THE FROBENIUS MAP: THE POWER OF PRIME CHARACTERISTIC

JACK JEFFRIES

These are lecture notes and exercises for a short graduate lecture series on positive characteristic methods for the SLMath/SMS Summer School An Introduction to Recent Trends in Commutative Algebra in June 2025. My goal in this series is to give an appreciation for the power of techniques involving the Frobenius map to prove statements that have nothing to do with Frobenius. It is not my goal to thoroughly develop the tools needed for research in this area. The audience has a varied background, so I am not assuming any background beyond a first year graduate sequence on algebra. There is not enough time in this course to cover background material from commutative algebra and homological algebra in addition to the specific content of these lectures, so instead I will often give statements that are specialized to more concrete situations rather than giving the most general statements, and sometimes also offer a "more generally version" for those have have additional background. For time reasons, I will often sketch proofs, occasionally leaving some details to the exercises.

In the first lecture, I will discuss the basic perspectives and terminology of the Frobenius map. The first problem set is intended to solidify these notions, though there are also a few problems that build towards the later lectures. The second lecture will briefly introduce tight closure and an application. The third lecture will introduce a couple of notions of F-singularities and outline a couple more applications. The second problem set will explore the notions from the last two lectures, and fill in some details of the proofs.

Throughout these notes, all rings are commutative with $1 \neq 0$, and p will denote a positive prime integer.

1. Basics with the Frobenius map

Recall that a ring R has characteristic p if

$$p = \underbrace{1 + \cdots + 1}_{p \text{ times}}$$

is zero in R. This is equivalent to R containing a field of characteristic p as a subring: if R has characteristic p, the image of the homomorphism $\mathbb{Z} \longrightarrow R$ is isomorphic to $\mathbb{F}_p$.

The Frobenius map. Let us start with an observation about binomial coefficients. For any integer i with $0 < i < p$, the binomial coefficient

$$\binom{p}{i} = \frac{p!}{(p-i)! \cdot i!}$$

has a factor of p in the numerator, but not the denominator. Since we also know this coefficient is an integer, e.g., for combinatorial reasons, the Fundamental Theorem of Arithmetic says that

it is a multiple of p. Thus, when R has characteristic p, for any $r, s \in R$, one has

$$\begin{aligned}(r+s)^p &= r^p + \binom{p}{1} r^{p-1}s + \binom{p}{2} r^{p-2}s^2 + \cdots + \binom{p}{p-1} rs^{p-1} + s^p \\ &= r^p + s^p, \quad \text{and} \\ (rs)^p &= r^p s^p,\end{aligned}$$

and $1^p = 1$, so the map

$$F\colon R \longrightarrow R, \quad F(r) = r^p$$

is a ring homomorphism from R to itself, called the **Frobenius map** on R. We may denote this as F_R to indicate the ring when useful.

One can apply the Frobenius map multiple times:

$$F^e\colon R \longrightarrow R, \quad F^e(r) = r^{p^e}$$

which we may call the **e-th Frobenius** or **e-th Frobenius iterate**. Note that no power map is a ring homomorphism in characteristic zero.

Example 1.1. For $R = \mathbb{F}_p$ the Frobenius map is the identity: this is Fermat's Little Theorem.

Example 1.2. For $R = \mathbb{F}_p[x]$, the Frobenius map is given by

$$F(a_n x^n + \cdots + a_1 x + a_0) = a_n x^{pn} + \cdots + a_1 x^p + a_0$$

and the iterates by

$$F^e(a_n x^n + \cdots + a_1 x + a_0) = a_n x^{p^e n} + \cdots + a_1 x^{p^e} + a_0.$$

Every ring of characteristic p has a Frobenius map, and the Frobenius map is compatible with every ring homomorphism between rings of characteristic p:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle F_R}\downarrow & & \downarrow{\scriptstyle F_S} \\ R & \xrightarrow{\varphi} & S \end{array} \qquad \begin{array}{ccc} r & \longmapsto & \varphi(r) \\ \downarrow & & \downarrow \\ r^p & \longmapsto & \varphi(r^p) = \varphi(r)^p. \end{array}$$

This universality and naturality is a clear sign of the importance of the Frobenius map.

Injectivity and surjectivity. Let us start with a simple relationship between the Frobenius map and something that has nothing to do with it.

Lemma 1.3. *Let R be a ring of characteristic p. The Frobenius map on R is injective if and only if R is reduced (meaning that R has no nonzero nilpotents).*

Proof. We will prove the contrapositive of each direction. ($\Leftarrow$) : If F_R is not injective, then there is some $r \neq 0$ with $r^p = 0$; such an element is a nonzero nilpotent of R.

($\Rightarrow$): If R is not reduced, then there is some $r \neq 0$ with $r^n = 0$ for some $n \geq 2$. Take n maximal such that $r^n \neq 0$; then $np > n$, so $F(r^n) = r^{pn} = 0$, and r^n is a nonzero element of the kernel of F_R. □

It is rarer for the Frobenius map to be surjective. The image of the Frobenius map is evidently the p-th powers of elements in R. A ring of positive characteristic is **perfect** if its Frobenius map is bijective. You are likely familiar with this consideration for fields. Perfect fields include all finite fields, like $\mathbb{F}_p$ and $\mathbb{F}_{p^7}$, and all algebraically closed fields, like $\overline{\mathbb{F}_p}$ and $\overline{\mathbb{F}_p(t)}$. However,

a field like $\mathbb{F}_p(t)$ is not perfect, as t is not a p-th power. However $\mathbb{F}_p[x]$ is evidently not perfect. One can show that when R is Noetherian then F_R is surjective if and only if R is a finite product of perfect fields.

Alternative perspectives. One of the most confusing aspects of the Frobenius map is the fact that the source and target are the same, though the map is typically not an isomorphism. It is often useful to separate the source and target of the Frobenius to clarify the situation. One can think of this as analogous to the case of linear algebra, where some aspects of an endomorphism of a vector space are easier to understand with separate bases on the source and target.

Our first alternative perspective on Frobenius is based on renaming the target copy of R. We will decorate every element in the target of the e-th Frobenius F^e with the decoration F^e_*. That is, F^e_*R is just an collection of doppelgängers of elements R:

$$F^e_*R = \{F^e_*r \mid r \in R\}$$
$$F^e_*r + F^e_*s = F^e_*(r+s) \quad \text{and} \quad F^e_*rF^e_*s = F^e_*(rs),$$

so the map

$$R \longrightarrow F^e_*R \qquad r \longmapsto F^e_*r$$

is an isomorphism. After rewriting "target R" as F^e_*R via the isomorphism above, the e-th Frobenius map takes the form

$$R \longrightarrow F^e_*R \qquad r \longmapsto F^e_*(r^{p^e}).$$

One should think of this as follows: the e-th Frobenius map sends $r \longrightarrow r^{p^e}$, and the F^e_* symbol simply says which copy of R the element r^{p^e} lives in. Put another way, we have the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{F^e} & R \\ {\scriptstyle =}\downarrow & & \downarrow{\scriptstyle \cong} \\ R & \longrightarrow & F^e_*R \end{array} \qquad \begin{array}{ccc} r & \longmapsto & r^{p^e} \\ \downarrow & & \downarrow \\ r & \longmapsto & F^e_*(r^{p^e}) \end{array}$$

where the bottom row is the Frobenius from $R \longrightarrow F^e_*R$ and the right map is the isomorphism "adding the decoration F^e_*".

