The Module of Differentials, Evolutions, and the Eisenbud-Mazur Conjecture

Adam Boocher

A Senior Thesis

Presented to the Faculty

of the University of Notre Dame

in Partial Fulfillment of the Requirements

for the Degree

of Bachelor of Science in Mathematics

Claudia Polini, Advisor

April 2008

Acknowledgements

I am deeply grateful for the help of my thesis advisor Claudia Polini, and for the countless hours she devoted to the development of this thesis. I am especially thankful for her extensive help with corrections and revisions. Her support, encouragement, and enthusiasm throughout our two years of directed readings have had an invaluable effect on me as a student. Our discussions about commutative algebra, mathematics, and life have had a great impact on many areas of my life, and I have sincerely enjoyed working on this project.

I would also like to thank Bernd Ulrich for the use of his wonderful lecture notes in Commutative Algebra, specifically his notes on the module of differentials. Conversations with Prof. Ulrich and his graduate students led to a better understanding of many of the proofs presented in this paper.

I would like to thank Liviu Nicolaescu, Misha Gekhtman, Frank Connolly, Susan Loepp, Jim Hoste, Sam Evens, Juan Migliore, Nero Budur, and all of my professors at Notre Dame for their support and encouragement during my time here. Finally, I would like to thank Angela Kohlhaas and Bonnie Smith for many helpful conversations in their office and during seminars.

Contents

Chapter 1

Introduction

Differentiation is one of the first operations students learn in calculus. Originally used to measure the rate of change of real-valued functions, derivatives now appear in many different areas. In differential geometry, the notion of smoothness is closely tied to differentiation, while in algebraic geometry, partial derivatives help one study singularities of varieties. In both cases, the geometric intuition of the derivative accounts for its utility.

In addition to geometric insight, there is much information that can be obtained by studying differentiation from a purely algebraic viewpoint. For example if A is a commutative ring, R is an A-algebra and M is an R-module then one can study A-linear maps $d : R \to M$, which satisfy the famous Leibniz product rule:

$$d(xy) = xd(y) + yd(x).$$

Such maps are called *derivations*, and give rise to a universal object known as the *module of differentials*, $\Omega_A(R)$. The module of differentials turns out to have several applications, and provides methods for proving statements in commutative algebra which would otherwise be very difficult. For example, the module of differentials turns out to be necessary for a proper study of separable field extensions!

The module of differentials also appears in algebraic number theory in the form of *evolutions* of algebras. Roughly speaking, an evolution of an algebra is a surjective ring homomorphism ϕ which induces an isomorphism of modules of differentials, the evolution being trivial if ϕ is an isomorphism. Evolutions arise naturally in the study of Galois deformations and were at the heart of Wiles' proof of Fermat's Last Theorem. A crucial step in Wiles' proof was showing that a particular algebra had no nontrivial evolutions, which took considerable work to prove.

Mazur conjectured that Wiles' result should hold in for more general algebras. In particular, he conjectured that all evolutions of reduced algebras in equicharacteristic zero were trivial. In 1997, Eisenbud and Mazur showed that this conjecture can be stated beautifully in commutative algebra in terms of the symbolic square of a radical ideal.

Hence to prove the conjecture of Mazur concerning evolutions, it is sufficient to study radical ideals. Much work has been done on this problem and the conjecture has been proven for classes of ideals including (quasi)homogeneous, height 2 perfect, licci, monomial, and almost complete intersection ideals.

This thesis is the result of two years of directed readings in commutative algebra under the supervision of Prof. Claudia Polini. In this paper, we tell the story of the Eisenbud-Mazur conjecture. We begin by giving a thorough treatment of the module of differentials, proving some major theorems along the way. Later, we will define evolutions and the related work of Eisenbud and Mazur. In particular we provide a detailed study of their paper [2] and the translation of the number theoretic statement to commutative algebra. Finally we list major results for this problem, and give counterexamples in the nonzero characteristic case.

Assuming a moderate background in commutative algebra is unavoidable, but in the interest of keeping this as readable as possible, many examples are included, especially in the beginning. Near the end we will recall some less basic facts includ-

ing the Cohen structure theorem, but we will provide references to these nontrivial statements. For general reference, we refer the reader to [1] and [7].

Chapter 2

The Module of Differentials

We begin this section by introducing notation which we will retain throughout. Let R be a commutative ring, and M an R-module. We assume all of our rings are Noetherian. This section is taken from a set of lecture notes of Bernd Ulrich.

2.1 Basic Definitions

One of the first facts we learn in any differential calculus class is the power rule. Using analytic methods, one can show that the derivative of x^n is nx^{n-1} for all positive integers n. If however, we take this "result" as a "definition" we can abstractly define the notion of a "derivative with respect to x" in a polynomial ring $R[x]$. We do so by defining $d(\sum r_i x^i) = \sum i r_i x^{i-1}$. Using polynomial rings as basic examples, we will define algebraic definitions of differentiation in this chapter. We begin with the notion of derivations:

Definition 2.1.1. *A map $d\colon R \to M$ is a derivation if for every $x, y \in R$ we have*

1. $d(x+y) = d(x) + d(y)$ *(homomorphism of groups)*
2. $d(xy) = xd(y) + yd(x)$ *(product (Leibniz) rule)*

Example 2.1.2.

- The map $d : R \to M$ with $d(r) = 0$ for all r is a derivation and is called the *trivial derivation*. As we will soon see, there are some rings and modules which have no nontrivial derivations.
- Let A be a ring. If $R = A[x_1, \ldots, x_n]$ then $\partial/\partial x_i \colon R \to R$ (partial differentiation) is a derivation.

Many of the properties of derivatives one learned in calculus are also true in this general context as well. For instance we have that $d(1) = d(1 \cdot 1) = d(1) + d(1)$ which implies that $d(1) = 0$. For this reason, $\ker d$ is a subring of R.

Definition 2.1.3. *Suppose that $\phi \colon A \to R$ makes R into and A-algebra. Then we say that a derivation $d \colon R \to M$ is a derivation over A if $\phi(A) \subset \ker d$.*

Thus a derivation d is a derivation over A if it kills all of A. Equally useful, however is the equivalent fact that d is A-linear. We prove this statement as well as other important facts about derivations in the next proposition.

Proposition 2.1.4. *If R is an A algebra, then*
(a) $\phi(A) \subset \ker d \iff d$ is A-linear.
(b) Every derivation is a derivation over $\mathbb{Z}$.
(c) Two derivations over A coincide if they have the same values on a generating set of R as an A-algebra.

Proof. (a) $\Rightarrow$: Let $a \in A$ and $x \in R$. Then

$$d(a \cdot x) = d(\phi(a)x) = \phi(a)d(x) + xd(\phi(a)) = \phi(a)d(x) = a \cdot d(x).$$

To see the other direction, just note that if d is A linear, then $d(\phi(a)) = d(a \cdot 1) = a \cdot d(1) = 0$

(b) Let $n \in \mathbb{Z}$ then $d(n)$ is either $d(1 + \cdots + 1)$ or $d(-1 - \cdots - 1)$ which is equal to $nd(1) = 0$ by linearity.
(c) Let $f \in R$. To compute $d(f)$ suffices to write f in terms of the generators of R and then use the Leibniz and linearity rules repeatedly. The result follows. □

Note that adding two derivations $R \to M$ or multiplying a derivation by an element in R yields another derivation. Thus the set of all derivations naturally forms an R-module.

Definition 2.1.5. *We denote the set of all derivations $d\colon R \to M$ over A by $\mathrm{Der}_A(R, M)$. This is an R-module. If $M = R$ then we write $\mathrm{Der}_A(R)$ for $\mathrm{Der}_A(R, R)$ which is called the module of derivations of R over A.*

In general it is difficult to compute $\mathrm{Der}_A(R, M)$. Below we compute it in a the simple case of a polynomial ring over A:

Example 2.1.6. *Let $R = A[x_1, \ldots, x_n]$. Then $\partial_i = \partial/\partial x_i \in \mathrm{Der}_A(R)$. Furthermore, $\{\partial_1, \ldots, \partial_n\}$ form a basis of $\mathrm{Der}_A(R)$ as an R-module.*

Proof. Let $d \in \mathrm{Der}_A(R)$. Then $d = d(x_1)\partial_1 + \cdots + d(x_n)\partial_n$ since these have the same values on each x_i and thus by Proposition 2.1.4, these derivations coincide. To show linear independence, suppose that

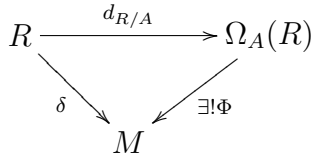
$$a_1\partial_1 + \cdots + a_n\partial_n = 0$$

for $a_i \in R$. Now just evaluate at x_i to show $a_i = 0$. □

Just as adding derivations resulted in new ones, we can compose derivations with homomorpisms as follows: If $d \in \mathrm{Der}_A(R, M)$, and $\phi\colon A \to R$ is a ring homomorphism, then $d \circ \phi \in \mathrm{Der}_A(A, M)$. Also, if $\Phi\colon M \to N$ is a homomorphism of R-modules, then $\Phi \circ d \in \mathrm{Der}_A(R, N)$.

Because $\mathrm{Der}_A(R, M)$ is difficult to compute, we focus our attention on the *module of differentials of R over A*, denoted $\Omega_A(R)$. This object, which will be defined in the next theorem, is a universal object with respect to the set of derivations over A. It is easy to compute if one has a reasonable presentation of R, and furthermore, $\mathrm{Der}_A(R, M)$ is the dual of the module of differentials. Thus the computation of $\mathrm{Der}_A(R, M)$ reduces to computing a dual. In the following theorem, we use the fact that any A-algebra can be written as a polynomial ring modulo some relations.

Theorem 2.1.7. *(Definition of the module of differentials) Let R be an A-algebra.*
(a) There exists a module $\Omega_A(R)$ and a derivation $d_{R/A}\colon R \to \Omega_A(R)$ over A having this property: For every derivation $\delta\colon R \to M$ over A there exists a unique R-linear map $\Phi\colon \Omega_A(R) \to M$ with $\delta = \Phi \circ d_{R/A}$.



(b) The universal property (a) determines $(\Omega_A(R), d_{R/A})$ uniquely up to a canonical R-isomorphism.

Proof. (b) is clear by the standard diagram chase for universal objects.
(a) Case 1: $R = A[\{x_i \mid i \in \mathcal{I}\}]$ is a polynomial ring. Set

$$\Omega_A(R) = \Omega = \bigoplus_{i \in \mathcal{I}} R\, dx_i$$

the free module with basis $\{dx_i \mid i \in \mathcal{I}\}$, and $d_{R/A}\colon R \to \Omega$ the map defined by $d_{R/A}(f) = \sum_i \frac{\partial f}{\partial x_i} dx_i$. This sum is finite since f only involves finitely many variables. Notice that $d_{R/A}$ is well defined and $d_{R/A}(x_i) = dx_i$. We must show that Ω has the universal property described above.

To this end, let $\delta\colon R \to M$ be any derivation over A. Then there exists an R-linear map $\Phi\colon \Omega \to M$ with $\Phi(dx_i) = \delta(x_i)$ since Ω is free. Thus $\Phi \circ d_{R/A}$ and δ are both derivations over A and agree on the x_i so we have $\Phi \circ d_{R/A} = \delta$. Furthermore, ϕ is uniquely determined since $Rd_{R/A}(R) = \Omega$. In other words, Ω is generated by the image of R.

