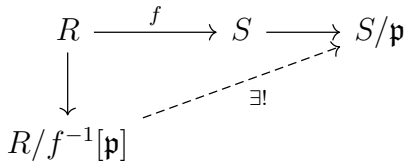
(1) There were two main approaches to this problem: supposing that $char(R)$ is composite and using its factorization to directly find some zero divisors, or using the map $\mathbb{Z} \longrightarrow R$ and proving that its kernel is prime from the fact that R is a domain (which is a special case of the fact that the preimage of a prime ideal is prime). These two approaches are essentially equivalent - they both effectively reduce the problem to determining when $\mathbb{Z}/n\mathbb{Z}$ is a domain, which can be understand via the arithmetic/ring theory of $\mathbb{Z}$. It's worth knowing how to do both - explicitly finding elements and computing, as well as abstractly playing with ideals (though personally, I'm partial to the latter, which I find more elegant).

(2) There weren't many errors, so I'll just present a way to think about pulling back prime ideals vs maximal ideals. Let $f : R \longrightarrow S$ and $\mathfrak{p} \subseteq S$ a prime ideal. Consider the composition

$$R \xrightarrow{f} S \longrightarrow S/\mathfrak{p}$$

The kernel of the map $R \longrightarrow S/\mathfrak{p}$ is exactly $f^{-1}[\mathfrak{p}]$. You can check this by manually testing elements, or by recalling how to take preimages of a composition. Anyway, by the first isomorphism theorem we therefore have an induced map



The map $R/f^{-1}[\mathfrak{p}] \longrightarrow S/\mathfrak{p}$ is an injective ring homomorphism. Now, as $\mathfrak{p}$ is prime we have that $S/\mathfrak{p}$ is a domain. Any subring of a domain is a domain, so $R/f^{-1}[\mathfrak{p}]$ is a domain, which means $f^{-1}[\mathfrak{p}]$ is a prime ideal of R.

This method also explains why the result is not necessarily true for maximal ideals. If $\mathfrak{p}$ was in fact maximal in S, then $S/\mathfrak{p}$ is a field, but subrings of fields needn't be fields. For instance, $\mathbb{Z} \subseteq \mathbb{Q}$. Hence, if we did the same argument for $\mathfrak{p}$ maximal, we'd end up showing that $R/f^{-1}[\mathfrak{p}]$ is (isomorphic to) a subring of a field, so we cannot conclude that it's a field, and hence we cannot conclude that $f^{-1}[\mathfrak{p}]$ is maximal, only prime.

(3) The main issue was in not showing well definition of addition and multiplication on $S^{-1}R$. Indeed, this means that if (r, s) (r', s') and (a, b) (a', b') that

$$\frac{r}{s} + \frac{a}{b} = \frac{r'}{s'} + \frac{a'}{b'}$$
$$\frac{r}{s}\frac{a}{b} = \frac{r'}{s'}\frac{a'}{b'}$$

I'd also like to mention another interesting way to construct this localization, which has the advantage of clearly being a ring with the right universal property, but the disadvantage of being harder to concretely write elements of. Indeed, let $S \subseteq R$ be a multiplicative subset. Then we define the ring

$$R[S^{-1}] = R[x_s : s \in S]/(x_s s - 1 : s \in S)$$

That is, we adjoin a formal variable x_s to R for every $s \in S$, and then induce the relation $x_s s = 1$ for all $s \in S$. Notice the notation here - we are formally adjoining inverses of elements

of S to R. This is similar to writing $R[\sqrt{2}]$, by which we mean formally adjoining a solution to the equation $x^2 - 2$ over R. This ring comes equipped with a map $\phi : R \longrightarrow R[S^{-1}]$ which send elements of S to units, as in $R[S^{-1}]$ we have $s^{-1} = x_s$.