When R is a domain, there is another useful way to think of F^e_*R. In this case, R has a field of fractions K, which admits an algebraic closure $\overline{K}$. Every element of R has a unique p^e-th root r^{1/p^e} in $\overline{K}$, as $\overline{K}$ is a perfect field. Define

$$R^{1/p^e} := \{r^{1/p^e} \in \overline{K} \mid r \in R\}.$$

One can verify that R^{1/p^e} is a subring of $\overline{K}$, and the map

$$R \longrightarrow R^{1/p^e} \qquad r \longmapsto r^{1/p^e}$$

is a ring isomorphism. We can think of the exponent $^{1/p^e}$ as a decoration that yields an isomorphic copy of R. After rewriting "target R" as R^{1/p^e} via this isomorphism, the Frobenius map takes the form

$$R \longrightarrow R^{1/p^e} \qquad r \longmapsto (r^{p^e})^{1/p^e} = r.$$

That is, after the identification above, the Frobenius map identifies with the inclusion of $R \subseteq R^{1/p^e}$. Put another way, we have the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{F^e} & R \\ {\scriptstyle =}\downarrow & & \downarrow{\scriptstyle \cong} \\ R & \longrightarrow & R^{1/p^e} \end{array} \qquad \begin{array}{ccc} r & \longmapsto & r^{p^e} \\ \downarrow & & \downarrow \\ r & \longmapsto & r = (r^{p^e})^{1/p^e}, \end{array}$$

where the bottom row is the inclusion map and the right map is the isomorphism $R \cong R^{1/p^e}$ of taking p^e-th roots. This notion of roots equally well makes sense when R is reduced: in this case, R embeds into product of fields, which embeds into a product of algebraically closed fields, where every element again has a unique p^e-th root.

A third perspective on the Frobenius on a reduced ring is by identifying the source of Frobenius with R^{p^e}, the subring consisting of p^e-th powers of elements of R. In this case, the Frobenius map corresponds to the inclusion map $R^{p^e} \subseteq R$.

Typical constructions. We now discuss some typical constructions for ring maps applied to special case of the Frobenius. For a general ring homomorphism $\varphi : A \longrightarrow B$, one has the notion of extension of an ideal $I \subseteq A$ given as the ideal of B given by $(\varphi(a) \mid a \in I)$. This leads to the notion of Frobenius powers. Given an ideal $I \subseteq R$, we define the **Frobenius powers** of I as

$$I^{[p^e]} = (a^{p^e} \mid a \in I) = (F^e(a) \mid a \in I).$$

If $I = (a_1, \ldots, a_t)$, then $I^{[p^e]} = (a_1^{p^e}, \ldots, a_t^{p^e})$, as is the case in general for extension of ideals. Observe that $I^{[p^e]} \subseteq I^{p^e}$, but these are typically different when I is not principal.

Another important construction comes from restriction of scalars. For a general ring homomorphism $\varphi : A \longrightarrow B$, one can view B as an A-module by restriction of scalars: B becomes an A-module by the rule $a \cdot b = \varphi(a)b$. One can view R as an R-module by restriction of scalars through F^e, so R acts on R by the rule

$$r \cdot s = r^{p^e} s.$$

It is especially helpful to use the alternative notations for the Frobenius map in this setting. Consider the Frobenius map in the form

$$R \longrightarrow F_*^e R \quad r \longmapsto F_*^e(r^{p^e}).$$

The R-module action on $F_*^e R$ is then

$$r \cdot F_*^e s = F_*^e(r^{p^e} s).$$

For R reduced, we may also consider the Frobenius map in the form

$$R \subseteq R^{1/p^e}.$$

The R-module action on R^{1/p^e} is then the straightforward action

$$r \cdot s^{1/p^e} = r s^{1/p^e} = (r^{p^e} s)^{1/p^e}.$$

We will return to discuss this structure in great detail for a polynomial ring soon.

One can also apply the restriction of scalars to an arbitrary R-module. For a general ring homomorphism $\varphi : A \longrightarrow B$, and B-module N, one can view N as an A-module by restriction

of scalars: N becomes an A-module by the rule $a \cdot n = \varphi(a)n$. To apply this with the Frobenius map, we let M be an R-module. Let us think of the Frobenius map in the form

$$R \longrightarrow F^e_* R \quad r \longmapsto F^e_*(r^{p^e}),$$

and think of M as a module over the target; we will rewrite M as

$$F^e_* M = \{F^e_* m \mid m \in M\}$$

with $F^e_* R$-action

$$F^e_* r \cdot F^e_* m = F^e_*(rm).$$

The action of R on $F^e_* M$ is then

$$r \cdot F^e_* m = F^e_*(r^{p^e}) F^e_* m = F^e_*(r^{p^e} m).$$

Finally, we discuss extension of scalars. For a general ring homomorphism $\varphi : A \longrightarrow B$, and A-module M, one can create a new B-module by extension of scalars. The construction is most naturally stated in terms of tensor products, but we give a slightly more concrete construction. One can write M in terms of generators and relations: M has generating set $\{m_i\}_i$ with relations $\{\sum_i a_{ij} m_i\}_j$, meaning $\sum_i a_{ij} m_i = 0$ in M for all j, and that these generate the tuples of relations on these generators. The module $\varphi^* M$ is then the B-module with generating set $\{m_i\}_i$ with relations $\{\sum_i \varphi(a_{ij}) m_i\}_j$. To apply this with the Frobenius map, we let M be an R-module. If M is as above, the Frobenius restriction of scalars module is the R-module $F^{e*}(M)$ with generating set $\{m_i\}_i$ with relations $\{\sum_i a_{ij}^{p^e} m_i\}_j$.

Polynomial rings and Kunz' Theorem. We will now analyze the R-module structure of $F^e_* R$ in detail in an important case.

Theorem 1.4. *Let K be a perfect field of characteristic p, and $S = K[x_1, \ldots, x_n]$ be a polynomial ring in n variables over K. Then $F^e_* S$ is a free S-module with basis*

$$B = \{F^e_*(x_1^{a_1} \cdots x_n^{a_n}) \mid 0 \leq a_i < p^e\}.$$

Proof. We need to show that every element of $F^e_* S$ can be written as an S-linear combination of the elements above.