Case 2: $R = S/I$ with $S = A[\{x_i \mid i \in \mathcal{I}\}]$. Write

$$D = d_{S/A}\colon S \to \Omega = \Omega_A(S)$$

where D, $\Omega_A(S)$ are obtained as in the first case. Define

$$\Omega_A(R) = \Omega/(SD(I) + I\Omega) = \Omega/(SD(I) + ID(S)),$$

which is an R-module.

We have an R-module, now we need the map $d_{R/A}\colon R \to \Omega_A(R)$. Consider the commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\quad D \quad} & \Omega \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle P} \\ R = S/I & \overset{\overline{D}}{\dashrightarrow} & \Omega/(SD(I) + ID(S)). \end{array}$$

The induced map $\overline{D}$ exists since $I \subset \ker(P \circ D)$. Since D is a derivation over A, so is $\overline{D}$. We define $d_{R/A} = \overline{D}$.

Now we prove the universal property: Let $\delta\colon R \to M$ be any derivation over A. Then $\delta \circ \pi\colon S \to M$ is also a derivation over A. Hence by case 1, there exists an S-linear map $\Phi\colon \Omega_A(S) \to M$ with $\delta \circ \pi = \Phi \circ D$. Now $\Phi(D(I)) = \delta(\pi(I)) = 0$, hence $\Phi(SD(I)) = 0$. Also, $\Phi(ID(S)) = I\Phi(D(S)) = 0$ since M is an R-module and is thus

killed by I. So now Φ induces

$$\overline{\Phi}\colon \Omega_A(S)/(SD(I)+ID(S)) \to M \quad \text{with} \quad \Phi = \overline{\Phi}\circ P.$$

Now $\overline{\Phi}$ is R-linear. Also, $\delta\circ\pi = \Phi\circ D = \overline{\Phi}\circ P\circ D = \overline{\Phi}\circ\overline{D}\circ\pi$. Hence $\delta = \overline{\Phi}\circ\overline{D} = \overline{\Phi}\circ d_{R/A}$. Furthermore, $\overline{\Phi}$ is uniquely determined as $Rd_{R/A}(R) = \Omega_A(R)$. □

This module $\Omega_A(R)$ is called the module of differentials (universal module of differentials or module of Kähler differentials) of R over A, and $d_{R/A}$ is the universal derivation of R over A.

Remark 2.1.8. *The module of differentials can equivalently be defined as the R-module with generators $\{d(f) \mid f \in R\}$ subject to the relations*

$$d(f+g) = d(f)+d(g), \quad d(af) = ad(f), \quad d(fg) = fd(g)+gd(f)$$

where $a \in A, f, g \in R$. We will sometimes find it more useful to use this definition. The fact that these are equivalent is immediate from the construction in Theorem 2.1.7.

As promised, there is a natural bijection between the $\mathrm{Der}_A(R,M)$ and the dual of $\Omega_A(R)$. In particular, given any homomorphism $\Omega_A(R) \to M$ we can compose with the universal derivation to get a derivation $R \to M$. Conversely, given any derivation, the universal property yields an R-module homomorphism. This result and some computational tools are outlined below.

Remark 2.1.9. *(a)* $\mathrm{Der}_A(R,M) \cong \mathrm{Hom}_R(\Omega_A(R),M)$ *in a natural way by the universal property defining the module of differentials.*

(b) If $R = S/I$ with $S = A[\{x_i \mid i \in \mathcal{I}\}]$ a polynomial ring and $I = (f_j \mid j \in \mathcal{J})$, then

$$\begin{aligned}\Omega_A(R) &\cong \bigoplus_{i\in\mathcal{I}} Rdx_i/(\sum \overline{\frac{\partial f}{\partial x_i}}dx_i \mid f \in I) \\ &\cong \bigoplus_{i\in\mathcal{I}} Rdx_i/(\sum \overline{\frac{\partial f_j}{\partial x_i}}dx_i \mid j \in \mathcal{J})\end{aligned}$$

where $\{dx_i \mid i \in \mathcal{I}\}$ is an R-basis and $\overline{\ }$ denotes images in R. Moreover, $d_{R/A}(\overline{x_i})$ is the image of dx_i in $\Omega_A(R)$.

(c) $\Omega_A(R) = Rd_{R/A}(R)$. (This follows from the proof of Theorem 2.1.7)

Proof. It suffices to prove (b). The first isomorphism follows from the proof of Theorem 2.1.7 since we simply go modulo the derivatives of elements in I. To see that the second equality holds, i.e. we can just consider the derivatives of the generators of I, note that if $s \in S$ then

$$\overline{\frac{\partial(sf_j)}{\partial x_i}} = \overline{s}\overline{\frac{\partial(f_j)}{\partial x_i}} + \overline{\frac{\partial(s)}{\partial x_i}}\overline{f_j} = \overline{s}\overline{\frac{\partial(f_j)}{\partial x_i}}$$

since $f_j \in I$. □

2.2 Standard Properties

When we define a new object, the natural question in commutative algebra is to ask how it behaves with respect to standard operations. For example, does it localize nicely? How is it related to exact sequences? Fortunately, the module of differentials localizes nicely as proven in Propositions 2.2.1, 2.2.2 and then later in Corollary 2.3.2. We later handle exactness properties in Propositions 2.3.1 and 2.4.1.

Proposition 2.2.1. *Let R be an A-algebra, $W \subset R$ a multiplicatively closed subset*

of R, $d = d_{R/A}$. Then $\Omega_A(W^{-1}R) = W^{-1}\Omega_A(R)$ and for $r \in R$, $w \in W$,

$$d_{W^{-1}R/A}(r/w) \cong \frac{wd(r) - rd(w)}{w^2}.$$

Proof. The verification that $d_{W^{-1}R/A}$ is well defined is straightforward. To show that it is a derivation is even easier. To prove the isomorphism, let d^* be the canonical map $W^{-1}R \to \Omega_A(W^{-1}R)$. We only need to observe that there is a unique $W^{-1}R$-module homomorphism $\phi\colon \Omega_A(W^{-1}R) \to W^{-1}\Omega_A(R)$ such that $\phi \circ d^* = d_{W^{-1}R/A}$. Now a simple diagram chase shows the isomorphism. □

This fact has an obvious corollary which we state below. The proof follows from Proposition 2.2.1 and Remark 2.1.9

Proposition 2.2.2. *If $R = W^{-1}(S/I)$ with $S = A[\{x_i \mid i \in \mathcal{I}\}]$ a polynomial ring, $W \subset S$ a multiplicative set, $I = (f_j \mid j \in \mathcal{J})$. Then*

$$\Omega_A(R) \cong \bigoplus_{i \in \mathcal{I}} R dx_i / (\sum \overline{\frac{\partial f_j}{\partial x_i}} dx_i \mid j \in \mathcal{J})$$

and $d_{R/A}(\overline{x_i})$ is the image of dx_i. In particular if $\mathcal{I}$ is finite then $\Omega_A(R)$ is a finite R-module, and if $\mathcal{I}$ and $\mathcal{J}$ are finite, then $\Omega_A(R)$ is a finitely presented R-module, presented by the Jacobian matrix.

$$\left(\overline{\frac{\partial f_j}{\partial x_i}}\right).$$

We now present a few examples.

Example 2.2.3. *If $R = k[x, y, z]/(x^2 + y^2, x^2y^2z^2)$* then

$$\Omega_k(R) = \frac{Rdx \oplus Rdy \oplus Rdz}{(2xdx + 2ydy, 2xy^2z^2dx + 2x^2yz^2dy + 2x^2y^2zdz)}$$

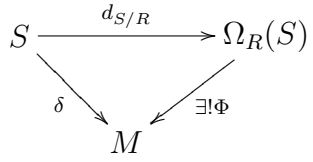
Note that if $\operatorname{char} k = 2$ then $\Omega_k(R)$ is free.

Example 2.2.4. *Let M be an R-module, and let $S = R \ltimes M$, the "trivial extension of R by M"; that is, as an R-module $S = R \oplus M$, and the multiplication is*

$$(r, m) \cdot (s, n) = (rs, rn + sm).$$

Then $\Omega_R(S) \cong M$.

Proof. $\Omega_R(S) = \{d(f) \mid f \in S\}$ modulo some relations. It is clear that $d(r, m) = d(r, 0) + d(0, m)$, so $\Omega_R(S)$ is generated by elements of the form $d(r, 0)$ and $d(0, m)$. But since we are taking derivatives with respect to R, $d(r, 0) = r \cdot d(1, 0) = 0$. Finally we claim that $\Omega_R(S) \cong M$. Notice M is an S-module via $(r, m)n = rn$. Consider the map $\delta : S \to M$ given by $\delta(r, m) = m$. This is a derivation, and thus induces a unique map Φ in the diagram below.



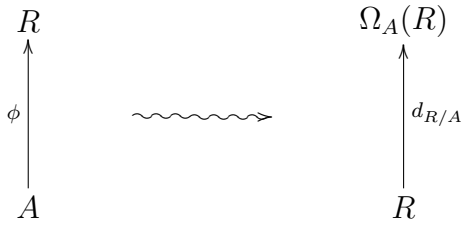
Finally, this map has an inverse given by $m \to d(0, m)$, establishing the isomorphism.

□

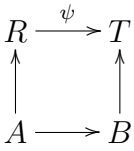
2.3 Modules of Differentials of Ring Extensions and Products

To properly study how the module of differentials behaves with respect to exact sequences, it is natural to begin by studying relationships among different sets of modules of differentials. In particular we discuss how commutative diagrams of rings give rise to corresponding diagrams of modules of differentials. We also discuss why

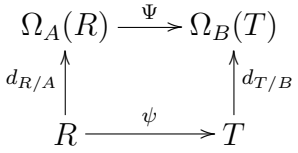
the association



is functorial. Given a commutative diagram of homomorphisms of rings,

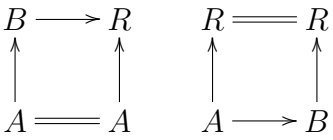


there exists a unique R-linear map Ψ by the universal property so that the diagram



commutes. Notice that $\Psi(d_{R/A}(r)) = d_{T/B}(\psi(r))$. We also have that Ψ induces a T-linear map $T \otimes_R \Omega_A(R) \to \Omega_B(T)$ where the map is $t \otimes d(f) \mapsto t\Psi(d(f))$. This observation we have just collected will become useful in what follows.

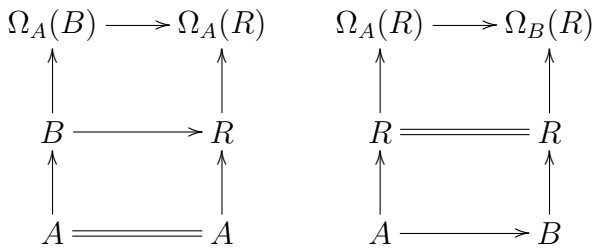
An important question to ask is how the module of differentials changes if we change the base ring. Given homomorphisms of rings $A \to B \to R$ we have two diagrams



and the induced R-linear maps from above

$$R \otimes_B \Omega_A(B) \to \Omega_A(R) \quad \text{and} \quad \Omega_A(R) \to \Omega_B(R).$$

To better see what is going on, we can extend these diagrams to:



Proposition 2.3.1. *Let $A \to B \to R$ be ring homomorphisms. Then the induced sequence*

$$R \otimes_B \Omega_A(B) \to \Omega_A(R) \to \Omega_B(R) \to 0$$

is exact.

