NÉRON-POPESCU DESINGULARIZATION

RICHARD G. SWAN

The University of Chicago

ABSTRACT. This is a purely expository paper giving a detailed presentation of D. Popescu's proof that a regular morphism of noetherian rings is a filtered colimit of smooth morphisms. Applications to Artin approximation and the Bass-Quillen conjecture are included. Comments, corrections, and improvements are welcome as always.

INTRODUCTION

The following consists of an expanded version of notes on a series of lectures which I gave at the University of Chicago in the Spring of 1995 on D. Popescu's General Néron Desingularization. I am distributing these notes in the hope of dispelling any lingering doubts about the correctness of Popescu's proof and also in the hope of making Popescu's proof accessible to a wider audience. To this end I have included a considerable amount of background material, assuming only standard commutative algebra. The few results needed from the André-Quillen cohomology theory are developed ab ovo following [EGA IV]. I have also avoided any use of the theory of formal smoothness, making use of an argument of Faltings [F] to give a simple proof of the only fact needed from this theory.

The main outline of the proof follows closely Popescu's paper [Pl]. I also have made considerable use of André's notes [A5] and Ogoma's paper [O] in working out many of the technical details.

I would like to thank M. P. Murthy for many useful discussions of this material.

PART I. STATEMENT OF RESULTS

1. Popescu's Theorem. We begin by recalling some standard definitions and facts. The following property is usually referred to as formal smoothness. I have changed the terminology to 'quasi-smoothness' to avoid any confusion with the topological notion of formal smoothness used in [EGA IV]. All rings considered in these notes will be commutative with unit.

Definition. A ring homomorphism $f : R \to A$ (i.e. an R-algebra) is called quasi-smooth if for any R-algebra B and ideal $I \subset B$ with $I^2 = 0$, any R-algebra homomorphism $g : A \to B/I$ lifts to an R-algebra homomorphism $h : A \to B$. If moreover any such lifting is unique, then f is called quasi-étale.

1991 *Mathematics Subject Classification.* Primary 13H05; Secondary 14B12.

Key words and phrases. Néron desingularization, Artin approximation, Bass-Quillen conjecture.

Partly supported by the NSF.

We say that A is smooth over R if it is finitely presented and quasi-smooth. Similarly A is étale over R if it is finitely presented and quasi-étale.

We say that A is essentially smooth over R if it is essentially finitely presented (i.e. a localization of a finitely presented R-algebra) and quasi-smooth. Similarly A is essentially étale over R if it is essentially finitely presented and quasi-étale.

Examples.

(1) If $A \xrightarrow{f} B \xrightarrow{g} C$ and f and g are quasi-smooth (resp. quasi-étale) so is gf.
(2) If $A \xrightarrow{f} B$ is quasi-smooth (resp. quasi-étale) so is $C \xrightarrow{f} C \otimes_A B$ for any $A \to C$.
(3) A polynomial extension $R \to R[x_1, \dots, x_n]$ is smooth.
(4) A localization $R \to R_S$ is essentially étale (and étale if S is generated by one element).
(5) If f is a monic polynomial in one variable then $R \to (R[X]/(f))_{f'}$ is étale. More generally, if $f_1, ..., f_n \in R[X_1, ..., X_n]$ and $\Delta = \det|\partial f_i/\partial X_j|$ then $R \to (R[X_1, ..., X_n]/(f_1, ..., f_n))_\Delta$ is étale.

To prove (5) note that if $g(X_i) = \bar{b}_i$ lifts to b_i, then $f_i(b) \in I$ and we must send X_i to $b_i + \epsilon_i$ with $\epsilon_i \in I$ such that $f_i(b+\epsilon) = f_i(b) + \sum \partial f_i/\partial X_j(b)\epsilon_j = 0$. Since Δ maps to a unit, these equations have a unique solution.

Conversely, Grothendieck [SGA1] has shown that any étale R-algebra looks locally like $(R[Y]/f)_{f'}$ and any smooth R-algebra looks locally like $(R[X_1, \dots, X_n, Y]/f)_{\partial f/\partial Y}$ where f is monic in Y. More precisely if A is a smooth R-algebra, then $A = \sum A s_i$ where A_{s_i} is isomorphic to a localization of $(R[X_1, \dots, X_n, Y]/f)_{\partial f/\partial Y}$ (where n and f depend on i). We will only need the local case of this result here. See Theorem 2.5.

It is clear from this that a smooth R-algebra is flat and it is also easy to check the well-known fact that a smooth algebra over a field is regular. The converse is not true in general.

Definition. A local ring R containing a field k is called geometrically regular over k if $k' \otimes_k R$ is regular for any finite field extension k'/k with $k'^p \subset k$ where p is the characteristic of k. (In characteristic 0 this just means that R is regular.)

It is well known that this implies the regularity of $k' \otimes_k R$ for any finite field extension k'/k. We will not prove this here since it follows from Popescu's theorem 1.1.

If R is essentially of finite type over a field k, it is well-known that R is geometrically regular over k if and only if R is essentially smooth over k. We will not need this fact here.

Remark. If R is essentially of finite type over a field k, then R is geometrically regular over k if and only if $\bar{k} \otimes_k R$ is regular where $\bar{k}$ is the algebraic closure of k. This is not true in the general case. For example, $\bar{Q}$ is clearly geometrically regular over Q but $\bar{Q} \otimes_Q \bar{Q}$ is not regular since it is not noetherian.

Definition. A ring homomorphism $f : R \to A$ is called geometrically regular if it is flat and its fibers are geometrically regular i.e. for each prime ideal P of R, and for each prime ideal Q of A lying over P, $A_Q/PA_Q = k(P) \otimes_R A_Q$ is geometrically regular over $k(P) = R_P/P_P$.

It is customary to just say that f is regular in this case. I have inserted the extra word 'geometrically' to avoid any possible confusion when R is a field.

We can now state Popescu's theorem.

Theorem 1.1. (D. Popescu) *Let $f : R \to \Lambda$ be a homomorphism of noetherian rings. Then f is geometrically regular if and only if Λ is a filtered colimit of smooth R-algebras.*

Note that these smooth R-algebras are not assumed to be subalgebras of Λ.

Corollary 1.2. *If $R \to \Lambda$ is a geometrically regular homomorphism of noetherian rings, and if $R \to A \to \Lambda$ with A of finite type over R, then we can find $R \to A \to B \to \Lambda$ where B is smooth over R.*

I will say that $R \to A \to \Lambda$ can be desingularized if the conclusion of Corollary 1.2 holds for it.

Corollary 1.3. *If $R \to \Lambda$ is a geometrically regular homomorphism of noetherian local rings, then Λ is a filtered colimit of essentially smooth local R-algebras.*

In fact if $\Lambda = \operatorname{colim} A_\alpha, P$ is a prime ideal of Λ, and P_α is its image in $\operatorname{Spec} A_\alpha$, then $\Lambda_P = \operatorname{colim} A_{\alpha P_\alpha}$.

The 'only if' part of Theorem 1.1 is an immediate consequence of André's cohomological criterion for regularity [Ah] but as Popescu observes [Pa], one can give a very simple proof. Suppose $\Lambda = \operatorname{colim} A_\alpha$ where the A_α are smooth over R. Then Λ is flat as a filtered colimit of flat R-algebras. If P is a prime ideal of R and $k/k(P)$ is a finite field extension, then $k \otimes_R \Lambda = \operatorname{colim} k \otimes_R A_\alpha$. Therefore it is enough to prove the following lemma.

Lemma 1.4. *If a noetherian ring B is a filtered colimit of regular rings then B is regular.*

Proof. Let $B = \operatorname{colim} A_\alpha$. By the proof of Corollary 1.3, it is enough to do the case where B and the A_α are local. If $\mathfrak{m}$ is the maximal ideal of B and $k = B/\mathfrak{m}$, there is a natural map of the symmetric algebra $S_k(\mathfrak{m}/\mathfrak{m}^2)$ to $\operatorname{gr} B = \bigoplus \mathfrak{m}^n/\mathfrak{m}^{n+1}$ and B is regular if and only if this map is an isomorphism. In one direction this is well known. For the converse, note that $\sum_0^n \operatorname{length} \operatorname{gr}_i B = \operatorname{length}(B/\mathfrak{m}^n)$ is, for large n, a polynomial in n of degree $\dim B$ while the corresponding polynomial for $S_k(\mathfrak{m}/\mathfrak{m}^2)$ has degree equal to $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$. Since S_k and gr preserve filtered colimits, we see that B has the required property if the A_α do.

It is also easy to see that the properties considered in Theorem 1.1 and Corollary 1.2 are equivalent. This follows from the following simple fact of universal algebra.

Lemma 1.5. *Let $\mathcal{S}$ be a class of finitely presented R-algebras. Let Λ be any R-algebra. Then the following statements are equivalent.*

1. *Λ is a filtered colimit of algebras in $\mathcal{S}$.*
2. *If A is a finitely presented R-algebra and $f : A \to \Lambda$ is an R-algebra homomorphism, then f factors through some B in $\mathcal{S}$.*

Proof. Suppose $\Lambda = \operatorname{colim} B_\alpha$ and $A = R[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Let x_i map to λ_i so that $f_j(\lambda) = 0$. For some α we can find preimages b_i of the λ_i in B_α. Since the $f_j(b)$ map to 0 in Λ, for some $\beta \geq \alpha$ the $f_j(b)$ map to 0 in B_β and therefore $A \to \Lambda$ factors through B_β.

Conversely, suppose that (2) holds. Let $\mathcal{C}$ be the category whose objects are R-algebra homomorphisms $f : A \to \Lambda$ with A in $\mathcal{S}$, a morphism being a map $A \to B$ such that

$$\begin{tikzcd} A \arrow[r] \arrow[d] & \Lambda \arrow[d, equal] \\ B \arrow[r] & \Lambda \end{tikzcd}$$

commutes i.e. we have $A \to B \to \Lambda$. This category is filtered: If we have two maps $f, g : A \rightrightarrows B$ let $a_1 \dots, a_n$ generate A and let $C = B/I$ where I is the ideal generated by all $f(a_i) - g(a_i)$. Then C is finitely presented, $B \to \Lambda$ factors through C, and $B \to C$ equalizes f and g. By (2), $C \to \Lambda$ factors through some D in $\mathcal{S}$ and $B \to D$ equalizes f and g. If $f : A \to \Lambda$ and $g : B \to \Lambda$ are two objects, both map through $A \otimes_R B \to \Lambda$. Since $A \otimes_R B$ is finitely presented, the map $A \otimes_R B \to \Lambda$ factors through some C in $\mathcal{S}$ and f and g map to $C \to \Lambda$. We clearly have a map $\operatorname{colim}_{\mathcal{C}} A \to \Lambda$. It is onto since any λ can be the image of X in $R[X] \to \Lambda$ and we can apply (2) to this map. It is injective since if $x, y \in A$ have the same image in Λ, then, by (2), we can find $A \to A/(x - y) \to B \to \Lambda$ with $B \to \Lambda$ in $\mathcal{C}$ and x and y have the same image in B.

2. Applications.

One important application of Popescu's theorem is to the Bass-Quillen conjecture. The following theorem was proved by Lindel [L] for geometric local rings (those essentially of finite type over a field).

Theorem 2.1. ([Pp]) *Let R be a regular local ring containing a field. Then all projective modules over a polynomial ring $R[T_1, \dots, T_n]$ are free.*

Proof. Let $\mathbb{F}$ be the prime field contained in R. Since $\mathbb{F}$ is perfect, R is geometrically regular over $\mathbb{F}$ and therefore, by Corollary 1.3, R is a filtered colimit of essentially smooth local $\mathbb{F}$-algebras A_α. A projective module P over $R[T_1, \dots, T_n]$ can be described as the image of an idempotent matrix E over this ring. Since $R[T_1, \dots, T_n]$ is the filtered colimit of the rings $A_\alpha[T_1, \dots, T_n]$, we can lift E to an idempotent matrix E' over one of these rings. The image Q of E' is a projective module inducing P. But Q is free by Lindel's theorem.

If R is a regular local ring of characteristic 0 whose residue field k is of characteristic $p \neq 0$, we say that R is unramified if p is a regular parameter for R. This implies that R is geometrically regular over $\mathbb{Z}_{(p)}$ since $\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} R = R/pR$ is regular. An easy modification of Lindel's argument (see [Pp]) shows that the Bass-Quillen conjecture is true for unramified regular local rings essentially of finite type over $\mathbb{Z}_{(p)}$. We can now apply the same argument to this case.

Theorem 2.2. ([Pp]) *Let R be an unramified regular local ring. Then all projective modules over a polynomial ring $R[T_1, \dots, T_n]$ are free.*

The following theorem which answers affirmatively a special case of a conjecture of Quillen was proved by Bhatwadekar and Rao [BR] for geometric local rings.

Theorem 2.3. ([Pq]) *Let R be a regular local ring containing a field and with maximal ideal $\mathfrak{m}$. Let f be an element of $\mathfrak{m} - \mathfrak{m}^2$. Then all projective modules over the ring R_f are free.*

This follows from the result of Bhatwadekar and Rao by the argument used for Theorem 2.1 [Pq]. Some cases are also known for the unramified regular local case [T].

Another very important application of Popescu's theorem is to prove the most general form of the Artin approximation theorem. The following theorem was proved by Artin [Aa] for the case in which R is the henselization of a local ring essentially of finite type over an excellent discrete valuation ring. It had long been conjectured to hold in the following generality.

Theorem 2.4. *Let R be an excellent henselian local ring. Let $f_i(x_1, \ldots, x_n) = 0$ be a finite system of polynomial equations over R. If these equations have a solution in the completion $\hat{R}$, then they have a solution in R.*

Proof. The only fact about excellent rings needed is that $R \to \hat{R}$ is geometrically regular. Since R is henselian, if $f(Y)$ is a monic polynomial over R and $\alpha \in k = R/\mathfrak{m}$ satisfies $f(\alpha) = 0$ and $f'(\alpha) \neq 0$, then α lifts to an element $a \in R$ with $f(a) = 0$. To prove the theorem, let $A = R[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Then a solution of the equations in $\hat{R}$ is just an R-algebra homomorphism $A \to \hat{R}$. By Corollary 1.2 we can find a smooth R-algebra B with $R \to A \to B \to \hat{R}$. Let C be the localization of B at the prime ideal which is the image of the maximal ideal of $\hat{R}$. Then C is essentially smooth over R and we apply the following local version of the theorem of Grothendieck recalled in §1. A proof will be given in §10.

Theorem 2.5. (Grothendieck [SGA1]) *If C is a local R-algebra essentially smooth over R, then $C = (R[T_1, \ldots, T_n, Y]/(f(T, Y)))_P$ where f is monic in Y and $\partial f/\partial Y \notin P$.*

Proof of Theorem 2.4. Since A is of finite type over R, we can find an element g in $R[T_1, \ldots, T_n, Y]/(f(T, Y))$ such that g has the form $h\partial f/\partial Y$ and such that the map $A \to C$ factors through $D = (R[T_1, \ldots, T_n, Y]/(f(T, Y)))_g$. The map $D \to \hat{R}$ is given by $T_i \mapsto a_i$ and $Y \mapsto b$ where $f_j(a, b) = 0$ and $g(a, b)$ has non-zero image in $k = \hat{R}/\hat{\mathfrak{m}}$. Approximate a_i and b by elements a_i' and b' in R having the same image in k and such that the image of $g(a', b')$ is still non-zero in k. The monic polynomial $q(Y) = f(a', Y)$ has a root $\bar{b} = \bar{b}'$ in k with $q'(\bar{b}) \neq 0$ since $q'(Y) = \partial f/\partial Y(a', Y)$ divides $g(a', Y)$. Since R is henselian, we can find b'' in R with $f(a', b'') = 0$ and with $\bar{b}'' = \bar{b}$. The image of $g(a', b'')$ in k is non-zero so sending D to R by $T_i \mapsto a_i'$ and $Y \mapsto b''$ now gives the required map $A \to D \to R$.

PART II. BACKGROUND MATERIAL

3. Low dimensional cohomology. We give here a direct definition of two invariants which agree with the André-Quillen cohomology groups [Ah] [Q] in dimension 0 and 1. Let $R \to A$ be an R-algebra and choose a presentation $A = R[X]/I$ where X is a set of indeterminates (not necessarily finite). Let $\bigoplus A dx_i$ be the free A-module on a base dx_i in 1–1 correspondence with $X = \{x_i\}$ (so $\bigoplus A dx_i = A \otimes_{R[X]} \Omega_{R[X]/R}$). Define $d : I \to \bigoplus A dx_i$ by sending f to $\sum \partial f/\partial x_i dx_i$. Then $d(I^2) = 0$ so we get a map $d : I/I^2 \to \bigoplus A dx_i$.

Definition. Let $\Gamma_{A/R}$ and $\Omega_{A/R}$ be the kernel and cokernel of $d : I/I^2 \to \bigoplus A dx_i$.

Therefore we have $0 \to \Gamma_{A/R} \to I/I^2 \xrightarrow{d} \bigoplus A dx_i \to \Omega_{A/R} \to 0$.

Remark. In terms of André-Quillen homology we have $\Omega_{A/R} = H_0(R, A, A)$ and $\Gamma_{A/R} = H_1(R, A, A)$. Of course, $\Omega_{A/R}$ is just the usual module of Kähler differentials.

Lemma 3.1. *$\Omega_{A/R}$ and $\Gamma_{A/R}$ are independent of the choice of the presentation (up to a canonical isomorphism) and are functorial in A/R.*

Proof. Suppose we have a commutative diagram of ring homomorphisms

$$\begin{tikzcd} R \arrow[r] \arrow[d] & A \arrow[d, "f"] \\ S \arrow[r] & B \end{tikzcd}$$

We construct natural maps $\Gamma_{A/R} \to \Gamma_{B/S}$ and $\Omega_{A/R} \to \Omega_{B/S}$ as follows. Let $A = R[X]/I$ and $B = S[Y]/J$. Lift f to $\varphi : R[X] \to S[Y]$ with $\varphi(x_i) = g_i(y)$. Let $d\varphi : \bigoplus Adx_i \to \bigoplus Bdy_i$ by sending dx_i to $\sum \partial g_i/\partial y_j dy_j$. Then we get a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \Gamma_{A/R} \arrow[r] \arrow[d] & I/I^2 \arrow[r, "d_A"] \arrow[d, "\bar{\varphi}"'] & \bigoplus Adx_i \arrow[r] \arrow[d, "d\varphi"'] & \Omega_{A/R} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Gamma_{B/S} \arrow[r] & J/J^2 \arrow[r, "d_B"] & \bigoplus Bdy_j \arrow[r] & \Omega_{B/S} \arrow[r] & 0.
\end{tikzcd}$$

Let $\psi : R[X] \to S[Y]$, with $\psi(x_i) = h_i(y)$, be another lift. Then $h_i(y) = g_i(y) + q_i(y)$ with $q_i(y)$ in J. Let $\eta : \bigoplus Adx_i \to J/J^2$ by $dx_i \mapsto \bar{q}_i$. Then $d\psi - d\varphi = d_B \circ \eta$ and $\bar{\psi} - \bar{\varphi} = \eta \circ d_A$ showing that the induced maps $\Gamma_{A/R} \to \Gamma_{B/S}$ and $\Omega_{A/R} \to \Omega_{B/S}$ are the same.

Now if $R = S$ and $A = B$, we get $\Gamma_{A/R} \to \Gamma_{B/S} \to \Gamma_{A/R}$ and the composition is the identity. The same holds for $\Gamma_{B/S} \to \Gamma_{A/R} \to \Gamma_{B/S}$ and for Ω. This shows that Γ and Ω are well defined and it is clear from the above that they are functorial.

Example. If $A = R/I$ we can take X to be empty and so $\Gamma_{A/R} = I/I^2$ and $\Omega_{A/R} = 0$.

Lemma 3.2. *If $A = \operatorname{colim} A_\alpha$ is a filtered colimit of R-algebras, then $\Gamma_{A/R} = \operatorname{colim} \Gamma_{A_\alpha/R}$ and $\Omega_{A/R} = \operatorname{colim} \Omega_{A_\alpha/R}$.*

Proof. Choose X_α to be A_α itself with the identity map to A_α and similarly choose $X = A$. Then $R[X] = \operatorname{colim} R[X_\alpha]$ and the result follows easily.

Theorem 3.3. ("Jacobi-Zariski sequence" [Ah]) *If $R \to A \to B$, there is a natural exact sequence $\Gamma_{B/R} \to \Gamma_{B/A} \to B \otimes_A \Omega_{A/R} \to \Omega_{B/R} \to \Omega_{B/A} \to 0$. If $\Omega_{A/R}$ is flat over A, this sequence can be extended by putting the term $B \otimes_A \Gamma_{A/R}$ on the left.*

I will usually just refer to this sequence as the JZ sequence.

Remark. This is just the cohomology sequence of André-Quillen cohomology. The correct term to put on the left is $H_1(R, A, B)$. If $\Omega_{A/R}$ is flat over A, then $H_1(R, A, B) = B \otimes_A H_1(R, A, A)$. One can define $H_n(R, A, M)$ for $n = 0, 1$ and any A-module M to be the kernel and cokernel of the map $d \otimes M : I/I^2 \otimes M \to \bigoplus Adx_i \otimes M$.

Proof. Let $A = R[X]/I$ and $B = A[Y]/J = R[X,Y]/L$, where $J = L/R[X,Y]I$. We get a diagram

(*)

$$\begin{tikzcd}
& B \otimes_A I/I^2 \arrow[r] \arrow[d] & L/L^2 \arrow[r] \arrow[d] & J/J^2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \bigoplus Bdx_i \arrow[r] & \bigoplus Bdx_i \oplus \bigoplus Bdy_j \arrow[r] & \bigoplus Bdy_j \arrow[r] & 0
\end{tikzcd}$$

and the snake lemma gives the exact sequence $H_1(R, A, B) \to \Gamma_{B/R} \to \Gamma_{B/A} \to B \otimes_A \Omega_{A/R} \to \Omega_{B/R} \to \Omega_{B/A} \to 0$. If $\Omega_{A/R}$ is flat over A, let N be the image of d_A and consider the exact sequences $0 \to \Gamma_{A/R} \to I/I^2 \to N \to 0$ and $0 \to N \to \bigoplus Adx_i \to \Omega_{A/R} \to 0$. Then N is also flat over A and tensoring these sequences with B gives $0 \to B \otimes_A \Gamma_{A/R} \to B \otimes_A I/I^2 \to B \otimes_A N \to 0$ and $0 \to B \otimes_A N \to \bigoplus Bdx_i \to B \otimes_A \Omega_{A/R} \to 0$. Therefore $B \otimes_A \Gamma_{A/R}$ maps isomorphically onto the kernel $H_1(R, A, B)$ of $B \otimes_A I/I^2 \to \bigoplus Bdx_i$ as required.

Suppose now we have a commutative diagram of ring homomorphisms

$$\begin{tikzcd} R \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & B \arrow[d] \\ R' \arrow[r] & A' \arrow[r] & B' \end{tikzcd}$$

Write $A' = R'[X']/I'$ and $B' = A'[Y']/J' = R'[X',Y']/L'$. Lift $A \to A'$ to $\varphi : R[X] \to R'[X']$ with $\varphi(x_i) = f_i(X')$ and lift $B \to B'$ to $\psi : A[Y] \to A'[Y']$. Let $\psi(y_i) = g_i(Y')$. Lift $g_i(Y') \in A'[Y']$ to $h_i(X',Y') \in R'[X',Y']$. Then $R[X,Y] \to R'[X',Y']$ by $x_i \mapsto f_i(X')$, $y_i \mapsto h_i(X',Y')$ lifts $B \to B'$. Using these lifts, we check easily that $(*)$ maps to the corresponding diagram for $R' \to A' \to B'$ using maps defined as in the proof of Lemma 3.1. The naturality of the JZ sequence now follows from the naturality of the snake lemma sequence.

Theorem 3.4. *Let $A = R[X]/I$ be any R-algebra. Then the following conditions are equivalent*

(1) *$R \to A$ is quasi-smooth*
(2) *$d : I/I^2 \to \bigoplus Adx_i$ is a split monomorphism*
(3) *$\Gamma_{A/R} = 0$ and $\Omega_{A/R}$ is projective over A.*

The following conditions are also equivalent

(4) *$R \to A$ is quasi-étale*
(5) *$d : I/I^2 \to \bigoplus Adx_i$ is an isomorphism*
(6) *$\Gamma_{A/R} = 0$ and $\Omega_{A/R} = 0$.*

Proof. It is trivial that (2) $\iff$ (3) and (5) $\iff$ (6). To see that (2) $\implies$ (1), let B be an R-algebra with an ideal J such that $J^2 = 0$. Let $\varphi : A \to B/J$ by $x_i \mapsto \bar{b}_i$. Lift $\bar{b}_i$ to b_i in B and define $\psi : R[X] \to B$ by $\psi(x_i) = b_i$. Note that $\psi : I/I^2 \to J$. We need to find δ_i in J such that $x_i \mapsto b_i + \delta_i$ gives a map $A \to B$. To give such a set of δ_i is equivalent to giving a map $\delta : \bigoplus Adx_i \to J$ by $dx_i \mapsto \delta_i$ (note that J is an A-module since $J^2 = 0$). If $f \in I$ we need $f(b_i + \delta_i) = f(b_i) + \sum \partial f/\partial x_i(b)\delta_i = 0$. This condition, for all f in I, just means that

$$(*) \qquad \begin{tikzcd} I/I^2 \arrow[r, "d"] \arrow[d, "\psi"'] & \bigoplus Adx_i \arrow[d, "-\delta"] \\ J \arrow[r, equal] & J \end{tikzcd}$$

commutes. If d is a split monomorphism, it is clear that δ exists. If d is an isomorphism, δ exists and is unique showing that (5) $\implies$ (4).

For the converse, choose $B = R[X]/I^2, J = I/I^2$, and let $\varphi : A \to B/J$ be the identity. The resulting diagram $(*)$ has $\psi = 1$ so if δ exists, d is a split monomorphism. Now let J be any A-module and choose $B = A \oplus J$ (with $(a_1 + j_1)(a_2 + j_2) = a_1a_2 + a_1j_2 + a_2j_1$). Let φ be the identity and let $\psi : R[X] \to R[X]/I = A \subset B$ be the canonical quotient map. The diagram $(*)$ now has $\psi = 0$ showing that if δ is unique, then d is onto.

