Math 250A
Solutions to Homework 5

(II.1) Write Σ for the set of ideals of A which do not intersect S. We know that $\mathfrak{p}$ is a maximal element in this set. Suppose $\mathfrak{p}$ is not prime, so that we can find $x, y \in A - \mathfrak{p}$, $xy \in \mathfrak{p}$. Since $x \in A - \mathfrak{p}$, the ideal $\mathfrak{p} + Ax$ properly contains $\mathfrak{p}$. But $\mathfrak{p}$ is a maximal element in Σ. So $\mathfrak{p} + Ax \notin \Sigma$, which means $S \cap (\mathfrak{p} + Ax) \neq \emptyset$. Thus, there exist elements $r \in \mathfrak{p}$, $s \in A$ such that $r + sx \in S$. Similarly, $S \cap (\mathfrak{p} + Ay) \neq \emptyset$ so there exist elements $r' \in \mathfrak{p}$, $s' \in A$ such that $r' + s'y \in S$. So the product

$$ss' = (r + sx)(r' + s'y) = rr' + rs'y + r'sx + ss'xy \in S.$$

But $xy, r, r' \in \mathfrak{p}$. Hence, $ss' \in S \cap \mathfrak{p}$, which contradicts the assumption that $\mathfrak{p} \in \Sigma$. Thus $\mathfrak{p}$ must be prime.

(II.2) We first note that a commutative ring $R \neq 0$ is local iff the set of nonunits of R form an ideal. For $\Rightarrow$, suppose R is local with maximal ideal $\mathfrak{m}$. If $x \in R$ is not a unit, then $(x) \subsetneq R$ is a proper ideal and so must be contained in the maximal ideal $\mathfrak{m}$. For $\Leftarrow$, let $\mathfrak{a}$ be the ideal of nonunits of R. Then any proper ideal $\mathfrak{b} \subsetneq R$ cannot contain any units, and hence must be contained in $\mathfrak{a}$. This shows that $\mathfrak{a}$ is the unique maximal ideal of R.

Now let A be a local ring with maximal ideal $\mathfrak{m}$. Since $f : A \to A'$ is a surjective ring homomorphism, $f(\mathfrak{m})$ is an ideal of A' [*Indeed, if $r' \in A'$, we may pick $r \in A$ such that $f(r) = r'$. Then $r' f(\mathfrak{m}) = f(r\mathfrak{m}) \subseteq f(\mathfrak{m})$ and so $f(\mathfrak{m}) \subseteq A'$ is an ideal.*] If $s' \in A' - f(\mathfrak{m})$, then $s' = f(s)$ for some $s \in A$. Since $f(s) \notin f(\mathfrak{m})$, $s \notin \mathfrak{m}$ and so $s \in A$ is a unit. This shows that $s' = f(s) \in A'$ is a unit. By the above observation, we see that A' is a local ring.

(II.3) By the note in the first paragraph of (II.2), it suffices to show that $A_\mathfrak{p} - \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}$ consists of solely units of $A_\mathfrak{p}$. But this is clear: take any element of this set and write it in the form $\frac{r}{s} \in A_\mathfrak{p}$. Then $r \notin \mathfrak{p}$, $\notin \mathfrak{p}$. By definition of $A_\mathfrak{p}$, $\frac{s}{r}$ is also an element of $A_\mathfrak{p}$, and $\frac{r}{s} \cdot \frac{s}{r} = 1$. So we see that $A_\mathfrak{p}$ is local.

(II.4) First, let us prove a useful result.

Write $\phi : A \to S^{-1}A$ for the canonical map $a \mapsto \frac{a}{1}$. Now for any ideal $\mathfrak{b} \subseteq S^{-1}A$, the pullback $\phi^{-1}(\mathfrak{b})$ gives an ideal of A. On the other hand, for any ideal $\mathfrak{a} \subseteq A$, $S^{-1}\mathfrak{a}$ gives an ideal of $S^{-1}A$. We claim that composing gives $S^{-1}(\phi^{-1}(\mathfrak{b})) = \mathfrak{b}$. Indeed $\subseteq$ is easy: since for any $x \in \phi^{-1}(\mathfrak{b})$, we have $\frac{x}{1} \in \mathfrak{b}$ so that $\frac{x}{s} = \frac{1}{s} \cdot \frac{x}{1} \in \mathfrak{b}$ for any $s \in S$. Conversely for $\supseteq$, any element of $\mathfrak{b}$ can be written in the form $\frac{x}{s}$, $x \in A$, $s \in S$. Then $\frac{x}{1} = s \cdot \frac{x}{s} \in \mathfrak{b}$ and so $x \in \phi^{-1}(\mathfrak{b})$. Hence, $\frac{x}{s} = \frac{1}{s} \cdot x \in S^{-1}(\phi^{-1}(\mathfrak{b}))$.

Now to prove that $S^{-1}A$ is principal, let $\mathfrak{b} \subseteq S^{-1}A$ be an ideal. By the previous paragraph, $\mathfrak{b} = S^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq A$. Since A is principal, $\mathfrak{a} = A \cdot x$ for some $x \in A$. Then $\mathfrak{b} = S^{-1}\mathfrak{a} = S^{-1}A \cdot \frac{x}{1}$ is also principal.

