RAMIFICATION THEORY. NOTES

MANOJ KUMMINI

Outline

These are notes from a course during Aug–Nov 2018 on the ramification theory of noetherian local rings, following [AB59] and the various differents that appear in this context. These notes begin with a review of commutative algebra ([Eis95], [Mat80], [Mat89])Then comes a discussion of Kähler differentials ([Eis95], [Kun86], [Mat80], [Mat89]). The results of [AB59] and some topics on differents ([Ber61], [SS74]) are discussed next.

Notation

By a ring, we mean, unless something is mentioned explicitly to the contrary, commutative rings with identity. Ring homomorphisms are assumed to take the multiplicative identity to the multiplicative identity.

Mod_R: the category of all R-modules, for a ring R.

R, S: rings.

1. Examples

1.1. **Background**. Let $R \longrightarrow S$ be a ring homomorphism. For a prime ideal $\mathfrak{p}$ of R, we are interested in studying when $\mathfrak{p}S$ is *not* a prime ideal of S. We do not define ramification in this section, but look at two examples that illustrate the question.

1.2. **Example**: **Gaussian integers**. $R = \mathbb{Z}$, $S = \mathbb{Z}[\imath]$. Let $p \in \mathbb{Z}$ be a prime number. We look at the ideal pS. See [Art91, Section 11.5] for details.

(1) $p = 2$: In S, we can write $2 = (1+\imath)(1-\imath) = -\imath(1+\imath)^2$, so $(2)S = ((1+\imath)S)^2$. Use the euclidean norm $a + \imath b \mapsto a^2 + b^2$ for $a, b \in \mathbb{Z}$ to see that S is a PID and that $1 + \imath$ is irreducible and, hence, prime. Therefore we say that 2 *ramifies* in S. Precise definition will come later.

(2) $p = 5$. In R, $5 = 2^2 + 1^2$, so in S, $5 = (2+\imath)(2-\imath)$. Can check that $(2+\imath)$ and $(2-\imath)$ are irreducible in S, so they are prime elements. They are not multiples of each other by units in S, so we say that 5 *splits* into distinct primes in S. Same argument can be given for all prime numbers p that can be expressed as a sum of two squares in R; it is known that such p are exactly those congruent to $1 \mod 4$.

(3) $p = 3$. Suppose that $3 = (a + \imath b)(c + \imath d)$. Looking at the norms, we see that $(a^2 + b^2)(c^2 + d^2) = 9$, so $(a^2 + b^2) = 1, 3$ or 9. There do no exists integers a, b such that $(a^2 + b^2) = 3$. If $(a^2 + b^2) = 1$, $(a + \imath b)$ is a unit in S. If $(a^2 + b^2) = 9$, $(c + \imath d)$ is a unit in S. Hence 3 is irreducible and hence prime in S.

The following proposition is proved in [Art91, Section 11.5].

1.2.1. **Proposition**. *Let p be a prime number. Then p is prime in S or $p = \pi\overline{\pi}$ for a pair of complex conjugate primes in S.*

Proof. Since p is not a unit in S, it has a prime divisor $\pi := a + \imath b$. Then $\overline{\pi} = a - \imath b$ divides $\overline{p} = p$, so $a^2 + b^2$ divides p^2. Since $a + \imath b$ is not a unit in S, $a^2 + b^2 > 1$, so $a^2 + b^2 = p$, in which case $p = \pi\overline{\pi}$, or $a^2 + b^2 = p^2$, in which case $p = u\pi$ for some unit $u \in S$ (look at the euclidean norm), and, hence, p is a prime element in S. □

1.2.2. **Observation**. Note that $\mathbb{Q}(\imath) \simeq \mathbb{Q}(x)/(x^2+1)$ and that $\mathbb{Z}[\imath] \simeq \mathbb{Z}[x]/(x^2+1)$. The discriminant of $x^2 + 1$ is -4. The only prime number that divides it is 2; it is the only prime that ramifies in $\mathbb{Z}[\imath]$. We will later see that this is not a coincidence. □

1.3. **Example**: **Branched coverings of curves**. Let $R = \mathbb{C}[t]$ and $S = \mathbb{C}[t,x]/((x - f_1(t))(x - f_2(t))(x - f_3(t)))$, where the $f_i(t)$ belong to R. This gives a map $\operatorname{Spec} S \longrightarrow \operatorname{Spec} R \simeq \mathbb{C}^1$. Take a prime ideal $(t-\alpha)$ of R. $S/(t-\alpha)S \simeq \mathbb{C}[t,x]/((x-f_1(\alpha))(x-f_2(\alpha))(x-f_3(\alpha)), t-\alpha) \simeq \mathbb{C}[x]/((x-f_1(\alpha))(x-f_2(\alpha))(x-f_3(\alpha)))$, so if $f_i(\alpha) = f_j(\alpha)$ for some $i \neq j$, the prime ideal $(t-\alpha)$ ramifies in S. If the three $f_i(\alpha)$ are distinct, there are three distinct points of $\operatorname{Spec} S$ that map to the point $\alpha \in \mathbb{C}^1$. Again, ramification happens over the prime ideals $(t-\alpha)$ containing the discriminant $(f_1(t) - f_2(t))(f_1(t) - f_3(t))(f_2(t) - f_3(t))$.

1.4. **Example**: **blow-up**. Let $R = \mathbb{C}[x,y,z]/(x^2 + y^3 + z^5)$ and $\mathfrak{m} = (x,y,z)R$. Let $S = R \oplus \mathfrak{m} \oplus \mathfrak{m}^2 \oplus \cdots$, thought of as a graded R-algebra. Note that if $\mathfrak{p} \in \operatorname{Spec} R$, $\mathfrak{p} \neq \mathfrak{m}$, then $(R \smallsetminus \mathfrak{p})^{-1}S \simeq R_{\mathfrak{p}}[t]$. Hence $f : \operatorname{Proj} S \longrightarrow \operatorname{Spec} R$ is a morphism with the following property: over $\operatorname{Spec} R \smallsetminus \{\mathfrak{m}\}$, it is an isomorphism, since $\operatorname{Proj} A[t] \simeq \operatorname{Spec} A$ for every ring A. To understand what happens over $\{\mathfrak{m}\}$, we look at an affine covering of $\operatorname{Proj} S$ given by $\operatorname{Spec} R[\frac{y}{x}, \frac{z}{x}]$, $\operatorname{Spec} R[\frac{x}{y}, \frac{z}{y}]$ and $\operatorname{Spec} R[\frac{x}{z}, \frac{y}{z}]$. Write $A = R[\frac{x}{y}, \frac{z}{y}]$. Note that

$$\frac{\mathbb{C}[x,y,z,x_1,z_1]}{(y^2(x_1^2 + y + y^3z_1^5), x - yx_1, z - yz_1)} \simeq \frac{\mathbb{C}[y,x_1,z_1]}{(y^2(x_1^2 + y + y^3z_1^5))} \twoheadrightarrow A.$$

By looking at the dimensions and noting that y is a non-zero-divisor in A, we conclude that $A \simeq \mathbb{C}[y,x_1,z_1]/(x_1^2 + y + y^3z_1^5)$. Then $\mathfrak{m}A = yA = (x_1^2, y)A$. Hence there is a unique minimal prime $\mathfrak{P}$ over $\mathfrak{m}A$, with $\operatorname{ht} \mathfrak{P} = 1$. Further

$$\lambda_{A_{\mathfrak{P}}}\left(\frac{A_{\mathfrak{P}}}{\mathfrak{m}A_{\mathfrak{P}}}\right) = 2.$$

2. Tensor products

In this section, we review, mostly without proofs, some facts about tensor products.

Let M, N and P be R-modules. A function $f : M \times N \longrightarrow P$ (where $M \times N$ is the cartesian product, i.e., the product in the category of sets) is said to *R-bilinear* (or, merely *bilinear*, if no confusion is likely to arise) if for every $x \in M$, the function $N \longrightarrow P, y \mapsto f(x,y)$ is R-linear and for every $y \in N$, the function $M \longrightarrow P, x \mapsto f(x,y)$ is R-linear.

2.1. **Definition**. Let M, N be R-modules. Let F be the free R-module with basis $M \times N$ and Q the submodule generated by all the elements of F of the form

$$\begin{gathered}(x + x', y) - (x,y) - (x',y),\\ (x, y + y') - (x,y) - (x,y')\\ (rx, y) - (x, ry)\end{gathered}$$

where x, x' are in M, y, y' are in N and r is in R. The *tensor product of M and N*, denoted by $M \otimes_R N$, is the R-module F/Q. The image of $(x,y) \in M \times N$ under the map $M \times N \hookrightarrow F \longrightarrow M \otimes_R N$ is denoted $x \otimes_R y$.

We observe that the elements of $M \otimes_R N$ of the form $x \otimes_R y$ generate $M \otimes_R N$ as an R-module. The map $M \times N \longrightarrow M \otimes_R N$ is R-bilinear.

2.2. **Proposition.** *Let M, N and P be R-modules. Then every R-linear map $M \otimes_R N \longrightarrow P$ induces an R-bilinear map $M \times N \longrightarrow P$. Conversely, if $f : M \times N \longrightarrow P$ an R-bilinear map, then there exists a unique R-linear map $\widetilde{f} : M \otimes_R N \longrightarrow P$ such that $\widetilde{f}(x \otimes_R y) = f(x, y)$.*

This proposition implies that

$$\mathrm{Hom}_R(M \otimes_R N, P) \simeq \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, P))$$

for all R-modules M, N and P. We rephrase this to say that the functor $- \otimes_R N$ (from Mod_R to Mod_R) is left-adjoint to the functor $\mathrm{Hom}_R(N, -)$. Using this property, we can prove that the functor $- \otimes_R N$ is right exact.

Let M and N be R-modules, with generating sets $\{x_\lambda \mid \lambda \in \Lambda\}$ and $\{y_i \mid i \in \mathcal{I}\}$ respectively. Then $\{x_\lambda \otimes_R y_i \mid \lambda \in \Lambda, i \in \mathcal{I}\}$ is a generating set for $M \otimes_R N$. In particular, if M and N are finitely generated, so is $M \otimes_R N$.

We now discuss base-change. Let $\phi : R \longrightarrow S$ be a ring map. For an R-module M, we write $\phi^* M = S \otimes_R M$; for an S-module N, we write and $\phi_* N$ for the abelian group N thought of as an R-module through the map ϕ ('restriction of scalars'). If $\{x_\lambda \mid \lambda \in \Lambda\}$ is a generating set of M as an R-module, then $\{1 \otimes_R x_\lambda \mid \lambda \in \Lambda\}$ is a generating set of $\phi^* M$ as an S-module.

Let N be an R-module, and M and P S-modules. Then $M \otimes_R N$ has a natural S-module structure, with S acting on M; $\mathrm{Hom}_S(M, P)$ has an R-module structure through ϕ. Then there is a general version of this adjointness; see [Bou98, Chapter II, §4] for a proof (in an even more general set-up).

2.3. **Proposition.** $\mathrm{Hom}_S(M \otimes_R N, P) \simeq \mathrm{Hom}_R(N, \phi_* \mathrm{Hom}_S(M, P))$. *In particular (with $M = S$) we have* $\mathrm{Hom}_S(\phi^* N, P) \simeq \mathrm{Hom}_R(N, \phi_* P)$.

Let $f : R \longrightarrow S$ and $g : R \longrightarrow T$ be ring maps. Then the R-module $S \otimes_R T$ is a ring in which multiplication is defined by $(s \otimes_R t)(s' \otimes_R t') = ss' \otimes_R tt'$ and extended R-linearly. The maps

$$g' : S \longrightarrow S \otimes_R T, s \mapsto s \otimes_R 1, \text{ and}$$
$$f' : T \longrightarrow S \otimes_R T, t \mapsto 1 \otimes_R t$$

are ring homomorphisms giving a commutative diagram

$$\begin{tikzcd} T \arrow[r, "f'"] & S \otimes_R T \\ R \arrow[u, "g"] \arrow[r, "f"] & S, \arrow[u, "g'"'] \end{tikzcd}$$

of R-algebras. Moreover, if A is an R-algebra such that there are R-algebra maps $u : S \longrightarrow A$ and $v : T \longrightarrow A$, then there exists a unique R-algebra map $\mu : S \otimes_R T \longrightarrow A$ such that $u = \mu g'$ and $v = \mu f'$. This makes $S \otimes_R T$ the coproduct of S and T in the category of R-algebras. Note that this set-up commutes with localization in R.

We can write $T = R[\{X_\lambda : \lambda \in \Lambda\}]/\mathfrak{a}$ for a set $\{X_\lambda : \lambda \in \Lambda\}$ of variables and an ideal $\mathfrak{a} \in R[\{X_\lambda : \lambda \in \Lambda\}]$. Then we get an exact sequence

$$S \otimes_R \mathfrak{a} \longrightarrow S[\{X_\lambda : \lambda \in \Lambda\}] \longrightarrow S \otimes_R T \longrightarrow 0.$$

The image of $S \otimes_R \mathfrak{a} \longrightarrow S[\{X_\lambda : \lambda \in \Lambda\}]$ is the extension of $\mathfrak{a}$ under the morphism $R[\{X_\lambda : \lambda \in \Lambda\}] \longrightarrow S[\{X_\lambda : \lambda \in \Lambda\}]$ induced by f.

Taking $A = T = S$, $f = g$, $u = v = \mathrm{id}_S$, we get a map of

$$\mu : S \otimes_R S \longrightarrow S, s \otimes s' \mapsto ss' \tag{2.4}$$

R-algebras. This map comes up often while studying properties of morphisms.

2.5. **Example.** Let $S = R[X_1, \ldots, X_n]$, where the X_i are variables. Then $S \otimes_R S \simeq R[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ where the Y_j are variables, disjoint from the X_i. The kernel of μ is the ideal $(X_1 - Y_1, \ldots, X_n - Y_n)$.

2.6. **Remark.** $\operatorname{Spec}(-)$ is contravariant functor from the category of rings to the category of schemes. Fix a ring R. Then the restriction of $\operatorname{Spec}(-)$ to the full subcategory of R-algebras is a functor to the category of schemes over $\operatorname{Spec} R$. In fact, using $\operatorname{Spec}(-)$, we can identify the category of schemes over $\operatorname{Spec} R$ as the opposite category of the category of R-algebras. Hence $\operatorname{Spec}(S \otimes_R T)$ is the fibred product $\operatorname{Spec} S \times_{\operatorname{Spec} R} \operatorname{Spec} T$ [Har77, Section II.3].

3. Projective and flat modules

3.1. **Proposition.** *Let P be an R-module. Then the following are equivalent:*

(1) The functor $\operatorname{Hom}_R(P, -)$ is exact;

(2) for every surjective morphism $\alpha : M \longrightarrow N$ of R-modules, and every R-linear morphism $f : P \longrightarrow N$, there exists $g : P \longrightarrow M$ such that $f = \alpha g$, or equivalently, the morphism

$$\operatorname{Hom}_R(P, M) \longrightarrow \operatorname{Hom}_R(P, N), \phi \mapsto \alpha\phi$$

is surjective;

(3) every surjective homomorphism $M \longrightarrow P$ splits;

(4) P is a direct summand of a free R-module;

We first note that a functor is exact if and only if it takes short exact sequences to short exact sequences.

Proof. (1) $\iff$ (2): Assume (1). We have an exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(P, \ker\alpha) \longrightarrow \operatorname{Hom}_R(P, M) \longrightarrow \operatorname{Hom}_R(P, N) \longrightarrow 0$$

from which we conclude (2). Conversely if (2) holds, then $\operatorname{Hom}_R(P, -)$ takes short exact sequences to short exact sequences, so (1) holds.

(2) $\implies$ (3): Apply with $P = N$ and $f = \mathrm{id}_P$.

(3) $\implies$ (4): There is a free module F with a surjective map $F \longrightarrow P$.

(4) $\implies$ (2): Let F be a free module with P as a direct summand. Write $F = P \oplus P'$. Since morphism

$$\operatorname{Hom}_R(F, M) \longrightarrow \operatorname{Hom}_R(F, N)$$

splits the direct sum

$$(\operatorname{Hom}_R(P, M) \longrightarrow \operatorname{Hom}_R(P, N)) \oplus (\operatorname{Hom}_R(P', M) \longrightarrow \operatorname{Hom}_R(P', N))$$

it suffices to show that

$$\operatorname{Hom}_R(F, M) \longrightarrow \operatorname{Hom}_R(F, N)$$

is surjective. Hence we may assume that P is free, with basis $\{e_\lambda, \lambda \in \Lambda\}$. Let x_λ be a pre-image of $f(e_\lambda)$. Define $g(e_\lambda) = x_\lambda$.

□

3.2. **Definition**. An R-module P is said to be *projective* if it satisfies the equivalent conditions of the above proposition.

