Recall:

$$\begin{tikzcd} A/\mathfrak{p} = k_{\mathfrak{p}} \arrow[d, hook] & A \arrow[l, two heads, "\mathfrak{p}\in\mathrm{Spec}(A)^*"'] \arrow[r, hook] \arrow[d, hook] & \mathbb{Q} \arrow[d, hook, "\text{fin.-sep.}"] \\ B/B.\mathfrak{p} & B \arrow[l, two heads] \arrow[r, hook] & K \end{tikzcd}$$

$B = \mathcal{O}_K(B)$

We have proven that:

> If A is a PID, then $[K:\mathbb{Q}] = \dim_{k_{\mathfrak{p}}}(B/B.\mathfrak{p})$

Now what if A is not a PID?

- We localize at $A-\mathfrak{p}$, i.e., we look at $A_{\mathfrak{p}} = \{\frac{a}{q} : a, q \in A, q \notin \mathfrak{p}\} \hookrightarrow \mathbb{Q}$.

- Note that

$$\begin{tikzcd} A \arrow[r, hook] \arrow[dr, dashed, "\overline{\pi}"'] & A_{\mathfrak{p}} \arrow[d, "\pi"] \\ & A_{\mathfrak{p}}/A_{\mathfrak{p}}\cdot\mathfrak{p} \end{tikzcd}$$

Recall the localisation of A at $\mathfrak{p}$:

$$A \hookrightarrow A_{\mathfrak{p}} = \left\{ \frac{a}{q} : a \in A, q \in A - \mathfrak{p} \right\} \subseteq Q$$

and $A_{\mathfrak{p}}$ is local with principal maximal ideal $\underline{m}_{\mathfrak{p}} = A_{\mathfrak{p}} \cdot \mathfrak{p} = (\pi)$. Moreover, if $\underline{a}_{\mathfrak{p}} \subsetneq A_{\mathfrak{p}}$ is an ideal, then there is $k \in \mathbb{N}$ s.t. $\underline{a}_{\mathfrak{p}} = \underline{m}_{\mathfrak{p}}^k$. In part., $A_{\mathfrak{p}}$ is PID. uniformizer

Remark: $\underline{m}_{\mathfrak{p}} = \left\{ \frac{a}{q} : a \in \mathfrak{p}, q \in A - \mathfrak{p} \right\}$.

Finally, $k_{\mathfrak{p}} = A/\mathfrak{p} \cong A_{\mathfrak{p}}/\underline{m}_{\mathfrak{p}} =: k_{\underline{m}_{\mathfrak{p}}}$.

Proposition:

$$\mathcal{O}_K(A_\mathfrak{p}) = \overbrace{\left\{\frac{b}{q} : b \in B, q \in A - \mathfrak{p}\right\}}^{=: B_\mathfrak{p}}.$$

Proof: "$\supseteq$" Let $\frac{b}{q} \in B_\mathfrak{p}$, then $b \in B \Rightarrow \exists a_0, \dots, a_{n-1} \in A$ s.t.

$$b^n + a_{n-1} b^{n-1} + \dots + a_0 = 0$$

and thus

$$\left(\frac{b}{q}\right)^n + \frac{a_{n-1}}{q}\left(\frac{b}{q}\right)^{n-1} + \dots + \frac{a_0}{q^n} = 0$$

implies $\frac{b}{q} \in \mathcal{O}_K(A_\mathfrak{p})$.

"$\subseteq$" Let $x \in \mathcal{O}_K(A_\mathfrak{p})$, i.e.

$$x^n + \frac{a_{n-1}}{q_{n-1}} x^{n-1} + \dots + \frac{a_0}{q_0} = 0,$$

then

$$b := q_0 \cdot \dots \cdot q_{n-1} \cdot x \in \mathcal{O}_K(A) = B \Rightarrow x = \frac{b}{q_0 \cdots q_{n-1}} \in B_\mathfrak{p}.$$

$\ulcorner$ Let $q := q_0 \cdots q_{n-1}$, then

$$b^n + \frac{q a_{n-1}}{q_{n-1}} b^{n-1} + \dots + \frac{q^n a_0}{q_0} = 0.$$

$\lrcorner$

$\blacksquare$

Corollary:

$B_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank $d = [K:\mathbb{Q}]$ and $[K:\mathbb{Q}] = \dim_{k_{\mathfrak{m}_{\mathfrak{p}}}} \left(B_{\mathfrak{p}} / B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}} \right)$.

