MATH 615 LECTURE NOTES, WINTER, 2010

by Mel Hochster

ZARISKI'S MAIN THEOREM, STRUCTURE OF SMOOTH, UNRAMIFIED, AND ÉTALE HOMOMORPHISMS, HENSELIAN RINGS AND HENSELIZATION, ARTIN APPROXIMATION, AND REDUCTION TO CHARACTERISTIC p

Lecture of January 6, 2010

Throughout these lectures, unless otherwise indicated, all rings are commutative, associative rings with multiplicative identity and ring homomorphisms are *unital*, i.e., they are assumed to preserve the identity. If R is a ring, a given R-module M is also assumed to be *unital*, i.e., $1 \cdot m = m$ for all $m \in M$. We shall use $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ and $\mathbb{C}$ to denote the nonnegative integers, the integers, the rational numbers, the real numbers, and the complex numbers, respectively.

Our focus is very strongly on Noetherian rings, i.e., rings in which every ideal is finitely generated. Our objective will be to prove results, many of them very deep, that imply that many questions about arbitrary Noetherian rings can be reduced to the case of finitely generated algebras over a field (if the original ring contains a field) or over a discrete valuation ring (DVR), by which we shall always mean a Noetherian discrete valuation domain. Such a domain V is characterized by having just one maximal ideal, which is principal, say pV, and is such that every nonzero element can be written uniquely in the form up^n where u is a unit and $n \in \mathbb{N}$. The formal power series ring $K[[x]]$ in one variable over a field K is an example in which $p = x$. Another is the ring of p-adic integers for some prime $p > 0$, in which case the prime used does, in fact, generate the maximal ideal.

One can make this sort of reduction in steps as follows. First reduce to the problem to the local case. Then complete, so that one only needs to consider the problem for complete local rings.

We shall study Henselian rings and the process of Henselization. We shall give numerous characterizations of Henselian rings. In good cases, the Henselization consists of the elements of the completion algebraic over the original ring. The next step is to "approximate" the complete ring in the sense of writing it as a direct limit of Henselian rings that are Henselizations of local rings of finitely generated algebras over a field or DVR. But this is done in a "good" way, where many additional conditions are satisfied. The result needed is referred to as *Artin approximation*.

We are not yet done. Henselizations are constructed as direct limits of localized étale extensions, and so we are led to study étale and other important classes of ring extensions, such as smooth extensions and unramified extensiions. (The étale extensions are the extensions that are both smooth and unramified.) There is a beautiful structure theory for

these classes of extensions. Because étale extensions are finitely generated algebras, one can take the fourth step, which is to replace the Henselian ring by a ring that is finitely generated over a field or DVR. Carrying out these ideas in detail will take up a large portion of these notes.

Étale extensions have numerous applications to geometry: they are used to remedy the fact that the implicit function theorem does not hold in the allgebraic context in the same sense that it is does when working with C^∞ or analytic functions. As an example, we shall later use the theory of étale extensions to establish a relationship that is not obvious between intersection multiplicities defined algebraically and intersection multiplicities defined quite geometrically.

The structure theorems we want to prove depend on an algebraic result known as Zariski's Main Theorem, or ZMT. It has many applications in commutative algebra and algebraic geometry.

In our formal treatment, we shall first prove Zariski's Main Theorem, and then define and analyze the structure of smooth, étale, and unramified homomorphisms. We shall discuss Henselization, Artin approximation, and applications in which one reduces questions about arbitrary Noetherian rings to the case of algebras finitely generated over a field or a discrete valuation ring (DVR).

Another tool that we introduce provides a method for reducing many questions about finitely generated algebras over a field of characteristic 0 to corresponding questions for finitely generated algebras over a field of characteristic $p > 0$: in fact to the case where that field is finite! It may be surprising that one can do this: it turns out to be a very powerful technique.

I do want to emphasize that the theory we build here shows that the study of finitely generated algebras over a field or DVR is absolutely central to the study of arbitrary Noetherian rings.

Before stating Zariski's Main Theorem, we review some facts from commutative algebra that we assume in the sequel. Following the review, we state the algebraic form of the theorem, review some basic algebraic geometry, and then give a geometric version of ZMT. We explain how to deduce the geometric version from the algebraic version, and then go to work on the proof of the algebraic version, which is rather long and difficult.

A *prime* ideal of R is a a proper ideal such that R/P is an integral domain. The (0) ideal is prime if and only if R is an integral domain. The unit ideal is never prime. The set of prime ideals of R, denoted $\mathrm{Spec}\,(R)$ is a topological space in the Zariski topology, which is characterized by the fact that a set of primes is closed if and only if it has the the form $\mathcal{V}(I) = \{P \in \mathrm{Spec}\,(R) : I \subseteq P\}$. I may be any subset of R, but $\mathcal{V}(I)$ is unchanged by replacing I by the ideal it generates, so that one may assume that I is an ideal. When I is an ideal, $V(I)$ is unchanged by replacing I by $\mathrm{Rad}\,(I) = \{r \in R : \text{for some integer } n > 0, r^n \in I\}$. The closed sets of $\mathrm{Spec}\,(R)$ are in bijective order-reversing correspondence with the radical ideals of R. The closure of the point given by the prime ideal P is $\mathcal{V}(P)$, so that P is a closed point if and only if P is a maximal ideal of R. Note that $\mathrm{Spec}\,(R)$ is not, in general, T_1.

If $f \in R$, D_f denotes $\mathrm{Spec}\,(R) - \mathcal{V}(Rf)$, the set of prime ideals of R not containing f. The sets D_f are a basis for the open sets of the Zariski topology on R. Note that $D_{fg} = D_f \cup D_g$.

Let $h : R \to S$ be a ring homomorphism. Then h^* or $\mathrm{Spec}\,(h)$ denotes the map $\mathrm{Spec}\,(S) \to \mathrm{Spec}\,(R)$ whose value on $Q \in \mathrm{Spec}\,(S)$ is the inverse image $h^{-1}(Q)$ under h. This inverse image is also called the *contraction* of Q to R. Note that if $R \subseteq S$, the contraction of Q to R is simply $Q \cap R$. We assume some familiarity with categories and functors. Spec is a contavariant functor from the category of commutative rings and ring homomorphisms to the category of topological spaces and continuous maps. (Very briefly, functors assign values to objects and morphisms in a category in such a way that identity maps are preserved, and composition is either preserved or reversed. Functors preserving composition are called *covariant*, while those reversing composition are called *contravariant*.)

A *multiplicative system* W in a ring R is a subset that contains 1 is closed under multiplication. The localization of R at W, denoted $W^{-1}R$, is an R-algebra in which every element of W becomes invertible. Every R-module M also has a localization at W, denoted $W^{-1}M$, which is a $W^{-1}R$-module. ($W^{-1}M$ may be defined as equivalence classes of pairs $(m, w) \in M \times W$ where (m, w) is equivalent to (m', w') if there exists $v \in W$ such that $v(w'm - wm') = 0$. The equivalent class of (m, w) is denote m/w. $W^{-1}M$ and an $W^{-1}R$-module. Addition and multiplication by scalars are such that $(m/w) + (m'/w') = (w'm + wm')/(ww')$, $r(m/w) = (rm)/w$, and $(r/v)(m/w) = (rm)/((vw)$. There is an R-linear map $M \to W^{-1}M$ that sends $m \mapsto m/1$. *This map need not be injective.* In fact, the kernel consists of all elements $m \in M$ such that $wm = 0$ for some $w \in W$. These remarks include the case $M = R$. Note that $W^{-1}R$ is a ring, and the multiplication satisfies $(r/w)(r/w') = (rr')/(ww')$. $M \to W^{-1}M$ is injective if and only if no element of W is a zerodivisor on M, i.e., multiplication by every $w \in W$ gives an injective map $M \to M$.

Note also that a homomorphism $R \to S$ can be factored $R \to W^{-1}R \to S$ if and only if the image of W in S consists entirely of units, in which case the factorization is unique. This is referred to as *the universal mapping property of localization.* The notation M_W is used as an alternative to $W^{-1}M$, but we will not use this notation in these notes.

There is a canonical isomorphism $W^{-1}R \otimes_R M \to W^{-1}M$ such that $(r/w) \otimes m \mapsto (rm)/w$ and, under the inverse isomorphism, $m/w \mapsto (1/w) \otimes m$. $M \mapsto W^{-1}M$ is a covariant exact functor from R-modules to $W^{-1}R$-modules: if $f : M \to N$, there is a unique map $W^{-1}M \to W^{-1}N$ such that $m/w \mapsto f(m)/w$.

If P is a prime ideal of R, $W = R - P$ is a multiplicative system (this characterizes which ideals are prime). In this case $W^{-1}R$ is denoted R_P and is called the *localization of R at P*. Likewise, $W^{-1}M$ is denoted M_P. There is a canonical isomorphism of $R_P \otimes_R \cong M_P$.

If $S = W^{-1}R$, there is a bijective homeomorphism between $\mathrm{Spec}\,(W^{-1}R)$ and

$$\{P \in \mathrm{Spec}\,(R) : W \cap P = \emptyset\}$$

(with the inherited Zariski toipology from $\mathrm{Spec}\,(R)$. The maps send $Q \in \mathrm{Spec}\,(W^{-1}R)$ to its contraction to R, and $P \in \mathrm{Spec}\,(R)$ to its expansion PS to S. (For any homomorphism

$R \to S$, if I is an ideal of R its expansion IS is the ideal of S generated by the image of I.) Thus, there is bijection between the primes of $W^{-1}R$ and the primes of R that do not meet W.

If $R \to S$ is surjective, then $S \cong R/I$, where I is the kernel. In this case there is a homeomorphism of $\mathrm{Spec}\,(R/I)$ with $\mathcal{V}(I) \subseteq \mathrm{Spec}\,(R)$, again given by contraction and expansion.

When S is an R-algebra and W is a multiplicative system in S, we have a definition for $W^{-1}S$: we may think of S as an R-module. This is canonically isomorphic with S-algebra $V^{-1}S$ obtained by localizing S at the image of W. If P is a prime ideal and $W = R - P$, this gives an identification of R_P/PR_P with the fraction field of R/P. This field is often denoted κ_P, but the notation is ambiguous, since it conceals the dependence on R.

If W is a multiplicative system in R and I is an ideal of R, the R-algebras $S = W^{-1}(R/I)$ and $W^{-1}R/IW^{-1}R$ are canonically isomorphic. In this case we may put the facts above together to conclude that $\mathrm{Spec}\,(S) \to \mathrm{Spec}\,(R)$ gives a homeomorphism of $\mathrm{Spec}\,(S)$ with the set of prime ideals of R that contain I and are disjoint from W (in the inherited Zariski topology from $\mathrm{Spec}\,(R)$.

Let $h : R \to S$ be a ring homomorphism and let $f = \mathrm{Spec}\,(h)$ be the continuous map $\mathrm{Spec}\,(S) \to \mathrm{Spec}\,(R)$ given by contraction of prime ideals.. (Sometimes f is denote h^*.) The set-theoretic fiber of f over a prime P is $f^{-1}(P)$, i.e., the set of primes Q of S that contract to P. The primes that contract to P are also said to *lie over* P. By taking $I = P$ and $W = R - P$,

this set of primes may be identified with $\mathrm{Spec}\,(W^{-1})S/PS$, for Q lies over P if and only if it contains the image of P, and, hence, PS, and is disjoint from the image of W. The ring

$$W^{-1}(S/PS) \cong (W^{-1}S)/(PW^{-1}S) \cong \kappa_P \otimes_R S$$

is called the *scheme-theoretic fiber* of $R \to S$ over P. This point of view enables one to think of the set-theoretic fiber $f^{-1}(P)$ as the space of prime ideals of the scheme-theoretic fiber, $(R-P)^{-1}S/P(R-P)^{-1}S \cong \kappa_P \otimes_R S$.

A prime Q of S that lies over P in R is called *isolated in its fiber* or *isolated in the fiber over* P if it is both maximal and minimal among primes lying over P. In particular, if Q is the unique prime lying over P then it is isolated in its fiber. We shall return to this notion soon and explain the use of the word "isolated" here, but we first want to state Zariski's Main Theorem, which we sometimes abbreviate ZMT.

We next want to recall the notion of integral dependence of elements. If $R \subseteq S$ we say that an element $s \in S$ is *integral* over R if it is a root of some monic polynomial with coefficients in R. In other words, s satsifies an equation of the form $s^n + r_{n-1}s^{n-1} + \cdots + r_j s^j + \cdots + r_1 s + r_0 = 0$ where n is a positive integer and the $r_j \in R$. The set of elements of S integral over R is a subring of S containing R called the *integral closure* of R in S. R is said to be *integrally closed* in S if the integral closure of R in S is R, i.e., every element of S integral over R is in R. An integral domain is called *integrally closed* or *normal* if it is integrally closed in its fraction field. Every unique factorization domain (UFD) is normal.

Theorem (Zariski's Main Theorem. *Suppose that $R \subseteq R[\theta_1, \ldots, \theta_n] \subseteq S$ are commutative rings and that R is integrally closed in S while S is integral over $R[\theta_1, \ldots, \theta_n]$. Let Q be a prime ideal of S that is isolated in its fiber over $P \in \operatorname{Spec}(R)$. Then there exists an element $f \in R - P$ such that the induced homomorphism $R_f \to S_f$ is an isomorphism.*

We want to examine some consequences of this result, including a very important geometric corollary, before we give the proof, which is difficult and lengthy.

We next review some basic algebraic geometry. Let K be an algebraically closed field. For simplicity, at this point we shall restrict our attention primarily to closed algebraic sets in some $\mathbb{A}^N_K$. Let X be such a set. Unless otherwise specified, when we refer to "points of X" we mean closed points. By a *variety* we mean a nonempty irreducible closed algebraic set in some $\mathbb{A}^N_K$. (As a scheme, a variety is reduced and irreducible.) We write $K[X]$ for the coordinate ring of the affine (closed) algebraic set X: it is the ring of regular functions from X to $K = \mathbb{A}^1_K$. It is a finitely generated reduced K-algebra (and, up to isomorphism, all such algebras occur). X is a variety iff $K[X]$ is a domain. Note that the category of (closed) affine algebraic sets over K and regular morphisms is anti-equivalent to the category of finitely generated reduced K-algebras and K-algebra homomorphisms: essentially, these are opposite categories. If X is a variety then the fraction field of $K[X]$ is denoted $K(X)$ and is called the *function field* of X. Its elements may be regarded as regular functions defined on some nonempty (equivalently, dense) open set in X, where two functions are equivalent if they agree on the intersection of their domains, which will be another dense open set. A morphism $g : X \to Y$ of varieties is called *dominant* if its image is dense. This holds if and only if the induced map of $K[Y] \to K[X]$ is injective, for that map has kernel containing I if and only if the image of g is contained $V(I) \subseteq Y$. A dominant map induces a map of function fields $K(Y) \to K(X)$, which is necessarily injective. By definition, the variety Y is normal precisely when $K[Y]$ is normal, i.e., integrally closed in its field of fractions $K(Y)$.

The following is a corollary of ZMT, and is also referred to as Zariski's Main Theorem. The restriction to affine varieties is not needed and is only made for simplicity. We shall explain how the Corollary is deduced in detail later.

Corollary (Zariski's Main Theorem). *Let $g : X \to Y$, be a morphism of affine varieties as in the preceding discussion. If g is bijective on closed points, Y is normal, and $K(X)$ is separable over $K(Y)$, then g is an isomorphism.*

We have not yet *proved* anything. We first want to discuss why some hypothesis other than having g be bijective on closed points is needed.

Let Y be $V(y^3 - z^2)$ in $\mathbb{A}^2_K$, which may also be described as the set $\{(\lambda^2, \lambda^3) : \lambda \in K\}$. Then $K[Y] \cong K[y,z]/(y^3 - z^2) \cong K[x^2, x^3] \subseteq K[x]$. Let $X = \mathbb{A}^1_K$. The map $X \to Y$ that sends λ to (λ^2, λ^3) is bijective. It corresponds to the map $K[Y] = K[y,z]/(y^3 - z^2) \cong K[x^2, x^3] \subseteq K[x] \cong K[X]$ that sends the images of y and z to x^2 and x^3, respectively. This is an example of a bijective map of varieties that is not an isomorphism: the problem, in some sense, is that $K[Y]$ is not normal — the element x is in its integral closure. Thus, Y is not normal. Note that the map of varieties cannot be an isomorphism because the corresponding map of K-algebras is not surjective, and therefore is not an isomorphism.

Even when both varieties are normal, or even regular, the separability condition is needed. Let K be an algebraically closed field of prime characteristic $p > 0$ and let $X = Y = \mathbb{A}^1_K$. Let $g : X \to Y$ be the map sending $\lambda \mapsto \lambda^p$. Since K is algebraically closed it is perfect, and so the map is surjective and therefore bijective. This morphism corresponds to the K-algebra map of rings $K[x] \to K[x]$ sending $x \mapsto x^p$, or to the inclusion $K[x^p] \subseteq K[x]$. The map of rings is not surjective and so g is not an isomorphism. The induced map of function fields is $K(x^p) \subseteq K(x)$, which is evidently not separable: that is the problem.

We next want to note that ZMT is rather non-trivial even in very special cases: it implies a key lemma that can be used to deduce Hilbert's Nullstellensatz very quickly. Suppose that in the statement of (the ring-theoretic form of) ZMT one assume that $R = K \subseteq L = S$ where K is an algebraic closed field and S is a field that is finitely generated as a K-algebra. Then ZMT applies: K is integrally closed in L because it is algebraically closed in L. Take $P = (0) \subseteq K$ and $Q = (0) \subseteq L$ as the two primes (of course, there are no other primes to choose). Evidently Q is isolated in its fiber, since L has only one prime. Then there exists $f \in K - P$ such that $K_f \cong L_f$. Since $f \neq 0$ it is already invertible in K and L, and so we see that $K = L$. That is, a field finitely generated as an algebra over an algebraically closed field K must be equal to K. This result is sometimes called Zariski's lemma. However, our proof of ZMT will not give a new proof of Hilbert's Nullstellensatz: we make use of Hilbert's Nullstellensatz in the argument.

We next want to explain the used of the word "isolated" in the expression "isolated in its fiber." A point x of a topological space X is called *isolated* if it is both open and closed in X. The fiber, as a topological space, is the Spec of the ring $A = \kappa_P \otimes_R S$, and so may be thought of as a topological space. We want to make two observations:

(1) If a prime m is an isolated point of $\mathrm{Spec}\,(A)$, then m is both maximal and minimal among the prime ideals of A.

(2) If A is Noetherian or, much more generally, if the prime ideal m is finitely generated, then m is an isolated point of $\mathrm{Spec}\,(A)$ if and only if m is both maximal and minimal in $\mathrm{Spec}\,(A)$.

To see this, first note that $\{m\}$ is closed if and only if m is maximal. Now $\{m\}$ is open if and only if there exists $f \in R$ such that mR_f is the unique prime ideal of R_f: this is the condition for $D(f) = \{m\}$. Since a prime has arbitrarily small open neighborhoods of the form $D(f)$, the set consisting of just that prime cannot be open unless it is equal to $D(f)$ for some choice of f. But if $m = D(f)$ it must be minimal: any strictly smaller prime would also be in $D(f)$. Finally, suppose that m is both maximal and minimal and that it is finitely generated, say by $u_1, \ldots, u_h$. If we localize at m it becomes the only prime of R_m, and so every u_j has become nilpotent. This implies that for every j we can choose $f_j \in R - m$ and N_j such that $f_j u^{N_j} = 0$. Let $f = f_1 \cdots f_h$. In the ring R_f, every generator of m is nilpotent. Since m is maximal, it is the only prime ideal of R_f, and thus $\{m\}$ is open as well as closed.

We next want to show how the geometric form of ZMT stated above follows from the algebraic form. We need the following basic facts about the behavior of dominant maps of

varieties:

Lemma. *Let $g : X \to Y$ be a dominant map of algebraic varieties, so that we have an injection of domains $K[Y] \hookrightarrow K[X]$. Then:*

(a) *The transcendence degree of $K(X)$ over $K(Y)$ is $\delta = \dim(X) - \dim(Y)$.*

(b) *There is a dense open subset U of Y such that for every $u \in U$, the dimension of the fiber $g^{-1}(u)$, thought of as a closed algebraic set in X, is $\delta = \dim(X) - \dim(Y)$.*

(c) *If $\dim(Y) = \dim(X)$ then $K(X)$ is a finite algebraic extension of $K(Y)$. Assume also that $K(X)$ is separable over $K(Y)$. Then there is a dense open set $U \subseteq Y$ such that for all $u \in U$, the fiber $g^{-1}(u)$ is a finite set of cardinality $d = [K(X) : K(Y)]$.*

Proof. Given any three fields $K \subseteq \mathcal{F} \subseteq \mathcal{G}$ the transcendence degree of $\mathcal{G}$ over K is the sum of the transcendence degree of $\mathcal{F}$ over K and the transcendence degree of $\mathcal{G}$ over $\mathcal{F}$. Part (a) follows from applying this to $K \subseteq K(Y) \subseteq K(X)$ along with the theorem that the dimension of a variety over K is the transcendence degree of its function field over K.

To prove part (b), let $R = K[Y] \subseteq K[X] = S$. Then S is a domain finitely generated over the domain R, and by the Noether normalization theorem for domains, we may localize at one nonzero element $f \in R$ so that S_f is a module-finite extension of a polynomial ring over R. The number of variables must be δ, the transcendence degree. Let U be the open set corresponding to $D(f)$ in Y. Thus, after replacing R and S by R_f and S_f, it suffices to show that if S is a module-finite domain extension of $R[x_1, \ldots, x_\delta]$, then all fibers over maximal ideals m of R have dimension δ. Since S/mS is module-finite over $(R/m)[x_1, \ldots, x_\delta]$ the dimension is at most δ. Since S has prime ideal Q lying over $mR[x_1, \ldots, x_\delta]$ by the lying over theorem, and we have $S/mS \twoheadrightarrow S/Q$, while S/Q is a module-finite extension domain of $(R/m)]x_1, \ldots, x_\delta]$, we also have that the dimension is at least δ.

It remains to consider part (c). We continue the notations from the proof of (b). The first statement is immediate from (a) and the fact that $S = K[X]$ is finitely generated over K and, hence, over $R = K[Y]$. We may localize at $f \in R - \{0\}$ and so assume that S is module-finite over R. Then $K(Y) \otimes_R S = K(X)$. Choose a primitive element θ for $K(X)$ over $K(Y)$: by multiplying by a suitable nonzero element in R, we may assume that θ is in S. Let G be the minimal monic polynomial of θ over the fraction field of R. By our hypothesis on the field extension, G will be separable over R. By inverting one more element of $R - \{0\}$ we may assume that the coefficients of G are in R. Note that $S/R[\theta]$, as an R-module, is torsion. Therefore we may invert yet another element of R and assume without loss of generality that $S = R[\theta]$, and then $S \cong R[x]/G$.

Consider the roots of G in a suitably large extension field of the fraction field of R. The product of the squares of their differences (the discriminant of G) is a symmetric polynomial over $\mathbb{Z}$ in the roots of G, and therefore is expressible as a polynomial D over $\mathbb{Z}$ in the coefficients of G, which, up to sign, are the elementary symmetric functions of the roots. The discriminant is therefore a nonzero element of R. We localize at the discriminant as well, and so we may assume that it is a unit of R. Note that each localization has the effect of restricting out attention to a smaller dense open subset of Y.

The points of the fiber over a m, a maximal ideal of R, correspond to the maximal ideals of $(R/m)[x]/\overline{G}$, where $\overline{G}$ is simply the image of G modulo m. But $R/m = K$ and the discriminant of $\overline{G}$ is simply the image of the discriminant of G (one substitutes the images of the coefficients of G into D), and so is not zero. It follows that the roots of G are mutually distinct, and so the number of points in the finite fiber is precisely the degree of G, which is the same as the degree of G and is equal to $[K(Y) : K(X)]$. $\square$

Lecture of Janauary 8, 2010

Proof of the geometric form of ZMT. We are now ready to deduce the geometric form of ZMT from the algebraic form. The fact that the map $g : X \to Y$ is bijective implies that it is dominant. Therefore, we may consider $R = K[Y] \subseteq K[X] = S$. We want to prove that $R = S$. Consider S/R as an R-module. If it is nonzero, then there is a maximal ideal m of R such that $(S/R)_m \neq 0$, and then $R_m \neq S_m$, where S_m is simply $(R - m)^{-1}S$. The bijectivity of the map shows that all set-theoretic fibers over closed points consist of exactly one closed point. From part (b) of the preceding Lemma, we must have $\dim(X) = \dim(Y)$, and then part (c) shows that the extension is algebraic of degree 1, which means that $K(X) = K(Y)$: note that we are using separability here. Since R_m is normal, it is integrally closed in S_m, for S_m is contained in the fraction field of R. Since S is finitely generated over R, S_m is finitely generated over R_m. The fiber S_m/mS_m contains just one prime ideal, which is isolated in its fiber. Therefore we can choose $f \in R_m - mR_m$ such that $(R_m)_f = (S_m)_f$. But since f is already invertible in R_m and S_m, this implies that $R_m = S_m$, a contradiction. $\square$

We are now ready to begin the proof of the algebraic form of ZMT. We have that $Q \in \mathrm{Spec}(S)$ is isolated in its fiber over $P \in \mathrm{Spec}(R)$, where $R[\theta_1, \ldots, \theta_n] \subseteq S$ is integral, while R is integrally closed in S. We shall used induction on n. If $n = 0$, then S is integral over R, and since R is integrally closed in S, this implies that $R = S$, and we are done.

We postpone considering the case where $n = 1$. Instead, we assume this case for the moment, and carry through the inductive step. This will reduce the problem to studying the case where $n = 1$. For this purpose let T denote the integral closure of $R[\theta_1, \ldots, \theta_{n-1}]$ in S. Let $\theta = \theta_n$. Note that S is integral over $T[\theta]$. Let $q = Q \cap T$. We want to show that q is isolated in its fiber over R, which is the fiber over P, since it is clear that $q \cap R = Q \cap R = P$. Suppose that we can do this. Then we can choose $f \in R - P$ such that $R_f = T_f$, by the induction hypothesis. Now Q is evidently isolated in its fiber over q, since q lies over P in R, and this is preserved when we localize at f. Also, S is integral over $T[\theta]$, and so S_f is integral over $T_f[\theta]$. Thus, we can apply the case $n = 1$ to conclude that there exists $\gamma = T_f - qT_f$ such that $(T_f)_\gamma = (S_f)_\gamma$. Now, $T_f = R_f$, and it follows that $q_f = PR_f$, so that we may write $\gamma = g/f^h$ where $g \in R - P$. This gives $R_{fg} = (R_f)_\gamma = (T_f)_\gamma = (S_f)_\gamma = S_{fg}$, as required.

It remains to prove that q is isolated in its fiber over P.

We need the following result (think of S_0 as $R[\theta_1, \ldots, \theta_n]$).

Lemma. *Let $R \subseteq T \subseteq S$ be rings. Let Q be a prime of S lying over $P = Q \cap R$, and let $q = Q \cap T$.*

(a) *If Q is minimal in its fiber over T and $u \in T - q$ is such that $T_u = S_u$, then q is also minimal in its fiber over P.*

(b) *If S is integral over S_0, $R \subseteq S_0 \subseteq S$ with S_0 finitely generated over R, and Q is maximal in its fiber over T, then q is maximal in its fiber over P.*

(c) *If Q is isolated in its fiber, S is integral over a finitely generated R-subalgebra S_0, and there exists $u \in T - q$ such that $T_u = S_u$, then q is isolated in its fiber over T.*

Proof. To prove part (a) note that if q' is strictly contained in q and q' lies over P, we may expand q' to $T_u = S_u$ and then contract to S to obtain a prime Q' of S strictly smaller than Q and lying over P: we have a bijection between primes of T not containing u and prime of S not containing u.

For part (b), first replace R, T, and S by their localizations at P. Thus, we may assume that R is local with maximal ideal P. Then $R/P \subseteq T/q \subseteq S/Q$, and we also have $R/P \subseteq S_0/q' \subseteq S/Q$, where $q' = Q \cap S_0$. The fact that S is maximal in its fiber implies that S/Q is a field. Since S/Q is integral over S_0/q', S_0/q' is also a field, and it is finitely generated over R/P. It follows that S_0/q' is a finite algebraic extension of R/P. Now we get that S/Q is an algebraic extension of R/P. It now follows that T/q is a field, and this means that q is maximal in its fiber.

Part (c) is simply the result of combining (a) and (b). $\square$

We can now use this Lemma to to see that q as defined earlier is isolated in its fiber over P. We have the hypothesis of part (b). The hypothesis of part (a) also holds, because we may apply the case $n = 1$ to the inclusion $T \subseteq S$ (Q is obviously isolated in its fiber over q) to obtain $u \in T - q$ such that $T_f = S_f$). The result we need is now immediate from part (c). This completes the reduction to the case where $n = 1$. $\square$

Lecture of Janauary 11, 2010

For the remainder of the proof we shall be studying the case where $R \subseteq R[\theta] \subseteq S$. R is integrally closed in S, S is integral over $R[\theta]$, and Q, a prime of S, is isolated in its fiber over $P = Q \cap R$. We want to reduce to the case where S is actually module-finite over $R[\theta]$. For this purpose it will suffice to find T module-finite over $R[\theta]$ such that $R[\theta] \subseteq T \subseteq S$ and $q = Q \cap T$ is isolated in its fiber over P. For once we have T as specified, if we know the theorem in the module-finite case we can choose $f \in R - P$ such that $R_f = T_f \subseteq S_f$. Then R_f is integrally closed in S_f and S_f is integral over $T_f = R_f$ together imply that $R_f = S_f$. Quite generally, we are free to replace S by any ring T with $R[\theta] \subseteq T \subseteq S$ such that $Q \cap T$ is minimal in its fiber: by the argument just given, if the desired result holds for T then it holds for S.

Note that by part (b) of the Lemma of Janaury 8, we have that q is maximal in its fiber for any choice of T with $R[\theta] \subseteq T \subseteq S$. Thus, the problem is to choose T such that q is minimal in its fiber. Thus, we want to find $s_0, s_1, \ldots, s_h \in S$ such that with $T = R[\theta][s_0, s_1, \ldots, s_h]$, $q = Q \cap T$ is minimal in its fiber over P. For this purpose we may replace R, S by R_P, S_P and θ by its image in S_P. If we find elements

s_0/f_0, s_1/f_1, $\ldots$, s_h/f_h that work here, where the $s_j \in S$ and the $f_j \in R - P$, we may use s_0, s_1, $\ldots$, s_h, since the f_j become invertible in any case when we calculate the fiber. Let $K = R/P$. Let $\overline{\theta}$ be the image of θ in $R[\theta]/PR[\theta] \cong K[\overline{\theta}]$. If $\overline{\theta}$ satisfies a monic polynomial of positive degree over K, then we may take $T = R[\theta]$: the fiber is module-finite over K and, hence, zero-dimensional, and so all primes of the fiber of T over P will be isolated in that case. Therefore, we may assume without loss of generality that $\overline{\theta}$ is transcendental over K. Q lies over a prime of this ring that is maximal in its fiber, by part (b) of the Lemma of Janauary 8, and this prime will be generated by $g(\overline{\theta})$, where g is a monic polynomial over K. Lift this element to an element $\gamma \in R[\theta]$. Then $\gamma \in Q$ is nilpotent mod PS, since Q is minimal in its fiber.

Hence, we can choose $s_0 \in S - Q$, $p_1, \ldots, p_h \in P$, and $s_1, \ldots, s_h \in S$ such that $s_0\gamma^N = \sum_{j=1}^{h} s_j p_j$. Choose $T = R[\theta][s_0, s_1, \ldots, s_h]$. We claim that $q = Q \cap T$ is minimal in its fiber over P, for a smaller prime q_0 that lies over P will not contain s_0, and so must contain γ. But then q and q_0 contract to the same prime in $R[\theta]$, since there is only one prime that contains P and γ, and since T is integral over $R[\theta]$ it follows that $q = q_0$.

Once we have replaced S by a module-finite extension of $R[\theta]$, we may again replace R by R_P and S by S_P, and it suffices to see that $R_P = S_P$. For if these two are equal, then for each of the finitely many generators of S over R we may choose f_j multiplying that generator into R with $f_j \in R - P$. Let f be the product of the f_j. Then $R_f = S_f$. Henceforth we assume that $R = (R, P, K)$ is quasi-local as well.

If $A \subseteq B$ is module-finite the *conductor* of B in A is defined as $\{a \in A : Ba \subseteq A\}$. It is readily checked to be an ideal of A and an ideal of B. It is also easy to see that it is the largest ideal of A that is also an ideal of B, since any element a of such an ideal has the property that $Ba \subseteq A$.

Throughout the rest of the proof of ZMT, let J be the conductor of S in $R[\theta]$. The remainder of the proof breaks up into two cases: one where $J \nsubseteq Q$, which is easier, and one where $J \subseteq Q$. The second case will require two preliminary results.

We first discuss the case where $J \nsubseteq Q$. Let $u \in J - Q$. Then $R[\theta]_u = S_u$, and by part (a) of the Lemma of January 8, $Q \cap R[\theta]$ is isolated in its fiber over P. We may therefore replace S by $R[\theta]$: once we have the result for $R[\theta]$, the case of S follows, by the comment at the end of the first paragraph of the preceding page.

But then $R[\theta]/PR[\theta] = K[\overline{\theta}]$ cannot be a polynomial ring in $\overline{\theta}$ over K, for no prime could then be isolated. It follows that there is a polynomial in θ with at least one coefficient not in P whose value is in $PR[\theta]$. Subtracting, we find that there is a polynomial in θ over R that vanishes and has at least one coefficient not in P. Choose such a polynomial of least degree d, and call it $r_d\theta^n + r_{d-1}\theta^{d-1} + \cdots + r_0$. By multiplying the polynomial by r_d^{d-1}, we see that $r_d\theta$ is integral over R and therefore in R. Thus, we may re-write the polynomial as $(r_d\theta + r_{d-1})\theta^{d-1} + \cdots + r_0$, which has lower degree in θ. Therefore all of its coefficients are in P, and we conclude that $r_d\theta + r_{d-1} \in P$. If r_d is a unit, we find that $\theta \in R$, as required. If $r_d \in P$ and r_{d-1} is a unit, we find that $r_{d-1} \in PS$, a contradiction, since Q contains PS. This completes the proof for the case where $J \nsubseteq Q$.

In the remaining and most difficult case, where $J \subseteq Q$, we shall show that Q cannot be isolated in its fiber. We need two preliminary results.

Lemma. *If $R \subseteq R[\theta] \subseteq S$ are domains with S integral over $R[\theta]$ and θ is transcendental over R, then no prime ideal of S is isolated in its fiber.*

Proof. Suppose that Q is isolated in its fiber over $P = S \cap R$. Let S' be the integral closure of S in its fraction field. By the lying over theorem, there exists a prime ideal Q' of S' lying over Q. Q' must also be isolated in its fiber over P: a prime Q'_1 comparable to but distinct from it lying over P would yield such a prime lying over P and comparable to but distinct from Q when contracted to S (Q'_1 cannot lie over Q: primes lying over the same prime in an integral extension are mutually incomparable). Henceforth we assume that $S = S'$ is integrally closed. It then contains an integral closure R' of R in the fraction field of R. Then Q will be isolated in its fiber over $P' = Q \cap R'$: a comparable prime lying over P' will automatically lie over P (note that $P' \cap R \subseteq Q \cap R = P$). Therefore we may replace R by R' and $R[\theta]$ by $R'[\theta]$, and so assume that R is integrally closed. But now both going up and going down hold between $R[\theta]$ and S, since $R[\theta]$ is again normal, and it follows that $Q \cap R[\theta]$ is also isolated in its fiber over P. We may consequently replace S by $R[\theta]$. But now we can see that no prime is isolated in its fiber, since the fiber over P is the polynomial ring in one variable over a field, and there is no prime that is both maximal and minimal. $\square$

Lecture of January 13, 2010

We need one more preliminary result:

Lemma. *If $A \subseteq A[\tau] \subseteq B$ with B integral over $A[\tau]$ and A integrally closed in B, and there is a monic polynomial F with coefficients in A such that $F(\tau)B \subseteq A[\tau]$, then $B = A[\tau]$.*

Proof. Let $b \in B$ be arbitrary. Then $F(\tau)b = G(\tau)$ for some polynomial G with coefficients in A, since $F(\tau)B \subseteq A[\tau]$. By the division algorithm for monic polynomials we can write $G = QF + H$, where H is either 0 or of degree smaller than that of F, and where Q and H are polynomials with coefficients in A. Let $c = b - Q(\tau)$. It will suffice to show that $c \in A$, and for this it will suffice to show that c is integral over A. Now $F(\tau)b = F(\tau)(Q(\tau)+c)$, but $F(\tau)b = G(\tau) = Q(\tau)F(\tau) + H(\tau)$ as well, and so $F(\tau)c = H(\tau)$. Since $\deg(H) < \deg(F)$, this implies that $\tau/1 \in B_c$ is integral over the ring A'_c, where A' denotes the image of A in B_c. Since B is integral over $A[\tau]$, we have that B_c is integral over A'_c, and, in particular, $c/1 \in B_c$ is integral over A'_c. If we write down an equation of integral dependence in which the coefficients have common denominator c^M, we get

$$\left(\frac{c}{1}\right)^d + \frac{a_{d-1}}{c^M}\left(\frac{c}{1}\right)^{d-1} + \cdots + \frac{a_0}{c^M} = 0$$

and, multiplying by c^M, we have that

$$c^{M+d} + a_{d-1}c^{d-1} + \cdots + a_0$$

has image 0 in B_c, and so is killed by a power of c. This shows that c is integral over A, and so is in A, as required. $\square$

Proof of Zariski's Main Theorem: the finale. We shall now show that if J, the conductor of S into $R[t]$, is contained in Q that Q is not isolated in its fiber, which will complete the proof of the theorem. Recall that R is integrally closed in S and that S is module-finite over $R[\theta]$.

If $J \subseteq Q$ we can choose a minimal prime q of J in S such that $q \subseteq Q$. Let $p = q \cap R$. Let t denote the image of θ in the ring S/q. Now, $R/p \subseteq (R/p)[t] \subseteq S/q$, and S/q is integral over $(R/p)[t]$. The fact that Q is isolated in its fiber over P implies that Q/q is isolated in its fiber over $P/p \subseteq R/p$. By the final Lemma in the Lecture Notes from January 11, this means that t cannot be transcendental over R/p. We complete the proof by obtaining a contradiction.

If t is algebraic over R/p, localize at p and consider the image τ of θ in S_p. We then obtain a monic polynomial F with coefficients in R_p such that $F(\tau) \in qS_p$. Since q is a minimal prime of J, there exist a positive integer N and $w \in S - q$ such that $w\big(F(\tau)\big)^N \in JS_p$. Replacing F by F^N, we have F monic over R_p such that $wF(\tau) \in JS_p$. We now apply the Lemma above with $A = R_p$ and

$$B = R_p[\tau,\, wS_p] = R_p[\tau] + wS_p \subseteq S_p.$$

Note that since $F(\tau)w \in JS_p$, we have that

$$F(\tau)B \subseteq A[\tau] + JS_pS_p = A[\tau] + JS_p \subseteq A[\tau],$$

since $JS \subseteq R[\theta]$. Note also that A is integrally closed in B, because R_p is integrally closed in S_p. The Lemma above now applies, and we can conclude that $B = A[\tau]$, and so $wS_p \subseteq A[\tau]$. Since S is module-finite over $R[\theta]$, this implies that for some element $g \in R - p$, $gwS \subseteq R[\theta]$. But $g \notin q$ and $w \notin q$, and so $gw \notin q$, while we have just shown that $gw \in J$. This is a contradiction, since $J \subseteq q$ by our choice of q. $\square$

We next want to define smooth, étale, and unramified algebras. We first need to discuss finitely presented algebras a bit. Let R be any commutative ring. An R-algebra S is called *finitely presented* if it is finitely generated and for some set of R-algebra generators $s_1, \ldots, s_n$ of S, the ideal of polynomial relations on $s_1, \ldots, s_n$ over R is a finitely generated ideal. In more detail, note that a choice of R-algebra generators $s_1, \ldots, s_n$ yields a homomorphism of a polynomial ring $R[X_1, \ldots, X_n] \to S$ that is surjective, and so we have that $S \cong R[X_1, \ldots, X_n]/I$, where I is the kernel. I is the ideal of polynomial relations on $s_1, \ldots, s_n$ over R, and so we are requiring that I have some finite set of generators, say $F_1, \ldots, F_m$. That is, S is finitely presented over R if and only if it has the form $R[X_1, \ldots, X_n]/(F_1, \ldots, F_m)$, where $X_1, \ldots, X_n$ are indeterminates.

It is reasonable to ask what happens if one chooses a different finite set of algebra generators for S over R. The answer is that the ideal of polynomial relations is still finitely generated. It suffices to compare each set of generators with the union of the two sets, and

so we may assume that one set is contained in the other, say $s_1, \ldots, s_n$ and $s_1, \ldots, s_{n+h}$. By induction on h it suffices to consider the case where $h = 1$, i.e., to compare $s_1, \ldots, s_n$ and $s_1, \ldots, s_n, s$ where $s = s_{n+1}$. Since s is in the R-subalgebra generated by $s_1, \ldots, s_n$ we can choose a polynomial $F \in R[X_1, \ldots, X_n]$ such that $s = F(s_1, \ldots, s_n)$. Consider the R-algebra map $T = R[X_1, \ldots, X_n] \twoheadrightarrow S$ such that $X_j \mapsto s_j$, $1 \leq j \leq n$: let I be the kernel. We extend this to $T[X]$ so that $X \mapsto s$. It is easy to verify that the new kernel is $J = IT[X] + (X - F)T[X]$. Clearly, if I is finitely generated, so is J. On the other hand, if J is finitely generated we use the fact that there is an algebra retraction $T[X] \to T$ that fixes T and maps X to F: the image of J under this map is clearly I, and so a finite set of generators for J will map to a finite set of generators for I.

If S is finitely presented over R and T is finitely presented over S then T is finitely presented over R. For suppose that

$$S \cong R[X_1, \ldots, X_n]/(F_1, \ldots, F_m) \text{ and } T \cong S[Y_1, \ldots, Y_k]/(G_1, \ldots, G_h).$$

Each G_j can be lifted to an element H_j of $R[X_1, \ldots, X_n, Y_1, \ldots, Y_k]$ by lifting every coefficient to an element of $R[X_1, \ldots, X_n]$ that maps to it. Then

$$T \cong R[X_1, \ldots, X_n, Y_1, \ldots, Y_k]/(F_1, \ldots, F_m, H_1, \ldots, H_h),$$

as required.

Finally, note that a localization of R at one (and, hence, at finitely many) elements is finitely presented: $R_f \cong R[X]/(fX - 1)$. A localization (at any multiplicative system) of a finitely presented R-algebra is called *essentially finitely presented*. If the multiplicative system is finitely generated, the word "essentially" is not needed.

Let S be an R-algebra. Let (T, J) be a pair consisting of an R-algebra T and an ideal $J \subseteq T$ such that $J^2 = 0$. Then there is an obvious map

$$\Theta_{T,J} : \mathrm{Hom}_{R-\mathrm{alg}}(S, T) \to \mathrm{Hom}_{R-\mathrm{alg}}(S, T/J)$$

that sends $f : S \to T$ to its composition $\gamma \circ f$ with the natural surjection $\gamma : T \twoheadrightarrow T/J$. By a *smooth* R-algebra S we mean a finitely presented R-algebra such that for all R-algebras T and $J \subseteq T$ with $J^2 = 0$, the map $\Theta_{T,J}$ is surjective. By an *étale* R-algebra S we mean a finitely presented R-algebra such that for all R-algebras T and $J \subseteq T$ with $J^2 = 0$, the map $\Theta_{T,J}$ is bijective. By an *unramified* R-algebra S we mean a finitely presented R-algebra such that for all R-algebras T and $J \subseteq T$ with $J^2 = 0$, the map $\Theta_{T,J}$ is injective.

Thus, given an R-algebra map $S \to T/J$ with $J^2 = 0$, if S is smooth over R it has at least one lifting to an R-algebra map $S \to T$. If S is étale, it has a unique such lifting. If S is unramified it has at most one such lifting (but there may not be any lifting).

Note that some authors give these definitions while only requiring S to be essentially finitely presented rather than finitely presented. This creates only small differences in the theory and is convenient in certain ways, while adding a few complications in other ways.

Instead, we shall add the word "essentially" for this case and talk about maps that are essentially smooth, essentially étale, or essentially unramified.

Our next objective is to give many other characterizations of these three properties. These characterizations should offer deep insight into the nature of morphisms with these properties.

We first need to review the notions of *derivation* and of the *module of Kähler differentials*. A *derivation* of a ring R into an R-module M is a map $D : R \to M$ such that for all $f, g \in R$, $D(f+g) = D(f) + D(g)$ and $D(fg) = fD(g) + gD(f)$. The kernel of D is a subring of R: note that $D(1 \cdot 1) = 1D(1) + 1D(1)$ and so $D(1) = D(1) + D(1)$ and $D(1) = 0$. A derivation D always kills the image of $\mathbb{Z}$ in R. If R is an A-algebra then a derivation $D : R \to M$ is A-linear if and only if the image of A is killed by D. (If it is A-linear then $D(a \cdot 1) = aD(1) = 0$, while if the image of A is killed then $D(af) = D\big((a \cdot 1)f\big) = (a \cdot 1)D(f) + fD(a \cdot 1) = aD(f) + f \cdot 0 = aD(f)$.) An A-linear derivation is also called an *A-derivation*. The set of A-derivations $\mathrm{Der}_A(R, M)$ is an R-submodule of the set of all derivations $\mathrm{Der}\,(R, M)$ of R into M. The module structure may be described as follows: the value of $D_1 + D_2$ on $f \in R$ is $D_1(f) + D_2(f)$, and the value of rD on f is $rD(f)$.

There is a "universal" A-derivation from R into a specially constructed R-module $\Omega_{R/A}$. We sketch the construction. Let W be the free R-module with a basis in $\{b_f : f \in R\}$ in bijective correspondence with the elements of R. We want to kill a submodule of W in such a way that the map that takes $f \in R$ to the image of b_f in the quotient of W by this submodule is a derivation. We therefore kill the R-submodule of W spanned by the elements $b_{f+g} - b_f - b_g$ and $b_{fg} - fb_g - gb_f$ for $f, g \in R$, and also $b_{rf} - rb_f$ for all $r \in R$ in the image of A and all $f \in R$. Let $\Omega_{R/A}$ denote the quotient of W by the span V of all these elements. It should be clear that the map $d : R \to \Omega_{R/A}$ that sends f to the image of b_f is an A-derivation. We therefore use df to denote the image of b_f. The map $d : R \to \Omega_{R/A}$ has the following universal property: given any A-derivation D of R into an R-module M, there is a unique R-linear map $T : \Omega_{R/A} \to M$ such that $D = T \circ d$. Thus, every A-derivation arises from d, uniquely, by composition with an R-linear map. (It is straightforward to check that the composition of an A-derivation with an R-linear map is an A-derivation.) Otherwise said, for every R-module M we have an isomorphism $\mathrm{Hom}_R(\Omega_{R/A}, M) \cong \mathrm{Der}_A(R, M)$. This is the universal mapping property of $d : R \to \Omega_{R/A}$. (Another way of thinking about this is to note that $d : R \to \Omega_{R/A}$ represents the functor $M \mapsto \mathrm{Der}_A(R, M)$ in the category of R-modules.) This mapping property determines $d : R \to \Omega_{R/a}$ uniquely up to unique isomorphism.

The proof that every A-derivation D of $R \to M$ arises uniquely from an R-linear map $\Omega_{R/A} \to M$ is straightforward. Given D, it is clear that if one composes the required linear map with the quotient surjection $W \twoheadrightarrow \Omega_{R/A}$, it must map $b_f \mapsto D(f)$ for every $f \in R$. This shows uniqueness. There is certainly a unique such map from W to M. All that is needed is to show that it kills all the elements whose span V we took in constructing $\Omega_{R/A}$ as W/V. But these are killed precisely because D is an A-derivation. We shall have a lot more to say about derivations and Kähler differentials, but at this point we want to

explain how to use them to characterize smooth, étale, and unramified homomorphisms. The proof of the theorem we state next will occupy us for quite a while.

Theorem. *Let S be a finitely presented R-algebra.*
(a) *If R contains the rationals, S is smooth over R if and only if S is flat over R and $\Omega_{S/R}$ is projective as an R-module.*
(b) *S is étale over R if and only if S is flat over R and $\Omega_{S/R}$ is 0.*
(c) *S is unramified over R if and only if $\Omega_{S/R} = 0$.*

In part (a), when R does not necessarily contain the rationals a supplementary condition is needed: e.g., S is smooth over R if and only if for every maximal ideal Q of S lying over P in R, $(\Omega_{S/R})$ is S_Q-free of rank equal to the dimension of S_Q/PS_Q.

Lecture of January 15, 2010

It is obvious from the definition that a homomorphism is étale if and only if it is both smooth and unramified, and that is also obvious from our characterizations using differentials.

Note also that the composition of two smooth (respectively, étale, respectively, unramified) homomorphisms is again smooth (respectively, étale, respectively, unramified). For example, suppose that S_2 is smooth over S_1 and S_1 is smooth over R. Given a map $S_2 \to T/J$ where $J^2 = 0$ we have a composite map $S_1 \to S_2 \to T/J$ which lifts to a map $S_1 \to T$. Now, since T is an S_1-algebra and S_2 is smooth over S_1 we can lift to a map $S_2 \to T$. Likewise, given two R-algebra liftings of an R-algebra map $S_2 \to T/J$ to two maps $S_2 \to T$ that are distinct, the induced maps $S_1 \to S_2 \to T$ must also be distinct, since S_2 is unramified over S_1. But these both lift the same R-algebra map $S_1 \to T/J$, contradicting the fact that S_1 is unramified over R. The corresponding result for étale maps is the consequence of putting these two results together.

We want to give a bit more feeling for derivations and modules of differentials. Note that by a straightforward induction, if D is a derivation on R then

$$D(f_1\, f_2 \cdots f_k) = f_2 \cdots f_k D(f_1) + \cdots + f_1\, f_2 \cdots f_{k-1} D(f_k).$$

A typical term in the sum is the product of all the f_i except f_j times $D(f_j)$. An immediate consequence is that $D(f^k) = kf^{k-1}D(f)$. It then follows that $D(f_1^{k_1} \cdots f_h^{k_h})$ is the sum of the h terms of which a typical term is $k_j f_1^{k_1} \cdots f_j^{k_j - 1} \cdots f_h^{k_h} D(f_j)$. It also follows that the value of an A-derivation D on a polynomial in $f_1, \ldots, f_h$ with coefficients in A is uniquely determined by the values of $D(f_1), \ldots, D(f_h)$.

