# Solutions 1

PRIME IDEALS, INTEGRAL EXTENSIONS, LOCALIZATION, NORMALIZATION

1. Let $A$ be a ring. Prove that a proper ideal $\mathfrak{p} \subsetneq A$ is a prime ideal if and only if for any ideals $\mathfrak{a}, \mathfrak{b} \subset A$ with $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ we have $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$.

   *Solution*: Assume that $\mathfrak{p}$ is a prime ideal, that is, for any $a, b \in A$ with $ab \in \mathfrak{p}$ we have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Consider ideals $\mathfrak{a}, \mathfrak{b} \subset A$ with $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$. If $\mathfrak{a} \not\subset \mathfrak{p}$ and $\mathfrak{b} \not\subset \mathfrak{p}$ we can choose elements $a \in \mathfrak{a} \smallsetminus \mathfrak{p}$ and $b \in \mathfrak{b} \smallsetminus \mathfrak{p}$. As $\mathfrak{p}$ is prime and $a, b \notin \mathfrak{p}$ we then also have $ab \notin \mathfrak{p}$. But this is a contradiction to $ab \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$. This proves the 'only if' part.

   Conversely suppose that for any ideals $\mathfrak{a}, \mathfrak{b} \subset A$ with $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ we have $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$. Then for any $a, b \in A$ with $ab \in \mathfrak{p}$ we have $(a)(b) = (ab) \subset \mathfrak{p}$ and therefore $(a) \subset \mathfrak{p}$ or $(b) \subset \mathfrak{p}$. But this means $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$; hence $\mathfrak{p}$ is a prime ideal. This proves the 'if' part.

2. Give an example of a ring extension $A \subset B$ and

   (a) prime ideals $\mathfrak{q} \subsetneq \mathfrak{q}' \subset B$ with $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$.

   (b) a prime ideal $\mathfrak{p} \subset A$ for which there exists no prime ideal $\mathfrak{q} \subset B$ with $\mathfrak{q} \cap A = \mathfrak{p}$.

   *Solution*:

   (a) For any field $K$ the prime ideals $(0) \subsetneq (X) \subset K[X]$ have the same intersection $(0)$ with the subring $K$.

   (b) The zero ideal is the only prime ideal of $\mathbb{Q}$, and its intersection with $\mathbb{Z}$ is again the zero ideal. Thus for any prime $p$ the prime ideal $(p) \subset \mathbb{Z}$ has the desired property.

3. Let $A \subset B$ be an integral ring extension. Show that $a \in A$ is a unit in $B$ if and only if it is a unit in $A$.

   *Solution*: If $a$ is a unit in $A$, it is also a unit in $B$. Conversely assume that $a$ is a unit in $B$, so that $ab = 1$ for an element $b \in B$. Since $b$ is integral over $A$, there then exist $a_1, \ldots, a_n \in A$ such that $b^n + \sum_{i=1}^n a_i b^{n-i} = 0$. Multiplying by $a^n$ we deduce that
   $$1 + \sum_{i=1}^n a^i a_i \;=\; (ab)^n + \sum_{i=1}^n a^i a_i (ab)^{n-i} \;=\; 0.$$
   Thus the element $a' := -\sum_{i=1}^n a^{i-1} a_i \in A$ satisfies $aa' = 1$; hence $a$ is a unit in $A$.

*Aliter:* Assume that $a$ is not a unit in $A$. Then $(a) \subset A$ is a proper ideal and thus contained in a maximal ideal $\mathfrak{p} \subset A$. Then $\mathfrak{p}$ is in particular a prime ideal, and so by the lying over theorem there exists a prime ideal $\mathfrak{q} \subset B$ with $\mathfrak{q} \cap A = \mathfrak{p}$. As $a \in \mathfrak{p}$, this implies $a \in \mathfrak{q}$. But since $a$ is a unit in $B$, it cannot lie in the prime ideal $\mathfrak{q}$; contradiction.

