CLASS 20, MONDAY APRIL 16TH: FUN WITH FROBENIUS

Today we will play around with F_* and see what can be drawn out. Some things fall out quite naturally from the definition.

Proposition 0.1. *The map $F : R \to F_*R$ induces a bijection of prime ideals.*

Proof. I claim that the bijection is given by $F^{-1}(\mathfrak{p}) \leftarrow\!\shortmid F_*\mathfrak{p}$ and $\mathfrak{p} \mapsto \sqrt{\mathfrak{p} \cdot F_*R}$.

Let $\mathfrak{p} \subseteq R$ be a prime ideal. Then if $F_*a \cdot F_*b \in \sqrt{\mathfrak{p} \cdot F_*R}$, this implies that $F_*a \cdot F_*b = F_*c^n$ for some $c \in \mathfrak{p}$. But this implies that

$$F_*a^p \cdot F_*b^p = a \cdot b = c^{np} \in \mathfrak{p}$$

Therefore, either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, which implies $F_*a \in \sqrt{\mathfrak{p} \cdot F_*R}$ or $F_*b \in \sqrt{\mathfrak{p} \cdot F_*R}$, as desired.

Finally, it goes to show that they are mutually inverse to one another. It is clear that $F^{-1}(\sqrt{\mathfrak{p} \cdot F_*R}) = \mathfrak{p}$. On the other hand, if $\mathfrak{p} \subseteq F_*R$ is prime, $F^{-1}(\mathfrak{p}) = \{a \in R \mid a^p \in \mathfrak{p}\} = \mathfrak{p}$. So this is in fact a bijection. $\square$

This brings about a nice idea: studying how F_* behaves on modules. As a lemma, we can see how it behaves on ideals.

Lemma 0.2. *If I is an ideal of R, then $F(I) = I \cdot F_*R \cong F_*I^{[p]}$, where $I^{[p]}$ is the ideal consisting of p^{th} powers of elements of I. We can also characterize it in terms of generators: if $I = \langle a_1, \ldots, a_n \rangle$, then $I^{[p]} = \langle a_1^p, \ldots, a_n^p \rangle$.*

Proof. The first claim is completely definitional. For the second part, if $a \in I$, then

$$a = r_1a_1 + \ldots + r_na_n$$

$$a^p = r_1^pa_1^p + \ldots + r_n^pa_n^p$$

Therefore, $F_*a^p = r_1F_*a_1^p + \ldots + r_nF_*a_n^p \in \langle a_1^p, \ldots, a_n^p \rangle$. So $I^{[p]} \subseteq \langle a_1^p, \ldots, a_n^p \rangle$. On the other hand, $I^{[p]}$ certainly contains a_i^p, so equality is achieved. $\square$

Now, I make a very natural observation: If M is an R-module, we can form F_*M as the module M as an Abelian group, but having $r \cdot m = r^pm$. This makes F_* into a functor from R-modules to R-modules: $F_*\varphi : F_*m \mapsto F_*\varphi(m)$.

Proposition 0.3. *Let $0 \to M' \to M \to M'' \to 0$ be a SES. Then so is*

$$0 \to F_*M' \to F_*M \to F_*M'' \to 0$$

That is to say, F_* is an exact functor.

Next up, I would like to get a handle on how complicated F_*R is as an R-module. On the surface, it seems quite docile, being isomorphic to R as Abelian groups. However, things can get quite complication. As an issue, sometimes F_*R is not even finitely generated as an R-module, even when R is Noetherian or even a field (cf Homework 5). Therefore, we make the following definition:

Definition 0.4. A Noetherian ring R of positive characteristic is called F**-finite** if F_*R is a finitely generated R-module.

Notation 0.5. For the rest of the course, R will be a Noetherian F-finite ring of positive characteristic $p > 0$. If $(R, \mathfrak{m})$ is written, we add the local condition. If $(R, \mathfrak{m}, k)$ is written, $(R, \mathfrak{m})$ is local and $k = R/\mathfrak{m}$.

Because they make things somewhat *perfect* for our study, I introduce the following notion:

Definition 0.6. A field K is called **perfect** if (it is characteristic 0 or) the map $F : K \to F_*K$ is surjective (it is always injective, thus an isomorphism). Otherwise, K is called **imperfect**.

This notion naturally extends to the notion of a **perfect ring**. We can also always take the perfection of a field (or ring), which is usually denoted $k^{\frac{1}{p^\infty}}$ or k_∞. This exists as it can be identified with the union of F^e_*K for all $e \geq 0$.

Proposition 0.7. *Any $\mathbb{F}_q$ is a perfect field for $q = p^e$.*

Proof. We need to show that F is surjective. Take $0 \neq x \in \mathbb{F}_q$ ($0 \mapsto 0$ of course). Since $x \in \mathbb{F}_q^\times$, we know that the order of x, say d, divides $p^e - 1$. But p and $p^e - 1$ are relatively prime, so $\gcd(p, d) = 1$. Therefore, there is an integer equation $mp + nd = 1$. Therefore

$$x = x^1 = x^{mp+nd} = x^{pm}x^{nd} = x^{pm} = (x^m)^p$$

So $x = F(x^m) \in \operatorname{im}(F)$. But x was arbitrary, so we are done. $\square$

Example 0.8. Consider the ring $R = K[x]$ where K is a perfect field. If we consider the module F_*R, we can see that

$$F_*a = \sum_{n \geq 0} F_*a_i x^i$$

for $a_i \in K$. Doing a small bit of combinatorics, we note that by the division algorithm, there exists a unique m and $r = 0, 1, \ldots, p-1$ such that $n = mp + r$ (say $m = \lfloor \frac{n}{p} \rfloor$ and r their difference, where $\lfloor - \rfloor$ is the floor function, or the integer part). Therefore, we can rewrite

$$F_*a = \sum_{m \geq 0} \sum_{r=0}^{p-1} F_*a_{mp+r}x^{mp+r} = \sum_{m \geq 0} \sum_{r=0}^{p-1} a_{mp+r}^{\frac{1}{p}} x^m F_*x^r$$

where $a_{mp+r}^{\frac{1}{p}}$ is the standard notation for the unique element b such that $b^p = a_{mp+r}$. This demonstrates F_*x^r for $r = 0, \ldots, p-1$ is a basis for F_*R as an R-module. Therefore F_*R is free:

$$F_*R \cong R^{\oplus p}$$

Example 0.9. Let $R = K[x^2, x^3]$ be the CM ring which is not regular (from class 18), and K perfect. Let's examine F_*R. I specialize to the case of $\operatorname{char}(K) = 3$ and leave the general case to the ambitious student.

In this case, we see that a generating set of F_*R over R is

$$F_*1, F_*x^2, F_*x^3, F_*x^4, F_*x^5, F_*x^7$$

This can be demonstrated explicitly. Thus R is F-finite. Moreover, localizing at the origin, we can show that all of these generators are necessary by degree arguments. So if F_*R was projective, $F_*R_{\langle x^2, x^3 \rangle} \cong R^6_{\langle x^2, x^3 \rangle}$. However, we can further localize at 0 to conclude $F_*K(x) \cong K(x)^6$, which is certainly not true by Example 0.8.

We will explore this relationship via Kunz Theorem next time.