Worksheet: Primes Lying Over Primes

Throughout, $R \subseteq S$ is an extension of commutative rings with unity making S an R-algebra. Recall from the worksheet on localization of rings that the *radical* $\sqrt{I}$ of an ideal I of R is the ideal consisting of the elements $x \in R$ such that $x^n \in I$ for some $n \geq 1$.

Definition. Fix a prime ideal P of R. A prime ideal Q of S *lies over* P if it contracts to P in R, i.e., $Q \cap R = P$.

Theorem (Lying Over). *If $R \subseteq S$ is an integral extension, then the following hold.*

1. *If I is an ideal of R, then $I \subseteq IS \cap R \subseteq \sqrt{I}$.*
2. *The induced map $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ is surjective. That is, for every prime ideal P of R, there exists a prime ideal of S lying over P.*
3. *The inverse image of every prime ideal in $\operatorname{Spec}(R)$ under the map $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ consists of incomparable prime ideals of S. That is, if $Q \neq Q'$ are two prime ideals of S lying over the same prime ideal of R, then $Q \not\subseteq Q'$ and $Q' \not\subseteq Q$.*

1. **Warm-up.**
   (a) Characterize what it means for a prime ideal in S to lie over a prime ideal of R in terms of the induced map on prime spectra. Then verify that regardless of whether $R \subseteq S$ is integral, the two sentences in the statement of Lying over, Part 2 are equivalent.
   (b) Does Part 1 of the Lying over theorem hold for the extension $\mathbb{Z} \subseteq \mathbb{Q}$? What about Part 2?
   (c) Find all prime ideals of $\mathbb{Z}[i]$ lying over the prime ideal $\langle 2 \rangle$ of $\mathbb{Z}$, and the prime ideal $\langle 3 \rangle$ of $\mathbb{Z}$.
   (d) Let S be the ring of functions from some infinite set X to $R = \mathbb{Z}/2\mathbb{Z}$. Is $R \subseteq S$ integral? Find infinitely many mutually incomparable prime ideals of S lying over the zero ideal of R.

Lemma. *Suppose that $R \subseteq S$ is integral, and let I be an ideal of R. If an element $u \in S$ is in IS, the expansion of I to S, then u satisfies a monic polynomial with coefficients $r_i \in I$:*

$$u^n + r_{n-1}u^{n-1} + \cdots + r_1 u + r_0 = 0.$$

2. **Proving the lemma.**
   (a) Is the conclusion of the lemma obvious when $I = R$? Briefly explain.
   (b) Write $u \in IS$ as $u = a_1 s_1 + \cdots + a_m s_m$ with all $a_i \in I$. If T denotes the subring $R[s_1, \cdots, s_m]$ of S, explain why $u \in IT$, and why T is module finite over R.

   Hint: Review the worksheet on integral extensions.
   (c) Let $t_1, \cdots, t_n$ be generators for T as an R-module (we can take the t_i to be monomials in $s_1, \cdots, s_m$). As in the Integral Extensions Worksheet, notice that we can assume that $t_1 = 1$. Then explain why we have equations of the form

$$ut_i = \sum_{j=1}^{n} b_{ij} t_j$$

with $b_{ij} \in I$ for each i and j.

Hint: Because u is in IT, an ideal of T, then so is ut_i. Hence we can express ut_i as a T-linear combination of elements of I. Rewrite each of the T-coefficients in this expression as an R-linear combination of $t_1, \cdots, t_n$ and gather terms.

(d) Use the determinant trick from our previous worksheet to construct the desired monic polynomial.

(e) Does the polynomial you constructed satisfy the stronger property that each coefficient $r_i \in I^{n-i}$? Aside: Look up the definition of the integral closure of an ideal, and compare it to this situation

3. **Proving the Lying Over theorem, Part 1.**

(a) Prove that $I \subseteq IS \cap R$. Does your argument use the assumption that S is integral over R?

(b) Prove that $IS \cap R \subseteq \sqrt{I}$.

Hint: Let $u \in IS \cap R$, and solve for the largest power of u in the monic polynomial with coefficients in I that you constructed above.

(c) We say that an ideal I of R is *radical* if $\sqrt{I} = I$. What does the Lying Over theorem, Part 1 say in this case? Prove that every prime ideal is radical.

4. **Proving the Lying Over theorem, Part 2.** For $P \in \operatorname{Spec}(R)$, we aim to find $Q \in \operatorname{Spec}(S)$ such that $Q \cap R = P$.

(a) Let $U = R \setminus P$. Explain why U is a multiplicatively closed subset of S, and then find $U \cap PS$.

Hint: Use the last part of your proof of Lying Over, Part 1.

(b) Conclude that $U^{-1}(PS)$, the expansion of PS to $U^{-1}S$, is a proper ideal of $U^{-1}S$. Thus, there exists a maximal ideal of $U^{-1}S$ containing $U^{-1}(PS)$. Explain why this maximal ideal is of the form $U^{-1}Q$ for some $Q \in \operatorname{Spec}(S)$ with $Q \cap U = \varnothing$. Then, prove that $Q \cap R = P$.

Hint: What does $Q \cap U = \varnothing$ say about a containment involving $Q \cap R$ and P? What does the containment $U^{-1}(PS) \subseteq U^{-1}Q$ say about a containment involving $Q \cap R$ and P?

Congratulations! You've just proven the most complicated part of the Lying Over theorem.

Lemma. *Suppose that $R \subseteq S$ is an integral extension of domains. Then for every nonzero element $s \in S$, there exists nonzero $s' \in S$ such that ss' (which is nonzero since S is a domain) is an element of R. In other words, every nonzero element of S has a nonzero multiple in R.*

5. **Proving the Lying Over theorem, Part 3.**

(a) Prove the above lemma.

Hint: Consider a monic equation with coefficients over R satisfied by s. Factor out the largest power of s that you can from this expression to get an expression of the form $s^m \cdot g = 0$. Conclude that $g = 0$. But what is the constant term of g?

(b) Prove that if S, and hence R, is a domain, then the only prime of S lying over the zero ideal in R is the zero ideal.

Hint: If $Q \in \operatorname{Spec}(S)$ lies over $\langle 0 \rangle \in \operatorname{Spec}(R)$, then take any purported nonzero element of Q, and apply the previous part of this problem to it.

(c) Prove that if $Q \in \mathrm{Spec}(S)$ lies over $P \in \mathrm{Spec}(R)$, then $R/P \to S/Q$ is still integral.

Hint: Convince yourself that $R/P \to S/Q$ is injective. What is its image? Once this is clear to you, this should be pretty obvious.

(d) Convince yourself that to prove Part 3 of Lying Over, it suffices to prove that if $Q \subseteq Q'$ are two primes in $\mathrm{Spec}(S)$ that lie over $P \in \mathrm{Spec}(R)$, then $Q = Q'$. Then, prove this.

Hint: Why must $R/P \hookrightarrow S/Q$ be an integral extension of domains? Why is $Q'/Q \in \mathrm{Spec}(S/Q)$? What does Q'/Q contract to under $R/P \hookrightarrow S/Q$? Once all of this is clear to you, apply an earlier part of this problem.