

循环群和环

2022年12月5日 6:48

回忆 设 G 是群. $g \in G$, $\text{ord}(g) = k$

(i) 如果 $k = \infty$. 则 $\forall i, j \in \mathbb{Z}$, $g^i = g^j \Leftrightarrow i = j$

$$\text{于是 } \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

(ii) 如果 $k < \infty$. 则 $\forall i, j \in \mathbb{Z}$, $g^i = g^j \Leftrightarrow k \mid (i - j)$

$$\text{于是 } \langle g \rangle = \{e, g, g^2, \dots, g^{k-1}\}$$

$$(iii) \text{ord}(g^m) = \frac{k}{\gcd(k, m)} = \frac{\text{lcm}(k, m)}{m}$$

§2.7 子循环群的结构

定义 设 G 是群, $g \in G$

$\langle g \rangle$ 称 g 在 G 中生成的
循环子群. 如果 $\exists h \in G$
使得 $G = \langle h \rangle$. 则称 G 是循环群

$$\text{例: } (\mathbb{Z}, +, 0) = \langle 1 \rangle = \langle -1 \rangle$$

$$\underline{(\mathbb{Z}_n, +, \bar{0}) = \langle \bar{1} \rangle, n \geq 1}$$

$$\bar{k} \in \mathbb{Z}_n \text{ 则}$$

$$\langle \bar{k} \rangle \leq \mathbb{Z}_n \Leftrightarrow \text{ord}(\bar{k}) = n$$

$$\langle \bar{k} \rangle = \{\bar{0}, \bar{k}, 2\bar{k}, \dots, (n-1)\bar{k}\} \subseteq \mathbb{Z}_n$$

$$\langle \bar{k} \rangle = \{ \bar{0}, \bar{k}, 2\bar{k}, \dots, (n-1)\bar{k} \} \quad \text{有 } n \text{ 个元素}$$

$$\Rightarrow \langle \bar{k} \rangle = \mathbb{Z}_n$$

例: 如果 p 是素数, 群 G 只有 p 个元素, 则 G 是循环群

证: 设 $g \in G$, 且 $g \neq e$

$$\text{card}(\langle g \rangle) > 1$$

由 Lagrange 定理

$$1 < \text{card}(\langle g \rangle) \mid \text{card}(G) = p$$

$$\because p \text{ 是素数} \quad \therefore \text{card}(\langle g \rangle) = \text{card}(G)$$

$$\langle g \rangle = G. \quad \square$$

命题 (循环群的结构)

设 $(G, \cdot, e)$ 是循环群, 且 $\text{card}(G) > 1$

(i) 如果 $\text{card}(G) = \infty$, 则

$$G \cong (\mathbb{Z}, +, 0)$$

(ii) 如果 $\text{card}(G) = n < \infty$, 则

$$G \cong (\mathbb{Z}_n, +, \bar{0})$$

设 $G = \langle g \rangle$

$$\phi: \mathbb{Z} \longrightarrow G$$

证 (i)

$$\varphi: \mathbb{Z} \longrightarrow G$$

$$m \longmapsto \underline{g^m}$$

$$\begin{aligned}\varphi(m+k) &= \underline{g^{m+k}} \\ &= \underline{g^m g^k} \\ &= \varphi(m) \varphi(k)\end{aligned}$$

