1.(a) 写出 $G=(\mathbb{Z}_{12},+,0)$ 的所有生成元.

G 是一个循环群, $G=\langle \bar{1}\rangle$.

$G=\langle \bar{a}\rangle$., a ?

$G=\langle \bar{a}\rangle \Leftrightarrow \gcd(a,12)=1$.

$\Rightarrow a=1,5,7,11$.

$\Rightarrow G$ 的所有生成元为 $\bar{1},\bar{5},\bar{7},\bar{11}$

(b) 设 $G=\langle a\rangle$ 为循环群且 $\mathrm{card}(G)=+\infty$. 证明: G 只有2个生成元.

证: $\mathrm{card}(G)=+\infty$. 则 $\mathrm{ord}(a)=+\infty$. G 中的每个元素均可以表示成 $a^i, i\in\mathbb{Z}$.

设 $G=\langle a^k\rangle$, $k\in\mathbb{Z}$, 则 $\exists m\in\mathbb{Z}$, s.t. $(a^k)^m=a$.

$\Rightarrow a^{km-1}=e$, e 为 G 的单位元

由 $\mathrm{ord}(a)=+\infty$. 可得, $km-1=0$.

注意到 $k,m\in\mathbb{Z}$, 则 $k=\pm 1$. 另一方面 $a\neq a^{-1}$, 假设 $a=a^{-1}$, 则 $a^2=e\Rightarrow \mathrm{ord}(a)<\infty\rightarrow\leftarrow$.

$\Rightarrow$ G 只有两个生成元.

(c) 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: a^k 是 G 的生成元 $\Leftrightarrow \mathrm{ord}(a^k)=n \Leftrightarrow \frac{n}{\gcd(n,k)}=n$.

$\Leftrightarrow \gcd(n,k)=1$.

2 (a) 写出 $(\mathbb{Z}_{12},+,0)$ 的所有子群

(b). 证明: 当 $G=\langle a\rangle$ 为 n 阶循环群时, 对于每个 n 的正因子 k (即 $k\mid n, k>0$)

G 有且只有一个 k 阶子群, 且这个子群就是 $\langle a^{\frac{n}{k}}\rangle$.

解: (a) 循环群的子群是循环群.

$\langle \bar{0}\rangle$, $\langle \bar{1}\rangle$, $\langle \bar{2}\rangle$, $\langle \bar{3}\rangle$, $\langle \bar{4}\rangle$, $\langle \bar{6}\rangle$.

(b) 证明: 当 $G=\langle a\rangle$ 为 n 阶循环群时, 对于每个 n 的正因子 k (即 $k\mid n, k>0$), G 有且只有一个 k 阶子群, 且这个子群就是 $\langle a^{\frac{n}{k}}\rangle$.

Pf: 令 $q=\frac{n}{k}$, $ord(a^q) = \frac{n}{gcd(q,n)} = \frac{n}{q} = k$. } 存在性

$\Rightarrow \langle a^q \rangle$ 是 G 的一个 k 阶子群

~~G中任何一个元素都可以写成 a^i, $i \in N$~~

再设 $\langle a^m \rangle$ 是 G 的另一个 k 阶子群. 则 $ord(a^m) = k$.

唯一性:

$\Rightarrow k = \frac{n}{gcd(m,n)}$

$\Rightarrow gcd(m,n) = \frac{n}{k} = q$

$\Rightarrow q \mid m$

$\Rightarrow a^m \in \langle a^q \rangle$

$\Rightarrow \langle a^m \rangle \subset \langle a^q \rangle$

$\Rightarrow \langle a^m \rangle = \langle a^q \rangle$ ($\because card(\langle a^m \rangle) = card(\langle a^q \rangle) = k$)

$\Rightarrow$ G 有且只有一个 k 阶子群

环

(def) 五元组 $(R, +, 0, \cdot, 1)$ 其中 R 是集合, $0, 1 \in R$ 且 $0 \neq 1$, $+, \cdot$ 是 R 上的二元运算. 称为(含幺)环. 如果

(i) $(R, +, 0)$ 是交换群

(ii) $(R, \cdot, 1)$ 是含幺半群 且

(iii) 对于任意 $x, y, z \in R$.

