Prime factorizations in Dedekind domains. Might as well take

$$\begin{array}{c} L \\ | \\ K \end{array} \quad \text{finite extension} \qquad \begin{array}{c} \mathcal{O}_L \\ | \\ \mathcal{O}_K \end{array}$$

where $\mathcal{O}_L$: integral closure of $\mathcal{O}_K$ in L.

Here $\mathcal{O}_K$ can be arbitrary Dedekind domain, but often apply it to case where it is ring of ints.

<u>Fact</u>: $\mathcal{O}_L$ is Dedekind domain.

<u>pf</u>: Same as for $\mathcal{O}_K / \mathbb{Z}$ if L/K separable. (We assume this for now) Prop. 3.1 of Neukirch

check 3 conditions:

- integrally closed (def'n)
- every prime maximal: $\mathcal{O}/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$ is finite ext. of field.
- noetherian: every ideal is f. gen. as $\mathcal{O}_L$-module. using discriminant of basis $\alpha_1, \dots, \alpha_n$ of L/K (note: one time where not using ascending chain condition, but all submodules are finitely gen.)

So consider, for $\mathfrak{p} \neq 0$ prime in $\mathcal{O}_K$

$$(*) \qquad \mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

The $\mathfrak{P}_i$'s that appear are the finitely many $\mathfrak{P}$ prime with $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

$\Updownarrow$

As before, write $\mathfrak{P} \mid \mathfrak{p}$ for $\mathfrak{p} \subseteq \mathfrak{P}$ as $\mathcal{O}_L$-ideals.

Let $f_i = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ "inertia degree"

Lemma ~~Proposition~~ Given factorization as in $(*)$, with $[L:K]=n$

then $$n = \sum_{i=1}^{r} e_i f_i.$$

Main Theorem ~~Proposition~~: Let $L = K(\theta)$ with $\theta \in \mathcal{O}_L$. For almost all primes $\mathfrak{p}$ * (to be specified.)

let $\overline{\phi}_\theta(x) = \overline{\phi}_1(x)^{e_1} \cdots \overline{\phi}_r(x)^{e_r}$ be the factorization of $\phi_\theta(x)$: min polg. for θ

into monic irreducibles $\overline{\phi}_i$ over $\mathcal{O}_K/\mathfrak{p}$. Then $\mathfrak{P}_i \mid \mathfrak{p}$ are given explicitly by:

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + \phi_i(\theta)\mathcal{O}_L$$

i.e. $\langle \mathfrak{p}, \phi_i(\theta) \rangle$

for any monic ϕ_i in $\mathcal{O}_K[x]$ $\equiv \overline{\phi}_i$ after reduction mod $\mathfrak{p}$.

Moreover, inertia degree $f_i := [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ is $\deg(\bar{\phi}_i)$

and so $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$.

~~Proposition~~ Corollary: if L/K separable, $\exists$ finitely many* $\mathfrak{p} \in \mathcal{O}_K$ whose factorizations $\underbrace{\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \text{ have an } e_i > 1}_{\text{say } \mathfrak{p} \text{ "ramified"}}$.

*almost the same asterisk as before!

Take their pfs in order, since each depends on one before.

pf of ~~Proposition~~ Lemma: By Chinese Remainder Thm:

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \bigoplus_{i=1}^{r} \mathcal{O}_L/\mathfrak{P}_i^{e_i}.$$

claim: As $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ vector spaces,

(a) $\dim(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = n$

(b) $\dim(\mathcal{O}_L/\mathfrak{P}_i^{e_i}) = e_i f_i$.

For (a): show that reps. $\alpha_1, \dots, \alpha_m \in \mathcal{O}_L$ for basis of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ as vector space are basis for L/K. (first show linearly independent)

We show dependence over K for $\alpha_1, \dots, \alpha_m$ implies $\mathcal{O}_K/\mathfrak{p}$-dependence for $\bar{\alpha}_1, \dots, \bar{\alpha}_m$ in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$:

Given $a_1\alpha_1 + \cdots + a_m\alpha_m = 0$, $a_i \in K$, clear denoms to get $a_i \in \mathcal{O}_K$.

