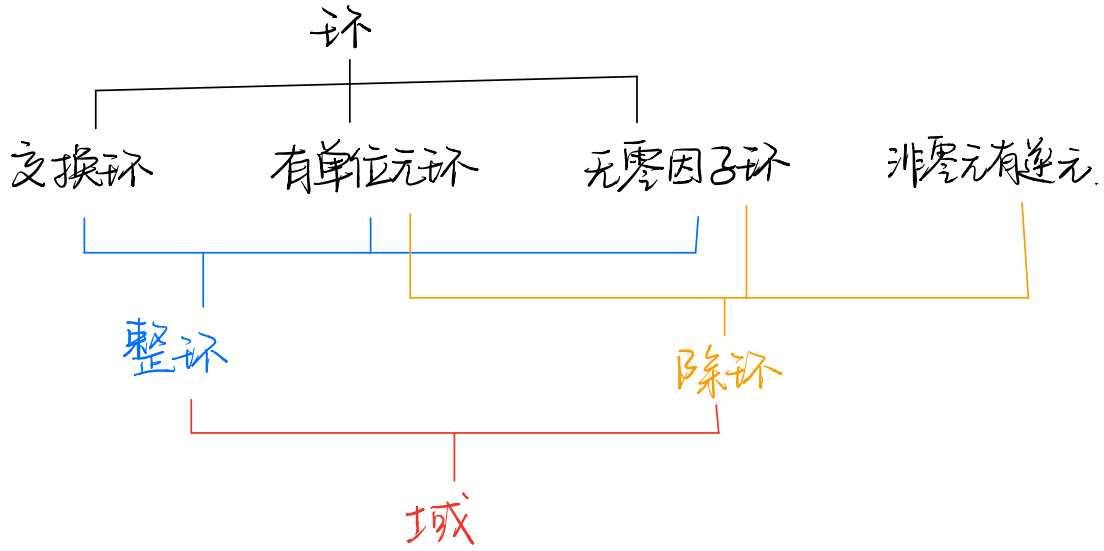
第十四次习题课

一、域

1. 定义：　整环 + 非零元可逆



hw1. 证明任意有限整环R是一个域。

证：　域：整环 + 非零元可逆

只需证 $\forall a \in R\setminus\{0\}$, $\exists b \in R\setminus\{0\}$ s.t. $ab = ba = 1$.

若 $a = 1$, 则 $b = 1$ 是 a 的逆.

若 $a \neq 1$, 则由环的乘法封闭性可知 $a, a^2, \cdots, a^n, \cdots \in R$

$\because \mathrm{card}(R) < \infty \quad \therefore \exists i, j \in \mathbb{Z}^+, i \neq j$ s.t. $a^i = a^j$

不妨设 $i < j$　则 $a^i(1 - a^{j-i}) = 0$

$\because R$ 是整环，有消去律且 $a \neq 0 \Longrightarrow a^{j-i} = 1$

若 $j - i = 1$, 则 $a = 1$ 与 $a \neq 1$ 矛盾

$\therefore j - i > 1$. 则 $a^{j-i-1} \cdot a = 1$.

令 $b = a^{j-i-1}$　即满足 $ab = ba = 1$.

法二：设 $R = \{r_1, \cdots, r_n\}$

$\forall\ r_i \in R\setminus\{0\}$　　$r_i \cdot r_j \neq r_i \cdot r_k \quad j \neq k$

$\therefore$ 集合 $\{r_1r_1, \cdots, r_1r_n\}$ 有 n 个元素且包含于 R

$\therefore R=\{r_1r_1, \cdots, r_1r_n\} \Rightarrow \exists j \in \{1, \cdots, n\}$ s.t. $r_1r_j=1$.

法三: $\forall\, a \in R,\ a \neq 0$

考虑映射 $\varphi_r : R \longrightarrow R$

$r \longmapsto ar$

R 为整环 $\Rightarrow \varphi_r$ 为单射. $|R| < \infty$

$\Rightarrow \exists\, b$ s.t. $\varphi_r(b)=1$ 即 ab

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

故 R 为域。

hw5.

$a^{\curvearrowright}\ {}^{\curvearrowright}b$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{2}$
$\bar{2}$	$\bar{1}$	$\bar{2}$	$\bar{2}$

记 $R=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle|\ a, b \in \{\bar{0}, \bar{1}, \bar{2}\}\right\}$.