4. Let $A$ be an integral domain and let $S \subset A \smallsetminus \{0\}$ be a multiplicative subset. Prove that the ring extension $A \subset S^{-1}A$ is integral if and only if $S \subset A^\times$.

   *Solution*: If $S \subset A^\times$, any element $\frac{a}{s} \in S^{-1}A$ already lies in $A$ and is therefore integral over $A$. This proves the 'if' part.

   Conversely observe that any $s \in S$ satisfies $s \cdot \frac{1}{s} = 1$ in $S^{-1}A$ and is therefore a unit in $S^{-1}A$. Thus if the extension $A \subset S^{-1}A$ is integral, the above Exercise 3 implies that $s$ is a unit in $A$. This proves the 'only if' part.

*5. Let $A$ be an integral domain and let $S \subset A \smallsetminus \{0\}$ be a multiplicative subset. Show that $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ induces a bijection from the set of prime ideals $\mathfrak{q} \subset S^{-1}A$ to the set of prime ideals $\mathfrak{p} \subset A$ satisfying $S \cap \mathfrak{p} = \varnothing$.

   (*Hint:* Show that the inverse map is given by $\mathfrak{p} \mapsto S^{-1}\mathfrak{p} := \big\{\frac{a}{s} \bigm| a \in \mathfrak{p},\ s \in S\big\}$.)

   *Solution*: We already know that the map sends prime ideals to prime ideals. Moreover, as any element of $S$ is a unit in $S^{-1}A$ and a prime ideal does not contain any unit, the prime ideal $\mathfrak{q} \cap A$ satisfies $S \cap (\mathfrak{q} \cap A) = \varnothing$.

   Conversely for any prime ideal $\mathfrak{p} \subset A$ we set

$$S^{-1}\mathfrak{p} := \Big\{\tfrac{a}{s} \Bigm| a \in \mathfrak{p},\ s \in S\Big\}.$$

   One easily shows that this is an ideal of $S^{-1}A$. Moreover it contains 1 if and only if there exists $s \in S$ with $1 = \frac{s}{s} \in S^{-1}\mathfrak{p}$, that is, with $s \in S \cap \mathfrak{p}$. In other words $S^{-1}\mathfrak{p}$ is a proper ideal if and only if $S \cap \mathfrak{p} = \varnothing$. In that case consider any $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$ with $\frac{ab}{st} \in S^{-1}\mathfrak{p}$. Then we have $\frac{ab}{st} = \frac{c}{u}$ for some $c \in \mathfrak{p}$ and $u \in S$. Thus $abu = stc \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this implies that one of $a, b, u$ lies in $\mathfrak{p}$. Since $S \cap \mathfrak{p} = \varnothing$ we already know that $u \notin \mathfrak{p}$, so one of $a, b$ lies in $\mathfrak{p}$. This now implies that one of $\frac{a}{s}, \frac{b}{t}$ lies in $S^{-1}\mathfrak{p}$. Together this shows that $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$ for any prime ideal $\mathfrak{p} \subset A$ with $S \cap \mathfrak{p} = \varnothing$.

   We have thus constructed well-defined maps in both directions, and it remains to show that they are mutually inverse.

   For this consider first a prime ideal $\mathfrak{q} \subset S^{-1}A$. Then for any $a \in \mathfrak{q} \cap A$ and any $s \in S$ we have $\frac{a}{s} = \frac{1}{s} \cdot a \in \mathfrak{q}$. This proves that $S^{-1}(\mathfrak{q} \cap A) \subset \mathfrak{q}$. Conversely consider any $a \in A$ and $s \in S$ with $\frac{a}{s} \in \mathfrak{q}$. Then $a = s \cdot \frac{a}{s} \in \mathfrak{q} \cap A$ and therefore $\frac{a}{s} \in S^{-1}(\mathfrak{q} \cap A)$. This proves that $\mathfrak{q} \subset S^{-1}(\mathfrak{q} \cap A)$. Together this shows that $S^{-1}(\mathfrak{q} \cap A) = \mathfrak{q}$.

