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

**Theorem:** For $\mathfrak{O}$ *integral* over $\mathfrak{o}$ and prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, there is at least one prime ideal $\mathfrak{P}$ of $\mathfrak{O}$ such that $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$.

$\mathfrak{P}$ is said to *lie over* $\mathfrak{p}$. $\mathfrak{P}$ is maximal if and only if $\mathfrak{p}$ is maximal. $\mathfrak{p} \cdot \mathfrak{O} \neq \mathfrak{O}$. There a natural commutative diagram

$$\begin{array}{ccc} \mathfrak{O} & \longrightarrow & \mathfrak{O}/\mathfrak{P} \\ \uparrow & & \uparrow \\ \mathfrak{o} & \longrightarrow & \mathfrak{o}/\mathfrak{p} \end{array}$$

*Localization* of $\mathfrak{o}$ with respect to $S = \mathfrak{o} - \mathfrak{p}$ is extremely useful.

**Galois action on primes lying over** $\mathfrak{p}$, then recap and amplification of *localization*.

*Proof of theorem:* $S = \mathfrak{o} - \mathfrak{p}$ is *multiplicative* because $\mathfrak{p}$ is prime. $S^{-1}\mathfrak{O}$ is integral over $S^{-1}\mathfrak{o}$, and $S^{-1}\mathfrak{o}$ has unique maximal ideal $\mathfrak{m} = \mathfrak{p} \cdot S^{-1}\mathfrak{o}$. [These features amplified below.]

To show $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$, it suffices to consider the local version, because

$$\mathfrak{p} \cdot S^{-1}\mathfrak{O} \;=\; \mathfrak{p} \cdot S^{-1}\mathfrak{o} \cdot S^{-1}\mathfrak{O} \;=\; \mathfrak{m} \cdot S^{-1}\mathfrak{O}$$

That is, it suffices to prove $\mathfrak{m} \cdot \mathfrak{O} \neq \mathfrak{O}$, with $\mathfrak{o}$ *local.*

For local $\mathfrak{o}$, if $\mathfrak{m} \cdot \mathfrak{O} = \mathfrak{O}$, then $1 \in \mathfrak{O}$ has an expression $1 = m_1 y_1 + \ldots + m_n y_n$, with $m_j \in \mathfrak{m}$ and $y_j \in \mathfrak{O}$. Let $\mathfrak{O}_1$ be the ring $\mathfrak{O}_1 = \mathfrak{o}[y_1, \ldots, y_n]$. It is a finitely-generated $\mathfrak{o}$-*algebra*, so by integrality is a finitely-generated $\mathfrak{o}$-*module.*

**Nakayama's Lemma (simple useful case):** for a local ring $\mathfrak{o}$ with maximal ideal $\mathfrak{m}$, if $\mathfrak{m}X = X$ for a finitely-generated $\mathfrak{o}$-module $X$, then $X = \{0\}$.

*Proof:* (of Lemma) For $X$ generated by $x_1, \ldots, x_n$, the hypothesis gives

$$x_1 \;=\; m_1 x_1 + \ldots + m_n x_n \qquad\qquad \text{(for some } m_j \in \mathfrak{m}\text{)}$$

$$(1 - m_1)x_1 \;=\; m_2 x_2 + \ldots + m_n x_n$$

Since $1 \notin \mathfrak{m}$, $1 - m_1 \notin \mathfrak{m}$. Every element of a commutative ring with 1 is either a unit or is in a maximal ideal. Thus, $1 - m_1$ is a unit, we can divide through by it, and $m_1$ is expressible in terms of the other generators. Induction. ///

Applying this to $\mathfrak{O}_1$ gives $\mathfrak{O}_1 = \{0\}$, contradiction, and $\mathfrak{m} \cdot \mathfrak{O} \neq \mathfrak{O}$.

Reverting to not-necessarily-local $\mathfrak{o}$, in

$$\begin{array}{ccc} \mathfrak{O} & \longrightarrow & S^{-1}\mathfrak{O} \\ \uparrow & & \uparrow \\ \mathfrak{o} & \longrightarrow & S^{-1}\mathfrak{o} \end{array}$$

$\mathfrak{m} \cdot S^{-1}\mathfrak{O} \;\neq\; S^{-1}\mathfrak{O}$, so is in some maximal ideal $\mathfrak{M}$ of $S^{-1}\mathfrak{O}$, and $\mathfrak{M} \cap S^{-1}\mathfrak{o} \;\supset\; \mathfrak{m}$. This cannot contain 1, since $\mathfrak{M} \not\ni 1$. By maximality of $\mathfrak{m}$, $\mathfrak{M} \cap S^{-1}\mathfrak{o} = \mathfrak{m}$.

