Recall

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, hook] \arrow[d, hook] & A = \mathcal{O}_Q(\mathbb{Z}) \arrow[r, hook] \arrow[d, hook] & B = \mathcal{O}_K(A) \arrow[d, hook] & \\
\mathbb{Q} \arrow[r, hook, "\text{fin.}"'] & Q = \mathrm{Frac}(A) \arrow[r, hook, "\text{fin.}"'] & K \arrow[r, hook] & \overline{\mathbb{Q}} \subseteq \mathbb{C}
\end{tikzcd}$$

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

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

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

In particular, the set of ramified primes is finite.

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

$$\begin{array}{c} \| \\ (A-\mathfrak{p})^{-1}\mathcal{D}_{B|A} \triangleleft A_{\mathfrak{p}} \end{array}$$

Proof of the theorem

(ii) ⇒ (i): Suppose $\mathfrak{p}$ is ramified, i.e., $B/B\mathfrak{p} \cong B_\mathfrak{p}/B_\mathfrak{p}\cdot\mathfrak{m}_\mathfrak{p}$ is non-reduced.

Let $K_\mathfrak{p} = B_\mathfrak{p}/B_\mathfrak{p}\cdot\mathfrak{m}_\mathfrak{p}$. Define $[\![x\,\cdot]\!] : K_\mathfrak{p} \longrightarrow \mathrm{End}_{k_\mathfrak{p}}(K_\mathfrak{p})$ by

$$\forall z, \xi \in K_\mathfrak{p} \quad [\![x z]\!](\xi) = z\xi.$$

As usual, this induces the $k_\mathfrak{p}$-bilinear trace-pairing $\langle z, \xi\rangle := \mathrm{tr}[\![x z\xi]\!]$. We let $\mathrm{disc} : K_\mathfrak{p}^d \longrightarrow k_\mathfrak{p}$ the induce discriminant, i.e.,

$d = [K:\mathbb{Q}]$
$= \dim_{k_\mathfrak{p}}(K_\mathfrak{p})$
by deg. formula

$$\forall \xi = (\xi_1, \dots, \xi_d) \in K_\mathfrak{p}^d \qquad \mathrm{disc}(\xi_1, \dots, \xi_d) = \det\left(\mathrm{tr}[\![x \xi_i \cdot \xi_j]\!]\right).$$

As $K_\mathfrak{p}$ is non-reduced, $\mathrm{disc}_{K_\mathfrak{p}|k_\mathfrak{p}} \equiv 0$ (exercise).

Recall that $B_\mathfrak{p}$ is $A_\mathfrak{p}$-free of rank $d = [K:\mathbb{Q}]$, as $\mathcal{O}_K(A_\mathfrak{p}) = B_\mathfrak{p}$ and $A_\mathfrak{p}$ is a PID.

Therefore, for $z \in B_\mathfrak{p}$, $\mathrm{tr}[x z]_{K|\mathbb{Q}} \in A_\mathfrak{p}$.

Claim Let $z \in B_{\mathfrak{p}}$ and $\bar{z} = z \bmod B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}}$, then

$$\operatorname{tr} [\![\times \bar{z}]\!] = \operatorname{tr}(z)_{K|\mathbb{Q}} \bmod \mathfrak{m}_{\mathfrak{p}}. \quad (\star)$$

In particular, letting $z_1, \dots, z_d \in B_{\mathfrak{p}}$ and $\bar{z}_i = z_i \bmod B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}}$, we have that

$$\operatorname{disc}(\bar{z}_1, \dots, \bar{z}_d) = \underbrace{\operatorname{disc}_{K|\mathbb{Q}}(z_1, \dots, z_d)}_{\in A_{\mathfrak{p}}} \bmod \mathfrak{m}_{\mathfrak{p}}$$

Note that for all $y \in B_{\mathfrak{p}}$ we have

$$[\![\times \bar{z}]\!] (\bar{y}) = \bar{z} \cdot \bar{y} = [\times z]_{K|\mathbb{Q}}(y) \bmod B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}} \quad (*)$$

and that for $z \in B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}}$ we have

$$[\times z]_{K|\mathbb{Q}}(y) \in B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}}.$$

Fix an $A_{\mathfrak{p}}$-basis $\mathcal{B} = (z_1, \dots, z_d) \in B_{\mathfrak{p}}^d$ of $B_{\mathfrak{p}}$, then

$$[\times z]_{K|\mathbb{Q}, \mathcal{B}} \in \operatorname{Mat}_d(A_{\mathfrak{p}}) \quad ([\times z]_{K|\mathbb{Q}, \mathcal{B}}(\underbrace{B_{\mathfrak{p}}}_{\cong A_{\mathfrak{p}}^d}) \subseteq B_{\mathfrak{p}})$$

