第十四次作业.

1. $R=\left\{\begin{pmatrix} a & b \\ -b & a\end{pmatrix} \middle| a,b\in\mathbb{R}\right\}\subset M_2(\mathbb{R})$. 证明: $(R,+,0,\cdot,E)$ 是 $(M_2(\mathbb{R}),+,0,\cdot,E)$ 的交换子环.

证: (细节自行验证)

(1) $(R,+,0)$ 是交换子群: $\forall A,B\in R$, $A-B\in R$ ∴ R 是子群. 交换显然成立.

(2) $(R,\cdot,E)$ 是含幺交换~~群~~半群:

(i) 乘法封闭: $\forall A,B\in R$, $AB\in R$

(ii) 结合律显然成立, $E\in R$

(iii) 交换: $\forall A,B\in R$, $AB=BA$.

(3) 分配律成立.

∴ R 是 $M_2(\mathbb{R})$ 的交换子环.

事实上, R 是域.

$\forall A=\begin{pmatrix} a & b \\ -b & a\end{pmatrix}\in R$. $|A|=a^2+b^2$. ∴ $|A|=0 \overset{a,b\in\mathbb{R}}{\Longleftrightarrow} a=b=0 \Leftrightarrow A=0$

i.e. $|A|\neq 0 \Leftrightarrow A\neq 0$.

意味着 R 中非零矩阵都可逆. 且若 $A\neq 0$, 则 $A^{-1}=\frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a\end{pmatrix}\in R$

∴ R 是域.

注: 证明 S 是 R 的子环. 只需证.

① S 关于 $+$ 封闭	或者	① S 关于 $-$ 封闭
② S 关于 $\cdot$ 封闭		② S 关于 $\cdot$ 封闭
③ $\pm 1_R\in S$		③ $1_R\in S$

2. $(G,\cdot,e)$群，$a,b\in G$. 证明：(1) $\mathrm{ord}(a)=\mathrm{ord}(b^{-1}ab)$；(2) $\mathrm{ord}(ab)=\mathrm{ord}(ba)$

证：(1). 若 $\mathrm{ord}(a)=\infty$，则 $\mathrm{ord}(b^{-1}ab)=\infty$.

如果 $\mathrm{ord}(b^{-1}ab)=k<\infty$，则

$$e=(b^{-1}ab)^k=\underbrace{(b^{-1}ab)\cdot(b^{-1}ab)\cdot\cdots\cdot(b^{-1}ab)}_{k个}=b^{-1}a^kb \Rightarrow a^k=bb^{-1}=e \text{ 矛盾.}$$

若 $\mathrm{ord}(a)=n<\infty$，则 $a^n=e$ 且

$$(b^{-1}ab)^n=b^{-1}a^nb=b^{-1}eb=e \Rightarrow \mathrm{ord}(b^{-1}ab)\mid n.$$

设 $\mathrm{ord}(b^{-1}ab)=m<\infty$. 则

$$(b^{-1}ab)^m=b^{-1}a^mb=e \Rightarrow a^m=beb^{-1}=e \Rightarrow n\mid m\ (=\mathrm{ord}(b^{-1}ab))$$

$\therefore\ \mathrm{ord}(a)=\mathrm{ord}(b^{-1}ab)$.

(2). 方法一：可以类似(1)的证法证明

若 $\mathrm{ord}(ab)=k<\infty$，下证 $\mathrm{ord}(ba)=k$.

$$\because (ab)^k=e \quad \therefore \underset{\substack{\parallel \\ (ba)^{k+1}}}{b(ab)^ka}=bea=ba \xRightarrow{消去律} (ba)^k=e$$

$\Rightarrow \mathrm{ord}(ba)\mid k$ 类似可证 $k\mid \mathrm{ord}(ba)$ $\therefore\ \mathrm{ord}(ab)=\mathrm{ord}(ba)$.

若 $\mathrm{ord}(ab)=\infty$，则 $\mathrm{ord}(ba)=\infty$.

如果 $\mathrm{ord}(ba)=k<\infty$，和上述类似的做法可得 $(ab)^k=e$. 矛盾.

方法二：直接用(1)的结论.

$$\mathrm{ord}(ba)=\mathrm{ord}(b^{-1}(ba)b)=\mathrm{ord}(ab)$$

P128. 3. G群，$a,b\in G$ 且 $ab=ba$，$ord(a)=s$，$ord(b)=t$ 且 $gcd(s,t)=1$，则在G中生成一个 st阶的循环子群：$\langle a,b\rangle=\langle ab\rangle$.