Proof. We prove this by looking at the generators and relations. By Remark 2.1.8, $\Omega_A(R)$ is generated by $d(f), f \in R$ subject to certain relations. But $\Omega_B(R)$ is generated by the same elements only with the added relation that $d(bf) = bd(f)$ for all $b \in B$. Thus the map $\Omega_A(R) \to \Omega_B(R)$ is surjective. The kernel of this map can be seen to be generated by the set of all $d(b)$ with $b \in B$. This is clear because the only way something could be zero in $\Omega_B(R)$ but not in $\Omega_A(R)$ is if it is due to the new relation $d(B) = 0$. Finally, the image of the lefthand map is the R-module generated by $d(B)$ as $\Omega_A(B)$ as a B-module is generated by $d(B)$ so we have proved exactness. □

As an application of this exact sequence, we prove the following result which concerns different localizations of the module of differentials.

Corollary 2.3.2. *Let $A \xrightarrow{\phi} R$ be an algebra, $V \subset A$, $W \subset R$ multiplicative subsets with $\phi(V) \subset W$. Then*

$$\Omega_{V^{-1}A}(W^{-1}R) \cong \Omega_A(W^{-1}R) \cong W^{-1}\Omega_A(R)$$

via the natural maps.

Proof. The second isomorphism is Proposition 2.2.1. The first isomorphism follows from the previous proposition since the maps $A \to V^{-1}A \to W^{-1}R$ induce the exact sequence

$$W^{-1}R \otimes \Omega_A(V^{-1}A) \to \Omega_A(W^{-1}R) \to \Omega_{V^{-1}A}(W^{-1}R) \to 0$$

and $\Omega_A(V^{-1}A) \cong V^{-1}\Omega_A(A) = 0$. □

This last corollary gives us an even stronger statement about localization of the module of differentials. It tells us that looking at the modules of differentials over A and $V^{-1}A$ are isomorphic. Next we would like to investigate the relationship between tensor products and the module of differentials.

Proposition 2.3.3. *a) Let $A \to A'$, $A \to R$ be algebras. There is an $A' \otimes_A R$-isomorphism $\Omega_{A'}(A' \otimes_A R) \cong A' \otimes_A \Omega_A(R)$ with $d(a' \otimes r) \mapsto a' \otimes d(r)$.*
b) Let $A \to R_1$, $A \to R_2$ be algebras, $T = R_1 \otimes_A R_2$. There is a T-isomorphism

$$\Omega_A(T) \cong R_1 \otimes_A \Omega_A(R_2) \oplus R_2 \otimes_A \Omega_A(R_1)$$

with

$$d(r_1 \otimes r_2) \mapsto r_1 \otimes d(r_2) + r_2 \otimes d(r_1).$$

Proof. a): There are two ways of proving this. One could argue using the universal property of the module of differentials, but we present a proof using Remark 2.1.9. Indeed, if $R = A[\{x_i\}]/(f_j)$ as before, then $A' \otimes_A R = A'[\{x_i\}]/(f_j)$ and

$$\Omega_{A'}(A' \otimes_A R) = \bigoplus (A' \otimes_A R)dx_i/(\star)$$

where $\star$ is as in Remark 2.1.9. But by comparison,

$$A' \otimes \Omega_A(R) = A' \otimes \bigoplus R dx_i/(\star) \cong \bigoplus (A' \otimes_A R) dx_i/(\star)$$

proving the desired isomorphism.

(b): By the universal property of the tensor product, there is an A-linear map

$$\delta \colon T = R_1 \otimes_A R_2 \to R_1 \otimes_A \Omega_A(R_2) \oplus R_2 \otimes_A \Omega_A(R_1)$$

with

$$\delta(r_1 \otimes r_2) \mapsto r_1 \otimes d_{R_2/A}(r_2) + r_2 \otimes d_{R_1/A}(r_1)$$

since the $d_{R_i/A}$ are A-linear. Now δ is a derivation over A since the $d_{R_i/A}$ are. Hence by the universal property of the module of differentials we have a T-linear map

$$\Phi \colon \Omega_A(T) \to R_1 \otimes_A \Omega_A(R_2) \oplus R_2 \otimes_A \Omega_A(R_1)$$

with $\Phi(d_{T/A}(r_1 \otimes r_2)) = r_1 \otimes d_{R_2/A}(r_2) + r_2 \otimes d_{R_1/A}(r_1)$.

On the other hand, the maps $A \to R_1 \to T$ and $A \to R_2 \to T$ combined with obvious facts about direct sums yield the induced map

$$\Psi \colon R_1 \otimes_A \Omega_A(R_2) \oplus R_2 \otimes_A \Omega_A(R_1) \cong T \otimes_{R_2} \Omega_A(R_2) \oplus T \otimes_{R_1} \Omega_A(R_1) \to \Omega_A(T)$$

with $1 \otimes d_{R_2/A}(r_2) \mapsto d_{T/A}(1 \otimes r_2)$ and $1 \otimes d_{R_1/A}(r_2) \mapsto d_{T/A}(r_1 \otimes 1)$. It follows that $\Phi \circ \Psi = \Psi \circ \Phi = \mathrm{id}$. □

Remark 2.3.4. *The same works for any finite collection of A-algebras $R_1, \ldots, R_s$*

and $T = R_1 \otimes_A \cdots \otimes_A R_s$. *We have*

$$\begin{aligned}\Omega_A(T) &\cong \bigoplus_j (\bigotimes_{\substack{A \\ i \neq j}} R_j) \otimes_A \Omega_A(R_i) \\ &\cong \bigoplus (T \otimes_A \otimes_{R_i} \Omega_A(R_i)).\end{aligned}$$

This remark gives us a new way to compute Ω for new classes of rings. In particular we have the following proposition.

Proposition 2.3.5. *Let* $A \to R$ *be a homomorphism of rings and let* $T = R[x_1, \ldots, x_n]$. *Then*

$$\Omega_A(T) = T \otimes_R \Omega_A(R) \oplus \bigoplus_i T dx_i.$$

Proof. Write $T' = A[x_1, \ldots, x_n]$. Then note that $T = R \otimes T'$. Thus

$$\begin{aligned}\Omega_A(T) &= T \otimes_R \Omega_A(R) \oplus T \otimes_{T'} \Omega_A(T') \\ &= T \otimes_R \Omega_A(R) \oplus T \otimes_{T'} \bigoplus_i T' dx_i \\ &= T \otimes_R \Omega_A(R) \oplus \bigoplus_i T dx_i. \quad \square\end{aligned}$$

Since we will have occasion to use it, we state without proof the relationship between module of differentials and direct limits. The reader may object that we have not explicitly given a directed set in the statement, but to do so would complicate the issue and take away from the point of the theorem. What is important to understand is that direct limits commute with $\Omega_A(-)$. A complete statement and proof can be found in [1].

Proposition 2.3.6. *Let* $T = \varinjlim R_i$. *There is a* T*-isomorphism*

$$\Omega_A(T) \cong \varinjlim \left(T \otimes_{R_i} \Omega_A(R_i)\right).$$

2.4 The Conormal Sequence

In this last section of the general introduction to the module of differentials we develop what is perhaps the most useful tool in their study. This is called the *conormal sequence* and gives a refinement of the exact sequence in Proposition 2.3.1.

Consider a set of algebras $A \to R \to T = R/I$. Then by Proposition 2.3.1 we obtain an exact sequence

$$T \otimes_R \Omega_A(R) \to \Omega_A(T) \to \Omega_R(T) \to 0.$$

But the first map is surjective since $\Omega_R(T) = 0$. Thus we have an exact sequence of the form

$$T \otimes \Omega_A(R) \xrightarrow{\psi} \Omega_A(T) \to 0.$$

We now compute the kernel of the map ψ. Notice that

$$\Omega_A(T) = \Omega_A(R/I) = \Omega_A(R)/(I\Omega_A(R) + Rd(I)).$$

Thus one sees that the kernel of ψ is generated by the image of $d_{R/A}(I)$. This is also the image of the map $I/I^2 \to T \otimes_R \Omega_A(R)$ given by $\delta(f + I^2) = 1 \otimes d(f)$. This map is well defined since by the Leibniz rule, $d(I^2) \subset I\Omega_A(R)$ which maps to zero in $T \otimes_R \Omega_A(R) \cong \Omega_A(R)/I\Omega_A(R)$. The map δ is T-linear since for $r \in R$ and $f \in I$ we have

$$\delta(rf + I^2) = 1 \otimes d(rf) = 1 \otimes (rdf + fdr) = 1 \otimes rdf = r\delta(f + I^2).$$

We have just proven

Proposition 2.4.1. *For $A \to R \to T = R/I$,*

$$I/I^2 \xrightarrow{\delta} T \otimes_R \Omega_A(R) \to \Omega_A(T) \to 0$$

is an exact sequence of T-linear maps. This is called the conormal sequence.

We can sharpen this result by noticing that $\delta((I \cap A)R) = 0$ and obtain

Corollary 2.4.2. *With notation as in Proposition 2.4.1 there is an induced exact sequence*

$$I/((I \cap A)R + I^2) \xrightarrow{\bar{\delta}} T \otimes_R \Omega_A(R) \to \Omega_A(T) \to 0$$

The left-hand map δ need not be injective. In fact, its kernel can be nontrivial in very simple cases. There is a necessary and sufficient condition, however, which says when the conormal sequence is splits exact. First we prove a lemma.

Lemma 2.4.3. *Let $\psi\colon R \to T$ be a homomorphism of A-algebras, I a T-ideal with $I^2 = 0$ and $\Delta\colon R \to I$ an A-linear map. Then Δ is a derivation over A if and only if $(\psi + \Delta)\colon R \to T$ is a homomorphism of A-algebras.*

Proof. Let $x, y \in R$. Then $(\psi + \Delta)(xy) = \psi(x)\psi(y) + \Delta(xy)$, and

$$(\psi + \Delta)(x) \cdot (\psi + \Delta)(y) = \psi(x)\psi(y) + \psi(x)\Delta(y) + \psi(y)\Delta(x)$$

since $I^2 = 0$. The result follows. □

Proposition 2.4.4. *The T-linear map δ in 2.4.1 has a left inverse (i.e. the sequence is split injective) if and only if the natural map of A-algebras $\pi\colon R/I^2 \to R/I = T$ has a right inverse.*

Proof. Note that since $d_{R/A}(I^2) \subset I\Omega_A(R)$, and since tensoring with R/I always kills

all of I, we have

$$R/I \underset{R/I^2}{\otimes} \Omega_A(R/I^2) \cong R/I \underset{R/I^2}{\otimes} \frac{\Omega_A(R)}{(Rd_{R/A}(I^2) + I^2\Omega_A(R))} \cong R/I \underset{R}{\otimes} \Omega_A(R).$$

So δ does not change if we replace R with R/I^2, and neither does π. So we may assume that $I^2 = 0$. We now begin the equivalences.

