第十三次习题课

一. 群的生成元

$$\langle S\rangle = \{x_1^{e_1}\cdots x_m^{e_m} \mid m\in\mathbb{Z}^+, x_1,\cdots,x_m\in S, e_1,\cdots e_m\in\mathbb{Z}\}$$

hw1. G是一个群, $a,b\in G$, $ab=ba$. $ord(a)=s$, $ord(b)=t$, $gcd(s,t)=1$.

证明: 元素ab的阶为st且$\langle a,b\rangle=\langle ab\rangle$

1) 证: $ord(ab)=st$. (即要说明ab的阶刚好为st).

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

$\therefore ord(ab)\mid st$.

令 $ord(ab)=m$, $(ab)^m=e$

则 $(ab)^{ms}=(a^s)^m b^{ms}=b^{ms}=e \Rightarrow t\mid ms$

同理可得 $s\mid mt$

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

2) $\langle a,b\rangle=\langle ab\rangle$

i) $\because ab\in\langle a,b\rangle$ $\therefore \langle ab\rangle\subset\langle a,b\rangle$

ii) 下证$\langle a,b\rangle\subset\langle ab\rangle$

$\forall g\in\langle a,b\rangle$ $g=a^ib^j$ 由 $\left.\begin{matrix}card\langle a,b\rangle\le st\\ \ge st\end{matrix}\right\}\Rightarrow$

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

则 $a=a^{su+tv}=(a^s)^u(a^t)^v=a^{tv}=a^{tv}(b^t)^v=a^{tv}b^{tv}$

$=(ab)^{tv}\in\langle ab\rangle$

同理 $b\in\langle ab\rangle$

$\therefore \langle a,b\rangle\subset\langle a,b\rangle$. 综上 $\langle a,b\rangle=\langle ab\rangle$

hw4. i) $\forall p \in \mathbb{Z} \mid p$ 为素数 为构成 $(\mathbb{Q}_+, \cdot)$ 的一个生成元集.
由算术基本定理可得 $\forall q \in \mathbb{Q}_+$, q 均能写成若干素数之积。
ii) 假设存在有限生成元素 设为 $q_1, \cdots q_m$.
则 $\exists$ 有限素数 $\forall p_1, \cdots, p_n$ 为 s.t $q_1, \cdots, q_m \in \langle p_1, \cdots, p_n \rangle$
则 $\langle q_1, \cdots, q_m \rangle \subseteq \langle p_1, \cdots p_n \rangle$
$\Rightarrow (\mathbb{Q}_+, \cdot) \subseteq \langle p_1, \cdots, p_n \rangle$ 矛盾.
因为 $\exists$ 素数 不在 $p_1 \cdots p_m$ 中.

二、循环群:

群论基本问题 { 给出一类群, 找出所有不同构的群.
研究子群的结构

循环群 { $\simeq (\mathbb{Z}, +, 0)$
$\simeq (\mathbb{Z}_n, +, \bar{0})$.

子群结构:

Lemma 1: $H \leq G = \langle a \rangle$, 则 $\exists k \in \mathbb{Z}$ s.t. $H = \langle a^k \rangle$.

证明: 设 $H = \{e\}$ 则 $H = \langle a^0 \rangle$.

对 $\forall x \in H$ 且 $x \neq e$ 且 $\exists m \in \mathbb{Z} \setminus \{0\}$ s.t $x = a^m$

不妨设 $a^k \in H$ 且 k 为最小正整数 显然 $\langle a^k \rangle \subseteq H$

另一方面. $\forall a^m \in H$ 为带余除法 $m = q \cdot k + r$ $(0 \leq r < k)$

$\because a^m, a^k \in H$ 则 $a^r = a^m \cdot (a^k)^{-q} \in H$

由 k 极小性 $\Rightarrow r = 0$

$\therefore a^m = (a^k)^q \in \langle a^k \rangle$ $\therefore \langle a^k \rangle = H$

Lemma 2.

$$ord(g^k) = \frac{m}{gcd(m,k)}$$

$ord(a) = n$.
$gcd(n,k) = 1$

$\Longrightarrow ord(a^k)=n$. $ord(a^{-1})=n$.

Cor: 群G，若 $a\in G$ 且 $ord(a)=n$，$\gcd(n,k)=1$

$\Longrightarrow ord(a^k)=n$.

循环群的子群是循环群.

无限循环群的非平凡子群与本身同构.

