Recap of the situation:

$G = \mathrm{Gal}(K|Q) = \mathrm{Hom}_Q(K,K)$

$$
\begin{tikzcd}
\overline{\mathbb{Q}} & & \\
\mathbb{Q} \arrow[u] \arrow[r, hook, "\text{finite}"'] & \overset{\mathrm{Frac}(A)}{\overset{\shortparallel}{Q}} \arrow[ul] \arrow[r, hook, "\text{finite}", "\text{Galois}"'] & K \arrow[ull] \\
\mathbb{Z} \arrow[u] \arrow[r, hook] & A = \mathcal{O}_Q(\mathbb{Z}) \arrow[u] \arrow[r, hook] & B = \mathcal{O}_K(A) \arrow[u]
\end{tikzcd}
$$

We have seen that for $\mathfrak{p} \in \mathrm{Spec}(A)$,

$$\boxed{\begin{array}{c} G \circlearrowright \mathrm{Spec}(B) \text{ by } \sigma.\mathfrak{P} := \sigma(\mathfrak{P}) \text{ and} \\ \text{for each } \mathfrak{P} \in \mathrm{Spec}(B) \quad G.\mathfrak{P} = \mathrm{Spec}_{A\cap\mathfrak{P}}(B). \end{array}}$$

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

$$Z_{\mathfrak{P}} = K^{D_{\mathfrak{P}}} := \{x \in K : \forall \sigma \in D_{\mathfrak{P}} \ \ \sigma x = x\}$$ $(K/Z_{\mathfrak{P}}$ is Galois, $\mathrm{Gal}(K/Z_{\mathfrak{P}}) = D_{\mathfrak{P}})$

<u>Note</u>: $[K : Z_{\mathfrak{P}}] = |D_{\mathfrak{P}}| = e_{\mathfrak{p}} \cdot f_{\mathfrak{p}}$.

Theorem:

Let $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$ (the contraction of $\mathfrak{P}$ to $Z_{\mathfrak{P}}$), $\mathfrak{p} = \mathfrak{P} \cap A$.

(i) $\mathfrak{P}_Z$ is totally ramified in K (i.e. $|\mathrm{Spec}_{\mathfrak{P}_Z}(B)| = 1$)

(ii) $e_{\mathfrak{P}_Z} = e_{\mathfrak{p}}$, $f_{\mathfrak{P}_Z} = f_{\mathfrak{p}}$ $\quad$ ($e_{\mathfrak{P}_Z} = e_{\mathfrak{P}|\mathfrak{P}_Z}$, $e_{\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{p}}$)

(iii) $\mathfrak{p} = \mathfrak{P}_Z \cap A$ and $e_{\mathfrak{P}_Z|\mathfrak{p}} = f_{\mathfrak{P}_Z|\mathfrak{p}} = 1$

<u>Proof</u>: (i) $\mathfrak{P}'$ a prime above $\mathfrak{P}_Z \Rightarrow \mathfrak{P}' = \sigma\mathfrak{P}$ for some $\sigma \in D_{\mathfrak{P}} \Rightarrow \mathfrak{P}' = \mathfrak{P}$

$\mathrm{Gal}(K/Z_{\mathfrak{P}}) = D_{\mathfrak{P}}$ $\qquad$ $\sigma\mathfrak{P} = \mathfrak{P}$

(ii) $e_{\mathfrak{p}} \cdot f_{\mathfrak{p}} = |D_{\mathfrak{P}}| = [K : Z_{\mathfrak{P}}] \overset{(i)}{=} e_{\mathfrak{P}_Z} \cdot f_{\mathfrak{P}_Z}$.

Using $\mathfrak{p} = \mathfrak{P}_Z \cap A$ ($\mathfrak{P}_Z \cap A \lhd A$ being a prime contained in $\mathfrak{p}$), one checks

$$e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{P}_Z} \cdot e_{\mathfrak{P}_Z|\mathfrak{p}} \quad (*)$$

$$f_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{P}_Z} \cdot f_{\mathfrak{P}_Z|\mathfrak{p}} \quad (**)$$

Exercise

$$\Rightarrow e_{\mathfrak{P}_Z} \cdot f_{\mathfrak{P}_Z} = e_{\mathfrak{p}} \cdot f_{\mathfrak{p}} \overset{(**)}{=} e_{\mathfrak{p}} \cdot a f_{\mathfrak{P}_Z} \quad \text{for some } a \in \mathbb{N}$$

$$\Rightarrow e_{\mathfrak{P}_Z} = e_{\mathfrak{p}} \cdot a \geq e_{\mathfrak{p}} \overset{(*)}{\geq} e_{\mathfrak{P}_Z}$$