φ 是同态

满射由 G 是循环群而 g 是生成元可得

$$\text{设 } \varphi(m) = \varphi(k), \text{ 则 } g^m = g^k$$

$$\therefore \text{card}(G) = \infty \quad \therefore \text{ord}(g) = \infty$$

$$\Rightarrow m = k.$$

故 φ 是单的 $\Rightarrow \varphi$ 是同构

(ii) 定义

$$\varphi: \mathbb{Z}_n \longrightarrow G$$

$$\overline{m} \longmapsto \underline{g^m}$$

验证良定义 设 $\overline{m} = \overline{m'}$

$$\text{则 } m \equiv_n m' \quad (m \equiv m' \pmod{n})$$

$$m' = m + kn, \quad \text{其中 } k \text{ 是整数}$$

$$g^{m'} = g^{m+kn} = g^m \cdot (g^n)^k$$

$$g^{m'} = g^{m+k''} = g^m \cdot (g^n)$$

$$\therefore \text{Card}(G) = n \text{ 且 } G = \langle g \rangle$$

$$\text{ord}(g) = n \Rightarrow g^n = e$$

$$\Rightarrow g^{m'} = g^m$$

证定义 ✓

$$\varphi(\bar{m} + \bar{k}) = \varphi(\overline{m+k})$$

$$= g^{m+k} = g^m g^k$$

$$= \varphi(\bar{m}) \varphi(\bar{k}) \quad \text{同态} \checkmark$$

验证 φ 是单射

设 $\varphi(\bar{m}) = \varphi(\bar{k})$. 则

$$g^m = g^k \Rightarrow n \mid (m-k)$$

$$\Rightarrow m \equiv k \pmod{n}$$

$$\Rightarrow \bar{m} = \bar{k} \quad \text{于是} \varphi \text{ 单}$$

φ 满足验证 $\Rightarrow \varphi$ 是同构

例 设 G 是群 $\text{Card}(G) = p$, p 素数

$$\text{则 } G \cong (\mathbb{Z}_p, +, \bar{0})$$

$$\triangleq (\mathbb{Z}_5, +, \bar{0})$$

例. 设 $(G, \cdot, e)$ 是循环群. 则
它的子群也是循环群.

它的子群也是循环群.

证: 由循环群的结构可知

我们只要证明

$(\mathbb{Z}, +, 0)$ 和 $(\mathbb{Z}_n, +, \bar{0})$

的子群都是循环群

① 证 $(\mathbb{Z}, +, 0)$ 的子群都是循环的

设 A 是 $\mathbb{Z}$ 的子群
 $\text{card}(A) > 1$

取 A 中最小的正整数 m

断言 $A = \langle m \rangle$

断言的证明: $\langle m \rangle \subset A$

设 $k \in A$. 由带余除法可知

$$k = qm + r, \quad \begin{array}{l} q \in \mathbb{Z} \\ r \in \{0, 1, \dots, m-1\} \end{array}$$

$$qm \in \langle m \rangle \Rightarrow r \in \langle m \rangle$$

$$\therefore 0 \leq r < m$$

$$\therefore r = 0 \Rightarrow k = qm \in \langle m \rangle$$

$$\boxed{A \subset \langle m \rangle}$$

同理: 设 A 是 $\mathbb{Z}_n$ 的子群

定理: 设 A 是 $\mathbb{Z}_n$ 的子群
 $\text{card}(A) > 1$. 则 $\exists$ 最小正整数
 $m \in \{1, 2, \dots, n-1\}$ 使得 $\bar{m} \in A$

证: $\langle \bar{m} \rangle = \langle A \rangle$
 $\langle \bar{m} \rangle \subset \langle A \rangle \checkmark$

设 $\bar{k} \in A$

$$k = qm + r, \quad r \in \{0, 1, \dots, m-1\}$$

$$\bar{k} = \bar{q} \bar{m} + \bar{r}$$

$$\Rightarrow \bar{r} \in A.$$

$$\Rightarrow \underbrace{r=0}_{r \text{ 为 } A \text{ 中元素}} \Rightarrow k = qm \Rightarrow \bar{k} = \bar{q} \bar{m} \Rightarrow \bar{k} \in \langle \bar{m} \rangle$$

$$\langle \bar{m} \rangle = A \quad \square$$

设 S 是所有正整数

$$(S, +, 0) \simeq (\mathbb{Z}, +, 0)$$

$$S \subsetneq \mathbb{Z}$$

2.8. Cayley 定理

引理 设 $\phi: G \rightarrow H$ 群同态

如果 ϕ 是单射, 则 $G \simeq \text{im}(\phi)$

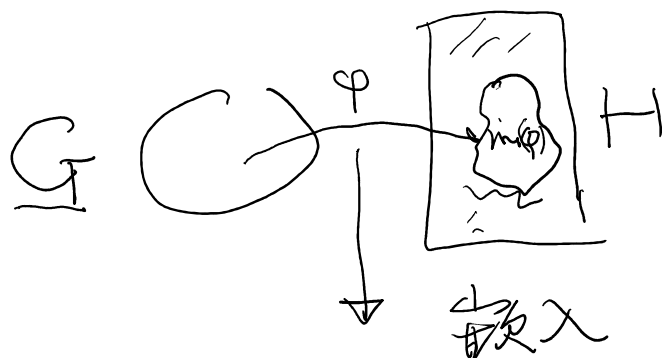
证: $\square$

如果 ϕ 是同构, 则

证: $\phi: G \rightarrow \text{im}(\phi)$ 是群同态
($\text{im}(\phi)$ 是 H 子群)