In the case of the a polynomial ring $B[x]$ there is B-derivation $\dfrac{\partial}{\partial x}$ (we use the partial derivative notation because B may be a polynomial ring involving other variables) whose value on $F(x)$ is

$$\left.\frac{F(x+\Delta) - F(x)}{\Delta}\right|_{\Delta=0}$$

where Δ is a new indeterminate. For $b \in B$, $\dfrac{\partial}{\partial x}(bx^k) = kbx^{k-1}$.

The polynomial ring R over A in variables x_i (there may be infinitely many) has a derivation $\dfrac{\partial}{\partial x_i}$ for each variable x_i: one may think of R as $B_i[x_i]$ where $B_i = A[x_j : j \neq i]$. Then if R is an A-algebra, $F \in A[X_1, \ldots, X_k]$ and $f_1, \ldots, f_k \in R$, for any A-derivation D we have that

$$D\big(F(f_1, \ldots, f_k)\big) = \sum_{i=1}^{k} \frac{\partial F}{\partial x_i}(f_1, \ldots, f_k) D(f_i)$$

.

It follows that if we have elements f_j that generate R over A then the elements df_j span $\Omega_{R/A}$ as an R-module. In particular, if R is a finitely generated A-algebra then $\Omega_{R/A}$ is a finitely generated R-module.

Given a polynomial ring R in variables x_i over A, a derivation D of R into M is uniquely determined by specifying values $u_i \in M$ for the variables x_i, and it is straightforward to check that there really is a derivation for each specified set of values $\{u_i\}_i$: it sends F to

$$\sum_i \frac{\partial F}{\partial x_i} u_i.$$

This implies that for the polynomial ring R, $\Omega_{R/A}$ is the free R-module on the dx_i. This is true whether the number of variables is finite or infinite.

Note that if we have an A-algebra homomorphism $R \to S$ and an S-module M there is an R-linear map $\mathrm{Der}_A(S, M) \to \mathrm{Der}_A(R, M)$ (where M is thought of as an R-module via restriction of scalars) that is simply induced by composition with the map $R \to S$. This implies that there is an R-linear map $\Omega_{R/A} \to \Omega_{S/A}$ sends df (this might more precisely be denoted $d_{R/A}f$) to df (which might more precisely be denoted $d_{S/A}f$). Hence, there is an S-linear map $S \otimes_R \Omega_{R/A} \to \Omega_{S/A}$.

Let I be an ideal of the A-algebra R. Given an A-derivation $R/I \to M$ we may compose to get an A-derivation $R \twoheadrightarrow R/I \to M$. An A-derivation $D : R \to M$ arises in this way if and only if M is an (R/I)-module and D kills I. It follows that if we have an A-algebra surjection $R \twoheadrightarrow S$ with kernel I, then $\Omega_{S/A} = S \otimes_R \Omega_{R/A}/\mathrm{Span}\,\{df : f \in I\}$. In the denominator here, it suffices to kill the R-span of the df_j for a set of elements f_j that generate I (note that $d(rf_j) = rd(f_j) + f_j dr$, and the second summand is 0 because I kills M).

Any A-algebra R may be thought of as a polynomial ring T in variables x_i modulo the ideal generated by polynomials F_j: both i and j may vary in an infinite set here. It follows that $\Omega_{R/A}$ may be thought of as the free R-module on the dx_i modulo the images of the elements dF_j calculated in $\Omega_{T/A}$, i.e., the images of the elements $\sum_i \frac{\partial F_j}{\partial x_i} dx_i$.

In the case of a finitely presented A-algebra R we may work with finitely many variables x_i and finitely many polynomials F_j, and then $\Omega_{R/A}$ is the cokernel of the matrix $\left(\dfrac{\partial F_j}{\partial x_i}\right)$

(each entry is replaced by its image in R). This matrix is called the *Jacobian matrix*. The Jacobian matrix depends on a choice of generators and relations for R over A, but its cokernel, $\Omega_{R/A}$, does not.

If R is an A-algebra, W is a multiplicative system in R, and $D : R \to M$ is a derivation, then any derivation $D : R \to M$ induces a unique derivation $W^{-1}D : W^{-1}R \to W^{-1}M$ whose restriction to R is D. Since $w(f/w) = f/1$ for $f \in R$ and $w \in W$, the extended derivation, if there is one, $\widetilde{D}$, must satisfy

$$D(f)/1 = \widetilde{D}(f) = \widetilde{D}\big(w(f/w)\big) - w\widetilde{D}(f/w) + (f/w)\widetilde{D}(w/1) = w\widetilde{D}(f/w) + (f/w)\big(D(w)/1\big).$$

We may multiply by $1/w$ to obtain

$$\widetilde{D}(f/w) = \frac{D(f)}{w} - \frac{fD(w)}{w^2} = \frac{wD(f) - fD(w)}{w^2},$$

the usual quotient rule. This proves that there is at most one way to define $\widetilde{D}$. It is straightforward to check that if one takes this as the definition (one must check that if $f_1/w_1 = f_2/w_2$ then one gets the same result from either of these representations) then one does in fact get a derivation that extends D. The remaining details are also straightforward.

It then follows easily from the universal mapping properties for the modules of differentials and for localization that

$$\Omega_{W^{-1}R/A} \cong W^{-1}\Omega_{R/A}.$$

Before proving the theorem we have already stated characterizing smooth, étale, and unramified morphisms in terms of the behavior of differentials, we want to give some further characterizations: the proofs of these results are likewise postponed for a while.

We need the notion of a geometrically regular algebra over a field. If K is a field, we say that a Noetherian K-algebra R is *geometrically regular* if for every finite purely inseparable extension L of K, the ring $L \otimes_K R$ is regular. This implies that R is regular, and in equal characteristic 0, it is equivalent to the condition that R be regular, since the only purely inseparable extension of K is K. Similarly, if K is algebraically closed or perfect, the condition that a K-algebra be geometrically regular is, again, simply the condition that it be regular. It turns out that if R is geometrically regular over K, then $L \otimes_K R$ is regular for every finite algebraic extension of K. In this generality, infinite field extensions L are slightly problematic in that one may lose the Noetherian property.

However, when R is essentially of finite type over K, i.e., a localization of a finitely generated K-algebra, the geometric regularity of R over K implies that $L \otimes_K R$ is regular for every field extension L of K. In this case it turns out that R is geometrically regular provided that $L \otimes_R K$ is regular for some field that contains a perfect closure of K (in characteristic p, this is a maximal purely inseparable algebraic extension, gotten by adjoining all p^e th roots of all elements). In particular, if R is essentially of finite type over K, then R is geometrically regular if and only if $\overline{K} \otimes_K R$ is regular, where $\overline{K}$ is an algebraic closure of K.

Note the following example. Let $R = k(t)$ be a field where k is a field characteristic $p > 0$ and t is transcendental over k. Let $K = K(t^p) \subseteq R$. K is a field, and R is a regular, but it is not a geometrically regular K-algebra: $k(t) \otimes_K R$ contains the nilpotent $t \otimes 1 - 1 \otimes t$, whose pth power is 0.

We will eventually prove all of the statements about geometric regularity made above. But we first want some additional characterizations of smooth, étale, and unramified morphisms, of which the next is:

Theorem. *Let S be a finitely presented R-algebra.*
(a) *S is smooth over R if and only if S is flat over R and for every prime P of R, the fiber $\kappa_P \otimes_R S$ is geometrically regular over κ_P.*
(b) *S is étale over R if and only if S is flat over R and for every prime P of R, the fiber $\kappa_P \otimes_R S$ is a finite product of finite separable algebraic field extensions of κ_P.*

Note that a smooth algebra over a field K is the same as a finitely generated geometrically regular algebra, while an étale algebra over a field K is the same thing as a finite product of finite separable algebraic field extensions.

For varieties over the complex numbers $\mathbb{C}$, étale has the following geometric interpretation: $R \to S$ is étale means that the map of corresponding varieties is, locally, like an open inclusion in a covering space with finite fibers. The interpretation of unramified is that the geometric map is like a locally closed inclusion in a covering space with finite fibers.

In the algebraic setting we now give very down-to-earth characterizations of all these notions. Let R be a ring and let x be an indeterminate over R. Let f be a monic polynomial in x, and let $g \in R[x]$ be such that f', the derivative of f with respect to x, is invertible in $R[x]_g$. It then turns out that $(R[x]/fR[x])_g$ is étale over R. Such an extension is called a *standard étale* R-algebra. The following is a deep result characterizing étale and unramified extensions:

Theorem. *Let S be a finitely presented R-algebra. Then S is étale (respectively, unramified) over R if and only if for every prime ideal Q of S with contraction P to R there exist $b \in S - Q$ and $a \in R - P$ such that S_b is isomorphic to a standard étale algebra over R_a (respectively, a homomorphic image of a standard étale algebra over R_a).*

The result just stated requires ZMT in the proof, and generalizes immensely that statement that a finite separable algebraic field extension has a primitive element.

There is a similar result characterizing smooth homomorphisms:

Theorem. *Let S be a finitely presented R-algebra. Then S is smooth over R if and only if for every prime ideal Q of S with contraction P to R there exist $b \in S - Q$ and $a \in R - P$ such that there is a factorization $R_a \to T \to S_b$, where T is a polynomial ring in finitely many variables over R_a and $T \to S_b$ is étale.*

If we are working with varieties over $\mathbb{C}$ then $R \to S$ is smooth means that, locally on $\mathrm{Spec}\,(R)$ and $\mathrm{Spec}\,(S)$, the map factors as an open inclusion in a covering space with finite fibers of the product of the base with $\mathbb{A}^m_{\mathbb{C}}$ for some m.

Filling in the proofs of the results we have stated will be a considerable task.

Lecture of Janauary 20, 2010

An R-algebra S is called *formally smooth*, respectively *formally étale*, respectively *formally unramified* if for all R-algebras T and ideals $J \subseteq T$ such that $J^2 = 0$, the map $\Theta_{T,J}$ is surjective, respectively bijective, respectively injective. Evidently, in each case, the word "formally" may be dropped, if the property of finite presentation for S over R is assumed as well. If two homomorphisms $f : R \to S$ and $g : S \to T$ are formally smooth (or formally étale, or formally unramified), then their composition $g \circ f : R \to T$ has the same property.

Proposition. *Let S be an R-algebra. If S is a polynomial ring over R, then S is formally smooth, and it is smooth if the number of indeterminates is finite. If $S = W^{-1}R$ then S is formally étale over R, and it is étale if W is finitely generated. If $S = R/I$ then S is formally unramified over R, and it is unramified if I is finitely generated.*

Proof. For the result on polynomial rings, note that the values on the indeterminates x_i are elements $\bar{t}_i$ of T/J, where $\bar{t}_i$ is the image mod J of $t_i \in T$. One may lift the map by sending $x_i \mapsto t_i$ for all i. This does not use that $J^2 = 0$.

Given a map of $f : W^{-1}R \to T/J$, one has a map of $R \to T/J$, and this has a unique lifting to a map $R \to T$. The map $W^{-1}R \to T$ that lifts f must extend this map, and there is at most one map that does so: it exists if and only if every element of W maps to a unit of T. But this is true, because every element of W maps to a unit of T/J, and killing nilpotents does not affect the invertibility of elements.

Finally, if an R-algebra map $R/I \to T/J$ has two liftings to maps $R/I \to T$, these will induce, by composition with $R \to R/I$, distinct R-algebra maps $R \to T$, a contradiction. $\square$

We next note that if S is formally smooth, or étale, or unramified over R, and if R' is any R-algebra, then $R' \otimes_R S$ is formally smooth, or étale, or unramified over R'. The same result holds with the word "formally" omitted, since if S is finitely presented over R then $R' \otimes_R S$ is finitely presented over R': if $S = R[x_1, \ldots, x_n]/(F_1, \ldots, F_m)$ then $R' \otimes_R S \cong R'[x_1, \ldots, x_n]/(F'_1, \ldots, F'_m)$, where F'_j is the image of F_j in $R'[x_1, \ldots, x_n]$. The point in the proofs is that if T is an R'-algebra, then $\mathrm{Hom}_{R'-\mathrm{alg}}(R' \otimes_R S, T) \cong \mathrm{Hom}_{R-\mathrm{alg}}(S, T)$ as sets, and the same holds when T is replaced by T/J. The required results are then immediate.

We shall say that $\delta : R \to M$, where M is an R-module, is a *universal derivation* for the A-algebra R if for every derivation $D : R \to N$, where N is an R-module, there is a unique R-linear map $L : M \to N$ such that $D = L \circ \delta$. We have already noted that $d : R \to \Omega_{R/A}$ is a universal derivation. If $\delta : R \to M$ is another, the universal mapping properties give unique R-linear maps $L : \Omega_{R/A} \to M$ and $L' : M \to \Omega_{R/A}$ that are mutually inverse (e.g., $L' \circ L$ is the unique map from $\Omega_{R/A}$ to itself whose composition with d gives d, and so is the identity). Note that $\delta = L \circ d$.

If S is an R-algebra, let I be the kernel of the map $S \otimes_R S \to S$. The ideal I is generated by elements of the form $s \otimes 1 - 1 \otimes s$. Now $S \otimes_R S$ has two S-module structures coming from the two maps of S into it (one structural morphism maps s to $s \otimes 1$ and the other maps s to $1 \otimes s$), and every ideal of $S \otimes_R S$ has these two S-module structures. In particular, I and I^2 have two S-module structures. However, we claim that on I/I^2 these two S-module structures agree. The reason is that

$$I/I^2 = \big(S \otimes_R S)/I\big) \otimes_{S \otimes_R S} I$$

is an $\big((S \otimes_R S)/I\big)$-module, and $(S \otimes_R S)/I = S$. Notice that we have a map $\delta : S \to I$ such that for all $s \in S$, $\delta(s) = s \otimes 1 - 1 \otimes s$. This map is easily seen to be R-linear. In fact, it is an R-derivation of $S \to I/I^2$, since

$$s\delta(t) + t\delta(s) = s(t \otimes 1 - 1 \otimes t) + t(s \otimes 1 - 1 \otimes s).$$

In evaluating $s(f \otimes g)$ we may use either $sf \otimes g$ or $f \otimes sg$. Thus, this expression becomes

$$st \otimes 1 - s \otimes t + s \otimes t - 1 \otimes st = st \otimes 1 - 1 \otimes st = \delta(st),$$

as required.

Theorem. *With notation as just above, $\delta : S \to I/I^2$ is a universal R-derivation on S, and so $\Omega_{S/R} \cong I/I^2$ in such a way that ds corresponds to $s \otimes 1 - 1 \otimes s$.*

Proof. Let $S = K[X_i : i]/(F_j : j)$ be a presentation of S, where i and j are both permitted to vary in index sets that may be infinite. We shall think of this as the copy of S on the right in $S \otimes_R S$. Let Y_i be a new family of indeterminates indexed in the same way as the X_i and let $G_j = F_j(Y)$ be the corresponding family of polynomials in the Y_i, so that $S \cong R[Y : i]/(G_j : j)$ as well, which we shall think of as the copy of S on the left in the $S \otimes_R S$. Then

$$S \otimes_R S \cong R[X_i,\, Y_i : i]/(F_j, G_j : j).$$

Let $\Delta_i = Y_i - X_i$ for every i. Then we may describe $S \otimes_R S$ using the indeterminates X_i and Δ_i, replacing Y_i by $X_i + \Delta_i$ for al i. We replace $G_j = F_j(Y)$ by $F_j(X + \Delta)$: we use this notation to indicate that in F_j, every X_i has been replaced by $X_i + \Delta_i$. In this presentation, if x_i is the image of X_i in S, then $\delta(x_i)$ is the image of $Y_i - X_i = \Delta_i$. Thus, the ideal I corresponds to the ideal generated by all the Δ_i in

$$R[X_i,\, \Delta_i : i]/(F_j, F_j(X + \Delta) : j).$$

By the multi-variable version of Taylor's formula, for all j,

$$F_j(X + \Delta) = F_j(X) + \sum_i \frac{\partial F_j}{\partial X_i}\Delta_i + \text{ terms of degree 2 or more in the } \Delta_i \ .$$

This leads to the result that

$$(S \otimes_R S)/I^2 \cong R[X_i, \Delta_i : i]/\big((F_j : j) + (\sum_i \frac{\partial F_j}{\partial X_i}\Delta_i : j) + (\Delta_i : i)^2\big).$$

Since $R[X_i : i]/(F_j : j) \cong S$, $(S \otimes_R S)/I^2$ may be identified with the free S module with basis 1 together with the Δ_i modulo the S-span of the relations $\sum_i \frac{\partial F_j}{\partial X_i}\Delta_i$ as j varies, where each $\frac{\partial F_j}{\partial X_i}$ is identified with its image in S. It follows that I/I^2 may be identified with quotient of the free S-module on the elements Δ_i modulo the S-span of those same relations, and we have already seen (see the fifth paragraph of the second page of the Lecture Notes of January 15) that this module is isomorphic with $\Omega_{S/R}$ in such a way that Δ_i corresponds to dx_i. $\square$

Theorem. *Let S be an R-algebra. Then S is formally unramified over R if and only if $\Omega_{S/R} = 0$, and this is equivalent to the condition that, with $I = \mathrm{Ker}\,(S \otimes_R S \twoheadrightarrow S)$, $I = I^2$.*

Proof. Since $\Omega_{S/R} \cong I/I^2$, it is obvious that $\Omega_{S/R} = 0$ if and only if $I = I^2$. We work with the latter condition.

We first show that if $I = I^2$ then S is unramified over R. Suppose that $I = I^2$ and also suppose we have two R-algebra maps ϕ_1 and ϕ_2 of $S \to T$ that agree mod J, with $J^2 = 0$. This gives an R-algebra map $S \otimes_R S \to T$ such that $s \otimes t \mapsto \phi_1(s)\phi_2(t)$. The fact that the ϕ_i induce the same map to T/J implies that for all $s \in S$, $s \otimes 1 - 1 \otimes s$ maps to 0 in T/J, and this implies that I maps into J. But then $I = I^2$ maps into $J^2 = 0$, and so I is killed. Since $s \otimes 1 - 1 \otimes s \in I$ maps to $\phi_1(s) - \phi_2(s)$, it follows that $\phi_1 = \phi_2$.

Conversely, suppose that S is formally unramified over R. Then let $T = (S \otimes_R S)/I^2$, and let $J = I/I^2 \subseteq T$. We have two obvious R-algebra maps of S into $S \otimes_R S$ (one sending s to $s \otimes 1$, and one sending s to $1 \otimes s$, and, hence, two obvious maps into T. Since the two maps agree mod J, they agree. But this means that each element $s \otimes 1 - 1 \otimes s$ is 0 in T/I^2, and since these elements generate I, we have that $I \subseteq I^2$. since the other inclusion is obvious, $I = I^2$.

Lecture of January 22, 2010

Proposition. *Let R be a ring.*

(a) *If $S = R[x]_g/(f)$ where f is any polynomial whose derivative f' with respect to x is invertible in S, then S is étale over R.*

(b) *More generally, if $S = R[x_1, \ldots, x_n]_g/(f_1, \ldots, f_n)$ is such that the image of the Jacobian determinant $\det\big(\frac{\partial f_j}{\partial x_i}\big)$ is invertible in S, then S is étale over R.*

Proof. It is evident that (a) is a special case of (b) and it will suffice to prove (b). Suppose that we are given a homomorphism $\phi : S \to T/J$ where $J^2 = 0$ and we seek a lifting to T. Let $y_i \in T$ lift the values of the $\phi(x_j)$, where x_j is the image of X_j in S. Then we must have that $f_j(y) \in J$ for every j, where $y = y_1, \ldots, y_n$, and we also know that $g(y)$ is a unit of T, since it is a unit of T/J. Then we want to prove that there are unique elements $\delta_i \in J$ such that $f_j(y + \delta) = 0$ for all j, where $y + \delta$ indicates $y_1 + \delta_1, \ldots, y_n + \delta_n$. By Taylor's formula with remainder, the fact that the δ_j will be chosen in J, and $J^2 = 0$, these equations are equivalent to the equations

$$f_j(y) + \sum_{i=1}^{n} \frac{\partial f_j}{\partial x_i}\Big|_{x=y} \delta_i = 0,$$

with the proviso that the $\delta_i \in J$. Let $\mathcal{J}$ be the $n \times n$ matrix whose i, j entry is $\left.\dfrac{\partial f_j}{\partial x_i}\right|_{x=y}$. The determinant of this matrix is a unit, because that is true mod J, and so the matrix is invertible. Let Δ be a column vector whose entries are the unknown elements δ_i of J that we seek, and let Γ be a column vector whose j th entry is $f_j(y) \in J$. Thus, we seek to solve $\mathcal{J}\Delta = -\Gamma$ where Δ has unknown entries in J, $-\Gamma$ has entries in J, and the matrix $\mathcal{J}$ is invertible. It is now clear that the unique solution is $\Delta = -\mathcal{J}^{-1}\Gamma$, and the entries of the solution do happen to be in J. $\square$

Note that part (a) has the desirable consequence that standard étale extensions are, indeed, étale.

Corollary. *A finite separable algebraic extension L of a field K is étale over K.*

Proof. By the theorem on the primitive element, $L = K[\theta]$, where the monic minimal polynomial f of θ is separable over L. This implies that the image of f' in L does not vanish, and so is invertible. Thus $L \cong K[x]/(f)$ where f' is invertible in L. $\square$

Proposition. *If J is contained in the ideal of nilpotents of T, there is a bijection between the idempotents of T and the idempotents of T/J induced by the quotient surjection $T \twoheadrightarrow T/J$.*

Proof. Clearly, the image of an idempotent $e \in T$ is idempotent in T/J. Suppose that $e' \equiv e \bmod J$. Then $e - e'$ is nilpotent, and hence so is $e(e - e')$, i.e., $e = e^2 \equiv ee' \bmod J$, and so $e(1 - e')$ is nilpotent. But e and $1 - e'$ are both idempotent, and, hence, so is their product. It follows that $e(1 - e') = 0$, i.e., that $e = ee'$. But $ee' = e'$ similarly. Thus, the map on idempotents is injective.

It remains to show that it is surjective. Let e be an element whose image mod J is idempotent and let $f = 1 - e$. Then $e + f = 1$ and $e^n f^n = 0$ for some n. Expand $(e + f)^{2n-1}$ by the binomial theorem. Each term is either a multiple of e^n or a multiple of f^n. The multiples of e^n include e^{2n-1} and other terms involving f, and similarly for the multiples of f^n. Thus,

$$1 = (e + f)^{2n-1} = e^n(e^{n-1} + fu) + f^n(f^{n-1} + ev).$$

Let $e' = e^n(e^{n-1} + fu)$ and $f' = f^n(f^{n-1} + ev)$. Then $e' + f' = 1$, $e'f'$ is a multiple of $e^n f^n = 0$, and, mod J, $e' \equiv e^{2n-1} + e^n fu \equiv e$. Thus, e' is an idempotent of T that lifts e. $\square$

Proposition. *Let $S_1, \ldots, S_n$ be R-algebras. Consider any of the following properties: finite presentation, (formal) smoothness, being (formally) étale, or being (formally) unramified. Then $S = S_1 \times \cdots \times S_n$ has this property if and only if all of the S_i have this property.*

Proof. By a straightforward induction it suffices to consider the case where $n = 2$. We leave the property of finite presentation as an exercise. Once that is known, it suffices to consider the properties of being formally smooth and formally unramified: the property of being formally étale then follows. Note that giving a map $S_1 \times S_2 \to T/J$ yields an

idempotent in T/J that lifts uniquely to an idempotent in T, and so $T = T_1 \times T_2$. We may then write $J = J_1 \times J_2$ where J_i is an ideal of T_i and $J_i^2 = 0$, $i = 1, 2$. The problem of lifting a map is a componentwise problem, and so if both factors are smooth (respectively, unramified) so is the product. Now suppose that S is smooth (respectively, unramified). Let T_1 be an S_1-algebra and J_1 an ideal such that $J_1^2 = 0$. Let $T = T_1 \times S_2$ with $J_2 = 0$, and let $J = J_1 \times J_2$. The problem of lifting maps $S_1 \to T_1/J$ to maps $S_1 \to T$ is equivalent to the problem of lifting maps $S_1 \times S_2 \to T/J$ of the form $\phi \times \mathbf{1}_{S_2}$ to maps $S_1 \times S_2 \to T$. It follows that if S is formally smooth (respectively, unramified), then so is S_1, and the argument for S_2 is similar. $\square$

We are aiming next to prove the following characterization of étale extensions of fields.

Theorem. *Let K be a field and let R be a finitely generated K-algebra. The following conditions are equivalent:*
(a) *R is étale over K.*
(b) *R is unramified over K.*
(c) *R is a finite product of finite separable algebraic field extensions of K.*
(d) *If L is an algebraic closure of K, then $L \otimes_K R$ is K-isomorphic with a finite product of copies of L.*

We postpone the proof until we have established some preliminary results on modules of differentials for field extensions. These results themselves need further preliminaries.

Let $K \subseteq L$ be a field extension. A family of algebraically independent elements $\{x_i\}_i$ of L over K is called a *separating transcendence basis* for L over K if L is separable over $K(x_i : i) \subseteq L$. We need the following result of S. MacLane:

Theorem. *If K is algebraically closed or perfect of characteristic $p > 0$ and L is finitely generated over K then L has a separating transcendence basis over K.*

Proof. If F is a subfield of L, let F^{sep} denote the separable closure of F in L. Choose a transcendence basis $x_1, \ldots, x_n$ so as to minimize $[L : L']$ where $L' = K(x_1, \ldots, x_n)^{\text{sep}}]$. Suppose that $y \in L$ is not separable over $K(x_1, \ldots, x_n)$. Choose a minimal polynomial $F(z)$ for y over $K(x_1, \ldots, x_n)$. Then every exponent on z is divisible by p. Put each coefficient in lowest terms, and multiply $F(z)$ by a least common multiple of the denominators of the coefficients. This yields a polynomial $H(x_1, \ldots, x_n, z) \in K[x_1, \ldots, x_n][z]$ such that the coefficients in $K[x_1, \ldots, x_n]$ are relatively prime, and such that the polynomial is irreducible over $K(x_1, \ldots, x_n)[z]$. By Gauss's Lemma, this polynomial is irreducible in $K[x_1, \ldots, x_n, z]$. It cannot be the case that every exponent on every x_j is divisible by p, for if that were true, since the field is perfect, H would be a pth power, and not irreducible. By renumbering the x_i we may assume that x_n occurs with an exponent not divisible by p. Then the element x_n is separable algebraic over the field $K(x_1, \ldots, x_{n-1}, y)$, and we may use the transcendence basis $x_1, \ldots, x_{n-1}, y$ for L. Note that $x_n, y \in K(x_1, \ldots, x_{n-1}, y)^{\text{sep}} = L''$, which is therefore strictly larger than $L' = K(x_1, \ldots, x_n)^{\text{sep}}$. Hence, $[L : L''] < [L : L']$, a contradiction. $\square$

Lemma. *Let R be a ring.*
(a) *Let S be a direct limit of R-algebras S_j. Then $\Omega_{S/R}$ may be viewed as the direct limit of the modules $\Omega_{S_j/R}$ (or of the modules $S \otimes_{S_j} \Omega_{S_j/R}$).*

(b) *Let S be an R-algebra and let $T = S[X_i : i]$, a polynomial ring. Then*

$$\Omega_{T}/R \cong T \otimes_S \Omega_{S/R} \bigoplus (\bigoplus_i T dX_i),$$

and the value of $d_{T/R}$ on $F = \sum_{\mu \in \mathcal{M}} s_\mu \mu$, where μ runs through some finite set of monomials $\mathcal{M}$ in the X_i, is

$$\sum_{\mu \in \mathcal{M}} \mu \otimes d_{S/R}(s_\mu) + \sum_i \frac{\partial F}{\partial x_i} dX_i.$$

Hence, if $U = T/(F_j : j)$ then

$$\Omega_{U/R} \cong U \otimes_T \Omega_{T/R}/\langle d_{T/R}(F_j) : j \rangle,$$

where the brackets $\langle\ \rangle$ indicate span over T.

Proof. (a) One may deduce this using universal mapping properties. Here is another argument. Since S is the union of the images of the S_j, the images of the ds_j, $s_j \in S_j$, span $\Omega_{S/R}$. Each relation coming from addition, multiplication by a scalar in R, or the product rule in some S_j continues to hold when we map to $\Omega_{S/R}$, while it is clear that each such relation that holds in $\Omega_{S/R}$ comes from one that holds in some S_j.

In part (b), the second statement is immediate from the first. The formula for $d_{T/R}$ is forced by linearity and the product rule, and it is straightforward to verify that $d_{T/R}$ as defined is a derivation. (Note that in checking the product rule, one has that both sides are bilinear. Therefore it suffices to check it when each of the two elements is the product of an element of S with a monomial.) $\square$

Lecture of January 25, 2010

Proposition. *Let $K \subseteq L$ be fields.*

(a) *If $L = K(x_i : i \in I)$ is a purely transcendental extension of K then $\Omega_{L/K}$ is the free L-module on the dx_i.*
(b) *If L' is a separable algebraic extension field of L, then $\Omega_{L'/K} \cong L' \otimes_L \Omega_{L/K}$.*
(c) *If $\{x_i : i \in I\}$ is a separating transcendence basis for L/K, then $\Omega_{L/K}$ is the free L-module on the basis dx_i.*
(d) *If K is perfect and L is finitely generated over K, then $\dim {}_L\Omega_{L/K}$ is the transcendence degree of L over K.*

Proof. Part (a) follows from the corresponding fact for polynomial rings together with the fact that localization commutes with formation of the module of differentials.

For part (b), a direct limit argument enables us to reduce to the case of a finite separable algebraic extension field L of K, and by the theorem on the primitive element, $L' =$

$L[x]/(f)$ where f is separable over L. Let $f = \sum_t \lambda_t x^t$. By part (b) of the final Lemma from the Lecture Notes of January 22,

$$\Omega_{L'/K} \cong \big(L' \otimes_L \Omega_{L/K} \oplus L'dx\big)/L'd_{L[x]/K}f.$$

But

$$d_{L[x]/K}f = \sum_t d_{L/K}(\lambda_t)x^t + f'dx.$$

Since the image of f' in L is invertible, the quotient is simply the isomorphic with the module $L' \otimes_L \Omega_{L/K}$.

(c) is immediate from parts (a) and (b), while (d) is immediate from (c) and MacLane's theorem on the existence of separating transcendence bases. $\square$

We are now ready prove the characterization of étale extensions of fields stated in the Lecture Notes of January 22.

Proof of the theorem characterizing étale extensions of fields. We will prove that (c) $\Rightarrow$ (a) $\Rightarrow$ (b) $\Rightarrow$ (d) $\Rightarrow$ (c). Note that since R is finitely generated over a field, it and its quotients are finitely presented. For these rings, étale is equivalent to formally étale and unramified is equivalent to formally unramified.

The fact that (c) $\Rightarrow$ (a) follows from the Corollary to the first Proposition of the Lecture Notes of January 22 together with the Proposition from those same notes on behavior of finite products, while (a) $\Rightarrow$ (b) is immediate. To prove that (b) $\Rightarrow$ (d), note that $L \otimes_K R$ is unramified over L, and so it will suffice to prove that a finitely generated algebra over L is unramified if and only if it is isomorphic with a finite product of copies of L. We first claim that R must be zero-dimensional. If not, we may kill a minimal prime that is contained in a maximal ideal that is different from it, and so obtain an unramified finitely generated L-algebra that is a domain. The module of differentials of the fraction field $\mathcal{F}$ has vector space dimension equal to the transcendence degree of $\mathcal{F}$ over L, which is the Krull dimension of R. But this must be zero. Therefore $\mathcal{F}$ must be equal to L, a contradiction.

Since R is zero-dimensional, it is a finite product of Artin local rings, and these may be considered separately. To complete the argument, we show that if an Artin local ring is a finitely generated L-algebra and is unramified, then it is $\cong L$. The residue field must be the image of L. If the maximal ideal is nonzero, we may kill $m^2 \neq m$ to obtain an example in which $m^2 = 0$ but $m \neq 0$. We may now kill all but one element in a minimal set of generators of m. The resulting ring has the form $R = L[x]/x^2$. But then $\Omega_{R/L}$ is the cokernel over R of the matrix $\big(2x\big)$, and is not zero since the image of $2x$ is in the maximal ideal of R, a contradiction. This concludes the proof that (b) $\Rightarrow$ (d).

It remains only to show that (d) => (c). Suppose that $L \otimes_K R$ is a finite product of copies of L. Then R is a finite-dimensional vector space over K. Since it is module-finite over K, it has Krull dimension zero. Since $R \subseteq L \otimes_K R$ (since L is free over K, this extension is faithfully flat), we see that R is reduced. Then R is a finite product of reduced Artinian

local rings, each of which stays reduced when we apply $L \otimes_K \_$. It follows that each local ring of R is a finite algebraic field extension K' of K such that $L \otimes_K K'$ is reduced. It remains to show that K' is separable. Let $\theta \in K'$ have minimal polynomial $f = f(x)$ over K. Then $L \otimes_K K[\theta] \subseteq L \otimes_K K'$ is reduced, and $L \otimes_K K[\theta] \cong L \otimes_K K[x]/(f) \cong L[x]/(f)$ is reduced, which implies that f is square-free in $L[x]$, as required. $\square$

The following is a variant of Zariski's Main Theorem, and we shall refer to it as Zariski's Main Theorem.

Theorem (Zariski's Main Theorem). *Suppose that $R \subseteq S$ and that S is finitely generated as an R-algebra. Let Q be a prime ideal of S that is isolated in its fiber over P, a prime in R. Then there exists a module-finite extension R'' of R with $R \subseteq R'' \subseteq S$ and $f \in R'' - Q$ such that $R''_f = S_f$.*

Proof. Let R' be the integral closure of R in S and $P' = Q \cap R'$. Then Q is isolated in its fiber over P', and by the earlier version of ZMT, there exists $f \in R' - P' = R' - Q$ such that $R'_f = S_f$. Hence, for each of the finitely many generators u_j of S over R, we can choose N_j such that $f^{N_j} u_j = v_j/1$ with $v_j \in R'$. Let R'' be the subring of R' generated by f and the v_j. Clearly, $R'_f = S_f$. $\square$

Let $\mathcal{P}$ be a property of ring homomorphisms, and let $R \to S$ be a ring homomorphism. Let Q be a prime ideal of S lying over a prime P in R. We shall say that $\mathcal{P}$ *holds near* Q or that $R \to S$ *has* $\mathcal{P}$ *near* Q if there exist $b \in S - Q$ and $a \in R - P$ such that the image of a in S_b is invertible (so that there is an induced map R-algebra map $R_a \to S_b$: we say that $R_a \to S_b$ *is defined* in this case) and such that $R_a \to S_b$ has property $\mathcal{P}$. Thus, we may talk about a homomorphism $R \to S$ that is étale near Q, or smooth near Q, or unramified near Q, or formally unramified near Q, and so forth.

The following result makes major inroads in classifying étale and unramified morphisms.

Theorem. *Let S be an R-algebra, and Q a prime ideal of S lying over P in R.*

If S is finitely presented over R then $R \to S$ is unramified near Q if and only if there exist $a \in R - P$ and $b \in S - Q$ such that $R_a \to S_b$ is defined and S_b is a homomorphic image by a finitely generated ideal of a standard étale algebra over R_a.

If S is finitely generated over R then S is formally unramified near Q if and only if there exist $a \in R - P$ and $b \in S - Q$ such that $R_a \to S_b$ is defined and S_b is a homomorphic image of a standard étale algebra over R_a.

The proof involves Zariski's Main Theorem, the theorem on the primitive element for separable field extensions, our understanding of unramified homomorphisms when the base ring is a field, Nakayama's lemma, and additional trickery.

Before beginning the proof, we want to make several remarks. If $R \to S$ is finitely presented so is $R \to S_b$ and, hence, $R_a \to S_b$ when it is defined. Likewise, if S is finitely generated over R, then S_b is finitely generated over R and, hence, over R_a when $R_a \to S_b$ is defined. Also note that if we have maps $R \to R' \to S$ such that R' and S are finitely presented over R, then S is finitely presented over R'. (Take finitely many generators and relations for R' over R. Include the images of these generators and relations in a finitely

many generators and relations for S over R. The additional generators and relations needed give a finite presentation of S over R'.)

Note that we already know the "if" part of the theorem: a standard étale algebra is unramified, and a quotient by an ideal is formally unramified and unramified if the ideal is finitely generated. Thus, we need only be concerned with proving the "only if" part.

The result in the final paragraph may be paraphrased as follows: if S is finitely generated over R it is formally unramified near Q if and only if it is a homomorphic image of a standard étale algebra near Q. The result in the second paragraph may be paraphrased as follows: if S is finitely presented over R, it is unramified near Q if and only if it is locally a homomorphic image, by a finitely generated ideal, of a standard étale algebra.

The statement in the second paragraph is immediate from the statement in the final paragraph: S_b will be finitely presented over the standard étale algebra, and therefore, if it is a homomorphic image of it, the ideal must be finitely generated.

Thus, we need only prove the "only if" part of the statement in the final paragraph.

Lecture of January 27, 2010

Proof of the "only if" statement in the final paragraph of the theorem classifying unramified homomorphisms. Note first that if T is another finitely generated R algebra with an element $c \in T$ is such that $T_c \cong S_b$ where $b \notin Q$, then we may study T instead of S: T_c will have a prime ideal $Q'T_c$ corresponding to QS_b, where Q' is a prime ideal of T not containing c, and any localization of S_b at one element not in QS_b corresponds to a localization of T_c at one element not in QT_c.

We next want to observe that we may replace R and S by R_P and $R_P \otimes_R S = S_P$: this is a base change, and the hypotheses still hold. If we know the case where R is quasilocal then we know that for suitable elements $\alpha \in R_P - PR_P$ and $\beta \in S_P - QS_P$, we have that $(S_P)_\beta$ is a homomorphic image of a standard étale algebra over $(R_P)_\alpha$, say of $\big((R_P)_\alpha[x]\big)_g/(f)$, where f is monic over $(R_P)_\alpha$, g has coefficients in $(R_P)_\alpha$, and f' is invertible in the quotient. If we localize at the denominators in representations for α, β, the coefficients of f and g, and elements needed to show the invertibility of f' in $\big((R_P)_\alpha[x]\big)_g/(f)$ we get a standard étale algebra over a ring of the form R_a, namely $C = R_a[x]_g/(f)$ that will map to $(S_Q)_\beta$, where β may be assumed to be in $S - Q$. This map becomes onto if we invert all elements of $R - P$. Thus, we can find a single $a' \in R - P$ such that the image of $C_{a'}$ contains all of the generators in some finite set of generators for S over R, then map $C_{a'} \to S_{a'\beta}$ will be surjective.

Henceforth, we assume, as we may, that $(R,\ P, K)$ is quasi-local. Let $\overline{R}$ denote the image of R in S. Consider the fiber $K \to K \otimes S = S'$. This map is also formally unramified near the prime Q' corresponding to Q, which means that after localizing at one element b' of $S' - Q'$, we have an unramified map $K \to S'_{b'}$, and so $\operatorname{Spec}(S'_{b'})$ is finite. This means that Q is isolated in its fiber over P: it is obviously minimal, and for finitely generated algebras over a field, maximal ideals contract to maximal ideals, and so it is maximal as

well. Moreover, the field extension $K \to S/Q$ is a finite separable algebraic extension. We now apply the form of Zariski's Main Theorem proved in the Lecture Notes of January 25 to conclude that we have a module-finite R-algebra T with $R \subseteq T \subseteq S$ and an element $b \in T - Q$ such that $T_b = S_b$. It follows that T is also formally unramified over R near $Q \cap T$, and it will suffice to prove the theorem with S and Q replaced by T and $Q \cap T$. We may therefore assume without loss of generality that S is module-finite over R, where (R, P, K) is quasi-local.

Now the fiber S/PS is zero-dimensional. One of the factors, call it L, is S/Q, a finite separable algebraic extension of K. Let us write $S/PS = L \times B$, where B is simply the product of the other Artin local rings (there are finitely many) in the factorization of S/PS. Note that Q/PS corresponds to the ideal generated by $(0, 1)$, which is $\{0\} \times B$, in $L \times B$.

Let $\overline{\theta}$ denote a non-zero primitive element for L over K, so that $L = K[\overline{\theta}]$ (the condition that $\overline{\theta} \neq 0$ is automatic except in the case where $L = K$), and let $\theta \in S$ be an element that maps to $(\overline{\theta}, 0)$ in $S/PS \cong L \times B$.

Let q be the contraction of Q to $\overline{R}[\theta]$. Note that $\theta \in S$ is integral over $\overline{R}$. We claim that $\overline{R}[\theta]_q = S_q = S_Q$ (once we know this, we will be able to replace S by $\overline{R}[\theta]$.) To prove that $\overline{R}[\theta]_q = S_q$ we may use Nakayama's lemma: since S is module-finite over R, S_q is module-finite over R_q. It therefore will suffice to show that $\overline{R}[\theta]_q/q\overline{R}[\theta]_q = S_q/qS_q$. We first consider what happens to the extension $\overline{R}[\theta] \subseteq S$ when we work mod the expansions of P, since $P\overline{R}[\theta] \subseteq q$. The image of $\overline{R}[\theta]/P\overline{R}[\theta]$ in S/PS is $\overline{R}[\theta]/(PS \cap \overline{R}[\theta]) \subseteq S/PS \cong L \times B$. Let $\theta' = (\theta, 0)$. Then the image of $\overline{R}[\theta]/(PS \cap \overline{R}[\theta])$ in $L \times B$ is $K[\theta']$, where we have identified K with its image in $L \times B$. The typical element of the image has the form $H(\theta') = (H(\theta), H(0))$, where H is an element of $K[x]$. Since we may choose H to be the minimal polynomial of $\theta \neq 0$, which has nonzero constant term α, the image contains $(0, \alpha)$, and hence, the image contains $e = (1, 1) - \alpha^{-1}(0, \alpha) = (1, 0) \in L \times B$. The element e lies outside the contraction of Q/PS. Therefore, $(S/PS)_q$ is a localization of $(L \times B)_e \cong L$. Therefore, $(S/PS)_q = L$. It is also clear that $\overline{R}[\theta]/q = L$, since $\overline{\theta}$ is a primitive element for L over K. We have verified that $\overline{R}[\theta]_q = S_q$, and so S_q is already local with residue class field L. It follows as well $S_q = S_Q$.

We may now replace S by $\overline{R}[\theta]$. Let h denote the dimension of the K-vector space $K \otimes_R S = S/PS$, which is now spanned over K by the powers of the image of θ, which we call θ_1. Then $1, \theta_1, \theta_1^2, \ldots, \theta_1^{h-1}$ is a K-vector space basis for $K \otimes_R S$. By Nakayama's lemma, it follows that $1, \theta, \theta^2, \ldots \theta^{h-1}$ span S over R, and that there is a monic polynomial f in $R[x]$ such that if $\overline{f}$ denotes the image of f in $\overline{R}[x]$, then $\overline{f}(\theta) = 0$. Let C denote the ring $R[x]/\big(f(x)\big)$: we have that C maps onto S and that $K \otimes_R C \to K \otimes_R S$ is an isomorphism. Let $\mathfrak{n}$ denote the contraction of Q to C. Note that $C_{\mathfrak{n}}/\mathfrak{n}C_n \cong K[\overline{\theta}] \cong S_Q/QS_Q = L$.

We then have that $K \otimes_R \Omega_{C/R} \to K \otimes_R \Omega_{S/R}$ is an isomorphism, since the former is isomorphic to $\Omega_{K \otimes_R C/K}$, the latter to $\Omega_{K \otimes_R S/K}$, and $K \otimes_R C \cong K \otimes_R S$. Now,

$$L \otimes_C \Omega_{C/R} \cong (L \otimes_C C/PC) \otimes_C \Omega_{C/R} \cong L \otimes_C (K \otimes_R \Omega_C/R) \cong L \otimes_{C/PC} (K \otimes_R \Omega_C/R)$$

and, by an entirely similar argument, $L \otimes_S \Omega_{S/R} \cong L \otimes_{S/PS} \otimes (K \otimes_R \Omega_{C/R})$. Since $S/PS \cong C/PC$, we have that $L \otimes_C \Omega_{C/R} \cong L \otimes_S \Omega_{S/R}$, and so

$$(C_{\mathfrak{n}}/\mathfrak{n}C_{\mathfrak{n}}) \otimes_C \Omega_{C/R} \cong (S_Q/QS_Q) \otimes_S \Omega_{S/R} \cong (\Omega_{S/R})_Q/Q(\Omega_{S/R})_Q.$$

Since S_b is formally unramified over R, the numerator is 0, for even $\Omega_{S_b/R} \cong (\Omega_{S/R})_b = 0$. Thus,

$$0 = (C_{\mathfrak{n}}/\mathfrak{n}C_{\mathfrak{n}}) \otimes_C \Omega_{C/R} = L \otimes \Omega_{C_{\mathfrak{n}}/R},$$

and since $\Omega_{C_{\mathfrak{n}}/R}$ is finitely generated over $C_{\mathfrak{n}}$, we may apply Nakayama's lemma to conclude that $(\Omega_{C/R})_{\mathfrak{n}} \cong \Omega_{C_{\mathfrak{n}}/R} = 0$. Since $\Omega_{C/R}$ is finitely generated over C, we may choose a single element $g = g(x)$ with image not in $\mathfrak{n}$ such that $\Omega_{C_g/R} = 0$. Thus, C_g is unramified over R, and we may replace g by a multiple that maps to a multiple of b. We replace b by this multiple, and then we have a surjection $C_g \twoheadrightarrow S_b$. Since $C_g = R[x]_g/(f)$ is formally unramified over R and $\Omega_{C_g/R} = 0$ is the cokernel over C_g of the matrix $\begin{pmatrix} f' \end{pmatrix}$ (one takes the image of f' in C_g), we have that the image of f' in invertible in $C_g = R[x]_g/(f)$, so that $R[x]_g/(f)$ is the required standard étale algebra. $\square$

Lecture of January 29, 2010

We are now really classify étale homomorphisms. First note that the property of $R \to S$ being flat is local on S: if S_Q is flat for every prime Q of S, so is S. For if $0 \to N \to M$ is an injection of R-modules, and $S \otimes_R N \to S \otimes_R M$ is not injective, the kernel is supported at some prime ideal Q of S, and $S_Q \otimes_R N \to S_Q \otimes_R M$ will have non-trivial kernel, a contradiction. Thus, if S is flat near Q for all prime ideals Q if and only if S is flat.

Theorem. *Let S be a finitely presented R-algebra. The following are equivalent:*
(a) *S is étale over R.*
(b) *S is flat over R and $\Omega_{S/R} = 0$.*
(c) *S is flat and unramified over R.*
(d) *Near every prime Q of $\operatorname{Spec}(S)$, S is standard étale over R (that is, there exists $b \in S - Q$ and $a \in R$ not in the contraction P of Q such that $R_a \to S_b$ is defined and is standard étale).*

Proof. We already know that (b) and (c) are equivalent. We next observe that (d) $\Rightarrow$ (a). Suppose that we have an R-algebra map $\phi : S \to T/J$ and we want to show that it has a unique lifting $S \to T$. This is very easy if we make use of the local nature of a map of schemes. For every prime Q of $\operatorname{Spec}(S)$ we can choose $b \in S - Q$ and $a \in R - P$, where P is the contraction of Q, such that $R_a \to S_b$ is defined and standard étale. Fix an element $\beta \in T$ that maps to the image of b in T/J. Then we have a surjection $T_\beta \twoheadrightarrow T_\beta/JT_\beta \cong (T/J)_b$. Note that T_β is independent of the choice of β: if β' also maps to the image of b, the images of the two differ by a nilpotent in T_β, and so β' also is invertible in T_β. The sets $D(b)$ cover $\operatorname{Spec}(S)$ (there is a choice of b outside any given prime Q), and for each of them we have a unique map $S_b \to T_\beta$ lifting the map $S_b \to (T/J)_b$. If we think in terms of schemes we have a map from the open set $\operatorname{Spec}(T_\beta) \to \operatorname{Spec}(S_b)$. These

maps agree on overlaps: given b_1, b_2 and corresponding elements β_1, β_2, we may localize the map $S_{b_1} \to T_{\beta_1}$ at b_2 and the map $S_{b_2} \to T_{\beta_2}$ at b_1: the results must agree, because we get two liftings of $S_{b_1 b_2} \to (T/J)_{b_1 b_2}$ to $T_{\beta_1 \beta_2}$, and $R \to S_{b_1 b_2}$ is étale. Therefore there is a unique homomorphism $S \to T$ such that for all b, $S_b \to T_b$ is the same as $S_b \to T_\beta$. It is easy to check that this unique homomorphism gives the unique lifting.

The condition in (d) also implies that S is flat over R, since standard étale algebras are flat. Thus, (d) implies not only (a) but (b) and (c) as well.

To complete the proof, we shall show both that (a) $\Rightarrow$ (d) and that (c) $\Rightarrow$ (d). In either case, we have that S is unramified over R, and so after passing to a suitable choice of $R_a \to S_b$ (our hypothesis is preserved) we may assume that $S = C/I$ where $C = R[x]_g/(f)$ where f is monic and f' is invertible in C, i.e., C is standard étale over R. Let q be the contraction of Q to C. To complete the proof, it will suffice to show that I becomes 0 after localizing at some element of $C - q$. From the finite presentation condition, I is finitely generated. Therefore, it suffices to show that $I_q = 0$. We may now replace R by R_P and assume that (R, P, K) is quasi-local.

By Nakayama's lemma, to show that $I_q = 0$ it will suffice to show instead that $I_q = I_q^2$, i.e., that $I_q/I_q^2 = 0$. Let $L = C_q/qC_q$. By another application of Nakayama's lemma it will suffice to show that $L \otimes_{C_q} (IC_q/I^2C_q) = 0$. Now, because C is unramified over R, C/PC is unramified over $R/P = K$, and so is reduced and zero-dimensional. But then C_q/PC_q is local, reduced, and zero-dimensional, which means that it is a field. It follows that $C_q/PC_q = L$ and that $PC_q = qC_q$. For any C_q-module M,

$$L \otimes_{C_q} M \cong (C_q/qC_q) \otimes_{C_q} M \cong M/qM \cong M/PM \cong R/P \otimes_R M = K \otimes_R M.$$

Applying this with $M = IC_q/I^2C_Q$, we see that to complete the proof it suffices to show that $K \otimes_R (IC_q/I^2C_q) = 0$.