(Cayley定理). a.单同态 b.嵌入映射. c.G可嵌入T_G中.

半群

hw2. G是一个幺半群，s.t $\forall a,b\in G$，方程 $ax=b$，$ya=b$ 有唯一解，证明：G为一个群。

证：分析：G已是幺半群 + G中每个元都可逆 $\Rightarrow$ G为群

注意：左逆与右逆刚开始写的时候要区分.

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

则 $(y_0\cdot g)\cdot x_0 = e\cdot x_0 = x_0$

$\quad\ \ \| $

$y_0\cdot(g x_0) = y_0\cdot e = y_0$

故 $x_0=y_0$

$\therefore \exists\, x_0\in G$ s.t. $gx_0=x_0g=e$

则 x_0 为g的逆元，由g的任意性可知G为群.

证：i) 左单位元的存在

对于一个固定的元b，$yb=b$ 在G中有解 称为e.

(1) $eb=b$

我们说对于G中的一个任意元 a

(2) $ea=a$ 成立.

由已知 $bx=a$ 有解 c

$bc=a$

由(1)(2) $ea=e(bc)=(eb)c=bc=a$

我们证明了 e 存在.

ii) 单位元+可逆

$\forall a\in G$, $y\cdot a=e$ 有解 记为 a'

(3) $a'\cdot a=e$ 故 a' 为 a 的左逆元.

又 $\forall a\in G$, $\exists a'\in G$ s.t $a'\cdot a=e$

由(3) $\Rightarrow \exists a''$ s.t $a''\cdot a'=e$.

故 $a\cdot a'=e\cdot(a\cdot a')=(a''a')(a\cdot a')=a''(a'\cdot a)a'$

$=a''ea'=e$

且 $a\cdot e=e\cdot a=a$

综上 e 为单位元, 且任意元素 a 有逆 a'.

eg1. 设 G 是群, $1\in G$ 为单位元. 证明 $\forall x\in G$, $x^2=1$, 则 G 交换。

证: $\forall x,y\in G$ $(xy)^2=(xy)(xy)=x(yx)y=1$

$=1\cdot 1=x^2\cdot y^2=x(xy)y$

$\Rightarrow x^{-1}(x(yx)y)y^{-1}=x^{-1}(x(xy)y)y^{-1}$

$\Rightarrow yx=xy$

$\Rightarrow$ G 交换. □

hw3. i) 设 G 为4阶群 即 $|G|=4$ 则 $\forall a\in G$

$ord(a)\mid 4$, 则 $ord(a)$ 可能取 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中无四阶元，则 $\forall a \in G$，$a^2 = e$ 由eg1知 G交换.
综上所有四阶群均交换。

若 $\exists a$ s.t $G = \langle a \rangle$
∵ 任意的四阶循环群均同构于 $(\mathbb{Z}_4, +, \bar{0})$.
∴ $G \simeq \mathbb{Z}_4 \simeq \cup = \langle (1234) \rangle$

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

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(若 $ab = a$ 则 $a \cdot a \cdot b = a \cdot a = e$
$\Rightarrow b = e$ →←)

$\varphi : G \longrightarrow V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$
$e \longmapsto (0, 0)$
$a \longmapsto (\bar{1}, 0)$
$b \longmapsto (0, \bar{1})$
$c \longmapsto (\bar{1}, \bar{1})$.

构造的映射：良定义，
同态 + 双射. $\Rightarrow$ φ 同构.

构造 $\varphi' : G \longrightarrow V_4$
$e \longmapsto e$
$a \longmapsto (12)(34)$
$b \longmapsto (13)(24)$
$c \longmapsto (14)(23)$

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

ii) 素数阶群均为循环群.
$|G| = 1, 2, 3, 5$ 其为循环群.
若 $|G| = 4$ 由i)知 G交换.

iii) S_3: $|S_3| = 3! = 6$

$(12)(123) = (23) \neq (123)(12) = (13)$.

hw5. G 有限乘法群, H 是 G 非空子集, H 关于 G 的乘法封闭, 证明: H 是一个子群。

Thm 1. 一个群 G 的一个不空子集 H 作成 G 的一个子群

$\Longleftrightarrow$ (i) $a, b \in H$, $ab \in H$

(ii) $a \in H$, $a^{-1} \in H$.

$\Longleftrightarrow$ (iii) $a, b \in H \Rightarrow ab^{-1} \in H$.