$\mathfrak{M}$ is non-zero prime, so $\mathfrak{P} = \mathfrak{M} \cap \mathfrak{O}$ is prime, because intersecting a prime ideal with a subring gives a prime ideal. $\mathfrak{P}$ is not $\{0\}$, because of integrality: $0 \neq m \in \mathfrak{M}$ satisfies
$m^n + a_{n-1}m^{n-1} + \ldots + a_o = 0$ with $a_i \in \mathfrak{o}$ and $0 \neq a_o \in \mathfrak{o} \cap \mathfrak{M}$.
Then

$$\mathfrak{o} \cap \mathfrak{P} \;=\; \mathfrak{o} \cap (\mathfrak{O} \cap \mathfrak{M}) \;=\; \mathfrak{o} \cap \mathfrak{M} \;=\; \mathfrak{o} \cap (S^{-1}\mathfrak{o} \cap \mathfrak{M}) \;=\; \mathfrak{o} \cap \mathfrak{m} \;=\; \mathfrak{p}$$

[Discussion of $\mathfrak{P}$ maximal $\Longleftrightarrow$ $\mathfrak{p}$ maximal not repeated.] ///

**Sun-Ze's theorem:** For ideals $\mathfrak{a}_j$ in $\mathfrak{o}$ such that $\mathfrak{a}_i + \mathfrak{a}_j = \mathfrak{o}$ for $i \neq j$, given $x_j$, there is $x \in \mathfrak{o}$ such that $x = x_j \bmod \mathfrak{a}_j$ for all $j$.

*Proof:* The hypothesis gives $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2$ such that $a_1 + a_2 = 1$. Then $x = x_2 a_1 + x_1 a_2$ solves the problem for two ideals.

Induction: for $j > 1$, let $b_j \in \mathfrak{a}_1$ and $c_j \in \mathfrak{a}_j$ such that $b_j + c_j = 1$. Then

$$1 \;=\; \prod_{j>1} (b_j + c_j) \;\in\; \mathfrak{a}_1 + \prod_{j>1} \mathfrak{a}_j$$

That is, $\mathfrak{a}_1 + \prod_{j>1} \mathfrak{a}_j \;=\; \mathfrak{o}$. Thus, there is $y_1 \;\in\; \mathfrak{o}$ such that $y_1 \;=\; 1 \bmod \mathfrak{a}_1$ and $y_1 \;=\; 0 \bmod \prod_{j>1} \mathfrak{a}_j$. Similarly, find $y_i \;=\; 1 \bmod \mathfrak{a}_i$ and $y_i \;=\; 0 \bmod \prod_{j\neq i} \mathfrak{a}_j$. Then $x \;=\; \sum_j x_j y_j$ is $x_i \bmod \mathfrak{a}_i$. ///

**Transitivity of Galois groups on primes lying over $\mathfrak{p}$**

Let $K/k$ be finite *Galois*, $\mathfrak{o}$ integrally closed in $k$, $\mathfrak{O}$ its integral closure in $K$. Let $\mathfrak{p}$ be prime in $\mathfrak{o}$. The Galois group $G = \mathrm{Gal}(K/k)$ is *transitive* on primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

*Proof:* Localize to assume $\mathfrak{p}$ *maximal.* For two primes $\mathfrak{P}, \mathfrak{Q}$ over $\mathfrak{p}$, if no Galois image $\sigma\mathfrak{P}$ is $\mathfrak{Q}$, then there is a solution to

$$x = \begin{cases} 0 \bmod \mathfrak{Q} \\ \\ 1 \bmod \sigma\mathfrak{P} \ \text{ for all } \sigma \in G \end{cases}$$

The norm $N_k^K(x)$ is in $k \cap \mathfrak{O} = \mathfrak{o}$, by integral closure of $\mathfrak{o}$, and then is in $\mathfrak{Q} \cap \mathfrak{o} = \mathfrak{p}$. On the other hand, $\sigma^{-1}x \notin \mathfrak{P}$, for all $\sigma \in G$, so $N_k^K(x) \notin \mathfrak{P}$, contradicting $N_k^K(x) \in \mathfrak{p} \subset \mathfrak{P}$. ///

**Corollary:** In $\mathfrak{O}/\mathfrak{o}$ in $K/k$, there are only finitely-many prime ideals lying over a given prime of $\mathfrak{o}$.

*Proof:* If we can reduce to the Galois-extension case, we're done, by the previous.