We have an exact sequence of R-modules:

$$(**) \qquad 0 \to IC_q/I^2C_q \xrightarrow{\alpha} C_q/I^2C_q \xrightarrow{\beta} S_Q \to 0$$

(recall that $S_Q = C_q/IC_q$). If we are assuming (a) we have that S is étale over R and so S_Q is formally étale over R. Therefore the R-algebra isomorphism $S_Q \to C_q/IC_q$ has a unique lifting to a homomorphism $S_Q \to C_q/I^2C_q$. This map is a splitting, over R, of the map $\beta : C_q/I^2C_q \to S_Q$, so that $C_q/I^2C_q \cong S_Q \oplus IC_q/I^2C_q$. This implies that the exact sequence $(**)$ remains exact when we apply $K \otimes_R \_$. On the other hand, if we are assuming that S is flat over R then so is S_Q. This implies that $\mathrm{Tor}_R^1(K, S_Q) = 0$, and so the sequence $(**)$ remains exact when we apply $K \otimes_R \_$ as well. Thus, in either of the two cases, we see that we may identify $K \otimes_R (IC_q/I^2C_q)$ with the kernel of the map $K \otimes_R \beta$, and so we have reduced to proving that $K \otimes_R \beta$ is an injective map.

Since both $R \to C$ and $R \to C \twoheadrightarrow S$ are unramified over R, these two homomorphisms are unramified over K once we apply $K \otimes_R \_$. This implies that

$$K \to K \otimes_R C_q \qquad \text{and} \qquad K \to K \otimes_R C_q \twoheadrightarrow K \otimes_R S_Q$$

are maps of K into separable algebraic finite field extensions of K. We therefore have that the map $K \otimes_R C_q \to K \otimes_R S_Q$ is injective. Since we have a factorization

$$K \otimes_R C_q \twoheadrightarrow K \otimes_R C_q/I^2C_q \twoheadrightarrow K \otimes_R S_Q,$$

both these maps are injective as well as surjective, and the second of them is $K \otimes_R \beta$. $\square$

Lecture of February 1, 2010

Our next main objective is the Jacobian criterion for smoothness. We need some preliminary results. The first gives a useful criterion for when the cokernel of a matrix over a quasilocal ring is free. For this lemma we need some discussion of ideals of minors.

If M is a matrix over a ring a ring R we denote by $I_t(M)$ the ideal generated by the size t minors (or subdeterminants) of M. By convention, $I_0(M) = R$. (The determinant of a 0×0 matrix ought to be 1, because it is the determinant of an identity map, albeit on a zero module. With this convention, the determinant of the direct sum of two square matrices is the product of their determinants, even if one of the matrices is 0×0.) Note that $I_t(M) = I_1\big(\bigwedge^t(M)\big)$. If M and N are matrices whose sizes are such that MN is defined, we have that $\bigwedge^t(MN) = \bigwedge^t(M)\bigwedge^t(N)$. It follows easily that every size t minor of MN is a sum in which each term is the product of a size t minor of M and one of N, and so $I_t(MN) \subseteq I_t(M)I_t(N)$. If U is invertible, $I_t(UM) \subseteq I_t(U)I_t(M) \subseteq I_t(M)$, while

$$I_t(M) = I_t\big(U^{-1}(UM)\big) \subseteq I_t(U^{-1})I_t(UM) \subseteq I_t(UM),$$

and so $I_t(M) = I_t(UM)$, provided, of course, that UM is defined. Similarly, if V is invertible and MV is defined we have that $I_t(M) = I_t(MV)$.

Lemma. *Let M be an $n \times m$ matrix over a quasilocal ring (A, q, K). Then the cokernel of the linear map induced by M from $A^m \to A^n$ (we also use M to denote this map) is free of rank d if and only if $I_{n-d+1}(M) = 0$ while $I_{n-d}(M) = A$.*

Moreover, if $d = n - m$ the following conditions are equivalent:

(a) $\operatorname{Coker}(M)$ *is free of rank $n - m$.*
(b) $I_m(M) = A$.
(c) *Some size m minor of A is a unit.*
(d) *The image of M mod q has rank m.*
(e) *The rows of M span A^m.*
(f) *There exists an $m \times n$ matrix $\mathcal{W}$ such that $\mathcal{W}M$ is the size m identity matrix.*

Proof. Replacing M by UMV, where U and V are invertible, does not affect the ideals of minors of various sizes, and does not affect the cokernel. If some entry of M is a unit we may perform elementary row and column operations until the unit is in the upper left hand corner and is replaced by the element 1. We may then perform elementary row and column operations to get the rest of the entries in the first column and row to be 0. We may then iterate this process with the $n - 1 \times m - 1$ matrix in the lower right corner.

Eventually, we express M is the direct sum of a size k identity matrix $\mathbf{1}_k$ (k may be 0) and an $n-k \times m-k$ matrix M' all of whose entries are in q, and we need only consider this case. The cokernel of the M is the direct sum of the two cokernels, and therefore is equal to the cokernel of M'. This cokernel is free if and only if $M' = 0$, since otherwise one has non-trivial relations on what must be a minimal set of generators. Note that if $M' = 0$, the cokernel is free of rank $n-k$, and one has that $I_{k+1}(M) = 0$ while $I_k(M) = A$. Here, $d = n-k$, and so $k = n-d$. It remains only to see that if $M' \neq 0$, then we cannot have one ideal of minors be the unit ideal while the ideal generated by the next larger size minors is 0. Consider the ideals of minors mod q. It is clear that, $I_k(M) = A$ while $I_t(M) \subseteq q$ for $t > k$. We can complete the proof of the first statement by showing that if $M' \neq 0$, then $I_{k+1}(M) \neq 0$. Let w be a nonzero entry of w and form the submatrix determined by the first k rows of M and the row of w together with the first k columns of M and the column of w. This submatrix is the direct sum of I_k and the 1×1 matrix $\big(w\big)$, and has determinant $w \neq 0$, as required.

The equivalence of the six conditions for the case $d = n - m$ is then easy: (a) $\Leftrightarrow$ (b) by what we have already proved, and (b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d) is clear. We have that (d) $\Rightarrow$ (e) by Nakayama's lemma, while (e) $\Rightarrow$ (f) is an easy exercise: the ith row of $\mathcal{W}$ consists of the coefficients needed to express the ith standard basis vector as a linear combination of the rows of M. Finally, (f) $\Rightarrow$ (b) because $A = I_m(\mathbf{1}_m) = I_m(\mathcal{W}M) \subseteq I_m(\mathcal{W})I_m(M) \subseteq I_m(M)$. $\square$

We also need:

Lemma. *Let S be an R-algebra and let T be any formally smooth R-algebra that maps onto S (we know that a polynomial ring over R or a localization of a polynomial ring is formally smooth). Let $S = T/I$. Then S is formally smooth over R if and only if the R-algebra homomorphism $T/I^2 \xrightarrow{\beta} S = T/I$ splits in the category of R-algebras.*

Proof. Evidently, if S is formally smooth one has a lifting of the identity on $S = T/I$ to an R-algebra map $\beta : S \to T/I^2$ which gives the splitting. Now suppose that one has this splitting and that one has a map $S \to U/J$ where $J^2 = 0$. Then we have a composite map $T \twoheadrightarrow S \to U/J$ from which we get an R-algebra map $T \to U$, lifting $T \to U/J$ (because T is formally smooth over R) such that I maps into J. Thus, I^2 maps into $J^2 = 0$, and so we have an induced map $T/I^2 \to U$ that lifts $T/I \to U/J$. The composite $S \xrightarrow{\beta} T/I^2 \to U$ gives the lifting we want. $\square$

We are now ready to prove the following:

Theorem (Jacobian criterion for smoothness). *Let $S = R[x]/I = R[x_1, \ldots, x_n]/I$, where I is finitely generated, and let $Q \in Spec(S)$. Let $\widetilde{Q}$ denote the inverse image of Q in $R[x]$. Let $h(Q)$ denote the least number of generators of $I_{\widetilde{Q}}$. Then $R \to S$ is smooth near Q if and only if $(\Omega_{S/R})_Q$ is free of rank $n - h(Q)$, and this holds iff S_Q is formally smooth over R.*

Moreover, a localization S' of S is formally smooth over R if and only if $(S')_Q$ is formally smooth for every prime (respectively, maximal) ideal Q of S'.

Proof. Consider a localization $S' = W^{-1}R[x]/I$, where $I = (F_1, \dots, F_m)R[x]$. By the preceding Lemma, S' is formally smooth if and only if $W^{-1}R[x]/I^2 \to S$ splits. Let $\overline{x}_i$ be the image of x_i mod I^2 and x_i' be its image mod I. Constructing the splitting is equivalent to finding elements $\delta_1, \dots, \delta_n \in I/I^2$ such that the n elements $\overline{x}_1 + \delta_1, \dots, \overline{x}_n + \delta_n$ can serve as the images of the x_i' under the splitting, and the condition is simply that the m elements

$$F_j(\overline{x}_1 + \delta_1, \dots, \overline{x}_i + \delta_i, \dots, \overline{x}_n + \delta_n)$$

vanish in $W^{-1}R[x]/I^2W^{-1}R[x]$. Using Taylor's formula, this system may be written as

$$F_j + \sum_i \frac{\partial F_j}{\partial x_i}\delta_i \equiv 0 \text{ mod } I^2W^{-1}R[x].$$

That is, the expression on the left vanishes when each F_j and each $\dfrac{\partial F_j}{\partial x_i}$ is replaced by its image in $W^{-1}R[x]/I^2W^{-1}R[x]$.

Let $v_1, \dots, v_m$ be the images of $F_1, \dots, F_m$ in $IW^{-1}R[x]/I^2W^{-1}R[x]$, and let $v = (v_1 \ \dots \ v_m)$. Let $\mathcal{J}$ be the image of the matrix $\left(\dfrac{\partial F_j}{\partial x_i}\right)$ in S'. Since each δ_i is to be a linear combination of the elements v_j, say $\delta_i = \sum_{k=1}^m v_k w_{ki}$, with the $w_{ki} \in S'$, we see that S' is formally smooth over R if and only if there exists an $m \times n$ matrix $\mathcal{W}$ with entries in S' such that $-v = v\mathcal{W}\mathcal{J}$.

Here, v and $\mathcal{J}$ are fixed and we seek the unknown entries of $\mathcal{W}$. The system is a system of linear equations over S' in unknowns w_{ki} that are allowed to be arbitrary elements of S'. The coefficients are in $IW^{-1}R[x]/I^2W^{-1}R[x]$. The problem of whether such a system has a solution is local on S', that is, it has a solution in S' if and only if it has a solution after localization at every prime ideal if and only if it has a solution after localization at every maximal ideal. The reason is that such a system has a solution if and only if a certain element of a certain module is in the span of certain other elements of the module. The final statement of the theorem is now clear.

In the remainder of the proof we may assume that $W = R[x]-\widetilde{Q}$. Moreover, in analyzing this case we may assume that the F_j have been chosen to be a minimal system of generators of $IR[x]_{\widetilde{Q}}$. Thus, we are in the situation where $m = h(Q)$. The statement that $(\Omega_{S/R})_Q$ is free of rank $n - m$ is equivalent to the statement that $I_m(\mathcal{J})$ is the unit ideal. By part (f) of the Lemma on freeness of cokernels, if $I_m(\mathcal{J})$ is the unit ideal then we can choose $\mathcal{W}$ such that $\mathcal{W}(-\mathcal{J}) = \mathbf{1}_m$. On the other hand, if $-v = v\mathcal{W}\mathcal{J}$ then after tensoring with the residue class field (I/I^2 becomes an m-dimensional vector space with the images of the v_j as a basis), we see that the image of $\mathcal{J}$ has rank m. $\square$

Lecture of February 3, 2010

We next want to give some alternative characterizations of smooth algebras.

Theorem. *Let S be a finitely presented R-algebra. The following conditions are equivalent:*

(a) *S is smooth over R.*
(b) *Near every prime Q of S, S is étale over a polynomial ring in finitely many variables.*
(c) *Near every maximal ideal Q of R, S is étale over a polynomial ring.*

In consequence, if S is smooth over R, then S is flat over R.

Proof. Polynomial and étale extensions are flat, and flatness is local on *Spec*(S), so that condition (b) implies flatness. Therefore it will suffice to show that (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a). It is clear that (b) $\Rightarrow$ (c). Assume (c). To prove that S is smooth, it suffices to prove that S_Q is formally smooth for every Q. Since every S_Q is a localization of S_m for some maximal $m \supseteq Q$, it suffices to show that S_m is formally smooth when m is maximal. This is clear from the condition in (c), since étale homomorphisms and adjunction of finitely many indeterminates are both smooth, and localization is formally smooth.

This means we need only prove the most interesting of the implications, namely, that (a) $\Rightarrow$ (b). Suppose that $S = R[x_1, \ldots, x_n]/I$ is smooth over R, where I is finitely generated. Fix $Q \in \text{Spec}\,(S)$, and let $\widetilde{Q}$ be the inverse image of Q in $R[x]$. Suppose that $IR[x]_{\widetilde{Q}}$ has m generators. Then we may choose $g \in R[x] - \widetilde{Q}$ such that these m generators $F_1, \ldots, F_m$ are in $R[x]_g$ and $IR[x]_g = (F_1, \ldots, F_m)R[x]_g$. Here, $m = h(Q)$ in the notation of the Jacobian criterion from the preceding lecture. Let $\mathcal{J}$ denote the image of the matrix $(\dfrac{\partial f_j}{\partial x_i})$ over S. The fact that S is smooth near Q together with the Jacobian criterion for smoothness imply that some $m \times m$ minor of $\mathcal{J}$ is not in $\widetilde{Q}$. Without affecting any relevant issues, we may replace S by its localization at the image of this minor, and therefore assume that the image of this minor is invertible in S. By renumbering, we may assume that this minor is formed from the last m rows of $\mathcal{J}$.

Let $d = n - m$, and let $z_i = x_{i+d}$, $1 \leq i \leq m$. Let $R' = R[x_1, \ldots, x_d]$, and let G_j denote F_j thought of as an element of $R'[z_1, \ldots, z_m]$. Then we may think of S (after localizing at one element) as a localization at one element of $R'[z_1, \ldots, z_m]/(G_1, \ldots, G_m)$ such that the image of $(\dfrac{\partial G_j}{\partial z_i})$ is invertible: the determinant Δ is the minor that we know is not in $\widetilde{Q}$. This shows that

$$R'[z_1, \ldots, z_m]_{g\Delta}/(G_1, \ldots, G_m)$$

is étale over the polynomial ring $R' = R[z_1, \ldots, z_d]$, by part (b) of the first Proposition in the Lecture Notes of January 22. But this ring is the localization of S at the image b of $g\Delta$ $\square$

Before proceeding further, we want to characterize smooth extensions first over algebraically closed fields and then over arbitrary fields.

Lemma. *Let K be an algebraically closed field and let S be a finitely generated K-algebra. Let Q be a maximal ideal of S. The following conditions are equivalent:*

(a) *S_Q is (formally) smooth over K.*
(b) *S_Q is a regular local ring.*

(c) $(\Omega_{S/K})_Q$ *is free of rank equal to the Krull dimension of* S_Q.

Proof. S is generated over K by elements of Q ($S = K + Q$) and so we can map $K[x_1, \ldots, x_n] \twoheadrightarrow S$ so that all x_i map into Q. Let $\widetilde{Q} = (x_1, \ldots, x_n)$. Then $S_Q \cong W^{-1}K[x_1, \ldots, x_n]/(F_1, \ldots, F_m)$ where $W = K[x_1, \ldots, x_n] - \widetilde{Q}$. Moreover, we may assume that the F_i are a minimal set of generators for the ideal they generate in the ring $W^{-1}K[x_1, \ldots, x_n]$. The fact that (a) and (b) are equivalent may now be deduced from the Jacobian criterion for smoothness. Think of K as S/Q, and let $\mathcal{J}$ be the Jacobian matrix. Then $K \otimes_S \mathcal{J}$ has rank m if and only if the linear forms occurring in $F_1, \ldots, F_m$ are linearly independent: the coefficient of x_i in F_j is the same as the image of $(\dfrac{\partial F_j}{\partial x_i})$ mod Q. This is equivalent to the condition that the F_j are part of a minimal system of generators for $\widetilde{Q}K[x_1, \ldots, x_n]_{\widetilde{Q}}$, which is tested mod $\widetilde{Q}^2$. But we know that a quotient of a regular ring is regular if and only if the ideal being killed is part of a minimal set of generators of the maximal ideal: see Problem **4.** of Problem Set #2 from Math 615. This shows that (a) $\Leftrightarrow$ (b). Moreover, when these equivalent conditions hold, we have also seen that $n - m = \dim(S_Q)$, so that the equivalent conditions (a) and (b) imply (c).

Now assume (c), so that $(\Omega_{S/K})_Q$ is free of rank equal to $\dim(S_Q)$. We must show S_Q is regular. To see this, renumber the F_j so that $F_1, \ldots, F_h$ have linearly independent linear forms, where h is the dimension of the span of the linear forms of the F_j. By subtracting K-linear combinations of $F_1, \ldots, F_h$ from the remaining F_j, we may assume that $F_{h+1}, \ldots, F_m$ are in $\widetilde{Q}^2$. Let $T = W^{-1}K[x_1, \ldots, x_n]/(F_1, \ldots, F_h)$. Then T is a regular local ring of Krull dimension $n-h$. Since the cokernel of $\mathcal{J}$ is free once we localize, the rank of $\mathcal{J}$ once we tensor with S_Q may be computed modulo QS_Q, and so is h. It follows that $(\Omega_{S/K})_Q$ has rank $n - h$. But we are given that the rank is $\dim(S_Q)$. It follows that $\dim(S_Q) = n - h$. But S_Q is a homomorphic image of the regular local ring T, which has dimension $n - h$ and is a domain. If the kernel were nonzero, the dimension of the quotient would drop. It follows that $S_Q = T$, and so S_Q is regular. Therefore (c) $\Rightarrow$ (b). $\square$

Lecture of February 5, 2010

We next want to characterize smooth algebras over an arbitrary field. In order to do so, we need to discuss geometrically regular K-algebras. We need a lemma first.

Lemma. *Let $S \to T$ be a ring homomorphism.*

(a) *If T is faithfully flat over S then for every prime ideal P of S there is a prime ideal Q of T lying over P: in fact, any minimal prime of PT has this property.*

(b) *If $S \to T$ is a faithfully flat homomorphism and T is a regular Noetherian ring then S is regular.*

(c) *If S is Noetherian and is a direct limit $\varinjlim_t S_t$ of regular Noetherian rings, then S is regular.*

(d) *If $(S, P) \to (T, Q)$ is flat local, where the rings are Noetherian, then* $\dim(T) = \dim(S) + \dim(S/PS)$.

(e) *If $(S, P) \to (T, Q)$ is flat local such that (S, P) and and T/PT (the closed fiber) are regular, then T is regular.*
(f) *if $S \to T$ is flat, T is Noetherian, S is regular, and all fibers of $S \to T$ are regular, then T is regular.*
(g) *If $K \subseteq S$ where K is a field and L is a field containing K such that $L \otimes_K S$ is regular, then S is regular.*
(h) *If $K \subseteq S$ where K is a field and S is regular, and if L is a finite separable algebraic extension of K, then $L \otimes_K S$ is regular.*

Proof. For part (a), since T is faithfully flat PT is a proper ideal of T and has a minimal prime Q. We want to show that Q lies over P. Suppose that Q lies over P'. Then $R_{P'} \to S_Q$ is faithfully flat, and so is $R_{P'}/PR_{P'} \to S_Q/PS_Q$. This map is therefore injective. Since Q is minimal over PS, every element of the maximal ideal of S_Q/PS_Q is nilpotent, and so every element of the maximal ideal of $P'R_{P'}$ is nilpotent mod $PR_{P'}$. Since $PR_{P'}$ is prime, this shows that $P' = P$.

For (b), let P be any any prime of S. By part (a), we can choose Q lying over P, and then $S_P \to T_Q$ is a faithfully flat local map of local rings. Since T_Q is regular, so is S_P, by the second corollary on the first page of the Math 615 Lecture Notes from February 18.

In (c), let Q be any prime ideal of S and let Q_t be its contraction to S_t for all t. Then S_Q is the direct limit of the rings $(S_t)_{Q_t}$. Thus, we may assume without loss of generality that all the rings and maps are local. We use induction on $\dim(S)$.

Note that S is clearly a domain, since all the S_t are and a direct limit of domains is a domain. The case of dimension 0 is clear, since then S must be a field. If S has positive dimension let x be an element of $Q - Q^2$. Then for sufficiently large t_0, we have $x_{t_0} \in S_{t_0}$, mapping to x. We may restrict to $t \geq t_0$ without changing the direct limit. Let x_t be the image of x_{t_0} in S_t. Then we must have that $x_t \in Q_t - Q_t^2$: if x_t were a unit, x would be a unit, while if x_t were in Q_t^2, x would be in Q^2. Then the rings S_t/x_tS_t are regular, and their direct limit is S/xS. By the induction hypothesis, S/xS is regular, and, therefore, S is.

We prove (d) by induction on $\dim(S)$. If $\dim(S) = 0$ then P is nilpotent. Therefore, $\dim(T) = \dim(T/PT)$, as required. If $\dim(S) > 1$ we first reduce to the case where S is reduced: let J be the ideal of nilpotents in S and we may study $S/J \to T/JT$ instead. In the reduced case there is a nonzerodivisor x in S. Then x is a nonzerodivisor in T, since we may apply $T \otimes_S \_$ to $0 \to S \xrightarrow{x} S$, and we may apply the induction hypothesis to $S/xS \to T/xT$. The closed fiber is unaltered, and so $\dim(T) - 1 = \dim(T/xT) = \dim(S/xS) + \dim(T/PT)$ (by the induction hypothesis) $= \dim(S) - 1 + \dim(T/PT)$, and the result follows.

To prove (e), let d be the dimension of S and let n be the dimension of T/PT, so that T has dimension $d + n$ by part (e). P has d generators, and Q/PS has n generators, and putting together the former with liftings of the latter to Q, we see that Q has $d + n$ generators. This shows that T is regular.

For part (f), let Q be a maximal ideal of T lying over P in S. Then $S_P \to T_Q$ is faithfully flat and local, and the closed fiber is the fiber of $S \to T$ over P localized at Q, and so is regular. Thus, T_Q is regular by part (e).

Part (g) is immediate from (b), since $L \otimes_K S$ is faithfully flat over S (even free: L is free over K).

For part (h), note that since $S \to L \otimes S$ is flat, it suffices to prove that the fibers are regular, and each has the form $L \otimes_K K'$, where $K' = S_P/PS_P$ for some prime P. Let F be an algebraically closed field containing K'. Then it suffices to prove that $L \otimes_K F$ is regular, by part (g). But $L \cong K[x]/(f)$ where f is a polynomial with distinct roots in F, and so $L \otimes_K F \cong F[x]/(f)$ and, by the Chinese Remainder theorem, this is simply a product of copies of F, and is therefore regular. $\square$

In part (f), note that the result holds if we only assume that the fibers of $S \to T$ are regular over prime ideals P of S lying under maximal ideals of T.

Proposition. *Let K be a field and let S be a Noetherian K-algebra. The following conditions are equivalent:*

(a) *For every finite purely inseparable algebraic extension L of K, the ring $L \otimes_K S$ is regular.*
(b) *For every finitely generated field extension L of K, the ring $L \otimes_K S$ is regular.*

Moreover, if S is finitely generated over K the following conditions are also equivalent to these:

(c) *For some perfect field extension L of K, $L \otimes_K S$ is regular.*
(d) *For some algebraically closed field L with $L \supseteq K$, $L \otimes_K S$ is regular.*
(e) *For every field $L \supseteq K$, $L \otimes_K S$ is regular.*

Before we give the proof, we note that conditions (c), (d), and (e) cannot be used in the general case because the ring $L \otimes_K S$ need not be Noetherian.

Proof. We first note that if $L \subseteq L'$ are fields and $L' \otimes_K S$ is regular, then $L \otimes_K S$ is regular by part (g) of the Lemma. Evidently, (b) $\Rightarrow$ (a). For the other direction, note that given L, we may consider a field L' generated by finitely many generators for L over K over a perfect closure K' of K. Then L' has a separating transcendence basis over K', and can be obtained as a finite separable algebraic extension of a finite purely transcendental extension of K'. After replacing K' by a smaller field K_1 gotten by adjoining finitely many of elements of K' to K, we obtain a field L_1 finitely generated over K_1 (and, hence over K) which contains L and is obtained from K in three steps: a finite purely inseparable algebraic extension, then a finite transcendental extension, and finally, a finite separable algebraic extension. The first step gives a regular ring by hypothesis, the second obviously does not disturb regularity (one has a localization of a polynomial ring in finitely many variables), and the third preserves regularity by part (h) of the Lemma. This shows that (a) $\Rightarrow$ (b).

Now, when S is finitely generated over K, note that (e) $\Rightarrow$ (d) $\Rightarrow$ (c) $\Rightarrow$ (a) is clear (the last because a perfect extension contains every finite purely inseparable algebraic

extension, coupled with part (g) of the Lemma), and we have already shown that (a) $\Rightarrow$ (b). Finally (b) $\Rightarrow$ (e) because every field extension is a direct limit of finitely generated field extensions, and we may apply $\_ \otimes_K S$ and use part (c) of the Lemma. $\square$

We shall say that a Noetherian K-algebra is *geometrically regular* if the equivalent conditions (a) and (b) of the Proposition hold for S. If S is a finitely generated K-algebra this property is characterized by the equivalent conditions (a) through (e) of the proposition.

Lecture of February 8, 2010

We next prove:

Theorem. *Let K be a field and let S be a finitely generated K-algebra (finite presentation is automatic). The following conditions are equivalent:*

(a) *S is smooth over K.*
(b) *$L \otimes_K S$ is smooth over L for some (equivalently, every field) L.*
(c) *For some algebraically closed field $L \supseteq K$, $L \otimes_K S$ is regular.*
(d) *For every field $L \supseteq K$, $L \otimes_K S$ is regular.*
(e) *For every maximal ideal Q of S, $(\Omega_{S/K})_Q$ is S_Q-free of rank equal to $\dim(S_Q)$.*

Proof. We shall show that (a) $\Rightarrow$ (b) for all $L \Rightarrow$ (b) for some $L \Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (e) $\Rightarrow$ (a). That (a) $\Rightarrow$ (b) for all L is immediate from our results on base change, and this evidently implies (b) for some L. If $L \otimes_K S$ is smooth over L, and $\overline{L}$ is an algebraic closure of L, then $\overline{L} \otimes_K R$ is smooth over $\overline{L}$, and the result of the previous lecture then implies that $\overline{L}_K \otimes_R S$ is regular. Thus, (b) $\Rightarrow$ (c). We have already seen that (c) and (d) are equivalent.

Now assume that (d) holds. In particular, (d) holds when L is an algebraic closure of K. Let $S' = L \otimes_K S$. Then $\Omega_{S'/L} \cong L \otimes_K \Omega_{S/K} \cong S' \otimes_S \Omega_{S/K}$. Let Q' be a maximal ideal of S' lying over a given maximal ideal Q of S. Then $\dim(S'_{Q'}) = \dim(S_Q)$ and it now suffices to see that if M is a finitely generated module over S_Q the becomes free when we tensor with $S'_{Q'}$ then it was already free. This is clear, because a minimal resolution over S_Q is preserved by applying $S'_{Q'} \otimes_{S_Q} \_$.

Finally, we need to see that (e) implies (a). This follows because (e) continues to hold after we tensor with an algebraically closed field L containing K. This implies that $L \otimes_K S$ is smooth, and therefore regular. It follows that S is regular, and, therefore, every S_Q is regular. Fix a maximal ideal Q of S and write $S = K[x_1, \ldots, x_n]_{\widetilde{Q}}/(F_1, \ldots, F_m)$, where $\widetilde{Q}$ is the inverse image of Q in a polynomial ring $K[x_1, \ldots, x_n]$ mapping onto S and $F_1, \ldots, F_m \in K[x_1, \ldots, x_n]$ are minimal generators for the kernel $K[x]_{\widetilde{Q}} \to S_Q$. We know that $(\Omega_{S/K})_Q$ is free of rank equal to $\dim(S_Q)$, and we want to show that it is free of rank $n - m$. But since S_Q is regular, we know that these two numbers are equal. $\square$

Theorem. *Let S be a finitely generated R-algebra. Then the following are equivalent:*
(a) *S is smooth over R.*
(b) *S is R-flat and every fiber $\kappa_P \otimes_R S$ is geometrically regular, where $\kappa_P = R_P/PR_P$.*

(c) *S is R-flat and for every maximal ideal Q of S lying over P in* $\operatorname{Spec}(R)$*, $(\Omega_{S/R})_Q$ is free of rank equal to* $\dim(\kappa_P \otimes_R S_Q)$.

Proof. We shall prove (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a). We already know that smooth algebras are flat, since they are locally polynomial followed by étale, and that fibers, which are the result of a base change, are smooth and therefore geometrically regular. Thus, (a) $\Rightarrow$ (b). Next assume that S is R-flat, fix a maximal ideal Q, and write $S_Q \cong R[x]_{\widetilde{Q}}/IR[x]_{\widetilde{Q}}$ where $F_1, \ldots, F_m \in R[x]$ are minimal generators for $IR[x]_{\widetilde{Q}}$, as usual. The sequence

$$0 \to IR[x]_{\widetilde{Q}} \to R[x]_{\widetilde{Q}} \to S_Q \to 0$$

remains exact when we apply $\kappa_P \otimes_{R_P} \_$: since S is R-flat, S_Q is R_P flat and

$$\operatorname{Tor}_1^{R_P}(\kappa_P, S_Q) = 0.$$

It follows that the minimum number of generators m for the kernel of $K[x]_{\widetilde{Q}} \twoheadrightarrow S_Q$ does not change when we apply $\kappa_P \otimes_{R_P}$: it is still m. Let $\mathcal{J}$ denote the image of $\left(\frac{\partial F_j}{\partial x_i}\right)$ in S. Now, $(\Omega_{\kappa_P \otimes_R S/\kappa_P})_Q$ is free of rank $n-m$ iff $\kappa_P \to \kappa_P \otimes_{R_P} S_Q$ is formally smooth iff $\kappa_P \otimes \mathcal{J}$ has rank m if and only if a size m minor of $\mathcal{J}$ has invertible image in S_Q. It is now clear that in the presence of flatness for $R \to S$, we have that (b) $\Rightarrow$ (c) $\Rightarrow$ (a). $\square$

This completes our basic treatment of unramified, étale, and smooth morphisms. We next want to use our knowledge of étale morphisms to construct the Henselization of a quasilocal ring, as well as to gain understanding of what a Henselian ring is.

We recall that a quasilocal ring (R, P, K) is called *Henselian* if for every monic polynomial $F \in R[x]$ and each factorization $\overline{F} = gh$ into relatively prime monic polynomials g, h of $K[x]$, where $\overline{F}$ denotes the image of F in $K[x]$, there is a lifting of that factorization $F = GH$ to $R[x]$, where G and H are monic and $G \equiv g \bmod PR[x]$ while $H \equiv h \bmod PR[x]$. It is a theorem, Hensel's lemma, that if R is complete and P-adically separated then such a lifted factorization exists. That is, a complete P-adically separated ring is Henselian. In this case, and whenever R is P-adically separated, the factorization is unique: this follows from its uniqueness mod P^t for all t. See the Lecture Notes of January 9 from Math 615.

A module-finite extension ring S of a quasilocal ring (R, P, K) is said to *decompose* if it is a product of quasilocal rings. By a *pointed étale extension* of a quasilocal ring (R, P, K) we mean a localization (S, Q, L) of an étale algebra over R at a prime lying over P such that the induced map of residue fields $R/P \to S/Q$ is an isomorphism. Note that a pointed étale extension actually is an extension, since it is faithfully flat.

We shall prove:

Theorem. *Let (R, P, K) be quasilocal. Then the following seven conditions are equivalent:*
(1) *R is Henselian.*
(2) *Every module-finite extension of R decomposes.*

(3) *Every free module-finite extension of R decomposes.*
(4) *Every module-finite extension of R of the form $R[x]/(F)$, where F is a monic polynomial, decomposes.*
(5) *If F is a monic polynomial over R whose reduction $\overline{F}$ mod P has a simple root $\lambda \in K$, then there is an element $r \in R$ such that $r \equiv \lambda$ mod P and $F(r) = 0$.*
(6) *If $R \to S$ is a pointed étale extension, then $R \cong S$.*
(7) *If $F_1, \ldots, F_n$ are n polynomials in n variables whose images $\overline{F}_j$ mod P vanish simultaneously at $(\lambda_1, \ldots, \lambda_n) \in K^n$ and the Jacobian determinant $\det\big(\dfrac{\partial F_j}{\partial x_i}\big)$ does not vanish mod P at $x_1 = \lambda_1, \ldots, x_n = \lambda_n$, then there are unique elements $r_1, \ldots, r_n \in R$ such that for all i, $r_i \equiv \lambda_i$ modulo P and $F_j(r_1, \ldots, r_n) = 0$, $1 \leq j \leq n$.*

The proof is postponed for a bit. It is easiest to make the connection between (1) and (4), and we shall discuss this first. Note that (5) is more special than (7), and we could have made a uniqueness statement in (5) as well as in (7).

Lecture of February 10, 2010

Before giving the proof of the Theorem stated at the end of the previous lecture, we want to discuss the general problem of when a module-finite extension of a quasilocal domain decomposes.

Let (R, P, K) be quasilocal and let S be a module-finite extension of R. For every maximal ideal Q of S, S/Q is a field integral over $R/(Q \cap R)$, and so $R/(Q \cap R)$ is a field: that is, every maximal ideal of S lies over P, the unique maximal ideal of R. Since S/PS is module-finite over $K = R/P$, it is zero-dimensional. The maximal ideals of S correspond bijectively to the prime ideals of the Artin local ring S/PS, and so there are finitely many of them, say $Q_1, \ldots, Q_r$. Let $q_j = Q_j/PS$, $1 \leq j \leq r$. Then

$$S/PS \cong \prod_{j=1}^{r} (S/PS)_{q_j}$$

and $(S/PS)_{q_j} \cong (S/PS)_{Q_j}$, $1 \leq j \leq r$. Note that since P is contained in every Q_j, PS is contained in every maximal ideal of S, i.e., it is contained in the Jacobson radical of S. It is now clear that S decomposes if and only if $S \cong \prod_j S_{Q_j}$.

There are 2^r idempotents in S/PS: S/PS is a product of r indecomposable factors, and for each subset $\mathcal{S}$ of the factors there is a unique idempotent that corresponds to 1 in the factors that are in $\mathcal{S}$ and 0 in the factors in the complementary subset.

In the product ring S/PS, we shall refer to the idempotent e_j the corresponds to 1 in the factor $(S/PS)_{Q_j}$ and 0 in the other factors as the idempotent *associated with* Q_j or with $q_j = Q_j/PS$. It is characterized among the idempotents by the condition that $e_j \notin q_j$ while $e_j \in q_i$ for $i \neq j$. It is then easy to see that S decomposes if and only if all idempotents of S/PS lift to idempotents of S, and it suffices if the idempotents e_j lift. (Any other idempotent is a sum of mutually distinct e_j or 0.) An idempotent e of S lifts

e_j if and only if $e \notin Q_j$ while $e \in Q_i$ for $i \neq j$. The reason is that the image of e in S/PS is an idempotent with the corresponding membership property, and this means that the image must be e_j.

We next consider exactly what it means for $S = R[x]/(F)$ to decompose when F is monic and (R, P, K) is quasilocal. Let $f \in K[x]$ be the image of F modulo $PR[x]$. Then f factors uniquely, except for the order of the terms, as $g_1 \cdots g_r$ where the g_i are monic and are powers of mutually distinct monic irreducible polynomials. Thus, g_i and g_j generate the unit ideal in $K[x]$ if $i \neq j$. We claim that $S = R[x]/(F)$ decomposes if and only if the factorization $f = g_1 \cdots g_r$ lifts to a factorization $F = G_1 \cdots, G_r$ over $R[x]$, where every G_j is monic and $G_j \equiv g_j \bmod PR[x]$. Suppose one has the lifted factorization. Then the principal ideals G_jS are pairwise comaximal: since PS is in every maximal ideal of S, it suffices to see this working over $R[x]/PR[x] \cong K[x]$, and in this ring the G_j map to the g_j. It follows from the Chinese remainder theorem that $S \cong \prod_j S/G_jS$, and this shows that S decomposes.

For the converse, suppose that $S = \prod S_j$ decomposes, where $S_j/PS_j \cong K[x]/(g_j)$. Let $d_j = \deg(g_j)$. By Nakayama's lemma, the images of $1, x, \ldots, x^{d_j-1}$ generate S_j as an R-module, since their images in $S_j/PS_j \cong K[x]/(g_j)$ generate that ring as K-vector space, and PS_j is in the Jacobson radical. Therefore, the image of x_j^d is in the R-span of the images of $1, x, \ldots, x^{d_j-1}$ in S_j, and this means that we can choose a monic polynomial $G_j \in R[x]$ of degree d_j such that $G_j(x)$ maps to 0 in S_j. This implies that the image of G_j in $K[x]$ is divisible by g_j. Since they have the same degree, g_j is the image of G_j mod $PR[x]$. Let $G = \prod_j G_j$. Then $\deg(G) = \sum_j \deg(G_j) = \sum_j \deg(g_j) = \deg(f) = \deg(F)$. Now, x satisfies $G(x) = 0$ in S: since S is the product of the S_j, it is enough to check that this is true in every S_j, and that follows because G_j divides G. Since $S = R[x]/F$, it follows that F divides G. Since they are monic of the same degree, they are equal.

Note that if (R, P, K) is Henselian, a factorization of the image f of $F \in R[x]$ over $k[x]$, say $f = g_1 \cdots, g_r$, where the g_i, g_j are relatively prime in pairs, lifts to such a factorization into monic polynomials over $R[x]$. When $r = 2$ it is the definition of Henselian, and one may prove the result in general by induction on r: if $r \geq 3$, since $g^* = g_1 \cdots g_{r-1}$ and g_r are relatively prime, we may lift the factorization $g = g^*g_r$ to a factorization $G = G^*G_r$, and then apply the induction hypothesis to G^* and the factorization $g^* = g_1 \cdots g_{r-1}$.

We are now ready to prove the equivalence of the first four conditions in the statement of the Theorem from the previous lecture.

Proof of the equivalence of (1), (2), (3), and (4). The remarks above show that (1) $\Leftrightarrow$ (4), while (2) $\Rightarrow$ (3) $\Rightarrow$ (4) is clear. We can therefore complete the proof by showing that (4) $\Rightarrow$ (2). Let $R \subseteq S$ be module finite and let Q be a maximal ideal of R. Let e_0 be the corresponding idempotent in S/PS, so that e_0 is in Q/PS and not in any other maximal ideal. It suffices to show that e_0 lifts to S. Choose any lifting c of e_0 to S: of course, c need not be idempotent, but c is not in Q and and is in every other maximal ideal of S. Of course, c satisfies some monic polynomial $F \in R[x]$. Let $T = R[x]/(F)$. We have an R-algebra map $T \to S$ that sends the image of x in T to $c \in S$. Let q be the inverse image of Q in T, which is a maximal ideal of T. Since T decomposes it contains an idempotent e_0

that is not in q but is in every other maximal ideal of T. The image e of e_0 is an idempotent of S that is evidently not in Q. It will suffice to show that e is in every maximal ideal Q' of S other than Q, for then e must lift e_0. It suffices to show that if $Q' \neq Q$ then Q' does not lie over q, for e_0 will then be in the contraction of Q' to T, and so e will be in Q'. But if Q' lies over q then T/q injects into S/Q'. The image of x is sent to the image of c under this map, and so is sent to 0. Hence, the image of x in T is in q, and so is sent to 0 under the injection $T/q \to S/Q$. But $c \notin Q$, a contradiction. $\square$

Lecture of February 12, 2010

Proof that conditions (1), (5), (6), and (7) are equivalent. We show that (1) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (7) $\Rightarrow$ (1). Suppose that the ring is Henselian and that we have a monic polynomial F such that mod $PR[x]$ the image f of F has a simple root $\lambda \in K$. This gives a factorization $f = (x - \lambda)g$, and the fact that λ is a simple root means that $x - \lambda$ and g are relatively prime. Hence, the factorization lifts to a factorization $F = (x - r)G$ where $r \equiv \lambda \bmod P$. But then $F(r) = 0$. This shows that (1) $\Rightarrow$ (5).

Now suppose that (5) holds, and let S be a pointed étale extension of R. Then S is a localization of standard étale extension of R near Q lying over P, and so $S = (R[x]_g/F)_Q$ where F is monic, F' is invertible in S, and Q lies over P. Let λ denote the image of x in the residue field of S, which is K. Thus, if f is the image of F modulo $PR[x]$, we have that $f(\lambda) = 0$, and since F' is invertible in S, its image $f'(\lambda)$ in K is nonzero, so that λ is a simple root of F. Thus, we can choose $r \in R$ such that $F(r) = 0$, and it follows that $F = (x-r)G(x)$ for $G \in R[x]$. Since λ is a simple root of f, the image of $G(x)$ is invertible in S, which means that S is a localization of $R[x]/(x - r) \cong R$. Since $R \to S$ is a local map, we must have that $R = S$. Thus, (5) $\Rightarrow$ (6).

Assume that we have condition (6) and consider a system of equations as in (7). Let Q be the kernel of the map $R[X_1, \ldots, X_n] \to K$ that agrees with the quotient surjection $R \twoheadrightarrow R/P = K$ on R and sends $X_j \mapsto \lambda_j$, $1 \leq j \leq n$. Then the hypothesis implies that $S = R[X_1, \ldots, X_n]_Q/(F_1, \ldots, F_n)$ is a pointed étale extension of R, using part (b) of the Proposition in the Lecture Notes of January 22, and is therefore equal to R. Solving the equations in R so as to lift the solution $(\lambda_1, \ldots, \lambda_n)$ is equivalent to giving an R-algebra mapping $R[X_1, \ldots, X_n]/(F_1, \ldots, F_n) \to R$ so that under the composite $R[X_1, \ldots, X_n]/(F_1, \ldots, F_n) \to R \twoheadrightarrow K$ the elements x_j map to the elements λ_j, which is equivalent to the condition that Q map into P. Thus, giving a lifting of the solution to R is equivalent to giving a local R-algebra mapping $S \to R$. Since $R \cong S$ as R-algebras, there is a unique such mapping, and so the equations have a unique solution.

Finally, assume that (7) holds, let $F \in R[x]$ be monic of degree n, and suppose we have a factorization $f = gh$ over $K[x]$ where g, h are monic of degrees d and e respectively and $d + e = n$. Let $g = \sum_{j=0}^{d} \alpha_j x^j$ with all $\alpha_i \in K$ and $\alpha_d = 1$, and let $h = \sum_{i=0}^{k} \beta_k x^k$ with all $\beta_k \in K$ and $\beta_e = 1$. We seek to lift this factorization to $R[x]$. Proceed by letting the coefficients of the factors be unknown, i.e., we seek values for $Y_0, \ldots, Y_{d-1}$ and

$Z_0, \ldots, Z_{e-1}$ in R such that

$$F = (x^d + Y_{d-1}x^{d-1} + \cdots + Y_1 x + Y_0)(x^e + Z_{e-1}x^{e-1} + \cdots + Z_1 x + Z_0).$$

Let $F = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ where the c_i are given elements of R. This leads to a system of n equations in the $d + e = n$ unknowns Y_j, Z_k by setting the coefficient of x^t, expressed in terms of the Y_j, Z_k, equal to c_t, $0 \le t \le n-1$. After transposing c_t to the other side of the equation, the typical equation looks like:

$$\sum_{j+k=t} Y_j Z_k - c_t = 0$$

where $Y_d = 1$ and $Z_e = 1$ (these are *not* indeterminates) and where $0 \le j \le \min\{d, t\}$ and $0 \le k \le \min\{e, t\}$. We want to solve so that $Y_j \equiv \alpha_j$, $Z_k \equiv \beta_k$, $0 \le j \le d-1$, $0 \le k \le e-1$.

Explicitly, the first two equations are $Y_0 Z_0 - c_0 = 0$ and $Y_0 Z_1 + Y_1 Z_0 - c_1 = 0$, while the last equation is $Y_{d-1} + Z_{e-1} - c_{n-1} = 0$. Of course, the factorization of $f = gh$ gives a solution in K^n in which α_j is the image of Y_j and β_k is the image of Z_k. To complete the proof, it suffices to show that the Jacobian determinant of these n equations with respect to $Y_0, \ldots, Y_{d-1}, Z_0, \ldots, Z_{d-1}$, evaluated at the point $(\alpha, \beta) \in K^n$, is nonzero: condition (7) will then allow us to lift this solution to R^n, giving the required factorization.

Explicitly, the Jacobian matrix $\mathcal{J}$ is obtained by differentiating all of the polynomials we are setting equal to 0 by $Y_0, \ldots, Y_{d-1}$ and then $Z_0, \ldots, Z_{e-1}$. Each row is the sequence of partial derivatives with respect to one of the variables. The matrix is

$$\begin{pmatrix}
Z_0 & Z_1 & Z_2 & \cdots & Z_{e-1} & 1 & 0 & \cdots & 0 \\
0 & Z_0 & Z_1 & \cdots & Z_{e-2} & Z_{e-1} & 1 & \cdots & 0 \\
 & & & & \cdots & & & & \\
 & & & & \cdots & & & & \\
 & & & & \cdots & & & & \\
0 & 0 & \cdots & 0 & Z_0 & \cdots & Z_{e-2} & Z_{e-1} & 1 \\
Y_0 & Y_1 & Y_2 & \cdots & Y_{d-1} & 1 & 0 & \cdots & 0 \\
0 & Y_0 & Y_1 & \cdots & Y_{d-2} & Y_{d-1} & 1 & \cdots & 0 \\
 & & & & \cdots & & & & \\
 & & & & \cdots & & & & \\
 & & & & \cdots & & & & \\
0 & 0 & \cdots & 0 & Y_0 & \cdots & Y_{d-2} & Y_{d-1} & 1
\end{pmatrix}$$

There are d rows involving the Z_k and e rows involving the Y_j. Let $\mathcal{J}_0 = \mathcal{J}|_{(\alpha,\beta)}$ be this matrix after the α_j are substituted for the Y_j and the β_k for the Z_k.

Now consider instead the following problem: find polynomials u, v, not both 0, in $K[x]$ of degrees at most $e-1$ and $d-1$, respectively, such that $ug + vh = 0$. This problem has a solution if and only if g and h have a common factor w of positive degree. If they have such a factor, say w, for then we may write $g = vw$ and $h = -uw$ and we have that

$ug+vh = 0$. On the other hand, if g and h have no common factor but we have $ug+vh = 0$ ($u = 0$ iff $v = 0$ here) then h divides u and g divides v, contradicting the degree bounds unless both vanish. Given g, h, we can look for u and v by letting their coefficients be unknowns. Suppose that $u = \sum_{k=0}^{e-1} B_k x^k$ and $v = \sum_{j=0}^{d-1} A_j x^j$. Setting the coefficients on powers of x equal to 0 gives a system of n linear equations in the n unknowns A_j B_k: the coefficients of these equations are functions of the coefficients α, β of g and h. Consider the $n \times n$ matrix $\mathcal{M}$ of this system of linear equations. The t th row may be thought of as the coefficients of A_j and B_k occurring in the coefficient of x^t in $ug + vh = 0$. Therefore, each column consists of the coefficients on some fixed A_j (or on some fixed B_k) as t varies. For A_j we get the coefficients in $A_j x^j h$, which is a row of $\mathcal{J}_0$. For B_k we get the coefficients in $B_k x^k g$, which is also a row of $\mathcal{J}_0$. With the columns suitably ordered, we see that $\mathcal{J}_0$ is the transpose of $\mathcal{M}$. Since g and h are relatively prime, the only element in the kernel of $\mathcal{M}$ is 0, so that $\mathcal{M}$ is invertible. Hence, $\mathcal{J}_0$ is invertible. $\square$

The determinant described in the proof above is an *eliminant* for f and g: when f and g are monic of fixed degrees but their non-leading coefficients are varying, it vanishes precisely on the set of n-tuples of non-leading coefficients such that f and g have a common factor (i.e., a common root in an algebraic closure of K), which shows that this set is Zariski closed. This is the classical approach to elimination theory, and has been largely hidden by recent methods. The theorem that a projective morphism is proper, i.e., gives a closed map even after base change, contains much the same sort of information. However, specific descriptions of the equations defining the closed sets are sometimes needed.

We want to construct the Henselization of the quasilocal ring R as the direct limit of all (up to isomorphism) pointed étale extensions of R. To make this idea precise, we need to study the category of pointed étale extensions of R. The following result contains the information we need.

Theorem. *Let (R, P, K) be a quasilocal ring and let S and T denote pointed étale R-algebras.*

(a) *If I is any proper ideal of R, then $R/I \to S/IS$ is a pointed étale extension.*

(b) *The maximal ideal of S is PS.*

(c) *There exists a pointed étale R-algebra U together with local R-algebra maps $S \to U$ and $T \to U$. In fact, one may take U to be $(S \otimes_R T)_Q$ where Q is the kernel of the composite R-algebra surjection $S \otimes_R T \twoheadrightarrow K \otimes_K K \cong K$.*

(d) *If $T = S$ in the construction in (c) just above, then $(S \otimes_R S)_Q \cong S$ via the obvious map that takes $(s \otimes s')/1$ to ss'.*

(e) *There is at most one local R-algebra homomorphism from S to T, and if there is such a homomorphism then T is pointed étale over S.*

(f) *If there are local R-algebra homomorphisms from S to T and from T to S then $S \cong T$ as local R-algebras. Moreover, this isomorphism is canonical.*

(g) *If the cardinality of R is finite so is the cardinality of S. In all other cases, R and S have the same cardinality. Therefore, there exists a set $\mathcal{R}$ of pointed étale extensions of R such that $\mathcal{R}$ contains exactly one representative from each isomorphism class of pointed étale extensions (isomorphism as local R-algebras). Moreover, $\mathcal{R}$ is partially*

ordered by the rule that $S \leq T$ if and only if there exists a local R-algebra map from S to T. With this partial ordering, $\mathcal{R}$ is a directed set.

Proof. Part (a) is clear: this is base change so the map remains localized étale. It is clear that the map is still local and the the map of residue class fields does not change.

By part (b), S/PS is a pointed étale extension of the field $K = R/P$: since it is local, it is a field, and so $K \to S/PS$ must be an isomorphism. This proves (b).