   Finally consider a prime ideal $\mathfrak{p} \subset A$ satisfying $S \cap \mathfrak{p} = \varnothing$. Then for any $a \in \mathfrak{p}$ we have $a = \frac{a}{1} \in S^{-1}\mathfrak{p} \cap A$, proving that $\mathfrak{p} \subset S^{-1}\mathfrak{p} \cap A$. Conversely consider any $a \in \mathfrak{p}$

and $s \in S$ such that $b := \frac{a}{s} \in A$. Then $bs = a \in \mathfrak{p}$, and since $\mathfrak{p}$ is a prime ideal with $S \cap \mathfrak{p} = \varnothing$ we must have $b \in \mathfrak{p}$. This proves that $S^{-1}\mathfrak{p} \cap A \subset \mathfrak{p}$. Together this shows that $S^{-1}\mathfrak{p} \cap A = \mathfrak{p}$, as desired.

*6. Consider an integral domain $A$ and an element $s \in A \smallsetminus \{0\}$. Show that for the multiplicative subset $S := \{s^n \mid n \geqslant 0\}$ we have

$$S^{-1}A \;\cong\; A[X]/(sX-1).$$

*Solution*: Consider the evaluation homomorphism

$$\varphi\colon A[X] \to S^{-1}A, \quad f \mapsto f(\tfrac{1}{s}).$$

Every element of $S^{-1}A$ has the form $\frac{a}{s^n}$ for some $a \in A$ and $n \geqslant 0$ and is therefore equal to $\varphi(aX^n)$, so $\varphi$ is surjective. By the fundamental homomorphism theorem $\varphi$ thus induces an isomorphism $A[X]/\ker(\varphi) \cong S^{-1}A$. It therefore remains to show that $\ker(\varphi) = (sX-1)$.

For this we first observe that $\varphi(sX-1) = \frac{s}{s} - 1 = 0$ and hence $(sX-1) \subset \ker(\varphi)$. For the reverse inclusion set $K := \mathrm{Quot}(A)$ and consider any $f \in \ker(\varphi)$. Then $f(s^{-1}) = 0$; hence $f$ is divisible by $X - \frac{1}{s}$ in $K[X]$. Thus there exists $g \in K[X]$ with $f = (sX-1)\cdot g$. Writing out $g = \sum_{i\geqslant 0} g_i X^i$ with $g_i \in K$ we thus have

$$f \;=\; (sX-1)\cdot g \;=\; \sum_{i\geqslant 1}(sg_{i-1} - g_i)X^i - g_0$$

with all coefficients in $A$. Thus we find that $g_0 \in A$, and since $sg_{i-1} - g_i \in A$ and $s \in A$ we deduce by induction that $g_i \in A$ for all $i \geqslant 0$. Thus $g \in A[X]$, and so $f$ lies in the ideal $(sX-1)$. We therefore have $\ker(\varphi) \subset (sX-1)$, as desired.

7. Let $L := k(t)$ be the field of rational functions in one variable over a field $k$, and let $K := k(s)$ be the subfield generated over $k$ by $s := t + t^{-1}$. Determine the integral closure $B$ of $A := k[s]$ in $L$.

*Solution*: The field extension $L/K$ has degree 2 with the generator $t$, and it is galois with the non-trivial galois automorphism $t \mapsto t^{-1}$. Also the equation $t^2 - st + 1 = 0$ shows that $t \in B$. Thus we also have $t^{-1} \in B$ and therefore $k[t^{\pm 1}] \subset B$. Since $k[s] = k[t + t^{-1}]$ is contained in $k[t^{\pm 1}]$, and $L$ is the quotient field of $k[t^{\pm 1}]$, it follows that $B$ is the normalization of $k[t^{\pm 1}]$. Now observe that $k[t]$ is a factorial ring and therefore normal. As a localization of $k[t]$ the ring $k[t^{\pm 1}]$ is thus normal as well. Therefore $B = k[t^{\pm 1}]$, and we are done.

