Let X be an algebraic variety smooth at a point $a \in X$ and let $\phi_1,...,\phi_n$ be local parameters at a. We have seen that every element f of the local ring $\mathcal{O}_a$ has unique Taylor series expansion in terms of $\phi_1, ..., \phi_n$, i.e. there are unique homogeneous polynomials $F_i(x_1, ..., x_n)$, $i = 0, 1, 2, ...$ such that F_i has degree i and $f - \sum_{i=0}^{N} F_i(\phi_1, ..., \phi_n) \in \mathfrak{m}_a^{N+1}$ for all integers $N \geq 0$. The assignment $f \mapsto \sum_{i=0}^{\infty} F_i(x_1, ..., x_n)$ defines a homomorphism $\Psi : \mathcal{O}_a \longrightarrow R_n$, where $R_n = k[[x_1, ..., x_n]]$ is the power series ring in n-variables over k. By the definition of the Taylor series expansion, $\ker \Psi = \bigcap_{i=1}^{\infty} \mathfrak{m}^i$. Our goal now is to show that $\ker \Psi = \{0\}$. We will see that it is a consequence of a more general and important result about Noetherian rings.

Lemma 1. *Let R be a commutative Noetherian ring and let I, J be ideals of R. For any $b \in J$ there is a positive integer N such that $I \cap b^N J \subseteq IJ$.*

Proof: Suppose that the result is false and let $b \in J$ be such that for every positive integer n there is $j_n \in J$ such that $b^n j_n \in I - IJ$. Since R is Noetherian, the ideal $< j_1, j_2, j_3, ... >$ is generated by $j_1, j_2, ..., j_{N-1}$ for some N. Thus $j_N = \sum_{k=1}^{N-1} r_k j_k$ for some $r_k \in R$. It follows that

$$b^N j_N = b \sum_{k=1}^{N-1} b^{N-1-k}(b^k j_k).$$

Each summand of the sum on the right belongs to I so the whole sum is an element of I and since $b \in J$, we see that the right hand side belongs to IJ. This contradicts the assumption that the left hand side is not in IJ. □

Theorem 1. *Let R be a commutative Noetherian ring and let I, J be ideals of R. There is a positive integer K such that $I \cap J^K \subseteq IJ$.*

Proof: Suppose that the theorem is false for R and an ideal J and let I be maximal among the ideals of R such that $I \cap J^n \nsubseteq IJ$ for all n (such I exists since R is Noetherian). Let $b \in J$ and let N be such that $I \cap b^N J \subseteq IJ$ (which exists by Lemma 1). We claim that $b^N \in I$. Indeed, suppose that b^N is not in I. Then the ideal $I + b^N R$ properly contains I, so by the definition of I there is an integer M such that $(I + b^N R) \cap J^M \subseteq (I + b^N R)J = IJ + b^N J$. Thus

$$I \cap J^M = I \cap (I + b^N R) \cap J^M \subseteq I \cap (IJ + b^N J) = IJ + (I \cap b^N J) \subseteq IJ$$

(since $I \cap b^N J \subseteq IJ$), a contradiction.

We showed therefore that for each $b \in J$ there is N such that $b^N \in I$. Let $J =< b_1, ..., b_t >$. Then we can find N such that $b_i^N \in I$ for $i = 1, 2, ..., t$. It follows that $J^{Nt} \subseteq I$ and therefore $I \cap J^{Nt+1} = J^{Nt+1} = J^{Nt} J \subseteq IJ$, a contradiction. □

As a simple corollary we get the following important result.

Theorem 2. (Krull's Intersection Theorem) *Let R be a local Noetherian ring with maximal ideal $\mathfrak{m}$. For any ideal T of R we have $\bigcap_{k=1}^{\infty}(T + \mathfrak{m}^k) = T$.*

Proof: Replacing R by R/T we reduce to the case when $T = \{0\}$. Now take $I = \bigcap_{k=1}^{\infty} \mathfrak{m}^k$, $J = \mathfrak{m}$ in Theorem 1. Then for some K we have $I = I \cap J^K \subseteq IJ$. Thus $I = \mathfrak{m}I$ and therefore $I = 0$ by Nakayama's Lemma. □

An immediate consequence of the last theorem is the vanishing of $\ker \Psi$. Thus $\mathcal{O}_a$ can be considered as a subring of R_n (note however, that this depends on the choice of local parameters). In particular, $\mathcal{O}_a$ is a domain. Thus

Theorem 3. *If a variety X is smooth at a then $\mathcal{O}_a$ is a domain and therefore only one irreducible component of X contains a.*

We proved that R_n is a UFD. We will now show that $\mathcal{O}_a$ is a UFD. To start, let us make some basic observations about the way $\mathcal{O}_a$ is embedded in R_n. We will write R for $\mathcal{O}_a$ and $\hat{R}$ for R_n. Furthermore, $\mathfrak{m}$ and $\hat{\mathfrak{m}}$ denote the maximal ideals of R, $\hat{R}$ respectively. Note that

(1) $\hat{\mathfrak{m}}^j \cap R = \mathfrak{m}^j$ for $j = 1, 2, ...$;

(2) for any integer $j > 0$ and any $x \in \hat{R}$ there is $r \in R$ such that $x - r \in \hat{\mathfrak{m}}^j$.