Application 3.5. Suppose $R \to A$ is quasi-smooth and $B = A/I$ for some I. Then $\Gamma_{A/R} = 0$ and $\Omega_{A/R}$ is projective over A. Since $\Gamma_{B/A} = I/I^2$, the JZ sequence becomes $0 \to \Gamma_{B/R} \to I/I^2 \xrightarrow{d} B \otimes_A \Omega_{A/R} \to \Omega_{B/R} \to 0$. Therefore, in the definition of $\Gamma_{B/R}$ and $\Omega_{B/R}$, we can replace $R[X]$ by any quasi-smooth R-algebra. Note that Theorem 3.4 continues to hold for such presentations since (2) $\iff$ (3) and (5) $\iff$ (6) still hold.

Theorem 3.6. *Let S be a multiplicative subset of A. Then $\Gamma_{A_S/R} = (\Gamma_{A/R})_S$ and $\Omega_{A_S/R} = (\Omega_{A/R})_S$.*

Proof. This result for Ω is well-known and also follows immediately from the JZ sequence for $R \to A \to A_S$ since $A \to A_S$ is quasi-étale so that $\Gamma_{A_S/A} = 0 = \Omega_{A_S/A}$. For Γ, let $A = R[X]/I$ and let T be the inverse image of S in $R[X]$. We have $\bigoplus Adx_i = A \otimes_{R[X]} \Omega_{R[X]/R}$ so $0 \to \Gamma_{A/R} \to I/I^2 \xrightarrow{d} A \otimes_{R[X]} \Omega_{R[X]/R} \to \Omega_{A/R} \to 0$. Localizing this at T gives $0 \to (\Gamma_{A/R})_S \to I_T/I_T^2 \xrightarrow{d} A_S \otimes_{R[X]_T} \Omega_{R[X]_T/R} \to (\Omega_{A/R})_S \to 0$. Note that $A_S \otimes_{R[X]_T} (\Omega_{R[X]/R})_T = A_S \otimes_{R[X]_T} \Omega_{R[X]_T/R}$ by the Ω case. By 3.5 we can calculate $\Gamma_{A_S/R}$ and $\Omega_{A_S/R}$ from the presentation $A_S = R[X]_T/I_T$ and the result follows.

Remark. If S is a multiplicative subset of R it is clear from the definition that $\Gamma_{A_S/R_S} = (\Gamma_{A/R})_S$ and $\Omega_{A_S/R_S} = (\Omega_{A/R})_S$.

Corollary 3.7. *Let $A = R[X]/I$ be an R-algebra and let S be a multiplicative subset of A. Then A_S is quasi-smooth over R if and only if $d_S : (I/I^2)_S \to (\bigoplus Adx_i)_S$ is a split monomorphism.*

The following is a well-known observation.

Lemma 3.8. *Let $f : M \to N$ be a map of A-modules with M finitely generated and N finitely presented. Let S be a multiplicative subset of A. If $f_S : M_S \to N_S$ is a split monomorphism, then there is an element $s \in S$ such that $f_s : M_s \to N_s$ is a split monomorphism.*

Proof. Let $g \in \mathrm{Hom}_{A_S}(N_S, M_S)$ with $gf_S = 1$. Since N is finitely presented, we have $\mathrm{Hom}_{A_S}(N_S, M_S) = \mathrm{Hom}_A(N, M)_S$ so we can write $g = h/s$ with $h \in \mathrm{Hom}_A(N, M)$ and $s \in S$. Let $g' = h/s$ in $\mathrm{Hom}_{A_s}(N_s, M_s)$. Then $g'f_s - 1 : M_s \to M_s$ localizes to $0 : M_S \to M_S$. Since M is finitely generated, $(g'f_s - 1)_t : M_{st} \to M_{st}$ is 0 for some $t \in S$ so $g'_t f_{st} = 1$.

Corollary 3.8. *Let A be a finitely presented R-algebra and let S be a multiplicative subset of A. If A_S is essentially smooth over R, there is some $s \in S$ such that A_s is smooth over R.*

This is clear from Corollary 3.7 and Lemma 3.8.

Corollary 3.9. *Let $R \to A \to \Lambda$ with A finitely presented over R. If we can find $R \to A \to B \to \Lambda$ with B essentially smooth over R, then we can find $R \to A \to C \to \Lambda$ with C smooth over R.*

Proof. Let $B = C_S$ where C is finitely presented over R. By Corollary 3.8, some C_s is smooth over R. Let $A = R[Y_1, \dots, Y_n]/(f_1, \dots, f_m)$ and let Y_i map to c_i/t in B. Let $\varphi : R[Y] \to C_{st}$ by $Y_i \mapsto c_i/t$. Then $\varphi(f_j)$ maps to 0 in $B = C_S$ so for some $u \in S$, $\varphi(f_j)$ maps to 0 in C_{stu}. We get $R \to A \to C_{stu} \to \Lambda$ and C_{stu} is smooth over R.

4. The smooth locus. Let A be a finitely presented R-algebra and let $A = R[X]/I$ where $X = \{x_1, \dots, x_n\}$ is a finite set. If $f_1, \dots, f_r$ is any finite set of elements of I let $\Delta(f_1, \dots, f_r)$ be the ideal of A generated by all $r \times r$-minors of the Jacobian matrix $(\partial f_i/\partial x_j)$. We set $\Delta() = A$ if $r = 0$. It is a classical fact that the non-smooth locus can be described in terms of the Jacobian matrix but the following very explicit definition seems to have appeared first in Elkik's paper [E].

Definition. Let $H_{A/R}$ be the radical in A of $\sum \Delta(f_1,\dots,f_r)[(f_1,\dots,f_r){:}I]$, the sum being taken over all finite sets of elements $f_1,\dots,f_r$ of I.

If S is a multiplicative set in R it will clearly suffice to compute H_{A_S/R_S} using $f_i \in I$. Since I is finitely generated, $(f){:}I$ localizes and we see that $H_{A_S/R_S} = (H_{A/R})_S$.

Theorem 4.1. *Let A be a finitely presented R-algebra. Let P be a prime ideal of A. Then A_P is essentially smooth over R if and only if $P \not\supset H_{A/R}$.*

Therefore $H_{A/R}$ is the intersection of all primes P such that A_P is not essentially smooth over R, showing that $H_{A/R}$ is independent of the choice of presentation.

Proof. Let $A = R[X]/I$ where X is a finite set and I is finitely generated. Suppose that $P \not\supset H_{A/R}$. Let $f_1,\dots,f_r$ be elements of I such that $\Delta(f_1,\dots,f_r)[(f_1,\dots,f_r){:}I]$ is not contained in P. If Q is the inverse image of P in $R[X]$, then $(f_1,\dots,f_r){:}I$ is not contained in Q so $f_1,\dots,f_r$ generate I_Q. Therefore, the images of $f_1,\dots,f_r$ generate $(I/I^2)_P = I_Q/I_Q^2$. Also, the image of some minor, say $|\partial f_i/\partial x_j|$ for $1 \le i,\ j \le r$, does not lie in P. Let $p : \bigoplus A dx_i \to A^r$ be the projection on the first r summands. Then the composition $(A_P)^r \xrightarrow{f_1,\dots,f_r} (I/I^2)_P \xrightarrow{d_P} \bigoplus A_P dx_i \xrightarrow{p} (A_P)^r$ is given by the invertible matrix $(\partial f_i/\partial x_j)$ so the left hand map is an isomorphism and d_P is a split monomorphism.

Conversely, if d_P is a split monomorphism, then $(I/I^2)_P$ is free, say of rank r. Let $f_1,\dots,f_r$ be elements of I mapping to a base of $(I/I^2)_P = I_Q/I_Q^2$. By Nakayama's lemma, these elements generate I_Q so $(f_1,\dots,f_r){:}I$ is not contained in Q. Since $(A_P/PA_P)^r \to \bigoplus(A_P/PA_P)dx_i$ is a monomorphism of vector spaces, we can find a subset of $\{1,\dots,n\}$ say $\{1,\dots,r\}$ such that $(A_P/PA_P)^r \to \bigoplus(A_P/PA_P)dx_i \xrightarrow{p} (A_P/PA_P)^r$ is an isomorphism where p, as above, is the projection on the first r summands. Since this map is given by the matrix $(\partial f_i/\partial x_j)$ mod P, we see that $|\partial f_i/\partial x_j|$ is a unit in A_P.

Corollary 4.2. *If A is a finitely presented R-algebra, then A_s is smooth over R if and only if s lies in $H_{A/R}$.*

Proof. Since A is finitely presented, $\Omega_{A/R}$ is a finitely presented A-module and therefore $(\Omega_{A/R})_s = \Omega_{A_s/R}$ is a finitely presented A_s-module. Therefore $(\Omega_{A/R})_s$ is projective if and only if it is locally free, i.e. if and only if all $(\Omega_{A/R})_P = \Omega_{A_P/R}$ are projective for $s \notin P$. Also, $(\Gamma_{A/R})_s = 0$ if and only if all $\Gamma_{A_P/R}$ are 0 for $s \notin P$. Therefore A_s is smooth over R if and only if all A_P are essentially smooth for all P with $s \notin P$, so that $s \notin P$ implies $P \not\supset H_{A/R}$ or, equivalently, $s \in \bigcap_{P \supset H_{A/R}} P = H_{A/R}$.

Definition. Let A be a finitely presented R-algebra and let a be an element of $H_{A/R}$. We say that a is standard with respect to the presentation $A = R[X]/I$ if a lies in the radical of $\Delta(f_1,\dots,f_r)[(f_1,\dots,f_r){:}I]$ for some finite set of elements $f_1,\dots,f_r$ of I. We say that a is strictly standard if a lies in $\Delta(f_1,\dots,f_r)[(f_1,\dots,f_r){:}I]$ itself.

The following results, due to Elkik [E], enable us to reduce to this case for any a in $H_{A/R}$.

Lemma 4.3. *Let $A = R[X]/I$ be a finitely presented R-algebra and let a lie in $H_{A/R}$. If $(I/I^2)_a$ is free then a is standard.*

Proof. Let $f_1,\dots,f_r \in I$ be a base for $(I/I^2)_a$. Let $J = (f_1,\dots,f_r) \subset I$. Let $h \in R[X]$ represent a. Then $I_h = J_h + I_h^2$ so there is an α in I_h with $(1+\alpha)I_h \subset J_h$. Let $\alpha = g/h^n$. Then $(h^n + g)I_h \subset J_h$ so for some N, $h^N(h^n+g)I \subset J$. Therefore $h^N(h^n+g) \in (f){:}I$ so

a^{N+n} lies in the image of $(f){:}I$ in A. Also $0 \to I_h/I_h^2 \xrightarrow{d} \bigoplus A_a dX_i$ is a split monomorphism by Theorem 3.4 (2) (see 3.5), since A_a is smooth over R by Corollary 4.2. This map has the form $A_a^r \to A_a^n$ given by the matrix $(\partial f_j/\partial X_i)$ so the $r \times r$ minors of this matrix generate the unit ideal in A_a. (Localize and reduce modulo the maximal ideal. The rank of the result is r so some $r \times r$ minor is non-zero). Therefore some power of a lies in $\Delta(f_1, \dots, f_r)$.

Lemma 4.4. *Let $A = R[X]/I$ be a finitely presented R-algebra with $X = \{X_1, \dots, X_n\}$ and let a lie in $H_{A/R}$. If $(\Omega_{A/R})_a = \Omega_{A_a/R}$ is free then a is standard with respect to the presentation $A = R[X,Y]/(I,Y)$ where $Y = (Y_1, \dots, Y_n)$.*

Proof. Since A_a is smooth over R, $(I/I^2)_a \oplus (\Omega_{A/R})_a \approx \bigoplus A_a dX_i$ so $\Omega_{A_a/R}$ is free of rank $\leq n$ and $(I/I^2)_a \oplus A_a^n$ is free. Let $J = (I, Y)$. We have $0 \to (J/J^2)_a \to \bigoplus A_a dX_i \oplus \bigoplus A_a dY_j \to \Omega_{A_a/R} \to 0$ with a surjection $\varphi : (I/I^2)_a \oplus \bigoplus A_a \bar{Y}_j \twoheadrightarrow (J/J^2)_a$. The term $\bigoplus A_a \bar{Y}_j$ maps isomorphically onto $\bigoplus A_a dY_j$. After splitting this off, there remains $(I/I^2)_a \to \bigoplus A_a dX_i \to \Omega_{A_a/R} \to 0$. Since this is exact with a zero on the left, φ must be an isomorphism and therefore $(J/J^2)_a$ is free so Lemma 4.3 applies.

Lemma 4.5. *If M is an R-module and $S_R(M)$ is its symmetric algebra over R, then $\Omega_{S_R(M)/R} = S_R(M) \otimes_R M$.*

Proof. Let $R^m \xrightarrow{f} R^n \to M \to 0$ be a presentation of M where f is given by the matrix (a_{ij}). Then $S(M) = S(R^n)/J$ where J is generated by $\operatorname{im} f$, so $S(M) = R[X_1, ..., X_n]/(\sum a_{ij} X_j)$. Therefore $\Omega_{S(M)/R}$ is the cokernel of $S(M)^m \xrightarrow{f} \bigoplus S(M) dX_i$ which is $S(M) \otimes_R M$.

Proposition 4.6. *Let $A = R[X]/I$ be a finitely presented R-algebra. Let $M = I/I^2$ and let $C = S_A(M)$. Then $H_{A/R}C \subset H_{C/R}$ and $\Omega_{C_a/R}$ is free for each a in $H_{A/R}$. Therefore C has a presentation such that the image in C of any a in $H_{A/R}$ is standard.*

Proof. If $a \in H_{A/R}$, then $0 \to (I/I^2)_a \to \bigoplus A_a dX_i \to \Omega_{A_a/R} \to 0$ is split exact so M_a is projective. Therefore C_a is locally isomorphic to $A_a[X_1, ..., X_r]$ and so is smooth over R showing that the image of a lies in $H_{C/R}$. The JZ sequence for $R \to A_a \to C_a$ gives $0 = \Gamma_{C_a/A_a} \to C_a \otimes_{A_a} \Omega_{A_a/R} \to \Omega_{C_a/R} \to \Omega_{C_a/A_a} \to 0$. By Lemma 4.5, $\Omega_{C_a/A_a} = C_a \otimes_{A_a} M_a$ which is projective so $\Omega_{C_a/R} \approx C_a \otimes_{A_a} (\Omega_{A_a/R} \oplus M_a) \approx C_a \otimes_{A_a} (\bigoplus A_a dX_i)$ which is free.

Remark. Note that A is a retract of C (by letting M go to 0). Therefore if we have maps $R \to A \to \Lambda$, we can extend $A \to \Lambda$ to $A \to C \to \Lambda$. This is very convenient in the proof of Popescu's theorem which requires certain elements to be standard. Ogoma [O] refers to C as the standardizer of $R \to A$.

We end this section with two elementary observations.

Lemma 4.7. *Let A be a finitely presented R-algebra, let $R \to R'$, and let $A' = R' \otimes_R A$. Then $H_{A/R}A' \subset H_{A'/R'}$*

Proof. If $a \in H_{A/R}$, then A_a is smooth over R so $A'_a = R' \otimes_R A_a$ is smooth over R'.

Lemma 4.8. *Let $A = R[X]/I$ be a finitely presented R-algebra, with $I = (g_1, \dots, g_m)$. Let $R \to R'$, and let $A' = R' \otimes_R A$. Let g'_i be the image of g_i in $R'[X]$. If $a \in A$ is strictly standard with respect to the given presentation, then its image a' in A' is strictly standard with respect to the presentation $A' = R'[X]/(g'_1, \dots, g'_m)$.*

Proof. We know that a lies in $\Delta(f_1, \dots, f_r)[(f_1, \dots, f_r){:}I]$ for some finite set of elements $f_1, \dots, f_r$ of I so we can write $a = \sum m_j h_j$ where the m_j are minors of $(\partial f_i/\partial x_k)$ and

$h_jI \subset (f_1, \dots, f_r)$ so that $h_j g_k = \sum b_{jks} f_s$. Now in A' we get $a' = \sum m'_j h'_j$, showing that a' is strictly standard with respect to this presentation as required.

5. Field extensions. We recall here some standard material on separability of field extensions from the point of view of the above theory. Following the usual practice, I will say that a field extension is of finite type if it is essentially of finite type. The following theorem was proved by Mac Lane but the present formulation is due to Cartier [EGA IV,Ch.0,§21.7].

Theorem 5.1. (Mac Lane-Cartier equality). *Let E/F be a field extension of finite type. Then* $\dim_E \Omega_{E/F} = \dim_E \Gamma_{E/F} + \operatorname{tr.deg} E/F$.

Proof. Let $x_1, \dots, x_n$ be a transcendence base for E/F. Then E is a finite extension of $F(x_1, \dots, x_n)$ so we can write $E = F(x_1, \dots, x_n)[y_1, \dots, y_m]/(f_1, \dots, f_m)$ where f_{i+1} is the minimal polynomial of y_{i+1} over the field $E_i = F(x_1, \dots, x_n)[y_1, \dots, y_i]/(f_1, \dots, f_i)$. It is clear that $f_1, \dots, f_m$ is a regular sequence in $A = F(x_1, \dots, x_n)[Y_1, \dots, Y_m]$. Now $E = A/I$ with $I = (f_1, \dots, f_m)$ and A is essentially smooth over F so by 3.5 we have $0 \to \Gamma_{E/F} \to I/I^2 \xrightarrow{d} \bigoplus E dx_i \oplus \bigoplus E dy_j \to \Omega_{E/F} \to 0$. Since I is generated by a regular sequence, I/I^2 is free on m generators and the theorem follows by adding up dimensions.

Corollary 5.2. *If $F \subset E \subset K$ is an extension of fields, the JZ sequence takes the form* $0 \to K \otimes_E \Gamma_{E/F} \to \Gamma_{K/F} \to \Gamma_{K/E} \to K \otimes_E \Omega_{E/F} \to \Omega_{K/F} \to \Omega_{K/E} \to 0$

In other words, we can put a zero on the left.

Proof. It is sufficient to prove this for the case in which E and K are of finite type over F since we can obtain any $F \subset E \subset K$ as a filtered colimit of such extensions and apply Lemma 3.2. By Theorem 3.3, the sequence is exact except possibly for the zero on the left. If the extensions are of finite type, all terms in the sequence are finite dimensional and, by Theorem 5.1, the alternating sum of the dimensions of the terms is $\operatorname{tr.deg} E/F - \operatorname{tr.deg} K/F + \operatorname{tr.deg} K/E = 0$ and the result follows.

Definition. A field extension E/F is separable if E is quasi-smooth over F.

Equivalently it is separable if $\Gamma_{E/F} = 0$ since $\Omega_{E/F}$ is free over E.

Remark. It follows from Corollary 5.2 that if $F \subset E \subset K$ is an extension of fields, and K/F is separable then so is E/F. It also follows that K/F is separable if K/E and E/F are.

This definition of separability is equivalent to the classical definition. For the case of a finite extension this can be seen as follows. If E/F is finite then $\Gamma_{E/F} = 0$ if and only if $\Omega_{E/F} = 0$ by Theorem 5.1. If $E = F(a)$ is an algebraic extension with one generator a having minimal polynomial f over F, then $I/I^2 \xrightarrow{d} E dx$ is just $E \xrightarrow{f'(a)} E$ so that E/F is separable if and only if $f'(a) \neq 0$ as expected. In particular, if E/F is separable in the classical sense it is separable. Conversely, if K/F is finite and separable we can write $K = E(a)$ where E is a proper subfield of K. By induction on $|K : F|$, E/F is separable in the classical sense. The JZ sequence shows that $\Omega_{K/F}$ maps onto $\Omega_{K/E}$, so $\Omega_{K/E} = 0$ showing that K/E, and so K/F, is separable in the classical sense.

Corollary 5.3. *If E/F is a field extension of finite type, then $\Omega_{E/F} = 0$ if and only if E/F is finite separable. If A is a local ring essentially of finite type over F, then A is essentially étale over F if and only if A is a finite separable field extension of F.*

Proof. By Theorem 5.1, $\Omega_{E/F} = 0$ if and only if $\Gamma_{E/F} = 0$ and $\operatorname{tr.deg} E/F = 0$. This also shows that E is étale over F if E/F is finite separable. For the second part, let $E = A/\mathrm{m}$.

Since $\Omega_{A/F} = 0$ and $\Omega_{E/A} = 0$, the JZ sequence for $F \to A \to E$ shows that $\Omega_{E/F} = 0$. Therefore E/F is finite separable so $\Gamma_{E/F} = 0$ also. The JZ sequence now shows that $\mathfrak{m}/\mathfrak{m}^2 = \Gamma_{E/A} = 0$ so $\mathfrak{m} = 0$.

Remark. This does not hold without the assumption that the extension is of finite type. For example let F be a field of characteristic p and consider the extension $E = F(x_1, x_2, x_3, \dots)$ where $x_n = (x_{n+1})^p$ for all n. (So E is a subfield of the algebraic closure of the transcendental extension $F(x_1)$ of F). Then it is easy to see that $\Gamma_{E/F} = 0 = \Omega_{E/F}$ but E has transcendence degree 1 over F. This example also shows that Theorem 5.1 does not hold without the assumption of finite type.

Definition. A field extension K/F is called separably generated if there is a subfield E of K purely transcendental over F such that K is separable algebraic over E. A set of algebraically independent generators for such a subfield E is called a separating transcendence base for K/F.

In characteristic 0 every field extension is separably generated but in characteristic p the preceding example shows that a separable extension need not be separably generated. For extensions of finite type, however, the next proposition shows that the two concepts are equivalent.

Definition. A set $\{x_i\}$ of elements of K will be called an Ω-base for K/F if the dx_i form a basis for $\Omega_{K/F}$ over K.

Proposition 5.4. *A field extension of finite type K/F is separable if and only if it is separably generated. If so, a subset $\{x_i\}$ of K is a separating transcendence base if and only if it is an Ω-base.*

Proof. If K is separable algebraic over a pure transcendental extension $E = F(\{x_i\})$, the JZ sequence for $F \subset E \subset K$ shows that $\Gamma_{K/F} = 0$ and that $K \otimes_E \Omega_{E/F} \to \Omega_{K/F}$ is an isomorphism, $\Omega_{E/F}$ being free on the dx_i. Conversely, if K/F is separable, $\{x_1, \dots, x_n\}$ is an Ω-base, and $E = F(\{x_i\})$, then $K \otimes_E \Omega_{E/F} \to \Omega_{K/F}$ is onto, and therefore an isomorphism since the dx_i generate $\Omega_{E/F}$. The x_i are algebraically independent since $\operatorname{tr.deg} E/F = n$ by Theorem 5.1. The JZ sequence for $F \subset E \subset K$ shows that $\Omega_{K/E} = 0$ so K/E is finite separable by Corollary 5.3.

Corollary 5.5. *A field extension is separable if and only if it is a filtered union of separably generated subextensions of finite type.*

This shows that our definition of separability agrees with the classical one.

For field extensions in characteristic p, the notion of an Ω-base coincides with the classical notion of a p-base. Let K/F be such an extension. A set $\{x_i\}$ of elements of K is called a p-base for K/F if the monomials $x_{i_1}^{m_1} \dots x_{i_n}^{m_n}$ with $0 \le m_j < p$ (and distinct i_j) form a base for K over K^pF. We say that $\{x_i\}$ is a p-base for a field K of characteristic p if it is a p-base for K over the prime field (equivalently: for K over K^p).

Lemma 5.6. *Let K/F be an extension of fields of characteristic p such that $K^p \subset F \subset K$. Let $\{x_i\}$ be a set of elements of K and let $x_i^p = a_i$. Then*

(1) *The dx_i generate $\Omega_{K/F}$ if and only if $K = F(\{x_i\})$.*
(2) *The dx_i are linearly independent in $\Omega_{K/F}$ if and only if the map $A = F[\{X_i\}]/(\{X_i^p - a_i\}) \to K$ is injective.*

Proof. Clearly $\Omega_{A/F}$ is A-free on the dX_i. If $A \to K$ is onto, it follows that dx_i generate $\Omega_{K/F}$. If $A \to K$ is injective, enlarge the set $\{x_i\}$ to one maximal with respect to this property. Let E be the image of the new map $A \to K$. It is a field since K is algebraic over F. If $E \neq K$, choose $E \subset E' \subset K$ with $|E' : E| = p$. Let $E' = E(y)$ with $y^p = b$. Then $A[Y]/(Y^p - b) \to K$ is injective so the set $\{x_i\}$ can be enlarged further to $\{x_i, y\}$. Therefore $A \xrightarrow{\approx} K$ so $\Omega_{K/F} = \Omega_{A/F}$ is free on the dx_i which are therefore linearly independent.

For the reverse implication in (2), it will suffice to consider the case where $\{x_i\}$ is finite. By induction on its order n, we can assume that $A' = F[X_1, \ldots, X_{n-1}]/(X_i^p - a_i) \to K$ is injective with image E. Then $A \to K$ is $E[X]/(X^p - a) \to K$ where $X = X_n$ and $a = a_n$. If this map is not injective, then $X^p - a$ is reducible over E but this implies that x_n lies in E so that dx_n is linearly dependent on $dx_1, \ldots, dx_{n-1}$.

For the reverse implication in (1), we can, if necessary, omit some of the x_i so that the dx_i are a base for $\Omega_{K/F}$. Then $A \xrightarrow{\approx} E \subset K$ by (2). If $E \neq K$ then, as above, we can enlarge $\{x_i\}$ to $\{x_i, y_j\}$ such that the new A maps isomorphically onto K. By (2) again, the dx_i and the dy_j are linearly independent. Since the dx_i are already a base for $\Omega_{K/F}$, no y_j can occur.

Corollary 5.7. *Let K/F be an extension of fields of characteristic p. Let $\{x_i\}$ be a set of elements of K. Then $\{x_i\}$ is a p-base for K/F if and only if $\{x_i\}$ is an Ω-base for K/F.*

Proof. Since $dK^p = 0$ in $\Omega_{K/F}$, $\Omega_{K/F} = \Omega_{K/K^pF}$. Therefore we can replace F by K^pF and Lemma 5.6 applies.

6. An argument of Faltings. A theorem of André [Ah] states that $H_1(R, A, -) = 0$ if A is a geometrically regular R-algebra. It follows from this that the JZ sequence for any $R \to A \to B$ reduces to $0 \to \Gamma_{B/R} \to \Gamma_{B/A} \to B \otimes_A \Omega_{A/R} \to \Omega_{B/R} \to \Omega_{B/A} \to 0$. In particular, if $B = \bar{A} = A/I$ we get $0 \to \Gamma_{\bar{A}/R} \to I/I^2 \to \bar{A} \otimes_A \Omega_{A/R} \to \Omega_{\bar{A}/R} \to 0$. The following is a special case of this result. We give a direct proof using a method of Faltings [F] to avoid the need for André's difficult theorem. Popescu [Pa] has remarked that André's theorem follows immediately from Theorem 1.1 since it is clear from the definition that it is true for smooth R-algebras (See the remark following Theorem 3.3. If d is a split monomorphism, so is $M \otimes d$).

