

环和域回忆 设 $(R, +, 0, \cdot, 1)$ 是环如果 $S \subset R$ 且 $(S, +, 0, \cdot, 1)$ 是环. 则称 S 是 R 的子环例: $(\mathbb{Z}, +, 0, \cdot, 1)$ 是 $(\mathbb{Q}, +, 0, \cdot, 1)$ 的子环设 $A \in M_n(\mathbb{R})$ ~~非零~~
 $\mathbb{R}[A]$ 是 $M_n(\mathbb{R})$ 的交换子环.

命题: 设 $\varphi: R \rightarrow S$ 是环同态
则 $\text{im } \varphi$ 是 S 的子环

证: $\because \varphi: (R, +, 0_R) \rightarrow (S, +, 0_S)$
 群同态
 $\therefore (\text{im}(\varphi), +, 0_S)$ 是 $(S, +, 0_S)$
 的子群

设 $x, y \in \text{im}(\varphi)$
 则 $\exists u, v \in R$ 使得
 $x = \varphi(u), y = \varphi(v)$

$$xy = \varphi(u)\varphi(v) = \varphi(uv)$$

$\Rightarrow xy \in \text{im}(\varphi)$ [乘法封闭]

$$\therefore \varphi(1_R) = 1_S$$

$$\therefore 1_S \in \text{im}(\varphi)$$

运算规律由 R 中规律直接
 可得. $\square$

§3.3 零因子和可逆元

定义 设 a, b 是环 R 中的两个非零元
 且 $ab = 0$. 则称

二二

如果 $ab=0$, 则称

a 是左零因子

b 是右 " " " "

当 R 是交换环时, a, b 称为
零因子 (zero-divisor)

设 $x \in R$. 如果 $\exists y \in R$ 使得
 $xy = yx = 1$

则称 x 是可逆元, y 是 x 的逆
记为 x^{-1} .

注: 设 $u \in R$. 则 u 不可逆
就是左或右零因子, 又是可逆元

验证: 设 $uv=0$
 u 可逆 $\Rightarrow u^{-1}(uv)=0$
 $\Rightarrow (u^{-1}u)v=0$
 $\Rightarrow 1v=0$
 $\Rightarrow v=0$ ✓

例: $(\mathbb{Z}, +, 0, 1)$ 中无零因子
可逆元 ± 1

可逆元 ± 1
 $(\mathbb{Q}, +, \cdot, 0, 1)$ 无零因子
 非零元都可逆

$(\mathbb{Z}_n, +, \cdot, \bar{0}, \bar{1})$
 $\bar{k} \in \mathbb{Z}_n$ 可逆 $\Leftrightarrow \gcd(k, n) = 1$

证: $\bar{k}$ 是零因子 $\Leftrightarrow 1 < \gcd(k, n) < n$
 设 $g = \gcd(n, k)$

$$\boxed{n = mg}$$

" $\Rightarrow$ " 设 $\bar{k}$ 是零因子, 则 $\bar{k}$ 不是可逆
 且 $\bar{k} \neq \bar{0}$. $\Rightarrow 1 < \gcd(k, n) < n$

" $\Leftarrow$ " 设 $\bar{k}$ 不是可逆, 则 $\bar{k} \neq \bar{0}$

设 $l = \text{lcm}(n, k)$

$$l = \frac{kn}{g} = mk$$

$$n \mid l \quad \bar{k} = \bar{0} \Rightarrow m\bar{k} = \bar{0} \Rightarrow \bar{k} \text{ 是零因子.}$$

$\mathbb{Z}_n$ 中的元素 $\begin{cases} \text{可逆} \\ \text{零因子} \\ \bar{0} \end{cases}$

例: 设 $A \in M_n(\mathbb{R})$, 非零
 证明 A 是左或右零因子
 $\Leftrightarrow \text{rank}(A) < n$.

$$\text{证毕} \quad \Leftrightarrow \text{rank}(A) < n.$$

证: " $\Rightarrow$ " 设 A 是右零因子

则 $\exists B \in M_n(\mathbb{R}), B \neq O$

$$\text{使得} \quad AB = O$$

由 Sylvester 秩不等式

$$\text{rank}(AB) \geq \text{rank}(A) + \text{rank}(B) - n$$

$$\Rightarrow \text{rank}(A) + \text{rank}(B) \leq n$$

$$\because \text{rank}(B) > 0 \quad \therefore \text{rank}(A) < n$$

A 是右零因子时. 证毕

$\Leftarrow$ 设 $\text{rank}(A) < n$

则 $\exists \alpha_1, \dots, \alpha_n \in \mathbb{R}$ 不全为零

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \vec{0}_n$$

$$\text{令 } B = \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ \alpha_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_n & 0 & \dots & 0 \end{pmatrix}$$

$$AB = (A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, A \vec{0}_n, \dots, A \vec{0}_n) = O_n$$