Note that, if $z \in B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}}$, then

$$[\times z]_{K|\mathbb{Q}}(B_{\mathfrak{p}}) \subseteq B_{\mathfrak{p}} \cdot \mathfrak{m}_{\mathfrak{p}} = \pi \cdot B_{\mathfrak{p}}, \text{ where } \pi \in A_{\mathfrak{p}} \text{ is a uniformizer.}$$

In particular,

$$[\times z]_{K|\mathbb{Q}, \mathcal{B}} \in \operatorname{Mat}_d(\mathfrak{m}_{\mathfrak{p}}) \quad (**).$$

IV

With $\mathbb{B}$ as above, let $\overline{\mathbb{B}} = (\bar{z}_1, \dots, \bar{z}_d)$ and recall that $\overline{\mathbb{B}}$ is a $k_{\mathfrak{p}}$-basis of $K_{\mathfrak{p}}$.

Using (✱) and (✱✱), it follows that for all $z \in B_{\mathfrak{p}}$

$$[\![x\bar{z}]\!]_{\overline{\mathbb{B}}} = [xz]_{K|\mathbb{Q},\mathbb{B}} \mod \mathfrak{m}_{\mathfrak{p}}.$$

Hence

$$\operatorname{tr} [\![x\bar{z}]\!] = \operatorname{tr}(z) \mod \mathfrak{m}_{\mathfrak{p}},$$

which proves the first part of the claim (the second part follows from the fact that the canonical projection mod $\mathfrak{m}_{\mathfrak{p}}$ is a ring homomorphism).

Using the claim (☆) and degeneracy of the trace bilinear form on $K_{\mathfrak{p}}|k_{\mathfrak{p}}$, it follows that

$$\forall\ z_1, \dots, z_d \in B_{\mathfrak{p}}^d \qquad \operatorname{disc}_{K|\mathbb{Q}}(z_1, \dots, z_d) \in \mathfrak{m}_{\mathfrak{p}}$$

and therefore

$$\mathfrak{m}_{\mathfrak{p}} \mid \mathfrak{D}_{B_{\mathfrak{p}}|A_{\mathfrak{p}}} \underset{\substack{\uparrow \\ \text{exercise}}}{=} \mathfrak{D}_{B|A, \mathfrak{p}}.$$

In particular, $\mathfrak{p} \mid \mathfrak{D}_{B|A}$ ← cf. Sheet 8.

V

(i) ⇒ (ii): Suppose $\mathfrak{p} \mid \mathfrak{D}_{B|A}$. We want to show that $K_{\mathfrak{p}} = B/B\cdot\mathfrak{p}$ is not reduced.

$$\mathfrak{m}_{\mathfrak{p}} \mid \mathfrak{D}_{B_{\mathfrak{p}}|A_{\mathfrak{p}}} \Rightarrow \forall z_1,\dots,z_d \in B_{\mathfrak{p}} \quad \mathrm{disc}_{K|\mathbb{Q}}(z_1,\dots,z_d) \in \mathfrak{m}_{\mathfrak{p}}$$

$$\Rightarrow \forall z_1,\dots,z_d \in B_{\mathfrak{p}} \quad \mathrm{disc}(\bar{z}_1,\dots,\bar{z}_d) = 0 \quad (\text{in } k_{\mathfrak{m}_{\mathfrak{p}}}).$$

But

$$K_{\mathfrak{p}} \cong \bigoplus_{\mathfrak{P}\mid\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}} \qquad (\text{as a } k_{\mathfrak{p}}\text{-algebra})$$

and thus

$$\mathrm{disc} = \prod_{\mathfrak{P}\mid\mathfrak{p}} \mathrm{disc}_{B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}} \quad (***).$$

⌈ (***) Suppose $F: V \longrightarrow V$ is an endomorphism, $V = \bigoplus_i V_i$ an F-invariant decomposition, then

$$\mathrm{tr}(F) = \sum_i \mathrm{tr}(F|_{V_i}).$$

Hence

$$\forall z_i, z_j \quad \langle z_i, z_j\rangle_{K_{\mathfrak{p}}|k_{\mathfrak{p}}} = \sum_{\mathfrak{P}\mid\mathfrak{p}} \langle z_i, z_j\rangle_{B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}|k_{\mathfrak{p}}}$$

i.e. $K_{\mathfrak{p}}|k_{\mathfrak{p}}$ is an orthogonal sum of the trace bilinear forms. In particular, there is a basis such that the representation matrix of $\langle\cdot,\cdot\rangle_{K_{\mathfrak{p}}|k_{\mathfrak{p}}}$ is block-diagonal and the diagonals are representation matrices of $\langle\cdot,\cdot\rangle_{B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}|k_{\mathfrak{p}}}$.

