Math 615: Lecture of February 19, 2007

If R is a ring of prime characteristic p we write $F_R : R \to R$ for the *Frobenius endomorphism*: $F_R(r) = r^p$. If $e \in \mathbb{N}$, we write F_R^e for the composition of F_R with itself e times, the iterated Frobenius endomorphism. Thus, $F_R^e(r) = r^{p^e}$. The subscript $_R$ is often omitted.

Quite generally, if R is a regular Noetherian ring, $F^e : R \to R$ is faithfully flat. We shall not prove this fact in general at this point, but we do want to prove that when R is a polynomial ring over a field K, $F^e : R \to R$ makes the right hand copy of R into a free R-module over the left hand copy of R. Note that F^e is an injective homomorphism, since the polynomial ring has no nonzero nilpotents. The image of R under this map is $R^q = \{r^q : r \in R\}$, where $q = p^e$.

We first note the following:

Lemma. *If T is free as S-algebra and S is free as an R-algebra, then T is free as an R-algebra. In fact, if $\{t_j\}_{j\in\mathcal{J}}$ is a free basis for T over S and $\{s_i\}_{i\,\in\mathcal{I}}$ is a free basis for S over R then the set of products $\{t_j s_i : j \in \mathcal{J},\, i \in \mathcal{I}\}$ is a free basis for T over R.*

Proof. If $t \in T$, we can write $t = \sum_{k=1}^n u_k t_{j_k}$, where the $u_k \in S$, and then we may express every u_k as an R-linear combination of finitely many of the elemnts s_i. It follows that the specified products span. If some R-linear combination of the products is 0, we may enlarge the set so that it consists of elements $s_{i_h} t_{j_k}$ for $1 \leq h \leq m$ and $1 \leq k \leq n$. If

$$\sum_{1\leq h\leq m, 1\leq k\leq n} r_{hk} s_{i_h} t_{j_k} = 0$$

where the $r_{hk} \in R$. We can write this as

$$\sum_{k=1}^{n} (\sum_{h=1}^{m} r_{hk} s_{i_h}) t_{j_k} = 0,$$

from which we first conclude that every $\sum_{h=1}^m r_{hk} s_{i_h} = 0$ and then that every $r_{hk} = 0$. $\square$

Proposition. *If B is a free A-algebra, $x_1, \ldots, x_n$ are indeterminates, and $k_1, \ldots, k_n$ are positive integers, then $B[x_1, \ldots, x_n]$ is free over $A[x_1^{k_1}, \ldots, x_n^{k_n}]$.*

Proof. By a straightforward induction, this reduces at once to the case where $n = 1$. We let $x = x_1$ and $k = k_1$. Then $B[x] \cong A[x] \otimes_A B$ is free over $A[x]$. By the preceding Lemma, it suffices to show that $A[x]$ is free over $A[x^k]$. But it is quite easy to verify that the elements x^a for $0 \leq x \leq a - 1$ are a free basis. $\square$

Theorem. *Let K be field and let $R = K[x_1, \dots, x_n]$ be a polynomial ring over K. Then $F_R^e : R \to R$ makes the right hand copy of R into a free module over the left hand copy of R.*

Proof. The image of R under F^e is $R^q = K^q[x_1^q, \dots, x_n^q]$. It suffices to show that R is free over R^q. Note that since K^q is a field, K is free over K^q. The result is now immediate from the preceding Proposition. $\square$