证：(1) 先证 $\langle a,b\rangle=\langle ab\rangle$.

$\because ab\in\langle a,b\rangle$ $\therefore \langle ab\rangle\subset\langle a,b\rangle$. 下证 $\langle a,b\rangle\subset\langle ab\rangle$.

$\because gcd(s,t)=1$，$\therefore \exists\ u,v\in\mathbb{Z}$ s.t. $us+vt=1$.

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

同理 $b\in\langle ab\rangle$. $\therefore \langle a,b\rangle\subset\langle ab\rangle$. 因此 $\langle a,b\rangle=\langle ab\rangle$.

(2) 再证 $ord(ab)=st$. 即 $|\langle ab\rangle|=st$

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

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

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

$\therefore ord(ab)=st$

综上，$\langle a,b\rangle=\langle ab\rangle$是$G$的$st$阶循环子群.

7. $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}\in SL_2(\mathbb{Z})$, $ord(A)=4$, $ord(B)=3$.

证：$\langle AB\rangle$是$SL_2(\mathbb{Z})$中无限循环子群.

这说明G中两个有限阶元素的乘积不一定是有限阶元. 这件事在阿贝尔群中成立吗?

证：$$AB=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}0&0\\-1&-1\end{pmatrix}=\begin{pmatrix}-1&-1\\0&-1\end{pmatrix}=-\begin{pmatrix}1&1\\0&1\end{pmatrix}$$

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

$$=(-1)^n\begin{pmatrix}1&n\\0&1\end{pmatrix}\neq E_2.\quad(\forall n\in\mathbb{Z}^+)$$

$\therefore AB$是无限阶元

若G是Abel群(交换群)，则两个有限阶元相乘一定是有限阶元.

$a,b\in G$，$ord(a)=s$，$ord(b)=t$，$s,t\in\mathbb{Z}^+$

则 $(ab)^{st}=a^{st}b^{st}=(a^s)^t\cdot(b^t)^s=e \Rightarrow ord(ab)\mid st \Rightarrow ord(ab)<\infty$.

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

证：方法一：(反证法). 假设G中无二阶元 i.e. $\forall g\in G, g\neq e, g^2\neq e \Rightarrow g\neq g^{-1}$.

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$\forall i,j$，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 $g_i=g_j^{-1}$)

去掉重复的集合得到G的一个分拆

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

$\Rightarrow |G|=2s+1$. 奇数. 矛盾.

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

G中一阶元只有1个：e

当$ord(g)\geq 3$时，$g\neq g^{-1}$.

G中m阶元($m\geq 3$)是成对出现的. 有偶数个 ($\because ord(g)=ord(g^{-1})$)

$\because |G|$是偶数 $\therefore G$中2阶元有奇数个 $\Rightarrow G$中至少有一个2阶元.

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

解：是

方法一：(1) $m=0$，显然 $(BA)^m=E$

(2) $m>0$. $(AB)^m=E \Rightarrow 1=|(AB)^m|=|A|^m|B|^m \Rightarrow |A|\neq 0, |B|\neq 0$
$\Rightarrow A,B$可逆.

又 $(AB)^m=E \Rightarrow \underset{(BA)^mBB^{-1}}{\underset{\shortparallel}{B(AB)^mB^{-1}}}=BB^{-1} \Rightarrow (BA)^m=E$

(3) $m<0$. $(AB)^m=E$意味着AB可逆 $\Rightarrow |AB|=|A||B|\neq 0 \Rightarrow |A|\neq 0, |B|\neq 0$
$\Rightarrow A,B$可逆.

~~又 $(AB)^m=E \Rightarrow B(AB)^m=B \Rightarrow (BA)^m=E$~~
~~$(BA)^mB$~~

$m<0$, $E=(AB)^m=\left((AB)^{-1}\right)^{-m}=(B^{-1}A^{-1})^{-m}=\underbrace{(B^{-1}A^{-1})\cdots(B^{-1}A^{-1})}_{-m}$