⌋

It follows that there are an $A_\mathfrak{p}$-basis $(z_1,\dots,z_d)$ of $B_\mathfrak{p}$ and some $\mathfrak{P}|\mathfrak{p}$ such that

$$\mathrm{disc}_{B_\mathfrak{p}/B_\mathfrak{p}\cdot\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}|k_\mathfrak{p}}(\overline{z_1}^{\mathfrak{P}},\dots,\overline{z_d}^{\mathfrak{P}})=0.$$

Claim: Let $\mathfrak{P}|\mathfrak{p}$ and suppose that $1\leq e\leq e_{\mathfrak{P}|\mathfrak{p}}$, then

$$B/\mathfrak{P}^e \cong B_\mathfrak{p}/B_\mathfrak{p}\cdot\mathfrak{P}^e \qquad (****)$$

as $k_\mathfrak{p}$-algebras.

Proof of $(****)$:

$$\mathfrak{P}^e\subseteq B_\mathfrak{p}\cdot\mathfrak{P}^e \Rightarrow \begin{array}{ccc} B & \longrightarrow & B_\mathfrak{p} \\ \downarrow & & \downarrow \\ B/\mathfrak{P}^e & \xrightarrow[\psi]{} & B_\mathfrak{p}/B_\mathfrak{p}\cdot\mathfrak{P}^e \end{array}$$

The proof that ψ is bijective is essentially the same as the proof of $B/B\cdot\mathfrak{p}\cong B_\mathfrak{p}/B_\mathfrak{p}\cdot\mathfrak{m}_\mathfrak{p}$.

$\ulcorner$ ψ onto: Denote $S=A-\mathfrak{p}$ and let $b\in B$, $q\in S$. Let $a\in A$ s.t. $a\cdot q\equiv 1 \mod \mathfrak{p}$, hence

$$\frac{a}{1}-\frac{1}{q}\in S^{-1}\mathfrak{p}=S^{-1}(A\cap\mathfrak{P}^e)\subseteq S^{-1}\cdot\mathfrak{P}^e=B_\mathfrak{p}\cdot\mathfrak{P}^e,$$

i.e., $\frac{b}{q}\equiv\frac{ba}{1} \mod B_\mathfrak{p}\cdot\mathfrak{P}^e$.

<u>φ injective:</u> We need to prove $\mathfrak{P}^e = B \cap B_{\mathfrak{p}} \cdot \mathfrak{P}^e$.

"$\subseteq$" is clear

"$\supseteq$" Let $b \in B$ and suppose $b \in B_{\mathfrak{p}} \cdot \mathfrak{P}^e = S^{-1}\mathfrak{P}^e$. Hence $b = \frac{r}{q}$, where $r \in \mathfrak{P}^e$ and $q \in S$. In particular, $q \cdot r \in \mathfrak{P}^e$ and thus

$$\mathfrak{P}^e \mid (q)\cdot(r),$$

i.e.

$$e \le v_{\mathfrak{P}}((q)\cdot(r)) = v_{\mathfrak{P}}((q)) + v_{\mathfrak{P}}((r)) \overset{q \in A-\mathfrak{p}}{=} v_{\mathfrak{P}}((r)).$$

Hence $r \in \mathfrak{P}^e$ and thus $b = \frac{r}{q} \in B_{\mathfrak{p}} \cdot \mathfrak{P}^e$.

⌟

But $(\bar{z}_1^{\mathfrak{P}}, \dots, \bar{z}_d^{\mathfrak{P}})$ is a $k_{\mathfrak{p}}$-basis of $B_{\mathfrak{p}} / B_{\mathfrak{p}} \cdot \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}} \cong B / \mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$. Hence $B/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$ is

since disc vanishes identically

<u>not</u> separable over $k_{\mathfrak{p}}$. If $e_{\mathfrak{P}|\mathfrak{p}} = 1$, then $k_{\mathfrak{P}} = B/\mathfrak{P}$ is a finite extension of $k_{\mathfrak{p}}$ and therefore separable. It follows that $e_{\mathfrak{P}|\mathfrak{p}} > 1$ and thus $K_{\mathfrak{p}}$ is <u>not</u> reduced.

finite, since A is $\mathbb{Z}$-f.g. and $\mathbb{Z}/\mathbb{Z}\cap\mathfrak{p}$ is finite.

