

在群论中，我们比较两个群，所用的工具是群的同态与同构，
 同样地，在环论中，我们也将使用同态与同构去比较两个环，
 环是具有两个运算的代数系统，
 因此在第一章所介绍的有关代数系统的同态、同构的概念可以如下移植到环中
 设 R 和 R' 是环，若存在映射 $\varphi: R \rightarrow R'$ ，使得映射 φ 保持环的运算，
 即对属于 R 的任意 a, b 有下列等式

$$\varphi(a+b) = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = \varphi(a)\varphi(b),$$

则称 φ 是 R 到 R' 的环同态，记为 $R \sim R'$ ，
 设 φ 是 R 到 R' 的环同态，
 若 φ 是单射(或满射)，则称 φ 是 R 到 R' 的单同态(或满同态)，
 特别地，若 φ 是双射，则称 φ 是 R 到 R' 的环同构，记为 $R \cong R'$ ，
 若 φ 是 R 到自身的环同构，则称 φ 是 R 的环自同构，
 设 φ 是 F 到 F' 的环同构，若 F 和 F' 都是域，则称 φ 是 F 到 F' 的域同构，
 特别地，若 φ 是 F 到自身的域同构，称 φ 为 F 的域自同构，
 注意，同构的代数对象具有“一样”的代数结构和运算性质，
 令 φ 是环 R 到 R' 的同态映射，
 则称 $\text{Ker } \varphi = \{a \in R \mid \varphi(a) = 0\} = \varphi^{-1}(0)$ 为映射 φ 的同态核，其中 0 是 R' 的零元，
 而称 $\text{Im } \varphi = \{\varphi(a) \mid a \in R\} = \varphi(R)$ 为映射 φ 的同态像，

命题 4.1 设 φ 是环 R 到 R' 的环同态，则如下结论成立：

$$(1) \varphi(0) = 0, \varphi(-a) = -\varphi(a),$$

其中第一个 0 是 R 的零元，第二个 0 是 R' 的零元， a 属于 R ；

(2) $\text{Ker } \varphi$ 是 R 的理想；

(3) $\text{Im } \varphi$ 是 R' 的子环；

$$(4) \varphi \text{ 是单同态} \Leftrightarrow \text{Ker } \varphi = \{0\},$$

证：若 φ 是环 R 到环 R' 的环同态，则 φ 是加法群 R 到加法群 R' 的群同态，

因此，根据群同态的性质可知，(1)和(4)成立，

下面我们仅需证明(2)和(3)，

证明(2)：显然 0 属于 $\text{Ker } \varphi$ ，即 $\text{Ker } \varphi$ 是 R 的非空子集，

另外，对属于 R 的 a ，和属于 $\text{Ker } \varphi$ 的 x, y ，我们有

$$\varphi(x-y) = \varphi(x) - \varphi(y) = 0 - 0 = 0,$$

$$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)0 = 0,$$

$$\varphi(xa) = \varphi(x)\varphi(a) = 0\varphi(a) = 0,$$

即 $x-y, ax, xa$ 属于 $\text{Ker } \varphi$ ，所以，根据本章定理 3.1 可知， $\text{Ker } \varphi$ 是 R 的理想

证明(3)：显然 $\text{Im } \varphi$ 是非空集合，

对属于 $\text{Im } \varphi$ 的 $\varphi(a), \varphi(b)$ ，

有 $\varphi(a) - \varphi(b) = \varphi(a-b)$ 属于 $\text{Im } \varphi$ 和 $\varphi(a)\varphi(b) = \varphi(ab)$ 属于 $\text{Im } \varphi$ ，

所以，根据本章定理 1.1 可知， $\text{Im } \varphi$ 是 R' 的子环，

例 4.1 设 I 是环 R 的理想，则映射 $\pi: R \rightarrow R/I, a \rightarrow a+I = \bar{a}$ 是满射，

$$\text{并且 } \pi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \pi(a) + \pi(b), \quad \pi(ab) = \overline{ab} = \bar{a}\bar{b} = \pi(a)\pi(b),$$

