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)

since L/K separable or that all roots of all min polys in L

Then, letting $G := \mathrm{Gal}(L/K)$, with $\sigma \in G$,

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

(i.e. if $\beta \mid \mathfrak{p}$ then $\sigma(\beta) \mid \mathfrak{p}$)

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

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

$x \equiv 0 \mod \mathfrak{P}'$ $\quad x \equiv 1 \mod \sigma\mathfrak{P}$ $\forall\ \sigma \in G$ for two non-assoc. $\mathfrak{P}, \mathfrak{P}'$ over $\mathfrak{p}$.

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

But $x \notin \sigma\mathfrak{P}$ $\forall\ \sigma \in G$, i.e. $\sigma(x) \notin \mathfrak{P}$ $\forall\ \sigma \in G$.

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

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

Define "decomposition gp" $G_{\mathfrak{P}} = \{ \sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P} \}$

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

Notice that $G_{\sigma(\mathfrak{P})} = \sigma G_{\mathfrak{P}} \sigma^{-1}$ since

$$\tau \in G_{\sigma(\mathfrak{P})} \Leftrightarrow \tau(\sigma(\mathfrak{P})) = \sigma(\mathfrak{P}) \Longleftrightarrow \sigma\tau\sigma^{-1}(\mathfrak{P}) = \mathfrak{P}$$

$$\Longleftrightarrow \sigma\tau\sigma^{-1} \in G_{\mathfrak{P}} \Longleftrightarrow \tau \in \sigma G_{\mathfrak{P}} \sigma^{-1}.$$

Nice remark in Neukirch: Even when L/K not Galois, merely separable, still take Galois ext'n containing L, call it N

$$\begin{array}{ccc} & N & \mathfrak{q}\text{'s} \\ H = \mathrm{Gal}(N/L) & | & ||| \\ & L & \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \\ G & | & ||| \\ & K & \mathfrak{p} \end{array}$$

then $H \backslash G / \underbrace{G_{\mathfrak{q}}}_{\text{decomp}} \xleftrightarrow{1\text{-}1} \{ \mathfrak{P} \text{ in } \mathcal{O}_L \mid \mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L \}$

$H \sigma G_{\mathfrak{q}}$ - double coset $\longmapsto \sigma(\mathfrak{q}) \cap L$

Proposition: $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ with L/K Galois ext'n then $e_1 = \cdots = e_r$ and $f_1 = \cdots = f_r$. (common to call all e_i's by "e", all f_i's by "f")

pf: The Galois gp acts transitive, so $\exists\ \sigma_i \in G$ s.t. $\sigma_i(\mathfrak{P}_1) = \mathfrak{P}_i$.

Then $\mathcal{O}/\mathfrak{P}_1 \simeq \mathcal{O}/\mathfrak{P}_i \Rightarrow f_1 = f_i$ for any i.

$a \bmod \mathfrak{P}_1 \longmapsto \sigma_i(a) \bmod \mathfrak{P}_i$ $\qquad f_1 = [\mathcal{O}_L/\mathfrak{P}_1 : \mathcal{O}_K/\mathfrak{p}]$

Furthermore,

$$\mathfrak{P}_1^{\nu} \mid \mathfrak{p}\mathcal{O}_L \Longleftrightarrow \sigma_i(\mathfrak{P}_1^{\nu}) \mid \sigma_i(\mathfrak{p}\mathcal{O}_L) \Longleftrightarrow \overbrace{\sigma_i(\mathfrak{P}_1)}^{\mathfrak{P}_i}{}^{\nu} \mid \mathfrak{p}\mathcal{O}_L$$

since $\sigma_i(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$ as σ_i permutes divisors

So e_i's must all be equal.