Galois extensions

We are going to study Galois extensions $K|\mathbb{Q}$ where K and $\mathbb{Q}$ are number fields. E.g. $[K:\mathbb{Q}]=2$.

Definition

A finite extension $K|\mathbb{Q}$ is Galois if $\forall z\in K$ $[\times z]_{K|\mathbb{Q}}$ is diagonalizable over K.

Proposition

Let $K|\mathbb{Q}$ finite. T.f.a.e.

(i) $K|\mathbb{Q}$ is Galois

(ii) $|\mathrm{Hom}_{\mathbb{Q}}(K,K)|=[K:\mathbb{Q}]$

Remark: $K|\mathbb{Q}$ is normal if $\mathrm{Hom}_{\mathbb{Q}}(K,K)=\mathrm{Hom}_{\mathbb{Q}}(K,\overline{\mathbb{Q}})$. Thus $K|\mathbb{Q}$ Galois iff $K|\mathbb{Q}$ is separable and normal.

Definition:

$\mathrm{Gal}(K|\mathbb{Q})=(\mathrm{Hom}_{\mathbb{Q}}(K,K),\mathrm{id}_K,\circ)$

For Galois extensions, we obtain additional information, e.g., the parameters $e_{\mathfrak{P}|p}$ and $f_{\mathfrak{P}|p}$ are independent of the prime $\mathfrak{P}|p$.

Proof of the proposition:

"$\Rightarrow$" $K|\mathbb{Q}$ Galois $\Rightarrow K|\mathbb{Q}$ separable $\Rightarrow K = \mathbb{Q}(z)$ for some $z \in K$. In particular, every embedding of K in $\overline{\mathbb{Q}}$ is completely determined by the image of z. Let $\mathbb{Q} \subset L \subset \overline{\mathbb{Q}}$. $z \mapsto \varphi(z) \in L$ extends to a $\mathbb{Q}$-linear $K \hookrightarrow L$ iff $\varphi(z)$ is a root of $\min_{\mathbb{Q}}(z)$.

As z is a primitive element, we have

$$\mathrm{char}_{K|\mathbb{Q}}(z) = \min_{\mathbb{Q}}(z)$$

and thus diagonalizability over K implies that all the roots of $\min_{\mathbb{Q}}(z)$ lie in K. Thus

$$\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}) = \mathrm{id}_{K \hookrightarrow \overline{\mathbb{Q}}} \circ \mathrm{Hom}_{\mathbb{Q}}(K, K).$$

$K|\mathbb{Q}$ separable $\Leftrightarrow |\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})| = [K:\mathbb{Q}]$.

"$\Leftarrow$" $[K:\mathbb{Q}] = |\mathrm{Hom}_{\mathbb{Q}}(K,K)| \leq |\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})| \leq [K:\mathbb{Q}]$

$\rightarrow K|\mathbb{Q}$ is separable.

$\Rightarrow \forall z \in K$ $[xz]_{K|\mathbb{Q}}$ is diagonalizable over $\overline{\mathbb{Q}}$ and the roots of $\mathrm{char}_{K|\mathbb{Q}}(z)$ are exactly the roots of $\min_{\mathbb{Q}}(z)$ (with multiplicity $[K:\mathbb{Q}(z)]$).

The roots of $\min_{\mathbb{Q}}(z)$ are the images of z under $\mathbb{Q}$-embeddings of $\mathbb{Q}(z)$ in $\overline{\mathbb{Q}}$. Any such embedding extends to an embedding of K in $\overline{\mathbb{Q}}$ and thus by hypothesis has image contained in K. Therefore $[xz]_{K|\mathbb{Q}}$ diagonalizable over K.

$\boxtimes$

Lemma:

$K|\mathbb{Q}$ Galois, $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$, then $\sigma(\mathcal{O}_K(A)) = \mathcal{O}_K(A)$.

Pf: As σ is arbitrary, it suffices to show the inclusion $\sigma(\mathcal{O}_K(A)) \subseteq \mathcal{O}_K(A)$.

Let $b \in \mathcal{O}_K(A)$, $P \in A[X]$ monic s.t. $P(b) = 0$. Then $P(\sigma(b)) = \sigma(P(b)) = 0$. ∎

Lemma:

Let $\mathfrak{p} \in \mathrm{Spec}(A)^\times$, $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$, then $\sigma(\mathrm{Spec}_\mathfrak{p}(B)) = \mathrm{Spec}_\mathfrak{p}(B)$.

