

## 0.1 唯一分解整环 (UFD)

### 定理 0.1

设  $R$  是交换整环, 由命题????知  $R^* = R \setminus \{0\}$  对乘法构成交换幺半群且消去律成立. 以  $U$  表示  $R^*$  中加法可逆元素的集合, 则  $U$  对加法构成一个 Abel 群, 称为  $R$  的单位群.  $U$  中元素称为  $R$  的单位.



证明



### 定义 0.1 (整数)

设  $R$  是交换整环,  $R^* = R \setminus \{0\}$ ,  $a, b \in R^*$ , 若  $\exists c \in R^*$ , 使  $b = ac$ , 则称  $a$  能整除  $b$ , 或  $a$  是  $b$  的因子, 或  $b$  是  $a$  的倍式. 记为  $a|b$ .  $a$  不能整除  $b$ , 记为  $a \nmid b$ .



### 定义 0.2 (相伴)

设  $R$  是交换整环,  $R^* = R \setminus \{0\}$ ,  $a, b \in R^*$ , 且  $a|b, b|a$ , 则称  $a$  与  $b$  相伴, 记为  $a \sim b$ .



### 定理 0.2

设  $R$  是交换整环,  $R^* = R \setminus \{0\}$ ,  $a, b \in R^*$ , 则

- (1)  $a|a, \forall a \in R^*$ .
- (2) 若  $a|b, b|c$ , 则  $a|c$ .
- (3)  $u \in U$ , 则  $u|a, \forall a \in R^*$ .
- (4)  $u \in U \iff u|1$ .
- (5)  $a \sim b \iff \exists u \in U$ , 使  $b = au$ .
- (6) 相伴关系是幺半群  $R^*$  中的同余关系.
- (7)  $u \in U \iff u \sim 1$ .



证明

- (1) 这是因为  $a = 1 \cdot a$ .
- (2) 由  $b = ad, c = be$  得  $c = a(de)$ .
- (3) 这是因为  $a = u(u^{-1}a)$ .
- (4) 由性质 (3) 知  $u \in U$  时,  $u|1$ . 反之, 若  $u|1$ , 即有  $v$ , 使得  $1 = vu$ , 故  $v = u^{-1}(u \in U)$ .  
由性质 (3) 知  $\forall u \in U, a \in R^*, u$  是  $a$  的因子, 这种因子称为平凡因子.
- (5) 事实上, 若  $b = au(u \in U)$ , 则  $a = bu^{-1}$ . 因而  $a|b, b|a$ , 即  $a \sim b$ .  
反之, 若  $a|b, b|a$ , 即有  $c, d \in R^*$ , 使得  $b = ac, a = bd$ . 于是  $b = b(dc)$ . 故  $dc = 1$ , 因而  $d, c \in U$ .
- (6) 相伴关系显然是等价关系. 设  $a \sim b, c \sim d$ . 于是  $\exists u_1, u_2 \in U$ , 使得  $b = au_1, d = cu_2$ . 于是  $bd = ac(u_1u_2)$ . 由  $u_1u_2 \in U$  及性质 1 知  $ac \sim bd$ , 即相伴关系是同余关系.
- (7) 这是整除的性质 (3) 与性质 (4) 的直接推论.



### 定义 0.3

设  $a, b \in R^*$ . 若  $b|a$ , 但  $a \nmid b$ , 则称  $b$  为  $a$  的真因子. 换言之,  $b$  为  $a$  的真因子当且仅当  $b$  是  $a$  的因子且  $b$  与  $a$  不相伴.



如果  $u \in U$ , 则  $u$  无真因子. 事实上若  $v$  是  $u$  的因子, 即  $v|u$ , 又  $u|1$ , 故  $v|1$ , 因而  $v \in U$ , 亦即  $v \sim u$ , 由此知  $u$  无真因子.

**定义 0.4**

设  $a \in R^* \setminus U$ . 若  $a$  无非平凡的真因子, 则称  $a$  为不可约元素. 若  $a$  有非平凡的真因子, 则称  $a$  为可约元素.



**例题 0.1** 在整数环  $\mathbb{Z}$  中,  $U = \{1, -1\}$ , 于是  $a \sim b \iff a = \pm b$ , 因而  $a$  为不可约元素当且仅当  $a$  为素数或负素数.

**例题 0.2** 设  $\mathbf{P}$  为数域, 则  $\mathbf{P}$  上一元多项式环  $\mathbf{P}[x]$  为交换整环. 此时  $U = \mathbf{P}^* = \mathbf{P} \setminus \{0\}$ .  $f(x) \sim g(x)$  iff  $\exists c \in \mathbf{P}^*$ , 使得  $f(x) = cg(x)$ , 因而  $f(x)$  为不可约元素当且仅当  $f(x)$  为不可约多项式.

**定义 0.5**

若  $p \in R^* \setminus U$  且满足

$$p|ab \Rightarrow p|a \text{ 或 } p|b,$$

则称  $p$  为素元素.



例 2.4.1 与例 2.4.2 中的不可约元素都是素元素.

**引理 0.1**

素元素一定是不可约元素.



**证明** 若  $a$  是素元素  $p$  的一个因子, 即有  $b \in R^*$ , 使  $p = ab$ , 因而  $p|a$  或  $p|b$ . 在  $p|a$  的情况, 说明  $a$  不是  $p$  的真因子. 若  $p|b$ , 即有  $c \in R^*$ , 使  $b = pc$ , 于是  $p = pac$ , 故  $ac = 1(a \in U)$ , 即  $a$  为平凡因子. 这说明  $p$  没有非平凡的真因子, 故  $p$  是不可约元素.

