

环: $\langle R, +, \cdot \rangle$ 有集合, 在集合上定义了加法 & 乘法, 且满足:

$$\begin{cases} \forall a, b \in R, a+b \in R, a \cdot b \in R & (R \text{ 对 } +, \cdot \text{ 均封闭}) \\ 0 \in R, 1 \in R & (\text{含零元与幺元, 后面会严格定义}) \\ \forall a \in R, \text{有 } -a \in R & (\text{加法定义下有逆元}) \end{cases}$$

则称 R 是环 (Ring)

eg: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ Even 无统 $\{a+bi \mid a, b \in \mathbb{Z}\}$ 或环. 记作 $\mathbb{Z}[i]$

def: 不可约元: $a \in R$ 为不可约元若:

$$\begin{cases} a \text{ 不为单位} \\ \forall bc = a (b, c \in R) \text{ 则 } b \text{ 或 } c \text{ 为单位} \end{cases}$$

def: 素元: $a \in R$ 为素元, 若:

$$\begin{cases} a \neq 0, a \neq \pm 1 \\ \forall b, c \in R, \text{ 若 } a \mid bc \text{ 则 } a \mid b \text{ 或 } a \mid c \quad (a \mid bc : \exists k \in R \text{ s.t. } ak = bc) \end{cases}$$

素元与不可约元关系:

i) 素元一定是不可约元.

反证: 设 $p \in R$ 是素元但不是不可约元, 则 $\exists a, b \in R$ 且均不是单位, $ab = p$.

由 $1 \in R$ 则 $1 \cdot p = a \cdot b \Rightarrow p \mid a$ 或 $p \mid b$ (p 是素元)

不妨设 $p \mid a, \exists k \in R \text{ s.t. } a = kp$

由 $ab = p \Rightarrow bkp = p \Rightarrow p(1-bk) = 0$ 而 $p \neq 0 \Rightarrow bk = 1$ 与 b 不是单位矛盾.

ii) 不可约元不一定是素元.

找反例: $\mathbb{Z}[\sqrt{5}] = \{a+b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ 中: 2 是不可约元但不是素元.

单位有: $\pm 1, \pm 2\sqrt{5}$ $\begin{cases} 2 \mid (1-\sqrt{5})(1+\sqrt{5}) \text{ 但 } 2 \nmid (1-\sqrt{5}) \text{ 且 } 2 \nmid (1+\sqrt{5}) \text{ 非素元} \\ 2 \text{ 不可约元} \dots \text{ 没有单位 (忽略模4)} \end{cases}$

iii) 若 R 中不可约元都是素元, 则 R 中有唯一-台解. 台解或不可约元的乘积

先看: $\mathbb{Z}[\sqrt{5}]$ 中存在唯一-台解?

$b = (1-\sqrt{5})(1+\sqrt{5}) = 2 \times 3$ 不存在唯一-台解. (以后再看环上的唯一-台解)