Our description of primes in extension is even nicer when we have $L/K$ is Galois extension. ($L$ is splitting field for polynomial over $K$)

Then, letting $G := \text{Gal}(L/K)$, with $\beta \in G$, since $L/K$ separable, any prime $\mathfrak{P}$ in $L$ that all roots of $\mathfrak{P}$ in $L$ prime.

$\beta \mathfrak{P}$ is an ideal of $\mathcal{O}_L$ with $\beta \mathfrak{P} \cap \mathfrak{O}_K = \beta ((\beta \mathfrak{P}) \cap \mathfrak{O}_K) = \mathfrak{P}$.

(i.e. if $\beta | \mathfrak{P}$ then $\beta((\beta \mathfrak{P}) \cap \mathfrak{O}_K) | \mathfrak{P}$)

Proposition: $G = \text{Gal}(L/K)$ acts transitively on prime ideals $\mathfrak{p}$ of $\mathcal{O}_L$ lying above $\mathfrak{P}$.

If: Suppose not. By CRT, we can find $x \in \mathcal{O}_L$ s.t.

\[
x \equiv 0 \pmod{\mathfrak{p}} \quad x \equiv 1 \pmod{\mathfrak{p}'} \text{ for two non-associating } \mathfrak{p}, \mathfrak{p}' \text{ over } \mathfrak{P}.
\]

\[
N_{L/K}(x) = \prod_{\beta \in G} \beta(x) \in \mathfrak{p'} \cap \mathcal{O}_L = \mathfrak{P}
\]

But $\mathfrak{P} \neq \beta(x) \neq \mathfrak{p} \cap \mathcal{O}_L$, i.e. $\mathfrak{p}(x) \neq \mathfrak{P}$ for all $\beta \in G$.

$\Rightarrow$ $\prod_{\beta \in G} \beta(x) \neq \mathfrak{p} \cap \mathcal{O}_L = \mathfrak{P}$. Contradiction.

$\Rightarrow$ So we seek to understand the action of $G$ on the $\mathfrak{p}'s$ over $\mathfrak{P}$ more precisely...

Define "decomposition group" $G_{\mathfrak{P}} = \{ \beta \in G | \beta(\mathfrak{P}) = \mathfrak{P} \}$

named so because # of prime ideals dividing $\mathfrak{p} \mathcal{O}_L$ is $|G|/|G_{\mathfrak{P}}|$. 

Notice that $G_b = bG_b b^{-1}$ since

$$T \in G_b \iff T(b(g)) = b((g)) \iff 6Tb^{-1}(g) = gb$$

$$\iff 6Tb^{-1} \in G_b \iff T \in 6G_b b^{-1}.$$  

Nice remark in Newboud: Even when $L/k$ not Galois, merely separable,

still take Galois extn containing $L$, call it $N$

$$H \left\{ \begin{array}{c}
N \\{ G \} \\
L \{ G \} \\
K \end{array} \right\} \{ g_1, \ldots , g_r \}$$

then

$$H \backslash G / G_q \leftarrow \begin{array}{c}
\{ g \in G \mid gq_1 \} \\
\text{decomp} \\
H \not\in G_b \text{-double coset} \\
\rightarrow b(g) \cap L
\end{array}$$

Proposition: \[ p = g_{e_1} \cdots g_{e_r} \text{ with } L/K \text{ Galois extn then }\]

\[ e_1 = \cdots = e_r \text{ and } f_i = \cdots = f_r \] (common to call all $e_i$'s by "e" and all $f_i$'s by "f".)

Proof: The Galois gp acts transitively, so \( \exists i \in G \) s.t. \( b_i(g) = g_i \).

Then \( O/b_i \sim O/g_i \) \( \Rightarrow f_i = f_i \) for any $i$.

\[ a \mod \beta \rightarrow b(a) \mod \beta: [O_b/\beta, :O_h/\beta] \]

Furthermore, \( \beta_i \mid \beta_\theta \Leftrightarrow b_i(\beta_i) \mid b_i(\beta_\theta) \Leftrightarrow \beta_i b_i(\beta_i) \mid \beta_\theta \]

\( \text{since } b_i(\beta_\theta) = \beta_\theta \)

as $b_i$ permutes divisors

\( \text{so } e_i \)’s must all be equal.
We can also define decomposition field $\mathbb{Z}_\mathfrak{g} = \{ x \in L \mid 6x = x \forall \mathfrak{g} \in \mathbb{G}_\mathfrak{g} \}$, so for example $G_{\mathfrak{g}} = 1 \iff \mathbb{Z}_\mathfrak{g} = L \iff \mathfrak{g}$ splits completely.

