0.1 环同态

定义 0.1 (环同态)

设 $(R,+,\cdot),(R',+',*)$ 都是环,$f:(R,+,\cdot)\to(R',+',*)$ 是一个映射, 我们说 f 是个**环同态**, 若

(i) $f(1)=1'$,

(ii) $f(a+b)=f(a)+'f(b),\forall a,b\in R$.

(iii) $f(ab)=f(a)*f(b),\forall a,b\in R$.

♣

注 未来, 在不引起歧义的情况下, 我们会忽略两个环中加法与乘法的区别, 都记作 $+$ 和 $\cdot$, 称环同态是

$$f:(R,+,\cdot)\to(R',+,\cdot).$$

命题 0.1

设 $(R,+,\cdot),(R',+',*)$ 都是环,$f:(R,+,\cdot)\to(R',+',*)$ 是一个映射, 则 f 是环同态等价于 f 既是加法的群同态, 又是乘法的幺半群同态.

♠

证明 根据环同态的定义不难证明. □

定义 0.2 (环同态的核与像)

设 $f:(R,+,\cdot)\to(R',+',*)$ 是一个环同态, 则我们定义 f 的**核与像**, 记作 $\ker(f)$ 与 $\operatorname{im}(f)$, 分别为

$$\ker(f)=\{x\in R:f(x)=0'\}\subset R,$$

$$\operatorname{im}(f)=\{y\in R':\exists x\in R,y=f(x)\}=\{f(x):x\in R\}\subset R'.$$

♣

注 注意核在大多数情况下不会是一个子环.

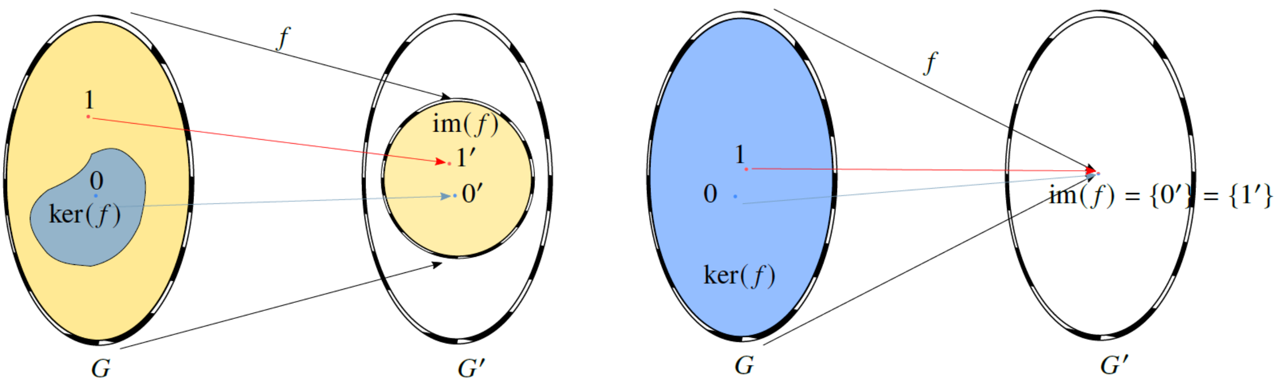

图 1: 环同态的核与像示意图

定义 0.3 (理想)

设 $(R,+,\cdot)$ 是一个环, 而 $I\subset R$. 我们定义, 称 I 是 R 的**左理想**, 若

$$(I,+)<(R,+),$$

$$\forall r\in R,\forall a\in I,ra\in I.$$

即 $RI\subset I$, 也即 $RI=I$. 也等价于 $SI=I,\forall S\subset R$.

类似地, 我们称 I 是 R 的**右理想**, 若

$$(I,+)<(R,+),$$

$$\forall a \in I, \forall r \in R, ar \in I.$$

即 $IR \subset I$, 也即 $IR = I$. 也等价于 $IS = I, \forall S \subset R$.

如果 I 既是左理想又是右理想, 我们就称 I 是 R 的一个**理想**, 记作 $I \lhd R$.

