Notes on Characteristic p commutative algebra
Math 7830 - Spring 2017

Karl Schwede

Department of Mathematics, University of Utah, Salt Lake City, UT 84112

E-mail address: schwede@math.utah.edu

CHAPTER 1

Frobenius and Kunz's theorem

These are notes for Math 7830, taught by Karl Schwede in Spring 2017.

Acknowledgements: The author would like to thank all the students in the class for stimulating discussions (and pointing out slicker proofs on the fly). He also thanks Pinches Dirnfeld for correcting some typos in an earlier draft of these notes.

1. Rings of interest and Frobenius

Setting 1.1. We will be working with rings (commutative with unity). These rings are usually Noetherian. Recall that a Noetherian ring is called *local* if it has a single unique maximal ideal.

We start with some examples of the types of rings we are interested in.

Example 1.2.
(a) $\mathbb{C}[x_1, \ldots, x_n]$, we can view this as polynomial functions on $\mathbb{C}^n$.
(b) $k[x_1, \ldots, x_n]$ ($k = \overline{k}$), we can view this as polynomial functions on k^n.
(c) $k[x, y]/\langle x^3 - y^2 \rangle$, ($k = \overline{k}$). These are polynomial functions on k^2 but we declare two functions to be the same if they agree where $x^3 = y^2$.
(d) $k[x_1, \ldots, x_n]/I$ ($k = \overline{k}$, $I = \sqrt{I}$). These are polynomial functions on k^n but we declare two functions to be equal if they agree on $V(I)$.

Let's now work in characteristic $p > 0$. The special thing about rings in characteristic $p > 0$ is that they have a Frobenius morphism, $F : R \longrightarrow R$ which sends $r \mapsto r^p$.

Lemma 1.3. *$F : R \longrightarrow R$ is a ring homomorphism.*

Proof. Since R is commutative, $F(rr') = (rr')^p = r^p r'^p = F(r)F(r')$. The additive part is slightly trickier, $F(r + r') = (r + r')^p = r^p + \binom{p}{1} r^{p-1} r' + \ldots + \binom{p}{p-1} r r'^{p-1} + r'^p$. Since R has characteristic p, all of the mixed terms (the foiled terms) vanish. Hence $F(r + r') = r^p + r'^p = F(r) + F(r')$. □

The Frobenius turns out to be a very useful tool in characteristic $p > 0$ algebra (and algebraic geometry) as we will see throughout the semester. For now, let's explore what this Frobenius map means.

Lemma 1.4. *Frobenius is injective if and only if R is reduced (has no nilpotents).*

Proof. Suppose first that Frobenius is injective and that $x^n = 0 \in R$, we will show that $x = 0$. Since $x^n = 0$, we know that $x^{p^e} = 0$ for some integer $e > 0$ (so that $p^e \geq n$). But $F^e = F \circ F \circ \cdots \circ F$ sends $x \mapsto x^{p^e} = 0$, and hence $x = 0$ as desired.

Conversely, if R is reduced, F is obviously injective because $F(x) = x^p = 0$ implies that $x = 0$. $\square$

Remark 1.5. In our examples above, the Frobenius morphism is almost never surjective.

1.1. Other ways to think about the Frobenius.

$R^p \subseteq R$**:** Let R be a reduced ring (for example, a domain) and let R^p denote the subring of pth powers of R. Then the map $R \longrightarrow R^p$ which sends $r \longrightarrow r^p$ is a ring isomorphism. Hence the Frobenius map $F : R \longrightarrow R$ factors through $R^p \hookrightarrow R$, and in fact can be identified with that inclusion.

$R \subseteq R^{1/p}$**:** Again let R be a domain (or a reduced ring). Let $R^{1/p}$ denote the ring of pth roots of all elements of R (inside an algebraic closure of the fraction field of R). Again $R^{1/p}$ is abstractly isomorphic to R via the map $R^{1/p} \longrightarrow R$ which sends $x \mapsto x^p$. In particular the Frobenius on $R^{1/p}$ has image R (inside $R^{1/p}$). Hence F can also be viewed as the inclusion $R \subseteq R^{1/p}$.

If $I \subseteq R$ is an ideal, then we can also write $I^{1/p}$ to be the pth roots of elements of I, note this is the image of I under the identification $R \leftrightarrow R^{1/p}$ which sends $r \mapsto r^{1/p}$.

F_*R**:** Whenever we have a ring homomorphism $f : R \longrightarrow S$, we can view S as an R-module via f $(r.s = f(r)s)$. Hence we can view R as an R-module via Frobenius. It can be confusing to write R for this module. There are a several options.

(a) $R^{1/p}$ works (at least when R is reduced).
(b) Otherwise, some people use F_*R (this borrows from sheaf theoretic language).

More generally $F_*\bullet$ is a functor (the restriction of scalars functor), and so we can apply it to any R module. Indeed, if M is an R-module then F_*M is the R-module which is the same as R as an Abelian group but such that if $r \in R$, and $m \in F_*M$, then $r.m = r^p m$. Because it can be confusing to remember which module m is in, sometimes we write F_*m instead of m, then $r.F_*m = F_*r^p m$.

We will switch between these descriptions freely.

Example 1.6 (Polynomial ring in one variable)**.** Consider $R = \mathbb{F}_p[x]$. Then R is a free R^p-module of rank p with basis $1, x, \ldots, x^{p-1}$. Equivalently, $R^{1/p}$ is a free R-module with basis $1, x^{1/p}, \ldots, x^{(p-1)/p}$. Finally, F_*R is a free R-module with basis $1, x, \ldots, x^{p-1}$. To avoid confusion, we frequently denote this basis by $F_*1, F_*x, \ldots, F_*x^{p-1}$ even though F_*, as a functor, doesn't act on elements exactly.

Example 1.7 (Polynomial ring in n variables)**.** Consider $R = \mathbb{F}_p[x_1, \ldots, x_n]$. Then R is a free R^p-module of rank p^n with basis $\{x_1^{a_1} \cdots x_n^{a_n} \mid 0 \leq a_i \leq p-1\}$. Likewise

$R^{1/p}$ is a free R-module with basis $\{x_1^{\frac{a_1}{p-1}} \cdots x_n^{\frac{a_n}{p-1}} \mid 0 \leq a_i \leq p-1\}$, similarly with F_*R as an R-module.

If we iterate Frobenius $F^e : R \longrightarrow R$, then we can also view R as an R-module via e-iterated Frobenius.

Exercise 1.1. Write down a basis for $F^e_*\mathbb{F}_p[x_1, \ldots, x_n]$ over $\mathbb{F}_p[x_1, \ldots, x_n]$.

Interestingly enough, the situation is more complicated for non-polynomial rings.

Example 1.8. Consider $R = \mathbb{F}_p[a, b]/\langle a^3 - b^2\rangle = \mathbb{F}_p[x^2, x^3] \subseteq \mathbb{F}_p[x]$. Let's try to understand the structure of $R^{1/p}$ as an R-module at least for some specific p.

We begin in the case that $p = 2$. $R^{1/p} = \mathbb{F}_p[x, x^{3/2}]$. Let's try to write down a minimal set of monomial generators of $R^{1/p}$ over R. So a first computation suggests that we need $1, x, x^{3/2}, x^{5/2}$, in particular we need at least four elements and it is easy to see that these are enough. On the other hand, $R^{1/p}$ cannot be a free module of rank 4 since if $R^{1/p} = R^{\oplus d}$ then if $W = R \setminus \{0\}$,

$$W^{-1}R^{1/p} = ((W^p)^{-1}R)^{1/p} = \mathbb{F}_p(x)^{1/p}$$

since any fraction of $k(x)$ can be written as $f(x)/g(x) = f(x)g(x)^{p-1}/g(x)^p \in (W^p)^{-1}R$. But $\mathbb{F}_p(x)^{1/p}$ has rank 2 as a $\mathbb{F}_p(x)$-module. Thus it can't be free since if $R^{1/p}$ needs three generators, if free it must be $R \oplus R \oplus R$, so $W^{-1}R^{1/p}$ would be isomorphic to $k(x) \oplus k(x) \oplus k(x)$.

Ok, how do we really check that $R^{1/p}$ needs at least 4 generators in characteristic p (maybe there is a more clever way to pick just two generators)? One option is to localize. If M is a module which can be generated by d elements, then for any multiplicative set W, $W^{-1}M$ can also be generated by d elements (why?) So let's let W be the elements of R not contained in $\langle x^2, x^3\rangle$. Set $S = W^{-1}R$. Then it's enough to show that $S^{1/p}$ is not a free S-module. Note S is local with maximal ideal $\mathfrak{m} = \langle x^2, x^3\rangle$. So consider $S^{1/p}/\mathfrak{m}S^{1/p}$, this is a $\mathbb{F}_p = S/\mathfrak{m}$-module of rank equal to the number of generators. We rewrite it as

$$S^{1/p}/\mathfrak{m}S^{1/p} = S^{1/p}/\langle x^2, x^3\rangle_{S^{1/p}}$$

and then obviously $1, x, x^{3/2}, x^{5/2}$ are nonzero in the quotient and they are linearly independent over k since they are different degree, and so $R^{1/p}$ has at least 3 generators as an R-module.

Exercise 1.2. If $R = k[x^2, x^3]$, verify that $R^{1/p}$ is not a free R-module for any prime p.

Our work above leads us to a lemma.

Lemma 1.9. *Suppose R is a ring and W is a multiplicative set. In this case, $W^{-1}F^e_*R \cong F^e_*(W^{-1}R)$ where the second F^e_* can be viewed as either as an $W^{-1}R$-module or as an R-module. This can be viewed as either an isomorphism of rings or of F^e_*R-modules.*

Note this is the same $W^{-1}R^{1/p^e} \cong (W^{-1}R)^{1/p^e}$ if these terminologies make sense (ie, R is a domain).

Proof. There is an obvious map $W^{-1}F^e_*R \longrightarrow F^e_*(W^{-1}R)$ which sends $1/g.F^e_*r \mapsto F^e_*(r/g^{p^e})$. It is certainly surjective by the argument above since

$$F_*(x/g) = F_*(xg^{p^e-1}/g^{p^e}) = 1/g.F^e_*xg^{p^e-1}$$

it is also easily verified to be linear in all relevant ways. Thus we simply need to check that it is injective. Hence suppose that $F^e_*(r/g^{p^e}) = 0$. This means that there exists $h \in W$ such that $hr = 0$. We want to show that $1.F_*r = 0$ as well in $W^{-1}F^e_*R$. But to show that it suffices to show that $h^{p^e}r = 0$ which obviously follows from $hr = 0$. $\square$

Finally, we will frequently extend ideals via Frobenius, and so we need a notation for that.

Notation 1.10. Given an ideal $I = \langle f_1, \dots, f_n \rangle \subseteq R$, we write $I^{[p^e]} := \langle f_1^{p^e}, \dots, f_n^{p^e} \rangle$. Note that

$$I \cdot R^{1/p^e} = (I^{[p^e]}R)^{1/p^e} \text{ and } I \cdot F^e_*R = F^e_*I^{[p^e]}.$$

1.2. Frobenius and Spec. Remember, associated to any ring R there is $\operatorname{Spec} R$, the set of prime ideals. It is given the Zariski topology (the set of primes containing any fixed ideal I is closed). To any ring homomorphism $f : R \longrightarrow S$, note we get a (continuous) map $\operatorname{Spec} S \longrightarrow \operatorname{Spec} R$ which sends $Q \in \operatorname{Spec} S$ to $f^{-1}(Q) \in \operatorname{Spec} R$.

Proposition 1.11. *The Frobenius morphism $F : R \longrightarrow R$ induces the identity map on* $\operatorname{Spec} R$.

Proof. Choose $Q \in \operatorname{Spec} R$. Since Q is an ideal $F(Q) \subseteq Q$. Thus $Q \subseteq F^{-1}(Q)$. Conversely, if $x \in F^{-1}(Q)$, then $x^p \in Q$ and so since Q is prime and hence radical, $x \in Q$. $\square$

The Frobenius is a morphism that acts as the identity on points of Spec but acts by taking powers/roots on functions.

2. Regular rings

Commutative algebra can be viewed as "local" algebraic geometry. If you are studying manifolds locally, you are going to be pretty bored, but in algebraic geometry, not everything is a manifold, so we have to study a lot of "singularities". To talk about singularities, we need to have some variant of tangent spaces / some variant of dimension.

Definition 2.1. The *Krull dimension* of a ring R is defined to be the maximal length n of a chain of prime ideals

$$P_0 \subseteq P_1 \subseteq P_2 \subseteq \dots \subseteq P_n \subsetneq R.$$

More generally, given any prime ideal Q, the height m of Q is the maximal length of a chain of prime ideals

$$P_0 \subseteq P_1 \subseteq P_2 \subseteq \dots \subseteq P_m = Q.$$

Example 2.2. Here are some examples of dimension.

(a) The dimension of a field k is zero, as it has only one prime ideal $\langle 0\rangle$. Notice that $\operatorname{Spec} k$ is a single point.
(b) The dimension of a PID (such as $k[x]$) is one since nonzero prime ideals are incomparable. Notice that if $k = \overline{k}$ then $\operatorname{Spec} k$ is a copy of k plus the zero ideal (the generic point).
(c) The dimension of $k[x, y]$ is 2 assuming k is a field. A maximal chain of prime ideals is $0 \subseteq \langle x\rangle \subseteq \langle x, y\rangle$.

We recall some facts about dimension, most of which are easy to prove.

Lemma 2.3. *Suppose R is a ring.*

(a) For any ideal I, $\dim R \geq \dim R/I$.
(b) For any multiplicative set W, $\dim R \geq \dim W^{-1}R$.
(c) If $(R, \mathfrak{m})$ is a Noetherian local ring, then $\dim R$ is finite and

$$\dim R = \textit{ least number of generators of an ideal } I \textit{ with } \sqrt{I} = \mathfrak{m}.$$

(d) If R is a Noetherian local ring and x is not a zero divisor, then $\dim R - 1 \geq \dim(R/\langle x\rangle)$.
(e) If R is a domain of finite type over a field and $Q \in \operatorname{Spec} A$, then

$$\dim A = \textit{ height} Q + \dim R/Q.$$

(this condition is close to something called being catenary*, not all rings satisfy it?!?!?)*

Definition 2.4. A local (implicitly Noetherian) ring $(R, \mathfrak{m}, k)$ is called *regular* if $\mathfrak{m}$ can be generated by $\dim R$ number of elements.

Note the minimal number of generators of $\mathfrak{m} = \dim_k \mathfrak{m}/\mathfrak{m}^2$ by Nakayama's lemma. Hence it seems reasonable to study $\mathfrak{m}/\mathfrak{m}^2$.

Proposition 2.5. *Suppose that $k = \overline{k}$, $R = k[x_1, \ldots, x_n]/I$ is a domain and that $A = R_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m} \subseteq R$. Then $\mathfrak{m}/\mathfrak{m}^2$ is canonically identified with the dual of the tangent space of $V(I) \subseteq k^n$ at the point corresponding to $\mathfrak{m}$.*

PROOF. Before proving this, let's fix our definition of the tangent space of $V(I)$ at $P = V(\mathfrak{m})$ to be the k-vector space of derivations at P. Remember, the set of derivations at P is the set of k-linear functions $A \longrightarrow k$ which satisfy a Leibniz rule (note, A is basically germs of functions at P). Note if $f, g \in \mathfrak{m}$ and T is a derivation, then $T(fg) = f(P)T(g) + g(P)T(f)$ and so $T(fg) = 0$ since $f(P) = g(P) = 0$. It follows from the same argument that $T(\mathfrak{m}^2 A) = 0$.

On the other hand, consider derivations acting on constants $T(1) = T(1 \cdot 1) = 1T(1) + 1T(1) = 2T(1)$. Hence $T(1) = 0$. Thus a derivation is completely determined by its action on $\mathfrak{m}/\mathfrak{m}^2$. In particular, derivations are k-linear maps $\mathfrak{m}/\mathfrak{m}^2 \longrightarrow k$ satisfying a Leibniz rule. But all k-linear maps $\mathfrak{m}/\mathfrak{m}^2 \longrightarrow k$ satisfy a Leibniz rule, and so the set of derivations is just the k-vector space dual of $\mathfrak{m}/\mathfrak{m}^2$. □

In other words, the dimension of the tangent space is just $\dim_k \mathfrak{m}/\mathfrak{m}^2$. Thus to call a ring regular is exactly the same as requiring the tangent space to have the same dimension as the ambient space (the Spec of the germ of functions).

Fortunately, for most rings there is a convenient way to check whether a local ring is regular (rather than messing about with derivations).

Proposition 2.6 (Essentially taken from [**Har77**])**.** *Suppose $k = \overline{k}$ and $R = k[x_1, \dots, x_n]/I = S/I$ is a domain with $I = \langle f_1, \dots, f_t \rangle$. If $P \subseteq R$ is a maximal ideal then R_P is regular if and only if the Jacobian matrix $||(\partial f_i/\partial x_j)(P)||$ has rank $n - r$ where $r = \dim R$.*

Proof. Let $\mathfrak{m} = \langle g_1 = x_1 - a_1, \dots, g_n = x_n - a_n \rangle$ be the ideal corresponding to P in the polynomial ring S. Consider the map $\rho : S \longrightarrow k^n$ defined by

$$\rho(f) = \Big(\frac{\partial f}{\partial x_1}(P), \dots, \frac{\partial f}{\partial x_n}(P) \Big).$$

Note $\rho(g_i)$ form a basis for k^n and that $\rho(\mathfrak{m}^2) = 0$. Hence we get $\rho : \mathfrak{m}/\mathfrak{m}^2 \longrightarrow k^n$. This is an isomorphism (by direct computation, we are still in the polynomial ring setting). Now, $\rho(I)$ has k-vector space dimension equal to the rank of the Jacobian matrix at that point. Thus the rank of the Jacobian matrix is the same as $\dim_k (I + \mathfrak{m}^2)/\mathfrak{m}^2$.

The dimension of the tangent space of $V(I)$ at P however is

$$\dim_k (\mathfrak{m}/I)/(\mathfrak{m}/I)^2 = \dim_k (\mathfrak{m}/(\mathfrak{m}^2 + I)).$$

It follows that

$$n = \dim_k(\mathfrak{m}/(\mathfrak{m}^2+I)) + \dim_k(I+\mathfrak{m}^2)/\mathfrak{m}^2 = (\text{tangent space dimension}) + (\text{Jacobian rank}).$$

The result follows immediately. □

Remark 2.7 (Warning!)**.** This only works over algebraically closed fields since we can write their maximal ideals in a very special way.

The above gets us a way to identify the locus where a ring (of finite type over an algebraically closed field) is regular.

Algorithm 2.8. Given $k = \overline{k}$ and a domain $R = k[x_1, \dots, x_n]/I$ of dimension r, compute the following algorithm to find a canonical ideal defining the locus where R is not regular (where it localizations are not regular).

(a) Let $M = ||\partial f_i/\partial x_j||$ denote the Jacobian matrix where $I = \langle f_1, \dots, f_t \rangle$.
(b) Let J the ideal defined by the determinants of all $(n - r) \times (n - r)$-minors of J.
(c) $J + I$ is the desired ideal.

By the Nullstellensatz, a maximal ideal contains $J + I$ if and only if it is in $V(I)$ and if $M(P)$, the evaluation of M at P, has rank $< n - r$.

Example 2.9. Consider $k[x, y, z]/\langle x^2y - z^2 \rangle$, a ring of dimension 2. The Jacobian matrix has only three entries, $2xy, x^2, 2z$, and we want to form the ideal made up by the 1×1 determinants. $J + I = \langle 2xy, x^2, 2z, x^2y - z^2 \rangle$. We have two cases.

If $\operatorname{char} k = 2$, $J + I = \langle x^2, z^2\rangle$. If $\operatorname{char} k \neq 2$, then $J + I = \langle xy, x^2, z\rangle$. Notice that in both cases, the radical of the ideal $\sqrt{J + I} = \langle x, z\rangle$, so the singular *locus* is the same, even though the Jacobian ideals are somewhat different.

However, it can even happen that an equation can define a ring which is singular in some characteristics but nonsingular in others.

Example 2.10. Consider $k = \mathbb{F}_p(t)$ and $R = k[x]/\langle x^p - t\rangle$. Obvious R is regular since it is a field $\cong k(t^{1/p})$. The Jacobian matrix has a single entry, $\frac{\partial}{\partial x} x^p - t = 0$ and hence the rank of the Jacobian matrix is 0. On the other hand $n = 1$ since there is one variable and $r = 0$ since a field has dimension zero. In particular,

$$0 = (\text{Jacobian rank}) \neq 1 - 0 = 1.$$

Definition 2.11. A Noetherian ring is called *regular* if all of its localizations at prime ideals are regular local rings.

This is a bit confusing, since it is not clear yet whether a regular local ring satisfies this property.

Theorem 2.12 (Serre, Auslander-Buchsbaum)**.** *If R is a regular local ring and $Q \in \operatorname{Spec} R$ is a prime ideal, then R_Q is a regular local ring.*

The point is that a Noetherian local ring is regular if and only if it has finite global dimension (the projective dimension of every module is finite and in fact $\leq \dim$).

Exercise 2.1. Use the fact that a Noetherian local ring is regular if and only if it has finite global dimension to prove that if R is a regular local ring, then so is R_Q for any $Q \in \operatorname{Spec} R$.

Here are some facts about regular rings which we will use without proof (including the one just mentioned above). Recall first the following definitions.

Definition 2.13. An R-module M is called *flat* if the functor $\_\_ \otimes_R M$ is (left) exact. A module M is called *projective* if the functor $\operatorname{Hom}_R(M, \_\_)$ is (right) exact.

Theorem 2.14. *(a) A regular ring is normal*[1].

(b) If R is regular so is $R[X]$ and $R[\![x]\!]$.

(c) A regular local ring is a UFD.

(d) If $(A, \mathfrak{m}) \subseteq (B, \mathfrak{n})$ is a local[2] *extension of Noetherian local rings with A regular and B Cohen-Macaulay (for example, regular) and if we have $\dim B = \dim A + \dim(B/\mathfrak{m}B)$, then B is a flat A-module.*

(e) A local ring $(R, \mathfrak{m})$ is regular if and only if the global dimension of R is finite (in other words, the projective dimension of any module is finite, and in particular $\leq \dim R$. It is sufficient to find the global dimension of $k = R/\mathfrak{m}$.).

PROOF. See for example [**Mat89**, Theorem 19.2, Theorem 19.4, Theorem 19.5, Theorem 20.3, Theorem 23.1]. □

[1]This means that R is its own integral closure in its ring of fractions, recall $x \in K(R)$ is integral over R if it satisfies a monic equation $x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$ for $r_i \in R$.

[2]This just means that $\mathfrak{m} \subseteq \mathfrak{n}$, note $\mathbb{Z} \subseteq \mathbb{Q}$ is not local.

Let's give some examples which show that the conditions of (d) are sharp.

Example 2.15 (Non-flat local extension with the wrong dimensions)**.** Consider $R = k[x,y]_{\langle x,y\rangle} \subseteq k[x, y/x]_{\langle x, y/x\rangle} = S$. It is easy to check that this is a local extension since $\langle x, y/x\rangle_S \cap R$ contains both x and Y and so must equal $\langle x, y\rangle_R$. Now, $\dim R = 2$ (since we just localize $\mathbb{A}^2$ at the origin) and likewise $\dim S = 2$ since S is abstract isomorphic to R. Finally, let $\mathfrak{m} = \langle x, y\rangle_R$ and consider $\mathfrak{m}S = \langle x, y\rangle_S = \langle x\rangle_S = xS$. Thus $S/\mathfrak{m}S = S/xS = k[y/x]$ and so $\dim S/\mathfrak{m}S = 1$. Thus note that

$$2 = \dim S \neq \dim R + \dim(S/\mathfrak{m}S) = 2 + 1 = 3$$

and so Theorem 2.14(d) does not apply. Let's next verify that S is *not* a flat R-module. Consider the injection of R-modules,

$$k[y] = R/xR \hookrightarrow R/xR = k[y].$$

Example 2.16 (Non-flat local extensions where the base is not regular)**.** Consider $R = k[x^2, xy, y^2]_{\langle x^2, xy, y^2\rangle} \subseteq k[x,y]_{\langle x,y\rangle} = S$ and set $\mathfrak{m} = \langle x^2, xy, y^2\rangle_R$ and $\mathfrak{n} = \langle x, y\rangle_S$. We view S as an R-module.

First note that $2 = \dim S = \dim R + \dim(S/\mathfrak{m}S) = 2 + 0$. On the other hand R is not smooth since $\dim(\mathfrak{m}/\mathfrak{m}^2) = 3 > 2$.

Now we show that S is not a free R-module (next lecture, we will see that flat and locally free are equivalent for finitely generated modules, so this is relevant). Indeed, consider $S/\mathfrak{m}S = S/\langle x^2, xy, y^2\rangle_S$, this is clearly a 3-dimensional k-vector space (with basis $\{\overline{1}, \overline{x}, \overline{y}\}$) and so S needs at least 3 generators to generate as an R-module. On the other hand when we work at the generic point, consider $k(x^2, xy, y^2) \subseteq k(x,y)$. Note that $k(x^2, xy, y^2) = k(x^2, xy)$ since $y^2 = (xy)^2/x^2$ and hence we only need consider $k(x^2, xy) \subseteq k(x,y)$. This is obviously a rank 2 field extension since we only need to adjoin x which satisfies the quadratic polynomial $X^2 - x^2$. In particular, we see that S is not a free R module since it requires 3 generators but has generic rank 2.

Our goal for the short term is to prove the following theorem of Kunz.

Theorem 2.17 (Kunz)**.** *If R is a Noetherian ring of characteristic $p > 0$, then R is regular if and only if F_*R is a flat R-module.*

3. Some notes on Kunz' theorem and the easy direction

Remember, we are trying to show that R is regular if and only if F_*R is a flat R-module. We will give two proofs of the easy direction (that regular implies flat). The first is quite easy but not very illuminating (especially since it relies on facts we haven't proven). Second, we will give essentially Kunz's original proof which I think yields quite a bit more intuition.

Proof #1. We suppose that R is regular and will show that $R^{1/p}$ is a flat R-module. Note that $(R^{1/p})_{\mathfrak{m}} = (R_{\mathfrak{m}})^{1/p}$ since inverting a pth power is the same as inverting the element. Thus, since flatness can be checked locally, we may localize R (and $R^{1/p}$) at a maximal ideal and from here on out assume that $(R, \mathfrak{m})$ is local.

Next consider the extension $R \subseteq R^{1/p}$. This is a local extension since $\mathfrak{m} \subseteq \mathfrak{m}^{1/p}$ and both R and $R^{1/p}$ are regular rings. It follows from Theorem 2.14(d) that $R^{1/p}$ is a flat R module and so we are done. □

Let's consider in a bit more detail the difference between flat, projective and free modules. It is easy to see that free modules are both flat and projective (think about how Hom and $\otimes$ work).

Lemma 3.1. *If M is a projective module over a local ring $(R, \mathfrak{m})$, then M is free.*

Proof. We only prove the case when M is finitely generated, the general case is hard and due to Kaplansky.

Let $n = \dim_{R/\mathfrak{m}} M/\mathfrak{m}M$. Then, by Nakayama's lemma, we have a surjection $\kappa : R^{\oplus n} \twoheadrightarrow M$. Since M is projective, we have a map $\sigma : M \longrightarrow R^{\oplus n}$ so that $\kappa \circ \sigma : M \longrightarrow R^{\oplus n} \longrightarrow M$ is the identity (and in particular σ is injective). It follows that

$$M/\mathfrak{m}M \xrightarrow{\overline{\sigma}} (R/\mathfrak{m})^{\oplus n} \xrightarrow{\overline{\kappa}} M/\mathfrak{m}M$$

is also the identity. Thus $\overline{\sigma}$ must also be an isomorphism (since it is an injective map between vector spaces of the same dimension). Hence by Nakayama's lemma, $\sigma : M \longrightarrow R^{\oplus n}$ is also surjective. But thus σ is both injective and surjective and hence an isomorphism, which proves that M is free. □

Next let's verify that flatness is local (this was asserted without proof earlier).

Lemma 3.2. *If M is an R-module, and $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module, for every maximal ideal $\mathfrak{m} \subseteq R$, then M is flat.*

Proof. Suppose that $0 \longrightarrow A \longrightarrow B$ is an injection of R-modules. Consider $K = \ker(A \otimes M \longrightarrow B \otimes M)$, we will show that $K = 0$. Consider the exact sequence

$$0 \longrightarrow K \longrightarrow A \otimes M \longrightarrow B \otimes M,$$

since localization is exact, for every maximal ideal $\mathfrak{m} \subseteq R$, we have that

$$0 \longrightarrow K \otimes R_{\mathfrak{m}} \longrightarrow A \otimes M \otimes R_{\mathfrak{m}} \longrightarrow B \otimes M \otimes R_{\mathfrak{m}},$$

is exact. But this is the same as saying that

$$0 \longrightarrow K_{\mathfrak{m}} \longrightarrow A_{\mathfrak{m}} \otimes M_{\mathfrak{m}} \longrightarrow B_{\mathfrak{m}} \otimes M_{\mathfrak{m}}$$

is exact. Since $M_{\mathfrak{m}}$ is flat by hypothesis, this implies that $K_{\mathfrak{m}} = 0$, and this holds for every maximal ideal. Thus $K = 0$. □

Next let's show that finite flat modules are projective.

Lemma 3.3. *If R is Noetherian and M is a finite R-module that is flat, then M is projective.*

Proof. Since localization commutes with Hom from finitely presented modules, and exactness may be checked locally, we may assume that $(R, \mathfrak{m})$ is a local ring. In this case, we will show that M is free. Choose a minimal generating set for M and the corresponding surjection $R^{\oplus t} \longrightarrow M \longrightarrow 0$ with kernel K (which is finitely generated). We tensor with $R/\mathfrak{m}$ to obtain

$$\mathrm{Tor}_1(M, R/\mathfrak{m}) \longrightarrow K \otimes R/\mathfrak{m} \longrightarrow (R/\mathfrak{m})^{\oplus t} \xrightarrow{\alpha} M \otimes R/\mathfrak{m} \longrightarrow 0$$

Since we picked a minimal generating set for M, α is bijective. Since M is flat, $\mathrm{Tor}_1(M, \mathbb{R}/\mathfrak{m}) = 0$ and hence $K \otimes R/\mathfrak{m} = K/\mathfrak{m}K = 0$ and so $K = \mathfrak{m}K$. By Nakayama's lemma this implies that K is zero. □

Note we didn't really need that R was Noetherian above, we just needed M to be finitely presented.

We now give another proof of the "easy" direction of Kunz's theorem, that regular implies Frobenius is flat. We have already checked this for polynomial rings over perfect fields, and now we want to essentially reduce to that case.

To do that, we need *completion.* Suppose that R is a ring and I is an ideal. Then

$$\widehat{R} := \lim_{\leftarrow} R/I^n$$

is called the completion of R with respect to the I-adic topology (the powers of I form a neighborhood basis of 0). Most often, $(R, \mathfrak{m})$ is a local ring and we are completing with respect to the maximal ideal $\mathfrak{m}$. In this case, $R/\mathfrak{m}$ is the residue field, $R/\mathfrak{m}^2$ records first order tangent information, $R/\mathfrak{m}^3$ records second order tangent information, etc. Thus $\widehat{R}$ somehow knows all the tangent information around R.

Definition 3.4. A local ring is called *complete* if it is complete (for example, equal to its own completion) with respect to the maximal ideal.

Example 3.5. It is easy to verify that if $R = k[x_1, \dots, x_n]$ is a polynomial ring and $\mathfrak{m} = \langle x_1, \dots, x_n \rangle$ is the ideal defining the origin. Then $\widehat{R} = k[\![x_1, \dots, x_n]\!]$, formal power series in the x_i. Note this ring is still Noetherian.

Example 3.6. Consider $R = k[x, y]/\langle y^2 - x^3 + x \rangle$ and complete with respect to $\mathfrak{m} = \langle x, y \rangle$. Now, any polynomial in x, y can be rewritten, say up through some fixed degree n, as a power series only in y (for example, replace all the xs with $x^3 - y^2$, and repeat, until the x degree is too high). It follows that the completion is isomorphic to $k[\![y]\!]$ (a picture will explain why this is reasonable).

In particular, even though the completion of R is a powerseries ring in one variable, the localization $R_{\langle x,y \rangle}$ is not.