因此， π 是 R 到 R/I 的满同态，

一般地，称 π 为自然同态，容易验证， π 的核为 $\text{Ker } \pi = I$ ，

例 4.1 说明了一个环与其商环之间的关系，

下面的环同态基本定理将告诉我们这种环与环之间的关系具有一般性，

定理 4.1(环同态基本定理), 若 φ 是环 R 到环 R' 的环同态, 则 $R/\text{Ker } \varphi \cong \text{Im } \varphi$

证: 只需证明映射 $\bar{\varphi}: R/\text{Ker } \varphi \rightarrow \text{Im } \varphi, a+\text{Ker } \varphi \rightarrow \varphi(a)$ 是环同构即可, 如图 3.1

首先, 证明 $\bar{\varphi}$ 是映射,

若 $a+\text{Ker } \varphi=b+\text{Ker } \varphi$, 则 $a-b$ 属于 $\text{Ker } \varphi$, 即 $\varphi(a-b)=0$, 因此, $\varphi(a)=\varphi(b)$,

其次, 证明 $\bar{\varphi}$ 是同态,

对属于 R 的 a, b , 有

$$\begin{aligned} & \bar{\varphi}((a+\text{Ker } \varphi)+(b+\text{Ker } \varphi)) \\ &= \bar{\varphi}((a+b)+\text{Ker } \varphi) \\ &= \varphi(a+b) \\ &= \varphi(a)+\varphi(b) \\ &= \bar{\varphi}(a+\text{Ker } \varphi)+\bar{\varphi}(b+\text{Ker } \varphi), \\ & \bar{\varphi}((a+\text{Ker } \varphi)(b+\text{Ker } \varphi)) \\ &= \bar{\varphi}(ab+\text{Ker } \varphi) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \end{aligned}$$

$$= \bar{\varphi}(a+\text{Ker } \varphi)\bar{\varphi}(b+\text{Ker } \varphi),$$

最后, 证明 $\bar{\varphi}$ 是双射, 显然, $\bar{\varphi}$ 是满射,

另外, 若 $\bar{\varphi}(a+\text{Ker } \varphi)=\varphi(a)=0$,

则 a 属于 $\text{Ker } \varphi, a+\text{Ker } \varphi=\text{Ker } \varphi$, 即 $\text{Ker } \bar{\varphi}=\{\text{Ker } \varphi\}$, $\bar{\varphi}$ 是单射,

综上, 商环 $R/\text{Ker } \varphi$ 与环 $\text{Im } \varphi$ 同构

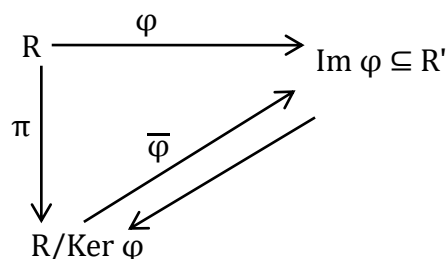


图 3,

在群论中, 我们有群的第一、第二同构定理,

在环论中, 同样有环的第一、第二同构定理,

定理 4.2 设 I 是环 R 的理想, S 是环 R 的子环, 则如下结论成立:

(1) $I+S$ 是环 R 的子环, I 是 $I+S$ 的理想;

(2) (环的第一同构定理) $S/(S \cap I) \cong (I+S)/I$;

(3) (环的第二同构定理), 若 J 也是环 R 的理想且 I 包含于 J , 则 $(R/I)/(J/I) \cong R/J$

证: (1) 首先证明 $I+S$ 是子环, 显然, $I+S$ 是 R 的非空子集,

另外, 对属于 I 的 a_1, a_2 , 和属于 S 的 s_1, s_2 ,

有 $(a_1+s_1)-(a_2+s_2)=(a_1-a_2)+(s_1-s_2)$ 属于 $I+S$,

$(a_1+s_1)(a_2+s_2)=(a_1a_2+a_1s_2+s_1a_2)+s_1s_2$ 属于 $I+S$,

所以, $I+S$ 是 R 的子环,

因为 I 是环 R 的理想, 且 I 包含于 $I+S$, 所以, I 是 $I+S$ 的理想,

(2) 显然 $\varphi: S \rightarrow (I+S)/I, s \mapsto s+I = \bar{s}$ 是满射,

又因对属于 S 的 s_1, s_2 , 有

$$\varphi(s_1+s_2) = \overline{s_1+s_2} = \overline{s_1} + \overline{s_2} = \varphi(s_1) + \varphi(s_2),$$

$$\varphi(s_1s_2) = \overline{s_1s_2} = \overline{s_1} \overline{s_2} = \varphi(s_1)\varphi(s_2),$$