$\Rightarrow A$ 是右零因子

$$L(A^t)$$

$\therefore \text{rank}(A) = \text{rank}(A^t)$
 $\therefore$ 由上述结论可知 $\exists$ 非零矩阵
 $C \in M_n(\mathbb{R})$ 使得

$$A^t C = 0$$

$$\Rightarrow C^t A = 0$$

$\Rightarrow A$ 是右零因子

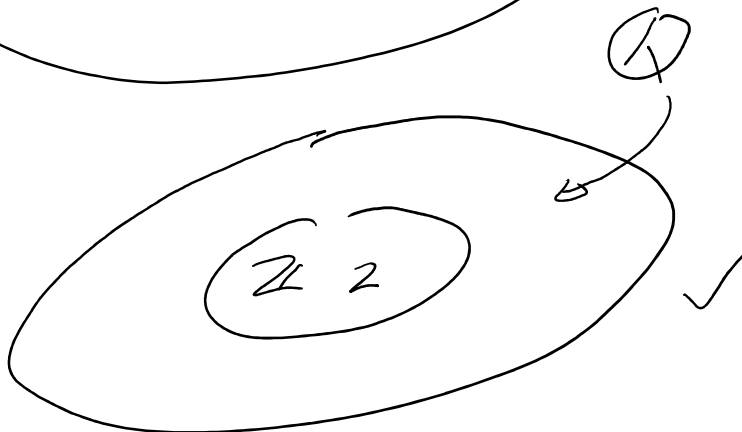
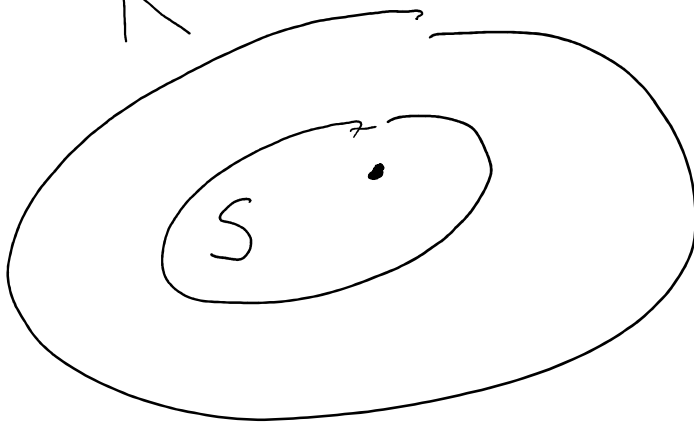
可逆元

左且右零因子

$M_n(\mathbb{R})$

0

R



例: 设 $A \in M_n(\mathbb{R})$, $A \neq 0$
 $\dots$ 非零

例: 设 $\Gamma \sim \dots$

设 $B \in \mathbb{R}[A]$ 非零

证: B 在 $\mathbb{R}[A]$ 可逆
 $\Leftrightarrow \text{rank}(B) = n$

证: 设 m 是最小的正整数使得
 $\exists \alpha_0, \alpha_1, \dots, \alpha_m \in \mathbb{R}$ 不全为 0
 $\alpha_0 B^0 + \alpha_1 B + \dots + \alpha_m B^m = 0$

由矩阵求逆的多项式法

B 可逆 $\Leftrightarrow \alpha_0 \neq 0$

此时 $\alpha_1 B + \dots + \alpha_m B^m = -\alpha_0 E$

$$-\alpha_0^{-1} \alpha_1 B + \dots + (-\alpha_0^{-1} \alpha_{m-1}) B^{m-1} + (-\alpha_0^{-1} \alpha_m) B^m = E$$

$$B \left(-\alpha_0^{-1} \alpha_1 E + \dots + (-\alpha_0^{-1} \alpha_{m-1}) B^{m-2} + (-\alpha_0^{-1} \alpha_m) B^{m-1} \right) = E$$

$\Leftrightarrow B$ 可逆

$$B^{-1} \in \mathbb{R}[B] \subset \mathbb{R}[A] \quad (\because B \in \mathbb{R}[A])$$