$\therefore \phi$ 是满射且单射

$\therefore \phi$ 是同构.



$$G \not\subseteq H$$

引理 设 $\phi: (G, \cdot, e) \rightarrow (H, *, \varepsilon)$
是同态. 则 ϕ 单 $\Leftrightarrow \begin{cases} \phi(g) = \varepsilon \\ \text{则 } g = e \end{cases}$

(习题)

回忆: 设 X 是非空集

$$T_X = \{f \mid f: X \rightarrow X\}$$

$(T_X, \circ, \text{id}_X)$ 是群.

T_X 称为 X 上的变换群

设 G 是群, 则

1x 1-
Cayley 定理: 设 G 是群, 则
 G 可以嵌入到 T_G 中

证: 定义 $\varphi: G \longrightarrow T_G$
 $g \longmapsto L_g$

$$L_g: G \longrightarrow G$$

$$x \longmapsto gx$$

验证 φ 是单同态

设 $g, h \in G$

$$\varphi(gh) = L_{gh} = L_g \circ L_h$$

$$L_{gh}: G \longrightarrow G$$

$$x \longmapsto (gh)x$$

$$\varphi(g) \circ \varphi(h)$$

$$L_g \circ L_h(x) = L_g(L_h(x))$$

$$= L_g(hx)$$

$$= g(hx) = (gh)x = L_{gh}(x)$$

$$L_g \circ L_h = L_{gh}$$

于是 φ 是同态

下面验证 φ 是单射

$$\varphi(g) = \text{id}_G = L_g$$

$$1 \cdot 1 = e$$

$$L_{g(e)} = e$$

$$\begin{matrix} \parallel \\ ge \\ \parallel \\ g \end{matrix}$$

$$\Rightarrow g = e$$

故由上述引理 (或者习题), ϕ 单射

$$\Rightarrow G \cong \text{im}(\phi) \subset T_G.$$

推论: 设 G 是群 $n = \text{card}(G) < \infty$
 则 G 可以嵌入到 (S_n) 中

回忆 $S_n = \langle \underbrace{(12)}, \underbrace{(12 \dots n)} \rangle^V$

§3 环 (Ring)

§3.1 定义和基本性质

定义: 五元组 $(R, +, \cdot, 0, 1)$

其中 R 是集合, $+$, $\cdot$ 是 R 上 $u \cdot v = uv$

运算, $0, 1 \in R$, $0 \neq 1$.

称为环 (含么环)

(i) $(R, +, 0)$ 是交换群

如半

$$\left\{ \begin{array}{l} \forall x, y, z \in R \\ x + y = y + x \\ (x + y) + z = x + (y + z) \\ x + 0 = x \\ x + (-x) = 0 \end{array} \right.$$

(i) ...

(ii) $(R, 1)$ 是含么半群

$$\begin{cases} x + (-x) = 0 \\ (xy)z = x(yz) \\ x \cdot 1 = 1 \cdot x = x \end{cases}$$

(iii) 分配律

$$\begin{aligned} (x+y)z &= xz + yz \\ x(y+z) &= xy + xz \end{aligned}$$

如果 $(R, \cdot, 1)$ 是交换. 则称

R 是交换环.

例: 交换环 $(\mathbb{Z}, +, 0, \cdot, 1)$
 $(\mathbb{Z}_n, +, \bar{0}, \cdot, \bar{1})$

$\mathbb{R}$
 $\mathbb{Q}$ $(\mathbb{Q}, +, 0, \cdot, 1)$
 $\mathbb{M}_n(\mathbb{R})$ 非交换环 $(\mathbb{M}_n(\mathbb{R}), +, \mathbf{O}, \cdot, E)$
 $n > 1$