3.3. **Proposition**. *Let P be a finitely generated R-module. Then P is projective if and only if $P_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module for every $\mathfrak{p} \in \operatorname{Spec} R$.*

Proof. It follows from Proposition 3.1 that an R-module M is projective if and only if $M_{\mathfrak{p}}$ is a projective $R_{\mathfrak{p}}$-module for every $\mathfrak{p} \in \operatorname{Spec} R$. Hence it suffices to show that a finitely generated projective module over a local ring is free. Without loss of generality we may assume that $(R, \mathfrak{m}, \Bbbk)$ is a local ring. Let $t = \operatorname{rk}_{\Bbbk} P/\mathfrak{m}P$. Hence there exists a split exact sequence

$$0 \longrightarrow P' \longrightarrow R^t \longrightarrow P \longrightarrow 0.$$

We want to show that $P' = 0$. This follows from observing that

$$t = \operatorname{rk}_{\Bbbk} R^t/\mathfrak{m}R^t = \operatorname{rk}_{\Bbbk} P/\mathfrak{m}P + \operatorname{rk}_{\Bbbk} P'/\mathfrak{m}P' = t + \operatorname{rk}_{\Bbbk} P'/\mathfrak{m}P'. \qquad \square$$

Let N be an R-module. The functor $\operatorname{Hom}_R(-, N)$ is not exact. However, if $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ is an exact sequence with M_3 projective, it splits, and, therefore, the sequence

$$0 \longrightarrow \operatorname{Hom}_R(M_3, N) \longrightarrow \operatorname{Hom}_R(M_2, N) \longrightarrow \operatorname{Hom}_R(M_1, N) \longrightarrow 0$$

is split exact. Every R-module M has a projective resolution, i.e., a complex

$$P_\bullet : \cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

that is exact everywhere except at the 0th stage, where the homology is isomorphic to M. Now any exact sequence $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ of R-modules, we can find projective resolutions P, P' and P'' of M_1, M_2 and M_3 respectively that fit into a double complex

$$\begin{tikzcd}
 & {} \arrow[d] & {} \arrow[d] & {} \arrow[d] & \\
0 \arrow[r] & P_{i+1} \arrow[r] \arrow[d] & P'_{i+1} \arrow[r] \arrow[d] & P''_{i+1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_i \arrow[r] \arrow[d] & P'_i \arrow[r] \arrow[d] & P''_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_{i-1} \arrow[r] \arrow[d] & P'_{i-1} \arrow[r] \arrow[d] & P''_{i-1} \arrow[r] \arrow[d] & 0 \\
 & {} & {} & {} &
\end{tikzcd}$$

Applying $\operatorname{Hom}_R(-,N)$ yields the double complex

$$\begin{tikzcd}
 & \uparrow & \uparrow & \uparrow & \\
0 \arrow[r] & \operatorname{Hom}_R(P''_{i+1},N) \arrow[r] \arrow[u] & \operatorname{Hom}_R(P'_{i+1},N) \arrow[r] \arrow[u] & \operatorname{Hom}_R(P_{i+1},N) \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & \operatorname{Hom}_R(P''_i,N) \arrow[r] \arrow[u] & \operatorname{Hom}_R(P'_i,N) \arrow[r] \arrow[u] & \operatorname{Hom}_R(P_i,N) \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & \operatorname{Hom}_R(P''_{i-1},N) \arrow[r] \arrow[u] & \operatorname{Hom}_R(P'_{i-1},N) \arrow[r] \arrow[u] & \operatorname{Hom}_R(P_{i-1},N) \arrow[r] \arrow[u] & 0 \\
 & \arrow[u] & \arrow[u] & \arrow[u] &
\end{tikzcd}$$

in which the rows are (split) exact, by the earlier remark. Now apply the snake lemma to conclude that there exists an exact sequence

$$\begin{tikzcd}
 & \cdots \arrow[r] & \mathrm{H}_{i-1}(\operatorname{Hom}_R(P_\bullet,N)) \arrow[dll, rounded corners] \\
\mathrm{H}_i(\operatorname{Hom}_R(P''_\bullet,N)) \arrow[r] & \mathrm{H}_i(\operatorname{Hom}_R(P'_\bullet,N)) \arrow[r] & \mathrm{H}_i(\operatorname{Hom}_R(P_\bullet,N)) \arrow[dll, rounded corners] \\
\mathrm{H}_{i+1}(\operatorname{Hom}_R(P''_\bullet,N)) \arrow[r] & \cdots &
\end{tikzcd}$$

We note that $\mathrm{H}_0(\operatorname{Hom}_R(P_\bullet,N)) \simeq \operatorname{Hom}_R(M_1,N)$, and similarly for M_2 and M_3. Hence this construction "repairs" the lack of surjectivity at the right end of the exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(M_3,N) \longrightarrow \operatorname{Hom}_R(M_2,N) \longrightarrow \operatorname{Hom}_R(M_1,N).$$

We write $\operatorname{Ext}^i_R(M_1,N) = \mathrm{H}_i(\operatorname{Hom}_R(P_\bullet,N))$, and similarly for M_2 and M_3. One has to check that this is independent of the choice of the choice of projective resolutions. We summarise this discussion by saying that projectives are *acyclic* for the functor $\operatorname{Hom}_R(-,N)$ and that the its *higher derived functors* can be defined using projective resolutions.

We now consider the functor $- \otimes_R N$. Let $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ be an exact sequence of R-modules. Apply $N \otimes_R -$. We now "repair" the lack of injectivity at the left end of the exact sequence

$$N \otimes_R M_1 \longrightarrow N \otimes_R M_2 \longrightarrow N \otimes_R M_3 \longrightarrow 0$$

in a way similar to the earlier situation. If M_3 is projective, then the sequence $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ is split, so

$$0 \longrightarrow N \otimes_R M_1 \longrightarrow N \otimes_R M_2 \longrightarrow N \otimes_R M_3 \longrightarrow 0$$

is a (split) exact sequence. By taking projective resolutions, applying the functor and taking homology, we get, using the snake lemma, an exact sequence

$$\cdots \longrightarrow \mathrm{H}_{i+1}(P''_\bullet \otimes_R N) \longrightarrow \mathrm{H}_i(P_\bullet \otimes_R N) \longrightarrow \mathrm{H}_i(P'_\bullet \otimes_R N) \longrightarrow \mathrm{H}_i(P''_\bullet \otimes_R N) \longrightarrow \mathrm{H}_{i-1}(P_\bullet \otimes_R N) \longrightarrow \cdots$$

Since $-\otimes_R N$ is right-exact, we see that $\mathrm{H}_0(P_\bullet \otimes_R N) \simeq M \otimes_R N$. Hence we have "repaired" the lack of injectivity at the left end of the exact sequence. We write $\mathrm{Tor}_i^R(M_1, N) = \mathrm{H}_i(P_\bullet \otimes_R N)$, and similarly for M_2 and M_3. One has to check that this is independent of the choice of the choice of projective resolutions. We summarise this discussion by saying that projectives are *acyclic* for the functor $(- \otimes_R N)$ and that the its higher derived functors can be defined using projective resolutions.

3.4. **Definition**. An R-module M is said to be *flat* if $M \otimes_R -$ is an exact functor.

Note that M is flat if and only if for every injective R-module map $N \longrightarrow N'$, the map $M \otimes_R N \longrightarrow M \otimes_R N'$ is injective. R is flat. For a family $M_\lambda, \lambda \in \Lambda$ of R-modules, $\oplus_{\lambda\in\Lambda} M_\lambda$ is flat if and only if M_λ is flat for every $\lambda \in \Lambda$. Hence projective modules are flat.

3.5. **Proposition**. *An R-module M is flat if and only if* $\mathrm{Tor}_1^R(M, -) = 0$.

Proof. Let

$$0 \longrightarrow N \longrightarrow N' \longrightarrow N'' \longrightarrow 0$$

be an exact sequence. Since $\mathrm{Tor}_1^R(M, N') = 0$, we see that

$$0 \longrightarrow M \otimes_R N \longrightarrow M \otimes_R N' \longrightarrow M \otimes_R N'' \longrightarrow 0$$

is exact. Conversely, let N be an R-module and $\alpha : P \longrightarrow N$ be a surjective R-module map with P a projective R-module. Then we have an exact sequence

$$\longrightarrow \mathrm{Tor}_1^R(M, P) \longrightarrow \mathrm{Tor}_1^R(M, N) \longrightarrow M \otimes_R (\ker \alpha) \longrightarrow M \otimes_R P \longrightarrow M \otimes_R N \longrightarrow 0$$

Now $\mathrm{Tor}_1^R(M, P) = 0$, since P is projective. By hypothesis the map $M \otimes_R (\ker \alpha) \longrightarrow M \otimes_R P$ is injective, so $\mathrm{Tor}_1^R(M, N) = 0$. □

4. Integral extensions

Let $R \subseteq S$ be an integral extension. Suppose that S is a field. Let $r \in R$. Let $s \in S$ be the inverse of r in S. We then have an equation

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0$$

with the r_i in R. Multiplying by r^{n-1}, we conclude that

$$s = s^n r^{n-1} = -(r_1 + \cdots + r_n r^{n-1}) \in R$$

so R is a field. Conversely suppose that R is a field and that S is a domain. Let $s \in S$. Consider an integral equation

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0$$

over R. Let n be the smallest such integer. Since S is a domain, $r_n \neq 0$. Then

$$-\frac{1}{r_n}(s^{n-1} + r_1 s^{n-2} + \cdots + r_{n-1})$$

is the inverse of s. Hence S is field.

Let $R \longrightarrow S$ be a ring map and $\mathfrak{p} \in \operatorname{Spec} R$. A prime ideal $\mathfrak{q} \in \operatorname{Spec} S$ is said to *lie over* $\mathfrak{p}$ if $\mathfrak{q} \cap R = \mathfrak{p}$.

4.1. **Remark**. Let $\mathfrak{p}$ be a prime ideal of R. Write $\kappa(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Then $\mathfrak{p}$ corresponds to the point $\operatorname{Spec} \kappa(\mathfrak{p}) \longrightarrow \operatorname{Spec} R$. The fibre over $\mathfrak{p}$ is $\operatorname{Spec}(\kappa(\mathfrak{p}) \otimes_R S)$. Let $\mathfrak{q}$ be a prime ideal of S. Suppose that $\mathfrak{q}$ lies over $\mathfrak{p}$. Then $\mathfrak{p}S \subseteq \mathfrak{q}$ and $\mathfrak{q}$ is disjoint from the image of $R \smallsetminus \mathfrak{p}$ inside S; in other words, $\mathfrak{q}(\kappa(\mathfrak{p}) \otimes_R S)$ is a prime ideal of $\kappa(\mathfrak{p}) \otimes_R S$. Conversely, if $\mathfrak{q}(\kappa(\mathfrak{p}) \otimes_R S)$ is a prime ideal of $\kappa(\mathfrak{p}) \otimes_R S$, then $\mathfrak{p}S \subseteq \mathfrak{q}$, so $\mathfrak{p} \subseteq \mathfrak{q} \cup R$ and $\mathfrak{q}$ is disjoint from the image of $R \smallsetminus \mathfrak{p}$ inside S, so $\mathfrak{p} \supseteq \mathfrak{q} \cup R$, so $\mathfrak{q}$ lies over $\mathfrak{p}$.

Now let $R \subseteq S$ be any integral extension. Let $\mathfrak{p}$ be a maximal ideal of $\operatorname{Spec} R$ and $\mathfrak{q} \in \operatorname{Spec} S$ lie over $\mathfrak{p}$. Then the extension $R/\mathfrak{p} \longrightarrow S/\mathfrak{q}$ is integral, so by the earlier observation $\mathfrak{q}$ is a maximal ideal of S. Conversely if $\mathfrak{p}$ is a prime ideal that is not maximal, then $\mathfrak{q}$ is not maximal. Note that $R_\mathfrak{p} \longrightarrow (R \smallsetminus \mathfrak{p})^{-1}S$ is integral. Applying the above observation to this extension, we see that there cannot be any containment relation between two S-ideal $\mathfrak{q}, \mathfrak{q}'$ lying over $\mathfrak{p}$. The same argument shows that every maximal ideal of $(R \smallsetminus \mathfrak{p})^{-1}S$ lies over $\mathfrak{p}$. In other words, the map $\operatorname{Spec} S \longrightarrow \operatorname{Spec} R$ is surjective.

4.2. **Theorem** (Going-up). *Let $R \subseteq S$ be an integral extension and $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ be prime ideals of R. Let $\mathfrak{q}_1$ be a prime ideal of S lying over $\mathfrak{p}_1$. Then there exists a prime ideal $\mathfrak{q}_2$ of S lying over $\mathfrak{p}_2$.*

Proof. $R/\mathfrak{p}_1 \subseteq S/\mathfrak{q}_1$ is an integral extension. There exists a prime ideal of $S/\mathfrak{q}_1$ lying over $\mathfrak{p}_2/\mathfrak{p}_1$; lift it to get $\mathfrak{q}_1$. □

4.3. **Corollary**. *Let $R \subseteq S$ be an integral extension. Then $\dim R = \dim S$. For any S-ideal J, $\operatorname{ht} J \leq \operatorname{ht}(J \cap R)$.*

Proof. For any chain of prime ideals $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \cdots$ of S, the prime ideals $\mathfrak{q}_1 \cap R \subsetneq \mathfrak{q}_2 \cap R \subsetneq \cdots$ of R are distinct, so $\dim S \leq \dim R$. The goind-up theorem implies that $\dim S \geq \dim R$. Suppose first that J is a prime ideal. Choose a chain $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \cdots \subseteq J$ and apply the above argument. For general J, note that $\operatorname{ht} J = \inf_{\mathfrak{q} \supseteq J} \operatorname{ht} \mathfrak{q}$. □

4.4. **Theorem** (Going-down). *Let $R \subseteq S$ be an integral extension, with R a normal domain, and S a domain. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ be prime ideals of R. Let $\mathfrak{q}_2$ be a prime ideal of S lying over $\mathfrak{p}_2$. Then there exists a prime ideal $\mathfrak{q}_1$ of S that lies over $\mathfrak{p}_1$.*

4.5. **Lemma**. *Let R be a normal domain and K its field of fractions. Let L be a normal extension of K and $G = \operatorname{Aut}_K(L)$. Let S be the integral closure of R in L. Then for all $\mathfrak{p} \in \operatorname{Spec} R$, G acts transitively on the set of prime ideals of S lying over $\mathfrak{p}$.*

Proof. We will prove this for *finite* G; see [Ser00, III.A, §3] or [Mat89, Theorem 9.3] for the general case. Let $\mathfrak{p} \in \operatorname{Spec} R$. Let $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of S lying over $\mathfrak{p}$. Note that for every $g \in G$, $g\mathfrak{q}$ is a prime ideal of S, lying over $\mathfrak{p}$. We want to show that there exists $g \in G$ such that $g\mathfrak{q} = \mathfrak{q}'$. By remarks above, it suffices to show that there exists $g \in G$ such that $\mathfrak{q}' \subseteq g\mathfrak{q}$. By the prime avoidance lemma, it suffices to show that $\mathfrak{q}' \subseteq \cup_{g \in G} g\mathfrak{q}$. Let $x \in \mathfrak{q}'$. Then $y := \prod_{g \in G} gx \in L$ and is fixed by G. Since L/K is normal, L^G/K is a purely inseparable extension; so there exists $q \in \mathbb{N}$ such that $y^q \in K$. Hence $y^q \in K \cap S = R$ (since R is integrally closed). Moreover $y^q \in \mathfrak{q}' \cap R = \mathfrak{p} \subseteq \mathfrak{q}$. Therefore there exists $g \in G$ such that $gx \in \mathfrak{q}$, so $x \in g^{-1}\mathfrak{q}$. □

Proof of the going-down theorem. Let K and L, respectively, be the fraction fields of R and S. L is an algebraic extension of K. Let L' be a normal extension of K containing L and let S' be the integral closure of R in L'. Let $\mathfrak{q}_2'$ be a prime ideal of S' lying over $\mathfrak{q}_2$. Let $\mathfrak{q}_1'$ be a prime ideal of S' lying over $\mathfrak{p}_1$. By the going-up theorem, there exists a prime S'-ideal $\mathfrak{q}_2''$ lying over $\mathfrak{p}_2$ and containing $\mathfrak{q}_1'$. Let $G = \operatorname{Aut}_K(L')$. There exists $g \in G$ such that $g\mathfrak{q}_2'' = \mathfrak{q}_2'$. Then $g\mathfrak{q}_1' \subseteq \mathfrak{q}_2'$ and $g\mathfrak{q}_1' \cap R = \mathfrak{p}_1$. Define $\mathfrak{q}_1 = g\mathfrak{q}_1' \cap S$. □

5. Normal domains

A *normal domain* is a noetherian domain that is integrally closed in its field of fractions.