$\Rightarrow E=B(AB)^mB^{-1}=B\underbrace{(B^{-1}A^{-1})\cdots(B^{-1}A^{-1})}_{-m}B^{-1}=\underbrace{(A^{-1}B^{-1})\cdots(A^{-1}B^{-1})}_{-m}$

$$=(A^{-1}B^{-1})^{-m}=\left((BA)^{-1}\right)^{-m}=(BA)^m$$

i.e. $(BA)^m=E$

方法二：$m=0$ 显然成立．下设 $m\neq 0$．由方法一可知 A,B 可逆，$\therefore A,B\in GL_n(\mathbb{R})$．

$(GL_n(\mathbb{R}),\cdot,E_n)$ 是群，由本次作业第2题(2)的结论可知

$\mathrm{ord}(AB)=\mathrm{ord}(BA)$．

如果 $\exists\, m\in\mathbb{Z}^*$ s.t. $(AB)^m=E$ 则 $\mathrm{ord}(AB)<\infty$ 且 $\mathrm{ord}(AB)\mid m$．

$\Rightarrow \mathrm{ord}(BA)\mid m \Rightarrow (BA)^m=E$．

环

1. 定义：$(R,+,0,\cdot,1)$，$0,1\in R$ 且 $0\neq 1$，$+,\cdot$ 是 R 上的二元运算

(1) $(R,+,0)$ 是交换群

(2) $(R,\cdot,1)$ 是含幺半群

(3) $\forall x,y,z\in R$，$x(y+z)=xy+xz$，$(x+y)z=xz+yz$（左右分配律）

交换环：$\forall a,b\in R$，$ab=ba$，乘法可交换

eg：交换环：$(\mathbb{Z},+,0,\cdot,1)$，$(\mathbb{Z}_n,+,\bar{0},\cdot,\bar{1})$

非交换环：$(M_n(\mathbb{R}),+,O_n,\cdot,E_n)$

prop：$(R,+,0,\cdot,1)$ 环.

(1) $\forall x\in R$，$0x=x0=0$

(2) $\forall x\in R$，$(-1)x=x(-1)=-x$

(3) $\forall x,y\in R$，$(-x)y=x(-y)=-(xy)$，$(-x)(-y)=xy$

(4) $\forall m,n\in\mathbb{Z}$，$x,y\in R$，$(mx)(ny)=(mn)(xy)$（广义分配律的推论）

2. 子环和环同态

子环：$(R,+,0_R,\cdot,1_R)$ 环，$S\subset R$ s.t. $(S,+,0_R,\cdot,1_R)$ 也是环，称 S 是 R 的子环.

eg：整数环是有理数环的子环.

环同态：$\varphi:(R,+,0_R,\cdot,1_R)\longrightarrow(S,+,0_S,\cdot,1_S)$ 满足 $\forall x,y\in R$

$$\varphi(x+y)=\varphi(x)+\varphi(y),\quad \varphi(xy)=\varphi(x)\varphi(y),\quad \varphi(1_R)=1_S$$

若 φ 是单射，称 φ 是环嵌入；若 φ 是双射，称为环同构.

注：加法有消去律，$\therefore \varphi(0_R)=0_S$ 但乘法一般无消去律，需定义 $\varphi(1_R)=1_S$.

prop：$\varphi:R\to S$ 环同态，则 $\mathrm{im}(\varphi)$ 是子环.

3. 零因子和可逆元

零因子：R 环，$a,b\in R\setminus\{0\}$，若 $ab=0$，则称 a 是 R 的左零因子

b 是 R 的右零因子。

注：左、右零因子成对出现。

eg：(1) 无零因子的环：$\mathbb{Z}$，$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$。

(2) 有零因子的环：

(i) $\mathbb{Z}_n$。$\bar{a}\in\mathbb{Z}_n\setminus\{\bar{0}\}$，$\bar{a}$ 是可逆元 $\Leftrightarrow \gcd(a,n)=1$

$\bar{a}$ 是零因子 $\Leftrightarrow \gcd(a,n)>1$

(ii) $M_n(\mathbb{R})$。$A\in M_n(\mathbb{R})\setminus\{0\}$。$A$ 是可逆元 $\Leftrightarrow \mathrm{rank}(A)=n$。

A 是左或右零因子 $\Leftrightarrow \mathrm{rank}(A)<n$。

可逆元：R 环，含幺半群 $(R,\cdot,1)$ 中可逆元称为 R 中可逆元。

prop：$U_R=\{a\in R\mid \underbrace{a\text{ 可逆}}_{\text{(乘法可逆)}}\}$，$R$ 环，则 $(U_R,\cdot,1)$ 是群。

Fermat 小定理：p 素数，$m\in\mathbb{Z}$，$p\nmid m$，则 $m^{p-1}\equiv 1 \bmod p$。

另一种说法：$\mathbb{Z}_p$，p 素数，$\forall\, \bar{m}\in\mathbb{Z}_p\setminus\{\bar{0}\}$，$\bar{m}^{p-1}=\bar{1}$。(~~事实上，若 $\bar{m}\neq\bar{1}$，$\mathrm{ord}(\bar{m})=p-1$~~ ~~关于乘法的阶~~)

