0.1 唯一析因环 (唯一分解整环)

因本节讨论并未用到 R 中的加法, 因而可以认为 R^* 是满足消去律的幺半群. 因此, 可定义**唯一析因幺半群** (或 **Gauss 幺半群**). 引理 0.2, 引理 0.3与定理 0.6对 Gauss 幺半群也成立.

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^* 中乘法可逆元素的集合, 则 U 对乘法构成一个 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 $a \nmid b$. 在 R 中约定 $a|0, \forall a \in R$.

♣

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,$R^* = R \setminus \{0\}, a, b, c \in R^*$, U 表示 R^* 中乘法可逆元素的集合, 则

(1) $a|a, \forall a \in R^*$.

(2) 若 $a|b, b|c$, 则 $a|c$.

(3) $a \sim b$ 的充要条件是 $ac \sim bc$.

(4) 若 $u \in U$, 则 $u|a, \forall a \in R^*$.

(5) $u \in U \iff u|1$.

(6) $a \sim b \iff \exists u \in U$, 使$b = au \iff \langle a \rangle = \langle b \rangle$.

(7) 相伴关系是乘法幺半群 R^* 中的同余关系.

(8) $u \in U \iff u \sim 1$.

(9) 若 $a|b, a|c$, 则 $a|(xb + yc), \forall x, y \in R$.

♡

证明

(1) 这是因为 $a = 1 \cdot a$.

(2) 由 $b = ad, c = be$ 得 $c = a(de)$.

(3) **必要性**: 由 $a \sim b$ 知 $b = ad, a = be (d, e \in R)$, 于是 $bc = adc, ac = bec$, 故 $ac \mid bc, bc \mid ac$, 即 $ac \sim bc$.
充分性: 由 $ac \sim bc$ 知 $ac = dbc, bc = eac (d, e \in R)$. 由命题????知 R^* 对乘法满足消去律, 故 $a = db, b = ea$, 因此 $a \sim b$.

(4) 这是因为 $a = u(u^{-1}a)$.

(5) 由性质 (4)知 $u \in U$ 时,$u|1$. 反之, 若 $u|1$, 即有 v, 使得 $1 = vu$, 故 $v = u^{-1} (u \in U)$. 再利用定理????可得

$$\langle b \rangle = bR = auR \xlongequal{\text{定理????}} aR = \langle a \rangle.$$

(6) 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 $b = b(dc)$. 由命题????知 R^* 对乘法满足消去律, 故 $dc = 1$, 因而 $d, c \in U$.

(7) 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 (6)知 $ac \sim bd$, 即相伴关系是同余关系.

(8) 注意到 $1 \in U$, 故由性质 (4)知 $1|u$. 再由性质 (5)知 $u \in U \iff u|1 \iff u \sim 1$.

(9)

□

定义 0.3

设 R 是交换整环,$R^* = R \setminus \{0\}$, U 表示 R^* 中乘法可逆元素的集合, 则 $\forall u \in U, a \in R^*$, 由定理 0.2(1)和定理 0.2(4)知 u 是 a 的因子, 这种因子称为**平凡因子**.

定义 0.4

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

定理 0.3

设 R 是交换整环,$R^* = R \setminus \{0\}$, U 表示 R^* 中乘法可逆元素的集合, 则如果 $u \in U$, 则 u 无真因子.

证明 事实上若 v 是 u 的因子, 即 $v|u$, 又由定理 0.2(5)知 $u|1$, 故 $v|1$, 因而再由定理 0.2(5)知 $v \in U \subseteq R^*$, 故由定理 0.2(4)知 $u|v$. 因此 $v \sim u$, 由此知 u 无真因子.

□

定义 0.5

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, $a \in R^* \setminus U$. 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**.

注 由定义知若 a 是不可约元素, 则 $n \mid a \iff n \sim 1$或$n \sim a$.

命题 0.1

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合,$u \in U$,a 为 R 的不可约元素, 则 au 也是不可约的. 进而, 若 $a \sim b$, 则 b 也不可约.

证明 反证, 假设 au 可约, 则存在 $e \in R^*$ 为 au 的非平凡真因子. 从而存在 $x \in R^*$, 使 $au = ex$, 进而 $a = exu^{-1}$. 于是 e 也是 a 的非平凡真因子, 这与 a 不可约矛盾! 故 au 不可约. 由定理 0.2(6)可知存在 $u' \in U$, 使 $b = au'$. 由之前证明知 $b = au'$ 也不可约.

□

定义 0.6

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 若 $p \in R^* \setminus U$ 且满足

$$p|ab \Rightarrow p|a或p|b,$$

则称 p 为**素元素**.

命题 0.2

设 R 是交换整环,$R^* = R\setminus\{0\}$,U 表示 R^* 中乘法可逆元素的集合, 若 p 是素元素,$u \in U$,$a_i \in R (i = 1, 2, \cdots, l)$, 且 $p \mid u\prod_{i=1}^{k} a_i$, 则存在 $i_0 \in \{1, 2, \cdots, k\}$, 使 $p \mid a_{i_0}$.

证明 由素元素定义可得 $p \mid u$ 或 $p \mid \prod_{i=1}^{k} a_i$. 若 $p \mid u$, 则由定理 0.2(4)知 $u \mid p$, 故 $p \sim u$. 再由定理 0.2(6)知存在 $u' \in U$, 使 $p = uu' \in U$, 这与 p 不可约矛盾! 故下设 $p \mid \prod_{i=1}^{k} a_i$.

