Lemma：R是整环，p是R的一个任意的素元，对$\forall\ \alpha\in R^{\times}$，有：$\alpha p=p\alpha$是$R$的素元.

Proof：$\because$ p是R的素元 $\therefore$ $p\in R$ 且 $p\neq 0_R$ 且 $p\notin R^{\times}$.

$\because$ $\cancel{\alpha\in R^{\times}}$ R是整环 $\therefore$ R是非零环 $\therefore$ $R^{\times}\subseteq R\setminus\{0_R\}$

$\because$ $\alpha\in R^{\times}\subseteq R$ $\therefore$ $\alpha p\in R$. $\because$ $\alpha\neq 0_R$ 且 $p\neq 0_R$ $\therefore$ $\alpha p\neq 0_R$

假设 $\alpha p\in R^{\times}$，则$\exists\,\beta\in R$，s.t. $\beta(\alpha p)=1_R=(\alpha p)\beta$

$\therefore$ $(\beta\alpha)p=1_R=p(\beta\alpha)$ $\therefore$ $p\in R^{\times}$ 矛盾. $\therefore$ $\alpha p\notin R^{\times}$

$\therefore$ R是整环，$\alpha p\in R$，$\alpha p\neq 0_R$，$\alpha p\notin R^{\times}$

$\because$ R是整环 $\therefore$ R是交换环 $\therefore$ $\alpha p=p\alpha$

对$\forall\ a,b\in R$，若 $\alpha p\mid ab$，则$\exists\,d\in R$，s.t. $ab=d(\alpha p)$

$\because$ $ab=(d\alpha)p$，$d\alpha\in R$ $\therefore$ $p\mid ab$ $\because$ p是R的素元 $\therefore$ $p\mid a$或$p\mid b$

若$p\mid a$，则$\exists\,\lambda\in R$，s.t. $a=\lambda p$ $\because$ $\alpha\in R^{\times}$ $\therefore$ $a=(\lambda\alpha^{-1})(\alpha p)$

$\therefore$ $\alpha p\mid a$

若$p\mid b$，则$\exists\,\mu\in R$，s.t. $b=\mu p$ $\therefore$ $b=(\mu\alpha^{-1})(\alpha p)$ $\therefore$ $\alpha p\mid b$

$\therefore$ $\alpha p\mid a$ 或 $\alpha p\mid b$

$\therefore$ $\alpha p=p\alpha$是R的素元. $\square$

定义（偏序集的极大元）$(A, \leqslant)$ 是偏序集，$a_{max} \in A$. 若不存在 $a' \in A$ 使得 $a' > a_{max}$，则称 a_{max} 为 A 的一个极大元.

定义（子集在偏序集中的上界）$(A, \leqslant)$ 是偏序集，$C \subseteq A$，$a \in A$. 若对 $\forall c \in C$，都有 $c \leqslant a$，则称 a 为 C 在 A 中的一个上界.

定义（偏序集中的链）$(A, \leqslant)$ 是偏序集，$C \subseteq A$，若 $(C, \leqslant)$ 是全序集，则称 C 为 A 中的链.

Zorn引理：$(A, \leqslant)$ 是非空偏序集，而且 A 中的每个链 C 在 A 中都有上界，则在 A 中存在极大元 a_{max}.

定义（环的乘法封闭子集）R 是环，$S \subseteq R$，若 $1_R \in S$ 且 S 对于 R 的乘法运算封闭，则称 S 是环 R 的乘法封闭子集.

Lemma（Krull's separation lemma）R 是交换环，I 是 R 的理想，M 是 R 的乘法封闭子集，$I \cap M = \emptyset$，则有：存在 R 的素理想 P，使得：$I \subseteq P$ 且 $P \cap M = \emptyset$.

Proof：定义集合 $\Sigma = \{J \mid J \text{是}R\text{的理想且} I \subseteq J \text{且} J \cap M = \emptyset\}$

$\because$ I 是 R 的理想，$I \subseteq I$，$I \cap M = \emptyset$ $\quad \therefore I \in \Sigma \quad \therefore \Sigma \neq \emptyset$

对 $\forall J \in \Sigma$，$\because$ J 是 R 的理想 $\quad \therefore$ J 是 R 的子集 $\quad \therefore J \subseteq J$ 反身性成立.

对 $\forall J_1, J_2, J_3 \in \Sigma$，若 $J_1 \subseteq J_2$ 且 $J_2 \subseteq J_3$，则 $J_1 \subseteq J_3$ 传递性成立.