$\Rightarrow B^{-1}$ 在 $\mathbb{R}[A]$ 中 $\square$

$$\Rightarrow B^{-1} \text{ 在 } \mathbb{R}[A] \text{ 中} \quad (*)$$

注: B 是 $\mathbb{R}[A]$ 中的零因子
 $\Leftrightarrow \text{rank}(B) < n$

命题: 设 U_R 是环 R 中所有可逆元的集合. 则 $(U_R, \cdot, 1)$ 是群

证: 设 $x, y \in U_R$
 xy 也可逆 这是因为

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

$$\Rightarrow xy \in U_R \quad \text{乘法封闭}$$

结合律自然成立

$$1 \in U_R \quad \checkmark$$

设 x^{-1} 逆元是 x 故 $x^{-1} \in U_R$
 $\Rightarrow (U_R, \cdot, 1)$ 是群.

例: $U_{\mathbb{Z}} = \{1, -1\}$

$$U_{\mathbb{Q}} = \{\text{非零有理数}\} =: \mathbb{Q}^{\times}$$

$$U_{\mathbb{Q}} = \{\text{非零有理数}\} =: \mathbb{Q}^*$$

$$U_{\mathbb{Z}_n} = \{\bar{k} \mid \gcd(k, n) = 1\}$$

特别 设 $n = p$ 是素数

$$U_{\mathbb{Z}_p} = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\} \quad \begin{matrix} \text{共 } p-1 \\ \text{个元素} \end{matrix}$$

换言之

$\mathbb{Z}_p$ 中的非零元都可逆

例: (Fermat 小定理) 设 p 是素数
 $m \in \mathbb{Z} \setminus \{0\}$ 且 $p \nmid m$

$$m^{p-1} \equiv 1 \pmod{p}$$

证: $U_{\mathbb{Z}_p}$ 中有 $p-1$ 个元素

由 Lagrange 定理 (的性质)

设 G 是有限群, 则 $\forall g \in G$

$$g^{\text{card}(G)} = e$$

$$\forall m. \quad \bar{m}^{p-1} = \bar{1} \quad \left(\begin{matrix} \bar{m} \neq \bar{0} \\ \bar{m} \in U_{\mathbb{Z}_p} \end{matrix} \right)$$

$$m^{p-1} \equiv 1 \pmod{p} \quad \square$$

$$\underbrace{m^{p-1} \equiv 1 \pmod{p} \quad | \quad p \nmid m}$$

推广: $\forall m \in \mathbb{Z}$

$$\underline{m^p \equiv m \pmod{p}}$$

证: 如果 m 不是零且不被 p 整除
 则 $m^{p-1} \equiv 1 \pmod{p}$ (FLT)

$$\begin{aligned} & \text{即 } p \mid (m^{p-1} - 1) \\ \Rightarrow & p \mid (m^p - m) \Rightarrow m^p \equiv m \pmod{p} \end{aligned}$$

若 $p \mid m$, 则 $m^p \equiv m \pmod{p}$
 仍然成立. $\square$

§3.4 消去律

设 $\underline{xy = xz} \Rightarrow y = z$

如果 x 可逆, 则

$$x^{-1}(xy) = x^{-1}(xz)$$

$$1y = 1z$$

$$y = z$$

命题: 设 R 是环, $a, b \in R \setminus \{0\}$
 $x, y \in R$ 则

$ax = ay \Rightarrow x = y$ 或 $bx = by \Rightarrow x = y$

$x, y \sim$

(i) (左消去律) 如果 a 不是左零因子
 则 $ax = ay \Rightarrow x = y$

(ii) (右消去律). 如果 b 不是右零因子
 则 $xb = yb \Rightarrow x = y$.

证: (i) $ax = ay$
 $\Rightarrow ax - ay = 0$
 $\Rightarrow a(x - y) = 0$
 $\therefore a$ 不是左零因子 $\therefore x - y = 0$
 $\Rightarrow x = y$.

(ii) 类似 ✓

定义: 设 D 是交换环. 如果
 D 中没有零因子, 则 D 称为
 整环 (domain)

推论: 整环中消去律成立
 即 $\forall a, x, y \in D, a \neq 0$
 $ax = ay \Rightarrow x = y$.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

2.5 环的性质.