笔记 理想的第二条性质表明: 理想在乘法下"吸收"了整个环到理想上, 也就是说

$$RI \subset I \quad , IR \subset I.$$

其中子集的乘法, 定义为所有元素乘积的集合. 而显然有 $I \subset RI, IR$. 故

$$\forall r \in R, \forall a \in I, ra \in I \Leftrightarrow RI \subset I \Leftrightarrow RI = I,$$

$$\forall r \in R, \forall a \in I, ar \in I \Leftrightarrow IR \subset I \Leftrightarrow IR = I.$$

引理 0.1

(1) 设 $(R, +, \cdot)$ 是一个环,$H < R$, 则 $HH = H$.

(2) 设 $(R, +, \cdot)$ 是一个环,$H \lhd R$, 则 $HH = H$.

证明

(1) 一方面, 根据 $H < R$ 可知, H 是 R 的一个乘法子幺半群. 于是由引理**??**可知, 对 $\forall h_1, h_2 \in H$, 都有 $h_1 h_2 \in H$. 故 $HH \subset H$.

另一方面, 设 $h \in H$,e 是 R 的乘法单位元. 则 $h = he \in HH$. 故 $H \subset HH$.

综上, $HH = H$.

(2) 一方面, 对 $\forall h_1, h_2 \in H$, 根据 $H \lhd R$ 的定义及 $h_1 \in R$ 可知, $h_1 h_2 \in H$. 故 $HH \subset H$.

另一方面, 设 $h \in H$,e 是 R 的乘法单位元. 则 $h = he \in HH$. 故 $H \subset HH$.

综上, $HH = H$.

□

引理 0.2 (理想是整个环的充要条件)

(1) 设 $(R, +, \cdot)$ 是一个环, 而 $I \lhd R$. 则 $I < R$ 当且仅当 $I = R$.

(2) 设 $(R, +, \cdot)$ 是一个环,1 是其乘法单位元,$I \lhd R$, 则 $1 \in I$ 当且仅当 $I = R$.

(3) 设 $(R, +, \cdot)$ 是一个环,1 是其乘法单位元,$I \lhd R$, 则 $R^\times \cap I \neq \varnothing$ 当且仅当 $I = R$.

证明

(1) 充分性是显然的, 因为一个环当然是自己的子环.

我们来证明必要性. 设 $I < R$, 则特别地,$1 \in I$. 可是 $I \lhd R$, 因此对任何 $r \in R$, 我们有

$$r = r \cdot 1 \in I.$$

这就证明了 $I = R$.

综上所述, 一个理想是子环当且仅当它是整个环.

(2) 充分性是显然的. 下证必要性.

由 $I \lhd R$ 可知 $I \subset R$. 因为 $1 \in I$, 且 $I \lhd R$, 所以 $\forall r \in R$, 都有 $r = r \cdot 1 \in I$. 因此 $R \subset I$.

综上, 我们就有 $I = R$.

(3) 充分性是显然的. 下证必要性.

设 $a \in R^\times \cap I$, 则 a 是 R 中的一个单位. 从而存在 $b \in R$, 使得 $ab = 1$. 又由 $I \lhd R$ 可知,$1 = ab \in I$. 于是由 (2) 可知 $I = R$.

□

命题 0.2

设 $(R, +, \cdot)$ 是一个交换环, 则 I 是一个左理想当且仅当 I 是一个右理想, 又当且仅当 I 是一个理想.

证明 根据交换环对乘法的交换律, 这是显然的. □

命题 0.3

设 $n \in \mathbb{N}_1$, 则 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想, 即

$$n\mathbb{Z} \lhd \mathbb{Z}.$$

证明 首先, 由命题??我们知道 $(n\mathbb{Z}, +)$ 是 $(\mathbb{Z}, +)$ 的（加法）正规子群.

其次, 注意到 $\mathbb{Z}$ 是一个交换环, 故根据命题 0.2可知, 我们只须证明 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的左理想, 也即 $\mathbb{Z} \cdot n\mathbb{Z} \subset n\mathbb{Z}$.