Theorem 6.1. *Let k be a field and let A be a geometrically regular local k-algebra with maximal ideal $\mathfrak{m}$ and residue field $K = A/\mathfrak{m}$. Then $0 \to \Gamma_{K/k} \to \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{d} K \otimes_A \Omega_{A/k} \to \Omega_{K/k} \to 0$ is exact.*

Proof. (After Faltings [F]) Note that $\mathfrak{m}/\mathfrak{m}^2 = \Gamma_{K/A}$. The sequence is just the JZ sequence for $k \to A \to K$ and is therefore exact except possibly on the left. We must show that $\Gamma_{K/k} \to \Gamma_{K/A}$ is injective. This is clear if K/k is separable so we can assume k has characteristic $p \neq 0$. Let $\mathbb{F} \subset k$ be the prime field. Since $\mathbb{F}$ is perfect, $\Gamma_{K/\mathbb{F}} = 0$. The JZ sequences for

$$\begin{tikzcd}
\mathbb{F} \arrow[r, phantom, "\subset"] \arrow[d] & k \arrow[r, phantom, "\subset"] \arrow[d] & K \arrow[d] \\
\mathbb{F} \arrow[r, phantom, "\subset"] & A \arrow[r, two heads] & K
\end{tikzcd}$$

form a diagram

$$\begin{tikzcd}
0 \arrow[r] & \Gamma_{K/k} \arrow[r] \arrow[d] & K \otimes_k \Omega_{k/\mathbb{F}} \arrow[r] \arrow[d] & \Omega_{K/\mathbb{F}} \arrow[r] \arrow[d] & \Omega_{K/k} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Gamma_{K/A} \arrow[r] & K \otimes_A \Omega_{A/\mathbb{F}} \arrow[r] & \Omega_{K/\mathbb{F}} \arrow[r] & 0 \arrow[r] & 0
\end{tikzcd}$$

and it will clearly suffice to show that $K \otimes_k \Omega_{k/\mathbb{F}} \to K \otimes_A \Omega_{A/\mathbb{F}}$ is injective. Let $x_1, \dots, x_n$ be elements of k such that $dx_1, \dots, dx_n$ are linearly independent in $\Omega_{k/\mathbb{F}}$ and let $k' = k(x_1^{1/p}, \dots, x_n^{1/p})$. Then $A' = k' \otimes_k A$ is regular by hypothesis. Note that A' is local since $A'^p \subset A$. Let $\mathfrak{m}' = \mathfrak{m}_{A'} = \{x \in A' | x^p \in \mathfrak{m}\}$ and let $K' = A'/\mathfrak{m}'$. Since $K'/\mathbb{F}$ is separable, $0 \to \mathfrak{m}'/\mathfrak{m}'^2 \xrightarrow{d} K' \otimes_{A'} \Omega_{A'/\mathbb{F}} \to \Omega_{K'/\mathbb{F}} \to 0$ is exact. Tensoring the bottom row of the previous diagram with K' we get a diagram

$$\begin{tikzcd}
0 \arrow[r] & K' \otimes_K \mathfrak{m}/\mathfrak{m}^2 \arrow[r, "d"] \arrow[d] & K' \otimes_A \Omega_{A/\mathbb{F}} \arrow[r] \arrow[d] & K' \otimes_K \Omega_{K/\mathbb{F}} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathfrak{m}'/\mathfrak{m}'^2 \arrow[r, "d"] & K' \otimes_{A'} \Omega_{A'/\mathbb{F}} \arrow[r] & \Omega_{K'/\mathbb{F}} \arrow[r] & 0.
\end{tikzcd}$$

Since A' is finite over A, A and A' have the same Krull dimension and therefore the two left hand terms in this diagram have the same dimension. The JZ sequence for $\mathbb{F} \subset K \subset K'$ gives $0 \to \Gamma_{K'/K} \to K' \otimes_K \Omega_{K/\mathbb{F}} \to \Omega_{K'/\mathbb{F}} \to \Omega_{K'/K} \to 0$. By Theorem 5.1, $\dim \Gamma_{K'/K} = \dim \Omega_{K'/K}$. By applying the snake lemma to the previous diagram, we see that the kernel and cokernel of $K' \otimes_A \Omega_{A/\mathbb{F}} \to K' \otimes_{A'} \Omega_{A'/\mathbb{F}}$ have the same finite dimension.

Now $k' = k[T_1, \dots, T_n]/(T_1^p - x_1, \dots, T_n^p - x_n)$ so $A' = A[T_1, \dots, T_n]/(T_1^p - x_1, \dots, T_n^p - x_n)$. Therefore, $d = 0$ in the exact sequence $0 \to \Gamma_{A'/A} \to I/I^2 \xrightarrow{d} \bigoplus A' dT_i \to \Omega_{A'/A} \to 0.$ so $\Omega_{A'/A}$ is free on n generators.

If $A = \mathbb{F}[Z]/(g_j(Z))$, then $A' = \mathbb{F}[Z, T_1, \dots, T_n]/(g_j(Z), T_1^p - x_1, \dots, T_n^p - x_n)$. Therefore $\Omega_{A'/\mathbb{F}}$ is generated by the dZ and the dT_i with relations $dg_j = 0$ and $dx_i = 0$ so $\Omega_{A'/\mathbb{F}} = A' \otimes_A \Omega_{A/\mathbb{F}}/(dx_1, \dots, dx_n) \oplus \bigoplus A' dT_i$. In particular, the kernel of $K' \otimes_A \Omega_{A/\mathbb{F}} \to K' \oslash_{A'} \Omega_{A'/\mathbb{F}}$ is generated by $dx_1, \dots, dx_n$. Since this kernel has the same dimension n as the cokernel $K' \otimes_{A'} \Omega_{A'/A}$, the dx_i must be linearly independent in $K' \otimes_A \Omega_{A/\mathbb{F}}$, proving the theorem.

Corollary 6.2. *Let k be a field and let A be a geometrically regular local k-algebra with maximal ideal $\mathfrak{m}$ and residue field $K = A/\mathfrak{m}$. Then* $\dim_K \Gamma_{K/k} < \infty$.

Corollary 6.3. (Mac Lane's criterion of separability) *A field extension E/F is geometrically regular if and only if it is separable.*

Proof. If E/F is separable, and F'/F is purely inseparable, then E and F' are linearly disjoint over F so $F' \otimes_F E$ is a field. In the opposite direction we can take $A = E$ and the theorem gives $\Gamma_{E/F} = 0$.

7. Flatness.

The local criterion of flatness is usually presented in the form of a long list of implications [M]. Since this is rather difficult to remember, I will just recall those parts of the result which we will need here. The reader familiar with this criterion can simply skip to the applications.

Theorem 7.1. (Local criterion of flatness). *Let $R \to A$ be a map of noetherian rings. Let I be an ideal of R such that IA is contained in the Jacobson radical of A. Let M be a finitely generated A-module. Then M is flat over R if and only if M/I^nM is flat over R/I^n for all n.*

Proof. The 'only if' part is trivial. For the converse it will suffice to show that, for any short exact sequence $0 \to N' \to N \to N'' \to 0$ of finitely generated R-modules, $0 \to M \otimes_R N' \to M \otimes_R N$ is injective. By Artin-Rees we have $N' \cap I^nN = I^{n-r}N'_0$ for some r and $n \geq r$. Tensoring the sequence $0 \to N'/I^{n-r}N'_0 \to N/I^nN \to N''/I^nN'' \to 0$ with M/I^nM over R/I^n gives $0 \to M \otimes_R (N'/I^{n-r}N'_0) \to M \otimes_R (N/I^nN)$. If $L = \mathrm{im}[M \otimes_R N'_0 \to M \otimes_R N']$ then $I^{n-r}L = \mathrm{im}[M \otimes_R I^{n-r}N'_0 \to M \otimes_R N']$. Therefore $(M \otimes_R N')/I^{n-r}L = M \otimes_R (N'/I^{n-r}N'_0)$ and so $0 \to (M \otimes_R N')/I^{n-r}L \to (M \otimes_R N)/I^n(M \otimes_R N)$ is exact. This shows that $\ker[M \otimes_R N' \to M \otimes_R N] \subset \bigcap_n I^{n-r}L$ which is 0 because L is a finitely generated A-module and IA lies in the Jacobson radical of A.

Lemma 7.2. *Let $R \to A$ and let M be an A-module. Then $\mathrm{Tor}_1^R(M,N) = 0$ for all A-modules N if and only if $M \otimes_R A$ is flat over A and $\mathrm{Tor}_1^R(M,A) = 0$.*

Proof. If $\mathrm{Tor}_1^R(M,N) = 0$ for all A-modules N, then $M \otimes_R N = M \otimes_R A \otimes_A N$ is exact in N so $M \otimes_R A$ is flat over A. For the converse, let N be any A-module and form $0 \to L \to F \to N \to 0$ with F free over A. Then, since $M \otimes_R N = M \otimes_R A \otimes_A N$ is exact in N, $0 = \mathrm{Tor}_1^R(M,F) \to \mathrm{Tor}_1^R(M,N) \to M \otimes_R L \rightarrowtail M \otimes_R F$ so $\mathrm{Tor}_1^R(M,N) = 0$.

Corollary 7.3. *Let $R \to A$ be a map of noetherian rings. Let I be an ideal of R such that IA is contained in the Jacobson radical of A. Let M be a finitely generated A-module. Then M is flat over R if and only if M/IM is flat over R/I and $\mathrm{Tor}_1^R(R/I,M) = 0$.*

Proof. The 'only if' part is trivial. For the converse, Lemma 7.2 with $A = R/I$ shows that $\mathrm{Tor}_1^R(M,N) = 0$ if $IN = 0$ and therefore (by the exact Tor sequence) also if $I^nN = 0$ for some n. Lemma 7.2 with $A = R/I^n$ now shows that M/I^nM is flat over R/I^n and we can apply Theorem 7.1.

We now apply these results to prove some facts about flat extensions.

Lemma 7.4. *Let $R \to A \to B$ with A and B noetherian. Let I be an ideal of R such that IB lies in the Jacobson radical of B. If B is flat over R and B/IB is flat over A/IA, then B is flat over A.*

Proof. Apply Corollary 7.3 to $A \to B$ and IA. We need to show that $\mathrm{Tor}_1^A(A/IA,B) = 0$. Using the resolution $0 \to IA \to A \to A/IA \to 0$ we see that this is equivalent to showing that $IA \otimes_A B \to IB$ is an isomorphism. Since B is flat over R, the same argument shows that $I \otimes_R B \xrightarrow{\approx} IB$. We have epimorphisms $I \otimes_R B = I \otimes_R A \otimes_A B \twoheadrightarrow IA \otimes_A B \twoheadrightarrow IB$. Since the composition is an isomorphism, both these maps must be isomorphisms.

Lemma 7.5. *Let $A \to B$ and let $x_1, \ldots, x_n \in A$ be a regular sequence on A and on B. Then $\mathrm{Tor}_1^A(A/(x_1, \ldots, x_n)A, B) = 0$.*

Proof. Let $I = (x_1, \ldots, x_{n-1})A$ and let $x = x_n$. By induction on n, $\mathrm{Tor}_1^A(A/I,B) = 0$. Now $0 \to A/I \xrightarrow{x} A/I \to A/(I,x) \to 0$ gives $0 \to \mathrm{Tor}_1^A(A/(I,x),B) \to B/IB \overset{x}{\rightarrowtail} B/IB$ and the last map is injective.

Lemma 7.6. *Let $A \to B$ be a local morphism of regular local rings. Suppose that $B \otimes_A \mathfrak{m}_A/\mathfrak{m}_A^2 \rightarrowtail \mathfrak{m}_B/\mathfrak{m}_B^2$ is injective i.e. a regular system of parameters of A maps to part of a regular system of parameters of B. Then B is flat over A and $B/\mathfrak{m}_A B$ is regular of dimension* $\dim B - \dim A$.

Proof. We apply Corollary 7.3. Since $B/\mathfrak{m}_A B$ is flat over $A/\mathfrak{m}_A$, we only need to show that $\mathrm{Tor}_1^A(A/\mathfrak{m}_A, B) = 0$. This follows from Lemma 7.5. The last statement is clear.

Lemma 7.7. *Let $A \to B$ be a flat local morphism of local rings. Suppose that $B/\mathfrak{m}_A B$ is regular of dimension d. Let $\varphi : A[X_1, \ldots, X_n] \to B$ where the X_i map to part of a regular system of parameters of $B/\mathfrak{m}_A B$. Let $P = \varphi^{-1}(\mathfrak{m}_B)$. Then $A[X_1, \ldots, X_n]_P \to B$ is flat. In particular, φ is flat and B/PB is regular of dimension $d - n$.*

Proof. Applying Lemma 7.4 to $A \to A[X]_P \to B$, we see that it is sufficient to work modulo $\mathfrak{m}_A$. Therefore we can assume that A is a field k. Now $\varphi : k[X_1, \ldots, X_n] \to B$ has $P = (X_1, \ldots, X_n)$ and Lemma 7.6 applies. The last statement is clear.

Lemma 7.8. *Let $A \to B$ be a flat local morphism of local rings with residue class fields $F \subset K$. Let $\varphi : A[X_1, \ldots, X_n] \to B$ send the X_i to elements whose images in K are algebraically independent over F. Then φ is flat.*

Proof. Let P be the inverse image of $\mathfrak{m}_B$ in $A[X]$. Applying Lemma 7.4 to $A \to A[X]_P \to B$, we see that it is sufficient to work modulo $\mathfrak{m}_A$. Therefore we can assume that $A = F$. In this case, $P = 0$ so $A[X]_P$ is a field and B is obviously flat over it.

Except for Corollary 6.2, the only place we will need Theorem 6.1 is in the proof of the following lemma ([Pl,Lemma 5]).

Lemma 7.9. *Let $A \to B$ be a flat local morphism of local rings. Suppose that $B/\mathfrak{m}_A B$ is geometrically regular of dimension d over $k = A/\mathfrak{m}_A$. Let $K = B/\mathfrak{m}_B$ and let $k \subset E \subset K$ where E is a field of finite type over k. Let $y_1, \ldots, y_s \in B$ map to a p-base $\bar{y}_1, \ldots, \bar{y}_s$ for E over k. Let $\varphi : A[Y_1, \ldots, Y_s] \to B$ by sending Y_i to y_i. Let $P = \varphi^{-1}(\mathfrak{m}_B)$. Then $A[Y_1, \ldots, Y_n]_P \to B$ is flat. In particular, φ is flat and B/PB is regular of dimension* $\dim B - \dim_E \Gamma_{E/k} = \dim B - \dim_L \Gamma_{L/k}$ *where $L = k(\bar{y}_1, \ldots, \bar{y}_n) \subset E$.*

Proof. Applying Lemma 7.4 to $A \to A[Y]_P \to B$, we see that it is sufficient to work modulo $\mathfrak{m}_A$. Therefore we can assume that $A = k$. Let $C = k[Y]_P$ so that $C/\mathfrak{m}_C = L$. Since C is essentially smooth over k, $\Gamma_{C/k} = 0$ and $\Omega_{C/k}$ is projective. The JZ sequence of $k \to C \to L$ is $0 \to \Gamma_{L/k} \to \Gamma_{L/C} \to L \otimes_C \Omega_{C/k} \to \Omega_{L/k} \to 0$. The dy_i generate $\Omega_{C/k}$ and their images are linearly independent in $\Omega_{E/k}$ and so also in $\Omega_{L/k}$. Therefore $L \otimes_C \Omega_{C/k} \to \Omega_{L/k}$ is an isomorphism and hence so is $\Gamma_{L/k} \to \Gamma_{L/C} = \mathfrak{m}_C/\mathfrak{m}_C^2$, so that the Krull dimension of C is $\dim_L \Gamma_{L/k}$. Consider the diagram

$$\begin{tikzcd}
 & K \otimes_L \Gamma_{L/k} \arrow[r, "\approx"] \arrow[d] & K \otimes_L \Gamma_{L/C} \arrow[r, equal] \arrow[d] & K \otimes_L (\mathfrak{m}_C/\mathfrak{m}_C^2) \arrow[d] \\
0 \arrow[r] & \Gamma_{K/k} \arrow[r] & \Gamma_{K/B} \arrow[r, equal] & \mathfrak{m}_B/\mathfrak{m}_B^2
\end{tikzcd}$$

The lower map is injective by Theorem 6.1 and the left vertical map is is injective by Corollary 5.2. It follows that the right vertical map is injective so B is flat over C by Lemma 7.6 which also shows that $\dim B/PB = \dim B - \dim C = \dim B - \dim_L \Gamma_{L/k}$. Finally note that $E \otimes_L \Omega_{L/k} \to \Omega_{E/k}$ is onto so $\Omega_{E/L} = 0$ by the JZ sequence of $k \subset L \subset E$. By Corollary 5.3, E/L is finite separable. Therefore $\Gamma_{E/L} = 0$ and the JZ sequence shows that $E \otimes_L \Gamma_{L/k} \to \Gamma_{E/k}$ is an isomorphism so $\dim_L \Gamma_{L/k} = \dim_E \Gamma_{E/k}$.

8. Results from commutative algebra. The following 3 sections contain well-known standard material and are included only for the sake of completeness. They may be skipped by the reader familiar with these results. In the present section we recall some well-known facts of commutative algebra beginning with some standard facts about Cohen-Macaulay rings.

If I is an ideal of a noetherian ring R and M is a finitely generated R-module, $\operatorname{depth}_I M$ is the least n such that $\operatorname{Ext}_R^n(R/I, M) \neq 0$ (or ∞ if no such n exists). We have $\operatorname{depth}_I M = 0$ if and only if $\operatorname{Hom}_R(R/I, M) \neq 0$ which occurs if and only if I consists of zero-divisors on M. If x is regular on M, the long exact Ext sequence of $0 \to M \xrightarrow{x} M \to M/xM \to 0$ shows that $\operatorname{depth}_I M/xM = \operatorname{depth}_I M - 1$. From these facts it follows easily that every maximal regular sequence on M in I has length equal to $\operatorname{depth}_I M$. Therefore $I \subset J$ implies $\operatorname{depth}_I M \leq \operatorname{depth}_J M$.

Lemma 8.1. $\operatorname{depth}_I M = \min \operatorname{depth}_P M$ *over prime ideals* $P \supset I$.

Proof. This follows immediately from the long exact sequence and the fact that R/I has a finite filtration with quotients of the form R/P. Alternatively, if it is false for some I, choose I maximal. We claim that I is prime. If not, let $ab \in I$ with $a, b \neq I$. Then $0 \to R/I' \to R/I \to R/I'' \to 0$ with $I' = I{:}(a)$ and $I'' = (I, a)$. Note $b \in I'$. The long exact sequence now gives $\operatorname{depth}_I M \geq \min(\operatorname{depth}_{I'} M, \operatorname{depth}_{I''} M)$ but the lemma is true for I' and I'' and any P containing I contains one of I' and I''.

Remark. If S is a multiplicative set then $\operatorname{depth}_{I_S} M_S \geq \operatorname{depth}_I M$ since $Ext_R^n(R/I, -)$ localizes.

Definition. The grade of I is defined to be $\operatorname{gr} I = \operatorname{depth}_I R$

Lemma 8.2. $\operatorname{gr} I \leq \operatorname{ht} I$.

Proof. Since $\operatorname{ht} I = \min \operatorname{ht} P$ over primes $P \supset I$ we can assume $I = P$ is prime. Since $\operatorname{gr} P \leq \operatorname{gr} P_P$ we can assume that R is local with maximal ideal P. Let $n = \operatorname{gr} P$ and let $x_1, \ldots, x_n$ be a regular sequence in P. Since $\dim R/(x) = \dim R - 1$ for x regular, we have $\dim R/(x_1, \ldots, x_n) = \dim R - n$ so $n \leq \dim R = \operatorname{ht} P$.

Definition. We say R is Cohen-Macaulay (CM for short) if $\operatorname{gr} I = \operatorname{ht} I$ for all I

It is clearly sufficient just to assume that this condition holds for prime ideals. Since $\operatorname{gr} P_S \geq \operatorname{gr} P$ while $\operatorname{ht} P_S = \operatorname{ht} P$ if $P_S \neq R_S$, we see that if R is Cohen-Macaulay then so is any localization R_S.

Lemma 8.3. *If P is prime but not maximal then* $\operatorname{depth}_P M \geq \min_{Q > P} \operatorname{depth}_Q M - 1$ *over primes $Q > P$. In particular,* $\operatorname{gr} P \geq \min_{Q > P} \operatorname{gr} Q - 1$.

Proof. Suppose that $a \notin P$. The long exact sequence for $0 \to R/P \xrightarrow{a} R/P \to R/(P, a) \to 0$ gives $\operatorname{Ext}_R^n(R/P, M) \xrightarrow{a} \operatorname{Ext}_R^n(R/P, M) \to \operatorname{Ext}_R^{n+1}(R/(P, a), M)$ and the Ext^{n+1} term is 0 if $n+1 < \min_{Q > P} \operatorname{depth}_Q M$ since $\operatorname{depth}_{(P,a)} M = \min \operatorname{depth}_Q M$ over $Q \supset (P, a)$. Therefore, if $\mathfrak{a}$ is the annihilator of $\operatorname{Ext}_R^n(R/P, M)$ we have $\mathfrak{a} + Ra = R$. If $\mathfrak{a} > P$, choose $a \in \mathfrak{a} - P$ and get $\mathfrak{a} = R$. If $\mathfrak{a} = P$, then $P + Ra = R$ for all $a \notin P$ so P is maximal.

Corollary 8.4. *The following are equivalent.*

(1) R *is CM.*
(2) $\operatorname{gr}\mathfrak{m} = \operatorname{ht}\mathfrak{m}$ *for all maximal ideals* $\mathfrak{m}$ *of* R.
(3) $R_\mathfrak{m}$ *is CM for all maximal ideals* $\mathfrak{m}$ *of* R.

To see that (3) implies (2), note that $\operatorname{Ext}^n_R(R/\mathfrak{m}, R)$ is annihilated by $\mathfrak{m}$ and so is unchanged by localization showing that $\operatorname{gr}\mathfrak{m} = \operatorname{gr}\mathfrak{m}_\mathfrak{m}$

Corollary 8.5. *If* R *is Cohen-Macaulay and* P *is prime, then all maximal chains of primes* $P = P_0 > \cdots > P_0$ *have the same length.*

Proof. It is sufficient to show that if $P > Q$ with no prime between, then $\operatorname{ht}P = \operatorname{ht}Q + 1$. For this we can localize at P and Lemma 8.3 then gives $\operatorname{gr}Q \geq \operatorname{gr}P - 1$ so $\operatorname{ht}Q \geq \operatorname{ht}P - 1$. The reverse inequality is trivial.

Recall that for a local ring R and a non-unit x we have $\dim R \geq \dim R/(x) \geq \dim R - 1$ and $\dim R/(x) = \dim R - 1$ if x is regular.

Lemma 8.6. *If* R *is a local Cohen-Macaulay ring and* x *is a non-unit,then* $\dim R/(x) = \dim R - 1$ *if and only if* x *is regular*

Proof. If x is regular there is no problem. If x is not regular let P be minimal over (x). Then $\operatorname{gr}P = 0$ so $\operatorname{ht}P = 0$. By Corollary 8.5, $\dim R/P = \dim R$ so $\dim R/(x) = \dim R$

Corollary 8.7. *If* R *is a local Cohen-Macaulay ring and* $x_1, \ldots, x_n$ *is a system of parameters then* $x_1, \ldots, x_n$ *is a regular sequence.*

Proof. $\dim R/(x_1, \ldots, x_i) = \dim R - i$ so x_{i+1} is regular on $\dim R/(x_1, \ldots, x_i)$ by Lemma 8.6.

Lemma 8.8. *If* R *is Cohen-Macaulay, so is the polynomial ring* $R[x]$.

Proof. Let $\mathfrak{m}$ be a maximal ideal of $R[x]$ and let $P = \mathfrak{m} \cap R$. Since $R[x]_\mathfrak{m}$ is a localization of $R_P[x]$, we can replace R by R_P and assume that R is local with maximal ideal P. Let $k = R/P$. Then $\mathfrak{m}/P[x]$ is maximal in $k[x]$ and so is generated by a monic polynomial $\bar{f}$. Lift this to a monic polynomial f over R. Then $\mathfrak{m} = (P, f)$. Let $x_1, \ldots, x_n$ be a regular sequence in P on R. Then $f, x_1, \ldots, x_n$ is regular on $R[x]$ since $R[x]/(f)$ is a free R-module. It follows that $\operatorname{gr}\mathfrak{m} \geq 1 + \operatorname{gr}P = 1 + \operatorname{ht}P = \operatorname{ht}\mathfrak{m}$.

We next recall some standard results about the behavior of prime ideals in integral extensions.

Theorem 8.9. *Let* $A \subset B$ *be an integral extension. Let* $\mathfrak{p}$ *be a prime ideal of* A. *Then an ideal* P *of* B *is a prime ideal lying over* $\mathfrak{p}$ *(i.e.* $P \cap A = \mathfrak{p}$*) if and only if* P *is maximal such that* $P \cap A \subset \mathfrak{p}$.

Proof. Suppose first that P is prime and $P \cap A = \mathfrak{p}$. We must show that no bigger ideal $I > P$ satisfies $I \cap A = \mathfrak{p}$. We can clearly work modulo P and therefore suppose that $P = \mathfrak{p} = 0$ which implies that A and B are domains. Suppose that $x \in I$ is non-zero. Let x satisfy $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with all a_i in A, and with n least. Then $a_n \neq 0$ otherwise we could divide by x. But $a_n \in I \cap A$ so $I \cap A \neq 0$.

Conversely, if P is maximal such that $P \cap A \subset \mathfrak{p}$, then P is prime because it is maximal with respect to $P \cap S = \emptyset$ where S is the multiplicative set $A - \mathfrak{p}$. We can again work modulo P and therefore suppose that $P = 0$ and that $I \cap A \subset \mathfrak{p}$ implies $I = 0$. It will suffice to show that $x \in \mathfrak{p}$ implies $Bx \cap A \subset \mathfrak{p}$ since this then shows that $x = 0$. Let $b \in B$ satisfy $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ with all a_i in A. Suppose bx lies in A. Then $(bx)^n + a_1 x(bx)^{n-1} + \cdots + a_n x^n = 0$ so $(bx)^n$ lies in Ax and therefore in $\mathfrak{p}$. Since $\mathfrak{p}$ is prime, bx lies in $\mathfrak{p}$.