由素元素定义可得 $p \mid a_k$ 或 $p \mid \prod_{i=1}^{k-1} a_i$. 若 $p \mid a_k$ 则结论已经成立. 若 $p \mid \prod_{i=1}^{k-1} a_i$, 则再由素元素定义可得 $p \mid a_{k-1}$ 或 $p \mid \prod_{i=1}^{k-2} a_i$. 若 $p \mid a_{k-1}$ 则结论已经成立. 若 $p \mid \prod_{i=1}^{k-2} a_i$, 则再由素元素定义可得 $p \mid a_{k-2}$ 或 $p \mid \prod_{i=1}^{k-3} a_i$. 继续做下去, 因为 $\prod_{i=1}^{k} a_i$ 中只有 k 个元素, 所以必在有限步终止, 故必存在 $i_0 \in \{1, 2, \cdots, k\}$, 使 $p \mid a_{i_0}$.

□

例题 0.1 在整数环 $\mathbf{Z}$ 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. 并且整数环 $\mathbf{Z}$ 的不可约元素都是素元素.

证明

□

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. 并且一元多项式环 $\mathbf{P}[x]$ 的不可约元素都是素元素.

证明

□

引理 0.1

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 则 R 中的素元素一定是不可约元素.

♡

注 不可约元素不一定是素元素, 反例见例题 0.3.

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 $p = pac$, 由命题????知 R^* 对乘法满足消去律, 故 $ac = 1$, 从而 $a \in U$, 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.

□

例题 0.3 令 $R = \mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$. 设 $\alpha = a + b\sqrt{-5}$, 称 $\overline{\alpha} = a - b\sqrt{-5}$ 为 α 的共轭, 称 $N(\alpha) = \alpha\overline{\alpha} = a^2 + 5b^2$ 为 α 的范数, 显然 $N(\alpha) \in \mathbf{Z}$ 且 $N(\alpha) \geqslant 0$, 当且仅当 $\alpha = 0$ 时等号成立. 则 $\mathbf{Z}[\sqrt{-5}]$ 的单位群 $U = \{1, -1\}$, 且 3 是 $\mathbf{Z}[\sqrt{-5}]$ 的不可约元素, 但不是 $\mathbf{Z}[\sqrt{-5}]$ 的素元素.

证明 注意到 $\forall \alpha, \beta \in R$ 有 $N(\alpha\beta) = N(\alpha)N(\beta)$. 先求 R 的单位群 U.$\alpha \in U$, 则有 $\alpha\alpha^{-1} = 1$, 故 $N(\alpha)N(\alpha^{-1}) = N(1) = 1$, 故 $N(\alpha) = 1$. 由此即得 $U = \{1, -1\}$, 因而 $\alpha \sim \beta \iff \alpha = \pm\beta$.

再证明 3 是 $\mathbf{Z}[\sqrt{-5}]$ 的不可约元素, 但不是 $\mathbf{Z}[\sqrt{-5}]$ 的素元素. 设 $\alpha = a + b\sqrt{-5}$ 是 3 的一个因子, 故有 β, 使 $3 = \alpha\beta$, 于是 $N(3) = N(\alpha)N(\beta)$. 由 $N(3) = 9$ 知 $N(\alpha)$ 有以下三种可能:

(1) $N(\alpha) = 1$, 则 $\alpha = \pm 1$, 即 α 是 3 的平凡因子;

(2) $N(\alpha) = 3$, 于是 $a^2 + 5b^2 = 3$, 但此方程无整数解, 故这种情况不存在;

(3) $N(\alpha) = 9$, 于是 $N(\beta) = 1, \beta = \pm 1$, 即有 $\alpha = \pm 3, \alpha \sim 3$, 即 α 不是 3 的真因子.

由上知 3 是不可约元素. 另一方面,$3 \mid 9, 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$. 由于 $N(2 + \sqrt{-5}) = N(2 - \sqrt{-5}) = N(3) = 9$, 而 3 与 $2 \pm \sqrt{-5}$ 不相伴, 因而 $3 \nmid 2 \pm \sqrt{-5}$, 即 3 不是素元素. □

定义 0.7

若一个交换整环 R 的不可约元素是素元素, 则称 R 满足**素性条件**.

♣

定义 0.8

设 R 是交换整环,$R^* = R \setminus \{0\}, b, c \in R^*$. 若 $d \in R^*$ 满足 $d \mid b, d \mid c$, 则称 d 为 b, c 的**公因子**. 若对 b, c 的任一公因子 d_1 有 $d_1 \mid d$, 则称 d 是 b, c 的**最大公因子**. 也记为 (b, c). 若 $(a, b) \sim 1$, 则称 a 与 b 为**互素**

对 R^* 中任意有限个元素也可类似地定义它们的最大公因子.

♣

注 一般来说,R^* 中任意两个元素的最大公因子不一定存在.

