同态

2023 年 10 月 17 日

目录

1 同态

我们在这节研究环的同态，看看和群比起来有什么不同的。

1.1 定义：同态

若A, B是交换环，一个同态指的是像$f : A \to R$

1. $f(1) = 1$
2. $f(a + a') = f(a) + f(a')$对所有$a, a' \in A$
3. $f(aa') = f(a)f(a')$对所有$a, a' \in A$成立

一个同态如果是双射，则它被我们叫成同构。若有同构$f : A \to R$，则交换环A和B是同构，被记为$A \cong B$

1.1.1 例子

1. 令R是整环和$F = Frac(R)$为分式域。我们断言R是F的子环，但这不是真的。准确的来说，R甚至都不是F的子集。我们来找F的子环R'，它和R有非常强的联系，即，$R = \{[a, 1] : a \in R\} \subseteq F$，函数$f : R \to R'$由$f(a) = [a, 1]$给出，可以看得出来是一个同构。在之后我们可以看到，分式域是唯一的，若其同构则视为一样。

1.1.2 更多的例子

1. 复共轭$z = a + ib \to a - ib$是同态$C \to C$。这是因为$\bar{1} = 1, \overline{z + w} = \bar{z} + \bar{w}$，并且$\overline{zw} = \bar{z}\bar{w}$，我们也可以证明这是一个同构，因为这就是其自身的逆，对所有复数z，我们有$\bar{\bar{z}} = z$
2. 我们给出一些环的同态但不是同构的例子，选择$m \geq 2$并第一$f : Z \to I_m$由$f(n) = [n]$定义的。注意f是满射但不是双射。

1.2 命题

令R, S是交换环，且令$\varphi : R \to S$是同态。若$s_1, \cdots, s_n \in S$，则这里存在唯一一个同态$\widetilde{\varphi} : R[x_1, \cdots, x_n] \to S$，其中对所有$i$有$\widetilde{\varphi}(x_i) = s_i$且满足所有$r \in R$有$\widetilde{\varphi}(r) = \varphi(r)$

证明： 我们对$n \geq 1$归纳，若$n = 1$，把x记为x_1和s_1记为s，定义$\widetilde{\varphi} : R[x] \to S$像这样子：若$f(x) = \sum_i r_i x^i$，则

$$\widetilde{\varphi} : r_0 + \cdots + r_n x^n \to \varphi(r_0) + \cdots \varphi(r_1)s + \cdots + \varphi(r_n)s^n = \widetilde{\varphi}(f)$$

而这个公式给出了$\widetilde{\varphi}(x) = s$和对所有$r \in R$有$\widetilde{\varphi}(r) = \varphi(r)$

而我们还得证明$\widetilde{\varphi}$是同态。首先，$\widetilde{\varphi}(1) = (1) = 1$，这是因为$\varphi$是同态。其次，若$g(x) = a_0 + a_1 x + \cdots + a_m x^m$，则

$$\begin{aligned}
\widetilde{\varphi}(f+g) =& \widetilde{\varphi}(\sum_i (r_i + a_i)x^i) \\
=& \sum_i \varphi(r_i + a_i)s^i \\
=& \sum_i (\varphi(r_i) + \varphi(a_i))s^i \\
=& \sum_i \varphi(r_i)s^i + \sum_i \varphi(a_i)s^i \\
=& \widetilde{\varphi}(f) + \widetilde{\varphi}(g)
\end{aligned}$$

然后，令$f(x)g(x) = \sum_k c_k x^k$，其中$c_k = \sum_{i+j=k} r_i a_j$，则

$$\begin{aligned}
\widetilde{\varphi}(fg) =& \widetilde{\varphi}(\sum_k c_k x^k) \\
=& \sum_k \varphi(\sum_{i+j=k} r_i a_j)s^k \\
=& \sum_k (\sum_{i+j=k} \varphi(r_i)\varphi(a_j))s^k
\end{aligned}$$

