1. 对于环 R，如果对任意 $a \in R$ 有 $a^2 = a$，证明 R 是交换环并且对任意 $a \in R$，有 $2a = 0$.

$\langle R, +, * \rangle$ 有两个运算，都要考虑、

$\begin{cases} (2a)^2 = 4a^2 = 4a \\ (2a)^2 = 2a \end{cases}$ $\rightarrow [(2a)^2 = (a+a)(a+a) = a^2 + \cdots = 4a^2]$ $\Rightarrow 4a = 2a \Rightarrow 2a(2-1) = 0$ 即 $2a = 0$

$2\boxed{ab} = 0$
$ab = -ab$

再：$\begin{cases} (ab)^2 = abab = ab \\ (a+b)^2 = a^2 + ab + ba + b^2 = a+b \end{cases}$

$\quad\quad\quad a + ab + ba + b \Rightarrow ab + ba = 0$ 即 $ab = -ba$

于是 $ab = abab \overset{ab=-ba}{=\!=} -aabb = -ab = ba$

则 R 是交换环且 $2a = 0$.

2. 设 I_1 和 I_2 是环 R 的理想，令

$$I_1 + I_2 = \{r_1 + r_2 \mid r_1 \in I_1, r_2 \in I_2\},$$

$$I_1 \cdot I_2 = \{\sum_{i=1}^{k} r_{1i} \cdot r_{2i} \mid r_{1i} \in I_1, r_{2i} \in I_2 (1 \leq i \leq k), k \in \mathbb{N}+\}.$$

证明 $I_1 \cap I_2$, $I_1 + I_2$, $I_1 \cdot I_2$ 都是 R 的理想（注意环 R 未必交换）。

$\rightarrow$ I 是 R 的理想：$\begin{cases} a, b \in I \Rightarrow a - b \in I \\ \forall r \in R, a \in I, ra, ar \in I \end{cases}$

1) $I_1 \cap I_2$：$\forall a, b \in I_1 \cap I_2$，$\begin{cases} a, b \in I_1 \Rightarrow a - b \in I_1 \\ a, b \in I_2 \Rightarrow a - b \in I_2 \end{cases}$ $\Rightarrow a - b \in I_1 \cap I_2$

$\forall r \in R, a \in I_1 \cap I_2$：$\begin{cases} ra, ar \in I_1 \\ ra, ar \in I_2 \end{cases}$ $\Rightarrow ra, ar \in I_1 \cap I_2$

故 $I_1 \cap I_2$ 是 R 的理想、

2) $I_1 + I_2$ $\forall a, b \in I_1 + I_2$：$\exists a_1, b_1 \in I_1, a_2, b_2 \in I_2$ s.t $\begin{cases} a = a_1 + a_2 \\ b = b_1 + b_2 \end{cases}$

于是 $a - b = (a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2)$ （加法交换律）

而 $\begin{cases} a_1 - b_1 \in I_1 \\ a_2 - b_2 \in I_2 \end{cases}$ $\Rightarrow (a_1 - b_1) + (a_2 - b_2) \in I_1 + I_2$

$\forall r \in R$. $a \in I_1 + I_2$ 即 $\exists a_1 \in I_1, a_2 \in I_2$ s.t $a = a_1 + a_2$

$$\begin{cases} r*a = r*(a_1+a_2) = r*a_1 + r*a_2 \\ a*r = (a_1+a_2)*r = a_1*r + a_2*r \end{cases}$$

其中 $\begin{cases} r*a_1,\ a_1*r \in I_1 \\ r*a_2,\ a_2*r \in I_2 \end{cases}$ 故 $r*a,\ a*r \in I_1+I_2$

故 I_1+I_2 是 R 的理想

3) I_1*I_2 $\forall x, y \in I_1*I_2$ 有: $\begin{cases} x = \sum_{i=1}^{m} a_i b_i, & a\in I_1, b\in I_2 \\ y = \sum_{i=1}^{n} c_i d_i & c\in I_1, d\in I_2 \end{cases}$

$$\Rightarrow x-y = \sum_{i=1}^{m} a_i b_i + \sum_{i=1}^{n} (-c_i) d_i = \sum_{i=1}^{m+n} p_i q_i \in I_1*I_2$$