则 R 有九个元。

i) $\because a, b \in \mathbb{Z}_3$ $\therefore ab$ 符合 $\mathbb{Z}_3$ 运算.

加法封闭; 结合律成立; 有单位元 $\begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix} \triangleq O$

逆元: $\forall\, A \in R\ \exists\, B \in R$ s.t. $A+B=B+A=O$.

交换: $A+B=B+A$.

ii) 乘法封闭; 结合律成立; 有单位元 $\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$.

即 $A\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}=\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}A=\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$

交换: $BA=AB$

iii) 分配律成立.

此时已证 R 为交换环.

iv) 无零因子

$\forall a \in R\backslash\{0\}$, 不存在 $b \in R\backslash\{0\}$, s.t. $ab=0$

此时已证整环.

v) 非零元可逆

$\forall\ a\neq 0$ or $b\neq 0$ $\quad a^2+b^2\neq 0$.

$\forall \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq 0$ 我们有

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

此时已证 R 为域.

八个元: $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\ \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\ \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

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

$R = \left\langle \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{2} & \bar{1} \end{pmatrix} \right\rangle$

$\forall\ A \in R$ 证 $A^8 = E$. $\qquad A = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{1} & \bar{1} \end{pmatrix}$.

$\therefore\ ord(A) \mid 8$.

$\therefore\ ord(A) = 1, 2, 4, 8$.

$\because\ A^2, A^4 \neq E$. $\therefore\ ord(A) = 8$.

2. 特征:

$$\mathrm{char}(F)=\begin{cases}0 & \forall m\in\mathbb{Z}^+ \quad m\cdot 1\neq 0\\ p & \exists p \ \text{ s.t. } p\cdot 1=0.\end{cases}$$

hw4. 首先域的特征为 0 或者素数。

i) $\mathrm{char}(F)=2$.

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

$\mathrm{rank}(A)=1$.

$\mathrm{char}(F)\neq 2$. $\det(A)\neq 0$ $\mathrm{rank}(A)=4$.

ii) $\mathrm{char}(p)=2$.

$$A\longrightarrow\begin{pmatrix}1&1&1&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$$

$\dim(\mathrm{im}(\varphi_A))=\mathrm{rank}(A)=1$.

$\dim(\ker(\varphi_A))=4-1=3$.

$\mathrm{im}(\varphi_A)$ 取 A 的列向量 $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ $\mathrm{im}(\varphi_A)=\begin{pmatrix}\bar{1}\\\bar{1}\\\bar{1}\\\bar{1}\end{pmatrix}$

$\ker(\varphi_A)$: $x_1=\bar{1}x_2+\bar{1}x_3+\bar{1}x_4$

$\bar{1}$	$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{0}$

$$\left\langle \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{0} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{1} \\ \bar{0} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{1} \\ \bar{0} \end{pmatrix} \right\rangle.$$

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

3. 分式域

4. 域同态

注: $char(E) \neq char(F)$ 则不可能存在域同态.

5. 域上的线性代数

考虑 $F_p = (\mathbb{Z}_p, +, \bar{0}, \cdot, \bar{1})$

$$F_p^n = \left\{ \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_n \end{pmatrix} \mid \bar{x}_i \in \mathbb{Z}_p \right\}$$

加法: $\bar{x} + \bar{y} = \begin{pmatrix} \overline{x_1+y_1} \\ \vdots \\ \overline{x_n+y_n} \end{pmatrix}$

数乘 $\bar{\alpha} \cdot \bar{x} = \begin{pmatrix} \overline{\alpha x_1} \\ \vdots \\ \overline{\alpha x_n} \end{pmatrix}$

线性相关/无关: 称 $\bar{w}_1, \cdots, \bar{w}_\ell \in F_p^n$ 线性相关. 如果存在不全为 $\bar{0}$ 的 $\bar{r}_1, \cdots, \bar{r}_\ell \in \mathbb{Z}_p$ s.t

$$\bar{r}_1 \cdot \bar{w}_1 + \cdots \bar{r}_\ell \cdot \bar{w}_\ell = \vec{0} = \begin{pmatrix} \bar{0} \\ \vdots \\ \bar{0} \end{pmatrix}$$