提示: 按照群的定义来证即可. (i)(ii) 成立, (iii) 也就成立.

Thm 2. 一个群 G 的一个不空有限子集 H 作成 G 的一个子群

$\Longleftrightarrow$ (iv) $a, b \in H \Rightarrow ab \in H$.

证: "$\Rightarrow$" 无需证

"$\Leftarrow$" 即证 H 满足群的条件

封闭性由 (iv) 给出.

结合律 因为 $H \subset G$ 满足

单位元、逆元 } 若怎 $\varphi: H \to H$ 双射

$h \to hh_0$ 其中 $h_0 \in H$.

$hh_0, h^2h_0, \cdots h^nh_0 \cdots$ H 有限 必有 $h^{n_1}h_0 = h^{n_2}h_0$

$h^{n_1-n_2} = e \in H$.

反过来看 $\exists\ h$ s.t. $\varphi(h) = hh_0 = e$.

证: $\because$ G 有限 $\therefore$ H 一定有限

故由 Thm 2. 只需证 $\forall\ a, b \in H \Rightarrow ab \in H$.

又由题设 H 关于乘法封闭.

$\therefore$ H 是一个子群。

hw6. $(G,\cdot,e_G)$ $(H,\cdot,e_H)$ 设 $\varphi: G\to H$ 为群同态.

i) 反身性: $\forall g\in G$, $g\cdot g^{-1}=e\in\ker\varphi \Rightarrow g\sim g$.

对称性: $\forall g,g'\in G$ 若 $g\sim g'$ $g\cdot g'^{-1}\in\ker\varphi$

$\Rightarrow g'\cdot g^{-1}=(g\cdot g'^{-1})^{-1}\in G \Rightarrow g'\sim g$.

传递性: 若 $g\sim g'$, $g'\sim g''$

则 $g\cdot g'^{-1}\in\ker\varphi$, $g'\cdot g''^{-1}\in\ker\varphi$

$\Rightarrow g\cdot g''^{-1}=g\cdot g'^{-1}\cdot g'\cdot g''^{-1}\in\ker\varphi$

$\Rightarrow g\sim g''$ (自己验证三条性质).

ii) 群运算良定义

若 $\bar g=\bar g'$, $h=\bar h'$ 要证 $\overline{gh}=\overline{g'h'}$.

$gh(g'h')^{-1}=gh\cdot(h')^{-1}(g')^{-1}\in\ker\varphi$

$h(h')^{-1}\in\ker\varphi$, $g\cdot(g')^{-1}\in\ker\varphi$

$\Rightarrow \varphi(ghh'^{-1}g'^{-1})=e$

封闭

结合律成立.

单位元 $\forall \bar g\in G/\sim$, $\bar e\cdot\bar g=\overline{e\cdot g}=\bar g=\overline{g\cdot e}=\bar g\cdot\bar e$

逆元. $\forall \bar g\in G/\sim$. $\bar g^{-1}\cdot\bar g=\overline{g^{-1}\cdot g}=\bar e=\overline{g\cdot g^{-1}}=\bar g\cdot\bar g^{-1}$

综上 $(G/\sim,\cdot)$ 为一个群.

iii) $\bar\varphi:(G/\sim,\cdot)\longrightarrow H$ $\bar\varphi(\bar g)=\varphi(g)$.

$\bar\varphi$ 良定义: 若 $\bar g=\bar g'$, 则 $g\cdot(g')^{-1}\in\ker\varphi$

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

$\Rightarrow \varphi(g)=\varphi(g')$

则 $\bar\varphi(\bar g)=\varphi(g)=\varphi(g')=\bar\varphi(\bar g')$

$\bar{\varphi}$ 同态：　$\forall \bar{g}, \bar{g'} \in G/\sim$

$$\bar{\varphi}(\bar{g}\cdot\bar{g'}) = \bar{\varphi}(\overline{g\cdot g'}) = \varphi(g\cdot g') = \varphi(g)\cdot\varphi(g') = \bar{\varphi}(\bar{g})\cdot\bar{\varphi}(\bar{g'})$$

iv). $\bar{\varphi}$ 是一个单射，$\mathrm{im}(\varphi) = \mathrm{im}(\bar{\varphi})$ 有 $(G/\sim, \cdot) \cong \mathrm{im}(\varphi)$.