再 $\forall r\in R$. $x\in I_1*I_2$ 有 $\begin{cases} r*x = r\sum_{i=1}^{k} a_i b_i = \sum_{i=1}^{k} (ra_i) b_i \in I_1*I_2 \\ x*r = (\sum_{i=1}^{k} a_i b_i) r = \sum_{i=1}^{k} a_i (b_i r) \in I_1*I_2 \end{cases}$

故 I_1*I_2 是 R 的理想

3. 考虑模 6 的剩余系所构成的环 $\langle \mathbb{Z}_6, +, \cdot \rangle$，在其中找出一个元素，它是素元但不是不可约元。

$\begin{cases} \text{素元}: p \mid ab \Rightarrow p\mid a \text{或} p\mid b \\ \text{不可约元}: \text{因子必有单位} \end{cases}$

$\gcd(5, 6) = 1$ 则 1、5 均为 $\mathbb{Z}_6$ 的单位.

考虑 2: 设 2 不是素元, 有 $2\mid ab$ 且 $2\nmid a$ 且 $2\nmid b$, 则 $a, b \in \{1, 3, 5\}$

此时 $ab \in \{1, 3, 5\}$ 与 $2\mid ab$ 矛盾. 故 2 是素元

再考虑 $2 = 2\times 4 \pmod 6$ 其中 2、4 均非单位, 故 2 不是不可约元

综上, 2 是素元而非不可约元

4. 证明：对于交换环 R，若 R 是整环，则 R 中$\boxed{\text{素元}}$必是$\boxed{\text{不可约元}}$。

整环：$\begin{cases} R\text{ 对乘法可交换} \\ a*b=0 \text{ 则 } a=0 \text{ 或 } b=0 \end{cases}$

$\forall\, p\in R$ 为素元，有 $p|ab \Rightarrow p|a$ 或 $p|b$

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

由 $p=ab \Rightarrow p|a$ 或 $p|b$ 不妨设 $p|a$（另一种情况同理）

则 $\exists\, k\in R$ s.t. $a=kp=kab$

$\Rightarrow a(kb-1)=0$ （交换律）

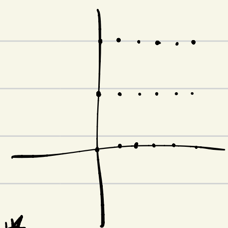
$a\neq 0$ 则 $kb-1=0$ （整环定义）

则 b 是单位.

从而，整环 R 中素元一定是不可约元

5. 考虑环 $\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$，该环是不是主理想整环？若是请证明，若不是请给出一个不是主理想的理想。

见 $\mathbb{Z}[\sqrt{-5}]$ 多用模长解决问题



$\begin{cases} \text{主理想：由一个元素生成的理想} \quad aR=\{a*r \mid r\in R\} \\ \text{主理想整环：所有理想均是主理想的整环} \end{cases}$

考虑 $I=\langle 2, 1+\sqrt{-5}\rangle = \{2(a+b\sqrt{-5})+(1+\sqrt{-5})(c+d\sqrt{-5}) \mid a,b,c,d\in\mathbb{Z}\}$

$=\{(2a+c-5d)+(2b+c+d)\sqrt{-5} \mid a,b,c,d\in\mathbb{Z}\}$

1) 说明 $I\neq R$，观察 I 中系数：$(2a+c-5d)-(2b+c+d)=2a-2b-6d$ 为偶数

也即 $x=p+q\sqrt{-5}$ 时 p, q 奇偶性相同，显然无法取到所有组合 $\Rightarrow I\neq R$

2) 设 I 为主理想，则 $\exists\,\alpha$ s.t. $\langle 2, 1+\sqrt{-5}\rangle=\langle\alpha\rangle$

首先有 $\begin{cases} 2\in\langle\alpha\rangle \\ 1+\sqrt{-5}\in\langle\alpha\rangle \end{cases}$ 则 $\exists\, r_1, r_2\in R$ s.t. $\begin{cases} 2=\alpha r_1 \\ 1+\sqrt{-5}=\alpha r_2 \end{cases}$ 首先有 $|\alpha|\leq 2$ 且 $|\alpha|\leq\sqrt{6}$

于是 $|\alpha|\leq 2 \Rightarrow |\alpha|$ 可取 $1, 2$ 则 α 可取 $\pm1, \pm2$.