We can also quickly verify the universal property for $R[S^{-1}]$. Indeed, let $\psi : R \longrightarrow T$ be a ring homomorphism sending elements of S to units in T. Then we define a map $\Phi : R[x_s : s \in S] \longrightarrow T$ via ψ on the coefficients and $x_s \mapsto \psi(s)^{-1}$ on the variables. Recall that this is all we need to do to define a map out of a polynomial ring. Notice that $\Phi(x_s s - 1) = \psi(s)^{-1}\psi(s) - 1 = 0$, so this map factors through the quotient

$$\begin{array}{ccc} R[x_s : s \in S] & \xrightarrow{\quad\Phi\quad} & T \\ \downarrow & \nearrow_{\exists!} & \\ R[x_s : s \in S]/(x_s s - 1 : s \in S) & & \end{array}$$

We let $\overline{\Phi}$ be the induced map $R[S^{-1}] \longrightarrow T$. Then we have a commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\psi} & T \\ \downarrow & \nearrow_{\overline{\Phi}} & \\ R[S^{-1}] & & \end{array}$$

and $\overline{\Phi}$ is unique with respect to this condition.

This sort of construction is very typical in algebra - adjoin indeterminates and mod out by relations. We saw this with group presentations as well, create a free group then mod out by whatever equations you wish to make true. In this way, algebra gives us the ability to make any equation we want true, so long as we are willing to change our domain. If we want a square root of 2 or -1, we can adjoin an indeterminate x and mod out by $x^2 - 2$ or $x^2 + 1$. If we want to invert 2, we adjoin an indeterminate x and mod out by $2x - 1$. And so on for whatever sort of algebraic equation you would like.

(4) There weren't many notable mistakes, other than not having enough detail. So I'll just talk about some stuff that's tangentially related.

First off, you can use this "universal property" to prove uniqueness of localization. That is, suppose there is a ring homomorphism $R \longrightarrow T$ sending S to units so that the universal property holds for this arrow, i.e. for all maps $R \longrightarrow R'$ sending S to units there is a unique map $T \longrightarrow R'$ so that the diagram commutes:

$$\begin{array}{ccc} R & \longrightarrow & T \\ & \searrow & \downarrow{\scriptstyle \exists!} \\ & & R' \end{array}$$

Then there's a unique isomorphism $S^{-1}R \longrightarrow T$ so that this diagram commutes:

$$\begin{array}{ccc} R & \longrightarrow & S^{-1}R \\ & \searrow & \downarrow \\ & & T \end{array}$$

This means that there is only one solution to the "localization problem", i.e. the most efficient way to force all the elements of S to be units. We can think of this categorically as describing the functor $R - \mathsf{Alg}(S^{-1}R, -)$.

Next, let's consider the map $\phi : R \longrightarrow S^{-1}R$. We will show that for any maps $f, g : S^{-1}R \longrightarrow T$ that if $f \circ \phi = g \circ \phi$ then $f = g$. In categorical terms, this means that ϕ is an epimorphism. Note that this is not how Prof. Elman uses the term! For him, "epimorphism" means surjective, but for category theorists, it's what I defined.

Anyways, here's the proof. We have by assumption that $f(r/1) = g(r/1)$ for all $r \in R$. Thus, for $s \in S$, we have $f(1/s) = f(s/1)^{-1}$ and $g(1/s) = g(s/1)^{-1}$. Hence,

$$\begin{aligned} f(r/s) &= f(r/1)f(1/s) \\ &= f(r/1)f(s/1)^{-1} \\ &= g(r/1)g(s/1)^{-1} \\ &= g(r/1)g(1/s) \\ &= g(r/s) \end{aligned}$$

so indeed, $f = g$.

Intuitively, if we know where R goes we know what happens to fractions. In a sense, this means R "generates" $S^{-1}R$.

For those who know topology, let Haus be the category of Hausdorff topological spaces with continuous maps. Then prove that a map $f : X \longrightarrow Y$ in Haus is epic in the sense of the above cancellation property ($g \circ f = h \circ f$ implies $g = h$) if and only if its image is dense. Note that in Top, epimorphisms are simply surjections.

This is also true in Set, that epimorphisms are precisely surjections. Furthermore, this holds in Group, but this is hard to prove. In Ab, epimorphisms are also precisely surjections, and this is easier than in Group.