Completion should be thought of as one analog of a local analytic neighborhood (localization still remembers too much about the global geometry for some applications). In particular, the follow theorem makes this precise.

Theorem 3.7. (Cohen Structure Theorem, [**Mat89**, Section 29]) *Suppose that $(R, \mathfrak{m}, k)$ is a complete local Noetherian ring containing a field F. Then $R \cong k[\![x_1, \dots, x_n]\!]/I$. Furthermore, if R is regular then $R \cong k[\![x_1, \dots, x_n]\!]$.*

We are not going to prove this, but we will take it on faith. Note that hard part is to show that R actually contains a copy of k (this copy is not unique in characteristic $p > 0$). Also note that the x_is are a set of generators of the maximal ideal $\mathfrak{m}$.

We need one other lemma.

Lemma 3.8. [**Mat89**, Theorem 8.8] *If $(R, \mathfrak{m})$ is a local ring with completion $\widehat{R}$, then $\widehat{R}$ is a faithfully flat R-module.*

What the Cohen-Structure theorem lets us reduce the problem of flatness of F_*R over R to flatness of $F_*\widehat{R}$ over $\widehat{R}$, and for regular rings, we have just reduced to the power series case (which is essentially the same as the case of polynomial rings).

Theorem 3.9 (Kunz). *If R is Noetherian and regular then F_*R is a flat R-module.*

PROOF. Since flatness can be checked locally, as we showed above, we may assume that R is local. We know that $\widehat{R} \cong k[\![x_1, \ldots, x_n]\!]$. There is an induced map

$$\widehat{R} \longrightarrow \varprojlim (F_*R)/\mathfrak{m}^n(F_*R) = \varprojlim (F_*R)/(F_*(\mathfrak{m}^n)^{[p]}R) = F_* \varprojlim (R/(\mathfrak{m}^n)^{[p]}) \cong F_*\widehat{R}$$

where the final equality is due to the fact that $(\mathfrak{m}^n)^{[p]}$ defines the same topology of $\mathfrak{m}^n$ (the powers are cofinal with each other). Note that this map is the Frobenius map. We have the following diagram:

$$\begin{array}{ccc} \widehat{R} & \xrightarrow{F} & F_*\widehat{R} \\ \uparrow & & \uparrow \\ R & \xrightarrow[F]{} & F_*R \end{array}$$

The top horizontal arrow is flat by direct computation that we now do. Write $R = k[\![x_1, \ldots, x_n]\!]$. Then notice that $F_*R = R^{1/p} = k^{1/p}[\![x_1^{1/p}, \ldots, x_n^{1/p}]\!]$ and so we can factor $R \subseteq R^{1/p}$ as

$$k[\![x_1, \ldots, x_n]\!] \subseteq k[\![x_1^{1/p}, \ldots, x_n^{1/p}]\!] \subseteq k^{1/p}[\![x_1^{1/p}, \ldots, x_n^{1/p}]\!]$$

The first extension is flat because it is free (using the same basis you are writing down in the homework). The second extension is flat because it is just a residue field extension (technically, tensor up with $\otimes_k k^{1/p}$ and then complete again, remember completion of Noetherian rings yields flat extensions). The vertical arrows are flat since completion is always flat (note the right vertical arrow is just F_* of the left arrow). It follows that $F_*\widehat{R}$ is flat over R. We need to show that the bottom horizontal arrow is flat, this is a basic commutative algebra fact but lets prove it.

Suppose that $M' \hookrightarrow M$ injects but $M' \otimes_R F_*R \longrightarrow M \otimes_R F_*R$ does not and so let K be the nonzero kernel so that we have an exact sequence $0 \longrightarrow K \longrightarrow M' \otimes_R F_*R \longrightarrow M \otimes_R F_*R$ of F_*R-modules. We tensor this with $\_\_ \otimes_{F_*R} F_*\widehat{R}$ to obtain

$$\begin{array}{ccccccc} 0 \longrightarrow & K \otimes_{F_*R} F_*\widehat{R} & \longrightarrow & M' \otimes_R F_*R \otimes_{F_*R} F_*\widehat{R} & \longrightarrow & M \otimes_R F_*R \otimes_{F_*R} F_*\widehat{R} \\ & \updownarrow \wr & & \updownarrow \wr & & \updownarrow \wr \\ 0 \longrightarrow & K \otimes_{F_*R} F_*\widehat{R} & \longrightarrow & M' \otimes_R F_*\widehat{R} & \longrightarrow & M \otimes_R F_*\widehat{R} \end{array}$$

Since completion is *faithfully* flat, $K \otimes_{F_*R} F_*\widehat{R} \neq 0$ hence $M' \otimes_R F_*\widehat{R} \longrightarrow M \otimes_R F_*\widehat{R}$ is not injective. But the contradicts the flatness of $F_*\widehat{R}$ over R. □

4. A crash course in using derived categories

Before doing the other direction of the proof, it will be very helpful if we learn a little bit about the derived category.

In a nutshell, taking Hom and Ext is very useful, but dealing with individual cohomology groups can be a hassle.

Solution: Deal with the complexes instead!

Definition 4.1. A *complex* of R-modules (or $\mathscr{O}_X$-modules if you prefer) is a collection of $\{C^n\}_{n\in\mathbb{Z}}$ of R-modules plus maps $d^n : C^n \longrightarrow C^{n+1}$ such that $d^{i+1} \circ d^i = 0$.

$$\dots \xrightarrow{d^{-2}} C^{-1} \xrightarrow{d^{-1}} C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \dots \xrightarrow{d^{n-1}} C^n \xrightarrow{d^n} C^{n+1} \xrightarrow{d^{n+1}} \dots$$

A complex is *bounded below* if $C^i = 0$ for $i \ll 0$, it is *bounded above* if $C^i = 0$ for $i \gg 0$, and it is *bounded* if $C^i = 0$ for $|i| \gg 0$.

Remark 4.2. In a *chain complex*, the differentials take C_i to C_{i-1}, we will deal exclusively with complexes however.

There are some problems. The category of complexes isn't quite right, so we fix it. We only consider morphisms of complexes up to homotopy equivalence (two maps of complexes are homotopic if their difference is null homotopic), and we *declare* two complexes to be isomorphic if there is a map between them which gives us an isomorphism on cohomology (formally add an inverse map to our category).

Examples 4.3. Here are some examples you hopefully all are familiar with.

(a) Given a module M, we view it as a complex by considering it in degree zero (all the differentials of the complex are zero) and all the other terms in the complex.

(b) Given any complex $C^\bullet$, (like a modules viewed as a complex as above), we can form another complex by shifting the first complex $C[n]^\bullet$. This is the complex where $(C[n])^i = C^{i+n}$ and where the differentials are shifted likewise and multiplied by $(-1)^n$. Note this shifts the complex n spots to *the left*.

(c) Given a module M, and a projective resolution

$$\dots \longrightarrow P^{-n} \longrightarrow \dots \longrightarrow P^{-2} \longrightarrow P^{-1} \longrightarrow P^0 \longrightarrow M \longrightarrow 0$$

it is easy to see that there is a map $P^\bullet \longrightarrow M$ and this is a map of complexes in the sense that M is a complex via (a).

$$\begin{array}{ccccccccccccc}
\dots & \longrightarrow & P^{-n} & \longrightarrow & \dots & \longrightarrow & P^{-2} & \longrightarrow & P^{-1} & \longrightarrow & P^0 & \longrightarrow & 0 & \longrightarrow & \dots \\
 & & \downarrow & & & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & 0 & \longrightarrow & \dots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & M & \longrightarrow & 0 & \longrightarrow & \dots
\end{array}$$

This map is a quasi-isomorphism (an isomorphism in the derived category).

(d) Given a module M and an injective resolution

$$0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \dots$$

we get a map of complexes $M \to I^\bullet$

$$\begin{array}{ccccccccccc} \dots & \longrightarrow & 0 & \longrightarrow & M & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \dots \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ \dots & \longrightarrow & 0 & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow & \dots \end{array}$$

which is also a quasi-isomorphism (again viewing M as a complex via (a)).

(e) Given two modules M and N, we form $\mathbf{R}\operatorname{Hom}_R(M, N)$. This is the complex whose cohomologies are the $\operatorname{Ext}^i(M, N)$. It is computed by either taking a projective resolution of M or an injective resolution of N. Note that while you get different complexes in either of those cases, it turns out the resulting objects in the derived category are isomorphic (in the derived category).

(f) Given two modules M and N, we form $M \otimes^L_R N$, the cohomologies of this complex are the $\operatorname{Tor}^i_R(M, N)$. It is obtained by taking a projective resolution of M or N.

(g) Note that not every quasi-isomorphism between complexes is invertible. Indeed, consider

$$\begin{array}{ccccccccccc} \dots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \dots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \dots \end{array}$$

This obviously induces a quasi-isomorphism since the top row is a projective resolution of the bottom, but the map of complexes is not invertible. In the *derived* category, we formally adjoin an inverse morphism.

(h) Not every pair of complexes with isomorphic cohomologies are quasi-isomorphic, indeed consider the complexes

$$\dots \to 0 \to \mathbb{C}[x, y] \xrightarrow{0} \mathbb{C} \to 0 \to \dots$$

and

$$\dots \to 0 \to \mathbb{C}[x, y]^{\oplus} \xrightarrow{[x,y]} \mathbb{C}[x, y] \to 0 \to \dots.$$

It is easy to see that they have isomorphic cohomologies. Some discussion of the fact that these complexes are not quasi-isomorphic can be found in the responses to this question on `math.stackexchange`, [**hf**].

Remark 4.4. There are different ways to enumerate things, but complexes have maps that go left to right. Thus a projective resolution of a module M has entries only in *negative* degrees. Thus when I write $\operatorname{Tor}^i_R(M, N)$ above, the i that can have interesting cohomology are the $i \leq 0$.

Definition 4.5. The *derived category of R-modules* denoted $D(R)$ is the category of complexes with morphisms defined up to homotopy and with quasi-isomorphisms formally inverted.

If we look at the full subcategory of complexes bounded above, and then construct the derived category as above, the result is denoted by $D^-(R)$. From bounded below complexes, we construct $D^+(R)$. Finally, if the complexes are bounded on both sides the result is denoted by $D^b(R)$.

5. Triangulated categories

Derived categories are *not* an Abelian category, short exact sequences don't exist, but we have something almost as good, exact triangles. In particular, the derived category is a triangulated category.

Remark 5.1. The notation from the following axioms is taken from [**Wei94**] (you can find different notation on for instance Wikipedia).

Definition 5.2 (Triangulated categories)**.** A *triangulated category* is an additive[3] category with a fixed automorphism T equipped with a distinguished set of triangles and satisfying a set of axioms (below). A *triangle* is an ordered triple of objects (A, B, C) and morphism $\alpha : A \longrightarrow B$, $\beta : B \longrightarrow C$, $\gamma : C \longrightarrow T(A)$,

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} T(A).$$

A *morphism of triangles* $(A, B, C, \alpha, \beta, \gamma) \longrightarrow (A', B', C', \alpha', \beta', \gamma')$ is a commutative diagram

$$\begin{array}{ccccccc} A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \xrightarrow{\gamma} & T(A) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle T(f)} \\ A' & \xrightarrow[\alpha']{} & B' & \xrightarrow[\beta']{} & C' & \xrightarrow[\gamma']{} & T(A') \end{array}$$

We now list the required axioms to make a triangulated category.

(a) The triangle $A \longrightarrow A \xrightarrow{0} 0 \xrightarrow{0} T(A)$ is one of the distinguished triangles.
(b) A triangle isomorphic to one of the distinguished triangles is distinguished.
(c) Any morphism $A \longrightarrow B$ can be embedded into one of the distinguished triangles $A \longrightarrow B \longrightarrow C \longrightarrow T(A)$.
(d) Given any distinguished triangle $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} T(A)$, then both

$$B \xrightarrow{\beta} C \xrightarrow{\gamma} T(A) \xrightarrow{-T(\alpha)} T(B)$$

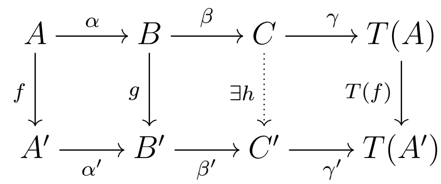
and

$$T^{-1}C \xrightarrow{-T^{-1}(\gamma)} A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

are also distinguished.

[3]Hom sets are Abelian groups and composition is bilinear.

(e) Given distinguished triangles with maps between them as pictured below, so that the left square commutes,



then the dotted arrow also exists and we obtain a morphism of triangles.

(f) We finally come to the feared *octahedral axiom*. Given objects A, B, C, A', B', C' and three distinguished triangles:

$$A \xrightarrow{u} B \xrightarrow{j} C' \xrightarrow{\partial} T(A)$$

$$B \xrightarrow{v} C \xrightarrow{x} A' \xrightarrow{i} T(B)$$

$$A \xrightarrow{v \circ u} C \xrightarrow{y} B' \xrightarrow{\delta} T(A)$$

then there exists a fourth triangle

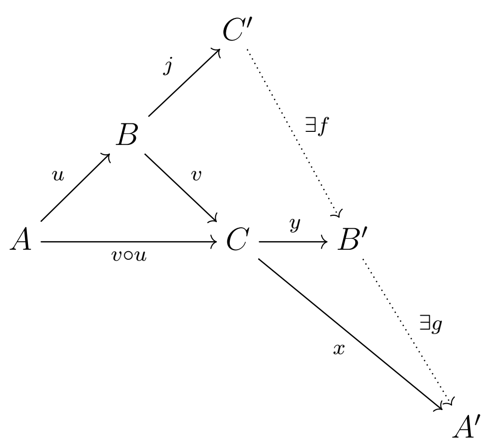
$$C' \xrightarrow{f} B' \xrightarrow{g} A' \xrightarrow{(T(j)) \circ i} T(C')$$

so that we have

$$\partial = \delta \circ f, x = g \circ y, y \circ v = f \circ j, u \circ \delta = i \circ g.$$

These can be turned into a nice octagon (with these equalities being commuting faces) that I am too lazy to LaTeX.

Remark 5.3. It is much easier to remember the octahedral axiom (without the compatibilities at least) with the following diagram.



Any of the derived categories we have discussed are triangulated categories with $T(\bullet) = \bullet[1]$. The main point is if we have a morphism of complexes, $A^\bullet \overset{\alpha}{\to} B^\bullet$, then we can always take the cone $C(\alpha)^\bullet = A[1]^\bullet \oplus B^\bullet$ with differential

$$C^i = A^{i+1} \oplus B^i \xrightarrow{-d_A^{i+1}, \alpha^i + d_B^i} A^{i+2} \oplus B^{i+1}$$

Exercise 5.1. Verify that this really is a complex.

Exercise 5.2. Suppose that $0 \longrightarrow A^\bullet \xrightarrow{\alpha} B^\bullet \xrightarrow{\beta} D^\bullet \longrightarrow 0$ is an exact sequence of complexes. Show that $D^\bullet$ is quasi-isomorphic to $C(\alpha)^\bullet$.

Then we have $A^\bullet \xrightarrow{\alpha} B^\bullet \xrightarrow{\beta} C(\alpha)^\bullet \gamma A[1]^\bullet$ a distinguished triangle where β and γ are given by maps to and projecting from the direct summands that make up $C(\alpha)^\bullet$. Note that morphisms in the derived category are more complicated than maps between complexes (since we might have formally inverted some quasi-isomorphisms) but this still is enough for our purposes since the cone of a quasi-isomorphism is exact.

Fact 5.4. Given a triangle $A^\bullet \longrightarrow B^\bullet \longrightarrow C^\bullet \longrightarrow A[1]^\bullet$ in the derived category of R-modules, taking cohomology yields a long exact sequence

$$\ldots \longrightarrow h^{i-1}(C^\bullet) \longrightarrow h^i(A^\bullet) \longrightarrow h^i(B^\bullet) \longrightarrow h^i(C^\bullet) \longrightarrow h^{i+1}(A^\bullet) \longrightarrow \ldots$$

Exercise 5.3. Verify that fact.

Exercise 5.4. Suppose that

$$A^\bullet \xrightarrow{\alpha} B^\bullet \xrightarrow{\beta} C^\bullet \xrightarrow{0} T(A^\bullet)$$

is a distinguished triangle in $D(R)$. Show that $B^\bullet \simeq_{\text{qis}} A^\bullet \oplus B^\bullet$ compatibly so that α and β are identified with the canonical inclusion and projections.

In particular, show that there exist maps $p : B^\bullet \longrightarrow A^\bullet$ and $s : C^\bullet \longrightarrow B^\bullet$ so that $p \circ \alpha$ is the identity on $A^\bullet$ and that $\beta \circ s$ is the identity on $C^\bullet$.

6. Common functors on our derived categories

Suppose we are forming the derived category $D(R)$ of the category of R-modules for some ring R. We have lots of functors we like to apply to R-modules, notably Hom and $\otimes$ but also things like Γ_I (the submodule of things killed by a power of I). Associated to any of these functors we get derived functors, as follows.

Derived functors are functors between triangulated categories which preserve the triangulation structure (ie, send triangles to triangles and commute with the $T(\bullet)/[\bullet]$ operation) and which satisfy a certain universal property which we won't need too much (see for example [**Wei94**, Section 10.5] for details). The point for us is that derived functors exist for the functors we care about.

Lemma 6.1. [**Wei94**, Corollary 10.5.7] *Suppose $F : \mathscr{M}\text{od}(R) \longrightarrow \mathscr{M}\text{od}(S)$ is an additive functor which takes R-modules to S-modules. Then the right derived functors $\mathbf{R}F : D^+(R) \longrightarrow D(S)$ are morphisms between triangulated categories and can be computed by $\mathbf{R}F(C^\bullet) = F(I^\bullet)$ where $I^\bullet$ is a complex of injectives quasi-isomorphic to $C^\bullet$. In particular, $h^i\mathbf{R}F(C^\bullet) = \mathbb{R}^i F(C^\bullet)$.*

Likewise, the left derived functors $\mathbf{L}F : D^-(R) \longrightarrow D(S)$ can be computed by $\mathbf{R}F(C^\bullet) = F(P^\bullet)$ where $P^\bullet$ is a complex of projectives quasi-isomorphic to $C^\bullet$.

If you are really Hom'ing or tensoring two complexes together, you typically need to actually compute this by forming the associated double complex and then taking the total complex, see for example page 8 of [**Wei94**]. For example if $M^\bullet$ and $N^\bullet$ are complexes made up of projectives (or at least one of them is), then the total complex of the double complex represents the object $M^\bullet \otimes^{\mathbf{L}}_R N^\bullet$.

Notably, we have

- $\mathbf{R}\operatorname{Hom}_R(A^\bullet, B^\bullet)$ can be computed by taking a complex of projectives quasi-isomorphic to $A^\bullet \in D^-(R)$ or a complex of injectives quasi-isomorphic to $B^\bullet \in D^+(R)$. Note if A, B are modules, then $h^i\mathbf{R}\operatorname{Hom}(A, B) = \operatorname{Ext}^i(A, B)$
- $A^\bullet \otimes^{\mathbf{L}}_R B^\bullet$ can be computed by taking a complex of projectives quasi-isomorphic to either $A^\bullet$ or $B^\bullet$ in $D^-(R)$. Note if A, B are modules, then $h^{-i}(A \otimes^{\mathbf{L}}_R B) = \operatorname{Tor}^R_i(A, B)$.
- For any ideal $I \subseteq R$, recall that $\Gamma_I(M) = \{m \in M \mid I^n m = 0 \text{ for some } n \gg 0\}$. Then $\mathbf{R}\Gamma_I(A^\bullet)$ is computed by finding a complex of injectives quasi-isomorphic to $A^\bullet \in D^+(R)$. Note that if A is a module, then $h^i\mathbf{R}\Gamma_I(A) = H^i_I(A)$ is just local cohomology.

The rest of the chapter is devoted to how these functors play with each other.

Theorem 6.2 (Composition of derived functors, left-exact case)**.** *Given left exact functors $G : \mathscr{M}\mathrm{od}(R) \longrightarrow \mathscr{M}\mathrm{od}(S)$ and $F : \mathscr{M}\mathrm{od}(S) \longrightarrow \mathscr{M}\mathrm{od}(T)$ (or suitable Abelian categories with enough injectives), and suppose that G sends injective objects to F-acyclic objects, then $\mathbf{R}F \circ \mathbf{R}G \cong \mathbf{R}(F \circ G)$ as functors from $D^+(R) \longrightarrow D^+(T)$.*

For a more general statement, see [**Wei94**, Theorem 10.8.2]. Things that imply the above, make a lot of the formulas we already know relating Hom and $\otimes$ and other functors hold in the derived category as well.

We list some of them here without proof, see for example [**Wei94**, Section 10.8] or [**Har66**, II, Section 5].

Proposition 6.3. *The following hold:*

(a) Let $f : R \longrightarrow S$ be a map of rings with functors $f^* : \mathscr{M}\mathrm{od}(R) \longrightarrow \mathscr{M}\mathrm{od}(S)$ defined by $f^*(M) = M \otimes_R S$ and $f_* : \mathscr{M}\mathrm{od}(S) \longrightarrow \mathscr{M}\mathrm{od}(R)$ defined by f_*N is N viewed as an R-module via restriction of scalars. Then for $A^\bullet \in D^-(R), B^\bullet \in D^-(S)$ we have

$$\mathbf{L}f^*(A^\bullet) \otimes^{\mathbf{L}}_S B^\bullet \cong A^\bullet \otimes^{\mathbf{L}}_R f_*B^\bullet.$$

This is a special case (the affine case) of the derived projection formula you might have seen in your algebraic geometry class.

(b) For $A^\bullet, B^\bullet \in D^-(R)$ and $C^\bullet \in D^+(R)$, we have

$$\mathbf{R}\operatorname{Hom}_R(A^\bullet, \mathbf{R}\operatorname{Hom}_R(B^\bullet, C^\bullet)) \cong \mathbf{R}\operatorname{Hom}_R(A^\bullet \otimes^{\mathbf{L}}_R B^\bullet, C^\bullet)$$

in $D^+(R)$. This is just derived Hom, $\otimes$ *adjointness.*

(c) *For $A^\bullet \in D^-(R)$ and $B^\bullet \in D^+(R)$ and $C^\bullet \in D^b(R)$ of bounded* Tor-*dimension (for example, bounded projective dimension), ie the projective resolution of anything in a regular ring, then*

$$\mathbf{R}\operatorname{Hom}_R(A^\bullet, B^\bullet) \otimes^{\mathbf{L}}_R C^\bullet \cong \mathbf{R}\operatorname{Hom}_R(A^\bullet, B^\bullet \otimes^{\mathbf{L}}_R C^\bullet).$$

(d) *Consider two ideals $I, J \subseteq R$ in a Noetherian ring. Then $\Gamma_I \circ \Gamma_J = \Gamma_{I+J} = \Gamma_{\sqrt{I+J}}$ as is easily checked. Next suppose that M is an injective module, we want to show that $\Gamma_J(M)$ is Γ_I-acyclic. This is normally done by showing that $\Gamma_J(M)$ is flasque and I won't reproduce it here. Thus we have that*

$$\mathbf{R}\Gamma_I \circ \mathbf{R}\Gamma_J = \mathbf{R}\Gamma_{I+J}$$

In the case case that $I \supseteq J$ we see that

$$\mathbf{R}\Gamma_I \circ \mathbf{R}\Gamma_J = \mathbf{R}\Gamma_I.$$

7. The other direction of Kunz's theorem

Recall Kunz's theorem

Theorem 7.1. *If R is a Noetherian ring of characteristic $p > 0$, then R is regular if and only if F_*R is a flat R-module.*

Earlier we proved that "regular $\Rightarrow$ F_*R is flat", and now we want to prove the converse.

Definition 7.2. Suppose R is a domain (or simply is reduced) of characteristic $p > 0$ and let $R^\infty = R^{1/p^\infty} = \bigcup_{e \geq 0} R^{1/p^e}$. This is called the *perfection* of R. If R is not reduced, we can still define

$$R^\infty = \lim_{\to} R = \lim_{\to} F^e_* R$$

where the transition maps are Frobenius.

Remark 7.3. Note that even if R is not reduced, the Frobenius map on R^∞ is injective (since if something is killed by Frobenius, it is also killed by a transition map). Hence R^∞ is reduced even R is not. In particular, Frobenius always acts bijectively on R^∞.

Example 7.4. Note that R^∞ is rarely Noetherian even if R is (even though it is easy to check that $\operatorname{Spec} R^\infty \longrightarrow \operatorname{Spec} R$ is an isomorphism). If $R = R^\infty$ then R is called *perfect*. Indeed, let $R = \mathbb{F}_p[x]$ then $R^\infty = \mathbb{F}_p[x, x^{1/p}, x^{1/p^2}, x^{1/p^3}, \ldots]$.

Lemma 7.5. [**BS15**, Lemma 3.16, Lemma 5.10] *If $R \xleftarrow{g} S \xrightarrow{h} R'$ is are surjections of Noetherian rings of characteristic $p > 0$ with induced surjection $R^\infty \xleftarrow{g^\infty} S^\infty \xrightarrow{h^\infty} R'^\infty$ of perfect rings. Then $\operatorname{Tor}^i_{S^\infty}(R^\infty, R'^\infty) = 0$ for all $i \neq 0$ or in other words*

$$R^\infty \otimes^{\mathbf{L}}_{S^\infty} R'^\infty \simeq_{qis} R^\infty \otimes_{S^\infty} R'^\infty.$$

In particular, specializing to the case $R' = R$, the multiplication map $R^\infty \otimes^{\mathbf{L}}_{S^\infty} R^\infty \longrightarrow R^\infty$ is a quasi-isomorphism.

PROOF. Let $I = \ker g = \langle f_1, \dots, f_n\rangle$ so that $R = S/I$. It is easy to see that $\ker g^\infty = \ker(S^\infty \longrightarrow R^\infty) = \langle f_1^{1/p^e}, \dots, f_n^{1/p^e}\rangle_{e\geq 0}$.

We now proceed by induction on n. Indeed, if we let $I_j = \langle f_1^{1/p^e}, \dots, f_j^{1/p^e}\rangle_{e\geq 0} \subseteq S^\infty$ and $R_j^\infty = S^\infty/I_j$, then assuming the induction hypothesis

$$R_j^\infty \otimes^{\mathbf{L}}_{S^\infty} R' \simeq_{\text{qis}} (R_j^\infty \otimes^{\mathbf{L}}_{R_{j-1}^\infty} R_{j-1}^\infty) \otimes^{\mathbf{L}}_{S^\infty} R' = R_j^\infty \otimes^{\mathbf{L}}_{R_{j-1}^\infty} (R_{j-1}^\infty \otimes^{\mathbf{L}}_{S^\infty} R') \simeq_{\text{qis}} R_j^\infty \otimes_{R_{j-1}^\infty} (R_{j-1}^\infty \otimes_{S^\infty} R')$$

where the final quasi isomorphism is just assuming our induction hypothesis twice. Hence it suffices to prove the base case that $I = \langle f\rangle$ and $I^\infty = \langle f^{1/p^e}\rangle_{S^\infty}$.

Consider the directed system

$$\{S^\infty, \cdot f^{\frac{p-1}{p^n}}\} = S^\infty \xrightarrow{\cdot f^{\frac{p-1}{p^2}}} \cdots \xrightarrow{\cdot f^{\frac{p-1}{p^{n-1}}}} S^\infty \xrightarrow{\cdot f^{\frac{p-1}{p^n}}} S^\infty \xrightarrow{\cdot f^{\frac{p-1}{p^{n+1}}}} \cdots$$

There is a map from this directed system to I^∞

$$\{S^\infty, \cdot f^{\frac{p-1}{p^n}}\} \longrightarrow I^\infty = \langle f^{1/p^e}\rangle.$$

sending s (from the nth spot) to $f^{1/p^n}a$. Note this really compatible with the maps of the directed system since $f^{1/p^{n+1}} f^{\frac{p-1}{p^{n+1}}} a = f^{1/p^n}a$. This obviously yields a surjective map

$$\mu : \varinjlim \{S^\infty, \cdot f^{\frac{p-1}{p^n}}\} \longrightarrow I^\infty.$$

Claim 7.6. *μ is an isomorphism.*

PROOF OF CLAIM. We need to show that μ is injective, note this is trivial if S is a domain. For the general case suppose that $s \in S^\infty$ (living in the nth spot) is sent to zero. This means that $f^{1/p^n}s = 0 \in S^\infty$. But then since S^∞ is perfect and reduced, $f^{1/p^{n+1}}s^{1/p} = 0$ as well, and so $f^{1/p^{n+1}}s = 0$ which proves that s is killed by a transition map (which multiplies by even more). ☐

Likewise consider $IR' = \bigcup f^{1/p^e}R'^\infty$, the ideal generated by the image of f^{1/p^e} in R'^∞ and thus the direct system

$$\{R'^\infty, \cdot f^{\frac{p-1}{p^n}}\} = R'^\infty \xrightarrow{\cdot f^{\frac{p-1}{p^2}}} \cdots \xrightarrow{\cdot f^{\frac{p-1}{p^{n-1}}}} R'^\infty \xrightarrow{\cdot f^{\frac{p-1}{p^n}}} R'^\infty \xrightarrow{\cdot f^{\frac{p-1}{p^{n+1}}}} \cdots$$

and hence a map as before

$$\nu : \varinjlim \{R'^\infty, \cdot f^{\frac{p-1}{p^n}}\} \longrightarrow I^\infty R'^\infty$$

Claim 7.7. *μ is an isomorphism.*

PROOF. The proof is the same as the previous claim. ☐

Now,

$$I^\infty \otimes^{\mathbf{L}}_{S^\infty} R'^\infty \cong \varinjlim \{S^\infty, \cdot f^{\frac{p-1}{p^n}}\} \otimes^{\mathbf{L}}_{S^\infty} R'^\infty \cong \varinjlim \{R'^\infty, \cdot f^{\frac{p-1}{p^n}}\} \cong I^\infty R'^\infty$$

and so it follows that for $i \neq 0$, $h^i\big(I^\infty \otimes^{\mathbf{L}}_{S^\infty} R'^\infty\big) = 0$. In particular, we have the map of distinguished triangles

$$\begin{array}{ccccccccc} & & I^\infty \otimes^{\mathbf{L}}_{S^\infty} R'^\infty & \longrightarrow & S^\infty \otimes^{\mathbf{L}}_{S^\infty} R'^\infty & \longrightarrow & R^\infty \otimes^{\mathbf{L}}_{S^\infty} R'^\infty & \xrightarrow{+1} & \\ & & \downarrow\sim & & \downarrow\sim & & \downarrow & & \\ 0 & \longrightarrow & I^\infty R'^\infty & \longrightarrow & R'^\infty & \longrightarrow & R^\infty \otimes_{S^\infty} R'^\infty & \longrightarrow & 0 \end{array}$$

The result follows. □

Remark 7.8. In [**BS15**], they obtained a more general statement. They started with perfect rings (that were not necessarily the perfections of Noetherian rings).

Proposition 7.9. [**BS15**, Proposition 5.31] *Let R^∞ be the perfection of a complete local ring R. Then R^∞ has finite global dimension.*

Proof. Write $R = S/I$ for $S = k[\![x_1, \dots, x_n]\!]$ and note we still have a surjection $S^\infty \to R^\infty$.

Let M be an arbitrary R^∞-module. Then

$$M = M \otimes^{\mathbf{L}}_{R^\infty} R^\infty = M \otimes^{\mathbf{L}}_{R^\infty} (R^\infty \otimes^{\mathbf{L}}_{S^\infty} R^\infty) = M \otimes^{\mathbf{L}}_{S^\infty} R^\infty$$

by Lemma 7.5. We are trying to show that $\mathbf{R}\operatorname{Hom}_R(M, N)$ has (uniformly) bounded cohomology but

$$\begin{aligned} & \mathbf{R}\operatorname{Hom}_{R^\infty}(M, N) \\ = \ & \mathbf{R}\operatorname{Hom}_{R^\infty}(M \otimes^{\mathbf{L}}_{S^\infty} R^\infty, N) \\ = \ & \mathbf{R}\operatorname{Hom}_{S^\infty}(M, \mathbf{R}\operatorname{Hom}_{R^\infty}(R^\infty, N)) \\ = \ & \mathbf{R}\operatorname{Hom}_{S^\infty}(M, N). \end{aligned}$$

and so it suffices to prove the result of S^∞. Let $d = \dim S$ and note that $S^\infty = \lim_{\longrightarrow} S^{1/p^e}$. Now, we can view M as an S^{1/p^e}-module by restriction, and write $F_e = M \otimes_{S^{1/p^e}} S^\infty$ for its base change back to S^∞. Obviously we have maps

$$\dots \to M \otimes_{S^{1/p^e}} S^\infty \to M \otimes_{S^{1/p^{e+1}}} S^\infty \to \dots \to M$$

The direct limit $\lim_{\longrightarrow} F_e$ is in fact equal to M since any element of S^∞ is in some S^{1/p^e} for $e \gg 0$. On the other hand, M has projective dimension $\leq d$ as an S^{1/p^e}-module and so F_e has projective dimension $\leq d$ as an S^∞-module.