对 $\forall J_1, J_2 \in \Sigma$，若 $J_1 \subseteq J_2$ 且 $J_2 \subseteq J_1$，则 $J_1 = J_2$. 反称性成立.

$\therefore (\Sigma, \subseteq)$ 是非空偏序集.

设 C 为 Σ 中的一个任意的链 $\therefore C\subseteq\Sigma$，且 $(C,\subseteq)$ 是全序集.

令 $U=\bigcup\limits_{J\in C}J$

对 $\forall J\in C$，有：$J\in\Sigma$ $\therefore J$ 是 R 的理想 $\therefore J$ 是 R 的非空子集

$\therefore U=\bigcup\limits_{J\in C}J$ 是 R 的非空子集.

对 $\forall x,y\in U$，$\because x\in U$ $\therefore\exists J_1\in C$，s.t. $x\in J_1$

$\because y\in U$ $\therefore\exists J_2\in C$，s.t. $y\in J_2$

$\because(C,\subseteq)$ 是全序集 $\therefore J_1\subseteq J_2$ 或 $J_2\subseteq J_1$ 至少有一者成立.

若 $J_1\subseteq J_2$，则 $x\in J_2$，$y\in J_2$，$J_2\in\Sigma$ $\therefore J_2$ 是 R 的理想 $\therefore x+y\in J_2$

$\therefore x+y\in U$

若 $J_2\subseteq J_1$，则 $x\in J_1$，$y\in J_1$，$J_1\in\Sigma$ $\therefore J_1$ 是 R 的理想 $\therefore x+y\in J_1$

$\therefore x+y\in U$

$\therefore x+y\in U$

对 $\forall r\in R$，任取 rU 中的一元：rx（其中 $x\in U$）

$\because x\in U$ $\therefore\exists J\in C$，s.t. $x\in J$ $\because J\in C$ $\therefore J\in\Sigma$ $\therefore J$ 是 R 的理想

$\therefore rx\in rJ\subseteq J$ $\therefore rx\in U$ $\therefore rU\subseteq U$

任取 Ur 中的一元：xr（其中 $x\in U$）

$\because x\in U$ $\therefore\exists J\in C$，s.t. $x\in J$ $\because J\in C$ $\therefore J\in\Sigma$ $\therefore J$ 是 R 的理想

$\therefore xr\in Jr\subseteq J$ $\therefore xr\in U$ $\therefore Ur\subseteq U$

$\therefore U$ 是 R 的理想.

对 $\forall J\in C$，有：$J\in\Sigma$ $\therefore I\subseteq J$ $\therefore I\subseteq U$

假设 $U\cap M\neq\emptyset$，则 $\exists x\in U$ 且 $x\in M$ $\therefore\exists J\in C$，s.t. $x\in J$

$\because J\in C$ $\therefore J\in\Sigma$ $\therefore J\cap M=\emptyset$ $\because x\in J$ 且 $x\in M$ $\therefore x\in J\cap M=\emptyset$

矛盾. $\therefore U\cap M=\emptyset$

$\therefore U\in\Sigma$.

$(\Sigma,\subseteq)$是非空偏序集，$C\subseteq\Sigma$，$U\in\Sigma$

对$\forall J\in C$，有：$J\subseteq U$ $\therefore U$为C在Σ中的一个上界.

$\therefore(\Sigma,\subseteq)$是非空偏序集，$\Sigma$中的一个任意的链$C$在$\Sigma$中都有上界.

$\therefore$由Zorn引理，在Σ中存在极大元P

$\because P$是Σ的极大元 $\therefore P\in\Sigma$ $\therefore P$是R的理想且$I\subseteq P$且$P\cap M=\emptyset$

$\because M$是R的乘法封闭子集 $\therefore 1_R\in M$ $\because P\cap M=\emptyset$ $\therefore 1_R\notin P$

$\because R$是交换环，P是R的理想，$1_R\notin P$ $\therefore P\neq R$ $\therefore P$是R的真理想

假设P不是R的素理想，则$\exists a,b\in R$，s.t. $ab\in P$且$(a\notin P$且$b\notin P)$

$\therefore a,b\in R$，$ab\in P$，$a\notin P$，$b\notin P$

$\because R$是交换环，$a\in R$ $\therefore (a)=aR=\{ar: r\in R\}$是$R$的理想

$\because R$是交换环，$b\in R$ $\therefore (b)=bR=\{br: r\in R\}$是$R$的理想

$\because R$是交换环，P是R的真理想，(a)是R的理想，(b)是R的理想.