$\begin{cases} \alpha=\pm1 \text{ 时 } \langle\alpha\rangle=R \text{ 不可} \\ \alpha=\pm2 \text{ 时，} 1+\sqrt{-5}\notin\langle\alpha\rangle \quad \text{cause } \exists\, r\in R \text{ s.t. } r\alpha=1+\sqrt{-5} \Rightarrow |r|=\frac{\sqrt{6}}{2} \text{ 不存在.} \end{cases}$

故 $\langle 2, 1+\sqrt{-5}\rangle$ 非主理想 $\Rightarrow \mathbb{Z}[\sqrt{-5}]$ 非 PID

6. 设 R 为含幺交换整环，对于任意 $a \in R$ 且 $a \neq 0$，令 (a) 表示由 a 生成的理想。证明：

(a) a 是素元当且仅当 (a) 是素理想。

(b) 若 R 是主理想整环，则 a 是不可约元当且仅当 (a) 是极大理想。

(c) 若 R 是主理想整环，则 R 中的极大理想必是素理想，进而 R 中的不可约元必是素元。

a) a是素元：$a \mid xy \Rightarrow a \mid x$ 或 $a \mid y$

$\langle a \rangle$是素理想：$xy \in \langle a \rangle$ 则 $x \in \langle a \rangle$ 或 $y \in \langle a \rangle$

($\Rightarrow$) $xy \in \langle a \rangle$ 则 $\exists\, r \in R$ s.t $ar = xy$ 即 $a \mid xy$

由素元定义 $a \mid x$ 或 $a \mid y$ 则 $x \in \langle a \rangle$ 或 $y \in \langle a \rangle$

($\Leftarrow$) 设 a 非素元，且 $\exists\, x, y$ s.t $a \mid xy$ 但 $a \nmid x$ 且 $a \nmid y$

此时：$xy \in \langle a \rangle$ 但 $a \nmid x$ 且 $a \nmid y$ 即 $x \notin \langle a \rangle$ 且 $y \notin \langle a \rangle$

则 $\langle a \rangle$不是素理想　　毕.

b) R为PID：R中所有理想都是主理想.

a是不可约元：$a = xy$ 则 x 为单位或 y 为单位.

$\langle a \rangle$是极大理想：不存在理想J s.t. $\langle a \rangle \subsetneq J \subsetneq R$

($\Rightarrow$) a是不可约元. 设$\langle a \rangle$不是极大理想. 则 $\exists\, b$ s.t $\langle a \rangle \subsetneq \langle b \rangle \subsetneq R$ （主理想环）

于是 $a \in \langle b \rangle \Rightarrow \exists\, r \in R$ s.t $a = br$ $\begin{cases} b\text{为单位，则}\langle b \rangle = R \text{ 矛盾} \\ r\text{为单位 则}\langle b \rangle = \langle a \rangle \text{矛盾} \end{cases}$　　故($\Rightarrow$)成立

($\Leftarrow$) 反证：设 $a = bc$ 且 b, c 均不为单位

构造$\langle b \rangle$ 那么有 $\langle a \rangle \subsetneq \langle b \rangle \subsetneq R$　与$\langle a \rangle$是极大理想矛盾. 故($\Leftarrow$)成立.

c不是单位　　b不是单位.

c) 设极大理想I不是素理想，则 $\exists\, ab \in I$ 但 $a, b \notin I$

此时考虑 $I + aR$ 是R的理想（见T2）

$a \notin I$ 故 $I \subsetneq I + aR$，又I是极大理想 $\Rightarrow$ $I + aR = R$ 有 $1 \in aR$ 故有 $aR = R \Rightarrow a$可逆

这个不一定

同理 b可逆. 由 $ab \in R \Rightarrow a^{-1}ab = b \in I$ 矛盾.

