NOTES ON CHARACTERISTIC p COMMUTATIVE ALGEBRA JANUARY 9TH, 2017

KARL SCHWEDE

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 $x = 0$. □

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 we definitely 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 four 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? 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 so $R^{1/p}$ has at least 4 generators as an R-module.