Every element of $F^e_* S$ is a sum of elements of the form $F^e_*(\gamma x_1^{b_1} \cdots x_n^{b_n})$ with $\gamma \in K$ and $b_1, \ldots, b_n \geq 0$. Write $b_i = p^e c_i + a_i$ with $0 \leq a_i < p^e$. Then

$$\begin{aligned} F^e_*(\gamma x_1^{b_1} \cdots x_n^{b_n}) &= F^e_*(\gamma x_1^{p^e c_1 + a_1} \cdots x_n^{p^e c_n + a_n}) \\ &= F^e_*(\gamma x_1^{p^e c_1} \cdots x_n^{p^e c_n}) F^e_*(x_1^{a_1} \cdots x_n^{a_n}) \cdot \\ &= \gamma^{1/p^e} x_1^{c_1} \cdots x_n^{c_n} \cdot F^e_*(x_1^{a_1} \cdots x_n^{a_n}) \end{aligned}$$

Note that we have used that K is perfect in the last step. This shows that the purported basis spans.

To see this set is linearly independent, suppose that we have some $\beta_1, \ldots, \beta_t \in B$ and $s_1, \ldots, s_t \in S$ such that $\sum_i s_i \beta_i = 0$. Note that in a product

$$s_i \beta_i = s_i \cdot F^e_*(x_1^{a_1} \cdots x_n^{a_n}) = F^e_*(s_i^{p^e} x_1^{a_1} \cdots x_n^{a_n}),$$

every monomial occurring in the polynomial $s_i^{p^e} x_1^{a_1} \cdots x_n^{a_n}$ has exponents $b_1, \ldots, b_n$ such that $b_i \equiv a_i \mod p^e$. In particular, writing each $s_i \beta_i$ as F^e_* of some polynomial as above, the polynomials that occur have mutually distinct monomials, and thus cannot cancel each other.

It follows that $s_i\beta_i = 0$ for each i, which implies $s_i = 0$ for each i. This shows that B is a free basis. □

Intuitively, this proof shows that viewing S as the S-module F^e_*S breaks apart into pieces of the form $S \cdot F^e_*(x_1^{a_1} \cdots x_n^{a_n})$ consisting of all polynomials whose exponent vectors are coordinatewise congruent to $(a_1, \ldots, a_n)$. Various applications of the Frobenius are based on taking an element of S, viewing it as an element F^e_*S, and breaking it into its components in this free S-basis, or equivalently, applying S-linear maps from F^e_*S back to S. We will return to this idea soon.

This decomposition a special case of the "Fundamental Theorem of Frobenius".

Theorem 1.5 (Kunz). *Let R be a Noetherian ring of characteristic p, and let $e \geq 1$. The module F^e_*R is a flat R-module if and only if R is a regular ring.*

A flat module is a weakening of free module (free implies flat), and a polynomial ring over a field is a key example of a regular ring.

We end with a technical definition that is useful for many purposes.

Definition 1.6. A ring R of characteristic p is **F-finite** if F_*R is a finitely generated R-module; equivalently, F^e_*R is a finitely generated R-module for all e.

This is a finiteness property, somewhat akin to Noetherianity. In the exercises, you will show that every finitely generated algebra over a perfect field is F-finite. We can get a more concrete version of Kunz' theorem when R is F-finite and local. Recall that a **local ring** is a ring with a unique maximal ideal. We often write $(R, \mathfrak{m})$ for a local ring to denote R and its maximal ideal, or $(R, \mathfrak{m}, k)$ to denote the residue field $k = R/\mathfrak{m}$ as well. Given any ring R and prime ideal $\mathfrak{p}$, we can obtain a local ring $R_\mathfrak{p}$ for adjoining inverses to every element outside of $\mathfrak{p}$, a process called localization.

A typical example of a local ring is, for a field K and some variables $x_1, \ldots, x_n$, the collection of rational functions for the form

$$\left\{ \frac{f(x)}{g(x)} \;\middle|\; g(x) \text{ has nonzero constant term} \right\}.$$

This is the local ring $K[x_1, \ldots, x_n]_{(x_1, \ldots, x_n)}$ obtained from the polynomial ring by localization at the prime (maximal) ideal consisting of polynomials with constant term zero. Another key example of a local ring is the power series ring $K[\![x_1, \ldots, x_n]\!]$. These are the two typical examples to keep in mind of regular local rings.

Corollary 1.7 (Kunz). *Let $(R, \mathfrak{m})$ be an F-finite Noetherian local ring of characteristic p. The module F^e_*R is a free R-module if and only if R is a regular ring.*

Example 1.8. If K is a perfect field and S is either

$$K[x_1, \ldots, x_n]_{(x_1, \ldots, x_n)} \qquad \text{or} \qquad K[\![x_1, \ldots, x_n]\!],$$

then F^e_*S is free with basis

$$B = \{F^e_*(x_1^{a_1} \cdots x_n^{a_n}) \mid 0 \leq a_i < p^e\}$$

as in the polynomial case.

Exercise set #1

Throughout this problem set all rings have characteristic p.

(1) * Convince yourself, as succinctly as possible, that $r \in I$ if and only if $F^e_* r \in F^e_* I$.
(2) Let $S = \mathbb{F}_3[x,y]$. Find an element in $(x,y)^3$ that is not in $(x,y)^{[3]}$.
(3) Let $S = \mathbb{F}_3[x,y]$. Write out the free basis B for F_*S from the proof of Theorem 1.4 and write the element $F_*(2x^6y^7 + x^5y^3 + x^3y^4 + 2xy^2)$ as an S-linear combination of B.
(4) Let $\mathfrak{p}$ be a prime ideal in R. Show that $F^{-1}(\mathfrak{p}) = \mathfrak{p}$.
(5) * Let R be a ring and I be an ideal. Show that $F^e_*(I^{[p^e]}) = IF^e_*(R)$.
(6) Show that $R^{p^e} = \{r^{p^e} \mid r \in R\}$ is a subring of R.
(7) Suppose that R is reduced. Show that $R \cong R^{p^e}$, and that after identifying the source of the e-th Frobenius map with R^{p^e} via the isomorphism you found, the Frobenius map identifies with the inclusion map $R^{p^e} \subseteq R$.
(8) * Let $R = \mathbb{F}_p[x,y]/(xy)$.
   (a) Explain why R has $\mathbb{F}_p$-vector space basis $\{1, x, x^2, x^3, \dots, y, y^2, y^3, \dots\}$ (where, by abuse of notation, we write x for the equivalence class of x in the quotient).
   (b) Find an $\mathbb{F}_p$-vector space basis for F^e_*R, and describe the action of R on F^e_*R explicitly in terms of the action of each basis element of R with each basis element of F^e_*R.
   (c) Show that the ideal (x) of multiples of x in R is isomorphic to $R/(y)$ as an R-module.
   (d) Show that, as R-modules,

$$F^e_*R \cong R \cdot F^e_*1 \oplus \bigoplus_{0<i<p^e} R/(y) \cdot F^e_*(x^i) \oplus \bigoplus_{0<j<p^e} R/(x) \cdot F^e_*(y^j).$$