因此, φ 是 S 到 $(I+S)/I$ 的满同态, 而 $\text{Ker } \varphi = \{s \in S | \bar{s} = I\} = \{s \in S | s \in I\} = S \cap I$,

所以, 由环同态基本定理有 $S/(S \cap I) \cong (I+S)/I$,

(3) 要证明 $(R/I)/(J/I) \cong R/J$, 根据环同态基本定理,

只需证明 $\varphi: R/I \rightarrow R/J, a+I \mapsto a+J$ 是满同态, 且 $\text{Ker } \varphi = J/I$,

首先, 若 $a_1+I = a_2+I$, 则 a_1-a_2 属于 I 包含于 J , 从而 $a_1+J = a_2+J$, 即 φ 是映射,

φ 的满射性是显然的,

其次, 对属于 R 的 a_1, a_2 , 有

$$\begin{aligned} \varphi((a_1+I)+(a_2+I)) &= \varphi((a_1+a_2)+I) & \varphi((a_1+I)(a_2+I)) &= \varphi(a_1a_2+I) \\ &= (a_1+a_2)+J & &= a_1a_2+J \\ &= (a_1+J)+(a_2+J) & &= (a_1+J)(a_2+J) \\ &= \varphi(a_1+I)+\varphi(a_2+I), & &= \varphi(a_1+I)\varphi(a_2+I); \end{aligned}$$

所以 φ 保持运算, 从而 φ 是 R/I 到 R/J 的满同态,

另外, $\text{Ker } \varphi = \{a+I | a+J = J\} = \{a+I | a \in J\} = J/I$,

所以由环同态基本定理有 $(R/I)/(J/I) \cong R/J$,

例 4.2 设 R 是环，证明 $R/\{0\} \cong R$ 和 $R/R \cong \{0\}$ ，

证：显然， R 上的恒等映射 $\text{id}_R: R \rightarrow R$ 是 R 到 R 的满同态，且 $\text{Ker } \text{id}_R = \{0\}$ ，

所以由环同态基本定理可知 $R/\{0\} \cong R$ ，

若映射 $\varphi: R \rightarrow \{0\}$ ，使等式 $\varphi(a) = 0$ 成立，则 φ 是 R 到 $\{0\}$ 的满同态，且 $\text{Ker } \varphi = R$ ，

所以，由环同态基本定理可知 $R/R \cong \{0\}$ ，

推论 4.1 设 φ 是环 R 到环 R' 的单同态，则环 R 与环 $\text{Im } \varphi$ 同构，

例 4.3 设四元数体 $H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$ ，证明存在实数域 $\mathbb{R}$ 到环 H 的单同态

证：令 $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ，定义映射 $\varphi: \mathbb{R} \rightarrow H, a \mapsto aE$ ，则对属于 $\mathbb{R}$ 的 a, a' ，有

