Recap: A better version of localization...

Then: More about *primes lying over*...

$\mathfrak{p}$ **splits completely** in K when there are $[K : k]$ distinct primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

Corollary: For an *abelian* K/k, the decomposition subfield $K^{\mathfrak{P}}$ is the maximal subfield of K (containing k) in which $\mathfrak{p}$ splits completely.

Frobenius map/automorphism

Artin map/automorphism

... and then **Dedekind rings**.

Recap: For arbitrary $S \subset \mathfrak{o}$, the localization $j : \mathfrak{o} \to S^{-1}\mathfrak{o}$ is *uniquely characterized* by: for $\varphi : \mathfrak{o} \to R$ with $\varphi(S) \subset R^\times$, there is a unique Φ giving

$$\begin{tikzcd} S^{-1}\mathfrak{o} \arrow[dr, dashed, "\exists\Phi"] & \\ \mathfrak{o} \arrow[u, "i"] \arrow[r, "\forall\varphi"'] & R \end{tikzcd}$$

Construction as quotient of a polynomial ring with indeterminates x_s for all $s \in S$:

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

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

This produces a *ring*, for any S, although possibly $0 = 1$. Given $\varphi : \mathfrak{o} \to R$ with $\varphi(S) \subset R^\times$, the universal property of polynomial rings gives a unique $\widetilde{\varphi}$ extending φ to the polynomial ring by $\widetilde{\varphi}(x_s) \;=\; \varphi(s)^{-1}$. Then $\widetilde{\varphi}$ factors uniquely through the *quotient*, since

$$\widetilde{\varphi}(sx_s - 1) \;=\; \varphi(s)\widetilde{\varphi}(x_s) - \varphi(1) \;=\; 1 - 1 \;=\; 0$$

Thus,

$$\begin{tikzcd}
\mathfrak{o}[\ldots, x_s, \ldots] \arrow[rr, "\exists\,!\,\mathrm{quot}"] \arrow[drr, dotted, "\exists!\,\widetilde{\varphi}"] & & \dfrac{\mathfrak{o}[\ldots, x_s, \ldots]}{\langle \ldots, sx_s - 1, \ldots \rangle} \arrow[d, dashed, "\exists!\,\Phi"] \\
& \mathfrak{o} \arrow[ul] \arrow[ur, bend left, "j"] \arrow[r, "\forall\varphi"] & R
\end{tikzcd}$$

Last: $S^{-1}\mathfrak{o}$ is not the trivial ring $\{0\}$ with $0 = 1$ if and only if no product of elements of S is 0. [Proven last time.]

With $i : \mathfrak{o} \to \mathfrak{o}_{\mathfrak{p}}$ the localization with $S = \mathfrak{o} - \mathfrak{p}$, prime $\mathfrak{p}$, we really should check that $\mathfrak{o}_{\mathfrak{p}}$ has a unique maximal (proper!) ideal $\mathfrak{m}$ generated by the image $j(\mathfrak{p})$ of $\mathfrak{p}$, and that $j^{-1}(j(\mathfrak{o}) \cap \mathfrak{m}) = \mathfrak{p}$ ... since this was one of the key points in proof of lying-over:

First, because $\mathfrak{p}$ is prime, $S = \mathfrak{o} - \mathfrak{p}$ does *not* contain 0, and no product of its elements is 0. Thus, $0 \neq 1$ in $\mathfrak{o}_{\mathfrak{p}}$.

Let $\mathfrak{m} = j(\mathfrak{p}) \cdot \mathfrak{o}_{\mathfrak{p}}$. This certainly contains $j(\mathfrak{p})$.

From its characterization, any element of $\mathfrak{o}$ outside $\mathfrak{p}$ becomes a *unit* in $\mathfrak{o}_{\mathfrak{p}}$.

Thus, as long as $\mathfrak{m} \neq \mathfrak{o}_{\mathfrak{p}}$, we know $j^{-1}(j(\mathfrak{o}) \cap \mathfrak{m}) = \mathfrak{p}$.

...