To prove (c), first note that the statement that the tensor product of two étale algebras is étale is left as an exercise: cf. the first problem of Problem Set #2. The composite

$$R \to S \otimes_R T \to K \otimes_K K \to K$$

is isomorphic with the quotient surjection $R \twoheadrightarrow R/P = K$, and so $R \to (S \otimes_R T)_Q$ is local, and the induced map of residue class fields is an isomorphism.

Note that the map $S \otimes_R S \to S$ sends Q onto the maximal ideal of S, and is surjective. Since S is a localization of a finitely presented R-algebra, the kernel I of $S \otimes_R S \to S$ is a finitely generated ideal I_0, and since S is formally étale and therefore formally unramified over R, $I_0^2 = I_0$. Let $I = I_0(S \otimes_R S)_Q$, the kernel of the map $(S \otimes_R S)_Q \twoheadrightarrow S$. Then I is finitely generated and contained in the maximal ideal, and $I^2 = I$. It follows from Nakayama's lemma that $I = 0$, and so $(S \otimes_R S)_Q \to S$ is an isomorphism. This completes the proof of (d).

Suppose that there are two local R-algebra homomorphisms from $S \to T$, call them f and g. Then there is an R-algebra homomorphism $S \otimes_R S \to T$ that sends $s \otimes s' \mapsto f(s)g(s')$, and, with notation as in part (d), it carries Q into the maximal ideal of T and so induces a map $(S \otimes_R S)_Q \to T$ whose value on $s \otimes 1/1$ is $f(s)$ and whose value on $1 \otimes s/1$ is $g(s)$. But under the isomorphism of $(S \otimes_R S)_Q \cong S$ established in (d), both $s \otimes 1$ and $1 \otimes s$ map to s, i.e., $s \otimes 1/1 = 1 \otimes s/1$ in $(S \otimes_R S)_Q$. It follows that $f(s) = g(s)$, and this establishes the first statement in (e).

Now suppose that we have local R-algebra maps $R \to S \to T$ where S and T are pointed étale over R. We want to show that T is pointed étale over S. The module of differentials $\Omega_{T/S} = 0$ simply because $\Omega_{T/R} = 0$, and so T is formally unramified over S. It follows from the structure theory that we may write $T = U/I$ where U is a local ring of an étale S-algebra. We know that all of the residue class fields are isomorphic. Thus, to complete the proof, it will suffice to show that $I = 0$. We know that I is finitely generated. Consider the exact sequence $0 \to I \to U \to T \to 0$. Since T is R-flat, we have that $\mathrm{Tor}_1^R(K, T) = 0$. Therefore the sequence remains exact when we apply $K \otimes_R \_$, giving $0 \to I/PI \to U/PU \to T/PT \to 0$. Since U and T are both pointed étale over R, the map $U/PU \to T/PT$ is an isomorphism: these quotients are both K, by part (b). It follows that $I/PI = 0$, and then $I = (0)$ by Nakayama's lemma.

Part (f) is then immediate because the compositions of the two maps must be the respective identity maps on S and T: the only local R-algebra map from $S \to S$ (or $T \to T$) is the identity. The isomorphisms are obviously unique, since there is at most one local R-algebra map from $S \to T$ or $T \to S$.

Let $|\ \ |$ indicate cardinality. Then $|R[x]/(F)|$ is $|R|^n$ for F monic of degree n. Elements of $W^{-1}T$ are parametrized by $T \times W$ and so $|W^{-1}T| \leq |T|^2$. It follows that $|R| \leq |S| \leq |R|^{2n}$ for any pointed étale extension S of R (note that $R \hookrightarrow S$ here). Therefore, $|S|$ is finite if $|R|$ is and $|S| = |R|$ otherwise. The existence of the set $\mathcal{R}$ is then immediate from the axiom of choice. The relation $\leq$ is transitive because one can compose local R-algebra maps, and we have a partially ordered set using (f). The set is directed because of (c). This proves (g). $\square$

It is easy to see that the construction $(S \otimes_R T)_Q$ in part (c) gives the coproduct of S and T in the category of pointed étale R-algebras and local R-algebra homomorphisms.

Lecture of February 15, 2010

Let (R, P, K) be a quasilocal ring. By a *Henselization* (S, Q, L) for R we mean a quasilocal ring together with a local homomorphism $R \to S$ such that every local homomorphism from R to a Henselian quasilocal ring T, the map $R \to T$ factors uniquely $R \to S \to T$. If S' is another Henselization of R the mapping properties give that $R \to S'$ factors uniquely as $R \to S \to S'$ and $R \to S$ factors uniquely as $R \to S' \to S$. The maps $S \to S'$ and $S' \to S$ must compose to give the respective identity maps on S and S'. Thus, a Henselization of R is unique up to unique isomorphism.

We can now construct the Henselization of a quasilocal ring (R, P, K) as follows: choose a set $\mathcal{R}$ of pointed étale extensions of R containing exactly one representative of every isomorphism class. Then $\mathcal{R}$ is a directed set indexing itself, and when $S \leq T$ there is a unique local R-algebra map $S \to T$. We may therefore take the direct limit, $\varinjlim_{S \in \mathcal{R}} S$. We denote this direct limit as R^{h}.

Theorem. *R^{h} is a Henselization of the quasilocal ring (R, P, K). It is faithfully flat over R, and has maximal ideal PR^{h}. Its residue class field is K.*

Proof. Let $g : R \to T$ be a local map from R to a Henselian ring T. We want to show that it has a unique local extension to R^{h}, and it suffices to show that it has a unique local extension to (S, Q, K) for every pointed étale extension S of R. Note that we have $S \otimes_R T \to K \otimes_R L \cong L$: call the kernel $\mathcal{Q}$. Then $(S \otimes_R T)_{\mathcal{Q}}$ is a localization of an étale extension of T, $T \to (S \otimes_R T)_{\mathcal{Q}}$ induces an isomorphism $L \cong K \otimes_R L \cong L$ of residue fields. Thus, $(S \otimes_R T)_{\mathcal{Q}}$ is a pointed étale extension of T. Since T is Henselian, it is equal to T. The local map $S \to (S \otimes_R T)_{\mathcal{Q}} = T$ is the map we want. The fact that $(S \otimes_R T)_{\mathcal{Q}} = T$ also implies uniqueness.

Since R^h is a direct limit of flat quasilocal rings and local R-algebra homomorphisms, it is a flat R-algebra, and the map $R \to R^{\mathrm{h}}$ is local, so that R^{h} is faithfully flat. P expands to the maximal ideal of R^{h} because that is true for every pointed étale extension, and $K \cong R^{\mathrm{h}}/PR^{\mathrm{h}}$ because $K \cong S/PS$ for every pointed étale extension S of R. $\square$

We pause in our treatment of Henselization to consider further our results on smooth homomorphisms. The following result was stated in the lecture of January 13 as the last Theorem, to be proved later:

Theorem. *Let S be a finitely presented R-algebra.*
(a) *If R contains the rationals, S is smooth over R if and only if S is flat over R and $\Omega_{S/R}$ is projective as an R-module.*
(b) *S is étale over R if and only if S is flat over R and $\Omega_{S/R}$ is 0.*
(c) *S is unramified over R if and only if $\Omega_{S/R} = 0$.*

We eventually proved (b) and (c), but we never proved (a), although we did give criteria for smoothness involving the local freeness of the module of differentials subject to a condition on its rank.

With no condition on the rank, the hypothesis of characteristic 0 (or some other additional hypothesis) is needed. For example, let R be a field K of characteristic $p > 0$ and let $S = K[x]/(x^p)$. Then $d(x^p) = 0$, and from this is it follows that $\Omega_{S/R}$ is S-free of rank one on dx.

We want to prove (a) in equal characteristic 0. To analyze the situation it will help to consider differentials over complete local rings (R, m, K) with coefficient field K, but we want to use a somewhat different notion in this case: the ordinary module of differentials $\Omega_{R/K}$ need not be finitely generated, but its m-adic completion $\widehat{\Omega}_{R/K}$ is. (The power series ring $R = K[[x_1, \ldots, x_n]]$ typically has uncountable transcendence degree over K, even when $n = 1$. If K has characteristic 0, and $\{u_j\}_{j\in J}$ is a transcendence basis in R for $\mathcal{F}$, the fraction field of R, over K, then because the extension $K(u_j : j \in J) \subseteq \mathcal{F}$ is separable, we have that $\Omega_{\mathcal{F}/K}$ is free on the du_j, and needs uncountably many generators. This is a localization of $\Omega_{T/K}$, which must also need uncountably many generators. In characteristic p, if K is perfect then any derivation kills $T_0 = K[[x_1^p, \ldots, x_n^p]]$. Since T is module-finite over T_0 it is certainly finitely generated as an algebra over T_0 by the elements dx_j. It follows that $\Omega_{T/K} = \Omega_{T/T_0}$ is a finitely generated T-module and so is already complete and $\widehat{\Omega}_{T/K} = \Omega_{T/K}$ in this case.)

In order to see that $\widehat{\Omega}_{R/K}$ is finitely generated, we first want to define $\dfrac{\partial}{\partial x}$ for a power series ring $R[[x]]$. We may define this formally by the rule

$$\frac{\partial}{\partial x}\sum_{i=0}^{\infty} r_i x^i = \sum_{i=1}^{\infty} r_i i x^{i-1},$$

where the $r_i \in R$. Alternatively, we may obtain $\dfrac{\partial}{\partial x}F$ by introducing a new formal indeterminate Δ, noting that $F(x+\Delta) - F(x)$ is divisible by Δ in $R[[x, \Delta]]$, and letting

$$\frac{\partial}{\partial x}F = \left.\frac{F(x+\Delta) - F(x)}{\Delta}\right|_{\Delta=0}.$$

This is an R-derivation of $R[[x]]$ into itself. Now, consider $A[[x_1, \ldots, x_n]]$, the formal power series ring in n variables over A. We may define $\dfrac{\partial}{\partial x_i}$ for $1 \leq i \leq n$ by letting R_i be the formal power series ring over A in the variables other than x_i and thinking of $A[[x_1, \ldots, x_n]]$ as $R_i[[x_i]]$.

Now let (R, m, K) be a complete local ring with coefficient field K, so that we have $K \hookrightarrow R$ as well as $R \twoheadrightarrow K$ and the composition is the identity. We write $\widehat{\Omega}_{R/K}$ for the m-adic completion of $\Omega_{R/K}$. By a *complete* R-module M we mean an R-module that is complete and separated in the m-adic topology. The composition $d : R \to \Omega_{R/K} \to \widehat{\Omega}_{R/K}$ gives a K-derivation of R into $\widehat{\Omega}_{R/K}$ which we still denote by d.

Then:

Proposition. *Let (R, m, K) be complete local with coefficient field K.*

(a) *For every complete R-module M, there is a bijection between $\mathrm{Hom}_R(\widehat{\Omega}_{R/K}, M)$ and K-derivations of R into M: every derivation is obtained from a unique R-linear map $L : \widehat{\Omega}_{R/K} \to M$ by composition with d. This mapping property together with the condition that $\widehat{\Omega}_{R/K}$ be complete characterizes $\widehat{\Omega}_{R/K}$ up to unique isomorphism.*

(b) *If R is a formal power series ring $K[[x_1, \ldots, x_n]]$, then $\widehat{\Omega}_{R/K}$ is the free R-module on the basis dx_i, and*

$$dF = \sum_i \frac{\partial F}{\partial x_i} dx_i$$

(c) *If R is the quotient of $K[[x_1, \ldots, x_n]]$ by the ideal with generators $F_1, \ldots, F_m$, $\widehat{\Omega}_{R/K}$ is quotient of the free R-module on the dx_i by the images of the df_j: thus $\widehat{\Omega}_{R/K}$ is the cokernel of the Jacobian matrix $\left(\frac{\partial F_j}{\partial x_i}\right)$, which is consequently independent of the choice of presentation $K[[x_1, \ldots, x_n]]/(F_1, \ldots, F_m)$. In particular, $\widehat{\Omega}_{R/K}$ is finitely generated.*

Proof. For part (a), the derivation induces a unique linear map $\Omega_{R/K} \to M$: since M is complete, this factors uniquely through $\widehat{\Omega}_{R/K}$. The rest of the argument is routine.

For part (b), it suffices to see that a K-derivation D of R into a complete module M is uniquely determined by the images of the dx_i, and that there is a derivation for every specified set of values. If values $u_1, \ldots, u_n \in M$ are specified one simply checks that the map taking $F \in K[[x_1, \ldots, x_n]]$ to $\sum_{i=1}^n \frac{\partial F}{\partial x_i} u_i$ is a derivation. To see that the derivation is determined by its values on the x_i, fix $N \in \mathbb{N}$. Given F, let f be the polynomial containing all terms of F of degree $\leq 2N$, and let $w \in P^{2N}$ be the sum of remaining terms of F. The definition of a derivation forces

$$dF = \sum_{i=1}^n \frac{\partial f}{\partial x_i} u_i$$

and since $w = F - f \in P^{2N} = (P^N)^2$, the product rule forces Dw to be in $P^N M$. Thus,

$$DF - \sum_i \frac{\partial F}{\partial x_i} u_i \in P^N M$$

for all N, and the result follows.

To prove part (c), we note that a K-derivation $R = K[[x_1, \ldots, x_n]]/(F_1, \ldots, F_m) \to M$ induces a K-derivation $K[[x_1, \ldots, x_n]] \twoheadrightarrow K[[x_1, \ldots, x_n]]/(F_1, \ldots, F_m) \to M$ by composition. The condition that a K-derivation $K[[x_1, \ldots, x_n]] \to M$ factor through $K[[x_1, \ldots, x_n]]/(F_1, \ldots, F_m)$ is simply that every dF_j be mapped to 0, and so the cokernel over R of $\left(\dfrac{\partial F_j}{\partial x_i}\right)$ has the required mapping property. $\square$

Proposition. *Let (R, P, K) be complete with coefficient field $K \subseteq R$.*

(a) *If K has characteristic 0, then R is regular if and only if $\widehat{\Omega}_{R/K}$ is free, in which case it is free of rank $\dim(R)$.*

(b) *If K has characteristic $p > 0$, then R is regular if and only of $\widehat{\Omega}_{R/K}$ is free of rank $\leq \dim(R)$, in which case it is free of rank $\dim(R)$. If K is perfect, R is reduced, and $\widehat{\Omega}_{R/K}$ is free, then R is regular.*

Proof. We can represent R as a quotient $K[[x_1, \ldots, x_n]]/(F_1, \ldots, F_m)$ in such a way that $F_1, \ldots, F_m$ are minimal generators of I and all $F_j \in (x_1, \ldots, x_n)^2$: if any F_j has a nonzero linear form, $K[[x_1, \ldots, x_n]]/(F_j)$ is regular and can be written as power series ring in fewer variables. Then $\widehat{\Omega}_{R/K}$ is the cokernel of the image of $\left(\frac{\partial F_j}{\partial x_i}\right)$, which has entries in P, and so the cokernel is free if and only if all of the partial derivatives are in the ideal. In characteristic 0 this cannot happen unless all the F_j are 0, by the Lemma that follows. In characteristic p, again by the Lemma that follows, one has that every variable occurs in every term of every F_j with exponent that is a multiple of p. Therefore, all the F_j are pth powers if K is perfect. In this case, the module of differentials is free of rank n, but if some F_j is nonzero then $\dim(R) < n$. If K is perfect the fact that R is reduced and F_j is a pth power contradicts the assumption that F_j is a minimal generator of m. $\square$

Lecture of February 17, 2010

Lemma. *Let K be a field and let $T = K[[x_1, \ldots, x_n]]$ be a formal power series ring over K. Let $I = (f_1, \ldots, f_m)$ be an ideal, and suppose that for all i, j, $\dfrac{\partial f_j}{\partial x_i} \in I$.*

(a) *If K has characteristic 0, then $I = 0$ or $I = T$.*

(b) *If K has characteristic $p > 0$, then I is generated by elements of $K[[x_1^p, \ldots, x_n^p]]$. If K is perfect, these elements are pth powers.*

Proof. First note that if all the partial derivatives of all of a given set of generators of I are in I, then I is closed under partial differentiation:

$$\frac{\partial}{\partial x_i}\sum_j g_j f_j = \sum_j \left(\frac{\partial g_j}{\partial x_i} f_j + g_j \frac{\partial f_j}{\partial x_i}\right),$$

and all terms are in I.

In the characteristic 0 case, if I is not (0), choose an element h of I whose lowest degree term H is of smallest degree. If $I \neq R$, then H has positive degree. Choose a variable x_i that occurs in H. Then $\dfrac{\partial H}{\partial x_i} \neq 0$ and is the lowest degree term of $\dfrac{\partial h}{\partial x_i}$, a contradiction.

In the case of characteristic $p > 0$, note that the set $\mathcal{M}$ of monomials $\mu = x_1^{a_1} \cdots x_n^{a_n}$ such that all of the $a_t < p$ form a free basis for T over $T_0 = K[[x_1^p, \ldots, x_n^p]]$. Also note that all of the derivations $\dfrac{\partial}{\partial x_i} : T \to T$ are T_0-linear. Suppose that I has an element $\sum_{\mu \in \mathcal{M}} g_\mu \mu$ where the $g_\mu \in T_0$. We want to show that all of the $g_\mu \in I$. Evidently, if we have a counterexample, we still have a counterexample if we omit all terms such that $g_\mu \in I$. Therefore we may assume that $g_\mu \notin I$ for all μ that occur, i.e., such that $g_\mu \neq 0$. Choose $\mu^* = x_1^{a_1} \cdots x_n^{a_n}$ occurring of highest degree. Then apply

$$D = \frac{\partial^{a_1}}{\partial x_1^{a_1}} \cdots \frac{\partial^{a_n}}{\partial x_n^{a_n}}.$$

The value on μ^* is $a_1! \cdots a_n!$. All other μ occurring are killed by D, since some exponent in μ will be strictly less than the corresponding exponent a_i in μ^*, and D is T_0-linear. Thus, $a_1! \cdots a_n! g_{\mu^*} \in I$, and it follows that $g_{\mu^*} \in I$, a contradiction. $\square$

Corollary. *Let S be finitely presented and R-flat. If R contains the rational numbers, S is smooth over R iff $\Omega_{S/R}$ is a locally free S-module. More generally, S is smooth over R if and only if for every maximal ideal Q of S lying over P in R, $(\Omega_{S/R})_Q$ is free of rank less than or equal to the dimension of the localized fiber S_Q/PS_Q, in which case its rank is that dimension.*

Proof. We have already proved the necessity of these conditions. To see sufficiency, note that it suffices to show that the localized fibers at maximal ideals are formally smooth. Thus, we may assume that R is a field K. We may make a base change to the algebraic closure of K without affecting the issue. Therefore, we may assume that S_Q has residue field K, and K is a coefficient field. The regularity of S_Q and the freeness and rank of Ω are unaffected by completion if we use $\widehat{\Omega}_{R/K}$ in the complete case. The result is now immediate from the preceding Proposition. $\square$

Remark. When S is finitely presented and flat over R, it is smooth if and only if for every maximal ideal Q of S with contraction P to R, S_Q/PS_Q is formally smooth over $K = R_P/PR_P$. Therefore, suppose that we restrict attention to the case where $R = K$ is a field. We may make a base change to the case where K is algebraically closed without affecting smoothness. Suppose that K is a perfect field of positive characteristic. Then S_Q is formally smooth over K if and only if $(\Omega_{S/K})_Q$ is S_Q-free and S_Q is reduced. However, the proof needs one fact that we have not established: if a local ring of a finitely generated K-algebra is reduced, then so is its completion.

We return to the subject of Henselization.

Proposition. *If I is a proper ideal of a quasilocal ring R, then there is a canonical local R-isomorphism $(R/I)^{\mathrm{h}} \cong R^h/IR^h$ (since both are killed by I, this is equivalent to saying that there is a canonical local (R/I)-isomorphism).*

Proof. A homomorphic image of a Henselian ring is Henselian: given the problem of lifting a factorization over the residue class field K, one can lift to R, and then take the image of that lifting in the quotient. Thus, $R^{\mathrm{h}}/IR^{\mathrm{h}}$ is Henselian, and so $R/I \to R^{\mathrm{h}}/IR^{\mathrm{h}}$ induces a

unique (R/I)-algebra map $(R/I)^{\rm h} \to R^{\rm h}/IR^{\rm h}$. Likewise, the map $R \to (R/I)^{\rm h}$ induces a unique local R-algebra map $R^{\rm h} \to (R/I)^{\rm h}$, and, since it kills I, we get a unique local (R/I)-algebra map $R^{\rm h}/IR^{\rm h} \to (R/I)^{\rm h}$. The composite map $(R/I)^{\rm h} \to (R/I)^h$ is the identity on elements of R/I and so is the identity. Consider the composite map $\alpha : R^{\rm h}/IR^{\rm h} \to R^{\rm h}/IR^{\rm h}$ and compose with the surjection $R^{\rm h} \to R^{\rm h}/IR^{\rm h}$: the resulting map $\beta : R^{\rm h} \to R^{\rm h}/IR^{\rm h}$ takes the image of $r \in R$ to its image in R^h/IR^h, and since β extends uniquely to $R^{\rm h}$, it must be the quotient surjection. This means that α must be the identity map. $\square$

Theorem. *Let (R, P, K) be a Noetherian local ring. Then there are unique local maps $R \to R^{\rm h} \to \widehat{R}$ and these are injective. If S is any pointed étale extension of R this also factors uniquely $R \to S \to R^{\rm h} \to \widehat{R}$ and if we tensor with R/P^n these maps all become isomorphisms:*

$$R/P^nR \cong S/P^nS \cong R^{\rm h}/P^nR^{\rm h} \cong \widehat{R}/P^n\widehat{R}.$$

$R^{\rm h}$ may be canonically identified with a subring of $\widehat{R}$ and is Noetherian. Moreover, the induced maps $\widehat{R} \to \widehat{S} \to \widehat{R^{\rm h}} \to \widehat{R}$ are all isomorphisms, i.e.,

$$\widehat{R} \cong \widehat{S} \cong \widehat{R^{\rm h}} \cong \widehat{R}.$$

Proof. By Hensel's lemma, $\widehat{R}$ is Henselian, and this gives a unique local R-algebra factorization $R \to R^{\rm h} \to \widehat{R}$. Moreover, S is part of the direct limit system used to obtain $R^{\rm h}$. Once we kill P^n we have that R/P^n is complete, and therefore Henselian. S/P^nS is a pointed étale extension of R/P^n and therefore equal to it, while, $R^{\rm h}/P^nR^{\rm h}$ is the Henselization of R/P^n and so equal to R/P^n as well. This shows that for each pointed étale extension S of R, $\widehat{S} \to \widehat{R}$ is an isomorphism. If $u \in R^{\rm h}$ mapped to 0 in $\widehat{R}$ we can choose $u \in S$ for some S, and now we have a contradiction since $\widehat{S} \to \widehat{R}$ is an isomorphism. Thus, $R^{\rm h}$ injects into $\widehat{R}$.

Suppose that $I \subseteq R^{\rm h}$ is not finitely generated. Then we can find a sequence of finitely generated subideals $\{I_t\}_t$ that is strictly ascending. The expansions to $\widehat{R}$ must stabilize. Suppose that s is so large that $I_t\widehat{R} = I_s\widehat{R}$ for all $t \geq s$, and that $f_1, \ldots, f_n \in R^{\rm h}$ generate $I_s\widehat{R}$. We claim that these elements generate I_t for all $t \geq s$. To see this choose $g \in I_t$. Choose a pointed étale extension S of R sufficiently large that it contains all of $f_1, \ldots, f_h$ and g. But after completion the isomorphisms $S/P^nS \to \widehat{R}/P^n\widehat{R}$ show that $\widehat{S} \cong \widehat{R}$, and this implies that $\widehat{R}$ is faithfully flat over S. Since $g \in (f_1, \ldots, f_h)\widehat{R}$, we must have $g \in (f_1, \ldots, f_h)S \subseteq (f_1, \ldots, f_h)R^{\rm h}$. The final statement is clear from the isomorphisms mod every P^n. $\square$

Lecture of February 19, 2010

If R is Noetherian local, one may take a representative of every isomorphism class of pointed étale extensions inside $\widehat{R}$, and the directed union of these is a canonical Henselization of R. If (R, P, K) is any quasilocal ring, for each subalgebra B of R finitely generated over the prime ring in R, we may form $B_{P\cap B}$, which has a local map $B_{P\cap B} \to R$. Then

$$R = \varinjlim_B B_{P\cap B}$$

and

$$R^{\rm h} = \varinjlim_B \left(B_{P\cap B}\right)^{\rm h}$$

gives a canonical Henselization of B.

The ring of germs of real-valued C^∞ functions or real analytic functions at a point of $\mathbb{R}^d$ or of germs of complex analytic functions at a point of $\mathbb{C}^d$ is Henselian. The germs of real analytic functions may be identified with the subring of $\mathbb{R}[[x_1, \ldots, x_d]]$ consisting of power series that converge on some neighborhood of the origin, and a similar comment applies to complex analytic functions. The Henselian property follows because there is an implicit function theorem that applies in each case. Shift coordinates so that the point is at the origin. The map from the local ring to the residue class field consists of evaluation of a representative of the germ at the origin. Given n polynomial equations in n unknowns whose coefficients are germs, each germ may be represented by an actual function on some open neighborhood of the origin. We may restrict to the intersection of these open neighborhoods. We can now work with polynomials whose coefficients are functions. The hypothesis on the Jacobian determinant enables one to apply an implicit function theorem for the appropriate category to get functions that satisfy the equations.

One version of an implicit function theorem is this: let X, Y denote the $n+d$ variables $X_1, \ldots, X_n, Y_1, \ldots, Y_d$ and let $F_1, \ldots, F_n$ be n $\mathbb{R}$-valued C^∞ functions defined on a neighborhood of a point $(x, y) \in \mathbb{R}^{n+d}$ that vanish at that point. Suppose that $\det\left(\dfrac{\partial F_j}{\partial X_i}\right)$ (note that the matrix is $n \times n$) does not vanish at (x, y). Then there are unique C^∞ functions $g_1(Y), \ldots, g_n(Y)$ defined on a neighborhood U of y such that

$$x_j = g_j(y),\ 1 \leq j \leq n, \text{ and } F_j(g_1(Y), \ldots, g_n(Y), Y_1, \ldots, Y_d) = 0$$

identically on U, $1 \leq j \leq m$. Thus, the equations determine a unique solution for the X_i in terms of the Y_k near the point (x, y). The condition in the hypothesis is very natural if one thinks of the case where all the F_j are linear. The same statement holds if one replaces the condition that functions in both the hypothesis and conclusion be C^∞ by the condition that they be real analytic, and also if one works with $\mathbb{C}$-valued functions on $\mathbb{C}^{n+d}$ and replaces the C^∞ condition by the condition that the functions in both the hypothesis and conclusion be holomorphic.

We next want to review some material concerning excellent rings. We shall not give proofs, but we will not be making use of the theorems we do not prove. A Noetherian ring is called *catenary* if whenever $P \subseteq Q$ are prime ideals all saturated chains of primes from P to Q have the same length. This property obviously passes to quotient rings and localizations. A Noetherian ring is called *universally catenary* if every finitely generated algebra over it is catenary. It suffices that polynomial rings in finitely many variables over it be catenary: other finitely generated algebras over it are quotients of these. The Appendices to Nagata's book on local rings contain examples of Noetherian rings that are not catenary, and catenary rings that are not universally catenary. However, Cohen-Macaulay rings are catenary. Since a polynomial ring over a Cohen-Macaulay ring is again

Cohen-Macaulay, we have that Cohen-Macaulay rings are universally catenary, and that means that homomorphic images of Cohen-Macaulay rings are universally catenary.

A map of rings is said to be a $\mathcal{P}$ map, where $\mathcal{P}$ is a property of rings, if it is flat and all the fibers have property $\mathcal{P}$. Thus, a map is Cohen-Macaulay if it is flat with Cohen-Macaulay fibers, and a map is geometrically regular if it is flat with geometrically regular fibers. With this terminology, $R \to S$ is smooth if and only if it is finitely presented and geometrically regular. However, some authors use the term "regular" to mean geometrically regular. In this course we shall use the term geometrically regular, and avoid the term "regular."

A Noetherian ring R is called a *G-ring* ("G" as in "Grothendieck") if for every local ring A of R, the map $A \to \widehat{A}$ is geometrically regular.

An *excellent* ring is a universally catenary Noetherian G-ring R such that in every finitely generated R-algebra S, the regular locus $\{P \in \mathrm{Spec}\,(S) : S_P \text{ is regular}\}$ is Zariski open. Excellent rings include the integers, fields, complete local rings, convergent power series rings, and are closed under taking quotients, localization, and formation of finitely generated algebras. All of the rings that come up in algebraic geometry, number theory, and several complex variables are excellent. Excellent rings tend very strongly to share the good behavior exhibited by rings that are finitely generated over a field. The normalization of an excellent domain is a finite module over it, the completion of a reduced excellent local ring is reduced, and the completion of a normal excellent local domain is normal. It is also true that the Henselization of an excellent local ring is again excellent.

In the sequel we shall refer from time to time to excellent discrete valuation rings. We always mean Noetherian rank one discrete valuation domains. We use the abbreviation DVR. In this case one can give a simpler characterization of excellence, and we shall take this characterization as our working definition of excellence for DVRs throughout the remainder of these Lecture Notes.

We first define an algebra S over a field K to be *separable* if for every finite purely separable algebraic extension L of K, the ring $L \otimes_K S$ is reduced. We shall say a bit more about this shortly. Notice that if K has characteristic 0, then every reduced K-algebra is separable. We shall say a DVR V with fraction field K is excellent if $K \otimes_V \widehat{V}$ is separable. This is equivalent to the general definition of excellence given earlier in the special case of a DVR. Notice that every DVR of equal characteristic 0 or of mixed characteristic is excellent. There can be no problem unless the ring has positive characteristic p.

We define a Noetherian ring (R, P, K) to be an *approximation ring* if every finite system of polynomial equations in finitely many variables over R that has a solution in $\widehat{R}$ has a solution in R. The reason for the use of the term "approximation" is explained in part by the following fact.

Proposition. *Let R be an approximation ring, let $F_j(X_1, \ldots, X_n) = 0$, $1 \leq j \leq m$ be a system of polynomial equations over R, and let $(s_1, \ldots, s_n)$ be a solution of the equations in $\widehat{R}^n$. Then for every positive integer N there exists a solution $(r_1, \ldots, r_n)$ in R^n such that for all i, $r_i \cong s_i$ mod $P^N \widehat{R}$. In other words, the solutions of the equations over R are P-adically dense in the solutions over $\widehat{R}$.*

Proof. Fix N and fix elements $r_i' \in R$ such that $r_i' \cong s_i \bmod P^N\widehat{R}$, $1 \leq i \leq n$. Fix generators $u_1, \ldots, u_k$ for P^n in R. For each i we can find elements $y_{ij} \in \widehat{R}$ such that $s_i - r_i' - \sum_{j=1}^k y_{ij}u_j = 0$. Now consider the equations $F_1 = 0, \ldots, F_m = 0$ together with the additional equations involving new variables Y_{ij}, namely $X_i - r_i' - \sum_{j=1}^k Y_{ij}u_j = 0$. These equations have a solution $(s_1, \ldots, s_n, y_{ij})$ in $\widehat{R}$. Hence, they have a solution in R, and for this solution the values for the X_i will satisfy the congruence condition. $\square$

Thus, solutions over $\widehat{R}$ can be "approximated" arbitrarily closely, in the P-adic topology, by solutions over R.

Based on a wonderful result of Popescu, one can prove that every excellent Henselian ring is an approximation ring. The original proof of the result of Popescu has gaps. Popescu's theorem asserts that if S is a geometrically regular R-algebra, and one has a finitely generated R-subalgebra S_0 of S, then there is a smooth R-algebra T and a factorization $R \to S_0 \to T \to S$. (It is not known that the map $T \to S$ can be taken to be injective.) This means that S is a sort of limit of smooth algebras. A proof by Ogoma filled some of the gaps in Popescu's argument, while Swan eventually wrote an exposition of the proof that definitively answered all questions about the earlier versions. The proof is very long and difficult, and we shall not prove the full result here.

We will however, prove the following beautiful result of Mike Artin, which motivated the later work.

Theorem (Artin approximation). *Let R be a local ring of a finitely generated algebra over a field or over an excellent DVR. Then $R^{\rm h}$ is an approximation ring. In particular, every finite system of polynomial equations over R that has a solution in $\widehat{R}$ has a solution in a pointed étale extension of R.*

This is a hard theorem: it will take us a while before we can prove it.

Artin also proved that the ring of convergent power series over $\mathbb{C}$ is an approximation ring. This is an amazing statement: it says that if a system of polynomial equations with convergent power series coefficients has a solution in the formal power series ring, then it has a solution in the convergent power series ring.

Both of these results of Artin are special cases of the statement that every excellent Henselian ring is an approximation ring.

Lecture of February 22, 2010

We discuss separable algebras a bit further. Recall that a K-algebra R is *separable* if for every finite purely inseparable extension L of K, $L \otimes_K R$ is reduced.

Lemma. *Let K be a field and let R be a K-algebra. Let L denote an extension field of K.*
(a) *If K has characteristic 0, the R is separable if and only if it is reduced.*
(b) *If $L \otimes_K R$ is reduced, then for every subfield L_0 of L containing K, $L_0 \otimes_K R$ is reduced.*
(c) *If R is separable over K then every K-subalgebra of R is separable over K.*

(d) *A direct limit of separable K-algebras is separable.*
(e) *R is separable over K if and only if all of its finitely generated K-subalgebras are separable over K.*
(f) *If R is reduced and L is separable algebraic over K, then $L \otimes_K R$ is reduced.*
(g) *If R is reduced and L is pure transcendental over K, then $L \otimes_K R$ is reduced.*

Proof. Part (a) is immediate from the definition, since the only purely inseparable extension of K is K itself. Part (b) holds because $L_0 \otimes_K R \subseteq L \otimes_K R$, since R is K-flat. For the same reason, if R_0 is a K-subalgebra of R we have that $L \otimes_K R_0 \subseteq L \otimes_K R$, from which (c) follows. Part (d) is a consequence of the fact that tensor product commutes with direct limit, since a direct limit of reduced rings is reduced. Part (e) is immediate from (c) and (d). To prove (f), note that since L is a direct limit of finite separable algebraic extensions, we may assume that L is finite separable algebraic over K. Since R is a direct limit of finitely generated K-subalgebras, we may assume that R is reduced and finitely generated over K. Then R embeds in its localization $W^{-1}R$ at the multiplicative system of all nonzerodivisors, and because R is Noetherian and reduced, this is a finite product of fields. Thus, it suffices to prove the result when L is finite separable algebraic over K and R is a field. But then L is étale over K and so $L \otimes_K R$ is étale over R, and, consequently, a finite product of separable field extensions of R. Thus, it is reduced. Part (g) is clear because the pure transcendental extension is a localization of a polynomial ring over R. □

Proposition. *Let K be a field and let R be a K-algebra. The following conditions are equivalent:*
(1) *R is separable over K.*
(2) *If L is the perfect closure of K, then $L \otimes_K R$ is reduced.*
(3) *If L is the algebraic closure of K, then $L \otimes_K R$ is reduced*
(4) *For every field extension L of K, $L \otimes_K R$ is reduced.*
(5) *For some perfect field L containing K, $L \otimes_K R$ is reduced.*

Proof. (1) and (2) are equivalent because the perfect closure of K is a directed union of finite purely inseparable extensions of K, and contains all of them. Clearly, (4) $\Rightarrow$ (3) $\Rightarrow$ (5) $\Rightarrow$ (2) (since the algebraic closure is perfect and since every perfect field containing K contains a K-isomorphic copy of the perfect closure), and so it will suffice to prove that (2) $\Rightarrow$ (4). Since every field is contained in a larger field that contains the perfect closure L of K, it suffices to show that $L' \otimes_K R$ is reduced when L' is a field containing L. L' is the directed union of finitely generated extensions L'_0 of L within L'. Therefore, we may assume that L' is finitely generated over the perfect field L. But then L' has a separating transcendence basis over L, and may be reached by a pure transcendental extension followed by a separable algebraic extension. The result now follows from parts (f) and (g) of the Lemma. □

We also note:

Proposition. *If L is an algebraic field extension of K, then L is separable as a K-algebra if and only if it is a separable field extension of K.*

Proof. If L' is any field extension of K, then $L' \otimes_K L$ is reduced by part (f) of the Lemma. Now suppose that L is not a separable field extension of K. Then L contains an inseparable

element θ whose minimal monic polynomial $f = f(x)$ has multiple roots. Let $\overline{K}$ denote an algebraic closure of K. Then $\overline{K} \otimes_K L \supseteq \overline{K} \otimes_K K[\theta] \cong \overline{K} \otimes_K K[x]/(f) \cong \overline{K}[x]/(f)$, and since f is not square-free over $\overline{K}$, the last ring has nilpotents. $\square$

Let k be any perfect field of positive characteristic p, and let $t_1, \ldots, t_n, \ldots$ be countably many indeterminates over K. Let $K_0 = K(t_i^p : i)$, and let $K_n = K_0(t_1, \ldots, t_n)$, so that $K_0 \subseteq K_1 \subseteq \cdots$ is a strictly increasing sequence of fields. Let K denote the union. Let $V = \bigcup_{n=0}^{\infty} K_n[[x]]$. Every $K_n[[x]]$ is complete and, therefore, Henselian, and a direct limit of Henselian rings is Henselian. Therefore, V is Henselian. Every nonzero element of V is a unit times a power of x, since that is true in every V_n. It follows that V is a discrete valuation ring in which x generates the maximal ideal. $V/x^N \cong K[[x]]/(x^N)$, and it follows that $\widehat{V}$ may be identified with $K[[x]]$. But $K[[x]]^p = K^p[[x^p]] = K_0[[x^p]] \subseteq K_0[[x]] \subseteq V$, so that $\widehat{V}$ is purely inseparable over V, and this remains so when we localize at $V - \{0\}$ (equivalently, at x). Note that, for example, $u = \sum_{n=1}^{\infty} t_n x^n \in \widehat{V} - V$. Thus, V is a DVR that is not excellent.

Also note that Artin approximation fails for V. The equation $z^p - u^p = 0$ (note that $u^p \in V$) has the unique solution $z = u$ in the domain $\widehat{V}$, but it has no solution in V: the only possibility is $z = u$, and $u \notin V$.

It is also worth noting that approximation rings must be Henselian. Given an approximation ring (R, P, K) and a factorization of a monic polynomial over R into relatively prime factors in $K[x]$, the problem of lifting the factorization may be translated into solving a system of equations for the coefficients. It will have a solution in R, since that ring is complete, and therefore Henselian. Hence, it must have a solution in R as well.

Here is an alternative characterization of approximation rings:

Proposition. *Let R be a local ring. Then R is an approximation ring if and only if it is an R-algebra retract of every finitely generated R-subalgebra S of $\widehat{R}$, i.e., if and only if for every such S there is an R-algebra homomorphism $\rho : S \to R$ such that if $\iota : R \hookrightarrow S$ is the inclusion map, $\rho \circ \iota = \mathbf{1}_R$.*

Proof. Suppose that R is an approximation ring and let $S = R[s_1, \ldots, s_n]$ be given. Map a polynomial ring $R[X_1, \ldots, X_n] \twoheadrightarrow R[s_1, \ldots, s_n]$ as R-algebras by sending $X_j \mapsto s_j$, $1 \leq j \leq n$, and let $F_1, \ldots, F_m$ generate the kernel. Then $(s_1, \ldots, s_n)$ is a solution for the m equations $F_j = 0$ in R. Therefore the equations have a solution $(r_1, \ldots, r_n)$ in R. The R-algebra map $R[X_1, \ldots, X_n] \to R$ sending $X_j \mapsto r_j$ kills the F_j and so induces the required retraction $S \cong K[x_1, \ldots, x_n]/(F_1, \ldots, F_m)$ to R.

To prove the "if" part let $F_j = 0$, $1 \leq j \leq m$ be a system of polynomial equations over R with a solution $(s_1, \ldots, s_n)$ in $\widehat{R}$, and let $S = R[s_1, \ldots, s_n]$. Choose an algebra retraction ρ of S to R. Let $r_i = \rho(s_i)$, $1 \leq i \leq n$. Since the s_i satisfy the equations $F_j = 0$ and ρ is an R-algebra homomorphism, the r_i also give a solution. $\square$

We next want to use Zariski's Main Theorem and our theory of Henselization and étale maps to compare a very geometric notion of intersection multiplicity that we shall introduce with Serre's definition using alternating sums of lengths of Tor.

The first step is to introduce the geometric notion. To this end, we consider two algebraic varieties X, Y in $A^n_{\mathbb{C}} = \mathbb{C}^n$. That is, X and Y are irreducible closed algebraic sets. We deal only with closed points here. Suppose that u is an isolated point of intersection of $X \cap Y$. In the situation where $\dim(X) + \dim(Y) = n$ (X and Y are said to be intersecting *properly* at u, we want to introduce a positive integer that represents the intersection multiplicity of X and Y at u.

Here is one example. Suppose that $n = 2$ with coordinates x, y in $\mathbb{A}^2_{\mathbb{C}}$ and that $X = V(y - x^2)$ while $Y = V(y)$. The origin $(0, 0)$ is an isolated point of intersection of these two varieties. However if we replace the line $y = 0$ with the line $y = \epsilon$ for any small $\epsilon \neq 0$, $X = V(y - x^2)$ and $Y_\epsilon = V(y - \epsilon)$ have two points of intersection: $\epsilon \neq 0$ has two distinct square roots, and the points are $(\pm\sqrt{\epsilon}, \epsilon)$. It is therefore natural to define the intersection multiplicity to be 2 in this case.

If X and Y are arbitrary varieties one can simplify the problem of understanding the intersection by the process of "reduction to the diagonal." Let Δ denote the diagonal subvariety of $\mathbb{A}^n_{\mathbb{C}} \times \mathbb{A}^n_{\mathbb{C}} \cong \mathbb{A}^{2n}_{\mathbb{C}}$: $\Delta = \{(v, v) : v \in \mathbb{A}^n_{\mathbb{C}}\}$. This variety is a vector subspace defined by n linear equations. Set-theoretically there is a bijection between $X \cap Y$ and $(X \times Y) \cap \Delta$ under which u corresponds to (u, u). This bijection is an isomorphism of algebraic sets. Moreover, a great deal of experience has shown that one can replace the problem of understanding the manner in which X meets Y by the problem of understanding the manner in which $X \times Y$ meets Δ. For example, u is an isolated point of intersection of X and Y iff (u, u) is an isolated point of intersection of $X \times Y$ and Δ. Moreover, X and Y meet properly in $\mathbb{A}^n_{\mathbb{C}}$ iff $X \times Y$ and Δ meet properly in $\mathbb{A}^{2n}_{\mathbb{C}}$: the dimension of $X \times Y$ is $\dim(X) + \dim(Y)$.

We shall therefore focus attention on the problem of defining intersection multiplicities when one is intersecting a variety with a linear space. Note that if the linear space is defined by independent linear equations $L_1, \ldots, L_d$ then one can imitate the example with the parabola by counting points of intersection with $V(L_1 - \epsilon_1, \ldots, L_d - \epsilon_d)$, where the ϵ_j are small, varying complex numbers. Here, one hopes that the number of points of intersection that are "near" the isolated point u will be constant for "almost all" choices of $(\epsilon_1, \ldots, \epsilon_d)$ consisting of "sufficiently small" complex values. In the case of the parabola we only had to exclude the value 0 for ϵ. Our next task is to make all of this precise.

Lecture of February 24, 2010

Given a finitely generated $\mathbb{C}$-algebra R, if the module differentials $\Omega_{R/\mathbb{C}}$ is locally free over R then R is regular (which is equivalent to being smooth over $\mathbb{C}$). What if one assumes instead that the R-module of derivations $\mathrm{Der}_{\mathbb{C}}(R, R)$ is locally free? Must R be regular? Note that $\mathrm{Der}_{\mathbb{C}}(R, R) \cong \mathrm{Hom}_R(\Omega_{R/\mathbb{C}}, R)$. This has been conjectured to be true and is known as the Zariski-Lipman conjecture.

It is known that if the module of derivations is locally free then R must be normal (see [J. Lipman, *Free derivation modules on algebraic varieties*, Amer. J. Math. **87** (1965) 874–898]) and it is known that the conjecture is correct if R is a hypersurface (a regular

domain modulo one nonzero element) (see [G. Scheja and U. Storch, *Über differentielle Abhängigkeit bei idealen analytischer Algebren*, Math. Z. **114** (1970) 101–112] and [____, *Differentielle Eigenschaften des Lokaliserungen analytischer Algebren*, Math. Ann. **197** (1972) 137–170]), or if R is graded [M. Hochster, *The Zariski-Lipman conjecture in the graded case*, J. of Alg. **47** (1977) 411–424]. By a result of Flenner [H. Flenner, *Extendability of differential forms on nonisolated singularities*, Invent. Math. **94** (1988) 317–326], if the theorem is true in dimension two then it is true. It remains open in dimension two, even if the ring is a complete intersection in a polynomial ring in four variables.

We return to the problem of defining the intersection multiplicity of a variety X and a linear space Y in $\mathbb{A}^n_{\mathbb{C}}$. Let $\dim(X) = d$. We assume that the intersection is proper, so that $\dim(Y) = n - d$, and we make a change of coordinates so that the point of intersection that we are studying is the origin, which we assume is an isolated point of intersection. Then Y can be defined by the vanishing of d homogeneous linear equations L_j, and we write $Y = V(L_1, \ldots, L_d)$. For each d-tuple of complex numbers $\underline{\epsilon} = (\epsilon_1, \ldots, \epsilon_d)$ we let $Y_{\underline{\epsilon}} = V(L_1 - \epsilon_1, \ldots, L_d - \epsilon_d)$. By the Euclidean topology on $\mathbb{A}^N_{\mathbb{C}}$ we mean the usual metric space topology, which is Hausdorff and locally compact. There is a Euclidean topology on any closed algebraic set, inherited from a copy of $\mathbb{A}^N_{\mathbb{C}}$ in which it is embedded. The topology is independent of the embedding, since isomorphisms of closed algebraic sets are given, in both directions, by polynomial maps in the coordinates, and these will be continuous in the respective Euclidean topologies and therefore provide a homeomorphism.

We next switch points of view. The functions $L_1, \ldots, L_d$, restricted to X, give d elements of the coordinate ring $\mathbb{C}[X]$. Let $(R, P, \mathbb{C})$ be the local ring of $\mathbb{C}[X]$ at the point we are interested in. The assertion that this point is an isolated point of the intersection means precisely that $L_1, \ldots, L_d$ is a system of parameters in R: the contraction of P to $\mathbb{C}[X]$ is a minimal prime of $(L_1, \ldots, L_d)\mathbb{C}[X]$, because the point in question is an irreducible component of the intersection. Moreover, $\dim(R) = \dim(\mathbb{C}[X]) = d$. Consider the map $\Gamma : X \to \mathbb{A}^d_{\mathbb{C}}$ given in coordinates by $(L_1, \ldots, L_d)$. This is the same as the map of algebraic sets induced by the $\mathbb{C}$-algebra inclusion $\mathbb{C}[L_1, \ldots, L_d] \subseteq \mathbb{C}[X]$. Then $X \cap Y_{\underline{\epsilon}}$ is precisely the same as $\Gamma^{-1}(\underline{\epsilon})$. The fact that we want can now be phrased as follows:

Theorem. *Let $\Gamma : X \to \mathbb{A}^d_{\mathbb{C}}$ as described and let x be the point of X that we are studying, so that Γ maps x to the origin $\mathbf{0}$ in $\mathbb{A}^d_{\mathbb{C}}$. Then there are Euclidean neighborhoods B' of x and B of $\mathbf{0}$ in $\mathbb{A}^d_C$ and a proper Zariski closed subset Z of $\mathbb{A}^d_C$ such that for all $\underline{\epsilon} \in B - Z$, the cardinality of $\Gamma^{-1}(\underline{\epsilon}) \cap B'$ is a constant μ, and all points in $\Gamma^{-1}(\underline{\epsilon}) \cap B'$ approach x as $\underline{\epsilon}$ approaches $\mathbf{0}$. Moreover μ is the torsion-free rank of $\widehat{R}$ as a module over $\mathbb{C}[[L_1, \ldots, L_d]]$.*

It will take us a while to prove this result. Once we have this theorem, we can define the intersection multiplicity of X and Y at x as the value of μ. When Y is not necessarily linear we replace X and Y by $X \times Y$ and Δ.

Let us define the distance between two monic polynomials of degree m as the supremum of the absolute values of differences of corresponding coefficients. By the root set $\mathcal{S}(f)$ of a monic polynomial f, we mean a sequence that gives the roots $\theta_1, \ldots, \theta_m$ of the polynomial, each occurring a number of times equal to its multiplicity, but we consider these sequences only up to equivalence: if π is a permutation of $\{1, \ldots, m\}$ then we regard $\theta_1, \ldots, \theta_m$ as

the same root set as $\theta_{\pi(1)}, \ldots, \theta_{\pi(m)}$. If $\mathcal{S}(f)$ is represented by the sequence $\theta_1, \ldots, \theta_m$ and $\mathcal{S}(g)$ is represented by $\theta'_1, \ldots, \theta'_m$, then we define the distance between the root sets as

$$\min_{\pi \in S_m} \sup_{1 \leq t \leq m} \{|\theta_t - \theta'_{\pi(t)}|\}.$$

Thus, two root sets are close if and only if for some choice of orderings of their terms, the corresponding terms are all close.