5.1. **Proposition** ([Ser00, Chapter III, Part C, §1]). *Let R be a noetherian domain. Then R is normal if and only if the following two conditions are satisfied:*

(1) For every prime R-ideal $\mathfrak{p}$ of height 1, $R_\mathfrak{p}$ is a DVR.
(2) For every $r \neq 0 \in R$ and for every $\mathfrak{p} \in \operatorname{Ass} R/(r)$, $\operatorname{ht} \mathfrak{p} = 1$.

In many applications, we would like the following to be true: Let R be a noetherian domain with field of fractions K. Let L/K be an extension of fields, and S the integral closure of R in L; then the map $R \longrightarrow S$ is of finite-type (equivalently, since S is integral over R, finite, i.e., S is a finitely generated R-module). However, this is not true in general; we look at two situations where this holds for *normal* R.

5.2. **Proposition.** *Let R be a normal domain with field of fractions K. Let L be a finite separable field extension of K. Then the integral closure of R in L is a finitely generated R-module.*

For a proof see [Ser00, Chapter III, Part C, §3], [Eis95, Proposition 13.14] or [HS06, Theorem 3.1.3].

5.3. **Proposition.** *Let $\Bbbk$ be a field, R a domain that is finitely generated as a $\Bbbk$-algebra, K its field of fractions, and L a finite extension field of K. Then the integral closure of R in L is a finitely generated R-module.*

(See [Ser00, Chapter III, Part D §4] or [Eis95, Corollary 13.13].)

Proof. Step 1: Let $A = \Bbbk[x_1, \dots, x_n]$ be a Noether normalization of R. We have

$$\begin{array}{ccc} S & \subseteq & L \\ | & & | \\ R & \subseteq & K \\ | & & | \\ A & \subseteq & \Bbbk(x_1, \dots, x_n) \end{array}$$

If S is finitely generated A-module, then it is a finitely generated R-module. Hence, replacing R by A we may assume that $R = \Bbbk[x_1, \dots, x_n]$ and $K = \Bbbk(x_1, \dots, x_n)$.

Step 2: Let L'/L be a extension so that $L'/\Bbbk$ is normal and finite. Let S' be the integral closure of S in L'; it is also the integral closure of R in L'. We have

$$\begin{array}{ccc} S' & \subseteq & L' \\ | & & | \\ S & \subseteq & L \\ | & & | \\ R & \subseteq & K \end{array}$$

If S' is a finite generated R-module, then so is S. Hence, without loss of generality, L/K is normal.

Step 3: Let $G = \mathrm{Aut}_K(L)$. Then L^G/K is a purely inseparable extension. Let S_1 be the integral closure of R in L^G. We have

$$\begin{array}{ccc} S & \subseteq & L \\ | & & | \\ S_1 & \subseteq & L^G \\ | & & | \\ R & \subseteq & K \end{array}$$

L/L^G is Galois, so it is separable; note that S is the integral closure of S' in L. By the earlier proposition S is a finitely generated S'-module. Hence, if S' is a finitely generated R-module, S is a finitely generated R-module. Therefore replacing L by L^G, we may assume that L/K is purely inseparable.

Step 4: Let $y_1, \ldots, y_m \in L$ be a generating set for L as a K-algebra. There exists power q of the characteristic exponent of $\Bbbk$ such that $y_i^q \in K$ for every $1 \leq i \leq m$. Hence for each $1 \leq i \leq m$, y_i^q is a rational function in $\Bbbk(x_1, \ldots, x_n)$. Let $c_1, \ldots, c_r \in \Bbbk$ be the set of coeffecients of these rational functions. Let $\Bbbk' = \Bbbk(c_1^{\frac{1}{q}}, \cdots c_m^{\frac{1}{q}})$. Then $y_i \in \Bbbk'(x_1^{\frac{1}{q}}, \cdots x_n^{\frac{1}{q}})$ for each i, so $L \subseteq \Bbbk'(x_1^{\frac{1}{q}}, \cdots x_n^{\frac{1}{q}})$. Let S_2 be integral closure of R in $\Bbbk'(x_1^{\frac{1}{q}}, \cdots x_n^{\frac{1}{q}})$. Thus we have

$$\begin{array}{ccccccc} & & S_2 & \subseteq & \Bbbk'(x_1^{\frac{1}{q}}, \cdots x_n^{\frac{1}{q}}) & & \\ & & | & & | & & \\ & & S & \subseteq & L & & \\ & & | & & | & & \\ \Bbbk[x_1, \ldots, x_n] & = & R & \subseteq & K & = & \Bbbk(x_1, \ldots, x_n) \end{array}$$

If S_2 is a finitely generated R-module, then so is S; hence, without loss of generality, $L = \Bbbk'(x_1^{\frac{1}{q}}, \cdots x_n^{\frac{1}{q}})$.

Step 5: Let $f \in L$ be integral over R. Then $f^q \in K$ is integral over R, so $f^q \in R$. Hence $f \in \Bbbk'[x_1^{\frac{1}{q}}, \cdots x_n^{\frac{1}{q}}]$. Conversely, every element of $\Bbbk'[x_1^{\frac{1}{q}}, \cdots x_n^{\frac{1}{q}}]$ is integral over R. Hence $S = \Bbbk'[x_1^{\frac{1}{q}}, \cdots x_n^{\frac{1}{q}}]$ which is a finitely generated (free) R-module. □

6. Derivations, Kahler differentials

Primary references for this section are [Mat89, § 25], [Kun86, § 1] and [Eis95, Chapter 16].

6.1. **Definition**. Let $\Bbbk$ be a ring, R a $\Bbbk$-algebra and M an R-module. A *$\Bbbk$-derivation of R in M* (or a *derivation of R in M over* $\Bbbk$) is a $\Bbbk$-linear map $\mathrm{d} : R \longrightarrow M$ such that $\mathrm{d}(ab) = a\mathrm{d}(b) + b\mathrm{d}(a)$. When $\Bbbk = \mathbb{Z}$, we refer to such maps as *derivations of R in M*. We write $\mathrm{Der}_{\Bbbk}(R, M)$ for the set of $\Bbbk$-derivations of R in M and denote $\mathrm{Der}_{\mathbb{Z}}(R, M)$ by $\mathrm{Der}(R, M)$. When $M = R$, we write $\mathrm{Der}_{\Bbbk}(R)$ and $\mathrm{Der}(R)$.

6.2. **Example**. Let $U \subseteq \mathbb{R}^n$ be an open subset and R the ring of C^∞-functions on U. The partial differential operators

$$\frac{\partial}{\partial x_i} : R \longrightarrow R$$

are $\mathbb{R}$-derivations of R.

6.3. **Example**. Let $U \subseteq \mathbb{R}^n$ be an open subset and R the ring of C^∞-functions on U. Fix $x \in U$. Let $\mathfrak{m}_x = \{f \in R \mid f(x) = 0\}$. It is a maximal ideal of R and $R/\mathfrak{m}_x \simeq \mathbb{R}$. Through this, we can think of $\mathbb{R}$ as an R-module. The maps

$$\mathrm{d}_i : R \longrightarrow \mathbb{R}, f \mapsto \frac{\partial f}{\partial x_i}(x)$$

are $\mathbb{R}$-derivations of R in $\mathbb{R}$.

6.4. **Example**. Let $R = \Bbbk[x_1, \dots, x_n]$ a polynomial ring over $\Bbbk$ in n variables. We can define derivatives formally by setting

$$\frac{\partial}{\partial x_i}(x_1^{e_1} \cdots x_n^{e_n}) = e_i x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_n^{e_n},$$

and extending it $\Bbbk$-linearly to R. Let $M = \oplus_{i=1}^n R\mathrm{d}x_i$, where $\mathrm{d}x_1, \dots, \mathrm{d}x_n$ are symbols. The map

$$\mathrm{d} : R \longrightarrow M, f \mapsto (\frac{\partial f}{\partial x_i})\mathrm{d}x_i$$

is a $\Bbbk$-derivation of R in M. This is a formal way of defining differentials of (polynomial) functions. Similar arguments can be carried over to $\Bbbk[[x_1, \dots, x_n]]$ also.

6.5. **Example**. Consider the map $\mu : R \otimes_{\Bbbk} R \longrightarrow R$ from (2.4). Write $I = \ker \mu$. For every $a \in R$, $a \otimes 1 - 1 \otimes a \in I$. One can show that I is the $(R \otimes_{\Bbbk} R)$-ideal generated by $\{a \otimes 1 - 1 \otimes a \mid a \in R\}$. On $R \otimes_{\Bbbk} R$, there are two R-module structures (from the ring maps $a \mapsto a \otimes 1$ and $a \mapsto 1 \otimes a$), and so on I. However, on I/I^2, these structures agree, since

$$(r \otimes 1 - 1 \otimes r)(a \otimes 1 - 1 \otimes a) \in I^2.$$

We can define a $\Bbbk$-derivation $\delta : R \longrightarrow I/I^2, a \mapsto (a \otimes 1 - 1 \otimes a) \mod I^2$.

6.6. **Example**. Let F be the free R-module generated by the set $\{\mathrm{d}r \mid r \in R\}$ and N the R-submodule generated by

$$\{\mathrm{d}(rr') - r\mathrm{d}r' - r'\mathrm{d}r \mid r, r' \in R\} \cup \{\mathrm{d}(ar + a'r') - a\mathrm{d}r - a'\mathrm{d}r' \mid r, r' \in R, a, a' \in \Bbbk\}.$$

Let $M = F/N$. The map $\mathrm{d} : R \longrightarrow M$, $r \mapsto \mathrm{d}r$ is a $\Bbbk$-derivation of R in M. The pair (M, d) has the following universal property: For every R-module M' and every $\mathrm{d}' \in \mathrm{Der}_{\Bbbk}(R, M')$, there exists a unique R-linear map $f : M \longrightarrow M'$ such that $\mathrm{d}' = f\mathrm{d}$. Indeed, there exists a unique R-linear map $\tilde{f} : F \longrightarrow M'$, $\mathrm{d}r \mapsto \mathrm{d}'r$. Since d' is a $\Bbbk$-derivation, $N \subseteq \ker \tilde{f}$. Thus we get the unique R-linear map $f : M \longrightarrow M'$ such that $\mathrm{d}' = f\mathrm{d}$.

6.7. **Definition**. The module M in Example 6.6 is called the *module of Kähler differentials of R over $\Bbbk$* and is denoted $\Omega_{R/\Bbbk}$. The map $\mathrm{d} : R \longrightarrow \Omega_{R/\Bbbk}$ is called the *universal $\Bbbk$-derivation of R*.

6.8. **Remark**. Let F and N be as in Example 6.6. Let N' be the R-submodule of R generated by

$$\{\mathrm{d}(rr') - r\mathrm{d}r' - r'\mathrm{d}r \mid r, r' \in R\} \cup \{\mathrm{d}(r + r') - \mathrm{d}r - \mathrm{d}r' \mid r, r' \in R\} \cup \{\mathrm{d}a \mid a \in \Bbbk\}.$$

Note that, for every $a \in \Bbbk$, $\mathrm{d}a = \mathrm{d}(a \cdot 1 + 0 \cdot 0) - a\mathrm{d}1 - 0\mathrm{d}0 \in N$, so $N' \subseteq N$. Conversely, let $a, a' \in \Bbbk$ and $r, r' \in R$. Then $\mathrm{d}(ar + a'r') - \mathrm{d}(ar) - \mathrm{d}(a'r') \in N'$ and $\mathrm{d}(ar) - a\mathrm{d}r = \mathrm{d}(ar) - a\mathrm{d}r - r\mathrm{d}a + r\mathrm{d}a \in N'$; hence $\mathrm{d}(ar + a'r') - a\mathrm{d}r - a'\mathrm{d}r' = \mathrm{d}(ar + a'r') - \mathrm{d}(ar) - \mathrm{d}(a'r') + \mathrm{d}(ar) + \mathrm{d}(a'r') - a\mathrm{d}r - a'\mathrm{d}r' \in N'$. Therefore $N = N'$.

The map $M \longrightarrow \operatorname{Der}_\Bbbk(R, M)$ is a covariant left-exact functor from R-modules to R-modules. We have established that $\operatorname{Der}_\Bbbk(R, -) = \operatorname{Hom}_R(\Omega_{R/\Bbbk}, -)$. (One says that $\Omega_{R/\Bbbk}$ *represents* the functor $\operatorname{Der}_\Bbbk(R, -)$.)

6.9. **Proposition**. *Let $I = \ker(\mu : R \otimes_\Bbbk R \longrightarrow R)$ and $\delta : R \longrightarrow I/I^2, r \mapsto (r \otimes 1 - 1 \otimes r) \bmod I^2$. Then for every R-module M and every $e \in \operatorname{Der}_\Bbbk(R, M)$, there is a unique R-linear map $\tilde{e} : I/I^2 \longrightarrow M$ such that $e = \tilde{e}\delta$. In particular, there is a unique isomorphism $\phi : \Omega_{R/\Bbbk} \longrightarrow I/I^2$ such that such that the diagram*

$$\begin{tikzcd}
 & M & \\
 & R \arrow[u, "e"] \arrow[dl, "\mathrm{d}"'] \arrow[dr, "\delta"] & \\
\Omega_{R/\Bbbk} \arrow[uur, "e'"] \arrow[rr, "\phi"] & & I/I^2 \arrow[uul, "\tilde{e}"']
\end{tikzcd}$$

commutes (where e' is the unique R-linear map $\Omega_{R/\Bbbk} \longrightarrow M$).

Proof. For now, assume the assertion about the existence of the unique map $\tilde{e}$. Applying it to the derivation $\mathrm{d} : R \longrightarrow \Omega_{R/\Bbbk}$, we get a unique R-linear map $\psi : I/I^2 \longrightarrow \Omega_{R/\Bbbk}$ such that $\mathrm{d} = \psi\delta$. On the other hand, from the universal property of the pair $(\Omega_{R/\Bbbk}, \mathrm{d})$, we get a map $\phi : \Omega_{R/\Bbbk} \longrightarrow I/I^2$ such that $\phi\mathrm{d} = \delta$. Hence $\psi\phi\mathrm{d} = \mathrm{d}$ and $\phi\psi\delta = \delta$. Since $\Omega_{R/\Bbbk}$ is generated by $\{\mathrm{d}r \mid r \in R\}$, we see that $\psi\phi = \mathrm{id}_{\Omega_{R/\Bbbk}}$. Similarly, since I/I^2 is generated by $\{\delta r \mid r \in R\}$, we see that $\phi\psi = \mathrm{id}_{I/I^2}$. This proves the existence of the unique isomorphism ϕ.

Continuing with our assumption of the existence of $\tilde{e}$, we need to show that $e' = \tilde{e}\phi$. It suffices to show that $e'\mathrm{d}r = \tilde{e}\phi\mathrm{d}r$ for every $r \in R$. This indeed is true: $e'\mathrm{d}r = er = \tilde{e}\delta r = \tilde{e}\phi\mathrm{d}r$.

Now to prove the existence of $\tilde{e}$. Let N be an R-module Let $R \ltimes N$ be the R-module $R \oplus N$ with multiplication $(r, x)(r', x') := (rr, rx' + r'x)$. There are two natural $\Bbbk$-algebra maps: $i : R \longrightarrow R \ltimes N, r \mapsto (r, 0)$ which is injective and $\pi : R \ltimes N \longrightarrow R, (r, x) \mapsto r$, which is surjective. Now let $f \in \operatorname{Der}_\Bbbk(R, N)$. The map $\hat{f} : R \longrightarrow R \ltimes N$, $r \mapsto (r, f(r))$ is a map of $\Bbbk$-algebras.

Let $\hat{e} : R \longrightarrow R \ltimes M$ be the $\Bbbk$-algebra map associated to e. The universal property of $R \otimes_{\Bbbk} R$ gives a morphism

$$h : R \otimes_{\Bbbk} R \longrightarrow R \ltimes M, r \otimes r' \mapsto \hat{e}(r)i(r') = (r, er)(r', 0) = (rr', r'er).$$

Note that $h(r \otimes 1 - 1 \otimes r) = (0, er)$, so $h(I^2) = 0$. Hence $\hat{e}$ induces an R-linear mapping $\tilde{e} : I/I^2 \longrightarrow M, \tilde{e}(r \otimes 1 - 1 \otimes r) = er$. This is unique since I is generated by $\{r \otimes 1 - 1 \otimes r \mid r \in R\}$. □

For the next two results, we follow the proof in [Eis95, Chapter 16].

