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:

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "F_R"'] & S \arrow[d, "F_S"] \\ R \arrow[r, "\varphi"] & S \end{tikzcd} \qquad \begin{tikzcd} r \arrow[r, mapsto] \arrow[d, mapsto] & \varphi(r) \arrow[d, mapsto] \\ r^p \arrow[r, mapsto] & \varphi(r^p) = \varphi(r)^p. \end{tikzcd}$$

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:

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

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

$$\begin{tikzcd} R \arrow[r, "F^e"] \arrow[d, "="'] & R \arrow[d, "\cong"] \\ R \arrow[r] & F^e_* R \end{tikzcd} \qquad \begin{tikzcd} r \arrow[r, mapsto] \arrow[d, mapsto] & r^{p^e} \arrow[d, mapsto] \\ r \arrow[r, mapsto] & F^e_*(r^{p^e}) \end{tikzcd}$$

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

$$\begin{tikzcd} R \arrow[r, "F^e"] \arrow[d, "="'] & R \arrow[d, "\cong"] \\ R \arrow[r] & R^{1/p^e} \end{tikzcd} \qquad \begin{tikzcd} r \arrow[r, mapsto] \arrow[d, mapsto] & r^{p^e} \arrow[d, mapsto] \\ r \arrow[r, mapsto] & r = (r^{p^e})^{1/p^e}, \end{tikzcd}$$

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, one passes to the total ring of quotients by localization; this is a 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

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

If $I = (a_1, \dots, a_t)$, then $I^{[p^e]} = (a_1^{p^e}, \dots, a_t^{p^e})$, 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

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

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

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

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

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

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 $S = K[x_1, \dots, x_n]$ be a polynomial ring in n variables over K. Then $F^e_* S$ is a free S-module with basis*

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

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 $b_1, \dots, b_n \ge 0$. Write $b_i = p^e c_i + a_i$ with $0 \le a_i < p^e$. Then

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

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 $\beta_1, \dots, \beta_t \in B$ and $s_1, \dots, s_t \in S$ 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 $b_1, \dots, b_n$ 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. $\square$

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 $(a_1, \dots, a_n)$. 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 $x_1, \dots, x_n$, the collection of rational functions for the form

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

This is the local ring $K[x_1, \dots, x_n]_{(x_1, \dots, x_n)}$ 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 $K[\![x_1, \dots, x_n]\!]$. 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

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

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.

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