另一方面

$$\begin{aligned}
\widetilde{\varphi}(f)\widetilde{\varphi}(g) =& (\sum_i \varphi(r_i)s^i)(\sum_j \varphi(a_j)s^j) \\
=& \sum_k (\sum_{i+j=k} \varphi(r_i)\varphi(a_j))s^k
\end{aligned}$$

最后我们证明唯一性，设$\theta : R[x] \to S$是另一个同态且$\theta(x) = s$并且$\theta(r) = \varphi(r)$对所有$r \in R$成立。则

$$\theta(r_0 + r_1 x + \cdots + r_n x^n) = \sum_{i=0}^{n} \varphi(r_i)s^i = \varphi(r_0) + \varphi(r_1)s + \cdots + \varphi(r_n)s^n = \widetilde{\varphi}$$

成立

1.3 定义：赋值

若R是交换环取$s \in R$，则赋值s指的是存在一个函数$e_s : R[x] \to R$被定义为$e_s(f(x)) = f(s)$，由此可得$e_s(\sum_i r_i x^i) = \sum_i r_i s^i$

1.4 引理

若R是交换环且$s \in R$，则赋值映射$e_s : R[x] \to R$是同态。

证明： 利用命题1.2并令$R = S$和$\varphi = 1_R$，则有$\widetilde{\varphi} = e_s$

1.5 引理

若$f : A \to R$是一个环同态，则对所有$a \in A$有

1. $f(a^n) = f(a)^n$对所有$n \geq 0$成立
2. 若a是单位，则$f(a)$是单位且$f(a^{-1}) = f(a)^{-1}$
3. 若a是单位，则$f(a^{-n}) = f(a)^{-n}$对所有$n \geq 1$成立

证明1： 若$n = 0$，则$f(a^0) = 1 = (f(a))^0$，这是利用环中任意元素$r^0 = 1$证明的。并且有环同态满足$f(1) = 1$

证明2： 对$a^{-1}a = 1$应用函数f，则$f(a)$是单位，$f(a^{-1}a) = f(1) = 1$且逆为$f(a^{-1})$

证明3： $a^{-n} = (a^{-1})^n$，利用上述两个定理即可。

1.6 推论

若$f : A \to R$是环同态，则

$$f(U(A)) \subseteq U(R)$$

其中$U(A)$是由A的单位构成的群，若f是同构，则存在群同构

$$U(A) \cong U(R)$$

证明： 第一个部分指的是引理1.5的第二个命题：若a是A中的单位，则$f(a)$是R中的单位。

若f是同构，则逆$f^{-1}: R \to A$说不定是个环同态。那么$f^{-1}f(r) = r$，若r是环中的单位，则$f^{-1}(r)$是A的单位。为了看出这一点，我们来看，r是单位，则存在$ur = 1$，那么$f^{-1}(1) = 1$得到$f^{-1}(1) = f^{-1}(ur) = 1 = f^{-1}(u)f^{-1}(r)$得到$f^{-1}(r)$实际上也是一个单位。现在我们来检查$\varphi : U(A) \to U(R)$，且用函数$a \to f(a)$定义该映射。那么它的逆$\Psi : U(R) \to U(A)$由函数$f(a) \to a$定义，所以就有

$$U(A) \cong U(R)$$

1.7 定义：环的核

若$f : A \to R$是环同态，则它的核是

$$\ker f = \{a \in A, f(a) = 0\}$$

它的像是

$$\mathrm{im} f = \{r \in R : r = f(a), a \in A\}$$

注意，若我们抛弃乘法，则环A和R是加法阿贝尔群且定义就与我们在群论那章定义的一样。

令k是域，$a \in K$，就像命题1.2，考虑赋值同态$e_a : k[x] \to k$把$f(x)$变成$f(a)$。e_a总是满射的。若$b \in k$，则$b = e_a(f)$，其中$f(x) = x - a + b$由定义可知$\ker e_a$考虑所有对a的零多项式$g(a) = 0$