定义 0.9

设 R 是交换整环,$R^* = R \setminus \{0\}$, 如果 R^* 中任意两个元素的最大公因子存在, 则称 R 满足**最大公因子条件**. ♣

引理 0.2

设交换整环 R 满足最大公因子条件,$a, b, c, a_1, \cdots, a_r, b_1, \cdots, b_r \in R$, 则有下列结论:

(1) 设 d 是 a, b 的一个最大公因子, 则 d_1 为 a, b 的最大公因子当且仅当 $d_1 \sim d$, 即 a, b 的最大公因子在相伴意义下是唯一的;

(2) $\forall a_1, a_2, \cdots, a_r \in R$ 均有最大公因子;

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

(4) $((a, b), c) \sim (a, (b, c))$;

(5) $c(a_1, a_2, \cdots, a_r) \sim (ca_1, ca_2, \cdots, ca_r)$;

(6) 若 $a \in U$, 则 $(a, b) \sim 1$.

(7) 若 $(a, b_i) \sim 1, 1 \leqslant i \leqslant r$, 则 $(a, b_1 b_2 \cdots b_r) \sim 1$.

(8) 若 p 是不可约元素, 则 $p \nmid a \iff (p, a) \sim 1$.

(9) 若 p 是不可约元素, 则 $(p, (a_1, a_2, \cdots, a_r)) \sim 1$ 当且仅当存在 $s \in \{1, 2, \cdots, r\}$, 使

$$p \mid a_i,\ 1 \leqslant i \leqslant s-1, \quad p \nmid a_s.$$

♡

证明

(1) 由于 d, d_1 是 a, b 的最大公因子, 故 $d \mid d_1, d_1 \mid d$. 于是 $d \sim d_1$. 反之,$d_1 \sim d$, 故 $d_1 \mid d$. 又 $d \mid a, b$, 于是 $d_1 \mid a, b$, 因而 d_1 是 a, b 的公因子. 又若 c 是 a, b 的公因子, 则 $c \mid d$, 而 $d \mid d_1$, 故有 $c \mid d_1$, 因而 d_1 是 a, b 的最大公因子.

(2) 令 $d_1 = (a_1, a_2), d_2 = (d_1, a_3), d_3 = (d_2, a_4), \cdots, d = d_{r-1} = (d_{r-2}, a_r)$. 下面证明 d 是 $a_1, a_2, \cdots, a_r$ 的最大公因子. 显然有 $d \mid d_k\ (1 \leqslant k \leqslant r-2), d \mid a_r$. 又 $d_k \mid a_{k+1}$, 故 $d \mid a_i\ (1 \leqslant i \leqslant r)$, 即 d 为公因子. 又若 $a \mid a_i\ (1 \leqslant i \leqslant r)$, 则 $a \mid d_1$ 且依次 $a \mid d_2, a \mid d_3, \cdots$, 最后有 $a \mid d_{r-1}$, 即 $a \mid d$, 因而 d 是最大公因子.

(3) 设 $d = (a, b)$, 则 $d \mid a, b$. 由 $b \sim c$ 知 $b \mid c$, 故 $d \mid a, c$, 即 d 是 a, c 的公因子. 又设 d_1 也是 a, c 的公因子, 又 $b \sim c$, 故 $c \mid b$, 从而 $d_1 \mid a, b$, 即 d_1 是 a, b 的公因子. 故 $d_1 \mid d$. 因此 d 是 a, c 的最大公因子. 由结论 (1)知 $d \sim (a, c)$.

(4) 由结论 (2)同理可知 $((a, b), c)$ 与 $(a, (b, c))$ 都是 a, b, c 的最大公因子. 由结论 (1) 知它们相伴.

(5) 设 $d = (a, b), e = (ca, cb)$, 则 $cd \mid ca, cd \mid cb$. 于是 $cd \mid e$, 因而 $e = cdu (u \in R^*)$. 又由 $ca \mid e$ 知 $ca = ex (x \in R^*)$. 由此知 $ca = ex = xucd$. 由命题**????**知 R^* 对乘法满足消去律, 故 $a = xud$, 即 $ud \mid a$, 同样有 $ud \mid b$, 故 $ud \mid d$, 于是 $d = udk (k \in R^*)$, 同样由 R^* 对乘法满足消去律可得 $uk = 1$, 因而 $u \in U$. 于是由定理 0.2(6)知 e 与 cd 相伴. 再利用数学归纳法易证.

(6) 显然 $1 \mid a, b$. 设 $d \mid a, b$, 则存在 $a_1 \in R^*$, 使 $a = da_1$. 于是由 $a \in U$ 知 $1 = aa^{-1} = d\left(a_1 a^{-1}\right)$, 故 $d \mid 1$. 因此 $(a, b) \sim 1$.

(7) 因为 $(a, b) \sim 1, (1, c) \sim 1$, 由结论 (5) 知 $(ac, bc) \sim c, (a, ac) \sim a$, 故由结论 (4)及结论 (3)有 $1 \sim (a, c) \sim (a, (ac, bc)) \sim ((a, ac), bc) \sim (a, bc)$. 再利用数学归纳法易证.

(8) $\Longleftarrow$: 假设 $p \mid a$, 则存在 $a_1 \in R^*$, 使 $a = pa_1$. 于是由结论 (5)和结论 (6)知 $1 \sim (p, a) = (p, pa_1) = p(1, a_1) = p$. 但由 p 不可约知 $p \notin U$, 由定理 0.2(6)知 $p \nmid 1$, 矛盾!