6.10. **Theorem** (First fundamental exact sequence). *Let $\Bbbk \longrightarrow R \longrightarrow S$ be ring maps. Then there exists an exact sequence*

$$S \otimes_R \Omega_{R/\Bbbk} \longrightarrow \Omega_{S/\Bbbk} \longrightarrow \Omega_{S/R} \longrightarrow 0$$

of S-modules, where the maps are given by $s \otimes \mathrm{d}_{R/\Bbbk}r \mapsto s\mathrm{d}_{S/\Bbbk}r$ (thinking of r as its image in S) and $\mathrm{d}_{S/\Bbbk}s \mapsto \mathrm{d}_{S/R}s$.

Proof. It follows from Remark 6.8 that the map

$$\Omega_{S/\Bbbk} \longrightarrow \Omega_{S/R}, \quad \mathrm{d}_{S/\Bbbk}s \mapsto \mathrm{d}_{S/R}s$$

is surjective and that its kernel is generated by $\{\mathrm{d}_{S/\Bbbk}r \mid r \in R\}$. This is precisely the image of the map

$$S \otimes_R \Omega_{R/\Bbbk} \longrightarrow \Omega_{S/\Bbbk} \quad s \otimes \mathrm{d}_{R/\Bbbk}r \mapsto s\mathrm{d}_{S/\Bbbk}r.$$ □

6.11. **Theorem** (Second fundamental exact sequence). *Let R be a $\Bbbk$-algebra and I an ideal of R. Write $S = R/I$. Then there exists an exact sequence*

$$I/I^2 \longrightarrow S \otimes_R \Omega_{R/\Bbbk} \longrightarrow \Omega_{S/\Bbbk} \longrightarrow 0$$

of S-modules, where the maps are $r \mod I^2 \mapsto 1 \otimes_R \mathrm{d}_{R/\Bbbk}r$ and $s \otimes \mathrm{d}_{R/\Bbbk}r \mapsto s\mathrm{d}_{S/\Bbbk}r$ (thinking of r as its image in S).

The map $S \otimes_R \Omega_{R/\Bbbk} \longrightarrow \Omega_{S/\Bbbk}$ is the same from the first fundamental exact sequence. It is surjective, since $\Omega_{S/R} = 0$ as $S \otimes_R S \longrightarrow S$ is an isomorphism. The content of this theorem is that its kernel is given by I/I^2.

Proof. The map $S \otimes_R \Omega_{R/\Bbbk} \longrightarrow \Omega_{S/\Bbbk}$, $s \otimes \mathrm{d}_{R/\Bbbk}r \mapsto s\mathrm{d}_{S/\Bbbk}r$ is the same as the map

$$\frac{\Omega_{R/\Bbbk}}{I\Omega_{R/\Bbbk}} \longrightarrow \Omega_{S/\Bbbk},$$

which is induced from the map $\Omega_{R/\Bbbk} \longrightarrow \Omega_{S/\Bbbk}$, $\mathrm{d}_{R/\Bbbk}r \mapsto \mathrm{d}_{S/\Bbbk}r$. Consider the map

$$\bigoplus_{r \in R} R\mathrm{d}_{R/\Bbbk}r \longrightarrow \bigoplus_{\bar{r} \in S} S\mathrm{d}_{S/\Bbbk}\bar{r}, \quad \mathrm{d}_{R/\Bbbk}r \mapsto \mathrm{d}_{S/\Bbbk}\bar{r}$$

where by $\bar{r}$, we mean the image of r in S. The kernel of this map is

$$\left(\bigoplus_{r \in R} I\mathrm{d}_{R/\Bbbk}r\right) + R\{\mathrm{d}_{R/\Bbbk}r \mid r \in I\}.$$

Hence, the kernel of the map $\Omega_{R/\Bbbk} \longrightarrow \Omega_{S/\Bbbk}$, $\mathrm{d}_{R/\Bbbk}r \mapsto \mathrm{d}_{S/\Bbbk}r$ is $I\Omega_{R/\Bbbk} + R\{\mathrm{d}_{R/\Bbbk}r \mid r \in I\}$. This shows that the kernel of $S \otimes_R \Omega_{R/\Bbbk} \longrightarrow \Omega_{S/\Bbbk}$, $s \otimes \mathrm{d}_{R/\Bbbk}r \mapsto s\mathrm{d}_{S/\Bbbk}r$ is generated by $\{1 \otimes \mathrm{d}_{R/\Bbbk}r \mid r \in I\}$. Hence it suffices to justify why the map

$$I/I^2 \longrightarrow S \otimes_R \Omega_{R/\Bbbk}, \quad r \mod I^2 \mapsto 1 \otimes_R \mathrm{d}_{R/\Bbbk}r$$

is S-linear. Let $a \in R$ and $r \in I$. Then $1 \otimes a\mathrm{d}_{R/\Bbbk}r + 1 \otimes r\mathrm{d}_{R/\Bbbk}a = a(1 \otimes \mathrm{d}_{R/\Bbbk}r) + 0 \otimes \mathrm{d}_{R/\Bbbk}a$, so $a(r \mod I^2) \mapsto a(1 \otimes \mathrm{d}_{R/\Bbbk}r)$. □

6.12. **Example**. Let $R = \Bbbk[x_1, \ldots, x_n]$ be a polynomial ring in the variables $x_1, \ldots, x_n$ and $I \subseteq R$ an R-ideal, generated by $\{f_1, \ldots, f_m\}$. Write $S = R/I$. Then $S \otimes_R \Omega_{R/\Bbbk} = \oplus_{i=1}^n S\mathrm{d}x_i$ is a free S-module of rank n. The image of $I/I^2 \longrightarrow S \otimes_R \Omega_{R/\Bbbk}$ is the submodule $\{1 \otimes \sum_{i=1}^n \frac{\partial f}{\partial x_i}\mathrm{d}x_i \mid f \in I\}$. which is generated (as an S-module) by $\{1 \otimes \sum_{i=1}^n \frac{\partial f_j}{\partial x_i}\mathrm{d}x_i \mid 1 \leq j \leq m\}$. Let

$$J := \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_2}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_1} \\ \frac{\partial f_1}{\partial x_2} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_m}{\partial x_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial x_n} & \frac{\partial f_2}{\partial x_n} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}$$

be the *jacobian matrix* of $f_1, \ldots, f_m$ with respect to $x_1, \ldots, x_n$. Let $\oplus_{j=1}^m S\xi_j$ be a free module with basis $\xi_1, \ldots, \xi_m$ and let $\oplus_{j=1}^m S\xi_j \longrightarrow I/I^2$ be the surjective map with $\xi_j \mapsto f_i \mod I^2$. Thinking of J as a matrix over S, we have the following diagram:

$$\begin{tikzcd} \bigoplus_{j=1}^m S\xi_j \arrow[d] \arrow[dr, "J"] & & & \\ I/I^2 \arrow[r] & \oplus_{i=1}^n S\mathrm{d}x_i \arrow[r] & \Omega_{S/\Bbbk} \arrow[r] & 0 \end{tikzcd}$$

in which the horizontal part is exact and the triangle commutes.

6.13. **Proposition**. *Let $\Bbbk$ be a field and $L/\Bbbk$ an algebraic field extension. Let $K \subseteq L$ be the subfield of elements that are seperable over $\Bbbk$. Then for all L-modules M and for all $\Bbbk$-derivations $\mathrm{d} : L \longrightarrow M$, $K \subseteq \ker \mathrm{d}$. In particular if $L/\Bbbk$ is seperable, then every $\Bbbk$-derivation of L is trivial.*

Proof. Let $a \in K$. Let $x^n + a_1x^{n-1} + \cdots + a_n \in \Bbbk[x]$ be the minimal polynomial of a over $\Bbbk$. Then

$$0 = \mathrm{d}(0) = (na^n + (n-1)a_1a^{n-2} + \cdots + a_{n-1})\mathrm{d}a = f'(a)\mathrm{d}a.$$

Since a is seperable over $\Bbbk$, $f'(a) \neq 0$, so $\mathrm{d}a = 0$. □

6.14. **Corollary**. *With notation as in Proposition 6.13, $\Omega_{K/\Bbbk} = 0$ and $\Omega_{L/\Bbbk} = \Omega_{L/K}$.*

Proof. It follows immediately from Proposition 6.13 that $\Omega_{K/\Bbbk} = 0$. The other assertion follows from the first fundamental exact sequence (Theorem 6.10). □

7. Auslander-Buchsbaum paper, §2

In this section, R is an $\Bbbk$-algebra, and we will denote by R^e the $\Bbbk$-algebra $R \otimes_\Bbbk R$ with the structure map $a \mapsto a \otimes 1$. Write μ for the $\Bbbk$-algebra map $R^e \longrightarrow R, r \otimes r' \mapsto rr'$, I for $\ker \mu$ and $\mathfrak{a} = \mathrm{Ann}_{R^e}(I)$.

For a prime ideal $\mathfrak{p}$ of a ring $\Bbbk$, we denote $\Bbbk_\mathfrak{p}/\mathfrak{p}\Bbbk_\mathfrak{p}$ by $\kappa(\mathfrak{p})$.

7.1. **Definition**. Let $\Bbbk$ be a field. Then R is said to be *separable* if it is a finite-dimensional $\Bbbk$-algebra that is a product of separable field extensions of $\Bbbk$.

7.2. **Definition**. A prime ideal $\mathfrak{q}$ of R is *unramified* if, with $\mathfrak{p} = \mathfrak{q} \cap \Bbbk$, $\mathfrak{p}S_\mathfrak{q} = \mathfrak{q}S_\mathfrak{q}$ and $\kappa(\mathfrak{q})$ is a (finite) seperable field extension of $\kappa(\mathfrak{p})$. We say that the map $\Bbbk \longrightarrow R$ is *unramified* (or $R/\Bbbk$ is *unramified*, or, merely, R is *unramified*, if no confusion is likely to occur) if every prime ideal of R is unramified and over every prime $\Bbbk$-ideal, only finitely many prime R-ideals lie over.

The goal of this section is to understand the proof of the following theorem.

7.3. **Theorem** ([AB59, Theorem 2.5]). *Suppose that R is a noetherian ring and that I is a finitely generated ideal of R^e. Then the following are equivalent:*
(1) R is a projective R^e-module;
(2) the map $\Bbbk \longrightarrow R$ is unramified;
(3) every maximal ideal of R is unramified;
(4) $\mathrm{Der}_\Bbbk(R, M) = 0$ for every finitely generated R-module M.

7.4. **Example**. Suppose $R/\Bbbk$ is an algebraic extension of fields. Then for the statements in Theorem 7.3(2) and (3) to hold, it is necessary and sufficient that $R/\Bbbk$ is a separable extension. By Proposition 6.13, the statement of Theorem 7.3(4) holds. Conversely, suppose that $\mathrm{Der}_\Bbbk(R, N) = 0$ for every finitely generated R-module M. Since $\Omega_{R/\Bbbk}$ is a free R-module, this means that $\Omega_{R/\Bbbk} = 0$. We want to conclude that $R/\Bbbk$ is separable. We will do this assuming that $R/\Bbbk$ is a *finite* extension, although it is not necessary to make this restriction. By way of contradiction, assume that $R/\Bbbk$ is not separable. Then $\mathrm{char}\, \Bbbk = p > 0$. Enlarging $\Bbbk$ by adjoining the elements of R that are separable over $\Bbbk$, we may assume that $R/\Bbbk$ is purely inseparable and that $R \neq \Bbbk$. Adjoining $\{r^p \mid r \in R\}$, we may assume that $R^p \subseteq \Bbbk$ and that $R \neq \Bbbk$. By induction $\mathrm{rk}_\Bbbk R$, we may assume that $R = \Bbbk[x]/(x^p - r)$ for some $r \in \Bbbk$. Then

$$\Omega_{R/\Bbbk} \simeq (R \otimes_{\Bbbk[x]} \Omega_{\Bbbk[x]/\Bbbk})/R \cdot (\mathrm{d}(x^p - r)) = R \otimes_{\Bbbk[x]} \Omega_{\Bbbk[x]/\Bbbk} \neq 0.$$

To see the statement of Theorem 7.3(1), again assume that $R/\Bbbk$ is a finite separable extension. Write $R = \Bbbk(r)$ and $f(x) \in \Bbbk[x]$ for the minimal polynomial of r over $\Bbbk$. Note that $f(x) = (x - r)g(x) \in R[x]$ for some $g(x) \in R[x]$ such that $g(r) \neq 0$. Hence $(x - r, g(x))R[x] = R[x]$, so $R^e \simeq R[x]/f(x) \simeq R[x]/(x - r) \times R[x]/g(x)$. Therefore R is a direct summand of R^e as an R^e-module.

7.5. **Lemma**. *Then the following are equivalent:*
(1) R is a projective R^e-module;
(2) the exact sequence $0 \longrightarrow I \longrightarrow R^e \xrightarrow{\mu} R \longrightarrow 0$ splits;
(3) there exists an element $z \in R^e$ such that $z(x \otimes 1) = z(1 \otimes x)$ for every $x \in R$ and $\mu(z) = 1$.
(4) $\mu(\mathfrak{a}) = R$.

Proof. (1) $\iff$ (2): Immediate.

(2) $\implies$ (3): Let $f : R \longrightarrow R^e$ be an R^e-linear map splitting μ. Define $z := f(1)$. The R^e-linear structure of R is through μ, so $z(x\otimes 1) = f(1\cdot\mu(x\otimes 1)) = f(x) = f(1\cdot\mu(1\otimes x)) = z(1 \otimes x)$. Note that $\mu(z) = 1$.

(3) $\implies$ (4): $z \in \mathfrak{a}$ and $1 = \mu(z) \in \mu(\mathfrak{a})$.

(4) $\implies$ (2): Let $z \in \mathfrak{a}$ be such that $\mu(z) = 1$. Define $f : R \longrightarrow R^e$, $r \mapsto (r\otimes 1)z$. It is easy to see that f is additive. Let $r_1 \otimes r_2 \in R^e$. Then $f((r_1 \otimes r_2)r) = (r_1 s_2 s \otimes 1)z = (r_1 \otimes r_2)(r \otimes 1)z$ since $(r_1 s_2 s \otimes 1) - (r_1 \otimes r_2)(r \otimes 1) = (r_1 \otimes 1)(r \otimes 1)(r_2 \otimes 1 - 1 \otimes r_2) \in I$ and $zI = 0$. Hence f is an R^e-linear splitting of μ. ◻

7.6. **Lemma**. *Suppose that $\Bbbk$ is a field. Then R is a separable $\Bbbk$-algebra if and only if it is a finite-dimensional $\Bbbk$-algebra and for every extension L of $\Bbbk$, $L \otimes_\Bbbk R$ is semisimple.*

Proof. If: Since R is a finite-dimensional semisimple $\Bbbk$, we can write $R = \prod_{i=1}^n R_i$ for some positive integer n and finite extensions R_i of $\Bbbk$. We need to show that R_i is separable for each i. If R_j is not separable for some j, $R_j \otimes_{\Bbbk} R_j$ is not semisimple, so $R_j \otimes_{\Bbbk} R$, which contains $R_j \otimes_{\Bbbk} R_j$ as a factor, is not semisimple.

Only if: R is a finite-dimensional $\Bbbk$-algebra, by definition. Write $R = \prod_{i=1}^{n} R_i$ for some positive integer n and finite separable extensions R_i of $\Bbbk$. It suffices to show that $L \otimes_{\Bbbk} R_i$ is semisimple for every i, so we may assume that R is a finite separable field extension of $\Bbbk$. Write $R = \Bbbk[x]/(f(x))$ for a separable polynomial $f(x) \in \Bbbk[x]$. Since $f(x)$ factors as a product of separable polynomials in $L[x]$, none of which share any zero in any extension field of L, $L \otimes_{\Bbbk} R \simeq L[x]/(f(x))$ is a product of fields, and hence semisimple. □

7.7. **Lemma**. *If R is R^e-projective, then for every $\Bbbk$-algebra L, the L-algebra $(L \otimes_{\Bbbk} R)$ is $(L \otimes_{\Bbbk} R)^e$-projective.*

Proof. Write $R' = L \otimes_{\Bbbk} R$, Write μ' for the natural map $(R' \otimes_L R') \longrightarrow R'$ and ϕ for the map $R' \otimes_L R' \longrightarrow L \otimes_{\Bbbk} R^e, ((b_1 \otimes_{\Bbbk} r_1) \otimes_L (b_2 \otimes_{\Bbbk} r_2)) \mapsto (b_1 b_2 \otimes_{\Bbbk} (r_1 \otimes_{\Bbbk} r_2))$. Note that ϕ is an isomorphism and that $\mu' = (1 \otimes \mu) \circ \phi$. Let f be a splitting of μ. Then the map $\phi^{-1} \circ (1 \otimes f)$ is a splitting of μ'. Now apply Lemma 7.5. □

7.8. **Lemma**. *Suppose that $\Bbbk$ is a field and that R is a projective R^e-module. Then $\operatorname{rk}_{\Bbbk} R < \infty$.*

Proof. Let $\{r_i\}_{i \in \Lambda}$ be an $\Bbbk$-basis of R. Then $\{r_i \otimes r_j\}_{i,j \in \Lambda}$ is a basis of R^e. Let $z \in R^e$ be as in Lemma 7.5(3). Write $z = \sum_{ij} a_{ij} r_i \otimes r_j$. Let $r_i' := \sum_{j \in \Lambda} a_{ij} r_j$. Let $\Lambda_1 = \{i \in \Lambda \mid r_i' \neq 0\}$; it is a finite set. Note that $\sum_{i \in \Lambda_1} r_i r_i' = \mu(z) = 1$ and that for every $x \in R$, $\sum_{i \in \Lambda_1} r_i x \otimes r_i' = z(x \otimes 1) = z(1 \otimes x) = \sum_{i \in \Lambda_1} r_i \otimes r_i' x$. Let $R' := \sum_{i \in \Lambda_1} \Bbbk r_i' \subseteq R$.