证明：$\mathrm{im}\,\bar{\varphi} = \{\bar{\varphi}(\bar{g}) \mid \bar{g} \in G/\sim\} = \{\varphi(g) \mid g \in G\} = \mathrm{im}\,\varphi$.

若 $\bar{g} \in \ker\bar{\varphi}$，则 $\bar{\varphi}(\bar{g}) = \varphi(g) \in \ker\varphi$

$\Rightarrow g \in \ker\varphi \Rightarrow \bar{g} = \bar{e}$.

$\Rightarrow \ker\bar{\varphi} = \{\bar{e}\} \Rightarrow \bar{\varphi}$ 为单射.

故而我们有　$\bar{\varphi}: G/\sim \longrightarrow \mathrm{im}\,\bar{\varphi}$ 为同态+双射.

$\Rightarrow G/\sim \simeq \mathrm{im}\,\bar{\varphi} = \mathrm{im}\,\varphi$.

三、环

1. $+, \cdot$ R 上两个二元运算　　$(R, +, 0, \cdot, 1)$

0_R　1_R

i) $(R, +, 0)$ 交换群

ii) $(R, \cdot, 1)$ 含幺半群　交换含幺半群　R为交换环.

iii) 分配律成立.

1'. $\forall a, b, c \in R$.

i). 结合律 $(a+b)+c = a+(b+c)$

单位　$0 + a = a + 0 = a$

逆　$\exists\, d$ s.t $a + d = d + a = 0$

交换　$a+b = b+a$.

ii) 结合律　$(a\cdot b)\cdot c = a\cdot(b\cdot c)$

单位　$1\cdot a = a\cdot 1 = a$.

交换　$a\cdot b = b\cdot a$

iii) $\begin{cases} a\cdot(b+c)=a\cdot b+a\cdot c \\ (a+b)\cdot c=a\cdot c+b\cdot c \end{cases}$

注：Cor 3.7 $(ma)(nb)=(mn)(ab)$ （环中乘法）

（ma：加法；mn：整数乘法）

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

$$\begin{cases} \varphi(a+b)=\varphi(a)+\varphi(b) \\ \varphi(a\cdot b)=\varphi(a)\cdot\varphi(b) \\ \varphi(1_R)=1_S \end{cases}$$

注：有加法消去律

但乘法一般无定义…

eg $\varphi:\mathbb{Z}\longrightarrow\mathbb{Z}_n$

$m\longmapsto\bar{m}=\{m+kn\mid k\in\mathbb{Z}\}$

3. 子环 $S\subseteq R$ 满足 $0_R,1_R\in S$ 且 $(S,+,0_R,\cdot,1_R)$ 构成环.

注：一般证子环 $\begin{cases} \text{i)}\ \text{加法封闭} \\ \text{ii)}\ \text{乘法} \\ \text{iii)}\ \pm 1_R\in S \end{cases}$

$\varphi:R\to S$ 环同态 $\quad im(\varphi)$ 为子环.

4. 零因子和可逆元.

定义. 注. 左、右零因子成对出现

eg. 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 中零因子和可逆元.

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

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

Step 2.

$$A\cdot B=\begin{pmatrix} a_1a_2-b_1b_2 & a_1b_2+a_2b_1 \\ -(a_2b_1+a_1b_2) & a_1a_2-b_1b_2 \end{pmatrix}\in R.$$

Step 3. $1E_2\in R$.

Step 4. $AB=BA$.

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

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

则 $|A|=0 \Longleftrightarrow A=0$

$\therefore$ 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实则为域.

eg 设环R 若 $\forall a\in R\ \exists!\ b\in R$ s.t. $aba=a$

$\Longrightarrow$ R无零因子.

注：非交换环无零因子。

证：(反证法) 假设R有左零因子设为a，则$\exists c\in R$的

s.t. $ac=0 \Rightarrow a\cdot c\cdot a=0\cdot a=0$

又$\because \exists b\in R$ s.t. $aba=a$.

$\Rightarrow aca+aba=a \Rightarrow a(c+b)a=a$

$\because c\neq 0 \quad \therefore c+b\neq b$. 矛盾. □.

5. 整环：交换环 + 无零因子(有消去律).

eg. $\mathbb{Z}_{24}$的零因子和可逆元

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

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

6. 特征：

$ord(1) = \infty \quad char(R) = 0$

$ord(1) = m < \infty \quad char(R) = m$.

注：整环的特征为 0 or 素数.