Lemma. *Let $f \in \mathbb{C}[z]$ be a monic polynomial of degree $m \geq 1$. Then for all $\epsilon > 0$ there exists $\delta > 0$ such that if g is within distance δ of f then $\mathcal{S}(g)$ is within distance ϵ of $\mathcal{S}(f)$: that is, the root set of f is a continuous function of the coefficients of f as f varies in the set of monic polynomials of degree m. Yet another formulation is that if g_t is a sequence of monic polynomials of degree m that converges to f, then the root sets $\mathcal{S}(g_t)$ converge to $\mathcal{S}(f)$.*

Proof. This is obvious if $m = 1$. We assume that $m > 1$ and use induction. It will suffice to prove the final statement. Choose a root θ of f. Replace f by $f(z + \theta)$ and g_t by $g_t(z + \theta)$. We still have that $g_t(z + \theta) \to f(z + \theta)$, and all root sets have been translated by $-\theta$, so that the distance from the root set of $g_t(z + \theta)$ to the root set of $f(z + \theta)$ is the same as the distance from the root set of g_t to the root set of f. Therefore, we may assume without loss of generality that 0 is a root of f, i.e., that its constant term is 0. Let c_t be the constant term of g_t. By hypothesis $c_t \to 0$ and so $|c_t| \to 0$. It follows as well that $|c_t|^{1/m} \to 0$. Since the product of the absolute values of the roots of g_t is $|c_t|$, we know that g_t has at least one root θ_t with $|\theta_t| \leq |c_t|^{1/m}$. Then $\theta_t \to 0$, from which it follows $h_t = g_t(z + \theta_t) \to f$. Each h_t has 0 as a root, and so $h_t = zh_t^*$ and $f = zf^*$. But then $h_t^* \to f^*$, and $\mathcal{S}(h_t^*) \to \mathcal{S}(f^*)$ by the induction hypothesis. It follows that $\mathcal{S}(h_t) \to \mathcal{S}(f)$. Since the distance between the root sets of h_t and g_t is at most $|\theta_t|$ and $|\theta_t| \to 0$, it follows that $\mathcal{S}(g_t) \to \mathcal{S}(f)$ as well. $\square$

We next want to use this result to prove that if we have a map of closed algebraic sets $G : X \to W$ with $x \in X$ mapping to $w \in W$ and the map is étale near x, i.e., the map $\mathbb{C}[W] \to \mathbb{C}[X]$ is étale near the maximal ideal Q_x of $\mathbb{C}[X]$ corresponding to x, then there are Euclidean open neighborhoods U of x and V of w such that G maps U homeomorphically onto V.

Lecture of February 26, 2010

Before proceeding further, we note the following: if one uses a different set of d linearly independent linear equations $L'_1, \ldots, L'_d$ to define Y, the number μ obtained by counting points in fibers does not change. Thus, μ does not depend on the choice of the L_i, only on Y.

The reason is that the effect of the change is that one winds up studying $A \circ \Gamma : X \to \mathbb{A}^d_{\mathbb{C}}$ instead of Γ, where $A : \mathbb{A}^d_{\mathbb{C}} \to \mathbb{A}^d_{\mathbb{C}}$ is an invertible linear transformation. Since A is a homeomorphism in both the Zariski and Euclidean topologies, this has no effect on the number of points close to x in fibers over points near $\mathbf{0}$ when one restricts the points

considered to the intersection of a Euclidean open neighborhood of **0** with a non-empty Zariski open set.

We next prove:

Proposition. *Let $G : X \to W$ be a map of closed algebraic sets of $\mathbb{C}$ and $x \in X$ be such that $G(x) = w \in W$. Suppose that G is étale near x, i.e., that the map $\mathbb{C}[W] \to \mathbb{C}[X]$ is étale near the maximal ideal Q of $\mathbb{C}[X]$ corresponding to x. Then there are Euclidean open neighborhoods U of x and V of w such that G maps U homeomorphically onto V.*

Proof. Let $R = \mathbb{C}[W]$ and $S = \mathbb{C}[X]$. Since S is étale near Q, we may replace R and S by localizations such that the map $R \to S$ is standard étale. Therefore, we may assume without loss of generality that $S = R[z]_g/(f)$, where the image of f' is invertible in S. Think of W as a Zariski closed set in $\mathbb{A}^s_{\mathbb{C}}$. Then $X \subseteq A^{s+1}_{\mathbb{C}}$ and

$$X = \{(v, \lambda) \in W \times \mathbb{A}^1_{\mathbb{C}} : f(v, \lambda) = 0, \;\; g(v, \lambda) \neq 0\}.$$

The map G now corresponds to the product projection on the first coordinate, suitably restricted.

We write $f_v(z)$ for the polynomial $f(z)$ with its coefficients (which are in R and therefore functions on W) evaluated at the point v of W. The coefficients of $f_v(z)$ are continuous functions on W. Let x correspond to (w, θ_w), where θ_w is a root of f_w such that $g_w(\theta_w) \neq 0$.

We also know that at (w, θ_w), the derivative of f_w does not vanish, and so the roots of the monic polynomial $f_w(z)$ giving points where g does not vanish are simple: evaluation at the point gives a map $R[x]_g/(f) \to \mathbb{C}$, and since f' is invertible in $R[x]_g/(f)$, it maps to a nonzero element of $\mathbb{C}$. Let c be less than half the distance between any other root of f_w and θ_w. Then there is a Euclidean open neighborhood V of w such that for all $v \in V$, the distance between the root set of f_v and the root set of f_w is $< c/4$. For every $v \in V$ there is a unique root of f_v within $c/4$ of of θ_w: call this root $\Theta(v)$. Each root of f_v is within distance $c/4$ of a root of f_w, and so any root of f_v other than $\Theta(v)$ is at distance at least $2c - c/4 - c/4 > c$ from $\Theta(v)$.

Because the coefficients of f_v vary continuously with v, so does the root set of f_v, and it follows that $\Theta(v)$ is a continuous function of v. By decreasing V, if necessary, we may assume that $g\big(v, \Theta(v)\big) \neq 0$ for $v \in V$. Then the map H defined by $H(v) = (v, \Theta(v))$, and the product projection on the first coordinate (which is G) are mutually inverse continuous functions. Let $U = H(V)$. It suffices to show that U is open in X, and for this it suffices to show that U is open in $G^{-1}(V)$. But the ball of radius $c/4$ around a point $\big(v, \Theta(v)\big)$ of U is contained in U, for if (v', λ) is in that ball, λ is within $c/4$ of $\Theta(v)$ and therefore with $c/4 + c/4$ of $\Theta(w) = \theta_w$. Therefore, $\Theta(v')$ is within $c/4 + c/4 + c/4 < c$ of λ, which forces $\Theta(v') = \lambda$, and we are done, since $\big(v', \Theta(v')\big) \in U$. $\square$

The next step is to prove the following:

Theorem. *Suppose that $\Gamma : X \to \mathbb{A}^d_{\mathbb{C}}$ and that $x \in X$ is isolated in its fiber over $\mathbf{0} \in \mathbb{A}^d_{\mathbb{C}}$. Then there is a commutative diagram of closed algebraic sets:*

$$\begin{array}{ccc} \widetilde{X} & \xrightarrow{G} & \widetilde{\mathbb{A}}^d_{\mathbb{C}} \\ \downarrow & & \downarrow \\ X & \xrightarrow[\Gamma]{} & \mathbb{A}^d_{\mathbb{C}} \end{array}$$

such that $\widetilde{\mathbb{A}}^d_{\mathbb{C}}$ is smooth and irreducible, the vertical arrows are étale, and G is finite. Moreover, there are points $\widetilde{x} \in \widetilde{X}$ and $\widetilde{\mathbf{0}} \in \widetilde{\mathbb{A}}^d_{\mathbb{C}}$ such that $G(\widetilde{x}) = \widetilde{\mathbf{0}}$, $\widetilde{x} \mapsto x$, $\widetilde{\mathbf{0}} \mapsto \mathbf{0}$, and $\widetilde{x}$ is the only point of $\widetilde{X}$ that maps to $\widetilde{\mathbf{0}}$.

The statement that G is finite means that the corresponding map of rings is module-finite. For the purpose of doing counting of points in fibers we will be able to replace the map Γ by the map G and the points x and $\mathbf{0}$ by $\widetilde{x}$ and $\widetilde{\mathbf{0}}$. A key point is that near these points, each point has a Euclidean neighborhood carried homeomorphically by the appropriate map to a Euclidean open neighborhood of $\mathbf{0}$ or $\widetilde{\mathbf{0}}$. Instead of passing to Euclidean neighborhoods, we have passed to "étale neighborhoods."

We postpone the proof for a bit. We first prove a purely ring-theoretic result that will be helpful.

Theorem. *Let A be a Noetherian ring, R a finitely generated A-algebra, let m be a maximal ideal of A and let $n \subseteq R$ be a maximal ideal of R that is a minimal prime of mR. Then R^{h}_n is module-finite over A^{h}_m, and is a localization of $R \otimes_A A^{\mathrm{h}}_m$ at one element.*

Note that if A and R are finitely generated algebras over $\mathbb{C}$ and m, n are maximal ideals, the residue class fields are both $\mathbb{C}$.

Note that $\widehat{R_n}$ is module-finite over $\widehat{A_m}$: it is easy to see that the extension of residue class fields is finite algebraic, and mR_n is n-primary. This illustrates a frequently recurring phenomenon: a result for completions often has an analogue for Henselizations.

The Theorem above is quite non-trivial: the proof uses Zariski's Main Theorem.

Lecture of March 8, 2010

Proof of the Theorem. Note that since R is finitely generated as an A-algebra, R/n is a field finitely generated as an algebra over the field A/m. By one form of Hilbert's Nullstellensatz, this implies that that $L = R/n$ is a finite algebraic extension of $K = A/m$.

Let T be the integral closure of $C = A^{\mathrm{h}}_m$ in $C \otimes_A R$. We have an obvious map

$$C \otimes_A R \twoheadrightarrow C/mC \otimes_R R/n \cong K \otimes_K L \cong L.$$

The kernel of the composite map is evidently a maximal ideal Q of $C \otimes_A R$ lying over the maximal ideal mC of C (mC is the maximal ideal of C because C is the Henselization of

(A, mA_m)). The ideal Q is evidently maximal in its fiber over $mC \in \mathrm{Spec}\,(C)$, but it is minimal as well, since

$$C \otimes_A R/(mC)^{\mathrm{e}} \cong C/mC \otimes_A R/mR \cong K \otimes_A R/mR \cong R/mR,$$

and n is minimal over mR. It follows that there exists $t \in T - Q$ such that $T_t = (C \otimes_A R)_t$. Since $C \otimes_A R$ is finitely generated over C by a finite set of generators of R, we can choose a power t^N of t and a subalgebra T_0 of T containing t and module-finite over C such that t^N multiplies the image of every generator of R into T_0. It follows that $(T_0)_t \cong (C \otimes_A R)_t$.

Now, $(C \otimes_A R)_Q$ is a local ring of $(C \otimes_A R)_t$ at a maximal ideal, and so it is also a local ring of $(T_0)_t$ at a maximal ideal. But T_0 is module-finite over the Henselian local ring C, and therefore it decomposes as a product of local rings: one of these must be the same as $(C \otimes_A R)_Q$, Each of these local rings is module-finite over the Henselian ring C via a local map, and, therefore, Henselian: we leave this an exercise. It follows that $(R \otimes_A C)_Q$ is Henselian. It is the localization of $(T_0)_t$ at an idempotent, and it is therefore the localization of T_0 at one element. But then it is also the localization of $C \otimes_A R$ at one element.

We may now complete the proof by showing that $(R \otimes_A C)_Q$ is the Henselization of R. First note that since there is a local R-algebra map $R \to (R \otimes_A C)_Q$ and this ring is Henselian, we have a unique local R-algebra map $R_n^{\mathrm{h}} \to (R \otimes_A C)_Q$. On the other hand, C is a direct limit of pointed étale extensions C_i of A. Each of these, when tensored with R, is a localization of an étale extension of R. Let Q_i be the kernel of the composite map

$$C_i \otimes_A R \twoheadrightarrow K \otimes_K R/n \cong L.$$

Then $(C \otimes_A R)_Q$ is the direct limit of the $(C_i \otimes_A R)_{Q_i}$, each of which is pointed étale over R. But this gives a unique local R-algebra map $(C \otimes_A R)_Q \to R_n^{\mathrm{h}}$, and it is injective. The composition

$$R_n^{\mathrm{h}} \to (C \otimes_A R)_Q \to R_n^{\mathrm{h}}$$

is a local R-algebra map $R_n^{\mathrm{h}} \to R_n^{\mathrm{h}}$, and so is evidently the identity, which forces the injection $(C \otimes_A R)_Q \to R_n^{\mathrm{h}}$ to be surjective as well. $\square$

The next result is aimed at replacing the Henselizations A_m^{h} and R_n^{h} by étale extensions. We want to descend from the Henselizations to pointed étale extensions and then "unlocalize" these, in a manner of speaking. For this result we impose some additional hypotheses, namely that C be a domain and that $\dim(A) = \dim(R)$. C is a domain if A is regular, and these hypotheses will hold in the geometric situation in which we want to apply the result.

Theorem. *Let A, m, R, n be as in the preceding theorem. Let $C = A_m^{\mathrm{h}}$ and $D = R_n^{\mathrm{h}}$. Assume that C is a domain, which is true when A_m is regular, and that* $\dim(A_m) = \dim(R_n)$. *Then $C \to D$ is injective, and since D is module-finite, it has a torsion-free rank $\mu > 0$ over C. Moreover, $\widehat{D} \cong \widehat{R_n}$ has torsion-free rank μ over $\widehat{C} \cong \widehat{A_m}$.*

Let $\eta \in C \otimes_A R$ be such that $(C \otimes_A R)_\eta \cong D$. Then there are étale extensions $\widetilde{A}$ of A and $\widetilde{R}$ of R such that there is a commutative diagram

$$\begin{array}{ccc} C & \longrightarrow & D \\ \uparrow & & \uparrow \\ \widetilde{A} & \longrightarrow & \widetilde{R} \\ \uparrow & & \uparrow \\ A & \longrightarrow & R \end{array}$$

and such that:

(1) *There is a unique maximal ideal $\widetilde{m}$ of $\widetilde{A}$ lying over m in A; moreover, $\widetilde{m} = m\widetilde{A}$ and is the contraction of mC.*
(2) *There is a unique maximal ideal $\widetilde{n}$ of $\widetilde{R}$ lying over $\widetilde{m}$ in $\widetilde{A}$ (equivalently, lying over m in A). This maximal ideal is also the unique maximal ideal of $\widetilde{R}$ lying over n in R, and it is the contraction of nD.*
(3) *There is an element $\eta_0 \in \widetilde{A} \otimes_A R$ such that η_0 maps to η in $C \otimes_A R$ and $\widetilde{R} = (\widetilde{A} \otimes_A R)_{\eta_0}$.*
(4) *$\widetilde{R}$ is a module-finite extension of $\widetilde{A}$ of torsion-free rank μ.*

Proof. We know that $\dim(C) = \dim(A_m)$ and $\dim(D) = \dim(R_n) = \dim(A_m)$, so that $\dim(C) = \dim(D)$. Since D is module-finite over C, it has the same dimension as the image of C. Since C is a domain, $C \to D$ cannot have a kernel, or the dimension of D will be strictly smaller than the dimension of C. Thus, D has some torsion-free rank $\mu > 0$ over C, and there will be an exact sequence

$$0 \to C^\mu \to D \to W \to 0$$

where W is killed by a nonzero element of C. Since completion is exact,

$$0 \to \widehat{C}^\mu \to \widehat{D} \to \widehat{W} \to 0$$

is exact, and it follows that the torsion-free rank of $\widehat{D}$ over $\widehat{C}$ is also μ.

Next observe that C is a directed union of pointed étale extensions of A_m. Here, the maps are faithfully flat and, hence, injective. Each of these pointed étale extensions is a direct limit of localizations of an étale extension at one element, and these are simply étale extensions themselves. Thus, C is a direct limit of étale extensions of A. Each may be localized further at an element to kill the kernel of the map to C if there is any. Thus, we may view C as a directed union of étale extensions $\widetilde{A}$ of A. Each of these may be viewed as a localization at one element of a standard étale extension of A, and so will be the localization at one element of a module-finite extension of A. In a pointed étale extension of A_m, m generates the maximal ideal, which is contracted from mC. It follows that in a suitable localization of $\widetilde{A}$, the expansion of m will be the contraction of mC. We henceforth use $\widetilde{A}$ for an étale extension of A satisfying these conditions: we are free to enlarge the choice of $\widetilde{A}$ further to satisfy some additional conditions.

Choose a finite set of elements v_j of $C \otimes_A R$ whose images generate $(C \otimes_A R)_\eta$ as a C-module. We may further assume, enlarging the set of generators if necessary, that the images of $v_1, \ldots, v_\mu$ are linearly independent over C and, and that we have a nonzero element $c \in C$ that kills $(C \otimes_A R)_\eta$ modulo the C-span of the elements $v_1, \ldots, v_\mu$.

Now choose $\widetilde{A}$ in the direct limit system of étale extensions of A so large that $\widetilde{A}$ contains an element $\widetilde{c}$ that maps to c, so large that $\widetilde{A} \otimes_A R$ contains an element η_0 that maps to η, and so large that $(\widetilde{A} \otimes_A R)_{\eta_0}$ contains elements $\widetilde{v}_j$ that map to the v_j. Then

$$(\widetilde{A} \otimes_A R)_{\eta_0} / \sum_j \widetilde{A}\widetilde{v}_j$$

is killed when we apply $C \otimes_{\widetilde{A}} \_$, and it follows that if we replace $\widetilde{A}$ by a suitably larger étale extension this quotient will be zero. Similarly, after replacing $\widetilde{A}$ by a suitably larger étale extension, $\widetilde{c}$ will multiply $(\widetilde{A} \otimes_A R)_{\eta_0}$ into $\sum_j \widetilde{A}\widetilde{v}_j$.

Localization of $\widetilde{A}$ at one element will again guarantee that $mC \cap \widetilde{A} = m\widetilde{A}$ is the only maximal ideal of $\widetilde{A}$ lying over m. Consider the corresponding choice of $\widetilde{R} = (\widetilde{A} \otimes_A R)_{\eta_0}$. The contraction of nD to $\widetilde{R}$ lies over m in A, since nD lies over m in A, and therefore lies over $m\widetilde{A}$ in $\widetilde{A}$. The maximal ideals of $\widetilde{R}$ lying over m in A correspond to the maximal ideals of $\widetilde{R}/m\widetilde{R} \cong \left((\widetilde{A}/m\widetilde{A}) \otimes_A R\right)_{\eta_0} \cong (K \otimes_A R)_{\eta_0} \cong (R/mR)_{\eta_0}$. On the other hand, D has a unique maximal ideal, nD, lying over mA^{h}, and we conclude that $\left((A^{\mathrm{h}}/mA^h) \otimes_A R\right)_\eta$ has only one maximal ideal, and this ring becomes $(K \otimes_A R)_\eta \cong (R/mR)_\eta$. Since η_0 maps to η, they have the same image in R/mR. Therefore, $(R/mR)_{\eta_0} = (R/mR)_\eta$, and there is a unique maximal ideal of $\widetilde{R}$ lying over $m\widetilde{A}$. It is the only maximal ideal lying over n, since n lies over m. $\square$

Lecture of March 10, 2010

The preceding Theorem now immediately implies the result stated in the Lecture Notes of February 26:

Theorem. *Suppose that $\Gamma : X \to \mathbb{A}^d_{\mathbb{C}}$ and that $x \in X$ is isolated in its fiber over $\mathbf{0} \in \mathbb{A}^d_{\mathbb{C}}$. Then there is a commutative diagram of closed algebraic sets:*

$$\begin{array}{ccc} \widetilde{X} & \xrightarrow{G} & \widetilde{\mathbb{A}}^d_{\mathbb{C}} \\ \downarrow & & \downarrow \\ X & \xrightarrow[\Gamma]{} & \mathbb{A}^d_{\mathbb{C}} \end{array}$$

such that $\widetilde{\mathbb{A}}^d_{\mathbb{C}}$ is smooth and irreducible, the vertical arrows are étale, and G is finite. Moreover, there are points $\widetilde{x} \in \widetilde{X}$ and $\widetilde{\mathbf{0}} \in \widetilde{\mathbb{A}}^d_{\mathbb{C}}$ such that $G(\widetilde{x}) = \widetilde{\mathbf{0}}$, $\widetilde{x} \mapsto x$, $\widetilde{\mathbf{0}} \mapsto \mathbf{0}$, and $\widetilde{x}$ is the only point of $\widetilde{X}$ that maps to $\widetilde{\mathbf{0}}$.

We can now use this to justify our earlier statements about counting of points in fibers. But we first need one more fact:

Proposition. *Let $g : Y \to Z$ be a finite morphism of affine algebraic sets over $\mathbb{C}$, and suppose that $y \in Y$ is the only point lying over $z \in Z$. Then there for every Euclidean neighborhood U of y in Y there is a Euclidean neighborhood V of z in Z such that for all points $v \in V$, $g^{-1}(v) \subseteq U$.*

Proof. If not, we can choose a real number $\epsilon > 0$, a sequence of points $\{z_i\}_i$ in Z converging to z, and points $\{y_i\}_i \in Y$ such that for all i, $g(y_i) = z_i$ while $|y_i - y| > \epsilon$. Think of Y as embedded in $\mathbb{A}^N_{\mathbb{C}}$ and let $F_1, \ldots, F_N$ be coordinate functions on Y. Since $\mathbb{C}[Y]$ is module-finite over $\mathbb{C}[Z]$, each F_j satisfies a monic polynomial equation over $\mathbb{C}[Z]$, say

$$F_j^{d_j} + \sum_{t=0}^{d_j-1} r_{j,t} F_j^t = 0,$$

where the $r_{j,t} \in \mathbb{C}[Z]$.

This implies that the coordinates of the y_i are bounded. To see this for $F_j(y_i)$, note that it is in the root set of $F_j^{d_j} + \sum_{t=0}^{d_j-1} r_{j,t}(z_i) F_j^t = 0$: as $z_i \to z$, this root set converges to the root set of $F_j^{d_j} + \sum_{t=0}^{d_j-1} r_{j,t}(z) F_j^t = 0$. It follows that the sequence $\{y_i\}_i$ has a subsequence that converges, in the Euclidean topology, to a point $y' \in \mathbb{A}^N_{\mathbb{C}}$. Since Y is closed in the Zariski topology in $\mathbb{A}^N_{\mathbb{C}}$, it is closed in the Euclidean topology, and $y' \in Y$. Change notation, replacing the original sequence of y_i by this subsequence and taking the corresponding subsequence of the z_i. Then $y' \neq y$, but $g(y') = z$, by the continuity of g in the Euclidean topology, a contradiction. $\square$

We are now ready to justify the statement we made earlier about counting points in fibers. The torsion-free rank μ of $\mathbb{C}[\widetilde{X}]$ over $\mathbb{C}[\widetilde{\mathbb{A}}^d]$ is the same as the degree of the extension of function fields. By part (c) of the Lemma on the third page of the Lecture Notes of January 6, off a proper Zariski closed subset Z' of $\widetilde{\mathbb{A}}^d$, all fibers have μ distinct points. Since the map is finite, by the preceding Proposition all points of any fiber over a point close to $\widetilde{\mathbf{0}}$ are approaching $\widetilde{x}$, and off Z' there are always μ such points. Thus, for any small Euclidean neighborhood U of $\widetilde{x}$ there is a small Euclidean neighborhood V of $\widetilde{\mathbf{0}}$ such that all fibers over points of $V - Z'$ are contained in U and have cardinality μ. But, since the vertical arrows are étale, by the first Proposition of the Lecture Notes of February 26, sufficiently small neighborhoods of $\widetilde{x}$ and $\widetilde{\mathbf{0}}$ respectively will be carried homeomorphically to Euclidean open neighborhoods of x and $\mathbf{0}$, respectively. The image of Z' will be constructible of dimension smaller than d, and so its closure Z will be a proper closed subset of $\mathbb{A}^d_C$. This establishes our earlier statements about counting points in fibers. Note that μ will also be the torsion-free rank of the Henselization of the local ring at x over the Henselization of the local ring at $\mathbf{0}$ (or we may use $\widetilde{x}$ and $\widetilde{\mathbf{0}}$: the Henselizations don't change), and will also be the torsion-free rank of the completion of the local rings at x over the completion of the local ring at $\mathbf{0}$: the latter is a regular local ring.

We next want to relate multiplicities thought of in this geometric way with Serre's definition using alternating sums of lengths of Tor.

Let A be the completion of the local ring at $\mathbf{0}$: $L_1, \ldots, L_d$ is a regular system of parameters. Let $\underline{L} = L_1, \ldots, L_d$. Let R be the completion of the local ring at x. Let M

be any finitely generated A-module. We first observe that the torsion-free rank of M over A may also be obtained as

$$\chi(\underline{L}; M) = \sum_{i=0}^{d} (-1)^i \ell\big(H_i(\underline{L}; M)\big)$$

where $H_i(\underline{L}; M)$ indicates Koszul homology. To check that the rank of M is the same as $\chi(\underline{L}; M)$, first note that both are additive on short exact sequences of finitely generated modules. From this it follows that if

$$0 \to A^{b_d} \to \cdots \to A^{b_1} \to A^{b_0} \to M \to 0$$

is a free resolution of M, then the rank of M is $b_0 - b_1 + \cdots + (-1)^d b_d$ times the rank of A, which is 1, and it is also $b_0 - b_1 + \cdots + (-1)^d b_d$ times $\chi(\underline{L}; A)$. But this is also 1: because $L_1, \ldots, L_d$ is a regular sequence, the Koszul complex is a free resolution of $A/(\underline{L}) \cong \mathbb{C}$, the residue class field. All higher Koszul homology is 0, and $H_0(\underline{L}; A) \cong \mathbb{C}$, from which $\chi(\underline{L}; A) = 1$ follows. Note also that the Koszul homology modules are the same as the modules $\operatorname{Tor}_i^A(\mathbb{C}, M)$, since the Koszul complex resolves $\mathbb{C} \cong A/(\underline{L})$.

Now suppose that we are considering varieties $X = V(P)$ and $Y = V(Q)$ with an isolated point of intersection x. For convenience we translate coordinates so that x is the origin. Our geometric method of getting at the intersection multiplicity is to work with $X \times Y$ and Δ, the diagonal, instead. The completed local ring of $X \times Y$ at (x, x) is the complete tensor product over $\mathbb{C}$ of the completed local rings A/PA and A/QA of X and Y, respectively. Let $f_1, \ldots, f_d$ be the images of the defining linear forms of the diagonal in $(A/PA)\widehat{\otimes}_{\mathbb{C}}(A/QA)$. From the remarks above, μ is

$$\sum_{i=0}^{d} (-1)^i \ell\big(H_i(f_1, \ldots, f_d; (A/PA)\widehat{\otimes}_{\mathbb{C}}(A/QA))\big).$$

Since $f_1, \ldots, f_d$ is a regular sequence in $B = A\widehat{\otimes}_{\mathbb{C}}A$, this is

$$\sum_{i=0}^{d} (-1)^i \ell\big(\operatorname{Tor}_i^B(A, (A/PA)\widehat{\otimes}_{\mathbb{C}}(A/QA))\big),$$

where the copy of A on the left in Tor is $A\widehat{\otimes}_{\mathbb{C}}A/(f_1, \ldots, f_d) \cong A$.

We can calculate this as follows. Take finite free resolutions of A/PA and A/QA over A, and form a double complex by taking their complete tensor product over $\mathbb{C}$. The total complex of this double complex is a free resolution of $(A/PA)\widehat{\otimes}_{\mathbb{C}}(A/QA)$ over $B = A\widehat{\otimes}_{\mathbb{C}}A$ because complete tensor product over $\mathbb{C}$ is exact. When we apply $A \otimes_B \_$ we get a complex whose homology is $\operatorname{Tor}_i^B(A, (A/PA)\widehat{\otimes}_{\mathbb{C}}(A/QA))$. But this complex is also obtained by taking the total complex of the ordinary tensor product over A of the resolutions of A/PA and A/QA over A. Thus,

$$\operatorname{Tor}_i^B(A, (A/PA)\widehat{\otimes}_{\mathbb{C}}(A/QA)) \cong \operatorname{Tor}_A^i(A/PA, A/QA).$$

But then

$$\mu = \sum_{i=0}^{d} (-1)^i \ell\big(\mathrm{Tor}_A^i(A/PA, A/QA)\big).$$

and there is no need to use reduction to the diagonal in the definition.

One more wrinkle: because the point of intersection is isolated, $P+Q$ is primary to the maximal ideal that corresponds to that point. This means not only that the Tor modules in this formula for μ have finite length, but also that the formula for μ is valid if we use the local ring at x instead of the completed local ring A at x throughout the formula: these finite length modules don't change when we complete.

Lecture of March 12, 2010

We return to the study of approximation rings.

Proposition. *If R is an approximation ring and I is a proper ideal of R, then R/I is an approximation ring.*

Proof. Let $I = (r_1, \ldots, r_s)R$. Given a system of polynomial equations

$$F_j(X_1, \ldots, X_n) = 0, \quad 1 \le j \le m$$

with coefficients in R/I, we may lift coefficients to obtain corresponding polynomials $\widetilde{F}_j(X_1, \ldots, X_n)$ over R. Introduce additional variables Y_{ik} and consider the system

$$(*) \quad \widetilde{F}_j(X_1, \ldots, X_n) - \sum_{i=1}^{s} r_i Y_{ij} = 0$$

$1 \le j \le m$ over R. If the F_j have a solution in the completion of R/I, which may be identified with $\widehat{R}/I\widehat{R}$, then the system $(*)$ has a solution in $\widehat{R}$. Thus, $(*)$ has a solution in R, and its image in R/I gives the required solution of the $F_j(X_1, \ldots, X_n) = 0$ in R/I. $\square$

Proposition. *If $R \to S$ is local, where R is an approximation ring and S is module-finite over R, then S is an approximation ring.*

Proof. The idea of the proof is to "push down" a given system of equations over S to a system over R (in different variables) such that solving the original system over S (respectively, $\widehat{S}$) is equivalent to solving the new system over R (respectively, $\widehat{R}$).

Let $\theta_1, \ldots, \theta_h$ be elements of S that span S over R. Let $\big(r_{ij}\big)$ be an $N \times h$ matrix whose rows span the module of relations over R on the elements $\theta_1, \ldots, \theta_h$. For all i, j there are elements $b_{ijk} \in R$ such that

$$(\#) \quad \theta_i \theta_j = \sum_{k=1}^{h} b_{ijk} \theta_k.$$

Notice that $\theta_1, \ldots, \theta_h$ also span $\widehat{S}$ over $\widehat{R}$, that the rows of the matrix $\left(r_{ij}\right)$ still span the relations over $\widehat{R}$ (by the right exactness of tensor), and that the equations (#) hold for $\widehat{R}$ and $\widehat{S}$.

Any element of S (respectively, $\widehat{S}$) can be written as an R-linear (respectively, as an $\widehat{R}$-linear) combination of the elements $\theta_1, \ldots, \theta_h$. Instead of seeking the elements of S that satisfy the equations F_j directly, we look for the coefficients needed to write them as linear combinations of $\theta_1, \ldots, \theta_h$.

We therefore introduce nh new variables Y_{ki} (these will take values in R or $\widehat{R}$). We substitute $\sum_{k=1}^{h} Y_{ki}\theta_k$ for X_i in each equation $F_j = 0$. Using the equations (#) repeatedly, we can rewrite

$$F_j(\sum_{k=1}^{h} Y_{k1}\theta_k, \ldots, \sum_{k=1}^{h} Y_{kn}\theta_k)$$

in the form

$$G_{j1}\theta_1 + \cdots + G_{jh}\theta_h$$

where every G_{jt} is a polynomial in the variables Y_{ki} with coefficients in R. The condition that this vanish after we substitute elements of R (or $\widehat{R}$) for the Y_{ki} is that the value of

$$(G_{j1}, \ldots, G_{jh})$$

be in the span of the rows of $\left(r_{ij}\right)$. Let $\rho_1, \ldots, \rho_N$ denote the rows of this matrix, and let Z_{jt} be mN new indeterminates. Solving the original system over S (or $\widehat{S}$) is equivalent to solving the system

$$(G_{j1}, \ldots, G_{jh}) - \sum_{t=1}^{N} Z_{jt}\rho_t = 0$$

over R (or $\widehat{R}$). This becomes a system of polynomial equations over R if we equate the entries of the vectors on the left to 0 for every j.

A solution of the original system $\widehat{S}$ gives a solution of the new system of $\widehat{R}$. Since R is an approximation ring we get a solution of the new system over R, and this yields the required solution of the original system over S. $\square$

Our next objective is to prove the following:

Lemma. *Let R denote the localization at a prime ideal of a finitely generated algebra over a field K or a DVR (V, tV). Then R^{h} is a homomorphic image of a module-finite local extension of A^{h}, where A is a regular local ring that has the form $\Lambda[\underline{x}]_Q$, where Λ is either a field or else a DVR that is a localization of a finitely generated V-algebra, $\underline{x} = x_1, \ldots, x_n$, and Q is generated by the maximal ideal of Λ and $\underline{x}$.*

Lecture of March 15, 2010

Before proving the result stated at the end of the Lecture Notes from March 12, we observe the following fact. (This result can also be deduced from the harder and deeper Theorem stated at the end of the notes from February 26, but that argument uses Zariski's Main Theorem, which is not needed here.)

Proposition. *Let T be a module-finite extension of a quasilocal ring (R, P, K) and let Q be a maximal ideal of T. Then $T^{\rm h}_Q$ is a local ring of $R^{\rm h} \otimes_R T$, and the map $R^{\rm h} \to T^{\rm h}$ is module-finite and local.*

Proof. Because $R^{\rm h}$ is Henselian and $R^{\rm h} \otimes_R T$ is module-finite over R_h, it decomposes. The maximal ideals of this ring all contract to the maximal ideal P of R, and so correspond bijectively to the maximal ideals of

$$(R/P) \otimes_R (R^{\rm h} \otimes_R T) \cong K \otimes_R T \cong T/PT,$$

and, hence, to the maximal ideals of T. Suppose that $\mathcal{Q}$ is the maximal ideal of $R^{\rm h} \otimes_R T$ corresponding to Q. Then

$$T_Q \to (R^{\rm h} \otimes_R T)_{\mathcal{Q}}$$

is a local map. Since $R^{\rm h}$ is Henselian, $R^{\rm h} \otimes_R T$ decomposes, and $(R^{\rm h} \otimes_R T)_{\mathcal{Q}}$ is one of the factors. Since direct product and direct sum of finitely many modules are the same, $(R^{\rm h} \otimes_R T)_{\mathcal{Q}}$ is a direct summand of a module-finite extension of $R^{\rm h}$, and is local. By the first problem of Problem Set #3, it follows that $(R^{\rm h} \otimes_R T)_{\mathcal{Q}}$ is Henselian. We therefore have a local map

$$T^{\rm h}_Q \to (R^{\rm h} \otimes_R T)_{\mathcal{Q}}.$$

Since $R^{\rm h}$ is a direct limit if pointed étale extensions of R, we have that $(R^{\rm h} \otimes_R T)_{\mathcal{Q}}$ is a direct limit of pointed étale extensions of T_Q, which provides an injective local map $(R^{\rm h} \otimes_R T)_{\mathcal{Q}} \to T^{\rm h}_Q$. Since the composite

$$T^{\rm h}_Q \to (R^{\rm h} \otimes_R T)_{\mathcal{Q}} \to T^{\rm h}_Q$$

is a local map that is the identity on T_Q, it is the identity, and so $(R^{\rm h} \otimes_R T)_{\mathcal{Q}} \to T^{\rm h}_Q$ is surjective as well as injective. □

We next prove the result stated at the end of the Lecture Notes from March 12, which we state again here.

Lemma. *Let R denote the localization at a prime ideal of a finitely generated algebra over a field K or a DVR (V, tV). Then $R^{\rm h}$ is a homomorphic image of a module-finite local extension of $A^{\rm h}$, where A is a regular local ring that has the form $\Lambda[\underline{x}]_Q$, where Λ is either a field or else a DVR that is a localization of a finitely generated V-algebra, $\underline{x} = x_1, \ldots, x_n$, and Q is generated by the maximal ideal of Λ and $\underline{x}$.*

Proof. Write $R = T_P$ where T is a finitely generated K or V-algebra and P is prime. Since T is a homomorphic image of a domain (even a polynomial ring) finitely generated over K or V, we may assume that T is a domain. In the case of a DVR V, we might as well assume that P contains t: otherwise, we can replace T and V by T_t and V_t, a field, and we are in the case where the base is a field.

The residue class field of R may be assumed to be a finitely generated field over K (in the DVR case, $K = V/tV$). Choose $z_1, \ldots, z_h$ in T such that the images of these elements form a transcendence basis for R/PR over K. If $K \subseteq T$ then $K[z_1, \ldots, z_h] \subseteq T$ and the elements $z_1, \ldots, z_h$ are algebraically independent over K since this is true even mod P. Since the nonzero elements are not in P, they all have inverses, and so

$$\Lambda = K(z_1, \ldots, z_h) \subseteq R.$$

Similarly, if T is finitely generated over V then $z_1, \ldots, z_h$ are algebraically independent over V, and every element of $V[z_1, \ldots, z_h]$ not in (t) has an inverse in R. Let $V(z_1, \ldots, z_h)$ denote the localization of $V[z_1, \ldots, z_h]$ at the prime ideal (t). Then

$$\Lambda = V(z_1, \ldots, z_h) \subseteq R,$$

and Λ is a DVR with maximal ideal generated by (t). We may then replace K or V by Λ, and think of T as a finitely generated Λ-algebra.

In this way we may assume without loss of generality that R/P is a finite algebraic extension of K (which is $\Lambda/t\Lambda$ in the DVR case), so that P is a maximal ideal. We also know that when Λ is a DVR, P contains t. We map a polynomial ring

$$T = \Lambda[Y_1, \ldots, Y_n]$$

onto R. Let $\widetilde{P}$ be the maximal ideal that is the inverse image of P. Modulo $\widetilde{P}$, the image of every Y_j is algebraic over K, which is the image of Λ in the DVR case. For each j, let $F_j(W_j)$ denote a monic polynomial in one variable W_j such that the coefficients, other than the leading coefficient, are in K or Λ, that lifts the polynomial over K satisfied by Y_j. Then $x_j = F_j(Y_j) \in \widetilde{P}$. We now see that T is module-finite over $\Lambda[\underline{x}]$, because for $1 \leq j \leq n$, Y_j satisfies the monic polynomial $F_j(Y_j) - x_j = 0$ (here, $-x_j$ becomes part of the constant term of this polynomial). It follows that the x_j are algebraically independent over Λ. The contraction of $\widetilde{P}$ contains t and all the x_j, and so must be equal to $Q = (t, \underline{x})\Lambda[\underline{x}]$. Since T is module-finite over $\Lambda[\underline{x}]$, $(T_{\widetilde{P}})^{\mathrm{h}}$ is module-finite over $\Lambda[\underline{x}]^{\mathrm{h}}_Q$, by the preceding Proposition. $\square$

Lecture of March 17, 2010

By the result proved last time, we need only prove that rings of the form $V[\underline{x}]^{\rm h}_Q$ are approximation rings, where (V, tV) denotes either $(K, 0)$, where K is a field, or (V, tV) where V is an excellent DVR.

We need to show that given a solution of a finite system of polynomial equations over such a ring with coefficients in $A^{\rm h}$, where $A = V[\underline{x}]_Q$, if there is a solution in $\widehat{A}$, there is a solution in $A^{\rm h}$.

First, we want to get rid of coefficients in $A^{\rm h}$: we want to use coefficients in A. The idea is to use systems over A with a congruence condition instead.

Lemma. *Let (A, m) be as above and suppose that for every system of polynomial equations $F_j(Y_1, \ldots, Y_d) = 0$, $1 \leq j \leq s$, with coefficients in A, if there is a solution $(\widehat{y}_1, \ldots, \widehat{y_d})$ over $\widehat{A}$, then for every positive integer N there is a solution $(y'_1, \ldots, y'_d)$ over $A^{\rm h}$ such that $y'_j \equiv \widehat{y}_j \mod m^N \widehat{A}$, $1 \leq j \leq d$. Then $A^{\rm h}$ is an approximation ring.*

Proof. Suppose that we are given a system of equations $F_j(Y_1, \ldots, Y_d) = 0$ over $A^{\rm h}$ with a solution $(\widehat{y}_1, \ldots, \widehat{y_d})$ over $\widehat{A}$. We must show that these equations have a solution in $A^{\rm h}$. For each coefficient $c_{\mu,j}$ of F_j in (we have that $c_{\mu,j} \in A^{\rm h}$) we introduce a new variable $Z_{\mu,j}$. Let $G_j = G_j(Y, Z)$ be the polynomial obtained from F_j by replacing every coefficient $c_{\mu,j}$ by the corresponding variable. Thus, G_j has coefficients each of which is 1 or 0.

Every $c_{\mu,j}$ is algebraic over A: for every choice of μ and j, choose a nonzero polynomial equation $H_{\mu,j}(Z_{\mu,j}) = 0$ with coefficients in A that is satisfied by $c_{\mu,j}$. For all μ, j we can choose N so large that if c is any root of $H_{\mu,j}(Z_{\mu,j}) = 0$ in $A^{\rm h}$ with $c \neq c_{\mu,j}$, then $c - c_{\mu,j} \notin m^N A^{\rm h}$, and since there are only finitely many choices of μ, j we can choose a single value of N so large that this condition holds simultaneously for all μ, j.

Now consider the family of equations $G_j(Y, Z) = 0$ together with $H_{\mu,j}(Z_{\mu,j}) = 0$. These have the solution $Y = (\widehat{y}_1, \ldots, \widehat{y}_d)$, $Z_{\mu,j} = c_{\mu,j}$ in $\widehat{A}$. It follows from our hypothesis that these equations have a solution $(y'_1, \ldots, y'_d)$, $c'_{\mu,j}$ in $A^{\rm h}$ that is congruent to the first solution mod $m^N \widehat{A}$. For all μ, j , we have that $c'_{\mu,j}$ and $c_{\mu,j}$ are both roots of $H_{\mu,j}(Z_{\mu,j}) = 0$ in $A^{\rm h}$, and that $c'_{\mu,j} - c_{\mu,j} \in m^N \widehat{A} \cap A^{\rm h} = m^N A^{\rm h}$. By our choice of N, we must have that $c'_{\mu,j} = c_{\mu,j}$ for all μ, j. But when these values are used for the $Z_{\mu,j}$, the polynomials $G_j(Y, Z)$ become the polynomials $F_j(Y)$ with which we started. Therefore $(y'_1, \ldots, y'_d)$ is a solution of the equations $F_j(Y) = 0$ in $A^{\rm h}$, as required. $\square$

We next observe that once we know the coefficients are in $A = T_Q$, we may multiply by an element of $T - Q$ to clear denominators. Since $\widehat{A}$ is regular it is a domain, and the solutions of the equations in both $A^{\rm h}$ and in $\widehat{A}$ are unaffected. Hence:

Corollary. *Let (A, m) and $T = V[x_1, \ldots, x_n]$ be as above and suppose that for every system of polynomial equations $F_j(Y_1, \ldots, Y_d) = 0$, $1 \leq j \leq s$, with coefficients in T, if there is a solution $(\widehat{y}_1, \ldots, \widehat{y_d})$ over $\widehat{A}$, then for every positive integer N there is a solution*

$(y'_1, \ldots, y'_d)$ over A^{h} such that $y'_j \equiv \widehat{y}_j$ mod $m^N\widehat{A}$, $1 \leq j \leq d$. Then A is an approximation ring. $\square$

We next observe that we can state the result somewhat more conceptually this way: given a finitely generated T-subalgebra S of $\widehat{A}$ and a power of the maximal ideal m^N, there is a T-algebra map $\phi : S \to A^{\mathrm{h}}$ such that for every element $u \in S$, $\phi(u) \equiv u$ mod $m^N\widehat{A}$. Here, S is generated by solutions $\widehat{y_j}$ of a system of equations $F_j(Y)$ over T, and the elements $\widehat{y_j}$ satisfy these equations. The images under the homomorphism also satisfy the same equations. Note that the condition that $\phi(u) \equiv u$ mod $m^N\widehat{A}$ for all $u \in S$ is equivalent to the same condition imposed on a set of generators of S over T: the set of elements of S that satisfy this condition is a T-subalgebra of S, and so will be all of S if it contains generators for S as a T-algebra. We henceforth shall usually write $s_1, \ldots, s_d$ for a set of generators of S over T instead of writing $\widehat{y}_1, \ldots, \widehat{y}_d$.

By phrasing the problem in terms of S we achieve certain freedoms: we can change the generators of S and this changes the equations we need to solve. (We can even replace S by a larger finitely generated T-subalgebra of $\widehat{A}$: a homomorphism from the larger subalgebra may be restricted to the original subalgebra. We will not need to do this now, but will later in the DVR case.) We can map $T[Y_1, \ldots, Y_d] \twoheadrightarrow S$ and consider the kernel, which is a prime ideal P of $T[Y_1, \ldots, Y_d]$. We can take the equations we need to solve to be any set of generators of P. By making use of a congruence condition as well, we can do a little bit more.

Let h denote the height of the ideal P. Then $T[T_1, \ldots, T_d]_P$ is a regular local ring of dimension h, and we can choose h generators $F_1, \ldots, F_h$ for $PT[Y_1, \ldots, Y_d]_P$ such that $F_1, \ldots, F_h \in T[Y_1, \ldots, Y_d]$. Then $P/(F_1, \ldots, F_h)$ becomes 0 when we localize at P, and so there is an element $G \in T - P$ such that $GP \subseteq (F_1, \ldots, F_d) \subseteq P$.

Since $G(s_1, \ldots, s_d) \neq 0$ in $\widehat{A}$, by increasing the value of N, if necessary, we may guarantee that $G(s_1, \ldots, s_d) \notin m^N\widehat{A}$. Then it suffices to approximate the solution of $F_j(Y) = 0$ mod m^N, that is, it suffices to find $y'_1, \ldots, y'_d \in A^{\mathrm{h}}$ such that $y'_i \equiv s_i$ mod $m^N\widehat{A}$, $1 \leq i \leq d$ and $F_j(y'_1, \ldots, y'_d) = 0$, $1 \leq j \leq h$. We claim that it now follows that $F(y'_1, \ldots, y'_d) = 0$ for all $F \in P$. The reason is that we know that $GF \in (F_1, \ldots, F_h)$, and so

$$G(y'_1, \ldots, y'_d)F(y'_1, \ldots, y'_d) = 0$$

in the domain $\widehat{A}$. But

$$G(y'_1, \ldots, y'_d) \equiv G(s_1, \ldots, s_d) \bmod m^N\widehat{A},$$

and since $G(s_1, \ldots, s_d) \notin m^N\widehat{A}$, it follows that $G(y'_1, \ldots, y'_d) \notin m^n\widehat{A}$, and, in particular, $G(y'_1, \ldots, y'_d) \neq 0$. Therefore, $F(y'_1, \ldots, y'_d) = 0$.

We shall soon see that we can assume that some $h \times h$ minor of $(\dfrac{\partial F_j}{\partial Y_i})$ is not contained in P, and in the DVR case we shall show by enlarging S so that $\widehat{A}/S$ is torsion-free over V that we may even assume that the image of some minor in $\widehat{A}$ is not divisible by t.

We shall also need the following generalization of the implicit function theorem characterization of Henselian local rings:

Lemma (Tougeron's implicit function theorem). *Let (R, m) be a Henselian quasilocal ring and let $F_1, \ldots, F_h \in R[Y_1, \ldots, Y_d]$. Let $\mathfrak{A} \subseteq m$ be any ideal. Let*

$$\delta = \delta(Y) = \det\Big(\frac{\partial F_j}{\partial Y_i}\Big)$$

be an $h \times h$ minor of the Jacobian matrix obtained by choosing h of the variables (equivalently, h rows of the Jacobian matrix).

Suppose that we can find elements $y'_1, \ldots, y'_d \in R$ such that for $1 \leq j \leq h$,

$$F_j(y') \equiv 0 \bmod \delta(y')^2\mathfrak{A}.$$

Then there exist $y_1, \ldots, y_d \in R$ such that for $1 \leq j \leq h$,

$$F_j(y) = 0 \text{ and } y \equiv y' \bmod \delta(y')\mathfrak{A}.$$

This statement looks a bit technical, but notice that if $d = h$, $\mathfrak{A} = m$, and $\delta(y')$ is a unit, this is precisely the implicit function theorem characterization of Henselian rings.

Lecture of March 19, 2010

We shall prove a generalized version of the theorem we stated last time, which is given below, but before doing so we want to make a comment about a strengthening of the usual implicit function theorem that requires no effort to prove.

Let (R, m) be a Henselian quasilocal ring and let $\mathfrak{A} \subseteq m$ be a proper ideal of R. Suppose that one has a system of n equations in n unknowns $X_1, \ldots, X_n$, say $F_j(X) = 0$, $1 \leq j \leq n$. Suppose that one has a solution of these equations, say $\overline{y}_1, \ldots, \overline{y}_n$ in $R/\mathfrak{A}$, and also suppose that the image of the Jacobian determinant

$$\det\Big(\frac{\partial F_j}{\partial X_i}\Big)$$

evaluated at $(\overline{y}_1, \ldots, \overline{y}_n)$ is an invertible element of $R/\mathfrak{A}$. Then the equations have a solution $y_1, \ldots, y_n$ in R, and for all j, y_j is congruent to $\overline{y}_j$ mod $\mathfrak{A}$. The point here is that the solution mod $\mathfrak{A}$ obviously gives a solution mod m, and so the usual implicit function theorem characterization gives a unique solution $(y_1, \ldots, y_n)$ in R lifting the given solution. But the usual implicit function theorem also tells us that the solution in $R/\mathfrak{A}$ is unique (given what it becomes mod m), and so the images of the y_j in $R/\mathfrak{A}$ must be the $\overline{y}_j$. $\square$

Theorem (Tougeron's implicit function theorem). *Let (R, m) be a Henselian quasi-local ring and let $F_1, \ldots, F_h \in R[Y_1, \ldots, Y_d]$. Let $\mathfrak{A} \subseteq m$ be any ideal. Let $\mathcal{J} = \mathcal{J}(Y)$ denote the the $h \times d$ matrix $\big(\partial F_i/\partial Y_j\big)$, which is the transpose of the Jacobian matrix. Let $y'_1, \ldots, y'_d \in R$. Let $\Delta(y')$ denote an ideal of R that annihilates the cokernel of the linear map $R^d \to R^h$ with matrix $\mathcal{J}(y')$, and suppose that*

$$F_j(y') \equiv 0 \bmod \Delta(y')^2\mathfrak{A}.$$

Then there are elements $y_1, \ldots, y_d \in R$ such that

$$F_j(y) = 0,\ 1 \leq j \leq h, \text{ and } y \equiv y' \bmod \Delta(y')\mathfrak{A}.$$

Proof. Let $\delta_1, \ldots, \delta_\nu$ generate $\Delta(y')$. Let e_j be a column of the size h identity matrix. Then

$$\delta_i e_j = \mathcal{J}(y')\rho_j^{(i)}$$

for some $\rho_j^{(i)}$. The $\rho_j^{(i)}$ give the columns of a $d \times h$ matrix M_i such that

$$\mathcal{J}(y')M_i = \delta_i \mathbf{1}.$$

Every $F_k(y')$ has the form $\sum_{i,j} \delta_i\delta_j\alpha_{ijk}$ for suitable $\alpha_{ijk} \in \mathfrak{A}$. We shall write α_{ij} for the vector $(\alpha_{ij1}, \ldots, \alpha_{ijh})$.