Pf: Again, we only need to show inclusion. Given $\mathfrak{P} \in \mathrm{Spec}_\mathfrak{p}(B)$, $\sigma\mathfrak{P} \triangleleft B$ is prime, as

$$B/_{\sigma\mathfrak{P}} = \sigma B/_{\sigma\mathfrak{P}} \cong B/_{\mathfrak{P}}$$

is a field.

Moreover, $A \cap \sigma\mathfrak{P} = \sigma(A \cap \mathfrak{P}) = \sigma(\mathfrak{p}) = \mathfrak{p}$. ∎

Corollary:

$\mathrm{Gal}(K|\mathbb{Q}) \curvearrowright \mathrm{Spec}_\mathfrak{p}(B)$

Theorem:

$\mathrm{Gal}(K|\mathbb{Q}) \curvearrowright \mathrm{Spec}_p(B)$ is transitive

$\mathfrak{P} \neq \mathfrak{P}'$

$\Uparrow$

Proof: We give a proof by contradiction. Suppose $\mathfrak{P}, \mathfrak{P}'$ lie above p and $\sigma(\mathfrak{P}') \neq \mathfrak{P}$ for all $\sigma \in \mathrm{Gal}$.

Let $\mathcal{J} = \{\sigma(\mathfrak{P}') : \sigma \in \mathrm{Gal}\} \subseteq \mathrm{Spec}_p(B)$. By CRT, there is $z \in B$ such that

$$z \equiv \begin{cases} 1 \mod \mathfrak{a} \in \mathcal{J}, \\ 0 \mod \mathfrak{P} \ . \end{cases}$$

$\mathfrak{P} \subseteq B \Rightarrow \mathfrak{P} \cap \mathbb{Q} = \mathfrak{P} \cap A$

Then $$N_{K|\mathbb{Q}}(z) = \prod_{\sigma \in \mathrm{Gal}} \sigma(z) = z \prod_{\sigma \neq \mathrm{id}_K} \sigma(z) \in \mathfrak{P} \cap \mathbb{Q} = p.$$

As $z \notin \sigma(\mathfrak{P}')$ for all $\sigma \in \mathrm{Gal}$, we know that $\sigma z \notin \mathfrak{P}'$ for all $\sigma \in \mathrm{Gal}$, thus

$$N_{K|\mathbb{Q}}(z) \notin \mathfrak{P}' \cap \mathbb{Q} = p \quad \lightning$$

$\blacksquare$

Definition

Let $\mathfrak{P} \in \mathrm{Spec}(B)$. The decomposition group of $\mathfrak{P}$ is

$$D_{\mathfrak{P}} := \mathrm{Stab}_G(\mathfrak{P})$$

Remarks: · Let $\mathfrak{P}, \mathfrak{P}'$ primes above $p \in \mathrm{Spec}(A)^{\times}$, then $D_{\mathfrak{P}}$ and $D_{\mathfrak{P}'}$ are conjugate in G:

$$\mathfrak{P}' = \sigma(\mathfrak{P}) \quad \text{for some } \sigma \in G.$$

$$\cdot\ |D_{\mathfrak{P}}| = \frac{[K:\mathbb{Q}]}{|\mathrm{Spec}_{A\cap\mathfrak{P}}(B)|} = e_p \cdot f_p \ : \ |\mathrm{Spec}_{A\cap\mathfrak{P}}(B)| = \left| G/D_{\mathfrak{P}} \right|$$

constant in $\mathfrak{P}$ (exercise)

$\Rightarrow [K:\mathbb{Q}] = e \cdot f \cdot |\mathrm{Spec}_p(\mathfrak{P})|$

Definition

Let $\mathfrak{P} \in \mathrm{Spec}(B)^{\times}$. The decomposition field $Z_{\mathfrak{P}}$ of $\mathfrak{P}$ is the fixed field of $D_{\mathfrak{P}}$, i.e.,

$$Z_{\mathfrak{P}} = \{x \in K : \forall \sigma \in D_{\mathfrak{P}} \ \sigma x = x\}$$

Exercise: (i) $D_{\mathfrak{P}} = \{1\} \Leftrightarrow Z_{\mathfrak{P}} = K \Leftrightarrow p$ is unramified (i.e. $e_p = 1$)

(ii) $D_{\mathfrak{P}} = G \Leftrightarrow Z_{\mathfrak{P}} = \mathbb{Q} \Leftrightarrow p$ is totally ramified (i.e. $|\mathrm{Spec}_p(B)| = 1$)

Remark: $\mathrm{Gal}(K|Z_{\mathfrak{P}}) = D_{\mathfrak{P}}$