CLASS 19, FRIDAY APRIL 13TH: CHARACTERISTIC AND THE FROBENIUS

We now have a lot of the prerequisite material required to begin studying some of the most important properties of rings in positive characteristic. To begin, I will start by reviewing (from the Day 1 introduction) the notion of characteristic, and then issuing some of the various notations surrounding the Frobenius.

Rings come in many flavors. As mentioned on the first day, one of the most basic invariants is whether it is equal characteristic or mixed characteristic.

Definition 0.1. We define the **characteristic** of a ring R to be the smallest $n > 0$ such that $1+ \overset{n-times}{\cdots\cdots} +1 = 0$. If there is no such positive n, the characteristic is set to 0. Generally, we write $\mathrm{char}(R) = n$ to represent this quantity.

A ring R is called **equal characteristic** n if there exists a field K such that $K \hookrightarrow R$ and such that $\mathrm{char}(K) = n$. Otherwise, we say the ring is **mixed characteristic**.

Sometimes the **equal** is dropped. All rings fall into one of these categories:

Proposition 0.2. *A ring R is equal characteristic 0 if and only if $\mathbb{Q} \subseteq R$. A ring is characteristic $p > 0$, where p is a prime number, if and only if $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subseteq R$. All other rings are mixed characteristic, which holds if and only if $\mathrm{char}(R) \neq \mathrm{char}(R/\mathfrak{m})$ for some maximal ideal $\mathfrak{m}$.*

Proof. See homework 5. □

Example 0.3.

- $\mathbb{Z}$ is a ring of mixed characteristic. Indeed, it does not contain a field. Moreover, we note that $R/\mathfrak{m}$ can be a field of any possible characteristic.
- $R = \mathbb{Z}_{\langle p \rangle}$ is a local ring of mixed characteristic. R itself is characteristic 0, where as $R/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$ has characteristic p.
- $R[x_1, x_2, \ldots, x_n]$ and R are either both mixed characteristic or equal characteristic. In the second case, we can also consider $R[x_1, x_2, \ldots, x_n]/I$ where I is any proper ideal.
- As a corollary of the previous statement, $\mathbb{C}[x_1, x_2, \ldots, x_n]$ is equal characteristic 0 and $\mathbb{F}_p[x_1, x_2, \ldots, x_n]$ is equal characteristic p.
- $\mathbb{Z}/n\mathbb{Z}$ with n composite is mixed characteristic. Indeed, it does not contain a field and has characteristic n vs. characteristic p_i for all quotients by $\mathfrak{m}$, where $n = p_1^{e_1} \cdots p_m^{e_m}$.

Here is a theorem that is commonly proven in an abstract algebra or Galois theory course:

Theorem 0.4. *Any finite field has cardinality $q = p^e$, where p is a prime number. Moreover, there is a unique field of such cardinality, which can be thought of as formally adjoining the roots of the (splitting) polynomial $x^q - x$ over $\mathbb{F}_p$ to $\mathbb{F}_p$. Finally, the algebraic closure is the union of all such fields:*

$$\overline{\mathbb{F}_p} = \cup_{n \geq 0} \mathbb{F}_{p^e}$$

Proof. Given Proposition 0.2, and $\mathbb{Q}$ is infinite, we know finite field K has characteristic $p > 0$ prime. Therefore, $\mathbb{F}_p \subseteq K$. This makes K into an $\mathbb{F}_p$-module, or vector space, so $K \cong \mathbb{F}_p^e$ for some $e > 0$. Therefore, $|K| = p^e$.

If K, L are two such fields, we know that they are isomorphic as $\mathbb{F}_p$-modules (in many ways). Furthermore, we can consider $K^\times$ and $L^\times$, the group of non-zero elements under multiplication. Every element satisfies $x^{p^e-1} = 1$ because that is the order of the groups. If we put 0 back in, we see that the roots are necessarily those satisfying $x^{p^e} - x$. This shows $K \cong L$.

Finally, the algebraic closure of a field is always the union of all the algebraic extensions of the field, which are precisely those represented above. □

Caution: $\mathbb{F}_{p^e} \subseteq \mathbb{F}_{p^{e'}}$ if and only if $e|e'$ (not if $e \leq e'$). Also as noted, not all positive characteristic fields are finite. We have $\overline{\mathbb{F}_p}$ as an example already, and others include $\mathbb{F}_p(x)$, the rational functions with coefficients in $\mathbb{F}_p$.

We can now begin talking of the Frobenius morphism:

Definition 0.5. If R is a ring of characteristic $p > 0$, then the ring homomorphism

$$F : R \to R : r \mapsto r^p$$

is called the **Frobenius**.

This can be iterated, to produce $F^e = F \circ \overset{e-times}{\cdots\cdots} \circ F$. As noted (on day 1), this is a homomorphism of rings:

$$(r+s)^p = r^p + pr^{p-1}s + \ldots + \binom{p}{i} r^{p-i}s^i + \ldots + prs^{p-1} + s^p \equiv r^p + s^p$$

$$(rs)^p = r^p s^p$$

However, this quite obviously is not a R-module homomorphism:

$$(rs)^p = r^p s^p \neq r(s)^p = rs^p$$

There are a few ways to get around this:

1) We can think about R^p as a ring, containing only p^{th} powers of elements of R. In this case, the Frobenius can be viewed as the inclusion $R^p \subseteq R$.
2) We can similarly think of $R^{\frac{1}{p}}$ of formal p^{th} roots of elements of R. The Frobenius is then the inclusion $R \subseteq R^{\frac{1}{p}}$.
3) We can write F_*R for the range of the Frobenius: $F : R \to F_*R$. F_*R is an R-module which is R as an additive abelian group, but with multiplicative structure $r \cdot s = r^p s$. If confusion can arise, sometimes we write F_*s for s, and $rF_*s = F_*r^p s$.

I end today's lecture by demonstrating that the Frobenius gives some small information about the ring (also mentioned day 1):

Proposition 0.6. *If R is a ring of characteristic $p > 0$, then $F : R \to R$ is injective if and only if R is reduced (e.g. the nilradical $\mathcal{N} = 0$).*

Proof. See homework 5. □