We can also define <u>decomposition field</u> $Z_{\mathfrak{P}} = \{ x \in L \mid \sigma x = x \ \forall\ \sigma \in G_{\mathfrak{P}} \}$

so for example $G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L \iff \mathfrak{p}$ splits completely

$G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K \iff \mathfrak{p}$ non-split (totally inert)

Can also define $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$, a prime ideal of $Z_{\mathfrak{P}}$

$$\begin{array}{cc} L & \mathfrak{P} \\ | & | \\ Z_{\mathfrak{P}} & \mathfrak{P}_Z \\ | & | \\ K & \mathfrak{p} \end{array}$$

<u>Proposition</u>: (i) $\mathfrak{P}_Z$ is inert in L (i.e. $\mathfrak{P}$ is <u>only</u> ideal dividing $\mathfrak{P}_Z \cdot \mathcal{O}_L$.)

(ii) $\mathfrak{P}$, as ideal of L over $Z_{\mathfrak{P}}$, has ramification index e, inertia deg. f.

(iii) $\mathfrak{P}_Z$, as ideal of $Z_{\mathfrak{P}}$ over K, has ramification index 1, inertia deg. 1.

<u>pf</u> (i): By construction, $\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$ so ideals over $\mathfrak{P}_Z$, given by $\sigma(\mathfrak{P})$ with $\sigma \in G_{\mathfrak{P}}$, which is just $\mathfrak{P}$ itself.

(ii) $|\underset{\overset{\shortparallel}{G}}{\mathrm{Gal}(L/K)}| = [L:K] = e \cdot f \cdot r$

where $r = |G| / |G_{\mathfrak{P}}|$ so $|G_{\mathfrak{P}}| = [L : Z_{\mathfrak{P}}] = ef$.

We don't yet know how ramification e distributes over $Z_{\mathfrak{P}}/K$ and $L/Z_{\mathfrak{P}}$ (likewise for f)

until we apply (i), which says

$[L : Z_{\mathfrak{P}}] = e'f'$ where $e' \mid e$, $f' \mid f$ (e': ramif. in $Z_{\mathfrak{P}}$ up to L; f': inertial deg. — " —)

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 $G_{\mathfrak{P}}$ fixes both $\mathcal{O}_L$ and $\mathfrak{P}$, its elements σ induce automs. of residue field:

$$\bar{\sigma} : \mathcal{O}_L/\mathfrak{P} \longrightarrow \mathcal{O}_L/\mathfrak{P}$$
$$a \pmod{\mathfrak{P}} \longmapsto \sigma(a) \pmod{\mathfrak{P}}$$

Moreover there is a homomorphism

$$G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}\left(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p} \right)$$
$$\sigma \longmapsto \bar{\sigma}$$

where (a) $\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p}$ is normal extension

(b) the map is surjective

and ~~them~~ the kernel of the map is called the inertia gp. of $\mathfrak{P}$ over K, denoted $I_{\mathfrak{P}}$.

pf of (a): WLOG, take $K = Z_{\mathfrak{P}}$ since their residue fields are same. Given $\bar{\theta} \in \mathcal{O}_L/\mathfrak{P}$, with min poly $\bar{g}(x)$ over $\mathcal{O}_K/\mathfrak{p}$, over $\mathcal{O}_K/\mathfrak{p}$.

want to show $\bar{g}(x)$ has roots in $\mathcal{O}_L/\mathfrak{P}$ (i.e. splits in $\mathcal{O}_L/\mathfrak{P}$).

If θ is lift of $\bar{\theta}$ to $\mathcal{O}_L$, with min poly $f(x)$ (over K) then $\bar{f}$ is divisible by $\bar{g}$ (as $\bar{\theta}$ is zero of $\bar{f}$)

Now L/K Galois (and in part. normal) $\Rightarrow$ $f(x)$ splits over $\mathcal{O}_L$

$\Rightarrow$ $\bar{f}$ splits over $\mathcal{O}_L/\mathfrak{P}$ $\Rightarrow$ $\bar{g}$ splits over $\mathcal{O}_L/\mathfrak{P}$ ✓.

pf of (b): If $\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p}$ separable (true when residue field finite)

then let $\bar{\theta}$ be primitive elt. (Neukirch: max. separable subextension gen by $\bar{\theta}$)

Again let $\bar{g}(x)$ be its minimal poly, and if $\theta \in \mathcal{O}_L$ is rep for $\bar{\theta}$ in $\mathcal{O}_L/\mathfrak{P}$, then $f(x)$ its minimal polynomial.