Now consider

$$\bigoplus F_e \to \bigoplus F_e$$

where $(\dots, 0, a_e, 0, 0 \dots) \mapsto (\dots, 0, a_e, -a_e, 0, \dots)$ and the remainder of the map is defined by linearity. The cokernel of this map is exactly $\lim_{\longrightarrow} F_e = M$ and the map is clearly injective. Hence the projective dimension of M is $\leq d + 1$ which completes the result. □

Corollary 7.10. *Suppose that R is a complete Noetherian local domain of characteristic $p > 0$ and that R^∞ is a flat R-module, then R is regular.*

PROOF. By Proposition 7.9, every R^∞-module has finite global-dimension. On the other hand, $R \longrightarrow R^\infty$ is also *faithfully* flat by hypothesis.

We now prove that R has finite global dimension. Let n denote the global-dimension of R^∞. Suppose that M, N are R-modules with M finite such that $\operatorname{Ext}^i_R(M,N) \neq 0$ for some $i > n$ (recall you can verify global dimension just for finitely generated modules). Then $\operatorname{Ext}^i_R(M,N) \otimes_R R^\infty \neq 0$ by the faithfulness of R^∞/R. But $\operatorname{Ext}^i_R(M,N) \otimes_R R^\infty = \operatorname{Ext}^i_{R^\infty}(M \otimes_R R^\infty, N \otimes_R R^\infty)$ by the flatness of R^∞/R and the fact that M is finitely presented. The fact that this is nonzero contradicts n being the global-dimension of R^∞ and proves the claim.

Now that R has finite global dimension, we conclude that R is regular as claimed. □

Corollary 7.11. *Suppose R is a Noetherian ring such that F_*R is a flat R-module. Then R is regular.*

PROOF. Since flatness localizes and regularity is measured locally, we may assume that R is a local ring. Let $\widehat{R}$ denote the completion, we first want to show that $F_*\widehat{R}$ is flat over $\widehat{R}$. Apply the completion functor to $R \longrightarrow F_*R$ (note, this is not necessarily the same as tensoring with $\widehat{R}$ since F_*R may not be a finite R-module). Note that $\widehat{F_*R} = \lim_n (F_*R)/\mathfrak{m}^n = \lim_n (F_*R/(\mathfrak{m}^{[p]})^n) = F_*\widehat{R}$. We need that $\widehat{R} \longrightarrow F_*\widehat{R}$ is still flat but we only know that $\widehat{R} \longrightarrow (F_*R) \otimes_R \widehat{R}$ is flat (since $\widehat{R}$ is flat over R). On the other hand the complete tensor product[4] $(F_*R)\widehat{\otimes}_R\widehat{R}$ is $\widehat{F_*R}$. It follows that the composition $\widehat{R} \longrightarrow (F_*R) \otimes_R \widehat{R} \longrightarrow F_*\widehat{R}$ is flat and thus $\widehat{R}$ is regular. But then R is regular as well (since $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ doesn't change in completion). □

[4]just the completion of the tensor product

CHAPTER 2

Frobenius splittings

We saw that Frobenius is flat if and only if the ring is regular. It is then natural to ask, how can we weaken the condition that F_*R is flat. We are primarily interested in the case that F_*R is a finite and hence locally free R-module, thus consider the following.

Proposition 0.1. *Suppose R is a regular F-finite Noetherian ring of characteristic $p > 0$. Then there exists an R-linear map $F_*R \longrightarrow R$ sending $F_*1 \mapsto 1$, a* Frobenius splitting*.*

Proof. First suppose that R is a regular *local* ring. Then F_*R being locally free implies that F_*R is actually free as an R-module. In particular, there exists a surjective R-linear map $\phi : F_*R \longrightarrow R$ (project onto one of the factors). Say $\phi(F_*a) = 1$. Consider the new R-linear map

$$\psi(F_*\_\_) = \phi(F_*(a \cdot \_\_)).$$

It satisfies $\psi(F_*1) = 1$ and so we have handled the case when R is local.

Now suppose that R is not local, consider the map $\sigma : \mathrm{Hom}_R(F_*R, R) \longrightarrow R$ which sends $\phi \mapsto \phi(F_*1)$. It is easy to see that this is a map of R-modules hence it is surjective if and only if it is locally surjective. On the other hand if σ is surjective, the existence of the desired map is produced. Hence it suffices to show that

$$\mathrm{Hom}_R(F_*R, R)_{\mathfrak{m}} \longrightarrow R_{\mathfrak{m}}$$

is surjective (where $\mathfrak{m}$ is some maximal ideal of R). On the other hand

$$\mathrm{Hom}_R(F_*R, R)_{\mathfrak{m}} \cong \mathrm{Hom}_{R_{\mathfrak{m}}}((F_*R)_{\mathfrak{m}}, R_{\mathfrak{m}}) \cong \mathrm{Hom}_{R_{\mathfrak{m}}}(F_*R_{\mathfrak{m}}, R_{\mathfrak{m}})$$

and it is not difficult to see that our localized map above agrees (via this isomorphism) with the evaluation at F_*1 map $\mathrm{Hom}_{R_{\mathfrak{m}}}(F_*R_{\mathfrak{m}}, R_{\mathfrak{m}}) \longrightarrow R_{\mathfrak{m}}$. This completes the proof. □

Thus it is clear that having a is a potential weakening of being regular (in fact, it is quite close to the notion of being semi-log canonical from birational algebraic geometry). This leads us to our next section.

1. Frobenius split rings

Definition 1.1. A ring R containing a field of characteristic $p > 0$ is called *(locally) Frobenius split* if there exists an R-linear map $\phi : F_*R \longrightarrow R$ such that $\phi(F_*1) = 1$. The map ϕ is called a *Frobenius splitting*.

Frobenius splittings behave best when F_*R is a finitely generated (thus finitely presented in the Noetherian) R-module. Because of this, we make the following definition.

Definition 1.2. A ring R of characteristic $p > 0$ is said to be *F-finite* if F_*R is a finite R-module.

We will see later that F-finite rings avoid most of the pathologies that other arbitrary rings can satisfy.

Lemma 1.3. *The following are equivalent.*

(a) R is F-split.
(b) The map $R \longrightarrow F^e_*R$ is split for some $e > 0$.
(c) The map $R \longrightarrow F^e_*R$ is split for all $e > 0$.
(d) There exists a surjective R-linear map $F^e_*R \longrightarrow R$ for all $e > 0$.
(e) There exists a surjective R-linear map $F^e_*R \longrightarrow R$ for some $e > 0$.

Proof. (a) $\Rightarrow$ (b) follows simply from taking $e = 1$. We now show (b) $\Rightarrow$ (c). First if $R \longrightarrow F^e_*R$ splits, then so does $R \longrightarrow F_*R \longrightarrow F^e_*R$, and hence so does $R \longrightarrow F_*R$. Thus any $e > 1$ implies that $e = 1$ case so let $\phi : F_*R \longrightarrow R$ be the map which sends F_*1 to 1. Then $\phi \circ (F_*\phi) : F^2_*R \longrightarrow R$ sends F^2_*1 to 1 as well. Likewise $\phi \circ (F_*\phi) \circ \cdots \circ (F^{n-1}_*\phi) : F^n_*R \longrightarrow R$ sends $F^n_*1 \mapsto 1$ as desired.

Next, obviously (c) $\Rightarrow$ (d) since if 1 is contained in the image, then so are all multiplies of 1 (the entire ring). Furthermore (d) $\Rightarrow$ (e) and so it suffices to show that (e) $\Rightarrow$ (a). Let $\phi : F^e_*R \longrightarrow R$ be a surjective map with $\phi(F^e_*a) = 1$. Then forming $\psi(F^e_*\_\_) = \phi(F^e_*(a \cdot \_\_))$ shows that there exists a splitting $\psi : F^e_*R \longrightarrow R$. Forming the composition $F_*R \longrightarrow F^e_*R \xrightarrow{\psi} R$ constructs a splitting of Frobenius. $\square$

Lemma 1.4. *A Frobenius split ring is reduced.*

Proof. Suppose R is not reduced but it is Frobenius split. Then there exists some $0 \neq r \in R$ with $r^p = 0$. Let $\phi : F_*R \longrightarrow R$ be a Frobenius splitting then we have the composition:

$$R \xrightarrow{F} F_*R \xrightarrow{\phi} R$$

$$r \longmapsto F_*r^p \longmapsto r.$$

But the middle term is zero, a contradiction. $\square$

Exercise 1.1. Suppose R is an F-finite Noetherian ring. Show that R is F-split if and only if $R_{\mathfrak{m}}$ is F-split for every maximal ideal $\mathfrak{m} \subseteq R$.

At this point, we don't even know that *any* interesting examples of F-split rings that are not regular. There's a good way to construct lots of them however.

Theorem 1.5. *Suppose that $R \subseteq S$ is an extension of rings such that there exists a surjective R-linear map $T : S \longrightarrow R$. Then if S is F-split, so is R.*

PROOF. Via the argument we used in Lemma 1.3, we may assume that the map $T : S \longrightarrow R$ sends $1_S \mapsto 1_R$. Let $\phi_S : F_* S \longrightarrow S$ be a Frobenius splitting. We have the following composition:

$$F_* R \hookrightarrow F_* S \xrightarrow{\phi_S} S \xrightarrow{T} R.$$

It is R-linear and it is easy to check that it sends $F_* 1_R \longrightarrow 1_R$. Thus R is F-split. $\square$

Example 1.6. Consider $R = k[x^2, xy, y^2] \subseteq k[x, y] = S$ where k is an F-finite field of characteristic $p > 0$. Obviously S is F-split since it is regular. On the other hand

$$S = k[x, y] = k \bigoplus (k \cdot x \oplus k \cdot y) \bigoplus (k \cdot x^2 \oplus k \cdot xy \oplus k \cdot y^2) \bigoplus \dots .$$

R is just the subring of even degree terms, and hence it is clear that $R \subseteq S$ splits.

Definition 1.7. Suppose that $R \subseteq S$ is an extension of rings. If there exists a splitting $S \longrightarrow R$ (or equivalently any surjective map $S \longrightarrow R$) then we say that the extension $R \subseteq S$ *splits* and that R *is a summand of* S.

Just as we did in the example:

Corollary 1.8. *If R is an F-finite Noetherian ring of characteristic $p > 0$ that is a summand of a regular ring, then R is F-split.*

It turns out that summands of regular rings are really quite common!

2. Fedder's criterion and computations

The main goal is to prove Fedder's Lemma, Theorem 2.9, a remarkably useful tool for explicitly working with p^{-e}-linear maps (equivalently R-linear maps $F^e_* R \longrightarrow R$). For instance, using Fedder's Lemma it is easy to determine whether a given F-finite ring is F-split. The organization of this section is as follows. First we prove Fedder's lemma and some corollaries, we then do numerous computations with Fedder's lemma. Finally, we discuss Fedder's criterion outside the F-finite case and define F-purity in general.

2.1. Fedder's Lemma on p^{-e}-linear maps. We begin with the following:

Notation 2.1. Throughout the rest of the section, k is an F-finite field and $S = k[x_1, \dots, x_n]$, or a localization thereof, or $S = k[\![x_1, \dots, x_n]\!]$.

Some of the facts below we have proven previously, but we recall them for ease of reference.

Example 2.2. Consider the polynomial ring $S = k[x_1, \dots, x_n]$ for k an F-finite field. Then S is also F-finite and of course $F^e_* S$ is a free S-module with basis $\{F_* a_i \mathbf{x}^\lambda\}$ where the $F^e_* a_i$ are a basis for $F^e_* k$ over k and $\mathbf{x}^\lambda$ denotes the monomials of the form $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ such that $0 \leq \lambda \leq p^e - 1$.

Lemma 2.3. *Suppose that k is an F-finite finite field, then* $\operatorname{Hom}_k(F^e_* k, k) \cong F_* k$ *as $F_* k$-modules.*

PROOF. Suppose that $m = [F^e_* k : k]$. Obviously $\mathrm{Hom}_k(F^e_* k, k)$ has rank m as a k-module since it is the dual of a rank m vector space. On the other hand, if an $F^e_* k$-module has rank m as a k-module, it clearly has rank 1 as an $F^e_* k$-module, and so the result follows. □

Lemma 2.4. *Suppose that k is an F-finite field, $S = k[x_1, \dots, x_n]$, (or its localization at the origin, or $S = k[\![x_1, \dots, x_n]\!]$). Then $\mathrm{Hom}_S(F^e_* S, S)$ is isomorphic to $F^e_* S$ as an $F^e_* S$-module with generator equal to the following map:*

$$\Phi_S(F^e_* \mathbf{x}^\lambda) = \left\{ \begin{array}{ll} 1 & \text{if } \lambda_1 = \dots = \lambda_n = p^e - 1 \\ 0 & \text{otherwise} \end{array} \right\}$$

defined on the a basis $\{a_i \mathbf{x}^\lambda\}$ where the a_i form a basis for $F^e_* k$ over k, $a_1 = 1$ and $\lambda = (\lambda_1, \dots, \lambda_n)$ satisfies $0 \leq \lambda_i \leq p^e - 1$.

PROOF. We first do the case where k is perfect. To see that it is cyclic, it is sufficient to show that each of the projections $\rho_{\mathbf{x}^\lambda} : F^e_* S \longrightarrow S$ onto the $F^e_* \mathbf{x}^\lambda$-summand is an $F_* S$-multiple of Φ_S with $\mathbf{x}^\lambda$ defined as in Example 2.2. But simply observe that

$$\rho_{\mathbf{x}^\lambda}(F^e_* \_\_) = \Phi_R((F^e_* \mathbf{x}^{\mathbf{p^e - 1} - \lambda}) \cdot F^e_* \_\_).$$

On the other hand $\mathrm{Hom}_S(F^e_* S, S)$ is certainly torsion free and the lemma is proven when k is perfect and S is a polynomial ring.

Now assume that k is not perfect, choose a basis $\{F_* a_i\}_{i=1}^m$ of $F_* k$ over k with $a_1 = 1$. Note that $\{a_i \mathbf{x}^\lambda \mid \lambda_j = 0, \dots, p^e - 1, i = 1, \dots, m\}$ form a basis for $F^e_* S$ over S. Choose maps $\mu_i : F_* k \longrightarrow k$ which project onto the a_i. For each $m \geq i > 1$, choose $b_j \in k$ such that $\mu_1(F^e_* b_i \_\_) = \mu_i(\_\_)$. On the other hand each $F_* k \longrightarrow k$ induces

$$\nu_i : (F^e_* k)[x_1, \dots, x_n] \longrightarrow k[x_1, \dots, x_n]$$

by acting as the identity on the x_i. On the other hand, using the same argument we made in the perfect case, we can find maps

$$\rho_\lambda : F^e_* k[x_1, \dots, x_n] \longrightarrow (F^e_* k)[x_1, \dots, x_n]$$

projecting onto $\mathbf{x}^\lambda$ as above. Composing ρ_λ with ν_i gives us all the projections onto our basis. On the other hand, it is easy to see that those maps can all be obtained by properly pre-multiplying by appropriate $b_i \mathbf{x}^{\mathbf{p^e - 1} - \lambda}$. This proves the lemma in the case of a polynomial ring. The other cases are the same. □

With S as above, we next suppose that $I = \langle f_1, \dots, f_m \rangle \subseteq S$ is an ideal and set $R = S/I$. We want to relate the maps $\mathrm{Hom}_R(F^e_* R, R)$ to the maps $\mathrm{Hom}_S(F^e_* S, S)$. We begin with an easy observation in slightly greater generality.

Fix another ideal $J \subseteq S$, choose $\phi \in \mathrm{Hom}_S(F^e_* S, S)$ and pick $u \in I^{[p^e]} : J \subseteq S$. Consider the map $\psi : F^e_* S \longrightarrow S$ defined by $\psi(F^e_* z) = \phi(F^e_*(u \cdot z))$, frequently in the future we will write $\psi = (F^e_* u) \cdot \phi$ in this situation. We claim that $\psi((F^e_* J)) \subseteq I$ (this has nothing to do with S being regular). To see this claim, choose $z \in J$ and notice that $uz \in I^{[p^e]}$ can be written $uz = a_1 f_1^{p^e} + \dots + a_m f_m^{p^e}$. Then

$$\psi(F^e_* z) = \phi(F^e_*(uz)) = \phi(F^e_*(a_1 f_1^{p^e} + \dots + a_m f_m^{p^e})) = \sum_{i=1}^m \phi(F^e_* a_i) f_i \in I$$

as claimed. In fact, linearity implies that any $\psi \in \left(F^e_*\big(I^{[p^e]} : J\big)\right) \cdot \mathrm{Hom}_S(F^e_* S, S)$ satisfies $\psi(F^e_* J) \subseteq I$.

Remark 2.5. The notation $\left(F^e_*\big(I^{[p^e]} : J\big)\right) \cdot \mathrm{Hom}_S(F^e_* S, S)$ has been known to cause some confusion. The point is that $\mathrm{Hom}_S(F^e_* S, S)$ is an S-module (with S acting on either the source or target of a homomorphism) and simultaneously it is an $F^e_* S$-module, where an element $F^e_* z$ acts on $\alpha : F^e_* S \longrightarrow S$ by forming the composition

$$F^e_* S \xrightarrow{\cdot F^e_* z} F^e_* S \xrightarrow{\alpha} S.$$

Our previous observation about ψ is very useful in the case that $J = I$, consider the following diagram for any ψ satisfying $\psi(F^e_* I) \subseteq I$:

$$\begin{array}{ccc} F^e_* I & \longrightarrow & I \\ \big\downarrow & & \big\downarrow \\ F^e_* S & \xrightarrow{\psi} & S \\ \big\downarrow & & \big\downarrow \\ F^e_* R & \xrightarrow[\psi_R]{\cdots\cdots} & R \end{array}$$

In particular, each ψ determines an element of $\mathrm{Hom}_R(F^e_* R, R)$. We have just shown that:

Lemma 2.6. *There exists an $F^e_* S$-module homomorphism*

$$\rho : \left(F^e_*\big(I^{[p^e]} : I\big)\right) \cdot \mathrm{Hom}_S(F^e_* S, S) \longrightarrow \mathrm{Hom}_R(F^e_* R, R).$$

We will study this map extensively (and in fact prove it is surjective and identify its kernel). First we make the following observations which help show what was described above.

Lemma 2.7. *With notation as above,*

(i) *Suppose that $\phi(F^e_* J) \subseteq I$ for all $\phi \in \mathrm{Hom}_S(F^e_* S, S)$, then $J \subseteq I^{[p^e]}$.*

(ii)

$$\left(F^e_*\big(I^{[p^e]} : J\big)\right) \cdot \mathrm{Hom}_S(F^e_* S, S) = \{\psi \in \mathrm{Hom}_S(F^e_* S, S) \mid \psi(F^e_* J) \subseteq I\}.$$

Proof. With our notations for this section, $F^e_* S$ is a free S-module. Write $F^e_* S \cong S^{\oplus d}$ with basis elements $\{F^e_* g_i\}_{i=1}^d \subseteq F^e_* S$. Let $\pi_1, \ldots, \pi_d$ denote the corresponding projections. Observe that under the isomorphism $F^e_* S \cong S^{\oplus d}$ we have $F^e_* I^{[p^e]} = I \cdot F^e_* S \cong I^{\oplus d}$. Now, suppose that $\phi(F^e_* J) \subseteq I$ for all $\phi \in \mathrm{Hom}_S(F^e_* S, S)$. In particular, $\pi_i(F^e_* J) \subseteq I$ for each $\pi_1, \ldots, \pi_d$. Thus $F^e_* J$ is identified with a subset of $I^{\oplus d}$ which proves that $J \subseteq I^{[p^e]}$. This proves the first statement.

The argument before the lemma yields the containment $\subseteq$. Fix $\psi \in \mathrm{Hom}_S(F^e_* S, S)$ such that $\psi(F^e_* J) \subseteq I$. Choose a $F^e_* S$-module generator $\Phi \in \mathrm{Hom}_S(F^e_* S, S)$ by

Lemma 2.4. Write $\psi = (F^e_* u) \cdot \Phi$ and observe that $\Phi(F^e_*(uJ)) \subseteq I$. Since Φ generates $\mathrm{Hom}_S(F^e_* S, S)$, we see that $uJ \subseteq I^{[p^e]}$ from part (i). Thus $u \in I^{[p^e]} : J$ and hence

$$\psi = (F^e_* u)\Phi \in \Big(F^e_*\big(I^{[p^e]} : J\big)\Big) \cdot \mathrm{Hom}_S(F^e_* S, S)$$

as claimed. ☐

Remark 2.8. The previous lemma absolutely does *not* hold for non-regular rings.

Theorem 2.9 (Fedder's Lemma)**.** *With notation as above*

$$\rho : \Big(F^e_*\big(I^{[p^e]} : I\big)\Big) \cdot \mathrm{Hom}_S(F^e_* S, S) \longrightarrow \mathrm{Hom}_R(F^e_* R, R)$$

is surjective and $\ker \rho$ *is isomorphic to* $\Big(F^e_* I^{[p^e]}\Big) \cdot \mathrm{Hom}_S(F^e_* S, S)$*. In particular*

$$\mathrm{Hom}_R(F^e_* R, R) \cong \frac{\Big(F^e_*\big(I^{[p^e]} : I\big)\Big) \cdot \mathrm{Hom}_S(F^e_* S, S)}{\Big(F^e_* I^{[p^e]}\Big) \cdot \mathrm{Hom}_S(F^e_* S, S)}.$$

Proof. First we prove that ρ is surjective. Choose $\alpha \in \mathrm{Hom}_R(F^e_* R, R)$. Consider the following diagram of S-modules

$$\begin{array}{ccc} F^e_* S & \overset{\overline{\alpha}}{\dashrightarrow} & S \\ \downarrow & & \downarrow \\ F^e_* R & \underset{\alpha}{\longrightarrow} & R. \end{array}$$

The dotted arrow $\overline{\alpha}$ exists since $F^e_* S$ is a projective S-module (although it is not unique). The commutativity of the diagram implies that $\overline{\alpha}(F^e_* I) \subseteq I$ (as $F^e_* I$ and I are kernels of the vertical projection maps) and therefore we see that $\overline{\alpha} \in \Big(F^e_*\big(I^{[p^e]} : I\big)\Big) \cdot \mathrm{Hom}_S(F^e_* S, S)$ by **??**. This proves the surjectivity of ρ.

Next we identify the kernel of ρ. Suppose that $\psi \in \mathrm{Hom}_S(F^e_* S, S)$ satisfies $\psi(F^e_* I) \subseteq I$ and also that $\rho(\psi) = 0$. This second condition means that $\psi(F^e_* S) \subseteq I$. Applying **??** in the case that $J = S$ we see that $\psi \in \Big(F^e_* I^{[p^e]}\Big) \cdot \mathrm{Hom}_S(F^e_* S, S)$. The reverse inclusion also follows immediately from Lemma 2.7. The final isomorphism then of course follows from the first isomorphism theorem. ☐

The real beauty of Fedder's Lemma is that it allows us to compute numerous things with ease!

2.2. Computations with Fedder's Lemma. Fedder's lemma gives us a very explicit way to compute the locus where a ring is not F-split.

Theorem 2.10. *Suppose that S is an F-finite regular ring and $R = S/I$. Let $J_e \subseteq S$ denote the image of the evaluation-at-1 map*

$$\mathrm{Image}\left(\Big(F^e_*\big(I^{[p^e]} : I\big)\Big) \cdot \mathrm{Hom}_S(F^e_* S, S) \longrightarrow S\right)$$

for some integer $e > 0$. Then the set theoretic locus $V(J_e) \subseteq V(I) \subseteq \operatorname{Spec} S$ is the set of points of $V(I) \cong \operatorname{Spec} R$ where $\operatorname{Spec} R$ is not F-split.

Before proving this result, we notice that the result implies that $V(J_e)$ is independent of e. However, scheme theoretically, $V(J_e)$ is generally not independent of e.

Proof. Using Theorem 2.9, we see that the evaluation-at-1 map in the statement of the theorem is surjective at all points $\mathfrak{q} \in V(I) \subseteq \operatorname{Spec} S$ where $\operatorname{Hom}_R(F^e_* R, R) \longrightarrow R$ is also surjective. Of course, outside of $V(I)$, $(I^{[p^e]} : I)$ agrees with S and the surjectivity is obvious. The result follows since $R_{\mathfrak{q}} \longrightarrow F^e_* R_{\mathfrak{q}}$ splits if and only if $R_{\mathfrak{q}} \longrightarrow F_* R_{\mathfrak{q}}$ splits Lemma 1.3. ☐

Via the identification $\operatorname{Hom}_S(F^e_* S, S) \cong F^e_* S$ (sending Φ to 1, where Φ is the projection onto the $F^e_* \mathbf{x}^{\mathbf{p^e-1}}$-basis element), we get a map $F^e_* S \longrightarrow S$. It is not hard to see that this map is itself Φ. In particular:

Corollary 2.11. *The locus where $\operatorname{Spec} R$ is not split is closed and it is equal to $V\big(\Phi^e(F^e_*(I^{[p^e]} : I))\big)$.*

Remark 2.12. The ideal $\Phi^e(F^e_*(I^{[p^e]} : I))$ depends on the choice of e, although the locus it defines does not!

Exercise 2.1. Show that $\Phi^e(F^e_*(I^{[p^e]} : I)) \supseteq \Phi^{e+1}(F^{e+1}_*(I^{[p^{e+1}]} : I))$.

Hint: Show that $\Phi^e(F^e_*(I^{[p^e]} : I))\cdot R$ is the same as the image of the evaluation-at-1 map $\operatorname{Hom}_R(F^e_* R) \longrightarrow R$.

Question 2.13 (Open question)**.** It is an open question whether the descending ideals from the previous exercise stabilize (are all equal for $e \gg 0$). This is known if R is a hypersurface or more generally Gorenstein or even more generally $\mathbb{Q}$-Gorenstein. The Gorenstein case is essentially a key step in a famous result of Hartshorne and Speiser [**HS77**].

Remark 2.14. Since Φ is additive, note that $\Phi(F^e_*\langle f_1, \dots, \rangle f_m\rangle) = \Phi(F^e_*\langle f_1\rangle) + \Phi(F^e_*\langle f_2\rangle) + \cdots + \Phi(F^e_*\langle f_m\rangle)$. Hence from a computational perspective, it is sufficient to compute $\Phi(F^e_*\langle f\rangle)$.

Suppose now that k is perfect for simplicity, if one writes $F^e_* f$ in terms of the basis $F^e_* \mathbf{x}^\lambda$ as

$$F^e_* f = F^e_* \sum f_\lambda^{p^e} \mathbf{x}^\lambda = \sum f_\lambda F^e_* \mathbf{x}^\lambda$$

then we claim that $\Phi(F^e_*\langle f\rangle) = \langle \dots, f_\lambda, \dots\rangle$. The point is that $\Phi(F^e_* f)$ simply projects from the term $f_{(\mathbf{p^e-1})} F^e_* \mathbf{x}^{(\mathbf{p^e-1})}$, on the other hand $\mathbf{x}^\lambda f \in \langle f\rangle$ and $\Phi(F^e_* \mathbf{x}^{(\mathbf{p^e-1})-\lambda} f)$ projects from $f_\lambda F^e_* \mathbf{x}^\lambda$. Doing the various projections proves that

$$\Phi(F^e_*\langle f\rangle) = \langle \dots, f_\lambda, \dots\rangle$$

as claimed.

As another corollary of Fedder's Lemma, we state a frequently easy to check criterion for whether or not a ring is F-split at some point. Recall by Lemma 1.3, to show that R is F-split, it is sufficient to show that there exists a single surjective $\phi : F^e_* R \longrightarrow R$.

Theorem 2.15 (Fedder's F-purity criterion)**.** *Suppose that S is an F-finite regular ring and $R = S/I$. Then R is F-split in a neighborhood of a prime ideal $\mathfrak{q} \in V(I) \subseteq \operatorname{Spec} S$ if and only if*

$$(I^{[p^e]} : I) \not\subseteq \mathfrak{q}^{[p^e]}.$$

Proof. Suppose that R is F-split in a neighborhood of a prime ideal $\mathfrak{q} \in V(I)$. It follows that the evaluation-at-1 map $\operatorname{Hom}_R(F^e_* R, R) \longrightarrow R$ surjects in a neighborhood of $\mathfrak{q}$. Let $\phi_R \in \operatorname{Hom}_R(F^e_* R, R)$ be such that $\phi(F^e_* a) \notin \mathfrak{q}/I$ for some $\overline{a} \in R$. It follows from Theorem 2.9 that there exists $\phi_S \in \Big(F^e_*\big(I^{[p^e]} : I\big)\Big) \cdot \operatorname{Hom}_S(F^e_* S, S)$ such that

$$\phi_S(F^e_* a) \notin \mathfrak{q}$$

where $a \in S$ maps to $\overline{a} \in R$. On the other hand, suppose for a contradiction now that $(I^{[p^e]} : I) \subseteq \mathfrak{q}^{[p^e]}$ and so $\phi_S \in \Big(F^e_* \mathfrak{q}^{[p^e]}\Big) \cdot \operatorname{Hom}_S(F^e_* S, S)$. But since $\mathfrak{q}^{[p^e]} = \mathfrak{q}^{[p^e]} : S$, we have that $\phi_S(F^e_* S) \subseteq \mathfrak{q}$ by Lemma 2.7. But this contradicts our choice of $\overline{a}$.

Conversely we suppose that $b \in (I^{[p^e]} : I) \setminus \mathfrak{q}^{[p^e]}$. Let $\Phi \in \operatorname{Hom}_S(F^e_* S, S)$ be the generating homomorphism as in Lemma 2.4 and let $\phi_S(F^e_* \_\_) = \Phi^e(F^e_*(b \cdot \_\_))$. Since $b \notin \mathfrak{q}^{[p^e]}$, we know that $\phi_S(F^e_* S) \notin \mathfrak{q}$ by Lemma 2.7. Hence there exists $a \in \phi_S(F^e_* S)$, $a \notin \mathfrak{q}$. Thus, $\overline{a} \in R_{\mathfrak{q}}$ is a unit. On the other hand, by our choice of ϕ_S, it induces $\phi_R : F^e_* R \longrightarrow R$ and so by localization, $\phi_{R_{\mathfrak{q}}} : F^e_* R_{\mathfrak{q}} \longrightarrow R_{\mathfrak{q}}$ and $\overline{a}$ is in the image. Thus $\phi_{R_{\mathfrak{q}}}$ surjects and so $R_{\mathfrak{q}}$ is F-split as desired. ☐

Exercise 2.2. Suppose that R is a regular Noetherian ring of characteristic $p > 0$ and that $\mathfrak{q}$ is a prime ideal. Prove that $\mathfrak{q}^{[p^e]}$ is $\mathfrak{q}$-primary.

Hint: Show that if $f \notin \mathfrak{q}$, then $0 \longrightarrow R/\mathfrak{q}^{[p^e]} \xrightarrow{\cdot f} R/\mathfrak{q}^{[p^e]}$ injects.

Corollary 2.16. *Suppose that $R = S/\langle f \rangle_S$. Then R is F-split at the origin if and only if $f^{p-1} \notin \mathfrak{m}^{[p]} = \langle x_1^p, \ldots, x_n^p \rangle$.*

Example 2.17. Consider the following examples of F-split rings. We assume S is as before and consider $R = S/\langle f \rangle$ where f is as specified in each case below.