$G_{\mathfrak{g}} = \mathcal{G} \iff \mathbb{Z}_\mathfrak{g} = K \iff \mathfrak{g}$ non-split (totally inert)

Can also define $\mathfrak{g}_L = \mathfrak{g} \cap \mathbb{Z}_\mathfrak{g}$, a prime ideal of $\mathbb{Z}_\mathfrak{g}$

$\begin{array}{c|c|c}
L & \mathfrak{g} & \mathbb{Z}_\mathfrak{g} \\
\hline
\mathbb{Z}_\mathfrak{g} & \mathfrak{g}_L & \mathfrak{g}_L
\end{array}$

Proposition: (i) $\mathfrak{g}_L$ is inert in $L$ (i.e., $\mathfrak{g}_L$ is only ideal dividing $\mathfrak{g}_L \cdot \mathcal{O}_L$).

(ii) $\mathfrak{g}_L$, as ideal of $L$ over $\mathbb{Z}_\mathfrak{g}$, has ramification index $e$, inertia deg. $f$.

(iii) $\mathfrak{g}_L$, as ideal of $\mathbb{Z}_\mathfrak{g}$ over $\mathfrak{g}$, has ramification index $1$, inertia deg. $1$.

(i): By construction, $\text{Gal}(L/\mathbb{Z}_\mathfrak{g}) = G_{\mathfrak{g}}$, so ideals over $\mathfrak{g}_L$, given by $\mathcal{O}_L(x)$, with $x \in \mathbb{G}_\mathfrak{g}$, which is just $\mathfrak{g}_L$ itself.

(ii) $|\text{Gal}(L/K)| = [L:K] = e \cdot f \cdot r$

where $r = |G_{\mathfrak{g}}|/|G_{\mathfrak{g}}|$ so $|G_{\mathfrak{g}}| = [L:K] = ef$.

But we don't yet know how ramification $e$ distributes over $\mathbb{Z}_\mathfrak{g}/K$ and $L/\mathbb{Z}_\mathfrak{g}$ until we apply (i), which says (likewise for $f$)

$[L:Z_{\mathfrak{g}}] = e'f'$ where $e'|e$, $f'|f$ ($e'$: ramif. in $\mathbb{Z}_\mathfrak{g}$ up to $L$)

so $e' = e$, $f' = f$ giving (ii) and (iii) simultaneously.

We separated $r$ from $ef$ in making this tower of field extensions, but we can go further...
Finally, since $G_{\bar{\wp}}$ fixes both $O_L$ and $\wp$, its elements $6$ induce automorphisms of residue field:

\[ \bar{\sigma} : \frac{O_L}{\wp} \to \frac{O_L}{\wp} \]

\[ a \mapsto \bar{\sigma}(a) \pmod{\wp} \]

Moreover, there is a homomorphism

\[ G_{\bar{\wp}} \to \text{Gal}(\frac{O_L}{\wp} / \frac{O_k}{\wp}) \]

\[ 6 \mapsto 2 \]

where (a) $O_L/\wp / O_k/\wp$ is a normal extension

(b) the map is surjective

and hence the kernel of the map is called the inertia group of $\wp$ over $K$, denoted $I_{\bar{\wp}}$.

Proof of (a): WLOG, take $K = \mathbb{Z}/p$ since their residue fields are same over $O_k/\wp$. Given $\bar{\sigma} \in O_L/\wp$, with min poly $\bar{f}(x)$ over $O_k/\wp$, want to show $\bar{f}(x)$ has roots in $O_L/\wp$ (i.e. splits in $O_L/\wp$).

If $\theta$ is lift of $\bar{\sigma}$ to $O_L$, with min poly $f(x)$ then $\bar{f}$ is divisible (over $K$) by $\bar{g}$ (as $\bar{\sigma}$ is zero of $f$).

Now $L/K$ Galois $\Rightarrow$ every $f(x)$ splits over $O_L$ (and in part. normal)

\[ \Rightarrow \bar{f} \text{ splits over } O_L/\wp \Rightarrow \bar{g} \text{ splits over } O_L/\wp \text{ } \checkmark \]

Proof of (b): If $O_L/\wp / O_K/\wp$ is separable (true when residue field finite) then let $\bar{\sigma}$ be primitive elt. (Neukirch: max. separable subextension gen by $\bar{\sigma}$)
Again let $\tilde{g}(x)$ be its minimal poly, and if $\Theta \in \mathbb{O}_L$ is rep for $\tilde{\Theta}$ in $\mathbb{O}_L / \mathbb{Q}$, then fix its minimal polynomial.