Note that (1) and (2) together are equivalent to saying that $\mathfrak{m} \subseteq \hat{\mathfrak{m}}$ and for every j the natural homomorphism $R/\mathfrak{m}^j \longrightarrow \hat{R}/\hat{\mathfrak{m}}^j$ is an isomorphism. To justify (1) observe that elements in $\mathfrak{m}^j$ are exactly those elements of R whose Taylor series have no terms of degree $< j$, i.e. belong to $\hat{\mathfrak{m}}^j$. For (2) note that if $x = \sum_{i=0}^{\infty} F_i(x_1, ..., x_n)$ (F_i homogeneous of degree i), then the image of $r = \sum_{i=0}^{j-1} F_i(\phi_1, ..., \phi_n) \in R$ in $\hat{R}$ is $\sum_{i=0}^{j-1} F_i(x_1, ..., x_n)$ so $x - r = \sum_{i=j}^{\infty} F_i(x_1, ..., x_n) \in \hat{\mathfrak{m}}^j$.

From now on we are going to assume that $R \subseteq \hat{R}$ are local rings which satisfy (1) and (2) and such that R is Noetherian and $\hat{R}$ is a UFD. Our goal is to prove that then R is a UFD too.

(A) *For any ideal I of R we have $I\hat{R} \cap R = I$.*

In fact, let $x \in I\hat{R} \cap R$ so $x = \sum_{i=1}^{m} a_i x_i$ with $a_i \in I$ and $x_i \in \hat{R}$. For a given integer $l > 0$ there are $r_i \in R$ such that $x_i - r_i = m_i \in \hat{\mathfrak{m}}^l$. Thus $x = \sum_{i=1}^{m} a_i r_i + \sum_{i=1}^{m} a_i m_i$. Clearly $\sum_{i=1}^{m} a_i r_i \in I$ and therefore $\sum_{i=1}^{m} a_i m_i \in R \cap \hat{\mathfrak{m}}^l = \mathfrak{m}^l$. In other words, $x \in I + \hat{\mathfrak{m}}^l$. Since l was arbitrary, we have $I\hat{R} \cap R \subseteq \bigcap_{k=1}^{\infty}(I + \mathfrak{m}^k) = I$ (by Krull's intersection). The reversed inclusion $I \subseteq I\hat{R} \cap R$ is obvious. □

(B) *If $a, b \in R$ and $b = ac$ for some $c \in \hat{R}$ then $c \in R$.*

Indeed, we have $b \in a\hat{R} \cap R$. Since $a\hat{R} \cap R = aR$ by (A), we see that $b = ac'$ for some $c' \in R$ and therefore $c = c'$ (since $\hat{R}$ is a domain).

(C) *If $a, b \in R - \{0\}$ and x is a greatest common divisor of a, b in $\hat{R}$ then $xu \in R$ for some u invertible in $\hat{R}$.*

This is the key observation. To justify it write $a = x\alpha$, $b = x\beta$, where $\alpha, \beta \in \hat{R}$ are relatively prime. Thus $a\beta = b\alpha$. There are integers i, j such that $\alpha \notin \hat{\mathfrak{m}}^i$ and $\beta \notin \hat{\mathfrak{m}}^j$ (since we are not assuming that $\hat{R}$ is Noetherian, this requires justification: if we had $\alpha \in \hat{\mathfrak{m}}^s$ for every s then also $a \in \hat{\mathfrak{m}}^s$ for every s, i.e. $a \in \hat{\mathfrak{m}}^s \cap R = \mathfrak{m}^s$. Now R is Noetherian, so $a = 0$ by Krull's intersection, a contradiction.). Let N be an integer larger than both i, j. By Theorem 1, there is $M > 0$ such that $(a, b) \cap \mathfrak{m}^{MN} \subseteq (a, b)\mathfrak{m}^N$. By (2), we may write $\alpha = a' + r$, $\beta = b' + s$, where $a', b' \in R$ and $r, s \in \hat{\mathfrak{m}}^{MN}$. Thus $ab' - ba' = br - as$. Note that the left hand side of this equality is in (a, b) and the right hand side belongs to $\hat{\mathfrak{m}}^{MN} \cap R = \mathfrak{m}^{MN}$. Thus both sides belong to $(a, b) \cap \mathfrak{m}^{MN}$, hence also to $(a, b)\mathfrak{m}^N$. Consequently, there are $e, f \in \mathfrak{m}^N$ such that $ab' - ba' = ae - bf$, i.e. $a(b' - e) = b(a' - f)$. Dividing this equality by x we get $\alpha(b' - e) = \beta(a' - f)$. Since α and β are relatively prime, we have $(a' - f) = \alpha v$ for some $v \in \hat{R}$. Recall now that $a' = \alpha - r$

so $\alpha(1-v) = f + r$. Note that $f, r \in \hat{\mathfrak{m}}^N$ and $\alpha \notin \hat{\mathfrak{m}}^N$ (since $N > i$). Thus $(1-v)$ is not invertible in $\hat{R}$, i.e. it belongs to $\hat{\mathfrak{m}}$. Equivalently, $v \notin \hat{\mathfrak{m}}$, i.e. v is invertible in $\hat{R}$. Let $u = v^{-1}$. Then $a = x\alpha = (ux)(v\alpha) = (ux)(a' - f)$. Since a and $a' - f$ are in R, also $ux \in R$ by (B).

(D) *If p is irreducible in R then it is prime.*

In fact, suppose that $p|ab$ in R. Since p is not a unit in R, we have $p \in \mathfrak{m} \subseteq \hat{\mathfrak{m}}$ and therefore p is not a unit in $\hat{R}$. There is q irreducible in $\hat{R}$ such that $q|p$ in $\hat{R}$. Thus in $\hat{R}$ we have $q|ab$ and therefore $q|a$ or $q|b$. Without loss of generality we may assume that $q|a$. Thus p and a are not relatively prime in $\hat{R}$. By (C), there is $d \in R$ which is a greatest common divisor of p and a in $\hat{R}$. But p is irreducible in R, so p/d is invertible and therefore $p|a$ in R.

We showed that irreducible elements in R are prime and since R is Noetherian this implies that R is UFD.