Lemma：R是环，I是R的理想，A是R的子环，则有：

$A \cap I$是环A的理想

Proof：$\because$ R是环 $\therefore (R, +, \cdot, 0_R, 1_R)$是环. $\because$ A是R的子环

$\therefore (A, +, \cdot, 0_R, 1_R)$是环 $\therefore A \cap I \subseteq A$

$\because$ I是R的理想 $\therefore 0_R \in I$ $\because$ A是R的子环 $\therefore 0_R \in A$ $\therefore 0_R \in A \cap I$

$\therefore A \cap I$是环A的非空子集.

对$\forall x, y \in A \cap I$，有：$\because x, y \in A$ $\therefore x+y \in A$ $\because x, y \in I$ $\therefore x+y \in I$

$\therefore x+y \in A \cap I$

对$\forall a \in A$，

任取$a(A \cap I)$中的一元：ax（其中$x \in A \cap I$）

$\because a \in A$，$x \in A$ $\therefore ax \in A$ $\because a \in A$，$x \in I$ $\therefore ax \in aI \subseteq I$

$\therefore ax \in A \cap I$ $\therefore a(A \cap I) \subseteq A \cap I$

任取$(A \cap I)a$中的一元：xa（其中$x \in A \cap I$）

$\because x \in A$，$a \in A$ $\therefore xa \in A$ $\because x \in I$，$a \in A$ $\therefore xa \in Ia \subseteq I$

$\therefore xa \in A \cap I$ $\therefore (A \cap I)a \subseteq A \cap I$

$\therefore A \cap I$是环A的理想. □

Lemma：R和R'是交换环，$f:R\to R'$是满同态，I是R的极大理想，$\ker(f)\subseteq I$，则有：$f(I)$是环R'的极大理想.

Proof：已知$f(I)$是环$f(R)$的极大理想

$\because f:R\to R'$是满同态 $\therefore f(R)=R'$

$\therefore f(I)$是环R'的极大理想. □

Lemma：R和R'是环，$f:R\to R'$是环同态，I是R'的理想，则有：

$$R/f^{-1}(I)\simeq f(R)/(f(R)\cap I)$$

Proof：$\because R$和R'是环，$f:R\to R'$是环同态，I是R'的理想

$\therefore f^{-1}(I)$是环R的理想 $\therefore R/f^{-1}(I)$是环.

$\because R$和R'是环，$f:R\to R'$是环同态 $\therefore f(R)$是环R'的子环. $\therefore f(R)$是环.

$\because R'$是环，I是R'的理想，$f(R)$是R'的子环 $\therefore f(R)\cap I$是环$f(R)$的理想

$\therefore f(R)/(f(R)\cap I)$是环.

定义映射 $\varphi:R\longrightarrow f(R)/(f(R)\cap I)$

$$x\longmapsto f(x)+f(R)\cap I$$

对$\forall x\in R$，$\because f:R\to R'$是环同态 $\therefore f(x)\in f(R)$

$\therefore \varphi(x)=f(x)+f(R)\cap I\in f(R)/(f(R)\cap I)$

对$\forall x_1,x_2\in R$，若$x_1=x_2$，则$f(x_1)=f(x_2)$

$\therefore \varphi(x_1)=f(x_1)+f(R)\cap I=f(x_2)+f(R)\cap I=\varphi(x_2)$

$\therefore \varphi:R\to f(R)/(f(R)\cap I)$是一个映射.

任取 $f(R)/(f(R)\cap I)$ 中的一元：$\lambda + f(R)\cap I$ （其中 $\lambda \in f(R)$）

$\because \lambda \in f(R)$ $\therefore \exists \mu \in R$, s.t. $\lambda = f(\mu)$

$\therefore \mu \in R$，且 $\varphi(\mu) = f(\mu) + f(R)\cap I = \lambda + f(R)\cap I$

$\therefore \varphi: R \to f(R)/(f(R)\cap I)$ 是一个满射.

对 $\forall x_1, x_2 \in R$，

$$\varphi(x_1+x_2) = f(x_1+x_2) + f(R)\cap I = (f(x_1)+f(x_2)) + f(R)\cap I$$

$$= (f(x_1) + f(R)\cap I) + (f(x_2) + f(R)\cap I) = \varphi(x_1) + \varphi(x_2)$$

$$\varphi(x_1 \cdot x_2) = f(x_1 \cdot x_2) + f(R)\cap I = f(x_1)\cdot f(x_2) + f(R)\cap I$$

$$= (f(x_1) + f(R)\cap I)\cdot (f(x_2) + f(R)\cap I) = \varphi(x_1)\cdot\varphi(x_2)$$

$$\varphi(1_R) = f(1_R) + f(R)\cap I = 1_{R'} + f(R)\cap I = 1_{f(R)} + f(R)\cap I$$

$$= 1_{f(R)/(f(R)\cap I)}$$

$\therefore \varphi: R \to f(R)/(f(R)\cap I)$ 是一个满同态.

