主理想整环与 Euclid 环

定义 1 (生成的理想)**.** 设 R 是环，集合 $A \subset R$，称包含 A 的 R 的最小理想为集合 A **生成的理想**，记作 $\langle A \rangle$.

由于理想的交仍为理想，所以 A 生成的理想也可定义为 R 中所有包含 A 的理想的交. 且 $\langle A \rangle$ 总是存在.

定义 2 (主理想)**.** 若集合 A 只包含一个元素 a，则由 A 生成的理想称为**主理想**，记作 $\langle a \rangle$.

定义 3 (主理想环)**.** 若交换幺环 R 的理想都是主理想，则称 R 为**主理想环**.

注. *主理想环定义在交换幺环上，避免左理想、右理想以及双边理想的讨论.*

定义 4 (主理想整环)**.** 定义在整环上的主理想环，即无零因子的主理想环称为**主理想整环**，记为 PID.

命题 1. $\mathbb{Z}$ 是主理想整环.

交换幺环 R 中，由 a 生成的主理想可以写成

$$\langle a \rangle = \{ra \mid r \in R\}.$$

下面是主理想整环中的一些性质.

性质 1. 设 R 是 PID，$a, b \in R$，则 $a \mid b \iff \langle a \rangle \supset \langle b \rangle$.

证明. 若 $a \mid b$，则存在 $r \in R$ 使得 $b = ra$，于是

$$\langle b \rangle = \{bx \mid x \in R\} = \{rax \mid x \in R\} = r \cdot \langle a \rangle \subset \langle a \rangle.$$

反之，若 $\langle a \rangle \supset \langle b \rangle$，则 $b \in \langle b \rangle \subset \langle a \rangle$，存在 $c \in R$ 使得 $b = ca$，于是 $a \mid b$. □

推论 1. $a \sim b \iff \langle a \rangle = \langle b \rangle$.

推论 2. $a \sim 1 \iff \langle a \rangle = \langle 1 \rangle = R$.

定义 5 (主理想升链)**.** 对整环 R 中的一个主理想序列，若有

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_n \rangle \subset \langle a_{n+1} \rangle \subset \cdots,$$

则称这个序列为**主理想升链**.

定义 6 (主理想升链条件)**.** 若在 R 的任一主理想升链中，存在 m，当 $n > m$ 时，有 $\langle a_m \rangle = \langle a_n \rangle$，则称 R 满足**主理想升链条件**.

由主理想整环中的性质立即可得，主理想升链条件和因子链条件是互相等价的.

定理 1. 主理想整环是唯一析因环.

证明. 只需证明主理想整环 R 满足主理想升链条件和最大公因子条件即可.

设主理想整环 R 中有一主理想升链

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_n \rangle \subset \langle a_{n+1} \rangle \subset \cdots,$$

并设 $I = \bigcup \langle a_k \rangle$，对任意 $a \in \langle a_i \rangle, b \in \langle a_j \rangle$，不妨设 $i \leqslant j$，则 $a \in \langle a_i \rangle \subset \langle a_j \rangle$，于是 $a - b \in \langle a_j \rangle \subset I$. 且对任意 $r \in R$，有 $ra \in \langle a_j \rangle \subset I$，于是 I 是 R 的理想. 又因为 R 是主理想整环，于是存在 $d \in R$ 使得 $I = \langle d \rangle$. 于是 $d \in I$，存在 $m \in \mathbb{N}^+$ 使得 $d \in \langle a_m \rangle = \{ra_m \mid r \in R\}$，存在 $r_0 \in R$ 使得 $d = r_0 a_m$，于是 $a_m \mid d$，有 $\langle d \rangle \subset \langle a_m \rangle$，于是有

$$I = \langle d \rangle \subset \langle a_m \rangle \subset \cdots \subset \langle a_n \rangle \subset I,$$

对任意 $n > m$，有 $\langle a_m \rangle = \langle a_n \rangle$，于是 R 满足主理想升链条件.

对任意 $\langle a_i \rangle, \langle a_j \rangle$，按理想的等价条件可以证明 $\langle a_i \rangle + \langle a_j \rangle$ 仍是理想. 于是存在 $d \in R$ 使得 $\langle d \rangle = \langle a_i \rangle + \langle a_j \rangle$，于是 $\langle a_i \rangle \subset \langle d \rangle$，$\langle a_j \rangle \subset \langle d \rangle$，则 $d \mid a$，$d \mid b$. 若另有 $c \mid a$，$c \mid b$，则 $\langle a_i \rangle \subset \langle c \rangle$，$\langle a_j \rangle \subset \langle c \rangle$，则 $\langle a_i \rangle + \langle a_j \rangle \subset \langle c \rangle$，即 $\langle d \rangle \subset \langle c \rangle$，于是 $c \mid d$. □

推论 3. 设 R 是 PID，$a, b, d \in R$，若 d 是 a, b 的最大公因子，则存在 $u, v \in R$ 使得

$$d = ua + vb.$$

推论 4. a, b 互素的充要条件是存在 $u, v \in R$ 使得

$$ua + vb = 1.$$

由于主理想整环是唯一析因环，于是满足最大公因子条件，即任意两个非零元素的最大公因子都存在. 在整数环中，求任意两个整数的最大公因子，用到了**辗转相除法**，但并不是所有环都可以用这个方法. 把那些可以进行辗转相除法的整环称为 Euclid 环. 具体地，有

定义 7 (Euclid 环)**.** 设 R 是整环，若存在映射 $\delta : R \to \mathbb{N}$ 使得任意 $a, b \in R$，且 $b \neq 0$，都存在 $q, r \in R$ 使得

$$a = qb + r, \qquad \delta(r) < \delta(b),$$

则称 R 为 **Euclid 环**，记为 ED.

注. 可以进行辗转相除等价于满足带余除法条件. 定义中的映射 δ 未必唯一.

定理 2. Euclid 环是主理想整环.

证明. 证明 Euclid 环 R 中的理想都是主理想即可. 设 $I \lhd R$，若 $I = \{0\}$，则 $I = \langle 0 \rangle$ 是主理想. 下设 $I \neq 0$，则 I 中存在 $b \neq 0$，取为

$$\delta(b) = \min \{\delta(c) \mid c \in I, c \neq 0\},$$

对任意 $a \in I$，由 Euclid 环定义，存在 $q, r \in R$ 使得 $a = qb + r$ 且 $\delta(b) > \delta(r)$，于是 $r = 0$，则 $a = qb$，于是 $I = \langle b \rangle$. □

推论 5. Euclid 环是主理想整环，因而也是唯一析因环.