故极大理想一定是素理想

设极大理想 I 不是素理想，则 $\exists\, ab \in I$ 但 $a, b \notin I$

此时考虑 $I + aR$ 是 R 的理想 (见T2)

$$a, b \notin I \Rightarrow \begin{cases} I \subsetneqq I + aR \\ I \subsetneqq I + bR \end{cases} \Rightarrow \begin{cases} I + aR = R \\ I + bR = R \end{cases} \text{(因 } I \text{ 是极大理想)}$$

则 $\exists\, i_1, i_2 \in I,\ r_1, r_2 \in R$ s.t. $\begin{cases} i_1 + ar_1 = 1_R \\ i_2 + br_2 = 1_R \end{cases}$ (含幺环)

$$\Rightarrow (i_1 + ar_1)(i_2 + br_2) = \underline{i_1 i_2} + \underline{ar_1 i_2} + \underline{i_1 br_2} + ar_1 br_2 = 1_R$$

其中 $i_1 i_2$, $ar_1 i_2$, $i_1 br_2 \in I$ (理想的吸收律)

而 $\begin{cases} ar_1 br_2 = abr_1 r_2 \text{ (交换环)} \\ ab \in I \end{cases} \Rightarrow ar_1 br_2 \in I$

$\Rightarrow 1_R \in I$ 与 I 是极大理想矛盾.

or 用商环的特性:

I 是极大理想 $\Rightarrow$ R/I 是域 (因为 R/I 只有平凡理想)

$\begin{cases} I \text{ 是 } R \text{ 中极大理想} \Longleftrightarrow \text{商环 } R/I \text{ 是域 (因 } R/I \text{ 中只有平凡理想)} \\ P \text{ 是 } R \text{ 中素理想} \Longleftrightarrow \text{商环 } R/P \text{ 是整环.} \\ \text{域一定是整环} \end{cases}$

$\Rightarrow$ 后面再证

7. 整环 R 被称作欧式整环：如果存在一个从 R 中元素到非负整数集 $\mathbb{Z}$ 的映射 ϕ，使得

N

(a) $\phi(a)=0$ 当且仅当 $a=0$。

(b) 对于任意 $a,b\in R$ 且 $b\neq 0$，均有 $q,r\in R$ 使得 $a=bq+r$，并且 $\phi(r)<\phi(b)$.

请给出一个欧式整环的例子，并证明欧式整环一定是主理想环。

1) 简单例子：整数环 $\langle Z,+,\times\rangle$: $\phi: Z\to N: \phi(a)=|a|$

(还可取 $Q[x]$，能做带余除法的都行)

由整数带余除法，Z 是欧式整环

2) 对于欧式整环 E：

对其中一个理想 I，取其中 ϕ 值最小的正数 b $\longrightarrow$ (给定义一下)

由 $b\in I$，于是 $\langle b\rangle\in I$

同时 $\forall a\in I$，由 E 定义，$\exists q,r\in E$ s.t. $a=qb+r$，$\phi(r)<\phi(b)$

而 $\phi(b)$ 是 0 以外最小数 $\Rightarrow \phi(r)=0 \Rightarrow r=0$

故 $b|a \Rightarrow a\in\langle b\rangle$

故而 $\langle b\rangle = I$ 即任一理想均为主理想 $\Rightarrow$ 则 E 为 PID

8. 证明：含幺交换有限环的素理想必是极大理想。

1) 直接做：设此环为 R，设 P 是 R 的一个素理想

$a\cdot a^{k-1}\in P$ 则 $a^{k-1}\in P$ ($a\notin P$) 递推

$\begin{cases} \forall a\in R\backslash P,\ \forall k\in Z^{+}，有\ a^k\notin P\ (P为素理想，若\ a^k\in P\ 可证\ a\in P) \\ 又\ 0\in P \Rightarrow a\neq 0 \end{cases}$

而 R 是有限环：$\exists i<j$ s.t. $a^i=a^j\neq 0 \Rightarrow a^i(a^{j-i}-1)=0\in P$

由素理想定义：$a^i\notin P$ 则 $a^{j-i}-1\in P$ 即 $\exists p\in P$ s.t. $a^{j-i}=1+p$

即：$\forall a\in R\backslash P$，$\exists b=a^{j-i-1}\in R$ s.t. $ab=1+p$，对某 $p\in P$ 成立.