$\pi\colon R \to R/I$ has a right inverse

$\iff$ there exists a homomorphism of A-algebras $\gamma\colon R/I \to R$
with $\pi\gamma = \mathrm{id}_{R/I}$

$\iff$ there exists a homomorphism of A-algebras $\tau\colon R \to R$ with $\tau_{|I} = 0$
and $(\mathrm{id}_R - \tau)(R) \subset I$

$\iff$ there exists a derivation $\Delta\colon R \to I$ over A with $\Delta_{|I} = \mathrm{id}_I$
(We can let $\Delta = \mathrm{id}_R - \tau$ by Lemma 2.4.3 since $I^2 = 0$ and $-\mathrm{id}\colon R \to R$
is a homomorphism of A-algebras.)

$\iff$ there exists an R-linear map $\Phi\colon \Omega_A(R) \to I$ with $\Phi(d_{R/A}(f)) = f$
for all $f \in I$ (from the universal property)

$\iff$ there exists a T-linear map $\Psi\colon T \otimes_A \Omega_A(R) \to I = I/I^2 = I \otimes T$
with $\Psi(1 \otimes d_{R/A}(f)) = f + I^2$ for all $f \in I$

$\iff$ δ has a left inverse.

□

Chapter 3

Field extensions and the Module of Differentials of Local Rings

Let $k \subset K$ be a field extension. We can consider the module of differentials $\Omega_k(K)$. This is a K-module and hence a K-vector space. Therefore we can ask what is $\dim_K \Omega_k(K)$? As it turns out, the answer to this question is the transcendence degree (or in nonzero characteristic, what is called the p-degree) of the extension. Additionally the notion of separable and inseparable extensions is crucial to studying $\Omega_k(K)$. Not surprisingly, a proper study of of the module of differentials $\Omega_k(K)$ requires a good deal of field theory, but interestingly enough, a proper study of field extensions is actually dependent on the module of differentials! In this chapter we discuss the basic tools needed to compute the module of differentials for field extensions, and along the way, state several results in field theory.

Due to the technical nature of the proofs, especially in characteristic p, we will omit some proofs. A good source for the field theory discussed here is in Appendix A.1 of [1] and also in [6].

3.1 Basic Definitions

We begin by defining transcendence bases and their analogue in positive characteristic called a p-basis. We will then use these tools to prove statements about the module of differentials. Throughout this section, $k \subset K$ will be a field extension.

Definition 3.1.1. *A subset $U \subset K$ is a transcendence basis of K over k if U is algebraically independent over k and $k(U) \subset K$ is algebraic.*

Example 3.1.2.

a) If k is a field, then $\{x\}$ is a transcendence basis for $k \subset k(x)$.

b) If k is a field, then $\{x\}$ is a transcendence basis for
$k \subset \text{Quot}(k[x,y]/(y^2 - x))$. □

The following proposition has an analogous statement in linear algebra but the statement here is much stronger. It proves the existence of transcendence bases for field extensions as we show the existence of a vector space basis.

Proposition 3.1.3. *(a) Let $V \subset W$ be (possibly empty) subsets of K so that V is algebraically indpendent over k and $k(W) \subset K$ is algebraic. Then there exists a transcendence basis U of K over k with $V \subset U \subset W$.*

(b) Let U, U' be transcendence bases of K over k. Then for every $u' \in U'$ there exists $u \in U$ so that $U' \setminus \{u'\} \cup \{u\}$ is a transcendence basis of K over k.

(c) Any two transcendence bases of K over k have the same cardinality.

It follows that any field extension $k \subset K$ has a transcendence basis and that the cardinality of any such basis only depends on the field extension itself. This cardinality is called the *transcendence degree* of K over k, $\text{trdeg}_k K$. Recall that for towers of algebraic extensions, the degree of the extensions was multiplicative. There is a similar result for transcendence degree, as shown in the following corollary which has a simple proof.

Corollary 3.1.4. *Let $k \subset K \subset L$ be field extensions. Then*

$$\operatorname{trdeg}_k L = \operatorname{trdeg}_k K + \operatorname{trdeg}_K L.$$

Proof. If U is a transcendence basis of K over k and V a transcendence basis of L over K, then clearly $U \cup V$ is a transcendence basis of L over k. □

For a field extension of a field of characteristic $p > 0$ we give a definition of another type of basis for a field extension. Recall that if $k \subset K$ are fields of characteristic p then $kK^p = \{\sum a_i x_i^p \mid a_i \in k,\, x_i \in K\}$ is a subfield of K.

Definition 3.1.5. *Let k be a field with $\operatorname{char} k = p > 0$. A subset $U \subset K$ is p-independent over k if*

$$U_p = \{u_1^{\nu_1} \cdots u_n^{\nu_n} \mid n \in \mathbb{N}, u_i \in U,\, 0 \leq \nu_i \leq p-1\}$$

is linearly independent over kK^p. We say that U is a p-basis of K over k if U_p is a basis of K over kK^p.

Example 3.1.6.

(a) Let $k = \mathbb{Z}/p\mathbb{Z} \subset k(x) = K$. Then $\{x\}$ is a p-basis of K over k. Indeed, $U_p = \{1, x, \ldots, x^{p-1}\}$ and $kK^p = k(x^p)$, so it is immediate that U_p spans K over kK^p and is linearly independent over kK^p.

(b) Similarly, if $k = \mathbb{Z}/p\mathbb{Z} \subset k(x, y) = K$ then $\{x, y\}$ is a p-basis for K over k.

An analogous, (but more technical) version of Proposition 3.1.3 exists for p-bases, and can be used to show that p-bases always exist. The cardinality of such a basis is called the p-degree. Notice that for a field extension in positive characteristic p we now have two cardinalities - $\operatorname{trdeg}_k K$ and $p\text{-}\deg_k K$. When these values are finite they will be important in computing $\dim_K \Omega_k(K)$ as we will later see.

We now recall the notion of a separable algebraic field extension, something that is well studied in any field theory course. We take a different approach, however, and study the relationship to the module of differentials.

Definition 3.1.7. *A field extension $k \subset K$ is called separable algebraic if it is algebraic and for any $\alpha \in K$, the minimal polynomial of α over k has no repeated roots.*

If k is a field with the property that all algebraic extensions of k are separable algebraic then we say that k is perfect. Examples of perfect fields include all fields of characteristic zero, and finite fields.

Separable algebraic field extensions are very nice to work with. Since they are algebraic, $\operatorname{trdeg}_k K = 0$ and the separability turns out to be a very important property as well. The following proposition computes the module of differentials for separable algebraic extensions.

Proposition 3.1.8. *Let $k \subset K \subset L$ be field extensions with $K \subset L$ separable algebraic. Then $\Omega_k(L) \cong L \otimes_K \Omega_k(K)$ via the natural L-linear map.*

Proof. We have $L = \cup L_i = \varinjlim L_i$, where the L_i are finite field extensions of K contained in L. Since direct limits are compatible with both tensor products and modules of differentials, we may assume that $K \subset L$ is finite separable, hence simple ($L = K[\alpha]$). Write $L = K[\alpha] = K[x]/(f(x))$ with $f'(x) \neq 0$ in L. Now by Proposition 2.3.5 and the conormal sequence, we see that

$$\Omega_k(L) \cong L \underset{K[x]}{\otimes} \Omega_k(K[x])/(\operatorname{im}\, \delta) \cong L \underset{K}{\otimes} \Omega_k(K) \oplus Ldx/(\star, f'(x)dx)$$

and since $f'(x) \neq 0$ it is a unit, the last factor is 0. Thus we have $\Omega_k(L) \cong L \otimes_K \Omega_k(K)$. □

Separable algebraic field extensions are convenient in the theory of differentials, as

if $k \subset K$ is separable algebraic, then $\Omega_k(K) = 0$. This is clear from the proposition by applying it to the tower $k \subset k \subset K$. We will later see that this condition is equivalent to the fact that $k \subset K$ is separable algebraic.

3.2 Main Results for Field Extensions

We are now ready to state many of the main results of this section. We begin with a "formula" for the dimension of $\Omega_k(K)$:

Theorem 3.2.1. *If $k \subset K$ is any field extension then*

$$\dim_K \Omega_k(K) = \begin{cases} \operatorname{trdeg}_k K & \text{if } \operatorname{char} k = 0 \\ p\text{-}\deg_k K & \text{if } \operatorname{char} k = p > 0 \end{cases}$$

Note that this theorem is true for all field extensions. One might wonder when the two numbers on the right are equal. To answer this question, we introduce a generalization of separable algebraic extensions.

Definition 3.2.2. *A field extension $k \subset K$ is called separably generated if there exists a transcendence basis U of K over k so that $k(U) \subset K$ is separable algebraic. Such U is called a separating transcendence basis. A field extension $k \subset K$ is called separable if $k \subset K'$ is separably generated for every finitely generated field extension $k \subset K'$ with $K' \subset K$.*

Note that in characteristic zero all algebraic extensions are separable, thus all extensions are separably generated and separable. It is not immediate at the moment whether separably generated implies separable or vice versa. It is in fact true that separably generated implies separable, and the converse is true for finitely generated field extensions, which we state below.

Example 3.2.3.

Let $\operatorname{char} k = p > 0$, $K = k(x)$. Then $\{x\}$ is a separating transcendence basis. Note that $\{x^p\}$ is another transcendence basis, but not separating, since the minimal polynomial of x in $k(x^p)[y]$ is $y^p - x^p$ which is purely inseparable.

Proposition 3.2.4. *Let $k \subset K \subset L$ be field extensions with $K \subset L$ finitely generated. Then*

$$\dim_L \Omega_k(L) \geq \dim_K \Omega_k(K) + \operatorname{trdeg}_K L.$$

We are now ready to state necessary and sufficient conditions for $\Omega_k(K) = 0$ for a field extension $k \subset K$.

Theorem 3.2.5. *Let $k \subset K$ be a finitely generated field extension. Then*

1. *$\Omega_k(K) = 0$ if and only if $k \subset K$ is separable algebraic.*

2. *$p\text{-}\deg_k(K) \geq \operatorname{trdeg}_k(K)$.*

It would seem that these two statements are very different. The first is about derivatives, while the second can be stated completely in terms of field theory. It is the relationship between these two notions which is truly remarkable. We close this section by stating the results which answer the questions raised earlier in this section. In particular they give a characterization separable extensions and also says when the two numbers $\operatorname{trdeg}_k K$ and $p\text{-}\deg_k K$ are equal.

Theorem 3.2.6. *The following are equivalent for a finitely generated field extension $k \subset K$:*

(1) $\dim_K \Omega_k(K) = \operatorname{trdeg}_k K$

(2) $p\text{-}\deg_k K = \operatorname{trdeg}_k K$ *if* $\operatorname{char} k = p > 0$

(3) some p-basis is algebraically independent over k, if $\operatorname{char} k = p > 0$

(4) every p-basis is a separating transcendence basis of $k \subset K$

(5) $k \subset K$ is separably generated.

Proposition 3.2.7. *Let $k \subset K$ be a field extension.*

(a) $k \subset K$ separably generated $\Rightarrow$ separable.

(b) If $k \subset K$ is finitely generated: $k \subset K$ separably generated $\iff$ separable.

3.3 Modules of Differentials of Local Rings

Having treated the case of field extensions, in this section we will prove some facts about the module of differentials of local k-algebras. In particular, we will compute the minimal number of generators of certain modules of differentials in terms of the transcendence degree of certain field extensions. This will naturally lead to a discussion about ramification and the singular locus.

