1、 证明任意有限整环 R 是一个域.

Pf: $\forall\ a \in R,\ a \neq 0$

考虑映射 $\varphi_a: R \longrightarrow R$

$r \longmapsto a \cdot r$

R整环 $\Rightarrow \varphi_a$ 单射，$|R| < \infty$

$\Rightarrow \exists\ b$ s.t. $\underset{a\cdot b}{\underset{\parallel}{\varphi_a(b)}} = 1$

a交换 $\Rightarrow a \cdot b = b \cdot a = 1 \Rightarrow \forall a \neq 1,\ \exists a^{-1} = b \in R.$

i.e. R为域.

2、 设 p 是一个素数, R 是有单位元的交换环, 使得任取 $x \in R$, $px = 0$. 证明

$$(x+y)^{p^m} = x^{p^m} + y^{p^m}$$

对任意 $x, y \in R$ 成立.

Pf: 对m作归纳:

$m=1 \quad (x+y)^p = x^p + C_p^1 x y^{p-1} + \cdots + C_p^{p-1} x^{p-1} y + y^p$

$p \mid C_p^i \qquad = 0$

$m = i-1$ 成立

$m = i$ 时 $\quad (x+y)^{p^i} = \left((x+y)^{p^{i-1}}\right)^p$

$= (x^{p^{i-1}} + y^{p^{i-1}})^p$

$= x^{p^i} + C_p^1(-) - \cdots + C_p^{p-1}(-) + y^{p^i}$

$= x^{p^i} + y^{p^i}.$

$\square$

Rem: $p \mid C_{p^m}^k$, $1 \leq k \leq p^m-1$

$(1+x)^p = (1+C_p^1 x + \cdots + C_p^{p-1} x^{p-1} + x^p)$

$(1+x)^{p^2} = (1+C_p^1 x + \cdots + C_p^{p-1} x^{p-1} + x^p)^p$

$= 1+C_{p^2}^1 x + \cdots + C_{p^2}^{p^2-1} x^{p^2-1} + x^{p^2}$

以此类推，比较系数有 $C_{p^m}^k$ 为一些低次

C_p^j 乘积的组合. 故而 $p \mid C_{p^m}^k$.

一般情况下 $p^m \nmid C_{p^m}^k$. $C_{2^2}^2 = 6$ $2^2 \nmid 6$

3、环 R 的非零元素 x 称为幂零的，若存在 $n \in N$，使得 $x^n = 0$. 证明:

i) 若 R 是任意有单位元的环，x 是幂零元，则 $1-x$ 是可逆元;

ii) 环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 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.

Pf: i) 设 $x^m = 0$

$(1-x)(1+x+x^2 \cdots + x^{m-1}) = 1-x^m = 0$.

ii) "⇒" 若 $\bar{a} \in \mathbb{Z}_m$ 为幂零元，$a \nmid m$.

$\exists\, r \in \mathbb{Z}$ s.t. $\bar{a}^i \neq \bar{0}$ $1 \leq i < r$, $\bar{0} = \bar{a}^r = \overline{a^r}$

$\Rightarrow m \mid a^r$ $m \nmid a^i$ $1 \leq i < r$

设 $a = q_1^{t_1} \cdots q_s^{t_s}$ 素数. $t_1, \cdots, t_s \geq 1, \in \mathbb{Z}$

$m \mid a^r \Rightarrow m = q_1^{a_1} \cdots q_s^{a_s}$, $a_1, \cdots, a_s \in \mathbb{Z}, a_i \geq 0$.

$m \nmid a \Rightarrow \exists\, a_i > t_i \geq 1 \Rightarrow a_i \geq 2$

$\Rightarrow p_i^2 \mid m$.

"$\Leftarrow$" 若 m 可以被某整数平方整除

设 $m = p_1^{r_1} \cdots p_n^{r_n}$，则 $\exists\ r_i \geq 2$，$\in \mathbb{Z}$.

p_i 素数

取 $a = p_1 \cdots p_n$ 则 $\bar{a} \neq \bar{0}$

取 $r = \max\{r_i\}$ $r > 1$

$m \mid a^r \Rightarrow \bar{a}^r = 0.$ $\square$

4、设 F 是一个域,

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

根据 F 的特征,

i) 讨论 $\operatorname{rank}(A)$ 的取值;

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

i) 设 $\operatorname{char}(F) = p$,

$p = 2$，$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$，$\operatorname{rank} = 1$.

$p \neq 2$，$(4, p) = 1$，$\Rightarrow \exists\ a, b$ s.t. $4a + pb = 1$

$\Rightarrow$ 4 在 F 中可逆

$A^t \cdot A = 4 \cdot E \Rightarrow \det(A) \neq 0$ $. \Rightarrow \operatorname{rank} = 4.$

ii) 若 $\operatorname{char}(p) = 2$，$A \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

$\ker \varphi_A = \left\langle \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$ $\quad \operatorname{im} \varphi_A = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle$

若 $char(p) \neq 2$ $\ker \varphi_A = \{0\}$. , $\operatorname{im}\varphi_A = F^4$.

Rem: 特征必为素数.

5、证明矩阵 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$，其中 $a, b \in \mathbb{Z}_3$，在矩阵加法乘法下，构成一个 9 元域，而这个域的乘法群是 8 阶循环群.