(9) Let $R = \mathbb{F}_2[x^2, xy, y^2]$; i.e., R is the subring of the polynomial ring $\mathbb{F}_2[x,y]$ with $\mathbb{F}_2$ vector space basis consisting of $\{x^iy^j \mid i+j \text{ is even}\}$. Find a generating set for F_*R as an R-module. Is your generating set a free basis?
(10) Let $K = \mathbb{F}_p(t_1, t_2, t_3, \dots)$, the field of rational functions over $\mathbb{F}_p$ in countably many variables. Is K an F-finite field?
(11) (a) Let R be an F-finite ring and I be an ideal. Show that R/I is also F-finite.
   (b) Let R be an F-finite ring and x be an indeterminate. Show that $R[x]$ is also F-finite. Deduce that every finitely generated algebra over a perfect field is F-finite.
(12) Let R be as in (9). Verify directly that F_*R has no free basis.
It may be useful to use the fact that if M is a free R-module with basis B and I is an ideal, then M/IM is a free R/I-module with basis given by the images of B; try different maximal ideals.

*To be used later in the lectures.

(13) [§] Let K be a perfect field and $S = K[x_1, \dots, x_n]$. Consider $\mathrm{Hom}_S(F^e_* S, S)$, the set of S-linear maps from $F^e_* S$ to S. Let $A = \{(a_1, \dots, a_n) \in \mathbb{Z}^n \mid 0 \leq a_i < p^e\}$.

(a) Show that for each $\alpha \in A$, there is a map $\Phi_\alpha \in \mathrm{Hom}_S(F^e_* S, S)$ such that

$$\Phi_\alpha(F^e_*(x_1^{a_1} \cdots x_n^{a_n})) = \begin{cases} 1 & \text{if } (a_1, \dots, a_n) = \alpha \\ 0 & \text{if } (a_1, \dots, a_n) \in A \smallsetminus \{\alpha\}. \end{cases}$$

(b) Consider $\mathrm{Hom}_S(F^e_* S, S)$ as an S-module by the rule $s \cdot \varphi(-) = s\varphi(-)$. Show that $\mathrm{Hom}_S(F^e_* S, S)$ is a free S-module with this action, and find a basis.

(c) Consider $\mathrm{Hom}_S(F^e_* S, S)$ as an $F^e_* S$-module by the rule $F^e_* s \cdot \varphi(-) = \varphi(F^e_* s \cdot -)$. Show that $\mathrm{Hom}_S(F^e_* S, S)$ is a free $F^e_* S$-module with basis the singleton $\{\Phi := \Phi_{(p^e-1, \dots, p^e-1)}\}$.

(14) Let R be a ring and I be an ideal. Show that $F^{e*}(R/I) \cong R/I^{[p^e]}$.

(15) [†] Let W be a multiplicatively closed subset of R. Show that $F^e_*(W^{-1}R) \cong W^{-1}F^e_* R$.

(16) Let $K = \mathbb{F}_p(t_1, t_2, t_3, \dots)$, and $R = K[\![x]\!]$. Show that $F_* R$ is not a free module. Compare with Corollary 1.7.

(17) Let R be a ring and I be an ideal. Is $F^{e*}(I) \cong I^{[p^e]}$ in general?

(18) Let R be a ring containing $\mathbb{Q}$, let n be a positive integer, and I an ideal of R. Show that the ideal $(a^n \mid a \in I)$ is equal to I^n. Compare to problem (2).

(19) [†] Let R be a Noetherian ring of positive characteristic. Show that F_R is surjective if and only if R is a finite product of perfect fields.

(20) [†] Let R be an F-finite Noetherian ring. Show that the singular locus of R is a closed subset of $\mathrm{Spec}(R)$.

(21) [†] Let R be a regular Noetherian ring and M be a finitely generated module.

(a) Show that $\mathrm{Ass}_R(M) = \mathrm{Ass}_R(F^e_* M)$ for all e.

(b) Show that $\mathrm{Ass}_R(M) = \mathrm{Ass}_R(F^{e*} M)$ for all e.

(c) Do the statements (21a) and (21b) hold if R is not assumed to be regular?

[§] To be used in Problem set #2.

[†] Requires some background from Commutative Algebra.

2. Tight closure

We now discuss a notion based on the Frobenius map that has many powerful applications.

Definition 2.1. Let R be a ring of characteristic p and $I \subseteq R$ be an ideal. The **Frobenius closure** of I is the ideal

$$I^F := \{a \in R \mid a^{p^e} \in I^{[p^e]} \text{ for some } e > 0\}.$$

Definition 2.2 (Hochster-Huneke). Let R be a domain of characteristic p and $I \subseteq R$ be an ideal. The **tight closure** of I is the ideal

$$I^* := \{a \in R \mid \exists c \neq 0 \ : \ ca^{p^e} \in I^{[p^e]} \text{ for all } e \gg 0\}.$$

When R is not necessarily a domain, we instead insist that c is not in any minimal prime ideal of R.

It follows from the definitions that $I \subseteq I^F \subseteq I^*$. These are notions that say that an element is in asymptotically in I, in various senses. The main fact about tight closure we will observe today is the following:

Theorem 2.3. *Let S be a polynomial ring over a perfect field K (or more generally, a regular ring of characteristic p). Then for any ideal $I \subseteq S$, we have $I^* = I$.*

The statement may look a bit odd, but the point of the theorem is that it can be much easier to check that an element is in I^* rather than I. We need a lemma to prepare for the proof.

Lemma 2.4. *Let $\varphi : A \longrightarrow B$ be a homomorphism of rings such that B is a free (or more generally, flat) A-module by restriction of scalars, and let I be an ideal of A, and $f \in A$. Then $(IB :_B f) = (I :_A f)B$.*

Proof. The containment $\supseteq$ follows from the definitions without assuming anything about B. For the other containment, let $g \in (IB :_B f)$, so there exist $a_i \in I$ and $b_i \in B$ such that

$$gf = \sum_i a_i b_i.$$

Let $\{\beta_j\}$ be a basis for B as an A-module, so we can write

$$g = \sum_j g_j \beta_j \quad b_i = \sum_j b_{ij} \beta_j$$

for some $g_j, b_{ij} \in A$. Then substituting in we get

$$\left(\sum_j g_j \beta_j\right) f = \sum_i a_i \left(\sum_j b_{ij} \beta_j\right)$$

$$\sum_j f g_j \beta_j = \sum_j \left(\sum_i a_i b_{ij}\right) \beta_j$$

Now, using the A-linear independence of β_j, we get equations of the form

$$f g_j = \sum_i a_i b_{ij},$$

so $g_j \in (I :_A f)B$; then since g is a B-linear combination of g_j, we have $g \in (I :_A f)B$. □

