Homework 1

Remember you are allowed to discuss with classmates (or an AI tool), but that you need to tell me who/what you discussed with + the final submitted writeup should be your own work.

(1) Prove the following statement:

Proposition 1. *Let $(R, \mathfrak{m}, k)$ be an F-finite local ring containing a* coefficient field, *i.e., there exists an injection $\gamma : k \to R$ such that $\pi \circ \gamma$ is an isomorphism, where π is the natural surjection $\pi : R \to R/\mathfrak{m} \cong k$. Then number of minimal generators for $F^e_* R$ as an R-module is*

$$[k : k^{p^e}] \cdot \dim_k(R/\mathfrak{m}^{[p^e]})$$

Solution: Use NAK! The number of minimal generators is $\dim_k F^e_* R/\mathfrak{m} F^e_* R$. Then compute

$$F^e_*(R)/\mathfrak{m} F^e_*(R) = F^e_*(R)/F^e_*(\mathfrak{m}^{[p^e]}) \cong F^e_*\left(R/\mathfrak{m}^{[p^e]}\right)$$

where first equality is by definition of bracket power and second is by fact that $F^e_*(-)$ is an exact functor.

Using our coefficient field, $F^e_*(R/\mathfrak{m}^{[p^e]})$ is a $F^e_* k$-vector space in a way that is compatible with the action of the k-vector space structure coming from the residue field. Concretely, the action from the residue field descends from the action of R and would be $c \cdot F^e_* \overline{r} = F^e_* \overline{c^{p^e} r}$. And the coefficient field perspective means that we get an action $F^e_* c \cdot F^e_* \overline{r} = F^e_* \overline{\gamma(c) r}$. And these actions are compatible in the sense that $F^e : k \to F^e_* k$ is a field extension, and the action via the smaller field is the restriction of scalars of the action via the larger field—in other words, $c \cdot F^e_* \overline{r} = F^e(c) \cdot F^e_* \overline{r}$.

Now use the standard fact of dimensions over field extensions to go from viewing $F^e_*(R/\mathfrak{m}^{[p^e]}$ as a $F^e_* k$-vector space to viewing it as our desired k-vector space, and notice that $[F^e_* k : k] = [k : k^p]$.

Or if you don't remember that fact, prove it in this special case via something like this:

Lemma 1. *Let k be char p and V be a k-vector space, let $q = p^e$. Then*

$$\dim_k F^e_* V = [k : k^q] \dim_k(V).$$

Proof. Let $\mathcal{U}$ be a k-basis for V, and let $\mathcal{C}$ be a k^q-basis for k. Then we claim that

$$\{F^e_*(cu) \mid u \in \mathcal{U}, c \in \mathcal{C}\}$$

is a k-basis for $F^e_* V$.

It spans because any $v \in V$ can be written first as a finite sum $\sum_i a_i u_i$ for some $u_i \in \mathcal{U}$ and $a_i \in k$, and then we can expand each $a_i = \sum_j b^p_{ij} c_j$ for $c_j \in \mathcal{C}$ and $b_{ij} \in k$ (since everything in k^q is of the form b^q for $b \in k$). Now

$$F^e_*(v) = F^e_*\left(\sum_{ij} (b^p_{ij} c_j) u_i\right) = \sum_{ij} b_{ij} F^e_*(c_j u_i).$$

For independence, we see that if $\sum_{ij} a_{ij} F^e_*(c_i u_j) = 0$ for $a_{ij} \in k$, then $F^e_*(\sum_{ij} a^p_{ij} c_i u_j) = 0$ and this forces first all the $\sum_i a^p_{ij} c_i = 0$ for all j, which then forces $a^p_{ij} = 0$ for all i, j as desired. $\square$

(2) (Exercise 5 in Ma–Polstra) Prove that if R is essentially of finite type[1] over an F-finite field, then R is also F-finite. Do this via first proving each of the following three facts:

(a) If R is F-finite, then R/I is F-finite for all ideals I.

Solution: Suppose $\{F_*g_i\}$ generates F_*R as an R-module. For any $r \in R$, write $F_*r = \sum_i s_i F_*g_i = F_*(\sum_i s_i^p g_i)$. Thus $r = \sum_i s_i^p g_i$, and so

$$F_*(\overline{r}) = F_*(\sum_i \overline{s_i}^p \overline{g_i}) = \sum_i \overline{s_i} F_* \overline{g_i} \in F_*(R/I)$$

so that $\{F_*\overline{g}_i\}$ is a generating set of $F_*(R/I)$ as an R/I-module.

(b) If R is F-finite, then $W^{-1}R$ is F-finite for all multiplicative sets W.