$W \subseteq F_p^n$ 子空间, 若 W 对上述加法、数乘封闭

eg. $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ 求解 $\begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{2} & \bar{1} & \bar{2} \\ \bar{1} & \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix}$

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

$$\begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{2} & \bar{1} & \bar{2} \\ \bar{1} & \bar{0} & \bar{1} \end{pmatrix} \to \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & -\bar{3} & \bar{0} \\ \bar{0} & -\bar{2} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \end{pmatrix}$$

$$\begin{cases} x_1 + x_3 = \bar{0} \\ x_2 = \bar{0} \end{cases} \quad \text{解：} \begin{pmatrix} \bar{1} \\ \bar{0} \\ -1 \end{pmatrix} = \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{2} \end{pmatrix}$$

解空间维数 1.

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

hw 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。

证：数学归纳法：对 m 作归纳

$m=1$ 时，$(x+y)^p = x^p + y^p$ 成立.

假设 当 $m=k$ 时，$(x+y)^{p^k} = x^{p^k} + y^{p^k}$ 成立.

证当 $m=k+1$ 时，

$$\begin{aligned} (x+y)^{p^{k+1}} &= ((x+y)^{p^k})^p = (x^{p^k} + y^{p^k})^p \\ &= x^{p^{k+1}} + \binom{p}{1}(x^{p^k})(y^{p^k})^{p-1} + \cdots + y^{p^{k+1}} \\ &= x^{p^{k+1}} + y^{p^{k+1}}. \end{aligned}$$

□

hw 3. 环 R 的非零元素 x 称为幂零的，若存在 $n \in \mathbb{N}$, s.t. $x^n = 0$.

证：$\Rightarrow$ R 是任意有单位元的环，x 是幂零元，则 $1-x$ 是可逆元。

设 $x^m = 0$. 则 $1 - x^m = 1$

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

$\because x^{m-1}+x^{m-2}+\cdots+1 \in R$.

$\therefore (1-x)$ 存在逆元：$x^{m-1}+x^{m-2}+\cdots+1$

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。($\exists s\in\mathbb{Z}, s>1$ s.t. $s^2\mid m$).

"$\Longleftarrow$" 设 $m=s^2t$, $m>1$, $t\in\mathbb{Z}^+$

$\because st<m$ $\therefore \overline{st}\neq\overline{0}$ 且

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

$\therefore \overline{st}$ 是 $\mathbb{Z}_m$ 中幂零元。

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

即 $m\nmid x$, $m\mid x^n$.

下证 m 可被一个大于 1 的整数平方整除。

(反证). 假设上述结论不成立. 若 m 的素分解 $m=p_1p_2\cdots p_s$. p_i 是互不相同的素数

$\because m\mid x^n$ $\therefore \forall i$, $p_i\mid x^n$

$\because p_i$ 是素数 $\therefore p_i\mid x \Longrightarrow p_1p_2\cdots p_s\mid x$

$m\mid x$ 矛盾.

Lemma (上次作业题.)：设 G 为交换群, $a,b\in G$, $o(a)=m$, $o(b)=n$, 且 $(m,n)=1$, 则 $o(ab)=mn$.

hw 6. i) G: 有限交换群. $\exists a$ s.t. $ord(a)=(card(G))^n$ 即所有元素的阶的最小公倍数.

证：设 G 是有限交换群, a 是 G 中阶最大的元素 $o(a)=m$.

又设 $b\in G$, $o(b)=n$, 我们来证明 $n\mid m$.

若 $n\nmid m$, 则 $\exists$ 素数 p s.t. $p^s\mid n$, $p^t\mid m$, 但 $s>t$.

设 $n=up^s$, $m=vp^t$ (且 $(u,p)=(v,p)=1$).

$\Rightarrow$ $o(b^u)=p^s$, $o(a^{p^t})=v$.

由 Lemma 可知. $o(b^ua^{p^t})=p^sv>p^tv=m$

与 $o(a)$ 最大矛盾.

ii) G循环 $\Leftrightarrow$ $\forall m\in\mathbb{Z}^+$, $x^m=e$ 在G中最多有m个解。

"$\Rightarrow$" 设 $G=\langle a\rangle$, $|G|=o(a)=n$. 又设 $x=a^t$ 满足 $x^m=e$. 易见 $x^{(m,n)}=e$

[设 $u,v\in\mathbb{Z}$ s.t. $um+vn=(m,n)$ 则 $x^{(m,n)}=(x^m)^u(x^n)^v=ee=e$]

即 $a^{t(m,n)}=e$.