Proof of Theorem 2.3. We always have $I \subseteq I^*$ so there is only one containment left to show. Let $a \in I^*$, so there exists $c \neq 0$ with $ca^{p^e} \in I^{[p^e]}$ for all $e \gg 0$. In particular, for $e \gg 0$ have

$$c \in (I^{[p^e]} :_S a^{p^e})$$

Let us consider the analogue of this same containment in $F_*^e R$:

$$F_*^e c \in (F_*^e(I^{[p^e]}) :_{F_*^e S} F_*^e(a^{p^e})) = (IF_*^e S :_{F_*^e S} a),$$

where we have applied the exercise. By the Lemma and Kunz' Theorem, we have

$$F_*^e c \in (I :_S a)F_*^e S = F_*^e\left((I :_S a)^{[p^e]}\right),$$

again using the exercise. That is,

$$c \in (I :_S a)^{[p^e]}.$$

If $a \notin I$, then $(I :_S a) \subsetneq S$ and

$$c \in \bigcap_{e \gg 0} (I :_S a)^{[p^e]} \subseteq \bigcap_{e \gg 0} (I :_S a)^{p^e} = 0,$$

a contradiction. Thus, we must have $a \in I$. □

Let us illustrate a typical application of tight closure. By way of motivation, let K be a field, and $R = K[x]$ be a polynomial ring in one variable. Given any two elements $f, g \in R$, we claim that $fg \in (f^2, g^2)$. To see it, let d be the GCD of f and g, and write $f = df'$ and $g = dg'$. Then f' and g' are coprime and R is a PID so we can find r, s with $rf' + sg' = 1$. Then

$$fg = d^2 f'g' = d^2 f'g'(rf' + sg') = rg'(d^2 f'^2) + sf'(d^2 g'^2) = rg'f^2 + sf'g^2 \in (f^2, g^2).$$

Now take a polynomial ring in two variables $K[x, y]$. The previous argument certainly fails since R is not a PID, and even more convincingly since

$$xy \notin (x^2, y^2).$$

The next best thing to hope for that for any $f, g, h \in K[x, y]$ we have $fgh \in (f^2, g^2, h^2)$. This is also false; we learned the following example from Anurag K. Singh:

$$(xy)(x^2 - y^2)(x^2 + y^2) \notin \left((xy)^2, (x^2 - y^2)^2, (x^2 + y^2)^2\right),$$

at least if K has characteristic other than two.

However, the next best thing is true: for any $f, g, h \in K[x, y]$ we have $f^2 g^2 h^2 \in (f^3, g^3, h^3)$.

Theorem 2.5. *Let K be a field, and $S = K[x_1, \ldots, x_n]$ be a polynomial ring in n variables over K. Then for any $f_1, \ldots, f_{n+1} \in S$, the containment*

$$f_1^n \cdots f_{n+1}^n \in (f_1^{n+1}, \ldots, f_{n+1}^{n+1})$$

holds.

We will prove this theorem in the case that K algebraically closed of characteristic p, and $n = 2$ just to keep notation simpler. One can in fact deduce the theorem for all fields from this case. The Theorem holds more generally when S is a regular local ring of dimension n, though it requires different techniques in mixed characteristic.

Lemma 2.6. *Let R be a local ring of dimension n with an infinite residue field, $f \in R$, and I be an ideal of R. If $f^s \in I^s$ for some s, then there exists c not in any minimal prime of R such that $cf^t \in (\ell_1, \ldots, \ell_n)^t$ for all $t \gg 0$, where $\ell_1, \ldots, \ell_n$ are n general linear combinations of the generators of I.*

The Lemma follows from some standard facts in integral closure theory; we outline a self-contained proof in the next exercise set.

Proof of Theorem 2.5 for K of positive characteristic. Standard reductions allow us to replace the polynomial ring with a regular local ring R of dimension n with an infinite residue field. Let's just do the case $n = 2$ for simplicity.

Let $f, g, h \in R$ a regular local ring of dimension two with infinite residue field. We need to show that $(fgh)^2 \in (f^3, g^3, h^3)$. Observe that $(fgh)^3 \in (f^3, g^3, h^3)^3$. We can apply the Lemma to get some $c \neq 0$ such that $c(fgh)^t \in (\ell_1, \ell_2)^t$ for $t \gg 0$. Now take $e \gg 0$ and set $t = 2p^e$:

$$\begin{aligned} c(fgh)^{2p^e} \in (\ell_1, \ell_2)^{2p^e} &\subseteq (\ell_1^{2p^e}, \ell_1^{2p^e-1}\ell_2, \ldots, \ell_1^{p^e}\ell_2^{p^e}, \ldots, \ell_1\ell_2^{2p^e-1}, \ell_2^{2p^e}) \\ &\subseteq (\ell_1^{p^e}, \ell_2^{p^e}) = (\ell_1, \ell_2)^{[p^e]} \subseteq (f^3, g^3, h^3)^{[p^e]}. \end{aligned}$$

We can rewrite this as

$$c\left((fgh)^2\right)^{p^e} \in (f^3, g^3, h^3)^{[p^e]}$$

for $e \gg 0$. This means that $(fgh)^2 \in (f^3, g^3, h^3)^*$. By Theorem 2.3, we deduce that $(fgh)^2 \in (f^3, g^3, h^3)$. The proof for $n > 2$ is similar. □

The last thing we want to illustrate is that statements over fields of characteristic zero can be deduced from statements in characteristic p. We will use the following facts from Commutative Algebra:

Lemma 2.7. *Let A be a finitely generated ring over $\mathbb{Z}$; for example a finitely generated subring of a field K. Then*

(1) For any maximal ideal $\mathfrak{m}$ of A, the quotient $A/\mathfrak{m}$ is a finite field.
(2) For a polynomial ring $S = A[x_1, \ldots, x_n]$, and element $f \in S$ and ideal $I \subseteq S$, if $f \in I + \mathfrak{m}S$ for every maximal ideal $\mathfrak{m}$ of A, then $f \in I$.

This is all we need to deduce the Theorem in characteristic zero!