(a) $f = z$. The ring R is regular so we already know it is F-split, but we can alternately observe that $z^{p-1} \notin \langle x^p, y^p, z^p \rangle$.
(b) If $f = xyz$, then R is F-split (at the origin) since $x^{p-1}y^{p-1}z^{p-1} \notin \langle x^p, y^p, z^p \rangle$.
(c) If $f = xy - z^2$ then R is F-split (at the origin) since

$$(xy - z^2)^{p-1} = x^{p-1}y^{p-1} + \text{other terms} \notin \langle x^p, y^p, z^p \rangle.$$

(d) If $p = 2$, then $R = S/\langle f \rangle$ is F-split (at the origin) if and only if $f \notin \langle x^2, y^2, z^2 \rangle$ (note $p - 1 = 2 - 1 = 1$). So for example $f = x^7 + y^4 + z^3 + xyz$ yields an F-split ring.

(e) Consider $f = x^3 + y^3 + z^3$ and suppose $1 \equiv p \pmod 3$. Note that the degree of every monomial of f^{p-1} is equal to $3(p-1)$. Thus the only way that $f^{p-1} \notin \langle x^p, y^p, z^p \rangle$ is if $x^{p-1}y^{p-1}z^{p-1}$ has non-zero coefficient in f^{p-1}. Since each monomial x^3, y^3 and z^3 to be raised to the same power we must have $3|(p-1)$ which implies that $1 \equiv p \pmod 3$ as we already assumed. Now we need the multinomial coefficent of $x^{p-1}y^{p-1}z^{p-1}$ to not be divisible by p. But this coefficient is

$$\binom{p-1}{\frac{p-1}{3}, \frac{p-1}{3}, \frac{p-1}{3}} \equiv \frac{(p-1)!}{\left(\frac{p-1}{3}\right)! \left(\frac{p-1}{3}\right)! \left(\frac{p-1}{3}\right)!}.$$

which clearly is not divisible by p.

Now we consider several non-F-split rings.

(a′) $f = z^2$. The ring R is not reduced, so it can't be F-split, but also $z^{2(p-1)} \in \langle x^p, y^p, z^p \rangle$.

(b′) $f = x^2y - z^2$ with $p = 2$. Note that $f \in \langle x^2, y^2, z^2 \rangle$. R actually is F-split if $p \neq 2$.

(c′) $f = x^4 + y^4 + z^4$. This is not F-split since every monomial in the expansion of $(x^4 + y^4 + z^4)^{p-1}$ has degree equal to $4 \cdot (p-1)$. In particular, each such monomial is divisible by x^p, y^p or z^p by the pigeon-hole-principal.

(d′) $f = x^3 + y^3 + z^3$ and $1 \not\equiv p \pmod 3$. In this case, there is no $x^{p-1}y^{p-1}z^{p-1}$ term in the expansion of $(x^3 + y^3 + z^3)^{p-1}$ by the argument in (e) above. Thus since each monomial in said expansion has degree $3(p-1)$, we see that $f^{p-1} \in \langle x^p, y^p, z^p \rangle$ which implies that R is not F-split.

3. A crash course in local cohomology

We'll be doing a series of crash courses over the next few days. We'll start with local cohomology and the Cohen-Macaulay condition, and then we'll move to Matlis and local duality (as well as a study of the dualizing complex). Today, local cohomology, tomorrow the world!

Let R be a Noetherian ring and I an ideal. There is a functor from R-modules to R-modules Γ_I which is defined by

$$\Gamma_I(M) = \{m \in M \mid I^n m = 0 \text{ for some } n > 0\}.$$

Because I is finitely generated we also have

$$\Gamma_I(M) = \{m \in M \mid x^{n_x} m = 0 \text{ for all } x \in I \text{ and some } n_x > 0 \text{ depending on } x\}.$$

It is not difficult to see that $\Gamma_I(M)$ is left exact and so we make the following definition.

Definition 3.1. With R, I, M above, we denote by $H^i_I(M) = h^i \mathbf{R}\Gamma_I(M)$ the ith right derived functor of Γ_I. It is called the *ith local cohomology group.*

There is another important related functor. Let $U = \operatorname{Spec} R \setminus V(I)$. Choose a generating set $\langle f_0, \ldots, f_t \rangle$ for I and for each m-tuple $f_{i_1}, \ldots, f_{i_m}$ of these generators, we can form the localization $M_{f_{i_1}\cdots f_{i_m}}$. Most notably, we have

$$d_0 : \bigoplus_j M_{f_j} \longrightarrow \bigoplus_{a<b} M_{f_a f_b}$$

where

$$d_0(m_1/f_1^{n_1}, \ldots, m_t/f_t^{n_t}) = (\ldots, m_a/f_a^{n_a} - m_b/f_b^{n_b}, \ldots).$$

The kernel of d_0 is denoted by $\Gamma(U, M)$ and it is independent of the choice of generators of I.

Exercise 3.1. Prove that $\Gamma(U, M)$ really is independent of the choice of generators.

Hint: It suffices to consider the case where you add a single generator to the list.

Example 3.2. Suppose $M = R = k[x]$ and $I = \langle x \rangle$. Then $\Gamma(U, M) = k[x, x^{-1}]$ (there are no $M_{f_a f_b}$ terms).

Example 3.3. Suppose $M = R = k[x, y]$ and $I = \langle x, y \rangle$. Consider the kernel of

$$k[x, y, x^{-1}] \oplus k[x, y, y^{-1}] \xrightarrow{-} k[x, y, x^{-1}, y^{-1}]$$

and deduce that $\Gamma(U, M) = k[x, y]$.

On the other hand, if $M = \langle x, y \rangle$, then $\Gamma(U, M) = k[x, y]$ since $\langle x, y \rangle_x = k[x, y, x^{-1}]$ and $\langle x, y \rangle_y = k[x, y, y^{-1}]$.

Lemma 3.4. *Suppose that $Q \in U$, then $\Gamma(U, M)_Q = M_Q$.*

Proof. We localize the map α_0 at Q and notice that since $Q \in U$, at least one $f_j \notin Q$, and so $(M_{f_j})_Q = M_Q$. We may assume that $j = 1$ and so write

$$M_Q \oplus \bigoplus_{j>1} (M_Q)_{f_j} \longrightarrow \left(\bigoplus_j (M_Q)_{f_j} \right) \bigoplus \left(\bigoplus_{1<a<b} (M_Q)_{f_a f_b} \right).$$

In particular, it is easy to see that if an element is in the kernel, it is completely determined by its entry in $(M_Q)_{f_1} = M_Q$ and any such entry gives an element of the kernel. The lemma follows. ☐

Alternate proof. Alternately, simply observe that $IR_Q = \langle 1 \rangle_{R_Q}$, and then the result immediately follows by change of the generating set. ☐

It is also easy to see that $\Gamma(U, \bullet)$ is a left exact functor, and its higher derived functors are denoted by $H^i(U, \bullet)$.

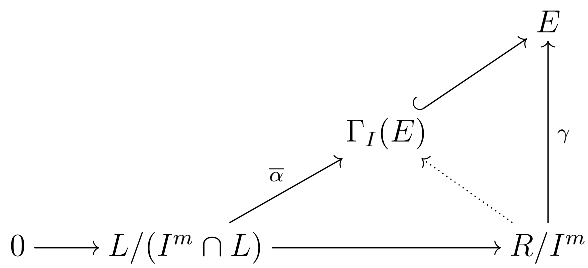
Lemma 3.5. *With notation as above, suppose E is an injective module. Then $\Gamma_I(E)$ is also injective.*

Proof. Suppose we have $0 \longrightarrow L \xrightarrow{f} M$ exact as well as a map $\alpha : L \longrightarrow \Gamma_I(E)$. We need to show that there exists $\beta : M \longrightarrow \Gamma_I(E)$ such that $\alpha = \beta \circ f$. In fact, by [**Sta16**, Tag 0AVF][1], it suffices to consider the case when $M = R$ and L is an ideal

[1]The trick is to look at the largest submodule to which the map extends, and derive a contradiction if it's not M.

(and so in particular, finitely generated since R is Noetherian). Consider the finitely generated submodule $\alpha(L) \subseteq \Gamma_I(E)$ and choose $n > 0$ so that $0 = I^n \alpha(L) = \alpha(I^n L)$. By Krull's theorem, there exists some m such that $I^m \cap L \subseteq I^n L$ and so $\alpha(I^m \cap L) = 0$ as well. In particular, α factors as $\alpha : L \longrightarrow L/(I^m \cap L) \xrightarrow{\overline{\alpha}} \Gamma_I(E)$. It thus suffices to show that $\overline{\alpha}$ extends to $\overline{\beta} : R/I^m \longrightarrow E$.

On the other hand, we certainly have



where the map labeled γ exists by the injectivity hypothesis on E. Applying $\Gamma_I(\bullet)$ to the entire diagram yields $\Gamma_I(\gamma) = \overline{\beta}$, the map we desired since $\Gamma_I(R/I^m) = R/I^m$. □

Corollary 3.6. *If M is I-torsion (in other words $M = \Gamma_I(M)$), then M can be embedded in an injective I-torsion module $M \subseteq E$. In particular, $M \simeq_{qis} \mathbf{R}\Gamma_I(M)$ (and thus $H^i_I(M) = 0$ for $i > 0$).*

Proof. For the first statement, simply embed M in an injective module $M \subseteq E$ and then apply the functor $\Gamma_I(\bullet)$ using Lemma 3.5. For the second statement, it follows from the first that we can take an injective resolution of an I-torsion module by I-torsion injective modules. But then Γ_I acts as the identity on such a resolution. □

There is a canonical map $M \longrightarrow \Gamma(U, M)$ (the diagonal), the kernel of which is easily seen to be exactly $\Gamma_I(M)$.

Theorem 3.7. [**Har77**, III, Exercise 2.3] *For any $I \subseteq R$, an ideal in a Noetherian ring, there is a long exact sequence*

$$\begin{array}{ccc} \dots & \dots & \dots \\ H^i_I(M) \longrightarrow & \mathrm{Id}^i(M) \longrightarrow & H^i(U, M) \longrightarrow \\ H^{i+1}_I(M) \longrightarrow & \mathrm{Id}^{i+1}(M) \longrightarrow & H^{i+1}(U, M) \longrightarrow \\ \dots & \dots & \dots \end{array}$$

Where $\mathrm{Id}^i(M)$ is the ith derived functor of the identity, in particular equal to zero for $i > 0$.

Exercise 3.2. Prove Theorem 3.7.

Hint: Show that if M is injective, then $0 \longrightarrow \Gamma_I(M) \longrightarrow M \longrightarrow \Gamma(U, M) \longrightarrow 0$ is exact (we showed in class everything but the exactness on the right, to do that use the fact that if I is injective, then $I \longrightarrow I_f$ is surjective). Now take an injective resolution of M, use what you just proved, and chase.

Corollary 3.8. *With notation as above, $H^{i+1}_I(M) = H^i(U, M)$ for all $i \geq 1$ and*

$$0 \longrightarrow H^0_I(M) \longrightarrow M \longrightarrow H^0(U, M) \longrightarrow H^1_I(M) \longrightarrow 0$$

is exact.

3.1. Vanishing and non-vanishing theorems.

Proposition 3.9. *If R is Noetherian, $I \subseteq R$ is an ideal and M is an R-module then $H^i_I(M) = 0$ for $i > \dim M =: d$,*[2] *in particular for $i > \dim R$.*

Proof. It is easy to see that $H^i_I(M)_{\mathfrak{m}} = H^i_{IR_{\mathfrak{m}}}(M_{\mathfrak{m}})$ for any maximal ideal $\mathfrak{m}$ and so it suffices to work in the local case (in the Noetherian case, a localization of an injective module is still injective).

Because the local cohomology functor commutes with direct limits, it is harmless to assume that M is finitely generated. First consider the short exact sequence

$$0 \longrightarrow \Gamma_I(M) \longrightarrow M \longrightarrow M/\Gamma_I(M) \longrightarrow 0.$$

Note that $\Gamma_I(M)$ is I-torsion and so $H^i_I(\Gamma_I(M)) = 0$ for $i > 0$ by Corollary 3.6. Hence $H^i_I(M) \cong H^i_I(M/\Gamma_I(M))$ for all $i > 0$ and so it suffices to prove the proposition in the case that M is I-torsion free.

We now proceed by induction on the dimension of M. In the case that M is dimension zero, we are already done since then M is I-torsion and hence zero.

Claim 3.10. *There exists $x \in I \subseteq \mathfrak{m}$ such that x is a regular element for M (in particular, $M \xrightarrow{\cdot x} M$ is injective.*

Proof of claim. Since M is already assumed to be finitely generated, it has finitely many associated primes $P_i = \operatorname{Ann}_R m_i$. On the other hand, since M is I-torsion free, $I \cdot m_i \neq 0$, thus $I \not\subseteq P_i$. By *Prime Avoidance*[3], we have that $I \not\subseteq \bigcup P_i$. So choose $x \in I \setminus \left(\bigcup P_i\right)$. We claim that x is a regular element M. If $M \xrightarrow{\cdot x} M$ is not injective with kernel K, then K has an associated prime containing x, and thus so does M. This is a contradiction which proves the claim. □

Using the claim, consider now the short exact sequence

$$0 \longrightarrow M \xrightarrow{\cdot x} M \longrightarrow M/xM \longrightarrow 0$$

and note that $\dim(M/xM) \leq \dim M - 1 = d - 1$ by [**AM69**] (in that source, this is only proved for rings but since M is finitely generated, one can reduce to the case that $\operatorname{supp} M = \operatorname{supp} R$ and so this is easy since M/xM is a R/xR-module). By our induction hypothesis, we have

$$\ldots \longrightarrow H^{i-1}_I(M/xM) \longrightarrow H^i_I(M) \xrightarrow{\cdot x} H^i_I(M) \longrightarrow \ldots$$

and so $H^i_I(M) \xrightarrow{\cdot x} H^i_I(M)$ injects for $i < \dim M$.

Claim 3.11. *The induced map on local cohomology is still multiplication by x.*

Proof of claim. The functor $H^i_I(M)$ is R-linear (since it is a derived functor of an R-linear functor). Note that being R-linear that $\operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(H^i_I(M), H^i_I(N))$ is an R-module homomorphism. In the case that $N = M$, this means that not only

[2]The dimension of a module is the maximal length of a chain of primes $\mathfrak{q}_0 \subseteq \mathfrak{q}_n$ such that $M_{\mathfrak{q}_i} \neq 0$.
[3]This says that if an ideal I is not contained in any of a set of prime ideals P_i, then $I \not\subseteq_i P_i$.

the identity is sent to the identity but also that the identity multiplied by r is sent to the identity multiplied by r, which is exactly what we want. □

Now that we have proved the claim, this implies that $H^i_I(M) \xrightarrow{\cdot x^m} H^i_I(M)$ injects for each integer m. But every element of $H^i_I(M)$ is I-torsion, and so killed by some x^m, which proves that $H^i_I(M) = 0$ for $i < \dim M$. □

Definition 3.12. Suppose $(R, \mathfrak{m})$ is a Noetherian local ring and M is a finitely generated R-module. Then M has *depth* $\geq n$ if $H^i_{\mathfrak{m}}(M) = 0$ for $i < n$. M is called *Cohen-Macaulay* if $H^i_{\mathfrak{m}}(M) = 0$ for $i < \dim R$.

Example 3.13. A Noetherian regular local ring is Cohen-Macaulay. To see this we proceed by induction on dimension and note it is obvious in dimension zero (the case of a field). More generally let x be part of a regular system of parameters (a minimal generating set of the maximal ideal) and note we have $0 \longrightarrow R \xrightarrow{\cdot x} R \xrightarrow{R} /xR \longrightarrow 0$. As before, we have injections $H^i_{\mathfrak{m}}(R) \xrightarrow{\cdot x} H^i_{\mathfrak{m}}(R)$ for $i < \dim R$ but since $H^i_{\mathfrak{m}}(R)$ is $\mathfrak{m}$-torsion, this is a contradiction.

The proof we just performed shows that in order to verify that R is Cohen-Macaulay, it suffices to show that there exists a sequence of elements $x_1, \ldots, x_d \in \mathfrak{m}$ such that x_{i+1} is not a zero divisor on $R/\langle x_1, \ldots, x_i\rangle$ (likewise for a finitely generated module). In fact, that is the usual definition of a Cohen-Macaulay ring (likewise module).

Lemma 3.14. *Suppose that M is an R-module but that R is not necessarily local. If $\mathfrak{m}$ is a maximal ideal then $H^i_{\mathfrak{m}}(M) \cong H^i_{\mathfrak{m}R_{\mathfrak{m}}}(M_{\mathfrak{m}})$ where the second term is viewed as an R-module via restriction.*

Proof. It is easy to see that the functors $\Gamma_{\mathfrak{m}}(\bullet) \cdot R_{\mathfrak{m}}$ and $\Gamma_{\mathfrak{m}R}(\bullet_{\mathfrak{m}})$ are equal and hence the same also holds for the associated local cohomology functors (since injective modules over a Noetherian ring stay injective after localization). But now the result follows from the following claim.

Claim 3.15. *If N is a $\mathfrak{m}$-torsion module, then $N \cong N_{\mathfrak{m}} = NR_{\mathfrak{m}}$ (as R-modules).*

Proof of claim. Consider the map $N \longrightarrow N_{\mathfrak{m}}$. The kernel is the set of elements $n \in N$ such that $un = 0$ for some $u \notin \mathfrak{m}$. Consider the submodule nR for such a n with fixed u. Since N is $\mathfrak{m}$-torsion, $\mathfrak{m}^l n = 0$ for some $l > 0$. Thus nR is compatibly a $R/\mathfrak{m}^l$-module. But $R/\mathfrak{m}^l$ is a local ring and $\overline{u}$ kills $n \in nR$, but $\overline{u}$ is a unit in $R/\mathfrak{m}^l$, a contradiction. □

□

Example 3.16. The ring $R = k[x, y, u, v]/\langle xu, xv, yu, vx\rangle = k[x, y, u, v]/\langle x, y\rangle \cap \langle u, v\rangle$ localized at the origin has depth 1. To see this, it suffices to show that $H^0_{\mathfrak{m}}(R) = 0$ and $H^1_{\mathfrak{m}}(R) \neq 0$. The vanishing statement is obvious because no element is killed by all powers of $\mathfrak{m}$. For the second statement, note we have a short exact sequence

$$\begin{array}{ccccccccc}
0 \longrightarrow & k[x,y,u,v]/\langle x,y\rangle \cap \langle u,v\rangle & \longrightarrow & k[x,y,u,v]/\langle x,y\rangle \oplus k[x,y,u,v]/\langle u,v\rangle & \xrightarrow{-} & k[x,y,u,v]/\langle x,y,u,v\rangle & \longrightarrow 0 \\
 & \| & & \| & & \| & \\
0 \longrightarrow & k[x,y,u,v]/\langle x,y\rangle \cap \langle u,v\rangle & \longrightarrow & k[u,v] \oplus k[x,y] & \longrightarrow & k & \longrightarrow 0.
\end{array}$$

Now apply $H^i_{\mathfrak{m}}(\bullet)$ and consider the long exact sequence

$$0 \longrightarrow H^0_{\mathfrak{m}}(k) \longrightarrow H^1_{\mathfrak{m}}(R) \longrightarrow H^1_{\mathfrak{m}}(k[u,v] \oplus k[x,y])$$

Now, $H^1_{\mathfrak{m}}(k[u,v] \oplus k[x,y]) = 0$ since this is just a direct sum of local cohomologies of regular local rings, and $H^0_{\mathfrak{m}}(k) = k$. The result follows. (Note we were not very careful about localization here, but it doesn't matter due to Lemma 3.14.

Now we move to a non-vanishing theorem which we state but do not prove.

Theorem 3.17. *Suppose that $(R, \mathfrak{m})$ is local and M is a nonzero finitely generated R-module of dimension n, then $H^n_{\mathfrak{m}}(M) \neq 0$.*

As an easy consequence, we obtain the following:

Corollary 3.18. *If Q is a prime ideal such that $M_Q \neq 0$ and $d = \dim R_Q$, then $H^d_Q(M) \neq 0$.*

Proof. $H^d_Q(M) \otimes_R R_Q = H^d_{QR_Q}(M_Q) \neq 0$. □

3.2. F-splitting's implications for local cohomology. Local cohomology $H^i_I(\bullet)$ is a functor and so if we consider the e-iterated Frobenius map $R \longrightarrow F^e_* R$, there is an induced map

$$H^i_I(R) \xrightarrow{F^e} H^i_I(F^e_* R) \cong F^e_* H^i_I(R).$$

called the Frobenius action on local cohomology.

Lemma 3.19. *If R is F-split, then Frobenius acts injectively on $H^i_I(R)$ for any ideal I and any $i \geq 0$.*

Proof. $H^i_I(\bullet)$ is a functor, apply it to $R \longrightarrow F^e_* R \xrightarrow{s} R$ where the composition is the identity. □

Thus we have the following definition which is a weakening of the F-splitting condition.

Definition 3.20. A Noetherian local ring $(R, \mathfrak{m})$ of characteristic $p > 0$ is called *F-injective* if $F : H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(F_* R)$ injects for all $i \geq 0$.

Remark 3.21. Note we only looked at the Frobenius action on the local cohomology of the maximal ideal above, it doesn't necessarily imply injectivity of Frobenius on the local cohomology of other ideals. We will see later though, that under certain conditions (for example, R is Gorenstein and F-finite), R being F-injective implies that R is F-split.

Corollary 3.22. *Suppose that Frobenius acts injective only $H^i_I(R)$ for some $I \subseteq R$ and $i > 0$. Further suppose that $J \cdot H^i_I(R) = 0$, then also $\sqrt{J} \cdot H^i_I(R) = 0$. In particular, in an F-injective local ring $(R, \mathfrak{m}, k)$, if $H^i_{\mathfrak{m}}(R)$ has finite length then $H^i_{\mathfrak{m}}(R)$ is a k-vector space.*

PROOF. Suppose that $x \in \sqrt{J}$ with $x^n \in I$ and hence that $x^{p^e} \in I$ for some $e > 0$. Choose now $z \in H^i_I(R)$ and suppose for a contradiction that $x \cdot z \neq 0$. □

There are ways to weaken the Cohen-Macaulay condition which appear in the commutative algebra literature. We give only the definitions that are convenient for our purposes.

Definition 3.23. A Noetherian d-dimensional local ring $(R, \mathfrak{m}, k)$ is called *quasi-Buchsbaum* if each $H^i_{\mathfrak{m}}(R)$ is a finite dimension k-vector space for each $i < \dim R$. It is called *quasi-Buchsbaum* if when we consider an exact triangle

$$K^{\bullet} \longrightarrow \mathbf{R}\Gamma_{\mathfrak{m}}(R) \longrightarrow H^d_{\mathfrak{m}}(R)[-d] \xrightarrow{+1}$$

then $K^{\bullet} \in D^b(k)$.[4] In particular, since every short exact sequence of K vector spaces is split, $K^{\bullet}$ is quasi-isomorphic to the direct sum of its cohomologies (appropriately shifted).

It was known that for F-pure rings, being quasi-Buchsbaum implies the Buchsbaum condition [**GO83**], but it had been an open question popularized by S. Takagi whether this implication also holds for F-injective rings. This was shown recently to be the case by L. Ma [**Ma15**]. We give a proof of this now due to B. Bhatt, L. Ma and the author which can be found in [**BMS15**]. We first need a lemma.

Proposition 3.24. *Let $A \longrightarrow B$ be a surjection of Noetherian rings with induced surjection $A^{\infty} \longrightarrow B^{\infty}$. Let $K^{\bullet} \in D^b(A^{\infty})$ be a complex such that each $h^i(K^{\bullet})$ is a B^{∞}-module. Then $K^{\bullet} \simeq K^{\bullet} \otimes^{\mathbf{L}}_{A^{\infty}} B^{\infty}$ via the canonical map, and thus $K^{\bullet}$ comes from $D^b(B^{\infty})$ via the forgetful functor $D^b(B^{\infty}) \longrightarrow D^b(A^{\infty})$.*

PROOF. We must check that the canonical map $K^{\bullet} \longrightarrow K^{\bullet} \otimes^{\mathbf{L}}_{A^{\infty}} B$ is an isomorphism for $K^{\bullet}$ as above. We first prove the result for $K = M[0]$ being a B-module M placed in degree 0. But then $K^{\bullet} \otimes^{\mathbf{L}}_{A^{\infty}} B^{\infty} \simeq M[0] \otimes^{\mathbf{L}}_{B^{\infty}} (B^{\infty} \otimes^{\mathbf{L}}_{A^{\infty}} B^{\infty})$, so the claim follows from Lemma 7.5.

For the general case, we induct on the maximum length $l = j - i$ such that $h^j(K^{\bullet}) \neq 0$ and $h^i(K^{\bullet}) \neq 0$. We have already handled the base case since a complex that has cohomologies only in degree zero is quasi-isomorphic to a module viewed as a complex in that degree. Next suppose that the result is true in the case of $\leq l$ and consider a complex $K^{\bullet}$ where $h^j(K^{\bullet}) \neq 0$ and $h^i(K^{\bullet}) \neq 0$ where $l + 1 = j - i$.

Consider the exact triangle

$$h^i(K^{\bullet})[-i] \rightarrow K^{\bullet} \rightarrow C^{\bullet} \xrightarrow{+1}$$

[4]Note $H^d_{\mathfrak{m}}(R)$ is the top cohomology of $\mathbf{R}\Gamma_{\mathfrak{m}}(R)$ and so there always exists such a map.

$C^{\bullet}$ is just the truncation of $K^{\bullet}$ at the ith spot and so the inductive hypothesis implies that $C^{\bullet} \simeq_{\mathrm{qis}} C^{\bullet} \otimes^{\mathbf{L}}_{A^\infty} B^\infty$. Thus we have

$$\begin{array}{ccccccc} h^i(K^{\bullet})[-i] & \longrightarrow & K^{\bullet} & \longrightarrow & C^{\bullet} & \xrightarrow{+1} & \\ \downarrow\sim & & \downarrow & & \downarrow\sim & & \\ h^i(K^{\bullet})[-i] \otimes^{\mathbf{L}}_{A^\infty} B^\infty & \longrightarrow & K^{\bullet} \otimes^{\mathbf{L}}_{A^\infty} B^\infty & \longrightarrow & C^{\bullet} \otimes^{\mathbf{L}}_{A^\infty} B^\infty & \xrightarrow{+1} & \end{array}$$

The the vertical maps on the ends are quasi-isomorphisms and thus so is the map in the middle which proves the proposition. ☐

Theorem 3.25. *Let $(R, \mathfrak{m}, k)$ be a local d-dimensional F-injective ring of characteristic $p > 0$ such that $H^i_{\mathfrak{m}}(R)$ has finite length for $i < d$. Fix $K^{\bullet} \in D(R)$ as the $< d$-truncation of $\mathbf{R}\Gamma_{\mathfrak{m}}(R)$. Then $K^{\bullet} \in D^b(k)$ and hence R is Buchsbaum.*

Proof. We prove this only in the case when k is perfect (for simplicity) where we see that $R^\infty/\mathfrak{m}^\infty = k$. For the general case (with a proof along the same lines), see [**BMS15**].

Note $K^{\bullet}$ still has a Frobenius map $F : K^{\bullet} \longrightarrow K^{\bullet}$ which is injective on its cohomologies (which are the $H^i_{\mathfrak{m}}(R)$. But since the cohomologies have finite length, and so are finite dimensional k-vector spaces by Corollary 3.22, the Frobenius map is bijective on the cohomologies of $K^{\bullet}$.

Define $K^{\bullet}_\infty$ to be the $< d$-truncation of $\mathbf{R}\Gamma_{\mathfrak{m}}(R^\infty)$ and note that

$$h^i(K^{\bullet}_\infty) = \varinjlim_e F^e_* h^i(K^{\bullet}) = h^i(K^{\bullet})$$

where the second to last equality follows from the fact that Frobenius acts bijectively on the cohomology of $h^i(K^{\bullet})$. It follows that the canonical map $K^{\bullet} \longrightarrow K^{\bullet}_\infty$ is a quasi-isomorphism. But now $K^{\bullet} \simeq_{\mathrm{qis}} K^{\bullet}_\infty \simeq_{\mathrm{qis}} K^{\bullet}_\infty \otimes_{R^\infty} k$, which shows that $K^{\bullet}$ is quasi-isomorphic to a complex of k-vector spaces, as claimed. ☐

3.3. Serre's conditions and Hartog's Phenomenon. Suppose that S has dimension n and depth m. If $\mathfrak{q}$ is an ideal of height say $n-1$, it is possible that $\mathrm{depth}_{S_{\mathfrak{q}}} S_{\mathfrak{q}} = m$ and it is *also* possible that $\mathrm{depth}_{S_{\mathfrak{q}}} S_{\mathfrak{q}}$ has depth $m-1$. For example, consider R from Example 3.16 and set $S = R[w]$. It is not difficult to see that S has depth 2 at the origin (since if you mod out by w you get back R, which has depth 1). However, if one localizes at the prime ideal $\langle x, y, u, v\rangle$, you obtain a ring of depth 1 (you essentially get R with enlarged base field k to $k(w)$). On the other hand, localizing at $\langle x, y, u, w\rangle$ inverts v and so kills x and y and thus produces $k(v)[u, w]_{u,w}$, a ring of depth 2.

Because of this unpredictable behavior of depth under localization, we have the following definition.

Definition 3.26. A finitely generated module M over a Noetherian ring R is said to satisfy $\mathbf{S}_n$ if for every prime $\mathfrak{q} \in \mathrm{Spec}\, R$, $\mathrm{depth}\, M_{\mathfrak{q}} \geq \min\{n, \dim R_{\mathfrak{q}}\}$.[5]

[5] In some published work, $\dim R_{\mathfrak{q}}$ is replaced by $\dim M_{\mathfrak{q}}$ in this definition.

In particular, an $\mathbf{S}_n$-module is Cohen-Macaulay in codimension n and has depth $\geq n$ elsewhere.

A crucially important condition is $\mathbf{S}_2$, because it implies a Hartog's-like phenomenon. Before we do that, let's make a simple observation.

Lemma 3.27. *If $(R, \mathfrak{m})$ is a local ring, M is a module of depth ≥ 2, and $U = \operatorname{Spec} \setminus \mathfrak{m}$, then*

$$M \cong \Gamma(U, M).$$

PROOF. We have an exact sequence $H^0_{\mathfrak{m}}(M) \longrightarrow M \longrightarrow \Gamma(U, M) \longrightarrow H^1_{\mathfrak{m}}(M)$ and the two local cohomologies are zero by the depth condition. □

The point is that if a module is has depth ≥ 2, then it is completely determined by its behavior outside the origin. A more general statement holds when the module is $\mathbf{S}_2$.

Theorem 3.28. *Suppose $(R, \mathfrak{m})$ is a Noetherian local ring of dimension ≥ 2 and that M is an $\mathbf{S}_2$-module. If $I \subseteq R$ is an ideal such that $\dim V(I) \leq \dim R - 2$ and $U = \operatorname{Spec} R \setminus V(I)$, then $M \cong \Gamma(U, M)$.*

PROOF. We need to show that $M \longrightarrow \Gamma(U, M)$ is bijective and so let K be the kernel of C be the cokernel. Let Q be a minimal prime in the support of $K \oplus C$. In particular, $M_Q \longrightarrow \Gamma(U, M)_Q = \Gamma(U \cap \operatorname{Spec} R_Q, M_Q)$ is not bijective and $(K \oplus C)_Q$ is supported only at the maximal ideal. Since $\Gamma(U, M)_Q = M_Q$ (essentially by definition) if Q has height 1, we may assume that Q has height at least 2. Thus depth $M_Q \geq 2$ and so by Lemma 3.27, $M_Q \longrightarrow \Gamma(U \cap \operatorname{Spec} R_Q, M_Q)$ is bijective, a contradiction. □

Remark 3.29. $\mathbf{S}_2$-modules are often viewed as the modules that are determined by their behavior in codimension 1.

4. Local duality and Gorenstein rings

In this section we state local duality. First we need a brief review of injective hulls.

Definition 4.1. Suppose that R is a ring and M is an R-module. An overmodule $E \supseteq M$ is said to be an *essential extension of* M if for every submodule $D \subseteq E$, if $D \cap M = 0$ then $D = 0$.

An *injective hull* $E(M)$ of M is an essential extension of M that is also injective as an R-module.

Fact 4.2.
- Injective hulls exist for any module M.
- Injective hulls are unique up to *non*-unique isomorphism (fixing M).
- The formation of injective hulls commutes with localization, $W^{-1}E_R(M) = E_{W^{-1}R}(W^{-1}M)$.