Let $K'$ be a Galois closure of $K/k$, with integral closure $\mathfrak{O}'$, and $\mathfrak{Q}_1, \mathfrak{Q}_2$ prime ideals in $K'$ lying over $\mathfrak{P}_1, \mathfrak{P}_2$ in $\mathfrak{O}$ lying over $\mathfrak{p}$ in $\mathfrak{o}$. For $\mathfrak{P}_1 \neq \mathfrak{P}_2$, since (from above) $\mathfrak{Q}_j \cap \mathfrak{O} = \mathfrak{P}_j$, necessarily $\mathfrak{Q}_1 \neq \mathfrak{Q}_2$. Thus, the finitude of primes in $\mathfrak{O}'$ lying over $\mathfrak{p}$ implies that in $\mathfrak{O}$. ///

In Galois $K/k$, since $\mathfrak{O}$ is integrally closed, it is stable under $\mathrm{Gal}(K/k)$.

For maximal $\mathfrak{P}$ lying over $\mathfrak{p}$ in $\mathfrak{o}$, the *decomposition group* [sic] $G_{\mathfrak{P}}$ is the *stabilizer* of $\mathfrak{P}$.

The *decomposition field* of $\mathfrak{P}$ is

$$K^{\mathfrak{P}} = \text{subfield of } K \text{ fixed by } G_{\mathfrak{P}}$$

Let

$$\mathfrak{o}' = \text{integral closure of } \mathfrak{o} \text{ in } K^{\mathfrak{P}} \qquad \mathfrak{q} = K^{\mathfrak{P}} \cap \mathfrak{P} = \mathfrak{o}' \cap \mathfrak{P}$$

**Corollary:** $\mathfrak{P}$ is the only prime of $\mathfrak{O}$ lying above $\mathfrak{q}$.

*Proof:* $\mathrm{Gal}(K/K^{\mathfrak{P}}) = G_{\mathfrak{P}}$ doesn't move $\mathfrak{P}$, but is transitive on primes lying over $\mathfrak{q}$. ///

**Localization:** important special cases.

Simplest case: field-of-fractions $k$ of an integral domain $\mathfrak{o}$.

We know what is intended: $\mathfrak{o}$ injects to $k$, every non-zero element of $\mathfrak{o}$ becomes invertible, and there's nothing extra.

A mapping characterization proves uniqueness: for *any* ring hom $\varphi : \mathfrak{o} \to K$ to a field $K$, there is a unique $\Phi : k \to K$ giving a commutative diagram

$$\begin{tikzcd} k \arrow[dr, dashed, "\exists \Phi"] & \\ \mathfrak{o} \arrow[u, "i"] \arrow[r, "\forall \varphi"'] & K \end{tikzcd}$$

Existence is proven by (the usual) construction: ...

The candidate for $k$ is pairs $(a,b) = $ " $\dfrac{a}{b}$ " with $b \neq 0$, modulo the equivalence derived from equality of fractions: $(a,b) \sim (a',b')$ when $ab' - a'b = 0$, and $j : \mathfrak{o} \to k$ by $j(x) = (x,1)$.

Thus, the *value* of a fraction is unchanged when top and bottom are multiplied by the same (non-zero) element of $\mathfrak{o}$, or when the same (non-zero) factor is removed. However, for non-UFDs $\mathfrak{o}$ the equivalence relation is more complicated.

Addition, multiplication, and inversion are defined as expected:

$$(a,b) + (c,d) \;=\; (ad,bd) + (bc,bd) \;=\; (ad+bc,bd)$$

$$(a,b)\cdot(c,d) \;=\; (ac,bd) \qquad\qquad (a,b)^{-1} \;=\; (b,d)$$

... but well-definedness, commutativity, associativity, and distributivity need proof.

For well-definedness of addition, suppose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, and show $(ad+bc, bd) \sim (a'd'+b'c', b'd')$:

$$b'd'(ad+bc)-bd(a'd'+b'c') \;=\; (ab')dd'+(cd')bb'-(a'b)dd'-(c'd)bb'$$

$$= \;(ab'-a'b)dd' + (cd'-c'd)bb' \;=\; 0 \cdot dd' + 0 \cdot bb' \;=\; 0$$

Then, commutativity and associativity are as usual, by putting things over a common denominator. Commutativity follows from the formula and from commutativity of addition and multiplication in $\mathfrak{o}$:

$$\frac{a}{b} + \frac{a'}{b'} \;=\; \frac{ab'}{bb'} + \frac{a'b}{bb'} \;=\; \frac{ab'+a'b}{bb'}$$

Associativity of addition:

$$\frac{a}{b} + (\frac{a'}{b'} + \frac{a''}{b''}) \;=\; \frac{a}{b} + (\frac{a'b''}{b'b''} + \frac{a''b'}{b'b''})$$

$$= \;\frac{a}{b} + \frac{a'b'' + a''b'}{b'b''} \;=\; \frac{ab'b''}{bb'b''} + \frac{ba'b'' + a''bb''}{bb'b''}$$

$$= \;\frac{ab'b'' + a'bb'' + a''bb''}{bb'b''} \;=\; \text{symmetrical}$$

Commutativity and associativity of multiplication are easier. Distributivity is similar.

