Math 711: Lecture of September 6, 2006

These lectures will deal with several advanced topics in commutative algebra, including the behavior of codimension after base change. However, we will begin with the Lipman-Sathaye Jacobian theorem and its applications, including, especially, the Briançon-Skoda theorem.

A special (but very important) case of the Lipman-Sathaye theorem is as follows:

Theorem (Lipman-Sathaye). *Let $R \subseteq S$ be a homomorphism of Noetherian domains such that R is regular and S is a localization of a finitely generated R-algebra. Assume that the integral closure S' of S is module-finite over S and that the extension of fraction fields* $\mathrm{frac}\,(S)/\mathrm{frac}\,(R)$ *is a finite separable algebraic extension. Then the Jacobian ideal $\mathcal{J}_{S/R}$ multiplies S' into S.*

Both the Jacobian ideal and the notion of integral closure will be treated at length below. We shall also prove a considerably sharper version of the theorem, in which several of the hypotheses are weakened. An algebra S that is a localization of a finitely generated R-algebra is called *essentially of finite type* over R. The hypothesis that the integral closure of S is module-finite over S is a weak assumption: it holds whenever S is essentially of finite type over a field or over a complete local ring, and it tends to hold for the vast majority of rings that arise naturally: most of the rings that come up are *excellent*, a technical notion that implies that the integral closure is module-finite.

While the Briançon-Skoda theorem can be proved in equal characteristic by the method of reduction to characteristic $p > 0$, where tight closure methods may be used, the only known proof in mixed characteristic uses the Lipman-Sathaye theorem. Another application is to the calculation of the integral closure of a ring, while a third is to the construction of test elements for tight closure theory. Our emphasis is definitely on the Briançon-Skoda theorem which, in one of its simplest forms, may be formulated as just below. We shall denote by $\overline{J}$ the integral closure of the ideal J: integral closure of ideals will be discussed in detail in the sequel.

Theorem (Briançon-Skoda). *If I is an ideal of a regular ring and is generated by n elements, then $\overline{I^n} \subseteq I$.*

Before beginning our discussion of integral closure, we mention two corollaries of the Briançon-Skoda theorem that are of some interest. First:

Corollary. *Suppose that $f \in \mathbb{C}\{z_1, \ldots, z_n\}$ is a convergent power series in n variables with complex coefficients that defines a hypersurface with an isolated singularity at the origin, i.e., f and its partial derivatives $\partial f/\partial z_i$, $1 \leq i \leq n$, have an isolated common zero at the origin. Then f^n is in the ideal generated by the partial derivatives of f in the ring $\mathbb{C}\{z_1, \ldots, z_n\}$.*

This answers affirmatively a question raised by John Mather. Second:

Corollary. *Let $f_1, \ldots, f_{n+1}$ be polynomials in n variables over a field. Then $f_1^n \cdots f_n^n \in (f_1^{n+1}, \ldots, f_{n+1}^{n+1})$.*

For example, when $n = 2$ this implies that if $f, g, h \in K[x, y]$ are polynomials in two variables over a field K then $f^2g^2h^2 \in (f^3, g^3, h^3)$. This statement is rather elementary: the reader is challenged to prove it by elementary means.

We shall need to develop the subject a bit before we can see why these are corollaries: we postpone the explanation for the moment.

In these notes all given rings are assumed to be commutative, associative, and to have a multiplicative identity 1, unless otherwise stated. Most often given rings will be assumed to be Noetherian as well, but we postpone making this a blanket assumption.

Our next objective is to review some facts about integral elements and integral ring extensions.

Recall that if $R \subseteq S$ are rings then $s \in S$ is *integral* over R if, equivalently, either

(1) s satsifies a monic polynomial with coefficients in R or

(2) $R[s]$ is finitely generated as an R-module.

The elements of S integral over R form a subring of S containing R, which is called the *integral closure* of R in S. If S is an R-algebra, S is called *integral* over R if every element is integral over the image of R in S. S is called *module-finite* over R if it is finitely generated as an R-module. If S is module-finite over R it is integral over R. S is module-finite over R if and only if it is finitely generated as an R-algebra and integral over R. S is integral over R if and only if every finitely generated R-subalgebra is module-finite over R.