Corollary 8.10. *(Lying over theorem). If $A \subset B$ is an integral extension then* $\operatorname{Spec} B \to \operatorname{Spec} A$ *is onto.*

Remark. In particular, if $R \subset F$ is integral and F is a field, then R is also a field since its only prime ideal is 0. It follows that if $A \subset B$ is integral and $\mathfrak{m}$ is maximal in B, then $\mathfrak{m} \cap A$ is maximal in A.

Corollary 8.11. *(Going up theorem). Let $A \subset B$ be an integral extension. Let P be a prime ideal of B, $\mathfrak{p} = P \cap A$ and let $\mathfrak{p} \subset \mathfrak{q}$ where $\mathfrak{q}$ is a prime ideal of A. Then there is a prime ideal Q of B with $\mathfrak{q} = Q \cap A$ and $P \subset Q$.*

In the other direction, we require some additional hypotheses.

Theorem 8.12. *(Going down theorem). Let $A \subset B$ be an integral extension. Assume that A is a normal domain and that B is torsion free as an A-module. Let P be a prime ideal of B, $\mathfrak{p} = P \cap A$ and let $\mathfrak{p} \supset \mathfrak{q}$ where $\mathfrak{q}$ is a prime ideal of A. Then there is a prime ideal Q of B with $\mathfrak{q} = Q \cap A$ and $P \supset Q$.*

This is usually proved using Galois theory. We will instead give the proof of Cohen and Seidenberg [CS] which is more direct.

Lemma 8.13. *Let A be a normal domain with quotient field K. Let B be an A-algebra torsion free as an A-module. Let b be an element of B integral over A. Let $f(X)$ be the minimal monic equation of $b \in KB$ over K. Then $\{g(X) \in A[X] | g(b) = 0\} = A[X]f(X)$. In particular, f is in $A[X]$.*

Proof. Note that $f(b) = 0$ since B is torsion free and hence is contained in KB. If $g(b) = 0$, then $g = fh$ in $K[X]$. Suppose first that g lies in $A[X]$ and is monic. Such a g exists since b is integral over A. The roots of g are then integral over A so the same is true of f and of h. Therefore the coefficients of f and h are integral over A and thus in A which is normal. If g is not monic we apply this argument to $g + f^N$ for large N.

Lemma 8.14. *Let $A \subset B$ be an integral extension and let I be an ideal of A. Then $\sqrt{IB}$ is the set of all x in B which satisfy an equation $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with all a_i in I.*

Proof. It is clear that the set of such x lies in $\sqrt{IB}$. For the converse, let $y = x^N$ lie in IB. There is a subring $C = \sum A\omega_i$ of B, finite over A, with $y \in IC$. Let $y\omega_i = \sum q_{ij}\omega_j$ with the q_{ij} in I. Then $|yI - (q_{ij})|\omega_i = 0$ so $|yI - (q_{ij})| = 0$ which gives an equation of the required type for y and substituting $x^N = y$ gives the required equation for x.

Proof of Theorem 8.12. Let $S = (B - P)(A - \mathfrak{q})$. It will suffice to show that S is disjoint from $B\mathfrak{q}$. We then take $Q \supset B\mathfrak{q}$ maximal such that $Q \cap S = \emptyset$. Suppose that $ab \in B\mathfrak{q}$ where $a \in A - \mathfrak{q}$ and $b \in B - P$. Let $f(b) = 0$ where $f(X) = X^n + c_1 X^{n-1} + \cdots + c_n$, with all c_i in A, is the minimal equation of b over A as in Lemma 8.13. Then $h(ab) = 0$, where $h(X) = X^n + ac_1 X^{n-1} + \cdots + a^n c_n$, is the minimal equation for ab over A. Since ab lies in $B\mathfrak{q}$, Lemma 8.14 shows that ab satisfies a monic equation $g(ab) = 0$ where $\bar{g}(X) = X^m$, the bar denoting reduction mod $\mathfrak{q}$. By Lemma 8.13, we see that h divides g and therefore

$\bar{h}$ divides $\bar{g}$ so that $\bar{h} = X^n$. Therefore all $a^i c_i$ lie in $\mathfrak{q}$. Since $a \in A - \mathfrak{q}$, all c_i lie in $\mathfrak{q}$, i.e. $\bar{f} = X^n$. By Lemma 8.14, b lies in $\sqrt{\mathfrak{q}B} \subset P$, a contradiction.

I will say that an inclusion $\mathfrak{q} \subset \mathfrak{p}$ of prime ideals in A satisfies going down with respect to $B \supset A$ if every prime ideal P of B over $\mathfrak{p}$ contains a prime ideal Q over $\mathfrak{q}$.

Corollary 8.15. *Let A be a domain and let A' be the integral closure of A in its quotient field. If $\mathfrak{q} \subset \mathfrak{p}$ in A satisfies going down with respect to A', then it satisfies going down with respect to any $B \supset A$ with B integral over A and torsion free as an A-module.*

Proof. Let P be a prime ideal of B over $\mathfrak{p}$. Let K be the quotient field of A. Since B is torsion free over A, B is a subring of KB and we can construct $A'B$ inside KB. Since $A'B$ is integral over B, there is a prime P' of $A'B$ over P. Let $\mathfrak{p}' = P' \cap A'$. This lies over $\mathfrak{p}$ so, by hypothesis, there is a prime $\mathfrak{q}' \subset \mathfrak{p}'$ lying over $\mathfrak{q}$. Now $A' \subset A'B$ satisfies all the hypotheses of Theorem 8.12 so there is a prime Q' of $A'B$ over $\mathfrak{q}'$ with $Q' \subset P'$. Let $Q = B \cap Q'$.

Corollary 8.16. *Let R be a domain and let $A = R[X]$ be a polynomial ring over R. Let $\mathfrak{p}$ be a prime ideal of A, set $\mathfrak{p}_0 = R \cap \mathfrak{p}$, and let $\mathfrak{q} = \mathfrak{p}_0 A$. Then $\mathfrak{q} \subset \mathfrak{p}$ satisfies going down with respect to any $B \supset A$ with B integral over A and torsion free as an A-module.*

Proof. By Corollary 8.15, it suffices to consider the case $B = A' = R'[X]$. Let $\mathfrak{p}'$ be a prime of A' over $\mathfrak{p}$, and let $\mathfrak{p}'_0 = R' \cap \mathfrak{p}'$. Then $\mathfrak{q}' = \mathfrak{p}'_0 A'$ is the required prime.

9. Zariski's Main Theorem. If $\mathcal{P}$ is any property of algebras, we say that an A-algebra B is essentially $\mathcal{P}$ if B is the localization of an A-algebra with the property $\mathcal{P}$. Here are a few trivial facts we will find useful.

(1) If $A \subset C \subset B$ and B is a localization of A then B is a localization of C. (In fact, if $B = A_S$ then $B = A_S \subset C_S \subset B_S = B$).

(2) If $A \subset C \subset B$ and B is essentially integral over A then B is essentially integral over C. (If B is a localization of $D \subset B$ with D integral over A, then, by (1), B is a localization of $CD \subset B$ and CD is integral over C).

(3) $A \subset B$ is essentially finite if and only if it is essentially of finite type and essentially integral.

The 'only if' part is clear. For the converse, let B be a localization of $C \subset B$ with $C = A[c_1, \ldots, c_n]$ of finite type over A, and let B be a localization of $D \subset B$ with D integral over A, say $B = D_S$. We can find $E \subset D$ with E finite over A and $T \subset S$ such that the $c_1, \ldots, c_n$ lie in E_T. Note that $E_T \subset B$ since T consists of units of B. Now $C \subset E_T$ so, by (1), B is a localization of E_T and hence of E.

Theorem 9.1. (Zariski's Main Theorem) *Let $A \subset B$ be a local morphism of quasi-local rings which is essentially of finite type. Suppose that $B/\mathfrak{m}_A B$ is finite over $A/\mathfrak{m}_A$. Then $A \subset B$ is essentially finite.*

Proof. (after Peskine [Pz]. See also [Ez], [I], and [R]).We first reduce to the following lemma. Throughout this section, extensions given as $A \subset A[t]$, etc. are not assumed to be polynomial extensions.

Lemma 9.2. *Let $A \subset B$ be a local inclusion of quasi-local rings with A integrally closed in B. Suppose that $A \subset A[t] \subset B$ with B essentially finite over $A[t]$. If $B/\mathfrak{m}_A B$ is finite over $A/\mathfrak{m}_A$, then $A = B$.*

To deduce the theorem, note that we have $A \subset A[t_1, \ldots, t_n] \subset B$ with B essentially integral over $A[t_1, \ldots, t_n]$. If $n = 0$, the result is clear by (3). If $n > 0$, let A' be the integral closure of $A[t_1, \ldots, t_{n-1}]$ in B, let $P = \mathfrak{m}_B \cap A'$ and let $A'' = A'_P$. Then the lemma applies to $A'' \subset A''[t_n] \subset B$ since B is essentially finite over $A''[t_n]$ by (3). Therefore $B = A''$ which is essentially integral over $A[t_1, \ldots, t_{n-1}]$ and the theorem follows by induction on n.

Lemma 9.3. *Let R be quasi-local with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let $R \subset R[t]$. If R is integrally closed in $R[t]$, then either $R[t] = R_r$, a localization of R, or $R[t]/\mathfrak{m}R[t] = k[T]$ with T, the image of t, being transcendental over k.*

Proof. Assume that T is not transcendental over k. Then there is a polynomial $f(X)$ over R such that $f(t)$ lies in $\mathfrak{m}R[t]$ and such that $\bar{f}$, the reduction of f mod $\mathfrak{m}$, is non-zero. We can write $f(t) = g(t)$ where all coefficients of g are in $\mathfrak{m}$, and replace f by $f - g$ so that $f(t) = 0$. If f has degree 0, it is a unit of R which is nonsense. If $f = rX + s$ has degree 1, either $r \notin \mathfrak{m}$ so that $R[t] = R$ or $s \notin \mathfrak{m}$ so that $R[t]$ is a quotient of $R[X]/(rX + s) = R_r$. But then $R[t] = R_r/I_r$ and $I = 0$ since $R \subset R[t]$.

If $\deg f = n > 1$, we use induction on n. Let $f = aX^n + bX^{n-1} + \ldots$. If $a \notin \mathfrak{m}$, then t is integral over R so $R[t] = R$. If $a \in \mathfrak{m}$ then at is integral over R and so lies in R. If $b \notin \mathfrak{m}$ but $at + b = c \in \mathfrak{m}$, then $at + b - c = 0$ gives an equation of degree 1. Otherwise $(at + b)t^{n-1} + \cdots = 0$ gives an equation of lower degree.

Proof of Lemma 9.2. We have $A \subset A[t] \subset C \subset B$ with A integrally closed in B, $B = C_P$, and C finite over $A[t]$. Let $\mathfrak{f}$ be the conductor of $A[t] \subset C$. If $\mathfrak{f} \not\subset P$, let $r \in \mathfrak{f} - P$. Then $C_r = A[t]_r$ so B is a localization of $A[t]$. If $A[t]$ is a localization of A, so is B hence $B = A$ since $A \subset B$ is local. If not, $B/\mathfrak{m}_A B$ is a localization of $k[T]$ by Lemma 9.3 which is impossible if $B/\mathfrak{m}_A B$ is finite over $A/\mathfrak{m}_A$.

There remains the case $\mathfrak{f} \subset P$ in which we use the following result.

Lemma 9.4. *Let $R \subset R[t] \subset D$ with R integrally closed in D and with D finite over $R[t]$. Let $\mathfrak{f}$ be the conductor of $R[t] \subset D$. Let $f(X) = aX^n + \cdots \in R[X]$ be such that $f(t)$ lies in $\mathfrak{f}$. Then some power a^N lies in $\mathfrak{f}$.*

Proof. Note that some a^N lies in $\mathfrak{f}$ if and only if $R[t]_a = D_a$ since D is finite over $R[t]$. Therefore, we can localize with respect to a and so assume that f is monic. We must then show that $D = R[t]$. Let $x \in D$. Then $f(t)x$ lies in $R[t]$ so $f(t)x = g(t)$ for some g in $R[X]$. Write $g = fq + r$ with $\deg r < \deg f$. Let $y = x - q(t)$. Then $f(t)y = r(t)$. Let $\bar{D} = D_y$ and let $\bar{R}$, $\bar{t}$,$\bar{y}$ be the images of R, t, y in $\bar{D}$. The equation $f(\bar{t}) = \bar{y}^{-1}r(\bar{t})$ shows that $\bar{t}$ is integral over $\bar{R}[\bar{y}^{-1}]$. But $\bar{y}$ is integral over $\bar{R}[\bar{t}]$ and therefore over $\bar{R}[\bar{y}^{-1}]$. It follows that $\bar{y}$ is integral over $\bar{R}$. If $\bar{y}^n + \bar{a}_1\bar{y}^{n-1} + \cdots = 0$, then, for some M, $y^M(y^n + a_1 y^{n-1} + \ldots) = 0$ showing that y is integral over R. Therefore $y \in R$ and $x = y + q(t)$ lies in $R[t]$.

Returning to the proof of Lemma 9.2, we must consider the case in which $\mathfrak{f} \subset P$. Let $Q \subset P$ be a prime of C minimal over $\mathfrak{f}$. Let $\mathfrak{q} = A \cap Q$ and let $\bar{A} = A/\mathfrak{q}$, $\bar{C} = C/Q$ so that $\bar{A} \subset \bar{A}[\bar{t}] \subset \bar{C}$. We claim that $\bar{t}$ is transcendental over $\bar{A}$. If not, let $f(X) = aX^n + \ldots$ be a polynomial with $a \in A - \mathfrak{q}$ such that $f(t) \in Q$. Since Q is minimal over $\mathfrak{f}$, there is an element s in $C - Q$ such that $sf(t)^N \in \mathfrak{f}$. Therefore, $f(t)^N$ lies in the conductor of $A[t] \subset D = A[t][sC] = A[t] + sC$ which is finite over $A[t]$. By Lemma 9.4, some a^M lies in this conductor and so sa^M lies in $\mathfrak{f}$. Since $\mathfrak{f} \subset Q$, a lies in Q and so in $\mathfrak{q}$, contradicting our choice of a.

We now have $\bar{A} \subset \bar{A}[\bar{t}] \subset \bar{C} \subset \bar{B}$. where $\bar{B} = \bar{C}_{\bar{P}}$ with $\bar{P} = P/Q$. Let $\mathfrak{p} = \bar{A}[\bar{t}] \cap \bar{P}$ and let $\mathfrak{p}_0 = \bar{A} \cap \bar{P} = \mathfrak{m}_{\bar{A}}$. Then $\mathfrak{p}_0[\bar{t}] < \mathfrak{p}$ otherwise $\bar{B}/\mathfrak{m}_{\bar{B}} = B/\mathfrak{m}_B$ would contain the polynomial ring $A/\mathfrak{m}_A[\bar{t}]$ and would not be finite over $A/\mathfrak{m}_A$. By Corollary 8.16, there is a prime ideal $\bar{P}'$ of $\bar{C}$ contained in $\bar{P}$ and lying over $\mathfrak{p}_0[\bar{t}]$. We have $\mathfrak{m}_{\bar{A}}\bar{C} \subset \bar{P}' < \bar{P}$ showing that $\bar{B}/\mathfrak{m}_{\bar{A}}\bar{B}$, a quotient of $B/\mathfrak{m}_A B$, has Krull dimension at least 1. Therefore $B/\mathfrak{m}_A B$ cannot be finite over $A/\mathfrak{m}_A$ showing that the case $\mathfrak{f} \subset P$ cannot occur.

10. Unramified extensions. We say that a local morphism $R \to A$ of quasi-local rings is unramified if it is essentially of finite type, $\mathfrak{m}_R A = \mathfrak{m}_A$, and $A/\mathfrak{m}_A$ is a finite separable extension of $R/\mathfrak{m}_R$. The following characterization appears in [SGAI] (see also [R]).

Theorem 10.1. *Let $R \to A$ be an unramified local morphism. Then there is an R-algebra $D = (R[X]/f(X))_P$ with $f(X)$ monic such that $f'(X) \notin P$, and a surjection $D \twoheadrightarrow A$ such that $D/\mathfrak{m}_R D \xrightarrow{\approx} A/\mathfrak{m}_A$.*

We first prove an analogous result without assuming separability.

Lemma 10.2. *Let $R \to A$ be a local morphism which is essentially of finite type. Suppose that $\mathfrak{m}_R A = \mathfrak{m}_A$ and that $K = A/\mathfrak{m}_A$ is a finite extension of $k = R/\mathfrak{m}_R$ with one generator $K = k(\alpha)$. Then there is an R-algebra $D = (R[X]/g(X))_P$ with $g(X)$ monic and a surjection $D \twoheadrightarrow A$, with X mapping to α in K, such that $D/\mathfrak{m}_R D \xrightarrow{\approx} A/\mathfrak{m}_A$.*

We can assume that $\alpha \neq 0$ since if $\alpha = 0$, we can take $\alpha = 1$ and then replace X by $X - 1$. We first investigate the artinian case.

Lemma 10.3. *Let Λ be a finite dimensional commutative algebra over a field k. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be the maximal ideals of Λ and let $\Lambda_i = \Lambda_{\mathfrak{m}_i}$. Then $\Lambda \xrightarrow{\approx} \Lambda_1 \times \cdots \times \Lambda_n$. If $\Lambda_1 = k(\alpha)$ is a field (with $\alpha \neq 0$) let $\gamma = (\alpha, 0, \dots, 0) \in \Lambda_1 \times \cdots \times \Lambda_n$, let $\Gamma = k[\gamma] \subset \Lambda$, and let $\mathfrak{n} = \Gamma \cap \mathfrak{m}_1$. Then $\Gamma_{\mathfrak{n}} = \Lambda_{\Gamma - \mathfrak{n}} = \Lambda_1$.*

Proof. The first statement is, of course, a classical theorem on commutative artinian rings. To prove it, it is enough to check that the map is a local isomorphism but this is clear since all but one of the Λ_i vanish under localization at a maximal ideal. For the second statement, let f be the minimal polynomial of α over k. Then $f(\gamma) = (f(\alpha), f(0), \dots, f(0)) = (0, f(0), \dots, f(0))$ lies in $\mathfrak{m}_1$ and therefore in $\mathfrak{n}$. Since $f(0) \neq 0$, $f(\gamma) - f(0)$ lies in $\Gamma - \mathfrak{n}$ as well as in all $\mathfrak{m}_i$ with $i \neq 1$. Therefore $\Lambda_{\Gamma - \mathfrak{n}}$ is local and hence must be Λ_1. Since Γ maps onto Λ_1 and $\Gamma_{\mathfrak{n}} \subset \Lambda_{\Gamma - \mathfrak{n}} = \Lambda_1$, we have $\Gamma_{\mathfrak{n}} = \Lambda_1$.

Proof of Lemma 10.2. By Zariski's Main Theorem, A is a localization $A = B_P$ of a finite R-algebra B. Note that P is maximal since it lies over $\mathfrak{m}_R$. Let $\Lambda = B/\mathfrak{m}_R B$ and $\mathfrak{m}_1 = P/\mathfrak{m}_R B$. Find γ as in Lemma 10.3 and lift it to an element $x \in B$. Let $C = R[x]$ and $Q = P \cap C$. Note that C is finite over R since x is integral over R. Clearly C maps to Γ in $\Lambda = B/\mathfrak{m}_R B$, Q maps to $\mathfrak{n}$, and $C - Q$ to $\Gamma - \mathfrak{n}$. The map $C_Q \to B_{C-Q}$ is finite and is surjective mod $\mathfrak{m}_R$ since C_Q maps onto $\Gamma_{\mathfrak{n}} = \Lambda_{\Gamma - \mathfrak{n}} = B_{C-Q}/\mathfrak{m}_R B_{C-Q}$. Therefore $C_Q = B_{C-Q}$ by Nakayama's lemma. Since $C_Q \to A$ is local and A is a localization of $C_Q = B_{C-Q}$, we see that $C_Q = A$.

Let $1, \bar{x}, \dots, \bar{x}^{r-1}$ be a base for $C/\mathfrak{m}_R C$ over k (choose r maximal such that these elements are linearly independent). Then $1, x, \dots, x^{r-1}$ generate C over R by Nakayama's lemma. Let $g(x) = x^r + a_1 x^{r-1} + \cdots + a_r = 0$. We get $\varphi : R[X]/g(X) \twoheadrightarrow C$ so if $P' = \varphi^{-1}(Q)$, then $D = (R[X]/g(X))_{P'} \twoheadrightarrow A$. Since $k[X]/\bar{g}(X) = C/\mathfrak{m}_R C$ we see that $D/\mathfrak{m}_R D = C_Q/\mathfrak{m}_R C_Q = A/\mathfrak{m}_R A = K$ as required. Note that X maps to γ and therefore to α in K.

Proof of Theorem 10.1. Here K/k is finite separable so $K = k(\alpha)$. By Lemma 10.2, we get a surjection $D = (R[X]/g(X))_P \twoheadrightarrow A$, with $X \mapsto \alpha$ such that $D/\mathfrak{m}_R D \xrightarrow{\approx} K = A/\mathfrak{m}_A$. Write $C = R[X]/g(X)$. Let $\bar{f}(X) = 0$ be the minimal equation for α over k. Since $\bar{g}(\alpha) = 0$, $\bar{f}$ divides $\bar{g}$. Write $\bar{g} = \bar{f}^e \bar{h}$ where $\bar{f}$ does not divide $\bar{h}$ so $\bar{h}(\alpha) \neq 0$. Therefore $\bar{C} = C/\mathfrak{m}_R C = k[X]/\bar{g}(X) = k[X]/\bar{f}^e(X) \times k[X]/\bar{h}(X)$. The first factor must be K since it is the only factor in which $f(X)^e$ maps to 0. Therefore $e = 1$. We now have $\bar{g} = \bar{f}\bar{h}$ and $\bar{g}' = \bar{f}'\bar{h} + \bar{f}\bar{h}'$. Therefore $\bar{g}'(\alpha) = \bar{f}'(\alpha)\bar{h}(\alpha) \neq 0$ showing that $g'(X)$ does not lie in P.

Corollary 10.4. *Let $\varphi : R \to A$ be a local morphism of quasi-local rings which is essentially finitely presented. Then the following are equivalent.*

(1) *φ is essentially étale.*
(2) *φ is flat and unramified*
(3) *$A = (R[X]/f(X))_P$ with $f(X)$ monic and $f'(X) \notin P$.*

Proof. It is clear that (3) implies (1) and the flatness of f. If (1) holds then $k = R/\mathfrak{m}_R \to A/\mathfrak{m}_R A = k \otimes_R A$ is essentially étale so $k \otimes_R A$ which is local, must be a finite separable extension K of k by Corollary 5.3. Therefore $R \to \Lambda$ is unramified. It follows that (3) implies (2) also. Suppose that (2) holds. By Theorem 10.1, we can find $D = (R[X]/f(X))_P$ with $f(X)$ monic and $f'(X) \notin P$, and a surjection $D \twoheadrightarrow A$ such that $D/\mathfrak{m}_R D \xrightarrow{\approx} A/\mathfrak{m}_A = A/\mathfrak{m}_R A$. Write $A = D/I$. Note that I is finitely generated since A is essentially finitely presented over R. We have $0 \to I \to D \to A \to 0$. Since A is flat over R, we get $0 \to I/\mathfrak{m}_R I \to D/\mathfrak{m}_R D \xrightarrow{\approx} A/\mathfrak{m}_R A \to 0$ showing that $I/\mathfrak{m}_R I = 0$ and hence that $I/\mathfrak{m}_D I = 0$. Since I is finitely generated, $I = 0$ and (3) holds.

Finally, suppose (1) holds. We saw above that $R \to A$ is then unramified. As before we get $0 \to I \to D \to A \to 0$. The JZ sequence gives us $\Gamma_{A/R} \to \Gamma_{A/D} \to A \otimes \Omega_{D/R}$. Since A and D are essentially étale over R, $\Gamma_{A/R} = 0 = \Omega_{D/R}$. Since $\Gamma_{A/D} = I/I^2$, we get $I/I^2 = 0$ and therefore $I = 0$.

Proof of Theorem 2.5. Let C be a local R-algebra essentially smooth over R. Then we must show that $C = (R[T_1, \dots, T_n, Y]/(f(T, Y)))_P$ where f is monic in Y and $\partial f/\partial Y \notin P$. Suppose that $C = R[X_1, \dots, X_N]_P/I_P$. Since $H_{C/R} \not\subset P$ we can find $f_1, \dots, f_n \in I$ such that $I_P = (f_1, \dots, f_n)_P$ and, after renumbering the X_i, $\det|\partial f_i/\partial X_j|_{1 \leq i,j \leq n} \notin P$. Let $A = R[X_{n+1}, \dots, X_N]$ and let $Q = A \cap P$. Then $C = A_Q[X_1, \dots, X_n]_P/(f_1, \dots, f_n)_P$ which is essentially étale over A_Q by example (5) of §1. By Corollary 10.4, we can write $C = (A_Q[Y]/g(Y))_{\mathfrak{P}}$ with $g(Y)$ monic and $g'(Y) \notin \mathfrak{P}$. If s is a common denominator for the coefficients of g then $s^m g(Y) = f(sY)$ where $f(Y) \in A[Y]$ is monic. If $Z = sY$, we can write $C = (A[Z]/f(Z))_{\mathfrak{P}}$ which has the required form.

Corollary 10.5. *Let $f : R \to A$ be a flat local map of noetherian local rings which is essentially of finite type. Suppose that $\mathfrak{m}_R A = \mathfrak{m}_A$ and that the residue field K of A is separable over the residue field F of R. Then A is essentially smooth over R.*

Proof. Since K is of finite type over F, it has a separating transcendence base $\{\alpha_1, ..., \alpha_n\}$ over F. Let $R' = R[X_1, ..., X_n] \to A$ send X_i to an element a_i lifting α_i. Let P be the inverse image in R' of $\mathfrak{m}_A$ and let $R'' = R'_P$. Then A is flat over R'' by Lemma 7.8. The residue field K of A is finite separable over that of R'' so $R'' \to A$ is essentially étale by Corollary 10.4 and R'' is clearly essentially smooth over R.

