

# 整环中的整除理论

本节讨论的是整环  $R$  去掉  $\{0\}$  后的关于乘法作成的交换幺半群  $R^*$ .

**定义 1 (单位).**  $R^*$  中的可逆元全体  $U$  关于乘法作成 Abel 群, 称为  $R$  的**单位群**,  $U$  中的元素称为**单位**.

**定义 2 (整除).** 对  $a, b \in R^*$ , 若存在  $p \in R^*$  使得  $b = pa$ , 则称  $a$  整除  $b$ , 记作  $a \mid b$ . 反之, 称  $a$  不整除  $b$ , 记作  $a \nmid b$ . 称  $a$  是  $b$  的**因子**,  $b$  是  $a$  的**倍式**.

**定义 3 (平凡因子).** 任意单位  $u \in U \subset R^*$ , 对任意  $a \in R^*$ , 都有  $u \mid a$ , 称为  $a$  的**平凡因子**.

**注.** 因为  $u(u^{-1}a) = a$ , 而  $u^{-1}a \in R^*$ , 于是  $u \mid a$ .

**定义 4 (相伴).** 对  $a, b \in R^*$ , 若  $a \mid b$ ,  $b \mid a$ , 则称  $a$  与  $b$  **相伴**, 记作  $a \sim b$ .

**性质 1.**  $a \sim b$  当且仅当存在  $u \in U$  使得  $b = ua$ .

**性质 2.** 相伴关系是同余关系.

**证明.** 易证相伴关系是等价关系. 对任意  $a, b, c, d \in R^*$ , 若  $a \sim b$ ,  $c \sim d$ , 则存在  $u_1, u_2 \in U$  使得  $b = u_1a$ ,  $d = u_2c$ , 于是

$$bd = u_1au_2c = u_1u_2ac,$$

而  $u_1u_2 \in U$ , 于是  $bd \sim ac$ . □

**性质 3.**  $u \in U \iff u \sim 1$ .

**定义 5 (真因子).** 对  $a, b \in R^*$ , 若  $a \mid b$ ,  $b \nmid a$ , 则称  $a$  是  $b$  的**真因子**.

**定义 6.** 真因子即不与之相伴的因子.

**定义 7 (不可约元素, 可约元素).** 若  $a \in R^* \setminus U$  没有非平凡的真因子, 即只有平凡的真因子, 则称  $a$  为**不可约元素**. 反之, 则称  $a$  为**可约元素**.

**注.** 不可约和可约的概念只对  $R^*$  中非单位的元素有定义, 单位不存在这个概念.

**定义 8 (素元素).** 设  $p \in R^* \setminus U$ ,  $a, b \in R^*$ , 若  $p \mid ab$  能推出  $p \mid a$  或  $p \mid b$ , 则称  $p$  为**素元素**.

不可约元素和素元素存在密切的关系.

**引理 1.** 素元素是不可约元素.

证明. 设  $a \mid p$ , 则存在  $b \in R^*$  使得  $p = ab$ , 于是  $p \mid a$  或  $p \mid b$ . 若  $p \mid a$ , 则  $a \sim p$ ,  $a$  不是  $p$  的真因子. 若  $p \mid b$ , 则存在  $c \in R^*$  使得  $b = pc$ . 于是  $p = ab = apc = pac$ ,  $ac = 1$ , 于是  $a \in U$  是  $p$  的平凡因子.  $\square$

不可约元素不一定是素元素, 下面是一个反例.

**例 1.** 设  $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ , 则 3 是  $R$  的不可约元素, 但不是素元素.

为找出单位群, 先定义  $\mathbb{Z}[\sqrt{-5}]$  中范数的概念.

**定义 9.** 设  $\alpha = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ ,  $\bar{\alpha} = a - b\sqrt{-5}$ ,  $N(\alpha) = \alpha\bar{\alpha} = a^2 + 5b^2$  为  $\alpha$  的范数.

显然  $N(\alpha)$  是非负整数,  $N(\alpha) = 0$  当且仅当  $\alpha = 0$ . 且对任意  $\alpha, \beta \in R$ , 有

$$N(\alpha\beta) = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta).$$

下面是例1的证明.

证明. 对任意  $\alpha \in U$ , 有  $\alpha\alpha^{-1} = 1$ . 于是  $N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$ . 由于  $N(\alpha)$  是非负整数, 于是  $N(\alpha) = N(\alpha^{-1}) = 1$ . 于是  $\alpha = \pm 1$ . 当  $\alpha = \pm 1$  时, 显然  $\alpha \in U$ , 于是  $U = \{1, -1\}$ .