$(R, +, \underline{0}, \cdot, \underline{1})$

例: 设 $\uparrow$ 是环, R

(i) $\forall x \in R, 0x = x0 = 0.$

(ii) $\forall x, y \in R$
 $(-x)y = x(-y) = -(xy)$

$(-x)(-y) = xy$

(iii) $\forall x \in R, (-1)x = x(-1) = -x.$

证: (i) $0x = (0+0)x \stackrel{(i)}{=} 0 \cdot x + 0x$
 $\Rightarrow 0 = 0x$ $\hookrightarrow$ 分配律
 同理 $\underline{x0 = 0}$

(ii) $x + (-x) = 0$

$(x + (-x))y \stackrel{(i)}{=} 0 \cdot y = 0$

$xy + (-x)y = 0$

$\Rightarrow (-x)y = -xy$ [加法逆元] $\left[\frac{1}{2} \right]$

同理 $x(-y) = -xy$

$(-x)(-y) = - (x(-y)) = -(-xy) = xy$

(iii) $1 + (-1) = 0$

$(1 + (-1))x = 0 \cdot x = 0$

$x + (-1)x = 0$

$\Rightarrow (-1)x = -x$ $\checkmark$

定理 (广义分配律)

设 R 是环, $x_1, \dots, x_m, y_1, \dots, y_n \in R$

证 $\left(\sum_{i=1}^m x_i \right) \left(\sum_{j=1}^n y_j \right)$

$= \sum_{i=1}^m \sum_{j=1}^n x_i y_j$ $\leftarrow \neq y_j x_i$
 $= \sum_{j=1}^n \sum_{i=1}^m x_i y_j$

$$j=1 \quad i=1$$

证:

先证 $\mathbb{R}$. $\forall x \in \mathbb{R}$

$$x(y_1 + y_2 + \dots + y_n) = xy_1 + xy_2 + \dots + xy_n$$

对 n 直接归纳即可

$$\begin{aligned} \text{设 } x &= \sum_{i=1}^m x_i \\ \left(\sum_{i=1}^m x_i \right) \left(\sum_{j=1}^n y_j \right) &= x \sum_{j=1}^n y_j \\ &= \sum_{j=1}^n x y_j \\ &= \sum_{j=1}^n \left(\sum_{i=1}^m x_i \right) y_j \quad [\text{分配律}] \\ &= \sum_{j=1}^n \sum_{i=1}^m x_i y_j \\ &= \sum_{i=1}^m \sum_{j=1}^n x_i y_j \quad \checkmark \end{aligned}$$

类似: 设 $m, n \in \mathbb{Z}, x, y \in \mathbb{R}$

$$\text{则 } (mx)(ny) = (mn)(xy)$$

证: $m > 0, n < 0$

$$\begin{aligned} (mx)(ny) &= \underbrace{(x + \dots + x)}_m \underbrace{((-y) + \dots + (-y))}_{-n} \\ &= \sum_{i=1}^m \sum_{j=1}^{-n} x(-y) \end{aligned}$$

$$= (m+n) x(-y)$$

$$= -(mn) x(-y)$$

$$= \underline{-(mn)} (-xy) = mn(xy)$$

例子情形自己验证,

$$\text{证 } (mx)(ny) = (mn)(xy)$$

$$= m(nxy) = n(m(xy))$$

§3.2. 环同态和子环

定义: 设 $(R, +, \cdot, 1_R)$

$(S, +, \cdot, 1_S)$

是两个环. $\varphi: R \rightarrow S$ 满足

(i) φ 是 $(R, +, \cdot)$ 到 $(S, +, \cdot)$ 的群同态
(即 $\forall x, y \in R \quad \varphi(x \pm y) = \varphi(x) \pm \varphi(y)$)

(ii) $\varphi(xy) = \varphi(x) \varphi(y)$ [保持乘法]

(iii) $\boxed{\varphi(1_R) = 1_S}$ [保持乘法单位]

则称 φ 是从 R 到 S 的环同态

如果 φ 是双射, 则称 φ 是环同构.