It is not currently clear that local k-algebras and separable field extensions should have any relationship. This becomes transparent in this section because of our use of the Cohen structure theorem, which is necessary for most of the results in this section. We omit the proof of this theorem, referring the reader to [8]. First we recall the definition of a coefficient ring.

Definition 3.3.1. *Let $(R, \mathfrak{m}, K)$ be a local ring with residue field K, $p = \operatorname{char} K \geq 0$. A coefficient ring of R is a subring $R_0 \subset R$ so that $(R_0, \mathfrak{m}_0)$ is a Noetherian complete local ring with $\mathfrak{m}_0 = pR_0$ and $R_0/\mathfrak{m}_0 = K$.*

We note that this coefficient ring is a field if and only if $\operatorname{char} K = \operatorname{char} R$ in which case it is called a coefficient field. Furthermore, if $(R, \mathfrak{m}, K)$ has a coefficient field, then the map $R \to K$ has a right inverse $\phi\colon K \to R$, namely the isomorphism between K and the coefficient field of R.

Theorem 3.3.2. *(Cohen's Structure Theorem) Let R be a complete local ring with residue field K and $\pi\colon R \to K$ the natural map. Let $k \subset R$ be any field so that $\pi(k) \subset K$ is separable. Then R has a coefficient field containing k.*

Remark 3.3.3. *(a) k as in Theorem 3.3.2 always exists if* $\operatorname{char} R = \operatorname{char} K$. *One can take the prime field $\mathbb{F}_p$, which is perfect, hence makes $\pi(k) \subset K$ separable.*

The following theorem is crucial for the rest of this section, and for the results of Eisenbud and Mazur. The theorem gives a relationship between $\operatorname{trdeg}_k K$ and the minimal number of generators of the module of differentials, a useful invariant. Notice that this is the first time that the invariants from dimension theory are appearing in this paper. We use edim to denote the minimum number of generators of the maximal ideal - the embedding dimension.

Theorem 3.3.4. *Let k be a field, $(R, \mathfrak{m})$ a local k-algebra essentially of finite type with $K = R/\mathfrak{m}$, and assume $k \subset K$ is separable. Then*

$$\mu(\Omega_k(R)) = \operatorname{edim} R + \operatorname{trdeg}_k K.$$

Proof. The ring $R/\mathfrak{m}^2$ is complete and local. Since $k \subset K$ is separable, Theorem 3.3.2 shows that $R/\mathfrak{m}^2$ has a coefficient field containing k. Equivalently, the natural map $\pi\colon R/\mathfrak{m}^2 \to K$ has a right inverse as a map of k-algebras. Thus Proposition 2.4.4 gives an exact sequence

$$0 \to \mathfrak{m}/\mathfrak{m}^2 \to K \otimes_R \Omega_k(R) \to \Omega_k(K) \to 0.$$

Now use the fact that these are all K vector spaces, $\dim_K K \otimes M = \mu(M)$, and that $\dim_K \Omega_k(K) = \operatorname{trdeg}_k K$. Thus since we have a short exact sequence,

$$\mu(\Omega_k(R)) = \operatorname{trdeg}_k K + \mu(m) = \operatorname{trdeg}_k K + \operatorname{edim} R. \quad \square$$

There is also a slightly more general version of this theorem, where we do not assume that the rings are k-algebras.

Corollary 3.3.5. *Let $(A, \mathfrak{n}) \to (R, \mathfrak{m})$ be a local map making R an A-algebra es-*

sentially of finite type and assume the residue field extension $k \subset K$ is separable. Then

$$\mu(\Omega_A(R)) = \mu(\mathfrak{m}/R\mathfrak{n}) + \operatorname{trdeg}_k K.$$

Proof. Replacing $A \to R$ by $k = A/\mathfrak{n} \to R/R\mathfrak{n}$ we are in the situation of Theorem 3.3.4. Then by Proposition 2.3.3(a)

$$\Omega_k(R/Rn) = \Omega_k(A/\mathfrak{n} \otimes_A R) = \Omega_k(k \otimes_A R) = k \otimes_A \Omega_A(R)$$

showing that $\mu(\Omega_k(R/R\mathfrak{n})) = \mu(\Omega_A(R))$. The result then follows from Theorem 3.3.4. □

We close this section by discussing the very powerful Jacobian Criterion for determining when a ring is regular. To do this, we need to recall the notion of Fitting ideals. These are treated nicely in chapter 20 of [1], and we will state without proof some of the basic properties.

Definition 3.3.6. *Let $R^s \xrightarrow{\phi} R^n \to M \to 0$ be exact. Then define the ith Fitting ideal of M, $\operatorname{Fitt}_i(M) = I_{n-i}(\phi)$ the ideal generated by the $(n-i) \times (n-i)$ minors of ϕ.*

We recall some basic properties:

Proposition 3.3.7.

(a) The ideals $\operatorname{Fitt}_i(M)$ depend only on M and not on the matrix ϕ.

(b) The ideals $\operatorname{Fitt}_i(M)$ form an increasing chain of ideals

(c) $V(\operatorname{Fitt}_i(M)) = \{q \in \operatorname{Spec}(R) \mid \mu(M_q) > i\}$

(d) $V(\operatorname{Fitt}_0(M)) = \operatorname{Supp}(M)$. □

If R is an algebra essentially of finite type over a Noetherian ring A and $M = \Omega_A(R)$ then M is finitely presented and the matrix ϕ can be obtained from a Jacobian matrix

(see Proposition 2.2.2). One calls

$$\mathcal{V}_K(R/A) = \mathrm{Fitt}_0(\Omega_A(R))$$

the Kähler different of R over A or the Jacobian ideal. We now state the Jacobian Criterion for regularity, which is extremely useful in determining whether a local ring is regular.

Theorem 3.3.8. *(Jacobian Criterion) Let k be a field, $(R, \mathfrak{m})$ a local k-algebra essentially of finite type with $K = R/\mathfrak{m}$, write $D = \dim R + \mathrm{trdeg}_k K$ and assume $k \subset K$ is separable. The following are equivalent:*

(1) R is regular.

(2) $\Omega_k(R)$ is free of rank D

(3) $\mathrm{Fitt}_D(\Omega_k(R))) = R$.

In this case, $k \subset L = \mathrm{Quot}(R)$ is a separable field extension and $\mathrm{trdeg}_k L = D$.

Theorem 3.3.9. *Let K be a perfect field and R a local k-algebra essentially of finite type. Assume R is reduced or $\mathrm{char}\, k = 0$. Then R is regular if and only if $\Omega_k(R)$ is free.*

Example 3.3.10.

Let $R = \mathbb{C}[x, y, z]/(x^2 - yz)$. Then $\Omega_{\mathbb{C}}(R)$ is presented by the Jacobian matrix $(2x, -y, -z)$, and thus $\mathrm{Fitt}_D(\Omega_{\mathbb{C}}(R)) \cong (x, y, z)$. Hence by the Jacobian criterion, R_P is a regular local ring for all primes P not containing (x, y, z). Geometrically, this says that the variety corresponding to R is regular at every point except at the origin.

Chapter 4

Evolutions and the Eisenbud-Mazur Conjecture

We now arrive to the main part of this paper, which concerns the Eisenbud-Mazur Conjecture. Naturally a statement in number theory, the conjecture concerns the question of the existence of nontrivial evolutions of certain algebras. Evolutions, defined below, arise naturally in the study of Hecke algebras, as in the work of Wiles, Taylor-Wiles and Flach [9, 10, 3] related to the proof of Fermat's Last Theorem. In [2], Eisenbud and Mazur show that this problem is equivalent to one concerning symbolic squares in regular rings. Particularly, they ask whether a symbolic square of an unmixed ideal I contains a minimal generator of I. They conjecture this is never the case in characteristic zero, and are able to prove it in many situations. This section incorporates results of Eisenbud, Huneke, Hübl, Mazur, and Ribbe related to this question [5, 2, 4], and is an attempt to explain well the current status of the conjecture.

4.1 Definitions and Preliminary Results

Definition 4.1.1. *Let A be a ring and let T be a local A-algebra essentially of finite type (a localization of a finitely generated A-algebra). An **evolution** of T over A is a local A-algebra R essentially of finite type and a surjection $R \to T$ of A-algebras inducing an isomorphism*

$$\Omega_A(R) \otimes_R T \to \Omega_A(T).$$

The evolution is called trivial if $R \to T$ is an isomorphism.

We note the relationship between this definition and the conormal sequence. Indeed, if $T = R/I$, then we have an exact sequence

$$I/I^2 \xrightarrow{\delta} \Omega_A(R) \otimes_R T \to \Omega_A(T) \to 0.$$

Thus a surjection $R \to T$ is an evolution if and only if the image of δ is 0. One might ask if any nontrivial evolutions exist. The answer is yes, and the following proposition provides a large source of examples.

Proposition 4.1.2. *Let $f \in S := A[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$ and let $I =: \partial(f)$ the ideal generated by the partial derivatives of f. Then $R = S/I$ is an evolution of $T = S/(I, f)$, nontrivial when f is not contained in I.*

Proof. Note that the kernel of the map $R \to T$ is exactly $K = (I, f)/I$, so we must show that $\delta(K) = 0$. Since $I = 0$ in K we just need to show that $\delta(rf) = 0$ for all $r \in R$. Notice

$$\delta(rf) = 1 \otimes rd(f) + 1 \otimes fd(r) = r \otimes d(f) + f \otimes d(r) = 0 \in S/(I, f) \otimes \Omega_A(S/I)$$

where we see the first term is 0 since $d(f) = \sum \frac{\partial f}{\partial x_i} dx_i \in I\Omega_A(S/I)$ (by Theorem 2.1.7) and the second since $f = 0$ in T. □

This proposition may lead us to believe that nontrivial evolutions are everywhere, but for example, if we work over a field of characteristic zero, and f is quasi-homogeneous, then by the Euler formula, f is always contained in the ideal of partial derivatives. That is, $f \in \partial(f)$. We prove this in the following proposition and remark.

Proposition 4.1.3. *Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ be a homogeneous polynomial of degree k. Then*

$$k \cdot f = \sum x_i \frac{\partial f}{\partial x_i}$$

Proof. First suppose f is a monomial. Then we can write f as

$$x_1^{e_1} \cdots x_n^{e_n}$$

with $\sum e_i = k$. Then

$$\sum x_i \frac{df}{dx_i} = \sum e_i f = k \cdot f.$$

The result for general f follows by writing f as a sum of monomials and applying this result repeatedly. □

Remark 4.1.4. *This result holds more generally, when f is quasi-homogeneous, that is, if it is possible to assign strictly positive weights to the variables so that f becomes homogeneous. If x_i has weight w_i then the formula is*

$$\deg(f) \cdot f = \sum w_i x_i \frac{df}{dx_i}.$$

Further, it is straightforward to show that for all $f \in \mathbb{C}[x_1, \ldots, x_n]$ we have $f \in \sqrt{\partial(f)}$ so if I is a radical ideal then the construction in Proposition 4.1.2 will always produce a trivial evolution. In fact, there are no known examples of nontrivial evolutions of any reduced algebra T in equi-characteristic zero. To put this into perspective, consider the following question:

Question 4.1.5. *Suppose $f \in \mathbb{C}[[x_1, \ldots, x_n]]$ is a power series without constant term over the complex numbers, and I is the ideal of the reduced singular locus of f, that is, I is the radical of the ideal generated by the partial derivatives of f. Does it follow that $f \in (x_1, \ldots, x_n)I$?*

Although it seems incredibly elementary, this is a quite difficult question to answer. It is conjectured that the answer is "yes" and we will later see that this question is equivalent to asking whether reduced local $\mathbb{C}$ algebras have nontrivial evolutions.