$\Longrightarrow$: 设 $d = (p, a)$, 则存在 $p_1, a_1 \in R^*$, 使 $p = dp_1, a = da_1$. 假设 $d \nmid 1$, 则由定理 0.2(6)知 $d \notin U$, 从而 $d \in R^* \setminus U$. 若 $p \mid d$, 则由 $d \mid a$ 知 $p \mid a$, 这与 $p \nmid a$ 矛盾! 故 $p \nmid d$.

若 $d \neq p$, 则由 $p = dp_1, p \nmid d$ 及 $d \in R^* \setminus U$ 知 d 是 p 的非平凡真因子, 这与 p 不可约矛盾!

若 $d = p$, 则由 $a = da_1$ 知 $a = pa_1$, 即 $p \mid a$, 这与 $p \nmid a$ 矛盾!

因此 $d \mid 1$, 故 $d \sim 1$.

(9) $\Longrightarrow$: 假设 $p \mid a_i$, $1 \leqslant i \leqslant s$, 则 $p \mid (a_1, a_2, \cdots, a_r)$. 从而 $(p, (a_1, a_2, \cdots, a_r)) \sim p$ 矛盾! 故可设 $s_1, s_2, \cdots, s_k \in \{1, 2, \cdots, r\}$, 使

$$p \mid a_i,\ i \notin \{s_1, s_2, \cdots, s_k\}, \quad p \nmid a_s,\ i \in \{s_1, s_2, \cdots, s_k\}.$$

取 $s = \min\limits_{j=1,2,\cdots,k} s_j$, 则

$$p \mid a_i,\ 1 \leqslant i \leqslant s-1, \quad p \nmid a_s.$$

$\Longleftarrow$: 由 $p \nmid a_s$ 知 $p \nmid (a_1, a_2, \cdots, a_r)$, 否则由 $p \mid (a_1, a_2, \cdots, a_r)$ 知 $p \mid a_s$ 矛盾! 于是由结论 (8)知

$$(p, (a_1, a_2, \cdots, a_r)) \sim 1.$$

□

定义 0.10 (唯一析因环)

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 如果 R 满足下列条件:

(1) **有限析因条件**: $\forall a \in R^* \setminus U$, 可分解为有限个不可约元素的乘积, 即有不可约元素 $p_i (1 \leqslant i \leqslant r)$ 及单位 $u \in U$, 使

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

(2) 若 $a \in R^* \setminus U$ 有两种不可约元素乘积的分解:

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

则有 $r = s$ 且 $\exists \pi \in S_n$, 使 $p_i \sim q_{\pi(i)} (1 \leqslant i \leqslant r)$.

那么称 R 为**唯一析因环** (简记为 **UFD**) 或**唯一分解整环**或 **Gauss 环**. 称 $|a| \triangleq r$ 为 a 的**长度**. 若 $u \in U$, 约定 $|u| \triangleq 0$.

♣

注 所谓唯一析因环也就是使因式分解唯一性定理成立的交换整环, 因而前面例题 0.1与例题 0.2中的环 $\mathbf{Z}$ 与 $\mathbf{P}[x]$ 都是 UFD, 而例题 0.3中的环 $\mathbf{Z}[\sqrt{-5}]$ 就不是. 因为 $9 = 3^2$ 与 $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ 是 9 的两种本质上不同的分解, 即 $\mathbf{Z}[\sqrt{-5}]$ 不满足唯一析因环定义中的条件 (2).

定理 0.4

设 R 是唯一析因环 (UFD),$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 则

(1) 对 $\forall a \in R^* \setminus U$, 都存在 $r \in \mathbf{N}$, 单位 $u \in U$ 以及互不相伴的不可约元素 $p_1, p_2, \cdots, p_r$, 使

$$a = u p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \quad n_i \in \mathbf{N}.$$

若 c 是 a 的一个非平凡因子, 则存在 $u_1 \in U$ 以及 $n_i' \leqslant n_i$ 且 $n_i' \in \mathbf{N} (i = 1, 2, \cdots, r)$, 使

$$c = u_1 p_1^{n_1'} p_2^{n_2'} \cdots p_r^{n_r'}.$$

(2) 若 $a, b \in R^* \setminus U$, 则存在 $r \in \mathbf{N}$, 单位 $u, v \in U$ 以及互不相伴的不可约元素 $p_1, p_2, \cdots, p_r$, 使

$$a = u p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \quad n_i \in \mathbf{N} \cup \{0\};$$

$$b = v p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}, \quad m_i \in \mathbf{N} \cup \{0\}.$$