Given a commutative diagram of algebras

$$\begin{array}{ccc} S & \xrightarrow{\ f\ } & U \\ \uparrow & & \uparrow \\ R & \longrightarrow & T \end{array}$$

and an element $s \in S$ integral over the image of R, the image of S in U is integral over the image of T. One can see this simply by applying the homomorphism f to the monic equation s satisfies. When the vertical maps are inclusions, we see that the integral closure of R in S maps into the integral closure of T in U.

Note also that if $R \to S$ and $S \to T$ are both module-finite (respectively, integral) then $R \to T$ is also module-finite (respectively, integral).

The total quotient ring of the ring R is $W^{-1}R$, where W is the multiplicative system of all nonzerodivisors. We have an injection $R \hookrightarrow W^{-1}R$. If R is a domain, its total quotient ring is its field of fractions. If R is reduced, R is called *normal* or *integrally closed* if it is integrally closed in its total quotient ring. Thus, a domain R is integrally closed if and only if every fraction that is integral over R is in R.

Let $(H, +)$ be an additive commutative semigroup with additive identity 0. A commutative ring R is said to be *H-graded* if it has a direct sum decomposition

$$R \cong \bigoplus_{h \in H} R_h$$

as abelian groups such that $1 \in R_0$ and for all $h, k \in H$, $R_h R_k \subseteq R_{h+k}$. Elements of R_h are then called *homogeneous elements* or *forms* of *degree* h. If s is the sum of nonzero forms $s_1 + \cdots + s_n$ of mutually distinct degrees h_i, then $s_i \in R_{h_i}$ is called the *homogenous component* of s of degree h_i. The homogeneous components in other degrees are defined to be 0. The most frequent choices for H are the nonnegative integers $\mathbb{N}$ and the integers $\mathbb{Z}$.

Theorem. *Let $R \subseteq S$ be an inclusion of $\mathbb{N}$-graded (or $\mathbb{Z}$-graded) rings compatible with the gradings, i.e., such that $R_h \subseteq S_h$ for all h. Then the integral closure of R in S is also compatibly graded, i.e., every homogeneous component of an element of S integral over R is integral over R.*

Proof. First suppose that R has infinitely many units of degree 0 such that the difference of any two is a unit. Each unit u induces an endomorphism θ_u of R whose action on forms of degree d is multiplication by u^d. Then $\theta_u \theta_v = \theta_{uv}$, and θ_u is an automorphism whose inverse is $\theta_{u^{-1}}$. These automorphisms are defined compatibly on both R and S: one has a commutative diagrams

$$\begin{array}{ccc} S & \xrightarrow{\theta_u} & S \\ \uparrow & & \uparrow \\ R & \xrightarrow[\theta_u]{} & S \end{array}$$

for every choice of unit u. If $s \in S$ is integral over R, one may apply θ_u to the equation of integral dependence to obtain an equation of integral dependence for $\theta_u(s)$ over R. Thus, θ_u stabilizes the integral closure T of R in S. (This is likewise true for $\theta_{u^{-1}}$, from which one deduces that θ_u is an automorphism of T, but we do not really need this.)

Suppose we write

$$s = s_{h+1} + \cdots + s_{h+n}$$

for the decomposition into homogeneous components of an element $s \in S$ that is integral over R, where each s_j has degree j. What we need to show is that each s_j is integral over R. Choose units $u_1, \ldots, u_n$ such that for all $h \neq k$, $u_h - u_k$ is a unit — we are assuming that these exist. Letting the θ_{u_i} act, we obtain n equations

$$u_i^{h+1} s_{h+1} + \cdots + u_i^{h+n} s_{h+n} = t_i, \quad 1 \leq j \leq n,$$

where $t_i \in T$. Let M be the $n \times n$ matrix $\left(u_i^{h+j}\right)$. Let V be the $n \times 1$ column vector $\begin{pmatrix} s_{h+1} \\ \vdots \\ s_{h+n} \end{pmatrix}$ and let W be the $n \times 1$ column vector $\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}$. In matrix form, the displayed equations are equivalent to $MV = W$. To complete this part of the argument, it will suffice to show that the matrix M is invertible over R, for then $V = M^{-1}W$ will have entries in T, as required. We can factor u_i^{h+1} from the i th row for every i: since all the u_i are units, this does not affect invertibility and produces the Van der Monde matrix $\big(u_i^{j-1}\big)$. The determinant of this matrix is the product

$$\prod_{j>i}(u_j - u_i)$$

(see the Discussion below), which is invertible because every $u_j - u_i$ is a unit.