Proof of Theorem 2.5 for K of characteristic zero. We stick with f, g, h for simplicity. Suppose that we have $f, g, h \in K[x, y]$. Let A be the subring of K generated by the coefficients of f, g, h in K; this is a finite set, so A is a finitely generated ring, and $f, g, h \in A[x, y]$. Now let $\mathfrak{m}$ be a maximal ideal of A. Writing $\overline{*}$ for images modulo $\mathfrak{m}$, we have $\overline{f}, \overline{g}, \overline{h} \in A[x, y]/\mathfrak{m}A[x, y] \cong (A/\mathfrak{m})[x, y]$. Since $A/\mathfrak{m}$ is a field of characteristic zero, we have

$$(\overline{f}\,\overline{g}\,\overline{h})^2 \in (\overline{f}^3, \overline{g}^3, \overline{h}^3) \quad \text{in } (A/\mathfrak{m})[x, y].$$

This means that

$$(fgh)^2 \in (f^3, g^3, h^3) + \mathfrak{m}A[x, y] \quad \text{in } A[x, y].$$

Since this is true for all maximal ideals $\mathfrak{m}$, we deduce that

$$(fgh)^2 \in (f^3, g^3, h^3) \quad \text{in } A[x, y].$$

But since $A \subseteq K$, we obtain

$$(fgh)^2 \in (f^3, g^3, h^3) \quad \text{in } K[x, y].$$

□

3. F-singularities

So far we have largely focused on advantageous properties of the Frobenius map when R is a polynomial ring, or more generally, a regular ring, in light of Kunz' theorem. Let us focus on the case of the polynomial ring over a perfect field or the case of an F-finite regular local ring. In either of these cases, F^e_*R is free over R. We have applied this in the setting of tight closure to say that there are "no new relations" in F^e_*R, which then led to triviality of tight closure. We will now consider the following perspective on freeness of F^e_*R: this means that F^e_*R has many surjective maps back to R, namely the coordinate maps for a free basis. We will consider weakenings of the conclusion of Kunz' theorem by asking for fewer surjective maps back to R.

Definition 3.1. Let R be a ring of characteristic p. We say that R is **F-split** if there is an R-module homomorphism $\varphi : F_*R \longrightarrow R$ such that $\varphi(F_*1) = 1$.

Example 3.2. Let K be a perfect field and $S = K[x_1,\dots,x_n]$. Recall that F_*R is a free R-module with basis $B = \{F_*(x_1^{a_1}\cdots x_n^{a_n}) \mid 0 \le a_i < p\}$. Among this basis is F_*1. There is an S-linear map $\varphi : F_*S \longrightarrow S$ that sends any element $F_*s \in F_*S$ to the coefficient of F_*1 in the unique expresion of F_*s as an S-linear combination of the elements of B. In particular, $\varphi(F_*1) = \varphi(1\cdot F_*1 + 0\cdot \text{other elements of } B) = 1$. Thus S is F-split.

Example 3.3. Let K be a perfect field and $R = K[x,y]/(xy)$. We saw in the exercises that

$$F_*R \cong R\cdot F_*1 \oplus \bigoplus_{0<i<p} R/(y)\cdot F_*(x^i) \oplus \bigoplus_{0<j<p} R/(x)\cdot F_*(y^j).$$

An argument similar to the previous example shows that R is F-split.

Lemma 3.4. *An F-split ring is reduced.*

Proof. We will show that the Frobenius map $F : R \longrightarrow F_*R$ is injective. Let $\varphi : F_*R \longrightarrow R$ be an R-module homomorphism with $\varphi(F_*1) = 1$. Then for any $r \in R$,

$$\varphi F(r) = \varphi(F_*r^p) = \varphi(rF_*1) = r\varphi(F_*1) = r.$$

Thus, if $F(r) = 0$, then $r = \varphi F(r) = 0$ as well. This shows that F is injective, so R is reduced. □

There are a few useful equivalences for the F-split condition.

Lemma 3.5. *Let R be a ring of characteristic p. The following are equivalent:*

(1) R is F-split: there is an R-module homomorphism $\varphi : F_*R \longrightarrow R$ such that $\varphi(F_*1) = 1$.
(2) For all $e > 0$, there is an R-module homomorphism $\varphi : F^e_*R \longrightarrow R$ such that $\varphi(F^e_*1) = 1$.
(3) For some $e > 0$, there is an R-module homomorphism $\varphi : F^e_*R \longrightarrow R$ such that $\varphi(F^e_*1) = 1$.
(4) For some $e > 0$, there is some $c \neq 0$ and an R-module homomorphism $\varphi : F^e_*R \longrightarrow R$ such that $\varphi(F^e_*c) = 1$.

The implications (2)⇒(1)⇒(3)⇒(4) are clear. The rest are outlined in the exercises.

Lemma 3.6. *Let R be an F-split ring and I an ideal. Then $I^F = I$.*

Proof. Recall that $I^F = \{a \in R \mid a^{p^e} \in I^{[p^e]} \text{ for some } e\}$. Take some $a \in I^F$, so $a^{p^e} \in I^{[p^e]}$ for some e. We can rewrite this as

$$aF^e_*1 = F^e_*a^{p^e} \in F^e_*I^{[p^e]} = IF^e_*R,$$

so $aF_*^e 1 = \sum_i a_i F_*^e r_i$ with $a_i \in I$. By the equivalences above, since R is F-split, we have a map φ such that $\varphi(F_*^e 1) = 1$. We get

$$a = \varphi(aF_*^e 1) = \varphi\left(\sum_i a_i F_*^e r_i\right) = \sum_i a_i \varphi(F_*^e r_i) \in I. \qquad \square$$

There is an extremely useful criterion for checking when a ring is F-split.

Theorem 3.7 (Fedder's criterion). *Let $(S, \mathfrak{m})$ be an F-finite regular local ring of characteristic p, and I an ideal of S. Then the ring S/I is F-split if and only if*

$$I^{[p]} : I \not\subseteq \mathfrak{m}^{[p]}.$$

The colon ideal $I^{[p]} : I$ is easy to compute in the special case when $I = (f)$ is a principal ideal; in this case $I^{[p]} : I = (f^{p-1})$. More generally, the colon ideal $I^{[p]} : I$ is easy to compute in the case that I generated by a regular sequence $f_1, \ldots, f_t$. Recall that $f_1, \ldots, f_t$ is a regular sequence if f_i is a nonzerodivizor modulo $f_1, \ldots, f_{i-1}$ for each i. In this case $I^{[p]} : I = (f_1 \cdots f_t)^{p-1} + I^{[p]}$.

We will outline the proof of Fedder's criterion in the exercises.

Example 3.8. Let K be a field, and consider a 3×3 matrix

$$M = \begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix}.$$

M is **nilpotent** if $M^n = 0$ for some n. For any given n, we can write out the nine entries M^n as polynomial expressions of the entries x_{ij} (of degree n) and we get nine equations to determine if $M^n = 0$. Much better, M is nilpotent if and only if the characteristic polynomial of M is of the form $T^3 = 0$, so the coefficients of the characteristic polynomial vanish. These are

$$f = x_{11} + x_{22} + x_{33}\ ,\ g = \begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix} + \begin{vmatrix} x_{11} & x_{13} \\ x_{31} & x_{33} \end{vmatrix} + \begin{vmatrix} x_{22} & x_{23} \\ x_{32} & x_{33} \end{vmatrix}\ ,\ h = \begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix}.$$

One can see (e.g., from the next observation) that f, g, h form a regular sequence. Order the variables $x_{11} > x_{12} > x_{13} > x_{21} > \cdots > x_{33}$ and take the reverse lexicographic order on the polynomial ring. Then

$$LT((fgh)^{p-1}) = LT(f)^{p-1} LT(g)^{p-1} LT(h)^{p-1} = (x_{11}x_{12}x_{21}x_{13}x_{22}x_{31})^{p-1} \notin \mathfrak{m}^{[p]},$$

so the quotient ring is F-split.