Claim R' is an R-ideal. (To be proved.)

Hence $r_j r_i' \in R'$ for every $i \in \Lambda_1$ and $j \in \Lambda$. In particular $1 = \sum_{i \in \Lambda_1} r_i r_i' \in R'$, so $R' = R$. Hence R is a finitely generated $\Bbbk$-module. □

7.9. **Proposition**. *Suppose that $\Bbbk$ is a field. Then R is a projective R^e-module if and only if R is a separable $\Bbbk$-algebra.*

Proof. In view of Lemma 7.8 and the definition of separability, we may assume that $\operatorname{rk}_{\Bbbk} R < \infty$ before proving both the implications. Now suppose that R is R^e-projective. Then, by Lemma 7.7, $L \otimes_{\Bbbk} R$ is $(L \otimes_{\Bbbk} R)^e$-projective for every $\Bbbk$-algebra L. Hence by Corollary A.13, $(L \otimes_{\Bbbk} R)$ is semisimple. By Lemma 7.6, R is a separable $\Bbbk$-algebra.

Conversely assume that R is a separable $\Bbbk$-algebra. Assume, for now, that R is a finite separable field extension of $\Bbbk$. Write $R = \Bbbk[x]/(f(x))$, with $f(x)$ separable over $\Bbbk$, so $R^e \simeq S := \Bbbk[x,y]/(f(x), f(y))$. The map μ is $S \longrightarrow \Bbbk[x]/(f(x)), x \mapsto x, y \mapsto x$. Note that as an element of $\Bbbk[x,y]/(f(x))$, $f(y)$ splits as $(y-x)g(y)$, where, because of the separability of $f(y)$, $(y - x, g(y)) = \Bbbk[x,y]/(f(x))$. Hence there exist $e_1 \in g(y)S$ and $e_2 \in (y-x)S$ such that $e_1^2 = e_1, e_2^2 = e_2, e_1 e_2 = 0, e_1 + e_2 = 1$ and

$$Se_1 \simeq \Bbbk[x,y]/(f(x), y-x), \quad Se_2 \simeq \Bbbk[x,y]/(f(x), g(y)), \quad \text{and } S \simeq Se_1 \times Se_2$$

Note that $\mu(e_1) = 1$ and $\mu(e_2) = 0$. The S-linear map $R \longrightarrow S$, $1 \mapsto e_1$ is an S-linear splitting of μ.

Now suppose that $R = \prod_{i=1}^{t} R_i$ where the R_i are finite separable field extensions of $\Bbbk$. Write $R_i = Re_i$ for a set of orthogonal idempotents $e_1, \ldots, e_t$ (i.e., $\sum_{i=1}^{t} e_i = 1$; $e_i^2 = e_i$ for all i; $e_i e_j = 0$ for $i \neq j$). Then $\mu(e_i \otimes e_j) = e_i e_j = 0$. Hence

$$\mu\left(\left(\sum_{i=1}^{t} r_i e_i\right) \otimes \left(\sum_{j=1}^{t} r_j' e_j\right)\right) = \sum_{i=1}^{t} \mu\left(r_i e_i \otimes r_i' e_i\right)$$

Write $\mu_i = (R_i^e) \longrightarrow R_i$. There exist an (R_i^e)-linear splitting f_i of μ_i. Hence the map $\prod_{i=1}^t f_i$ is a R^e-linear splitting of μ. $\square$

7.10. **Lemma**. *If R is a projective R^e-module, then $R/\Bbbk$ is unramified.*

Proof. Note that $R/\Bbbk$ is unramified if and only if $R \otimes_{\Bbbk} \kappa(\mathfrak{p})$ is a separable $\kappa(\mathfrak{p})$-algebra for every $\mathfrak{p} \in \Bbbk$. Hence, by Proposition 7.9, it suffices to show that if R is R^e-projective, then $A := R \otimes_{\Bbbk} \kappa(\mathfrak{p})$ is a projective module over $A^e := (R \otimes_{\Bbbk} \kappa(\mathfrak{p})) \otimes_{\kappa(\mathfrak{p})} (R \otimes_{\Bbbk} \kappa(\mathfrak{p}))$. Write $\mu' : A^e \longrightarrow A$.

Let $f : R \longrightarrow R^e$ be an R^e-linear splitting of μ. Then the induced map is an A^e-linear splitting of μ'. $\square$

7.11. **Lemma**. *Assume that R is a noetherian ring, such that every maximal ideal of R is unramified. Then $\operatorname{Der}_{\Bbbk}(R, M) = 0$ for every finitely generated R-module M.*

Proof. Let $D \in \operatorname{Der}_{\Bbbk}(R, M)$. Let $\mathfrak{q}$ be a maximal ideal of R and $\mathfrak{p} = \mathfrak{q} \cap \Bbbk$. Write $D_{\mathfrak{q}}$ for the induced $\Bbbk_{\mathfrak{p}}$-derivation $R_{\mathfrak{q}} \longrightarrow M_{\mathfrak{q}}$.

Note that $\mathfrak{p}R_{\mathfrak{q}} = \mathfrak{q}R_{\mathfrak{q}}$. Note that $D_{\mathfrak{q}}(\mathfrak{p}R_{\mathfrak{q}}) \subseteq \mathfrak{p}M_{\mathfrak{q}} = \mathfrak{q}M_{\mathfrak{q}}$. Hence we get a $\kappa(\mathfrak{p})$-derivation $\overline{D_{\mathfrak{q}}} : R_{\mathfrak{q}}/\mathfrak{q}R_{\mathfrak{q}} \longrightarrow M_{\mathfrak{q}}/\mathfrak{q}M_{\mathfrak{q}}$, which is zero since $R_{\mathfrak{q}}/\mathfrak{q}R_{\mathfrak{q}}$ is a separable extension of $\kappa(\mathfrak{p})$. Hence $\operatorname{Im} D_{\mathfrak{q}} \subseteq \mathfrak{q}M_{\mathfrak{q}}$. Iterating we get $\operatorname{Im} D_{\mathfrak{q}} \subseteq \cap_i \mathfrak{q}_i M_{\mathfrak{q}} = 0$, so $D_{\mathfrak{q}} = 0$. Since this is true for every maximal ideal, $D = 0$. $\square$

Proof of Theorem 7.3. (1) $\Longrightarrow$ (2): Follows from Lemma 7.10. (2) $\Longrightarrow$ (3): immediate. (3) $\Longrightarrow$ (4): Follows from Lemma 7.11. (4) $\Longrightarrow$ (1): Since I/I^2 is a finitely generated R-module and $\operatorname{Der}_{\Bbbk}(R, -) = \operatorname{Hom}_R(I/I^2, -)$, we see that $\operatorname{Hom}_R(I/I^2, I/I^2) = 0$, so $I = I^2$. By the determinant trick (see, e.g., [Eis95, Corollary 4.8]) we see that there exists $r_0 \in I$ such that $rr_0 = r$ for every $r \in I$. Define $g : R^e \longrightarrow I, 1 \mapsto r_0$. For every $r \in I$, $g(r) = rg(1) = rr_0 = r$, so the inclusion $I \longrightarrow R^e$ is split. $\square$

7.12. **Definition**. The *Noether different* (*homological different* in [AB59]) $\mathscr{D}_N(R/\Bbbk)$ of $R/\Bbbk$ is the R-ideal $\mu(\mathfrak{a})$.

7.13. **Theorem**. *Suppose that R is a noetherian ring and that I is a finitely generated ideal of R^e. For every prime ideal $\mathfrak{q}$ of R, $\mathfrak{q}$ is unramified if and only if $\mathscr{D}_N(R/\Bbbk) \not\subset \mathfrak{q}$.*

7.14. **Lemma**. *With notation as in Theorem 7.13, let U be a multiplicatively closed set in $\Bbbk$ and V a multiplicatively closed set of R containing the image of U. Then*

$$V^{-1}\mathscr{D}_N(R/\Bbbk) = \mathscr{D}_N(V^{-1}R/\Bbbk) = \mathscr{D}_N(V^{-1}R/U^{-1}\Bbbk).$$

Proof. Write $I = \ker(R \otimes_{\Bbbk} R \longrightarrow R)$. Then

$$\begin{aligned}(V \otimes_{\Bbbk} V)^{-1} I &= \ker\left(V^{-1}R \otimes_{\Bbbk} V^{-1}R \longrightarrow V^{-1}R\right)\\ &= \ker\left(V^{-1}R \otimes_{U^{-1}\Bbbk} V^{-1}R \longrightarrow V^{-1}R\right).\end{aligned}$$

Since I is finitely generated, $\operatorname{Ann}_{(V^{-1}R \otimes_{\Bbbk} V^{-1}R)}((V \otimes_{\Bbbk} V)^{-1} I) = V^{-1}R \operatorname{Ann}_{R \otimes_{\Bbbk} R}(I)$. Hence the lemma follows. $\square$

Proof of Theorem 7.13. Every maximal ideal of $R_{\mathfrak{q}}$ is unramified over $\Bbbk$. By Theorem 7.3 and Lemma 7.5, $\mathscr{D}_N(R_{\mathfrak{q}}/\Bbbk) = R_{\mathfrak{q}}$. By Lemma 7.14, $\mathscr{D}_N(R/\Bbbk) \not\subset \mathfrak{q}$. Converse follows in a similar fashion. $\square$

7.15. **Proposition**. *Let $R = \Bbbk[X_1, \dots, X_n]/\mathfrak{a}$. Write x_i for the image of X_i in R. Then*

$$\mathscr{D}_N(R/\Bbbk) = \{f(x_1, \dots, x_n) \mid f(X_1, \dots, X_n)(X_i - x_i) \in \mathfrak{a}R[X_1, \dots, X_n] \textit{ for every } i\}.$$

Proof. Let $I = \ker(\mu : R \otimes_{\Bbbk} R \longrightarrow R)$. The exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow \Bbbk[X_1, \ldots, X_n] \longrightarrow R \longrightarrow 0$$

gives an exact sequence surjective map

$$0 \longrightarrow \mathfrak{a}R[X_1, \ldots, X_n] \longrightarrow R[X_1, \ldots, X_n] \xrightarrow{\rho} R \otimes_{\Bbbk} R \longrightarrow 0$$

using the isomorphism $R[X_1, \ldots, X_n] \longrightarrow R \otimes_{\Bbbk} \Bbbk[X_1, \ldots, X_n]$ which takes $rX_1^{e_1} \cdots X_n^{e_n}$ to $r \otimes X_1^{e_1} \cdots X_n^{e_n}$. The composite $\mu\rho$ is given by the substitution $X_i \mapsto x_i$. Hence $\{\rho(X_i - x_i) \mid 1 \leq i \leq n\}$ generate I as an $(R \otimes_{\Bbbk} R)$-ideal. Hence $\operatorname{Ann}_{R \otimes_{\Bbbk} R}(I) = \rho(\mathfrak{a}R[X_1, \ldots, X_n] : (X_1 - x_1, \ldots, X_n - x_n))$. Apply μ to conclude the result. □

A morphism $\Bbbk \longrightarrow R$ is said to be *essentially of finite-type* (or that R is an essentially finite-type $\Bbbk$-algebra) if R is a localization of a finite type $\Bbbk$-algebra. We now restrict to such morphisms of noetherian rings.

7.16. **Theorem**. *Let $\Bbbk$ be a noetherian ring and R an essentially finite-type $\Bbbk$-algebra. For every prime ideal $\mathfrak{q}$ of R, $\mathfrak{q}$ is unramified if and only if $(\Omega_{R/\Bbbk})_{\mathfrak{q}} = 0$.*

Proof. Note that $\Omega_{R/\Bbbk})_{\mathfrak{q}} = \Omega_{R_{\mathfrak{q}}/\Bbbk}$ [Eis95, 16.9]. Also note that $\mathfrak{q}$ is unramified if and only if the unique maximal ideal of $R_{\mathfrak{q}}$ is unramified. Replacing R by $R_{\mathfrak{q}}$, we may assume that $(R, \mathfrak{q})$ is a noetherian local ring that is an essentially finite-type $\Bbbk$-algebra and show that the unique maximal ideal of R is unramified if and only if $\Omega_{R/\Bbbk} = 0$. Note that $R \otimes_{\Bbbk} R$ is noetherian. Hence, by Theorem 7.3, the unique maximal ideal of R is unramified if and only if $\operatorname{Der}_{\Bbbk}(R, M) = 0$ for every finitely generated R-module M. Hence we need to show that $\operatorname{Der}_{\Bbbk}(R, M) = \operatorname{Hom}_R(\Omega_{R/\Bbbk}, M) = 0$ for every finitely generated R-module M if and only if $\Omega_{R/\Bbbk} = 0$. One direction is immediate; for the other direction use $M = \Omega_{R/\Bbbk}$, since $\Omega_{R/\Bbbk}$ is a finitely generated R-module (*cf.* Example 6.12 and localization). (Note that every nonzero module has a nonzero identity map.) □

8. Auslander-Buchsbaum paper, §3

Throughout this section, R is a normal domain, K its field of fractions, L a finite separable extension field of K, and S the integral closure of R in L.

8.1. **Definition**. The *complementary module* (or *inverse Dedekind different*) of the extension S/R is

$$\mathscr{D}_D^{-1}(S/R) := \{x \in L \mid \operatorname{Trace}_{L/K}(xS) \subseteq R\}.$$

The *Dedekind different* of S/R is

$$\mathscr{D}_D(S/R) := \{x \in L \mid x\mathscr{D}_D^{-1}(S/R) \subseteq S\}.$$

The Dedekind different is called *different* in [AB59]. Since $\operatorname{Trace}_{L/K}(S) \subseteq R$, it is immediate that $\mathscr{D}_D^{-1}(S/R)$ is an S-submodule of L containing S. Hence $\mathscr{D}_D(S/R)$ is an S-ideal.

8.2. **Discussion** ([Ben93, Section 3.10]). An S-module M is said to be *reflexive* if the natural map $M \longrightarrow \operatorname{Hom}_S(\operatorname{Hom}_S(M, S), S), x \mapsto [f \mapsto f(x)]$ is an isomorphism. $\mathscr{D}_D^{-1}(S/R)$ is a reflexive S-module. Let $M \subseteq L$ be an S-module. Let $s, s', t, t' \in S$, all non-zero, be such that $\frac{s}{t}, \frac{s'}{t'} \in M$. Let $\phi \in \operatorname{Hom}_S(M, S)$. It is not difficult to check that, as elements of L,

$$\frac{\phi\left(\frac{s}{t}\right)}{\frac{s}{t}} = \frac{\phi\left(\frac{s'}{t'}\right)}{\frac{s'}{t'}}.$$

Call this element α_ϕ. The map $\phi \mapsto \alpha_\phi$ gives an S-linear isomorphism

$$\operatorname{Hom}_S(M,S) \longrightarrow \{x \in L \mid xM \subseteq S\}.$$

Hence $\mathscr{D}_D(S/R) = \operatorname{Hom}_S(\mathscr{D}_D^{-1}(S/R), S)$, so it too is a reflexive S-module.

□

8.3. **Proposition**. *Let A be a normal domain with $\dim A \geq 2$. Let $0 \neq J \neq A$ be an A-ideal that is reflexive as an A-module. Then $\operatorname{ht}\mathfrak{p} = 1$ for every $\mathfrak{p} \in \operatorname{Ass}(A/J)$.*

Proof. Write $(-)^* = \operatorname{Hom}_A(-,A)$. We first argue that $\operatorname{ht} J = 1$. For otherwise, the exact sequence

$$0 \longrightarrow J \longrightarrow A \longrightarrow A/J \longrightarrow 0$$

gives an isomorphism $J^{**} \longrightarrow A^{**}$ since

$$\operatorname{Ext}^0_A(A/J,A) = \operatorname{Ext}^1_A(A/J,A) = 0.$$

Hence J is principal, which contradicts the hypothesis that $\operatorname{ht} J > 1$.

