0.1 素理想与极大理想

定义 0.1 (整环)

设 $(R,+,\cdot)$ 是一个环, 则我们称 R 是个**整环**, 若它是个非零交换环, 且没有零因子, 即

$$R \neq \{0\},$$
$$R\text{是个交换环},$$
$$\forall a,b \in R, (ab = 0 \implies a = 0 \text{ 或} b = 0).$$

若 $a \neq 0$ 且 $a \in R$ 满足 $\exists b \neq 0$ 且 $b \in R$ 使得 $ab = 0$, 我们就称 a 为 R 的一个**零因子**. ♣

引理 0.1

若 p 是一个素数,$a,b \in \mathbb{Z}$, 则

$$p \mid ab \iff p \mid a \text{ 或} p \mid b$$

♡

证明 见初等数论. □

定义 0.2 (合数)

除了 1 和其本身外还有其他正因数的大于 1 的正整数就称为**合数**. 此即大于 1 的不是素数的正整数. ♣

引理 0.2

若 n 是一个合数, 则存在 $a,b \in \mathbb{Z}$, 使得

$$n \mid ab, n \nmid a, n \nmid b.$$

♡

证明 证明是简单的. 若 n 是一个合数, 我们可以取一个非平凡分解 $n = ab$, 其中 $a,b \neq \pm 1$. 则 $n \mid ab$, 可是 $|n| > |a|$, 故 $n \nmid a$（因为若一个数整除另一个数, 则这个数的绝对值必须小于等于另一个数）. 同理 $n \nmid b$. 这样, 我们就证明了这个引理. □

定义 0.3 (素理想)

设 $(R,+,\cdot)$ 是一个交换环, 而 $\mathfrak{p} \lhd R$, 则我们称 $\mathfrak{p}$ 是个**素理想**, 若

$$\forall a,b \in \mathbb{Z}, (ab \in \mathfrak{p} \iff a \in \mathfrak{p} \text{ 或} b \in \mathfrak{p}),$$
$$\mathfrak{p} \neq R.$$

♣

例题 0.1 证明:$p\mathbb{Z}$ 是整数环 $(\mathbb{Z},+,\cdot)$ 的素理想, 而 $m\mathbb{Z}$,$\mathbb{Z}$ 不是整数环 $(\mathbb{Z},+,\cdot)$ 的素理想, 其中 p 是素数,m 是合数.

证明 首先由命题**??**可知 $p\mathbb{Z}$,$m\mathbb{Z}$,$\mathbb{Z}$ 都是 $\mathbb{Z}$ 的理想.

由引理 0.1可知, 对 $\forall a,b \in \mathbb{Z}$

$$ab \in p\mathbb{Z} \Leftrightarrow p \mid ab \Leftrightarrow p \mid a \text{或} p \mid b \Leftrightarrow a \in p\mathbb{Z} \text{或} b \in p\mathbb{Z}.$$

故 $p\mathbb{Z}$ 是整数环 $(\mathbb{Z},+,\cdot)$ 的素理想.

而由引理 0.2可知

$$ab \in m\mathbb{Z} \Leftrightarrow m \mid ab \Rightarrow m \nmid a \text{且} m \nmid b \Leftrightarrow a \notin m\mathbb{Z} \text{或} b \notin m\mathbb{Z}.$$

故 $m\mathbb{Z}$ 不是整数环 $(\mathbb{Z},+,\cdot)$ 的素理想.

