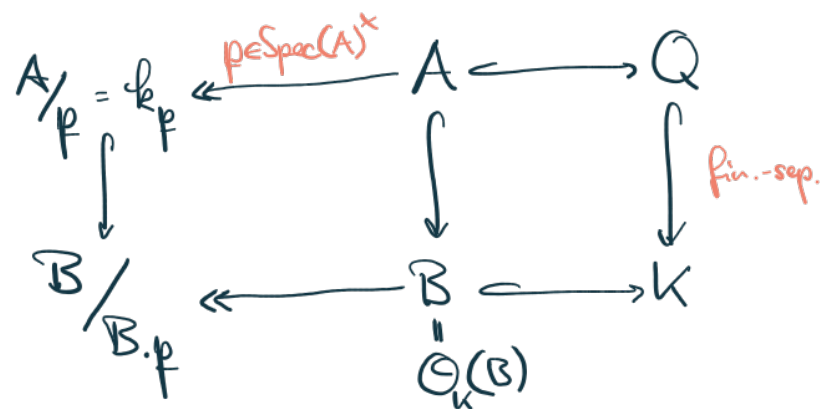


Recall:

I



We have proven that:

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

Now what if A is not a PID?

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

• Note that

$$\begin{array}{ccc}
 A & \hookrightarrow & A_p \\
 & \searrow \overline{\pi} & \downarrow \pi \\
 & & A_p/A_p.p
 \end{array}$$

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

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

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

Proposition:

$=: \mathbb{B}_p$

$$\mathcal{O}_K(A_p) = \left\{ \frac{b}{q} : b \in \mathbb{B}, q \in A - p \right\}.$$

Proof: " $\supseteq$ " Let $\frac{b}{q} \in \mathbb{B}_p$, then $b \in \mathbb{B} \Rightarrow \exists a_0, \dots, a_{n-1} \in A$ 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 $\frac{b}{q} \in \mathcal{O}_K(A_p)$.

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

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

then

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

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

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

┘

Corollary:

B_p is a free A_p -module of rank $d = [K:Q]$ and $[K:Q] = \dim_{k_p} (B_p / B_p \cdot \mathfrak{m}_p)$. IV

Proposition:

$B / B_p \cong B_p / B_p \cdot \mathfrak{m}_p$ as $k_p \cong k_{\mathfrak{m}_p}$ -algebras

Proof: $B_p \subseteq B_p \cdot \mathfrak{m}_p \Rightarrow$ we have a canonical homomorphism

$$B / B_p \longrightarrow B_p / B_p \cdot \mathfrak{m}_p.$$

of A -algebras and thus of k_p -algebras.

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

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

and thus

$$\frac{b}{q} \equiv \frac{b \cdot a}{1} \pmod{B_p \cdot \mathfrak{m}_p},$$

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

It remains to prove injectivity, i.e.

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

" $\supseteq$ " is clear.

" $\subseteq$ " Let $b \in B$ and suppose $b \in B_{p \cdot \mathfrak{m}_p}$, 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 $\mathfrak{p} \nmid q$, then $q \cdot b \in \mathfrak{p}^e \mathfrak{p}$. But $q \notin \mathfrak{p} \Rightarrow b \in \mathfrak{p}^e \mathfrak{p}$

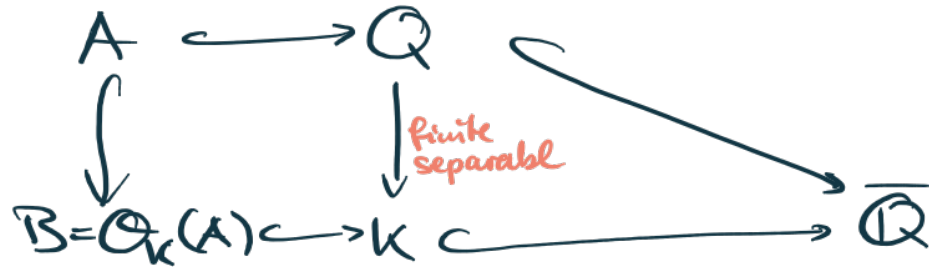
$$\therefore b \in \bigcap_{\mathfrak{p} \nmid q} \mathfrak{p}^e \mathfrak{p} = B \cdot \mathfrak{p}$$

follows from description
of $B_{p \cdot \mathfrak{m}_p}$.



Ramification

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



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 reduced 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 $\mathfrak{p} \in \text{Spec}(A)^{\times}$: $\mathfrak{p}$ is ramified in K if $B/B_{\mathfrak{p}}$ is not reduced.

Otherwise unramified.

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

Proposition

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

Proof: $B/B.p \cong \bigoplus_{\beta | p} B/\beta^{e_{\beta | p}}$

$(x + B.p \mapsto (x + \beta^{e_{\beta | p}})_{\beta | p}),$

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

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

$\forall \beta | p \ e_{\beta | p} = 1 \Rightarrow B/B.p$ is reduced (i.e. no non-zero nilpotent).

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



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

$$\text{disc}_{K/Q}(\underline{z}) := \det(\langle z_i, z_j \rangle_{K/Q}) = \det(\text{tr}_{K/Q}(z_i z_j)) \in A.$$

Definition

$$d = [K:Q]$$

$\mathcal{D}_{B/A} := \langle \{\text{disc}_{K/Q}(\underline{z}) : \underline{z} \in B^d\} \rangle \triangleleft A$ is the discriminant ideal.

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

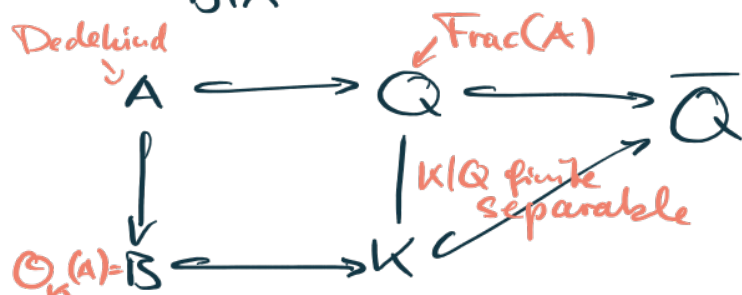
Theorem

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

Corollary:

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

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



Theorem:

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

- (i) $\mathfrak{p} \mid \mathcal{D}_{B/A}$.
- (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) $\Rightarrow$ (i) whenever A is Dedekind.

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

ii
 $(A - \mathfrak{p})^{-1} \mathcal{D}_{B/A} \triangleleft A_{\mathfrak{p}}$

Proposition:

Suppose A is a PID and let $z = (z_1, \dots, z_d) \in B^d$ an A -basis of B . Then

$$\mathcal{D}_{B/A} = (\text{disc}(z)).$$

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 $M \in \text{Mat}_d(A)$ s.t.

$$\text{disc}(z') = (\det M)^2 \text{disc}(z) \in (\text{disc}(z)).$$

$$\lceil z'_i = \sum_{j=1}^d a_{ij} z_j \Rightarrow M = (a_{ij})_{i,j} \rfloor$$

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

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