要证明 $\mathbb{Z} \cdot n\mathbb{Z} \subset n\mathbb{Z}$, 我们只须令 $m \in \mathbb{Z}, nk \in n\mathbb{Z}(k \in \mathbb{Z})$, 只要证明 $mnk \in n\mathbb{Z}$ 即可. 而这是因为

$$mnk = n(mk) \in n\mathbb{Z}.$$

综上所述, 这就证明了 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想. □

引理 0.3

设 $n \in \mathbb{N}_1$, 我们要定义映射 $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot)$. 对 $m \in \mathbb{Z}$, 我们定义

$$f(m) = m + n\mathbb{Z}.$$

则 f 是一个环同态, 而 $\ker(f) = n\mathbb{Z} \lhd R$.

证明 先证明 f 是加法的群同态.

设 $a, b \in \mathbb{Z}$, 由命题??可知,$(n\mathbb{Z}, +) \lhd (\mathbb{Z}, +)$. 从而

$$f(a) + f(b) = a + n\mathbb{Z} + b + n\mathbb{Z} = a + b + n\mathbb{Z} = f(a + b).$$

故 f 是加法的群同态.

下面证明 f 是乘法的幺半群同态.

第一,$f(1) = 1 + n\mathbb{Z}$ 是 $\mathbb{Z}_n$ 的乘法单位元.

第二, 设 $m, m' \in \mathbb{Z}$, 则利用上一章中我们证明过的 $\mathbb{Z}_n$ 对乘法的良定义性, 我们有

$$f(m)f(m') = (m + n\mathbb{Z})(m' + n\mathbb{Z}) = mm' + n\mathbb{Z} = f(mm').$$

故 f 是乘法的幺半群同态.

综上所述,f 是一个从 $\mathbb{Z}$ 到 $\mathbb{Z}_n$ 的环同态.

注意到

$$\ker f = \{m \in \mathbb{Z} : f(m) = n\mathbb{Z} = \overline{0}\} = \{m \in \mathbb{Z} : \overline{m} = m + n\mathbb{Z} = n\mathbb{Z} = \overline{0}\} = \{m \in \mathbb{Z} : m \in n\mathbb{Z}\} = n\mathbb{Z}.$$

因此由命题 0.3可知 $\ker(f) = n\mathbb{Z} \lhd R$. □

命题 0.4 (环同态的核是理想并且像是子环)

设 $f : (R, +, \cdot) \to (R', +, \cdot)$ 是一个环同态, 则 f 的核是 R 的理想,f 的像是 R' 的子环. 此即,

$$\ker(f) = \{a \in R : f(a) = 0'\} \lhd R,$$

$$\operatorname{im}(f) = \{b \in R' : \exists a \in R, b = f(a)\} = \{f(a) \in R' : a \in R\} < R'.$$

证明 我们先证明 $\ker(f) \lhd R$. 根据群同态的性质, 由群同构第一定理, 我们知道 $\ker(f)$ 是加法的（正规）子群. 为了方便起见, 令 $I = \ker(f)$. 我们只须证明 $RI \subset I$ 以及 $IR \subset I$.

令 $a \in R$,$b \in I = \ker(f)$, 故 $f(b) = 0'$. 因此,$f(ab) = f(a)f(b) = f(a)0' = 0'$, 从而 $ab \in \ker(f) = I$. 这就证明了 $RI \subset I$. 而另一个包含关系同理可证. 这样, 我们就证明了 $\ker(f) \lhd R$.

我们再证明 $\mathrm{im}(f) < R'$. 第一,$1' = f(1) \in \mathrm{im}(f)$.

第二, 令 $a', b' \in \mathrm{im}(f)$, 不妨设 $a' = f(a), b' = f(b)$. 只须证明 $a' - b', a'b' \in \mathrm{im}(f)$. 而由 f 对加法是群同态可知,f 保持加法逆元和加法. 由 f 对乘法是幺半群同态可知,f 保持乘法. 于是就有

$$\begin{aligned} a' - b' &= f(a) - f(b) = f(a-b) \in \mathrm{im}(f), \\ a'b' &= f(a)f(b) = f(ab) \in \mathrm{im}(f). \end{aligned}$$

这就证明了 $\mathrm{im}(f) < R'$.

