

理想: 环 R 中: $\emptyset \subsetneq I \subseteq R$ 称为 R 的理想

$$\text{若: } \begin{cases} \forall x, y \in I (x+y) \in I, & x-y \in I \Rightarrow \\ \forall r \in R, \forall x \in I, & x+r = r+x \in I \end{cases} \Rightarrow \begin{cases} x \in I \Rightarrow x-x=0 \in I & \text{证} \\ x \in I \Rightarrow 0-x=-x \in I & \text{证} \\ y-x \in I \Rightarrow y-(-x)=y+x \in I & \text{证} \end{cases} \Rightarrow \langle 1, + \rangle \text{ 是群}$$

eg: $\langle \mathbb{Z}, +, \times \rangle$ 中所有偶数 $2\mathbb{Z}$ 为 $\mathbb{Z}$ 的理想
 $\langle \mathbb{Z}, +, \times \rangle$ 中所有 3 的倍数, 为 $\mathbb{Z}$ 的理想
 $\langle \mathbb{Z}_6, +, \times \rangle$ 中 $\{0, 3\}$ 为 $\mathbb{Z}_6$ 的理想

$\langle 1, + \rangle$ 是 $\langle R, + \rangle$ 的子群

主理想: 对于交换环 R : $\forall a \in R$ 均有 $aR = \{ax \mid x \in R\}$ 为 R 的一个理想
 并称 aR 是环 R 的一个主理想

证: aR 为 R 的理想

1) $\forall x, y \in aR, x-y = ax'-ay' = a(x'-y') \Rightarrow x-y \in aR$

2) $\forall r \in R, x \in aR$ 则:

$$r \cdot x = r \cdot ax' = a(rx') \in aR$$

$$\text{同理 } x \cdot r = a \cdot x' \cdot r = a(x'r) \in aR$$

则 aR 为 R 的理想

eg: $\langle \mathbb{Z}, +, \times \rangle, \langle 3, \mathbb{Z} \rangle = \{3s \mid s \in \mathbb{Z}\}$ 为 $\mathbb{Z}$ 中所有 3 的倍数.
 则 $\langle 3, \mathbb{Z} \rangle$ 为 $\langle \mathbb{Z}, +, \times \rangle$ 的一个主理想

主理想环: 若一个环的所有理想均为主理想, 则称其为主理想环
 主理想环 + 整环 $\rightarrow$ 主理想整环 (PID)

eg: $\langle \mathbb{Z}, +, \times \rangle$ 为主理想整环 (PID)

证: $\forall I$ 为 $\langle \mathbb{Z}, +, \times \rangle$ 的一个理想, 则 a 为 I 中非零正整数, 下证 I 由 a 生成.

$$\rightarrow \text{证: 设 } \exists b \in I, a \nmid b \text{ 则 } \exists r (0 < r < a), b \in \mathbb{Z}, b = qa + r$$

$$\text{有 } b - qa = b - a - a \dots - a \text{ 由理想性质 } b - qa \in I \text{ 且 } 0 < b - qa < a$$

$\mathbb{Z}[x]$ 不是一个主理想整环 $\left\{ \sum_{i=0}^k a_i x^i \mid k \in \mathbb{N}, a_0 \in \mathbb{Z} \text{ 且 } 2 \nmid a_0 \right\}$ 是理想但非主理想

由多个元素生成的理想?

$\forall a, b \in R, aR + bR = \{a \cdot r_1 + b \cdot r_2 \mid r_1, r_2 \in R\}$ 也是一个理想

更一般的: 对有限 $S = \{a_1, a_2, \dots, a_k\}$:

由 S 生成的理想 $SR = \{a_1 r_1 + a_2 r_2 + \dots + a_k r_k \mid r_i \in R\}$

$\langle 2, x \rangle$ 是主理想整环

$\mathbb{Z}[x]$ 不是 PID: 易知有 $\{2, x\} \subseteq \mathbb{Z}[x]$ 的环

$\mathbb{Q}[x]$ 是 PID: 这里 $\{2, x\} \subseteq \mathbb{Q}[x] = \mathbb{Q}[x]$, 仍例子不通.