设 $\exists I$ s.t. $P\subsetneq I$ 则 $\exists a\in I\backslash P$ 进而由上：$\exists b\in R$ s.t. $ab=1+p\in I$ 其中 $p\in P\in I$

故而 $ab-p=1\in I \Rightarrow IR=R\subseteq I$ 则 $I=R$

综上：P 是极大理想.

2) 用商环：
$$\begin{cases}\text{lemma1}：P\text{为素理想，则 } R/P \text{ 是一个整环}\\ \text{lemma2}：\text{交换环中，}P\text{是极大理想} \Leftrightarrow R/P\text{是一个域}\\ \text{lemma3}：\text{有限整环一定是域}\end{cases}$$

由lemma1：现有 $S=R/P$ 是整环，且是有限整环

对 取 $\tilde S = S\setminus\{0\}$. $\forall a\in\tilde S$, $a\tilde S=\tilde S$ $\longrightarrow$ $f(x)=ax$ 是单射，且 $|a\tilde S| = |\tilde S|$ 故而是双射

则 $\exists\, r\in\tilde S$ s.t. $ar=1$. 即 a 均可逆 $\Rightarrow$ S 是一个域

再由lemma2，P 是极大理想。

商环中运算：
$$\begin{cases}(a+I)+(b+I)=(a+b)+I\\ (a+I)\cdot(b+I)=a\cdot b+I\end{cases}$$

证 lemma1：I 是素理想 $\Leftrightarrow$ R/I 是整环

$(\Rightarrow)$ 目标 R/I 中无零因子，即 $(a+I)(b+I)=0+I$ 则 $a+I=0+I$ 或 $b+I=0+I$

其中 $(a+I)(b+I)=0+I \Longleftrightarrow ab+I=0+I$ $(aI+bI+I^2\subseteq I)$ $\Longleftrightarrow ab\in I$

而 I 是素理想，$ab\in I\Rightarrow a\in I$ 或 $b\in I$ 则 $a+I=I$ 或 $b+I=I$

故而 R/I 是整环

$(\Leftarrow)$ R/I 是整环，已有 $(a+I)(b+I)=0+I$ 时 $a+I=0+I$ 或 $b+I=0+I$

即：$ab\in I$ 时已有 $a\in I$ 或 $b\in I$

则 I 为素理想。

证 lemma2：I 是极大理想 $\Leftrightarrow$ R/I 是域

$(\Rightarrow)$ I 是极大理想，证：R/I 中每个非零元均有乘法逆元

取 $a+I$ 为 R/I 中任非零元，有 $a\notin I$，考虑 $I+aR$，由 $a\notin I$ 有 $I\subsetneqq I+aR$

又 I 为极大理想 $\Rightarrow I+aR=R$. 则 $\exists\, i\in I, r\in R$ s.t. $i+ar=1_R$ 在商环中即 $(a+I)(r+I)=1+I$

此时 $r+I$ 即为 $a+I$ 的乘法逆元

$(\Leftarrow)$ 已知 R/I 是域 $=ar+I=1+I$

反证：设 $\exists J$ 为 R 的理想且 $I\subsetneqq J\subsetneqq R$

取 $b\in J\setminus I$，则 $b+I$ 是 R/I 中的非零元 (否元在 $I\cap J=I$ 中)

而 R/I 是域 $\Rightarrow$ $b+I$ 有乘法逆元，设 $r+I$.

$(b+I)(r+I)=1+I \Rightarrow br\equiv 1_R \pmod I$

$\Rightarrow 1\in J$ 则 $J=R$ 则 I 为极大理想