If \( I \subseteq J \) and \( J \) is integral over \( I \), we call \( I \) a \textit{reduction} of \( J \). With this terminology, we have shown that if \((R, m, K)\) is local with \( K \) infinite, every ideal \( I \subseteq m \) has a reduction with \( \operatorname{an}(I) \) generators, and one cannot do better than this whether \( K \) is infinite or not.

We have previously defined analytic spread for ideals of local rings. We can give a global definition as follows: if \( R \) is Noetherian and \( I \) is any ideal of \( R \), let

\[
\operatorname{an}(I) = \sup \{ P \in \operatorname{Spec}(R) : \operatorname{an}(IR_P) \},
\]

which is bounded by the the number of generators of \( I \) and also by the dimension of \( R \).

The Briançon-Skoda theorem then gives at once:

\textbf{Theorem.} \textit{Let} \( R \) \textit{be regular and} \( I \) \textit{an ideal. Let} \( n = \operatorname{an}(I) \). \textit{Then for all} \( k \geq 1 \), \( T^{n+k-1} \subseteq I^k \).

\textit{Proof.} If the two are not equal, this can be preserved while passing to a local ring of \( R \). Thus, without loss of generality, we may assume that \( R \) is local. The result is unaffected by replacing \( R \) by \( R(t) \), if necessary. Thus, we may assume that the residue class field of \( R \) is infinite. Then \( I \) has a reduction \( I_0 \) with \( n \) generators. From the form of the Briançon-Skoda theorem that we have already proved, we have that \( T^{n+k-1} = T_0^{n+k} \subseteq I_0^k \subseteq I \).

The intersection of all ideals \( I_0 \) in \( I \) such that \( I \) is integral over \( I_0 \) is called the \textit{core} of \( I \). It is not immediately clear that the core is nonzero, but we have:

\textbf{Theorem.} \textit{Let} \( R \) \textit{be regular local with infinite residue class field, and let} \( I \) \textit{be a proper ideal with} \( \operatorname{an}(I) = n \). \textit{Then the core of} \( I \) \textit{contains} \( T^n \).

\textit{Proof.} If \( I \) is integral over \( I_0 \) then they have the same analytic spread, and \( I_0 \) has a reduction \( I_1 \) with \( n \) generators. Then \( T^n = T_0^n \subseteq I_1 \subseteq I_0 \), and so \( T^n \) is contained in all such \( I_0 \).

We next want to give a proof of the Briançon-Skoda theorem in characteristic \( p \) that is, in many ways, much simpler than the proof we have just given. The characteristic \( p \) result can be used to prove the equal characteristic 0 case as well.

Recall that when \( x_1, \ldots, x_d \) is a regular sequence on \( M \), we require not only that \( x_i \) is a nonzerodivisor on \( M/(x_1, \ldots, x_{i-1})M \) for \( 1 \leq i \leq d \), but also that \((x_1, \ldots, x_d)M \neq M \). If \( (x_1, \ldots, x_d) \) has radical \( m \) in the local ring \((R, m, K)\), this is equivalent to the assertion \( mM \neq M \), for otherwise we get that \( m^tM = M \) for all \( t \), and for large \( t \), \( m^t \subseteq (x_1, \ldots, x_d) \).

Note that when \( x_1, \ldots, x_d \) is a regular sequence in a ring \( R \) and \( M \) is flat, we continue to have that \( x_i \) is a nonzerodivisor on \( M/(x_1, \ldots, x_{i-1})M \) for \( 1 \leq i \leq d \) (by induction on...
d this reduces to the case where \( d = 1 \) and the fact that \( x = x_1 \) is a nonzerodivisor on \( R \) give an exact sequence

\[
0 \rightarrow R \xrightarrow{x} R
\]

which stays exact when we tensor with \( M \) over \( R \). If \( M \) is faithfully flat, every regular sequence in \( R \) is a regular sequence on \( M \). If \( R \) is regular, this characterizes faithful flatness:

**Lemma.** Let \((R,m,K)\) be local. Then \( M \) is faithfully flat over \( R \) if and only if every regular sequence in \( R \) is a regular sequence on \( M \).