Notation 4.3. For the rest of the semester, if $(R, \mathfrak{m}, k)$ is a local ring, then $E = E_{R/\mathfrak{m}} = E_k$ will denote the injective hull of $k = R/\mathfrak{m}$.

Example 4.4. In the case that $(R, \mathfrak{m}, k)$ is a regular local Noetherian ring (or more generally a Gorenstein[6] local Noetherian ring), $E_k \cong H^{\dim R}_{\mathfrak{m}}(R)$. This will follow from local duality below, but that's not the right way to prove it.

Let's quickly state Matlis duality which roughly says that Homing into the injective hull of the residue field of a local ring does not kill (much) information.

Theorem 4.5 (Matlis Duality)**.** *Suppose that $(R, \mathfrak{m})$ is a Noetherian local ring. Then:*

(1) *The functor $T(\_\_) = \operatorname{Hom}_R(\_\_, E)$ is faithful on the category of finitely generated R-modules and also on the category of Artinian R-modules.*
(2) *For Artinian modules N, $T(T(N)) \cong N$.*
(3) *For Noetherian modules M, $T(T(M)) \cong \widehat{M} = M \otimes_R \widehat{R}$.*
(4) *$T(\_\_)$ takes modules of finite length to modules of the same finite length.*

If in addition R is complete then

(5) *$T(\_\_)$ induces an antiequivalence[7] of categories*

$$\left\{ \begin{array}{c} \textit{Noetherian} \\ R\textit{-modules} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{Artinian} \\ R\textit{-modules} \end{array} \right\}.$$

We now define dualizing complexes.

Definition 4.6. Suppose that R is a Noetherian ring. An object $\omega^{\bullet} \in D^b_{f.g.}(R)$ is called a *dualizing complex for R* if the following two conditions are satisfied.

(a) $\omega^{\bullet}$ has finite injective dimension (is quasi-isomorphic to a bounded complex of injectives) and,
(b) The functor $\mathbf{D}(\_\_) = \mathbf{R}\operatorname{Hom}_R(\_\_, \omega^{\bullet})$ has the property that the canonical map $C^{\bullet} \to \mathbf{D}(\mathbf{D}(C^{\bullet}))$ is an isomorphism for all $C^{\bullet} \in D^b_{f.g.}(R)$.
(b') Or equivalently to (b), $R \cong \mathbf{R}\operatorname{Hom}_R(\omega^{\bullet}, \omega^{\bullet})$.

Exercise 4.1. Prove that (b') implies (b) above.

Fact 4.7. Dualizing complexes are unique up to two operations.

- Shift (if $\omega^{\bullet}$ is a dualizing complex, so is $\omega^{\bullet}[n]$).
- Tensoring with rank-1 projective modules (if P is a projective module of rank-1[8] then if $\omega^{\bullet}$ is a dualizing complex, so is $\omega^{\bullet}[n]$).

Lemma 4.8. *If $\omega^{\bullet}$ is a dualizing complex for a Noetherian ring R and W is a multiplicatively closed set, then $W^{-1}\omega^{\bullet}$ is a dualizing complex for $W^{-1}R$.*

Proof. Inverting multiplicatively closed sets preserves injectives in Noetherian rings and so condition (a) is fine in the definition of the dualizing complex. The same operation also preserves the isomorphism of (b'). □

Definition 4.9. A ring R is called *Gorenstein* if R has finite injective dimension as an R-module. Note for a Gorenstein ring, R is its own dualizing complex.

[6] to be defined soon
[7] *i.e.* , a contravariant equivalence
[8] Meaning that $P_Q \cong R_Q$ for all $Q \in \operatorname{Spec} R$.

Lemma 4.10. *A Noetherian ring R is Gorenstein if and only if R has a dualizing complex $\omega_R^\bullet \cong M[n]$ such that M is projective of rank 1.*

Example 4.11. Suppose that R is a regular local ring, then R is Gorenstein. To see this let $d = \dim R$ and observe that

$$\mathrm{Ext}^{d+1}(M, R) = 0$$

for all R-modules M (because R has finite global dimension d). But since this holds for all R-modules M, it implies that R itself has finite injective dimension.

More generally, if R is a regular ring it is also Gorenstein.

Remark 4.12. Not every ring has a dualizing complex, but nearly all the rings we care about do. In particular, any ring that is a quotient of a regular ring (or more generally a Gorenstein ring) has a dualizing complex. In particular, if $R = S/I$ where S is regular, then

$$\omega_R^\bullet = \mathbf{R}\operatorname{Hom}_S(R, S)$$

is a dualizing complex. It is certainly of finite injective dimension because if I is an injective S-module, $\operatorname{Hom}_S(R, I)$ is an injective R-module (so if we take a finite injective resolution of S applying $\operatorname{Hom}_S(R, \_\_)$ gives a complex of R-modules finite injective dimension) and then observe that

$$\begin{aligned} & \mathbf{R}\operatorname{Hom}_R(\mathbf{R}\operatorname{Hom}_S(M, S), \mathbf{R}\operatorname{Hom}_S(R, S)) \\ \cong\ & \mathbf{R}\operatorname{Hom}_S(\mathbf{R}\operatorname{Hom}_S(M, S) \otimes_R^L R, S) \\ \cong\ & \mathbf{R}\operatorname{Hom}_S(\mathbf{R}\operatorname{Hom}_S(M, S), S) \\ \cong\ & M \end{aligned}$$

where the last $\cong$ holds because S is a dualizing complex for S. In fact the argument we just used implies that if $S \longrightarrow R$ is any map of rings such that R is a finite S-module, and if $\omega_S^\bullet$ is a dualizing complex for S then $\mathbf{R}\operatorname{Hom}_S(R, \omega_S^\bullet)$ is a dualizing complex for R.

Corollary 4.13. *Suppose that $(R, \mathfrak{m})$ is an F-finite Noetherian local ring of characteristic $p > 0$ with a dualizing complex. Then $\operatorname{Hom}_R(F_*^e R, \omega_R^\bullet) =: \omega_{F_*^e R}^\bullet$ is a dualizing complex for $F_*^e R$. Furthermore, $F_*^e \omega_R^\bullet \simeq_{qis} \omega_{F_*^e R}^\bullet$.*

Exercise 4.2. Prove Corollary 4.13.

Hint: The fact that it is a dualizing complex is just what was worked out in the above example. Dualizing complexes are unique up to shifting and twisting by rank-one projectives. Use the fact that it is local to handle the rank-1 projective case. Then use the that the localization of a dualizing complex is a dualizing complex to handle the shift (localize at a minimal prime).

Remark 4.14. With the notation in the above corollary, the induced map

$$F_*^e \omega_R^\bullet \longrightarrow \omega_R^\bullet$$

dual to $R \longrightarrow F_*^e R$ is often called the trace of Frobenius for reasons that we will see later.

Example 4.15. If R is Gorenstein with dualizing complex $\omega_R^\bullet \simeq_{\rm qis} \omega_R[n]$ and if $f \in R$ is a nonzero divisor, then R/f is Gorenstein with dualizing complex

$$\omega_{R/f}^\bullet = \omega_R/f[n-1] = \mathrm{Ext}^1(R/f, \omega_R[n])$$

To see this, consider the short exact sequence

$$0 \to R \xrightarrow{\cdot f} R \to R/f \to 0$$

and apply $\mathbf{R}\,\mathrm{Hom}_R(\_\_, \omega_R^\bullet) = \mathbf{R}\,\mathrm{Hom}_R(\_\_, \omega_R[n])$. We obtain

$$\mathbf{R}\,\mathrm{Hom}_R(R/f, \omega_R[n]) \to \mathbf{R}\,\mathrm{Hom}_R(R, \omega_R[n]) \xrightarrow{\cdot f} \mathbf{R}\,\mathrm{Hom}_R(R, \omega_R[n]) \xrightarrow{+1}$$

and taking cohomology (starting at $-n$) yields

$$0 \to \omega_R \xrightarrow{\cdot f} \omega_R \to \mathrm{Ext}^1(R/f, \omega_R) \to 0 \to \dots$$

where the first zero $0 = \mathrm{Hom}_R(R/f, \omega_R)$ holds because ω_R is locally free and in particular, torsion free.

Finally, in order to state local duality, we need one more definition.

Definition 4.16. Suppose that $(R, \mathfrak{m})$ is a d-dimensional Noetherian local ring with dualizing complex $\omega_R^\bullet \in D^b_{f.g}(R)$. The dualizing complex $\omega_R^\bullet$ is called *normalized* if $h^j(\omega_R^\bullet) = 0$ for $j < -d$ and $h^{-d}(\omega_R^\bullet) \neq 0$.

The module $h^{-d}(\omega_R^\bullet)$ is called the *canonical module* and typically denoted by ω_R.

Remark 4.17. A normalized dualizing complex does not remain normalized after localization. In particular, if $\omega_R^\bullet$ is normalized for $(R, \mathfrak{m})$ and $\mathfrak{q} \in \operatorname{Spec} R$ is a prime, then $(\omega_R^\bullet)_{\mathfrak{q}}$ is not normalized even though it is still surjective.

We now state local duality.

Theorem 4.18 (Local duality)**.** *Suppose that $(R, \mathfrak{m}, k)$ is a local Noetherian domain with dualizing complex $\omega_R^\bullet$ and $C^\bullet \in D^b_{f.g.}(R)$ and injective hull of the residue field E. Then*

$$\mathrm{Hom}(\mathbf{R}\,\mathrm{Hom}_R(C^\bullet, \omega_R^\bullet), E) \simeq_{qis} \mathbf{R}\Gamma_{\mathfrak{m}}(C^\bullet).$$

In the case that R is complete, this can also be written as

$$\mathbf{R}\,\mathrm{Hom}_R(C^\bullet, \omega_R^\bullet) \simeq_{qis} \mathrm{Hom}_R(\mathbf{R}\Gamma_{\mathfrak{m}}(C^\bullet), E).$$

Note we do not need to derive the $\mathrm{Hom}(\_\_, E)$ functor since E is injective.

We now specialize this to other settings in order to deduce standard facts (this is not the right way to prove these facts, but it's not a bad way to remember their statements).

Corollary 4.19. *A Noetherian local ring $(R, \mathfrak{m})$ with a dualzing complex $\omega_R^\bullet$ is Cohen-Macaulay if and only if the dualizing complex for R is centered in one degree,*

$$\omega_R^\bullet \simeq_{qis} \omega_R[n].$$

Corollary 4.20. *With notation as above, if $\omega_R^\bullet$ is a normalized dualizing complex then* $\mathrm{Hom}_R(\omega_R^\bullet), E) \cong \mathbf{R}\Gamma_{\mathfrak{m}}(R)$.

While the above is obvious from the definition.

Corollary 4.21. *With notation as above, R is Gorenstein if and only if the normalized dualizing complex $\omega_R^\bullet \simeq_{qis} R[\dim R]$.*

Definition 4.22. A local ring $(R, \mathfrak{m})$ with a dualizing complex is called *quasi-Gorenstein* (or 1-Gorenstein) if $\omega_R \cong R$.

Corollary 4.23. *An F-injective quasi-Gorenstein F-finite local ring is F-split.*

PROOF. Since R is F-injective, $H^d_{\mathfrak{m}}(R) \longrightarrow H^d_{\mathfrak{m}})(F_* R)$ is injective. But this map is Matlis dual to what we called the trace $F_*\omega_R \longrightarrow \omega_R$, which now must be surjective (if it had a cokernel, then the map on local cohomology would have a cokernel, which it doesn't). But since R is quasi-Gorenstein, $\omega_R \simeq R$ and so we have a surjective map $F_* R \longrightarrow R$. This implies that R is F-split. ☐

We'll state some more facts about dualizing complexes (taken for example out of [**Har66**] or [**Sta16**]). For time reasons, we'll skip the proofs.

Lemma 4.24. *Let $(R, \mathfrak{m}, k)$ be a local Noetherian ring with normalized dualizing complex $\omega_R^\bullet$ and canonical module $\omega_R = h^{-\dim R}\omega_R^\bullet$. Then*

(a) The support of ω_R is equal to the union of irreducible components of $\operatorname{Spec} R$ *of maximal dimension.*
(b) ω_R is $\mathbf{S}_2$.

PROOF. See [**Sta16**, Tag 0AWE], there are some subtle points here: for example rings with dualizing complexes are catenary. ☐

Corollary 4.25. *Suppose that $(R, \mathfrak{m})$ is a local Noetherian domain. Then for any $0 \leq i < \dim R$, $\operatorname{Ann}_R H^i_{\mathfrak{m}}(R) \neq 0$. In particular, for each $i < H^i_{\mathfrak{m}}(R)$, there exists some $0 \neq c \in R$ such that $c \cdot H^i_{\mathfrak{m}}(R) = 0$.*

PROOF. If $\omega_R^\bullet$ is a normalized dualizing complex for R, it is sufficient (in fact equivalent) to find $0 \neq c$ such that $c \cdot h^{-i}(\omega_R^\bullet) = 0$ by local duality (and the fact that $\operatorname{Hom}_R(\_\_, E)$ is faithful on the modules in question). Now, $h^{-i}(\omega_R^\bullet)$ is finitely generated so it suffices to show that it is not supported everywhere. Now, if we localize at the unique minimal prime Q, we end up with a dualizing complex on a field, which lives in exactly one degree. This degree must be $-\dim R$ by the previous lemma, and so all the other $h^{-i}(\omega_R^\bullet)$ are not supported everywhere as claimed. ☐

Note that $\operatorname{Ann}_R H^{\dim R}(R) = 0$ and so the above is about as good as one can do. Note a version of the above also holds for non-domains (you can pick c not in any minimal prime defining a maximal component of $\operatorname{Spec} R$).

5. F-regularity, a quick way to prove that rings are Cohen-Macaulay

Historically, F-splittings were used to prove lots of rings were Cohen-Macaulay. In modern times, we have learned some really slick ways to prove that integral domains are Cohen-Macaulay.

Definition 5.1. An F-finite ring is called *strongly F-regular* if for every $c \in R$ not contained in any minimal prime, there exists an $e > 0$ such that the map $R \longrightarrow F^e_* R \xrightarrow{F^e_* \cdot c} F^e_* R$ splits as a map of R-modules.

Remark 5.2. Strongly F-regular rings are now known to be the characteristic $p > 0$ analog of rings with KLT singularities in characteristic zero.

Theorem 5.3. *A strongly F-regular Noetherian local domain is Cohen-Macaulay.*

Proof. Fix some $i < \dim R$, we shall show that $H^i_{\mathfrak{m}}(R) = 0$. By Corollary 4.25, we can choose $0 \neq c \in R$ such that $c \cdot H^i_{\mathfrak{m}}(R) = 0$. Now choose an $e > 0$ so that $R \longrightarrow F^e_* R \xrightarrow{F^e_* \cdot c} F^e_* R$ splits as a map of R-modules. Applying $H^i_{\mathfrak{m}}(\_\_)$ we see that

$$H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(F^e_* R) \xrightarrow{F^e_* \cdot c} H^i_{\mathfrak{m}}(F^e_* R)$$

is also injective. But $H^i_{\mathfrak{m}}(F^e_* R) = F^e_* H^i_{\mathfrak{m}^{[p^e]}}(R) = F^e_* H^i_{\mathfrak{m}}(R)$ and so $F^e_* c$ kills it. Thus we have an injective map that is also the zero map, and so the source is zero as claimed. □

Remark 5.4. The *domain* hypothesis is not necessary above, indeed strongly F-regular local rings are normal as we will see shortly, which then implies that they are domains.

This is not so impressive unless you can show that various rings are strongly F-regular. Here are some common ways to prove that rings are strongly F-regular.

Proposition 5.5. *If $(R, \mathfrak{m})$ is a Noetherian local F-finite regular domain, then R is strongly F-regular.*

Proof. Fix $0 \neq c \in R$. Choose $e \gg 0$ so that $c \notin \mathfrak{m}^{[p^e]}$ and so $F^e_* c \notin \mathfrak{m} \cdot F^e_* R = F^e_* \mathfrak{m}^{[p^e]}$. Since a basis for $(F^e_* R)/\mathfrak{m}$ becomes a minimal generating set and hence a basis for the free module $F^e_* R$ (here we use that R is regular), we see that $F^e_* c$ is part of a basis for $F^e_* R$ over R. Thus we can project from $F^e_* c$ to R which produces the map we wanted. □

Proposition 5.6. *Suppose that $R \subseteq S$ is an inclusion of Noetherian domains such that $S \cong R \oplus M$ as R-modules. Then if S is strongly F-regular, so is R.*

Proof. Choose $0 \neq c \in R$. Since S is strongly F-regular, there exists a $\phi : F^e_* S \longrightarrow S$ such that $\phi(F^e_* c) = 1$. Let $\rho : S \longrightarrow R$ be such that $\rho(1_S) = 1_R$ (this exists since $S \cong R \oplus M$). Then the composition $F^e_* R \subset F^e_* S \xrightarrow{\phi} S \xrightarrow{\rho} R$ sends $F^e_* c$ to 1 which proves that R is strongly F-regular. □

Remark 5.7. The above is an open problem in characteristic zero for KLT singularities.

Corollary 5.8. *A direct summand of a regular ring in characteristic $p > 0$ is Cohen-Macaulay.*

The above is obvious if we are taking a finite local inclusion of local rings of the same dimension. It is not so obvious otherwise (indeed, it has perhaps only recently been discovered how to show that direct summands of regular rings in mixed characteristic are Cohen-Macaulay).

Proposition 5.9. *If R is an F-finite ring such that $R_{\mathfrak{m}}$ is strongly F-regular for each maximal $\mathfrak{m} \in \operatorname{Spec} R$, then R is strongly F-regular.*

PROOF. Obviously strongly F-regular rings are F-split (take $c = 1$) and so R is F-split. By post composing with Frobenius splittings, if we have a map $\phi : F^e_* R \longrightarrow R$ which sends $F^e_* c \mapsto 1$, then we can replace e by a larger e. Now, pick $0 \neq c \in R$. For each $\mathfrak{m} \in \operatorname{Spec} R$, $\operatorname{Hom}_R(F^e_* R, R)_{\mathfrak{m}} \xrightarrow{eval@c} R_{\mathfrak{m}}$ is surjective for $e \gg 0$. But thus for each $\mathfrak{m}$, there exists a neighborhood $U_{\mathfrak{m}}$ of $\mathfrak{m}$ and some $e_{\mathfrak{m}}$ such that $\operatorname{Hom}_R(F^e_* R, R)_{\mathfrak{n}} \xrightarrow{eval@c} R_{\mathfrak{n}}$ surjects for all $\mathfrak{n} \in U_{\mathfrak{m}}$ where we take $e = e_{\mathfrak{m}}$. These $U_{\mathfrak{m}}$ cover $\operatorname{Spec} R$ and since $\operatorname{Spec} R$ is quasi-compact, we may pick finitely many of them, choose a common large enough $e > 0$ and observer that $\operatorname{Hom}_R(F^e_* R, R) \xrightarrow{eval@c} R$ surjects as desired. □

Theorem 5.10. *Suppose that $0 \neq d \in R$ is such that $R[d^{-1}]$ is strongly F-regular and such that there exists a map $\phi : F^e_* R \longrightarrow R$ satisfying $\phi(F^e_* d) = 1$. Then R is strongly F-regular.*

PROOF. Note first that R is F-split (pre-multiply ϕ by $F^e_* d$). Choose $0 \neq c \in R$ and consider the map $\Phi_f : \operatorname{Hom}_R(F^f_* R, R) \xrightarrow{eval@c} R$ for some $f \gg 0$. Because $R[d^{-1}]$ is strongly F-regular, $d^m \in \operatorname{Image}(\Phi_f)$ for some $f \gg 0$ and some $m > 0$. Without loss of generality, we may assume that $m = p^l$ for some integer l (note making m larger is harmless). In particular, there exists $\psi \in \operatorname{Hom}_R(F^f_* R, R)$ such that $\psi(F^f_* c) = d^{p^l}$. Let $\kappa : F^l_* R \longrightarrow R$ be a Frobenius splitting and notice that $\kappa(F^l_* \psi(F^f_* c)) = \kappa(d^{p^l}) = d$. Finally

$$\phi(F^e_* \kappa(F^l_* \psi(F^f_* c))) = \phi(F^e_* d) = 1$$

and so $\phi \circ (F^e_* \kappa) \circ (F^{e+f}_* \psi)$ is the desired map. □

For a computer, the above is not so bad. To show that $R = S/I$ (where S is a polynomial ring say) is strongly F-regular, you just need to find $d \in S$ in the ideal of the singular locus of $V(I)$ such that $\Phi(c \cdot (I^{[p^e]} : I)) = S$ where Φ is the map from the second Macaulay2 assignment. Note that this can only prove that a singularity is strongly F-regular, it can't prove that a singularity isn't. We don't have a good algorithm to do this in general but we do have algorithms that work if the ring is quasi-Gorenstein (or $\mathbb{Q}$-Gorenstein, a notion we'll learn about later).

6. A crash course in (ab)normality

Definition 6.1. Suppose that R is a ring. We let

$$K(R) = \{a/b \mid a, b \in R \text{ where } b \text{ is not a zero divisor }\}.$$

denote the *total ring of fractions.*

In the case that R is a reduced Noetherian ring with minimal primes $Q_1, \dots, Q_t$, then each R/Q_i is an integral domain with field of fractions $K(R/Q_i)$. In this case, $K(R) \cong \prod K(R/Q_i)$ (easy exercise, or look it up).

Definition 6.2. Given a reduced Noetherian ring R, the *normalization* R^{N} *of* R *in* $K(R)$ (or just the *normalization of* R) is defined to be

$$\{x \in K(R) \mid x \text{ satisfies a monic polynomial with coefficients in } R\}.$$

R is called *normal* if $R = R^{\mathrm{N}}$.

Fact 6.3. Under moderate hypotheses (excellence, so for all rings we care about), R^{N} is a finitely generated R-module. We will take this as a fact at least for now.

Lemma 6.4. *In a reduced ring R, the set of zero divisors is equal to $\bigcup Q_i$ where Q_i is the set of minimal primes.*

Proof. Suppose x is a zero divisor $xy = 0$, $y \neq 0$. If $x \notin Q_i$ for any i, then since $xy = 0 \in Q_i$, $y \in Q_i$ for all i. But $\bigcap Q_i = \langle 0 \rangle$ since R is reduced.

For the reverse direction fix some minimal prime Q_i and let W be the multiplicative set generated by $R \setminus Q_i$ and by the set of nonzero divisors of R. Note $0 \notin W$ because if it was, then $0 = ab$ for $a \notin Q_i$ and b not a zero divisor. Let $W^{-1}P$ be a maximal ideal of $W^{-1}R$ with $P \subseteq R$ the inverse image in R. Thus P is a prime ideal of R which doesn't contain any element of W. Obviously then $P \subseteq Q_i$, but since Q_i is minimal $P = Q_i$. But P doesn't contain any non-zero divisors, and so Q_i is completely composed of zero divisors. $\square$

Our goal for this section is to understand normal rings, non-normal rings, and some weakenings of the condition that R is normal. First let's understand $K(R)$.

Lemma 6.5. *Suppose that R is a reduced Noetherian ring, then $K(R) = \prod_{i=1}^t K_i$ is a finite product of fields.*

Proof. First we observe that R has only finitely many minimal primes. To see this write $\langle 0 \rangle = \bigcap_{i=1}^t P_i$ as a primary decomposition of $\langle 0 \rangle$. Any prime (minimal with respect to the condition that it contains 0 – any prime) is among this set (since the primes in primary decomposition commute with localization in as much as possible). Next let Q_i be the minimal primes, we claim that $\langle 0 \rangle = \bigcap_i Q_i$, one containment is obvious. On the other hand, if x is in every minimal prime then it is in every prime, and so x is nilpotent.

Now, if we localize a reduced ring at a minimal prime, we get a reduced ring with a single prime, in other words a field. Consider the diagonal map

$$\delta : R \longrightarrow \prod_i R_{Q_i}.$$

Note that $Q_i R_{Q_i}$ is zero since it's a nonzero ideal in a field hence each $R \longrightarrow R_{Q_i}$ factors through R/Q_i (which injects into R_{Q_i}). Thus $\ker \delta = \bigcap Q_i = \langle 0 \rangle$. On the other hand, every nonzero divisor of R certainly maps to a nonzero divisor of $\prod_i R_{Q_i}$ where it is already invertible and so we have map $\gamma : K(R) \longrightarrow \prod_i R_{Q_i}$. We need to show that this map is a bijection. It is injective since $K(R)$ is itself Noetherian and the minimal primes of R contain only zero divisors and so the minimal primes of $K(R)$ agree with the minimal primes of R. From hear on, we may assume $K(R) = R$. Let Q_1, Q_2 be minimal primes of $K(R)$ and consider $Q_1 + Q_2$. Since $Q_1 + Q_2$ is not contained in any single minimal prime Q_i, $Q_1 + Q_2$ is not contained in $\bigcup Q_i$ by prime avoidance. But in a reduced ring, $\bigcup Q_i$ is the set of zero divisors and so $Q_1 + Q_2$ contains a nonzero divisor and so $Q_1 + Q_2 = K(R)$ (since nonzero divisors are invertible). But now we've show that the Q_i are pairwise relatively prime and so γ is surjective by the Chinese Remainder Theorem. □

Lemma 6.6. *If we have an extension of rings $R \subseteq R' \subseteq K(R)$ such that R' is a finite R-module and R is Noetherian, then $R' = R$.*

Proof. Choose $x \in R'$ and so reduce to the case where $R' = R[x] \subseteq K(R)$. On the other hand, consider the ascending chain of R-submodules of $K(R)$ $R \subseteq R \oplus xR \subseteq R \oplus xR \oplus x^2R \subseteq \cdots \subseteq \bigoplus_{i=1}^n x^iR \subseteq \ldots$. Eventually this stabilizes to R' and since R' is a Noetherian R-module, this happens at a finite step. Thus for some $n \gg 0$, $x^n \in \bigoplus_{i=1}^n x^iR \subseteq R'$. In other words, x satisfies a monic polynomial with coefficients in R and so $x \in R$ and thus $R' = R$ as claimed. □

Exercise 6.1. The formation of R^{N} commutes with localization, in particular if $W \subseteq R$ is a multiplicative set then $(W^{-1}R)^{\mathrm{N}} = W^{-1}(R^{\mathrm{N}})$.

As a corollary of the previous exercise, we immediately obtain the following.

Corollary 6.7. *A ring is normal if and only if each of its localizations $R_{\mathfrak{m}}$ are normal for maximal ideals $\mathfrak{m}$.*

Proposition 6.8. *If $(R, \mathfrak{m})$ is a reduced Noetherian local normal ring then R is an integral domain.*

Proof. Suppose that $K(R) = \prod_{i=1}^t K_i$ is a product of fields. We need to show that $t = 1$ since $R \subseteq K(R)$. □

Definition 6.9. A ring is called $\mathbf{R}_n$ if for every prime $Q \in \operatorname{Spec} R$ of height $\leq n$, R_Q is regular.

Lemma 6.10. *A Noetherian normal local 1-dimensional domain is regular. In particular, normal rings are $\mathbf{R}_1$.*

Proof. For the first statement, such a domain obviously has two prime ideals, 0 and $\mathfrak{m}$. We need to show that $\mathfrak{m}$ is principal and so choose $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Now, $R/\langle x \rangle$ is dimension zero and so as an R-module, has $\mathfrak{m}$ as an associated prime. Thus there exists $y \in R$ with $\overline{y} \in R/\langle x \rangle$ such that $\operatorname{Ann}_R \overline{y} = \mathfrak{m}$. In other words

$$y \notin \langle x \rangle \text{ but } y \cdot \mathfrak{m} \in \langle x \rangle.$$

Now consider $y/x \in K(R)$, we observe that $(y/x) \cdot \mathfrak{m} \subseteq R$ even though $y/x \notin R$ (since otherwise $y \in \langle x \rangle$).

Form $\mathfrak{m}^{-1} = R :_{K(R)} \mathfrak{m} = \{a \in K(R) \mid a\mathfrak{m} \subseteq R\}$ and consider $\mathfrak{m} \cdot \mathfrak{m}^{-1} \subseteq R$. Since $R \subseteq \mathfrak{m}^{-1}$, we see that $\mathfrak{m} \subseteq \mathfrak{m} \cdot \mathfrak{m}^{-1}$. By construction, $y/x \in \mathfrak{m}^{-1}$ and so if

$\mathfrak{m} = \mathfrak{m} \cdot \mathfrak{m}^{-1}$, then $y/x \cdot \mathfrak{m} \subseteq \mathfrak{m}$. Thus we can view $(\cdot(y/x)) \in \operatorname{Hom}_R(\mathfrak{m}, \mathfrak{m})$ and thus $(y/x)^n + a_1(y/x)^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathfrak{m}^i$ by the determinant trick (which leads to the proof of Nakayama's lemma). But then y/x is integral over R and thus since R is integrally closed, $y/x \in R$ a contradiction to the assumption that $\mathfrak{m} = \mathfrak{m} \cdot \mathfrak{m}^{-1}$. Thus $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$. Now consider $x \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{m} \cdot \mathfrak{m}^{-1} = R$ and observe that if $x \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{m}$, then $\langle x \rangle = x \cdot \mathfrak{m}^{-1}\mathfrak{m} \subseteq \mathfrak{m}^2$ contradicting our choice of x. Hence $x \cdot \mathfrak{m}^{-1} = R$ as well and so

$$\langle x \rangle = x \cdot \mathfrak{m}^{-1} \cdot \mathfrak{m} = \mathfrak{m} \cdot R = \mathfrak{m}$$

proving that $\mathfrak{m}$ is principal as desired.

The second statement is a direct corollary for the first since normality of Noetherian rings localizes by Exercise 6.1. □

Lemma 6.11. *A normal Noetherian reduced local ring $(R, \mathfrak{m})$ is a domain.*

Proof. Let $Q_1, \ldots, Q_m$ be the minimal primes of R. Then consider the inclusion $R \hookrightarrow \prod_i R/Q_i = R'$. Obviously R' is a finite R-module (since it's a product of finitely many finite R-modules). Thus since R is normal, and obviously $R' \subseteq K(R)$, we have that $R = R'$. But R' is not local unless there is only one Q_i (each R/Q_i is local). □

Lemma 6.12. *A normal Noetherian ring with a dualizing complex is $\mathbf{S}_2$.*

Proof. The statement is local so we assume that R is a normal local domain. It is easy to see that normal domains are $\mathbf{S}_1$ since they are domains and so regular elements are not hard to find. Thus we need to show that $H^1_Q(R_Q) = 0$ for all $Q \in \operatorname{Spec} R$ of height at least 2. Thus we may as well assume $(R, \mathfrak{m})$ is a local Noetherian, normal domain of dimension ≥ 2 and set $U = \operatorname{Spec} R \setminus \mathfrak{m}$ to be the punctured spectrum. We denote by $\omega_R^{\bullet}$ a normalized dualizing complex. By Corollary 3.8 it suffices to show that

$$R \longrightarrow R' := \Gamma(U, R)$$

is surjective. It is not difficult to see that $R' \subseteq K(R)$ since if you tensor map defining R' by $K(R)$, the kernel of the tensored map is clearly $K(R)$. We know that the cokernel of $R \longrightarrow R'$ is $H^1_{\mathfrak{m}}(R)$. Since R is reduced it is $\mathbf{S}_1$ so it is an easy exercise in localizing dualizing complexes to verify that $h^{-1}\omega_R^{\bullet}$ has zero dimensional support (is supported at the closed point). In particular, $\mathfrak{m}^d \cdot h^{-1}\omega_R^{\bullet} = 0$ and so $h^{-1}\omega_R^{\bullet}$ is Artinian. It follows that its Matlis dual $H^1_{\mathfrak{m}}(R)$ is Noetherian. Thus R' is an extension of Noetherian R-modules, R and $H^1_{\mathfrak{m}}(R)$ and so R' is Noetherian. But now every element of R' is integral[9] over R (basically for the same reason that finite field extensions are algebraic) and so $R' \subseteq R^{\mathrm{N}} = R$ which completes the proof. □

Theorem 6.13. *An excellent[10] reduced Noetherian ring R with a dualizing complex is normal if and only if it is $\mathbf{S}_2$ and $\mathbf{R}_1$.*

Proof. We already have seen that normal rings are $\mathbf{S}_2$ and $\mathbf{R}_1$. Conversely, if R is $\mathbf{S}_2$ and $\mathbf{R}_1$ and R^{N} is the normalization of R, then since R is is excellent, R^{N} is a finite

[9]satisfy a monic polynomial equation

[10]We only include this to guarantee that R^{N} is a finitely generated R-module

R-module and so the locus where R is not normal, $Z = V(\mathrm{Ann}_R(R^{\mathrm{N}}/R))$, is closed. Since R is $\mathbf{R}_1$, Z has codimension at least 2 locally in $\operatorname{Spec} R$, thus $U = \operatorname{Spec} R \setminus Z$ is the complement of a codimension 2 set and so $R \longrightarrow \Gamma(U, R)$ is an isomorphism since R is $\mathbf{S}_2$ using Theorem 3.28.