In particular, the ideal generated by f, g, h is a radical ideal. While one can see this directly from initial ideal methods in this example, the combination of such methods with Fedder's criterion is a useful technique for showing an ideal is radical.

There is a stronger condition that is closely related.

Definition 3.9. Let R be a ring of characteristic p. We say that R is **strongly F-regular** if for any c not in any minimal prime of R, there is some e and an R-module homomorphism $\varphi : F_*^e R \longrightarrow R$ such that $\varphi(F_*^e c) = 1$. When R is a domain, this simplifies to: for any $c \neq 0$, there is some e and an R-module homomorphism $\varphi : F_*^e R \longrightarrow R$ such that $\varphi(F_*^e c) = 1$.

It follows from the definition that any strongly F-regular ring is F-split: one can enforce the definition with $c = 1$, and use the equivalences established above. If R is strongly F-regular and c not in any minimal prime of R, given an e that "works", any larger e also "works."

Lemma 3.10. *Let R be a strongly F-regular ring and I an ideal. Then $I^* = I$.*

Proof. Recall that

$$I^* = \{a \in R \mid \text{there exists } c \text{ not in any minimal prime } : \ ca^{p^e} \in I^{[p^e]} \text{ for } e \gg 0\}.$$

Take some $a \in I^*$, so $ca^{p^e} \in I^{[p^e]}$ for some c not in any minimal prime and $e \gg 0$. We can rewrite this as

$$aF_*^e c = F_*^e(ca^{p^e}) \in F_*^e I^{[p^e]} = IF_*^e R.$$

From the definition of strongly F-regular with c and the note above, for all $e \gg 0$ there is some $\varphi : F_*^e R \longrightarrow R$ such that $\varphi(F_*^e c) = 1$. Applying φ, we get

$$a = a\varphi(F_*^e c) = \varphi(aF_*^e c) = \varphi\left(\sum_i a_i F_*^e r_i\right) = \sum_i a_i \varphi(F_*^e r_i) \in I. \qquad \square$$

It is a longstanding open question whether a ring with the property that every ideal is tightly closed is necessarily strongly F-regular.

Proposition 3.11. *Let $(R, \mathfrak{m}, k)$ be an F-finite regular local ring. Then R is strongly F-regular.*

Proof. The main point is the Corollary to Kunz' theorem: $F_*^e R$ is a free R-module for each e in this setting. Let $c \neq 0$. We also need a couple of standard facts from Commutative Algebra. First, the Krull Intersection Theorem says that $\bigcap_{n>0} \mathfrak{m}^n = 0$ in any local ring. Thus $\bigcap_{e>0} \mathfrak{m}^{[p^e]} \subseteq \bigcap_{e>0} \mathfrak{m}^{p^e} = 0$, so there is some e such that $c \notin \mathfrak{m}^{[p^e]}$. Second, a consequence of Nakayama's Lemma says that for M a finitely generated free module over a local ring $(R, \mathfrak{m})$, any element not in $\mathfrak{m}M$ is part of a free basis of M. Applying this to $F_*^e R$, we have $\mathfrak{m}F_*^e R = F_*^e \mathfrak{m}^{[p^e]}$. Thus, with e as above, $F_*^e c$ is part of a free basis for $F_*^e R$. Completing $\beta_1 = F_*^e c$ to a full basis $\{\eta_i\}$ for $F_*^e R$, there is an R-linear map φ that sends $\sum_i r_i \beta_i$ to r_1. In particular, $\varphi(F_*^e c) = 1$. $\square$

There is an analogue of Fedder's criterion, called Glassbrenner's criterion, for strong F-regularity. However, we will focus on another important source of strongly F-regular rings.

Definition 3.12. Let $R \subseteq S$ be an inclusion of rings. We say that R is a **direct summand** of S if there is an R-module homomorphism $\psi : S \longrightarrow R$ such that $\psi(1) = 1$.

Proposition 3.13. *Let $R \subseteq S$ be an inclusion of rings of characteristic p, and suppose that R is a direct summand of S.*

(1) If S is a strongly F-regular domain, then R is strongly F-regular.
(2) If S is F-split, then R is F-split.

Proof. We will prove the first statement, as the second is very similar. Let S be strongly F-regular, and $\psi : S \longrightarrow R$ such that $\psi(1) = 1$. Suppose that $c \neq 0$ in R. There is some e and S-linear map $\varphi : F_*^e S \longrightarrow S$ such that $\varphi(F_*^e c) = 1$. Since $R \subseteq S$, φ is R-linear as well. The restriction of the composition $\psi \circ \varphi|_{F_*^e R} : F_*^e R \longrightarrow R$ is an R-linear map sending $F_*^e c$ to 1. This shows that R is strongly F-regular. $\square$

Example 3.14. Let K be a perfect field. Let $R = K[x^2, xy, y^2] \subseteq S = K[x, y]$. We claim that R is a direct summand of S. Note that R is the K-vector space spanned by monomials whose total degree is even. Any element $s \in S$ has a unique expression of the form $s = s_{even} + s_{odd}$ where s_{even} is a linear combination of monomials of even degree, i.e., $s_{even} \in R$, and s_{odd} is a linear combination of monomials of odd degree. Thus, there is a well-defined map $\psi : S \longrightarrow R$ given by $\psi(s) = s_{even}$. This map is R-linear: if $r \in R$, then $rs = rs_{even} + rs_{odd}$, where rs_{even} is a linear

combination of monomials of even degree and rs_{odd} is a linear combination of monomials of odd degree. This means that $\psi(rs) = rs_{even} = r\psi(s)$, which says that ψ is R-linear.

We now loosely outline an application of strong F-regularity. A **magic square** of size t with row sum n is a $t \times t$ array of nonnegative integers such that each row and each column sums to n. For example,

1	14	14	4
11	7	6	9
8	10	10	5
13	2	3	15

is a particularly gaudy magic square of size 4 and row sum 33. There is only one magic square of size 1 and row sum n, namely

n

and there are $n+1$ magic squares of size 2 and row sum n, namely

i	$n-i$
$n-i$	i

$0 \le i \le n.$

Theorem 3.15 (Stanley). *Denote by $M_t(n)$ the number of $t \times t$ magic squares with row sum n. For any $t > 0$, the function $M_t(n)$ is a polynomial for $n \ge 0$.*

Outline. Step 1: Let K be a field of positive characteristic and $S = K[x_{11}, \ldots, x_{33}]$. We associate to each magic square a monomial in S:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \quad \rightsquigarrow \quad x_{11}^{a_{11}} x_{12}^{a_{12}} \cdots x_{33}^{a_{33}}$$

and we let R be the K-vector space spanned by these monomials. R is a subring of S. The number $M_t(n)$ is equal to the number of monomials in R of degree nt, or equivalently, the vector space dimension of R_{nt}. This part is elementary.