若还有 d 是 a, b 的公因子, 则存在 $w \in U$ 以及 $n_i' \leqslant \min\{n_i, m_i\}$ 且 $n_i' \in \mathbf{N} (i = 1, 2, \cdots, r)$, 使

$$d = w p_1^{n_1'} p_2^{n_2'} \cdots p_r^{n_r'}.$$

♡

证明

(1) 由 a 满足有限析因条件知, 存在不可约元素 $q_1, q_2, \cdots, q_s$, 使得

$$a = q_1 q_2 \cdots q_s.$$

将 $q_1, q_2, \cdots, q_s$ 按相伴关系分类, 不妨设存在 $r \in \mathbf{N}$ 和

$$0 = i_0 \leqslant i_1 \leqslant \cdots \leqslant i_r = s,$$

使 $q_{i_1}, q_{i_2}, \cdots, q_{i_r}$ 互不相伴且

$$q_{i_0+1} = q_1 \sim q_2 \sim \cdots \sim q_{i_1};$$

$$q_{i_1+1} \sim q_{i_1+2} \sim \cdots \sim q_{i_2};$$

$$\cdots\cdots$$

$$q_{i_{r-1}+1} \sim q_{i_{r-1}+2} \sim \cdots \sim q_{i_r} = q_s.$$

由定理 0.2(6)知存在

$$u_{11}, u_{12}, \cdots, u_{1,i_1-1}, u_{21}, u_{22}, \cdots, u_{2,i_2-1}, \cdots, u_{r1}, u_{r2}, \cdots, u_{r,i_r-1} \in U,$$

使得

$$q_1 = u_{11}q_{i_1}, \quad q_2 = u_{12}q_{i_1}, \cdots\cdots, q_{i_1-1} = u_{1,i_1-1}q_{i_1};$$

$$q_{i_1+1} = u_{21}q_{i_2}, \quad q_{i_1+2} = u_{22}q_{i_2}, \cdots\cdots, q_{i_2-1} = u_{2,i_2-1}q_{i_2};$$

$$\cdots\cdots\cdots\cdots$$

$$q_{i_{r-1}+1} = u_{r1}q_{i_r}, \quad q_{i_{r-1}+2} = u_{r2}q_{i_r}, \cdots\cdots, q_{i_r-1} = u_{r,i_r-1}q_{i_r}.$$

记 $p_j = q_{i_j}, n_j = i_j - i_{j-1} (j = 1, 2, \cdots, r), u = \prod\limits_{j=1}^{r}\prod\limits_{i=1}^{i_j-1} u_{ji} \in U$, 则 $p_1, p_2, \cdots, p_r$ 互不相伴且

$$a = q_1q_2\cdots q_s = q_{i_1}^{i_1-1}\prod_{i=1}^{i_1-1} u_{1i} \cdot q_{i_2}^{i_2-1}\prod_{i=1}^{i_2-1} u_{2i}\cdots q_{i_r}^{i_r-1}\prod_{i=1}^{i_r-1} u_{ri}$$

$$= \prod_{j=1}^{r}\prod_{i=1}^{i_j-1} u_{ji} \cdot q_{i_1}^{i_1-1}q_{i_2}^{i_2-1}\cdots q_{i_r}^{i_r-1} = up_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}.$$

由 c 是 a 的非平凡因子知, 存在 $d \in R^*$, 使 $a = cd$. 由 R 是唯一析因环 (UFD) 知 c, d 都满足有限析因条件, 故存在不可约元素 $c_1, c_2, \cdots, c_t$ 和 $d_1, d_2, \cdots, d_m$ 使

$$c = c_1c_2\cdots c_t, \quad d = d_1d_2\cdots d_m.$$

从而

$$q_1q_2\cdots q_s = a = cd = c_1c_2\cdots c_t \cdot d_1d_2\cdots d_m.$$

由 R 是唯一析因环 (UFD) 知 a 的不可约分解在相伴意义下唯一, 再记 $f_i = \begin{cases} c_i, & i = 1, 2, \cdots, t \\ d_{i-t}, & i = t+1, \cdots, t+m \end{cases}$, 故 $s = t + m$ 且存在 $\pi \in S_s$, 使 $q_i \sim f_{\pi(i)} (i = 1, 2, \cdots, s)$, 即 $q_{\pi^{-1}(i)} \sim f_i (i = 1, 2, \cdots, s)$. 于是 $c_i \sim q_{\pi^{-1}(i)} (i = 1, 2\cdots, t)$. 不妨设存在

$$0 = i'_0 \leqslant i'_1 \leqslant \cdots \leqslant i'_r = t,$$

使

$$\pi^{-1}(i'_{j-1} + 1), \cdots, \pi^{-1}(i'_j) \in \{i_{j-1} + 1, \cdots, i_j\}, \quad j = 1, 2, \cdots, r.$$

记 $n'_j = i'_j - i'_{j-1}$, 则由 $n_j = i_j - i_{j-1}$ 知 $n'_j \leqslant n_j$. 又因为

$$q_k \sim q_{i_j} = p_j, \quad k = i_{j-1} + 1, \cdots, i_j, \ j = 1, 2, \cdots, r.$$

所以

$$q_{\pi^{-1}(i'_{j-1}+1)} \sim \cdots \sim q_{\pi^{-1}(i'_j)} \sim p_j, \quad j = 1, 2, \cdots, r.$$

因此

$$c_{i'_{j-1}+1} \sim \cdots \sim c_{i'_j} = c_{i'_{j-1}+n'_j} \sim p_j, \quad j = 1, 2, \cdots, r.$$

由定理 0.2(6)知存在

$$u_{j1}, u_{j2}, \cdots, u_{jn'_j}, \quad j = 1, 2, \cdots, r.$$

使得

$$c_{i'_{j-1}+k} = u_{jk} p_j, \quad k = 1, 2, \cdots, n'_j, \ j = 1, 2, \cdots, r.$$