(5) The main issue I saw was in defining things in terms of numerators and denominators. This is subtle, as fractions are equivalence classes, for instance $\frac{1}{2} = \frac{2}{4}$ so we have to be careful. For instance, many people wrote the maximal ideal of $R_{\mathfrak{p}}$ as

$$\left\{ \frac{a}{b} : a \in \mathfrak{p}, b \notin \mathfrak{p} \right\}$$

It's clear what this means, and it is correct, but I would have preferred writing it as $\mathfrak{p}R_{\mathfrak{p}}$, ie the ideal of $R_{\mathfrak{p}}$ generated by the image of $\mathfrak{p}$ under the map $R \longrightarrow R_{\mathfrak{p}}$. To be clear, it's not at all wrong to work with explicit fractions in localizations. In fact, this is very important, so all I mean to do is suggest being cautious.

Here's a fallacious argument, proving a false statement, which centers around using numerators and denominators like this.

Theorem 0.1. *Let R be a commutative ring and S a multiplicative subset. Let $\phi : R \longrightarrow S^{-1}R$ Then there is a bijection*

$$\{\textit{proper ideals of } R \textit{ disjoint from } S\} \cong \left\{\textit{proper ideals of } S^{-1}R\right\}$$

via

$$\begin{aligned} I &\mapsto S^{-1}I \\ \phi^{-1}[J] &\hookleftarrow J \end{aligned}$$

Proof. We first prove that $\phi^{-1}[S^{-1}I] = I$. $S^{-1}I$ consists of fractions of the form $\frac{a}{b}$ with $a \in I$ and $b \in S$. Now, $\phi : I \longrightarrow S^{-1}I$ so $I \subseteq \phi^{-1}[S^{-1}I]$. Conversely, let $a \in \phi^{-1}[S^{-1}I]$. Then $\frac{a}{1} \in S^{-1}I$. Hence, as $S^{-1}I$ consists of fractions with numerator in I, we have that $a \in I$. Furthermore, as $S \cap I = \emptyset$, no element of S can be a numerator in $S^{-1}I$, so $S^{-1}I$ contains no units and is hence proper.

On the other hand, we prove that $S^{-1}\phi^{-1}[J] = J$, where here $J \subseteq S^{-1}R$. Indeed, the inclusion $S^{-1}\phi^{-1}[J] \subseteq J$ is clear. On the other hand, let $\frac{a}{b} \in J$ with $b \in S$. Then $b\frac{a}{b}$ is in J, as it is an ideal, so $\frac{a}{1} \in J$. Hence, $a \in \phi^{-1}[J]$. Thus $\frac{a}{b} \in S^{-1}I$. Furthermore, if $S \cap \phi^{-1}[J]$ was nonempty, then an element of S would be a numerator in J, and hence J would be the unit ideal. □

But this result is false! For instance, consider $S = \{1, 2, 4, 8, 16, \dots\} \subseteq \mathbb{Z}$ and $I = 6\mathbb{Z}$. Then in $S^{-1}\mathbb{Z} = \mathbb{Z}[1/2]$, we have that $S^{-1}I = 3\mathbb{Z}[1/2]$. And indeed, $\phi^{-1}[3\mathbb{Z}[1/2]] = 3\mathbb{Z}$ which is not $6\mathbb{Z}$. Note that we can compute $\phi^{-1}[3\mathbb{Z}[1/2]]$ as $\mathbb{Z} \cap \mathbb{Z}[1/2]$ when we embed both rings into $\mathbb{Q}$.

By the way, the only false part here is when proving $I \supseteq \phi^{-1}[S^{-1}I]$ - the other inclusion is true, and the converse equality $S^{-1}\phi^{-1}J = J$ is also true. Proving this direction more carefully (ie using the equivalence relation) and see where you can use primality, as this bijection is true for prime ideals.

(6) Not much to say here. I read somewhere that the following stronger result is true (due to Jacobson).

Theorem 0.2. *Let R be a ring so that for all $a \in R$ there is a positive integer $n(a)$ such that $a^{n(a)} = a$. Then R is commutative.*

This problem is the special case where $n(a) = 3$ for all a. I have no idea how to prove this, and it sounds nightmarish.