If well-defined, $\Phi(a/b) \;=\; \varphi(a)\varphi(b)^{-1}$ fits into the diagram. For well-definedness, with $ab' = a'b$,

$$\varphi(a)\varphi(b)^{-1} - \varphi(a')\varphi(b')^{-1} \;=\; \big(\varphi(a)\varphi(b') - \varphi(a')\varphi(b)\big)\cdot\varphi(b)^{-1}\varphi(b')^{-1}$$

$$= \;\varphi(ab' - a'b)\cdot\varphi(b)^{-1}\varphi(b')^{-1} \;=\; \varphi(0)\cdot\varphi(b)^{-1}\varphi(b')^{-1} \;=\; 0$$

*Finally,* verify that the constructed $\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$ truly is a ring hom.

For example, addition is respected:

$$\Phi(\frac{a}{b} + \frac{a'}{b'}) \;=\; \Phi(\frac{ab' + a'b}{bb'}) \;=\; \varphi(ab' + a'b)\varphi(bb')^{-1}$$

$$= \;\Big(\varphi(a)\varphi(b') + \varphi(a')\varphi(b)\Big)\varphi(b)^{-1}\varphi(b')^{-1}$$

$$= \;\varphi(a)\varphi(b)^{-1} + \varphi(a')\varphi(b')^{-1} \;=\; \Phi(\frac{a}{b}) + \Phi(\frac{a'}{b'})$$

**Remark:** The point is *not* the formulas for arithmetic of fractions, *nor* the checking that the construction succeeds, but that these formulas *succeed* in proving *existence*, by construction, of the field-of-fractions. Its *properties* are unequivocally determined by the mapping characterization.

**Important special case:** Localization at a prime.

For $\mathfrak{o}$ be a commutative ring with 1, and $\mathfrak{p}$ a prime ideal, we want to modify $\mathfrak{o}$ so that it has a unique maximal ideal $\mathfrak{m}$ coming from $\mathfrak{p}$, while all *other* ideals $\mathfrak{a}$ *not* contained in $\mathfrak{p}$ *disappear*.

More precisely, $\mathfrak{o}$-*localized-at*-$\mathfrak{p}$ should be a ring $\mathfrak{o}_\mathfrak{p}$ (subscript does *not* denote completion here) with ring hom $i : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ such that $i(\mathfrak{q}) \cdot \mathfrak{o}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}$ for all primes $\mathfrak{q}$ not contained in $\mathfrak{p}$, $i(\mathfrak{p}) \cdot \mathfrak{o}_\mathfrak{p}$ is the unique maximal ideal $\mathfrak{m}$ of $\mathfrak{o}_\mathfrak{p}$, and $j^{-1}\big(j(\mathfrak{o}) \cap \mathfrak{m}\big) = \mathfrak{p}$.

$\mathfrak{o}_\mathfrak{p}$ should be neither *needlessly big* nor *needlessly small*, so should be *characterized* by a *universal property*: for *any* ring hom $\varphi : \mathfrak{o} \to R$ with $\varphi(\mathfrak{a}) \cdot R = R$ for ideals $\mathfrak{a}$ not contained in $\mathfrak{p}$, there is a unique $\Phi$ giving a commutative diagram

$$\begin{tikzcd}
\mathfrak{o}_\mathfrak{p} \arrow[dr, dashed, "\exists\Phi"] & \\
\mathfrak{o} \arrow[u, "i"] \arrow[r, "\forall\varphi"'] & R
\end{tikzcd}$$

Characterization by a universal property proves uniqueness..., when *existence* is proven, probably by a *construction*.

The property $j^{-1}\big(j(\mathfrak{o}) \cap \mathfrak{m}\big) = \mathfrak{p}$ should *follow*.

**Example:** An *integral domain* $\mathfrak{o}$ sits inside its *field of fractions* $k$, and localizing at $\mathfrak{p}$ simply allows all denominators not in $\mathfrak{p}$

$$\mathfrak{o}_p \;=\; \Big\{\frac{x}{a} \;:\; a \notin \mathfrak{p},\; x \in \mathfrak{o}\Big\} \qquad\qquad \text{(integral domain } \mathfrak{o}\text{)}$$

The requisite map $\mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ is just *inclusion*.