Let $J = \cap_{i=1}^t \mathfrak{a}_i$ be an irredundant primary decomposition. Let us assume that there exists i such that $\operatorname{ht}\mathfrak{a}_i > 1$, and obtain a contradiction.

$$J_1 = \bigcap_{\substack{1\leq i\leq t\\ \operatorname{ht}\mathfrak{a}_i = 1}} \mathfrak{a}_i \text{ and } J_2 = \bigcap_{\substack{1\leq i\leq t\\ \operatorname{ht}\mathfrak{a}_i > 1}} \mathfrak{a}_i.$$

Since $\operatorname{ht}\operatorname{Ann}_A((J_1+J_2)/J_2) \geq \operatorname{ht} J_2 \geq 2$, we obtain, as ealier,

$$\operatorname{Ext}^0_A((J_1+J_2)/J_2,A) = \operatorname{Ext}^1_A((J_1+J_2)/J_2,A) = 0,$$

so the natural map $J_1^* \longrightarrow J^*$ is an isomorphism. We have an exact sequence

$$0 \longrightarrow A^* \longrightarrow J^* \longrightarrow \operatorname{Ext}^1_A(A/J,A) \longrightarrow 0,$$

from which, applying $(-)^*$ again, we get an injective map $J^{**} \longrightarrow A^{**}$. Under the natural identification $A^{**} = A$, $J^{**} = J$, and J_1^{**} is an ideal containing J_1. Hence

$$J \subseteq J_1 \subseteq J_1^{**} = J^{**} = J$$

which implies that $\operatorname{ht}\mathfrak{a}_i = 1$ for every i, a contradiction. □

We say that J has *pure height one* to express the conclusion of the above proposition. Note that if, in the above proposition, $\dim A = 1$, then A is a Dedekind domain, and therefore every non-zero proper ideal is of pure height one.

8.4. **Corollary**. *$\mathscr{D}_D(S/R) = S$ or it is an ideal of pure height one.*

8.5. **Theorem** ([AB59, Proposition 3.3]). *$\mathscr{D}_N(S/R) \subseteq \mathscr{D}_D(S/R)$. If S is a projective R-module, then equality holds.*

Proof. TBD. □

8.6. **Corollary**. *The following are equivalent:*

(1) $\mathscr{D}_D(S/R) = S$;

(2) For every $\mathfrak{q} \in \operatorname{Spec} S$ with $\operatorname{ht}\mathfrak{q} = 1$, $\mathfrak{q}$ is unramified.

If, additionally, S is a projective R-module, the above conditions are equivalent to:

(3) S is unramified.

Proof. (1) $\implies$ (2): Let $\mathfrak{q} \in \operatorname{Spec} S$ with $\operatorname{ht} \mathfrak{q} = 1$ and $\mathfrak{p} = \mathfrak{q} \cap R$. Then $\mathscr{D}_N((R \smallsetminus \mathfrak{p})^{-1}S/R_\mathfrak{p}) = (R \smallsetminus \mathfrak{p})^{-1}\mathscr{D}_N(S/R)$ and $\mathscr{D}_D((R \smallsetminus \mathfrak{p})^{-1}S/R_\mathfrak{p}) = (R \smallsetminus \mathfrak{p})^{-1}\mathscr{D}_D(S/R)$. Since $R_\mathfrak{p}$ is a DVR and $(R \smallsetminus \mathfrak{p})^{-1}S$ is finitely generated, it is free over $R_\mathfrak{p}$, so by $\mathscr{D}_N((R \smallsetminus \mathfrak{p})^{-1}S/R_\mathfrak{p}) = \mathscr{D}_D((R \smallsetminus \mathfrak{p})^{-1}S/R_\mathfrak{p}) = (R \smallsetminus \mathfrak{p})^{-1}S$; therefore $(R \smallsetminus \mathfrak{p})^{-1}S/R_\mathfrak{p}$ is unramified.

(2) $\implies$ (1): By Theorem 7.13, $\operatorname{ht} \mathscr{D}_N(S/R) \geq 2$, so by Theorem 8.5 and Corollary 8.4, $\mathscr{D}_D(S/R) = S$.

Now assume that S is a projective R-module and that $\mathscr{D}_D(S/R) = S$. Then $\mathscr{D}_N(S/R) = S$ (Theorem 8.5), and, therefore, S is unramified (Theorem 7.13). □

8.7. **Theorem**. *Let R be a two-dimensional regular domain and S its integral closure in a finite separable extension of its fraction field. Then S is unramified if and only if for every $\mathfrak{q} \in \operatorname{Spec} S$ with $\operatorname{ht} \mathfrak{q} = 1$, $\mathfrak{q}$ is unramified.*

Proof. Use Proposition C.17 (to see that S is a projective R-module) and Corollary 8.6. □

9. Kähler different

We begin with a discussion of Fitting ideals [Eis95, Chapter 20]. Let R be a ring and $\phi : F \longrightarrow G$ a map of free R-modules of finite rank. Fix bases for F and G and express ϕ by a matrix A. For an integer t, $I_t(\phi)$ is the R-ideal generated by the $t \times t$ minors of A. This is independent of the choice of the bases. If $t \leq 0$, $I_t(\phi) = R$.

9.1. **Lemma**. *Let M be a R-module, and let $F \xrightarrow{\phi} G \longrightarrow M \longrightarrow 0$ and $F' \xrightarrow{\phi'} G' \longrightarrow M \longrightarrow 0$ be two presentations of M, with F, F', G, G' free modules of finite rank. Let $n = \operatorname{rk}_R G$ and $n' = \operatorname{rk}_R G'$. Then*
$$I_{n-t}(\phi) = I_{n'-t}(\phi')$$
for every $t \in \mathbb{N}$.

Proof. Two ideals are equal if and only if they are equal at all localizations of R at prime ideals. Hence we may assume that R is local with maximal ideal $\mathfrak{m}$. Choose bases for F and G and express ϕ as an $n \times m$ matrix A. If any entry in A is a unit, then by suitable row and column operations, we may assume that
$$A = \begin{bmatrix} 1 & 0_{1\times(m-1)} \\ 0_{(n-1)\times 1} & B_{(n-1)\times(m-1)} \end{bmatrix}.$$
Since $I_{n-t}(A) = I_{n-1-t}(B)$ and $M \simeq \operatorname{coker} B$, we may replace F (respectively G) by a free module of rank one less than that of F (respectively G). Repeating this we may assume that $\operatorname{Im} \phi \subseteq \mathfrak{m}G$, i.e, ϕ is minimal. Repeating this for ϕ', we may assume that ϕ' is minimal. Note that in this case, $n = n' = \operatorname{rk}_{R/\mathfrak{m}}(M/\mathfrak{m}M)$. Hence it suffices to show that if ϕ and ϕ' are two minimal presentations of M, then $I_j(\phi) = I_j(\phi')$ for every j. This follows from noting that there are isomorphisms $\alpha : F \longrightarrow F'$ and $\beta : G \longrightarrow G'$ such that the following diagram commutes:
$$\begin{tikzcd} F \arrow[r, "\phi"] \arrow[d, "\alpha"] & G \arrow[r] \arrow[d, "\beta"] & M \arrow[r] \arrow[d, equal] & 0 \\ F' \arrow[r, "\phi'"] & G' \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$
□

9.2. **Definition**. Let M be an R-module with a finite free presentation $F \xrightarrow{\phi} G \longrightarrow M \longrightarrow 0$. Write $n = \operatorname{rk}_R G$. For $t \in \mathbb{N}$, the tth *Fitting ideal* $\operatorname{Fitt}_t(M)$ of M is $I_{n-t}(\phi)$.

9.3. **Lemma**. *Let M be a finitely presented R-module and S an R-algebra. Then for every $t \in \mathbb{N}$,* $\operatorname{Fitt}_t(S \otimes_R M) = \operatorname{Fitt}_t(M)S$.

Proof. Follows from noting that $\phi : F \longrightarrow G$ is a finite R-free presentation of M, then $1 \otimes \phi$ is a finite S-free presentation of $S \otimes_R M$. □

9.4. **Proposition**. *Let M be a finitely presented R-module. Then*

(1) $\operatorname{Fitt}_0(M) \subseteq \operatorname{Ann}(M)$*;*

(2) For every $j \geq 1$, $\operatorname{Ann}(M)\operatorname{Fitt}_j(M) \subseteq \operatorname{Fitt}_{j-1}(M)$. *In particular, if M can be generated by n elements, then* $(\operatorname{Ann}(M))^n \subseteq \operatorname{Fitt}_0(M)$.

Proof. TBD. □

9.5. **Proposition**. *Let M be a finitely presented R-module. Then* $\operatorname{Supp}(M) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq \operatorname{Fitt}_0(M)\}$.

Proof. Let $\xrightarrow{\phi} G \longrightarrow M \longrightarrow 0$ be a finite free presentation of M. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then $M_\mathfrak{p} = 0$ if and only if the map $\phi \otimes R_\mathfrak{p} : F_\mathfrak{p} \longrightarrow G_\mathfrak{p}$ is surjective, which holds if and only if some $\operatorname{rk}_R G \times \operatorname{rk}_R G$ minor of $\phi \otimes R_\mathfrak{p}$ is a unit in $R_\mathfrak{p}$, which holds if and only $\operatorname{Fitt}_0(M_\mathfrak{p}) = R_\mathfrak{p}$ (as an $R_\mathfrak{p}$-module) which happens if and only of $\operatorname{Fitt}_0(M) \not\subseteq \mathfrak{p}$. □

9.6. **Definition**. Let $\Bbbk$ be a noetherian ring and R an essentially finite-type $\Bbbk$-algebra. The *Kähler different* $\mathscr{D}_K(R/\Bbbk)$ is $\operatorname{Fitt}_0(\Omega_{R/\Bbbk})$.

9.7. **Theorem**. *Let $\Bbbk$ be a noetherian ring and R an essentially finite-type $\Bbbk$-algebra. For every prime ideal $\mathfrak{q}$ of R, $\mathfrak{q}$ is unramified if and only if $\mathscr{D}_K(R/\Bbbk) \not\subseteq \mathfrak{q}$.*

Proof. Follows from Theorem 7.16. □

9.8. **Theorem**. *Let $\Bbbk$ be a noetherian ring and R an essentially finite-type $\Bbbk$-algebra. Then*

$$\mathscr{D}_K(R/\Bbbk) \subseteq \mathscr{D}_N(R/\Bbbk) \subseteq \operatorname{Ann}_R(\Omega_{R/\Bbbk}).$$

Proof. Write $I = \ker(\mu : R \otimes_\Bbbk R \longrightarrow R)$. Then $\mathscr{D}_N(R/\Bbbk) = \mu(\operatorname{Ann}_{R\otimes_\Bbbk R}(I))$ (Definition 7.12) and $\Omega_{R/\Bbbk} \simeq I/I^2$ (Proposition 6.9). Hence $\mathscr{D}_N(R/\Bbbk) \subseteq \operatorname{Ann}_R(\Omega_{R/\Bbbk})$.

Write $R = U^{-1}S$ for a finite-type $\Bbbk$-algebra S and a multiplicatively closed system $U \subseteq S$. Since $\mathscr{D}_K(R/\Bbbk) = U^{-1}\mathscr{D}_K(S/\Bbbk)$, $\mathscr{D}_N(R/\Bbbk) = U^{-1}\mathscr{D}_N(S/\Bbbk)$ and $\operatorname{Ann}(\Omega_{R/\Bbbk}) = U^{-1}\operatorname{Ann}(\Omega_{S/\Bbbk})$, we may replace R by S and assume that $R = \Bbbk[X_1, \ldots, X_n]/\mathfrak{a}$. Write x_i for the image of X_i in R. Abbreviate $X_1, \ldots, X_n$ by X and $x_1, \ldots, x_n$ by x. Then, by Proposition 7.15,

$$\mathscr{D}_N(R/\Bbbk) = \{f(\mathrm{x}) \mid f(\mathrm{X}) \in R[\mathrm{X}] \text{ and } f(\mathrm{X})(X_i - x_i) \in \mathfrak{a}R[\mathrm{X}] \text{ for every } i\}.$$

Write π for the natural map $\Bbbk[\mathrm{X}] \longrightarrow R$; let ρ and $\mu : R \otimes_\Bbbk R$ be as in the proof of Proposition 7.15. Since $\mathscr{D}_K(R/\Bbbk)$ is generated (as an R-ideal) by

$$\left\{\pi\left(\det\left(\left[\frac{\partial f_j}{\partial X_i}\right]_{n\times n}\right)\right) \mid f_1, \ldots, f_n \in \mathfrak{a}\right\},$$

it suffices to show that

$$\det\left(\left[\frac{\partial f_j}{\partial X_i}\right]_{n\times n}\right) \cdot (X_k - x_k) \in \mathfrak{a}R[\mathrm{X}]$$

for every $f_1, \ldots, f_n \in \mathfrak{a}$ and $1 \leq k \leq n$. Let $f_1, \ldots, f_n \in \mathfrak{a}$. Note that $\mathfrak{a}R[\mathrm{X}] \subseteq \ker(\mu\rho) = (X_1 - x_1, \ldots, X_n - x_n)$, so there exist $h_{ij} \in R[\mathrm{X}]$ such that

$$f_i = \sum_{j=1}^{n} h_{ij}(X_j - x_j)$$

for every $1 \le i \le n$. Write

$$H = \left[h_{ij}\right]_{n\times n}$$

By Cramer's rule,

$$\operatorname{adj}(H)\begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix} = (\det H)\begin{bmatrix} X_1 - x_1 \\ \vdots \\ X_n - x_n \end{bmatrix}$$

so

$$(\det H)(X_k - x_k) \in (f_1, \dots, f_n)R[\mathrm{X}] \subseteq \mathfrak{a}R[\mathrm{X}]$$

for every $1 \le k \le n$. We conclude the proof by observing that

$$\mu\rho(H) = \mu\rho\left(\det\left(\left[\frac{\partial f_j}{\partial X_i}\right]_{n\times n}\right)\right). \qquad \square$$

9.9. **Corollary**. *Suppose R is a localization of $\mathbb{k}[X_1, \dots, X_n]/\mathfrak{a}$. Then*

$$(\mathscr{D}_N(R/\mathbb{k}))^n \subseteq \left(\operatorname{Ann}_R(\Omega_{R/\mathbb{k}})\right)^n \subseteq \mathscr{D}_K(R/\mathbb{k}) \subseteq \mathscr{D}_N(R/\mathbb{k}) \subseteq \operatorname{Ann}_R(\Omega_{R/\mathbb{k}}).$$

Proof. Since $\Omega_{R/\mathbb{k}}$ is a quotient of a free module of rank n (*cf.* Example 6.12),

$$\left(\operatorname{Ann}_R(\Omega_{R/\mathbb{k}})\right)^n \subseteq \mathscr{D}_K(R/\mathbb{k})$$

by Proposition 9.4. $\square$

9.10. **Example**. Let $S = \mathbb{C}[x, y]$ where x, y are variables and $R = \mathbb{C}[x^2, xy, y^2]$. We will show that $\mathscr{D}_K(S/R) = (x, y)^2$. It then follows from Theorem 9.8, Theorem 8.5 and Corollary 8.4 that $(x, y)^2 \subseteq \mathscr{D}_N(S/R) \subsetneq (x, y)$ and that $\mathscr{D}_D(S/R) = S$.

Let $L = \mathbb{C}(x, y)$ and $K = \mathbb{C}(x^2, \frac{y}{x})$ denote their respective fields of fractions. The extension L/K is Galois, with Galois group $\mathbb{Z}/2\mathbb{Z} = \{1, \sigma\}$ acting $\mathbb{C}$-linearly on L by $\sigma x = -x$ and $\sigma y = -y$. Hence $\operatorname{Trace}_{L/K} f = f + \sigma f$ for every

Note that

$$S \simeq \frac{R[U, V]}{(U^2 - x^2, UV - xy, V^2 - y^2, x^2V - xyU, xyV - y^2U)}.$$

Hence

$$\Omega_{S/R} \simeq \operatorname{coker}\left(S^5 \xrightarrow{J} S^2\right)$$

where J is the 2×5 jacobian matrix

$$\begin{bmatrix} 2x & y & 0 & -xy & -y^2 \\ 0 & x & 2y & x^2 & xy \end{bmatrix}.$$

Therefore $\mathscr{D}_K(S/R) = \operatorname{Fitt}_0(\Omega_{S/R}) = I_2(J) = (x, y)^2$.

