**Primes lying over/under** [recap/cont’d]

For $\mathcal{O}$ integral over $\mathfrak{o}$ and prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, there is at least one prime ideal $\mathfrak{P}$ of $\mathcal{O}$ such that $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$. $\mathfrak{P}$ is maximal if and only if $\mathfrak{p}$ is maximal. $\mathfrak{p} \cdot \mathcal{O} \neq \mathcal{O}$.

For $K/k$ finite Galois, the Galois group $G = \text{Gal}(K/k)$ is transitive on primes lying over $\mathfrak{p}$ in $\mathcal{O}$.

Generally, there are only finitely-many prime ideals lying over a given prime of $\mathfrak{o}$.

For maximal $\mathfrak{P}$ lying over $\mathfrak{p}$ in $\mathfrak{o}$, the decomposition group $G_{\mathfrak{P}}$ is the stabilizer of $\mathfrak{P}$. The decomposition field $K^\mathfrak{P}$ of $\mathfrak{P}$ is the subfield of $K$ fixed by $G_{\mathfrak{P}}$.

$\mathfrak{P}$ is the only prime of $\mathcal{O}$ lying above $\mathfrak{P} \cap K^\mathfrak{P}$.

*Next:* A less fussy/labor-intense version of localization...
Localization more generally: For non-integral-domains \( \mathfrak{o} \), collapsing can occur in localizations \( j : \mathfrak{o} \to \mathfrak{o}_p \).

Example: Localizing \( \mathfrak{o} = \mathbb{Z}/30 \) at the prime ideal \( \mathfrak{p} = 3 \cdot \mathbb{Z}/30 \) requires that \( 10 \notin \mathfrak{p} \) become a unit in the image \( j : \mathfrak{o} \to \mathfrak{o}_p \). Thus,

\[
j(3) = j(3) \cdot j(10) \cdot j(10)^{-1} = j(30) \cdot j(10)^{-1} = 0 \cdot j(10)^{-1}
\]

Thus (!) \( \mathfrak{o}_p = \mathbb{Z}/3 \), and \( \mathbb{Z}/30 \to \mathbb{Z}/3 \) is the quotient map. Generally, \( j : \mathfrak{o} \to \mathfrak{o}_p \) sends zero-divisors \( x \in \mathfrak{p} \) with \( xy = 0 \) for \( y \notin \mathfrak{p} \) to 0:

\[
0 = j(0) \cdot j(y)^{-1} = j(xy)j(y)^{-1} = j(x)j(y)j(y)^{-1} = j(x)
\]

This explains the more complicated equivalence relation in the more general proof-of-existence-by-construction of localization, via some sort of generalized fractions:
**Claim:** The localization $j : \mathfrak{o} \to \mathfrak{o}_p$ exists: it can be constructed as pairs $\{(a, b) : x \in \mathfrak{o}, \ b \not\in p\}$, identifying $(a, b), (a', b')$ when $c \cdot (ab' - a'b) = 0$ for some $c \in \mathfrak{o} - p$, with addition and multiplication as usual. Given $\varphi : \mathfrak{o} \to R$, the corresponding $\Phi : \mathfrak{o}_p \to R$ is $\Phi(\frac{a}{b}) = \varphi(a)\varphi(b)^{-1}$.

**Remark:** Now it becomes interesting so check that $\mathfrak{o}_p$ is not accidentally the degenerate ring $\{0\}$! This would use the hypothesis that no product of elements of $S = \mathfrak{o} - p$ is 0.

**Remark:** It would be reasonable to be impatient with, or even repelled by, the (tedious!) details involved in verification that things are well-defined, and that the construction really produces a ring, and that $\Phi$ is a ring homomorphism, etc.

What’s the alternative?
First, we may as well formulate the most general case:

For an arbitrary subset \( S \) (not just the complement of a prime ideal) of a commutative ring with identity \( \mathfrak{o} \), the localization \( j : \mathfrak{o} \to S^{-1}\mathfrak{o} \) can be characterized by a universal property: for any ring hom \( \varphi : \mathfrak{o} \to R \) with \( \varphi(S) \subset R^\times \), there is a unique \( \Phi \) giving a commutative diagram

\[
\begin{array}{ccc}
S^{-1}\mathfrak{o} & \xrightarrow{\exists \Phi} & R \\
\downarrow{i} & & \downarrow{} \\
\mathfrak{o} & \xrightarrow{\forall \varphi} & R
\end{array}
\]

Characterization by a universal property proves uniqueness..., when existence is proven, probably by a (hopefully graceful) construction.
Consider an expression as a quotient of a polynomial ring with indeterminates $x_s$ for all $s \in S$:

\[ S^{-1}\mathfrak{o} = \mathfrak{o}[\{x_s : s \in S\}] / \text{(ideal generated by } sx_s - 1, \forall s \in S) \]

with $j : \mathfrak{o} \rightarrow S^{-1}\mathfrak{o}$ induced by the inclusion $\mathfrak{o} \rightarrow \mathfrak{o}[\ldots, x_s, \ldots]$.