1.8 命题

若$f : A \to R$是环同态，其中R是非零环，则$\mathrm{im} f$是R的子环且$\ker f$是A的真子集满足如下条件

1. $0 \in \ker f$
2. $x, y \in \ker f$蕴含$x + y \in \ker f$
3. $x \in \ker f$和$a \in A$则$ax \in \ker f$

证明： 若$r, r' \in \mathrm{im} f$，则$r = f(a)$和$r' = f(a')$对某些$a, a' \in A$成立，我们验证子环的定义，$r - r' = f(a) - f(a') = f(a - a') \in \mathrm{im} f$，且$rr' = f(a)f(a') = f(aa') \in \mathrm{im} f$得到$f(1) = 1$所以$\mathrm{im} f$是$R$的子环。

另一方面，$f(0) = 0$，所以$0 \in \ker f$，若$x, y \in \ker f$，则$f(x + y) = f(x) + f(y) = 0 + 0 = 0$，因此$x + y \in \ker f$。若$x \in \ker f$和$a \in A$，则$f(ax) = f(a)f(x) = f(a)0 = 0$，所以$ax \in \ker f$。注意$\ker f$是$A$的真子集。对$f(1) = 1 \neq 0$，所以$1 \notin \ker f$

1.9 定义：理想

交换环R中的理想是一个R的子集I有着如下性质：

1. $0 \in I$
2. 若$a, b \in I$,则$a + b \in I$
3. 若$a \in I$且$r \in R$，则$ra \in I$

当$I \neq R$的时候叫真理想。我们可以藉由重申命题1.8. 若$f : A \to R$是环同态，其中R是非零环，则$\mathrm{im} f$是R的子环并且$\ker f$是A中的真理想。

这里存在在每个非零交换环中有2个显然理想的例子：环R自身和子集$\{0\}$。等一下我们将看到只有这些理想的交换环必定是个域。

1.9.1 例子

若$b_1, b_2, \cdots, b_n$是R中的元，则所有线性组合的集合

$$I = \{r_1 b_1 + r_2 b_2 + \cdots + r_n b_n : r_i \in R\text{所有i成立}\}$$

是R中的理想，可以写为$I = (b_1, b_2, \cdots, b_n)$

特别的，若$n = 1$，则$I = (b) = \{rb : r \in R\}$是$R$中的理想，且$(b)$由所有$b$的乘积组成，我们把这叫做主理想。

注意的是，我们始终把R和$\{0\}$认为是主理想。记为$R = (1)$和$\{0\} = (0)$。在Z中，偶数构成主理想(2)。

1.10 定理

每个Z中的理想都是主理想。

证明： 这是之前提到的定理：

> 令I是Z的子集且有如下性质：
>
> 1. $0 \in I$
> 2. $a, b \in I$，则$a - b \in I$
> 3. 若$a \in I$和$q \in Z$，则$qa \in I$
>
> 则存在一些非负整数$d \in I$且I为d的所有倍数组成的集合。

我们设$a = qd$是d的倍数，其中设d是I中最小的整数。由除法算式可知存在整数q, r使得$a = qd + r$，其中$0 \leq r < d$。由于$d \in I$ 且是I中最小的数，由$r = a - qd \in I$和$r < d$可知，$r = 0$

因此，I是R中的主理想。

1.11 命题

若R是交换环和$a = ub$对某个单位$u \in R$成立，则$(a) = (b)$。反过来，若R是域，则$(a) = (b)$有$a = ub$对某个单位$u \in R$成立

证明： 我们设$a = ub$对某个单位$u \in R$成立，若$x\imath(a)$，则$x = ra = rub \in (b)$对某个$r \in R$成立。因此$(a) \subseteq (b)$。对于反包含，若$y \in (b)$，则$y = sb$对某个$s \in R$成立，因此$y = sb = su^{-1}a \in (a)$，所以$(b) \subseteq (a)$且$(a) = (b)$

反过来，若$(a) = (b)$，则$a \in (a) = (b)$告诉我们$a = rb$对某个$r \in R$成立，因此$b \mid a$；类似的，$b \in (b) = (a)$暗示$a \mid b$，由于题设R是域，那么必然能找到单位$u \in R$使得$a = ub$