$\square$

9.11. **Example**. Continuing the above example, let $\mathbb{k} = \mathbb{C}[x^2, y^2]$. Write $\mathbb{k} = \mathbb{C}[u, w]$ and $R = \mathbb{k}[v]/(v^2 - uw)$. Then $\Omega_{R/\mathbb{k}} \simeq R/(v)$, so $\mathscr{D}_K(R/\mathbb{k}) = (v)$, which is a reduced ideal. Moreover, R is a free $\mathbb{k}$-module, with basis $\{1, v\}$. Hence $\mathscr{D}_K(R/\mathbb{k}) = \mathscr{D}_N(R/\mathbb{k}) = \mathscr{D}_D(R/\mathbb{k})$. Note that $(v) = (u, v) \cap (v, w)$, so the ramification locus has two components, one defined by (u, v) and the other by (v, w). Note that the branch locus (the image of the ramification locus in $\operatorname{Spec}\mathbb{k}$) has two components, one defined by $u\mathbb{k} = (u, v)R \cap \mathbb{k}$ and the other by $w\mathbb{k} = (v, w)R \cap \mathbb{k}$. $\square$

10. Discriminants

10.1. **Definition.** Let R be a ring, y a variable, $f(y) = \sum_{i=0}^{n} a_i y^i$, and $g(y) = \sum_{i=0}^{m} b_i y^i$, with $a_n b_m \neq 0$. The resultant $\operatorname{Res}(f,g)$ of f and g is the element

$$\det \begin{bmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & \\ 0 & a_n & a_{n-1} & \cdots & a_0 & 0 & \\ \ddots & \ddots & & & \ddots & & \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & \cdots & \\ 0 & b_m & b_{m-1} & \cdots & b_0 & 0 & \\ \ddots & \ddots & & & \ddots & & \\ 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & b_0 \end{bmatrix}$$

(There are m rows of the a_is and n rows of the b_is.) If $f = 0$ or $g = 0$, we set $\operatorname{Res}(f,g) = 0$. The *discriminant* $\operatorname{Disc}(f)$ is $\operatorname{Res}(f,f')$.

10.2. **Proposition.** *Let R be a UFD. If $a_n b_m = 0$, then f and g have a non-constant common divisor in $R[y]$ if and only if* $\operatorname{Res}(f,g) = 0$.

Proof. Claim: f and g have a non-constant common divisor in $R[y]$ if and only if there exist two non-zero polynomials $u, v \in R[y]$ such that

(1) $\deg u < \deg f$ and $\deg v < \deg g$;
(2) $vf = ug$.

Assume the claim. Write $u = \sum_{i=0}^{n-1} c_i y^i$ and $v = \sum_{i=0}^{m-1} d_i y^i$. Write M for the matrix in Definition 10.1. Expanding the relation $vf = ug$ gives linear equation

$$M \begin{bmatrix} d_{m-1} \\ d_{m-2} \\ \vdots \\ d_0 \\ -c_{n-1} \\ -c_{n-2} \\ \vdots \\ c_0 \end{bmatrix} = 0.$$

This proves the proposition, assuming the claim.

Now to prove the claim, assume that f and g have a non-constant common divisor $h \in R[y]$. Write $f = hu$ and $g = hv$. Conversely, assume that there exist u and v satisfying the conditions above. Since $R[y]$ is a UFD, every irreducible factor of f must divide ug; since $\deg u < \deg f$, some irreducible factor of f must divide g. □

10.3. **Theorem.** *Let R be a Dedekind domain, K its field of fractions, L a finite separable extension of K, and S the integral closure of R in L. Let $\delta_{S/R}$ be the R-ideal generated by*

$$\{\operatorname{Disc}(\mu_{\alpha,K}) \mid \alpha \in S \textit{ such that } L = K(\alpha)\}$$

where, for $\beta \in L$, we denote its minimal polynomial over K by $\mu_{\beta,K}$. Let $\mathfrak{p} \in \operatorname{Spec} R$. If $\mathfrak{p}$ ramifies in S then $\delta_{S/R} \subseteq \mathfrak{p}$. The converse is true if we assume that $S = R[\alpha]$ for some $\alpha \in S$.

There is a 'discriminant ideal' of R, which characterizes the prime ideals of R that ramify in S (without assuming that $S = R[\alpha]$ for some α), but we will not define it here.

Proof. Assume that $\mathfrak{p}$ ramifies in S. Then $\mathfrak{p}R_\mathfrak{p}$ ramifies in $(R \smallsetminus \mathfrak{p})^{-1}S$. As subsets, it is clear that $\delta_{S/R} \subseteq \delta_{(R\smallsetminus\mathfrak{p})^{-1}S/R_\mathfrak{p}}$, so it is enough to show that $\delta_{(R\smallsetminus\mathfrak{p})^{-1}S/R_\mathfrak{p}} \subseteq \mathfrak{p}R_\mathfrak{p}$. Hence without loss of generality, R is local (i.e., a DVR) with maximal ideal $\mathfrak{p}$. Then there exists $\alpha \in S$ such that $\operatorname{Disc}(\mu_{\alpha,K})R = \delta_{S/R}$.

Let $\mathfrak{q} \in \operatorname{Spec} S$ be such that $\mathfrak{q} \cap R = \mathfrak{p}$ and $\mathfrak{q}$ is ramified. INCOMPLETE. ◻

Appendix A. Semisimple rings

In this section, we summarize various results regarding global dimension and semisimplicity. The primary reference for this section is [CE99]. In the beginning of this section, we do not assume that R is necessarily commutative (but is associative and has 1); when we talk of ideals and modules, we mean left ideals and left modules.

A.1. **Definition**. Let R be a ring and M an R-module. It is said to be *simple* if it is nonzero and has no submodules different from M and 0. It is said to be *semisimple* if it is a direct sum of simple modules. R is said to be a *semisimple ring* if it is semisimple as an R-module.

A.2. **Proposition** ([CE99, I, 4.1]). *M is semisimple if and only if every submodule of it is a direct summand.*

A.3. **Proposition** ([CE99, I, 4.2]). *The following are equivalent:*

(1) *R is semisimple;*
(2) *every ideal of R is a direct summand of R;*
(3) *every ideal of R is an injective R-module;*
(4) *every R-module is semisimple;*
(5) *every short exact sequence of R-modules is split;*
(6) *every R-module is injective;*
(7) *every R-module is projective;*

A.4. **Theorem** (Wedderburn [Bou12, VIII, §7.1, Théorèm 1 and §8.1, Théorèm 1]). *Semisimple ring are precisely those of the form*

$$\prod_{i=1}^{n} M_{d_i}(D_i)$$

where $n > 0$ and $d_i, i = 1, \ldots, n$ are integers and $D_i, i = 1, \ldots, n$ are division rings.

A.5. **Corollary**. *Commutative semisimple rings are precisely the finite products of fields.*

Proof. It is necessary and sufficient that that $d_i = 1$ and D_i is commutative for every i, in Theorem A.4. ◻

A.6. **Definition**. We denote the projective dimension of an R-module M by $\operatorname{pd}_R M$.

A.7. **Theorem** ([CE99, VI, 2.6]). *Let $n \geq 0$ be an integer. The following are equivalent:*

(1) *$\operatorname{pd}_R M \leq n$ for every R-module M;*
(2) *$\operatorname{Ext}^k_R(M, -) = 0$ for every $k > n$;*
(3) *$\operatorname{Ext}^{n+1}_R(M, -) = 0$.*

Proof. The implications (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) are immediate; we will show that (3) $\Longrightarrow$ (1) assuming that $n = 0$, which is the only case that we need. Let M an R-module and F a free R-module with a surjective R-linear map $F \xrightarrow{f} M$. Since $\operatorname{Ext}^1_R(M, \ker f) = 0$, we see that f is split, so M is projective. ◻

A.8. **Definition.** By the *(left) global dimension* of R, denoted $\operatorname{gldim} R$, we mean the smallest integer n, if such an integer exists, satisfying the conditions of the above theorem; otherwise we say that $\operatorname{gldim} R = \infty$.

A.9. **Corollary.** *Let R be a ring. Then R is semisimple if and only if* $\operatorname{gldim} R = 0$.

In order to simplify our discussion, we will restrict ourselves to the commutative case for the rest of this section. Let $\Bbbk$ be a commutative ring and R a (commutative associative) $\Bbbk$-algebra.

A.10. **Definition.** Let M be an R-module. Define

$$\mathrm{H}_n(R, M) = \operatorname{Tor}_n^{R^e}(R, M) \text{ and } \mathrm{H}^n(R, M) = \operatorname{Ext}^n_{R^e}(R, M).$$

A.11. **Definition.** Define $\Bbbk\text{-}\dim(R)$ to be the projective dimension of R as an R^e-module.

A.12. **Proposition.** $\mathrm{H}^n(R, \operatorname{Hom}_{\Bbbk}(M, N)) \simeq \operatorname{Ext}^n_R(M, N)$ *for every pair of R-modules M, N and for every* $n \geq 0$.

A.13. **Corollary.** *If R is R^e-projective, then R is semisimple.*

Proof. By Proposition A.12, $\operatorname{Ext}^1_R(-,-) = 0$. Now use the implication Theorem A.7 (3) $\Longrightarrow$ (1) (which was proved for $n = 0$) to conclude that $\operatorname{gldim} R = 0$. Apply Corollary A.9. □

Appendix B. Free resolutions

Let R be a noetherian ring and M a finitely generated R-module. We build a free resolution of M as follows: Set $M_0 = M$ and let F_0 be a finitely generated free R-module with a surjective map $\epsilon_0 : F_0 \longrightarrow M_0$. Let $M_1 = \ker \epsilon_0$; it is a finitely generated R-module. Let F_1 be a finitely generated free R-module with a surjective map $\epsilon_1 : F_1 \longrightarrow M_1$. Repeating this process, assume by induction, we have constructed $M_i = \ker(\epsilon_{i-1} : F_{i-1} \longrightarrow M_{i-1})$ and a surjective map $\epsilon_i : F_i \longrightarrow M_i$ where F_i is a finitely generated free R-module. For $i \geq 1$, define $\partial_i : F_i \longrightarrow F_{i-1}$ to be the composite of the ϵ_i followed by the inclusion map $M_i \longrightarrow F_{i-1}$. Then the complex

$$(F_\bullet, \partial_\bullet) : \qquad \cdots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \longrightarrow 0$$

is a free resolution of M.

Now assume that $(R, \mathfrak{m}, \Bbbk)$ is a noetherian local ring. In the construction above, we may choose, recursively, F_i to be of the smallest possible rank, i.e., with $\operatorname{rk}_R F_i = \operatorname{rk}_{\Bbbk} M_i/\mathfrak{m}M_i$. Applying $- \otimes_R \Bbbk$ to the exact sequence

$$0 \longrightarrow M_{i+1} \longrightarrow F_i \xrightarrow{\epsilon_i} M_i \longrightarrow 0$$

we get the exact sequence

$$M_{i+1}/\mathfrak{m}M_{i+1} \longrightarrow F_i/\mathfrak{m}F_i \xrightarrow{\epsilon_i \otimes 1} M_i/\mathfrak{m}M_i \longrightarrow 0.$$

By the choice of F_i, the map $\epsilon_i \otimes 1$ is an isomorphism, so the $\operatorname{Im}(M_{i+1}/\mathfrak{m}M_{i+1} \longrightarrow F_i/\mathfrak{m}F_i) = 0$, i.e., $\operatorname{Im}(M_{i+1} \longrightarrow F_i) \subseteq \mathfrak{m}F_i$. Therefore $\operatorname{Im} \partial_{i+1} \subseteq \mathfrak{m}F_i$.

B.1. **Definition.** Let $(R, \mathfrak{m})$ be a noetherian local ring and M a finitely generated R-module. A free resolution

$$(F_\bullet, \partial_\bullet) : \qquad \cdots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \longrightarrow 0$$

of M that satisfies $\operatorname{Im} \partial_{i+1} \subseteq \mathfrak{m}F_i$ for every $i \geq 0$ is called a *minimal* free resolution of M.

Let $F_\bullet$ be a minimal free resolution and $G_\bullet$ any free resolution of M. Then $F_\bullet$ is a direct summand of $G_\bullet$; see, e.g., [Eis95, Theorem 20.2]. In particular,

$$\operatorname{pd}_R(M) = \sup\{i \mid F_i \neq 0\}.$$

Additionally, the maps in the complex

$$F_\bullet \otimes_R (R/\mathfrak{m})$$

are zero, so $\operatorname{rk}_R F_i = \operatorname{rk}_{R/\mathfrak{m}} \operatorname{Tor}_i^R(M, R/\mathfrak{m})$. In particular

$$\operatorname{pd}_R(M) = \sup\{i \mid \operatorname{Tor}_i^R(M, R/\mathfrak{m}) \neq 0\}. \tag{B.2}$$

We now look at a specific complex of finitely generated free R-modules that, in some important cases, becomes a resolution of a quotient of R by an ideal. Let $r_1, \dots, r_d \in R$. Define the *Koszul complex*

$$K_\bullet(r_i) : \qquad 0 \longrightarrow R \xrightarrow{r_1} R \longrightarrow 0$$

where the rank-one free modules are place in homological indices 0 and 1. Define

$$K_\bullet(r_1, \dots, r_d) := K_\bullet(r_1) \otimes_R \cdots \otimes_R K_\bullet(r_d).$$

Note that there is an exact sequence of complexes

$$0 \longrightarrow R \longrightarrow K_\bullet(r_d) \longrightarrow R[-1] \longrightarrow 0$$

where R is thought of as the complex with R at homological index 0 and 0s elsewhere, and $R[-1]$ is the complex with R at homological index -1 and 0s elsewhere. Identifying $K_\bullet(r_1, \dots, r_{d-1}) \otimes_R R$ with $K_\bullet(r_1, \dots, r_{d-1})$, and using the fact that, at each homological index, the above short exact sequence of complexes is a split exact sequence of R-modules, we get another exact sequence of complexes,

$$0 \longrightarrow K_\bullet(r_1, \dots, r_{d-1}) \longrightarrow K_\bullet(r_1, \dots, r_d) \longrightarrow K_\bullet(r_1, \dots, r_{d-1})[-1] \longrightarrow 0.$$

Abbreviate $K_\bullet(r_1, \dots, r_d)$ by $K_\bullet$ and $K_\bullet(r_1, \dots, r_{d-1})$ by $K'_\bullet$ for now. Further, note that $\mathrm{H}_i(K'_\bullet[-1]) \simeq \mathrm{H}_{i-1}(K'_\bullet)$. Then we have an an exact sequence in homology:

$$\longrightarrow \mathrm{H}_i(K'_\bullet) \longrightarrow \mathrm{H}_i(K_\bullet) \longrightarrow \mathrm{H}_{i-1}(K'_\bullet) \xrightarrow{\delta} \mathrm{H}_{i-1}(K'_\bullet) \longrightarrow \mathrm{H}_{i-1}(K_\bullet) \longrightarrow \tag{B.3}$$

It can be seen by diagram-chasing that the connecting morphism δ is given by multiplication by r_d.

Appendix C. Depth, Auslander-Buchsbaum formula, etc.

Let R be a ring, I an R-ideal and M an R-module.

C.1. **Definition**. Define $\Gamma_I(M) := \{x \in M \mid \text{there exists } n \geq 0 \text{ such that } I^n x = 0\}$.

The map $M \mapsto \Gamma_I(M)$ is a left-exact covariant functor from the category of R-modules to itself.

C.2. **Definition**. Define $\mathrm{H}^i_I(-)$ to be the right-derived functors of $\Gamma_I(-)$. $\mathrm{H}^i_I(M)$ is called *the ith local cohomology module of M with support in I.*

Note that $\Gamma_I(M) = \Gamma_{\sqrt{I}}(M)$; hence $\mathrm{H}^i_I(M) = \mathrm{H}^i_{\sqrt{I}}(M)$ for all $i \geq 0$.

C.3. **Definition**. An *M-regular sequence* in R is a sequence $r_1, \dots, r_t \in R$ such that r_1 is a non-zero-divisor on M, and for every $2 \leq i \leq t$, r_i is a non-zero-divisor on $M/(r_1, \dots, r_{i-1})M$ and such that $(r_1, \dots, r_t)M \neq M$. The length of the longest M-regular sequence in I is denoted $\operatorname{depth}_I(M)$. If R is local with maximal ideal $\mathfrak{m}$, we write $\operatorname{depth} M = \operatorname{depth}_{\mathfrak{m}}(M)$.