This produces a ring, for any $S \subset \mathfrak{o}$. Given $\varphi : \mathfrak{o} \rightarrow R$ with $\varphi(S) \subset R^\times$, the universal mapping properties of polynomial rings give a unique $\tilde{\varphi}$ extending $\varphi$ to the polynomial ring by

\[ \tilde{\varphi}(x_s) = \varphi(s)^{-1} \]

Then $\tilde{\varphi}$ factors uniquely through the quotient, since

\[ \tilde{\varphi}(sx_s - 1) = \varphi(s)\tilde{\varphi}(x_s) - \varphi(1) = 1 - 1 = 0 \]
The diagram of well-defined, uniquely-determined ring homs:

\[
\begin{array}{c}
\exists ! \text{quot} \\
\mathfrak{O}[\ldots, x_s, \ldots] \\
\downarrow \exists ! \tilde{\varphi} \\
\langle \ldots, sx_s - 1, \ldots \rangle \\
\downarrow \exists ! \Phi \\
0 \quad \rightarrow \\
\forall \varphi \rightarrow R
\end{array}
\]

with \( \tilde{\varphi} \) uniquely induced by \( \tilde{\varphi}(x_s) = \varphi(s)^{-1} \), and \( \Phi \) uniquely induced by \( \tilde{\varphi} \).

**What more is needed?** When the ring \( \mathfrak{O} \) has 0-divisors, it is not clear that there are any such rings \( R \) (with \( 0 \neq 1!!! \)) over which to quantify, and/or that \( S^{-1}\mathfrak{O} \) is not the trivial ring \{0\} with \( 0 = 1 \).

Indeed, if any product of elements of \( S \) is 0, \( S^{-1}\mathfrak{O} = \{0\} \), but the above construction seems to succeed without this hypothesis.
Claim: In $S^{-1}\mathfrak{o}$, $0 \neq 1$ if and only if no product of elements of $S$ is 0.

Proof: The degeneration $1 = 0$ in the quotient is equivalent to existence of an expression

$$\sum_{i=1}^{n} f_i(x_1, \ldots, x_n) \cdot (s_i x_i - 1) = 1 \in \mathfrak{o}[x_1, \ldots, x_n]$$

where $x_i = x_{s_i}$, for some finite subset $S_o = \{s_1, \ldots, s_n\}$ of $S$, where $f_i(x_1, \ldots, x_n)$ is a polynomial with coefficients in $\mathfrak{o}$.

One direction is easy: if $st = 0$ for $s, t \in S$, then in the quotient

$$S^{-1}\mathfrak{o} = \mathfrak{o}[x, y]/\langle sx - 1, ty - 1 \rangle$$

we compute

$$1 = 1 \cdot 1 = sx \cdot ty = st \cdot xy = 0 \cdot xy = 0 \quad (in \ S^{-1}\mathfrak{o})$$
That is, in \( o[x, y] \) itself,

\[
1 = (1 - sx + sx)(1 - ty + ty)
\]

\[
= (1 - sx)(1 - ty) + sx(1 - ty) + ty(1 - sx) + sxty
\]

\[
= (1 - sx)(1 - ty) + sx(1 - ty) + ty(1 - sx) + 0
\]

which is in the ideal generated by \( 1 - sx \) and \( 1 - ty \).

For the other direction, for \( S = \{s\} \) with a single element, a condition

\[
(c_\ell x^\ell + \ldots + c_1 x + c_o) \cdot (sx - 1) = 1
\]

gives \( c_o = -1 \) and \( c_k = -s^k \), and \( s^{\ell+1} = 0 \).
Inductively, suppose we have the claim for $|S| \leq n - 1$. Let $S = \{s_1, \ldots, s_n\}$, and suppose $S^{-1} \mathfrak{o} = \{0\}$.

From the mapping characterization, it is immediate that localization can be done stepwise: there is a natural isomorphism

$$(S_1 \cup S_2)^{-1} \mathfrak{o} \approx S_1^{-1} \left( S_2^{-1} \mathfrak{o} \right)$$

Let $\mathfrak{o}' = \{s_n\}^{-1} \mathfrak{o}$ and $S' = \{s_1, \ldots, s_{n-1}\}$. Then $0 = 1$ in $S'^{-1} \mathfrak{o}'$ implies that $s_1^{\ell_1} \ldots s_{n-1}^{\ell_{n-1}} = 0$ in $\mathfrak{o}'$, for some non-negative integer exponents. Since $\mathfrak{o}' = \mathfrak{o}[x]/\langle s_n x - 1 \rangle$, for some coefficients $c_i$

$$s_1^{\ell_1} \ldots s_{n-1}^{\ell_{n-1}} = (c_\ell x^\ell + \ldots + c_o)(s_n x - 1)$$

Then $c_o = -s_1^{\ell_1} \ldots s_{n-1}^{\ell_{n-1}}$, and $s_1^{\ell_1} \ldots s_{n-1}^{\ell_{n-1}} \cdot s_n^{\ell+1} = 0$. ///
Corresponding localization of modules and algebras:

Let \( i : \mathfrak{o} \to \mathfrak{o}_p \) be the localization.

For an \( \mathfrak{o} \)-module \( M \), it should not be surprising that the useful notion of localization of \( M \) creates an \( \mathfrak{o}_p \)-module \( M_p \) by

\[
M_p = \mathfrak{o}_p \otimes_\mathfrak{o} M
\]

Similarly, for a (commutative) \( \mathfrak{o} \)-algebra \( A \),

\[
A_p = \mathfrak{o}_p \otimes_\mathfrak{o} A
\]

Or, why not the other extension of scalars, \( M_p = \text{Hom}_\mathfrak{o}(\mathfrak{o}_p, M) \)?