又因为素理想一定不是整个环, 所以 $\mathbb{Z}$ 也不是整数环 $(\mathbb{Z},+,\cdot)$ 的素理想. □

命题 0.1

若 $m, n \in \mathbb{N}_1$, 由命题??可知 $m\mathbb{Z}, n\mathbb{Z}$ 一定是整数环的理想. 则

$$m\mathbb{Z}\text{和}n\mathbb{Z}\text{互素} \iff m, n\text{互素}.$$

证明 由理想互素的定义和命题??可知

$$\begin{aligned} m\mathbb{Z}\text{和}n\mathbb{Z}\text{互素} &\iff m\mathbb{Z}+n\mathbb{Z}=\mathbb{Z} \\ &\iff 1 \in m\mathbb{Z}+n\mathbb{Z} \\ &\iff \exists k, l \in \mathbb{Z}, \text{ s.t. } 1 = mk+nl \end{aligned}$$

又由 Bézout 定理可知

$$\exists k, l \in \mathbb{Z}, \text{ s.t. } 1 = mk+nl \iff \gcd(m,n)=1 \iff m, n\text{互素}$$

故

$$m\mathbb{Z}\text{和}n\mathbb{Z}\text{互素} \iff m, n\text{互素}.$$

□

命题 0.2 (素理想的充要条件)

设 $(R, +, \cdot)$ 是一个交换环, 而 $\mathfrak{p} \lhd R$. 则 $\mathfrak{p}$ 是一个素理想, 当且仅当商环 $R/\mathfrak{p}$ 是一个整环.

证明 先证必要性. 令 $\mathfrak{p}$ 是一个素理想. 因为 R 是交换环, 则显然 $R/\mathfrak{p}$ 也是交换环. 因为对 $a, b \in R$, 我们有

$$(a+\mathfrak{p})(b+\mathfrak{p}) = ab+\mathfrak{p} = ba+\mathfrak{p} = (b+\mathfrak{p})(a+\mathfrak{p}).$$

而且因为 $\mathfrak{p} \neq R$, 所以任取 $r \in R - \mathfrak{p}$, 则 $r+\mathfrak{p} \in R/\mathfrak{p}$. 注意到 $\mathfrak{p} \in R/\mathfrak{p}$, 且 $r \notin \mathfrak{p}$, 因此 $r+\mathfrak{p} \neq \mathfrak{p}$. 故 $R/\mathfrak{p}$ 中此时至少有两个互异的元素, 即 $R/\mathfrak{p}$ 不是零环.

我们只须证明 $R/\mathfrak{p}$ 中没有零因子. 假设

$$(a+\mathfrak{p})(b+\mathfrak{p}) = 0+\mathfrak{p} \Leftrightarrow ab+\mathfrak{p} = \mathfrak{p} \Leftrightarrow ab \in \mathfrak{p}.$$

根据 $\mathfrak{p}$ 是素理想, 不失一般性假设 $a \in \mathfrak{p}$. 则

$$a+\mathfrak{p} = 0+\mathfrak{p}.$$

这就证明了 $R/\mathfrak{p}$ 是一个整环.

再证充分性. 假设 $R/\mathfrak{p}$ 是一个整环. 类似地, 我们知道因为 $R/\mathfrak{p}$ 不是零环, 所以 $\mathfrak{p} \neq R$. 否则 $R/\mathfrak{p} = R/R = 0+R$, 只含一个元素, 与 R/R 不是零环矛盾.

再令 $a, b \in R$, 使得 $ab \in \mathfrak{p}$, 则

$$ab+\mathfrak{p} = (a+\mathfrak{p})(b+\mathfrak{p}) = 0+\mathfrak{p}.$$

由于 $R/\mathfrak{p}$ 是一个整环, 故不失一般性假设 $a+\mathfrak{p} = 0+\mathfrak{p}$, 这就证明了 $a \in \mathfrak{p}$, 即 $\mathfrak{p}$ 是一个素理想. □

定义 0.4 (极大理想)

设 $(R, +, \cdot)$ 是一个交换环, 而 $\mathfrak{m} \lhd R$. 则我们称 $\mathfrak{m}$ 是一个**极大理想**, 若 $\mathfrak{m} \neq R$, 且它是个极大的理想, 即对于任意 $I \lhd R$, 如果 $I \supsetneq \mathfrak{m}$, 则

$$I = R.$$

这就是说, 唯一严格大于 $\mathfrak{m}$ 的理想, 是整个环.