Claim 6.14. *R^{N} is $\mathbf{S}_2$ as an R-module.*

Proof of claim. Choose P a prime ideal of R and suppose that $P = Q \cap R$ a prime ideal of R^{N}. We know that $H^i_{QR^{\mathrm{N}}_Q}(R^{\mathrm{N}}) = 0$ for $i = 0, 1$ since R^{N} is $\mathbf{S}_2$. On the other hand, $\sqrt{PR^{\mathrm{N}}}$ is an intersection of finitely many prime ideals, $Q_1, \ldots, Q_d$ such that $Q_j \cap R = P$. Then

$$H^i_{PR_P}(R^{\mathrm{N}}_P) = H^i_{PR^{\mathrm{N}}_P}(R^{\mathrm{N}}_P) = H^i_{\sqrt{PR^{\mathrm{N}}_P}}(R^{\mathrm{N}}_P) = \bigoplus_j H^i_{Q_j}(R^{\mathrm{N}}_{Q_j})$$

where the last equality comes from the fact that the functors $\Gamma_{\sqrt{PR^{\mathrm{N}}}}(\underline{\quad}) = \bigoplus_j \Gamma_{Q_j}(\underline{\quad})$ for the semi-local ring R^{N}_P. But now we are done since the right side is zero for $i = 0, 1$. □

Since R^{N} is a $\mathbf{S}_2$ R-module, we have that $R^{\mathrm{N}} \longrightarrow \Gamma(U, R^{\mathrm{N}})$ is an isomorphism. Finally, we see that $\Gamma(U, R) \longrightarrow \Gamma(U, R^{\mathrm{N}})$ is an isomorphism as well (since R and R^{N} agree on U). Putting this together we get the commutative diagram

$$\begin{array}{ccc} R & \longrightarrow & R^{\mathrm{N}} \\ \sim\downarrow & & \downarrow\sim \\ \Gamma(U, R) & \xrightarrow[\sim]{} & \Gamma(U, R^{\mathrm{N}}) \end{array}$$

from which it follows that $R \longrightarrow R^{\mathrm{N}}$ is an isomorphism as well. □

Remark 6.15. We included some hypotheses above to make our lives easier that are not strictly necessary. Indeed, the above holds even without assuming that R is excellent with a dualizing complex.

Note, in many cases it is easy to verify that certain rings are normal. Indeed if R is Gorenstein (for example, if it is defined by a hypersurface or a complete intersection) and $\mathbf{R}_1$, then it is automatically normal. For example, $k[x, y, z]/\langle x^a + y^b - z^c \rangle$ is normal if p does not divide a, b, c since then the singular locus is at the origin (using the Jacobian criterion).

In the previous proof, the ideal $\mathrm{Ann}_R(R^{\mathrm{N}}/R)$ appeared, this ideal has a special name.

Definition 6.16. The ideal $\mathfrak{c} := \mathrm{Ann}_R(R^{\mathrm{N}}/R)$ is called the *conductor of R^{N} over R*. It is also an ideal of R^{N}.

Let's now move towards a proof that strongly F-regular rings are normal.

Lemma 6.17. *Suppose that R is an F-finite Noetherian reduced ring of characteristic $p > 0$ and pick $\phi \in \mathrm{Hom}_R(F^e_* R, R)$. Then $\phi(F^e_* \mathfrak{c}) \subseteq \mathfrak{c}$.*

Proof. Tensoring $\phi : F^e_* R \longrightarrow R$ by $K(R)$ induces a map $\phi_{K(R)} : F^e_* K(R) \longrightarrow K(R)$ which restricts to ϕ and so which we also denote by ϕ. Choose $x \in \mathfrak{c}$ and $r \in R^{\mathrm{N}}$. Then $\phi(F^e_* x) \cdot r = \phi(F^e_*(r^{p^e} x))$. But $r^{p^e} \in R^{\mathrm{N}}$ and $xR^{\mathrm{N}} \subseteq R$ so $\phi(F^e_*(r^{p^e} x)) \in R$. Thus $\phi(F^e_* x) \cdot R^{\mathrm{N}} \subseteq R$ and so $\phi(F^e_* x) \in \mathfrak{c}$ as desired. □

Corollary 6.18. *Strongly F-regular rings are normal.*

Proof. If R was not normal, then the conductor satisfies $0 \neq \mathfrak{c} \neq R$ and so choose $0 \neq c \in \mathfrak{c}$. By hypothesis, $\phi(F^e_* c) \subseteq \mathfrak{c}$ and so $\phi(F^e_* c) \neq 1$ for any $\phi \in \operatorname{Hom}_R(F^e_* R, R)$ which proves that R is not strongly F-regular. □

Example 6.19. $R = k[x,y]/\langle xy \rangle$ is F-split, by Fedder's criterion, but not normal since it is not $\mathbf{R}_1$. So we cannot weaken the above strongly F-regular hypothesis to simply being F-split.

Let's discuss an example of a non-normal ring.

Example 6.20 (The node)**.** Consider the ring $S = k[x]$ and consider the subring $R = \{f \in S \mid f(0) = f(1)\}$ which one can also view as the pullback of the diagram

$$S \xrightarrow{\alpha} S/\langle x \rangle \cap \langle x-1 \xleftarrow{\beta} k.$$

In other words $\{(s,t) \in S \oplus k \mid \alpha(s) = \beta(t)\}$. We claim that

$$R = k[x(x-1), x^2(x-1)] \subseteq k[x] = S.$$

Obviously $x(x-1)$ and $x^2(x-1)$ are both in R. On the other hand, if $f \in R$ with $f(0) = f(1) = \lambda$, then $f - \lambda \in R$ and viewing $f - \lambda \in S$, we see that $f \in \langle x(x-1) \rangle_S = I_S \subseteq R$. Thus the question is, are the elements $a = x(x-1)$, $b = x^2(x-1)$ enough to produce all of I_S by multiplying a, b together and scaling them by elements of k. For example, if we have $hx(x-1) \in I$ with $h = h_0 + h_1 x + h_2 x^2 + \dots$, we can certainly assume that $h = h_2 x^2 + \dots$ (since lower degree terms are easy to handle with a, b). But

$$c = x^2 \cdot x(x-1) = a^2 + b, d = x^3 * (x-1) = a * b - c$$

and so on...

On the other hand, it is easy to verify that $R = k[a,b]/\langle a^3 + a * b - b^2 \rangle$.

Example 6.21. Similarly, it is not difficult to see that $R = k[x^2, x^3] \subseteq k[x] = S$ is the pullback of $(S \longrightarrow S/\langle x^2 \rangle \leftarrow k)$. In particular, the cusp can be thought of as what you get when you kill first order tangent information at the origin of $\mathbb{A}^1$.

Theorem 6.22. *Suppose that we have a diagram of rings* $(A \twoheadrightarrow A/I \xleftarrow{g} B)$ *and let* $C = \{(a,b) \mid \overline{a} = g(b)\}$ *be the pullback. Then* $\operatorname{Spec} C$ *is the pushout of the diagram of induced map of topological spaces* $\{\operatorname{Spec} A \leftarrow \operatorname{Spec} A/I \rightarrow \operatorname{Spec} B\}$.

Proof. I will only sketch this in the category of sets, I will leave the verification that it behaves properly on thhe level of topological spaces as an exercise to the reader.

First consider the following ideal $J = \{(i,0) \mid i \in I\} \subseteq C$. It is easy to see that $C/J \cong B$ and so C contains a copy of $\operatorname{Spec} C$, $V(J) \subseteq \operatorname{Spec} C$. On the other hand, for any prime ideal of $\operatorname{Spec} C$ not containing J, doesn't contain some $(i,0)$ and so if we let $W = \{(i,0),(i^2,0),\dots\}$ denote the induced multiplicative set, we see that $W^{-1}(C) \cong W^{-1}A = A[i^{-1}]$. From this it is not hard to see that the primes of $\operatorname{Spec} C$ that don't contain J correspond precisely to the primes of $\operatorname{Spec} A$ that don't contain I (the map $\operatorname{Spec} C \longrightarrow \operatorname{Spec} A$ is an isomorphism outside of $V(J)$ and $V(I)$). Putting this together plus the commutative diagram

$$\begin{array}{ccccc} & & A/I & & \\ & \nearrow & & \nwarrow & \\ A & & & & B \\ & \nwarrow & & \nearrow & \\ & & C & & \end{array}$$

is enough to prove the result. $\square$

We now prove that every non-normal ring arises this way.

Proposition 6.23. *Suppose that R is a reduced non-normal ring with normalization R^{N} and suppose that $R \subseteq S \subseteq R^{\mathrm{N}}$. Let $\mathfrak{c} = \operatorname{Ann}_R(S/R)$ denote the conductor of $R \subseteq S$ and recall it is an ideal in both R and S. The R is the pullback of $(S \longrightarrow S/\mathfrak{c} \leftarrow R/\mathfrak{c})$.*

Proposition 6.24. *Let C denote the pullback and so by the universal property, we have a map $R \longrightarrow C$. We need to prove it is an isomorphism. It is obviously an injection since we already have $R \subseteq S$. Thus we need to show that $R \longrightarrow C$ is surjective. Choose an element $(s,\overline{r}) \in C$. Choose $r \in R$ whose image in $R/\mathfrak{c}$ is $\overline{r}$. Now then $s-r \in R^{\mathrm{N}}$ and is sent to zero $S/\mathfrak{c}$ and so $s-r \in \mathfrak{c} \subseteq R$. Therefore $s \in R$ as well and so $(s,\overline{r})$ is the image of $s \in R$ which proves that $R \longrightarrow C$ is an isomorphism.*

In other words, a normal ring is a ring without any excess gluing and non-normal rings are obtained from normal ones by gluing points (or subschemes) together and killing (higher) tangent spaces. At this point it is also not hard understand where non-$\mathbf{S}_2$ rings come from as well. They arise as gluings where the conductor has information in codimension 2. On the other hand if your gluing information is pure codimension 1, then the resulting non-normal ring will be $\mathbf{S}_2$ but not $\mathbf{R}_1$.

7. Frobenius splittings of non-normal rings

Suppose that R is not normal but that it is F-split (this isn't impossible, the node is F-split by Fedder's criterion, although the cusp is not).

Lemma 7.1. *Suppose that R is an F-finite reduced Noetherian ring with normalization R^{N}. Further suppose that $\phi : F^e_* R \longrightarrow R$ is an R-linear map. Then ϕ extends to $\phi_{K(R)} : F^e_* K(R) \longrightarrow K(R)$ which restricts to $\phi_{R^{\mathrm{N}}} : F^e_* R^{\mathrm{N}} \longrightarrow R^{\mathrm{N}}$.*

Proof. The extension is easy, simply consider the image $\phi \in \operatorname{Hom}_R(F^e_* R, R) \longrightarrow \operatorname{Hom}_R(F^e_* R, R) \otimes_R K(R) \cong \operatorname{Hom}_R(F^e_* K(R), K(R))$. It is easy to verify that this image $\phi_{K(R)}$ extends ϕ. By restriction we then get a map $\phi_{R^{\mathrm{N}}} : F^e_* R^{\mathrm{N}} \longrightarrow K(R)$. We just need to show that the image lies in R^{N}. Choose $x \in R^{\mathrm{N}}$ and consider $\phi_{R^{\mathrm{N}}}(F^e_* x)$.

Let Q_i denote the minimal primes of R. It is not hard to see that $\phi(F^e_* Q_i) \subseteq Q_i$ for all i (simply localize that Q_i which turns ϕ into a map on the field level, which sends 0 to 0) and so we have induced maps $\phi_i : F^e_*(R/Q_i) \longrightarrow R/Q_i$. But since $R^{\mathrm{N}} = \prod_i (R/Q_i)^{\mathrm{N}}$, it suffices to assume that R is a domain. Let $\mathfrak{c}$ denote the conductor of R in R^{N}. Consider $\mathfrak{c} \cdot \phi_{R^{\mathrm{N}}}(F^e_* R)$. For $z \in \mathfrak{c}$ and any integer $m > 0$

$$\begin{array}{rl} & z \cdot (\phi_{R^{\mathrm{N}}}(F^e_* x))^m \\ = & z \cdot (\phi_{R^{\mathrm{N}}}(F^e_* x)) \cdot (\phi_{R^{\mathrm{N}}}(F^e_* x))^{m-1} \\ = & \phi_{R^{\mathrm{N}}}(F^e_* z^{p^e} x) \cdot (\phi_{R^{\mathrm{N}}}(F^e_* x))^{m-1} \\ \in & \phi_{R^{\mathrm{N}}}(F^e_* \mathfrak{c})(\phi_{R^{\mathrm{N}}}(F^e_* x))^{m-1} \\ \subseteq & \mathfrak{c} \\ \subseteq & R \end{array}$$

In other words if $y = \phi_{R^{\mathrm{N}}}(F^e_* x)$, then $z \cdot y^m \in R$ for all $m > 0$. The result then follows from the following lemma. □

Lemma 7.2. *If R is a Noetherian normal domain with $y \in K(R)$ there exists $0 \neq c \in R$ such that $cy^m \in R$ for all $m > 0$, then $y \in R$.*

Proof. Consider the ideal $I = \langle c, cy, cy^2, cy^3 \ldots \rangle \subseteq R$. Since R is Noetherian, $I = \langle c, cy, \ldots, cy^n \rangle$ for some $n > 0$. Thus we can write $cy^{n+1} = a_n cy^n + \cdots + a_0 c$ for some $a_i \in R$. Dividing by c we obtain that

$$y^{n+1} = a_n y^n + \cdots + a_0$$

which proves that y is integral over R and thus $y \in R$. □

Remark 7.3. The converse to the above lemma holds too, exercise!

Corollary 7.4. *If R is F-split, so is R^{N}, $R/\mathfrak{c}$ and $R^{\mathrm{N}}/\mathfrak{c}$. In particular both $R/\mathfrak{c}$ and $R^{\mathrm{N}}/\mathfrak{c}$ are reduced rings.*

While F-split and F-injective rings are not necessarily normal, they are something called weakly normal.

Definition 7.5. Suppose R is a reduced Noetherian ring R with finite normalization R^{N}. An extension of rings $R \subseteq R' \subseteq R^{\mathrm{N}}$ is called *subintegral* if $\operatorname{Spec} R' \longrightarrow \operatorname{Spec} R$ is a homeomorphism and if $Q' \in \operatorname{Spec} R'$ then $k(Q' \cap R) \longrightarrow k(Q')$ is an isomorphism. R is called *seminormal* if the only subintegral extension of R is $R' = R$.

An extension of rings $R \subseteq R' \subseteq R^{\mathrm{N}}$ is called *weakly subintegral* if $\operatorname{Spec} R' \longrightarrow \operatorname{Spec} R$ is a homeomorphism and if $Q' \in \operatorname{Spec} R'$ then $k(Q' \cap R) \longrightarrow k(Q')$ is inseparable. R is called *weakly normal* if the only weakly subintegral extension of R is $R' = R$.

We state some facts about weak and semi-normalization without proof.

Lemma 7.6. *Suppose that R is an excellent Noetherian domain.*

- *The seminormalization of R exists. In other words there is a unique subintegral extension $R \subseteq R^{\mathrm{SN}} \subseteq R^{\mathrm{N}}$ with R^{SN} seminormal*

- *The formation of the seminormalization commutes with localization. In particular if R is seminormal so are its localizations.*
- *The weak normalization of R exists. In other words there is a unique weakly subintegral extension $R \subseteq R^{\mathrm{WN}} \subseteq R^{\mathrm{N}}$ with R^{WN} weakly normal.*
- *The formation of the weak normalization commutes with localization. In particular if R is weakly normal so are its localizations.*

Our goal for now is to show that F-injective rings (and hence F-split rings) are weakly normal. First we give another characterization of weakly normal rings.

Proposition 7.7. *Suppose that R is a reduced Noetherian ring of characteristic $p > 0$ with $R \subseteq R^{\mathrm{N}}$ finite. Then the following are equivalent.*

(a) *$x \in K(R)$ and $x^p \in R$ implies that $x \in R$.*
(b) *R is weakly normal.*

Proof. We first show that (a) $\Rightarrow$ (b). Suppose that R is not weakly normal, this means that there exists $R \subsetneq R'$ weakly subintegral. By localizing, we may assume that $(R, \mathfrak{m}, k)$ is weakly normal except at $\mathfrak{m}$ and so $(R', \mathfrak{m}', k')$ is local as well. Choose some $x \in R'$ which we will try to show is in R. Let $\mathfrak{c}$ be the conductor of R'/R and note it is $\mathfrak{m}$-primary by assumption (and also $\mathfrak{m}'$-primary in R'). It is easy to see that R is the gluing of $(R' \longrightarrow R'/\mathfrak{c} \leftarrow R/\mathfrak{c})$. Now, there are two possibilities.

(1) $x \in \mathfrak{m}'$. In this case $x^{p^e} \in \mathfrak{c}$ for some e. But $\mathfrak{c} \subseteq R$ and this case is taken careof.
(2) x is a unit in R' and so consider $\overline{x} \in R'/\mathfrak{m}' = k'$. Thus $\overline{x^{p^e}} \in k$ for some $e > 0$ since $k \subseteq k'$ is purely inseparable. Consider $y \in R$ with the same image in k. It follows that $z = x^{p^e} - y \in \mathfrak{m}'$ and so applying (1) to z, we see that $z \in R$. But then $x^{p^e} = z + y \in R$ as well. But now $x \in R$ again.

In either case, $x \in R$.

Now we prove that (b) $\Rightarrow$ (a). Choose $x \in K(R)$ with $x^p \in R$. Consider the extension $R \subseteq R[x]$. It suffices to prove that this is weakly subintegral. Since we have $R \subseteq R[x] \subseteq R^{1/p}$ are all integral extensions, we see that $\operatorname{Spec} R[x] \longrightarrow \operatorname{Spec} R$ is a bijection. On the other hand for each $Q' \in \operatorname{Spec} R[x]$ with $Q = R \cap Q'$, we see that $k(Q) \subseteq k(Q') \subseteq k(Q)^{1/p}$ by the above factorization. Thus $k(Q) \subseteq k(Q')$ is purely inseparable and so $R \subseteq R[x]$ is weakly subintegral as claimed. $\square$

We need one more lemma before proving our result on weak normality of F-injective rings.

Lemma 7.8. *Suppose that (R, m) is a reduced local ring of characteristic p, $X = \operatorname{Spec} R$ and that $X - m$ is weakly normal. Then X is weakly normal if and only if the action of Frobenius is injective on $H^1_m(R)$.*

Proof. We assume that the dimension of R is greater than 0 since the zero-dimensional case is trivial. Embed R in its weak normalization $R \subset R^{\mathrm{WN}}$ (which is of course an isomorphism outside of m). We have the following diagram of R-modules.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R & \hookrightarrow & \Gamma(X-m,\mathscr{O}_{X-m}) & \twoheadrightarrow & H^1_m(R) & \longrightarrow & 0 \\
 & & \big\downarrow & & \big\downarrow \cong & & \big\downarrow & & \\
0 & \longrightarrow & R^{\mathrm{WN}} & \hookrightarrow & \Gamma(X^{\mathrm{wn}}-m,\mathscr{O}_{X^{\mathrm{wn}}-m}) & \twoheadrightarrow & H^1_m(R^{\mathrm{WN}}) & \longrightarrow & 0
\end{array}$$

The left horizontal maps are injective because R and ${}^*R$ are reduced. One can check that Frobenius is compatible with all of these maps. Now, R is weakly normal if and only if R is weakly normal in R^{WN} if and only if every $r \in R^{\mathrm{WN}}$ with $r^p \in R$ also satisfies $r \in R$ by Proposition 7.7.

First assume that the action of Frobenius is injective on $H^1_m(R)$. So suppose that there is such an $r \in R^{\mathrm{WN}}$ with $r^p \in R$. Then r has an image in $\Gamma(X-m, \mathscr{O}_{X-m})$ and therefore an image in $H^1_m(R)$. But r^p has a zero image in $H^1_m(R)$, which means r has zero image in $H^1_m(R)$ which guarantees that $r \in R$ as desired.

Conversely, suppose that R is weakly normal. Let $r \in \Gamma(X-m, \mathscr{O}_{X-m})$ be an element such that the action of Frobenius annihilates its image $\overline{r}$ in $H^1_m(R)$. Since $r \in \Gamma(X-m, \mathscr{O}_{X-m})$ we identify r with a unique element of the total field of fractions of R. On the other hand, $r^p \in R$ so $r \in {}^*R = R$. Thus we obtain that $r \in R$ and so $\overline{r}$ is zero as desired. $\square$

Theorem 7.9. *Suppose that R is a reduced F-finite F-injective Noetherian ring. Then R is weakly normal.*

Proof. It is not difficult to verify that weak normality can be checked locally and so suppose that $(R, \mathfrak{m})$ is a local ring. Also recall that if Q is any prime of R then R_Q is also F-injective by the worksheet (here we use that R is F-finite). Now we need to show that R is weakly normal. If R is not weakly normal, choose a prime $P \in \operatorname{Spec} R$ of minimal height with respect to the condition that R_P is not weakly normal. Apply 7.8 to get a contradiction. $\square$

8. A quick introduction to $\mathbb{Q}$-Weil divisors

Setting 8.1. Throughout this section R is a normal Noetherian domain.

We first state some facts about S2 and reflexive modules.

Definition 8.2. A finitely generated R-module M is called *reflexive* if the canonical map $M \mapsto \operatorname{Hom}_R(\operatorname{Hom}_R(M, R), R)$ is an isomorphism. Given M, the *reflexification of* M is simply $\operatorname{Hom}_R(\operatorname{Hom}_R(M, R), R) =: M^{\vee\vee}$.

Exercise 8.1. Show that for any finitely generated module M, $\operatorname{Hom}_R(M, R)$ is reflexive.

Lemma 8.3. *A finitely generated R-module M is reflexive if and only if it is $\mathbf{S}_2$.*

Proof. We leave at as an exercise, see [**Har94**] for details. $\square$

Example 8.4. If M is a torsion-free R-module of rank-1 (meaning that $M \otimes_R K(R) \cong K(R)$), then because M is torsion free, the canonical map $M \longrightarrow M \otimes_R K(R)$ is injective. Thus we can embed $M \subseteq K(R)$. In this case, we see that $\mathrm{Hom}_R(M, R) \cong R :_{K(R)} M$. Indeed, any such $a \in R :_{K(R)} M$ yields a homomorphism by multiplication. Conversely, given any $\phi \in \mathrm{Hom}_R(M, R) \subseteq \mathrm{Hom}_{K(R)}(M \otimes_R K(R), K(R))$ and then our identification $M \otimes_R K(R) \cong K(R)$ lets us identify ϕ with multiplication by some element of $K(R)$.

In this case, $M^{\vee\vee}$, the reflexification of M, can be viewed as $R :_{K(R)} (R :_{K(R)} M)$. This is a subset of $K(R)$ that obviously contains M.

Definition 8.5. A Weil divisor $D = \sum a_i D_i$ on $\mathrm{Spec}\, R$ (or on R) is a finite formal $\mathbb{Z}$-sum of distinct height one prime ideals D_i. A $\mathbb{Q}$-(Weil-)divisor $D = \sum a_i D_i$ on $\mathrm{Spec}\, R$ is a finite formal $\mathbb{Q}$-sum of distinct height one prime ideals D_i. In either case, the divisor is called *effective* if all the $a_i \geq 0$.

Given any $0 \neq g \in K(R)$, we define $\mathrm{div}(g) = \sum v_{D_i}(g) D_i$ where $v_{D_i}(g)$ is the value of g with respect to the discrete valuation v_{D_i} which one obtains after localizing R at D_i.

Associated to any Weil divisor D is a reflexive fractional ideal[11] $R(D)$ (frequently denoted in the sheaf theory language as $\mathscr{O}_{\mathrm{Spec}\, R}(D)$). In particular, if $D = \sum a_i D_i$ then $R(D)$ is the subset of $K(R)$ that have poles of order at most a_i at D_i whenever $a_i > 0$ and have zeros of order at least $|a_i|$ at D_i whenever $a_i < 0$. Explicitly,

$$R(D) = \{g \in K(R) \mid \mathrm{div}(g) + D \geq 0\}.$$

Exercise 8.2. Using the definition, show that $R(D)$ is reflexive, or equivalently that it is $\mathbf{S}_2$.

Let's say what this is explicitly in some special cases.

(i) If $D = 0$, then $R(D) = R$.
(ii) If $D = D_i$ is a single prime ideal, then $R(D) := R :_{K(R)} D$.
(iii) If $D = -D_i$ is the negative of a single prime, then $R(D) = D_i$.
(iv) If $D = -nD_i$ (for $n \geq 0$) is the negative of a single divisor, then $R(D) = (D_i^n)^{\vee\vee}$.
(v) If $D = -\sum a_i D_i$ (for $a_i \geq 0$), then $R(D) = \left(\prod D_i^{a_i}\right)^{\vee\vee}$.
(vi) If $D \geq 0$ (is effective) then $R(D) = R :_{K(R)} R(-D)$.
(vii) If $D = A + B$, then $R(D) = \left(R(A) \cdot R(B)\right)^{\vee\vee}$.
(viii) For any D, $R(-D) = R :_{K(R)} R(D)$.
(ix) If $D = A - B$ then $R(D) \cong \mathrm{Hom}_R(R(B), R(A)) \cong R(A) :_{K(R)} R(B)$.
(x) For any $0 \neq f, g \in K(R)$, $-\mathrm{div}(g) = \mathrm{div}(1/g)$ and also $\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g)$.
(xi) $R(\mathrm{div}(g)) = \frac{1}{g} \cdot R$.

Definition 8.6 (Cartier divisors)**.** A Weil divisor D is called *Cartier* if $R(D)$ is projective (locally free). A ($\mathbb{Q}$-)divisor D is called $\mathbb{Q}$-*Cartier* if there exists an integer

[11] A fractional ideal is by definition a finitely generated submodule of $K(R)$.

$n > 0$ such that nD is Cartier. The smallest such integer $n > 0$ is called the (Cartier-)index of the divisor.

Example 8.7. In $k[x^2, xy, y^2]$ the ideal $Q = \langle x^2, xy \rangle$ corresponds to a prime divisor D but D is not Cartier (since it is not generated by a single element locally). However, D is $\mathbb{Q}$-Cartier since $R(-2D) = \langle x^2 \rangle$ (and hence $R(2D) = \frac{1}{x^2}R$).

Definition 8.8 (Linear equivalence)**.** Two Weil divisors D_1, D_2 are said to be *linearly equivalent* if $D_1 - D_2 = \mathrm{div}(g)$ for some $0 \neq g \in K(R)$. In this case we write $D_1 \sim D_2$. If D_1, D_2 are $\mathbb{Q}$-divisors, we say that they are $\mathbb{Q}$-*linearly equivalent* if there exists an integer $n > 0$ such that nD_1 and nD_2 are linearly equivalent Weil divisors.

Example 8.9. Working in $k[x^2, xy, y^2]$ set D_1 to be the prime divisor $\langle x^2, xy \rangle$ and D_2 to be the prime divisor $\langle xy, y^2 \rangle$, then $D_1 - D_2 = \mathrm{div}(x/y)$ and so $D_1 \sim D_2$.

Lemma 8.10. *Two divisors D_1 and D_2 are linearly equivalent if and only if there is an (abstract) isomorphism $R(D_1) \cong R(D_2)$.*

Proof. Suppose first that D_1 and D_2 are linearly equivalent, and so $D_1 - \mathrm{div}(g) = D_2$ for some $0 \neq g \in K(R)$. We claim that

$$R(D_1) \cdot g = R(D_2).$$

Choose $f \in R(D_1)$. Then $\mathrm{div}(f) + D_1 \geq 0$. It follows that $\mathrm{div}(f \cdot g) + D_1 = \mathrm{div}(f) + D_1 + \mathrm{div}(g) \geq \mathrm{div}(g)$. Thus $\mathrm{div}(f \cdot g) + D_1 - \mathrm{div}(g) = \mathrm{div}(f \cdot g) + D_2 \geq 0$ and so $f \cdot g \in R(D_2)$. Conversely, if $h \in R(D_2)$ then $\mathrm{div}(h) + D_2 \geq 0$ and so $0 \leq \mathrm{div}(h) + D_1 - \mathrm{div}(g) = \mathrm{div}(h/g) + D_1$ which implies that $h/g \in R(D_1)$ and so $h \in R(D_1) \cdot g$ as desired.

Conversely, suppose that $R(D_1) \cong R(D_2)$ and so $\mathrm{Hom}_R(R(D_1), R(D_2)) \cong R$. Since we have $R(D_1), R(D_2) \subseteq K(R)$ we see that $R(D_2) :_{K(R)} R(D_1) = h \cdot R$ for some $h \in K(R)$. We see that $h \cdot R(D_1) = R(D_2)$ and so an argument similar to the one above shows that $D_1 - D_2 = \mathrm{div}(h)$. ☐

Lemma 8.11. *If D is a divisor on R, then every $g \in R(D)$ determines an effective divisor $D_g \sim D$, explicitly $D_g := D + \mathrm{div}(g)$. Furthermore $h \in R(D)$ determines the same divisor as g if and only if h and g are associates in R (unit multiplies).*

Proof. We first observe that $\mathrm{div}(g) = \mathrm{div}(h)$ if and only if $\mathrm{div}(g/h) = 0$. But $\mathrm{div}(g/h) = 0$ if and only if g/h has zero valuation at each height one prime of R. Obviously units have this property. On the other hand if $\mathrm{div}(g/h) = 0$, then $g/h \in R$ and must also be a unit (because if not, it would vanish at some height one prime). This handles the uniqueness. Now we simply have to show that $D_g \geq 0$. But $R(D)$ is the set of elements $g \in K(R)$ such that $\mathrm{div}(g) + D \geq 0$. ☐

Remark 8.12. The choice of a finitely generated reflexive rank-1 module M and an embedding $M \subseteq K(R)$ also determines a divisor D such that $M = R(D)$. To see this, for each height one prime D_i with associated discrete valuation v_{D_i} set $a_i = \max\{-v_{D_i}(m) \mid 0 \neq m \in M\}$. It can be verified that $D = \sum a_i D_i$ is a divisor (one has to verify that the sum is finite using that M is finitely generated) and that

$M \subseteq R(D)$. By construction $R(D) \to M$ is an isomorphism at height one primes and so since both modules are $\mathbf{S}_2$, it is an isomorphism everywhere.

With this in mind, I like to think about a choice of $g \in R(D)$ as a choice of a new way to embed $R(D)$ into $K(R)$. In particular, it is just the embedding of $R(D)$ into $K(R)$ which sends g to 1.

Suppose now that R has a canonical module ω_R.

Lemma 8.13. *ω_R is $\mathbf{S}_2$.*

Proof. Note the canonical module is unique up to tensoring with a locally free module, which obviously does not change whether a module is $\mathbf{S}_2$, so any canonical module is as good as any other. The Lemma can be checked after localization and completion (since it is a statement about local cohomology and the completion of a dualizing complex is a dualizing complex say by local duality). Thus choose $A \subseteq R$ a finite extension with A complete and regular (this exists as part of the Cohen Structure Theorem, see for example [**Sta16**, Tag 032D]). It follows that $\mathbf{R}\operatorname{Hom}_A(R, A)$ is a dualizing complex for R. A canonical module for R is thus $h^0\mathbf{R}\operatorname{Hom}_A(R, A) = \operatorname{Hom}_A(R, A)$. Now, $\operatorname{Hom}_A(R, A)$ is obviously reflexive as an A-module and hence it is $\mathbf{S}_2$ as an A-module. But then it is not hard to see that $\operatorname{Hom}_A(R, A)$ is $\mathbf{S}_2$ as an R-module as well (this requires a bit of work). Hence $\omega_R = \operatorname{Hom}_A(R, A)$ is reflexive as claimed. □

Definition 8.14. Fix ω_R a canonical module. A *canonical divisor* is any Weil divisor K_R such that $\omega_R \cong R(K_R)$.