Solution: For ANY R-module M, if M is finitely generated as an R-mod, then $W^{-1}M$ is f.g. an a $W^{-1}R$-mod (e.g., by taking the image of the original generating set under the natural map to the localization).

(c) If R is F-finite, then $R[x]$ and $R[[x]]$ are F-finite for an indeterminate x.

Solution: Suppose $\{F_*g_i \mid 1 \le i \le t\}$ generates F_*R as an R-module. We claim that $\{F_*(g_i x^j) \mid 1 \le i \le t,\ 0 \le j < p\}$ Let $\sum_j r_j x^j$ be a polynomial (resp. power series) in $R[x]$ (resp. $R[[x]]$). For each $r_j \in R$, write $F_*r_j = \sum_i s_{ij} F_*g_i = F_*(\sum_i s_{ij}^p g_i)$. Then

$$F_*(\sum_j r_j x^j) = F_*(\sum_{i,j} s_{ij}^p g_i x^j) = \sum_{i,j} s_{ij} F_*(g_i x^j).$$

So it suffices to break down things of the form $F_*(g_i x^j)$. The only worry is that the exponent $j \ge p$. But in that case, write $j = ap + b$ for $b < p$, and so $F_*(g_i x^j) = x^a F_*(g_i x^b)$.

Solution: The solution to the whole problem is now clear, since finite type means we can write as $\cong k[[x_1, \dots, x_n]]/I$, and then we localize, so we're using steps (c) then (a) then (b) to get the result is F-finite as long as k is.

(3) (Exercise 1 in Ma–Polstra) Prove that if there exists an $e_0 > 0$ such that $F_*^{e_0}R$ is a finite R-module, then in fact $F_*^e R$ is a finite R-module for all $e > 0$.

Solution: Let $F_*^{e_0}g_1, \dots, F_*^{e_0}g_t$ be a generating set. First, observe that $\{F_*g_1, \dots, F_*g_t\}$ is a (probably very redundant) generating set of F_*R: for any $r \in R$ we can write

$$F_*^{e_0} r = \sum_i s_i F_*^{e_0} g_i = F_*^{e_0}(\sum_i s_i^{p^{e_0}} g_i)$$

, and so

$$F_* r = F_*(\sum_i s_i^{p^{e_0}} g_i) = \sum_i s_i^{p^{e_0-1}} F_*(g_i).$$

That lets us decrease the exponent.

Now let $F_(g_1), \dots, F_*g_t$ be a generating set for F_*R. Then we claim that $\{F_*^e(g_1^{a_1} \cdots g_t^{a_t} \mid 0 \le a_i \le p^{e-1}\}$ is a generating set. Proceed by induction. Base case $e = 1$ clear. Assume for e, try to prove for $e + 1$.

[1] essentially of finite type = a localization of something of finite type

For any $r \in R$, use the IH to write

$$F_*^{e+1} r = F_*(F_*^e r) = F_* \left(\sum_i s_i F_*^e (\prod_i g_i^{a_i}) \right) = \sum_i F_*(s_i) F_*^{e+1} (\prod_i g_i^{a_i})$$

and now use the base case to expand each s_i, so

$$F_*^{e+1} r = \sum_i \sum_j u_{ij} F_*(g_j) F_*^{e+1} (\prod_i g_i^{a_i}) = \sum_{ij} u_{ij} F_*^{e+1} (g_j^{p^e} F_*^{e+1} (\prod_i g_i^{a_i}).$$

Now recombining, the exponent on each individual g_i is of the form $p^e + a_i < p^e + p^{e-1} < p^{e+1}$.

(4) Let $R = \mathbb{F}_2[x^2, x^3]$. Prove that R is *not* F-split.[2][3]

Solution: Consider any map $\varphi : F_* R \to R$. This map must send

$$\varphi(F_* x^6) = \varphi(x^3 F_* 1) = x^3 \varphi(F_* 1).$$

On the other hand, we can also write this as

$$\varphi(F_* x^6) = \varphi(x^2 F_* x^2) = x^2 \varphi(F_* x^2).$$

If $\varphi(F_* 1) = 1$, this would then force $x^3 = x^2 \varphi(F_* x^2)$. But x^3 is not divisible by x^2 in R, so this is a contradiction. Thus $\varphi(F_* 1) \neq 1$ for any possible map.

[2]Hint: You are welcome to use the generators & relations for $F_* R$ we found in class, no need to reprove!

[3]Note: This problem is definitely doable by hand using what we've learned as of 1/22, but you are also welcome to use any other methods for testing F-splitting that we learn in-class between now and when this HW is due.