$\therefore$ 由环的第一同构定理知：$R/\ker(\varphi) \simeq f(R)/(f(R)\cap I)$

已知 $\ker(\varphi) \subseteq R$，$f^{-1}(I) \subseteq R$.

对 $\forall x \in f^{-1}(I)$，有：$x \in R$，且 $f(x) \in I$ $\because x \in R$ $\therefore f(x) \in f(R)$

$\therefore f(x) \in f(R)\cap I$ $\therefore f(x) + f(R)\cap I = 0_{f(R)/(f(R)\cap I)}$

$\therefore \varphi(x) = 0_{f(R)/(f(R)\cap I)}$ $\therefore x \in \ker(\varphi)$ $\therefore f^{-1}(I) \subseteq \ker(\varphi)$

对 $\forall x \in \ker(\varphi)$，有：$x \in R$ 且 $\varphi(x) = 0_{f(R)/(f(R)\cap I)}$

$\therefore f(x) + f(R)\cap I = 0_{f(R)/(f(R)\cap I)}$ $\because x \in R$ $\therefore f(x) \in f(R)$ $\therefore f(x) \in f(R)\cap I$

$\therefore f(x)\in I$ $\therefore x\in f^{-1}(I)$ $\therefore \ker(\varphi)\subseteq f^{-1}(I)$ $\therefore \ker(\varphi)=f^{-1}(I)$

$\therefore R/f^{-1}(I)\simeq f(R)/(f(R)\cap I)$ □

Remark: $\because R'$是环，$f(R)$是R'的子环，I是R'的理想

$\therefore$由环的第二同构定理知：$f(R)/(f(R)\cap I)\simeq (f(R)+I)/I$

$\therefore R/f^{-1}(I)\simeq (f(R)+I)/I$

$\because f(R)+I$是R'的子环 $\therefore (f(R)+I)/I\subseteq R'/I$

$\therefore (f(R)+I)/I$是R'/I的子环. 看

$\therefore R/f^{-1}(I)\simeq (f(R)+I)/I$ 且 $(f(R)+I)/I$是R'/I的子环. □

Lemma：R和R'是交换环，$f:R\to R'$是环同态，I是R'的素理想，则有：$f^{-1}(I)$是R的素理想.

Proof: $\because R$和R'是环，$f:R\to R'$是环同态，I是R'的理想

$\therefore R/f^{-1}(I)\simeq (f(R)+I)/I$ 且 $(f(R)+I)/I$是R'/I的子环.

$\because R'$是交换环，I是R'的素理想 $\therefore R'/I$是整环

$\therefore (f(R)+I)/I$是整环 $\therefore R/f^{-1}(I)$是整环

$\because$ 看 $f^{-1}(I)$是R的理想. $\therefore f^{-1}(I)$是R的素理想 □

Lemma：R和R'是交换环，$f:R\to R'$是满同态，I是R'的极大理想，则有：$f^{-1}(I)$是R的极大理想.

Proof: $\because f:R\to R'$是满同态 $\therefore f(R)=R'$ $\therefore f(R)+I=R'+I$

任取$R'+I$中的一元：$a+b$ (其中$a\in R'$且$b\in I$) $\because a\in R', b\in I\subseteq R'$

$\therefore a+b\in R'$ $\therefore R'+I\subseteq R'$

对$\forall a\in R'$，有：$a=a+0_R\in R'+I$ $\therefore R'\subseteq R'+I$ $\therefore R'+I=R'$

$\therefore f(R)+I=R'$ $\therefore R/f^{-1}(I)\simeq R'/I$

$\because R'$是交换环，I是R'的极大理想 $\therefore R'/I$是域.

$\therefore R/f^{-1}(I)$是域.

$\because f^{-1}(I)$是R的理想 $\therefore f^{-1}(I)$是R的极大理想. □

定义（Euclid环）R是整环，若存在良序集L和函数$N:R\setminus\{0_R\}\to L$，使得对$\forall x\in R$，$\forall d\in R\setminus\{0_R\}$都存在$q\in R$使$r:=x-qd$满足$r=0_R$或（$r\neq 0_R$且$N(r)<N(d)$），则称$R$是Euclid环.

Lemma：Euclid环必是主理想环.

Proof：设R是Euclid环.

$\because R$是Euclid环 $\therefore R$是整环. 设I是R的一个任意的理想.