综上所述, 我们证明了这个命题. □

定义 0.4 (商环)

设 $(R, +, \cdot)$ 是一个环, 而 $I \lhd R$. 我们定义 R 对 I 的**商环**, 定义为 $(R/I, +, \cdot)$, 其中

$$R/I = \{a + I : a \in R\}.$$

而加法和乘法分别对 $a + I, b + I \in R/I (a, b \in R)$, 定义为

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I, \\ (a + I)(b + I) &= (ab) + I. \end{aligned}$$

♣

证明 我们需要证明上述定义是良定义的, 即证上述的加法和乘法是良定义的, 且商环 $(R, +, \cdot)$ 是一个环.

注意到 $(R, +)$ 是 Abel 群, 又因为 I 是 R 的理想, 所以 $(I, +)$ 是 $(R, +)$ 的子群. 从而由命题**??**可知 $(I, +)$ 是 $(R, +)$ 的正规子群. 根据命题**??**可知, 正规子群 I 的陪集的加法是良定义的, 即上述加法是良定义的.

我们要证明商环对乘法是良定义的. 令 $a + I = a' + I, b + I = b' + I$, 即 $a - a' \in I, b - b' \in I$. 我们只须证明 $ab + I = a'b' + I$, 即 $ab - a'b' \in I$. 而这是因为

$$ab - a'b' = (ab - a'b) + (a'b - a'b') = (a - a')b + a'(b - b') \in IR + RI \subset I + I = I.$$

其中倒数第二个包含关系是根据理想对乘法的“吸引”性质, 而最后一个等号是根据引理**??**及 $(I, +) < (R, +)$. 这样, 我们就证明了商环对乘法是良定义的.

接下来, 要证明商环是个环, 其实只要将 R 上环的结构（利用良定义性）照搬过来即可.

利用 I 对加法构成正规子群, 因此利用命题**??**可知,R/I 对加法构成群. 我们只须证明 R/I 对乘法构成幺半群, 且乘法对加法有左右分配律.

乘法单位元是 $1 + I$, 因为对任意 $a + I (a \in R)$, 我们有

$$(a + I)(1 + I) = (1 + I)(a + I) = a + I.$$

R/I 对乘法有结合律, 这是因为对任意 $a + I, b + I, c + I (a, b, c \in R)$, 由 $(R, +, \cdot)$ 是一个环可得

$$((a + I)(b + I))(c + I) = (ab + I)(c + I) = (ab)c + I = a(bc) + I = (a + I)((b + I)(c + I)).$$

最后, 我们要证明乘法对加法有左右分配律. 利用对称性, 我们只证明左分配律. 对任意 $a+I, b+I, c+I (a, b, c \in R)$, 由 $(R, +, \cdot)$ 是一个环可得

$$\begin{aligned} (a + I)((b + I) + (c + I)) &= (a + I)((b + c) + I) = a(b + c) + I \\ &= (ab + ac) + I = (a + I)(b + I) + (a + I)(c + I). \end{aligned}$$

综上所述, 我们就证明了 R/I 是个环. 这个环被叫做 R 对 I 的商环. □

定义 0.5 (环同构)

设 $(R, +, \cdot), (R', +, \cdot)$ 都是环,$f : (R, +, \cdot) \to (R', +, \cdot)$ 是一个映射, 我们称 f 是一个**环同构**, 若 f 既是双射, 又是环同态.

♣

引理 0.4

设 $(R,+,\cdot),(R',+,\cdot)$ 都是环,$f:(R,+,\cdot)\to(R',+,\cdot)$ 是一个映射, 则 f 是环同构, 当且仅当 f 对加法是群同构, 而对乘法是幺半群同构.

证明 必要性是显然的. 下证充分性.

由于 f 对加法是群同构, 而对乘法是幺半群同构, 因此 f 是双射, 且 f 既对加法是群同态, 又对乘法是幺半群同态. 于是由命题 0.1可知 f 是环同态. 又因为 f 是双射, 所以 f 是环同构. □

引理 0.5

设 $(R,+,\cdot),(R',+,\cdot)$ 都是环, $f:(R,+,\cdot)\to(R',+,\cdot)$ 是个环同构, 则 f^{-1} 是个环同态, 进而也是环同构.