Step 2: The ring R is generated over K by magic squares of row sum 1; i.e., R is generated in a single degree. This boils down to the fact that any magic square is a sum of permutation matrices, which is a nontrivial fact from combinatorics/convex geometry called the Birkhoff-Von Neumann Theorem. If we divide all of the degrees in R through by t, then R is generated in degree one, and $M_t(n)$ is now just the Hilbert function of R. It follows from general facts that $M_t(n)$ *eventually* agrees with a polynomial, but we want to show that it agrees with a polynomial for all nonnegative values of n.

Step 3: The ring R is a direct summand of S. This is not too hard to show. It then follows that R is a strongly F-regular graded ring.

Step 4: The fact that R is strongly F-regular forces certain graded pieces of local cohomology to vanish, which then forces R to be Cohen-Macaulay and the regularity of R to be less than the dimension of R. These conditions then make the Hilbert function of R a polynomial. □

Exercise set #2

(1) Explain as succinctly as possible why the ring $K[x,y]/(x^2)$ is not F-split nor strongly F-regular.

(2) Let K be a perfect field of characteristic p and $S = K[x,y]_{(x,y)}$. Recall that this is an F-finite regular local ring. Apply Fedder's criterion to the rings $S/(x^2)$ and $S/(xy)$. Compare this to our other examples.

(3) Let K be a perfect field of characteristic p and $S = K[x,y,z]_{(x,y,z)}$. Apply Fedder's criterion to:
- $S/(x^2+y^2+z^2)$. It may be helpful to consider the cases with $p = 2$ and $p \neq 2$ separately.
- $S/(x^4+y^4+z^4)$.
- $S/(x^3+y^3+z^3)$. It may be helpful to consider the cases with $p = 3$, $p \equiv 1 \mod 3$, and $p \equiv 2 \mod 3$ separately.

(4) Let K be a field of characteristic $\neq 2$ and $S = K[x,y]$. Verify that $fgh \notin (f^2, g^2, h^2)$ for $f = xy$, $g = x^2 - y^2$, $h = x^2 + y^2$.

(5) Complete the proof of Lemma 3.5.

Hint: For (3)⇒(1)⇒(2), think of $R \xrightarrow{F^{e+e'}} F_*^{e+e}R$ as the composition $R \xrightarrow{F^e} F_*^e R \xrightarrow{F_*^{e'}F} F_*^{e+e'}R$. You may find it useful to show that if there is some e that "works" any smaller e "works", and if e "works", then $2e$ "works".

(6) Let K be a field, and $R \subseteq S = K[x_{11},\dots,x_{33}]$ be the K-vector space spanned by monomials $x_{11}^{a_{11}}x_{12}^{a_{12}}\cdots x_{33}^{a_{33}}$ such that $\{a_{ij}\}$ is a magic square. Explain why R is a ring, and show R is a direct summand of S via the K-vector space map $\psi : S \longrightarrow R$ given by

$$\psi(x_{11}^{a_{11}}x_{12}^{a_{12}}\cdots x_{33}^{a_{33}}) = \begin{cases} x_{11}^{a_{11}}x_{12}^{a_{12}}\cdots x_{33}^{a_{33}} & \text{if } \{a_{ij}\} \text{ is a magic square} \\ 0 & \text{otherwise.} \end{cases}$$

(7) Let K be a perfect field of characteristic p and $R = K[x,y,z]/(x^3+y^3+z^3)$.
(a) If $p \equiv 2 \mod 3$, show that $(z^2)^p \in (x,y)^{[p]}$. Deduce that $z^2 \in (x,y)^F$ and $z^2 \in (x,y)^*$. Compare this with (3) above.
(b) If $p \equiv 1 \mod 3$, show that $z^2 \in (x,y)^*$. Deduce that R is not strongly F-regular.

(8) † Lemma 2.6 follows from standard properties of integral closure, but we outline a self-contained argument in the case of polynomials $f_1,\dots,f_{n+1}$ homogeneous of the same degree in a polynomial ring $S = K[x_1,\dots,x_n]$ over an infinite field K.
(a) Let T be an indeterminate. Explain why $K[f_1,\dots,f_{n+1}] \cong K[f_1T,\dots,f_{n+1}T] \subseteq R[T]$.
(b) Let $f_1,\dots,f_{n+1} \in S$ be homogeneous polynomials of the same degree. Explain why the inclusion $K[\ell_1T,\dots,\ell_nT] \subseteq K[f_1T,\dots,f_{n+1}T]$ is module-finite for generic linear combinations $\ell_1,\dots,\ell_n$ of $f_1,\dots,f_{n+1}$.
(c) Show that the inclusion $R[\ell_1T,\dots,\ell_nT] \subseteq R[f_1T,\dots,f_{n+1}T]$ is module-finite for generic $\ell_1,\dots,\ell_n$.
(d) Take an equation $(f_iT)^k + \cdots = 0$ of integral dependence for f_iT over $R[\ell_1T,\dots,\ell_nT]$ and collect the terms of the form T^k. Use this to show that $f_i^{k+t} \in (\ell_1,\dots,\ell_n)^t$.

(9) † Let R be a strongly F-regular Noetherian local or graded ring. Show that R is a domain. Hint: If R has distinct minimal primes, start by finding nonzero f,g such that $fg = 0$ and $f+g$ is not in any minimal prime.

†Requires some background from Commutative Algebra.

(10) In this problem, we prove Fedder's criterion in the case of $R = S/I$ for $S = K[x_1, \dots, x_n]_{(x_1,\dots,x_n)}$ with K perfect. We will use the conclusion of (13) from Problem Set 1 in this setting.
   (a) Explain why every R-linear map $\varphi : F_*R \longrightarrow R$ is induced from a map $\psi : F_*S \longrightarrow S$ in the sense that $\varphi(\overline{s}) = \overline{\psi(s)}$, thinking of $F_*R = F_*S/F_*I$.
   (b) Let Φ be as in problem (13) from Problem Set 1 and $s \in S$. Show that $(F_*s \cdot \Phi)(S) \subseteq \mathfrak{m}$ if and only if $s \in \mathfrak{m}^{[p]}$.
   (c) Show that $(F_*s \cdot \Phi)(I) \subseteq I$ if and only if $s \in (I^{[p]} : I)$. Deduce Fedder's criterion.

(11) In the context of the previous problem, show that

$$\operatorname{Hom}_R(F_*R, R) \cong \frac{F_*(I^{[p]} : I) \cdot \operatorname{Hom}_S(F_*S, S)}{F_*I^{[p]} \cdot \operatorname{Hom}_S(F_*S, S)}.$$

(12) † Compute the degree of the polynomial $M_t(n)$ for every t.

Department of Mathematics, University of Nebraska, 203 Avery Hall, Lincoln, NE-68588, USA
Email address: jack.jeffries@unl.edu