命题 0.3 (极大理想的充要条件)

设 $(R, +, \cdot)$ 是一个交换环, 而 $\mathfrak{m} \lhd R$. 则 $\mathfrak{m}$ 是一个极大理想, 当且仅当商环 $R/\mathfrak{m}$ 是一个域.

证明 先证必要性. 令 $\mathfrak{m}$ 是一个极大理想. 因为 R 是交换环, 从而对 $a, b \in R$, 我们有

$$(a+\mathfrak{m})(b+\mathfrak{m}) = ab+\mathfrak{m} = ba+\mathfrak{m} = (b+\mathfrak{m})(a+\mathfrak{m}).$$

所以 $R/\mathfrak{m}$ 是交换环, 因此我们只须证明每个非零元素都有逆元. 令 $a+\mathfrak{m} \in R/\mathfrak{m}$ 且 $a+\mathfrak{m} \neq 0+\mathfrak{m}$, 也就是说 $a \notin \mathfrak{m}$. 只须证明存在 $b+\mathfrak{m} \in R/\mathfrak{m}(b \in R)$, 使得 $ab+\mathfrak{m} = 1+\mathfrak{m}$. 等价地, 我们只须证明存在 $b \in R, m \in \mathfrak{m}$, 使得

$$1 = ab + m.$$

由命题**??**可知 $\mathfrak{m}+(a) = \mathfrak{m}+Ra$, 又因为 $a \notin \mathfrak{m}$, 所以 $\mathfrak{m}+(a) = \mathfrak{m}+Ra$ 是一个严格包含了 $\mathfrak{m}$ 的理想. 因为 $\mathfrak{m}$ 是极大理想, 所以 $\mathfrak{m}+Ra = R$. 右边取 $1 \in R$, 我们就得到了, 存在 $b \in R, m \in \mathfrak{m}$, 使得 $1 = ab+m$, 这就证明了必要性.

再证充分性. 如果 $R/\mathfrak{m}$ 是一个域,$\mathfrak{m}$ 是一个极大理想, 那么对于任意理想 $I \supsetneq \mathfrak{m}$. 由命题**??**可知 $0 \neq 1$, 从而 $0+\mathfrak{m} \neq 1+\mathfrak{m}$, 于是 $1 \notin \mathfrak{m}$. 故 $\mathfrak{m} \neq R$, 否则, 由命题**??**可知 $1 \in \mathfrak{m}$ 矛盾!

再任取 $a \in I - \mathfrak{m}$. 则 $a+\mathfrak{m} \neq 0+\mathfrak{m}$. 由于 $R/\mathfrak{m}$ 是一个域, 故 $a+\mathfrak{m}$ 有逆元, 即存在 $b \in R$, 使得 $(a+\mathfrak{m})(b+\mathfrak{m}) = ab+\mathfrak{m} = 1+\mathfrak{m}$. 因此, 也存在 $m \in \mathfrak{m}$, 使 $1 = ab+m$. 因此, 对任意 $r \in R$, 由 I 和 $\mathfrak{m}$ 都是 R 的理想可知

$$r = r(ab+m) = rab + rm \in Ib + \mathfrak{m} \subset I + I = I.$$

这就证明了 $I \subset R$. 又因为 $I \subset R$, 所以 $I = R$. 因此 $\mathfrak{m}$ 是一个极大理想.

综上所述, 我们就证明了这个命题. □

引理 0.3 (域一定是整环)

设 $(R, +, \cdot)$ 是一个域, 则 R 是一个整环. ♡

证明 由域的定义可知, 一个域当然是一个交换环. 又由命题**??**可知 $0 \neq 1$, 故 $0, 1 \in R$, 因此 $R \neq \{0\}$. 令 $a, b \in R$, 使 $ab = 0$. 我们只须证明 $a = 0$ 或 $b = 0$.