证明 由 f 是个环同构可知,f 既对加法是群同态, 又对乘法是幺半群同态.. 从而由命题**??**和命题**??**可知, f^{-1} 既对加法是群同态, 又对乘法是幺半群同态. 于是由命题 0.1可知 f 是环同态. 又因为 f^{-1} 是双射, 所以 f^{-1} 是环同构.
□

定理 0.1 (环同构第一定理)

设 $f:(R,+,\cdot)\to(R',+,\cdot)$ 是一个环同态, 则 R 对 $\ker(f)$ 构成的商环, 同构于 $\operatorname{im}(f)$. 此即,

$$R/\ker(f)\cong\operatorname{im}(f).$$

证明 令 $\tilde f:R/\ker(f)\to\operatorname{im}(f)$, 对 $a+\ker(f)$, 定义为

$$\tilde f(a+\ker(f))=f(a).$$

我们根据群同构第一定理中对 $\tilde f$ 的证明同理可证 $\tilde f$ 是良定义的, 且对加法构成群同构. 要证明 $\tilde f$ 是环同构, 只须证明它对乘法是幺半群同态.

单位元: 由商环的定义及命题 0.4可知,$R/\ker(f)$ 的乘法单位元是 $1+\ker f$ 且 $\operatorname{im}(f)<R'$, 从而 $\operatorname{im}(f)$ 的乘法单位元就是 R' 的乘法单位元. 由 $\tilde f$ 的定义及 f 是环同态可得 $\tilde f(1+\ker f)=f(1)=1'$.

保持乘法: 令 $a+\ker(f),b+\ker(f)\in R/\ker(f)(a,b\in R)$, 则

$$\tilde f((a+\ker(f))(b+\ker(f)))=\tilde f(ab+\ker(f))=f(ab)=f(a)f(b)=\tilde f(a+\ker(f))\tilde f(b+\ker(f)).$$

综上所述,$\tilde f$ 给出了一个从商环 $R/\ker(f)$ 到像 $\operatorname{im}(f)$ 的环同构. 这就证明了这个定理. □

定理 0.2 (环同构第二定理)

设 $(R,+,\cdot)$ 是一个环, 而 $S<R,I\lhd R$. 则 $S+I<R,S\cap I\lhd S,I\lhd S+I$, 且

$$S/(S\cap I)\cong(S+I)/I.$$

证明 我们先证明 $S+I<R$. 对加法而言, 由 $S<R,I\lhd R$ 可知 $(S,+)<(R,+),(I,+)<(R,+)$, 又因为 $(R,+)$ 是 Abel 群, 所以 $(S,+),(I,+)\lhd(R,+)$. 从而由引理**??**可知 $(S+I,+)<(R,+)$. 因此我们只须证明 $S+I$ 对乘法构成幺半群, 即对乘法是封闭的, 且包含单位元. 第一,$1=1+0\in S+I$. 第二, 只须证明 $(S+I)(S+I)\subset(S+I)$. 由引理 0.1可知 $II=I$, 由引理**??**可知 $SS=S,I+I=I$. 根据 $I\lhd R$ 可知 $IS,SI=I$. 于是再利用 R 的乘法对加法满足左右分配律可得

$$(S+I)(S+I)=SS+SI+IS+II=S+I+I+I=S+I.$$

我们再证明 $S\cap I\lhd S$. 由命题**??**可知,$S\cap I$ 对加法构成子群. 我们只须证明 $S\cap I$ 对乘法的“吸收”性, 即 $(S\cap I)S\subset S\cap I$, 及 $S(S\cap I)\subset S\cap I$. 根据对称性, 我们只证明前面这个包含关系. 由 $SS=S,IS=I$ 可得

$$(S\cap I)S\subset SS=S,(S\cap I)S\subset IS=I\Leftrightarrow(S\cap I)S=S\cap IS=S\cap I.$$

根据对称性,$S\cap I\lhd S$.