1.11.1 例子

若交换环R中的理想I包含1，则$I = R$，因为I包含的$r = r1$对某个$r \in R$是成立的。实际上，一个理想I包含单位u当且仅当$I = R$

充分性是显然的，若$I = R$，则I包含单位，即1，若$u \in I$是某个单位，则I包含$u^{-1}u = 1$，这是因为I包含$r = r1$对每个$r \in R$成立。

1.12 命题

一个非零交换环R是域当且仅当其只有理想$\{0\}$和自身R。

证明： 设R是域，若$I \neq \{0\}$，那么包含一些非零元素并且非零元素在域中是单位，因此$I = R$。

反过来。设R是交换环且只有理想$\{0\}$和自身R。若$a \in R$且$a \neq 0$，则主理想$(a) = R$，且$(a) \neq 0$，因此$1 \in R = (a)$得到$1 = ra$，因此a是存在逆的，得到R是域

1.13 命题

一个环同态$f : A \to R$是单射当且仅当$\ker f = \{0\}$

证明： 若f是单射，则$a \neq 0$有$f(a) \neq f(0) = 0$，因此$a \notin \ker f$，所以$\ker f = \{0\}$。反过来若$\ker f = \{0\}$并且$f(a) = f(a')$，则$0 = f(a) - f(a') = f(a - a')$，所以$a - a' \in \ker f$得到$a = a'$。所以$f$是单射。

1.14 引理

若$f : k \to R$是环同态，其中R是非零环。且k是域，则f是单射。

证明： 利用命题1.13可知若是单射则$\ker f = \{0\}$。但$\ker f$是k中的真理想，利用命题1.12和命题1.8可知k只有两个真理想k和$\{0\}$。现在$\ker f \neq k$，因为$f(1) = 1 \neq 0$。因此$\ker f = \{0\}$得到f是单射。

2 练习

> 证明由$f(x) \to f(A)$定义的函数$k[x] \to k[A]$是满射环同态。其中A是域k上的$n \times n$矩阵。$f(x) = c_0 + c_1 x + \cdots + c_m x^m \in k[x]$，并定义$k[A] = \{f(A) : f(x) \in k[x]\}$

证明： 首先证明$k[A]$也是一个交换环，即对加法和乘法封闭。由于是在域k上选择的矩阵，所以每个矩阵都具有逆。利用子环的定义A上的元素都

是k中的数，那么自然的，对每个$a, b \in k$都存在$a - b \in k, ab \in K$，所以对于加法，容易验证$A - B$中的元素也在k内

而对于乘法，则由矩阵乘法可知，对两个矩阵AB中的元素是多项式$\sum_{k=1}^{n} a_{ik} b_{kj}$，对其中$a_{ik} b_{kj}$在$k$中封闭，因此$AB$也对k封闭，并且可以利用归纳法推广到幂次的结论。

因此，对$f, g \in k[x]$，其中$f = a_0 + \cdots + a_m x^m$和$g = b_0 + \cdots + b_m x^m$定义$f(A) + g(A)$得到

$$f(A) + g(A) = (a_0 + b_0) I_0 + \cdots + (a_m + b_m) A^m$$

对加法封闭。

其次，对于乘法$f(A)g(A)$则有

$$f(A)g(A) = \sum_{i+j=k} a^i b^j A^k$$

对乘法封闭，因此是一个环。

现在，定义函数$\varphi : f(x) \to f(A)$，首先，对于0和1，我们可以把$f(1) = 1$映射到单位矩阵上，即$f(1) \to f(I) = I$，其次对于加法，则取$f, g \in k[x]$

$$\varphi(f(x)) + \varphi(g(x)) = \sum_{i=0}^{m} c_i A^i + \sum_{k=0}^{m} d_i A^i = \sum_{i}^{n} (c_i + d_i) A^i = \varphi(f(x) + g(x))$$

而对于乘法有

$$\varphi(f(x))\varphi(g(x)) = \sum_{i+j=k}^{m} c_i d_j A^k = \varphi\left(\sum_{i+j=k}^{m} c_i d_j x^k\right) = \varphi(f(x)g(x))$$

证毕。

令A是交换环，证明其子集J是理想当且仅当$0 \in J, u, v \in J$使得$u - v \in J$且$u \in J, a \in A$使得$au \in J$.

