第十四次习题课.

循环群: $G=\langle a\rangle=\{a,a^2,a^3,\cdots,a^{n-1}\}$

循环群的子群也是循环群. 素数阶群是循环群.

(一). $\mathrm{card}(G)=\infty \Leftrightarrow \mathrm{ord}(a)=\infty$

$\mathrm{card}(G)=n<\infty \Leftrightarrow \mathrm{ord}(a)=n$.

(二). $\mathrm{card}(G)=\infty \Rightarrow G\cong(\mathbb{Z},+,0)$

$\mathrm{card}(G)=n<\infty \Rightarrow G\cong(\mathbb{Z}_n,+,\bar{0})$

$\phi:\ \mathbb{Z}\to G,\ m\mapsto g^m$

$\phi:\ \mathbb{Z}_n\to G,\ \underline{m}\mapsto g^m$

补充: 设 $G=\langle a\rangle$ 为有限阶循环群 且 $n=\mathrm{card}(G)$. 证明: a^k 是 G 的生成元当且仅当 k 和 n 互素.

证: 由于 $\langle a^k\rangle\subseteq\langle a\rangle=G$.

则 $G=\langle a^k\rangle \Leftrightarrow \mathrm{card}(G)=\mathrm{card}(a^k)=n$.

$\Leftrightarrow \mathrm{ord}(a^k)=n$

由 $\mathrm{ord}(a)=\mathrm{card}(G)=n$

$\Rightarrow \mathrm{ord}(a^k)=\dfrac{n}{\gcd(k,n)}$ 即 $\mathrm{ord}(a^k)=n\Leftrightarrow\gcd(k,n)=1$

环、子环和环同态

- 环的定义: 设集合 R 上有两个二元运算(加法和乘法), 其关于加法称为一个交换群, 关于乘法成为一个含幺半群, 且乘法和加法具有分配律, 则称 R 为一个环. 一般记 $0,1$ 为加法和乘法的单位元.
- 子环的定义: 设 $S\subset R$ 含有 $0,1$ 且关于 R 中的加法和乘法是一个环, 则称 S 为 R 的一个子环.
- 设 $\phi:\ R\to R'$ 为一个映射, 且满足:

  (1) $\phi(x+y)=\phi(x)+\phi(y),\ \forall x,y\in R$;

  (2) $\phi(xy)=\phi(x)\phi(y),\ \forall x,y\in R$;

  (3) $\phi(1_R)=1_{R'}$.

  则称 ϕ 为一个环同态. 进一步, 若 ϕ 为双射, 则称 ϕ 为一个环同构.
- 设 $\phi:\ R\to R'$ 为一个环同构, 则 $\mathrm{im}(\phi)$ 为 R' 的一个子环.

零因子、可逆元与整环

- 设 R 为一个环, $x\in R\backslash\{0\}$. 若存在 $y\in R\backslash\{0\}$ 使得 $xy=0$, 则称 x 是一个左零因子; 同样地, 可以定义右零因子.
- 非左零因子的元素具有左消去律; 非右零因子的元素具有右消去律.

- 设 R 为一个环, $x \in R$. 若存在 $y \in R$ 使得 $xy = yx = 1$, 则称 x 为 R 中的可逆元, x 的逆为 y, 记为 x^{-1}.
- 环 R 中可逆元全体关于环 R 的乘法构成一个群.
- 设 R 为一个交换环且无零因子, 则称 R 为整环. 整环具有消去律.

- 零因子一定不是可逆元.

模n剩余类环:

$(\mathbb{Z}_n, +, 0, \cdot, 1)$

(1) $\forall\ \bar{a} \in \mathbb{Z}_n$. $\bar{a}$ 关于乘法可逆 $\Longleftrightarrow$ $\gcd(a,n)=1$

(2) $\forall\ \bar{a} \in \mathbb{Z}_n$, $\bar{a}$ 是零因子 $\Longleftrightarrow$ $1<\gcd(n,a)<n$.

(3) $\mathbb{Z}_n$ 中元素一共只有三类: $\bar{0}$, 可逆元, 零因子.

矩阵环:

$(M_n(\mathbb{R}), +, O, \cdot, E)$

(1) 设 $A \in M_n(\mathbb{R})$ 是非零矩阵. A 是零因子 $\Longleftrightarrow$ $\mathrm{rank}(A)<n$.

(2) 设 $A \in M_n(\mathbb{R})$ 是非零矩阵. A 可逆 $\Longleftrightarrow$ $\mathrm{rank}(A)=n$

(3) $M_n(\mathbb{R})$ 中元素一共只有三类: O, 可逆元, 零因子.

引理 1.1 $\mathbb{Z}_n$ 的全部子群为 $\{\langle \bar{k} \rangle \mid k \in \mathbb{Z}\} = \{\langle \bar{k} \rangle \mid k \mid n \text{ 或 } k=0\}$

证: 由 Lagrange 定理 $H<G \Rightarrow \mathrm{card}(H) \mid \mathrm{card}(G)=n$.