$\downarrow$ $\forall f(x) \in \mathbb{Q}(x)$ $f(x)\mathbb{Q}(x)$ 为 $\mathbb{Q}(x)$ 理想且为主理想

$\mathbb{Q}(x)$ 为 $\mathbb{Q}(x)$ 理想, 取 $\mathbb{Q}(x)$ 中次数最小的首一多项式 $r(x)$ 唯一 (到可相乘)

证 $1 = r(x)\mathbb{Q}(x) \rightarrow$ 反证: 若 $\exists b(x) \in 1, b(x) \notin r(x)\mathbb{Q}(x)$

$b(x) = k(x)r(x) + r'(x)$ 且 $\deg(r'(x)) < \deg(r(x))$ 且 $\deg(r(x)) > 0$ 且 $r'(x) \in 1$
与 $r(x)$ 次数最小矛盾 $\Rightarrow r(x) \mid b(x)$ 则 $b(x) \in r(x)\mathbb{Q}(x)$

命题: 凡是至少做带余除法的整环称为欧氏整环 (ED) 且 ED 一定为 PID

$R: \delta: R \rightarrow \mathbb{N} \quad \delta(0) = 0 \quad \delta(a) > 0 \quad \forall a \neq 0$

$\forall a, b \in R \setminus \{0\} \quad \exists k, r \in R \text{ s.t. } a = kb + r \quad 0 \leq \delta(r) < \delta(b)$

什么样的环可以做唯一分解 (UFD)?

对任意整环 R (单位 $e \in R$ 为单位) $\exists b \in R \text{ s.t. } eb = 1$

素元: $p \in R$ 为素元 $p \mid a \cdot b \Rightarrow p \mid a$ 或 $p \mid b$

不可约元: $p \in R$ 为不可约元: 若 $\exists a, b, p = a \cdot b$ 则 a 或 b 一定是单位

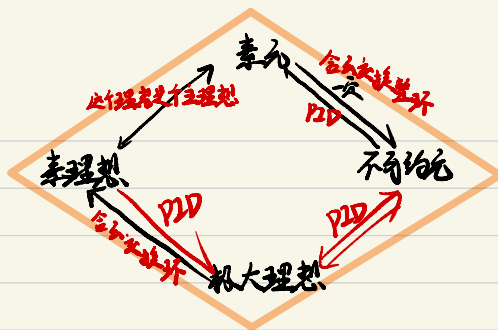
素元一定是不可约元, 不可约元不一定是素元

$\mathbb{Z}: \text{UFD} \quad \mathbb{Z}[\sqrt{-5}]: \text{非UFD} \quad 6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \times 3$

注: 不可约元 $\Leftrightarrow$ 素元 则存在 UFD

$\cdot$ 素理想: $\forall a, b \in R$, 若 $a \cdot b \in I$ 则 $a \in I$ 或 $b \in I$

$\cdot$ 极大理想: 若 $\exists$ 理想 $J (\neq I)$, 有 $I \subseteq J$, 则 $J = R$



→ 在 $\mathbb{Z}$ 上全价 ($\mathbb{Z}$ 为主理想整环 PID)

素元 → 不可约元:

定义: 素元 $p = axb$ 且 a, b 均不为单位.

由素元定义: $p|a$ 或 $p|b$, 不妨取 $p|a$

则 $\exists k \in R$ st $a = kp = kab \xrightarrow{\text{约去}} a(kb-1) = 0 \Rightarrow k, b$ 均为单位

添加整环: $a \times b = 0 \Rightarrow a$ 或 b 为 0

极大理想 → 素理想 (R 含么交换环)

反证: 极大理想 I 非素理想

则 $\exists a, b \in R, ab \in I$ 但 $a \notin I$ 且 $b \notin I$ (尝试构造更大的非 R 理想来推导矛盾)

若 $aR = R$, 则 a 一定是一个单位 ($a^{-1} \in R$)

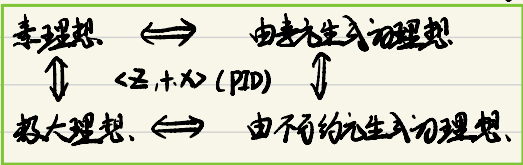
$|bR = R$ 则 b 一定是一个单位 ($b^{-1} \in R$)

$a^{-1}ab \in a^{-1}I = 1 \Rightarrow b \in I$ 与假设矛盾

故 $aR \subsetneq R$ 或 $bR \subsetneq R$ 此时 $1 \in aR \subsetneq R$ 与 I 是极大理想矛盾

故极大理想一定是素理想

$\langle \mathbb{Z}, +, \times \rangle$ (PID): I 为素理想 $\Leftrightarrow$ 素元 p 生成的理想 $\langle p \rangle$



k 是素元 (素数)