(7) There weren't any issues here, so I'll just talk about proving $p \mid \binom{p}{i}$ for $0 < i < p$ and p prime. The typical method people used to prove this was recalling the formula

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

and observing that p divides the numerator but not the denominator.

This is a very nice and perfectly valid proof, but I want to present another method which I think is fun. Let X be the set of cardinality i subsets of $\{1, \dots, p\}$. We will explicitly break X as a disjont union of subsets of size p, which will prove that $|X|$ is divisible by p. Indeed, we do this by concocting a group action of $\mathbb{Z}/p\mathbb{Z}$ on X.

Consider the permutation $\sigma : \{1, \dots, p\} \longrightarrow \{1, \dots, p\}$ given in cycle notation as $(12 \dots p)$. We let $\mathbb{Z}/p\mathbb{Z}$ act on X via $\overline{k} * A = \sigma^k(A)$, for $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$ and $A \in X$. This in turn decomposes X as a disjoint union of orbits via $\mathbb{Z}/p\mathbb{Z}$. To determine the size of each orbit, we use the orbit-stabilizer theorem. So we must determine, for $A \in X$ what its stabilizer under $\mathbb{Z}/p\mathbb{Z}$ is.

Let's let G_A be the stabilizer of A under the $\mathbb{Z}/p\mathbb{Z}$ action. Then G_A is a subgroup of $\mathbb{Z}/p\mathbb{Z}$. As p is prime, $G_A = \mathbb{Z}/p\mathbb{Z}$ or $G_A = 0$. Suppose that $G_A = \mathbb{Z}/p\mathbb{Z}$. Then for all $\overline{k} \in \mathbb{Z}/pZ$, we have that $\sigma^k(A) = A$. We claim that A is then either empty or all of $\{1, \dots, p\}$. Indeed, suppose A is nonempty and $\sigma(A) = A$. Pick some $j \in A$. Then $\sigma^k(j) \in A$ for all k. And $\sigma^k(j)$ ranges over all elements of $\{1, \dots, p\}$ as $\overline{k}$ ranges over $\mathbb{Z}/p\mathbb{Z}$. Hence, A must contain all of $\{1, \dots, p\}$. We concldue that $G_A = \mathbb{Z}/p\mathbb{Z}$ if and only if $A = \emptyset$ or $A = \{1, \dots, p\}$, and otherwise $G_A = 0$.

In the case of interest, $|A| = i$ with $0 < i < p$, so the two cases where $G_A = \mathbb{Z}/p\mathbb{Z}$ are precisely the ones ruled out. Thus, for any $A \in X$ we have $G_A = 0$. The orbit stabilizer theorem says

$$[\mathbb{Z}/p\mathbb{Z} : G_A] = |\mathbb{Z}/p\mathbb{Z} * A|$$

And the left hand side is p, as $G_A = 0$, so the orbit of A has precisely p elements. We conclude then, by decomposing X into these orbits, that

$$|X| = p|X/(\mathbb{Z}/pZ)|$$

where $X/(\mathbb{Z}/p\mathbb{Z})$ is the set of orbits of this group action. This proves that $p||X|$ as desired.

I guess this proof is longer, but I find it easier to understand why $p|\binom{p}{i}$ for $0 < i < p$ using this method of explicitly grouping X into sets of size p. To me, this proof explains why primality is used and why the range $0 < i < p$ is used more than the direct computation. Generally, I find combinatorial proofs most elegant when the proof explains where the combinatorial meaning of why counting this type of object naturally looks like a sum or a product. Divisibility results like this often come from some implicit symmetry which is nice to make explicit. For example, you can try proving the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ using a group action and the orbit stabilizer theorem. That proof will also explain why the denominator actually divides the numerator. As a hint, consider an action of S_n on the set of subsets of $\{1, \ldots, n\}$ of size k. Another cute application of this sort of thinking is proving Fermat's little theorem with the orbit stabilizer theorem.