若$I=\{0_R\}$，则有：R是交换环，$0_R\in R$，

$(0_R)=0_R R=\{0_R\cdot r:r\in R\}=\{0_R\}=I$ $\therefore I$是0_R确定的主理想.

若$I\neq\{0_R\}$，则有：$\because I$是R的理想 $\therefore 0_R\in I$ $\therefore\{0_R\}\subseteq I$

$\because I\neq\{0_R\}$ $\therefore\{0_R\}\subsetneq I$

考虑集合$S=\{N(a)\mid a\in I\text{且}a\neq 0_R\}\subseteq L$

$\because\{0_R\}\subsetneq I$ $\therefore\exists a\in I$, s.t. $a\neq 0_R$ $\because a\in I\subseteq R$且$a\neq 0_R$

$\therefore a\in R\setminus\{0_R\}$ $\therefore N(a)\in L$ $\because N(a)\in S$ $\therefore S\neq\emptyset$.

$\therefore S$是L的非空子集.

∵ L 是良序集，S 是 L 的非空子集 ∴ S 有极小元 λ ∴ $\lambda \in S$

∴ $\exists d \in I$ 且 $d \neq 0_R$，s.t. $\lambda = N(d)$ ∵ R 是交换环，$d \in R$.

任取 (d) 中的一元：$d\alpha$ （其中 $\alpha \in R$）

∵ $\alpha \in R$，$d \in I$，I 是 R 的理想 ∴ $d\alpha \in I\alpha \subseteq I$ ∴ $(d) \subseteq I$

对 $\forall x \in I$，有：$x \in R$. ∵ $x \in R$，$d \in R \setminus \{0_R\}$，$R$ 是 Euclid 环

∴ $\exists q \in R$ 使 $r := x - qd$ 满足 $r = 0_R$ 或 $(r \neq 0_R$ 且 $N(r) < N(d))$

∵ $qd \in qI \subseteq I$ ∴ $-qd \in I$ ∵ $x \in I$

∴ $r = x - qd = x + (-qd) \in I$ ∴ $r \in R$

假设 $r \neq 0_R$，则有：$r \neq 0_R$ 且 $N(r) < N(d)$ ∴ $N(r) < \lambda$

∵ $r \in I$ 且 $r \neq 0_R$ ∴ $N(r) \in S$. ∵ λ 是 S 的极小元 ∴ $N(r) \geqslant \lambda$

∴ $\lambda \leqslant N(r) < \lambda$ 矛盾. ∴ $r = 0_R$

∴ $x - qd = 0_R$

∴ $x = x + 0_R = x + \big((-qd) + qd\big) = \big(x + (-qd)\big) + qd$

$= (x - qd) + qd = 0_R + qd = qd = dq \in (d)$ ∴ $I \subseteq (d)$

∴ $I = (d)$ ∴ I 是 d 确定的主理想.

∴ I 是主理想. ∴ R 是主理想环. □

定理（多项式环的算术基本定理）F 是域，则 $F[X]$ 是唯一分解环.

Proof: ∵ F 是域 ∴ F 是非零环 ∵ F 是域 ∴ F 是整环

∴ $F[X]$ 是整环.

定义 $L = \{-\infty\} \cup \mathbb{Z}_{\geqslant 0}$ （其实取 $L = \mathbb{Z}_{\geqslant 0}$ 即可）.

定义 L 上的序关系如下：对 $\forall a, b \in L$，若 $a = -\infty$，则 $a \leq b$ 恒成立.

若 $b = -\infty$，则 $a \leq b \Leftrightarrow a = -\infty$.

若 $a, b \in \mathbb{Z}_{\geq 0}$，则 $a \leq b$ 按通常的非负整数的序关系理解

L 上的序关系 $\leq$ 满足反身性，传递性，反称性，且 L 中任意两个元素皆可比较大小. $\therefore (L, \leq)$ 是全序集.

L 的任意非空子集 S 都有极小元（若 $-\infty \in S$，则 $-\infty$ 是 S 的极小元.

若 $-\infty \notin S$，则 $S \subseteq \mathbb{Z}_{\geq 0}$，$\because \mathbb{Z}_{\geq 0}$ 是良序集 $\therefore S$ 有极小元）

$\therefore (L, \leq)$ 是良序集.

$deg: F[X] \setminus \{0_{F[X]}\} \to L$ 是函数.

对 $\forall x \in F[X]$，$\forall d \in F[X] \setminus \{0_{F[X]}\}$，$\exists q \in F[X]$，$r = x - dq \in F[X]$

s.t. $deg(r) < deg(d)$

$\therefore F[X]$ 是 Euclid 环.

$\therefore F[X]$ 是主理想环.

$\therefore F[X]$ 是唯一分解环. □