Hence to find examples of nontrivial evolutions of reduced algebras in characteristic zero, we cannot hope to use Proposition 4.1.2. In this vein, we now attempt to find those reduced algebras T who have no nontrivial evolutions. This is a lofty goal, and will eventually culminate with the Eisenbud Mazur conjecture. As a first step we show that an algebra T has only trivial evolutions if and only if the map δ in the conormal sequence has a special property.

Definition 4.1.6. *Let T be a ring, and $\phi\colon M \to N$ an epimorphism of T-modules. Then ϕ is* minimal *if there is no proper submodule $M' \subset M$ such that $\phi(M') = N$.*

Proposition 4.1.7. *(Lenstra) Let A be a Noetherian ring and let T be a local A-algebra, essentially of finite type over A. Every evolution of T is trivial if and only if for some (equivalently all) presentations $T = S/I$, where S is a localization of a polynomial ring over A, the map*

$$\delta\colon I/I^2 \to \ker(T \otimes_S \Omega_A(S) \to \Omega_A(T))$$

induced by the universal derivation is minimal.

Proof. Let $T = S/I$ be any presentation of T where S is a localization of a polynomial ring in finitely many variables over A. Let J be an ideal of S with $J \subset I$. We make the following claim.

Claim: The natural surjection $\phi\colon S/J \to S/I = T$ is an evolution if and only if δ carries $(J + I^2)/I^2$ onto the same image as I/I^2.

Proof of Claim: $\Rightarrow$: We need to show that $\delta((J + I^2)/I^2) = \delta(I/I^2)$. The inclusion $\subset$ is obvious, so we prove the other. Let $x \in I$. We need to find some $z \in J + I^2$ so that $\delta(z + I^2) = \delta(x + I^2)$. This amounts to finding a z such that

$$1 \otimes dz = 1 \otimes dx$$

where the tensor product is taken in $T \otimes_S \Omega_A(S)$. We know that $\phi\colon S/J \to S/I = T$ is an evolution and that $\ker \phi = I/J$ with

$$(I/J)/(I/J)^2 = I/(I^2 + J).$$

Hence $\overline{\delta}(I/(I^2 + J)) = 0$ where

$$\overline{\delta}\colon I/(I^2 + J) \to T \otimes_{S/J} \Omega_A(S/J).$$

Thus we know that $1 \otimes dx = 0$ in $T \otimes_{S/J} \Omega_A(S/J)$. If $1 \otimes dx = 0$ in the larger module $T \otimes_S \Omega_A(S)$ then we can just set $z = 0$. If not, then this means that $x \in J$ so we are done.

$\Leftarrow$: Suppose that $\delta(I/I^2) = \delta((J+I^2)/I^2)$. We examine the map $\overline{\delta}$ defined above. We need to prove that the image of $\overline{\delta}$ is 0. Let $x \in I$, so $\overline{\delta}(x + (I^2 + J)) = 1 \otimes dx$ in $T \otimes_{S/J} \Omega_A(S/J)$. But then looking at $1 \otimes dx$ in $T \otimes_S \Omega_A(S)$ we see that $1 \otimes dx = 1 \otimes dj$ for some $j \in J$ which is zero in $T \otimes_{S/J} \Omega_A(S/J)$. This completes the proof of the claim. $\square$

Assuming the claim, from Nakayama's Lemma, (since T is local, Noetherian)

$$J = I \iff (J + I^2) = I \iff (J + I^2)/I^2 = I/I^2.$$

So δ is minimal if and only if T has no nontrivial evolution of the form S/J. We are done once we prove the minimality of δ is independent of the presentation. For then, we can write any evolution as S/J.

The family of presentations is filtered, meaning that any two presentations are simultaneously dominated by a third one. To this end, we see that it suffices to show that if $T = S/I$ is a presentation and S' is a localization of the polynomial ring $S[x]$, and S'/I' is a presentation extending $T = S/I$ in the obvious way, then δ_S is minimal iff $\delta_{S'}$ is minimal.

Let $g \in S$ be an element with the same image in T as x. Thus $x - g \in I'$. If $x - g$ is not zero, we can just rename our variable to be $x - g$, so we assume $g = 0$. Then we have $x \in I'$ so that $I'/I'^2 = I/I^2 \oplus Tx$ since $x^2 = 0 \in I'/I'^2$. Finally, note that $\mathrm{im}(\delta_{S'}) = Tdx \oplus \mathrm{im}(\delta_S)$.

Suppose that δ_S is minimal. Then let M be a submodule of I'/I'^2 such that $\delta_{S'}(M) = Tdx \oplus \mathrm{im}(\delta_S)$. But $M \subset I'/I'^2 = I/I^2 \oplus Tx$ so write $M = M_1 \oplus M_2$ where $M_1 \subset I/I^2$ and $M_2 \subset Tx$. But then $\delta_S(M_1) = \mathrm{im}(\delta_S)$ so since δ_S is minimal, $M_1 = I/I^2$. But then M_2 is a subset of Tx, say aTx. But then by Nakayama's lemma, $aTdx = Tdx$ if and only if $a = 1$ so $M_2 = Tx$ and $M = I'/I'^2$.

Conversely, suppose $\delta_{S'}$ is minimal and that $M \subset I/I^2$ is such that $\delta_S(M) = \mathrm{im}(\delta_S)$. Then $\delta_{S'}(M \oplus Tx) = Tdx \oplus \mathrm{im}(\delta_S) = \mathrm{im}(\delta_{S'})$, so $M = I/I^2$. □

Now we can begin studying A-algebras R which are evolutionarily stable; i.e. all evolutions are trivial. Mazur raised the following question in [2]

Question 4.1.8. *Let k be a field of characteristic 0 or a discrete valuation ring of mixed characteristics. Is it true that every reduced, flat, local algebra, which is essentially of finite type over k, is evolutionarily stable?*

This question forms the crux of this paper. One form of the Eisenbud-Mazur conjecture is that the answer to the above question is "yes". As we shall shortly see,

once we further unwrap what it means for an algebra to have no nontrivial evolutions, this conjecture can be stated quite beautifully in terms of commutative algebra. The following chain of results will culminate in the statement of the Eisenbud-Mazur conjecture in its classic form. We take the first result from Hübl in [4].

Corollary 4.1.9. *Let A be a Noetherian ring and T a local algebra essentially of finite type over A. Then the following are equivalent:*

(a) The algebra T is evolutionarily stable

(b) If $(S, \mathfrak{m})$ is a local algebra, essentially of finite type over A and if $I \subset S$ is an ideal with $T = S/I$ and if $f \in I$ with $D(f) \in I$ for all $D \in \mathrm{Der}_A(S)$, then

$$f \in m \cdot I.$$

(c) There exists a local algebra $A \to (S, \mathfrak{m})$, essentially of finite type, and an ideal $I \subset S$ with $R = S/I$ such that, if $f \in I$ with $\delta(f) \in I$ for all $\delta \in \mathrm{Der}_A(S)$, then

$$f \in \mathfrak{m} \cdot I.$$

Proof. Suppose T is evolutionarily stable and the A-algebra $(S, \mathfrak{m})$ is defined as above with $I \subset S$ so that f is as in (b) but $f \notin \mathfrak{m} \cdot I$. Then there exists some $J \subset I$ such that $J \neq I$ but $(J, f) = I$. Set $R = S/J$. Then the canonical map $R \to T$ is a nontrivial evolution since $d(f) \in I\Omega_A(S)$ as in the proof of Proposition 4.1.2. This shows that (a) implies (b).

Next suppose we have a nontrivial evolution $\epsilon\colon S/J \to S/I = T$ with $J \subset I$ then for $J \subset J' \subsetneq I$, S/J' will still be a nontrivial evolution. Thus we assume that I/J is cyclic with $I/J \cong f \cdot K$ where $K = S/\mathfrak{m}$ and $f \in I$. Then clearly f is a minimal generator so $f \notin \mathfrak{m} \cdot I$.

Now

$$\Omega_A(S/I) \cong \frac{\Omega_A(S)}{(I\Omega_A(S) + Sd(I))} \cong \frac{\Omega_A(S)}{(J\Omega_A(S) + f\Omega_A(S) + Sd(I))}$$

by Theorem 2.1.7. And by assumption, since we have an evolution,

$$\Omega_A(T) \cong T \otimes \Omega_A(S/J) \cong \Omega_A(\frac{S}{J}) \otimes \frac{S}{I} = \frac{\Omega_A(S/J)}{f\Omega_A(S/J)}$$

$$\cong \frac{\Omega_A(S)}{(J\Omega_A(S) + Sd(J) + f\Omega_A(S))}.$$

Thus since we have an evolution, $\delta(f)$ must be zero in $\Omega_A(T)$, where $\delta(f) = 1 \otimes df$. Hence

$$df \in J\Omega_A(S) + SD(J) + f\Omega_A(S) = I\Omega_A(S) + SD(J).$$

Thus there exist $g_i \in J, r_i \in S$ so that $df - \sum r_i dg_i = \eta \in I\Omega_A(S)$. Then if $h = f - \sum r_i g_i$ we have that $I/J = h \cdot K$ still, so $h \notin \mathfrak{m} \cdot I$ and also

$$dh = df - \sum r_i dg_i - \sum g_i dr_i = \eta - \sum g_i dr_i \in I\Omega_A(S).$$

Thus for all derivations D, $D(h) \in I$. Hence (b) implies (a).

The equivalence of conditions (b) and (c) follows from an argument similar to the one used in Proposition 4.1.7. □

The above result shows that there is some relationship between minimal generators of an ideal I (those elements in $I \setminus mI$) and evolutions of R/I. The following theorem will make this more explicit by using the symbolic square.

Definition 4.1.10. *If I is an ideal of the ring R then we define the nth symbolic power of I to be the ideal*

$$I^{(n)} = \left\{ f \in R \mid f \in I_Q^n \subset R_Q \text{ for all minimal primes } Q \text{ of } I \right\}.$$

Example 4.1.11.

If P is a prime ideal, then $P^{(n)} = R \cap PR_P$, or equivalently,

$$P^{(n)} = \{y \in R \mid \text{there exists } x \notin P \text{ with } xy \in P^n\}.$$

In the following theorem, we recall that if k is a field, and T is a k-algebra, then T is *generically separable* if the residue field extension $k \subset k(P)$ is separable for each minimal prime ideal P of T.

Theorem 4.1.12. *Let k be a field. Let $(S, \mathfrak{m})$ be a localization of a polynomial ring in finitely many variables over k and let I be an ideal of S. If $T := S/I$ is reduced and generically separable over k, then the kernel of*

$$\delta \colon I/I^2 \to T \otimes_S \Omega_k(S)$$

is $I^{(2)}/I^2$ and every evolution of T is trivial iff $I^{(2)} \subset \mathfrak{m}I$.

We begin the proof with two simple lemmas.