*Aliter:* The field extension $L/K$ has degree 2 with the basis $1, t$, and it is galois with the non-trivial galois automorphism $t \mapsto t^{-1}$. Also the equation $t^2 - st + 1 = 0$ shows that $t \in B$ and hence $A + At \subset B$.

Consider an arbitrary element $f = g + ht \in L$ with $g, h \in K$. By Proposition 1.5.2 of the lecture this element lies in $B$ if and only if its minimal polynomial over $K$ has coefficients in $A$. If $h = 0$, this minimal polynomial is $X - g$, hence the condition is $f = g \in A$; so we do not get any new elements. If $h \neq 0$, the minimal polynomial is $(X - f)(X - \bar{f}) = X^2 - (f + \bar{f})X + f\bar{f}$ with $\bar{f} = g + ht^{-1}$. Thus $f \in B$ if and only if the elements

$$\begin{aligned} f + \bar{f} &= (g + ht) + (g + ht^{-1}) &= 2g + hs, \\ f\bar{f} &= (g + ht) \cdot (g + ht^{-1}) &= g^2 + ghs + h^2 \end{aligned} \qquad (*)$$

both lie in $A$.

*Case 1:* Suppose that $k$ has characteristic 2. Then the first condition is simply $hs \in A$. Multiplying the second equation by $s^2$ we find that another necessary condition is that $w := (gs)^2 + (gs)hs^2 + h^2s^2 \in A$. In that case $gs$ is a zero of the monic polynomial $X^2 + Xhs^2 + h^2s^2 - w \in A[X]$. Thus $gs \in K$ must be integral over $A$. As $A = k[s]$ is a unique factorization domain, this means that $gs \in A$. Together this shows that a necessary condition is $h, g \in A\frac{1}{s}$.

Now recall that we already know that $g + ht \in A$ for all $g, h \in A$. Thus it suffices to test the conditions for suitable representatives of all residue classes in $A\frac{1}{s}/A$. Since $A = k[s]$ we can therefore reduce ourselves to the case that $g = \frac{\alpha}{s}$ and $\beta = \frac{\beta}{s}$ with $\alpha, \beta \in k$. In that case the second element in $(*)$ is

$$f\bar{f} \;=\; g^2 + ghs + h^2 \;=\; \tfrac{\alpha^2}{s^2} + \tfrac{\alpha\beta}{s} + \tfrac{\beta^2}{s^2}.$$

Comparing coefficients this lies in $A$ if and only if $\alpha\beta = \alpha^2 + \beta^2 = 0$. But this is equivalent to $\alpha = \beta = 0$. This shows that $B = A + At$.

*Case 2:* Suppose that $k$ has characteristic $\neq 2$. Then $2 \in k^\times$, and by adding to $f$ a suitable element of $A$ we can achieve that $2g + hs = 0$. As the integrality condition does not change under this modification, it suffices to continue the computation under the assumption $2g + hs = 0$. Multiplying the second equation in $(*)$ by $4 \in k^\times$ the condition is then equivalent to

$$4g^2 + 4ghs + 4h^2 \;=\; h^2s^2 - 2hshs + 4h^2 \;=\; (4 - s^2)h^2 \;\in\; A.$$

Now observe that $2 \neq -2$ in $k$ implies that $4 - s^2 = (2 - s)(2 + s)$ is the product of two inequivalent primes in $A = k[s]$. By unique factorization it thus follows that $(4 - s^2)h^2 \in A$ if and only $h \in A$. Thus again we have found no new elements of $B$; hence $B = A + At$.

Finally, recall that $B$ is already a subring. In both cases we therefore find that

$$B \;=\; A + At \;=\; A[t] \;=\; k[t + \tfrac{1}{t}, t] \;=\; k[t^{\pm 1}].$$