4. 消去律

prop：R 环，$a,b\in R\setminus\{0\}$，$x,y\in R$。

(1)（左消去律）若 a 不是左零因子且 $ax=ay$，则 $x=y$。

(2)（右消去律）若 b 不是右零因子且 $xb=yb$，则 $x=y$。

整环 = 交换环 + 无零因子。

prop：整环中有消去律。

5. 环的特征

定义：$(R,+,0,\cdot,1)$ 环，如果 $(R,+,0)$ 中 1 的阶有限，则 $ord(1)$ 称为 R 的特征，否则定义成零，记为 $char(R)$.

i.e. 若 $\underset{\text{加法阶}}{ord(1)}=\infty$，则 $char(R)=0$.

若 $ord(1)=m<\infty$，则 $char(R)=m$.

eg：$char(\mathbb{Z})=0$，$char(\mathbb{Z}_n)=n$.

prop：(1) $char(R)=n>0$，$m\in\mathbb{Z}$ s.t. $n\mid m$. 则 $\forall r\in R$，$mr=0$.

设R交换

(2) (Freshmen's dream) $char(R)=p$. p素数. 则 $\forall x,y\in R$.

$$(x+y)^p=x^p+y^p$$

eg：p素数. $\forall x,y\in\mathbb{Z}_p$，$(x+y)^p=x^p+y^p$. $(\because char(\mathbb{Z}_p)=p)$

prop：$\varphi:(R,+,0_R,\cdot,1_R)\longrightarrow(S,+,0_S,\cdot,1_S)$ 环同态. 则

(1) $char(R)=0$ or $char(R)\geq char(S)>0$

(2) φ单同态，则 $char(R)=char(S)$.

注：

$char(R)=0$：例：$\varphi:\mathbb{Z}\longrightarrow\mathbb{Z}_n$，$m\longmapsto\bar{m}$. $char(S)$ 可以为 0，可以 >0.

$\varphi:\mathbb{Z}\hookrightarrow\mathbb{Q}$.

$m\longmapsto\frac{m}{1}$

$char(R)>0$：(1) $\varphi:(R,+,0_R)\longrightarrow(S,+,0_S)$ 群同态.

$1_R\longmapsto 1_S$.

由上次习题课结论 ($\varphi:G\to H$ 群同态，若 $a^n=e\ (n\in\mathbb{Z})$，则 $ord(\varphi(a))\mid n$. 若φ是同构，$ord(\varphi(a))=ord(a)$)

$\underset{\text{加法群的阶}}{ord(1_S)\mid ord(1_R)}\Rightarrow char(S)\mid char(R)$

8

(2) 如果φ单同态，则 $R\cong im(\varphi)$. $\Rightarrow ord(1_R)=ord(1_S)$，$1_S\in im(\varphi)\Rightarrow char(R)=char(S)$.

prop：整环的特征是零或素数．

域．

1．定义：F交换环，如果F中任何非零元都可逆，则F是域．

理解：F是域，则

① $(F, +, 0_F)$ 交换群

② $(F\setminus\{0\}, \cdot, 1_F)$ 交换群（R环，R中所有可逆元构成群）．

且 $0_F\cdot a = a\cdot 0_F = 0_F$．$\forall a\in F$．

③ 加法乘法之间分配律．

类似可定义子域的概念．

prop：域是整环，因此域的特征是0或素数．

pf：F域．$\forall a,b\in F\setminus\{0\}$．若 $ab=0$，则 $a^{-1}(ab)=0 \Rightarrow b=0$ 矛盾．

eg：特征为0的域：$\mathbb{Q}, \mathbb{R}, \mathbb{C}$．

特征为p的域：$\mathbb{Z}_p$．p素数．

prop：F, K域，$\varphi: F\to K$ 环同态，则φ是嵌入（$\Rightarrow char(F)=char(K)$）

注：特征不同的域之间没有环同态．

2．分式域．

D整环，$D^* = D\setminus\{0\}$．在集合 $D\times D^*$ 上定义二元关系（是等价关系）

设 $(a,b), (c,d)\in D\times D^*$．若 $ad=bc$，则 $(a,b)\sim(c,d)$

记 $Fr(D) = (D\times D^*)/\sim$．　　(a,b)关于$\sim$等价类记为$\frac{a}{b}$

$= \{\frac{a}{b} \mid a\in D, b\in D^*\}$．

在 $Fr(D)$ 上定义 $+$ 和 $\cdot$：

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

验证得 $\left(Fr(D),+,\frac{0}{1},\cdot,\frac{1}{1}\right)$ 是域. $\left(\frac{a}{b}=\frac{0}{1}\Leftrightarrow a=0\right)$

prop: D 整环. $\varphi: D\longrightarrow Fr(D)$ 是环的单同态.