Let $\mathfrak{a} = (a_1, \dots, a_m)$ and pick $a \in \mathfrak{a}^{-1}$ with $a \notin \mathfrak{a}^{-1}\mathfrak{p}$

so $a\mathfrak{a} \not\subseteq \mathfrak{p}$ i.e. aa_i, $i = 1, \dots, m$ not all in $\mathfrak{p}$, but in $\mathcal{O}_K$.

thus $aa_1\bar{\alpha}_1 + \cdots + aa_m\bar{\alpha}_m = 0$ is non-trivial linear relation over $\mathcal{O}_K/\mathfrak{p}$. // for (a)

To show $\alpha_1, \dots, \alpha_m$ span L as K-vector space,

take $\mathcal{O}_K$-module $M = \mathcal{O}_K \alpha_1 + \dots + \mathcal{O}_K \alpha_m$, $N = \mathcal{O}_L / M$

Because $\bar{\alpha}_i$ are basis of $\mathcal{O}_L / \mathfrak{p}\mathcal{O}_L$, then $\mathcal{O}_L = M + \mathfrak{p}\mathcal{O}_L \Rightarrow$

$N = \mathfrak{p}N$. (**) Both $\mathcal{O}_L$ and N are fin. gen. $\mathcal{O}_K$-modules since $\mathcal{O}_L$ is Noetherian.

Similar games as before: Write each generator γ_i $i=1,\dots,s$ of N according to (**).

as $\gamma_i = \sum_j a_{ij}\gamma_j$ $a_{ij} \in \mathfrak{p}$. Then setting

$A = (a_{ij}) - I_s$

we have $A \cdot \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_s \end{pmatrix} = 0$ and letting B be classical adjoint

$B \cdot A = \det(A) \cdot I_s$. so $0 = BA \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_s \end{pmatrix} = \begin{pmatrix} \det(A)\cdot\gamma_1 \\ \vdots \\ \det(A)\cdot\gamma_s \end{pmatrix}$

so $\det(A) \cdot N = 0 \iff \det(A) \cdot \mathcal{O}_L \subseteq M$ (remember $N := \mathcal{O}_L / M$)

also $\det(A) \neq 0$ since $\det(A) \equiv (-1)^s \mod \mathfrak{p}$ since all $a_{ij} \in \mathfrak{p}$.

But $L = \det(A) \cdot L = K \cdot \alpha_1 + \dots + K\alpha_m$,

as any elt of L has form $\frac{b}{a}$ with $b \in \mathcal{O}_L$, $a \in \mathcal{O}_K$

so elts of $\det(A) \cdot L$

have numerators in M, denoms. in $\mathcal{O}_K$.

For (b), use similar argument to before: Consider the chain

$\mathcal{O}_L \supset \mathfrak{P}_i \supset \mathfrak{P}_i^2 \supset \cdots \supset \mathfrak{P}_i^{e_i}$. We know $\mathcal{O}_L/\mathfrak{P}_i$ is f_i-dim'l vector space over $\mathcal{O}_K/\mathfrak{p}$; this is defn of f_i.

But there's no proper ideal between $\mathfrak{P}_i^j$ and $\mathfrak{P}_i^{j+1}$, so $\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ is 1-dim'l v.s. over $\mathcal{O}_L/\mathfrak{P}_i$, so also has dim'n f_i over $\mathcal{O}_K/\mathfrak{p}$.

Dividing through by $\mathfrak{P}_i^{e_i}$ and Adding it up for each successive quotient, we get $e_i f_i$ as degree of $\mathcal{O}_L/\mathfrak{P}^{e_i}$.

Proof of ~~Proposition~~ Main Thm: Suppose $\mathcal{O}_L = \mathcal{O}_K[\theta]$. ← the faliure of this will force finitely many exceptions. Then we claim

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \Big/ \bar{\phi}_\theta(x).$$

Indeed we have surjective map $\mathcal{O}_K[x] \longrightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \Big/ (\bar{\phi}_\theta(x))$

with kernel $\langle \mathfrak{p}, \phi_\theta(x) \rangle$, and

isomorphism follows since $\mathcal{O}_L = \mathcal{O}_K[\theta] \simeq \mathcal{O}_K[x]/(\phi_\theta(x))$

It is explicitly realized as $f(\theta) \longmapsto \bar{f}(x)$.

Given info about $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \Big/ \bar{\phi}_\theta(x)$: know $\bar{\phi}_\theta(x) = \bar{\phi}_1(x)^{e_1} \cdots \bar{\phi}_r(x)^{e_r}$

so C.R.T implies:

$$\underbrace{\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \Big/ (\bar{\phi}_\theta(x))}_{R} = \bigoplus_{i=1}^{r} \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K[x] \Big/ (\bar{\phi}_i(x)^{e_i})$$

so that prime ideals of R are the principal ideals gen'd by $\bar{\phi}_i(x)$ mod $\bar{\phi}_\theta(x)$. Moreover...