**Proof.** By the preceding discussion, we need only prove the “if” part. It will suffice to prove that for every \( R \)-module \( N \), \( \text{Tor}_R^i(N, M) = 0 \) for all \( i \geq 1 \). Since \( N \) is a direct limit of finitely generated modules, it suffices to prove this when \( N \) is finitely generated. We use reverse induction on \( i \). We have the result for \( i > \dim(R) \) because \( \dim(R) \) bounds the projective dimension of \( N \). We assume the result for \( i \geq k + 1 \), where \( k \geq 1 \), and prove it for \( i = k \). Since \( N \) has a filtration by prime cyclic modules, it suffices to prove the vanishing when \( N \) is a prime cyclic module \( R/P \). Let \( x_1, \ldots, x_d \) be a maximal regular sequence of \( R \) in \( P \). Then \( P \) is a minimal prime of \((x_1, \ldots, x_d)R \), and, in particular, an associated prime. It follows that we have a short exact sequence

\[
0 \rightarrow R/P \rightarrow R/(x_1, \ldots, x_d)R \rightarrow C \rightarrow 0
\]

for some module \( C \). By the long exact sequence for Tor, we have

\[
\cdots \rightarrow \text{Tor}_k^R(C, M) \rightarrow \text{Tor}_k^R(R/P, M) \rightarrow \text{Tor}_k^R(R/(x_1, \ldots, x_d)R, M) \rightarrow \cdots
\]

The leftmost term vanishes by the induction hypothesis and the rightmost term vanishes by problem 4 of Problem Set #3. \( \square \)

We write \( F \) or \( F_R \) for the Frobenius endomorphism of a ring \( R \) of positive prime characteristic \( p \). Thus \( F(r) = r^p \). We write \( F^e \) or \( F^e_R \) for the \( e \)th iterate of \( F \) under composition. Thus, \( F^e(r) = r^{p^e} \).

**Corollary.** Let \( R \) be a regular Noetherian ring of positive prime characteristic \( p \). Then \( F^e : R \rightarrow R \) is faithfully flat.

**Proof.** The issue is local on primes \( P \) of the first (left hand) copy of \( R \). But when we localize at \( R - P \) in the first copy, we find that for each element \( u \in R - P \), \( u^{p^e} \) is invertible, and this means that \( u \) is invertible. Thus, when we localize we get \( F^e : R_P \rightarrow R_P \). Thus, it suffices to consider the local case. But if \( x_1, \ldots, x_d \) is a regular sequence in \( R_P \), it operates on the right hand copy as \( x_1^{p^e}, \ldots, x_d^{p^e} \), which is regular in \( R_P \). \( \square \)

If \( I, J \subseteq R \), we write \( I:_R J \) for \( \{ r \in R : rJ \subseteq I \} \), which is an ideal of \( R \).
Proposition. Let $I$ and $J$ be ideals of the ring $R$ such that $J$ is finitely generated. Let $S$ be a flat $R$-algebra. Then $(I:_R J)S = IS :_S JS$.

Proof. Note that if $\mathfrak{A} \subseteq R$, $\mathfrak{A} \otimes_R S$ injects into $S$, since $S$ is flat over $R$. But its image is $\mathfrak{A}S$. Thus, we may identify $\mathfrak{A} \otimes_R S$ with $\mathfrak{A}S$.

Let $J = (f_1, \ldots, f_h)R$. Then we have an exact sequence

$$0 \rightarrow I :_R J \rightarrow R \rightarrow (R/I)^{\oplus h}$$

where the rightmost map sends $r$ to the image of $(rf_1, \ldots, rf_h)$ in $(R/I)^{\oplus h}$. This remains exact when we tensor with $S$ over $R$, yielding an exact sequence:

$$0 \rightarrow (I :_R J)S \rightarrow S \rightarrow (S/IS)^{\oplus h}$$

where the rightmost map sends $s$ to the image of $(sf_1, \ldots, sf_h)$ in $(S/IS)^{\oplus h}$. The kernel of the rightmost map is $IS :_S JS$, and so $(I :_R J)S = IS :_S JS$. □

