrightarrow 3\mid d_2\cdot 2$

$\Longrightarrow d_2=3$.

eg7. 设 $\varphi:(G,\cdot,e)\longrightarrow(G',*,e')$ 为群同态.

若 $a^n=e$ $(n\in\mathbb{Z})$ 则 $ord(\varphi(a))\mid n$.

若 φ 是同构, 则 $ord(\varphi(a))=ord(a)$.

证: 若 $n\in\mathbb{Z}$ $\underbrace{a\cdot a\cdot\cdots\cdot a}_{n}=e$ $\Longrightarrow \varphi(a^n)=\varphi(e)=e'$

$\because$ φ 是同态 $\varphi(a^n)=\varphi(a)^n=\underbrace{\varphi(a)*\varphi(a)*\cdots*\varphi(a)}_{n个}$

$\Longrightarrow ord(\varphi(a))\mid n$

若 $n\in\mathbb{Z}^-$, 则 $a^{-1}\cdots a^{-1}=e$ $\varphi((a^{-1})^{-n})=(\varphi(a^{-1}))^{-n}$

$=(\varphi(a))^{-1\cdot(-n)}=(\varphi(a))^n=e'$.

若 φ 同构, 则 φ^{-1} 也同构. 则

$$\underset{\underset{ord(a)}{\shortparallel}}{ord(\varphi^{-1}(\varphi(a)))}\mid ord(\varphi(a))\mid ord(a)$$

$\Longrightarrow ord(\varphi(a))=ord(a)=n$.

eg8.

$$\begin{tikzcd}[column sep=small]
 & GL_n(\mathbb{R}) \arrow[dl, dash] \arrow[dr, dash] & \\
GL_n(\mathbb{Q}) \arrow[dr, dash] & & SL_n(\mathbb{R}) \arrow[dl, dash] \\
 & SL_n(\mathbb{Q}) \arrow[d, dash] & \\
 & SL_n(\mathbb{Z}) \arrow[d, dash] & \\
 & \{E_n\} &
\end{tikzcd}$$

偏序集

证: $SL_n(\mathbb{R})\leq GL_n(\mathbb{R})$.

$GL_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \det A\neq 0\}$

$SL_n(\mathbb{R})=\{A\in GL_n(\mathbb{R})\mid \det A=1\}$

$\forall$ $A, B\in SL_n(\mathbb{R})$.

$|AB^{-1}|=|A||B^{-1}|=1$

$AB^{-1}\in SL_n(\mathbb{R})$.

其它的可仿行证。

$SL_n(\mathbb{Z})$是群：1) 封闭

2) 结合律成立.

3) E_n为单位元

4) $\forall A \in SL_n(\mathbb{Z})$ $\because |A|=1$ $\therefore A$关于乘法可逆.

且 $A^{-1}=\frac{A^{\vee}}{|A|}=A^{\vee} \in M_n(\mathbb{Z})$

又$\because |A^{-1}|=|A|^{-1}=1 \implies A^{-1} \in SL_n(\mathbb{Z})$

综上$SL_n(\mathbb{Z})$构成群.