$\because$ $n\mid t(m,n)$, 即 $\frac{n}{(m,n)}\mid t$,

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

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

$\therefore$ $x^m=e$ 在G中解的数目 $\le(m,n)\le m$.

"$\Leftarrow$" 设a是(i)中所选元素

只要证明 $o(a)=|G|=n$.

设 $o(a)=m$. 对 $\forall b\in G$, $\because o(b)\mid o(a)$

$\therefore b^m=e$.

$\therefore$ $x^m=e$ 在G中有n个解.

由条件可知 $n\le m$. 又 $m\mid n$ $\Rightarrow$ $m=n$.

hw7. 证明 A_4 没有6阶子群

证: $|A_4|=12$. $\forall\ G\in A_4$, $ord(G)=1,2,3,4$

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

i) 若 $o(a)=6$. 则 A_4 中存在6阶元. 矛盾.

ii) 若 G 中所有元为三阶元(除e) 则 $|G|$ 为奇数. 矛盾

iii) 若 G 中所有元为二阶元(除e) 若怎么 e, a, b, ab 为子群.

所若 $c\neq a$ 且 $c\neq b$, $c\in G$, $ord(c)=2$.

若 $ac=ab$, 则 $b=c$.

若 $cb=ab$ 则 $c=a$ 则为 e, a, b, ab, ac, cb 为

iv). 若 G 中既有二阶也有三阶元.

$ord(a)=2$, $ord(b)=3$.

$a=(12)(34)$ $b=(123)$.

$ab=(134)$ $ba=(243)$ $b^{-1}=(132)$

$(ab)^{-1}=(143)$ $(ba)^{-1}=(234)$.

与 G 为六阶群矛盾。

eg. 环 R, $\forall x\in R$ 均有 $x^3=x$ 则 R 为交换环。

证: $\forall x\in R$

$(x+x)^3=(2x)^3=8x^3=8x=2x \Rightarrow 3x=-3x$.

$(x+1)^3=x^3+3x^2+3x+1=x+1+3x^2+3x=x+1 \Rightarrow 3(x^2+x)=0$

$\forall\ x, y\in R$

$(x+y)^3=x^3+x^2y+xyx+xy^2+yx^2+yxy+y^2x+y^3$

$=x^3+y^3=x+y$

$\Rightarrow x^2y+xyx+xy^2+yx^2+yxy+y^2x=0$ ①

$(x-y)^3 = x^3 - x^2y - xyx + xy^2 - yx^2 + yxy + y^2x - y^3$

$= x^3 - y^3 = x - y$

$\Rightarrow -x^2y - xyx + xy^2 - yx^2 + yxy + y^2x = 0$ ②

①+②得 $2(xy^2 + yxy + y^2x) = 0$ ③

③左乘 y $2(yxy^2 + y^2xy + y^3x) = 0$

$\Rightarrow 2(yxy^2 + y^2xy + yx) = 0$ ④

右乘 y $2(xy^3 + yxy^2 + y^2xy) = 0$

$\Rightarrow 2(xy + yxy^2 + y^2xy) = 0$ ⑤

④-⑤得 $2(yx - xy) = 0$ ⑥

又 $\because \forall x \in R \quad 3(x^2 + x) = 0$ 则 $\forall x, y \in R$

$3((x+y)^2 + (x+y)) = 0$

$\Rightarrow 3(x^2 + xy + yx + y^2 + x + y) = 0$

$\Rightarrow 3(x^2 + x) + 3(y^2 + y) + 3(xy + yx) = 0 \Rightarrow 3(yx + xy) = 0$

又 $\because 3x = -3x$ 对 $\forall x \in R$ 成立

$\therefore 3xy = -3yx = 3yx$

$\therefore 3(yx - xy) = 0$ ⑦

⑥+⑦得 $xy - yx = 0$ 由 x, y 任意性，R 交换环。

二、一元多项式

1. 构造
2. deg 系数

$$\deg(pq) \le \deg(p) + \deg(q)$$

3. 赋值定理
4. 多项式除法：余式定理
5. 多项式的根