$x(y+z) = xy + xz$ $(x+y)z = xz + yz$

prop. ① $\forall r \in R$, $0 \cdot r = r \cdot 0 = 0$

② $\forall r \in R$, $-r = (-1) \cdot r = r \cdot (-1)$

③ $(-1) \cdot (-1) = 1$

④ $\forall a, b \in R$, $m, n \in \mathbb{Z}$. $(m a) \cdot (n \cdot b) = (m \cdot n)(a \cdot b)$

(注: m a 的"·"为累加法; n·b 为累加; m·n 为整数乘法; (a·b) → 环中乘法)

子环

设 R 为环, 集合 $S \subseteq R$, s.t $0, 1 \in S$. 且 $(S, +, 0, \cdot, 1)$ 构成环,

则称 S 为 R 的子环.

3. 设 $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}: a,b\in\mathbb{Z}\}$. 验证 $(\mathbb{Z}[\sqrt{2}],+,0,\cdot,1)$ 是 $(R,+,0,\cdot)$ 的子环. 确定这个子环中的所有可逆元.

Pf: $\mathbb{Z}[\sqrt{2}]$ 非空, $0,1\in\mathbb{Z}[\sqrt{2}]$

$\forall\ a+b\sqrt{2},\ c+d\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ 有

$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$

$(a+b\sqrt{2})-(c+d\sqrt{2})=(a-c)+(b-d)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$

$\Rightarrow (\mathbb{Z}[\sqrt{2}],+,0)$ 是 $(R,+,0)$ 的一个交换子群

$(a+b\sqrt{2})\cdot(c+d\sqrt{2})=(ac+2bd)+(bc+ad)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$

$\Rightarrow (\mathbb{Z}[\sqrt{2}],\cdot,1)$ 是 $(R,\cdot,1)$ 的含幺乘法半群

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

设 $a+b\sqrt{2}$ 可逆, 则 $\exists\ c+d\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ s.t.

$$(a+b\sqrt{2})(c+d\sqrt{2})=1$$

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

由 ② $\Rightarrow$ $b=-\frac{ad}{c}$ 代入 ① $\quad ac-\frac{2ad^2}{c}=1 \Rightarrow a(c^2-2d^2)=c$.

$d=-\frac{bc}{a}$ 代入 ①, $\quad ac-\frac{2b^2c}{a}=1 \Rightarrow c(a^2-2b^2)=a$.

$a\mid c$ ⇕ $c\mid a$.

$\Rightarrow a=\pm c$, 代入 ② 可得 $b=\pm d$.

$a=0$, $b\sqrt{2}$ 不可逆.

$a\neq 0$, 则有 $a^2-2b^2=\pm 1$

$a^2-2b^2=\pm 1$, $\quad \frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}\in\mathbb{Z}[\sqrt{2}]$

所有可逆元构成的集合为 $\{a+b\sqrt{2} \mid a^2-2b^2=\pm 1,\ a,b\in\mathbb{Z}\}$

4. 环 R 中非零元素 x 称为幂零的, 若存在 $n\in\mathbb{N}$, s.t. $x^n=0$. 证明:

(a) 若 D 是仅含有单位元的环, x 是幂零元, 则 $1-x$ 是可逆元.

(b) 环 $\mathbb{Z}_m$ 或 $\mathbb{Z}/m\mathbb{Z}$ 包含幂零元 $\Leftrightarrow$ m 可以被一个大于1的整数的平方整除.

证: (a). 设 x 是幂零元, 则 $\exists\ n\in\mathbb{N}.\ s.t.\ x^n=0$

$\Rightarrow 1-x^n=1$

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

$\Rightarrow (1-x)^{-1}=1+x+\cdots+x^{n-1}$.