$$x\longmapsto \frac{x}{1}$$

$\therefore D\cong \mathrm{im}(\varphi)=\left\{\frac{x}{1}\,\middle|\,x\in D\right\}$. D 可以看成 $Fr(D)$ 的子集.

eg: $\varphi: \mathbb{Z}\longrightarrow \mathbb{Q}$.

$$m\longmapsto \frac{m}{1}.$$

3. 域上的线性代数.

第一~三章关于线性代数的结论（除了用到 $2\neq 0$ 的）对任何域 F 和坐标空间 F^n 都成立.

eg1: $\mathbb{Z}_3=\{\bar0,\bar1,\bar2\}$. 求解 $\underbrace{\begin{pmatrix}\bar1&\bar2&\bar1\\ \bar2&\bar1&\bar2\\ \bar1&\bar0&\bar1\end{pmatrix}}_{=A}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=\begin{pmatrix}\bar0\\ \bar0\\ \bar0\end{pmatrix}$

$$A\to\begin{pmatrix}\bar1&\bar2&\bar1\\ \bar0&\bar0&\bar0\\ \bar0&\bar1&\bar0\end{pmatrix}\to\begin{pmatrix}\bar1&\bar2&\bar1\\ \bar0&\bar1&\bar0\\ \bar0&\bar0&\bar0\end{pmatrix}\to\begin{pmatrix}\bar1&\bar0&\bar1\\ \bar0&\bar1&\bar0\\ \bar0&\bar0&\bar0\end{pmatrix}\quad \mathrm{rank}(A)=2 \Rightarrow \dim(V_A)=1.$$

$$\begin{cases}x_1+x_3=\bar0\\ x_2=\bar0\end{cases}\quad \therefore V_A \text{ 一组基为 } \begin{pmatrix}\bar1\\ \bar0\\ -\bar1\end{pmatrix}=\begin{pmatrix}\bar1\\ \bar0\\ \bar2\end{pmatrix}$$

故 $V_A=\left\{\lambda\begin{pmatrix}\bar1\\ \bar0\\ \bar2\end{pmatrix}\,\middle|\,\lambda\in\mathbb{Z}_3\right\}=\left\{\begin{pmatrix}\bar0\\ \bar0\\ \bar0\end{pmatrix},\begin{pmatrix}\bar1\\ \bar0\\ \bar2\end{pmatrix},\begin{pmatrix}\bar2\\ \bar0\\ \bar1\end{pmatrix}\right\}$

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

$$\begin{pmatrix}\bar{1}&\bar{2}\\\bar{0}&\bar{1}\end{pmatrix}^n=\left(\begin{pmatrix}\bar{1}&\bar{0}\\\bar{0}&\bar{1}\end{pmatrix}+\begin{pmatrix}\bar{0}&\bar{2}\\\bar{0}&\bar{0}\end{pmatrix}\right)^n=\sum_{i=0}^{n}\binom{n}{i}\begin{pmatrix}\bar{0}&\bar{2}\\\bar{0}&\bar{0}\end{pmatrix}^i$$

$$=\binom{n}{0}\cdot\begin{pmatrix}\bar{0}&\bar{2}\\\bar{0}&\bar{0}\end{pmatrix}^0+\binom{n}{1}\begin{pmatrix}\bar{0}&\bar{2}\\\bar{0}&\bar{0}\end{pmatrix}\qquad\left(\begin{pmatrix}\bar{0}&\bar{2}\\\bar{0}&\bar{0}\end{pmatrix}^m=\begin{pmatrix}\bar{0}&\bar{0}\\\bar{0}&\bar{0}\end{pmatrix},\ m\geq 2\right)$$

$$=\begin{pmatrix}\bar{1}&\bar{0}\\\bar{0}&\bar{1}\end{pmatrix}+n\begin{pmatrix}\bar{0}&-\bar{1}\\\bar{0}&\bar{0}\end{pmatrix}$$

$$=\begin{pmatrix}\bar{1}&-\bar{n}\\\bar{0}&\bar{1}\end{pmatrix}$$