再记 $u_1 = \prod_{j=1}^{r} \prod_{k=1}^{n'_j} u_{jk}$, 于是

$$\begin{aligned} c = c_1 c_2 \cdots c_t &= \prod_{j=1}^{r} \prod_{k=1}^{n'_j} c_{i'_{j-1}+k} \\ &= \prod_{j=1}^{r} \left(\prod_{k=1}^{n'_j} u_{jk} p_j \right) = \prod_{j=1}^{r} p_j^{n'_j} \left(\prod_{k=1}^{n'_j} u_{jk} \right) \\ &= \prod_{j=1}^{r} p_j^{n'_j} \left(\prod_{k=1}^{n'_j} u_{jk} \right) = \left(\prod_{j=1}^{r} p_j^{n'_j} \right) \left(\prod_{j=1}^{r} \prod_{k=1}^{n'_j} u_{jk} \right) \\ &= u_1 p_1^{n'_1} p_2^{n'_2} \cdots p_r^{n'_r}. \end{aligned}$$

(2) 由 (1) 知存在 $t, s \in \mathbf{N}$, 单位 $u_1, v_1 \in U$, 互不相伴的不可约元素 $p_1, p_2, \cdots, p_s$ 和互不相伴的不可约元素 $q_1, q_2, \cdots, q_t$, 使

$$a = u_1 p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}, \quad n_i \in \mathbf{N};$$

$$b = v_1 q_1^{m_1} q_2^{m_2} \cdots q_t^{m_t}, \quad m_i \in \mathbf{N}.$$

不妨设存在 $k \leqslant \min\{s, t\}$, 使

$$p_j \sim q_j, \quad j = 1, 2, \cdots, k.$$

由定理 0.2(6)知存在 $w_j \in U (j = 1, 2, \cdots, k)$, 使

$$q_j = w_j p_j, \quad j = 1, 2, \cdots, k.$$

于是

$$\begin{aligned} b &= v_1 (w_1 p_1)^{m_1} (w_2 p_2)^{m_2} \cdots (w_k p_k)^{m_k} \cdot q_{k+1}^{m_{k+1}} \cdots q_t^{m_t} \\ &= (v_1 w_1 w_2 \cdots w_k) \left(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \cdot q_{k+1}^{m_{k+1}} \cdots q_t^{m_t} \right). \end{aligned}$$

再记 $p_{s+j} = q_j (j = k+1, \cdots, t), u = u_1, v = v_1 w_1 w_2 \cdots w_k$, 则

$$\begin{aligned} a &= u p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s} p_{s+1}^0 \cdots p_{s+t}^0, \\ b &= v p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} p_{k+1}^0 \cdots p_s^0 p_{s+1}^{m_{k+1}} \cdots p_{s+t}^{m_t}. \end{aligned}$$

再取 $r = s + t, n_j = m_l = 0 (j = s+1, \cdots, s+t; l = k+1, \cdots, s)$ 即得

$$a = u p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \quad b = v p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}.$$

若 $d \in U$, 则取 $n'_i = 0 (i = 1, 2, \cdots, r)$ 即可.

若 $d \in R^* \setminus U$, 则由 d 是 a, b 的公因子和 (1) 的结论可知, 存在单位 $u', u'' \in U$, 互不相伴的不可约元素 $p_1, p_2, \cdots, p_r$ 以及 $n'_i \leqslant n_i, n''_i \leqslant m_i (i = 1, 2 \cdots, r)$ 使

$$d = u' p_1^{n'_1} p_2^{n'_2} \cdots p_r^{n'_r} = u'' p_1^{n''_1} p_2^{n''_2} \cdots p_r^{n''_r}.$$

若存在 $j_1, j_2 \cdots, j_k \in \{1, 2 \cdots, r\}$, 使 $n'_{j_l} \neq n''_{j_l} (l = 1, 2, \cdots, k)$. 由命题????知 R^* 对乘法满足消去律, 故

$$u'(u'')^{-1} p_{j_1}^{n'_{j_1} - n''_{j_1}} p_{j_2}^{n'_{j_2} - n''_{j_2}} \cdots p_{j_k}^{n'_{j_k} - n''_{j_k}} = 1.$$

由此可知 $p_{j_l} \in U (l = 1, 2, \cdots, k)$, 这与 p_{j_l} 不可约矛盾! 故 $n'_i = n''_i (i = 1, 2, \cdots, r)$, 从而 $n'_i = n''_i \leqslant \min\{n_i, m_i\} (i = 1, 2 \cdots, r)$, 取 $w = u'$, 则

$$d = w p_1^{n'_1} p_2^{n'_2} \cdots p_r^{n'_r}.$$

□

定理 0.5

设 R 是唯一析因环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合,$a, b, c \in R^*$, 则

(1) $|ab| = |a| + |b|$;

(2) $a \mid b \Longrightarrow |a| \geqslant |b|$;

(3) $a \in U \iff |a| = 0$;

(4) $b \sim c \iff |b| = |c|$, $b | c$.

♡

证明

(1)

(2) 根据定义显然成立.

(3)

□

定义 0.11

设 R 是交换整环,$R^* = R \setminus \{0\}$,R^* 中的一个序列 $a_1, a_2, \cdots, a_n, a_{n+1}, \cdots$ 满足

$$a_{n+1} \mid a_n, \quad n = 1, 2, \cdots,$$

则称为 R 的一个**因子链**.