假设 $a \neq 0, b \neq 0$, 而 $ab = 0$. 由 R 是域可知, 存在 $c, d \in R$, 使 $ac = bd = 1$. 则

$$1 = 1 \cdot 1 = acbd = abcd = 0 \cdot cd = 0.$$

而由命题**??**可知 $0 \neq 1$ 矛盾! 因此每一个域都是整环. □

命题 0.4

设 $(R, +, \cdot)$ 是一个交换环, 则每一个极大理想都是素理想. ♠

证明 证法一: 令 $\mathfrak{m}$ 是一个极大理想, 则 $R/\mathfrak{m}$ 是一个域. 根据引理 0.3可知,$R/\mathfrak{m}$ 是一个整环, 再利用命题 0.2可知 $\mathfrak{m}$ 是一个素理想. 这就证明了这个命题.

证法二: 令 $\mathfrak{m}$ 是一个极大理想. 假设 $a, b \in R$, 使得 $ab \in \mathfrak{m}$, 我们只须证明 $a \in \mathfrak{m}$ 或 $b \in \mathfrak{m}$. 用反证法, 假设 $a, b \notin \mathfrak{m}$. 则由命题**??**可知 $\mathfrak{m}+(a) = \mathfrak{m}+Ra$, 又因为 $a \notin \mathfrak{m}$, 所以 $\mathfrak{m}+(a) = \mathfrak{m}+Ra$ 是一个严格包含了 $\mathfrak{m}$ 的理想. 因为 $\mathfrak{m}$ 是极大理想, 这就迫使

$$R = \mathfrak{m} + Ra.$$

从而由 $1 \in R$ 可知, 存在 $m \in \mathfrak{m}$ 与 $r \in R$, 使

$$1 = m + ra.$$

则由于 $ab \in \mathfrak{m}$ 及 $\mathfrak{m}$ 是一个理想, 我们有

$$b = bm + r(ab) \in \mathfrak{m} + r\mathfrak{m} \subset \mathfrak{m} + \mathfrak{m} = \mathfrak{m}.$$

可是这与 $b \notin \mathfrak{m}$ 相矛盾. 因此,$\mathfrak{m}$ 是一个素理想. □

定义 0.5 (模理想同余)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \lhd R$. 令 $a, b \in R$, 我们称 a, b **模 I 同余**, 记作

$$a \equiv b \bmod I$$

若它们的差在 I 中, 即

$$a - b \in I$$

或等价地,

$$a + I = b + I$$

命题 0.5 (模理想同余是一个等价关系)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \lhd R$. 令 $a, b, c \in R$, 则

(1) $a \equiv a \bmod I$.

(2) 若 $a \equiv b \bmod I$, 则 $b \equiv a \bmod I$.

(3) 若 $a \equiv b \bmod I, b \equiv c \bmod I$, 则 $a \equiv c \bmod I$.

证明

(1) 因为 $a - a = 0 \in I, (I, +) < (R, +)$, 所以 $a \equiv a \bmod I$.

(2) 由 $a \equiv b \bmod I$ 可知 $a - b \in I$. 于是由 $(I, +) < (R, +)$ 可知 $b - a = -(a - b) \in I$. 故 $b \equiv a \bmod I$.

(3) 由 $a \equiv b \bmod I, b \equiv c \bmod I$ 可知 $a - b, b - c \in I$. 从而由 $(I, +) < (R, +)$ 可知 $a - c = (a - b) + (b - c) \in I$. 故 $a \equiv c \bmod I$.

□

定义 0.6

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \lhd R$. 令 $a, b \in R$, 令 $a \in R$, 我们定义 a 在模 I 同余关系下的等价类为

$$\bar{a} = \{b \in R : b \equiv a \bmod I\}.$$

命题 0.6

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \lhd R, a \in R$, 则

$$\bar{a} = \{b \in R : b \equiv a \bmod I\} = a + I.$$

进而,$R/I = a + I : a \in R$ 就是 R 在模 I 同余关系下的一个分拆.