We seek values for variables Z_{ij} in $\mathfrak{A}$ such that

$$F_k(y' + \sum_{i=1}^{\nu} \delta_i Z_i) = 0$$

where Z_i is the vector $(Z_{i1}, \ldots, Z_{id})$. We write F for $(F_1, \ldots, F_h)$. By Taylor's formula, the equations become

$$F(y') + \mathcal{J}(y') \sum_i \delta_i Z_i + \sum_{ij} \delta_i\delta_j H_{ij}(Z) = 0$$

where the $H_{ij}(Z)$ are vectors of polynomials in the variables Z all of whose terms are degree two and higher.

Using that $F(y') = \sum_{ij} \delta_i\delta_j\alpha_{ij}$ we can write this as

$$\mathcal{J}(y') \sum_i \delta_i Z_i + \sum_{ij} \delta_i\delta_j \big(H_{ij}(Z) + \alpha_{ij}\big) = 0$$

or, since $\delta_j \mathbf{1} = \mathcal{J}(y')M_j$,

$$\sum_i \delta_i \mathcal{J}(y')Z_i + \sum_i \left(\delta_i J(y') \sum_j M_j \big(H_{ij}(Z) + \alpha_{ij}\big)\right) = 0$$

or

$$\sum_i \delta_i \mathcal{J}(y')\Big(Z_i + \sum_j M_j\big(H_{ij}(Z) + \alpha_{ij}\big)\Big) = 0$$

This, it suffices to find Z_i with entries in $\mathfrak{A}$ such that

$$Z_i + \sum_j M_j\big(H_{ij}(Z) + \alpha_{ij}\big) = 0.$$

These are vector equations: there are hd equations in hd unknowns. Mod m, the Jacobian matrix with respect to the Z_{ij}, evaluated at $Z_{ij} = 0$, is the identity, since the H_{ij} have only terms of degree 2 or more in the Z_{ij}. Since $Z_{ij} = 0$ is a solution mod $\mathfrak{A}$, by the remarks preceding the statement of the theorem we get a solution in R such that the z_{ij} are in $\mathfrak{A}$. $\square$

We next want to see that in the context of our continuing proof of the Artin approximation theorem, we may assume that one of the minors of the Jacobian matrix has nonzero image in $\widehat{A}$. To see this, we make use of the theory of separable algebras.

Lecture of March 22, 2010

Proposition. *Let B be a domain that is an algebra over a field $\mathcal{K}$ and let $\mathcal{L}$ denote the fraction field of B. We assume that B has characteristic $p > 0$, since in characteristic zero B is always separable over $\mathcal{K}$. The following conditions are equivalent:*

(1) *B is separable over $\mathcal{K}$.*
(2) *$\mathcal{L}$ is separable over $\mathcal{K}$.*

Moreover, if B is finitely generated over $\mathcal{K}$ the following conditions are also equivalent:

(3) *$\mathcal{K}^{1/p} \otimes_{\mathcal{K}} \mathcal{L}$ is reduced.*
(4) *$\mathcal{L}$ has a separating transcendence basis over $\mathcal{K}$.*
(5) *For some element $b \in B - \{0\}$, B_b is smooth over $\mathcal{K}$.*
(6) *If B is presented as $\mathcal{K}[Y_1, \ldots, Y_d]_G/(F_1, \ldots, F_h)$, where the quotient has dimension $d - h$, then some $h \times h$ minor of $\big(\dfrac{\partial F_j}{\partial Y_i}\big)$ has nonzero image in B.*

Proof. For any field extension $\mathcal{K}'$ of $\mathcal{K}$, $\mathcal{K}' \otimes_{\mathcal{K}} B \subseteq \mathcal{K}' \otimes_{\mathcal{K}} \mathcal{L}$, and the latter is a localization of the former, so that the two rings are reduced or not alike. Thus, (1) $\Leftrightarrow$ (2) is clear. Moreover, (2) $\Rightarrow$ (3) is immediate from the definition of separability.

The proof that (3) $\Rightarrow$ (4) is similar to the argument given earlier for the case where $\mathcal{K}$ is perfect. Choose a transcendence basis $\underline{u} = u_1, \ldots, u_s$ so as to minimize the degree of $\mathcal{L}$ over $\mathcal{L}_0 = \mathcal{K}(\underline{u})^{\rm sep}$, where $^{\rm sep}$ indicates separable closure in $\mathcal{L}$. If $v \in \mathcal{L}$ is not in $\mathcal{L}_0$, let $G(u_1, \ldots, u_d, V) \in \mathcal{K}[u_1, \ldots, u_d, V]$ be its minimal polynomial over $\mathcal{K}(u_1, \ldots, u_s)$, with denominators efficiently cleared. This polynomial is irreducible. If some exponent on one of the variables, say u_i, is not divisible by p, we can use the u_j for $j \neq i$ and v as a transcendence basis $\underline{u}'$. Then $\mathcal{K}(\underline{u}')^{\rm sep}$ contains u_i, because $G(\underline{u}, v)$ gives a polynomial that u_i satisfies that is separable over $\mathcal{K}(\underline{u}')$. This implies that $\mathcal{L}_1 = \mathcal{K}(\underline{u}')^{\rm sep} \supseteq \mathcal{L}_0$. But

$v \in \mathcal{K}(\underline{u}')^{\text{sep}}$, and so $[\mathcal{L} : \mathcal{L}_1] < [\mathcal{L} : \mathcal{L}_0]$. Thus, all exponents on all variables are divisible by p (this must be true for V, since G is not separable in V). Since G is irreducible, not all of its coefficients are pth powers, or it will be a pth power itself. We can therefore form $H(V) \in \mathcal{K}^{1/p} \otimes_{\mathcal{K}} \mathcal{K}[u_1, \ldots, u_s, V]$ such that $H^p = G$, and at least one coefficient of H is in $\mathcal{K}^{1/p} - \mathcal{K}$. It follows that $H(v)^p = G(v) = 0$, and to complete the proof it will suffice to check that $H(v)$ itself is nonzero. Note that $\mathcal{K}(\underline{u})(v) \cong \mathcal{K}(\underline{u})[V]/\big(G(V)\big)$, and so $\mathcal{K}^{1/p} \otimes_{\mathcal{K}} \mathcal{K}(\underline{u})(v) \cong \mathcal{K}^{1/p}(\underline{u})[V]/\big(G(V)\big)$, and this contains $H(v)$ and is contained in $\mathcal{K}^{1/p} \otimes_{\mathcal{K}} \mathcal{L}$. It therefore suffices to check that $H(V)$ is not a multiple of $G(V)$ in $\mathcal{K}^{1/p}(\underline{u})[V]$, which is obvious since $H(V)^p = G(V)$.

If there is a separating transcendence basis, after replacing B by a suitable localization at one element we may assume that the separating transcendence basis $\underline{u}$ is in B. We may then choose a primitive element v for the finite separable algebraic field extension $\mathcal{K}(\underline{u}) \subseteq \mathcal{L}$, and we may similarly assume that this element is in B. After inverting one more element, we may assume the extension is generated over a localization $\mathcal{K}[\underline{u}]_g$ by v, where v is a simple root of a monic polynomial $f(V)$ over $\mathcal{K}(\underline{u})$ whose coefficients are actually in $\mathcal{K}[\underline{u}]_g$. Inverting the value of f' makes this extension étale over a localization at one element of a polynomial ring, and, therefore, smooth.

But (5) and (6) are equivalent by the Jacobian criterion for smoothness: if a minor is nonzero we may invert it to achieve smoothness, while if the localization is smooth some $h \times h$ minor is invertible and, therefore, nonzero.

Finally, smooth algebras are obviously separable, since they remain regular, and so reduced, after any finite extension of the base field, so that (5) $\Rightarrow$ (2). $\square$

We now return to the problem of proving the Artin Approximation Theorem. Let $\delta(x, Y)$ be a nonvanishing minor of the Jacobian matrix, which we assume, by renumbering, comes from the first h rows. If the base V is a DVR we also assume for the moment that the image of $\delta(x, Y)$ in $\widehat{A}$ is not divisible by t. We will need to justify this assertion later.

Let $R = A^{\text{h}}$ and $\mathfrak{A} = m^N$ in the Tougeron implicit function theorem. It follows that in order to complete the proof of the Artin Approximation Theorem it suffices to show that given a finitely generated T-subalgebra $S = T[s_1, \ldots, s_d]$ of $\widehat{A}$ and

$$F_1, \ldots, F_h \in T[Y_1, \ldots, Y_d]$$

generating $PT[Y_1, \ldots, Y_d]_P$, where P is the prime ideal of relations on the $s_1, \ldots, s_d$, then for every positive integer N there exists $y' = y'_1, \ldots, y'_d \in A^{\text{h}}$ such that

$$(*) \qquad y' \equiv s \bmod m^N \widehat{A}$$

and

$$(**) \qquad F_j(y') \equiv 0 \bmod \delta^2(x, y') m^N.$$

The Tougeron Implicit Function Theorem enables us to pass from the solution of the equations mod $\delta^2(x, y')m^N$ to an "honest" solution. The next idea is this: we prefer to worry about a solution mod $\delta^2(x, y')$ and not about the factor m^N, which can be handled automatically by a trick.

The following Lemma permits this reduction:

Lemma. *Suppose that* $V[x_1, \ldots, x_\nu]^{\mathrm{h}}_{(t,x)}$ *is an approximation ring for* $\nu < n$. *Suppose that we have elements* $g, F_1, \ldots, F_h$ *and* $s_1, \ldots, s_d \in \widehat{A}$ *such that* t *does not divide* $g(x,s)$ *in* $\widehat{A}$ *while* $g(x,s)$ *divides* $F_j(x,s)$ *in* $\widehat{A}$ *for* $1 \leq j \leq h$.

Then for every positive integer N *there exists* $\underline{y}_N = y_{1N}, \ldots, y_{dN} \in (A^{\mathrm{h}})^d$ *such that* $F_j(x, \underline{y}_N)$ *is divisible by* $g(x, \underline{y}_N)$ *for all* j *and* $s \equiv \underline{y}_N$ *mod* $m^N \widehat{A}$.

By applying this with $g = \delta(x, Y)^2$ for larger and larger values of N, we can get the conclusions $(*)$ and $(**)$ we need to complete the proof of the Theorem. Of course, we still need to prove the Lemma, and for that we shall need the Weierstrass preparation theorem.

Lecture of March 24, 2010

We retain our earlier notations: (V, tV, K) is either a DVR or field (in the latter case, $V = K$ and $t = 0$), $T = V[x_1, \ldots, x_n]$, $A = T_{(t,x_1,\ldots,x_n)}$, $s_1, \ldots, s_d \in \widehat{A}$, $S = T[s_1, \ldots, s_d] \subseteq \widehat{A}$, P is the kernel of the map

$$\phi : T[Y] = T[Y_1, \ldots, Y_d] \twoheadrightarrow S \subseteq \widehat{A}$$

such that $Y_i \mapsto s_i$ for all i, $1 \leq i \leq d$, $F_1, \ldots, F_h \in T[Y]$ are minimal generators of PT_P, $\delta(x,Y)$ is an $h \times h$ minor of the Jacobian matrix $\left(\frac{\partial F_j}{\partial Y_i}\right)$ whose image in $\widehat{A}$ is not in $t\widehat{A}$. Let $R = A^{\mathrm{h}}$ and $\mathfrak{A} = m^N$ in the Tougeron Implicit Function Theorem. Then the Theorem shows that in order to complete the proof of the Artin Approximation Theorem, it suffices to prove that for every positive integer N there exists $y' = y'_1, \ldots, y'_d \in A^{\mathrm{h}}$ such that

$$(*) \qquad y' \equiv s \bmod m^N \widehat{A}$$

and

$$(**) \qquad F_j(y') \equiv 0 \bmod \delta^2(x,y') m^N.$$

The reason is that the Tougeron Implicit Function Theorem enables us to pass from the solution of the equations $F_j \equiv 0 \bmod \delta^2(x,y')m^N$ to an "honest" solution of the equations $F_j = 0$. The next idea is this: we prefer to worry about a solution mod $\delta^2(x,y')$ and not to worry about the factor m^N, which can be handled automatically by a trick.

The following Lemma permits this reduction:

Key Lemma. *Suppose that* $V[x_1, \ldots, x_\nu]^{\mathrm{h}}_{(t,x)}$ *is an approximation ring for* $\nu < n$. *Suppose that we have elements* $g, F_1, \ldots, F_h$ *and* $s_1, \ldots, s_d \in \widehat{A}$ *such that* t *does not divide* $g(x,s)$ *in* $\widehat{A}$ *while* $g(x,s)$ *divides* $F_j(x,s)$ *in* $\widehat{A}$ *for* $1 \leq j \leq h$.

Then for every positive integer N *there exists* $\underline{y}_N = y_{1N}, \ldots, y_{dN} \in (A^{\mathrm{h}})^d$ *such that* $F_j(x, \underline{y}_N)$ *is divisible by* $g(x, \underline{y}_N)$ *for all* j *and* $s \equiv \underline{y}_N$ *mod* $m^N \widehat{A}$.

We postpone the proof for a while. We first want to see why this Key Lemma enables us to prove the theorem.

Let $\widehat{m} = m\widehat{A}$ and for $u \in \widehat{A} - \{0\}$ let $\operatorname{ord}(u)$ denote the largest integer b such that $u \in \widehat{m}^b$, i.e., $u \in \widehat{m}^b - \widehat{m}^{b+1}$. Because the associated graded ring $\operatorname{gr}_{\widehat{m}}\widehat{A}$ is a polynomial ring, and, in particular, a domain, we have that $\operatorname{ord}(uv) = \operatorname{ord}(u) + \operatorname{ord}(v)$ for $u, v \in \widehat{A} - \{0\}$. Note that these remarks apply to any regular local ring, so that we have corresponding notions of order in A and A^{h}. The set of powers of the maximal to which an element of a regular local ring belongs does not change when we pass from the local ring to its completion. Thus, the order of an element is not affected by whether we think of it as being in A, A^{h}, or $\widehat{A}$.

Let $\operatorname{ord}\big(g(x,s)\big) = N_0$. Then for all $N > N_0$, $g(x, \underline{y}_N) \equiv g(x,s) \bmod m^N\widehat{A}$, from which it follows that for all $N > N_0$, $\operatorname{ord}\big(g(x,\underline{y}_N)\big) = N_0$. Since $F_j(x,\, s) = 0$ and $\underline{y}_N \equiv s \bmod m^N\widehat{A}$, we have that for all j, and all N,

$$F_j(x,\underline{y}_N) \in m^N\widehat{A} \cap A^{\mathrm{h}} = m^N A^{\mathrm{h}}.$$

But then for all j and all $N > 0$,

$$F_j(x,\underline{y}_{N+N_0}) \in g(x,\underline{y}_{N+N_0})A^{\mathrm{h}} \cap m^{N+N_0}A^{\mathrm{h}} \subseteq g(x,\underline{y}_N)m^N A^{\mathrm{h}},$$

as required, for an element of order smaller than N cannot multiply an element of order N_0 into $m^{N+N_0}A^{\mathrm{h}}$. $\square$

We shall soon return to the proof of the Key Lemma. In that proof, we shall want to use the Weierstrass Preparation Theorem to keep track of divisibility by g. It will be helpful if g is a regular element in x_n. We can use the following result to arrange this.

Lemma. *Let (V, tV, K) be a DVR or a field, so that we allow the possibility that $t = 0$ and $V = K$. Let n be a positive integer, and let $g \in V[[x_1, \ldots, x_n]]$, the formal power series ring. Suppose that $g \notin (t)$. Then there exist positive integers $b_1, \ldots, b_{n-1}$ such that the continuous V-automorphism mapping $x_i \mapsto x_i + x_n^{b_i}$, $1 \le i \le n-1$, $x_n \mapsto x_n$ takes g to an element that is regular in x_n, i.e., that is not in the ideal $(t, x_1, \ldots, x_{n-1})$.*

Proof. In proving this result we may work mod (t) without loss of generality. Therefore, we assume that $t = 0$, i.e., that $V = K$ in the rest of the argument. Our hypothesis on g becomes that g is a nonzero element of $K[[x_1, \ldots, x_n]]$.

We use induction on n. If $n = 1$ it is obvious from the fact that $g \neq 0$ that it is regular in x_1. Note, that quite generally, the condition that we need on $b_1, \ldots, b_{n-1}$ is simply that $g(x_n^{b_1}, \ldots, x_n^{b_{n-1}}, x_n) \neq 0$, for this is what the image of g under the automorphism becomes mod $(x_1, \ldots, x_{n-1})$.

If $n = 2$ we seek b such that $g(x_2^b, x_2) \neq 0$. This is equivalent to the condition that g not be divisible by $x_1 - x_2^b$. The elements $x_1 - x_2^b$ for $b = 1, 2, 3, \ldots$ are prime in the UFD $K[[x_1, x_2]]$, and no two are associates. If g is divisible by all of the elements $x_1 - x_2^b$ for $1 \le b \le B$, then it is divisible by the product of those elements, and is therefore in $(x_1, x_2)^B$. Since $g \neq 0$, it cannot be in $(x_1, x_2)^B$ for all B.

If $n \geq 3$, we may write $g = \sum_{j=i}^{\infty} \gamma_i x_n^j$ where all of the $\gamma_j \in K[[x_1, \ldots, x_{n-1}]]$ and $\gamma_i \neq 0$. By the induction hypothesis we may choose $b_1, \ldots, b_{n-2}$ such that

$$\gamma_i(x_{n-1}^{b_1}, \ldots, x_{n-1}^{b_n-2}, x_{n-1}) \neq 0.$$

Then $g(x_{n-1}^{b_1}, \ldots, x_{n-1}^{b_n-2}, x_{n-1}, x_n)$ is a nonzero formal power series in two variables, and by the case $n = 2$ we can substitute $x_{n-1} = x_n^b$ for some positive integer b and get a nonzero result. $\square$

Notice that an automorphism of $\widehat{V}[[x_1, \ldots, x_n]] = \widehat{A}$ of the form described in the preceding result, as well as its inverse, stabilize A, and hence also induce mutually inverse automorphisms of A^{h}. We henceforth assume that $g = g(x, s)$ is regular in x_n, and we let $\alpha = \alpha(x_n)$ denote its unique monic associate, so that

$$\alpha(x_n) = x_n^q + u_{q-1}x_n^{q-1} + \cdots + u_0$$

where the u_i are nonunits of $C = \widehat{V}[[x_1, \ldots, x_{n-1}]]$.

We want to convert our divisibility problem into an equational problem over

$$D = V[x_1, \ldots, x_{n-1}]^{\mathrm{h}}_{(t, x_1, \ldots, x_{n-1})},$$

which we know from the induction hypothesis is an approximation ring.

Towards this end, we introduce dq new variables $Z_{i,\nu}$ and substitute

$$Z_i = \sum_{\nu=0}^{q-1} Z_{i,\nu} x_n^{\nu}$$

for the Y_i in the $F_j(x, Y)$ and in $g(x, Y)$ to obtain $F_j(x, Z)$ and $g(x, Z)$. We also introduce new indeterminates $U_0, \ldots, U_{q-1}$ and a variable polynomial H in x_n with these coefficients, so that

$$H(x_n) = H(U, x_n) = x_n^q + \sum_{j=0}^{q-1} U_j x_n^j.$$

Let

$$\mathcal{T} = V[x_1, \ldots, x_{n-1}, Z_{i,\nu}, U_\nu].$$

Working in the polynomial ring $\mathcal{T}[x_n]$ we can formally divide $g(x, Z)$ and $F_j(x, Z)$ by $H(x_n)$ to obtain

$$(*) \qquad g(x, Z) = H(x_n)Q_0 + \sum_{\nu=0}^{q-1} W_{0,\nu} x_n^{\nu}$$

$$(**) \qquad F_j(x, Z) = H(x_n)Q_j + \sum_{\nu=0}^{q-1} W_{j,\nu} x_n^{\nu}$$

where the $Q_j \in \mathcal{T}[x_n]$ and the $W_{j,\nu} \in \mathcal{T}$ do *not* involve the variable x_n for all $j \geq 0$.

By the Weierstrass Preparation Theorem we can divide every s_i by $\alpha(x_n)$, the unique monic associate of $g = g(x, s)$, to obtain:

$$(\#) \qquad s_i = \alpha(x_n)\theta_i + \sum_{\nu=0}^{q-1} z_{i,\nu} x_n^\nu,$$

where $\theta_i \in \widehat{A}$ and the $z_{i,\nu} \in C$. We define

$$z_i = \sum_{\nu=0}^{q-1} z_{i,\nu} x_n^\nu.$$

Lecture of March 26, 2010

Since $s_i \equiv z_i \bmod \alpha(x_n)$, it follows that $g(x,\, z) \equiv g(x,\, s) \bmod \alpha(x_n)$ and that $F_j(x,\, s) \equiv F_j(x,\, z) \bmod \alpha(x_n)$ for all j. Since $\alpha(x_n)$ and $g(x,\, s)$ are associates, we have that $\alpha(x_n)$ divides $g(x,\, z)$. Since the hypothesis of the Key Lemma tells us that $g(x,\, s)$ divides every $F_j(x,\, s)$, we have that $\alpha(x_n)$ divides every $F_j(x,\, z)$.

Recall that

$$\alpha(x_n) = x_n^q + u_{q-1}x_n^{q-1} + \cdots + u_0.$$

We can now substitute the $z_{i,\nu}$ for the $Z_{i,\nu}$ and the u_ν for the U_ν in $(*)$ and $(**)$ above. The equations that result show that the elements

$$\sum_{\nu=0}^{q-1} W_{j,\nu}(x, z, u) x_n^\nu$$

are the remainders in the Weierstrass Preparation Theorem when $g(x,\, z)$ and the $F_j(x,\, z)$ are divided by $\alpha(x_n)$: note that the variable x_n does not occur in $W_{j,\nu}$. But the results of the preceding paragraph show that these remainders are 0. It follows that

$$W_{j,\nu}(x,\, z,\, u) = 0, \quad 0 \leq j \leq h, \quad 0 \leq \nu \leq q-1.$$

Put differently, the system of $(h+1)q$ polynomial equations

$$W_{j,\nu}(x,\, Z,\, U) = 0, \quad 0 \leq j \leq h, \quad 0 \leq \nu \leq q-1$$

in the variables Z, U, which has coefficients in

$$V[x_1,\, \ldots\, , x_{n-1}] \subseteq D = V[x_1,\, \ldots\, , x_{n-1}]^{\mathrm{h}}_{(t, x_1, \ldots, x_{n-1})},$$

has the solution $Z = z$, $U = u$ in $\widehat{D} = C$.

The induction hypothesis then guarantees that for every positive integer N there is a solution of these equations $Z = \underline{z}_N$, $U = \underline{u}_N$ in D which is congruent to z, u modulo $(t, x_1, \ldots, x_{n-1})^N C$. We shall now use this solution to construct the elements $\underline{y}_N$ needed to prove the Key Lemma.

For all i choose any $\theta_{i,N} \in A^{\mathrm{h}}$ such that $\theta_{i,N} \equiv \theta_i \bmod m^N \widehat{A}$. Let

$$\underline{u}_N = u_{0,N}, \ldots, u_{q-1,N}$$

and let the individual values of the $\underline{z}_N$ be denoted $z_{i,\nu,N}$. Define

$$\alpha_N(x_n) = H(\underline{u}_N, x_n) = x_n^q + u_{q-1,N} x_n^{q-1} + \cdots + u_{0,N},$$

while letting

$$z_{i,N} = \sum_{\nu=0}^{q-1} z_{i,\nu,N} x_n^{\nu}$$

and

$$y_{i,N} = \alpha_N(x_n)\theta_{i,N} + z_{i,N}.$$

Modulo $m^N \widehat{A}$ we know that $\underline{u}_N \equiv u$, and it follows that modulo $m^N \widehat{A}$ we also have that $\alpha_N(x_n) \equiv \alpha(x_n)$, that $z_{i,N} \equiv z_i$ and that $y_{i,N} \equiv s_i$. To complete the proof of the Key Lemma, it will suffice to show that $g(x, \underline{y}_N)$ divides $F_j(x, \underline{y}_N)$ for all j.

Since the $z_{i,\nu,N}$ and the $\underline{u}_N$ satisfy the equations

$$W_{j,\nu}(x, Z, U) = 0, \quad 0 \le j \le h, \quad 0 \le \nu \le q-1$$

when we substitute in $(*)$ and $(**)$ we find that $\alpha_N(x_n)$ divides $g(x, \underline{z}_N)$ and that it also divides every $F_j(x, \underline{z}_N)$. From the way we defined $y_{i,N}$ we also have that $z_{i,N} \equiv y_{i,N}$ modulo $\alpha_N(x_n)$. It follows as well that $\alpha_N(x_n)$ divides $g(x, \underline{y}_N)$ and every $F_j(x, \underline{y}_N)$. We can complete the argument by showing that $\alpha_N(x_n)$ is the unique monic associate of $g(x, y_N)$ for all sufficiently large N.

The point is that if N is large then the fact that

$$g(x, \underline{y}_N) \equiv g(x, s) \bmod m^N \widehat{A}$$

implies that $g(x, \underline{y}_N)$ is regular of order q in x_n, and so it has an associate $\alpha'(x_n)$ that is monic of degree q as a polynomial in x_n and has all coefficients on lower powers of x_n in the maximal ideal of C. Since $\alpha_N(x_n)$ divides $\alpha'(x_n)$ in $\widehat{A}$, since they are both monic of the same degree as polynomials in x_n, and since they both have lower degree coefficients in the maximal ideal of C, they must be equal. $\square$

This completes not only the proof of the Key Lemma, but finishes the proof of the Artin Approximation Theorem when $V = K$ is a field. When the base ring is a DVR, however,

we have more work to do. In particular, we need to justify the assumption that we can reduce to the case where $\delta(x, s)$ is not in $t\widehat{A}$.

In order to make this reduction we need to study an idea of Néron which Artin refers to as "Néron's p-desingularization." (In Artin's paper, p is the generator of the maximal ideal of the DVR, which we are calling t here.) However, we will simply use the term *Néron desingularization*.

Lecture of March 29, 2010

We now focus on the situation where the base is a discrete valuation ring (V, tV, K), so that we are no longer allowing the possibility that $t = 0$.

Recall that $T = V[x_1, \ldots, x_n]$, a polynomial ring, and that $A = T_{(t,\underline{x})}$, where $\underline{x}$ denotes $x_1, \ldots, x_n$. Recall also that $S = T[s_1, \ldots, s_d] \subseteq \widehat{A}$ is a finitely generated T-subalgebra of $\widehat{A}$. Consider the T-algebra map $T[Y_1, \ldots, Y_d] \twoheadrightarrow S \subseteq \widehat{A}$ such that $y_i \mapsto s_i$, $1 \leq i \leq d$. Let P be the kernel of this map, and let h be the height of P, as before. However, we shall now keep track of full set of generators of P, $F_1, \ldots, F_k$. (Previously, we were working with $F_1, \ldots, F_h$ such that $PT[Y_1, \ldots, Y_d]_P$ is generated by $F_1, \ldots, F_h$.)

Note that t is a prime element of $\widehat{A}$: in fact, $\widehat{A}/t\widehat{A} \cong K[[x_1, \ldots, x_n]]$. Let $\Lambda = \widehat{A}_{\mathcal{Q}}$ where $\mathcal{Q} = t\widehat{A}$, a DVR with maximal ideal $t\Lambda$. We let $\Omega' = \Lambda \otimes_S \Omega_{S/T}$.

Let $\mathcal{J}$ denote the image of the Jacobian matrix $\left(\dfrac{\partial F_j}{\partial Y_i}\right)$ mod P, which we view as a $d \times k$ matrix over S. Note that the cokernel of $\mathcal{J}$ is $\Omega_{S/T}$. We shall write $\mathcal{J}'$ for $\mathcal{J}$ viewed as a matrix or linear transformation over Λ. Thus, the cokernel of $\mathcal{J}'$ may be identified with the module $\Lambda \otimes_S \Omega_{S/T}$.

Note that for any finitely presented module M over any ring R, we can define *Fitting invariants*: the ith Fitting invariant of M is the ideal $I_{d-i}(J)$ where J is the $d \times k$ matrix of the map of free modules in a presentation $R^k \to R^d \twoheadrightarrow M \to 0$.

Fitting's Lemma. *The ith Fitting invariant as defined in the preceding paragraph is independent of the choice of finite presentation of M.*

Proof. To prove this, we first check that given a map $R^d \twoheadrightarrow M$ it is independent of the choice of finitely many column vectors spanning the kernel. Given two choices, we may compare each with the union. This, it suffices to see that the ideal does not change when one set of relations is included in the other, i.e., when some set of columns of the matrix, without loss of generality these may be taken to be the last s, are linear combinations of the preceding r columns. By subtracting linear combinations of the first r columns from the last s (we know this does not change the ideals of minors) we may assume that the last s columns are all 0, and the result is now clear.

It remains to check independence of the map $R^d \to M$, i.e., of the choice of generators for M. Again, we may compare each of two different sets of generators with their union, and so we reduce to the case where one set of generators is included in the other and then

to the case where there is one additional generator. We may assume that included among the relations is a relation expressing the additional generator, which we number last, as a linear combination of the others. This means that we may assume that the matrix with the additional generators present has a 1 in the last row, which we also assume, by permuting the columns, is in the last column. We can now perform elementary column operations, subtracting multiples of the last column from the others, until the last row consists of all zeros except for its final entry, so that the $(d+1) \times (k+1)$ matrix J_1 that we are considering has the block form $J_1 = \begin{pmatrix} J & C \\ 0 & 1 \end{pmatrix}$, where J is $d \times k$, 0 denotes a row of zeros of length k, C is a $d \times 1$ column, and 1 is the 1×1 identity matrix. Then J gives a matrix for the presentation using the first d generators. It is now straightforward to see that $I_{d+1-i}(J_1) = I_{d-i}(J)$. $\square$

We note that in the Lemma below, the ideal generated by the $h \times h$ minors of $\mathcal{J}$ is the $d-h$ th Fitting invariant of the module $\Lambda \otimes_\Omega$. The number $d-h$ does not depend on the presentation: it is the same as the dimension of $\mathrm{frac}\,(T) \otimes_T S$, which has the presentation $\mathrm{frac}\,(T)[Y_1, \ldots, Y_d]/(F_1, \ldots, F_k)$.

Lemma. *$\mathcal{J}$ has rank h. There is an $h \times h$ minor of $\mathcal{J}$ that is not divisible by t in $\widehat{A}$ (equivalently, in Λ) iff Ω' is torsion-free over Λ. More generally, the minimum order of a size h minor with respect to t is the length over Λ of the torsion submodule of Ω'.*

Proof. Let $\mathcal{F}$ be the fraction field of T, which is also the fraction field of A. Then $\mathcal{F} \to \mathcal{F} \otimes_A \widehat{A} = \mathcal{F} \otimes_T \widehat{A}$ is separable, and, hence, $\mathcal{F} \to \mathcal{F} \otimes_T S$ is separable. Note that $\mathcal{J}$ is also the Jacobian matrix for this extension, and that $\mathcal{F} \otimes_T S$ has dimension $d-h$. If we localize at one nonzero element to make this algebra smooth over $\mathcal{F}$ its dimension does not change, and then the determinantal rank of the Jacobian matrix must be h and, after localization, the size h minors must generate the unit ideal. Since S is a domain, we see that the rank is of $\mathcal{J}$ is exactly h.

The remaining statements follow from a general fact about matrices over a DVR, given in the next result.

Lemma. *Let M be any finitely generated module over a discrete valuation ring $(\Lambda, t\Lambda)$, and let J be the matrix of the map of free modules in a finite presentation of M. Suppose that J has rank h. Then the length of the torsion submodule of M is the same as the minimum order of an $h \times h$ minor of M, which is the same as the order of a generator of $I_h(M)$.*

Proof. The statements are unaffected by performing elementary row and column operations on M. This means that we may assume that J has the block form $\begin{pmatrix} J_0 & 0 \\ 0 & 0 \end{pmatrix}$ where M_0 is a diagonal matrix with diagonal entries $t^{a_1}, t^{a_2}, \ldots, t^{a_h}$. The only nonvanishing $h \times h$ minor is $t^{a_1 + \cdots + a_h}$, and $a_1 + \cdots + a_h$ is also the length of the torsion submodule $\Lambda/(t^{a_1}) \oplus \cdots \oplus \Lambda/(t^{a_h})$. $\square$

We want to note the following. Suppose that we have found a size h minor of $\mathcal{J}$ that is not zero. By, renumbering, we may assume that this minor occurs in the upper left hand corner of $\mathcal{J}$, so that it involves the partial derivatives of $F_1, \ldots, F_h$ with respect

to $Y_1, \ldots, Y_h$. We claim that it is then automatic that $(F_1, \ldots, F_h)T[Y_1, \ldots, Y_d]_P = PT[Y_1, \ldots, Y_d]_P$. Since $T - 0$ does not meet P, we are free to replace T by its fraction field $\mathcal{F}$ in considering this, i.e., we need only show that

$$(F_1, \ldots, F_h)\mathcal{F}[Y_1, \ldots, Y_d]_P = P\mathcal{F}[Y_1, \ldots, Y_d]_P.$$

Let $C = \mathcal{F}[Y_1, \ldots, Y_d]_P/(F_1, \ldots, F_h)$. Since there is a maximal minor of the Jacobian matrix that is invertible, $\Omega_{C/\mathcal{F}} = 0$, and so it is an C is unramified and essentially finitely presented over $\mathcal{F}$. Hence, it is a finite product of finite separable extensions of $\mathcal{F}$. But it is also local. Therefore C is a field. Since C maps onto $\mathcal{F}[Y_1, \ldots, Y_d]_P/P\mathcal{F}[Y_1, \ldots, Y_d]_P$, they are equal, and we must have

$$(F_1, \ldots, F_h)T[Y_1, \ldots, Y_d]_P = PT[Y_1, \ldots, Y_d]_P,$$

as claimed. □

We denote by ℓ_S the length of torsion-submodule of $\Lambda \otimes \Omega_{S/T}$, which is also the minimum order with respect to t of any size h minor of J'.

Theorem. *Let $Q = t\widehat{A} \cap S = t\Lambda_0 \cap S$, and let $S' = S[q/t : q \in Q]$. Then $\ell_{S'} \leq \ell_S$, and the inequality is strict unless $\ell_S = 0$.*

We put off the proof of this result momentarily. Notice that one we know this we may iterate the process of replacing S by S' at most ℓ_S times until we reach a finitely genrated T-subalgebra S^* of $\widehat{A}$ that contains S but such that $\ell_{S^*} = 0$. For this algebra, there will be a size h minor that will not be divisible by t. This enables us to carry through the inductive step in the proof the Artin Approximation Theorem.

However, before we give the proof of this Theorem, we want to observe that the same result also enables us to give a proof for the base case for the induction when V is a DVR and not a field!

To see this, note that in the base case $n = 0$: there are no variables x_i. $T = A = V$, and $\widehat{A} = \widehat{V}$. We may assume that we have $S = V[s_1, \ldots, s_d]$ such that $\ell_S = 0$, and we want to map S to V^{h} so that the residue class of every element of S is preserved mod (t^N). Some size h minor of $\mathcal{J}$ is an element of S not divisible by t, that is, it has an inverse in $\widehat{V}$. We may adjoin this inverse to S: constructing the algebra map we need only gets harder. But now we have that S is smooth over V, by the Jacobian criterion for smoothness. Let Q be the ideal $t\widehat{V} \cap S$. By the structure theorem for smooth morphism, locally S is an étale extension of a polynomial ring, and so S_Q is a pointed étale extension of a localization of a polynomial subring, $V[u_1, \ldots, u_r]_{Q'}$. The inclusion $S \subseteq \widehat{V}$ gives us a map of this localization in $\widehat{V}$, and the u_j have images in $\widehat{V}$. For every j, pick an element of $v_j \in V^{\mathrm{h}}$ such that $u_j \equiv v_j \bmod (t^N)$. Now map $V[u_1, \ldots, u_r] \to V^{\mathrm{h}}$ sending $u_j \mapsto v_j$ for all j. This extends to a map $V[u_1, \ldots, u_r]_{Q'} \to V^{\mathrm{h}}$. Since V^{h} is Henselian, this map extends to the pointed étale extension S_Q, and we have the required map $S \to S_Q \to V^{\mathrm{h}}$. □

This means that after we prove the Theorem stated above, we will have completed the proof of the Artin Approximation Theorem in all cases.

Lecture of March 31, 2010

Before proving the Theorem stated in the previous lecture, we introduce some ideas that will simplify the problem. We replace T by its localization at tT, which we call Λ_0. Then $(\Lambda_0, t\Lambda_0, L_0)$ is a DVR, and we have a local map $\Lambda_0 \to \Lambda$: we use L for the residue class field of Λ. We replace S by $\Lambda_0 \otimes_T S$, which is a localization of S and a subring of Λ. Note that this ring is $\Lambda_0[s_1, \ldots, s_d]$ and has the presentation

$$\Lambda_0[Y_1, \ldots, Y_d]/(F_1, \ldots, F_k).$$

The image of Jacobian matrix $\mathcal{J}$ is literally the same, although we now think of the entries as being in $\Lambda_0 \otimes_T S$, the "new" S, which we temporarily denote as S°. Again, we may use $\mathcal{J}'$ for the same matrix over Λ. We write $\mathcal{F}$ and $\mathcal{G}$ for the fraction fields of Λ_0 and Λ respectively.

The theory of excellent rings implies that the field extensions $\mathcal{F} \to \mathcal{G}$ and $L_0 \to L$ are separable. For the new S° we again have an operation of enlargement: if $Q = t\Lambda \cap S^\circ$ we may adjoin all the elements q/t for $q \in Q$ to S°: we need only do this for generators of Q, and so this is still finitely generated over Λ_0. In fact, one has $(S')^\circ = (S^\circ)'$, since $S^\circ = W^{-1}S$ with $W = T - tT$, and t divides s/w in Λ iff t divides $s \in S$. Thus, $t\Lambda \cap S^\circ$ is the expansion of $t\Lambda \cap S$. In fact, it will be convenient in the remainder of the argument to generalize substantially further: for example, we may relax the condition that S be finitely generated over Λ_0 by allowing arbitrary localizations at multiplicative systems disjoint from Q, especially at $S - Q$ itself. We shall also relax the condition that the map $S \to \Lambda$ be injective.

Néron Desingularization

We therefore start over in a new, abstract situation which captures what we need from the original situation. Let $(\Lambda_0, t\Lambda_0, L_0) \hookrightarrow (\Lambda, t\Lambda, L)$ be a local injection of discrete valuation rings such that induced map of fraction fields $\mathcal{F} \to \mathcal{G}$ is separable, and $L_0 \to L$ is separable. Let S be a localization of a finitely generated Λ_0-algebra, torsion-free over Λ_0, and suppose that we have a map $\phi : S \to \Lambda$, but now, instead of assuming that $S \to \Lambda$ is injective, we assume that the kernel is a minimal prime $\mathfrak{q}$ of S such that $S_\mathfrak{q}$ is a field. Then $S_\mathfrak{q}$ is a subfield of $\mathcal{G}$ finitely generated over $\mathcal{F}$.

We define $\Omega'_S = \Lambda \otimes \Omega_{S/\Lambda_0}$. We let ℓ_S denote the length of the torsion-submodule of Ω'_S. If we represent S as $W^{-1}\Lambda_0[Y_1, \ldots, Y_d]/P$ and choose generators $F_1, \ldots, F_k$ for P in $\Lambda_0[Y_1, \ldots, Y_d]$, then if $\mathcal{J}'$ denotes the image of the Jacobian matrix $\left(\frac{\partial F_j}{\partial Y_i}\right)$ in Λ, we have that the rank of $\mathcal{J}'$ is the same as the height of the minimal prime of P which is the inverse image of $\mathfrak{q}$ in $W^{-1}\Lambda_0[Y_1, \ldots, Y_d]$. We denote this height by h and we let ℓ_S be the length of torsion submodule of Ω'_S. This length is the same as the minimum order with respect to t of any size h minor of $\mathcal{J}'$, where the minor is viewed as an element of Λ. By enlarging W we can get P itself to be prime, and we can do this while only localizing at elements not divisible by t. As earlier, we may let Q be the contraction of $t\Lambda$ to S and we may let

$S' = S[q/t : q \in Q] \subseteq S_t$, which is finitely generated over S. This algebra is called *Néron's blowing-up of* S. The constructions of both S' and ℓ_S from S commute with localization at a multiplicative system disjoint from Q. Note that we still have a map $S' \to \Lambda$: its value on q/t for $q \in Q$ is $\phi(q)/t$, which is an element of Λ because, by definition of Q, $\phi(q) \in t\Lambda$.

We can now state and, eventually, prove a result more general than the Theorem stated last time. Before proving this, we note that if the field L' is separable over the field L and $u_1, \ldots, u_d$ is a set of field generators, then a separating transcendence basis may be chosen from the elements $u_1, \ldots, u_d$. To see this, consider the proof of (3) $\Rightarrow$ (4) in the first Proposition in the Lecture Notes from March 22. Choose a transcendence basis from $u_1, \ldots, u_d$, say $u_1, \ldots, u_s$, so as to minimize $[L' : L(u_1, \ldots, u_s)^{\mathrm{sep}}]$. If

$$L' \neq L(u_1, \ldots, u_s)^{\mathrm{sep}},$$

choose an element

$$v \in L' - L(u_1, \ldots, u_s)^{\mathrm{sep}}$$

from among the elements $u_{s+1}, \ldots, u_d$. The rest of the argument producing a contradiction is the same.

Theorem. *With notation as above, so that* $L_0 \to L$ *and* $\mathcal{F} \to \mathcal{G}$ *are both separable,* $\ell_{S'} \leq \ell_S$*, with equality if and only if* $\ell_S = 0$*.*

Proof. We replace S by S_Q. Henceforth we may assume that (S, Q) is local, and that it is a localization of $\Lambda_0[s_1, \ldots, s_d]$. Note that we have a presentation of S of the form

$$S \cong W^{-1}\Lambda_0[Y_1, \ldots, Y_d]/(F_1, \ldots, F_k).$$

We know that at least one size h minor of $\mathcal{J}'$ has minimum order ℓ_S. We are free to make local étale extensions Λ_0^* of Λ_0 and Λ^* of Λ to enlarge their residue class fields (we shall say more about this below). This is done in such a way that we still have a map $\Lambda_0^* \to \Lambda^*$. S is replaced by $\Lambda_0^* \otimes_{\Lambda_0} S$. The details of how to do this will be given in the next lecture.

After enlarging the residue class fields, if necessary, we can make an invertible linear change of variables among $Y_1, \ldots, Y_d$ over Λ_0 so that every h rows of the new $\mathcal{J}'$ will have a size h minor of order ℓ_S. Assuming this for the moment, we renumber the Y_j so that the images of $Y_1, \ldots, Y_\tau$ are a separating transcendence basis for S/Q over L_0: the images of Y_j are field generators, and so we can do this by the remarks prior to the statement of the Theorem. We now replace Λ_0 by

$$\Lambda_1 = \Lambda_0[s_1, \ldots, s_\tau]_{(t)}.$$

We need to understand what happens to ℓ_S and $\ell_{S'}$ when we do this. We shall show that we can keep ℓ_S the same while $\ell_{S'}$ can only increase. Again, the details will be given in the next lecture. Next, we adjust the rings Λ_0 and Λ again so that Λ_0 contains representatives of all elements of S/Q, which is a now a finite separable algebraic extension of L_0. Once again, the details will be given in the next lecture.

Lecture of April 2, 2010

We next consider certain changes that we can make without affecting the problem.

We can arrange for a finite separable extension of the residue class field of Λ_0: at the same time, we enlarge Λ. Any such separable extension is generated by a single primitive element θ. We may choose a monic minimal polynomial for θ over L_0: it will be a separable polynomial, and we then lift it to a monic polynomial, $f(z)$, of the same degree over Λ_0. Then $\Lambda_0^* = \Lambda_0[z]/\big(f(z)\big)$ is a module-finite étale extension of Λ_0. Mod (t) we get the desired extension of L_0. Because killing (t) produces a field, Λ_0^* is still a local ring and, in fact, a DVR with maximal ideal $t\Lambda_0^*$. However, this ring no longer maps to Λ. Consider $\Lambda_0^* \otimes_{\Lambda_0} \Lambda$, which is module-finite and étale over Λ: if we kill (t), we get $L[z]/(f)$, an étale extension of L which is necessarily a product of finite separable extensions of L. Thus, by localizing $\Lambda_0^* \otimes_{\Lambda_0} \Lambda$ at a minimal prime $\mathcal{Q}$ of t, we obtain a DVR, Λ^*, to which Λ_0^* maps, and its maximal ideal is still generated by t. Moreover, $S^* = \Lambda_0^* \otimes_{\Lambda_0} S$ maps to it as well, and we replace Λ_0, S, Λ and $S \to \Lambda$ by these. Note that $\mathcal{J}'$ does not change, although its entries are now considered in Λ^*, and the orders of its minors with respect to t don't change.

We also need to see that this process commutes with Néron's blowing-up. We are assuming that $S = S_Q$, so that S/Q is a field. Note that we might as well replace S^* by $S^*_{Q^*}$, where Q^* is the contraction of $t\Lambda^*$ to S^*. The key point is that the expansion of Q to $S^*_{Q^*}$ is $Q^*S^*_{Q^*}$. Thus, if $q_1, \ldots, q_k$ generate Q, their images generate $Q^*S^*_{Q^*}$, and so Néron's blowing-up of the latter is generated over it by the images of $q_1/t, \ldots, q_k/t$. To see this, it suffices to see that $S^*_{Q^*}/QS^*_{Q^*}$ is a field. But this ring is $(S^*/QS^*)_{Q^*}$, and $S^*/QS^* = \Lambda_0^* \otimes_{\Lambda_0} S/Q$, where S/Q is a field. This is an étale extension of S/Q, and so it is a finite product $\mathcal{F}_1 \times \cdots \times \mathcal{F}_j$ of finite separable algebraic field extensions of S/Q. Since $(S^*/QS^*)_{Q^*}$ is a local ring which is a localization of $S^*/QS^* \cong \mathcal{F}_1 \times \cdots \times \mathcal{F}_j$, it is isomorphic to some $\mathcal{F}_i$, and therefore is a field. It follows that $(S^*_{Q^*})' = (\Lambda_0^* \otimes_{\Lambda_0} S')_{Q^*}$. It then follows that the image of the Jacobian matrix for Néron's blowing-up after we enlarge the residue class field is the same as before, although it is now being considered in Λ^*. The smallest order of a minor with respect to t does not change, however, since $t^i\Lambda^* \cap \Lambda = t^i\Lambda$ for all i.

An invertible linear change of the variables $Y_1, \ldots, Y_d$ over Λ_0 produces a corresponding change in the Jacobian matrix. Suppose that for $1 \leq i \leq d$, we have that $Y_i = \sum_{k=1}^d \alpha_{ki} Y'_k$, where $\big(\alpha_{ki}\big)$ is an invertible matrix with entries in Λ_0. Then

$$dY_i = \sum_{k=1}^{d} \alpha_{ki} dY'_k,$$

and so

$$dF_j = \sum_{i=1}^{d} \frac{\partial F_j}{\partial Y_i} dY_i = \sum_{i=1}^{d} \Big(\frac{\partial F_j}{\partial Y_i} \sum_{k=1}^{d} \alpha_{ki} dY'_k\Big) = \sum_{k=1}^{d} \Big(\sum_{i=1}^{d} \alpha_{ki} \frac{\partial F_j}{\partial Y_i}\Big) dY'_k.$$

Thus, the new Jacobian matrix is $\big(\alpha_{ki}\big)\mathcal{J}$. We therefore see that an invertible linear change of variables over Λ_0 enables us to perform corresponding row operations on $\mathcal{J}$ and, hence, on $\mathcal{J}'$.

To see that we may assume that any h rows of $\mathcal{J}'$ have a size h minor of order ℓ_S, it suffices to prove the following:

Lemma. *Let $(\Lambda_0, t\Lambda_0, L_0) \subseteq (\Lambda, t\Lambda, L)$ be a local inclusion of discrete valuation rings. Suppose that the residue class field of L_0 is infinite. Let J be a $d \times k$ matrix over Λ of rank h such that the smallest order with respect to t of any size h minor is ℓ. Then one can perform elementary row operations on the matrix over Λ_0 such that any h distinct rows of the matrix have a size h minor of order ℓ.*

Proof. Note that column operations over Λ do not affect the order of the generator of the ideal of h size minors of a given set of h rows. Therefore, we may perform column operations over Λ and row operations over Λ_0 without affecting the issue. First permute rows and columns so that an element of least order is in the upper right hand corner of J. By multiplying the first column by a unit we may assume that the entry in the upper left corner is t^{a_1}. By performing elementary column operations over Λ we may assume that the other entries of the first row are 0. We now iterate this procedure, working with the submatrix obtained by deleting the first row and leftmost column. After h iterations we reach a matrix such that the $h \times h$ submatrix in the upper left corner is lower triangular with $t^{a_1}, \ldots, t^{a_h}$ on the diagonal, the entries to the right of these in the first h rows are 0, and each of the entries in the j th column below t^{a_j} is divisible by t^{a_j}, $1 \leq j \leq h$. It also follows that the entries in columns beyond the h th column and below the h th row must all be zero, or the rank will be larger than h.

We want to perform elementary row operations over Λ_0 to get every $h \times h$ minor of the first h columns to have order $a_1 + \cdots + a_h$ with respect to t. We factor t^{a_j} from the j th column for $1 \leq j \leq h$. We may drop all but the first h columns, since the other columns are 0. We thus obtain a matrix with h columns such that the submatrix formed from the first h rows is lower triangular, with 1 in each spot on the main diagonal. It will suffice to perform elementary row operations over Λ_0 so that all size h minors are units.

For this purpose we may work mod $t\Lambda_0$. Thus, we may view the given matrix as having entries in $L = \Lambda/t\Lambda$, and we need only select, for each of the last $d - h$ rows, an L_0-linear combination over Λ_0 of the first h rows to add to it, so as to produce a matrix in which any h rows are independent. This is clearly possible if L_0 is infinite. $\square$

We may now pass to a situation in which any h rows of $\mathcal{J}'$ have an $h \times h$ minor of order ℓ_S. If L_0 is infinite we can do this as in the the Lemma above. If L_0 is finite we can make an étale extension of Λ_0 to enlarge the residue class field enough so that we can make the required linear change of variables.