看 $\mathbb{Z}[X]$ / $\langle k \rangle$: $\forall f, g \in \mathbb{Z}[X]$ 有 $k|fg$; $fg \in \langle k \rangle \Leftrightarrow k|fg$ 则 $k|f$ 或 $k|g$

非PID $\langle X^2 \rangle$: $\forall f, g \in \langle X^2 \rangle$ 有 $X^2|fg$; $fg \in \langle X^2 \rangle \Leftrightarrow X^2|fg$ 则 $X^2|f$ 或 $X^2|g \Leftrightarrow t=1$

$\langle X, 2 \rangle$: $X, 2$ 是素元 $\langle X, 2 \rangle$ 是素理想, $\forall f, g \in \langle X, 2 \rangle$ 若 $fg \in \langle X, 2 \rangle$ 则 f 或 g 中有一个为偶

(对主理想) $aR, b \in R \Leftrightarrow a|_R b$

命题: 素元生成的理想一定为素理想? $\forall I \in \mathbb{Z}[x], I$ 由素元生成, I 是主理想 $\rightarrow$ 欧氏主理想

i) $I = \langle p \rangle$, p 为素元: $p|ab$ 则 $p|a$ 或 $p|b$

$\Downarrow$ $\downarrow$ $\updownarrow$ $\updownarrow$
 $\langle p \rangle$ 为素理想: $ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ 或 $b \in \langle p \rangle$

ii) $\langle a_1, a_2, \dots, a_n \rangle: \langle \{a_1 r_1 + a_2 r_2 + \dots + a_n r_n \mid r_i \in R\}, +, \times \rangle$

$\langle x, y \rangle = \langle x, x+y \rangle$ (变换性质, 一个理想的生成元唯一)

$\downarrow$ $\downarrow$
 素元 素元 (须验证)

$\langle k \rangle$ 是极大理想 $\Rightarrow k$ 是不可约元

证: $\langle k \rangle$ 不是极大理想, 则 $\exists I \subsetneq J \subsetneq R$ 证 $k \in J, k \nmid k$

取 $k_1 \in J$ 为 J 中最大正整数, 有 $k_1 > 1$ (否则 $J=R$)

在 J 中: 须 $k \mid k_1$ 则 $\exists r$ s.t. $k_1 = t \cdot k + r \Rightarrow r = k_1 - t \cdot k \in J$ 与 k_1 矛盾

则 $k \mid k$ 但 k 是不可约元, 矛盾, 则 I 为极大理想

$\Rightarrow \mathbb{Z}[x]$ 中: $\langle k \rangle$ 是素理想 $\Leftrightarrow k$ 是素元 $\Leftrightarrow k$ 是不可约元 $\Leftrightarrow \langle k \rangle$ 是极大理想

$\langle x \rangle$ 是素理想 $\Leftrightarrow t=1$, 则 x 为素元 $\Leftrightarrow x$ 为不可约元 $\Leftrightarrow \langle x \rangle$ 是极大理想

证 $\langle x \rangle$ 是极大理想 $\Rightarrow x$ 是不可约元

若 x 非不可约元, 有 $x = x_1 \cdot x_2$ 则 $\langle x \rangle \subsetneq \langle x_1 \rangle \subsetneq \mathbb{Z}[x]$, 则 $\langle x \rangle$ 非极大理想

$\langle x \rangle$ 不是极大理想: 想 $\exists J$ s.t. $\langle x \rangle \subsetneq J \subsetneq \mathbb{Z}[x]$

取 $J = \langle x, 2x^2 \rangle$ 无法定义

$\langle x, 2 \rangle$ 是素理想 $\Leftrightarrow \{x, 2\}$ 是素元 $\Leftrightarrow \{x, 2\}$ 是不可约元 $\leftarrow \langle x, 2 \rangle$ 是极大理想

设 $\langle x, 2 \rangle \subsetneq J \subsetneq R$, J 中有奇数 $\Rightarrow J$ 中有 1 (因 $1 \in \langle x, 2 \rangle$) 与 $J \subsetneq R$ 矛盾

$\langle x, 4 \rangle$, or $\langle x, x+4 \rangle$ 非素理想 非极大理想

很需要在PID下讨论

$\langle x, 2 \rangle$ 都满足

PID的素理想一定由素元生成

PID的极大理想一定由不可约元生成

若PID的素理想均为极大理想, 则PID的素元与不可约元等价

PID: 主理想整环, 每个理想均为素理想, 的整环 ($ab=0$ 则 $a=0$ 或 $b=0$)

且 $\mathbb{Z}(E) \Rightarrow \text{PID} \Rightarrow \text{UFD}$ (唯一分解)