我们接着证明 $I\lhd S+I$. 我们已经证明了 $S+I<R$, 因此 $S+I$ 对加法构成 Abel 群, 又 $I\subset S+I(0\in S,I=0+I\subset S+I)$, 故 $(I,+)<(S+I,+)$. 于是我们只须证明 $I(S+I)\subset I$, 及 $(S+I)I\subset I$. 根据对称性, 我们只证明前面这

个包含关系. 由 $I \lhd R$ 及 $S+I \subset R$ 可得

$$I(S+I) = IS + II = I + I = I.$$

根据对称性,$I \lhd S+I$.

我们最后证明 $S/(S\cap I) \cong (S+I)/I$. 和群同构第二定理的证明一样, 我们定义 $f: S \to (S+I)/I$, 对 $a \in S$, 定义为

$$f(a) = a + I \in (S+I)/I.$$

先证 f 是良定义的. 设 $a = a' \in S$, 则 $a - a' = 0 \in I$, 从而 $f(a) = a + I = a' + I = f(a')$. 故 f 是良定义的. 显然 f 是满射, 又由群同构第二定理的证明可知,f 对加法构成群同态, 且 $\ker(f) = \{a \in S : a + I = I\} = \{a \in S : a \in I\} = S \cap I$. 因此我们只要证明 f 对乘法是幺半群同态, 就可以利用环同构第一定理证明这个命题了. 而这是显然的, 因为若 $a, b \in S$, 则

$$f(a)f(b) = (a+I)(b+I) = ab + I = f(ab).$$

因此, 由环同构第一定理, 我们得到了

$$S/(S\cap I) \cong (S+I)/I.$$

综上所述, 我们就证明了这个命题. □

引理 0.6

设 $(R, +, \cdot)$ 是一个环,$I \lhd R, J < R$, 且 $I \subset J$, 则 $I \lhd J$.

证明 第一, 由 $I \lhd R$ 可知 $(I, +) < (R, +)$, 从而 I 对单位、加法和逆元都封闭. 又 $I \subset J$, 故 $(I, +) < (J, +)$.

第二, 由 $J < R$ 可知 $J \subset R$. 于是由 $I \lhd R$ 可得 $IJ = JI = I$.

综上,$I \lhd J$. □

定理 0.3 (环同构第三定理)

设 $(R, +, \cdot)$ 是一个环, 而 $I, J \lhd R$, 且 $I \subset J$. 则 $J/I \lhd R/I$, 且

$$(R/I)/(J/I) \cong R/J.$$

证明 首先, 由引理 0.6可知 $I \lhd J$. 故 J/I 是一个商环. 由 $I, J \lhd R$ 可知 $R/I, R/J$ 也是商环. 我们先证明 $J/I \lhd R/I$. 对加法而言 J/I 和 R/I 都是群, 从而它们都对单位元、加法和逆元封闭. 又 $J/I \subset R/I$, 故 J/I 是 R/I 的加法子群. 我们只须证明 $(J/I)(R/I) \subset J/I$, 及 $(R/I)(J/I) \subset J/I$. 根据对称性, 我们证明前面这个包含关系. 因为 $J \lhd R$, 所以

$$(J/I)(R/I) = (JR)/I \subset J/I.$$

这就证明了 $J/I \lhd R/I$.

和群同构第三定理一样, 我们令 $f: R/I \to R/J$, 对 $a + I (a \in R)$, 定义为

$$f(a+I) = a + J.$$

根据群同构第三定理的证明, 同理可知 f 是一个良定义的满射, 对加法构成群同态, 且 $\ker(f) = J/I$. 因此我们只要证明 f 对乘法是幺半群同态, 就可以利用环同构第一定理证明这个命题了. 而这是显然的, 因为若 $a+I, b+I \in R/I (a, b \in R)$, 则

$$f(a+I)f(b+I) = (a+J)(b+J) = ab + J = f(ab+I).$$

又因为 $f(1+I) = 1 + J$. 因此, 由环同构第一定理, 我们得到了

$$(R/I)/(J/I) \cong R/J. \tag{1}$$

综上所述, 我们就证明了这个命题. □