Localization of modules and algebras:

For an $\mathfrak{o}$-module M or (commutative) $\mathfrak{o}$-algebra A, it should not be surprising that the useful notions of *localization* of M and A are by

$$M_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} M \qquad\qquad A_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} A$$

Though, why not the *other* extensions of scalars,
$M_{\mathfrak{p}} = \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{o}_{\mathfrak{p}}, M)$ and $A_{\mathfrak{p}} = \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{o}_{\mathfrak{p}}, A)$? Recall what we needed in the argument.

$$\begin{tikzcd}
\mathfrak{O} \arrow[r] \arrow[d, dash] & S^{-1}\mathfrak{P} \supset \mathfrak{M} \arrow[d, dash] \\
\mathfrak{o} \arrow[r] & S^{-1}\mathfrak{o} \supset \mathfrak{m}
\end{tikzcd}$$

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

$\mathfrak{O}$ *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 maximal if and only if $\mathfrak{p}$ is maximal. $\mathfrak{p} \cdot \mathfrak{O} \neq \mathfrak{O}$. [Here use Nakayama, localization.]

Now $\mathfrak{o}$ is a *domain*, integrally closed in its field of fractions k. For K/k finite *Galois*, the Galois group $G = \mathrm{Gal}(K/k)$ is *transitive* on primes lying over $\mathfrak{p}$ in $\mathfrak{O}$. [Here use Sun-Ze.]

For K/k finite separable, there are only finitely-many prime ideals lying over a given prime of $\mathfrak{o}$. [Reduce to Galois case.]

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 $\mathfrak{O}$ lying above $\mathfrak{P} \cap K^{\mathfrak{P}}$. [Transitivity.]

More about primes-lying-over: The picture is

$$\begin{tikzcd}
K \arrow[r, dash, "\supset"] \arrow[dd, dash, "G_{\mathfrak{P}}"'] & \mathfrak{O} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[drr] & \mathfrak{P} \arrow[dd, dash] & \\
& & & \mathfrak{O}/\mathfrak{P} = \tilde{\kappa} \arrow[dd, dash] \\
K^{\mathfrak{P}} \arrow[r, dash, "\supset"] \arrow[dd, dash] & \mathfrak{O}^{\mathfrak{P}} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[drr] & \mathfrak{Q} = \mathfrak{P} \cap K^{\mathfrak{P}} \arrow[dd, dash] & \\
& & & \mathfrak{O}^{\mathfrak{P}}/\mathfrak{Q} \arrow[dd, dash, "="', "\text{[pf below]}"] \\
k \arrow[r, dash, "\supset"] & \mathfrak{o} \arrow[r, dash, "\supset"] \arrow[drr] & \mathfrak{p} & \\
& & & \mathfrak{o}/\mathfrak{p} = \kappa
\end{tikzcd}$$

Next:

Claim: The inclusion $\mathfrak{o}/\mathfrak{p} \to \mathfrak{O}^{\mathfrak{P}}/\mathfrak{Q}$ is an isomorphism.

Claim: $\tilde{\kappa} = \mathfrak{O}/\mathfrak{P}$ is *normal* over $\kappa = \mathfrak{o}/\mathfrak{p}$, and $G_{\mathfrak{P}}$ surjects to $\mathrm{Aut}(\tilde{\kappa}/\kappa)$.

More named objects: The **inertia group**: $I_{\mathfrak{P}}$ is the kernel of $G_{\mathfrak{P}} \to \mathrm{Gal}(\tilde{\kappa}/\kappa)$. The fixed field of $I_{\mathfrak{P}}$ is the **inertia subfield** of K. These will not be used much here.

$\mathfrak{p}$ **splits completely** in K when there are $[K : k]$ distinct primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

Corollary: For an *abelian* K/k, the decomposition subfield $K^{\mathfrak{P}}$ is the maximal subfield of K (containing k) in which $\mathfrak{p}$ splits completely.

Frobenius map/automorphism in the number field (or function field) case is anything that maps to $x \to x^q$ in the residue class field extension $\tilde{\kappa}/\kappa = \mathbb{F}_{q^n}/\mathbb{F}^q$.

Artin map/automorphism ... is Frobenius for *abelian* extensions.

A **fractional ideal** $\mathfrak{a}$ of $\mathfrak{o}$ in its fraction field k is an $\mathfrak{o}$-submodule of k such that there is $0 \neq c \in \mathfrak{o}$ such that $c\mathfrak{a} \subset \mathfrak{o}$.

Theorem: In Noetherian, integrally closed ring $\mathfrak{o}$ in which every non-zero prime ideal is *maximal*, every non-zero ideal is uniquely a product of prime ideals, and the non-zero fractional ideals form a *group* under multiplication. [Below...]

Noetherian, integrally-closed commutative rings in which every non-zero prime ideal is maximal are **Dedekind rings**.