(b) "$\Leftarrow$" 设 $m=s^2t$, $s,t\in\mathbb{Z}^+$, 且 $s>1$

$st<m\Rightarrow \overline{st}=\bar{s}\cdot\bar{t}\neq\bar{0}$,

$(st)^2=\bar{s}^2\cdot\bar{t}^2=\bar{m}\cdot\bar{t}=\bar{0}$

$\Rightarrow \overline{st}$ 是 $\mathbb{Z}_m$ 中幂零元.

$x^n\nmid m$, $k\in\mathbb{Z}$

"$\Rightarrow$" 设 $\bar{x}$ 是 $\mathbb{Z}_m$ 中幂零元且 $\bar{x}^n=\bar{0}$, $n\in\mathbb{N}$.

从而 $m\nmid x$, $m\mid x^n$

假设 m 中存在大于1的整数平方的因子. 考虑 m 的素因解

$m=p_1p_2\cdots p_s$, p_i 是互不相同的素数

$p\mid ab\Rightarrow p\mid a$ or $p\mid b$

$m\mid x^n\Rightarrow p_i\mid x^n$, $\forall i$

p_i 是素数, $p_i\mid x$, 故 $p_i\mid x^{n-1}$

$\vdots$

$p_i\mid x$

p_i 是素数, 则 $p_i\mid x$

$\Rightarrow p_1p_2\cdots p_s\mid x$

$\Rightarrow m\mid x$ $\rightarrow\leftarrow$

$\Rightarrow m$ 含有一个大于1的整数平方的因子.

5. 设 F 是一个域,

$$A=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}\in M_4(F)$$

如果下列性质

(a) 讨论 $\mathrm{rank}(A)$ 的取值.

(b) 设 $\phi_A: F^4 \to F^4$ 是以A为矩阵的线性映射, 求 $\ker(\phi_A)$ 和 $\mathrm{im}(\phi_A)$.

$1+\cdots+1-1=0$ (n 个)

环的特征

Def 设 $(R,+,0,\cdot,1)$ 是环. 如果加法群 $(R,+,0)$ 中 1 的阶有限, 且 $\mathrm{ord}(1)$ 称为R的特征. 否则, R的特征定义为0

例 $\mathrm{char}(\mathbb{Z}_n)=n$, $\mathrm{char}(\mathbb{Z})=0$

prop. 整环的特征只有是0或素数.

(a)
$$A=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}\to\begin{pmatrix}1&1&1&1\\0&0&-2&-2\\0&-2&0&-2\\0&-2&-2&0\end{pmatrix}\to\begin{pmatrix}1&1&1&1\\0&-2&0&-2\\0&0&-2&2\\0&0&-2&-2\end{pmatrix}$$
$$\to\begin{pmatrix}1&1&1&1\\0&-2&0&-2\\0&0&-2&2\\0&0&0&-4\end{pmatrix}$$

$A(e_1,\dots,e_n)=(e_1,\dots,e_n)C$

$\phi(e_i)$ 的坐标)

$\det(A)=-16$.

$\mathrm{char}(F)\neq 2$, $-16\neq 0_F$, 则 $\mathrm{rank}(A)=4$.

$\mathrm{char}(F)=2$, $1=-1$, $\mathrm{rank}(A)=1$.

(b) $\mathrm{char}(F)\neq 2$, $\mathrm{rank}(A)=4$, 则 $\ker(\phi_A)=\{0\}$, $\mathrm{im}(\phi_A)=F^4$.

$\mathrm{char}(F)=2$, $\mathrm{im}(\phi_A)=\left\langle\begin{pmatrix}1\\1\\1\\1\end{pmatrix}\right\rangle$

$\ker(\phi_A)=\left\langle\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\1\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\\1\end{pmatrix}\right\rangle$

$\Updownarrow$

$\left\{\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}\middle|\ x_1+x_2+x_3+x_4=0\right\}$

6. (a) 偶数阶群必含有2阶元.

pf. 设G为偶数阶群, 阶为1的元素只有1个, e.