例: $\pi: \mathbb{Z} \rightarrow \underline{\mathbb{Z}_n}$ 是环同态

$$\forall x, y \in \mathbb{Z}$$

$$\begin{aligned}\pi(x+y) &= \overline{x+y} = \bar{x} + \bar{y} \\ &= \pi(x) + \pi(y) \quad [\text{保持加法}]\end{aligned}$$

$$\pi(xy) = \overline{xy} = \bar{x} \bar{y} = \pi(x)\pi(y) \quad [\text{保持乘法}]$$

$$\pi(1) = \bar{1} \quad \forall \mathbb{Z}_n \text{ 中的单位元}$$

$$\Rightarrow \pi \text{ 是同态.}$$

例: 设 $C \in GL_n(\mathbb{R})$ 定义

$$\begin{aligned}\varphi_C: M_n(\mathbb{R}) &\longrightarrow M_n(\mathbb{R}) \\ A &\longmapsto C^{-1}AC\end{aligned}$$

证明: φ_C 是同构

证: 设 $A, B \in M_n(\mathbb{R})$

$$\varphi_C(A+B)$$

$$= C^{-1}(A+B)C$$

$$= C^{-1}AC + C^{-1}BC$$

$$= \varphi_C(A) + \varphi_C(B)$$

保持加法

$$\begin{aligned}
 \varphi_C(AB) &= C^{-1}ABC \\
 &= C^{-1}A \underline{C} C^{-1}B C \\
 &= (C^{-1}AC)(C^{-1}BC) \\
 &= \varphi_C(A)\varphi_C(B)
 \end{aligned}$$

保持乘法

$$\varphi_C(E) = C^{-1}EC = E$$

φ_C 是环同态.

$$\text{设 } \varphi_C(A) = \varphi_C(B)$$

$$\text{则 } C^{-1}A \underline{C} = C^{-1}B \underline{C}$$

$$\Rightarrow C^{-1}A \underline{C} C^{-1} = C^{-1}B \underline{C} C^{-1}$$

$$\Rightarrow C^{-1}A = C^{-1}B$$

$$\Rightarrow C C^{-1}A = C C^{-1}B$$

$$\Rightarrow A = B. \quad \text{证}$$

$$\begin{aligned}
 \varphi(CAC^{-1}) &= \underline{C^{-1}CAC^{-1}} \underline{C} \\
 &= A \quad \text{证}
 \end{aligned}$$

定义 设 $(R, +, \cdot, 0_R, 1_R)$ 是环
 $S \subset R$. 如果

$$(S, +, \cdot, 1_R)$$

是环, 则称 S 是 R 的子环 (subring)

例 $(\mathbb{Z}, +, 0, \cdot, 1) \stackrel{W}{=} (\mathbb{Q}, +, 0, \cdot, 1)$ 的子环.

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

$$[A] := \left\{ \sum_{i=0}^k \alpha_i A^i \mid k \in \mathbb{N}, \alpha_i \in \mathbb{R} \right\}$$

验证: $[A]$ 是 $M_n(\mathbb{R})$ 的子环且交换

证: 验证: $([A], +, \cdot)$ 是交换环

$$\text{设 } B = \sum_{i=0}^k \alpha_i A^i, C = \sum_{j=0}^l \beta_j A^j$$

其中 $\alpha_i, \beta_j \in \mathbb{R}$

$$B - C = \sum_{i=0}^k \alpha_i A^i + \sum_{j=0}^l (-\beta_j) A^j$$

$$\in [A]$$

故 $([A], +, \cdot)$ 是环

验证乘法封闭

$$BC = \left(\sum_{i=0}^k \alpha_i A^i \right) \left(\sum_{j=0}^l \beta_j A^j \right)$$

$$= \sum_{i=0}^k \sum_{j=0}^l (\alpha_i A^i) (\beta_j A^j)$$

$$= \sum_{i=0}^k \sum_{j=0}^l \alpha_i \beta_j A^{i+j} \quad \left[\begin{array}{l} \text{矩阵乘法结合律} \\ \text{的性质} \end{array} \right]$$

$$\therefore BC \in R[A]$$

$$\square BC = CB \quad \begin{array}{l} \text{非空即 } R[A] \text{ 封闭} \\ \square \text{ 在 } R[A] \text{ 非交换环} \end{array}$$

$$1. A^0 = E \in R[A]$$

故 $R[A]$ 中 $M_n(\mathbb{R})$ 的交换子环

习题 2.3

R 是环. $\forall x \in R, x^2 = x$

问 R 是交换环

如 $\forall x \in R, x^3 = x$. 问 R 是不是交换环?