If we're given $\bar{\sigma} \in \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p}) = \mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{p}[\bar{\theta}] \,/\, \mathcal{O}_K/\mathfrak{p}\right)$

then want to find $\sigma \in G_{\mathfrak{P}}$ mapping to $\bar{\sigma}$:

~~the~~ ~~enough~~ it suffices to show $\exists\ \sigma \in G_{\mathfrak{P}}$ with $\sigma(\theta) \equiv \bar{\sigma}(\bar{\theta})$ mod $\mathfrak{P}$.

But $\bar{\sigma}(\bar{\theta})$ is a root of $\bar{g}(x)$, hence of $\bar{f}(x)$ (which is divis. by $\bar{g}$)

$\Longleftrightarrow\ \exists\ \theta'$ in $\mathcal{O}_L$, a zero of $f(x)$, such that $\theta' \equiv \bar{\sigma}(\bar{\theta})$ mod $\mathfrak{P}$

But then θ', as a root of $f(x)$, the min poly of θ, satisfies $\sigma(\theta) = \theta'$ for some σ. This is the desired $\sigma \in \mathrm{Gal}(L/K)$ s.t. $\sigma(\theta) \equiv \bar{\sigma}(\bar{\theta})$ mod $\mathfrak{P}$.

—

So now we have exact sequence:

$$1 \longrightarrow \underset{\text{inertia gp}}{I_{\mathfrak{P}}} \longrightarrow \underset{\text{decomp. gp.}}{G_{\mathfrak{P}}} \longrightarrow G(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p}) \longrightarrow 1$$

and inertia field $T_{\mathfrak{P}} = \{ x \in L \mid \sigma x = x \ \forall\ \sigma \in I_{\mathfrak{P}} \}$

satisfying
$$\underbrace{K \subseteq Z_{\mathfrak{P}}}_{r} \underbrace{\subseteq T_{\mathfrak{P}}}_{f} \underbrace{\subseteq L}_{e}$$

since $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ is normal with $\mathrm{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p})$

$\mathrm{Gal}(L/T_{\mathfrak{P}}) \cong I_{\mathfrak{P}}$ with $\# I_{\mathfrak{P}} = e$

Since $\# G_{\mathfrak{P}} = ef$ 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 $\mathfrak{P}_Z$ is 1, inertia degree is f.

(see this by observing $\mathcal{O}_T/\mathfrak{P}_T = \mathcal{O}_L/\mathfrak{P}$, which follows from fact

that $I_{\mathfrak{P}}$: inertia gp. of $\mathfrak{P}$ over K = inertia gp. of $\mathfrak{P}$ over $T_{\mathfrak{P}}$

so applying previous result to $L/T_{\mathfrak{P}}$, $\mathrm{Gal}\left(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_{T_{\mathfrak{P}}}/\mathfrak{P}_T \right) = 1$

i.e. the residue fields are equal.)

so picture:

$$\begin{array}{ccl}
L & \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} & \\
| & | \quad | & \Big\} \text{ all ramification} \\
T_{\mathfrak{P}} & \mathfrak{P}_1 \cdots \mathfrak{P}_r & \\
| & | \quad | & \Big\} \text{ all inertia} \\
Z_{\mathfrak{P}} & \mathfrak{P}_1 \cdots \mathfrak{P}_r & \\
| & | & e,f=1 \Big\} \text{ all splitting} \\
K & \mathfrak{p} &
\end{array}$$