$\therefore P+(a)$是R的理想，$P\subseteq P+(a)$

$P+(b)$是R的理想，$P\subseteq P+(b)$

$\because a=a\cdot 1_R=0_R+a\cdot 1_R\in P+(a)$，$a\notin P$ $\therefore P\subsetneqq P+(a)$

$\because b=b\cdot 1_R=0_R+b\cdot 1_R\in P+(b)$，$b\notin P$ $\therefore P\subsetneqq P+(b)$

$\because I\subseteq P$ $\therefore I\subseteq P+(a)$且$I\subseteq P+(b)$

$\because(\Sigma,\subseteq)$是非空偏序集，$P\in\Sigma$，$P$是$\Sigma$的极大元.

$\because P+(a)\notin\Sigma$ 且 $P+(b)\notin\Sigma$

$\therefore P+(a)\cap M\neq\emptyset$, $P+(b)\cap M\neq\emptyset$

$\therefore \exists\alpha\in P+(a)\cap M$, $\exists\beta\in P+(b)\cap M$

$\because \alpha\in P+(a)$ $\therefore \alpha=p_1+ar_1$ (其中 $p_1\in P$, $r_1\in R$)

$\because \beta\in P+(b)$ $\therefore \beta=p_2+br_2$ (其中 $p_2\in P$, $r_2\in R$)

$\therefore \alpha\in M$ 且 $\beta\in M$

$\because M$是R的乘法封闭子集 $\therefore \alpha\beta\in M$

$\because \alpha\beta=(p_1+ar_1)(p_2+br_2)=p_1(p_2+br_2)+(ar_1)(p_2+br_2)$

$=p_1p_2+p_1(br_2)+(ar_1)p_2+(ar_1)(br_2)$

$=p_1p_2+p_1(br_2)+(ar_1)p_2+(ab)(r_1r_2)\in P$

$\therefore \alpha\beta\in P\cap M=\emptyset$ 矛盾.

$\therefore P$是R的素理想.

$\therefore P$是R的素理想 且 $I\subseteq P$ 且 $P\cap M=\emptyset$. $\square$

Lemma: R是整环, 定义 $T=R^{\times}\cup\{p_1p_2\cdots p_n \mid n\in\mathbb{Z}_{\geq 0}$, 对$\forall i=1,\cdots,n$, p_i是R的素元$\}$

(如果整环R中没有素元, 则这种情况就是 $n=0$ 的情况, 此时 $T=R^{\times}$)

对$\forall a,b\in R$, 若$ab\in T$, 则 $a\in T$且 $b\in T$.

Proof: $\because ab\in T$ $\therefore$分两种情况讨论:

① $ab\in R^{\times}$. $\because R$是整环 $\therefore R$是交换环 $\therefore ab=ba$

$\because ab\in R^{\times}$ $\therefore \exists\alpha\in R$, s.t. $\alpha(ab)=1_R=(ab)\alpha$

$\therefore (b\alpha)a=1_R=a(b\alpha)$ $\therefore a\in R^{\times}$ $\therefore a\in T$

$\because (\alpha a)b=1_R=b(\alpha a)$ $\therefore b\in R^{\times}$ $\therefore b\in T$ $\therefore a\in T$且$b\in T$

② $ab \in \{p_1p_2\cdots p_n \mid n\in\mathbb{Z}_{\geq 0}$，对$\forall i=1,\cdots,n$，$p_i$是$R$的素元$\}$.

$\therefore \exists n\in\mathbb{Z}_{\geq 1}$，$\exists R$的素元$p_1,p_2,\cdots,p_n$，s.t. $ab=p_1p_2\cdots p_n$

对$\forall i=1,\cdots,n$ $\because ab=p_1p_2\cdots p_n=(p_1\cdots p_{i-1}p_{i+1}\cdots p_n)p_i$ $\therefore p_i \mid ab$

$\therefore p_i\mid a$或$p_i\mid b$ $\because R$是交换环 $\therefore$可以交换$ab=p_1p_2\cdots p_n$中n个素元的顺序使前m个素元整除a，第$m+1$到n个素元整除b.

设$ab=p_1'\cdots p_m' p_{m+1}'\cdots p_n'$，其中$p_1',\cdots,p_n'$是$R$的素元.

$p_1'\mid a,\cdots,p_m'\mid a$，$p_{m+1}'\mid b,\cdots,p_n'\mid b$.