In the general case, suppose that

$$s = s_{h+1} + \cdots + s_{h+n}$$

as above is integral over R. Let t be an indeterminate over R and S. We can give this indeterminate degree 0, so that $R[t] = R_0[t] \otimes_{R_0} R$ is again a graded ring, now with 0 th graded piece $R_0[t]$, and similarly $S[t]$ is compatibly graded with 0 th graded piece $S_0[t]$. Let $U \subseteq R_0[t]$ be the multiplicative system consisting of products of powers of t and differences $t^j - t^i$, where $j > i \geq 0$. Note that U consists entirely of monic polynomials. Since all elements of U have degree 0, we have an inclusion of graded rings $U^{-1}R[t] \subseteq U^{-1}S[t]$. In $U^{-1}R[t]$, the powers of t constitute infinitely many units of degree 0, and the difference of any two distinct powers is a unit. We may therefore conclude that every s_j is integral over $U^{-1}R[t]$, by the case already done. We need to show s_j is integral over R itself.

Consider an equation of integral dependence

$$s_j^d + f_1 s_j^{d-1} + \cdots + f_d = 0,$$

where every $f_i \in U^{-1}R[t]$. Then we can pick an element $G \in U$ that clears denominators, so that every $Gf_i = F_i \in R[t]$, and we get an equation

$$Gs_j^d + F_1 s_j^{d-1} + \cdots + F_d = 0.$$

Let G have degree m, and recall that G is monic in t. The coefficient of t^m on the left hand side, which is an element of S, must be 0, and so its degree jd homogeneous component must be 0. The contribution to the degree jd component of this coefficient from Gs_j^d is, evidently, s_j^d, while the contribution from $f_i s_j^{d-i}$ clearly has the form $r_i s_j^{d-i}$, where $r_i \in R$ has degree ji. This yields the equation

$$s_j^d + r_1 s_j^{d-1} + \cdots + r_d = 0,$$

and so s_j is integral over R, as required. $\square$

Discussion: Van der Monde matrices. Let $u_1, \ldots, u_n$ be elements of a commutative ring. Let M be the $n \times n$ matrix $\big(u_i^{j-1}\big)$.

(a) We want to show that the determinant of M is $\prod_{j>i}(u_j - u_i)$. Hence, M is invertible if $u_j - u_i$ is a unit for $j > i$. It suffices to prove the first statement when the u_i are indeterminates over $\mathbb{Z}$. Call the determinant D. If we set $u_j = u_i$, then D vanishes because two rows become equal. Thus, $u_j - u_i$ divides D in $\mathbb{Z}[u_1, \ldots, u_n]$. Since the polynomial ring is a UFD and these are relatively prime in pairs, the product P of the $u_j - u_i$ divides D. But they both have degree $1 + 2 + \cdots + n - 1$. Hence, $D = aP$ for some integer a. The monomial $x_2 x_3^2 \cdots x_n^{n-1}$ obtained from the main diagonal of matrix in taking the determinant occurs with coefficient 1 in both P and D, so that $a = 1$. $\square$

(b) We can also show the invertibility of M as follows: if the determinant is not a unit, it is contained in a maximal ideal. We can kill the maximal ideal. We may therefore assume that the ring is a field K, and the u_i are mutually distinct elements of this field. If the matrix is not invertible, there a nontrivial relation on the columns with coefficients $c_0, \ldots, c_{n-1}$ in the field. This implies that the nonzero polynomial

$$c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

has n distinct roots, $u_1, \ldots, u_n$, in the field K, a contradiction. $\square$