Lemma 4.1.13. *Let R be an A-algebra, with I and R-ideal. Then $f \in I^{(2)}$ implies $f \in I$ and $D(f) \in I$ for all $D \in \mathrm{Der}_A(R)$.*

Proof. Suppose $f \in I^{(2)}$. Then there exists some nonzero divisor s on I so that $sf \in I^2$. Since s is a nonzero divisor on I we have $f \in I$ and taking a derivative, we see that

$$fD(s) + sD(f) \in D(I^2) \subset I.$$

But $f \in I$ so $sD(f) \in I$ and as before, $D(f) \in I$. □

Lemma 4.1.14. *In the situation of Theorem 4.1.12,* $\ker \delta = I^{(2)}/I^2$ *and $f \in I^{(2)}$ iff $f \in I$ and $D(f) \in I$ for all $D \in \mathrm{Der}_A(R)$*

Proof. Let L be the kernel of δ. By Lemma 4.1.13, if $f \in I^{(2)}$ then $f \in I$ and $D(f) \in I$. hence $I^{(2)}/I^2 \subset L$. To show the converse we consider the exact sequence

$$0 \to L \to I/I^2 \to T \otimes_S \Omega_k(S) \to \Omega_k(T) \to 0.$$

Localizing at a minimal prime Q of I and using the fact that the module of differentials localizes (See Proposition 2.2.1) we have

$$0 \to L_Q \to QS_Q/Q^2S_Q \to T_Q \otimes_{S_Q} \Omega_k(S_Q) \to \Omega_k(T_Q) \to 0.$$

Note here that we used that $k_{Q\cap k} = k$. Also, since T is reduced, this means I is radical, so $I = p_1 \cap \cdots \cap p_r$ for some primes p_i. But then localizing at any one of them, will yield

$$I_{p_i} = (p_i)_{p_i} = p_i S_{p_i}$$

justifying our use of $I_Q = QS_Q$. Finally, since T is reduced, if we localize at a minimal prime, we get a field K. Thus we can compute vector space dimensions along the exact sequence

$$0 \to L_Q \to QS_Q/Q^2S_Q \to K \otimes_{S_Q} \Omega_k(S_Q) \to \Omega_k(K) \to 0.$$

By generic separability, we have by Propositions 3.2.1 and 3.2.6.

$$\dim_K \Omega_k(K) = \operatorname{trdeg}_k K.$$

Since S is just a localization of a polynomial ring over k we have that $\Omega_k(S)$ is free (Theorem 2.1.7 and Proposition 2.2.1) so we have that $K \otimes_{S_Q} \Omega_k(S_Q)$ is free, so to compute the dimension, we can compute the minimal number of generators. Thus

Theorem 3.3.4 gives

$$\mu(K \otimes_{S_Q} \Omega_k(S_Q)) = \mu(\Omega_k(S_Q)) = \text{edim} S_Q + \text{trdeg}_k K.$$

Finally, since $\dim_K QS_Q/Q^2S_Q = \text{edim}\, S_Q$ and since dimension is additive, we have that the dimension of L must be 0.

If $L_Q = 0$ for all minimal primes Q then we will show that $L \subset I^{(2)}/I^2$. First note that

$$I^{(2)} = \{f \in S \mid \text{for primes } Q \text{ minimal over } I \text{ there exists } z \in S \setminus Q : fz \in I^2\}.$$

Now let $f \in L$ and let Q be a minimal prime. Then since $L_Q = 0$ we have $fz = 0 \in I/I^2$ for some $z \in S \setminus Q$. Hence $fz \in I^2$ so $f \in I^{(2)}$. □

Proof of Theorem 4.1.12: To complete the proof of the theorem, we must prove that every evolution of T is trivial iff $I^{(2)} \subset \mathfrak{m}I$. But by Corollary 4.1.9, T is evolutionarily stable iff for all $f \in I$ with $\partial(f) \in I$ for all derivations ∂, $f \in \mathfrak{m}I$. But then our result follows immediately from Lemma 4.1.14. □

This theorem completes the translation into commutative algebra, and we are now able to state the Eisenbud-Mazur Conjecture in its classic form.

Conjecture 4.1.15. *(Eisenbud-Mazur) Let I be an unmixed radical ideal in a regular local ring $(R, \mathfrak{m})$ over a field of characteristic zero. Then $I^{(2)} \subset \mathfrak{m}I$*

Notice that this conjecture corresponds to Question 4.1.8, although it is phrased slightly differently. Theorem 4.1.12 provides the link to original question of Mazur in the case of a polynomial ring over a field, and it is possible to extend the results of this Theorem to the case when k is an arbitrary Noetherian regular ring. We will later see that it is necessary to require that R be regular when as there are easy counterexamples to the above conjecture in the case of non-regular rings.

The Eisenbud-Mazur conjecture can be stated in many different ways, but perhaps the most interesting is Question 4.1.5. Eisenbud and Mazur prove a variation of Corollary 4.1.9 in [2] which we state below.

Corollary 4.1.16. *There exists a reduced local $\mathbb{C}$-algebra T of finite type whose localization at the origin has a nontrivial evolution if and only if there exists a polynomial $f \in \mathbb{C}[[x_1, \ldots, x_n]]$ without constant term such that*

$$f \notin (x_1, \ldots, x_n)\sqrt{(f, df/dx_1, \ldots, df/dx_n)}.$$

Thus we can effectively study this problem only looking at derivatives in power series rings!

4.2 Current Progress

In the previous section, we showed that studying the existence of nontrivial evolutions is equivalent to studying ideals and symbolic squares via Theorem 4.1.12. Not surprisingly, progress on this problem has come by analyzing certain classes of ideals. We will consider the following question:

Question 4.2.1. *Let $(R, \mathfrak{m})$ be a local ring over a field k, and I an unmixed ideal. Is $I^{(2)} \subset \mathfrak{m}I$?*

As it turns out, there is an easy counterexample if we do not require R to be regular, and in [2], the authors construct counterexamples in every positive characteristic. Thus the statement in Conjecture 4.1.15 above seems most promising.

In this section we give a positive answer to Question 4.2.1 in some special cases. We first prove the result for monomial ideals and quasi-homogeneous ideals and then for perfect ideals of height two. We end with the counterexamples in characteristic p and the in the non-regular case.

4.2.1 Monomial and Quasihomogenous Ideals

Proposition 4.2.2. *(From [2]). Suppose that I is an unmixed monomial ideal in a polynomial ring $k[x_1, \ldots, x_n]$. Let $\mathfrak{m} = (x_1, \ldots, x_n)$. If P is a monomial prime ideal containing I then for any $d > 0$ we have $I^{(d)} \subset PI^{(d-1)}$. In particular this shows that*

$$I^{(2)} \subset \mathfrak{m}I^{(1)} = \mathfrak{m}I.$$

Proof. Suppose that $I = Q_1 \cap \cdots \cap Q_r$ is a primary decomposition for I. Then all the Q_i are monomial. Thus Q_i is primary to the monomial prime $P_i = (x_{i_1}, \ldots, x_{i_s})$, if and only if Q_i contains a power of each of the variables x_{i_t}, and the minimal generators of Q_i do not involve any variables other than $x_{i_1}, \ldots, x_{i_s}$. Because of this characterization, any power of a primary monomial ideal is again primary, and we claim $I^{(d)} = Q_1^d \cap \cdots \cap Q_r^d$. To see this, note that by the discussion in this paragraph, both sides have the same associated primes, which by the unmixedness of I implies that they are minimal primes. Thus to check equality we can verify it at the minimal primes, which then boils down to the definition of symbolic power.

Next suppose that ℓ is a monomial in $I^{(d)}$. Then by the argument above, for each index j we can write

$$\ell = r_j m_{j,1} \cdots m_{j,d}, \quad m_{j,i} \in Q_j$$

since $\ell \in \cap Q_j^d$. Since $\ell \in P$, some variable $x_t \in P$ divides ℓ and thus divides one of the $r_j, m_{j,1}, \ldots, m_{j,d}$. Thus ℓ/x_t may be written as a product with at least $d-1$ factors in Q_j, so $\ell/x_t \in \bigcap Q_j^{d-1} = I^{(d-1)}$. Thus $\ell \in PI^{(n-1)}$. □

This theorem can be generalized slightly in characteristic zero, by using the Euler formula given in Remark 4.1.4.

Proposition 4.2.3. *Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring over a field k, and let $\mathfrak{m} = (x_1, \ldots, x_n)$. Suppose that I is a radical R-ideal which is quasihomogeneous (that*

is, homogeneous with respect to some system of strictly positive integer weights of the variables). If $f \in I^{(d)}$ is a quasihomogeneous element, then $\deg(f) \cdot f \in \mathfrak{m}I^{(d-1)}$. *In particular, if* $\operatorname{char}(k) = 0$ *then* $I^{(d)} \subset \mathfrak{m}I^{(d-1)}$.

Proof. If $f \in I^{(d)}$ then there is an element h not contained in any minimal prime of I such that $hf \in I^d$. Differentiating, we obtain

$$h \cdot df/dx_j + f \cdot dh/dx_j \in I^{d-1}$$

for each j. Since $f \in I^{(d-1)}$ we have $h \cdot df/dx_j \in I^{(d-1)}$, and since h is not contained in any minimal prime of I, $df/dx_j \in I^{(d-1)}$. By Euler's formula (see Remark 4.1.4),

$$\deg(f) \cdot f = w_j \cdot x_j \cdot df/dx_j$$

where w_j is the weight of x_j. This shows that

$$\deg(f) \cdot f \in \mathfrak{m}I^{(d-1)}. \qquad \square$$

4.2.2 Perfect ideals of Height 2

To prove the conjecture for perfect ideals of height two we will use Fitting ideals defined earlier. Before starting the proof, we recall some basic facts.

Remark 4.2.4. *Let M be a finitely generated R-module.*

- *If $M' \subset M$ is a submodule, then* $\operatorname{Fitt}_i(M) \subset \operatorname{Fitt}_i(M/M')$.
- *If $I \subset R$ is an ideal then* $\operatorname{Fitt}_i(M/IM) \subset \operatorname{Fitt}_i(M) + I$.

Both of these facts are straightforward to derive, and come almost immediately by thinking of the relationship between the presentation matrices for the different modules. We begin our proof of the theorem with a lemma about Fitting ideals which is given in [2]. The proof given is due to Huneke.

Lemma 4.2.5. *If I is an ideal of grade $\geq c$ in a Noetherian ring, then* $\mathrm{Fitt}_{c-1}(I) \subset I$.

Proof. It is possible to choose a set of generators $\{f_1, \ldots, f_m\}$ for I such that every subset of $c-1$ elements forms a regular sequence since the ideal has grade at least c. This is tedious to verify, but follows from the fact that a complete intersection can always be generated by a set of elements which is a regular sequence in any order. A proof of this statement is outlined in Exercise 17.6 of [1]. Let ϕ be the matrix of relations on these generators.

We now use Cramer's rule to see that every $m-c+1$ minor of a presentation matrix for I multiplies I into the ideal generated by some subset of $c-1$ of the f_i. We work this out in detail because it is interesting and a good review of linear algebra. Without loss of generality, we suppose the minor we are looking at is in the bottom left of the matrix ϕ. Suppose that ϕ has block form

$$\begin{bmatrix} * & * \\ B & * \end{bmatrix}$$

where B is an $(m-c+1) \times (m-c+1)$ square matrix. Then since ϕ is the matrix of relations,

$$[f_1, \ldots, f_m] \begin{bmatrix} * \\ B \end{bmatrix} = 0.$$

which implies that $[f_c, \ldots, f_m]B = (b_1, \ldots, b_{m-c+1})$ where $b_i \in (f_1, \ldots, f_{c-1})$.