$T = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{Z}_3 \right\} \subset M_3(\mathbb{Z}_3)$

Pf：T显然关于加法封闭，构成交换群.

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 - a_2b_1 \\ -a_1b_2 - a_2b_1 & a_1a_2 - b_1b_2 \end{pmatrix}$$

关于乘法封闭，

$\Rightarrow$ 此为一个环，由计算知其为交换环.

有单位元 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$a, b \in \mathbb{Z}_3$，$a^2 + b^2$ 计算如下

$b \backslash a$ (a^2+b^2)	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

$\Rightarrow$ $a \neq 0$ or $b \neq 0$

则 $a^2 + b^2 \neq 0$

$$\forall \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq 0 \Rightarrow (a^2+b^2)^{-1} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

$$= (a^2+b^2)^{-1} \begin{pmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

i.e. $\forall \begin{pmatrix} a & b \\ -b & b \end{pmatrix} \neq 0$, 其可逆. $\Rightarrow$ 此为一个域

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 2 & \\ & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}$$

验证 $\left\{ \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^i \middle| i \in \mathbb{Z} \right\} = T^\times$.

6、 证明如下命题:

i) 有限交换群中存在一个元素, 其阶是所有元素的最小公倍数.

ii) 设 G 是有限交换群, 则 G 是循环群的充分必要条件是对于任一正整数 m, $x^m = e$ 在 G 中最多有 m 个解.

Pf: i) 设此群为 G, $a \in G$ 设 $o(a) = ord(a)$

设 $m \in G$ s.t. $o(m) = \max\{g \in G \mid o(g)\}$.

我们证明, $\forall g \in G$ $o(g) \mid o(m)$

若 $o(g) \nmid o(m)$, 则 $\exists p$ 为素数, s.t.

p^r 恰好整除 $o(m)$, i.e. $p^r \mid o(m)$, $p^{r+1} \nmid o(m)$

记为 $p^r \| o(m)$,

$p^s \| o(g)$ $s > r \geq 0$.

设 $o(m)=u\cdot p^s$ $o(g)=v\cdot p^r$

$(u,p)=1$, $(v,p)=1$.

$\Rightarrow o(g^v)=p^t$, $o(m^{p^s})=u$

$(p,u)=1$, $g^v\cdot m^{p^s}=m^{p^s}\cdot g^v$

$\Longrightarrow o(g^v\cdot m^{p^s})=u\cdot p^t>u\cdot p^s=o(m)$

与 m 阶最大矛盾.

ii) ⇒ 若 $G=\langle a\rangle$, $|a|=o(a)=n$.

设 $x=a^t$ 满足 $x^m=e$

则 $x^{(m,n)}=e$ $\left(\exists\, u,v \text{ s.t. } am+bn=(m,n)\right)$

则 $a^{t(m,n)}=e \Rightarrow n\mid t(m,n)$

$\Rightarrow \frac{n}{(m,n)}\mid t \Rightarrow x=a^t\in\langle a^{\frac{n}{(m,n)}}\rangle$

$|\langle a^{\frac{n}{(m,n)}}\rangle|=(m,n)$

$\Rightarrow x^m=e$ 在 G 中解个数小于等于 m.

"$\Leftarrow$" 由(i) $\exists\, a\in G$ s.t. $o(a)=\max\{o(g)\mid g\in G\}$.

则 $\forall g\in G$ $g^{o(a)}=0$

$\Rightarrow x^{o(a)}=e$ 有 $|G|$ 个解.

$\Rightarrow |G|\le$ 方程解 $\le o(a)\le |G|$

$\Rightarrow |o(a)|=|G| \Rightarrow G$ 为循环群. $\square$

Cor: 设 F 是一个域, $F^\times$ 为其乘法子群.

$G\subset F^\times$ 为子群, 若 $|G|<\infty$, 则 G 为循环群.

Pf: 考虑方程 $x^n=1$, 其至多 n 个解. $\square$

Rem: 域上 n 次多项式最多 n 个解. (证明: 考虑带余除法 $f(x)/(x-a)$.)

7、证明 A_4 没有 6 阶子群.

Pf $A_4=12$.

设 $G\subset A_4$. $|G|=6$. $\forall a\in |G|$ $o(a)=1,2,3,6$.

- 若 $\exists\, o(a)=6$, 则 A_4 中存在 6 阶元 矛.
- 若所有元素均为 3 阶元(除 e), 则 g 与 g^{-1} 配对, 则 $|G|$ 为奇数 矛.
- 若所有元素均为 2 阶(除 e), 则 $\{e,a,b,ab\}$ 构成 $|G|$ 子群. 矛.

$\Rightarrow |G|$中有一2阶元与3阶元. 设为 a, b.

A_4中 2阶元只有.

$\{(12)(34),\ (13)(24),\ (14)(23)\}$.

3阶元为3轮换

a) 若$(12)(34) \in G$, $(123) \in G$

任取3阶元 $(123)(12)(34)(123)^{-1}$

$$= (123)(12)(123)^{-1}(123)(34)(123)^{-1}$$

$$= (23)(14)$$

$$(123)(23)(14)(123)^{-1} = (13)(24)$$

$\Rightarrow$ $K = \{e, (12)(34), (13)(24), (14)(23)\} \subset A_4$.

K为子群 .

b) 其余同理可得 矛盾.

故而 A_4 无 6阶子群. □