若J是A中的理想，由于$0 \in J$，那么就存在$u - v = 0 \in J$。可知存在一些$-v \in J$那么由封闭性可知$u + (-v) = u - v \in J$成立。而且也对$a \in A, u \in J$使得$au \in J$。

反过来，若J满足一些性质：

1. $0 \in J$
2. $u, v \in J$使得$u - v \in J$
3. $u \in J, a \in A$使得$au \in J$

对于第$1, 3$条性质是不言而喻的，对于第二条性质，有$u - v \in J$可以得到$u - (-v) = a + v \in J$得到J是一个理想。

令R是交换环，证明由

$$\eta : a_0 + a_1 x + \cdots + a_n x^n \to a_0$$

定义的函数$\eta : R[x] \to R$是同态。并用多项式的根描述$\ker \eta$

证明： 当$a_0 = 1$的时候，$\eta(1 + a_1 x + \cdots + a_n x^n) = 1$。对于$a_0$和$b_0$为零次的多项式$f, g \in R[x]$则有

$$\eta(f(x) + g(x)) = \eta\left(\sum_{i=0}^{n} (a_i + b_i) x^i\right) = a_0 + b_0 = \eta(f(x)) + \eta(g(x))$$

对于乘法，则

$$\eta(f(x)g(x)) = \eta\left(\sum_{i+j=k}^{n} a_i b_j x^k\right) = \eta(a_0 b_0 + \cdots) = a_0 b_0 = \eta(f(x))\eta(g(x))$$

对于$\ker \eta$，对于$x = 0$的根，则说明$x \mid f(x)$成立，这意味着$f(x)$是不存在常系数a_0的函数。因此

$$\ker \eta = \{f(x) : f(0) = 0 \in R[x]\}$$

令R和S是交换环且令$\varphi : R \to S$是同态，证明由函数

$$\varphi^* : r_0 + r_1 x + \cdots \to \varphi(r_0) + \varphi(r_1)x + \cdots$$

$\varphi^* : R[x] \to S[x]$是一个同态。

证明： 令$f(x), g(x) \in R[x]$是R上的多项式，那么

$$\varphi^*((1, 0, 0 \cdots,)) = \varphi(1) = 1$$

对于加法，则有

$$\begin{aligned}
\varphi^*(f(x)) + \varphi^*(g(x)) =& \sum_{i=0}^{n} (\varphi(a_i) + \varphi(b_i)) x^i \\
=& \varphi^* \left(\sum_{i=0}^{n} (a_i + b_i) x^i \right) \\
=& \varphi^*(f(x) + g(x))
\end{aligned}$$

对于乘法，则

$$\begin{aligned}
\varphi^*(f(x))\varphi^*(g(x)) =& \varphi(a_0)\varphi(b_0) + \cdots \\
=& \sum_{k=0}^{n} \left(\sum_{i+j=k} \varphi(a_i b_j) \right) x^k \\
=& \varphi^*(f(x)g(x))
\end{aligned}$$

所以φ^*是同态。

令R, S是交换环，再令$\psi : R \to S$是同态，其中$\ker \psi = I$，若J是S中的理想，证明$\psi^{-1}(J)$是理想且包含I

由于ψ是同态，那么I是真理想，则有$\psi(0) = 0$，所以$\psi^{-1}(J)$包含0，其次，由于I是理想，则有$a, b \in I$使得$\psi(a + b) = 0 = \psi(a) + \psi(b) \in J$，所以$a + b \in \psi^{-1}(J)$，最后，由于$a \in R, b \in I$使得$ab \in I$且$\psi(ab) = 0 \in J$，那么$ab \in \psi^{-1}(J)$，由此可得$\psi^{-1}(J)$是理想且包含$I$