0.1 主理想整环与唯一分解整环

定义 0.1 (主理想整环)

设 $(R,+,\cdot)$ 是一个交换环, 则我们称 R 是个**主理想整环**, 若 R 是一个整环, 而且每一个理想 $I \lhd R$ 都是主理想, 即可以写成

$$I = (a) = Ra$$

的形式.

命题 0.1

$(\mathbb{Z},+,\cdot)$ 是个主理想整环.

证明

□

引理 0.1

$(\mathbb{Z},+,\cdot)$ 的每个子群都具有 $n\mathbb{Z}$ 的形式.

证明 不妨令 $I < \mathbb{Z}$ 是加法子群.

假如 I 只包含了 0 一个元素, 那么 $I = \{0\} = 0\mathbb{Z}$.

假设 I 包含了 0 以外的元素, 那么根据逆元的封闭性,I 一定包含了一个正整数. 根据自然数集的良序公理, 我们可以取到最小的那个正整数, 称其为 n. 下面, 我们只须证明

$$I = n\mathbb{Z}$$

一方面, 因为 $n \in I$, 则 n 生成的（加法）子群也包含于 I, 而前者正是 $n\mathbb{Z}$, 因此

$$n\mathbb{Z} \subset I$$

另一方面, 假设存在 $I \setminus n\mathbb{Z}$ 的元素, 我们任取 $m \in I \setminus n\mathbb{Z}$. 则根据带余除法, 我们有

$$m = qn + r$$

其中 $1 \leqslant r \leqslant n-1$.

则根据子群的性质,

$$r = m - qn = m + (-q)n \in I$$

而这与 n 是 I 最小的正整数的事实相矛盾. 这就证明了这个引理, 进而证明了上面的命题, 即 $(\mathbb{Z},+,\cdot)$ 是个主理想整环. □

命题 0.2

若 $(R,+,\cdot)$ 是一个域, 则 R 是一个主理想整环.

证明

□

引理 0.2

若 $(R,+,\cdot)$ 是一个环, 则 R 是一个域当且仅当 $\{0\}$ 和 R 是 R 中唯二的理想 $(R \neq \{0\})$.

证明 先证充分性. 假设 R 是一个域, 而 I 是一个理想. 假设 $I \neq \{0\}$, 任取 $a \neq 0$. 则存在 $b \in R$, 使得

$$ab = 1$$

因此

$$1 \in Ra \subset RI \subset I$$

所以 $I = R$.

再证必要性. 假设 R 唯二的理想是零和整个环. 令 $a \neq 0$, 则 $(a) \neq 0$, 因此 $(a) = R$. 于是存在 $b, c \in R$, 使得

$$ab = 1 \in R$$

$$ca = 1$$

下面我们只须证明 $b = c$, 而证明方法和我们当时证明逆元是唯一时是一样的.

$$b = 1b = cab = c1 = c$$

这样, 就证明了 R 是一个域. □

命题 0.3

设 $(R, +, \cdot)$ 是一个主理想整环, 而 $\mathfrak{p} \lhd R$ 是一个素理想且 $\mathfrak{p} \neq \{0\}$, 则 $\mathfrak{p}$ 是一个极大理想.

证明 用反证法. 假设 $\mathfrak{p}$ 是素理想, 而不是极大理想, 则存在 $I \lhd R$, 使得 $\mathfrak{p} \subsetneq I \neq R$.

因为 R 是主理想整环, 我们记 $\mathfrak{p} = (p), I = (a)$. 则由于 $\mathfrak{p} \subset I$, 我们有

$$p \in I = (a)$$

故存在 $b \in R$, 使得

$$p = ab$$

显然,b 不能是单位（即存在乘法逆元的元素）, 因为不然的话我们就可以写 $a = pb^{-1}$, 进而 $\mathfrak{p} = I$, 导致矛盾. 因此,b 没有乘法逆元.

另外, 由于 I 是真理想, 故 a 也不是单位——否则 $1 \in (a)$, 进而 $(a) = R$.

现在 $ab \in \mathfrak{p}$, 则 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$. 假如 $a \in \mathfrak{p} = (p)$, 则不难证明 b 就是一个单位, 而这是不可能的. 假如 $b \in \mathfrak{p}$, 则同理,a 就是一个单位, 而这也是不可能的. 无论如何, 我们都会得到矛盾.

因此, 我们就证明了, 在主理想整环中, 每一个素理想都是极大理想, 因此两个概念在主理想整环中是等价的.
□

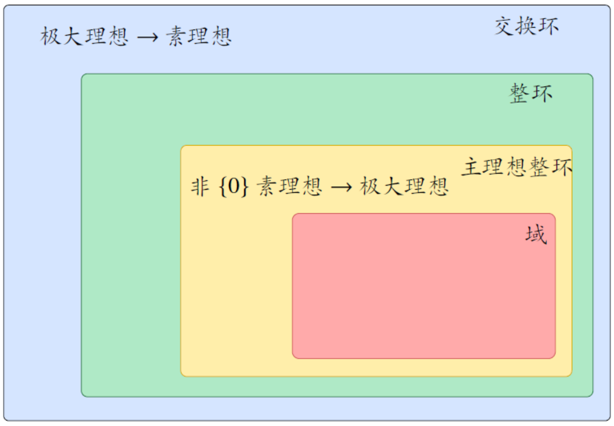

图 1: 环的层级关系以及素理想和极大理想之间的关系

命题 0.4

若 p 是一个素数, 则 $\mathbb{Z}_p$ 是一个域.

证明

□

** 命题 2.32**

命题 0.5

$\mathbb{Z}_p$ 是一个域.

证明 我们知道 $p\mathbb{Z} \lhd \mathbb{Z}$ 是个素理想, 而 $\mathbb{Z}$ 是个主理想整环, 因此 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想. 根据之前的引理, 这就证明了 $\mathbb{Z}_p$ 是一个域. □

定义 0.2

若 p 是一个素数, 则我们把 $\mathbb{Z}_p$ 记作 $\mathbb{F}_p$. 特别地, 这是一个有限域, 即只有有限多个元素的域.

引理 0.3

若 n 是一个合数, 则 $\mathbb{Z}_n$ 不是一个域.

证明 证明是类似的, 故留做练习. □