则只需证: $\langle \bar{k} \rangle = \langle \overline{\gcd(k,n)} \rangle$

首先, 有 $\langle \bar{k} \rangle \subseteq \langle \overline{\gcd(k,n)} \rangle$ since $\gcd(k,n) \mid k$.

另一方面. 由欧几里德算法 $\exists\ u,v \in \mathbb{Z}$ s.t. $uk+vn=\gcd(k,n)$

$\Rightarrow \bar{u}\cdot\bar{k} = \overline{\gcd(k,n)}$ $\Rightarrow$ $\overline{\gcd(k,n)} \in \langle \bar{k} \rangle$

$\Rightarrow \langle \overline{\gcd(k,n)} \rangle \subseteq \langle \bar{k} \rangle$.

1. 列出群 $(\mathbb{Z}_{12}, +, \bar{0})$的所有子群 (要求不重不漏)

12 的所有正因子: 1, 2, 3, 4, 6, 12.

子群: $\langle\bar{0}\rangle = \{\bar{0}\}$ $\langle\bar{1}\rangle = \mathbb{Z}_{12}$

$\langle\bar{2}\rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$

$\langle\bar{3}\rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$

$\langle\bar{4}\rangle = \{\bar{0}, \bar{4}, \bar{8}\}$

$\langle\bar{6}\rangle = \{\bar{0}, \bar{6}\}$

2. 设 G 为循环群且 $\mathrm{card}(G) = +\infty$, 证明 G 只有两个生成元;

证: 设 $G = \langle a \rangle$ 由 $\mathrm{card}(G) = +\infty \Rightarrow \mathrm{ord}(a) = +\infty$

再设 $G = \langle a^k \rangle$ $(k \in \mathbb{Z}) \Rightarrow \exists\, m \in \mathbb{Z}$ $(a^k)^m = a$

$\Rightarrow a^{km-1} = e$ 由 $\mathrm{ord}(a) = +\infty \Rightarrow km - 1 = 0$

即 $k = \pm 1$ 则 G 的生成元为 a, a^{-1}

显然, $a \neq a^{-1}$ 否则 $a^2 = e$ 与 $\mathrm{ord}(a) = +\infty$ 矛盾.

3. 证明 $\mathbb{Z}_{13}$ 中的乘法可逆元关于乘法构成循环群 (提示：计算 $\bar{2}$ 的阶).

证: 设 $\mathbb{Z}_{13}^* = \mathbb{Z}_{13} \setminus \{\bar{0}\}$

由于 13 是素数 则 $\mathbb{Z}_{13}^*$ 中所有元素均可逆.

$\mathrm{card}(\mathbb{Z}_{13}^*) = 12$

由 $(\bar{2})^{12} = \overline{2^{12}} = \bar{1} \pmod{13}$ 且 $\forall\, 1 \leq k < 12$ $(\bar{2})^k \neq \bar{1}$.

$\Rightarrow \mathrm{ord}(\bar{2}) = 12$ $\Rightarrow \mathbb{Z}_{13}^* = \langle\bar{2}\rangle$

4. 设 $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. 验证 $(\mathbb{Z}[\sqrt{2}], +, 0, \cdot, 1)$ 是 $(\mathbb{R}, +, 0, \cdot, 1)$ 的子环. 确定该子环中所有可逆元.

证: (一) ① 显然 $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$.

② $\mathbb{Z}[\sqrt{2}]$ 显然非空.

$\forall\, x, y \in \mathbb{Z}[\sqrt{2}]$

设 $x=a_1+b_1\sqrt{2}$ $y=a_2+b_2\sqrt{2}$

则 $x+y=y+x$ 显然成立　加法可交换

$x-y=(a_1-a_2)+(b_1-b_2)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$　且 $0\in\mathbb{Z}[\sqrt{2}]$.

$\Rightarrow(\mathbb{Z}[\sqrt{2}],+,0)$ 是 $(\mathbb{R},+,0)$ 的子群.

$\Rightarrow(\mathbb{Z}[\sqrt{2}],+,0)$ 是一个交换群.

③ $\forall\ x=a_1+b_1\sqrt{2},\ y=a_2+b_2\sqrt{2},\ z=a_3+b_3\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$

由 $x\cdot y=(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$

可验证: $x\cdot(y\cdot z)=(x\cdot y)\cdot z$　结合律成立

且 取 $a=1$ $b=0$ $\Rightarrow$ $1+0\cdot\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ 含幺.

$\Rightarrow(\mathbb{Z}[\sqrt{2}],\cdot,1)$ 作成含幺半群.

④ 显然 乘法对加法满足分配律.

综上. $(\mathbb{Z}[\sqrt{2}],+,0,\cdot,1)$ 是 $(\mathbb{R},+,0,\cdot,1)$ 的子环.