若对 R^* 中任一因子链, 存在自然数 m, 使

$$a_m \sim a_n, \quad \forall n \geqslant m,$$

则称 R 满足**因子链条件**.

♣

引理 0.3

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 若 R 满足因子链条件, 则必满足有限析因条件.

♡

证明 设 $a \in R^* \setminus U$. 先证 a 有不可约因子. 不妨设 a 是可约的, 则 a 有非平凡的真因子 a_1, 即有 $a = a_1 b_1$. 这时 b_1 也是 a 的非平凡真因子, 否则,$b_1 \in U$, 由定理 0.2(6)知 $a \sim a_1$, 这与 a_1 为 a 真因子矛盾! 若有 a_1, b_1 都可约, 则 $a_1 = a_2 b_2$, 其中,a_2, b_2 为 a_1 的真因子. 如此继续, 可得因子链

$$a, a_1, a_2, \cdots, a_n, a_{n+1}, \cdots$$

且 $a_{n+1} \mid a_n, a_n \mid a$. 这个因子链是在假设 $a_1, a_2, \cdots, a_n, \cdots$ 都可约且对 $\forall n \in \mathbf{N}$ 有 a_{n+1} 是 a_n 的真因子的条件下得到的. 而由因子链条件有 m, 使得 $a_m \sim a_{m+1}$, 这与 a_{m+1} 是 a_m 的真因子矛盾! 因而 a_m 是不可约的, 即 a_m 是 a 的不可约因子.

再证 a 可分解为有限多个不可约因子的乘积. 设 p_1 是 a 的一个不可约因子, 于是 $a = p_1 a^{(1)}$. 若 $a^{(1)} \in U$, 则由命题 0.1知 a 不可约. 此时 a 满足有限析因条件.

若 $a^{(1)} \in R^* \setminus U$, 则 $a^{(1)}$ 有不可约因子 p_2, 使 $a^{(1)} = p_2 a^{(2)}$, 即 $a = p_1 p_2 a^{(2)}$. 继续此过程, 即得因子链

$$a, a^{(1)}, a^{(2)}, \cdots, a^{(n)}, a^{(n+1)}, \cdots$$

且 $a^{(n+1)} \mid a^{(n)}, a^{(n)} \mid a, p_{n+1}$ 都是 $a^{(n)}$ 的不可约因子,$a^{(n)} = p_{n+1}a^{(n+1)}$. 这个因子链是在假设 $a^{(n)} \in R^* \setminus U (\forall n \in \mathbf{N})$ 的条件下得到的. 而由因子链条件有 s, 使 $a^{(s-1)} \sim a^{(s)}$. 于是存在 $b \in R^*$, 使 $a^{(s)} = ba^{(s-1)}$, 从而 $a^{(s-1)} = p_s a^{(s)} = p_s b a^{(s-1)}$. 由命题**????**知 R^* 对乘法满足消去律, 故 $p_s b = 1$, 即 $p_s \in U$, 这与 p_s 不可约矛盾! 故存在 m, 使得 $a^{(m)} \in U$. 于是记 $q_m = p_m a^{(m)}$, 则由命题 0.1知 q_m 不可约. 故此时

$$a = p_1 p_2 \cdots p_m a^{(m)} = p_1 p_2 \cdots q_m.$$

满足有限析因条件. 这就证明了 R 满足有限析因条件.

□

定理 0.6

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 则下列条件等价:

(1) R 是唯一析因环 (UFD);

(2) R 满足因子链条件与素性条件;

(3) R 满足因子链条件与最大公因子条件.

♡

注 由这个定理的结论 (2) 和引理 0.1知唯一析因环 (UFD) 中的素元素等价于不可约元素.

证明 (1) $\Rightarrow$ (3). 设 R 为唯一析因环. 先证 R 满足因子链条件. $\forall a \in R^* \setminus U$,$a$ 有不可约元素乘积分解 $a = up_1 p_2 \cdots p_r$. 现设 $a_1, a_2, \cdots, a_n, a_{n+1}, \cdots$ 是 R^* 的一个因子链. 于是由定理 0.5(2)知必有 $|a_i| \geqslant 0$ 且

$$|a_1| \geqslant |a_2| \geqslant \cdots \geqslant |a_n| \geqslant |a_{n+1}| \geqslant \cdots,$$

由于 $|a_1|$ 是一个有限数, 因而有 m, 使得当 $n \geqslant m$ 时,$|a_n| = |a_m|$, 由定理 0.5(4)知 $a_n \sim a_m$, 故 R 满足因子链条件.

现证 R 满足最大公因子条件. 设 $a, b \in R^*$, 若 a, b 中有一个是单位, 则由引理 0.2(6)知 $(a, b) = 1$, 故假定 $a, b \in R^* \setminus U$. 这时由定理 0.4(1), 不妨设

$$a = up_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \quad b = vp_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

其中,$u, v \in U, p_1, p_2, \cdots, p_r$ 是互不相伴的不可约元素,$n_i \geqslant 0, m_j \geqslant 0, 1 \leqslant i, j \leqslant r$. 令 $k_i = \min\{n_i, m_i\}$, 记

$$d = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \tag{1}$$

显然 d 是 a, b 的公因子. 又设 d_1 也是 a, b 的公因子, 则由定理 0.4(2)知存在 $u_1 \in U$ 以及 $n_i' \leqslant k_i$ 且 $n_i' \in \mathbf{N} (i = 1, 2, \cdots, r)$, 使

$$d_1 = u_1 p_1^{n_1'} p_2^{n_2'} \cdots p_r^{n_r'}.$$

故 $d_1 \mid d$. 因此 d 是 a, b 的最大公因子.