设  $\alpha = a + b\sqrt{-5}$  是 3 的一个因子, 则存在  $\beta \in R^*$  使得  $3 = \alpha\beta$ . 于是  $N(\alpha)N(\beta) = N(\alpha\beta) = N(3) = 9$ .  $N(\alpha)$  的取值有 1, 3, 9.

当  $N(\alpha) = 1$  时,  $\alpha = 1$  是 3 的平凡真因子.

当  $N(\alpha) = 3$  时,  $a^2 + 5b^2 = 3$  无整数解, 于是此情况不存在.

当  $N(\alpha) = 9$  时,  $N(\beta) = 1$ ,  $\beta = \pm 1$ , 于是  $\alpha \sim 3$ . 则  $\alpha$  不是 3 的真因子.

上述说明了 3 是不可约元素. 另一方面, 由于  $3 \mid 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ , 而  $3 \nmid 2 \pm \sqrt{-5}$ , 于是 3 不是素元素.  $\square$

**定义 10** (素性条件). 若整环  $R$  中的不可约元素都是素元素, 则称  $R$  满足素性条件.

**定义 11** (公因子). 设  $a, b \in R^*$ , 若有  $d \in R^*$  满足  $d \mid a$  且  $d \mid b$ , 则称  $d$  为  $a$  和  $b$  的公因子. 若有公因子  $d$ , 对任意公因子  $d_1$  都有  $d_1 \mid d$ , 则称  $d$  是  $a$  和  $b$  的最大公因子. 类似地可以定义有限多个元素的最大公因子.

最大公因子不一定存在. 若  $R^*$  中的任意两个元素的最大公因子都存在, 则称  $R$  满足最大公因子条件.

**引理 2.** 设整环  $R$  满足最大公因子条件, 则有

1.  $R$  中任意两个元素  $a, b$  的最大公因子在相伴意义下唯一, 记为  $(a, b)$ .
2.  $R$  中任意  $r$  个元素  $a_1, a_2, \dots, a_r$  的最大公因子存在.

$$3. ((a, b), c) \sim (a, (b, c)).$$

$$4. c(a, b) = (ca, cb).$$

5. 若  $(a, b) \sim 1$ ,  $(a, c) \sim 1$ , 则  $(a, bc) \sim 1$ . (若  $(a, b) \sim 1$ , 则称  $a$  和  $b$  互素)

证明. 1. 设  $d, d_1$  是  $a, b$  的两个最大公因子, 则  $d \mid d_1, d_1 \mid d$ , 于是  $d \sim d_1$ .

2. 设  $d_1 = (a_1, a_2), d_2 = (d_1, a_3), \dots, d = d_{r-1} = (d_{r-2}, a_r)$ , 则  $d \mid d_{r-2}, d_{r-2} \mid d_{r-3}$ , 以此类推, 有  $d \mid d_1 = (a_1, a_2)$ , 又  $d \mid a_r$ , 于是  $d$  是  $a_1, a_2, \dots, a_r$  的公因子. 对任意公因子  $a$ ,  $a \mid a_1, a \mid a_2$ , 于是  $a \mid d_1$ , 又  $a \mid a_3$ , 于是  $a \mid d_2$ , 以此类推,  $a \mid d$ . 于是  $d$  是  $a_1, a_2, \dots, a_r$  的最大公因子.

3. 由结论 2,  $((a, b), c)$  和  $(a, (b, c))$  都是  $a, b, c$  的最大公因子, 由结论 1, 它们相伴.

4. 设  $d = (a, b), e = (ca, cb)$ , 则  $d \mid a$ , 于是  $cd \mid ca$ , 同理  $cd \mid cb$ , 于是  $cd \mid e$ , 存在  $u \in R$  使得  $e = cdu$ . 而  $e \mid ca$ , 存在  $x \in R$  使得  $ca = ex = cdux$ , 于是  $a = dux$ ,  $a \mid du$ , 同理  $b \mid du$ , 于是  $du \mid d$ , 即  $u \in U$ , 于是  $e \sim cd$ .

5. 由  $(a, b) \sim 1$ , 有  $(ac, bc) \sim c$ , 于是

$$1 \sim (a, c) \sim (a, (ac, bc)) \sim ((a, ac), bc) \sim (a, bc).$$

□