*Proof:* On one hand, any ideal $\mathfrak{a}$ not contained in $\mathfrak{p}$ contains an element $s$ not in $\mathfrak{p}$, which therefore becomes a *unit* in the candidate $\mathfrak{o}_\mathfrak{p}$. That is, the ideal generated by $\mathfrak{a}$ in the candidate $\mathfrak{o}_\mathfrak{p}$ is the whole ring. In particular, the ideal generated by $\mathfrak{p}$ becomes the unique maximal ideal.

On the other hand, let $\varphi : \mathfrak{o} \to R$ with $\varphi(\mathfrak{a}) \cdot R = R$ for $\mathfrak{a}$ not contained in $\mathfrak{p}$. That is, $\varphi(\mathfrak{a})$ contains a unit in $R$. This hypothesis applied to principal ideals $\langle a \rangle$ shows that $\varphi(x)\varphi(a) = \varphi(xa) \in R^\times$ for some $x \in \mathfrak{o}$, and $\varphi(a)$ is a unit. That is, *every* $\varphi(a)$ for $a \notin \mathfrak{p}$ is a unit in $R$.

Try to define $\Phi(x/a) = \varphi(x) \cdot \varphi(a)^{-1}$ for $a \notin \mathfrak{p}$. Check well-definedness: $x/a = x'/a'$ in $k$ gives

$$\varphi(a)\varphi(a')\big(\varphi(x)\varphi(a)^{-1} - \varphi(x')\varphi(a')^{-1}\big)$$

$$= \varphi(a'x) - \varphi(ax') = \varphi(a'x - ax') = \varphi(0) = 0$$

Units $\varphi(a)$ and $\varphi(a')$ have inverses, giving well-definedness.

Multiplicativeness of $\Phi$ is easy.

Addition is preserved: via re-expression with a common denominator, as expected:

$$\Phi(\frac{x}{a}+\frac{x'}{a'}) \;=\; \Phi(\frac{xa'+x'a}{aa'}) \;=\; \Phi(xa'+x'a)\varphi(aa')^{-1}$$

$$=\; \big(\varphi(x)\varphi(a')+\varphi(x')\varphi(a)\big)\cdot\varphi(a)^{-1}\varphi(a')^{-1}$$

$$=\; \varphi(x)\varphi(a)^{-1}+\varphi(x')\varphi(a')^{-1} \;=\; \Phi(\frac{x}{a})+\Phi(\frac{x'}{a'})$$

This proves that the usual construction succeeds for *integral domains*, proving *existence* of the localization.

**Localization in general:** For non-integral-domains $\mathfrak{o}$, *collapsing* can occur in localizations $j : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$.

**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 $j : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$. Thus,

$$j(3) \;=\; j(3) \cdot j(10) \cdot j(10)^{-1} \;=\; j(30) \cdot j(10)^{-1} \;=\; 0 \cdot j(10)^{-1}$$

Thus (!) $\mathfrak{o}_\mathfrak{p} \;=\; \mathbb{Z}/3$, and $\mathbb{Z}/30 \;\to\; \mathbb{Z}/3$ is the quotient map. Generally, $j : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ 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 general proof-of-existence-by-construction of localization:

**Claim:** The localization $j : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ *exists*: it can be constructed as pairs $\{(a, b) : x \in \mathfrak{o},\ b \notin \mathfrak{p}\}$, identifying $(a.b)$, $(a', b')$ when $c \cdot (ab' - a'b) = 0$ for some $c \in \mathfrak{o} - \mathfrak{p}$, with addition and multiplication as usual. Given $\varphi : \mathfrak{o} \to R$, the corresponding $\Phi : \mathfrak{o}_\mathfrak{p} \to R$ is $\Phi(\frac{a}{b}) = \varphi(a)\varphi(b)^{-1}$.

*Proof:* There is a slight novelty in the well-definedness of $\Phi$: for $c \cdot (ab' - a'b) = 0$,

$$0 \;=\; \varphi(0) \;=\; \varphi(c) \cdot \Big(\varphi(a)\varphi(b') - \varphi(a')\varphi(b)\Big)$$

$\varphi(c)$, $\varphi(b)$, $\varphi(b') \in R^\times$. Divide by the product of their inverses:

$$0 \;=\; \varphi(a)\varphi(b)^{-1} - \varphi(a')\varphi(b')^{-1} \;=\; \Phi(\frac{a}{b}) - \Phi(\frac{a'}{b'}) \qquad ///$$