(II.5) We first claim that for any ring A, the prime ideals of $S^{-1}A$ are in bijection with the prime ideals of A which do not intersect S, with the correspondence given in the first paragraph of (II.1). [*Note: by convention, prime ideals exclude the ring itself A.*]

We have already proven, in (II.1), that the correspondence takes ideals of $S^{-1}A$ back to itself (I'll leave to the reader to check that if $\mathfrak{p}$ is a prime not intersecting S, $S^{-1}\mathfrak{p}$ is prime too). Conversely, suppose $\mathfrak{p}$ is a prime ideal of A such that $\mathfrak{p} \cap S = \emptyset$. We have to show that $\phi^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$, where $\phi : A \to S^{-1}A$ is the canonical map $a \mapsto \frac{a}{1}$. Now $\supseteq$ is easy. For the reverse inclusion, suppose $a \in A$ such that $\phi(a) = \frac{a}{1} \in S^{-1}\mathfrak{p}$. We can write $\frac{a}{1} = \frac{a'}{s'}$ where $a' \in \mathfrak{p}$, $s' \in S$. Then there exists a $t \in S$ such that $t(as' - a') = 0$. Since $a' \in \mathfrak{p}$, $as't \in \mathfrak{p}$ as well. But $\mathfrak{p}$ is prime and $s't \in S$. Since S does not intersect $\mathfrak{p}$, we have $a \in \mathfrak{p}$.

Immediately this implies one direction of the second statement: if $p \in A$ is prime and $(p) \cap S = \emptyset$, then $\frac{p}{1}$

generates a prime ideal of $S^{-1}A$ and is hence prime.

Now we show $S^{-1}A$ is factorial. Let $\frac{a}{s} \in S^{-1}A$. Since A is factorial, we can factorize a as a product of prime elements (unique up to multiplication by units). Now for each such prime element p, consider its image $\frac{p}{1} \in S^{-1}A$. If $(p) \cap S = \emptyset$, $\frac{p}{1}$ is prime. Otherwise, $xp \in S$ for some multiple of p so $\frac{1}{p} = x \cdot \frac{1}{xp}$ lies in $S^{-1}A$ and $\frac{p}{1}$ is a unit. Collecting the units, we have written $\frac{a}{s}$ as a product of prime elements of $S^{-1}A$ of the form $\frac{p}{1}$.

Note: Such a product is unique. In fact in any entire ring A, if $x \in A - \{0\}$ can be written as a product of prime elements, then such an expression is unique, up to permutation of prime elements, and multiplication by units. Indeed, if $P = p_1 \dots p_r = q_1, \dots q_s$ for some prime elements p_i, q_j, then since $\prod p_i \in (q_1)$, one of the p_i must be in (q_1). Since (p_i) is a prime ideal, we in fact must have $(p_i) = (q_1)$ so that $p_i = uq_1$ for some unit u. Now we divide the left by p_i and the right by q_1 and do this iteratively.

Hence, every element of $S^{-1}A$ can be uniquely factorized as a product of a unit, and primes of the form $\frac{p}{1}$ (where $p \in A$ is prime and $(p) \cap S = \emptyset$). In particular, this also shows that the only prime elements of $S^{-1}A$ are of the form $\frac{p}{1}$ (up to multiplication by a unit).

(II.6) Recall that by definition $A' = A_{(p)}$ consists of all $\frac{a}{s}$, $a \in A$, $s \notin (p)$. By (II.5), we know that $A' = A_{(p)}$ is factorial. Furthermore, its unique maximal ideal is generated by $\frac{p}{1}$. Replacing A by A', we may assume that A is a factorial, local ring, with maximal ideal generated by some $p \in A$. We need to show it is principal.

Now A has no prime elements other than p (and up for a unit u). For if $x \in A - \{0\}$ is prime, then x is not a unit, so by the first paragraph of (II.2), $x \in (p)$. Since x is prime, $(x) = (p)$, so that $x = up$ for some unit u. Hence, every $x \in A - \{0\}$ can be uniquely written as up^r, for some unit u and $r \geq 0$. We call r the *valuation* of x, written as $v(x)$.

Let $\mathfrak{a} \subset A$ be a nonzero ideal, and $m = \min\{v(x) \mid x \in \mathfrak{a} - \{0\}\}$. So some $x \in \mathfrak{a}$ has valuation m, i.e. $x = up^m$ for some unit u. Then $(x) \subseteq \mathfrak{a}$. Conversely, for any $y \in \mathfrak{a} - \{0\}$, its valuation $n = v(y) \geq m$ so we can write $y = u'p^n$ for some unit u'. Hence $y = \frac{u'}{u} p^{n-m} x \in (x)$. So $\mathfrak{a}$ is indeed principal.

(II.7) We have $(a_1, a_2, \dots, a_n) = (d)$. We wish to show that d is a greatest common divisor of the a_i's, i.e. d divides each a_i; and if d' is any other element dividing each a_i, then $d' | d$. The first statement follows immediately: since $(a_i) \subseteq (a_1, \dots, a_n) = (d)$, $a_i \in (d)$ and hence a_i is a multiple of d for each i.

On the other hand, suppose d' divides a_i for each i. Then $a_i \in (d')$. Since $a_1, \dots, a_n \in (d')$, the ideal they generate $(a_1, \dots, a_n)$ lies in (d'). Hence $(d) \subseteq (d') \implies d \in (d')$, and hence d is a multiple of d'.