Then, after renumbering variables, we may assume that the images of $Y_1, \ldots, Y_\tau$ are a separating transcendence basis for S/Q. We now replace Λ_0 by Λ_1, the localization of $\Lambda_0[Y_1, \ldots, Y_\tau]$ at $t\Lambda_0[Y_1, \ldots, Y_\tau]$. S remains the same: the elements we inverted to form Λ_1 are already invertible in $S = S_Q$. Note that ℓ_S does not change: the new Jacobian is

computed using only the Y_j for $j > \tau$, and so it is clear that ℓ_S cannot decrease. Moreover, it does not increase, because we have placed the coordinates in general position, and so we can find an $h \times h$ minor of some remaining h rows of order ℓ_S. S' does not change, but the relevant Jacobian matrix is a truncation of the one we used to compute $\ell_{S'}$ before, and so $\ell_{S'}$ can not decrease when replace Λ_0 by Λ_1.

In this way, we may assume that S/Q is a finite separable extension of L_0. But then an étale change of rings for Λ_0 enables us to reduce to the case where all residues in S/Q are represented in L_0. This means that by subtracting scalars in Λ_0 we may assume without loss of generality that all of $s_1, \ldots, s_d \in Q$. This means that the contraction of Q to $\Lambda_0[Y_1, \ldots, Y_d]$ is $(t, Y_1, \ldots, Y_d)$.

The main calculation in the proof of the Theorem. We can now complete the proof that iterating Néron's blowing-up eventually produces an algebra S such that $\ell_S = 0$. We need only show that $\ell_{S'} \leq \ell_S$ with strict inequality if $\ell_S > 0$.

Note that the generators of S' are the elements s_i/t. Let Z_i be variables mapping to these. We do not have to find all the relations on the Z_i: we only need sufficiently many to be able to see that some size h minor of the new Jacobian matrix has the same order as before, and that there exists a minor of smaller order if $\ell_S > 0$.

Let

$$F_j = b_j + \sum_{i=1}^{d} a_{ij} Y_i + H_j(Y)$$

where H_j has only terms of degree 2 and higher. Note that all coefficients are in Λ_0. Since $F_j(s_1, \ldots, s_d) = 0$, we may substitute $Y_i = tZ_i$ to get a polynomial in the Z_i which gives a relation on the s_i/t: it has the form

$$b_j + t \sum_{i=1}^{d} a_{ij} Z_i + t^2 H_j^*(Z),$$

where the coefficients are in Λ_0. Here $b_j \in \Lambda_0 \cap t\Lambda = t\Lambda_0$, and so we may write $b_j = tc_j$, with $c_j \in \Lambda_0$. We get a relation

$$G_j = c_j + \sum_{i=1}^{d} a_{ij} Z_i + tH_j^*(Z).$$

Note that $G_j(Z) = F_j(tZ)/t$, whence

$$\frac{\partial G_j(Z)}{\partial Z_i} = 1/t\big(\frac{\partial F_j}{\partial Y_i}(tZ)\big)t$$

where the final factor t arises from the chain rule. Substituting $Z_i = s_i/t$, we see that the image of the Jacobian matrix $\big(\frac{\partial G_j}{\partial Z_i}\big)$ in Λ is $\mathcal{J}'$. This proves that $\ell_{S'} \leq \ell_S$.

Finally, suppose that $\ell_S > 0$. This means that mod $t\Lambda$, all size h minors of $\mathcal{J}'$ vanish, so that the rank of this matrix mod $t\Lambda$ is at most $h-1$. Mod t, the matrix is the same as the image of $\big(a_{ij}\big)$ mod t. We may assume, after renumbering, that ℓ_S is achieved in the minor obtained by using the first h columns and the first h rows of $\mathcal{J}'$.

Now , mod $t\Lambda \cap \Lambda_0 = t\Lambda_0$, the the first h columns of $\mathcal{J}'$ are linearly dependent over L_0, and hence so are the first h columns of $\big(a_{ij}\big)$. By renumbering, we may assume without loss of generality that the first column is an L_0-linear combination of the columns numbered 2 through h. Lift the elements of L_0 needed to elements $\lambda_2, \ldots, \lambda_h \in \Lambda_0$, and consider $G_1 - \lambda_2 G_2 - \cdots - \lambda_h G_h$. The coefficients on quadratic and higher terms are divisible by t. By our choice of the λ_ν, the coefficients on the Z_i are divisible by t. The scalar is then forced to be divisible by t. Thus, $G_1 - \lambda_2 G_2 - \cdots - \lambda_h G_h$ may divided by t to get a new relation, which we call G_0. Consider the Jacobian matrix of $G_0, G_2, \ldots, G_h$ with respect to the variables $Z_1, \ldots, Z_h$, and compare this with the Jacobian matrix of $G_1, \ldots, G_h$ with respect to the variables $Z_1, \ldots, Z_h$. The first column has been altered first by subtracting off a sum of multiples of the other columns, which does not affect the minor, and then by factoring out t from the first column, while the other columns are the same as when we used for $G_1, \ldots, G_h$. The new minor clearly has order $\ell(S) - 1$ with respect to t. $\square$

This completes not only the proof of the Theorem asserted in the previous lecture, but also the proof of all cases of the Artin Approximation Theorem.

We now want to use Artin Approximation to prove the following:

Theorem. *Consider a family of finite systems of polynomial equations over $\mathbb{Z}$ such that each system in the family involves variables $x_1, \ldots, x_d$ and other variables $Y_{i,1}, \ldots, Y_{i,h_i}$ where both h_i and the variables are allowed to depend on which system in the family one is considering. Suppose that none of these systems has either*

(a) *a solution in a finitely generated algebra over a finite field such that the values of the x_j generated an ideal of height d, nor*

(b) *a solution in a finitely generated algebra over a DVR of mixed characteristic $p > 0$ such that the ideal generated by the values of the x_j has height d.*

Then no system in the family has a solution in a Noetherian ring in such a way that the values of the x_j generate an ideal of height d. Moreover, (a) alone guarantees that there is no solution in a Noetherian ring containing a field such the values of the x_j generate an ideal of height d.

Lecture of April 5, 2010

We begin our attack on the proof of the Theorem stated at the end of the Lecture Notes from April 2 by making several reductions in the problem. First note that it suffices to consider just one system of equations. We denote the equations

$$F_j(X_1, \ldots, X_d, Y_1, \ldots, Y_h) = 0, \quad 1 \leq j \leq n.$$

Second, we note that if there is a solution $x = x_1, \ldots, x_d,\ y = y_1, \ldots, y_h$ in a Noetherian ring R such that $(x_1, \ldots, x_d)R$ has height d, then we may localize R at a minimal prime of $(x_1, \ldots, x_d)R$ of height d. Thus, we get a solution of the system satisfying the height constraint if and only if we get a solution in a local ring of dimension d such that $x_1, \ldots, x_d$ is a system of parameters. We may evidently replace this local ring by its completion. Hence there is a solution satisfying the height constraint if and only if there is a solution in a complete local ring (R, m) such that $x_1, \ldots, x_d$ is a system of parameters.

This solution is preserved if we kill a minimal prime of R such that the quotient still has dimension d. Thus, we may assume that $(R,\ m)$ is a complete local domain. By the structure theory of complete local rings, we then have that R is module-finite over A, where A is a formal power series ring either over a field K or over a complete DVR (V, pV) of mixed characteristic p. Specifically, we write $A = K[[u_1, \ldots, u_d]]$ or $A = V[[u_2, \ldots, u_d]]$, and in the second case we let $u_1 = p$. In either case, $u_1, \ldots, u_d$ is a regular system of parameters for A.

Since R is module-finite over A, it has a set of generators $\theta_1 = 1, \theta_2, \ldots, \theta_s$. These are not free generators: let $\mathcal{M} = \big(a_{ij}\big)$ denote an $s \times t$ matrix over A whose t columns span the module of relations on $\theta_1, \ldots, \theta_s$ over A.

We next want to describe a finite system of polynomial equations in variables corresponding to the a_{ij} and other scalars from A. The equations have coefficients in $\mathbb{Z}$, and solving them in a ring A_1 enables one to construct a ring S module-finite over A_1 with a set of generators $\theta'_1 = 1, \theta'_2, \ldots, \theta'_s$.

First note that for all $i,\ j$ we can choose $a_{ijk} \in A$ such that

$$(*) \qquad \theta_i\theta_j = \sum_{\kappa=1}^{s} a_{ijk}\theta_k.$$

We need the a_{ij} and the a_{ijk} to satisfy certain equational conditions in order to guarantee that one gets a commutative associative ring with θ_1 as identity. We impose:

$$(1) \qquad a_{1jk} = \delta_{jk}$$

where δ is the Kronecker δ function which is 1 when $j = k$ and 0 otherwise. This guarantees the multiplication by θ_1 is the identity function.

To guarantee that multiplication will be commutative we impose

$$(2) \qquad a_{ijk} = a_{jik}$$

for all i, j, k.

We want to write down equations that will guarantee that multiplication is associative. To do this, for all i, j, k write down the formula for $\theta_i\theta_j$ as a linear combination of $\theta_1, \ldots, \theta_s$ using $(*)$, and then multiply on the right by θ_k and simplify each quadratic term by another

application of $(*)$. This yields a formula for $(\theta_i\theta_j)\theta_k$ as a linear combination of $\theta_1, \ldots, \theta_s$ in which every coefficient is a polynomial in the a_{ijk}. Similarly, use $(*)$ to write down $a_j a_k$ as a linear combination of $\theta_1, \ldots, \theta_s$ and then multiply by θ_i and use $(*)$ repeatedly again to give a formula for $\theta_i(\theta_j\theta_k)$ in which every coefficient is a polynomial with integer coefficients in the a_{ijk}. Subtract the two linear combinations to obtain $B_1^{(ijk)}\theta_1 + \cdots + B_s^{(ijk)}\theta_s$ where each $B_\mu^{(ijk)}$ is a polynomial in the a_{ijk} with coefficients in $\mathbb{Z}$. Write the coefficients as an $s \times 1$ column vector. Then this column vector gives a relation on $\theta_1, \ldots, \theta_s$, and so is a linear combination of the columns of $\big(a_{ij}\big)$. Thus, if $B^{(ijk)}$ denotes the column vector whose entries are $B_1^{(ijk)}, \ldots, B_s^{(ijk)}$ then for all i, j, k we can choose a $t \times 1$ vector $U^{(ijk)}$ of scalars from A such that

$$(3) \qquad B^{(ijk)} = \mathcal{M}U^{(ijk)},$$

where $\mathcal{M}$ is the $s \times t$ matrix $\big(a_{ij}\big)$ whose columns span the relations on $\theta_1, \ldots, \theta_s$.

We also need to write down equations that guarantee that multiplication is well-defined. The relation $\sum_{i=1}^s a_{ij}\theta_i = 0$ coming from the j the column of the matrix $\mathcal{M} = \big(a_{ij}\big)$, when multiplied by θ_k, produces a sum $\sum_{i=1}^s a_{ij}\theta_i\theta_k$ that can be rewritten, using (*), as a linear combination of the θ_i with coefficients that are polynomials in the a_{ij} and a_{ijk} with integer coefficients. Since this is 0, for each choice of j and k the column vector $C^{(jk)}$ of coefficients of the θ_i can be written in the form $\mathcal{M}W^{(jk)}$, where $W^{(jk)}$ is a $t \times 1$ column vector with entries in A, i.e.,

$$(4) \qquad C^{(jk)} = \mathcal{M}W^{(jk)}.$$

Note that the ring structure of R is completely determined by the choice of the ring A and the scalars $\mathcal{M} = \big(a_{ij}\big)$, a_{ijk}, and the entries of the $U^{(ijk)}$ and $W^{(jk)}$. Moreover, given any ring A_1 and corresponding subscripted elements of A_1 satisfying the equations (1), (2), (3), and (4), say b_{ij}, b_{ijk}, U_1^{ijk}, and $W_1^{(jk)}$ (the latter two are vectors over A_1), one gets a unique commutative, associative, ring S generated as an A_1-module by elements $\theta'_1, \ldots, \theta'_s$ such that θ'_1 is the identity, the columns of the matrix $\big(b_{ij}\big)$ span the relations on $\theta'_1, \ldots, \theta'_s$, and such that for all i and j

$$(*') \qquad \theta'_i\theta'_j = \sum_{k=1}^{s} b_{ijk}\theta'_k$$

S is defined as the cokernel of the matrix $\big(b_{ij}\big)$ over A_1 with $\theta'_1, \ldots, \theta'_s$ as the image of the standard basis. The equations $(*')$ are used to define the ring multiplication. The equations (1) guarantee that multiplication by θ_1 will be the identity map, the equations (2) guarantee that multiplication is commutative, the equations (3) guarantee that multiplication is associative, and the equations (4) guarantee that multiplication is well-defined.

We denote this ring as $\mathcal{R}(A_1; b_{ij}, b_{ijk}, U_1^{(ijk)}, W_1^{(jk)})$.

We use this idea to descend a solution of the equations

$$F_j(X_1, \ldots, X_d, Y_1, \ldots, Y_h) = 0, \quad 1 \le j \le n$$

over R, which is a module-finite extension of A, to a solution in a ring S with is a module-finite extension of the Henselian ring A_1, where A_1 is the Henselization of the localization at $(u_1, \ldots, u_d)$ of the ring $K[u_1, \ldots, u_d]$ (respectively, $V[u_2, \ldots, u_d]$), so that $\widehat{A_1} = A$. However we need three sets of additional equations.

In the original choice of R, we can write each x_μ and each y_ν as a linear combination of the θ_i with coefficients in A. These coefficients γ will all become unknowns, to be solved for in A_1. Each polynomial $F_j(x, y)$ can be expressed, using $(*)$ repeatedly, as a linear combination of the the θ_i each of whose coefficients is a polynomial in the a_{ijk} and the elements γ. This means that the column vector of coefficients of the θ_i can be written as the product of $\mathcal{M}$ with a column vector over A, whose entries will be a new set of unknowns. We refer to the equations obtained in this way as (5).

In R, the elements $x_1, \ldots, x_d$ are a system of parameters. This means that there is a fixed integer N such that every u_ν^N is an R-linear combination of $x_1, \ldots, x_d$. Each x_ν is already expressed as an A-linear combination of the θ_i. We can also write each coefficient of each x_ν as an A-linear combination of the θ_i: this introduces new elements that initially vary in A. The equations $(*)$ can be used to rewrite $u_\nu^N\theta_1$ minus the R-linear combination of the x_ν as a linear combination of the $\theta_1, \ldots, \theta_s$. The coefficients are polynomials in elements that may be thought of a varying in A. As in previous examples we set the column vector of coefficients equal to $\mathcal{M}$ multiplied by a column vector whose entries are in A, but which should be thought of as new variables. We refer to the equations one gets as (6).

Finally, we need equations which keep track of the condition that the map $A \to R$ is injective. If we tensor with the fraction field $\mathcal{F}$ of A, we get an injection $\mathcal{F} \to \mathcal{F} \otimes_A R$. Hence we have a $\mathcal{F}$-linear map $\mathcal{F} \otimes_A R \to \mathcal{F}$ that is nonzero. This gives a composite A-linear map $R \to \mathcal{F} \otimes_A R \to \mathcal{F}$ that is not zero. We can choose a common denominator in $A - \{0\}$ for the values of this nonzero A-linear map $R \to \mathcal{F}$ on the θ_i and multiply by it to obtain an A-linear map $\phi : R \to A$ that is not zero. Let $a_1, \ldots, a_s$ be the values on the θ_i. The condition that there exist an A-linear map with these values is that the matrix product

$$(7) \qquad \begin{pmatrix} a_1 & \ldots & a_s \end{pmatrix} \mathcal{M} = 0.$$

Suppose that $a_i \neq 0$. Then we can choose Q such that $a_i \notin m^Q$.

We now think of every subscripted element from A as a variable. However, in the equations (6) the elements u_ν^N are treated as fixed elements of A_1. The resulting system of polynomial equations over A_1 has a solution in A, and it therefore has a solution in A_1 congruent to the original solution mod m^Q, by the Artin Approximation Theorem.

The solution in A_1 gives rise to a ring S that is module-finite over A_1, generated as an A_1-module by $\theta_1' = 1, \ldots, \theta_d'$. The equations (1), (2), (3), and (4) guarantee that one has a well-defined commutative associative multiplication on A_1 such that multiplication by θ_1' is the identity map. The equations (5) guarantee that we have a solution for the equations

$$F_j(X_1, \ldots, X_d, Y_1, \ldots, Y_h) = 0, \quad 1 \leq j \leq n,$$

and the equations (6) guarantee that $(x_1, \ldots, x_d)S$ is primary to the maximal ideal of S. From the equations (7) we get a nonzero A_1-linear map $S \to A_1$ whose values on the θ_i' are the values corresponding to the variables introduced to replace the a_i. This map is not zero because the value on θ_i is congruent to the original value mod m^Q.

Finally, we may descend further, from A_1 to a suitable étale extension of $K[u_1, \ldots, u_d]$ or $V[u_2, \ldots, u_d]$. After localizing at one element, if necessary, we will still have that the radical of $(x_1, \ldots, x_d)S$ is maximal of height d. This completes the proof of the theorem in case we are working over a DVR.

In the case of a field K, we want to show that we can replace the field K by a finite field, even if K has characteristic 0 initially.

Henceforth, we assume that we have a solution in a finitely generated K-algebra, where K is a field that may be of positive characteristic or characteristic 0, and where the values $x_1, \ldots, x_d$ for $X_1, \ldots, X_d$ generate an ideal whose radical is a maximal ideal of height d. We may write this K-algebra in the form

$$R = K[X_1, \ldots, X_d, Y_1, \ldots, Y_h, Z_1, \ldots, Z_s]/\big(F_j(X,Y), G_k(X,Y,Z)\big)$$

where the X_d and Y_h map to the solution in the quotient ring. We may choose a finitely generated $\mathbb{Z}$-subalgebra B of K that contains all the coefficients of the polynomials generating the ideal we are killing, and then we may define

$$R_B = B[X_1, \ldots, X_d, Y_1, \ldots, Y_h, Z_1, \ldots, Z_s]/\big(F_j(X,Y), G_k(X,Y,Z)\big).$$

If K has characteristic $p > 0$, then B is a finitely generated $(\mathbb{Z}/p\mathbb{Z})$-algebra.

We make the convention that if C is a B-algebra then

$$R_C = C \otimes_B R_B \cong C[X_1, \ldots, X_d, Y_1, \ldots, Y_h, Z_1, \ldots, Z_s]/\big(F_j(X,Y), G_k(X,Y,Z)\big).$$

To complete the proof of the theorem, we shall prove two facts: the first is that for every maximal ideal μ of B, B/μ is a finite field. The second is that for the maximal ideals μ in some nonempty open subset of MaxSpec (B), $(x_1, \ldots, x_d)R_{B/\mu}$ has height d.

Lecture of April 7, 2010

Lemma. *Let R be an algebra finitely generated over its prime ring. Then the quotient of R by any maximal ideal is a finite field.*

Proof. The quotient S will be a field finitely generated as an algebra over its prime ring $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$. If the prime ring is $\mathbb{Z}$ then, by Noether normalization for domains, after localizing at one nonzero element of $\mathbb{Z}$, S is a module-finite extension of a polynomial extension by finitely many variables of $\mathbb{Z}_a$, $a \neq 0$. If the prime ring is $\mathbb{Z}/p\mathbb{Z}$, S is a module-finite extension of a polynomial extension of $\mathbb{Z}/p\mathbb{Z}$. Since S is a field, it has dimension 0, which is impossible if the prime ring is $\mathbb{Z}$, since module-finite extensions preserve dimension, and adjoining indeterminates increases dimension by the number of indeterminates adjoined. In the second case one sees that there are no indeterminates, and S is module-finite over $\mathbb{Z}/p\mathbb{Z}$, which means that it is a finite field. $\square$

Lemma (Generic Freeness). *Let M be a finitely generated module over R, where R is a finitely generated algebra over the Noetherian domain A. Then there is a nonzero element $a \in A$ such that M_a is A_a-free.*

Proof. M has a prime cyclic filtration by modules of the form R/P, and it suffices to show this for R/P, which can replace R. So it suffices to do the case $M = R$ and R is a domain. We use induction on $\dim(\mathcal{F} \otimes_A R)$, where $\mathcal{F}$ is the fraction field of A. By Noether normalization R is module-finite over a $A_a[X_1, \ldots, X_n]$, and so it suffices to consider a prime cyclic filtration of R_a over $A_a[X_1, \ldots, X_n]$. Those factors that are equal to $A_a[X_1, \ldots, X_n]$ are free, those that have A_a-torsion become zero after localization at one more element of $A - \{0\}$, while the other factors can be made free by localizing at one more element of $A - \{0\}$ by the induction hypothesis. $\square$

In the situation we were considering last time, we now know that every B/μ, for μ maximal in B, is a finite field. We want to preserve the condition that the $x_1, \ldots, x_d$ generate an ideal whose radical is a maximal ideal of height d, and this is equivalent to saying that the radical is maximal of height $\geq d$. Note that the height is correct when we pass to the fraction field $\mathcal{L}$ of B, since after that we are making a base change from one field to another, and the height will be preserved by the following much more general result:

Proposition. *Let S be a Noetherian ring faithfully flat over R and let I be an ideal of R. Then the height of IS is the same as the height of I. In particular, if R is a finitely generated $\mathcal{L}$-algebra and K is a field containing $\mathcal{L}$, then for every ideal I of R, the height of I is the same as the height of its expansion to $K \otimes_{\mathcal{L}} R$.*

Proof. The height of IS is the same as the minimum of the heights of minimal primes Q of S containing IS. If we replace S by S_Q for such a prime Q and R by its localization at the contraction of Q, then $R_P \to S_Q$ is faithfully flat. IS_Q is primary to QS_Q, and it follows that PR_P is nilpotent modulo IR_P. Then the height of Q is $\dim(S_Q) \geq \dim(R_P)$ which is at least the height of I. Now choose P prime in R so that it is a minimal prime of I and the height of I is $\dim(R_P)$. Choose Q to be a minimal prime of PS. Then $R_P \to S_Q$ is faithfully flat with closed fiber of dimension 0, and so we have that the height of IS is bounded by $\dim(S_Q) = \dim(R_P)$ (see part (d) of the first Lemma of the Lecture Notes of February 5) which is the height of I. The second statement follows from the first because K is faithfully flat over $\mathcal{L}$ and so $K \otimes_{\mathcal{L}} R$ is faithfully flat over R. $\square$

We are free to replace B by its localization at one nonzero element several (but finitely many) times: we shall retain the notation B as we do this.

Moreover, we are free to localize at one (equivalently, finitely many) nonzero elements of B: this is equivalent to looking at a dense open subset of $\mathrm{MaxSpec}(B)$. In $R_{\mathcal{L}} = \mathcal{L} \otimes_B R_B$ we can chooae a minimal prime contained in the radical of $(x_1, \ldots, x_d)$ so as to preserve the height when this prime is killed. We may kill the contraction of this prime to R_B, and so assume that R_B and $R_{\mathcal{L}}$ are domains. After localization at one element of $B - \{0\}$ we may assume that R_B is module-finite over a polynomial $B[u_1, \ldots, u_d]$, and embeds in a finitely generated free module G_B over $B[u_1, \ldots, u_d]$. After localizing at one more element of $B - \{0\}$ we may assume that G_B/R_B is free over B, by the Lemma on generic

freeness. Thus, for any μ, $R_{B/\mu}$ is module-finite over $(B/\mu)[u_1, \ldots, u_d]$ and embeddable in a torsion-free module over it: thw sequence $0 \to R_B \to G_B \to G_B/R_B \to 0$ remains exacts when we apply $\_ \otimes_B B/\mu$ because G_B/R_B is B-free and so $\operatorname{Tor}_1^B(G_B/R_B, B/\mu) = 0$. This implies that it has pure dimension d, and so every maximal ideal has height d. Now $\mathcal{L} \otimes_B R_B/(x_1, \ldots, x_d)$ is local and Artinian, with a nilpotent maximal ideal. The residue field is module-finite over $\mathcal{L}$. Therefore, after suitable localization, we may assume that $R_B/(x_1, \ldots, x_d)$ has a nilpotent prime such that the quotient is a domain module-finite over B. Now it is clear that all maximal ideals of $R_{B/\mu}$ have height d, and that the quotient of this ring by $(x_1, \ldots, x_d)$ is 0-dimensional, which forces $(x_1, \ldots, x_d)$ to have height d, since all of its minimal primes must be maximal ideals.

If there are several minimal primes among these maximal ideals, we can get back to the case where there is just one by localizing at one element. $\square$

We want to apply our method of reduction to characteristic p to prove that every local ring containing a field has a big Cohen-Macaulay module. A module M over a local ring (R, m, K) is called a *big Cohen-Macaulay module* for R if every system of parameters for R is a regular sequence on M and $mM \neq M$.

Theorem. *Every local ring that contains a field has a big Cohen-Macaulay module.*

We shall prove this by showing that the existence of a big Cohen-Macaulay module is an equational problem, and then it will suffice to solve the problem in positive characteristic. Stronger results are known: e.g., it is known that there are big Cohen-Macaulay algebras for local rings that contain a field and in mixed characteristic in dimension at most three. The proofs of these stronger results are extremely difficult.

The result of the Theorem above is very useful, and will illustrate the method of reduction to characteristic p. For rings of equal characteristic zero, no proof of the result is known without reduction to characteristic $p > 0$.

Lecture of April 9, 2010

In order to construct big Cohen-Macaulay modules over a local ring (R, m, K), we want to discuss the notion of a modification of a module M with respect to a set of relations in M with respect to sequences $x_1, \ldots, x_{k+1}$ that are part of a system of parameters for the local ring. The careful study of this idea will enable us to see that the existence of big Cohen-Macaulay modules is equivalent to the statement that a certain family of polynomial equations with a dimensional constraint has no solution.

Suppose that $\dim(R) = d$. Fix a non-empty family $\mathcal{F}$ of sequences of length d such that the elements of each sequence form a system of parameters for R. An important special case is when $\mathcal{F}$ has just one element. Another is when $\mathcal{F}$ consists of all such sequences.

We shall modify our terminology a bit and say that an R-module M is a *big Cohen-Macaulay module* with respect to $\mathcal{F}$ if every sequence in $\mathcal{F}$ is a regular sequence on M. (Thus, our original use of the term *big Cohen-Macaulay module* corresponds to the case where $\mathcal{F}$ consists of all sequences of parameters.) By our definition of regular sequence, for

$x_1, \ldots, x_n$ to be a regular sequence on M, we must have that $(x_1, \ldots, x_n)M \neq M$. For any ideal generated I generated by a system of parameters (or any m-primary ideal I), the condition that $IM \neq M$ is equivalent to the condition that $mM \neq M$. For if $mM = M$, we have that $m^2M = m(mM) = mM = M$, and, by induction, that $m^tM = M$ for all t. Since $m^t \subseteq I$ for some t, we have that $IM = M$. On the other hand, if $IM = M$ it is clear that $mM = M$.

By a type k-relation on a module M with respect to $\mathcal{F}$ we mean a sequence of elements $(u_1, \ldots, u_k, u)$ in M together with a sequence $x_1, \ldots, x_{k+1}$ that is an initial segment of an element of $\mathcal{F}$ such that

$$x_{k+1}u = \sum_{i=1}^{k} x_i u_i$$

(the case $k = 0$ is allowed, and then the right hand side is 0).

Given a set of relations $\mathcal{S}$ with respect to $\mathcal{F}$ (the types are allowed to vary), by the *modification* of M with respect to $\mathcal{S}$ we mean the map $M \to M'$ constructed as follows. For each element $\sigma \in \mathcal{S}$ of type $k = k_\sigma$, let G_σ be a free R-module of rank k with free basis $b_1^\sigma, \ldots, b_k^\sigma$, and let

$$M' = (M \oplus \bigoplus_{\sigma \in \mathcal{S}} G_\sigma)/\text{Span}_R\{\rho_\sigma : \sigma \in \mathcal{S}\}$$

where, if σ corresponds to

$$x_{k+1}u = \sum_{i=1}^{k} x_i u_i,$$

then

$$\rho_\sigma = u - \sum_{i=1}^{k} x_i b_i^\sigma.$$

The map $M \to M'$ is the composition of the obvious injection of M into the direct sum in the numerator composed with the quotient surjection.

If the set $\mathcal{S}$ has just one element, we shall say that M' is a *single modification* of M.

Given a modification of M with respect to a set of relations, call it M', one can then form a modification of M', call it M'', with respect to some set of relations on M''. Continuing in this way, one may consider sequences of modifications

$$M \to M' \to M'' \to \cdots \to M^{(r)}.$$

We start with R itself, and form a sequence in which, at each stage, we modify the given module with respect to the set of *all* relations on M with respect o $\mathcal{F}$. In this way we get a sequence of modifications

$$R = M_0 \to M_1 \to M_2 \to \cdots.$$

Each relation with respect to $\mathcal{F}$ on M_i becomes trivial in M_{i+1}. Let M_∞ be the direct limit of the M_i. The image of $1 \in R$ in M_i plays a special role here: call it 1_i. In particular, the image of 1 in M_∞ is denote 1_∞.

Lemma. *Let (R, m, K) of dimension d be given, let $\mathcal{F}$ be non-empty family of sequences of length d whose elements are systems of parameters, as above, let $x_1, \ldots, x_d$ be one element of $\mathcal{F}$ and let*

$$R = M_0 \to M_1 \to \cdots \to M_r \to \cdots$$

by the sequence of modifications with respect to $\mathcal{F}$ described in the preceding paragraph. Let M_∞ be the direct limit of the M_r, and let 1_r be the image of $1 \in R$ in M_r, $0 \leq r \leq \infty$. Then the following conditions are equivalent:

(1) *R has a big Cohen-Macaulay module with respect to $\mathcal{F}$.*

(2) *M_∞ is a big Cohen-Macaulay module over R with respect to $\mathcal{F}$.*

(3) *$1_\infty \notin (x_1, \ldots, x_d)M_\infty$.*

(4) *$1_r \notin (x_1, \ldots, x_d)M_r$ for all positive integers r.*

(5) *For every sequence $M_0 = R, \ldots, M_r$ such that each M_{i+1} is a modification of M_i with respect to some set of relations on M_i over $\mathcal{F}$, the image of $1 \in R$ in M_r is not in $(x_1, \ldots, x_d)M_r$.*

Moreover, if M is any R-module with a map ϕ to a big Cohen-Macaulay module B with respect to $\mathcal{F}$, and M' is any modification of M with respect to a set of relations on M over $\mathcal{F}$, then the map $M \to B$ factors through a map $M' \to B$, so that one has $M \to M' \to B$.

Proof. It is clear that (5) $\Rightarrow$ (4), while the equivalence of (3) and (4) follows from the fact that M_∞ is the direct limit of the M_r. If (3) holds, we claim that (2) holds. Evidently, with $I = (x_1, \ldots, x_d)R$ we have $IM \neq M$, and therefore, by the discussion at the end of the third paragraph of the first page, we have that $mM \neq M$. But given a relation on $x_1, \ldots, x_{k+1}$ in M_∞, where $x_1, \ldots, x_{k+1}$ is an initial segment of some sequence in $\mathcal{F}$, it must come from such a relation on some M_r that maps to it. This relation becomes trivial in M_{r+1}, and therefore in M_∞ as well. Of course, (2) $\Rightarrow$ (1) is clear.

It remains only to prove that (1) $\Rightarrow$ (5). It will suffice to show that given a big Cohen-Macaulay module B and an element $w \in B - mB$, we can map $M_r \to B$ in such a way that the image w_r of $1 \in R$ in M_r maps to w. We cannot then have $w_r \in (x_1, \ldots, x_d)M_r$, for we may apply the map $M_r \to B$ then gives that $w \in (x_1, \ldots, x_d)B \subseteq mB$, a contradiction.

We show that there is a map $M_r \to B$ by defining it successively on the sequence of modules $R = M_0, M_1, \ldots, M_r, \ldots$. In the case of R, we simply take the map that sends $1 \in R$ to $w \in B$. We use induction. Suppose that we have defined $\phi_i : M_i \to B$ such that $\phi_i(w_i) = w$, where w_i is the image of 1 in M_i. We want to define $\phi_{i+1} : M_{i+1} \to B$ such that the diagram

$$\begin{array}{ccc} B & \xrightarrow{=} & B \\ {\scriptstyle \phi_i}\uparrow & & \uparrow{\scriptstyle \phi_{i+1}} \\ M_i & \longrightarrow & M_{i+1} \end{array}$$

commutes. That is, we want to establish the final statement of the Lemma with $M = M_i$, $\phi = \phi_i$ and $M' = M_{i+1}$, and so we can complete the proof by proving the final statement of the Lemma.

We proceed by defining the new map ϕ' on each direct summand of $M \oplus \bigoplus_\sigma G_\sigma$ so as to kill all the relations ρ_σ. We define it to be ϕ on M. We need to specify values for ϕ' on the free generators of every G_σ in such a way that all the ρ_σ vanish. Given σ corresponding to $x_{k+1}u = \sum_{j=1}^k x_i u_i$ with the u_i and u in M, we apply ϕ to get

$$x_{k+1}\phi(u) = \sum_{j=1}^k x_i \phi(u_i).$$

Since B is a big Cohen-Macaulay module with respect to $\mathcal{F}$, it follows that $\phi(u) \in (x_1, \ldots, x_k)B$ which yields $\phi(u) = \sum_{j=1}^k x_i v_i$ for suitable elements $v_1, \ldots, v_k \in B$. We define the values of ϕ' on $b_1^\sigma, \ldots, b_k^\sigma$ to be $v_1, \ldots, v_k$, respectively. This clearly does what we need. $\square$

Remark. In conditions (3), (4), and (5) we could use mM instead of $(x_1, \ldots, x_d)M$. The given formulation is convenient when we formulate an equational version of the criterion.

Note that if $f : M \to N$ is any R-linear map, each type k relation on M with respect to $\mathcal{F}$ maps to a type k-relation on N with respect to $\mathcal{F}$: the point is simply that if

$$x_{k+1}u = \sum_{i=1}^k x_i u_i$$

then

$$x_{k+1}f(u) = \sum_{i=1}^k x_i f(u_i).$$

In particular, if one has a sequence of modifications of M, each type k relation on M maps to such a relation on the further terms in the sequence.

Our next objective is to show that the obstruction to the existence of big Cohen-Macaulay modules with respect to $\mathcal{F}$ can be phrased in terms of (all) finite sequences of single modifications of M. We make use of characterization (4). Suppose that $1_r \in (x_1, \ldots, x_d)M_r$. Only finitely many elements of M_r are needed as coefficients here. The same relation will hold if we modify M_{r-1} with respect to only finitely many of the relations used in the construction of M_r. All of these modifications can be described using only finitely many elements of M_{r-1}. All the elements and relations needed will be in a modification of M_{r-2} with respect to finitely many relations. We can continue working backward in this way. We therefore get the following:

Theorem. *Let (R, m, K) be local of dimension d, let $\mathcal{F}$ be a non-empty family of sequences of length d whose elements are systems of parameters for R, and let $x_1, \ldots, x_d$ be one element of $\mathcal{F}$. The following conditions are equivalent:*

(1) *R has a big Cohen-Macaulay module with respect to $\mathcal{F}$.*

(2) *For every finite sequence of modifications of R, say*

$$R = M_0 \to M_1 \to \cdots \to M_r,$$

each with respect to a finite set of relations over $\mathcal{F}$, the image w_r of $1 \in R$ in M_r is not in $(x_1, \ldots, x_d)M_r$.

(3) *For every finite sequence of single modifications of R, say*

$$R = M_0 \to M_1 \to \cdots \to M_r,$$

each with respect to a single relation over $\mathcal{F}$, the image w_r of $1 \in R$ in M_r is not in $(x_1, \ldots, x_d)M_r$.

Proof. The argument prior to the statement of the Theorem shows that if (2) holds then condition (4) of the Lemma holds, and so (2) $\Rightarrow$ (1). However, a modification of a module M with respect to finitely many relations $\sigma_1, \ldots, \sigma_h$ can be achieved by making, successively, h single modifications: one modifies M with respect to σ_1 to get M_1, and then modifies M_1 with respect to the image of σ_2, and so forth. At the inductive step, one modifies M_i with respect to the image of σ_{i+1}, if $i < h$. Then M_h is the same as the modification of M with respect to $\sigma_1, \ldots, \sigma_h$. Thus, (3) $\Rightarrow$ (2). Finally, (1) $\Rightarrow$ (3) follows from the implication (1) $\Rightarrow$ (5) in the preceding Lemma. $\square$

We next want to show that the problem of the existence of big Cohen-Macaulay modules can be viewed equationally. For simplicity, we first state the next result when there is only one system of parameters being used, and then indicated the modification needed when there may be many.

Theorem. *Suppose that (R, m, K) is a d-dimensional local ring with system of parameters $x_1, \ldots, x_d$. Let $k_1, \ldots, k_r$ be a sequence of integers with values between 0 and $d-1$. Then there is a system of polynomial equations with coefficients in $\mathbb{Z}$ and variables $X_1, \ldots, X_d, Y_1, \ldots, Y_h$ such that the system has a solution in R with $x_1, \ldots, x_d$ as the values of $X_1, \ldots, X_d$ if and only if R has a sequence of single modifications*

$$R = M_0 \to M_1 \to \cdots \to M_r$$

of types $k_1, \ldots, k_r$ with respect to $x_1, \ldots, x_d$ such that the image w_r of 1 is in the submodule $(x_1, \ldots, x_d)M_r$.

Before discussing the proof of this result in the general case, we want to discuss the case where $r = 1$. We write $k = k_1$. The modification comes from a relation

$$yx_{k+1} = \sum_{j=1}^{k} y_k x_k$$

over R. The modification may be described as $(R \oplus R^k)/R\rho$ where

$$\rho = (y, -x_1, \ldots, -x_k).$$

We are then concerned with whether, in this modified module M_1, we have that the image of $(1, 0, \ldots, 0)$ is in $(x_1, \ldots, x_d)M_1$. This leads to the additional equations coming from the vector equation

$$(1, 0, \ldots, 0) = (y_{11}x_1 + \cdots + y_{1d}x_d, \cdots, y_{k+1,1}x_1 + \cdots + y_{k+1,d}x_d) + y'\rho$$

This will give $k+1$ equations over $\mathbb{Z}$ in variables $Y, Y_1, \ldots, Y_k$, $Y_{\mu,\nu}, Y'$ and $X_1, \ldots, X_d$, where each lower case letter has been replaced by a correspondingly subscripted or superscripted upper case letter that is to be viewed as a variable.

In the general case, we give explicit presentations of each of $M_1, \cdots, M_r$. These are constructed recursively. M_i will be a quotient of $R \oplus R^{k_1} \oplus R^{k_i} \cong R^{1+k_1+\cdots k_i}$ by the span over R of i vectors, $\rho_1, \ldots, \rho_i$. The ρ_i will be thought of as having entries some unkonwn, and others satisfying certain equations over $\mathbb{Z}$ coming from relations on previous modules in the sequence. To get the presentation of M_{i+1}, one starts with a relation on M_i. This is given by using unknown coefficients: the relation is thought of as being given by vectors in the numerator, which is free, and one adds into the equation a linear combination of the vectors $\rho_1, \ldots, \rho_i$ with unknown coefficients. One adds a copy of $R^{k_{i+1}}$ in the numerator, and identifies $R^{1+k_1+\cdots k_i}$ with its image in $R^{1+k_1+\cdots k_i+k_{i+1}}$ (spanned by an initial segment of the standard basis). The vectors $\rho_1, \ldots, \rho_i$ one killed to get M_i may be identified with their images (one enters zeros in the last k_{i+1} spots). In addition, to get the presentation of M_{i+1} one kills one additional vector, ρ_{i+1}, derived from a new relation holding in M_i, whose entries are unknowns satsifying certain equations.

Eventually one constructs the presentation of M_r, and then one can express the condition that the image of $1 \in R$ is in $(x_1, \ldots, x_d)M_r$ by one additional vector equation, setting $(1, 0, \ldots, 0)$ equal to the sum of a vector whose entries are unknown linear combinations of $x_1, \ldots, x_d$ and a linear combination of the $\rho_1, \ldots, \rho_r$ with unknown coefficients. $\square$

Lecture of April 12, 2010

We next want to describe how the equational set-up changes if there is a family of systems of parameters and one has a modification with respect to a system that may be different at every stage. It is convenient to view one of the systems, $x_1, \ldots, x_d$ as special. This one is used when one writes down an equation corresponding to the fact that the image of $1 \in R$ is in $(x_1, \ldots, x_d)M_r$. In dealing with a finite sequence of single modifications, only finitely systems will occur. One can introduce variables that represent the elements in the finitely many systems of parameters. The equations connected with the modification process change only in obvious ways: in dealing with a modification with respect to a certain system of parameters or a relation on a certain system of parameters; one uses those parameters as coefficients (or variables corresponding to them in the system of equations). One introduces extra equations that keep track of the fact that each of the additional sequences has the same radical as $x_1, \ldots, x_d$. If $x'_1, \ldots, x'_d$ is one such sequence, it suffices to use the equations

$$x_j^N = \sum_{i=1}^{d} z_{ij} x'_i$$

(which will hold for some positive integer N and suitable elements $z_{ij} \in R$) and similar ones reversing the roles of the x_i and the x'_i: these equations guarantee that $(x_1, \ldots, x_d)$ and $(x'_1, \ldots, x'_d)$ have the same radical, so that $x'_1, \ldots, x'_d$ is also a system of parameters.

The problem of the existence of big Cohen-Macaulay modules has now been shown to be equational with dimension constraint in a sense that reduces the problem in equal characteristic to the case of local ring in characteristic $p > 0$. But we may then pass to the case of a complete local domain, and it will suffice to prove that case.

We next observe the following fact:

Theorem. *Let R be a complete local domain of positive characteristic p and let $x_1, \ldots, x_d$ be a system of parameters. Then there exists a nonzero element $c \in R$ such that for all k, $0 \leq k < d$, and for all $q = p^e$, $e \in \mathbb{N}$,*

$$(*) \quad c\big((x_1^q, \ldots, x_k^q)R :_R x_{k+1}^q\big) \subseteq (x_1^q, \ldots, x_k^q)R.$$

Hence, for any finite set of systems of parameters there exists a nonzero element c that has this property for all of these sets.

Moreover, if R is module-finite over a regular local ring A we can choose $c \in A - \{0\}$ so that it has this property for every system of parameters in A.

Proof. Given one system of parameters $x_1, \ldots, x_d$ we can choose a coefficient field K for R and let $A = K[[x_1, \ldots, x_d]]$. Since systems of parameters for A are closed under the operation of replacing every element by a power of that element, the statement for one system of parameters follows from the statement about A. But if one has several systems of parameters and elements $c_1, \ldots, c_k$, where for all of the systems of parameters one of the c_i satisfies the condition $(*)$ for that system, then $c = c_1 \cdots c_k$ satisfies the condition $(*)$ for all of them. It therefore suffices to prove the final statement for systems of parameters in A.

Let h denote the torsion-free rank of R as an A-module and let $u_1, \ldots, u_h$ be a maximal set of elements in R linearly independent over A. Let G be the A-span of these elements. Then $G \cong A^{\oplus h}$, and R/G is A-torsion. Thus, we may choose $c \in A - \{0\}$ such that c kills R/G, i.e., such that $cR \subseteq G$.

Let $y_1, \ldots, y_d$ be any system of parameters for A and suppose that

$$y_{k+1}r = \sum_{i=1}^{k} y_i r_i.$$

Multiply by c to obtain

$$y_{k+1}(cr) = \sum_{i=1}^{k} y_i(cr_i).$$

All of the elements cr, $cr_i \in G$. Since A is regular, it is Cohen-Macaulay, and $y_1, \ldots, y_d$ is a regular sequence on A and, therefore, on $G \cong A^{\oplus h}$ as well. It follows that

$$cr \in (y_1, \ldots, y_k)G \subseteq (y_1, \ldots, y_k)R. \qquad \square$$

We next note the following: let $(R, m) \to (S, n)$ be a local homomorphism of local rings of the same dimension such that mS is primary to n. This implies that the image of every

system of parameters for R is a system of parameters for S. Suppose that $x_1, \ldots, x_d$ has image $y_1, \ldots, y_d$ in S. Let $M \to M'$ be a single modification of M with respect to a relation

$$x_{k+1}u = \sum_{i=1}^{k} x_i u_i,$$

where the $u_i \in M$. Then $S \otimes_R M \to S \otimes_R M'$ is likewise a single modification of $S \otimes_R M$ with respect to the relation

$$y_{k+1}(1 \otimes u) = \sum_{i=1}^{k} y_i (1 \otimes u_i).$$

The verification is quite straightforward:

$$S \otimes_R (M \oplus R^{\oplus k}) \cong (S \otimes_R M) \oplus S^{\oplus k},$$

and the image of $(u, -x_1, \ldots, -x_k)$ is $(1 \otimes u, -y_1, \ldots, -y_k)$. Thus, a sequence of single modifications

$$R = M_0 \to M_1 \to \cdots \to M_r$$

becomes another sequence of single modifications

$$S = S \otimes_R M_0 \to S \otimes_R M_1 \to \cdots \to S \otimes_R M_r.$$

Moreover, if the image of $1 \in R = M_0$ in M_r is in $(x_1, \ldots, x_d)M_r$, then the image of $1 \in S = S \otimes_R M_0$ in $S \otimes_R M_r$ is in $(y_1, \ldots, y_d)(S \otimes_R M_r)$.

In particular, we can apply base change when $S = R$ and the map is a power of the Frobenius endomorphism, sending $r \mapsto r^q$ for all $r \in R$: here $q = p^e$ for some $e \in \mathbb{N}$.

We are now ready to prove:

Theorem. *Every local ring containing a field has a big Cohen-Macaulay module (with respect to all systems of parameters).*

Proof. As already noted, the problem is equational with dimension constraint and so reduces to the case of a complete local domain (R, m, K) of characteristic $p > 0$. Suppose that there is a series of single modifications with respect to various systems of parameters

$$R = M_0 \to M_1 \to \cdots \to M_r$$

such that the image of $1 \in M_0$ in M_r is in $(x_1, \ldots, x_d)M_r$, where $x_1, \ldots, x_d$ is a system of parameters. We shall obtain a contradiction. Choose $c \in R - \{0\}$ such that condition $(*)$ of the preceding Theorem holds for all of the finitely many systems of parameters that occur in the displayed sequence of modifications. Then for every $q = p^e$ we may apply base change using the eth power of the Frobenius endomorphism, and so obtain a new sequence of modifications

$$R = M_0^{(e)} \to M_1^{(e)} \to \cdots \to M_r^{(e)}$$

such that the image of $1 \in M_0$ in $M_r^{(e)}$ is in $(x_1^q, \ldots, x_d^q)M_r^{(e)}$. Each modification is with respect to a system of parameters consisting of q th powers of the elements in one of the original systems of parameters. We claim that there is is a commutative diagram:

$$\begin{array}{ccccccccccc}
R & \xrightarrow{c} & R & \xrightarrow{c} & \cdots & \xrightarrow{c} & R & \xrightarrow{c} & R & \xrightarrow{c} \cdots \xrightarrow{c} & R \\
{\scriptstyle id_R}\uparrow & & {\scriptstyle \phi_1}\uparrow & & & & {\scriptstyle \phi_i}\uparrow & & {\scriptstyle \phi_{i+1}}\uparrow & & {\scriptstyle \phi_r}\uparrow \\
R = M_0^{(e)} & \longrightarrow & M_1^{(e)} & \longrightarrow & \cdots & \longrightarrow & M_i^{(e)} & \longrightarrow & M_{i+1}^{(e)} & \longrightarrow \cdots \longrightarrow & M_r^{(e)}
\end{array}$$

where we shall show recursively that the vertical arrows can be constructed so that the diagram commutes. The leftmost arrow is simply the identity map on R.

Suppose that we have constructed the ϕ_j, $j \leq i$, so that the leftmost i squares commute, and suppose that $i < r$. Let $M = M_i^{(e)}$, and write $\phi = \phi_i$. We write $M' = M_{i+1}^{(e)}$. Then M' has the form

$$\big(M \oplus (Rb_1 \oplus \cdots \oplus Rb_k)\big)/Rv$$

where the b_i give a free basis, where

$$v = u - y_1 b_1 - \cdots - y_k b_k$$

where $y_1, \ldots, y_d$ is a system of parameters consisting of q th powers of one of the finitely many systems specified earlier, and where there is a relation

$$y_{k+1} u = \sum_{i=1}^{k} y_i u_i$$

for elements $u, u_1, \ldots, u_k \in M$. Then

$$y_{k+1}\phi(u) = \sum_{i=1}^{k} y_i \phi(u_i) \in R,$$

and we therefore have that

$$c\phi(u) = \sum_{i=1}^{k} y_i r_i \in R,$$

because of the special choice of c satisfying $(*)$ for each of the finitely many systems of parameters that occur. But this means that we can define the next map on the numerator module $M \oplus (Rb_1 \oplus \cdots \oplus Rb_k)$ by letting it agree with $c\phi$ on M and by mapping each b_i to r_i: our choice of the r_i is such that v is killed.

Once we have this commutative diagram we can compute the image of $1 \in M_0$ in the rightmost copy of R in the upper row by following two different paths: if we apply the leftmost vertical arrow and then all of the horizontal arrows in the top row, we get $1 \cdot c^r = c^r$. If we apply the horizontal arrows in the bottom row and then ϕ_r, we get the

image in R of an element in $(x_1^q, \ldots, x_d^q)M_r^{(e)}$, which will be in $(x_1^q, \ldots, x_d^q)R$. This shows that for all q,

$$c^r \in (x_1^q, \ldots, x_d^q)R \subseteq m^q,$$

and so $c^r \in \bigcap_q m^q = 0$, a contradiction. $\square$

We shall now use this theorem to prove two theorems that do not refer to any non-Noetherian objects.

The next result was proved in characteristic p and in certain characteristic 0 cases by Peskine and Szpiro [C. Peskine and L. Szpiro, *Dimension projective finie et cohomologie locale*, Publ. Math. I.H.E.S. (Paris) **42** (1973) pp. 323–395] (for the intersection theorem) and [_____, *Syzygies et multiplicités*, C. R. Acad. Sci. Paris Sér. A **278** (1974) pp. 1421–1424] (for the new intersection theorem) and by Paul Roberts [P. Roberts, *Two applications of dualizing complexes over local rings*, Ann. Sci. Ec. Norm. Sup. **9** (1976) pp. 103–106]. The equicharacteristic case in general was obtained in [M. Hochster, *Topics in the Homological Theory of Modules over Commutative Rings*, CBMS Regional Conference Series No. **24**, AMS, Providence, RI, 1975]; see also [_____, *Canonical elements in local cohomology modules and the direct summand conjecture*, J. of Algebra **84** (1983) pp. 503–553].