$$\varphi(a+a') = (a+a')E = aE + a'E = \varphi(a) + \varphi(a'),$$

$$\varphi(aa') = (aa')E = (aE)(a'E) = \varphi(a)\varphi(a'),$$

且 $\text{Ker } \varphi = \{0\}$ ，即 φ 是 $\mathbb{R}$ 到 H 的单同态，

所以，由推论 4.1 可知， $\mathbb{R}$ 与 $\text{Im } \varphi$ 同构，

因此，在同构意义下，可以将 $\mathbb{R}$ 视为四元数体的子域，

例 4.4 设 R 是整环，试证明：

若 $\text{Char } R = p$ (p 是素数)，则 R 包含一个同构于 $\mathbb{Z}_p$ 的子域，

若 $\text{Char } R = 0$ ，则 R 包含一个同构于整数环 $\mathbb{Z}$ 的子环，

证：我们先来构造一个环 $\mathbb{Z}$ 到环 R 的同态映射，

令 $\varphi: \mathbb{Z} \rightarrow R, n \mapsto ne$ ，其中 e 是环 R 中的单位元，

对属于 $\mathbb{Z}$ 的 s, t ，有

$$\varphi(s+t) = (s+t)e = se + te = \varphi(s) + \varphi(t),$$

$$\varphi(st) = (st)e = (se)(te) = \varphi(s)\varphi(t),$$

所以，是环 $\mathbb{Z}$ 到环 R 的环同态，根据环同态基本定理可知 $\mathbb{Z}/\text{Ker } \varphi \cong \text{Im } \varphi \subseteq R$ ，

另外， $\text{Ker } \varphi = \{n \in \mathbb{Z} \mid ne = 0\}$ ，即 $\text{Ker } \varphi$ 的元素是 e 的阶的倍数，

而 e 的阶就是 $\text{Char } R$ ，所以， $\text{Ker } \varphi = \langle \text{Char } R \rangle$ ，

由推论 4.1 可知，当 $\text{Char } R = 0$ 时， $\mathbb{Z} \cong \text{Im } \varphi$ ；当 $\text{Char } R = p$ 时， $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle \cong \text{Im } \varphi$ ，

最后我们来讨论剩余类环之间的关系，

例 4.5 证明 $\varphi: \bar{x} \rightarrow x\varphi(\bar{1})$ 是 Z_m 到 Z_n 的环同态的充分必要条件是

$$m\varphi(\bar{1})=\bar{0}, (\varphi(\bar{1}))^2=\varphi(\bar{1}),$$

证: 必要性是显然的，下面证明充分性，

首先，证明 φ 是 Z_m 到 Z_n 的映射，

若 $\bar{a}, \bar{b}$ 属于 Z_m ， $\bar{a}=\bar{b}$ ，则存在属于 Z 的 t ，使得 $a-b=tm$ ，

$$\text{从而，} a\varphi(\bar{1})-b\varphi(\bar{1})=(a-b)\varphi(\bar{1})=tm\varphi(\bar{1})=\bar{0},$$

$$\text{因此 } a\varphi(\bar{1})=b\varphi(\bar{1}), \text{ 即 } \varphi(\bar{a})=\varphi(\bar{b}),$$

另外，对属于 Z 的 $\bar{a}, \bar{b}$ ，由

$$\varphi(\bar{a}+\bar{b})=\varphi(\overline{a+b})=(a+b)\varphi(\bar{1})=a\varphi(\bar{1})+b\varphi(\bar{1})=\varphi(\bar{a})+\varphi(\bar{b}),$$

$$\varphi(\bar{a}\bar{b})=\varphi(\overline{ab})=(ab)\varphi(\bar{1})=(a\varphi(\bar{1}))(b\varphi(\bar{1}))=\varphi(\bar{a})\varphi(\bar{b}),$$

可知 $\varphi: \bar{x} \rightarrow x\varphi(\bar{1})$ 是 Z_m 到 Z_n 的环同态，

例 4.6 求 Z_5 到 Z_{10} 的所有环同态，

解: 设 φ 是 Z_5 到 Z_{10} 的环同态，则对属于 Z_5 的任意 $\bar{x}$ ，有 $\varphi(\bar{x})=\varphi(x\bar{1})=x\varphi(\bar{1})$ ，

这说明 φ 是由 $\varphi(\bar{1})$ 决定的，

设 $\varphi(\bar{1})=\bar{a}$ ，则由例 4.5 可知， $\bar{a}$ 应满足条件 $5\cdot\bar{a}=\bar{0}$ 和 $\bar{a}=\bar{a}^2$ ，

但是在 Z_{10} 中，满足这两个条件的元素 $\bar{a}$ 只有 $\bar{0}$ ， $\bar{6}$ ，

所以 $\varphi(\bar{1})=\bar{0}$ 或 $\varphi(\bar{1})=\bar{6}$ ，

那么 Z_5 到 Z_{10} 的环同态有两个： $\varphi(\bar{x})=x\bar{0}=\bar{0}$ 和 $\varphi(\bar{x})=x\bar{6}=\overline{6x}$ ，