证明 根据定义 0.6可知

$$\bar{a} = \{b \in R : b \equiv a \bmod I\} = \{b \in R : b - a \in I\} = \{b \in R : b \in a + I\} = a + I.$$

□

命题 0.7 (模理想同余的基本性质)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \lhd R$. 令 $n \in \mathbb{N}_1, a, b, c, d \in R$. 若

$$a \equiv b \bmod I$$

$$c \equiv d \bmod I$$

则

$$a + c \equiv b + d \bmod I$$

$$ac \equiv bd \bmod I$$

$$a^n \equiv b^n \bmod I$$

进而,$f(a) \equiv f(b) \bmod I$. 其中 $f(x)$ 是关于 x 的多项式.

注 一个关系若对加法、乘法和幂次都成立, 则它就一定对多项式也成立.

证明 由 $a \equiv b \bmod I, c \equiv d \bmod I$ 可知 $a-b, c-d \in I$.

第一条, 因为 $(I,+) < (R,+)$,$(R,+)$ 是 Abel 群, 所以 $(a+c)-(b+d) = (a-b)+(c-d) \in I$. 故 $a+c \equiv b+d \bmod I$.

第二条, 由 $a-b, c-d \in I$ 可知存在 $r, s \in I$, 使得 $a = b+r, c = d+s$. 从而由 I 是 R 的理想可得

$$ac - bd = (b+r)(d+s) - bd = bs + rd + rs \in I.$$

故 $ac \equiv bd \bmod I$.

第三条, 结合数学归纳法, 反复利用第二条结论即可得到 $a^n \equiv b^n \bmod I$. □

定理 0.1 (中国剩余定理)

设 $(R,+,\cdot)$ 是一个交换环, 而 $(I_i)_{1\leqslant i\leqslant n}$ 是一族两两互素的理想, 即对任何 $i \neq j$ 都有 $I_i + I_j = R$. 则对任何 $a_1, \cdots, a_n \in R$, 都存在 $x \in R$, 使

$$x \equiv a_1 \bmod I_1,$$
$$\cdots$$
$$x \equiv a_n \bmod I_n.$$

♡

证明 令 $a = (a_1, \cdots, a_n)$, 则

$$a = a_1(1,0,\cdots,0) + \cdots + a_n(0,\cdots,0,1).$$

假如 $x_i(1 \leqslant i \leqslant n)$ 分别满足

$$x_i \equiv 1 \bmod I_i.$$
$$若 j \neq i,\ x_i \equiv 0 \bmod I_j.$$

则根据模理想同余的基本性质可知,$x = a_1x_1 + \cdots + a_nx_n$ 就一定满足了同余方程组

$$x \equiv a_1 \bmod I_1,$$
$$\cdots$$
$$x \equiv a_n \bmod I_n.$$

因此我们只须证明对任何 $1 \leqslant i \leqslant n$, 我们能找到 $x_i \in R$, 使得

$$x_i \equiv 1 \bmod I_i,$$
$$若 j \neq i,\ x_i \equiv 0 \bmod I_j.$$

不失一般性, 我们假设 $i = 1$. 由于 I_1 与 $I_j(j \neq 1)$ 都互素, 特别地,$1 \in I_1 + I_j(j \neq 1)$. 则存在 $b_j \in I_1, c_j \in I_j(j \neq 1)$, 使得

$$b_2 + c_2 = 1,$$
$$\cdots$$
$$b_n + c_n = 1.$$

令 $x_1 = c_2 \cdots c_n \in R$. 则对任何 $j \neq 1$, 由 $I_j \lhd R$, 我们有

$$c_2 \cdots c_j \cdots c_n \in I_j.$$

即

$$x_1 \equiv c_2 \cdots c_j \cdots c_n \equiv 0 \bmod I_j.$$

并且

$$1 - c_2 \cdots c_n = (b_2 + c_2) \cdots (b_n + c_n) - (c_2 \cdots c_n).$$

根据分配律, 将上式展开后, 上面的每一项都包含至少某个 $b_i \in I_1$ 作为因子, 因此

$$1 - c_2 \cdots c_n \in I_1.$$

于是

$$x_1 = c_2 \cdots c_n \equiv 1 \bmod I_1.$$

这就完成了 x_1 的构造. 类似地, 我们可以构造出所有的 $x_i(1 \leqslant i \leqslant n)$, 因此

$$x \equiv a_1 x_1 + \cdots + a_n x_n.$$

给出了原命题所需的解.