Theorem (new intersection theorem). *Let R be a local ring that contains a field. Let $0 \to G_n \to \cdots \to G_0 \to 0$ be a finite complex of finitely generated free modules such that $H_0(G_0) \neq 0$ and all the homology modules have finite length. Then* $\dim(R) \leq n$.

Theorem. *Let R be a regular ring that contains a field. Then R is a direct summand of every module-finite extension algebra.*

The second result is easy in characteristic 0 by other means, where it holds for normal rings. The characteristic p result was not established until the early 1973, however. The first argument is in [M. Hochster, *Contracted ideals from integral extensions of regular rings*, Nagoya Math. J. **51** (1973) pp. 25–43]. The mixed characteristic case of this problem remains an open question in dimension ≥ 4.

Lecture of April 14, 2010

The new intersection theorem is known even for rings of mixed characteristic, but the proof in the mixed characteristic case, which is due to Paul Roberts, is quite difficult. Cf. [P. Roberts, *Le théorème d'intersection*, C. R. Acad. Sc. Paris Sér. I **304** (1987) pp. 177–180], [_____, *Intersection theorems,* in *Commutative Algebra*, Math. Sci. Research Inst. Publ. **15**, Springer-Verlag, New York-Berlin-Heidelberg (1989) pp. 417–436], and [_____, *Multiplicities and Chern classes in local algebra*, Cambridge Tracts in Mathematics **133**, Cambridge University Press, Cambridge, England, 1998]. Here we give the argument in equal characteristic. It is valid for any local ring that has a big Cohen-Macaulay module.

Proof of the new intersection theorem. Let

$$0 \to G_n \to \cdots \to G_1 \to G_0 \to 0$$

be the given free complex. Recall that $H_0(G_\bullet) \neq 0$ and choose a minimal generator u of $H_0(G_\bullet)$. Of course, u is killed by some power of the maximal ideal m of R. (In fact, the proof does not use that $H_0(G_\bullet)$ has finite length: only that it is nonzero and has a minimal generator u that is killed by a power of m.) Some element of G_0 maps onto u, and it must be a minimal generator of G_0. Thus, we may write $G_0 = Re_1 \oplus G_0'$ where both summands are R-free. We can choose an integer N_0 so large that $m^{N_0}u = 0$ and $m^{N_0}H_i(G_\bullet) = 0$ for $i \geq 1$. Let Z_i and B_i denote the modules of cycles and boundaries respectively in G_i, so that $H_i(G_\bullet) = Z_i/B_i$. Then $m^{N_0}e_1 \in B_0$ and $m^{N_0}Z_i \subseteq B_i$ for $i \geq 1$.

For each $i \geq 1$, we may use the Artin-Rees Lemma to choose N so large that

$$m^N G_i \cap Z_i \subseteq m^{N_0} Z_i.$$

Since we need only be concerned with $i \leq n$, we may choose $N \geq N_0$ so that for all i, $1 \leq i \leq n$, $m^N G_i \cap Z_i \subseteq m^{N_0} Z_i \subseteq B_i$.

Next, we choose a system of parameters $\underline{x} = x_1, \ldots, x_d$ for R inside m^N. We can do this by first choosing any system of parameters and then replacing every element by its N th power. Recall that what we want to prove is that $d \leq n$. Assume, to the contrary, that $d > n$. We shall obtain a contradiction. Let $\mathcal{K}_\bullet(\underline{x}; R)$ denote the Koszul complex on $x_1, \ldots, x_d$. First note that we have a commutative diagram

$$\begin{array}{ccccc} G_0 & \longrightarrow & H_0(G_\bullet) & \to & 0 \\ \uparrow & & \uparrow & & \\ R & \longrightarrow & R/(\underline{x}) & \to & 0 \end{array}$$

where the vertical arrow on the left takes $1 \in R$ to $e_1 \in G_0$ and the vertical arrow on the right maps $\overline{1} \in R/(\underline{x})$ to u (the second map exists since u is killed by m^{N_0} and $(\underline{x}) \subseteq m^N \subseteq m^{N_0}$).

Think of the copy of R on the left in the bottom row as $\mathcal{K}_0(\underline{x}; R)$. We shall show by induction that this diagram extends to a map from the Koszul complex $\mathcal{K}(\underline{x}; R)$ to $G_\bullet$:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \cdots & \longrightarrow & G_n & \longrightarrow & \cdots & \longrightarrow & G_0 & \longrightarrow & H_0(G_\bullet) & \longrightarrow & 0 \\ \uparrow & & & & \uparrow & & & & \uparrow & & \uparrow & & \\ \mathcal{K}_d(\underline{x}; R) & \longrightarrow & \cdots & \longrightarrow & \mathcal{K}_n(\underline{x}; R) & \longrightarrow & \cdots & \longrightarrow & R & \longrightarrow & R/(\underline{x}) & \longrightarrow & 0 \end{array}$$

Assume that the vertical maps have been constructed, starting on the right, up to and including $\phi : \mathcal{K}_i(\underline{x}; R) \to G_i$ so that the diagram commutes. Thus, we have:

$$\begin{array}{ccccccccc} \longrightarrow & G_{i+1} & \longrightarrow & G_i & \longrightarrow & G_{i-1} & \longrightarrow \\ & {\scriptstyle ?}\uparrow & & {\scriptstyle \phi_i}\uparrow & & {\scriptstyle \phi_{i-1}}\uparrow & \\ \longrightarrow & \mathcal{K}_{i+1}(\underline{x}; R) & \longrightarrow & \mathcal{K}_i(\underline{x}; R) & \longrightarrow & \mathcal{K}_{i-1}(\underline{x}; R) & \longrightarrow \end{array}$$

We want to define the map ϕ_{i+1} so that the square on the left will commute. Consider a free generator f of $\mathcal{K}_{i+1}(\underline{x};\, R)$. The matrices of the maps in the Koszul complex have entries each of which is 0 or $\pm x_j$ for some j: thus all entries are in $(x_1, \ldots, x_d) \subseteq m^N$. Hence, the image of f in $\mathcal{K}_i(\underline{x};\, R)$ is actually in $(x_1, \ldots, x_d)\mathcal{K}_i(\underline{x};\, R)$, and so the image of f in G_i is in $m^N G_i$. It is also in Z_i, that is, the image of f in G_{i-1} is 0, because we view the map $\mathcal{K}_{i+1}(\underline{x};\, R) \to G_{i-1}$ as factoring

$$\mathcal{K}_{i+1}(\underline{x};\, R) \to \mathcal{K}_i(\underline{x};\, R) \to \mathcal{K}_{i-1}(\underline{x};\, R) \to G_{i-1}$$

and the composition of the two maps on the left is 0. Thus, the image of f in G_i is in $m^N G_i \cap Z_i \subseteq B_i$, by our choice of N, and so we can choose $f' \in G_{i+1}$ such that f' maps to the image of f in G_i. We define the value of ϕ_{i+1} on f to be f'. We repeat this argument for every element in a free basis for $\mathcal{K}(\underline{x};\, R)$, and so define ϕ_{i+1}.

We now have the desired map of complexes. Now suppose that $\mathcal{B}$ is a big Cohen-Macaulay module for R (all we need is that $x_1, \ldots, x_d$ is a regular sequence on $\mathcal{B}$ and that some element $v \in \mathcal{B} - (x_1, \ldots, x_d)\mathcal{B}$). The image of v in $\mathcal{B}/(x_1, \ldots, x_d)\mathcal{B}$ spans a cyclic module of finite length: we replace v by a multiple, which we still denote by v, which is in the socle. That is, without loss of generality, we may assume that $v \notin (x_1, \ldots, x_d)B$ but $mv \subseteq (x_1, \ldots, x_d)B$.

Next note that because u is a minimal generator of $H = H_0(G_\bullet)$, it has nonzero image in the K-vector space H/mH. Hence, there is a map of H/mH onto $K\overline{v} \subseteq B/(x_1, \ldots, x_d)\mathcal{B}$ that sends the image of u to v, and so there is a map $H \to \mathcal{B}/(x_1, \ldots, x_d)$ that sends $u \to v$. This will lift to a map of $G_0 = Re_1 \oplus G_0'$ to B sending e_1 to v. We now extend this map to a map of complexes $G_\bullet \to \mathcal{K}_\bullet(\underline{x};\, \mathcal{B})$, which we can do because $G_\bullet$ is free and $\mathcal{K}(\underline{x};\, \mathcal{B})$ is acyclic. We can then compose with the map of complexes $\mathcal{K}_\bullet(\underline{x};\, R) \to G_\bullet$ already constructed to get a map of complexes $\mathcal{K}_\bullet(\underline{x};\, R) \to \mathcal{K}_\bullet(\underline{x};\, \mathcal{B})$ that sends $1 \in R = \mathcal{K}_0(\underline{x};\, R)$ to $v \in \mathcal{B} = \mathcal{K}_0(\underline{x};\, \mathcal{B})$. Note, however, that because of the assumption that $d > n$, the last map factors through $G_d = 0$, and so is the zero map.

We can give another map of complexes $\mathcal{K}_\bullet(\underline{x};\, R) \to \mathcal{K}_\bullet(\underline{x};\, \mathcal{B})$ that sends $1 \in R = \mathcal{K}_0(\underline{x};\, R)$ to $v \in \mathcal{B} = \mathcal{K}_0(\underline{x};\, \mathcal{B})$ as follows: take the map $R \to \mathcal{B}$ that sends 1 to v and tensor over R with the complex $\mathcal{K}_\bullet(\underline{x};\, R)$ to get a map of complexes. But now the last map sends $1 \in R = \mathcal{K}_d(\underline{x};\, R)$ to $v \in \mathcal{B} = \mathcal{K}_d(\underline{x};\, \mathcal{B})$, and we are close to the desired contradiction. Because the Koszul complex of R is free and the Koszul complex of $\mathcal{B}$ is acyclic, these two maps of complexes are homotopic. Therefore, the difference of the two maps $\mathcal{K}_d(\underline{x};\, R) \to \mathcal{K}_d(\underline{x};\, \mathcal{B})$ is the composition of a map $h : \mathcal{K}_{d-1}(\underline{x};\, R) \to \mathcal{K}_d(\underline{x};\, \mathcal{B})$ with the map $\delta : \mathcal{K}_d(\underline{x};\, R) \to \mathcal{K}_{d-1}(\underline{x};\, R)$ from the complex, where h is one of the maps giving the homotopy. (There is another relevant map involved in the homotopy, from $\mathcal{K}_d(\underline{x};\, R) \to \mathcal{K}_{d+1}(\underline{x};\, \mathcal{B})$, but it is the zero map, since $\mathcal{K}_{d+1}(\underline{x};\, , \mathcal{B}) = 0$.) Since the image of δ is contained in $(x_1, \ldots, x_d)\mathcal{K}_{d-1}(\underline{x};\, R)$, the image of $h \circ \delta$ is contained in $(x_1, \ldots, x_d)\mathcal{B}$, which shows that $v \in (x_1, \ldots, x_d)\mathcal{B}$, a contradiction. $\square$

From this one can easily deduce the original intersection theorem of Peskine-Szpiro, which was proved in their joint thesis. (From Roberts's work this is known without the equicharacteristic restriction.)

Theorem (Peskine-Szpiro intersection theorem). *Let R be an equicharacteristic local ring and let $M \neq 0$, $N \neq 0$ be finitely generated R-modules such that $\mathrm{pd}_R M$ is finite and $M \otimes_R N$ has finite length. Then $\dim(N) \leq \mathrm{pd}_R M$.*

This follows at once from the new intersection theorem: let $I = \mathrm{Ann}_R N$. Then R/I has the same dimension as N, and the length of $M \otimes_R (R/I)$ is finite, since the length of $M \otimes_R N$ is finite if and only if the sum of their annihilators is primary to the maximal ideal. Therefore we may replace N by R/I. Take a minimal free resolution of M, which has length $n = \mathrm{pd}_R M$, and tensor with $S = R/I$. One gets a free complex $G_\bullet$ over S which has finite length homology: the homology is $\mathrm{Tor}^R_\bullet(M, N)$ which is killed by $\mathrm{Ann}_R(M) + \mathrm{Ann}_R(N)$. Thus, the new intersection theorem may be applied over S to conclude that $\dim(R/I) \leq n$.

Peskine and Szpiro show that the intersection theorem implies M. Auslander's zerodivisor conjecture: that conjecture asserts that if R is local, and $M \neq 0$ is finitely generated and has finite projective dimension, then any zerodivisor in the ring R is a zerodivisor on M. It follows that a regular sequence on M must be a regular sequence in R.

They also proved that the intersection theorem implies an affirmative answer to a question of Bass (eventually known as Bass's conjecture): if a local ring possesses a nonzero module of finite injective dimension then the ring must be Cohen-Macaulay. (The converse was known: a Cohen-Macaulay local ring does possess a finitely generated module of finite injective dimension.)

It is worth noting that the new intersection theorem implies the Krull height theorem in a very simple way. Let I be an n generator ideal of a Noetherian ring R. We want to see that every minimal prime of I has height at most n. We may localize the minimal prime in question. The result therefore asserts that if $x_1, \ldots, x_n$ generates an ideal primary to the maximal ideal m of the local ring (R, m), then $\dim(R) \leq n$. This follows from considering the Koszul complex $\mathcal{K}(x_1, \ldots, x_n; R)$: it has finite length homology, since the homology is killed by the m-primary ideal $(x_1, \ldots, x_n)R$, and so $\dim(R) \leq n$, as required.

We remarked during the course of the proof the new intersection theorem that the argument shows more. The difference may seem rather technical, but it turns out to be important. The stronger result is:

Theorem (improved new intersection theorem). *Let R be a local ring that contains a field. Let $0 \to G_n \to \cdots \to G_0 \to 0$ be a finite complex of finitely generated free modules such that $H_0(G_0) \neq 0$ and has a minimal generator that is killed by a power of the maximal ideal, and such that all the higher homology modules have finite length. Then $\dim(R) \leq n$.*

This result is *not* known in mixed characteristic. It can be used to prove the Evans-Griffith Syzygy Theorem, which asserts that a k th module of syzygies of a finitely generated module over a regular local ring, if it is not free, must have rank at least k. The Evans-Griffith Syzygy theorem remains open in mixed characteristic. Cf. [M. Hochster, *Canonical elements in local cohomology modules and the direct summand conjecture*, J. of Algebra **84** (1983) pp. 503–553] for the argument deducing the syzygy theorem from the improved new intersection theorem, and [E. G. Evans and P. Griffith, *Syzygies*, London Math. Soc. Lecture Note Series **106**, Cambridge Univ. Press, Cambridge, England, 1985] for further background and variant results.

We next want to turn our attention to the question, is every regular local ring a direct summand of every module-finite extension ring?

We begin by noting several reductions that are possible in considering this problem. First, $R \hookrightarrow S$ splits if and only the map

$$\mathrm{Hom}_R(S,\, R) \to \mathrm{Hom}_R(R,\, R)$$

is onto. (The map $g \in \mathrm{Hom}_R(S,\, R)$ that maps to $\mathbf{1}_R$ is the splitting of $R \hookrightarrow S$.) Since localization commutes with Hom for finitely generated modules over a Noetherian ring, we may reduce to the case where R is local. Likewise, we may reduce to the complete case, since the completion of R is faithfully flat over R and flat base change commutes with Hom for finitely generated modules over a Noetherian ring.

Thus, we may assume that the regular ring is local or even complete local. Next, we may assume that S is a domain. For we may kill a minimal prime ideal P of S disjoint from $R - \{0\}$, so that we have $R \hookrightarrow S \twoheadrightarrow S/P$ and we still have $R \hookrightarrow S/P$. The composition of a splitting $g : S/P \twoheadrightarrow R$ with the map $S \twoheadrightarrow S/P$ will split $R \hookrightarrow S$.

We shall next use the existence of big Cohen-Macaulay modules to prove that regular rings are direct summands of their module-finite extensions in equal characteristic. But we first want to note that this proof is mainly of interest in characteristic $p > 0$. In equal characteristic 0, even normal rings are direct summands of their module-finite extensions, by a very simple argument: if R is a normal domain containing the rational numbers, S is a module-finite extension domain, and the fraction fields of R and S are $\mathcal{K}$ and $\mathcal{L}$, respectively, then if $d = [\mathcal{L} : \mathcal{K}]$, the map $\dfrac{1}{d}\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}$, field trace from $\mathcal{L}$ to $\mathcal{K}$, is an R-linear retraction from S to R. (The trace of $\lambda \in L$ is the trace of multiplication by λ as a $\mathcal{K}$-linear transformation on the d-dimensional $\mathcal{K}$-vector space $\mathcal{L}$. Thus, the trace of 1 is d.) The map is *a priori* defined from $\mathcal{L} \to \mathcal{K}$ and is $\mathcal{K}$-linear. We need to check that if $s \in S$ then the trace of s is in R, not just in $\mathcal{K}$.

One argument is as follows: let f be the minimal polynomial of s over $\mathcal{K}$. Since R is normal, the coefficients are in R. Let $\mathcal{L}_0 = \mathcal{K}[s]$. Then $\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}(s) = [\mathcal{L} : \mathcal{L}_0]\mathrm{Trace}_{\mathcal{L}_0/\mathcal{K}}(s)$, and the latter is the sum of the roots of f. Since the roots of f are all integral over R, $\mathrm{Trace}_{\mathcal{L}_0/\mathcal{K}}(s)$ is integral over R as well as being in $\mathcal{K}$, and so is in R. $\square$

An alternative argument in the Noetherian case uses that a normal ring R is an intersection of discrete valuation rings $V \subseteq \mathcal{K}$: one may let V run through the localizations of R at its height one primes. One needs to see that $\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}(s)$ is in each such V. Note that $V \subseteq \mathcal{K} \subseteq \mathcal{L}$ and $S \subseteq \mathcal{L}$, and so we may form the ring $W = V[S] \subseteq \mathcal{L}$ generated over V by the elements of S. In fact, a finite set of generators for S as an R-module will also be a finite set of generators for W as a V-module. We may work with V and W instead of R and S. But now W is free over V, since W is finitely generated and torsion-free over V and V is a principal ideal domain, and so the field trace of multiplication by s may be calculated using a free basis for W over V as the basis for $\mathcal{L}$ over $\mathcal{K}$. The entries of the matrix of multiplication by s will all be in V, and so the field trace of s is in V, as required. $\square$

Lecture of April 16, 2010

Let (R, m, K) be a regular local ring of dimension d and let $x_1, \ldots, x_d$ be a regular system of parameters, so that $(x_1, \ldots, x_d) = m$. We want to give a very down-to-earth criterion for when the regular ring R splits from a module-finite extension S. Before doing so, we establish some properties of regular sequences on a module. For some of these, we refer to the Lecture Notes, Problem Sets and Problem Set Solutions from Math 615.

Proposition. *Let R be a ring, let M be an R-module, and let $x_1, \ldots, x_d$ be a sequence of elements of R. Suppose that $x_1, \ldots, x_d$ is a regular sequence on M.*

(a) *For all positive integers $a_1, \ldots, a_d$, $x_1^{a_1}, \ldots, x_d^{a_d}$ is a regular sequence on M, and if $\sum_{j=1}^d x_j^{a_j} u_j = 0$, where the $u_j \in M$, then for all j, $1 \leq j \leq d$,*

$$u_j \in (x_1^{a_1}, \ldots, x_{j-1}^{a_{j-1}}, x_{j+1}^{a_{j+1}}, \ldots, x_d^{a_d})M.$$

(b) *Let $a_1, \ldots, a_d$ be nonnegative integers and let $b_1, \ldots, b_d$ be positive integers such that $b_j > a_j$, $1 \leq j \leq d$. Then*

$$(x_1^{b_1}, \ldots, x_d^{b_d})M :_M x_1^{a_1} \cdots x_d^{a_d} = (x_1^{b_1 - a_1}, \ldots, x_d^{b_d - a_d})M.$$

(c) *For every integer $t \geq 1$, the map*

$$M/(x_1^{t-1}, \ldots, x_d^{t-1})M \to M/(x_1^t, \ldots, x_d^t)M$$

induced by multiplication by $x_1 \cdots x_d$ is injective.

(d) *Let $y = x_1 \cdots x_d$. For every positive integer t,*

$$(x_1^t, \ldots, x_d^t)M :_M (x_1, \ldots, x_d) = (x_1^t, \ldots, x_d^t, y^{t-1})M.$$

(e) *The relations on $x_1, \ldots, x_d$ in $R_t = R/I_t$, where $I_t = (x_1^t, \ldots . x_d^t)$, are spanned by the Koszul relations $x_j e_i - x_i e_j$ and the relations $x_i^{t-1} e_i$, where $e_1, \ldots, e_d$ is the standard free basis for R_t^d.*

(f) *Let $J = (x_1^{b_1}, \ldots, x_d^{b_d})$ for positive integers $b_1, \ldots, b_d$, suppose that $1 \leq h \leq d$, and let $a_1, \ldots, a_h$ be nonnegative integers such that $a_i < b_i$, $1 \leq i \leq h$. Then*

$$\bigcap_{i=1}^h \big((x_i^{a_i}) + J\big) = (x_1^{a_1} \cdots x_h^{a_h}) + J.$$

In particular, if $h < d$, $b_{h+1} = t-1$ while the other b_i are all t, so that $J = (x_{h+1}^{t-1}) + I_t$, and $a_1 = \cdots = a_h = t-1$, we obtain that for $1 \leq h < d$,

$$\bigcap_{i=1}^h \big((x_i^{t-1}) + (x_{h+1}^{t-1}) + I_t\big) = (x_1^{t-1} \cdots x_h^{t-1}) + (x_{h+1}^{t-1}) + I_t.$$

(g) *With the same hypothesis and notation as in part (e), every R_t-linear homomorphism of $(x_1, \ldots, x_d)R_t$ into R_t is induced by multiplication by some $r \in R_t$. That is, if we start with the inclusion $(x_1, \ldots, x_d)R_t \hookrightarrow R_t$ then the map induced by applying $\mathrm{Hom}_{R_t}(\_, R_t)$ is surjective. This is equivalent to the assertion that*

$$\mathrm{Ext}^1_{R_t}\big(R/(x_1, \ldots, x_d),\, R_t\big) = 0.$$

Proof. The first statement in part (a) is the Extra Credit problem in Problem Set #3 from Math 615, and, given the first statement, the second statement is immediately reduced to the case where all the $a_i = 1$. We use induction on d. If $d = 1$ and $u_1x_1 = 0$, then $u_1 = 0$. Suppose that

$$x_1u_1 + \cdots + x_du_d = 0.$$

If $j = d$ the result is immediate from the definition of a regular sequence. If not, we write

$$u_d = x_1v_1 + \cdots + x_{d-1}v_{d-1},$$

and the original relation becomes

$$x_1(u_1 + x_dv_1) + \cdots + x_{d-1}(u_{d-1} + x_dv_{d-1}) = 0.$$

The result now follows from the induction hypothesis.

We prove part (b) using induction on the number of elements among $a_1, \ldots, a_d$ that are not zero. If all of the elements are zero the statement is obvious. Now suppose that $a_j > 0$. Suppose that

$$x_1^{a_1} \cdots x_d^{a_d}u = \sum_{i=1}^{d} x_i^{b_i}u_i$$

with $u, u_1, \ldots, u_d \in M$. Let $x = \prod_{k\neq j} x_k^{a_k}$. Then

$$x_j^{a_j}(xu - x_j^{b_j-a_j}u_j) = \sum_{i\neq j} x_i^{b_i}u_i.$$

From the second statement in part (a), we see that

$$xu - x_j^{b_j-a_j}u_j = \sum_{i\neq j} x_i^{b_i}v_i,$$

for suitable $v_i \in M$, i.e.,

$$xu = x_j^{b_j-a_j}u_j + \sum_{i\neq j} x_i^{b_i}v_i.$$

This is the same type of equality that we started with, except that the exponent on x_j on the right has been reduced to $b_j - a_j$, and one more exponent occurring in x on the left,

namely, the exponent on x_j, is now zero. The desired result is now immediate from the induction hypothesis.

Part (c) is a special case of part (b): the case where all the b_j are t and all the a_j are 1.

To prove (d), let $J = (x_1^t, \dots, x_d^t)$, let $I_h = (x_{d-h+1}, \dots, x_d)$, $0 \le h \le d$, where I_0 is interpreted to be (0). Let $y_h = x_{d-h+1} \cdots x_d$, $0 \le h \le d$, where y_0 is interpreted to be 1 and $y_d = y$. We shall prove by induction on h that $JM :_M I_h = (J, y_h^{t-1})M$. The case $j = 0$ is clear: the left hand side is $JM :_M 0 = M$, and the right hand side is $(J, R)M = M$. For the inductive step, suppose that we know the result for a certain $h < d$ and that $I_{h+1}u \subseteq JM$. Then $I_h u \subseteq JM$, and so we can write u in the form $v + y_h^{t-1}w$, where $v \in JM$ and $w \in M$. To complete the argument is suffices to show that $y_h^{t-1}w \in y_{h+1}^t M + JM$. But

$$x_{d-h}(v + y_h^{t-1}w) \in JM,$$

and since $v \in JM$ we have that

$$x_{d-h}y_h^{t-1}w \in JM.$$

By part (b),

$$w \in (x_1^t, \dots, x_{d-h-1}^t, x_{d-h}^{t-1}, x_{d-h+1}, \dots, x_d)M,$$

Since the first $d-h-1$ generators are already in J, the product of y_h^{t-1} with x_{d-h}^{t-1} is y_{h+1}^{t-1}, and the product of y_h^{t-1} with each of the remaining generators is in J, the result is proved.

For part (e), note that a relation on $x_1, \dots, x_d$ mod $(x_1^t, \dots, x_d^t)R$ is expressed by an equation of the form

$$\sum_j a_j x_j = \sum_j b_j x_j^t$$

where the a_j, $b_j \in R$, and this can be rewritten as

$$\sum_j (a_j - b_j x_j^{t-1})x_j = 0,$$

where in sums indexed by j, j runs from 1 to d. This shows that $\sum_j (a_j - b_j x_j^{t-1})e_j$ is a linear combination of Koszul relations on $x_1, \dots, x_d$ even over R, and subtracting from the original relation on the x_j evidently produces a relation which is a linear combination of the relations $x_j^{t-1}e_j$.

For part (f) we use induction on h. If $h = 1$ the result is tautological. At the inductive step what we need to show is that $\big((\mu) + J\big) \cap \big((\nu) + J\big) = (\mu\nu) + J$ where $\mu = x_1^{a_1} \cdots x_h^{a_h}$ and $\nu = x_{h+1}^{a_{h+1}}$. We need only show $\subseteq$, since the opposite inclusion is obvious. For an element u of the intersection we have $u = \mu v + j = \nu w + j'$ where $j, j' \in J$ and then $\mu v \in (\nu) + J$ and so $v \in \big((\nu) + J\big) : R\mu$. From part (b), this is

$$(x_1^{b_1 - a_1}, \dots, x_h^{b_h - a_h}, x_{h+1}^{a_{h+1}}) + J.$$

But μ times any of the first h generators is in J, and so $\mu v \in (\mu\nu) + J$, and the same holds for $u = \mu v + j$.

For part (g) suppose that $r_1, \ldots, r_d$ are elements of R such that there is a homomorphism $(x_1, \ldots, x_d)R_t \to R_t$ whose values on the images of $x_1, \ldots, x_d$ are represented by the images of $r_1, \ldots, r_d$. Then for all i and j,

$$r_j x_i - r_i x_j \in (x_1^t, \ldots, x_d^t),$$

and for all j,

$$r_j x_j^{t-1} \in (x_1^t, \ldots, x_d^t).$$

From part (b), it follows that

$$r_j \in (x_1^t, \ldots, x_{j-1}^t, x_j, x_{j+1}^t, \ldots, x_d^t),$$

and since we are free to alter each r_j by subtracting an element of I_t, we may assume without loss of generality that $r_j = s_j x_j$ for all j. We then find that $s_j x_j x_i - s_i x_i x_j = (s_j - s_i) x_i x_j \in I_t$ for all i, j, and so, again by part (b),

$$s_j - s_i \in (x_i^{t-1}, x_j^{t-1}) + (x_k^t : k \neq i, j).$$

We shall show by induction on h, $1 \leq h \leq d$, that $s_1, \ldots, s_h$ can be replaced by a single element $s \in S$ such that, mod I_t, $sx_i = s_i x_i$, $1 \leq i \leq h$. This is clear if $h = 1$. Now suppose that we have proved the result for $1 \leq h < d$. Then we may assume that $s_1 = \cdots = s_h = s$. Then $s_{h+1} - s \in (x_i^{t-1}, x_{h+1}^{t-1}) + (x_k^t : k \neq i, h+1)$ for $1 \leq i \leq h$, and we may intersect all of these ideals. The intersection is $\left((x_1 \cdots x_h)^{t-1}\right) + (x_{h+1}^{t-1}) + I_t$ by part (f). Thus, we may write

$$s_{h+1} - s = (x_1 \cdots x_h)^{t-1} v + x_{h+1}^{t-1} w + z$$

where $z \in I_t$, and so we may let

$$s' = s_{h+1} - x_{h+1}^{t-1} w - z = s + (x_1 \cdots x_h)^{t-1} v.$$

We now see that we can use s' instead of s or s_{h+1}, since $s' x_i \equiv s x_i$ mod I_t for $i \leq h$ (we have that x_i^{t-1} divides $s' - s$), and $s' x_{h+1} \equiv s_{h+1} x_{h+1}$ mod I_t (we have that, mod I_t, x_{h+1}^{t-1} divides $s_{h+1} - s$). This completes the inductive step. The homomorphism coincides with multiplication by s, where s is the element that is obtained in the case where $h = d$. $\square$

We give an alternative proof of part (g) of the preceding Proposition due to Yongwei Yao. This result is more general, but uses machinery other than elementary properties of regular sequences. The result of part (g) follows from the last statement in part (b) of the Proposition below in the case where $y_j = x_j^t$, $1 \leq j \leq d$, $M = R/(x_1, \ldots, x_d)R$ and $N = R$.

Proposition. *Let R be a ring, and let M and N be R-modules.*

(a) *Let $y \in R$ be such that $yM = 0$ and y is a nonzerodivisor on both R and N. Then $\operatorname{Ext}^i_{R/yR}(M, N/yN) \cong \operatorname{Ext}^{i+1}_R(M, N)$ for all $i \geq 0$.*

(b) *Let $\underline{y} = y_1, \ldots, y_d \in R$ be a regular sequence on R and N such that $(y_1, \ldots, y_d)M = 0$. Then $\operatorname{Ext}^i_{R/(\underline{y})}\big(M, N/(\underline{y})N\big) \cong \operatorname{Ext}^{i+d}_R(M, N)$. In particular, if $\operatorname{pd}_R M \leq d$, then for all $j > 0$, $\operatorname{Ext}^j_{R/(\underline{y})}\big(M, N/(\underline{y})N\big) = 0$.*

Proof. The first statement in part (b) is immediate from part (a) by induction on d, and the second statement in part (b) is immediate from the first statement. It remains only to prove part (a).

We give a separate proof when $i = 0$, although the result in this case can also be deduced along the same lines as in the argument below for the case $i > 0$.

If $i = 0$, note that applying $\operatorname{Hom}_R(M, \_)$ to the short exact sequence

$$0 \longrightarrow N \xrightarrow{y} N \longrightarrow N/yN \longrightarrow 0$$

yields a long exact sequence part of whose beginning is

$$\operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(M, N/yN) \xrightarrow{\delta} \operatorname{Ext}^1_R(M, N) \xrightarrow{y} \operatorname{Ext}^1_R(M, N) \longrightarrow \cdots .$$

Note that $\operatorname{Hom}_R(M, N) = 0$, that $\operatorname{Hom}_R(M, N/yN) \cong \operatorname{Hom}_{R/yR}(M, N/yN)$, and that multiplication by y is the zero map on $\operatorname{Ext}^1_R(M, N)$, so that δ induces an isomorphism $\operatorname{Hom}_R(M, N/yN) \xrightarrow{\cong} \operatorname{Ext}^1_R(M, N)$ as required. Henceforth we assume that $i \geq 1$.

Let $0 \to N \to E^0 \to E^1 \to \cdots \to E^n \to \cdots$ be an injective resolution of N, and let $E^\bullet$ be the complex $0 \to E^0 \to E^1 \to \cdots \to E^n \to \cdots$. The cohomology of the complex $\operatorname{Hom}_R(R/yR, E^\bullet)$ is $\operatorname{Ext}^\bullet_R(R/yR, N)$, which we may compute from the projective resolution $0 \to R \xrightarrow{y} R \to 0$ of R/yR: thus, $\operatorname{Hom}(R/yR, N) = 0$ and $\operatorname{Ext}^1_R(R/yR, N) \cong N/yN$, while $\operatorname{Ext}^i_R(R/yR, N) = 0$ for $i \geq 2$. Let $\overline{E}_i$ denote

$$\operatorname{Hom}_R(R/yR, E_i) \cong \operatorname{Ann}_{E_i} y,$$

Note that if E is injective over R, then $\overline{E} = \operatorname{Hom}_R(R/yR, E)$ is an injective module over R/yR: in fact, the functor $Q \mapsto \operatorname{Hom}_{R/yR}(Q, \overline{E})$ on (R/yR)-modules is isomorphic with the functor $Q \mapsto \operatorname{Hom}_R(Q, E)$ on (R/yR)-modules, since the image of a map $Q \to E$ must consist entirely of elements killed by y and so must be contained in $\overline{E}$.

Since $H^0(\overline{E}^\bullet) = 0$, $\overline{E}^0$ injects into $\overline{E}^1$ as a submodule of the module of cocycles $Z^1 \subseteq \overline{E}^1$: the image of $\overline{E}^0$ is the module of coboundaries B^1. Since $\overline{E}_0$ is injective over R/yR, it splits from $\overline{E}^1$, and so $\overline{E}^{1\prime} = \overline{E}^1/B^1$ is injective. Now, $Z^1/B^1 = Z^1/\overline{E}^1 = \operatorname{Ext}^1_R(R/yR, N) \cong N/yN$, and is the kernel of the map from $\overline{E}^{1\prime} \to \overline{E}^2$. This yields an exact sequence $0 \to N/yN \to \overline{E}^{1\prime} \to \overline{E}^2 \to \overline{E}^3 \cdots$ which is an injective resolution of N/yN over R/yR, with the numbering shifted by one from the usual numbering.

If we apply $\operatorname{Hom}_{R/yR}(M, \_)$ to

$$0 \to \overline{E}^{1\prime} \to \overline{E}^2 \to \overline{E}^3 \to \cdots$$

and take cohomology, we get the modules $\operatorname{Ext}^{\bullet}_{R/yR}(M, N/yN)$, with the term of the complex indexed by $i+1$ corresponding to $\operatorname{Ext}^i_{R/yR}(M, N/yN)$. We get the same cohomology at the spots indexed by 2, 3, ... by applying $\operatorname{Hom}_R(M, \_)$ to

$$0 \to E^0 \to E^1 \to E^2 \to E^3 \cdots \to .$$

Again, because M is killed by y, a map of M to E_i is the same as a map of M to $\overline{E}_i$. This cohomology will be $\operatorname{Ext}^{i+1}_R(M, N)$ as claimed, $i \geq 1$. When $i = 1$, one needs to make the observation as well that the image of $\operatorname{Hom}_R(M, \overline{E}_1) \to \operatorname{Hom}_R(M, \overline{E}_2)$ is the same as the image of $\operatorname{Hom}_R(M, \overline{E}_1{}') \to \operatorname{Hom}_R(M, \overline{E}_2)$, since $\overline{E}_0$ is in $\operatorname{Ker}(\overline{E}^1 \to \overline{E}^2)$ and $0 \to \overline{E}^0 \to \overline{E}^1 \to \overline{E}_1{}' \to 0$ is split exact. $\square$

Lecture of April 19, 2010

Theorem. *Let let (R, m, K) be a regular ring and let $x_1, \ldots, x_d$ be a regular system of parameters. Let $I_t = (x_1^t, \ldots, x_d^t)R$ and let $R_t = R/I_t$. Let $y = x_1 \cdots x_d$.*

(a) *The ring R_t has a one-dimensional socle represented by the element y^{t-1}. Hence, every ideal of R strictly larger than I_t contains y^{t-1}.*

(b) *The ring R_t is injective as an R_t-module.*

(c) *The map of R-modules $R_t \to R_{t+1}$ induced by multiplication by y mapping $R \to R$ is injective, and the direct limit $E = \varinjlim_t R_t$, where every map is induced by multiplication by y, is an injective R-module.*

(d) *If R is complete and E is as in part (c), the map $R \to \operatorname{Hom}_R(E, E)$ is an isomorphism.*

Proof. Since R is regular, it is Cohen-Macaulay, and every system of parameters is a regular sequence.

For (a), since $m = (x_1, \ldots, x_d)$, the result follows from the fact that

$$I_t :_R (x_1, \ldots, x_d) = I_t + y^{t-1}R,$$

which is immediate from part (d) of the first Proposition above.

To prove (b), first note that by part (2) of the third Proposition on the fifth page of the Lecture Notes of March 22 from Math 615, to establish that R_t is injective it suffices to show that $\operatorname{Ext}^1_{R_t}(R_t/\mathfrak{A}, R_t) = 0$ for every ideal $\mathfrak{A}$ of R_t. Now if M has a finite filtration with factors M_j such that $\operatorname{Ext}^t_{R_t}(M_j, N) = 0$ for all j, then $\operatorname{Ext}^t_{R_t}(M, N) = 0$ (if there are just two factors this follows from the long exact sequence for Ext; the general case follows by induction on the number of factors). Since R_t is Artinian, $R_t/\mathfrak{A}$ has a finite filtration in which all the factors are copies of K. It follows that R_t is injective if $\operatorname{Ext}^1_{R_t}(K, R_t) = 0$. But this is part (g) of the first Proposition.

The first statement in part (c) follows from part (d) of the Proposition on the first page. To see that E is injective, note that by the Proposition on the second page of the Lecture Notes of March 19 from Math 615, it suffices to show that every map of an ideal I of R to E extends to R. Since I is finitely generated, the map $I \to E$ factors $I \to R_t \hookrightarrow E$ for all sufficiently large t. The map $I \to R_t$ kills $I_t I$. For $s \gg 0$, $I_s \cap I \subseteq I_t I$ by the Artin-Rees lemma, since I_s is contained in arbitrarily high powers of m for $s \gg 0$. Thus, we have an induced map $I/(I_s \cap I) \twoheadrightarrow I/I_t I \to R_t \hookrightarrow R_s$ for $s \gg 0$. Here, $I/(I_s \cap I) \cong (I + I_s)/I_s \subseteq R/I_s$. Since R_s is injective as an R_s-module, this map extends to a map $R/I_s \to R_s \hookrightarrow E$, giving a map $R \twoheadrightarrow R/I_s \to R_s \hookrightarrow E$. This map extends the original map $I \to E_t \subseteq E$.

It remains to prove part (d). First note that $\operatorname{Ann}_E I_t$ is the copy of R_t in the direct limit system. It contains the copy of R_t, obviously. The fact that it agrees with R_t is equivalent to the assertion that for all $s > t$, the annihilator of I_t in R/I_s is spanned by the image of y^{s-t} (since this element spans the image of R_t in R_s in the direct limit system), i.e., that

$$(x_1^s, \ldots, x_d^s) :_R (x_1^t, \ldots, x_d^t) = (x_1^s, \ldots, x_d^s) + y^{s-t}.$$

But

$$(x_1^s, \ldots, x_d^s) :_R (x_1^t, \ldots, x_d^t) = \bigcap_j (x_1, \ldots, x_s) :_R x_j^t = \bigcap_j \big((x_j^{s-t}) + I_s\big),$$

by part (b) of the first Proposition. The result we need now follows from part (f) of the first Proposition.

Thus, every endomorphism of E stabilizes the image of R_t for all t. Any endomorphism of R_t is evidently given by multiplication by a unique element of R_t, and so $\operatorname{Hom}_R(E, E)$ may be identified with $\varprojlim_t R_t \cong \widehat{R} \cong R$, as required. $\square$

Theorem. *Let (R, m, K) be a regular local ring and let $x_1, \ldots, x_d$ be a regular system of parameters in R. Let $I_t = (x_1^t, \ldots, x_d^t)R$. Let M be a finitely generated R-module, and $R \hookrightarrow M$ an injection such that $1 \mapsto u \in M$. Then $R \to M$ splits if and only if $I_t M \cap Ru = I_t u$ for every positive integer t.*

In particular if $R \subseteq S = M$ is an R-algebra, $R \to S$ splits if and only if $I_t S \cap R = I_t$ for every positive integer t. Hence, $R \to S$ splits if and only if $x_1^{t-1} \cdots x_d^{t-1} \notin I_t S$ for all t.

Proof. Let $\phi : M \to R$ be a splitting and let I be any ideal of R. Suppose that $ru \in IM$. Applying ϕ, we get that $r\phi(u) \in IR = I$, so that $IM \cap Ru = Iu$ for every ideal I of R. This shows that the stated condition is necessary for splitting.

$R \hookrightarrow M$ splits if and only if the induced map $\operatorname{Hom}_R(M, R) \to \operatorname{Hom}_R(R, R)$ is onto, and this is unaffected by completion, since Hom commutes with flat base change for Noetherian modules over a Noetherian ring and $\widehat{R}$ is faithfully flat over R. Thus, we may assume that R is complete without loss of generality. Note also that $R/I_t \cong \widehat{R}/I_t\widehat{R}$ for all t, and that $M/I_t M \cong \widehat{M}/I_t\widehat{M}$ for all t.

Since $R/I_t \to M/I_tM \cong (R/I_t) \otimes_R M$ is injective for all t, we may take a direct limit and obtain that $E \to E \otimes_R M \cong M \otimes_R E$ is injective, where E is constructed as in part (c) of the preceding Theorem and is injective over R. Applying $\mathrm{Hom}_R(\_, E)$ we find that the map $\mathrm{Hom}_R(M \otimes_R E, E) \to \mathrm{Hom}_R(E, E)$ is surjective, and by the adjointness of tensor and Hom, the left hand module may be identified with $\mathrm{Hom}_R\big(M, \mathrm{Hom}_R(E, E)\big)$. By part (d) of the preceding Theorem, $R \to \mathrm{Hom}_R(E, E)$ is an isomorphism, and so we have that the map $\mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(R, R)$ is surjective, as required.

The very last statement follows because $x_1^{t-1} \cdots x_d^{t-1}$ generates the socle in R/I_t, and so every ideal of R strictly larger than I_t contains $x_1^{t-1} \cdots x_d^{t-1}$. Thus, if $I_tS \cap R$ is strictly larger than I_t, it must contain $x_1^{t-1} \cdots x_d^{t-1}$: see part (a) of the preceding Theorem. $\square$

Conjecture (monomial conjecture). *Let $x_1, \ldots, x_d$ be be elements of a Noetherian ring R that generate an ideal of height d. Then for every positive integer t,*

$$x_1^{t-1} \cdots x_d^{t-1} \notin (x_1^t, \ldots, x_d^t)R.$$

If one has a counterexample, one can always localize at a minimal prime of $(x_1, \ldots, x_d)R$ of height d, and so obtain a counterexample in a local ring of dimension d in which $x_1, \ldots, x_d$ is a system of parameters. One can then complete, and so get a counterexample in a complete local ring. One can also kill a minimal prime so as to get a new counter-example in a complete local domain for which $x_1, \ldots, x_d$ is a system of parameters. We shall not completely prove the following result: for one of the implications in mixed characteristic we give a reference.

Theorem. *For local domains of a given characteristic (where this may refer to mixed characteristic p) and a given dimension d, the direct summand conjecture for regular local rings of that dimension and characteristic is equivalent to the monomial conjecture for systems of parameters of local rings of that dimension and characteristic.*

Proof. Assume the monomial conjecture in that dimension and characteristic. It suffices to prove the direct summand conjecture for complete regular local rings R of that dimension and characteristic and module-finite extension domains S of R. Let $x_1, \ldots, x_d$ be a regular system of parameters for R. Then it is also a system of parameters for S. The monomial conjecture applied to $x_1, \ldots, x_d$ and S shows that R is a direct summand of S, by the last statement of the preceding Theorem.

Now let S be a complete equicharacteristic domain and $x_1, \ldots, x_d$ a system of parameters for S. Let K be a coefficient field for S. Let $R = K[[x_1, \ldots, x_d]] \subseteq S$: R is regular and S is module-finite over R. The direct summand conjecture for R shows that R to S splits, and the fact that

$$x_1^{t-1} \cdots x_d^{t-1} \notin (x_1^t, \ldots, x_d^t)S$$

now follows from the final statement of the preceding Theorem.

For the mixed characteristic case of this result we refer the reader to [M. Hochster, *The direct summand conjecture and canonical elements in local cohomology modules*, J. of Algebra **84** (1983), 503–553]. $\square$

We have already established the existence of big Cohen-Macaulay modules in equal characteristic. This immediately yields the monomial conjecture and, hence, the direct summand conjecture.

Theorem. *The monomial conjecture holds for every local ring that has a big Cohen-Macaulay module. In fact, the monomial conjecture holds for every sequence of elements $x_1, \ldots, x_d$ that is a regular sequence on some module M.*

Hence the monomial conjecture holds for Noetherian rings that contain a field, and a regular ring that contains a field is a direct summand of every module-finite extension algebra.

Proof. First note that if $x_1, \ldots, x_d$ is a regular sequence on M, then

$$(x_1^t, \ldots, x_d^t)M :_M x_1^{t-1} \cdots x_d^{t-1} = (x_1, \ldots, x_d)M$$

(by part (b) of the first Proposition), and $(x_1, \ldots, x_d)M \neq M$ by the definition of a regular sequence. Thus,

$$(x_1^{t-1} \cdots x_d^{t-1})M \notin (x_1^t, \ldots, x_d^t)M,$$

and therefore

$$x_1^{t-1} \cdots x_d^{t-1} \notin (x_1^t, \ldots, x_d^t)R.$$

This proves the statement in the second sentence of the Theorem, and the statement in the first sentence is then immediate. The monomial conjecture for equicharacteristic rings follows because it reduces to the local case, and we have shown the existence of big Cohen-Macaulay modules in the local case for equicharacteristic rings. The final result is immediate from the preceding Theorem. □

We conclude with some discussion of the notion of the *superheight* of an ideal I of a Noetherian ring R. If I is a proper ideal of R, we define the *superheight* of I as the supremum of heights of ideals IS, where $R \to S$ is a map of Noetherian rings such that IS is a proper ideal of S. (By convention, the height of the unit ideal is $+\infty$.) We want to make several observations about this notion.

First, the Krull height theorem is the same as the statement the the superheight of $\mathfrak{A} = (X_1, \ldots, X_d)$ in the polynomial ring $\mathbb{Z}[X_1, \ldots, X_d]$ is d, since the expansions $\mathfrak{A}$ to various choices of S are the same as the ideals with at most d generators in the various Noetherian rings S. It follows that the superheight of any ideal is at most the number of generators of that ideal. Since two ideals with the same radical have the same height, they also have the same superheight, and the superheight of I is bounded by the least number of generators of an ideal J such that J and I have the same radical.

If $R \to S$ is such that the height of IS is the superheight of I, this remains true when we local IS at a suitable minimal prime of IS, complete, and kill a suitable minimal prime. Thus, in the definition of superheight, it suffices to allow S to run through complete local domains to which R maps such that IS is primary to the maximal ideal of S.

Consider the following example: let K be a field, let $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ be indeterminates over K, let $T = K[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, and let P be the ideal generated by the size 2 minors of the matrix

$$\begin{pmatrix} X_1 & \cdots & X_n \\ Y_1 & \cdots & Y_n \end{pmatrix}.$$

Let $R = T/P$. It is known that R is a domain of dimension $n+1$. (See **3.** in Problem Set #4, Math 614, Fall 2003, and its solution, where it is shown that the corresponding algebraic set is irreducible: this at least shows that the radical of the ideal is prime. The open set where the first row is not 0 is dense. One sees that the dimension is $n+1$ because the matrix determines and is determined by the nonzero first row and the scalar whose product with the first row gives the second row. For a complete treatment of varieties of this type, see [M. Hochster and J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93** (1971), 1020–1058].) Let $I = (X_1, \ldots, X_n)R$. Then $R/I = K[Y_1, \ldots, Y_n]$ has dimension n, and so I is a height one prime ideal of R. Let $J = (Y_1, \ldots, Y_n)R$. Then $S = R/J \cong K[X_1, \ldots, X_n]$, a polynomial ring in n variables over K. The expansion of I to S has height n. Thus, even though I has height one, its superheight is n.

The problem of determining the superheight of an ideal is extremely difficult. Let Λ denote either a field or the integers $\mathbb{Z}$. Let

$$R_{d,t} = \Lambda[X_1, \ldots, X_d, Y_1, \ldots, Y_d]/F_{t,d},$$

where

$$F_{t,d} = X_1^{t-1} \cdots X_d^{t-1} - \sum_{j=1}^{d} Y_j X_j^t.$$

Let $I = (X_1, \ldots, X_d)R$. Then the monomial conjecture is precisely equivalent to the statement that, when $\Lambda = \mathbb{Z}$, the superheight of I is $d-1$. It is easy to see that it must be $d-1$ or d. But the question of which it is remains open if $\Lambda = \mathbb{Z}$ and $d \geq 4$. The direct summand conjecture is known to hold for rings containing a field, and so the superheight is $d-1$ if Λ is a field, but this is not obvious. The direct summand conjecture and even the existence of big Cohen-Macaulay algebras are known in mixed characteristic in dimension at most three (see [R. Heitmann, *The direct summand conjecture in dimension three*, Annals of Math. (2) **156** (2002) 695–712] and [M. Hochster, *Big Cohen-Macaulay algebras in dimension three via Heitmann's theorem*, J. Algebra **254** (2002) 395–408]. Thus the superheight is known to be $d-1$ when $\Lambda = \mathbb{Z}$ if $d \leq 3$.

The following result, which we will prove in seminar next semester, is essentially due to Serre:

Theorem. *If P is a prime ideal of a regular ring, the superheight of P is equal to the height of P.*

One can reduce to the case where R is regular local. Then, when S has the form R/Q, one needs to see that the height of $P(R/Q)$ is at most the height of P. This is Serre's

result, in [J.-P. Serre, *Algèbre Locale • Multiplicités*, Lecture Notes in Math. **11**, Springer-Verlag, Berlin • Heidelberg • New York, 1965]. The general case can be reduced to this one.

Note that this Theorem is a vast generalization of the Krull height theorem, which is the case where $R = \mathbb{Z}[X_1, \ldots, X_d]$ and $P = (X_1, \ldots, X_d)$.