PART III. PROOF OF POPESCU'S THEOREM

11. Preliminary reductions. Let $R \to \Lambda$ be a geometrically regular homomorphism of noetherian rings, and let $R \to A \to \Lambda$ with A of finite type over R. The theorem asserts that we can find $R \to A \to B \to \Lambda$ where B is smooth over R. Define $\mathfrak{h}_A = \sqrt{H_{A/R}\Lambda}$. We will proceed by noetherian induction on this ideal. We write $\mathfrak{h}_{A/R}$ for $\mathfrak{h}_A$ when it is necessary to specify R.

Lemma 11.1. *The theorem is true if* $\mathfrak{h}_A = \Lambda$.

Proof. Let $H_{A/R} = (a_1, \ldots, a_n)$. Then $\sum \Lambda a_i = \Lambda$ so we can write $\sum \lambda_i a_i = 1$. Let
A $B = \cancel{R}[X_1, \ldots, X_n]/(\sum a_i X_i - 1)$ and map B to Λ by sending X_i to λ_i. Then we have $R \to A \to B \to \Lambda$ and B is smooth over R since for each i, $B_{a_i} = A_{a_i}[X_1, \ldots, \hat{X}_i, \ldots, X_n]$ which is smooth over R so $a_i \in H_{B/R}$ for each i showing that $H_{B/R} = B$.

We now choose B of finite type over R with $R \to A \to B \to \Lambda$ so that $\mathfrak{h}_B$ is maximal and we claim that $\mathfrak{h}_B = \Lambda$. Suppose this is not so. Let $\mathfrak{P}$ be a prime ideal of Λ which is minimal over $\mathfrak{h}_B$. It will then suffice to find $R \to B \to C \to \Lambda$ with C of finite type over R such that $\mathfrak{h}_B \subset \mathfrak{h}_C \not\subset \mathfrak{P}$.

Remark. Let $u : R \to \Lambda$ be the given map and let $\mathfrak{a} = u^{-1}(\mathfrak{h}_B)$. Let $\mathfrak{p}$ be minimal over $\mathfrak{a}$. Then we can choose $\mathfrak{P}$ minimal over $\mathfrak{h}_B$ such that $u^{-1}(\mathfrak{P}) = \mathfrak{p}$.

Proof. Let $\mathfrak{h}_B = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_m$. Then $\mathfrak{a} = u^{-1}(\mathfrak{P}_1) \cap \cdots \cap u^{-1}(\mathfrak{P}_m) \subset \mathfrak{p}$. Therefore some $u^{-1}(\mathfrak{P}_i) \subset \mathfrak{p}$ but $\mathfrak{a} \subset u^{-1}(\mathfrak{P}_i)$ so $u^{-1}(\mathfrak{P}_i) = \mathfrak{p}$.

Therefore it suffices to prove the following.

Theorem 11.2. *Let* $u : R \to \Lambda$ *be a map of noetherian rings and let* $R \to A \to \Lambda$ *with* A *of finite type over* R. *Let* $\mathfrak{P}$ *be a prime ideal of* Λ *such that* $\mathfrak{P}$ *is minimal over* $\mathfrak{h}_A$ *and assume that* $\mathfrak{p} = u^{-1}(\mathfrak{P})$ *is minimal over* $\mathfrak{a} = u^{-1}(\mathfrak{h}_A)$. *Suppose that* $R_{\mathfrak{p}} \to \Lambda_{\mathfrak{P}}$ *is flat and that* $\Lambda_{\mathfrak{P}}/\mathfrak{p}\Lambda_{\mathfrak{P}}$ *is geometrically regular over* $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. *Then we can find* $R \to A \to B \to \Lambda$ *with* B *of finite type over* R *such that* $\mathfrak{h}_A \subset \mathfrak{h}_B \not\subset \mathfrak{P}$.

I will say that $R \to A \to \Lambda \supset \mathfrak{P}$ is resolvable if the conclusion of Theorem ~~11.1~~ holds 11.2
for it. Note that this is trivially true if $\mathfrak{h}_A \not\subset \mathfrak{P}$. The idea of Popescu's proof is to reduce to the case in which $\operatorname{ht}\mathfrak{P} = 0$ by the following method. Let $R \to A \to \Lambda \supset \mathfrak{P}$ satisfy the hypotheses of Theorem 11.2. Let $I \subset \mathfrak{a}$ be an ideal of R and let $\bar{R} = R/I$, $\bar{A} = A/IA$, $\bar{\Lambda} = \Lambda/I\Lambda$, and $\bar{\mathfrak{P}} = \mathfrak{P}/I\Lambda$. If $\mathfrak{h}_{\bar{A}} \subset \bar{\mathfrak{P}}$ then $\bar{R} \to \bar{A} \to \bar{\Lambda} \supset \bar{\mathfrak{P}}$ also satisfies the hypotheses of Theorem 11.2. This is clear for the flatness and regularity assumptions. If we assume that $\mathfrak{h}_{\bar{A}} \subset \bar{\mathfrak{P}}$ then $\bar{\mathfrak{P}}$ is minimal over $\mathfrak{h}_{\bar{A}}$ because $\mathfrak{h}_A\bar{\Lambda} \subset \mathfrak{h}_{\bar{A}} \subset \bar{\mathfrak{P}}$ and $\bar{\mathfrak{P}}$ is minimal over $\mathfrak{h}_A\bar{\Lambda} = \mathfrak{h}_A/I\Lambda$. Similarly $\bar{\mathfrak{p}}$ is minimal over $\bar{\mathfrak{a}} = \bar{u}^{-1}(\mathfrak{h}_{\bar{A}})$ since $\mathfrak{a}\bar{R} \subset \bar{\mathfrak{a}} \subset \bar{\mathfrak{p}}$ and $\bar{\mathfrak{p}}$ is minimal over $\mathfrak{a}\bar{R} = \mathfrak{a}/I\cancel{R}$. If I is chosen so $\operatorname{ht}\bar{\mathfrak{P}} < \operatorname{ht}\mathfrak{P}$ we can assume by induction that $\bar{R} \to \bar{A} \to \bar{\Lambda} \supset \bar{\mathfrak{P}}$ is resolvable. This will also be the case if $\mathfrak{h}_{\bar{A}} \not\subset \bar{\mathfrak{P}}$. We now look for conditions under which the resolution of $\bar{R} \to \bar{A} \to \bar{\Lambda} \supset \bar{\mathfrak{P}}$ implies that of $R \to A \to \Lambda \supset \mathfrak{P}$. Recall the following definition from §4.

Definition. Let A be a finitely presented R-algebra and let a be an element of $H_{A/R}$. We say that a is strictly standard with respect to the presentation $A = R[X]/I$ if a lies in $\Delta(f_1, \ldots, f_r)[(f_1, \ldots, f_r):I]$ for some finite set of elements $f_1, \ldots, f_r$ of I.

If $R \to A$ and a lies in R, I will write $a|A$ for the image of a in A. The following is the main technical lemma needed for the reduction to the case where $\operatorname{ht}\mathfrak{P} = 0$.

Lemma 11.3. *Let $R \to A \to \Lambda$ with A of finite type over R and with R and Λ noetherian. Let a be an element of R. Suppose that*

(1) $\mathrm{Ann}_R(a^2) = \mathrm{Ann}_R(a)$ *and* $\mathrm{Ann}_\Lambda(a^2) = \mathrm{Ann}_\Lambda(a)$.
(2) *$a|A$ is strictly standard.*

Let $c \geq 8$ and let $\bar{R} = R/a^cR$, $\bar{\Lambda} = \Lambda/a^c\Lambda$, etc. Let $\pi : \Lambda \to \bar{\Lambda}$ be the canonical map. Suppose that we have $\bar{R} \to \bar{A} \to \bar{C} \to \bar{\Lambda}$ with $\bar{C}$ of finite type over $\bar{R}$. Then we can find $R \to A \to B \to \Lambda$ with B of finite type over R such that $\pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \mathfrak{h}_B$.

The proof, which is by explicit computation, will be given in §§17 and 18. Note that it will suffice to prove this for the case $c = 8$ since if $\tilde{C} = C/a^8C$, then $H_{\bar{C}/\bar{R}}\tilde{C} \subset H_{\tilde{C}/\tilde{R}}$ by Lemma 4.7 and therefore $\mathfrak{h}_{\bar{C}}$ maps into $\mathfrak{h}_{\tilde{C}}$ under $\bar{\Lambda} \to \tilde{\Lambda} = \Lambda/a^8\Lambda$, showing that $\pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \pi^{-1}(\mathfrak{h}_{\tilde{C}})$ so it will suffice to find B with $\pi^{-1}(\mathfrak{h}_{\tilde{C}}) \subset \mathfrak{h}_B$.

Corollary 11.4. *Let $R \to A \to \Lambda \supset \mathfrak{P}$ with A of finite type over R and with R and Λ noetherian. Let $a \in R$ map to an element of $H_{A/R}$. Let $c \geq 8$ and let $\bar{R} = R/a^cR$, $\bar{\Lambda} = \Lambda/a^c\Lambda$, $\bar{\mathfrak{P}} = \mathfrak{P}/a^c\Lambda$, etc. Suppose that*

(1) $\mathrm{Ann}_R(a^2) = \mathrm{Ann}_R(a)$ *and* $Ann_\Lambda(a^2) = \mathrm{Ann}_\Lambda(a)$.
(2) *$a|A$ is strictly standard.*

If $\bar{R} \to \bar{A} \to \bar{\Lambda} \supset \bar{\mathfrak{P}}$ is resolvable, so is $R \to A \to \Lambda \supset \mathfrak{P}$.

Proof. Let $\bar{R} \to \bar{A} \to \bar{C} \to \bar{\Lambda}$ resolve $\bar{R} \to \bar{A} \to \bar{\Lambda} \supset \bar{\mathfrak{P}}$ so that $\mathfrak{h}_{\bar{A}} \subset \mathfrak{h}_{\bar{C}} \not\subset \bar{\mathfrak{P}}$. Lemma 11.3 gives us $R \to A \to B \to \Lambda$ with $\pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \mathfrak{h}_B$. Note that $\mathfrak{h}_A \subset \pi^{-1}(\mathfrak{h}_{\bar{A}})$ since $H_{A/R}\bar{A} \subset H_{\bar{A}/\bar{R}}$ by Lemma 4.7 so $H_{A/R}\bar{\Lambda} \subset H_{\bar{A}/\bar{R}}\bar{\Lambda}$ and $\mathfrak{h}_A\bar{\Lambda} \subset \mathfrak{h}_{\bar{A}}$. Therefore $\mathfrak{h}_A \subset \pi^{-1}(\mathfrak{h}_{\bar{A}}) \subset \pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \mathfrak{h}_B$. If $\mathfrak{h}_B \subset \mathfrak{P}$, then $\mathfrak{h}_{\bar{C}} = \pi\pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \pi(\mathfrak{P}) = \bar{\mathfrak{P}}$, a contradiction.

In the case where the residue field of $\mathfrak{P}$ has characteristic $p \neq 0$, it will be useful to do the whole reduction in one step using the following result.

Corollary 11.5. *Let $R \to A \to \Lambda$ with A of finite type over R with R and Λ noetherian. Let $a_1, \ldots, a_r$ be elements of R. Let $c = 8e$ with $e \geq 1$ and let $\bar{R} = R/(a_1^c, \ldots, a_r^c)R$, $\bar{\Lambda} = \Lambda/(a_1^c, \ldots, a_r^c)\Lambda$, etc. Suppose that*

(1) *For each i, $(a_1^c, \ldots, a_{i-1}^c){:}a_i^2 = (a_1^c, \ldots, a_{i-1}^c){:}a_i$ in R and in Λ.*
(2) *For each i, $a_i^e|A$ is strictly standard.*

Then if $\bar{R} \to \bar{A} \to \bar{\Lambda} \supset \bar{\mathfrak{P}}$ is resolvable, so is $R \to A \to \Lambda \supset \mathfrak{P}$.

Proof. We can replace each a_i by a_i^e. Therefore we can assume that $c = 8$ and that each $a_i|A$ is strictly standard. For $r = 1$, we are done by Corollary 11.4. Suppose the result is true for $r - 1$. Let $R' = R/(a_1^c, \ldots, a_{r-1}^c)R$ etc. with $a = a_r$. Then Corollary 11.4 applies to $R' \to A' \to \Lambda' \supset \mathfrak{P}'$ and a. Condition (1) is clear and (2) follows from the Lemma 4.8. Therefore Corollary 11.5 follows by induction on r.

Let $a \in \mathfrak{a}$ in the notation of Theorem 11.2. We can force (1) of Lemma 11.3 to hold by replacing a by a suitable power a^N. In order to get (2) to hold, we use the results of §4 and the following lemma.

Lemma 11.6. *Let $R \to A \to \Lambda$ with R noetherian and A of finite type over R. Let $a \in R$ be such that $a|\Lambda \in \mathfrak{h}_A$. Then we can find $R \to A \to B \to \Lambda$ with B of finite type over R such that $a|B \in H_{B/R}$ and such that $H_{A/R}B \subset H_{B/R}$ (so $\mathfrak{h}_A \subset \mathfrak{h}_B$).*

Proof. For some N, $a^N|\Lambda \in H_{A/R}\Lambda$. Let $H_{A/R} = (b_1, \ldots, b_n)$. Then $a^N = \sum \lambda_i b_i$ with the λ_i in Λ. Let $B = A[X_1, \ldots, X_n]/(a^N - \sum_i b_iX_i)$ and map B to Λ by sending X_i to

λ_i. Now $B_{b_i} = A_{b_i}[X_1,\dots,\hat{X}_i,\dots,X_n]$ which is smooth over R so $H_{A/R}B \subset H_{B/R}$ and a^N (and hence a) lies in $H_{B/R}$.

Corollary 11.7. *Under the same hypotheses we can find* $R \to A \to C \to \Lambda$ *where* C *is of finite type over* R*,* $H_{A/R}C \subset H_{C/R}$*, and* $a|C$ *is standard with respect to some presentation of* C.

Proof. Apply Proposition 4.6 to $R \to B$ getting $R \to B \to C$ with $H_{B/R}C \subset H_{C/R}$ and with $a|C$ standard. Since B is a retract of C, $B \to \Lambda$ extends to $C \to \Lambda$.

It follows that for some N, $a^N|C$ is strictly standard.

12. Relation to the case of height 0. The results of §11 will be applied to reduce the problem to the case in which $\operatorname{ht}\mathfrak{p} = \operatorname{ht}\mathfrak{P} = 0$. For $\mathfrak{p}$ this is easily done.

Lemma 12.1. *It is sufficient to prove Theorem 11.2 for the case in which* $\operatorname{ht}\mathfrak{p} = 0$.

Proof. Suppose that $\operatorname{ht}\mathfrak{p} > 0$. Since $\mathfrak{p}$ is minimal over $\mathfrak{a}$, we can find $a \in \mathfrak{a}$ such that a lies in no height 0 prime contained in $\mathfrak{p}$. Therefore $\operatorname{ht}\mathfrak{p}/(a) < \operatorname{ht}\mathfrak{p}$. By Corollary 11.7, we can find $R \to A \to C \to \Lambda$ with $a|C$ standard and $\mathfrak{h}_A \subset \mathfrak{h}_C$. If $\mathfrak{h}_C \not\subset \mathfrak{P}$ we have succeeded in resolving $R \to A \to \Lambda \supset \mathfrak{P}$. Otherwise, $\mathfrak{P}$ is minimal over $\mathfrak{h}_C$ and $\mathfrak{p}$ is minimal over $u^{-1}(\mathfrak{h}_C)$. After replacing a by a suitable power a^N we can apply Corollary 11.4 to $R \to C \to \Lambda \supset \mathfrak{P}$. By induction on $\operatorname{ht}\mathfrak{p}$, $\bar{R} \to \bar{C} \to \bar{\Lambda} \supset \bar{\mathfrak{P}}$ is resolvable, and therefore so is $R \to C \to \Lambda \supset \mathfrak{P}$. We get $R \to C \to D \to \Lambda \supset \mathfrak{P}$, and $R \to A \to D \to \Lambda \supset \mathfrak{P}$ then gives the required resolution.

To reduce to the case $\operatorname{ht}\mathfrak{P} = 0$, we will adjoin indeterminates to R which map to a system of parameters of $\Lambda_{\mathfrak{P}}$. This will be done later. Once we have reduced to the case $\operatorname{ht}\mathfrak{P} = 0$, we can reduce the proof to the artinian local case by the following lemmas [P1].

Lemma 12.2. *Let* $R \to A \to \Lambda \supset \mathfrak{P}$ *with* $\mathfrak{P}$ *minimal over* $\mathfrak{h}_A$*. Let* $\mathfrak{p} = u^{-1}(\mathfrak{P})$ *where* $u : R \to \Lambda$*. If* $R_{\mathfrak{p}} \to A_{R-\mathfrak{p}} \to \Lambda_{\mathfrak{P}} \supset \mathfrak{P}\Lambda_{\mathfrak{P}}$ *is resolvable, then we can find* $R \to A \to C \to \Lambda \supset \mathfrak{P}$ *with* $\mathfrak{h}_C \not\subset \mathfrak{P}$.

Note that we do not get $\mathfrak{h}_A \subset \mathfrak{h}_C$ in this generality.

Proof. Write $S = R - \mathfrak{p}$. We can find $R_{\mathfrak{p}} \to A_S \to B \to \Lambda_{\mathfrak{P}}$ with $\mathfrak{h}_B \not\subset \mathfrak{P}\Lambda_{\mathfrak{P}}$ so by Lemma 11.1, we can even assume B smooth over $R_{\mathfrak{p}}$. Let $B = A_S[X_1,\dots,X_n]/(F_1,\dots,F_m)$ and suppose that X_i maps to z_i/s in $\Lambda_{\mathfrak{P}}$. We can also assume that the coefficients of the F_i lie in A. For large N we get homogeneous polynomials $G_i(Y,T) = T^N F_i(Y/T)$ of positive degree such that $G_i(z,s) = 0$ in $\Lambda_{\mathfrak{P}}$. Find $u \in \Lambda - \mathfrak{P}$ such that $uG_i(z,s) = 0$ in Λ. Let $t = us$ and $y_i = uz_i$. Then X_i maps to y_i/t in $\Lambda_{\mathfrak{P}}$ and $G_i(y,t) = 0$ in Λ. Let $C = A[Y,T]/(G_1,\dots,G_m)$ and map C to Λ by sending Y_i to y_i and T to t. Then $C_{ST} = A_S[Y,T,T^{-1}]/(G_1,\dots,G_m) = A_S[X,T,T^{-1}]/(F_1,\dots,F_m) = B[T,T^{-1}]$ which is smooth over R_S. Therefore $T \in H_{C_S/R_S} = (H_{C/R})_S$ so there is some $r \in S$ such that $rT \in H_{C/R}$. The image of rT in Λ is rt which does not lie in $\mathfrak{P}$ so $H_{C/R}\Lambda \not\subset \mathfrak{P}$.

Lemma 12.3. *Let* $R \to A \to \Lambda \supset \mathfrak{P}$ *with* $\mathfrak{P}$ *minimal over* $\mathfrak{h}_A$*. Let* $\mathfrak{p} = u^{-1}(\mathfrak{P})$ *where* $u : R \to \Lambda$*. If* $\operatorname{ht}\mathfrak{P} = 0$ *and if* $R_{\mathfrak{p}} \to A_{R-\mathfrak{p}} \to \Lambda_{\mathfrak{P}} \supset \mathfrak{P}\Lambda_{\mathfrak{P}}$ *is resolvable, then so is* $R \to A \to \Lambda \supset \mathfrak{P}$.

Proof. Since $\operatorname{ht}\mathfrak{P}$ is 0, $\mathfrak{h}_A\Lambda_{\mathfrak{P}}$ is nilpotent so we can find $z \in \Lambda - \mathfrak{P}$ and N such that $z(\mathfrak{h}_A)^N = 0$. Let $H_{A/R} = (a_1,\dots,a_r)$ and let w_i be the image of a_i in Λ. Let $y_i = w_i^N$ so that $zy_i = 0$. Let C be as in Lemma 12.2 and write $C = A[X_1, \dots, X_n]/(F_1, \dots, F_m)$. Let $D = A[X, Y, T, Z]/(F_j - \sum_i Y_i T_{ij}, ZY_i)$ and map D to Λ by sending Y_i to y_i, T_{ij} to 0, Z to z, and X_i as in $C \to \Lambda$. Now D_{Y_i} is a polynomial ring over $A[Y_i, Y_i^{-1}]$ and so is smooth over A. Therefore, $D_{a_i Y_i}$ is smooth over A_{a_i} and so over R, showing that $a_i Y_i \in H_{D/R}$. The image in Λ is $w_i y_i = w_i^{N+1} = \operatorname{im} a_i^{N+1}$. Therefore $\mathfrak{h}_A \subset \mathfrak{h}_D$. But $D_Z = C[Z, Z^{-1}, T]$ is smooth over C. By Lemma 12.2, there is some $s \in H_{C/R}$ which maps to an element of $\Lambda - \mathfrak{P}$. Therefore Zs which lies in $H_{D/R}$ maps to an element of $\Lambda - \mathfrak{P}$, showing that $\mathfrak{h}_D \not\subset \mathfrak{P}$.

13. The case of characteristic 0. Let $R \to A \to \Lambda \supset \mathfrak{P}$ be as in Theorem 11.2 and assume that $\operatorname{ht} \mathfrak{p} = 0$. We consider here the case in which the residue field F of $R_{\mathfrak{p}}$ is of characteristic 0. Since $\mathfrak{P}$ is minimal over $\mathfrak{h}_A$ which is a radical ideal, $\mathfrak{h}_A \Lambda_{\mathfrak{P}} = \mathfrak{P}\Lambda_{\mathfrak{P}}$. In particular, the image of $\mathfrak{h}_A$ in $\Lambda_{\mathfrak{P}}/\mathfrak{p}\Lambda_{\mathfrak{P}}$ generates the maximal ideal so we can find $\xi \in \mathfrak{h}_A$ mapping to a regular parameter of $\Lambda_{\mathfrak{P}}/\mathfrak{p}\Lambda_{\mathfrak{P}}$. Extend the map $u : R \to \Lambda$ to $u' : R' = R[X] \to \Lambda$ by sending X to ξ. Let $\mathfrak{p}' = u'^{-1}(\mathfrak{P}) = (\mathfrak{p}, X)$. Then $R'_{\mathfrak{p}'} \to \Lambda_{\mathfrak{P}}$ is flat by Lemma 7.7 and $\Lambda_{\mathfrak{P}}/\mathfrak{p}'\Lambda_{\mathfrak{P}}$ is regular and therefore geometrically regular over F which is of characteristic 0. Consider $R[X] \to A[X] \to \Lambda \supset \mathfrak{P}$. By Lemma 4.7, $H_{A/R}A[X] \subset H_{A[X]/R[X]}$ so $\xi \in \mathfrak{h}_{A/R} \subset \mathfrak{h}_{A[X]/R[X]}$. By Corollary 11.7, we can find $R' = R[X] \to A[X] \to C \to \Lambda \supset \mathfrak{P}$ such that the image of X in C is standard. Let $a = X^N$ where N is large enough so that a satisfies the hypotheses of Corollary 11.4. It then follows that it will suffice to resolve $\bar{R}' \to \bar{C} \to \bar{\Lambda} \supset \bar{\mathfrak{P}}$ where $\bar{R}' = R'/a^8 R'$ etc. Since a is regular on R', it is also regular on $\Lambda_{\mathfrak{P}}$ which is flat over R' and therefore $\operatorname{ht} \bar{\mathfrak{P}} < \operatorname{ht} \mathfrak{P}$. By induction on $\operatorname{ht} \mathfrak{P}$, we can therefore reduce to the case $\operatorname{ht} \mathfrak{P} = 0$. By Lemma 12.3 we can then reduce to the case in which R and Λ are artinian local. In this case, $\Lambda/\mathfrak{m}_R\Lambda$ is regular artinian and therefore a field, showing that $\mathfrak{m}_R\Lambda = \mathfrak{m}_\Lambda$. The following lemma, together with Corollary 3.9, then finishes the proof.

Lemma 13.1. *Let $u : R \to \Lambda$ be a flat local map of artinian local rings with residue fields of characteristic* 0. *Assume that $\mathfrak{m}_R\Lambda = \mathfrak{m}_\Lambda$. Then Λ is the filtered union of local subrings which are essentially smooth over R.*

To prove this we first recall a bit of the Cohen structure theorem.

Lemma 13.2. *Let A be a quasi-local ring with maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^n = 0$ for some n. Suppose that $K = A/\mathfrak{m}$ has characteristic* 0. *Let $E \subset K$ be a subfield and let $s : E \to A$ be a ring homomorphism which is a section i.e. $E \to A \to K$ is the inclusion of E in K. Then s extends to a section $K \to A$.*

Equivalently, if $F \subset A$ is a subfield then there is a subfield L with $F \subset L \subset A$ such that L maps isomorphically onto K. In particular, the ring A contains a Cohen subfield, i.e. a subfield L which maps isomorphically onto K. It follows that if $\mathfrak{m} = (x_1, \dots, x_r)$, then $A = L[x_1, \dots, x_r]$ since each $\mathfrak{m}^m/\mathfrak{m}^{m+1}$ is spanned over L by monomials in the x_i. Since the x_i are nilpotent, A will also be finite over L.

Proof. Choose (E, s) maximal among sections. If $E \neq K$, let $x \in K - E$. Let F be the image of E in A. If x is transcendental over E, let $y \in A$ lift x, define $s : E[x] \approx F[y]$ by sending x to y, and extend to $E(x) \approx F(y)$. If x is algebraic over E, let f be its minimal polynomial. Then $f'(x) \neq 0$ since we are in characteristic 0. Let $y \in A$ lift x. If $f(y) \in \mathfrak{m}^r$, then $y' = y - f(y)/f'(y)$ lifts x and $f(y') \in \mathfrak{m}^{2r}$. Eventually we find a lift z with $f(z) = 0$ and extend s by sending x to z.