If we're given $\tilde{z} \in \text{Gal}(\mathbb{O}_L / \mathbb{Q} / \mathbb{O}_K / \mathbb{Q}) = \text{Gal}(\mathbb{O}_K[\tilde{\Theta}] / \mathbb{O}_K / \mathbb{Q})$, then want to find $\tilde{z} \in \mathbb{G}_\mathbb{Q}$ mapping to $\tilde{z}$:

the way it suffices to show $\exists \tilde{z} \in \mathbb{G}_\mathbb{Q}$ with $\tilde{z}(\Theta) = \tilde{z}(\tilde{\Theta}) \mod \mathbb{Q}$.

But $\tilde{z}(\tilde{\Theta})$ is a root of $\tilde{g}(x)$, hence of $\tilde{f}(x)$ (which is divs by $\tilde{g}$)

$\iff \exists \Theta'$ in $\mathbb{O}_L$, a zero of $\tilde{f}(x)$, such that $\Theta' \equiv \tilde{z}(\tilde{\Theta}) \mod \mathbb{Q}$.

But then $\Theta'$, as a root of $\tilde{f}(x)$, the min poly of $\Theta$, satisfies $\tilde{z}(\Theta) = \Theta'$

for some $\tilde{z}$. This is the desired $\tilde{z} \in \text{Gal}(L / K)$ s.t. $\tilde{z}(\Theta) \equiv \tilde{z}(\tilde{\Theta}) \mod \mathbb{Q}$.

So now we have exact sequence:

$$1 \rightarrow \mathbb{I}_\mathbb{Q} \rightarrow \mathbb{G}_\mathbb{Q} \rightarrow \text{Gal}(\mathbb{O}_L / \mathbb{Q} / \mathbb{O}_K / \mathbb{Q}) \rightarrow 1$$

inertial gp decmp. gp.

and inertia field $T_{\mathbb{Q}} = \{ x \in L \mid \exists x = x \forall x \in \mathbb{I}_\mathbb{Q} \}$

satisfying $K \subseteq T_{\mathbb{Q}} \subseteq T_{\mathbb{Q}} \subseteq L$

since $T_{\mathbb{Q}} / \mathbb{Q}_\mathbb{Q}$ is normal with $\text{Gal}(T_{\mathbb{Q}} / \mathbb{Q}_\mathbb{Q}) \cong \text{Gal}(\mathbb{O}_L / \mathbb{Q} / \mathbb{O}_K / \mathbb{Q})$

$\text{Gal}(L / T_{\mathbb{Q}}) \cong \mathbb{I}_\mathbb{Q}$ with $\# \mathbb{I}_\mathbb{Q} = \epsilon$.

Since $\# \mathbb{G}_\mathbb{Q} = \epsilon$ as proved earlier.
Working through definitions, if \( \mathfrak{p}_T = \mathfrak{p} \cap T \mathfrak{p} \), then

ramification index for \( \mathfrak{p} \) over \( \mathfrak{p}_T \) is \( e \), inertia degree 1.

ramification index for \( \mathfrak{p}_T \) over \( \mathfrak{p}_2 \) is 1, inertia degree is \( f \).

(see this by observing \( \Theta_T / \mathfrak{p}_T = \Theta_{T'} / \mathfrak{p}_2 \), which follows from fact

that \( I_{\mathfrak{p}} \) : inertia gr. of \( \mathfrak{p} \) over \( K \) = inertia gr. of \( \mathfrak{p} \) over \( T \mathfrak{p} \)

so applying previous result to \( L / T \mathfrak{p} \), \( \text{Gal}(\Theta_{T'}/\mathfrak{p}_2 / \Theta_{T'} / \mathfrak{p}_T) = 1 \)

i.e. the residue fields are equal.)

So picture:

\[
\begin{array}{c|c|c|c}
\mathfrak{p} & \mathfrak{p}_1 & \ldots & \mathfrak{p}_r \\
T \mathfrak{p} & \mathfrak{p}_1 & \ldots & \mathfrak{p}_r \\
\mathbb{Z}_T \mathfrak{p} & \mathfrak{p}_1 & \ldots & \mathfrak{p}_r \\
K & \mathfrak{p} & \ldots & \mathfrak{p}
\end{array}
\]

\( e, f = 1 \) \( \Rightarrow \) all splitting