综上所述, 我们通过线性性对原同余方程组进行了化简, 并不失一般性地证明了 $i = 1$ 的情形, 这就完成了中国剩余定理的证明. □

命题 0.8 (中国剩余定理推论)

设 $(R, +, \cdot)$ 是一个交换环, 而 $(I_i)_{1 \leqslant i \leqslant n}$ 是一族两两互素的理想, 即对任何 $i \neq j$ 都有 $I_i + I_j = R$. 则

$$\pi : R \to \prod_{i=1}^{n} (R/I_i),$$

$$\pi(a) = (a + I_1, \cdots, a + I_n).$$

是个满同态. 特别地,

$$R/\bigcap_{i=1}^{n} I_i \simeq \prod_{i=1}^{n} (R/I_i).$$

因此在以上条件下,π 是个同构当且仅当

$$\bigcap_{i=1}^{n} I_i = \{0\}.$$

证明 π 的每一个坐标都是环同态, 因此 π 也是环同态. 根据中国剩余定理的证明可知, 对任意 $(a_1 + I_1, \cdots, a_n + I_n) \in \prod_{i=1}^{n} (R/I_i)$, 都存在 $a \in R$, 使得

$$a \equiv a_i \bmod I_i \; (i = 1, 2, \cdots, n) \iff a + I_i = a_i + I_i \; (i = 1, 2, \cdots, n)$$
$$\iff \pi(a) = (a + I_1, \cdots, a + I_n) = (a_1 + I_1, \cdots, a_n + I_n).$$

故 π 是个满同态. 我们只须找到 π 的核即可. 根据 π 的定义,

$$\begin{aligned} \pi(a) = 0 &\iff \forall i, a + I_i = 0 + I_i \\ &\iff \forall i, a \in I_i \\ &\iff a \in \bigcap_{i=1}^{n} I_i. \end{aligned}$$

因此 $\ker \pi = \bigcap_{i=1}^{n} I_i$. 根据环同构第一定理, 这就证明了

$$R/\bigcap_{i=1}^{n} I_i \simeq \prod_{i=1}^{n} (R/I_i).$$

因此在以上的条件下,π 是同构当且仅当 π 是单的, 当且仅当 $\ker(\pi) = \{0\}$, 当且仅当

$$\bigcap_{i=1}^{n} I_i = \{0\}.$$

因此, 最特殊的情况即 R 中有有限多个两两互素且总的交集为 $\{0\}$ 的理想. 在这种情况下,

$$R \simeq \prod_{i=1}^{n} (R/I_i).$$

综上所述, 我们证明了这个命题. □

推论 0.1

设 $n \in \mathbb{N}_1$, 由算术基本定理可知,n 存在素幂因子分解, 即存在 $p_1, p_2, \cdots, p_m$ 两两互素,$\alpha_1, \alpha_2, \cdots, \alpha_m \in \mathbb{N}_1$, 使得

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}.$$

则

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \mathbb{Z}_{\prod_{i=1}^m p_i^{\alpha_i}} \cong \prod_{i=1}^m \mathbb{Z}_{p_i^{\alpha_i}}.$$

♡

证明 由命题**??**可知

$$n\mathbb{Z} = \prod_{i=1}^m p_i^{\alpha_i}\mathbb{Z} = \bigcap_{i=1}^m \left(p_i^{\alpha_i}\mathbb{Z}\right).$$

从而由中国剩余定理推论可知

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\bigcap_{i=1}^m \left(p_i^{\alpha_i}\mathbb{Z}\right) \cong \prod_{i=1}^m \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right) = \prod_{i=1}^m \mathbb{Z}_{p_i^{\alpha_i}}.$$

□