

唯一析因环

定义 1 (有限析因条件). 在整环 R 中, 对任意 $a \in R^* \setminus U$, 都可以分解为有限个不可约元素的乘积 $p_1 p_2 \cdots p_n$, 则称整环 R 满足**有限析因条件**.

定义 2 (唯一析因环). 若整环 R 满足有限析因条件且分解在相伴意义下唯一, 则称 R 为**唯一析因环**或**唯一分解整环**, 记为 UFD.

注. UFD 是使因式分解唯一性成立的整环, 类比于数论中的算术基本定理.

定义 3 (因子链). 若 R^* 中的一个序列 $a_1, a_2, \cdots, a_n, a_{n+1}, \cdots$ 满足 $a_{n+1} \mid a_n$, 则称这个序列是 R 的一个**因子链**.

定义 4 (因子链条件). 若 R 中不存在无限真因子链, 则称 R 满足**因子链条件**.

注. 也就是说, 存在 m , 对任意 $n \geq m$, 有 $a_m \sim a_n$.

引理 1. 若整环 R 满足因子链条件, 则一定满足有限析因条件.

证明. 对任意 $a \in R^* \setminus U$, 先证 a 有不可约因子. 若 a 是不可约元素, 则自然成立. 下设 a 是可约的. 设 $a = a_1 b_1$, 这里 a_1, b_1 都是非平凡的真因子. 若 a_1 是不可约元素, 则自然成立. 下设 a_1 是不可约的. 以此类推, 得到因子链

$$a, a_1, a_2, \cdots,$$

由因子链条件, 存在 m 使得 $a_m \sim a_{m+1}$, 于是 a_m 是不可约的, 即 a_m 是 a 的不可约因子.

再证 a 可以分解成有限个不可约因子的乘积. 设 p_1 是 a 的一个不可约因子, 则有 $a = p_1 a'$. 若 $a' \in U$, 则 $a = (p_1 a')$, 其中 $(p_1 a')$ 是不可约元素. 若 $a' \in R^* \setminus U$, 则 a' 有不可约因子, 设 $a' = p_2 a''$, 若 $a'' \in U$, 则 $a = p_1 (p_2 a'')$. 否则, a'' 有不可约因子. 以此类推, 得到因子链

$$a, a', a'', \cdots, a^{(n)}, a^{(n+1)}, \cdots,$$

由因子链条件, 存在 s 使得 $a^{(s)} \sim a^{(s+1)}$, 于是 $a^{(s)}$ 是不可约的, 得到

$$a = p_1 p_2 \cdots (p_s a^{(s)}).$$

□

定理 1. 若 R 是整环, 则以下命题等价.

1. R 是唯一析因环.

2. R 满足因子链条件和最大公因子条件.

3. R 满足因子链条件和素性条件.

证明. $1 \rightarrow 2$: 设 $a \in R^* \setminus U$ 可以分解为

$$a = p_1 p_2 \cdots p_r,$$

其中 p_i 为不可约元素. 称 r 为 a 的长度, 记作 $|a| = r$.

设 $a_1, a_2, \cdots, a_n, \cdots$ 是 R 中的一条因子链, 于是

$$|a_1| \geq |a_2| \geq \cdots \geq |a_n| \geq \cdots,$$

由于 $|a_i|$ 是非负整数, 于是存在 m 使得 $|a_m| = |a_{m+1}|$, 于是 $a_m \sim a_{m+1}$, R 满足因子链条件.

设 $a, b \in R$, 若其中之一为单位, 则 $(a, b) = 1$. 现设 $a, b \in R^* \setminus U$, 在相伴意义下对分解归类, 有

$$a = u_1 p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},$$

$$b = u_2 p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

其中 $u_1, u_2 \in U$, p_i 是互不相同的不可约元素. 令 $k_i = \min \{n_i, m_i\}$, 则

$$d = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

是 a 和 b 的最大公因子.

$2 \rightarrow 3$: 由于 R 满足最大公因子条件, 于是 $(a, b) \sim 1$, $(a, c) \sim 1$ 可以推出 $(a, bc) \sim 1$. 对任意不可约元素 $p \in R$, 若 $p \nmid a$, $p \nmid b$, 则 $(p, a) \sim 1$, $(p, b) \sim 1$, 于是 $(p, ab) \sim 1$, 即 $p \nmid ab$, 于是 p 是素元素, R 满足素性条件.

$3 \rightarrow 1$: 由引理1, R 满足有限析因条件, 下证相伴意义下的唯一性. 设 $a \in R^* \setminus U$ 有两种分解

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t,$$

当 $s = 1$ 时, $a = p_1$, 由于 p_1 是不可约元素, 于是不妨设 $a = p_1 \mid q_1$, 于是 $a \sim q_1$, $t = 1$.

假设当 $s - 1$ 时成立. 因为 $p_1 \mid a$, 于是 $p_1 \mid q_1 q_2 \cdots q_t$, 存在 q_i 使得 $p_1 \mid q_i$. 不妨设 $p_1 \mid q_1$. 因为 q_1 是不可约元素, 只有平凡因子, 于是存在 $u \in U$ 使得 $q_1 = u p_1$, 有

$$p_1 p_2 \cdots p_s = u p_1 q_2 \cdots q_t,$$

$$p_2 \cdots p_s = (u q_2) \cdots q_t,$$

由归纳假设, $s - 1 = t - 1$, 于是 $s = t$ 且 $p_i \sim q_{\pi(i)}$, 这里 $\pi \in S_t$. □