(二). 设 $a+b\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ 是一个可逆元

设 $(a+b\sqrt{2})(c+d\sqrt{2})=1$

$\Rightarrow(ac+2bd)+(ad+bc)\sqrt{2}=1$

$$\Rightarrow\begin{cases}ac+2bd=1\\ad+bc=0\end{cases}$$

整理得 $a(c^2-2d^2)=c$

$c(a^2-2b^2)=a$

若 $a=0$ 则 显然 $b\sqrt{2}$ 不可逆. $\Rightarrow a\neq0$

$\Rightarrow\ \cancel{a}(c^2-2d^2)(a^2-2b^2)=\cancel{a}$

$\Rightarrow\ a^2-2b^2=\pm1$

另一方面, 显然 $a^2-2b^2=\pm1$ 时, $(a+b\sqrt{2})^{-1}=\dfrac{a-b\sqrt{2}}{a^2-2b^2}=\pm(a-b\sqrt{2})\in\mathbb{Z}[\sqrt{2}]$

即 $(\mathbb{Z}[\sqrt{2}],+,0,\cdot,1)$ 的所有可逆元为 $\{a+b\sqrt{2}\mid a^2-2b^2=\pm1,\ a,b\in\mathbb{Z}\}$

5. 设 x 是环 R (有单位元) 的一个非零元素，则称 x 为幂零的若存在 $n \in \mathbb{Z}^+$, 使得 $x^n = 0$. 证明：

(1) 如果 x 是幂零元，则有 $1 - x$ 是可逆元；

(2) 环 $\mathbb{Z}_m$ 包含幂零元当且仅当 m 可以被一个大于 1 的整数的平方整除.

证: (1) 若 $x \in R$ 是幂零元

即 $\exists\ n \in \mathbb{Z}^+$, $x^n = 0$

则 $(1-x)\cdot(1+x+\cdots+x^{n-1}) = 1-x^n = 1$

$\Rightarrow$ $1-x$ 可逆，其逆元为 $1+x+\cdots+x^{n-1}$

(2) "$\Rightarrow$" 若 $\mathbb{Z}_m$ 包含幂零元 $\overline{a}$: $1 \le a \le m-1$, $a^n \equiv 0 \pmod m$

即 $m \mid a^n$ 设 $a^n = m \cdot q$ $q \in \mathbb{Z}^+$

假设 m 不可以被一个大于 1 的整数的平方整除

则 $m = p_1 p_2 \cdots p_s$ p_i 为互不相同的素数.

$\Rightarrow$ $p_i \mid a^n$ $\Rightarrow$ $p_i \mid a$ 即 $m \mid a$ 与 $\overline{a} \neq 0$ 矛盾.

"$\Leftarrow$" 若 m 可以被一个大于 1 的整数的平方整除.

设 $m = b^2 \cdot q$ $b, q \in \mathbb{Z}^+$

则 取 $a = bq < m$ $\Rightarrow$ $a^2 = b^2 q^2 = m \cdot q \equiv 0 \pmod m$

即 $(\overline{a})^2 = 0$ $\overline{a}$ 是一个幂零元.

6. 设 $(R, +, 0, \cdot, 1)$ 是一个环, $u \in R$. 若存在 $v \in R$ 使得 $uv = 1$, 我们称 u 有右逆. 现设 u 有右逆, 证明以下命题等价：

(1) u 不是 R 中的可逆元;

(2) u 为左零因子;

(3) u 有多于一个右逆.

证: (1) $\Rightarrow$ (2)

若 u 不是 R 中的可逆元 即 u 没有左逆.

假设 u 不是左零因子

由 $uv=1 \Rightarrow uv-1=0 \Rightarrow u(vu-1) = uvu-u$
$=0$

$\Rightarrow vu-1=0$

$vu=1$ 与 u 没有左逆矛盾.

(2) $\Rightarrow$ (3)

设 u 为左零因子 则 $\exists\, w \neq 0$ $uw=0$

则由 $uv=1 \Rightarrow uv+uw = u(v+w) = 1$

$\Rightarrow v+w$ 是另一个右逆.

(3) $\Rightarrow$ (1)

(一). 若 u 有多于一个右逆 $uw=1$ 右逆与左逆若均存在 则 相等且唯一

$\Rightarrow u$ 不可逆.

(二). 若 u 有多于一个右逆. 设 $uv_1=1$, $uv_2=1$ $v_1 \neq v_2$

又由 u 可逆. $\exists\ w$ s.t. $wu=uw=1$ (w 可以是 v_1 或 v_2)

$v_1 = 1\cdot v_1 = wu\cdot v_1 = w$

$v_2 = 1\cdot v_2 = wu\cdot v_2 = w$

$\Rightarrow v_1 = v_2$ 矛盾.

$\therefore$ u 不可逆.

补充: $(R,+,0,\cdot,1)$ 是环. $\forall a,b\in R$

证: 若 $1-ab$ 可逆, 则 $1-ba$ 也可逆.

设 $c \in R$ 使得 $c(1-ab) = (1-ab)c = 1$, 则 $c-1 = cab = abc$. 注意到 $(1-ba)bc = bc - babc = bc - b(c-1) = b$, 从而 $(1-ba)bca = ba$, $1-(1-ba)bca = 1-ba$. 进一步, $1 = (1-ba)(1+bca)$. 容易验证 $(1+bca)(1-ba) = 1$, 从而 $1-ba$ 可逆.