3.5 环的特征.

c characteristic

定义: 设 $(R, +, 0, \cdot, 1)$ 是环,
如果 $\text{ord}(1)$ 在群 $(R, +, 0)$ 有限
则 R 特征定义为 $\text{ord}(1)$
否则 R 特征定义为 0
环 R 的特征 记为 $\text{char}(R)$

例: $\text{char}(\mathbb{Z}) = 0$
 $\text{char}(\mathbb{Z}_n) = n$

引理 设环 R 的特征 $n > 0$, $m \in \mathbb{Z}$
 $r \in R$

如果 $n \mid m$, 则 $mr = 0$

证: 设 $m = kn$. 其中 k 是整数

$$mr = (kn)r = kn(r \cdot 1)$$

$$= (kr)(\underline{n \cdot 1})$$

$$= (kr) \cdot 0$$

$$= 0$$

[分配律]

证

命题 (freshmen's dream)

设 R 的特征是素数 p

例 1.7...

设交换环 R 的特征是素数 p

则 $\forall x, y \in R$

$$(x+y)^p = x^p + y^p$$

证: 因为 R 是交换环, 所以二项式定理成立, 故

$$(x+y)^p = \sum_{k=0}^p \binom{p}{k} x^{p-k} y^k$$

$$= x^p + \left(\sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k \right) + y^p$$

在第一节中, 我们证明了 $p \mid \binom{p}{k}$
 $k \in \{1, 2, \dots, p-1\}$

由上述引理和 $\text{char}(R) = p$

$$(x+y)^p = x^p + y^p$$

例: 设 p 是素数, $\forall x, y \in \mathbb{Z}_p$

$$(x+y)^{\textcircled{p}} = x^{\textcircled{p}} + y^{\textcircled{p}}$$

$$(\because \text{char}(\mathbb{Z}_p) = p)$$

$$\hookrightarrow \text{在 } (R + D_R, \cdot, \uparrow_R)$$

命题: 设 $(R, +, 0_R, \cdot, 1_R)$
 和 $(S, +, 0_S, \cdot, 1_S)$ 是两个环
 $\varphi: R \rightarrow S$ 环同态

证: (i) $\text{char}(R)=0$ 或 $\text{char}(R) \geq \text{char}(S) > 0$
 (ii) φ 又是单射, $\text{char}(R)=\text{char}(S)$

证: 设 $k = \text{char}(R)$, $m = \text{char}(S)$
 (i) 设 $k > 0$. 则 $\underline{k \cdot 1_R = 0_R}$

$$0_S = \varphi(0_R) = \varphi(k \cdot 1_R)$$

$$= \varphi(\underbrace{1_R + \dots + 1_R}_k)$$

$$= \underbrace{\varphi(1_R) + \dots + \varphi(1_R)}_k$$

$$= \underbrace{1_S + \dots + 1_S}_k$$

$$= k \cdot 1_S$$

$$\text{即 } k \cdot 1_S = 0_S$$

$$\text{于是 } \text{ord}(1_S) \neq 0 \\ \text{ord}(1_S) \mid k \Rightarrow \text{char}(S) \leq \text{char}(R)$$

$$\text{ord}(1_S) \mid k \Rightarrow \text{char}(S) \leq \text{char}(R)$$

(ii) 设 $m=0$. 由 (i) $k=0$

设 $m>0$.

$$\varphi(m \cdot 1_R) = \varphi(\underbrace{1_R + \dots + 1_R}_m)$$

$$= \underbrace{\varphi(1_R) + \dots + \varphi(1_R)}_m$$

$$= \underbrace{1_S + \dots + 1_S}_m = 0_S$$

$$\text{又有 } \varphi(0_R) = 0_S$$

$$\therefore \varphi \text{ 是单射 } \therefore m \cdot 1_R = 0_R$$

$$\Rightarrow k \mid m \Rightarrow k = m \text{ (由 (i))}$$

命题: 设 D 是整环, 则

$\text{char}(D)$ 要么是零

要么是素数

证: 设 $m = \text{char}(D)$. 只要证明

m 不可能是合数即可

假设 $m = kl$ 其中 $k, l \in \mathbb{Z}^+ \setminus \{1\}$

$$0 = \underbrace{m \cdot 1}_{\substack{\text{由 (i)} \\ \text{由 (ii)}}} = (kl)(1 \cdot 1) = (k \cdot 1)(l \cdot 1)$$

$$k \cdot 1 = 0 \text{ 或 } l \cdot 1 = 0$$

$0 = m \cdot 1 = (k \cdot 1) \cdot 1$
 $\therefore D$ 是整环 $\therefore k \cdot 1 = 0$ 或 $l \cdot 1 = 0$
 又有 $1 < k < m$ $1 < l < m$
 与 $m = \text{char}(D)$ 矛盾.