(3) $\Rightarrow$ (2). 为此只需证明素性条件成立. 设 p 是一个不可约元素且 $p \nmid a, p \nmid b$, 由定理 0.2(8)有 $(p, a) \sim 1, (p, b) \sim 1$. 由引理 0.2(7)知 $(p, ab) \sim 1$, 因而再由定理 0.2(8)知 $p \nmid ab$. 换言之, 若 $p \mid ab$, 则有 $p \mid a$ 或 $p \mid b$, 故 p 为素元素.

(2) $\Rightarrow$ (1). 由引理 0.3知 R 满足有限析因环条件, 故只需证因式分解的唯一性. 不妨设 $a \in R^* \setminus U$ 且 a 有两个不可约元素乘积的分解

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{2}$$

现对 s 用数学归纳法证. 若 $s = 1$, 则 a 为不可约元素, 由素性条件知 a 为素元素. 根据素元素的定义, 可不妨设 $a \mid q_1$, 则 $a \sim q_1$. 从而由定理 0.2(6)知存在 $u \in U$, 使 $a = q_1 u = q_1 q_2 \cdots q_t$, 故 $t = 1$. 设 $s-1$ 时已成立, 现证 s 时成立. 因 $p_s \mid a$, 故 $p_s \mid q_1 q_2 \cdots q_t$, 由素性条件知 p_s 也是素元素, 于是不妨设 $p_s \mid q_t$, 于是 $q_t = u_s p_s (u_s \in U)$. 由命题**????**知 R^* 对乘法满足消去律, 因而结合(2)式有

$$p_1 p_2 \cdots p_{s-1} p_s = q_1 q_2 \cdots q_{t-1} q_t = u_s q_1 q_2 \cdots q_{t-1} p_s \Longrightarrow p_1 p_2 \cdots p_{s-1} = u_s \prod_{i=1}^{t-1} q_i.$$

记 $q_1' = u_s q_1, q_i' = q_i (2 \leqslant i \leqslant t-1)$, 由命题 0.1知 q_1' 也不可约, 并且由定理 0.2(6)知 $q_i' \sim q_i (1 \leqslant i \leqslant t-1)$, 则

$$p_1 p_2 \cdots p_{s-1} = q_1' q_2' \cdots q_{t-1}'.$$

由归纳假设可知,$s-1=t-1$ 且存在 $\pi\in S_{t-1}$, 使 $p_i\sim q'_{\pi(i)}\sim q_{\pi(i)}(1\leqslant i\leqslant t-1)$. 由命题**????**知 R^* 对乘法满足消去律, 再结合(2)式及定理 0.2(6)知

$$u_sp_s\prod_{i=1}^{t-1}q_i=p_1p_2\cdots p_s=q_1q_2\cdots q_t\Longrightarrow u_sp_s=q_t\Longrightarrow p_s\sim q_t.$$

故 $s=t$ 且有 $\pi'\in S_t$, 使得 $p_i\sim q_{\pi'(i)}(1\leqslant i\leqslant t)$, 即 R 是一个 UFD.

□

命题 0.3

设 R 是唯一析因环, 若一组两两互素的素元素 $p_1,p_2,\cdots,p_k$ 都整除 a, 则 $\prod_{i=1}^{k}p_i\mid a$.

♠

证明 由定理 0.4知存在 $u\in U$ 和互不相伴的不可约元素 $q_1,q_2,\cdots,q_r$, 使

$$a=uq_1^{n_1}q_2^{n_2}\cdots q_r^{n_r},\quad n_i\in\mathbf{N}.$$

对 $\forall i\in\{1,2,\cdots,k\}$, 由条件知 $p_i\mid a$, 故由命题 0.2知存在 $r_i\in\{1,2,\cdots,r\}$, 使 $p_i\mid q_{r_i}$. 若 $q_{r_i}\nmid p_i$, 则 p_i 是 q_{r_i} 的真因子. 由 q_{r_i} 不可约知 $p_i\in U$, 这与 p_i 是素元素矛盾! 故 $p_i\sim q_{r_i}$, 由定理 0.2(6)知存在 $u_i\in U$, 使

$$q_{r_i}=u_ip_i,\quad i=1,2,\cdots,k.$$

因此

$$\begin{aligned}a&=u\prod_{i=1}^{r}q_i^{n_i}=u\prod_{i\notin\{r_1,\cdots,r_k\}}q_i^{n_i}\prod_{i=1}^{k}q_{r_i}^{n_{r_i}}\\&=u\prod_{i\notin\{r_1,\cdots,r_k\}}q_i^{n_i}\prod_{i=1}^{k}u_ip_i^{n_i}\\&=\left(u\prod_{i\notin\{r_1,\cdots,r_k\}}q_i^{n_i}\prod_{i=1}^{k}u_i\right)\prod_{i=1}^{k}p_i^{n_i}.\end{aligned}$$

故 $\prod_{i=1}^{k}p_i^{n_i}\mid a$.

□