Proposition:

$B / B.\mathfrak{p} \cong B_{\mathfrak{p}} / B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}}$ as $k_{\mathfrak{p}} \cong k_{\mathfrak{m}_{\mathfrak{p}}}$-algebras

Proof: $B.\mathfrak{p} \subseteq B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}} \Rightarrow$ we have a canonical homomorphism

$$B / B.\mathfrak{p} \longrightarrow B_{\mathfrak{p}} / B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}}.$$

of A-algebras and thus of $k_{\mathfrak{p}}$-algebras.

This map is onto. Indeed, let $b \in B$ and $q \in A - \mathfrak{p}$. Then q is invertible mod $\mathfrak{p}$ and thus there is $a \in A$ s.t. $a.q \equiv 1 \bmod \mathfrak{p}$. Then

$$\frac{a}{1} - \frac{1}{q} = \frac{a.q - 1}{q} \in \mathfrak{m}_{\mathfrak{p}} = \left\{ \frac{\alpha}{\gamma} : \alpha \in \mathfrak{p}, \gamma \in A - \mathfrak{p} \right\}$$

and thus

$$\frac{b}{q} \equiv \frac{b.a}{1} \bmod B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}},$$

i.e. $\frac{b}{q}$ is in the image of $B / B.\mathfrak{p}$.

It remains to prove injectivity, i.e.

$$B \cap B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}} = B \cdot \mathfrak{p}.$$

"$\supseteq$" is clear.

follows from descriptions of $B_{\mathfrak{p}}, \mathfrak{m}_{\mathfrak{p}}$.

"$\subseteq$" Let $b \in B$ and suppose $b \in B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}}$, i.e., $b = \frac{r}{q}$, where $r \in B \cdot \mathfrak{p}$, $q \in A - \mathfrak{p}$

$\Rightarrow q \cdot b \in B \cdot \mathfrak{p}$ for some $q \in A - \mathfrak{p}$.

$\Rightarrow b \in B \cdot \mathfrak{p}$: Suppose $\mathfrak{P} | \mathfrak{p}$, then $q \cdot b \in \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$. But $q \notin \mathfrak{P} \Rightarrow b \in \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$

$$\therefore b \in \bigcap_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}} = B \cdot \mathfrak{p}$$

∎

Ramification

We assume that Q is a number field, i.e. finite extension of $\mathbb{Q}$, $A = \mathcal{O}_Q(\mathbb{Z})$, and

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[d, hook] & Q \arrow[d, "\text{finite separable}"] \arrow[rr] & & \overline{\mathbb{Q}} \\
B = \mathcal{O}_K(A) \arrow[r, hook] & K \arrow[rru, hook] & &
\end{tikzcd}$$

We want to examine when $e_{\mathfrak{P}|\mathfrak{p}} > 1$. For this, we use the following notion:

Definition

Let S a ring. S is <u>reduced</u> if it has no non-trivial nilpotents, i.e.

$$\forall x \in S \quad (\exists n \in \mathbb{N} \; x^n = 0) \Rightarrow x = 0.$$

Definition

Let $\mathfrak{p} \in \mathrm{Spec}(A)^\times$: $\mathfrak{p}$ is <u>ramified in K</u> if $B/_{B \cdot \mathfrak{p}}$ is not reduced.

Otherwise <u>unramified</u>.

Remark: Let $x \in \mathfrak{P} - \mathfrak{P}^2$. Let $e > 1$, then $x^e \equiv 0 \bmod \mathfrak{P}^e$ but $x \not\equiv 0 \bmod \mathfrak{P}^e$. In particular, $B/_{\mathfrak{P}^e}$ is not reduced.

Proposition

$\mathfrak{p}$ is ramified $\Leftrightarrow \exists \mathfrak{P}|\mathfrak{p}$ s.t. $e_{\mathfrak{P}|\mathfrak{p}} > 1$.

Proof: $B/_{B.\mathfrak{p}} \cong \bigoplus_{\mathfrak{P}|\mathfrak{p}} B/_{\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}}$ $\qquad (x + B.\mathfrak{p} \longmapsto (x + \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}})_{\mathfrak{P}|\mathfrak{p}})$,

thus x is nilpotent in $B/_{B.\mathfrak{p}}$ iff it is nilpotent mod $\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$ for all $\mathfrak{P}|\mathfrak{p}$.