Now Cramer's rule says that

$$\det B \cdot f_k = \det(B_k),$$

where B_k is the matrix obtained from B by replacing the k^{th} column by $[b_1, \ldots, b_{m-c+1}]$.

Thus by expanding this determinant by the k^{th} column, we see that

$$\det B \cdot f_k \in (f_1, \ldots, f_{c-1})$$

as required. We have just proven that every $m-c+1$ minor of ϕ multiplies I into an ideal I' generated by some regular sequence generated by $c-1$ of the f_i. In symbols, $\det B \cdot I \subset I'$.

Because the grade of I is at least c, I contains a non zero divisor modulo I', this implies that $\det B \in I'$. This implies that $\mathrm{Fitt}_{c-1}(I) \subset I$. □

With this theorem in hand, we are ready to state a criterion for an element to be in the symbolic square of an ideal which involves the Fitting ideal.

Theorem 4.2.6. *Suppose I is an unmixed ideal of depth $\geq c$ in a Noetherian ring, and $x \in I$. If $x \in I^{(2)}$ then*

$$\mathrm{Fitt}_{c-1}(I/(x)) \subset I.$$

If I is generically a complete intersection of height c then the converse holds as well.

Note that when we say I is "generically a complete intersection of height c" we mean that I is unmixed of height c and that at all minimal primes Q of I, I_Q is a complete intersection - generated by a regular sequence.

Proof. First let $x \in I^{(2)}$. We would like to show that $\mathrm{Fitt}_{c-1}(I/(x)) \subset I$. It suffices to prove this inclusion at all associated primes of I, and since I is unmixed, at the minimal primes of I. After localizing, we may assume that $x \in I^2$.

Now $I/(x)$ surjects onto $I/I^2 = I \otimes R/I$, so from the relations in 4.2.4 we have

$$\mathrm{Fitt}_{c-1}(I/(x)) \subset \mathrm{Fitt}_{c-1}(I/I^2) \subset \mathrm{Fitt}_{c-1}(I) + I$$

and we are done by the previous lemma.

Conversely, suppose I is generically a complete intersection of depth c and $\mathrm{Fitt}_{c-1}(I/(x))$ is contained in I. To show that $x \in I^{(2)}$ it is enough to show this locally at the associated primes of $I^{(2)}$. Since the associated primes of $I^{(2)}$ are all minimal primes of I, we may begin by localizing at one and suppose that $I = (f_1, \ldots, f_c)$ is a complete intersection. In this situation we have $I^2 = I^{(2)}$, and we want to prove that $x \in I^2$.

The ideal I is generated by the c element f_i. We may take the same generators for $I/(x)$. One of the relations for $I/(x)$ may be represented as a column vector whose entries g_i satisfy $x = \sum g_i f_i$. From the definition of $\mathrm{Fitt}_{c-1}(I/(x))$, these are the minors of size $c - (c-1) = 1$ of the presentation matrix. Thus $g_i \in \mathrm{Fitt}_{c-1}(I/(x))$ which implies that $g_i \in I$ by assumption, so that $x = \sum g_i f_i \in I^2$. □

The ideas in the previous proof yield an easy generalization:

Proposition 4.2.7. *If I is an unmixed ideal of depth $\geq c$ in a Noetherian ring and I is generically a complete intersection then $x \in I^{(d+1)}$ if and only if*

$$\mathrm{Fitt}_{N-1}(I^{(d)}/(x)) \subset I,$$

where $N = \binom{c+d-1}{d}$.

Finally we are ready to state the main result of this section - that concerns the symbolic square of a grade 2 perfect ideal. Recall that a grade two perfect ideal is one which contains a regular sequence of length 2 and that has projective dimension 1 as an R-module. By the famous Hilbert-Burch theorem, these are ideals of maximal minors of $n \times (n-1)$ matrices.

Theorem 4.2.8. *Let $(R, \mathfrak{m})$ be a local ring. Suppose I is a perfect R-ideal of height two which is generically a complete intersection and is generated by the $(n-1)\times(n-1)$ minors of a matrix M. If J is the ideal generated by the entries of any column of the matrix of M, then $I^{(2)} \subset IJ$. In particular, if the entries of M are contained in $\mathfrak{m}$ then $I^{(2)} \subset \mathfrak{m}I$.*

Proof. By the Hilbert-Burch theorem, a free resolution of I is of the form

$$0 \to R^{n-1} \to R^n \to I \to 0$$

where the left hand map is given by M. The generator of I coming from the jth generator of R^n is exactly the minor obtained from M involving all but the jth row. Now let $x \in I$. We will show that x can be seen as the determinant of an $n \times n$ matrix, whose first $n-1$ columns are the columns in M.

To see this, let $\{f_1, \ldots, f_n\}$ be generators for i. Since $x \in I$ we have that $x = \sum r_i f_i$ for some $r_i \in R$. Then forming the matrix

$$N = \left(\begin{array}{c|c} & \pm r_1 \\ M & \vdots \\ & \pm r_n \end{array}\right)$$

with the appropriate signs, we see by expanding about the last column that $x = \det N$.

Now let $x \in I^{(2)}$. We will show $x \in IJ$ if J is the ideal generated by one of the columns. The matrix N is a presentation matrix of $I/(x)$, so by the previous theorem, $x \in I^{(2)}$ if and only if $\mathrm{Fitt}_1(I/(x)) \subset I$, that is, if and only if the $(n-1) \times (n-1)$ minors of N are contained in I. Expanding the determinant of N along a column of M we see that $x = \det N \in IJ$ where J is the ideal generated by the entries in that column. This completes the proof. □

4.2.3 Counterexamples

In this section we give two counterexamples to the Eisenbud-Mazur conjecture under weaker hypotheses. In the first we give an easy counterexample when R is not regular, and in the second we exhibit that $I^{(2)} \subset \mathfrak{m}I$ does not need to hold in rings of positive characteristic.

Example 4.2.9. *(Non-regular case)*

Let $R = \mathbb{C}[[x, y, z]]/(x^2 - yz)$ and let $P = (x, y)$. Then P is prime and $P^{(2)} = (y)$ since $y = x^2 \cdot z^{-1} \in P^2 R_P$. But y is clearly a minimal generator of P.

Example 4.2.10. *(Positive Characteristic Case)*

This counterexample is from [2]. Let k be a field of characteristic $p > 0$, and let I be the kernel of the map

$$\begin{aligned} k[x_1, \ldots, x_4] &\rightarrow k[t] \\ x_1,\ x_2,\ x_3,\ x_4 &\mapsto t^{p^2},\ t^{p(p+1)},\ t^{p^2+p+1},\ t^{(p+1)^2} \end{aligned}$$

(or the localization of this ideal at the maximal ideal $(x_1, \ldots, x_4)$). Let

$$f = x_1^{p+1} x_2 - x_2^{p+1} - x_1 x_3^p + x_4^p.$$

We will prove that f is a minimal generator of I but f is contained in $I^{(2)}$.

To show that $f \in I^{(2)}$, consider the following polynomials

$$\begin{aligned} g_1 &= x_1^{p+1} - x_2^p \\ g_2 &= x_1 x_4 - x_2 x_3 \\ g_3 &= x_1^p x_2 - x_3^p \end{aligned}$$

One can check by applying the homomorphism of rings above that

$$f, g_1, g_2, g_3 \in I.$$

Since $k[t]$ is a domain, by the first isomorphism theorem, $k[x_1, \ldots, x_4]/I$ is isomorphic

to a subring of $k[t]$ and thus is a domain so that I is prime. We note that

$$x_1^p f = g_1 g_3 + g_2^p$$

and $x_1 \notin I$ so that by Example 4.1.11 this shows $f \in I^{(2)}$.

All that remains now is to prove that f is a minimal generator. Since f has a term x_4^p, it suffices to show that no element of I has a term of the form x_4^a with $0 < a < p$. Since I is generated by binomials, it suffices to show that there is no binomial of the form $x_4^a - x_3^b x_2^c x_1^d$ in I, or equivalently that the equation

$$a(p+1)^2 = b(p^2+p+1) + cp(p+1) + dp^2 \qquad (\star)$$

cannot be satisfied by nonnegative integers a, b, c, d with $0 < a < p$.

Reducing $(\star)$mod p we see that $a \equiv b \mod p$. If $b = a + np$ for some $n \geq 1$ then subtracting $a(p+1)^2$ from both sides, the above equation becomes

$$0 = (np(p^2+p+1) - ap) + cp(p+1) + dp^2.$$

This implies that $ap \geq np(p^2+p+1)$. Now since $0 < a < p$ we have

$$(p-1)p \geq ap \geq np(p^2+p+1)$$

which is impossible. Thus $a = b$. Subtracting $a(p^2+p+1)$ from both sides of $(\star)$ we get

$$p(p-1) \geq ap = cp(p+1) + dp^2$$

but then the right hand is either 0 or greater than p^2, a contradiction. $\square$

4.3 Open Conjectures

In addition to the Eisenbud-Mazur conjecture, there are other (considerably older) conjectures concerning the module of differentials. We discuss a few in this section. In this section suppose that k is a perfect field and R is a local k-algebra, a domain, and essentially of finite type.

Conjecture 4.3.1. *(Berger) Suppose that* $\operatorname{trdeg}_k \operatorname{Quot}(R) = 1$. *Then* $\Omega_k(R)$ *is torsion free iff* R *is regular. Note especially that this implies that* $\Omega_k(R)$ *is torsion free iff it is free.*

A stronger statement that implies Berger's conjecture is the following. If $\dim R = 0$, then $\ell(\Omega_k(R)) \geq \ell(R)$.

The following conjecture is false in characteristic $p > 0$ and asks a question dual to Berger's conjecture.

Conjecture 4.3.2. *(Zariski-Lipman) Suppose* $\operatorname{char} k = 0$. *Then* $\operatorname{Der}_k(R)$ *is free iff* R *is regular.*

Finally, we ask a question about the projective dimension of the module of differentials. The follow suggests that the projective dimension is always $0, 1$ or infinite.

Conjecture 4.3.3. *(Vasconcelos) If* $\operatorname{pd}_R \Omega_k(R) < \infty$ *and* R *is a complete intersection, that is, the quotient of a regular local ring by a complete intersection, then* $\operatorname{pd}_R \Omega_k(R) \leq 1$.

Bibliography

[1] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[2] David Eisenbud and Barry Mazur. Evolutions, symbolic squares, and Fitting ideals. *J. Reine Angew. Math.*, 488:189–201, 1997.

[3] Matthias Flach. A finiteness theorem for the symmetric square of an elliptic curve. *Invent. Math.*, 109(2):307–327, 1992.

[4] Reinhold Hübl. Evolutions and valuations associated to an ideal. *J. Reine Angew. Math.*, 517:81–101, 1999.

[5] Craig Huneke and Juergen Ribbe. Symbolic squares in regular local rings. *Math. Z.*, 229(1):31–44, 1998.

[6] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[7] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[8] Masayoshi Nagata. *Local rings*. Interscience Tracts in Pure and Applied Mathematics, No. 13. Interscience Publishers a division of John Wiley & Sons New York-London, 1962.

[9] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[10] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.