§7.31: COHEN-SEIDENBERG THEOREMS: PROOFS

LYING OVER: Let $R \subseteq S$ be an integral inclusion. Then the induced map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective. That is, for any prime $\mathfrak{p} \in \mathrm{Spec}(R)$, there is a prime $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \cap R = \mathfrak{p}$; i.e., a prime *lying over* $\mathfrak{p}$.

INCOMPARABILITY: Let $R \to S$ be integral (but not necessarily injective). Then for any $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathrm{Spec}(S)$ such that $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$, we have $\mathfrak{q}_1 \not\subseteq \mathfrak{q}_2$. That is, any two primes lying over the same prime are *incomparable*.

GOING UP: Let $R \to S$ be integral (but not necessarily injective). Then for any $\mathfrak{p} \subsetneq \mathfrak{P}$ in $\mathrm{Spec}(R)$ and $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \cap R = \mathfrak{p}$, there is some $\mathfrak{Q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \subseteq \mathfrak{Q}$ and $\mathfrak{Q} \cap R = \mathfrak{P}$.

GOING DOWN: Let $R \subseteq S$ be an integral inclusion of domains, and assume that R is normal. Then for any $\mathfrak{p} \subsetneq \mathfrak{P}$ in $\mathrm{Spec}(R)$ and $\mathfrak{Q} \in \mathrm{Spec}(S)$ such that $\mathfrak{Q} \cap R = \mathfrak{P}$, there is some $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \subseteq \mathfrak{Q}$ and $\mathfrak{q} \cap R = \mathfrak{p}$.

LEMMA: Let $R \subseteq S$ be an integral inclusion and I an ideal of R. Then any element of $s \in IS$ satisfies a monic equation over R of the form[1]

$$s^n + a_1 s^{n-1} + \cdots + a_n = 0 \qquad \text{with } a_i \in I \text{ for all } i.$$

(1) Proof of Lying Over from the Lemma: Let $R \subseteq S$ be an integral inclusion.
- **(a)** Use the Lemma to show that if $\mathfrak{p}$ is prime, then $\mathfrak{p}S \cap R = \mathfrak{p}$.
- **(b)** Show that $(R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$ is not the zero "ring".
- **(c)** Deduce[2] the Theorem.

- **(a)** Let $r \in \mathfrak{p}S \cap R$. By the Lemma, we have an equation of the form $r^n + a_1 r^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathfrak{p}$, so $r^n \in \mathfrak{p}$, and hence $r \in \mathfrak{p}$.
- **(b)** Since $\mathfrak{p}S \cap R = \mathfrak{p}$, we have $\mathfrak{p}S \cap (R \smallsetminus \mathfrak{p}) = \varnothing$ so this is a legitimate ring.
- **(c)** We have $\mathrm{Spec}((R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)) \leftrightarrow \{\mathfrak{q} \in \mathrm{Spec}(S) \mid \mathfrak{q} \supseteq \mathfrak{p}S \text{ and } \mathfrak{q} \cap R \subseteq \mathfrak{p}\}$. The condition on the RHS is equivalent to $\mathfrak{q} \cap R = \mathfrak{p}$. We have that $\mathrm{Spec}((R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)) \neq \varnothing$, so some prime contracts to $\mathfrak{p}$.

(2) Proof of Lemma: Let $R \subseteq S$ be an integral inclusion and I an ideal of R.
- **(a)** Show that if $s \in IS$, then there is a module-finite R-subalgebra of S, say T, such that $s \in IT$, so we can assume that S is module-finite.
- **(b)** Write $S = \sum_i Rs_i$ and $v = [s_1, \ldots, s_t]$. Show that there is some $t \times t$ matrix A with entries in I such that $rv = vA$.
- **(c)** Apply a TRICK and conclude the proof.

- **(a)** If $s = \sum a_i b_i$ with $a_i \in I$ and $b_i \in S$, take $T = R[b_1, \ldots, b_t]$.
- **(b)** We can write $rs_i = \sum_j a_{ij} s_j$ with $a_{ij} \in I$. This gives the matrix equation we seek.
- **(c)** By the eigenvector trick, we have $\det(A - r\mathbb{1})v = 0$. In particular, $\det(A - r\mathbb{1})S = 0$, so $\det(A - r\mathbb{1}) = 0$. Thinking of this as the evaluation of the polynomial expression

[1] In fact, one can take $a_i \in I^i$ for each i by the same proof, which is often useful.

[2] The old bijection $\mathrm{Spec}(W^{-1}(T/J)) \longleftrightarrow \{\mathfrak{q} \in \mathrm{Spec}(T) \mid \mathfrak{q} \cap W = \varnothing \text{ and } J \subseteq \mathfrak{q}\}$ may come in handy.

$\det(A - X\mathbb{1})$, this is monic in X and going modulo I this becomes $\pm X^n$, so all the lower terms are in I. Thus, it is the polynomial that we seek.

(3) Proof of Incomparability: Let $R \to S$ be integral.

(a) Explain[3] why the Theorem is true when R is a field.

(b) Let $\mathfrak{p}$ in $\mathrm{Spec}(R)$. Use the definition to explain why the map $R/\mathfrak{p} \to S/\mathfrak{p}S$ is integral, and why the map $(R \smallsetminus \mathfrak{p})^{-1}(R/\mathfrak{p}) \to (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$ is integral.

(c) Use the previous parts (plus an old bijection) to prove the Theorem.

(a) If K is a field then any prime of S contracts to 0. But given any prime $\mathfrak{q}$ of S, $S/\mathfrak{q}$ is a domain and $K \subseteq S/\mathfrak{q}$ is integral, so $S/\mathfrak{q}$ is a field. Thus every prime in S is maximal, and we are done.