Remark 8.15. So far we seen that canonical modules are only unique up to twisting by locally free modules. In particular, based on what we have seen, canonical modules are only unique up to a Cartier divisor. For local rings this is file (all Cartier divisors are linearly equivalent to zero). For more general rings and especially for schemes, this is not so good since you want some compatibility between your dualizing complexes (you want them to behave reasonably with respect to morphisms). However, most of the time we are working with objects and morphisms (essentially) of finite type over a Gorenstein ring A (for example a field or $\mathbb{Z}_p$), say $f : X \to \operatorname{Spec} A$. In that case, there is a canonical choice of a dualizing complex, $f^! A[\dim A]$. In the case that R is a normal domain of finite type over a field k, $R = k[x_1, \ldots, x_n]/I$, then this choice boils down to $\omega_R = \operatorname{Ext}^{n-\dim R}_{k[x_1,\ldots,x_n]}(R, k[x_1, \ldots, x_n])$.

Note that a ring is Gorenstein if and only if K_R is Cartier and R is Cohen-Macaulay. We also have the following definition.

Definition 8.16 ($\mathbb{Q}$-Gorenstein)**.** *R is called $\mathbb{Q}$-Gorenstein if K_R is $\mathbb{Q}$-Cartier.* (Note there is no Cohen-Macaulay hypothesis). For a $\mathbb{Q}$-Gorenstein ring, the *($\mathbb{Q}$-Gorenstein-)index* is the smallest integer $n > 0$ such that nK_X is Cartier.

9. Frobenius splittings and divisors

Suppose that R is an F-finite Noetherian normal domain. Notice that $\operatorname{Hom}_R(F^e_* R, R)$ is a reflexive R-module and hence a $\mathbf{S}_2$ R-module. Since the $\mathbf{S}_2$ condition can be checked via local cohomology and localization, neither of which care whether we are viewing the Hom-set as an R-module or $F^e_* R$-module, it follows that $\mathrm{Hom}_R(F^e_* R, R)$ is $\mathbf{S}_2$ as an $F^e_* R$-module as well.

Exercise 9.1. Suppose R is an F-finite Noetherian normal domain, show carefully that the $F^e_* R$-module $\mathrm{Hom}_R(F^e_* R, R)$ is $\mathbf{S}_2$.

Thus $\mathrm{Hom}_R(F^e_* R, R)$ is a reflexive $F^e_* R$-module of rank 1 (it has rank 1 because its rank as an R-module is the same as the rank of $F^e_* R$ as an R-module). You might naturally ask what linear equivalence class of divisor this Hom set corresponds to?

First we work in the following setting.

Setting 9.1. Suppose R is as above in this section. Suppose we have a dualizing complex $\omega_R^{\mathbf{\cdot}}$ such that $\mathbf{R}\,\mathrm{Hom}_R(F^e_* R, \omega_R^{\mathbf{\cdot}}) \cong \omega^{\mathbf{\cdot}}_{F^e_* R}$ (this always exists if R is local or of finite type over a field, it probably also follows that such a dualizing complex exists in general by some unpublished work). We fix this dualizing complex forever more. Notice that if ω_R is the associated canonical module, the $\mathrm{Hom}_R(F^e_* R, \omega_R) \cong \omega_{F^e_* R} \cong F^e_* \omega_R$ (note we don't need to worry about the derived Hom's all the modules are reflexive and they are certainly isomorphic in codimension 1 where R is regular). We fix K_R to be a canonical divisor associated to this canonical module.

Lemma 9.2. *With notation above, $F^e_* R((1-p^e)K_R) \cong \mathrm{Hom}_R(F^e_* R, R)$. In particular, if R is local and quasi-Gorenstein, then $\mathrm{Hom}_R(F^e_* R, R) \cong F^e_* R$ as $F^e_* R$-modules.*

Proof. This follows from the following chain of isomorphisms (in this chain, in almost every step, we use that all modules are reflexive, and so it is enough to verify the isomorphisms in codimension 1 where we can treat the modules as if they were free).

$$\begin{array}{rl} & \mathrm{Hom}_R(F^e_* R, R) \\ \cong & \mathrm{Hom}_R((F^e_* R) \otimes_R R(K_R), R(K_R)) \\ \cong & \mathrm{Hom}_R(F^e_*(R \otimes_R R(p^e K_R)), \omega_R) \\ \cong & \mathrm{Hom}_{F^e_* R}(F^e_*(R \otimes_R R(p^e K_R)), \mathrm{Hom}_R(F^e_* R, \omega_R)) \\ \cong & \mathrm{Hom}_{F^e_* R}(F^e_*(R(p^e K_R)), F^e_* \omega_R) \\ \cong & F^e_* \mathrm{Hom}_R((R(p^e K_R)), R(K_R)) \\ \cong & F^e_* R((1-p^e)K_R). \end{array}$$

□

Corollary 9.3. *Every nonzero map $\phi \in \mathrm{Hom}_R(F^e_* R, R)$ determines an effective Weil divisor $D_\phi \sim (1-p^e)K_R$. Furthermore, two maps ϕ, ϕ' determine the same divisor if and only if they are the same up to pre-multiplication by a unit of $F^e_* R$.*

Corollary 9.4. *Suppose R is a normal Noetherian F-finite domain. There exists a $\phi \in \mathrm{Hom}_R(F^e_* R, R)$ which generates the* Hom*-set as an $F^e_* R$-module if and only if $(1-p^e)K_R \sim 0$. In the case that R is local, such a ϕ exists for some $e > 0$ if and only if R is $\mathbb{Q}$-Gorenstein with index not divisible by $p > 0$.*

In many cases you want this divisor to be in some sense independent of the characteristic, or more generally, independent of self-composition. In particular, you'd like the divisor corresponding to $\phi \circ F^e_* \phi$ to be the same as the divisor corresponding to ϕ. We can accomplish this by normalizing our divisor.

Definition 9.5. For any nonzero $\phi \in \mathrm{Hom}_R(F^e_* R, R)$ we define $\Delta_\phi := \frac{1}{p^e-1} D_\phi$. Note that $K_R + \Delta_\phi \sim_{\mathbb{Q}} 0$.

Lemma 9.6. *If $\Phi \in \mathrm{Hom}_R(F^e_* R, R)$ generates the module (as an $F^e_* R$-module), then $\Delta_\Phi = 0 = D_\Phi$. Furthermore, if we write $\phi(F^e_* \_\_) = \psi(F^e_*(r \cdot \_\_))$ for some $r \in R$, then $D_\phi = D_\psi + \mathrm{div}_R(r)$ and so $\Delta_\phi = \Delta_\psi + \frac{1}{p^e-1} \mathrm{div}_R(r)$.*

Proof. Left as an exercise to the reader. □

Lemma 9.7. *For any map ϕ and any integer n form $\phi^n := \phi \circ (F^e_* \phi) \circ (F^{2e}_* \phi) \circ \cdots \circ (F^{(n-1)e}_* \phi) \in \mathrm{Hom}_R(F^{ne}_* R, R)$. Then $\Delta_{\phi^n} = \Delta_\phi$.*

Proof. This statement may be verified in codimension 1 since divisors are defined in codimension 1. Thus we localize R at a height one prime to obtain the $(R, \mathfrak{m} = \langle r \rangle)$ is a DVR (remember, R was normal). Since regular rings are Gorenstein, we choose $\Phi \in \mathrm{Hom}_R(F^e_* R, R)$ generating the Hom set as an $F^e_* R$-module. Then we can write $\phi(F^e_* \_\_) = \Phi(F^e_* u r^n \_\_)$ for some integer $n > 0$ and unit $u \in R$. Note that in this case, $D_\phi = n \,\mathrm{div}(r)$ and so $\Delta_\phi = \frac{n}{p^e-1} \mathrm{div}(r)$. It follows that

$$\phi^2(F^{2e}_* \_\_) = \Phi^2(F^{2e}_* (ur^n)^{1+p^e} \_\_)$$

and so $\Delta_{\phi^2} = \frac{n(1+p^e)}{p^{2e}-1} \mathrm{div}(r) = \frac{n}{p^e-1} \mathrm{div}(r) = \Delta_\phi$. More generally

$$\phi^n(F^{ne}_* \_\_) = \Phi^n(F^{ne}_* (ur^n)^{1+p^e+\cdots+p^{(n-1)e}} \_\_)$$

and thus $\Delta_{\phi^n} = \frac{n(1+p^e+\cdots+p^{(n-1)e})}{p^{ne}-1} \mathrm{div}(r) = \frac{n}{p^e-1} \mathrm{div}(r) = \Delta_\phi$ □

Exercise 9.2. Suppose that $0 \neq \phi \in \mathrm{Hom}_R(F^e_* R, R)$ and $0 \neq \psi \in \mathrm{Hom}_R(F^d_* R, R)$. Find a formula for $\Delta_{\phi \circ F^e_* \psi}$ in terms of Δ_ϕ and Δ_ψ.

Putting together what we know now, we have a bijection

$$\left\{ \begin{array}{c} \mathbb{Q}\text{-divisors } \Delta \text{ such that} \\ K_R + \Delta \sim_{\mathbb{Q}} 0 \\ \text{with trivializing index}^{12} \text{ not} \\ \text{divisible by } p \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Nonzero} \\ \phi \in \mathrm{Hom}_R(F^e_* R, R) \end{array} \right\} \Big/ \sim$$

where the equivalence on the right is generated by self-composition and pre-multiplication by units.

Suppose that $\Delta = \Delta_\phi$ is such that $\phi \in \mathrm{Hom}_R(F^e_* R, R)$ satisfies $\phi(F^e_* I) \subseteq I$. For simplicity assume that R/I is normal, then ϕ induces a map $\phi_{R/I} : F^e_*(R/I) \longrightarrow R/I$ which, if this is not the zero map, induces a divisor $\Delta_{R/I}$. In particular for every such Δ_ϕ with $K_R + \Delta_\phi \sim_{\mathbb{Q}} 0$ we obtain a canonical $\Delta_{R/I}$ with $K_{R/I} + \Delta_{R/I} \sim_{\mathbb{Q}} 0$. This canonical way of associating a divisor on a subscheme is an analog of Kawamata's subadjunction theorem in the characteristic zero world [**Kaw98**].

Example 9.8. Suppose char$k > 2$, consider $S = k[x, y, z]$, $R = k[x, y, z]/\langle xy - z^2\rangle$ and $I = \langle x, z\rangle \subseteq R$. $\mathrm{Hom}_R(F^e_* R, R)$ is isomorphic to $F^e_* R$ and is generated by $\Phi_R(F^e_* \_\_)$, the restriction of the map $\Phi_S(F^e_*(xy - z^2)^{p^e-1} \cdot \_\_) \in \mathrm{Hom}_S(F^e_* S, S)$ (by Fedder's criterion). Now, consider the map

$$\psi(F^e_* \_\_) = \Phi_R(F^e_* x^{(p^e-1)/2} \cdot \_\_)$$

which is the restriction of $\Phi_S(F^e_*(xy - z^2)^{p^e-1} x^{(p^e-1)/2} \cdot \_\_)$. If you apply this map to the ideal $I = \langle x, z\rangle$ one obtains

$$\Phi_S(F^e_*(xy - z^2)^{p^e-1} x^{(p^e-1)/2} \langle x, z\rangle)$$

We claim that $(xy - z^2)^{p^e-1} x^{(p^e-1)/2} \langle x, z\rangle \subseteq \langle x^{p^e}, z^{p^e}\rangle$. Indeed, when we expand we get

$$\left((xy)^{p^e-1} x^{(p^e-1)/2} + \cdots + (xy)^{(p^e-1)/2} z^{(p^e-1)} x^{(p^e-1)/2} + \cdots + z^{2(p^e-1)} x^{(p^e-1)/2}\right)$$

which when multiplied by $\langle x, z\rangle$ is obviously contained in $\langle x^{p^e}, z^{p^e}\rangle$ which means that $\phi_R(F^e_* I) \subseteq I$. On the other hand, if we didn't multiply by $\langle x, z\rangle$ then the expansion is not in $\langle x^{p^e}, z^{p^e}\rangle$ which means that $\psi = \phi_{R/I}$ is not the zero map. In particular it induces a divisor on $k[y] = S/\langle x, z\rangle$ and so we can ask what divisor it gives us.

In the above expansion, the only term that is not in $\langle x^{p^e}, z^{p^e}\rangle$ is the middle term $(xy)^{(p^e-1)/2} z^{(p^e-1)} x^{(p^e-1)/2}$. The generating map for $\mathrm{Hom}(F^e_* S/\langle x, z\rangle, S/\langle x, z\rangle)$ is obtained from $\Phi_S(F^e_* x^{p^e-1} z^{p^e-1} \_\_)$. Hence the map ψ we found is the generating map for $\mathrm{Hom}(F^e_* k[y], k[y])$ pre-multiplied by $y^{(p^e-1)/2}$. In particular, the divisor corresponding to ψ is $\frac{1}{2}\,\mathrm{div}(y)$ on $\mathrm{Spec}\, k[y]$.

10. Divisors, Frobenius splittings and finite extensions

Suppose that $R \subseteq S$ is a finite extension of normal Noetherian domains. Suppose we have $\phi : F^e_* R \longrightarrow R$. It is natural to ask when ϕ extends to $\phi_S : F^e_* S \longrightarrow S$ and when it does, what is the relation between the divisors Δ_R and Δ_S.

Example 10.1. Suppose $R = k[x^2] \subseteq k[x] = S$ for char$k = p > 2$. Consider the generating homomorphism $\Phi \in \mathrm{Hom}_R(F_* R, R)$ which sends $F_*(x^2)^{p-1}$ to 1 and the other basis elements to zero. This map does not extend to a map $\mathrm{Hom}_S(F_* S, S)$, indeed if it did then $F_* x^{p-2} = F_* \frac{x^{2(p-1)}}{x^p}$ would necessarily be sent to $1/x$ which is not in S.

On the other hand, consider the map $\phi \in \mathrm{Hom}_R(F_* R, R)$ is the map that projects onto the basis monomial $F_*(x^2)^{(p-1)/2}$ and projects the other basis monomials to zero. It is easy to see that any extension of this map to S sends $F_* x^{p-1} \mapsto 1$ since $x^{p-1} = (x^2)^{(p-1)/2}$. Furthermore we claim such an extension also sends the other basis monomials to zero. Consider the element $F_* x^j$ for $0 \leq j < p - 1$. If j is even, then there is no problem, $F_* x^j$ is one of the other basis elements of $F_* R$ and is thus sent to zero. So suppose j is odd. Now, $j + p$ is even and $j + p \leq (p - 1) + p$ but since the right side is odd, $j + p \leq 2(p - 1)$. Thus $F_* x^{j+p}$ is a monomial basis element of $F_* R$. But since $j + p$ cannot equal $p - 1 = (2(p - 1))/2$, we see that any extension of ϕ must send $F_* x^{j+p}$ to zero. But then such an extension must send $F_* x^j$ to $0/p = 0$.

Therefore, because we can describe an extension of ϕ by describing what it does to the basis elements of F_*S, we see that ϕ can indeed extend. It follows immediately that any $\psi(F_* \_\_) := \phi(F_*(r \cdot \_\_))$ also extends.

Let us first analyze this in the case where R and S are fields.

Lemma 10.2. *Suppose K is an F-finite field and $\phi : F^e_* K = K^{1/p^e} \longrightarrow K$ is a nonzero map. If $K \subseteq L$ is a finite separable extension of fields then ϕ extends uniquely to a map $\phi_L : F^e_* L = L^{1/p^e} \longrightarrow L$.*

Proof. Since L and K^{1/p^e} are linearly disjoint extensions of K (one separable, the other purely inseparable), $L \otimes_K K^{1/p^e} = L \cdot K^{1/p^e} = L^{1/p^e}$ (to see the second equality, note we have the containment $\subseteq$ and also that $[L^{1/p^e} : L] = [K^{1/p^e} : K]$ since $[L^{1/p^e} : K^{1/p^e}] = [L : K]$). It follows that

$$\phi \otimes_K L : L^{1/p^e} \cong K^{1/p^e} \otimes_K L \longrightarrow K \otimes_K L$$

is a map extending ϕ. ☐

Exercise 10.1. Suppose that L/K is a finite extension of characteristic $p > 0$ fields and $x \in L \setminus K$ but $x^p \in K$. Show that if $\phi : K^{1/p^e} \longrightarrow K$ extends to $L^{1/p^e} \longrightarrow L$, then ϕ is the zero map on K. Conclude in general that if L/K is inseparable, then no nonzero $\phi : K^{1/p^e} \longrightarrow K$ can extend to $L^{1/p^e} \longrightarrow L$.

Recall that given a finite extension of fields $K \subseteq L$, we have the trace map $\mathrm{Tr} : L \longrightarrow K$. This is defined as follows, for each $y \in L$, we have a K-linear map $L \xrightarrow{\cdot y} L$, $\mathrm{Tr}(y)$ is then defined to be the trace of the linear operator $\cdot y$.

Lemma 10.3. *Suppose L/K is a separable extension of fields and that $\phi : K^{1/p^e} \longrightarrow K$ extends to $\phi_L : L^{1/p^e} \longrightarrow L$. Let $\mathrm{Tr} : L \longrightarrow K$ be the trace map. Then the following diagram commutes*

$$\begin{array}{ccc} L^{1/p^e} & \xrightarrow{\phi_L} & L \\ {\scriptstyle \mathrm{Tr}^{1/p^e}} \downarrow & & \downarrow {\scriptstyle \mathrm{Tr}} \\ K^{1/p^e} & \xrightarrow[\phi]{} & K. \end{array}$$

Proof. Choose $x_1^{1/p^e}, \ldots, x_n^{1/p^e}$ a basis for $K^{1/p^e}/K$. It follows since $L^{1/p^e} = L \cdot K^{1/p^e} = L \otimes_K K^{1/p^e}$ that $x_1^{1/p^e}, \ldots, x_n^{1/p^e}$ is a basis for $L^{1/p^e}/L$. On the other hand, if $z_1, \ldots, z_d$ is a basis for L/K, then it remains a basis for $L^{1/p^e}/K^{1/p^e}$. It follows that $(\mathrm{Tr})^{1/p^e}|_L = \mathrm{Tr}$. Now since ϕ extends to ϕ_L, $\phi(x_i^{1/p^e}) = \phi_L(x_i^{1/p^e})$. Finally, for any $y \in L$, write

$$y^{1/p^e} = \sum a_i x_i^{1/p^e}$$

for some $a_i \in L$. Thus

$$\begin{array}{rl} & \phi \circ \mathrm{Tr}^{1/p^e}(y^{1/p^e}) \\ = & \phi\big(\sum x_i^{1/p^e} (\mathrm{Tr}^{1/p^e}(a_i))\big) \\ = & \sum \phi(x_i^{1/p^e}) \, \mathrm{Tr}(a_i). \end{array}$$

and also

$$\begin{array}{rl} & \operatorname{Tr} \circ \phi_L(y^{1/p^e}) \\ = & \operatorname{Tr}(\sum a_i \phi(x_i^{1/p^e})) \\ = & \sum \operatorname{Tr}(a_i)\phi(x_i^{1/p^e}). \end{array}$$

The result follows. □

We need the following standard result.

Lemma 10.4. *Suppose $R \subseteq S$ is a finite*[13] *inclusion of normal Noetherian domains. Let* $\operatorname{Tr} : K(S) \longrightarrow K(R)$ *denote the trace map, then* $\operatorname{Tr}(S) \subseteq R$.

Proof. Since R is $\mathbf{S}_2$, it suffices to prove the result after localizing at a height one prime of R (to see this, simply notice that $\operatorname{Tr}(S) \subseteq R$ is a finite R-module and so if it agrees with R in codimension 1, it is contained in R). But since R is normal, such a localization is a DVR and so we may assume that R is a DVR. But now S is a free R-module so a basis for S/R becomes a basis for L/K. It follows that for any $s \in S$, $S \xrightarrow{\cdot s} S$ is written as a matrix with entries in R and so $\operatorname{Tr}(s) \in R$ as claimed. □

We now also explain how to pullback divisors under finite maps of normal domains.

Definition 10.5. Suppose $R \subseteq S$ is a finite inclusion of normal domains with induced map $\pi : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$. For any Weil divisor D on R, we define $\pi^* D$ to be the divisor such that $(R(D) \cdot S)^{\vee\vee} = S(\pi^* D)$. Alternately, for each height one prime Q of R, let $Q_1, \dots, Q_d$ be the primes of S lying over Q. In this case $R(D)_Q = g_Q R_Q$ since each R_Q is a DVR. We define $\pi^* D = \sum_Q \sum_{Q_i} -v_{Q_i}(g_Q) Q_i$. In particular, if $D = \operatorname{div}_R(f)$, then $\pi^* D = \operatorname{div}_S(f)$.

Example 10.6. If $S = F^e_* R$, then $\pi^* D = p^e D$.

If $R \subseteq S$ is a finite inclusion of normal domains such that $K(R) \subseteq K(S)$ is separable (with $\pi : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$ the induced map), the map $\operatorname{Tr} \in \operatorname{Hom}_R(S, R)$ is a nonzero[14] element in a rank-1 $\mathbf{S}_2$ S-module. Also note that if $\omega_S := \operatorname{Hom}_S(R, \omega_S)$, then

$$\begin{array}{rl} & \operatorname{Hom}_R(S, R) \\ = & \operatorname{Hom}_R(S \otimes_R \omega_R, \omega_R) \\ = & \operatorname{Hom}_R(S(\pi^* K_R), \omega_R) \\ = & \operatorname{Hom}_S(S(\pi^* K_R), \omega_S) \\ = & S(K_S - \pi^* K_R). \end{array}$$

and so the effective divisor D_{Tr} corresponding to Tr is linearly equivalent to $K_S - \pi^* K_R$.

Definition 10.7. With notation as above the effective divisor D_{Tr} corresponding to Tr is called the *ramification divisor (of $R \subseteq S$)*. Throughout the rest of the paper, it will be denoted by $\operatorname{Ram} = \operatorname{Ram}_{S/R}$.

[13]Finite means S is a finitely generated R-module.

[14]Tr of an extension of fields is nonzero if and only if the extension is separable.

You may have seen the ramification divisor defined somewhat differently, these two definitions are indeed the same. Let's do a hopefully convincing example.

Example 10.8. Consider $R = k[x^n] \subseteq k[x] = S$ where char$k$ does not divide n. We will compute the trace map and thus the ramification divisor. Note that S is a free R-module with basis $1, x, \dots, x^{n-1}$. It is easy to see that $\mathrm{Tr}(x^i) = 0$ for $0 < i < n$ and $\mathrm{Tr}(1) = n$ (just write down the matrices). On the other hand the map Φ that projects onto x^{n-1} obviously generates $\mathrm{Hom}_R(S, R)$ as an S-module. Note $\mathrm{Tr}(\_) = n \cdot \Phi(x^{n-1}\_)$ so that because $D_\Phi = 0$, we see that $D_{\mathrm{Tr}} = \mathrm{div}(x^{n-1})$.

Definition-Proposition 10.9. If $R \subseteq S$ is a finite separable extension of rings with R a DVR with uniformizer s, then it is said to have *tame ramification* at a maximal ideal $Q \in \operatorname{Spec} S$ (so that S_Q is a DVR with uniformizer s) if it satisfies the following two conditions:

- when we write $r = us^n$, p does not divide n
- and if $R/rR \subseteq S_Q/sS_Q$ is separable.

In this case, the coefficient of Ram at Q is equal to $n - 1$.

Exercise 10.2. Verify the above definition - proposition.

Lemma 10.10. *Suppose we have finite inclusions of normal domains $A \subseteq B \subseteq C$ with $\rho : \operatorname{Spec} C \longrightarrow \operatorname{Spec} B$ the induced map. If $\phi \in \mathrm{Hom}_A(B, A)$ and $\psi \in \mathrm{Hom}_B(C, B)$ then $D_{\phi\circ\psi} = D_\psi + \rho^* D_\phi$.*

Proof. Since we are concerned above divisors, we may assume that A is a DVR so that B and C are semi-local. In this case if Φ and Ψ generate their respective Hom groups, we see from an older homework assignment that so does $\Phi \circ \Psi$ and thus all divisors in question are zero. On the other hand, if $\phi(\_) = \Phi(b \cdot \_)$ and $\psi(\_) = \Psi(c \cdot \_)$, then $D_\phi = \mathrm{div}_B(b)$ and $D_\psi = \mathrm{div}_C(c)$ and $\mathrm{div}_{\phi\circ\psi} = \mathrm{div}_C(bc) = D_\psi + \rho^* D_\phi$. $\square$

Theorem 10.11. *Suppose that $R \subseteq S$ is a finite generically separable inclusion of F-finite normal domains with induced $\pi : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$. Then a map $\phi \in \mathrm{Hom}_R(F^e_* R, R)$ extends to a map $\phi_S \in \mathrm{Hom}_S(F^e_* S, S)$ if and only if $\pi^*\Delta_\phi - \mathrm{Ram} \geq 0$. In this case $\Delta_{\phi_S} = \pi^*\Delta_\phi - \mathrm{Ram}$.*

Proof. Suppose first that ϕ extends to ϕ_S (note Δ_{ϕ_S} is automatically effective) and so by Lemma 10.3 we have a commutative diagram

$$\begin{array}{ccc} S^{1/p^e} & \xrightarrow{\phi_S} & S \\ \downarrow{\scriptstyle \mathrm{Tr}^{1/p^e}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ R^{1/p^e} & \xrightarrow[\phi]{} & R. \end{array}$$

It follows from Lemma 10.10 that $\mathrm{Ram} + \pi^* D_\phi = D_{\phi_S} + p^e\mathrm{Ram}$. Thus $0 \leq \Delta_{\phi_S} = \frac{1}{p^e-1}(\pi^* D_\phi) - \mathrm{Ram} = \pi^*\Delta_\phi - \mathrm{Ram}$.

Conversely assume that $\pi^*\Delta_\phi - \mathrm{Ram} \geq 0$. We can still extend ϕ to $\phi_S : S^{1/p^e} \longrightarrow L = K(S)$. We need to show that the image of is contained in S. After localizing at a height one prime of R if necessary, we can assume that $\Phi_S \in \mathrm{Hom}_S(S^{1/p^e}, S)$ generates the Hom-set as an S^{1/p^e}-module. We may then write $\phi(\_\_) = \Phi_S(y^{1/p^e}\_\_)$ for some $y \in K(S)$. It suffices to show that $y \in S$, or in other words that $\mathrm{div}(y) \geq 0$. We still have the following diagram

$$\begin{array}{ccc} S^{1/p^e} & \xrightarrow{\phi_S} & K(S) \\ \downarrow{\scriptstyle \mathrm{Tr}^{1/p^e}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ R^{1/p^e} & \xrightarrow[\phi]{} & K(R). \end{array}$$

An argument similar to the one above proves that $\mathrm{div}(y) = \pi^* D_\phi - (1-p^e)\mathrm{Ram}$ (note this requires a slight modification of the proof of Lemma 10.10). □

Corollary 10.12. *Suppose that $R \subseteq S$ is a finite generically separable inclusion of F-finite normal domains with $\pi : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$ the induced map. Suppose R is F-split and that $\phi : F^e_* R \longrightarrow R$ is a Frobenius splitting such that $\pi^*\Delta_\phi \geq \mathrm{Ram}$. Then S is F-split as well.*

Definition 10.13. A finite inclusion of normal domains $R \subseteq S$ is *finite étale in codimension 1* if the ramification divisor $\mathrm{Ram} = 0$.

Corollary 10.14. *Suppose that $R \subseteq S$ is an inclusion of normal domains that is finite étale in codimension 1. If R is F-split, then so is S.*

Remark 10.15. The converse to these results does *not* hold in general, but it does hold with the additional hypothesis that $R \subseteq S$ splits (as we have seen). Note that in the case that $R \subseteq S$ is étale in codimension 1, this is equivalent to the hypothesis that $\mathrm{Tr}(S) = R$ since in that case $\mathrm{Tr} \in \mathrm{Hom}_R(S, R)$ generates the Hom-set.

There is a version that we can easily state for F-regularity as well.

Corollary 10.16. *Suppose that $R \subseteq S$ is a finite inclusion of normal F-finite domains. Fix a $0 \neq c \in R$ such that R_c and S_c are strongly F-regular. If there exists a map $\phi \in \mathrm{Hom}_R(F^e_* R, R)$ such that $\phi(F^e_* c) = 1$ and such that $\pi^*\Delta_\phi \geq \mathrm{Ram}$, then S is strongly F-regular as well. In particular, if $R \subseteq S$ is étale in codimension 1 and R is strongly F-regular, then so is S.*

Proof. Use Theorem 5.10 applied to $c \in S$. □

CHAPTER 3

Hilbert-Kunz multiplicity and F-signature

Consider the problem of measuring how singular an F-finite local ring $(R, \mathfrak{m})$ is. Based on Kunz's theorem, we should measure:

How close to free is $F^e_* R$ as an R-module.

Hilbert-Kunz multiplicity and F-signature are both attempts at quantifying that notion, asymptotically as $e \longrightarrow \infty$.

Hilbert-Kunz multiplicity: Measures how many generators $F^e_* R$ has relative to the expected number if R was regular.

F-signature: Measures how many free summands $F^e_* R$ has relative to the expected number if R was regular.

1. Hilbert-Kunz multiplicity

Suppose that $(R, \mathfrak{m}, k)$ is a local Noetherian ring and that M is an R-module. We let $\mu_R(M)$ denote the minimal number of generators of M as an R-module. Note that $\mu_R(M) = \ell_R(M/\mathfrak{m} \cdot M) = \mathrm{rank}_k(M/\mathfrak{m} \cdot M)$ by Nakayama's lemma.

Suppose that $R = k[\![x_1, \dots, x_d]\!]$ and that $k = k^p$ is perfect of characteristic $p > 0$. In this case, $F^e_* R$ is a free R-module with p^{ed} generators. Because of this we make the following definition:

Definition 1.1 (Hilbert-Kunz multiplicity, perfect residue field case)**.** Suppose that $(R, \mathfrak{m}, k)$ is a Noetherian local ring of characteristic $p > 0$ and dimension d. Suppose further that $k = k^p$ is perfect. Then we define the Hilbert-Kunz multiplicity of R to be the

$$\lim_{e \longrightarrow \infty} \frac{\ell(R/\mu^{[p^e]})}{p^{ed}} = \lim_{e \longrightarrow \infty} \frac{\mu_R(F^e_* R)}{p^{ed}}$$

if it exists. It is denoted by $e_{\mathrm{HK}}(R)$.

Example 1.2. If $R = k[\![x_1, \dots, x_d]\!]$ and $k = k^p$ is perfect, then $e_{\mathrm{HK}}(R) = 1$.

We'll show that this limit always exists later, after we generalize this definition a bit. For now, suppose that R is the localization (at some maximal ideal) of some finite type algebra over a perfect field. If $\dim R = d$, it follows that $[F^e_* K(R) : K(R)] = p^{ed}$, and so the generic rank of $F^e_* R$ over R is p^{ed}. Hence $\mu_R(F^e_* R) \geq p^{ed}$. On the other hand if we ever had that $\mu_R(F^e_* R) = p^{ed}$, then $F^e_* R$ would be a free R-module and hence R would be regular (and then an argument similar to the one above would show that $e_{\mathrm{HK}}(R) = 1$).

Next let's figure out what to do when k is not perfect, we'll use the case of an F-finite residue field as our starting point.

Lemma 1.3. *Suppose that $(R, \mathfrak{m}, k)$ is a local ring with F-finite residue field (i.e. such that $[k : k^p] < \infty$). If M is an R-module of finite length then*

$$\ell_R(F^e_* M) = [k : k^{p^e}] \cdot \ell_{F^e_* R}(F^e_* M) = [k : k^{p^e}] \cdot \ell_R(M). \tag{1.3.1}$$

In particular, $\mu_R(F^e_* R)$, the number of generators of $F^e_* R$ as an R-module satisfies

$$\mu_R(F^e_* R) = \ell_R((F^e_* R)/\mathfrak{m}) = \ell_R\big(F^e_*(R/\mathfrak{m}^{[p^e]})\big) = [k : k^{p^e}] \cdot \ell_R\big(R/\mathfrak{m}^{[p^e]}\big) \tag{1.3.2}$$

Proof. In (1.3.1), the second equality is trivial. The first equality follows from the fact that $[k : k^{p^e}] = \ell_R(F^e_* k)$.