Proof of Lemma 13.1. Let $F \subset K$ be the residue fields of R and of Λ. By Lemma 13.2, we can map F into R and extend to a map of K into Λ. Let $\mathfrak{P}$ be the maximal ideal of Λ and let $\lambda_1, \ldots, \lambda_r$ be a set of generators of $\mathfrak{P}$ which includes a set of generators of $\mathfrak{p} = \mathfrak{m}_R$. Then $K[X_1, \ldots, X_r] \rightarrow \Lambda$ sending X_i to λ_i is onto so we have $\Lambda = K[X_1, \ldots, X_r]/(F_1, \ldots, F_s)$. Since the λ_i are nilpotent, we can assume that some power of each X_i occurs among the F_j. Let E be any subfield of K of finite type over F and containing the coefficients of the F_i. Let $D = E[X_1, \ldots, X_r]/(F_1, \ldots, F_s)$. Then D is local with nilpotent maximal ideal $(X_1, \ldots, X_r)$ and $K \otimes_E D = \Lambda$. This shows that Λ is flat over D and therefore faithfully flat since $D \rightarrow \Lambda$ is local. It follows that $D \subset \Lambda$. Also $R \subset D$ since D contains F and a set of generators of $\mathfrak{m}_R$. Since $R \rightarrow \Lambda$ is flat, it follows that $R \rightarrow D$ is also flat. We have $\mathfrak{m}_R D \subset \mathfrak{m}_D$. Since Λ is faithfully flat over D and $\mathfrak{m}_\Lambda = \mathfrak{m}_R D\Lambda \subset \mathfrak{m}_D\Lambda \subset \mathfrak{m}_\Lambda$, we see that $\mathfrak{m}_R D = \mathfrak{m}_D$. Therefore D is essentially smooth over R by Corollary 10.5. It is clear that Λ is the filtered union of the subrings D.

14. Cohen subrings. We will give here a very explicit proof of the Cohen structure theorems following [BIV] and André's notes [A5]. Most of the results will only be stated for the case of a nilpotent maximal ideal which is the one actually needed in the proof of Popescu's theorem. The full Cohen structure theorem is proved in [BIV] using these methods.

Definition. Let $p > 0$ be a prime. An artinian p-ring is a quasi-local ring R whose maximal ideal $\mathfrak{m}$ is nilpotent and such that $\mathfrak{m} = pR$. The length $\ell(R)$ is defined to be the least n such that $\mathfrak{m}^n = 0$.

A non-artinian p-ring is a complete discrete valuation ring whose maximal ideal is generated by p. We set $\ell(R) = \infty$. Only the artinian case will be needed here.

Lemma 14.1. *Let R be a p-ring and let I be an ideal of R. Then $I = (p^n)$ for some $n \leq \ell(R)$.*

Proof. If $I = 0$ then $n = \ell(R)$. If not, let n be maximal such that $I \subset (p^n)$. Then $I = p^n J$ where $J = \{x | p^n x \in I\}$. But $J \not\subset \mathfrak{m}$ so $J = R$.

In particular, this shows that the length as defined above has its usual meaning.

Lemma 14.2. *Let R be a p-ring and let $m \leq \ell = \ell(R)$. Then the annihilator of (p^m) is $(p^{\ell-m})$.*

Proof. It must be (p^s) for some s but $(p^s p^m) = 0$ if and only if $s + m \geq \ell$.

Corollary 14.3. *If R is a p-ring and $m < \ell = \ell(R)$, then $R/(p^m)$ has a free resolution of the form* $\cdots \rightarrow R \xrightarrow{p^{\ell-m}} R \xrightarrow{p^m} R \xrightarrow{p^{\ell-m}} R \xrightarrow{p^m} R \rightarrow R/(p^m) \rightarrow 0$.

Proposition 14.4. *Let $R \rightarrow R'$ be a ring homomorphism of p-rings. If $\ell(R) = \ell(R')$, then R' is faithfully flat over R. In particular, this is true if $R \subset R'$.*

Proof. Use the resolution of Corollary 14.3 to compute $\mathrm{Tor}_i^R(R/I, R') = 0$ for $i > 0$. The faithfulness is then clear since R and R' are local.

Definition. Let A be a quasi-local ring with maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^n = 0$ for some n. Suppose that $K = A/\mathfrak{m}$ has characteristic p. A Cohen subring R of A is a subring which is a p-ring and is such that $R/\mathfrak{m}_R \xrightarrow{\approx} A/\mathfrak{m}$.

Definition. Fix a prime p. If R is any commutative ring let $R' = \{x^p + py | x, y \in R\}$. Let $R_0 = R$ and define $R_{n+1} = (R_n)'$ for $n \geq 0$.

Note that R' is a subring of R since it is the inverse image of the subring $(R/pR)^p$ of R/pR. More generally, if I is an ideal of R then $I' = \{x^p + py | x, y \in I\}$ is an ideal of R' because, if $x, y \in I$, $z \in R$, we have $x^p \pm y^p \equiv (x \pm y)^p \mod pI$ and $(z^p + pu)x^p \equiv (zx)^p \mod pI$. Note that, in general, $R'/I' \neq (R/I)'$. For example, let $R = \mathbb{F}_p[x]/(x^{p+1})$ and $I = (x^p)$.

Lemma 14.5. *Let D be a subring of R and let I be an ideal of R. Suppose that $D + I = R$, $p \in I$, and $I^{k+1} = 0$. Then $D_n = R_n$ for $n \geq k$.*

Proof. We have $D' + I' = R'$ since if $x = d + i$ and $y = e + j$, then $x^p + py = d^p + pe + i^p + pz$ where $z \in I$. Therefore, $D_n + I_n = R_n$ for all n. Now $I_n \subset I^{n+1}$ since this holds for $n = 0$ and, if it holds for n, then $I_{n+1} \subset (I^{n+1})^p + pI^{n+1} \subset I^{n+2}$. But $I^{n+1} = 0$ for $n \geq k$.

We can now give the construction of Cohen subrings. Let A be a quasi-local ring with maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^{k+1} = 0$ for some k. Suppose that $E = A/\mathfrak{m}$ has characteristic $p > 0$. Choose a p-base $\{\beta_i\}$ for E and lift it to a set $\{\alpha_i\}$ in A. If R is a subring of A we write $R[\alpha]$ for $R[\{\alpha_i\}]$.

Lemma 14.6. $A_n[\alpha] = A_{n+1}[\alpha]$ *for* $n \geq k$.

Proof. Since $E = E^p(\beta)$, we have $E^p = E^{p^2}(\beta^p)$, etc. so that $E = E^{p^n}(\beta)$ for all $n \geq 0$. The residue field of A_n is E^{p^n} so that of $A_n[\alpha]$ is $E^{p^n}(\beta) = E$ and hence $A = A_n[\alpha] + \mathfrak{m}$. By Lemma 14.5 applied to $A = A_{n+1}[\alpha] + \mathfrak{m}$ we see that, if $n \geq k$, then $A_n = (A_{n+1}[\alpha])_n$. Therefore A_n lies in $A_{n+1}[\alpha]$, but $A_{n+1} \subset A_n$ so $A_n[\alpha] = A_{n+1}[\alpha]$ for $n \geq k$.

Definition. Let $R[\alpha] = A_n[\alpha]$ for any $n \geq k$.

Lemma 14.7. *$R[\alpha]$ is a Cohen subring of A.*

Proof. We have seen that the residue field of $R[\alpha]$ is E. It remains to show that $R[\alpha]$ is a p-ring. Since $R[\alpha] = A_n[\alpha]$ for any $n \geq k$, it follows that $A_{n+1} \subset R[\alpha]'$ so that $R[\alpha] = A_{n+1}[\alpha] \subset R[\alpha]'[\alpha]$ and hence $R[\alpha] = R[\alpha]'[\alpha]$. Now all α_i^p lie in $R[\alpha]'$ so $R[\alpha]$ is generated as an $R[\alpha]'$-module by the elements $\alpha^I = \alpha_{i_1}^{m_1} \dots \alpha_{i_n}^{m_n}$ with $0 \leq m_i < p$ and thus $R[\alpha] = \sum R[\alpha]'\alpha^I$. Modulo $\mathfrak{m}$ this gives $E = \sum E^p \beta^I$ and the β^I are a base for E over E^p by the definition of a p-base. Let $\mathfrak{p} = \mathfrak{m} \cap R[\alpha]$. We must show that $\mathfrak{p} = pR[\alpha]$. Clearly $\mathfrak{p} \supset pR[\alpha]$. Let $x \in \mathfrak{p}$. Then $x = \sum(y_I^p + pz_I)\alpha^I$, with the y_I and z_I in $R[\alpha]$. Modulo $\mathfrak{p}$, we have $0 = \sum \bar{y}_I^p \beta^I$, so $\bar{y}_I = 0$, i.e. $y_I \in \mathfrak{p}$. Therefore $x \in \mathfrak{p}^p + pR[\alpha]$, so that $\mathfrak{p} = \mathfrak{p}^p + pR[\alpha]$. In $R[\alpha]/pR[\alpha]$, we have $\bar{\mathfrak{p}} = \bar{\mathfrak{p}}^p$ but $\bar{\mathfrak{p}}$ is nilpotent so $\bar{\mathfrak{p}} = 0$ showing that $\mathfrak{p} \subset pR[\alpha]$. To see that $R[\alpha]$ is quasi-local, note that if $q = p^n$ then $x^q \in A_n$ for all $x \in A$. If $x \in R[\alpha] - \mathfrak{p}$ then we have $xy = 1$ in A for some y so $xx^{q-1}y^q = 1$ in $R[\alpha]$.

Corollary 14.8. (Cohen structure theorem for artinian local rings). *Let A be an artinian local ring. Then A has a Cohen subring R and A is finite over it, being generated as an R-algebra by any set of generators of the maximal ideal of A.*

Proof. We have just seen that A has a Cohen subring even if we only assume that the maximal ideal is nilpotent. Suppose that A is artinian and let $\mathfrak{m}$ be the maximal ideal of A. Let $x_1, \dots, x_r$ generate $\mathfrak{m}$. Then each $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is generated over the residue field K by monomials of degree n in the x_i. Therefore the same is true over R which has the same residue field as A, so A is finite over R.

The following simple observations will be used in §15.

Lemma 14.9. *Let R be an artinian p-ring. Let $D \subset R$ be a subring of R such that $D + \mathfrak{m}_R = R$. Then $D = R$.*

Proof. We have $R = D + pR$. If $R = D + p^n R$, then $R = D + p^n(D + pR) = D + p^{n+1}R$. But $p^n R = 0$ for large n.

Corollary 14.10. *Let R be an artinian p-ring with residue field E. Let $A \subset R$ be a subring of R and let $\bar{A}$ be the image of A in E. If E is essentially of finite type over $\bar{A}$ then R is essentially of finite type over A.*

Proof. Let E be a localization of $\bar{A}[b_1, \ldots, b_n]$ and lift the b_i to a_i in R. Let $C = A[a_1, \ldots, a_n]$, let $\mathfrak{p} = \mathfrak{m}_R \cap C$, and let $D = C_{\mathfrak{p}}$. Then Lemma 14.9 applies.

15. Artinian rings as colimits. The main result of this section occurs as Lemma 8 of Popescu's paper [Pl]. The proof follows André's notes [A5]. We begin with an elementary lemma.

Lemma 15.1. *Let $f : V \to W$ be a linear map of vector spaces whose kernel is finite dimensional. Let $\{v_i\}$ be a set of linearly independent elements of V. Then we can omit a finite number of the v_i so that the remaining elements have linearly independent images in W.*

Proof. Enlarge $\{v_i\}$ to a basis of V. Let $\{u_j\}$ be a basis of $\ker f$. Write the u_j in terms of the v_i and omit the v_i which are used. Then no linear combination of the remaining v_i (other than 0) can lie in the kernel.

Theorem 15.2. *Let $R \hookrightarrow \Lambda$ be a local mapping of artinian local rings with residue fields $F \subset K$ of characteristic $p \neq 0$. Suppose that $\dim_K \Gamma_{K/F} < \infty$. Then there is a class of local subrings $\mathcal{D}$ of Λ such that*

(1) *The $D \in \mathcal{D}$ contain R and are essentially of finite type over R.*
(2) *Λ is the filtered union of the $D \in \mathcal{D}$.*
(3) *For all $D \in \mathcal{D}$, $D \to \Lambda$ is flat.*
(4) *If $D \subset D'$ are in $\mathcal{D}$ then D' is flat over D and $\mathfrak{m}_D D' = \mathfrak{m}_{D'}$. Also $\mathfrak{m}_D \Lambda = \mathfrak{m}_\Lambda$.*
(5) *Let $D \in \mathcal{D}$, $E = D/\mathfrak{m}_D$, and let $\lambda \in \Lambda$ have image $\bar{\lambda}$ in K. Then for all sufficiently high powers q of p we can find $D' \in \mathcal{D}$ with residue field $E' = E(\bar{\lambda}^q)$ such that $D \subset D'$ and $\lambda^q \in D'$.*

Proof. Let $U \subset R$ be a set such that its image $\bar{U}$ in F is a p-base for F. The JZ sequence for $\mathbb{F} \subset F \subset K$ where $\mathbb{F}$ is the prime field gives $\Gamma_{K/F} \to K \otimes_F \Omega_{F/\mathbb{F}} \to \Omega_{K/\mathbb{F}}$ so Lemma 15.1 applies to $K \otimes_F \Omega_{F/\mathbb{F}} \to \Omega_{K/\mathbb{F}}$. Therefore we can find a subset U_0 of U with $U - U_0$ finite such that the $d\bar{u}$, $u \in U_0$ are linearly independent in $\Omega_{K/\mathbb{F}}$. Consequently we can find a subset V of Λ with $U_0 \subset V$ such that $\bar{V}$ is a p-base for K. Let $\mathfrak{m}_\Lambda^{k+1} = 0$. Then $C = \Lambda_k[V]$ is a Cohen subring of Λ. Note that if $q = p^k$, then $\lambda^q \in C$ for every $\lambda \in \Lambda$.

In the following, E, E', etc. will denote subfields of K with $F \subset E \subset K$ and E of finite type over F. For such E, the JZ sequence for $\mathbb{F} \subset F \subset E$ gives $E \otimes_F \Omega_{F/\mathbb{F}} \to \Omega_{E/\mathbb{F}} \to \Omega_{E/F}$. The elements $d\bar{u}$, $u \in U_0$ span a subspace of finite codimension in $E \otimes_F \Omega_{F/\mathbb{F}}$ and their images in $\Omega_{E/\mathbb{F}}$ are linearly independent since they are even linearly independent in $\Omega_{K/\mathbb{F}}$. Since $\Omega_{E/F}$ is finite dimensional, the $d\bar{u}$ with $u \in U_0$ span a subspace of finite codimension in $\Omega_{E/\mathbb{F}}$. Therefore we can choose a set $W \subset C$ with $W \supset U_0$ and $W - U_0$ finite, such that $\bar{W}$ is a p-base for E.

Let $V_E = \{b \in V | \bar{b} \in E\}$. Then $U_0 \subset V_E$ and the $d\bar{b}$, $b \in V_E$, are linearly independent in $\Omega_{E/\mathbb{F}}$. Since the $d\bar{u}$ with $u \in U_0$ span a subspace of finite codimension in $\Omega_{E/\mathbb{F}}$, we see that $V_E - U_0$ is finite. We can choose $W \supset V_E$ but other choices will also be needed. Let $C_E = \pi^{-1}(E)_k[V_E]$. This need not be a p-ring but C is the filtered union of the C_E.

Let $B = \pi^{-1}(E)_k[W]$. Then B is a Cohen subring of $\pi^{-1}(E)$ lying in C. Since B is of finite type over $\pi^{-1}(E)_k[U_0]$ which lies in C_E, and C is the filtered union of the $C_{E'}$ for $E' \supset E$, we see that $B \subset C_{E'}$ for some E'. Moreover, given two of the B's, say B_1 and B_2, there is some E' with B_1 and B_2 in $C_{E'}$. But $C_{E'}$ in turn is contained in some B, showing that the set $\mathcal{B}_0$ of B's is filtered with union C.

The collection $\mathcal{B}_0$ also has the property (5) of the theorem. Let $B \in \mathcal{B}_0$ be given by $B = \pi^{-1}(E)_k[W]$ where $\bar{W}$ is a p-base for E and let $\lambda \in \Lambda$ have image $\bar{\lambda}$ in K. After replacing λ by some λ^q we can assume that $\lambda \in C$ and that $\bar{\lambda}$ is separable over E. Let $E' = E(\bar{\lambda})$. If λ is transcendental over E, then $W' = W \cup \{\lambda\}$ (which lies in C) maps to a p-base $\bar{W}'$ for E' and we can let $B' = \pi^{-1}(E')_k[W']$. If λ is separable algebraic over E then $\bar{W}$ is also a p-base for E' and we can let $B' = \pi^{-1}(E')_k[W]$. Since $\bar{\lambda} \in E'$, $\lambda \in \pi^{-1}(E')$ so if $q = p^m$ with $m \geq k$, then $\lambda^q \in \pi^{-1}(E')_k \subset B'$. Since $E' = E(\bar{\lambda})$ is separable algebraic over E and purely inseparable over $E(\bar{\lambda}^q)$ we see that $E' = E(\bar{\lambda}^q)$. Therefore the assertion of (5) is true for λ^q.

Let $\lambda_1, \ldots, \lambda_n$ generate $\mathfrak{m}_\Lambda$ and assume that some subset $\lambda_1, \ldots, \lambda_r$ generates $\mathfrak{m}_R$. By Corollary 14.8, we can write $\Lambda = C[X_1, ..., X_n]/(f_1, ..., f_m)$ and we can also assume that the powers X_i^{k+1} occur among the f_j. Let $\mathcal{B}_1$ be the set of $B \in \mathcal{B}_0$ such that B contains the coefficients of all f_i. Then $\mathcal{B}_1$ is filtered with union C. For $B \in \mathcal{B}_1$ let $D = B[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$. By Proposition 14.4, C is faithfully flat over B. Since $C \oslash_B D = \Lambda$ we have $D \subset \Lambda$ since $D \to C \otimes_B D = \Lambda$ is faithfully flat. Let $\mathcal{D}_0$ be the set of rings D just constructed. Properties (2) and (3) are now clear for $\mathcal{D}_0$. For (4), we have $D \subset D' \subset \Lambda$ with Λ faithfully flat over D and over D' so it follows that D' is faithfully flat over D. It is clear that $\mathfrak{m}_D D' = \mathfrak{m}_{D'}$ and $\mathfrak{m}_D \Lambda = \mathfrak{m}_\Lambda$ since $\mathfrak{m}_D$, $\mathfrak{m}'_D$, and $\mathfrak{m}_\Lambda$ are all generated by p and the X_i. Also, (5) is clear since it holds for the B's. It only remains to establish (1)

Now R is finite over its Cohen subring $R_k[U]$ by Corollary 14.8 and hence R is of finite type over $R_k[U_0]$ which lies in all $B \in \mathcal{B}_0$ and so in all $D \in \mathcal{D}_0$. Since $\mathcal{D}_0$ is filtered, R is contained in some $D \in \mathcal{D}_0$. We now choose $\mathcal{D} = \{D \in \mathcal{D}_0 | R \subset D\}$. Let $\bar{R}$ be the image of $R_k[U_0]$ in K. Then F, which is the image of $R_k[U]$, is of finite type over $\bar{R}$ and E, the image of B, is essentially of finite type over F and therefore over $\bar{R}$. By Corollary 14.10, B is essentially of finite type over $R_k[U_0]$. It follows that each $D \in \mathcal{D}$ is essentially of finite type over $R_k[U_0]$ and so also over R.

16. The case of characteristic p.

Let $R \to A \to \Lambda \supset \mathfrak{P}$ be as in Theorem 11.2 and assume that ht $\mathfrak{p} = 0$. We consider here the case in which the residue field F of $R_\mathfrak{p}$ is of characteristic $p \neq 0$. This case requires some delicate arbitration to insure that the various pieces of the construction fit together properly. We begin with the application of Theorem 15.2. We work modulo $\mathfrak{P}^n$ where n will be determined later.

Lemma 16.1. *Let $R \to A \to \Lambda \supset \mathfrak{P}$ be as in Theorem 11.2. Let $\mathfrak{p} = u^{-1}(\mathfrak{P})$ where $u : R \to \Lambda$. Let $F \subset K$ be the residue fields of $R_\mathfrak{p}$ and $\Lambda_\mathfrak{P}$. Assume that* char $F = p \neq 0$. *Given n, let $\tilde{\Lambda} = \Lambda_\mathfrak{P}/\mathfrak{P}^n\Lambda_\mathfrak{P}$ and let $\tilde{R}$ be the image of $R_\mathfrak{p}$ in $\tilde{\Lambda}$. Let G be a finite subset of $\tilde{\Lambda}$. Then we can find $u' : R' = R[Y] \to \Lambda$ extending u, where Y is a finite set of indeterminates,* *and a collection* $\tilde{\mathcal{D}}$ *of local subrings of* $\tilde{\Lambda}$ *with the following properties. We set* $P = u'^{-1}(\mathfrak{P})$ *and* $\tilde{R}' = R'_P/P^nR'_P$.

(1) $P\Lambda_{\mathfrak{P}} = \mathfrak{P}\Lambda_{\mathfrak{P}}$.

(2) $R'_P \to \Lambda_{\mathfrak{P}}$ *is flat.*

(3) *If* $\tilde{D} \in \tilde{\mathcal{D}}$ *then* $\tilde{R}' \subset \tilde{D}$ *and*

  (a) $G \subset \tilde{D}$.

  (b) $\tilde{R}' \to \tilde{D}$ *is essentially smooth.*

  (c) $\tilde{D} \to \tilde{\Lambda}$ *is flat.*

  (d) $\mathfrak{m}_{\tilde{D}} = P\tilde{D}$.

(4) *If* $\tilde{D} \in \tilde{\mathcal{D}}$ *and* $\tilde{\lambda}$ *is any element of* $\tilde{\Lambda}$, *then there is a power* q *of* p *and some* $\tilde{D}' \in \tilde{\mathcal{D}}$ *such that* $\tilde{D} \subset \tilde{D}'$ *and* $\tilde{\lambda}^q \in \tilde{D}'$.

Proof. If λ is an element of Λ we write $\tilde{\lambda}$ for its image in $\tilde{\Lambda}$ and $\bar{\lambda}$ for its image in K, the residue field of $\tilde{\Lambda}$. Let $c_1, \ldots, c_M$ generate $\mathfrak{P}$. We can assume that G contains the images $\tilde{c}_i$ of the c_i. By the assumptions of Theorem 11.2, $\Lambda_{\mathfrak{P}}/\mathfrak{p}\Lambda_{\mathfrak{P}}$ is geometrically regular over $F = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ and therefore $\dim \Gamma_{K/F} < \infty$ by Corollary 6.2. Let $\mathcal{D}$ be the class of subrings of $\tilde{\Lambda}$ given by Theorem 15.2 applied to $\tilde{R} \hookrightarrow \tilde{\Lambda}$. Since G is finite, we can choose $D \in \mathcal{D}$ such that $G \subset D$. Let $b_1, \ldots, b_m \in D$ lift a p-base $\bar{b}_1, \ldots, \bar{b}_m$ of E/F where E is the residue field of D. We claim that, after enlarging D by Theorem 15.2 (5), we can assume that the b_i lift to elements y_i of Λ. It is clear that we can lift the b_i to elements y_i/s of $\Lambda_{\mathfrak{P}}$. If q is a power of p we can rewrite this as $s^{q-1}y_i/s^q$ so we can replace s by s^q. If $\bar{s}$ is algebraic over E, we can, in this way, reduce to the case in which $\bar{s}$ is separable over E. As in the proof of Theorem 15.2 we then have $E' = E(\bar{s}) = E(\bar{s}^p)$ so, after replacing s by s^p, we can also assume that $d\bar{s} = 0$ in $\Omega_{E'}$.

By Theorem 15.2 (5) we can, after once more replacing s by some s^q, enlarge D to $D' \in \mathcal{D}$ with $\tilde{s} \in D$ and with residue field $E' = E(\bar{s})$. If $\bar{s}$ is transcendental over E, then $\{\bar{b}_i, \bar{s}\}$ is a p-base for E'/F. Since $\bar{y}_i = \bar{s}\bar{b}_i$ we have $d\bar{y}_i = \bar{s}d\bar{b}_i + \bar{b}_i d\bar{s}$ showing that $\{\bar{y}_i, \bar{s}\}$ is also a p-base for E'/F. If $\bar{s}$ is separable algebraic over E, the $\bar{b}_i$ are still a p-base for E'/F and, since we have arranged that $d\bar{s} = 0$, so are the $\bar{y}_i = \bar{s}\bar{b}_i$.

We have now found a subring $D \in \mathcal{D}$ with $\tilde{R} \subset D \subset \tilde{\Lambda}$ such that $G \subset D$ and such that D is essentially of finite type over $\tilde{R}$, $D \to \tilde{\Lambda}$ is flat, and $\mathfrak{m}_D\tilde{\Lambda} = \mathfrak{m}_{\tilde{\Lambda}}$. We also have elements y_i in Λ mapping to D such that the $\bar{y}_i$ are a p-base for E/F where E is the residue field of D. By Lemma 7.9, the map $R[Y'_1, \ldots, Y'_m] \to \Lambda$ sending Y'_i to y_i induces a flat map $R[Y'_1, \ldots, Y'_m]_Q \to \Lambda_{\mathfrak{P}}$ where Q is the image of $\mathfrak{P}$, and $\Lambda_{\mathfrak{P}}/Q\Lambda_{\mathfrak{P}}$ is regular. Let $\{y''_i\} \subset \{c_1, \ldots, c_M\}$ map to a regular system of parameters of $\Lambda_{\mathfrak{P}}/Q\Lambda_{\mathfrak{P}}$, let $R' = R[Y] = R[Y'_1, \ldots, Y'_m, Y''_1, \ldots, Y''_s]$, and define $R' \to \Lambda$ by sending Y''_i to y''_i. By Lemma 7.7, $R'_P \to \Lambda_{\mathfrak{P}}$ is flat where P is the inverse image of $\mathfrak{P}$ in R'. Moreover, $P\Lambda_{\mathfrak{P}} = \mathfrak{P}\Lambda_{\mathfrak{P}}$ since Q and the y''_i generate $\mathfrak{P}\Lambda_{\mathfrak{P}}$. It follows that $\tilde{R}' = R'_P/P^nR'_P \to \tilde{\Lambda} = \Lambda_{\mathfrak{P}}/\mathfrak{P}^n\Lambda_{\mathfrak{P}}$ is flat and therefore faithfully flat since it is local. In particular $\tilde{R}' \to \tilde{\Lambda}$ is injective. Since the y''_i were chosen from the set $\{c_1, \ldots, c_M\}$, their images in $\tilde{\Lambda}$ lie in D. Therefore $\tilde{R}' \subset D$. We have $PD \subset \mathfrak{m}_D$ and tensoring this with $\tilde{\Lambda}$ over D gives $P\tilde{\Lambda} = \tilde{\mathfrak{P}} \subset \mathfrak{m}_D\tilde{\Lambda} \subset \tilde{\mathfrak{P}}$. Since $D \to \tilde{\Lambda}$ is faithfully flat (being local), we see that $PD = \mathfrak{m}_D$.