When $R$ has positive prime characteristic $p$, we frequently abbreviate $q = p^e$, and $I^{[q]}$ denotes the expansion of $I \subseteq R$ to $S = R$ where, however, the map $R \rightarrow R$ that gives the structural homomorphism of the algebra is $F^e$. Thus, $I^{[q]}$ is generated by the set of elements $\{i^q : i \in I\}$. Whenever we expand an ideal $I$, the images of generators for $I$ generate the expansion. In particular, note that if $I = (f_1, \ldots, f_n)R$, then $I^{[q]} = (f_1^q, \ldots, f_n^q)R$. Note that it is not true $I^{[q]}$ consists only of $q$ th powers of elements of $I$: one must take $R$-linear combinations of the $q$ th powers. Observe also that $I^{[q]} \subseteq I^q$, but that $I^q$ typically needs many more generators, namely all the monomials of degree $q$ in the generators involving two or more generators.

Corollary. Let $R$ be a regular ring and let $I$ and $J$ be any two ideals. Then $(I :_R J)^{[q]} = I^{[q]} :_R J^{[q]}$.

Proof. This is the special case of in which $S = R$ and the flat homomorphism is $F^e$. □

The following result is a criterion for membership in an ideal of a regular domain of characteristic $p > 0$ that is slightly weaker, a priori, than being an element of the ideal. This criterion turns out to be extraordinarily useful.

Theorem. Let $R$ be a regular domain and let $I \subseteq R$ be an ideal. Let $r \in R$ be any element. Let $c \in R - \{0\}$. Then $r \in I$ if and only if for all $e \geq 0$, $cr^{p^e} \in I^{[p^e]}$.

Proof. The necessity of the second condition is obvious. To prove sufficiency, suppose that there is a counterexample. Then $r$ satisfies the condition and is not in $I$, and we may localize at a prime in the support of $(I + rR)/I$. This give a counterexample in which $(R, m)$ is a regular local ring. Then $cr^{p^e} \in I^{[p^e]}$ for all $e \geq e_0$ implies that

$$c \in I^{[p^e]} :_R (xR)^{[p^e]} = (I :_R xR)^{[p^e]} \subseteq m^{[p^e]} \subseteq m^{p^e}$$
for all $e \geq e_0$, and so $c \in \bigcap_{e \geq e_0} m^{p^e}$. But this is 0, since the intersection of the powers of $m$ is 0 in any local ring, contradicting that $c \neq 0$. □

We can now give a characteristic $p$ proof of the Briançon-Skoda Theorem, which we restate:

**Theorem (Briançon-Skoda).** Let $R$ be a regular ring of positive prime characteristic $p$. Let $I$ be an ideal generated by $n$ elements. Then for every positive integer $k$, $I^{n+k-1} \subseteq I^k$.

**Proof.** If $n = 0$ then $I = (0)$ and there is nothing to prove. Assume $n \geq 1$. Suppose $u \in I^{n+k-1} - I^k$. Then we can preserve this while localizing at some prime ideal, and so we may assume that $R$ is a regular domain. By part (f) of the Theorem on the first page of the Lecture Notes of September 15, the fact that $u \in I^{n+k-1}$ implies that there is an element $c \in R - \{0\}$ such that $cu^N \in (I^{n+k-1})^N$ for all $N$. In particular, this is true when $N = q = p^e$, a power of the characteristic. Let $I = (f_1, \ldots, f_n)$. We shall show that $(I^{n+k-1})^q \subseteq (I^k)^q$. A typical generator of $(I^{n+k-1})^q$ has the form $f_1^{a_1} \cdots f_n^{a_n}$ where $\sum_{i=1}^n a_i = (n + k - 1)q$. For every $i$, $1 \leq i \leq n$, we can use the division algorithm to write $a_i = b_i q + r_i$, where $b_i \in \mathbb{N}$ and $0 \leq r_i \leq q - 1$. Then

$$(n + k - 1)q = \sum_{i=1}^n a_i = (\sum_{i=1}^n b_i)q + \sum_{i=1}^n r_i \leq (\sum_{i=1}^n b_i)q + n(q - 1)$$

which yields

$$(\sum_{i=1}^n b_i)q \geq (n + k - 1)q - nq + n = (k - 1)q + n$$

and so $\sum_{i=1}^n b_i \geq k - 1 + \frac{n}{q} > k - 1$, and this shows that $\sum_{i=1}^n b_i \geq k$, as required □