(b) For any element of $S/\mathfrak{p}S$, an integral equation over R for a representative is an integral equation over $R/\mathfrak{p}$. Given s/w, one can take an integral equation for s and divide through by a suitable power of w to get an integral equation.

(c) The primes that contract to $\mathfrak{p}$ are in bijection with primes of $(R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$. But this is integral over the field $(R \smallsetminus \mathfrak{p})^{-1}(R/\mathfrak{p})$, where the primes are incomparable by part (a).

(4) Proof of Going Up: Show that $R/\mathfrak{p} \to S/\mathfrak{q}$ is an integral inclusion, apply Lying Over, and deduce the Theorem.

This is an inclusion since the kernel of $R \to S/\mathfrak{q}$ is $\mathfrak{q} \cap R = \mathfrak{p}$; it is integral, as an equation for a representative holds for an element of $S/\mathfrak{q}$. By Lying over, there is a prime of $S/\mathfrak{q}$ that contracts to $\mathfrak{P}/\mathfrak{p}$. We can write this prime as $\mathfrak{Q}/\mathfrak{q}$ for some $\mathfrak{Q} \supseteq \mathfrak{q}$. Then $\mathfrak{Q} \cap R$, which one checks directly is $\mathfrak{P}$.

(5) Proof of Going Down.

(a) Explain why it suffices to show that $(S \smallsetminus \mathfrak{Q})(R \smallsetminus \mathfrak{p}) \cap \mathfrak{p}S$ is empty.

(b) Let x be an element of the intersection. Show that[4] the minimal monic polynomial $f(x)$ of x over $\mathrm{Frac}(R)$ has all nonleading coefficients in $\mathfrak{p}$.

(c) Write $x = rs$ with $r \in R \smallsetminus \mathfrak{p}$ and $s \in S \smallsetminus \mathfrak{Q}$. Show that $g(s) = f(rs)/r^n$ is the minimal polynomial of s over $\mathrm{Frac}(R)$.

(d) Show that $g(s)$ has coefficients in R, and obtain a contradiction to the assumption that x was an element of the intersection.

(a) It will follow that there is a prime ideal $\mathfrak{q}$ containing $\mathfrak{p}S$ that does not intersect $(S \smallsetminus \mathfrak{Q})(R \smallsetminus \mathfrak{p})$; in particular it intersects neither. This means that $\mathfrak{q} \cap R \supseteq \mathfrak{p}$, and $\mathfrak{q} \subseteq \mathfrak{Q}$, and $\mathfrak{q} \cap R \subseteq \mathfrak{p}$, so $\mathfrak{q} \cap R = \mathfrak{p}$ and $\mathfrak{q} \subseteq \mathfrak{Q}$.

(b) First we check that $f(x)$ has coefficients in R. To do this, take an algebraic closure of $\mathrm{Frac}(R)$ and let $x = x_1, \ldots, x_t$ be the distinct roots of f. By definition, f divides a monic equation for x, so each x_i is integral over R. Then $T = R[x_1, \ldots, x_t]$ is integral over R. The coefficients of f lie in $T \cap \mathrm{Frac}(R)$, but this is R, since R is normal.

[3]Hint: Recall an old fact about integral extensions of domains...

[4]Hint: First show all the coefficients are in R. For this, note that every coefficient of the minimal polynomial is a polynomial expression of the roots of f in an algebraic closure of $\mathrm{Frac}(R)$.

Now consider the image of $f(X) \in R[X]$ modulo $\mathfrak{p}$. Since f divides an integral equation with coefficients in $\mathfrak{p}$, the image of f divides X^k in $R/\mathfrak{p}[X]$, so f itself must have all lower coefficients in $\mathfrak{p}$.

(c) If not, we would get a lower degree polynomial that x satisfies, contradicting that f is the minimal monic polynomial of x.

(d) This follows from the same argument as in part (b). Then each a_i/r^i is an element of R. But $r \notin \mathfrak{p}$ and $a_i \in \mathfrak{p}$ implies that each coefficient of g is in $\mathfrak{p}$, so $s \in \sqrt{\mathfrak{p}S} \subseteq \mathfrak{Q}$, a contradiction.

(6) (a) Show that if S is module-finite over R with t generators, then for every $\mathfrak{p} \in \mathrm{Spec}(R)$, at most t distinct primes of S contract to $\mathfrak{p}$.

(b) Give an example of an integral inclusion $R \subseteq S$ such that there are primes of R with arbitrarily many primes contracting to it.

(a) As in the proof of Incomparability, this reduces to the case where $R = K$ is a field. We claim that an integral extension of a field K that is a t-dimensional vector space has at most t maximal ideals. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be the maximal ideals of S. Since $\mathfrak{m}_i + \mathfrak{m}_j = S$ for each $i \neq j$, CRT applies, and $S/(\mathfrak{m}_1 \cdots \mathfrak{m}_s) \cong S/\mathfrak{m}_1 \times \cdots \times S/\mathfrak{m}_s$. The K-vector space dimension of the LHS is at most t, whereas the K-vectorspace dimension of the RHS is at least s, so $s \leq t$, as desired.

(b) One possibility is $R := \mathbb{C}[X_1, X_2^2, X_3^3, X_4^4, \ldots] \subseteq S := \mathbb{C}[X_1, X_2, X_3, X_4, \ldots]$. This is integrally generated, hence integral. Note that $(X_t^t - 1)$ in R is a prime ideal, and for each $j = 0 \ldots, t-1$, the prime $(X_t - e^{2\pi i j/t})$ of S contracts to it.