We now choose $\tilde{\mathcal{D}}$ to be the set of $\tilde{D} \in \mathcal{D}$ such that $D \subset \tilde{D}$ and such that the residue field E' of $\tilde{D}$ is separable over E, the residue field of D. It is clear that properties (1), (2), (3a), and (3c) of Lemma 16.1 are satisfied. Property (3d) has been shown for D and the general case follows from Theorem 15.2 (4). For (3b), note that the residue field E of D

is finite separable over that of $\tilde{R}'$ since the images of the y_i' in E form a p-base for E/F. Therefore, the residue field of $\tilde{D}$ is separable over that of $\tilde{R}'$. Since $\tilde{R}' \to \tilde{\Lambda}$ and $\tilde{D} \to \tilde{\Lambda}$ are faithfully flat, so is $\tilde{R}' \to \tilde{D}$. Since $\mathfrak{m}_{\tilde{D}} = P\tilde{D}$ by (3d), (3b) follows from Corollary 10.5.

Finally, for property (4), observe that, by Theorem 15.2, we can enlarge $\tilde{D}$ to $\tilde{D}'$ with residue field $E'' = E'(\bar{\lambda}^q)$ such that $\tilde{D} \subset \tilde{D}'$, and $\lambda^q \in \tilde{D}'$. By taking q sufficiently large, we can insure that $\bar{\lambda}^q$ is separable over E'. Then E'' will be separable over E as required.

Remark. In contrast to the collection $\mathcal{D}$ of Theorem 15.2, $\tilde{\mathcal{D}}$ need not be filtered in general because the collection of subfields of K separable over E is not filtered in general. For example suppose x is transcendental over E while y is inseparable over E. Then there is no separable extension containing $E(x)$ and $E(xy)$.

Suppose now that $R \to A \to \Lambda \supset \mathfrak{P}$ satisfies the hypothesis of Theorem 11.2. Let $r = \operatorname{ht}\mathfrak{P}$. We want to adjoin indeterminates $X_1, \ldots, X_r$ to R in order to apply Corollary 11.5 as in the characteristic 0 case. Choose N such that $(\operatorname{nil}\Lambda_{\mathfrak{P}})^N = 0$ and such that $\mathfrak{P}^N\Lambda_{\mathfrak{P}} \subset H_{A/R}\Lambda_{\mathfrak{P}}$. We can do this since we have assumed that $\mathfrak{P}$ is minimal over $H_{A/R}\Lambda$. The next step is to construct a generic standardizer for A. Let $b_1, \ldots, b_m$ generate $H_{A/R}$ and let $A' = A[X, Z]/(X_i^{2N} - \sum_j Z_{ij}b_j)$. Then A'_{b_j} is smooth over $A_{b_j}[X]$ since it is just a polynomial ring in the X_i and the Z_{ik} with $k \neq j$. Since A_{b_j} is smooth over R, $A_{b_j}[X]$ is smooth over $R[X]$ and hence so is A'_{b_j}. Therefore $b_j|A' \in H_{A'/R[X]}$ showing that $H_{A/R}A' \subset H_{A'/R[X]}$. It follows that $X_i|A' \in H_{A'/R[X]}$. Let A'' be the standardizer of A' over $R[X]$ given by Proposition 4.6 and let $\rho : A'' \to A'$ be a ring theoretic retraction which exists since A'' is a symmetric algebra over A'. By Proposition 4.6, $H_{A'/R[X]}A'' \subset H_{A''/R[X]}$ so $H_{A/R}A'' \subset H_{A''/R[X]}$ and, for a suitable presentation of A'' over $R[X]$, the $X_i|A''$ are standard. Choose an e such that all $X_i^e|A''$ are strictly standard and let $c = 8e$. We now apply Lemma 16.1 with $n = N + rc$ and with G containing the images $\tilde{b}_j \in \tilde{\Lambda}$ of the b_j.

Our next task is to choose images for the X_i in Λ so that A' also maps into an appropriate $\tilde{D} \in \tilde{\mathcal{D}}$. We follow here André's notes [A5]. The notation is as above and as in Lemma 16.1.

Lemma 16.2. *Given $d_1, \ldots, d_r \in P$, we can find $\tilde{D} \in \tilde{\mathcal{D}}$ and a map $A' \to \Lambda$ such that $X_i \mapsto d_i\epsilon_i$ with $\epsilon_i \in \Lambda - \mathfrak{P}$ and such that the image of A' in $\tilde{\Lambda}$ lies in $\tilde{D}$.*

It follows that the same is true for A'' since we can compose the map of Lemma 16.2 with the retraction $\rho : A'' \to A'$. It will be necessary to choose $d_1, \ldots, d_r$ after R' and $\tilde{\mathcal{D}}$ have been fixed so 16.2 does not follow directly from Lemma 16.1.

Proof. Choose some $\tilde{D} \in \tilde{\mathcal{D}}$. Since $\mathfrak{P}^N\Lambda_{\mathfrak{P}} \subset H_{A/R}\Lambda_{\mathfrak{P}}$, the equations $d_i^N = \sum b_j\lambda_{ij}$ have a solution λ_{ij} in $\Lambda_{\mathfrak{P}}$, and therefore in $\tilde{\Lambda}$. The following well-known fact then shows that they also have a solution in $\tilde{D}$.

Lemma 16.3. *Let $\sum a_{ij}x_j = b_i$ be a finite system of equations over a ring A. Let $A \to B$ be a faithfully flat map. If the equations have a solution in B, then they also have a solution in A.*

Proof. Let M be the pullback of the diagram

$$\begin{tikzcd} & A \arrow[d, "(b_i)"] \\ A^m \arrow[r, "(a_{ij})"] & A^n \end{tikzcd}$$

Shouldn't G also contain a set
of generators for A as an R-algebra?

The equations have a solution in A if and only if the map $M \to A$ is onto. Since B is faithfully flat over A, it is sufficient to check this condition over B.

Let $\tilde{d}_i^N = \sum b_j \tilde{z}_{ij}$ in $\tilde{D}$ and lift $\tilde{z}_{ij}$ to z'_{ij} in $\Lambda_{\mathfrak{P}}$. Then $d_i^N - \sum b_j z'_{ij}$ lies in $\mathfrak{P}^n \Lambda_{\mathfrak{P}} \subset \mathfrak{P}^{n-N} \Lambda_{\mathfrak{P}} H_{A/R}$ so we can write $d_i^N = \sum b_j (z'_{ij} + z''_{ij})$ with z''_{ij} in $\mathfrak{P}^{n-N}\Lambda_{\mathfrak{P}}$. Multiplying by d_i^N, we get $d_i^{2N} = \sum b_j z_{ij}$ where $z_{ij} = d_i^N z'_{ij} + d_i^N z''_{ij}$ which maps to an element of $\tilde{D}$ since $d_i^N z'_{ij}$ does, while $d_i^N z''_{ij}$, which lies in $\mathfrak{P}^N \mathfrak{P}^{n-N} \Lambda_{\mathfrak{P}} = \mathfrak{P}^n \Lambda_{\mathfrak{P}}$, maps to 0. Write $z_{ij} = w_{ij}/s_i$ with $w_{ij} \in \Lambda$ and $s_i \in \Lambda - P$ After replacing s_i by a sufficiently high power, we can enlarge $\tilde{D}$ by Lemma 16.1 (4) so as to have $\tilde{s}_i \in \tilde{D}$. There are elements $t_i \in \Lambda - P$ such that $t_i((s_i d_i)^{2N} - \sum b_j s_i^{2N-1} w_{ij}) = 0$. After once again replacing t_i by a sufficiently high power and enlarging $\tilde{D}$ we can assume that $\tilde{t}_i \in \tilde{D}$. It is now clear if $\epsilon_i = s_i t_i$, we get the required map $A' \to \Lambda$ by sending X_i to $d_i \epsilon_i$ and Z_{ij} to $\zeta_{ij} = s_i^{2N-1} t_i^{2N} w_{ij}$.

Remark. If η_i are any elements of $\Lambda - P$ with $\tilde{\eta}_i$ in $\tilde{D}$, we can replace ϵ_i by $\epsilon_i \eta_i$, sending X_i to $d_i \epsilon_i \eta_i$ and Z_{ij} to $\eta_i^{2N} \zeta_{ij}$.

We now must choose the sequence $d_1, \ldots, d_r$. Here we make the assumption that $\operatorname{ht} \mathfrak{p} = 0$ which is permissible by Lemma 12.1. Since $R' = R[Y]$, R'_P is a localization of $R_{\mathfrak{p}}[Y]$. Since we have assumed $\operatorname{ht} \mathfrak{p} = 0$, $R_{\mathfrak{p}}$ is artinian and hence Cohen-Macaulay. Therefore R'_P is also Cohen-Macaulay by Lemma 8.8. Also, $(R_{\mathfrak{p}})_{\mathrm{red}} = F$ is a field and it follows that $(R'_P)_{\mathrm{red}}$ is regular. Let $d_1, \ldots, d_s \in P$ map to a regular system of parameters of $(R'_P)_{\mathrm{red}}$. Then $d_1, \ldots, d_s$ is a system of parameters of R'_P and so is a regular sequence on R'_P by Corollary 8.7, and therefore also on $\Lambda_{\mathfrak{P}}$ which is flat over R'_P. In particular, $s \leq \dim \Lambda_{\mathfrak{P}} = r$. On the other hand, $(d_1, \ldots, d_s)$ is primary for PR'_P so for some M, $P^M R'_P \subset (d_1, \ldots, d_s) R'_P$ which implies that $\mathfrak{P}^M \Lambda_{\mathfrak{P}} \subset (d_1, \ldots, d_s)\Lambda_{\mathfrak{P}}$ so $r = \operatorname{ht} \mathfrak{P} \leq s$ showing that $s = r$.

Any permutation of the $d_1, \ldots, d_r$ is also a system of parameters and so a regular sequence on R'_P. (This is also clear since R'_P is local [K,Th.119]). Therefore the following lemma applies to this sequence.

Lemma 16.4. *Let $a_1, \ldots, a_s$ be elements of a ring A. Then the following conditions are equivalent.*

1. *Any permutation of $a_1, \ldots, a_s$ is a regular sequence on A.*
2. *Any subset of $a_1, \ldots, a_s$ (in the given order) is a regular sequence on A.*
3. *Let $T_1, \ldots, T_s$ be indeterminates. Then $a_1 T_1, \ldots, a_s T_s$ is a regular sequence on $A[T_1, \ldots, T_s]$.*

Proof. If $\alpha = (\alpha_1, \ldots, \alpha_s)$ write $T^\alpha = T_1^{\alpha_1} \ldots T_s^{\alpha_s}$. Then $R[T_1, \ldots, T_s]/(a_1 T_1, \ldots, a_{i-1} T_{i-1}) = \bigoplus_\alpha R/I_{i\alpha} T^\alpha = A_i$, say, where $I_{i\alpha}$ is the ideal of R generated by $\{a_\nu | \nu < i, \alpha_\nu > 0\}$. The map $a_i T_i : A_i \to A_i$ is the direct sum of the maps $a_i T_i : R/I_{i\alpha} T^\alpha \to R/I_{i\alpha} T^\alpha T_i$. Therefore $a_i T_i$ is regular on A_i if and only if a_i is regular on all $R/I_{i\alpha}$. Since all possible subsets of $\{1, \ldots, i-1\}$ occur as $\{\nu | \nu < i, \alpha_\nu > 0\}$, we see that (3) is equivalent to (2). It is clear that (1) implies (2). For the converse we need only show that two consecutive a_i can be permuted. After factoring out the previous terms we are reduced to showing that if a, b is a regular sequence and b is a regular element, then b, a is a regular sequence. This follows immediately from the definition.

We will also need the following standard fact about regular sequences [K,3–1,Ex.12].

Lemma 16.5. *If $a_1, \ldots, a_s$ is a regular sequence in any ring, and if $e_i > 0$, then $a_1^{e_1}, \ldots, a_s^{e_s}$ is also a regular sequence.*

Proof. If $0 \to M' \to M \to M'' \to 0$ is exact and c is regular on M' and M'', the snake lemma shows that c is regular on M and $0 \to M'/cM' \to M/cM \to M''/cM'' \to 0$ is exact. It follows that a sequence which is regular on M' and M'' is also regular on M. If $a, c_2, \ldots, c_s$ and $b, c_2, \ldots, c_s$ are regular on M, the exact sequence $0 \to M/bM \xrightarrow{a} M/abM \to M/aM \to 0$ shows that $ab, c_2, \ldots, c_s$ is regular on M. Therefore $a_1^{e_1}, a_2, \ldots, a_s$ is regular and we can now factor out $a_1^{e_1}$ and use induction on s.

We can modify the d_i to make them satisfy the condition (1) of Corollary 11.5 in $R'[T]$ by using the following lemma.

Lemma 16.6. (Ogoma [O]). *Let A be a noetherian ring and let M be a finitely generated A-module. Let $S \subset A$ be a multiplicative set. Suppose $a \in A$ satisfies $\ker_{M_S}(a) = \ker_{M_S}(a^2)$ in M_S. Then there is an element t of S such that for any $n > 0$, $s = t^n$ satisfies $\ker_M(as) = \ker_M((as)^2)$.*

Proof. Since $\ker_M(a^2)/\ker_M(a)$ localizes to 0, there is some $u \in S$ such that $u \ker_M(a^2) \subset \ker_M(a)$. Let $t = u^N$ where N is so large that $\ker_M(t^m) = \ker_M(t^{m+1})$ for all $m \geq N$. Then any $s = t^n$ with $n > 0$ will satisfy $s \ker_M(a^2) \subset \ker_M(a)$ and $\ker_M(s) = \ker_M(s^2)$. Now if $(as)^2 x = 0$, then $s^2 a^2 x = 0$ so $sa^2 x = 0$. Therefore sx lies in $\ker(a^2)$ so $s^2 x$ lies in $\ker(a)$ showing that $s^2 ax = 0$ and hence $sax = 0$.

Corollary 16.7. *We can replace the original d_i by elements $d_i s_i$ with s_i in $R' - P$ so that the new d_i satisfy $((d_1T_1)^c, \ldots, (d_{i-1}T_{i-1})^c){:}(d_iT_i)^2 = ((d_1T_1)^c, \ldots, (d_{i-1}T_{i-1})^c){:}d_iT_i$ in $R'[T]$ for each i.*

Proof. Apply Lemma 16.6 successively with $a = d_iT_i$, $A = R'[T]$, $S = R' - P$, and $M = A/((d_1T_1)^c, \ldots, (d_{i-1}T_{i-1})^c)$. Note that $(d_1T_1)^c, \ldots, (d_{i-1}T_{i-1})^c, d_iT_i, \ldots$ is a regular sequence on $R'_P[T]$ by Lemmas 16.4 and 16.5 so the hypothesis of Lemma 16.6 is satisfied.

Corollary 16.8. *We can enlarge $\tilde{D}$ as in Lemma 16.1(4) and find elements δ_i in $\Lambda - P$ such that*

(1) $\tilde{\delta}_i \in \tilde{D}$.
(2) *There is a map $A' \to \Lambda$ with $X_i \mapsto d_i\delta_i$ such that the image of A' in $\tilde{\Lambda}$ lies in $\tilde{D}$.*
(3) *The elements $d'_i = d_i\delta_i$ satisfy*

$$(*) \quad ({d'}_1^c, \ldots, {d'}_{i-1}^c){:}{d'}_i^2 = ({d'}_1^c, \ldots, {d'}_{i-1}{}^c){:}d'_i \text{ in } \Lambda \text{ for each } i.$$

Proof. Apply the method of Corollary 16.7 to the sequence $d_i\epsilon_i$ on Λ where the ϵ_i are the elements of $S = \Lambda - P$ given by Lemma 16.2. Suppose we have determined elements η_j in $\Lambda - P$ for $j < i$ such that for $\delta_j = \epsilon_j\eta_j$, the $d'_j = d_j\delta_j = d_j\epsilon_j\eta_j$ satisfy $(*)$ in Λ. Suppose also that we have enlarged $\tilde{D}$, using Lemma 16.1 (4), so that the $\tilde{\eta}_j$ lie in $\tilde{D}$. Lemma 16.6 then gives us an η_i such that $d'_i = d_i\epsilon_i\eta_i^n$ satisfies $(*)$ for any $n > 0$. By Lemma 16.1 (4), we can enlarge $\tilde{D}$ to $\tilde{D}'$ so that $\tilde{\eta}_i^n$ lies in $\tilde{D}'$ for some $n > 0$. Replace $\tilde{D}$ by $\tilde{D}'$ and η_i by η_i^n. Condition (2) is clear by the remark following the proof of Lemma 16.2.

Lemma 16.9. *We have $(d_1^c, \ldots, d_r^c)\Lambda_{\mathfrak{P}} \supset \mathfrak{P}^n\Lambda_{\mathfrak{P}}$ and $(d_1^c, \ldots, d_r^c)R'_P \supset P^n R'_P$.*

Proof. The d_i were chosen to generate the maximal ideal of $(R'_P)_{\text{red}}$ so PR'_P is generated by $d_1, \ldots, d_r$ and nilpotent elements. Since $\mathfrak{P}\Lambda_{\mathfrak{P}} = P\Lambda_{\mathfrak{P}} = PR'_P\Lambda_{\mathfrak{P}}$, we have $\mathfrak{P}\Lambda_{\mathfrak{P}} = (d_1, \ldots, d_r)\Lambda_{\mathfrak{P}} + \mathfrak{N}$ where $\mathfrak{N} = \operatorname{nil}(\Lambda_{\mathfrak{P}})$. Let $I = (d_1, \ldots, d_r)\Lambda_{\mathfrak{P}}$. Then $\mathfrak{P}^n\Lambda_{\mathfrak{P}} = (I + \mathfrak{N})^n = I^n + I^{n-1}\mathfrak{N} + \cdots + I^{n-N+1}\mathfrak{N}^{N-1}$ since $\mathfrak{N}^N = 0$ by the choice of N. Therefore

$\mathfrak{P}^n\Lambda_{\mathfrak{P}} \subset I^{n-N+1} = I^{rc+1} \subset I^{rc} \subset (d_1^c,\dots,d_r^c)\Lambda_{\mathfrak{P}}$. The fact that $(d_1^c,\dots,d_r^c)R'_P \supset P^nR'_P$ now follows by tensoring with $\Lambda_{\mathfrak{P}}$ which is faithfully flat over R'_P.

We now come to the application of Corollary 11.5. Let $T_1,\dots,T_r$ be indeterminates, let $R'' = R'[T]$ and define $R[X] \to R''$ by sending X_i to d_iT_i. Define $u'' : R'' \to \Lambda$ by sending T_i to δ_i. Let A'' be the standardizer of $A[X]$ constructed above (after the proof of Lemma 16.1), and let $B = R'' \otimes_{R[X]} A'' \to \Lambda$ by u'' on R'' and with $A'' \to \Lambda$ being given by the retraction $\rho : A'' \to A'$ composed with the map of Corollary 16.8. By Lemma 4.7, $H_{A''/R[X]}B \subset H_{B/R''}$. Since $H_{A/R}A'' \subset H_{A''/R[X]}$, we get $H_{A/R}B \subset H_{B/R''}$ showing that $\mathfrak{h}_{A/R} \subset \mathfrak{h}_{B/R''}$. Suppose that $R'' \to B \to \Lambda \supset \mathfrak{P}$ can be resolved. We then get $R'' \to B \to C \to \Lambda$ with $\mathfrak{h}_{B/R''} \subset \mathfrak{h}_{C/R''} \not\subset \mathfrak{P}$. Since R'' is smooth over R, $H_{C/R''} \subset H_{C/R}$ so we get $\mathfrak{h}_{A/R} \subset \mathfrak{h}_{B/R''} \subset \mathfrak{h}_{C/R''} \subset \mathfrak{h}_{C/R} \not\subset \mathfrak{P}$ and therefore, $R \to A \to C \to \Lambda$ resolves $R \to A \to \Lambda \supset \mathfrak{P}$ as required. We now resolve $R'' \to B \to \Lambda \supset \mathfrak{P}$ by applying Corollary 11.5 using the sequence $a_i = d_iT_i$. We have just arranged for condition (1) of that corollary to hold and condition (2) holds because $X_i^e|A''$ is strictly standard so its image $a_i^e|B$ under the base change $R[X] \to R''$ is also strictly standard by Lemma 4.8. By Corollary 11.5, it will suffice to check the resolvability of $R''/I \to B/IB \to \Lambda/I\Lambda \supset \mathfrak{P}/I\Lambda$ where $I = ((d_1T_1)^c,\dots,(d_rT_r)^c)$. By Lemma 16.9, we have $\operatorname{ht}\mathfrak{P}/I\Lambda = 0$ since the T_i map to units in $\Lambda_{\mathfrak{P}}$. Therefore, by Lemma 12.3, it will suffice to check the resolvability of $(R''/I)_{S'} \to (B/IB)_{S'} \to \Lambda_{\mathfrak{P}}/I\Lambda_{\mathfrak{P}}$ where $S' = R'' - Q$ with $Q = {u''}^{-1}(\mathfrak{P})$. It will therefore suffice to show that $(R''/I)_{S'} \to (B/IB)_{S'} \to \Lambda_{\mathfrak{P}}/I\Lambda_{\mathfrak{P}}$ can be desingularized, i.e. that we can find $(R''/I)_{S'} \to (B/IB)_{S'} \to E \to \Lambda_{\mathfrak{P}}/I\Lambda_{\mathfrak{P}}$ with E smooth over $(R''/I)_{S'}$.

Remark. Note that if $R \to A \to \Lambda$ can be desingularized, and $R \to R'$, then $R' \to R'\otimes_R A \to R'\otimes_R \Lambda$ can be desingularized since if $R \to A \to B \to \Lambda$ with B smooth over R then $R'\otimes_R B$ is smooth over R'.

Let $J = (d_1^c,\dots,d_r^c) \subset R'$. Since the T_i map to elements of $\Lambda - \mathfrak{P}$ they lie in S'. Therefore $I_{S'} = IR''_{S'} = JR''_{S'}$ so $(R''/I)_{S'} \to (B/IB)_{S'} \to \Lambda_{\mathfrak{P}}/I\Lambda_{\mathfrak{P}}$ can be written as $(R''/JR'')_{S'} \to (B/JB)_{S'} \to \Lambda_{\mathfrak{P}}/J\Lambda_{\mathfrak{P}}$. Now $Q \cap R' = P$ so $S' \supset S = R' - P$. By the above remark applied to $(R''/JR'')_S \to (R''/JR'')_{S'}$, it will suffice to desingularize $(R''/JR'')_S \to (B/JB)_S \to \Lambda_{\mathfrak{P}}/J\Lambda_{\mathfrak{P}}$ which can be rewritten as $R'_P[T]/J_P[T] \to R'_P[T]/J_P[T] \otimes_{R'[T]} B \to \Lambda_{\mathfrak{P}}/J_P\Lambda_{\mathfrak{P}}$. By Lemma 16.9, $P^nR'_P \subset J_P$ so by the above remark applied to $R'_P[T]/P^nR'_P[T] \to R'_P[T]/J_P[T]$, it will suffice to consider the case where J_P is replaced by $P^nR'_P$, in other words, it is sufficient to desingularize $\tilde{R}'[T] \to \tilde{R}'[T] \otimes_{R'[T]} B \to \tilde{\Lambda}$ which can be written as $\tilde{R}'[T] \to \tilde{R}'[T] \otimes_{R[X]} A'' \to \tilde{\Lambda}$.

We have arranged for the images of $\tilde{R}'[T]$ and of A'' in Λ to lie in $\tilde{D}$. Since $\tilde{D}$ is essentially smooth over $\tilde{R}'$, $\tilde{D}[T]$ will be essentially smooth over $\tilde{R}'[T]$ so, by Corollary 3.9, it will suffice to show that $\tilde{R}'[T] \otimes_{R[X]} A'' \to \tilde{D}$ factors through the map $\tilde{D}[T] \to \tilde{D}$ sending T_i to $\tilde{\delta}_i$. For this, it will be enough to show that $A' \to \tilde{D}$ factors through $\tilde{D}[T] \to \tilde{D}$ as an $R[X]$-algebra homomorphism. Then composing with the retraction $\rho : A'' \to A'$ gives a map $A'' \to \tilde{D}[T]$ which will obviously induce the required map. Recall that $A' = A[X,Z]/(X_i^{2N} - \sum Z_{ij}b_j) \to \Lambda$ with $X_i \mapsto d_i\delta_i$. Let ζ_{ij} be the image of Z_{ij} in Λ. Let $\tilde{\delta}_i$ and $\tilde{\zeta}_{ij}$ be the images of δ_i and ζ_{ij} in $\tilde{D} \subset \tilde{\Lambda}$. We are given that X_i maps to d_iT_i in $R'[T]$ so that X_i maps to $\tilde{d}_iT_i$ in $\tilde{D}[T]$. Therefore, we get the required map $A[X,Z]/(X_i^{2N} - \sum Z_{ij}b_j) \to \tilde{D}[T]$ by sending Z_{ij} to $(T_i/\tilde{\delta}_i)^{2N}\tilde{\zeta}_{ij}$. Note that $\tilde{\delta}_i$ is a unit in $\tilde{\Lambda}$ and therefore also in $\tilde{D}$.

17. The lifting lemma.

Lemma 17.1. *Let $R \to \Lambda$ be a map of noetherian rings and let $d \in R$ satisfy* $\operatorname{Ann}(d^2) = \operatorname{Ann}(d)$ *in R and in Λ. Let $\bar{R} = R/(d^2)$ and $\tilde{R} = R/(d)$, and similarly for Λ and other R-algebras. Suppose we are given $\bar{R} \to \bar{C} \to \bar{\Lambda}$ with $\bar{C}$ of finite type over $\bar{R}$. Then we can find $R \to D \to \Lambda$ with D of finite type over R such that*

(1) *There is a commutative diagram*

$$\begin{tikzcd}
\bar{R} \arrow[r] \arrow[d] & \bar{C} \arrow[r] \arrow[d] & \bar{\Lambda} \arrow[d] \\
\tilde{R} \arrow[r] & \tilde{D} \arrow[r] & \tilde{\Lambda}
\end{tikzcd}$$

where the left and right maps are the canonical quotient maps.