4 域 (field)

§4.1 域的定义和基本性质

定义: 设 F 是交换环, 如果 F 中任何非零元都可逆. 则称 F 是域.

注 域必然是整环.

例 $(\mathbb{Q}, +, 0, \cdot, 1)$, $\mathbb{R}$, $\mathbb{C}$ 是域.

如果 p 是素数, $\mathbb{Z}_p$ 也是域.

$$\text{char}(\mathbb{Q}) = 0, \text{char}(\mathbb{R}) = 0$$

$$\text{char}(\mathbb{Z}_p) = p$$

命题: 设 F 和 K 是域

$$\varphi: (F, +, 0_F, \cdot, 1_F) \rightarrow (K, +, 0_K, \cdot, 1_K)$$

的环同态
则 ϕ 单 (ϕ 是嵌入)

证: 注意到 ϕ 是 $(F, +, 0_F) \rightarrow (K, +, 0_K)$
的环同态. 故只要证 $\ker \phi = \{0_F\}$

$$\phi(x) = 0_K \Rightarrow x = 0_F$$

反证: 假设 $x \neq 0$ 且 $\phi(x) = 0_K$

$$\phi(x^{-1}x) = \phi(1_F) = 1_K$$

$$\parallel$$

$$\phi(x^{-1})\phi(x) = \phi(x^{-1})0_K = 0_K$$

$$\Rightarrow 1_K = 0_K$$

与环的定义矛盾 $\square$

§4.2 域上的线性代数

第一, 二章中关于线性方程组

矩阵, 线性空间, 子空间, 线性映射
行列式的结论, 当把 $\mathbb{R}$ 换成任意
域 F 中都成立, 除非用了 $\underline{\mathbb{Z} \neq 0}$

$\mathbb{Z}_2$ 是域

$$\phi: \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$$

$$x \mapsto x^2$$

$$x+y$$

(0) $\varphi: \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto x^2$

设 $\alpha, \beta \in \mathbb{Z}_2$

$$\begin{aligned}\varphi(\alpha x + \beta y) &= (\alpha x + \beta y)^2 \\ &= \alpha^2 x^2 + \beta^2 y^2 \quad (\text{费马小定理}) \\ &= \alpha \varphi(x) + \beta \varphi(y) \quad (\text{Fermat 小定理})\end{aligned}$$

(1) A 是斜对称矩阵. 则
 A 中对角线上的元素都等于 0

$$B = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \in M_2(\mathbb{Z}_2)$$

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

故 B 是斜对称

(2) 设 $A \in M_n(F)$ 中 A 的两行或两列相同

则 $\det(A) = 0$

此结论对特征为 2 的域

仍成立

例: 设 $A = \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{2} & \overline{4} \\ \overline{1} & \overline{4} & \overline{2} \end{pmatrix} \in M_3(\mathbb{Z}_5)$

求以 A 为系数矩阵的齐次线性方程组的解空间.

$$\begin{aligned} A &\rightarrow \left(\begin{array}{c|c|c} \overline{1} & \overline{2} & \overline{3} \\ \hline 0 & \overline{2} & \overline{4} \\ \hline 0 & 2 & 4 \end{array} \right) \\ &\rightarrow \left(\begin{array}{c|c|c} \overline{1} & \overline{2} & \overline{3} \\ \hline 0 & \overline{2} & \overline{4} \\ \hline 0 & \overline{0} & \overline{0} \end{array} \right) \end{aligned}$$

$$\begin{cases} x_1 + \overline{2}x_2 + \overline{3}x_3 = \overline{0} \\ \overline{2}x_2 + \overline{3}x_3 = \overline{0} \end{cases}$$

$$x_2 = \overline{2}^{-1}(\overline{-3})x_3 = \overline{3}x_3$$

$$x_1 = x_3$$

$$\text{rank}(A) = 2.$$

$$\text{sol}(H_A) = \left\langle \begin{pmatrix} \overline{1} \\ \overline{3} \\ \overline{1} \end{pmatrix} \right\rangle.$$

$$\overline{1} + \overline{1} = \overline{0}$$

$$2 \neq 0$$

$$\overline{2} = \overline{0}$$