"$\Rightarrow$": If $e_{\mathfrak{P}|\mathfrak{p}} = 1$, then $B/_{\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}}$ is a field, thus zero is the only nilpotent. Therefore

$$\forall \mathfrak{P}|\mathfrak{p} \;\; e_{\mathfrak{P}|\mathfrak{p}} = 1 \implies B/_{B.\mathfrak{p}} \text{ is reduced}$$ (i.e. no non-zero nilpotent).

"$\Leftarrow$": If $\mathfrak{p}$ is unramified, then $B/_{\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}}$ is reduced for all $\mathfrak{P}|\mathfrak{p}$. Thus $e_{\mathfrak{P}|\mathfrak{p}} = 1$ for all $\mathfrak{P}|\mathfrak{p}$ by the remark.

$\blacksquare$

Definition: Let $\underline{z}=(z_1,\dots,z_d)\in B^d$, then

$$\mathrm{disc}_{K|\mathbb{Q}}(\underline{z}) := \det\left(\langle z_i, z_j\rangle_{K|\mathbb{Q}}\right) = \det\left(\mathrm{tr}_{K|\mathbb{Q}}(z_i z_j)\right) \in A.$$

Definition

$d=[K:\mathbb{Q}]$

$\mathfrak{D}_{B|A} := \langle \{\mathrm{disc}_{K|\mathbb{Q}}(\underline{z}) : \underline{z}\in B^d\}\rangle \lhd A$ is the discriminant ideal.

Remark: $\mathfrak{D}_{B|A} \neq \{0\}$. Indeed, $K|\mathbb{Q}$ separable $\Leftrightarrow \exists\, \underline{z}\in B^d$ s.t. $\mathrm{disc}_{K|\mathbb{Q}}(\underline{z})\neq 0$.

Theorem

$\mathfrak{p}\in \mathrm{Spec}(A)^\times$ ramified (in K) $\Leftrightarrow \mathfrak{p} \mid \mathfrak{D}_{B|A}$

Corollary:

$\{\mathfrak{p}$ ramified$\}$ is finite

Recall

$$\mathcal{D}_{B|A} = \langle \{ \mathrm{disc}_{K|Q}(z) : z \in B^{[K:Q]} \} \rangle$$

$$\begin{tikzcd}
\overset{\text{Dedekind}}{A} \arrow[r, hook] \arrow[d, hook] & \overset{\mathrm{Frac}(A)}{Q} \arrow[r, hook] \arrow[d, dash, "K|Q \text{ finite separable}"] & \overline{Q} \\
\mathcal{O}_K(A) = B \arrow[r, hook] & K \arrow[ur, hook] &
\end{tikzcd}$$

Theorem:

Suppose Q is a number field and $A = \mathcal{O}_Q(\mathbb{Z})$.
Let $\mathfrak{p} \in \mathrm{Spec}(A)^{\times}$. The following are equivalent:

(i) $\mathfrak{p} | \mathcal{D}_{B|A}$.

(ii) $\mathfrak{p}$ is ramified.

In particular, the set of ramified primes is finite.

Remark: • The equivalence holds in greater generality, i.e., whenever $k_{\mathfrak{P}}|k_{\mathfrak{p}}$ is separable.
• (ii) ⇒ (i) whenever A is Dedekind.

Exercise: $\mathcal{D}_{B|A,\mathfrak{p}} = \mathcal{D}_{B_{\mathfrak{p}}|A_{\mathfrak{p}}}$.

$$\mathcal{D}_{B|A,\mathfrak{p}} \overset{\text{def}}{=} (A-\mathfrak{p})^{-1}\mathcal{D}_{B|A} \trianglelefteq A_{\mathfrak{p}}$$

Proposition:

Suppose A is a PID and let $z=(z_1,\dots,z_d)\in B^d$ an A-basis of B. Then
$$\mathcal{D}_{B|A}=(\operatorname{disc}(z)).$$

Proof: Let $(z_1',\dots,z_d')\in B^d$, then z_i' is an A-linear combination of $(z_1,\dots,z_d)$.

Thus there is $M\in \operatorname{Mat}_d(A)$ s.t.
$$\operatorname{disc}(z')=(\det M)^2\operatorname{disc}(z)\in(\operatorname{disc}(z)).$$

$$\ulcorner\ z_i'=\sum_{j=1}^{d}a_{ij}z_j \Rightarrow M=(a_{ij})_{i,j}\ \lrcorner$$

Remark: If $A=\mathbb{Z}$, then $\operatorname{disc}(z)$ is independent of the choice of the basis.

Indeed, in this $M\in GL_d(\mathbb{Z})$ and thus $(\det M)^2=1$.