阶大于2的元素都是成对出现 ☆

$\forall a\in G$, $ord(a)>2$,

① $ord(a)=ord(a^{-1})$ （设 $ord(a)=m$, $ord(a^{-1})=n$.

$a^m=e\Rightarrow (a^m)^{-1}=e\Rightarrow (a^{-1})^m=e \Rightarrow m|n$.

同理 $n|m$, 从而 $m=n$）.

② $a\neq a^{-1}$. 若 $a=a^{-1}\Rightarrow a^2=e\Rightarrow ord(a)<2 \Rightarrow \in$.

③ $\forall a\neq b, b^{-1}$, $\{a,a^{-1}\}\cap\{b,b^{-1}\}=\varnothing$.

$\Rightarrow$ 阶大于2阶元素是偶数个

由 card(G) 为偶数，从而 阶为2阶元素是奇数，从而非空。

(b) 由 Caley 定理可知，G 同构于 S_{2n} 的一个子群，设为 A.　　$G\xrightarrow{f}A$

由(a)知，G 存在2阶元，设为 a.

$a\xrightarrow{f}\tau a$.

$ord(\tau a)=ord(a)=2$.　　l_1　　l_m

τa 可以写成互不相交的轮换之积，设为 $\tau a=\tau a_1\tau a_2\cdots\tau a_m$.　$A,B\subset G$

$ord(\tau a)=lcm(l_1,\cdots l_m)=2$.

$\Rightarrow l_1=\cdots=l_m=2$.　　$C\rightarrow B$

$\Rightarrow \tau a$ 也写成互不相交的对换之积（n个）.　　$a\xrightarrow{射}\tau a$

由n为奇数可知，A 存在奇置换 τa.

claim: 若置换群 A_{2n} 存在奇置换，则奇偶置换各占一半，所有偶置换构成子群.

$B\xrightarrow{偶}C$ 奇

$a\xrightarrow{单}\tau a$,　$a\in B$

$\Rightarrow$ A中所有偶置换构成阶为n的子群.　　$|B|\leq|C|$　$\tau a_1=\tau a_2 \Rightarrow a_1=a_2$.

$\Rightarrow$ G 存在阶为n的子群　　$|C|\leq|B|\Rightarrow|B|=|C|$

例 $Z_3=\{\bar0,\bar1,\bar2\}$. 求解 $\begin{pmatrix}\bar1&\bar2&\bar1\\\bar2&\bar1&\bar2\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=\begin{pmatrix}\bar0\\\bar0\\\bar0\end{pmatrix}$

$$A \to \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \end{pmatrix}$$

$$\to \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix} \to \begin{pmatrix} \bar{1} & \bar{0} & \bar{1} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix}$$

$\Rightarrow \operatorname{rank}(A) = 2, \Rightarrow \dim(V_A) = 1$

$\begin{cases} x_1 + x_3 = \bar{0} \\ x_2 = \bar{0} \end{cases} \Rightarrow V_A$ 的一组基为 $\begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{2} \end{pmatrix}$

$$\Rightarrow V_A = \left\{ \lambda \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{2} \end{pmatrix} \mid \lambda \in \mathbb{Z}_3 \right\} = \left\{ \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{2} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{0} \\ \bar{1} \end{pmatrix} \right\}$$

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

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

$$= \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} + n \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{0} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2n} \\ \bar{0} & \bar{1} \end{pmatrix} \quad \binom{n}{0} \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{0} & \bar{0} \end{pmatrix}^0 + \binom{n}{1} \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{0} & \bar{0} \end{pmatrix}$$

例 $x^2 + x$ 在 $\mathbb{Z}_2$ 恒为0

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ $\bar{0}^2 + \bar{0} = \bar{0}$, $\bar{1}^2 + \bar{1} = \bar{2} = \bar{0}$.

但是 $x^2 + x$ 作为 $\mathbb{Z}_2$ 上面的多项式不是零多项式, $1 \neq \bar{0}$.