C.4. **Proposition.** *Let $r_1, \dots, r_t$ be an R-regular sequence. Then the Koszul complex $K_\bullet(r_1, \dots, r_t)$ is a free resolution of $R/(r_1, \dots, r_t)$.*

Proof. Induct on t. If $t = 1$, then it is immediate from the definition of $K_\bullet(r_1)$ that $\mathrm{H}_1(K_\bullet(r_1)) = \mathrm{Ann}_R(r_1) = 0$ and that $\mathrm{H}_0(K_\bullet(r_1)) = R/(r_1)$. Hence $K_\bullet(r_1)$ is a free resolution of $R/(r_1)$. Now assume that that the proposition holds for $r_1, \dots, r_{t-1}$, which is an R-regular sequence. From (B.3), with notation from there, we see that $\mathrm{H}_i(K_\bullet) = 0$ for $i > 1$. Further, we see that $\mathrm{H}_1(K_\bullet) \simeq \ker\left(\mathrm{H}_0(K'_\bullet) \xrightarrow{r_d} \mathrm{H}_0(K'_\bullet)\right)$. Since $\mathrm{H}_0(K'_\bullet) \simeq R/(r_1, \dots, r_{t-1})$ and r_t is a non-zero-divisor on $R/(r_1, \dots, r_{t-1})$, we conclude that $\mathrm{H}_1(K_\bullet) = 0$. Similarly, $\mathrm{H}_0(K_\bullet) \simeq \mathrm{coker}\left(\mathrm{H}_0(K'_\bullet) \xrightarrow{r_d} \mathrm{H}_0(K'_\bullet)\right) \simeq R/(r_1, \dots, r_t)$. □

C.5. **Proposition.** *Let R be a noetherian ring and M a finitely generated R-module. Then* $\mathrm{depth}_I(M) \leq \dim M$.

Proof. We prove this by induction on $t := \mathrm{depth}_I(M)$. If $t = 0$, the assertion is immediate. Hence assume that $t > 0$. Let $r_1, \dots, r_t \in I$ be an M-regular sequence. Write $M' = M/r_1M$. Then $r_2, \dots, r_t$ is an M'-regular sequence of maximum length in I, so $\mathrm{depth}\, M' = t - 1$. Hence, by induction, $\dim M' \geq t - 1$. Note that $r_1 \notin \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Supp}(M)$ with $\dim R/\mathfrak{p} = \dim M$ (for any such $\mathfrak{p}$ is in $\mathrm{Ass}(M)$), so $\dim M' < \dim M$. Hence $\dim M \geq t$. □

C.6. **Proposition.** *Let R be a noetherian ring and M a finitely generated R-module. Then*

$$\mathrm{depth}_I(M) = \min\{i \mid \mathrm{H}^i_I(M) \neq 0\}.$$

Proof. We apply induction on $t := \mathrm{depth}_I(M)$. Write $s = \min\{i \mid \mathrm{H}^i_I(M) \neq 0\}$. Suppose that $t = 0$. Since R is noetherian, $I \subseteq \cup_{\mathfrak{p} \in \mathrm{Ass}\, M} \mathfrak{p}$. By the prime avoidance lemma, there exists $\mathfrak{p} \in \mathrm{Ass}\, M$ such that $I \subseteq \mathfrak{p}$. Since there exists $0 \neq x \in M$ such that $\mathrm{Ann}_R(x) = \mathfrak{p}$, we see that $Ix = 0$, so $\mathrm{H}^0_I(M) \neq 0$.

Now suppose that $t > 0$. Since I contains a non-zero-divisor on M, $\Gamma_I(M) = 0$, so $s > 0$. Let $r_1, \dots, r_t \in I$ be an M-regular sequence. Write $M' = M/r_1M$. Then $r_2, \dots, r_t$ is an M'-regular sequence of maximum length in I, so $\mathrm{depth}\, M' = t - 1$. From the exact sequence

$$0 \longrightarrow M \xrightarrow{r_1} M \longrightarrow M' \longrightarrow 0$$

we get

$$\cdots \longrightarrow \mathrm{H}^i_I(M) \xrightarrow{r_1} \mathrm{H}^i_I(M) \longrightarrow \mathrm{H}^i_I(M') \longrightarrow \mathrm{H}^{i+1}_I(M) \xrightarrow{r_1} \mathrm{H}^{i+1}_I(M) \longrightarrow \cdots.$$

(To determine the maps we note that multiplication by r_1 on an injective resolution of M lifts the corresponding map on M; hence the induced map $\mathrm{H}^i_I(M) \longrightarrow \mathrm{H}^i_I(M)$ is, again, multiplication by r_1.) Hence $\mathrm{H}^i_I(M') = 0$ for every $i \leq s - 2$. Further, note that for every i, and every $x \in I$, $\ker(\mathrm{H}^i_I(M) \longrightarrow \mathrm{H}^i_I(M)) \neq 0$ if $\mathrm{H}^i_I(M) \neq 0$, since $\mathrm{H}^i_I(M)$ is a quotient of a submodule of $\Gamma_I(N)$ for some module N. Hence $\mathrm{H}^{s-1}_I(M') \neq 0$. By induction, $s - 1 = t - 1$. □

C.7. **Definition.** Let $I = (r_1, \dots, r_n)$. Define

$$\check{\mathrm{C}}^\bullet(r_i): \qquad 0 \longrightarrow R \longrightarrow R_{r_i} \longrightarrow 0$$

where the middle map is the natural (localization) map. This is indexed cohomologically: $\check{\mathrm{C}}^0(r_i) = R$ and $\check{\mathrm{C}}^1(r_i) = R_{r_i}$. Define

$$\check{\mathrm{C}}^\bullet(r_i, \dots, r_n) := \check{\mathrm{C}}^\bullet(r_1) \otimes_R \check{\mathrm{C}}^\bullet(r_2) \otimes_R \cdots \check{\mathrm{C}}^\bullet(r_n)$$

and for an R-module M, $\check{\mathrm{C}}^\bullet(r_i,\ldots,r_n;M) := \check{\mathrm{C}}^\bullet(r_i,\ldots,r_n) \otimes_R M$. These complexes are called *(extended) Čech complexes* or *stable Koszul complexes.*

C.8. **Proposition**. *Let $I = (r_1,\ldots,r_n)$.*

$$\mathrm{H}^i_I(M) \simeq \mathrm{H}^i(\check{\mathrm{C}}(r_1,\ldots,r_n;M)).$$

Sketch of the proof. Write $\check{\mathrm{H}}^i(-) = \mathrm{H}^i(\check{\mathrm{C}}(r_1,\ldots,r_n;M))$. By a standard argument in homological algebra involving δ-functors, it suffices to show the following:

(1) The assertion is true with $i = 0$ for all R-modules M.

(2) For every injective R-module M and every $i \neq 0$, $\check{\mathrm{H}}^i(M) = 0$.

(3) For every exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ there are connecting homomorphisms

$$\check{\mathrm{H}}^i(M'') \longrightarrow \check{\mathrm{H}}^{i+1}(M')$$

such that for every commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0
\end{tikzcd}$$

with exact rows (i.e., maps of short exact sequences)) there is a commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r] & \check{\mathrm{H}}^{i-1}(M'') \arrow[r] \arrow[d] & \check{\mathrm{H}}^i(M') \arrow[r] \arrow[d] & \check{\mathrm{H}}^i(M) \arrow[r] \arrow[d] & \check{\mathrm{H}}^i(M'') \arrow[r] \arrow[d] & \check{\mathrm{H}}^{i+1}(M') \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & \check{\mathrm{H}}^{i-1}(N'') \arrow[r] & \check{\mathrm{H}}^i(N') \arrow[r] & \check{\mathrm{H}}^i(N) \arrow[r] & \check{\mathrm{H}}^i(N'') \arrow[r] & \check{\mathrm{H}}^{i+1}(N') \arrow[r] & \cdots
\end{tikzcd}$$

with exact rows.

See, e.g., [ILL+07, Chapter 7] for details. □

C.9. **Proposition**. *(1) Let $R \longrightarrow S$ be a ring map, M an S-module and $I = (r_1,\ldots,r_n)R$. Then, for every i,*

$$\mathrm{H}^i_I(M) = \mathrm{H}^i_{IS}(M).$$

(2) Let $U \subseteq R$ be a multiplicatively closed set. Then

$$\mathrm{H}^i_{U^{-1}I}(U^{-1}M) = U^{-1}\,\mathrm{H}^i_I(M).$$

Proof. (1) Write ϕ for the map $R \longrightarrow S$. Notice that

$$\check{\mathrm{C}}^\bullet(r_1,\ldots,r_n;M) \simeq \check{\mathrm{C}}^\bullet(r_1,\ldots,r_n) \otimes_R S \otimes_S M \simeq \check{\mathrm{C}}^\bullet(\phi(r_1),\ldots,\phi(r_n)) \otimes_S M;$$

this proves the asserted isomorphism of homology.

(2) This follows from noting that localization is an exact functor.

□

C.10. **Definition**. Let $(R,\mathfrak{m})$ be a noetherian local ring and M a finitely generated R-module. M is said to be *Cohen-Macaulay* if $\operatorname{depth} M = \dim M$; R is said to be a *Cohen-Macaulay* ring if it is a Cohen-Macaulay module over itself. A noetherian ring is said to be *Cohen-Macaulay* if all its local rings at maximal ideals are Cohen-Macaulay.

C.11. **Proposition**. *Every two-dimensional local normal domain is Cohen-Macaulay.*

Proof. Let $(R, \mathfrak{m})$ be a two-dimensional local normal domain. Let $0 \neq r \in \mathfrak{m}$. Then $\operatorname{ht}\mathfrak{p} = 1$ for every $\mathfrak{p} \in \operatorname{Ass} R/(r)$, so, by the prime avoidance lemma, $\mathfrak{m} \not\subset \cup_{\mathfrak{p}\in \operatorname{Ass} R/(r)}\mathfrak{p}$. Hence there exists $r' \in \mathfrak{m}$ that is a non-zero-divisor on $R/(r)$. Therefore r, r' is an R-regular sequence. □

C.12. **Proposition**. *Let $(R, \mathfrak{m})$ be a two-dimensional noetherian local domain and S its integral closure in a finite separable extension field of its fraction field. Then S is a Cohen-Macaulay R-module.*

Proof. We need to show that $\operatorname{depth}_{\mathfrak{m}}(S) = 2$; since $\dim S = 2$, it suffices to show that $\operatorname{depth}_{\mathfrak{m}}(S) \geq 2$. Let $\mathfrak{n}_1, \dots, \mathfrak{n}_s$ be the maximal ideals of S. Since S is integral over R, we see that $\operatorname{ht}\mathfrak{n}_i = 2$ for every i and that $\sqrt{\mathfrak{m}S} = \mathfrak{n}_1 \cap \cdots \cap \mathfrak{n}_s$. Hence it suffices to show that

$$\mathrm{H}^i_{\mathfrak{n}_1\cap\cdots\cap\mathfrak{n}_s}(S) = 0$$

for $i = 0, 1$, for which it suffices to show that

$$\mathrm{H}^i_{\mathfrak{n}_1\cap\cdots\cap\mathfrak{n}_s}(S)_{\mathfrak{n}_j} = 0$$

for $i = 0, 1$ and $j = 1, \dots, s$. This is indeed true since

$$\mathrm{H}^i_{\mathfrak{n}_1\cap\cdots\cap\mathfrak{n}_s}(S)_{\mathfrak{n}_j} = \mathrm{H}^i_{\mathfrak{n}_j S_{\mathfrak{n}_j}}(S_{\mathfrak{n}_j})$$

for every i and j and $S_{\mathfrak{n}_j}$ is a two-dimensional Cohen-Macaulay ring for every j. □

C.13. **Theorem** (Auslander-Buchsbaum formula). *Let $(R, \mathfrak{m})$ be a noetherian local ring and M a finitely generated R-module of finite projective dimension. Then*

$$\operatorname{pd}_R(M) + \operatorname{depth} M = \operatorname{depth} R.$$

C.14. **Definition**. A noetherian local ring $(R, \mathfrak{m})$ is said to be a *regular local ring* if $\dim R = \operatorname{rk}_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$.

C.15. **Proposition**. *Let $(R, \mathfrak{m})$ be a d-dimensional regular local ring and $r_1, \dots, r_d$ be a minimal generating set for $\mathfrak{m}$. Then $r_1, \dots, r_d$ is an R-regular sequence. In particular, every regular local ring is Cohen-Macaulay.*

Proof. The key point is that regular local rings are domains; see [Eis95, 10.14]. We induct on dimension to prove the proposition, assuming the above fact. The proposition is true when $d = 1$. Let $d > 1$ be an integer and assume that the assertion holds for all regular local rings of dimension $\leq d-1$. Since R is a domain, r_1 is a non-zero-divisor on R. Write $R' = R/(r_1)$ and $\mathfrak{m}' = \mathfrak{m}R'$. Then $R'/\mathfrak{m}' \simeq R/\mathfrak{m}$ and $\operatorname{rk}_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = \operatorname{rk}_{R'/\mathfrak{m}'}(\mathfrak{m}'/\mathfrak{m}'^2) + 1$. If $d' := \dim R' < d-1$, then there would exist $r'_1, \dots, r'_{d'} \in \mathfrak{m}'$ such that $\sqrt{(r'_1, \dots, r'_{d'})R'} = \mathfrak{m}'$. Lifting them to R, we would get d' elements, which along with r_1 form an $\mathfrak{m}$-primary ideal, implying that $\dim R < d$, a contradiction. Hence $d' = d - 1 = \operatorname{rk}_{R'/\mathfrak{m}'}(\mathfrak{m}'/\mathfrak{m}'^2)$, so R' is a regular local ring. By induction, R' is Cohen-Macaulay, so $r_1, \dots, r_d$ is an R-regular sequence. □

C.16. **Proposition**. *Let R be a regular local ring. Then for every finitely generated R-module M,* $\operatorname{pd}_R(M) \leq \dim R$.

Proof. Let $d = \dim R$ and $r_1, \dots, r_d$ be a minimal generating set for the maximal ideal $\mathfrak{m}$ of R. Write $\Bbbk = R/\mathfrak{m}$. It follows from Proposition C.4 that the Koszul complex $K_\bullet :=$

$K_\bullet(r_1,\ldots,r_d)$ is a free resolution of $\Bbbk$, so $\operatorname{pd}_R(\Bbbk) \leq d$. (In fact, Since $\operatorname{Im}(K_i \longrightarrow K_{i-1}) \subseteq \mathfrak{m}K_{i-1}$, it is a minimal free resolution of $\Bbbk$, so $\operatorname{pd}_R(\Bbbk) = d$.) Therefore, by (B.2),

$$\operatorname{pd}_R(M) = \sup\{i \mid \operatorname{Tor}_i^R(M,\Bbbk) \neq 0\} \leq d.$$

□

C.17. **Proposition.** *Let R be a two-dimensional regular domain and S its integral closure in a finite separable extension field of its fraction field. Then S is a projective R-module.*

Proof. Since we want to show that $S_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module for every maximal ideal $\mathfrak{m}$ of R, we may localize R at a maximal ideal and assume that $(R,\mathfrak{m})$ is a two-dimensional regular local ring. Note that S is a finitely generated R-module. By Proposition C.12, S is a two-dimensional Cohen-Macaulay R-module. Hence $\operatorname{depth}_\mathfrak{m} S = 2$. Since R a two-dimensional Cohen-Macaulay ring (Proposition C.15), $\operatorname{depth} R = 2$. Hence $\operatorname{pd}_R(S) = 0$, i.e., S is free. □

References

[AB59] M. Auslander and D. A. Buchsbaum. On ramification theory in noetherian rings. *Amer. J. Math.*, 81:749–765, 1959. 1, 15, 17, 18, 19

[Art91] M. Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991. 1

[Ben93] D. J. Benson. *Polynomial invariants of finite groups*, volume 190 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993. 18

[Ber61] R. Berger. über verschiedene Differentenbegriffe. *S.-B. Heidelberger Akad. Wiss. Math.-Nat. Kl.*, 1960/61:1–44, 1960/1961. 1

[Bou98] N. Bourbaki. *Algebra I. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation [MR0979982 (90d:00002)]. 3

[Bou12] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitre et anneaux semi-simples*. Springer, Berlin, 2012. Second revised edition of the 1958 edition [MR0098114]. 24

[CE99] H. Cartan and S. Eilenberg. *Homological algebra*. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1999. With an appendix by David A. Buchsbaum, Reprint of the 1956 original. 24

[Eis95] D. Eisenbud. *Commutative algebra, with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. 1, 9, 11, 13, 17, 18, 20, 26, 29

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. 4

[HS06] C. Huneke and I. Swanson. *Integral closure of ideals, rings, and modules*, volume 336 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006. 9

[ILL+07] S. B. Iyengar, G. J. Leuschke, A. Leykin, C. Miller, E. Miller, A. K. Singh, and U. Walther. *Twenty-four hours of local cohomology*, volume 87 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. 28

[Kun86] E. Kunz. *Kähler differentials*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1986. 1, 11

[Mat80] H. Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980. 1

[Mat89] H. 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. 1, 8, 11

[Ser00] J.-P. Serre. *Local algebra*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. Translated from the French by CheeWhye Chin and revised by the author. 8, 9

[SS74] G. Scheja and U. Storch. *Lokale Verzweigungstheorie*. Institut des Mathématiques, Université de Fribourg, Fribourg, 1974. 1

Chennai Mathematical Institute, Siruseri, Tamilnadu 603103. India
Email address: mkummini@cmi.ac.in