(2) *Let $\pi : \Lambda \to \bar{\Lambda}$ be the canonical map. Then $\pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \mathfrak{h}_D$.*

Proof. Let $H_{\bar{C}/\bar{R}} = \sqrt{\sum \bar{C}\bar{P}_i}$ where $\bar{P}_i \in \Delta_{(\bar{f}^{(i)})}[(\bar{f}^{(i)}):\bar{I}]$ for some presentation $\bar{C} = \bar{R}[X]/\bar{I}$ where each $\{\bar{f}^{(i)}\}$ is a finite subset of I. Note that $\bar{C} = R[X]/I$ where $d^2 \in I$ and $\bar{I} = I/d^2R[X] \subset \bar{R}[X] = R[X]/d^2R[X]$. Choose a finite set of generators $\{f_1, \ldots, f_N\}$ for I such that $\{\bar{f}_1, \ldots, \bar{f}_N\}$ contains all elements of the sets $\{\bar{f}^{(i)}\}$. We can assume that each $\bar{P}_i$ is the image of some P_i in $R[X]$ which has the form $P_i = M_iN_i$ where M_i is an $n \times n$ minor of $(\partial f_j/\partial X_k)$ for some n, say for $1 \le j \le n$, and $\bar{N}_i\bar{I} \subset (\bar{f}^{(i)})$ where $\{\bar{f}^{(i)}\} = \{f_1, \ldots, f_n\}$ so that $N_iI \subset (d^2, f_1, \ldots, f_n)$. The ordering of the f_j here depends, of course, on i, as does n.

Let $\bar{C} \to \bar{\Lambda}$ be given by $X_i \mapsto \bar{\xi}_i$ and lift $\bar{\xi}_i$ to $\xi_i \in \Lambda$. Then $f_i(\xi) \in d^2\Lambda$ so $f_i(\xi) = d\zeta_i$ with $\zeta_i \in d\Lambda$. Let $g_i(X, Z) = f_i(X) - dZ_i$ with new variables Z_i. We will define D to be $R[X, Z]/J$ for some J with $(g) \subset J \subset (g) + [(g){:}d] \cap (Z, d) \subset (g){:}d$. The map $D \to \Lambda$ will be given by $X_i \mapsto \xi_i$ and $Z_i \mapsto \zeta_i$. It is clear that this sends all g_i to 0. It also sends $[(g){:}d] \cap (Z, d)$ to 0 since if $h \in [(g){:}d]$ then $dh \in (g)$ so $dh(\xi, \zeta) = 0$, but if also $h \in (Z, d)$, then $h(\xi, \zeta) \in d\Lambda$ (since $\zeta_i \in d\Lambda$) so $dh(\xi, \zeta) = 0$ implies $h(\xi, \zeta) = 0$ by our assumption on annihilators.

Since $I = (f_1, \ldots, f_N)$, $I \subset (g, d)$ and we have a map $\bar{C} = R[X]/I \to R[X, Z]/(g, d) \to \tilde{D} = D/dD$ since $R[X, Z]/(g)$ maps onto D. This map clearly satisfies condition (1). Note also that $d \in H_{D/R}$ since $D_d = R_d[X, Z]/(g) = R_d[X]$ which is smooth over R.

Let p be any of the P_i above. Suppose $pI \subset (d^2, f_1, \ldots, f_n)$ where n and the set $f_1, \ldots, f_n$ will depend on p. To avoid messy notation we will just assume that the f_i are reordered for each choice of p. Write $pf_i = \sum_{j=1}^n H_{ij}^{(p)} f_j + d^2G_i^{(p)}$ for $i = 1, \ldots, N$. Choose $H_{ij}^{(p)} = p\delta_{ij}$ and $G_i^{(p)} = 0$ if $i \le n$ and set $H_{ij}^{(p)} = 0$ for $j > n$ (which depends on the ordering of the f_i used for p). Let $F_i^{(p)} = pZ_i - \sum_{j=1}^n H_{ij}^{(p)} Z_j - dG_i^{(p)}$. Then $F_i^{(p)} = 0$ for $i \le n$ and $dF_i^{(p)} = p(f_i - g_i) - \sum_{j=1}^n H_{ij}^{(p)}(f_j - g_j) - d^2G_i^{(p)} = -pg_i + \sum_{j=1}^n H_{ij}^{(p)} g_j \in (g)$ showing that $F_i^{(p)} \in (g){:}d$. It is clear that $F_i^{(p)} \in (Z, d)$. We now define $J = (g, F)$ using all such F and set $D = R[X, Z]/J$.

Let f stand for the column vector with entries f_i and let $H^{(p)}$ be the matrix with entries $H_{ij}^{(p)}$ (for some fixed ordering of the f_i). Then we can write $pf \equiv H^{(p)}f \mod d$ so if $S^{(pq)} = qH^{(p)} - H^{(q)}H^{(p)}$ then $S^{(pq)}f \equiv qpf - H^{(q)}pf \equiv qpf - qpf = 0 \mod d$. Differentiating this gives $S^{(pq)}\partial f/\partial X_k \in (d, f) = (d, g)$.

Since $p = MN$ where M is an $n \times n$ minor of $(\partial f_i/\partial X_j)$ for $1 \le i \le n$, we can choose $k_1, \ldots, k_n$ so that $M = |\partial f_i/\partial X_{k_j}|$ is a factor of p. Note that $S_{ij}^{(pq)} = 0$ for $j > n$ (in the ordering corresponding to p) since $H_{ij}^{(p)} = 0$ for $j > n$. Therefore we can write $S^{(pq)} = (S\ 0)$ where S denotes the matrix formed by the first n columns. Let $\mathcal{M} = (\partial f_i/\partial X_{k_j})_{1\le i,j\le n}$. The relations $S^{(pq)}\partial f/\partial X_{k_j} \in (d,g)$ take the form $(S\ 0)\binom{\mathcal{M}}{*} \in (d,g)$ or $S\mathcal{M} \in (d,g)$. By multiplying this by the adjoint matrix of $\mathcal{M}$ and then by N, we get $pS^{(pq)} \equiv 0 \mod (d,g)$.

Now $H^{(p)}Z \equiv pZ \mod (d, F^{(p)})$ so $S^{(pq)}Z = qH^{(p)}Z - H^{(q)}H^{(p)}Z \equiv qpZ - pH^{(q)}Z = p(qZ - H^{(q)}Z) \equiv pF^{(q)} \mod (d, F^{(p)})$.

Let $E^{(p)} = (R[X,Z]/(g,F^{(p)}))_p$. Then $S^{(pq)} = 0$ in $E^{(p)}/dE^{(p)}$ so $F^{(q)} = 0$ in $E^{(p)}/dE^{(p)}$ showing that $F^{(q)} \in dE^{(p)}$. Now $dF^{(q)} \in (g)$ so $dF^{(q)}$ is 0 in $E^{(p)}$. We will show that $E^{(p)}$ is smooth over R. Therefore it is flat over R so that $\operatorname{Ann}(d) = \operatorname{Ann}(d^2)$ in $E^{(p)}$ (see Lemma 18.2) and we deduce that $F^{(q)}$ is 0 in $E^{(p)}$. This shows that $E^{(p)} = D_p$ so that $p \in H_{D/R}$. Since $\pi^{-1}(\mathfrak{h}_{\bar{C}})$ is the radical of the ideal generated by d and the p's, we conclude that $\pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \mathfrak{h}_D$ as required.

It remains to show that $E^{(p)}$ is smooth over R. Since $dF_i^{(p)} = -pg_i + \sum_{j=1}^{n} H_{ij}^{(p)} g_j$, all the g_i will be 0 in $(R[X,Z]/(g_1,\dots,g_n,F^{(p)}))_p$ so that $E^{(p)} = (R[X,Z]/(g_1,\dots,g_n,F^{(p)}))_p$. Since $F_i^{(p)} = pZ_i - \sum_{j=1}^{n} H_{ij}^{(p)} Z_j - dG_i^{(p)}$ (and is 0 for $i \le n$) we can solve for the Z_i with $i > n$ and conclude that $E^{(p)} = (R[X,Z_1,\dots,Z_n]/(g_1,\dots,g_n))_p$. Now $g_i = f_i - dZ_i$ so $\partial g/\partial(X,Z) = (\partial f/\partial X| - dI_n)$. By definition, some $n \times n$ minor of $\partial f/\partial X$ divides p showing that $E^{(p)}$ is smooth over R.

18. The desingularization lemma.

Lemma 18.1. *Let $R \to \Lambda$ be a map of noetherian rings and let $d \in R$ satisfy* $\operatorname{Ann}(d^2) = \operatorname{Ann}(d)$ *in Λ. Let $\tilde{R} = R/d^4R$, $\tilde{\Lambda} = \Lambda/d^4\Lambda$, and similarly for other R-algebras. Let $R \to A \to \Lambda$ with A of finite type over R. Suppose that $d|A$ is strictly standard and suppose there is a retraction (of $\tilde{R}$-algebras) $\rho : \tilde{A} \to \tilde{R}$ such that*

$$\begin{tikzcd} \tilde{A} \arrow[r] \arrow[d, "\rho"'] & \tilde{\Lambda} \arrow[d, equal] \\ \tilde{R} \arrow[r] & \tilde{\Lambda} \end{tikzcd}$$

commutes. Let $\mathfrak{a}$ be the annihilator in R of $\operatorname{Ann}_R(d^2)/\operatorname{Ann}_R(d)$. *Then we can find $R \to A \to B \to \Lambda$ with B of finite type over R such that $\mathfrak{a}B \subset H_{B/R}$.*

Proof. Let $A = R[X_1,\dots,X_N]/I$ and let $\rho(X_i) = \tilde{y}_i$ in $\tilde{R}$. Lift $\tilde{y}_i$ to y_i in R. If $q(X) \in I$ then $q(\tilde{y}) = 0$ in $\tilde{R}$ so $q(y) \in d^4R$. Let $P(X) \in \Delta_{(f)}[(f){:}I]$ (in $R[X]$) represent $d|A$ so that $d - P(X) \in I$. Then $d - P(y) \in d^4R$ so we can write $P(y) = ds$ where $s \in R$ satisfies $s \equiv 1 \mod d$.

Now $P(X) = \sum \ell_\nu m_\nu$ where the m_ν are the $r \times r$ minors of $(\partial f/\partial X)$. Let

$$H_1 = \begin{pmatrix} \partial f_1/\partial X_1 & \dots & \partial f_1/\partial X_N \\ \dots & \dots & \dots \\ \partial f_r/\partial X_1 & \dots & \partial f_r/\partial X_N \\ 0 & & I_{N-r} \end{pmatrix}$$

so that $\det H_1 = m_1$ and define H_ν similarly for each ν so that $\det H_\nu = m_\nu$ and the first r rows of H_ν are the same as for H_1. Let G'_ν be the adjoint matrix of H_ν and let

$G_\nu(X) = \ell_\nu G'_\nu$ so that $G_\nu H_\nu = H_\nu G_\nu = \ell_\nu m_\nu 1_N$ and therefore $P(X)1_N = \sum G_\nu H_\nu$. In particular, $P(y)1_N = \sum G_\nu(y)H_\nu(y) = \sum \ell_\nu(y)m_\nu(y) = sd1_N$.

Let ξ_i be the image of X_i in Λ and let η_i be the image of y_i in Λ. Then $\xi_i \equiv \eta_i \mod d^4\Lambda$ so we can write $\xi_i = \eta_i + d^3\epsilon_i$ with $\epsilon_i \in d\Lambda$. Let ϵ be the column vector $(\epsilon_1, \ldots, \epsilon_N)$ and let $H_\nu(y)\epsilon = v^{(\nu)}$ be the column vector $(v_1^{(\nu)}, \ldots, v_N^{(\nu)})$ with entries in $d\Lambda$. Then $\sum_\nu G_\nu(y)v^{(\nu)} = P(y)\epsilon = sd\epsilon$ in Λ so $s(\xi - \eta) = sd^3\epsilon = d^2 \sum G_\nu(y)v^{(\nu)}$.

Since the first r rows of H_ν are the same for all ν, we see that the same is true of $v^{(\nu)}$. In other words, $v^{(\nu)} = (u_1, \ldots, u_r, v_{r+1}^{(\nu)}, \ldots, v_N^{(\nu)})$ where the $u_1, \ldots, u_r$ are independent of ν.

Let $h_i(X, W, V) = s(X_i - y_i) - d^3W_i - d^2(\sum G_\nu(y)V^{(\nu)})_i$. Here the variables $V^{(\nu)}$ are assumed to have the form $V^{(\nu)} = (U_1, \ldots, U_r, V_{r+1}^{(\nu)}, \ldots, V_N^{(\nu)})$ where the $U_1, \ldots, U_r$ are independent of ν. Then h_i maps to 0 under the map $R[X, W, V] \to \Lambda$ sending X_i to ξ_i, W_i to 0, and $V^{(\nu)}$ to $v^{(\nu)}$.

Now $f_i(X) - f_i(y) = \sum_j \frac{\partial f_i}{\partial X_j}(y)[X_j - y_j]$ + higher order terms in $X_j - y_j$. Since $s(X_i - y_i) \equiv d^3W_i + d^2(\sum G_\nu(y)V^{(\nu)})_i \mod h$, we see that if $m = \max\deg f_i$ then, $s^m f_i(X) - s^m f_i(y) \equiv \sum_j s^{m-1} \frac{\partial f_i}{\partial X_j}(y)[d^3W_j + d^2(\sum G_\nu(y)V^{(\nu)})_j] + d^4Q'_i \mod h$ with $Q'_i \in (W, V)^2R[W, V]$. Therefore, $s^m f_i(X) - s^m f_i(y) \equiv s^{m-1}d^2 \sum_j \frac{\partial f_i}{\partial X_j}(y)[(\sum G_\nu(y)V^{(\nu)})_j] + d^3Q_i \mod h$, where $Q_i \in \sum RW_j + d(W, V)^2R[W, V]$.

But $\sum_j \frac{\partial f_i}{\partial X_j}(y)[(G_\nu(y)V^{(\nu)})_j$ is the i-th entry of $H_\nu(y)G_\nu(y)V^{(\nu)} = \ell_\nu(y)m_\nu(y)V^{(\nu)}$ and, since $i \leq r$, this entry is $\ell_\nu(y)m_\nu(y)U_i$. Summing on ν gives dsU_i. Therefore, we get $s^m f_i(X) - s^m f_i(y) \equiv s^m d^3U_i + d^3Q_i \mod h$.

Since $f_i(y)$ lies in d^4R, we can write $f_i(y) = d^3c_i$ with c_i in dR. Define $g_i = s^m c_i + s^m U_i + Q_i$, and note that g_i lies in $R[W, V]$ since no X_i occur. The above calculation shows that $d^3g_i = s^m d^3c_i + d^3(s^m U_i + Q_i) = s^m f_i(y) + d^3(s^m U_i + Q_i) \equiv s^m f_i(X) \mod h$ so we have

$$(*) \qquad d^3g_i \equiv s^m f_i(X) \mod h.$$

We now choose $B = R[X, W, V]/(I, g, h) = A[W, V]/(g, h)$ and define $\varphi : B \to \Lambda$ by sending X to ξ, W to 0, and $V^{(\nu)}$ to $v^{(\nu)}$. This is well defined: It is clear that $\varphi(h_i) = 0$. Since $\varphi(f_i) = 0$, $(*)$ implies that $d^3\varphi(g_i) = 0$ but c_i lies in dR, $\varphi(W) = 0$, $v^{(\nu)} \in d\Lambda$, and $\varphi(Q) \in d\Lambda$ because $Q \in \sum RW_j + d(W, V)^2R[W, V]$. Therefore $\varphi(g)$ lies in $d\Lambda$ so $d^3\varphi(g) = 0$ implies $\varphi(g) = 0$.

We claim that d lies in $H_{B/R}$. Note that $B_d = A_d[W, V]/(h)$ since $(*)$ implies that $g = 0$ in this ring. We can solve the equations $h_i = 0$ for the W_i so that $B_d = A_d[V]$. It follows that B_d is smooth over A_d which in turn is smooth over R (since $d \in H_{A/R}$), showing that $d \in H_{B/R}$ also.

Let $C = R[X, W, V]/(g, h)$ so that $B = C/IC$. By $(*)$ and the fact that $dI \subset (f)$ we have $C_{ds} \xrightarrow{\approx} B_{ds}$. Therefore $ds \in H_{C/R}$ since B_d is smooth over R.

Next we show that $s \in H_{C/R}$. Note first that, in $C_s = R_s[X, W, V]/(g, h)$, we can solve the equations $h_i = 0$ for the X_i so that $C_s = R_s[W, V]/(g)$. Now $(g){:}(g) = (1)$ and the Jacobian matrix $(\partial g/\partial U)$ satisfies $(\partial g/\partial U) \equiv s^m 1_r \mod d$ since $s^m c_i$ is constant and $Q \in \sum RW_j + d(W, V)^2R[W, V]$. Taking determinants, we see that for some e, $s^M + de$ lies in H_{C_s/R_s}. It follows that $s^{M+1} + sde \in H_{C/R}$ and therefore $s \in H_{C/R}$ since $ds \in H_{C/R}$.

Now $IC_s \subset dC_s$ since $X_i \equiv y_i \mod d$ in C_s (because $h = 0$), so if $q(X) \in I$ then $q(X) \equiv q(y) \equiv 0 \mod d$.

Since $dI \subset (f)$ and $f_i \mapsto 0$ in C_s by $(*)$, we get $dIC_s = 0$. But we have just seen that $IC_s \subset dC_s$ so $IC_s = d\mathfrak{b}$ for some $\mathfrak{b}$. Therefore $d^2\mathfrak{b} = 0$ but C_s is smooth and therefore flat over R so it follows that $d\mathfrak{a}\mathfrak{b} = 0$ by the following easy lemma. Note that $a \in \mathfrak{a}$ if and only if $a\,\mathrm{Ann}_R(d^2) \subset \mathrm{Ann}_R(d)$ which is equivalent to $\mathrm{Ann}_R(d^2) \subset \mathrm{Ann}_R(ad)$.

Lemma 18.2. *Let $A \to B$ be flat and let $a, b \in A$. If $\mathrm{Ann}_A(a) \subset \mathrm{Ann}_A(b)$, then $\mathrm{Ann}_B(a) \subset \mathrm{Ann}_B(b)$.*

Proof. Tensor the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ann}_A(a) \arrow[r] \arrow[d] & A \arrow[r, "a"] \arrow[d, "b"] & A \\
& 0 \arrow[r] & A &
\end{tikzcd}$$

with B.

Now $\mathfrak{a}IC_s = d\mathfrak{a}\mathfrak{b} = 0$ so if $a \in \mathfrak{a}$ then $IC_{sa} = 0$, showing that $C_{sa} = B_{sa}$ and therefore that $sa \in H_{B/R}$ since C_s is smooth over R. Since $s \equiv 1 \mod d$ and $d \in H_{B/R}$, we see that $a \in H_{B/R}$ as required.

Corollary 18.3. *Let $R \to \Lambda$ be a map of noetherian rings and let $d \in R$ satisfy $\mathrm{Ann}(d^2) = \mathrm{Ann}(d)$ in R and in Λ. Let $\tilde{R} = R/d^4R$, $\tilde{\Lambda} = \Lambda/d^4\Lambda$, and similarly for other R-algebras. Let $R \to A \to \Lambda$ with A of finite type over R. Suppose that $d|A$ is strictly standard. Let $R \to D \to \Lambda$ with D of finite type over R and suppose there is a map (of $\tilde{R}$-algebras) $f : \tilde{A} \to \tilde{D}$ such that*

$$\begin{tikzcd}
\tilde{R} \arrow[r] \arrow[d, equal] & \tilde{A} \arrow[r] \arrow[d, "f"'] & \tilde{\Lambda} \arrow[d, equal] \\
\tilde{R} \arrow[r] & \tilde{D} \arrow[r] & \tilde{\Lambda}
\end{tikzcd}$$

commutes. Then we can find $R \to B \to \Lambda$ with B of finite type over R with maps $A \to B$ and $D \to B$ such that

$$\begin{tikzcd}
R \arrow[r] \arrow[d, equal] & A \arrow[r] \arrow[d] & \Lambda \arrow[d, equal] \\
R \arrow[r] \arrow[d, equal] & B \arrow[r] & \Lambda \arrow[d, equal] \\
R \arrow[r] & D \arrow[r] \arrow[u] & \Lambda
\end{tikzcd}$$

commutes and such that $H_{D/R}B \subset H_{B/R}$ (so $\mathfrak{h}_D \subset \mathfrak{h}_B$).

Proof. Let $E = A \otimes_R D$. There is a retraction $\rho : \tilde{E} \to \tilde{D}$ given by $\rho(\tilde{a} \otimes \tilde{x}) = f(\tilde{a})\tilde{x}$ so Lemma 18.1 applies to $D \to E \to \Lambda$. Note that $d|E$ is strictly standard with respect to D by Lemma 4.8. We get $D \to E \to B \to \Lambda$ with $\mathfrak{a}B \subset H_{B/D}$ where $\mathfrak{a} = \mathrm{Ann}_D(\mathrm{Ann}_D(d^2)/\mathrm{Ann}_D(d))$. If $c \in H_{D/R}$, then D_c is smooth and therefore flat over R so $\mathrm{Ann}_{D_c}(d^2) = \mathrm{Ann}_{D_c}(d)$ by Lemma 18.2 since $\mathrm{Ann}_R(d^2) = \mathrm{Ann}_R(d)$. Therefore $\mathfrak{a}_c = D_c$ and so $B_c \subset (H_{B/D})_c = H_{B_c/D_c}$ showing that B_c is smooth over D_c and therefore over R so that $c \in H_{B/R}$.

Proof of Lemma 11.3. We have already observed that it will suffice to do the case $c = 8$. Let $R \to A \to \Lambda$ with $a \in R$ such that

(1) $\operatorname{Ann}_R a^2 = \operatorname{Ann}_R a$ and $\operatorname{Ann}_\Lambda a^2 = \operatorname{Ann}_\Lambda a$.
(2) $a|A$ is strictly standard.

Let $\bar{R} = R/a^8R$, $\bar{\Lambda} = \Lambda/a^8\Lambda$, etc. and let $\tilde{R} = R/a^4R$, $\tilde{\Lambda} = \Lambda/a^4\Lambda$, etc. Let $\pi : \Lambda \to \bar{\Lambda}$ be the canonical map.

Suppose that we have $\bar{R} \to \bar{A} \to \bar{C} \to \bar{\Lambda}$ with $\bar{C}$ of finite type over $\bar{R}$. By Lemma 17.1 with $d = a^4$, we can find $R \to D \to \Lambda$ with a map $\bar{C} \to \tilde{D}$ such that $\pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \mathfrak{h}_D$. Now apply Corollary 18.3 to $R \to A \to \Lambda$ and $R \to D \to \Lambda$ using $d = a$. The map $\tilde{A} \to \tilde{D}$ is given by $\tilde{A} \to \tilde{C} \to \tilde{D}$ induced by $\bar{C} \to \tilde{D}$. By Corollary 18.3 we get $R \to A \to B \to \Lambda$ with B of finite type over R such that $\pi^{-1}(\mathfrak{h}_{\bar{C}}) \subset \mathfrak{h}_D \subset \mathfrak{h}_B$.

REFERENCES

[A5] M. André, *Cinq exposés sur la désingularisation*, Handwritten manuscript, École Polytechnique Fédérale de Lausanne, 1991.

[Ah] M. André, *Homologie des Algèbres Commutatives*, Springer–Verlag, Berlin, 1974.

[Aa] M. Artin, *Algebraic approximation of structures over complete local rings*, Publ. Math. IHES **36** (1969), 23–58.

[BIV] R. Brüske, F. Ischebeck, und F. Vogel, *Kommutative Algebra*, B.I. Wissenschaftsverlag, Mannheim, 1989.

[BR] S. M. Bhatwadekar and R. A. Rao, *On a question of Quillen*, Trans. Amer. Math. Soc. **279** (1983), 801–810.

[CS] I. Cohen and A. Seidenberg, *Prime ideals and integral dependence*, Bull. Amer. Math. Soc. **52** (1946), 252–261.

[E] R. Elkik, *Solutions d'équations à coefficients dans un anneau hensélien*, Ann. Sci. ENS **6** (1973), 553–604.

[Ez] E. G. Evans, *A generalization of Zariski's Main Theorem*, Proc. Amer. Math. Soc. **26** (1970), 45–48.

[F] G. Faltings, *Ein einfacher Beweis, dass geometrische Regularität formale Glattheit impliziert*, Arch. Math. (Basel) **30** (1978), 284–285.

[SGA1] A. Grothendieck, *Revêtements étales et groupe fondamentale, SGA1*, Lecture Notes in Math. 224, Springer–Verlag, Berlin, 1971.

[EGA IV] A. Grothendieck and J. Dieudonné, *Éléments de géometrie algébrique IV*, Publ. Math. I.H.E.S. **20** (1964); **24** (1965); **28** (1966); **32** (1967).

[I] B. Iversen, *Generic Local Structure in Commutative Algebra*, Lecture Notes in Math. 310, Springer–Verlag, Berlin, 1973.

[K] I. Kaplansky, *Commutative Rings*, The University of Chicago Press, Chicago, 1974.

[L] H. Lindel, *On the Bass-Quillen conjecture concerning projective modules over polynomial rings*, Invent. Math. **65** (1981), 319–323.

[M] H. Matsumura, *Commutative Algebra*, Benjamin, New York, 1980.

[O] T. Ogoma, *General Néron desingularization based on the idea of Popescu*, J. Algebra **167** (1994), 57–84.

[Pz] C. Peskine, *Une généralisation du "Main Theorem" de Zariski*, Bull. Sci. Math. **90** (1966), 119–127.

[Pn] D. Popescu, *General Néron desingularization*, Nagoya Math. J. **100** (1985), 97–126.

[Pa] D. Popescu, *General Néron desingularization and approximation*, Nagoya Math. J. **104** (1986), 85–115.

[Pl] D. Popescu, *Letter to the Editor General Néron desingularization and approximation*, Nagoya Math. J. **118** (1990), 45–53.

[Pp] D. Popescu, *Polynomial rings and their projective modules*, Nagoya Math. J. **113** (1989), 121–128.

[Pq] D. Popescu, *On a question of Quillen*, to appear.

[Q] D. Quillen, *On the (co–) homology of commutative rings*, Applications of Categorical Algebra, Proc. Symp. Pure Math. XVII, Amer. Math. Soc., Providence, 1970, pp. 65–87.

[R] M. Raynaud, *Anneaux Henséliens*, Lecture Notes in Math. 169, Springer–Verlag, Berlin, 1970.

[S] M. Spivakovsky, *Smoothing of ring homomorphisms, approximation theorems, and the Bass-Quillen conjecture*, to appear (1993).

[T] B. Tessier, *Résultats récents sur l'approximation des morphisms en algèbre commutative, [d'après Artin, Popescu, et Spivakovsky]*, Séminaire Bourbaki **784** (1994), 1–15.

MATH. DEPT., UNIVERSITY OF CHICAGO, CHICAGO, IL 60637 USA
E-mail address: swan@math.uchicago.edu