In (1.3.2), the first equality is just Nakayama's lemma and the second is the fact that $(R/\mathfrak{m}) \cdot F^e_* R \cong F_*(R/\mathfrak{m}^{[p^e]})$. The third equality is simply (1.3.1) applied to the finite length module $M = R/\mathfrak{m}^{[p]}$. $\square$

On the other hand if $R = k$ is an imperfect but F-finite field, we still might want $e_{\mathrm{HK}}(R) = 1$ (since R is regular). Now, if $\mu_k(F_* k) = [F_* k : k] = [k : k^p] = n$, then $\mu_k(F^2_* k) = [F^2_* k : k] = n^2$ and more generally, $\mu_k(F^e_* k) = n^e$. Thus it is natural to try to normalize at the very least for the residue field. In particular, it would be natural to simply define

$$e_{\mathrm{HK}}(R) = \lim_{e \longrightarrow \infty} \frac{\mu_R(F^e_* R)}{[F^e_* k : k] p^{ed}} = \lim_{e \longrightarrow \infty} \frac{\ell_R(()F^e_*(R/\mathfrak{m}^{[p^e]})}{[F_* k : k]^e p^{ed}}.$$

However, based on our above lemma, this is already the same as:

$$e_{\mathrm{HK}}(R) = \lim_{e \longrightarrow \infty} \frac{\ell_R\big(R/\mathfrak{m}^{[p^e]}\big)}{p^{ed}}.$$

We take this to be our definition of Hilbert-Kunz multiplicity independent of whether or not k is perfect (*even* if k is not F-finite). At this point, there is one more generalization we will make. Instead of modding out by $\mathfrak{m}^{[p^e]}$, we fix J to be an $\mathfrak{m}$-primary ideal (ie, $\sqrt{J} = \mathfrak{m}$) and mod out by $J^{[p^e]}$.

Definition 1.4 (Hilbert-Kunz multiplicity, general case)**.** Suppose that $(R, \mathfrak{m})$ is a Noetherian local ring of characteristic $p > 0$ and dimension d. Suppose further that J is an $\mathfrak{m}$-primary ideal. Then we define the *Hilbert-Kunz multiplicity of R along J to be*

$$e_{\mathrm{HK}}(J; R) = \lim_{e \longrightarrow \infty} \frac{\ell_R\big(R/J^{[p^e]}\big)}{p^{ed}},$$

if it exists.

Before showing it exists, let's figure out what it is for regular rings in general.

Proposition 1.5. *Suppose $(R, \mathfrak{m}, k)$ is a regular local Noetherian ring of characteristic $p > 0$ and dimension d. Then $e_{\mathrm{HK}}(J; R) = \ell(R/J)$ and in particular, $e_{\mathrm{HK}}(\mathfrak{m}; R) = e_{\mathrm{HK}}(R) = 1$.*

Proof. We first handle the case when $J = \mathfrak{m}$. Consider $\widehat{R} \cong k[\![x_1, \ldots, x_d]\!]$. By construction, $\widehat{R}/(J\widehat{R})^{[p^e]} \cong R/J^{[p^e]}$, and so $e_{\mathrm{HK}}(J; R) = e_{\mathrm{HK}}(J\widehat{R}; \widehat{R})$. Thus we may assume that $R = k[\![x_1, \ldots, x_d]\!]$. But clearly then $\ell_R\big(R/\mathfrak{m}^{[p^e]}\big) = p^{ed}$.

For the general case, we will show that

$$\ell_R\big(R/J^{[p^e]}\big) = p^{ed}\ell_R(R/J)$$

which will complete the proof. Consider a decomposition $0 = N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_s = R/J$ where $s = \ell_R(R/J)$ and $N_{i+1}/N_i \cong k = R/\mathfrak{m}$. Tensoring with the flat module $F^e_* R$ we obtain

$$0 = (F^e_* R)\otimes_R N_0 \subsetneq (F^e_* R)\otimes_R N_1 \subsetneq (F^e_* R)\otimes_R N_2 \subsetneq \cdots \subsetneq (F^e_* R)\otimes_R N_s \cong F^e_*(R/J^{[p^e]}).$$

Each $(F^e_* R)\otimes_R N_{i+1}/(F^e_* R)\otimes_R N_i$ is isomorphic to $F^e_*(R/\mathfrak{m}^{[p^e]})$ and so has length p^{ed} as an $F^e_* R$-module. It follows that

$$\ell_R\big(R/J^{[p^e]}\big) = p^{ed}\ell_R(R/J)$$

as desired. □

Theorem 1.6. *For $(R, \mathfrak{m})$ a Noetherian local d-dimensional ring of characteristic $p > 0$, the following are equivalent:*

(a) *R is regular.*
(b) *$\ell_R\big(R/\mathfrak{m}^{[p^e]}\big) = p^{ed}$ for every $e > 0$.*
(c) *$\ell_R\big(R/\mathfrak{m}^{[p^e]}\big) = p^{ed}$ for some $e > 0$.*

Proof. We just showed that (a) $\Leftarrow$ (b) and obviously (b) $\Leftarrow$ (c), so it suffices to show that (c) implies (a). We essentially already sketched this when the residue field is perfect (since then (c) implies that $F^{ed}_* R$ is free). The general case is left as an exercise (if time permits, we may prove a more general theorem later showing that $e_{\mathrm{HK}}(R) = 1$ actually implies that R is regular). □

Exercise 1.1. Prove Theorem 1.6.

Before moving on to existence, let me make one more observation.

Proposition 1.7. *With notation as above*

$$p^{ad}e_{\mathrm{HK}}(J; R) = e_{\mathrm{HK}}(J^{[p^a]}; R).$$

Proof. It is obvious. □

1.1. Existence of the limit. We follow closely the recent proof of the existence of Hilbert-Kunz multiplicity as shown in [**PT16**].

First we state a fact that we won't have time to prove.

Lemma 1.8. *If $(R, \mathfrak{m}, k)$ is a local F-finite Noetherian domain of dimension d then*

$$[F^e_* K(R) : K(R)] = [F^e_* k : k] \cdot p^{ed}.$$

You probably already believe it anyways.

Lemma 1.9. *Suppose that $(R, \mathfrak{m}, k)$ is a local ring and that M is a finite R-module. Then there exists a constant (depending on M) so that*

$$\ell_R\big(M/\mathfrak{m}^{[p^e]}M\big) \le C \cdot p^{e \dim M}.$$

Proof. Suppose that $\mathfrak{m}$ is generated by t elements, then $\mathfrak{m}^{tp^e} \subseteq \mathfrak{m}^{tp^e-t+1} \subseteq \mathfrak{m}^{[p^e]}$ by the pigeon-hole principal. But

$$\ell_R\big(M/\mathfrak{m}^{tp^e}\big)$$

is eventually a polynomial

$$D \cdot (tp^e)^{\dim M} + \cdots = D \cdot t^{\dim M} \cdot p^{e \dim M} + \dots$$

of degree degree $\dim M$ in p^e. We can thus pick $C = D \cdot t^{\dim M}$ for $e \gg 0$, and choosing C even bigger for finitely many smaller e completes the proof. $\square$

Remark 1.10. The fact that $\ell_R\big(M/\mathfrak{m}^{tp^e}\big)$ is eventually a polynomial can be found for example in [**AM69**, Chapter 11] for the case that $M = R$. For the general case, if you only want to bound its length by a polynomial of degree $\dim M$ (which is all we actually need), write $J = \mathrm{Ann}_R(M)$ and note that $\dim R/J = \dim M$ and that there exists a surjection $(R/J)^{\oplus b} \longrightarrow M \longrightarrow 0$ for some $b > 0$.

Lemma 1.11. *Let R be an F-finite domain with $[F_* K(R) : K(R)] = p^\gamma$. Then there exists a short exact sequence*

$$0 \longrightarrow R^{\oplus p^\gamma} \longrightarrow F_* R \longrightarrow M \longrightarrow 0$$

such that $\dim(M) < \dim(R)$.

Proof. After inverting an element $c \in R$, we have that $R_c^{\oplus p^\gamma} \cong F_* R_c$. This gives us an injective map $R^{\oplus p^\gamma} \longrightarrow F_* R_c$. If the image is not in $F_* R \subseteq F_* R_c$, then multiplying by a high power of $c \in R$ will make it in R. This gives us the first map. Then if we we let M be the cokernel, it is easy to see that $\mathrm{Supp}\, M \subseteq V(c)$ and so $\dim(M) \leq \dim(R/cR) < \dim R$. $\square$

Theorem 1.12. *Suppose that $(R, \mathfrak{m}, k)$ is an F-finite Noetherian local domain of characteristic $p > 0$ and dimension $d > 0$ and that $\{I_e\}$ is a sequence of ideals such that $\mathfrak{m}^{[p^e]} \subseteq I_e$ for all $e > 0$. Suppose further that $I_e^{[p]} \subseteq I_{e+1}$. Then*

$$\lim_{e \longrightarrow \infty} \frac{\ell_R(R/I_e)}{p^{ed}}$$

exists

Proof. We follow [**PT16**]. Consider a short exact sequence as in Lemma 1.11

$$0 \longrightarrow R^{\oplus p^\gamma} \xrightarrow{\phi} F_* R \longrightarrow M \longrightarrow 0$$

with $\dim M < \dim R$. Now, $I_e^{[p]} \subseteq (I_{e+1})$ implies that $I_e F_* R \subseteq F_* I_{e+1}$ and so

$$\phi(I_e^{\oplus p^\gamma}) = \phi(I_e \cdot R^{\oplus p^\gamma}) \subseteq I_e F_* R = F_* I_e^{[p]} \subseteq F_* I_{e+1}.$$

Thus we have

$$\overline{\phi} : (R/I_e)^{p^\gamma} \longrightarrow F_*(R/I_{e+1}).$$

Therefore the length of $(R/I_e)^{p^\gamma}$ plus the length of the cokernel of ϕ is at least the length of $F_*(R/I_{e+1})$. In other words

$$\ell_R\big(\mathrm{coker}\, \overline{\phi}\big) + p^\gamma \ell_R(R/I_e) \geq \ell_R(F_* R/I_{e+1}) = [k^{1/p} : k] \cdot \ell_R(R/I_{e+1}). \tag{1.12.1}$$

Now, $\operatorname{coker}\overline{\phi}$ is the image of $F_*(R/I_{e+1})$ and so F_*I_{e+1} annihilates it. But

$$\mathfrak{m}^{[p^e]} \subseteq F_*\mathfrak{m}^{[p^{e+1}]} \subseteq F_*I_{e+1}$$

and so $\mathfrak{m}^{[p^e]}$ annihilates $\operatorname{coker}\overline{\phi}$. But $\operatorname{coker}\overline{\phi}$ is also the image over M and hence of $M/\mathfrak{m}^{[p^e]}M$. In particular

$$\ell_R\big(\operatorname{coker}\overline{\phi}\big) \leq \ell_R\big(M/\mathfrak{m}^{[p^e]}M\big).$$

By Lemma 1.9, this is bounded by $C_M p^{e(d-1)}$. Now, we divide (1.12.1) by $[F_*k : k]p^{(e+1)d} = p^{ed+\gamma}$ and obtain

$$\frac{C_M/p^\gamma}{p^e} + \frac{1}{p^{ed}}\ell_R(R/I_e) \geq \frac{1}{p^{(e+1)d}}\ell_R(F_*R/I_{e+1}). \tag{1.12.2}$$

The existence of the limit now follows from the following lemma. □

Lemma 1.13. *Suppose that p is prime, $d > 0$ an integer, and $\{t_e\}$ is a sequence of real real numbers such that $\{t_e/p^{ed}\}$ is bounded. Further suppose that there exists a constant C such that*

$$C/p^e + \frac{1}{p^{ed}}t_e \geq \frac{1}{p^{(e+1)d}}t_{e+1}.$$

Then $t := \lim_{e\longrightarrow\infty} \frac{t_e}{p^{ed}}$ exists and $t - 1/p^{ed}t_e \leq \frac{2C}{p^e}$.

Proof. Note that

$$C/p^{e+1} + C/p^e + \frac{1}{p^{ed}}t_e \geq C/p^{e+1} + \frac{1}{p^{(e+1)d}}t_{e+1} \geq \frac{1}{p^{(e+2)d}}t_{e+2}$$

and more generally that

$$2C/p^e + \frac{1}{p^{ed}}t_e \geq C(1/p^{e+m+1} + \cdots + 1/p^e) + \frac{1}{p^{ed}}t_e \geq \frac{1}{p^{(e+m)d}}t_{e+m}.$$

Let t^+ denote the limit supremum of $\{t_e/p^{ed}\}$ and t^- the limit infimum. Note

$$2C/p^e + \frac{1}{p^{ed}}t_e \geq t^+.$$

Apply the limit infimum to both sides we get $t^- \geq t^+$ and so the limit exists and hence so does the desired bound. □

Theorem 1.14. *For any $\mathfrak{m}$-primary ideal in a domain, and $J \subseteq \mathfrak{m}$ is $\mathfrak{m}$-primary, $e_{\mathrm{HK}}(J;R)$ exists.*

Proof. Suppose first that R is an F-finite domain. We'd be tempted to show that $\mathfrak{m}^{[p^e]} \subseteq J^{[p^e]}$, but this is impossible unless $J = \mathfrak{m}$. However, we certainly have $\mathfrak{m}^{[p^t]} \subseteq J$ for some integer t and so $\mathfrak{m}^{[p^e]} \subseteq J^{[p^{e-t}]}$ for all e. Hence we see that

$$\lim_{e\longrightarrow\infty} \frac{1}{p^{ed}}\ell_R\Big(R/J^{[p^{e-t}]}\Big) = \frac{1}{p^{td}} \lim_{e\longrightarrow\infty} \frac{1}{p^{ed}}\ell_R\big(R/J^{[p^e]}\big)$$

exists (say it equals b). Thus so does

$$bp^{td} = \lim_{e\longrightarrow\infty} \frac{1}{p^{ed}}\ell_R\big(R/J^{[p^e]}\big) = e_{\mathrm{HK}}(J;R).$$

For the non-F-finite case, it is harmless to assume that $R = k[\![x_1, \ldots, x_m]\!]/I$ is complete with residue/coefficient field k since the lengths $R/J^{[p^e]}$ are unchanged by completion. But now $S = \widehat{R \otimes_k \overline{k}}$ is F-finite and the R-lengths of $R/J^{[p^e]}$ are equal to the S-lengths of $S/(J^{[p^e]}S)$. □

2. F-signature

Suppose that $(R, \mathfrak{m}, k)$ is an F-finite domain of dimension d. For now, suppose that $k = k^p$ is perfect. Write

$$F^e_* R = R^{\oplus a_e} \oplus M_e$$

where M_e has no free summands. It turns out (we'll see shortly) that even though this sort of decomposition is not necessarily unique (it is if R is complete), the number a_e is independent of the decomposition. We'll define

$$s(R) = \lim_{e \longrightarrow \infty} \frac{a_e}{p^{ed}}$$

to be the F-signature of R. Note

(i) If R is regular, then $s(R) = 1$.
(ii) If R is not F-split, then $s(R) = 0$ (in fact, we'll see that if R is not F-regular, then $s(R) = 0$).
(iii) In general $0 \leq s(R) \leq 1$.

2.1. Existence of F-signature. Let's define $I_e = \{r \in R \mid \phi(F^e_* r) \subseteq \mathfrak{m} \text{ for all } \phi \in \operatorname{Hom}_R(F^e_* R, R)\}$.

Lemma 2.1. *I_e is an ideal of R.*

Proof. Obviously I_e is closed under sum. If $x \in I_e$ and $r \in R$, we need to show that $rx \in R$. For each $\phi \in \operatorname{Hom}_R(F^e_* R, R)$, define $\phi'(F^e_* \_\_) = \phi(F^e_* x \_\_)$. Then $\phi'(F^e_* r) \in \mathfrak{m}$ so then $\phi(F^e_* xr) \in \mathfrak{m}$ and so I_e is an ideal. □

Lemma 2.2. *With notation as above, $\ell_R(R/I_e) = a_e$. In particular, a_e is independent of the decomposition.*

Proof. Since M_e has no free R-summands, $\phi(M_e) \subseteq \mathfrak{m}$ for all $\phi \in \operatorname{Hom}_R(F^e_* R, R)$. Thus $M_e \subseteq I_e$. In fact we even have:

$$\mathfrak{m}^{\oplus a_e} \oplus M_e \subseteq I_e.$$

On the other hand, if $F^e_* x \in (F^e_* R) \setminus (\mathfrak{m}^{\oplus a_e} \oplus M_e)$, say the ith term in the direct sum decomposition is a unit u not in $\mathfrak{m}$. But then the projection onto the ith term sends $F^e_* x \mapsto u \notin \mathfrak{m}$. Hence

$$\mathfrak{m}^{\oplus a_e} \oplus M_e = I_e.$$

But $\ell R R/I_e = a_e$ as desired. □

Obviously $I_e \supseteq \mathfrak{m}^{[p^e]}$. Hence the F-signature limit exists if can show that

$$I_e^{[p]} \subseteq I_{e+1}$$

by our previous work with limits.

Lemma 2.3. *With notation as above $I_e^{[p]} \subseteq I_{e+1}$ and hence the F-signature limit exists by Theorem 1.12.*

PROOF. Choose $r \in I_e$. Then for any $\phi \in \mathrm{Hom}_R(F^{e+1}_* R, R)$, we have a restricted $\psi = \phi|_{F^e_* R}$. Note the elements in $F^e_* R \subseteq F^{e+1}_* R$ are the pth powers of elements of $F^{e+1}_* R$, hence

$$\phi(F^{e+1}_* r^p) = \psi(F^e_* r) \in \mathfrak{m}.$$

Thus $I_e^{[p]} \subseteq I_{e+1}$ as desired. $\square$

Remark 2.4. One can define $s(R) = \lim_{e \longrightarrow \infty} \ell_R(R/I_e)$ even if the residue field is not perfect. Our work above shows that the limit still exists.

2.2. Positivity of F-signature. Our next goal is to explain when the F-signature is positive. It is obviously zero if R is not F-split. First we need a lemma.

Lemma 2.5. *With notation as in the beginning of the section $\bigcap_e I_e = 0$ if and only if R is strongly F-regular.*

PROOF. Exercise! $\square$

Theorem 2.6. $s(R) > 0$ *if and only if R is strongly F-regular.*

PROOF. We suppose that the residue field is perfect for simplicity.

Suppose first that $\bigcap_e I_e \neq 0$ (ie, that R is not strongly F-regular) that $0 \neq c \in \bigcap_e I_e$. Since $\mathfrak{m}^{[p^e]} \subseteq I_e$, we see that

$$\ell_R(R/I_e) \leq \ell_R\left(\frac{R}{\langle c\rangle + \mathfrak{m}^{[p^e]}}\right) \leq C p^{e(d-1)}.$$

Therefore

$$s(R) = \lim_{e \longrightarrow \infty} \frac{1}{p^{ed}} \ell_R(R/I_e) = 0.$$

Now assume that R is strongly F-regular. Without loss of generality we may assume that $(R, \mathfrak{m}, k)$ is complete. The Cohen-Gabber-Structure Theorem says that we can find $A = k[\![x_1, \dots, x_n]\!] \subseteq R$ a finite *separable* extension (Noether normalization for complete rings). Furthermore, we can choose $0 \neq c \in A$ such that

$$c \cdot R^{1/p^e} \subseteq R[A^{1/p^e}] \cong R \otimes_A A^{1/p^e}$$

for all e. In other words, $c \cdot F^e_* R \subseteq R[F^e_* A]$. Now, since R is strongly F-regular, we can find $\phi \in \mathrm{Hom}_R(R^{1/p^{e_c}}, R)$ for some $e_c > 0$ such $\phi(c^{1/p^{e_c}}) = 1$. We will show that $s(R) \geq 1/p^{e_c d} > 0$.

Now, the p^eth roots of the monomials $\mathbf{x}^\alpha$, $\mathbf{0} \leq \alpha \leq \mathbf{p^e} - \mathbf{1}$ for a basis for A^{1/p^e} over A. Let p_α be the projection so that $p_\alpha(\mathbf{x}^{\alpha/p^e}) = 1$ and $p_\beta(\mathbf{x}^{\beta/p^e}) = 0$ for $\beta \neq \alpha$. We form the compositions

$$\pi_\alpha : R^{1/p^e} \xrightarrow{\cdot c} R \otimes_A A^{1/p^e} \xrightarrow{R \otimes \pi_\alpha} R.$$

Note $\pi_\alpha(\mathbf{x}^{\alpha/p^e}) = p_\alpha(c\mathbf{x}^{\alpha/p^e}) = c$. Now we post compose with ϕ and we obtain $\phi_\alpha = \phi \circ (\pi_\alpha)^{1/p^{e_c}}$ which sends $\mathbf{x}^{\alpha/p^{e+e_c}} \mapsto 1$ and $\mathbf{x}^{\beta/p^{e+e_c}} \mapsto 0$ for $\beta \neq \alpha$. Taking the direct sum of these maps gives a surjection

$$(\oplus\phi_\alpha) : R^{1/p^{e+e_c}} \longrightarrow R^{\oplus p^{ed}}.$$

Hence $s(R) \geq 1/p^{e_c d}$. □

Question 2.7. If one starts in characteristic zero with $R_{\mathbb{C}}$, can one find a lower bound on F-signatures of the mod p reductions $s(R_p)$? Better yet, it would be better to find a geometric interpretation of

$$\lim_{p \longrightarrow \infty} s(R_p)$$

(say in the case that R is essentially of finite type over $\mathbb{Q}$).

3. Transformation of F-signature under étale in codimension 1 extensions

Our goal in this section is to understand how F-signature behaves under finite extensions.

Lemma 3.1. *Suppose that $(R, \mathfrak{m}, k) \subseteq (S, \mathfrak{n}, k)$ is a finite extension of local domains with the same residue field. Then $\mathrm{Tr}(\mathfrak{n}) \subseteq \mathfrak{m}$.*

Proof. We prove it only in the case where the extension is generically Galois since the proof there is easier.

Let $G = \mathrm{Gal}(L/K)$ where $L = K(S)$ and $K = K(R)$. Then $\mathrm{Tr}(x) = \sum_{g \in G} g.x$. But if $x \in \mathfrak{n}$, then $g.x \in g.\mathfrak{n} = \mathfrak{n}$ (since the extension is local and finite). Thus $\mathrm{Tr}(x) \in \mathfrak{n} \cap R = \mathfrak{m}$. □

Lemma 3.2. *Suppose that $(R, \mathfrak{m}, k) \subseteq (S, \mathfrak{n}, k)$ is a finite extension of local domains with the same residue field. Further suppose that $R \subseteq S$ is étale in codimension 1 (or in other words that the ramification divisor is zero). Then S has at most one free R-summand.*

Proof. The fact that the ramification divisor is zero means that $\mathrm{Tr} \in \mathrm{Hom}_R(S, R)$ generates the Hom-set. Consider $J = \{s \in S \mid \mathrm{Tr}(sS) \subseteq \mathfrak{m}\}$. Now $\ell_S(S/J)$ is the number of free R-summands by the same argument as Lemma 2.2. But this length is at most one by Lemma 3.1 since $\mathfrak{n} \subseteq J$. □

Next we need the following result (whose proof we don't have time for).

Proposition 3.3 ([**Tuc12**])**.** *Suppose $(R, \mathfrak{m}, k)$ is a d-dimensional Noetherian local ring and for simplicity assume that $k = k^p$. Let M be a finitely generated R-module and let b_e denote the maximal rank of a R-free summand of $F^e_* M$. Then*

$$\lim_{e \longrightarrow \infty} \frac{b_e}{p^{ed}} = \mathrm{rank}(M) \cdot s(R)$$

where $\mathrm{rank}(M)$ *is the generic rank of M.*

We need one more result we probably should have proven earlier.

Theorem 3.4. *If R is strongly F-regular and $R \subseteq S$ is a module finite extension, then $R \longrightarrow S$ splits as a map of R-modules.*

Proof. For any $\phi \in \operatorname{Hom}_R(F^e_* R, R)$, consider the composition

$$\eta : F^e_* \operatorname{Hom}_R(S, R) = \operatorname{Hom}_{F^e_* R}(F^e_* S, F^e_* R) \longrightarrow \operatorname{Hom}_R(S, F^e_* R) \longrightarrow \operatorname{Hom}_R(S, R)$$

where the first map is induced by restriction and the second by ϕ. It is not difficult to verify that the follow diagram commutes

$$\begin{array}{ccc} \operatorname{Hom}_{F^e_* R}(F^e_* S, F^e_* R) & \xrightarrow{\ \eta\ } & \operatorname{Hom}_R(S, R) \\ \Big\downarrow {\scriptstyle \mathrm{ev@1}} & & \Big\downarrow {\scriptstyle \mathrm{ev@1}} \\ F^e_* R & \xrightarrow[\ \phi\ ]{} & R. \end{array}$$

But then the image of $\operatorname{Hom}_R(S, R)$ in R is stable under every ϕ. Any nonzero element in the image can be sent to 1 by some ϕ and hence $\operatorname{Hom}_R(S, R) \longrightarrow R$ must surject. $\square$

Next we obtain a transformation rule for F-signature.

Theorem 3.5. *Let $(R, \mathfrak{m}, k) \subseteq (S, \mathfrak{n}, k)$ be a module-finite local extension of F-finite d-dimensional normal local domains in characteristic $p > 0$, with corresponding extension of fraction fields $K \subseteq L$. Suppose $R \subseteq S$ is étale in codimension 1, and that R is strongly F-regular. Then the following equality holds:*

$$s(S) = [L : K] \cdot s(R).$$

Proof. We know the trace map $\operatorname{Tr} : S \longrightarrow R$ generates the S-module $\operatorname{Hom}_R(S, R)$. Moreover, the trace map is surjective since if not, then the evaluation-at-1 map

$$\operatorname{Hom}_R(S, R) \longrightarrow R$$

would not be surjective (since all maps are pre-multiples of Tr). Thus we know S has exactly one free R-module summand, $S = R \oplus M$.

Now let b_e denote the maximal rank of a free R-module-summand of S^{1/p^e}. We can also write an S-module decomposition

$$S^{1/p^e} = S^{\oplus a_e(S)} \oplus N_e$$

which we can further decompose as $(R \oplus M)^{\oplus a_e(S)} \oplus N_e$. While N_e has no free S-module summands, it is natural to think it might have R-module summands.

But $\operatorname{Hom}_R(N_e, R) \cong \operatorname{Hom}_R(N_e \otimes_S S, R) \cong \operatorname{Hom}_S(N_e, \operatorname{Hom}_R(S, R)) = \operatorname{Hom}_S(N_e, S)$ and it follows that any map $N_e \longrightarrow R$ factors through $\operatorname{Tr} : S \longrightarrow R$ (we did an exercise on this once). But if $N_e \longrightarrow R$ is surjective, so is the induced $N_e \longrightarrow S$ (since if not, the image would be contained in $\mathfrak{n}$ which is sent into $\mathfrak{m}$). Hence if N_e has an R-module summand, it has an S-module summand, which it does not.

By Proposition 3.3, if b_e is the number of free R-module summands of S^{1/p^e}, then

$$\lim_{e \longrightarrow \infty} \frac{b_e}{p^{ed}} = s(R) \cdot [L : K].$$

The above however shows that the number of R-module summands of S^{1/p^e} is $a_e(S)$. Hence

$$s(S) = s(R) \cdot [L : K]$$

as desired. □

4. An application to fundamental groups

Throughout this section we wuppose $(R, \mathfrak{m}, k)$ is a normal complete local domain and for simplicity that $k = \overline{k}$ is algebraically closed. (In fact, the results of this section hold if R is only strictly Henselian instead of complete with algebraically closed residue field). Note that if k is characteristic $p > 0$, then this implies that R is F-finite since it is a quotient of some $k[\![x_1, \dots, x_n]\!]$.

We will study the étale fundamental group of the regular locus of R. Let $U \subseteq \operatorname{Spec} R$ denote the regular locus of R (this is always an open set because R is complete and thus excellent). For example, if R has an isolated singularity at the origin, then $U = \operatorname{Spec} R \setminus V(\mathfrak{m})$.

Definition 4.1. We define the étale fundamental group

$$\pi_1^{\text{ét}}(U) = \lim_{\leftarrow S} \operatorname{Gal}(K(S)/K(R))$$

where the limit runs over (isomorphism classes of) finite local extensions of rings $R \subseteq S$ which are generically Galois and which are étale over U (or equivalently, étale in codimension 1 since the complement of U is regular and étale in codimension 1 extensions of regular schemes are étale).

This is not the normal / most general definition of the étale fundamental group, but it is equivalent see for example [**Mil80**].

Remark 4.2. An easy fact is that for any two finite extensions $R \subseteq S', S''$ satisfying the definition above, one can find a dominating finite extension $S \supseteq S', S''$ that also satisfies the condition of the definition. To do this, take the tensor product $S' \otimes_R S''$, mod out by a minimal prime and normalize (if needed).

Theorem 4.3. [**?**] *If R defined as above is also strongly F-regular and $U = (\operatorname{Spec} R)_{\text{reg}}$, then $\pi_1^{\text{ét}}(U)$ is finite and it size is bounded above by $1/s(R)$.*

Proof. Consider a finite local generically Galois extension $S \supseteq R$ which is étale in codimension 1. We know that $s(R) \cdot [K(S) : K(R)] = s(S) \leq 1$ by Theorem 3.5. Hence $[K(S) : K(R)] \leq 1/s(R)$. By Remark 4.2 there is a unique (up to isomorphism) largest such extension $S \supseteq R$. It follows that $\pi_1^{\text{ét}}(U) = \operatorname{Gal}(K(S)/K(R))$ for that extension and in part □

Remark 4.4. It is also possible to show that $p \not| \#(p_1^{\text{ét}}(U))$ even in the strictly Henselian case.

Bibliography

[AM69] M. F. Atiyah and I. G. Macdonald: *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802 (39 #4129)

[BMS15] B. Bhatt, L. Ma, and K. Schwede: *The dualizing complex of F-injective and Du Bois singularities*, arXiv:1512.05374.

[BS15] B. Bhatt and P. Scholze: *Projectivity of the Witt vector affine Grassmannian*, arXiv:1507.06490.

[GO83] S. Goto and T. Ogawa: *A note on rings with finite local cohomology*, Tokyo J. Math. **6** (1983), no. 2, 403–411. 732093

[Har66] R. Hartshorne: *Residues and duality*, Lecture notes of a seminar on the work of A. Grothendieck, given at Harvard 1963/64. With an appendix by P. Deligne. Lecture Notes in Mathematics, No. 20, Springer-Verlag, Berlin, 1966. MR0222093 (36 #5145)

[Har77] R. Hartshorne: *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116)

[Har94] R. Hartshorne: *Generalized divisors on Gorenstein schemes*, Proceedings of Conference on Algebraic Geometry and Ring Theory in honor of Michael Artin, Part III (Antwerp, 1992), vol. 8, 1994, pp. 287–339. MR1291023 (95k:14008)

[HS77] R. Hartshorne and R. Speiser: *Local cohomological dimension in characteristic p*, Ann. of Math. (2) **105** (1977), no. 1, 45–79. MR0441962 (56 #353)

[hf] B. F. (http://math.stackexchange.com/users/56960/brian fitzpatrick): *Proving two complexes are not quasi-isomorphic*, URL:http://math.stackexchange.com/q/373085 (version: 2013-04-26).

[Kaw98] Y. Kawamata: *Subadjunction of log canonical divisors. II*, Amer. J. Math. **120** (1998), no. 5, 893–899. MR1646046 (2000d:14020)

[Ma15] L. Ma: *F-injectivity and Buchsbaum singularities*, Math. Ann. **362** (2015), no. 1-2, 25–42. 3343868

[Mat89] H. Matsumura: *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid. MR1011461 (90i:13001)

[Mil80] J. S. Milne: *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. 559531

[PT16] T. Polstra and K. Tucker: *F-signature and hilbert-kunz multipicity: a combined approach and comparison*, arXiv:1608.02678.

[Sta16] T. Stacks Project Authors: *stacks project*, 2016.

[Tuc12] K. Tucker: *F-signature exists*, Invent. Math. **190** (2012), no. 3, 743–765. 2995185

[Wei94] C. A. Weibel: *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR1269324 (95f:18001)