(iii) The first part was discussed for (ii). For the second part, note that (ii) and (**) imply $f_{\mathfrak{P}_Z|\mathfrak{p}} = 1$ and (*) implies $1 \leq e_{\mathfrak{P}_Z|\mathfrak{p}} \leq \frac{e_{\mathfrak{p}}}{e_{\mathfrak{P}_Z}} = 1$

Remark: $\sigma \in D_{\mathfrak{P}} \Rightarrow$

$$\begin{tikzcd} B \arrow[r, "\sigma"] \arrow[d, "\pi"'] & B \arrow[d, "\pi"] \\ k_{\mathfrak{P}} \arrow[r, dashed, "\exists! \bar{\sigma}"'] & B/\mathfrak{P} = k_{\mathfrak{P}} \end{tikzcd}$$

and $\bar{\sigma}$ is an A-module hom, i.e., $k_{\mathfrak{p}}$-linear.

We define $\bullet_{\mathfrak{P}} : D_{\mathfrak{P}} \longrightarrow \mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, k_{\mathfrak{P}})$, $\sigma_{\mathfrak{P}} := \bar{\sigma}$.

Note: $(\sigma \circ \tau)_{\mathfrak{P}} = \sigma_{\mathfrak{P}} \circ \tau_{\mathfrak{P}}$ (i.e., group hom)

Definition:

The inertia group at $\mathfrak{P} \in \mathrm{Spec}(B)^{\times}$ is $I_{\mathfrak{P}} := \ker(\bullet_{\mathfrak{P}}) \lhd D_{\mathfrak{P}}$

Exercise:

Let $\mathfrak{P}, \mathfrak{P}' \in \mathrm{Spec}_{\mathfrak{p}}(B)$, then $I_{\mathfrak{P}}, I_{\mathfrak{P}'}$ are conjugate in G.

Theorem

Let $\mathfrak{p} \in \mathrm{Spec}(A)$ non-zero, $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$, then

(i) $k_{\mathfrak{P}} | k_{\mathfrak{p}}$ is Galois

(ii) $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \cong D_{\mathfrak{P}}/I_{\mathfrak{P}}$

(iii) $|I_{\mathfrak{P}}| = e_{\mathfrak{p}}$

Proof: (i) $k_{\mathfrak{P}}$ is a finite extension of $k_{\mathfrak{p}}$, which is a finite extension of $k_{\mathfrak{p} \cap \mathbb{Z}} \cong \mathbb{F}_p$. Thus $k_{\mathfrak{P}}$ is a finite extension of $\mathbb{F}_p$, hence Galois (splitting field of $X^{|k_{\mathfrak{P}}|} - 1$).

$$\begin{tikzcd} \mathbb{F}_p \arrow[r, hook] \arrow[rr, bend right, "\text{Galois}"'] & k_{\mathfrak{p}} \arrow[r, hook, "\text{Galois}"'] & k_{\mathfrak{P}} \end{tikzcd}$$

Pf: $k_{\mathfrak{p}}$ is finite, hence perfect and, therefore, $k_{\mathfrak{P}} | k_{\mathfrak{p}}$ is separable. Thus it suffices to show that

$\mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, \overline{\mathbb{F}}_p) = \mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, k_{\mathfrak{P}})$.

Let $\sigma \in \mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, \overline{\mathbb{F}}_p)$, then σ is $\mathbb{F}_p$-linear and therefore, since $k_{\mathfrak{P}}/\mathbb{F}_p$ is Galois,

$$\sigma \in \mathrm{Hom}_{\mathbb{F}_p}(k_{\mathfrak{P}}, \overline{\mathbb{F}}_p) = \mathrm{Hom}_{\mathbb{F}_p}(k_{\mathfrak{P}}, k_{\mathfrak{P}})$$

$$\Rightarrow \sigma(k_{\mathfrak{P}}) = k_{\mathfrak{P}} \Rightarrow \sigma \in \mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, k_{\mathfrak{P}}).$$

$\lrcorner$

(ii) Recall that $\mathrm{Gal}(K|Z_{\mathfrak{P}}) = D_{\mathfrak{P}}$ and $k_{\mathfrak{P}_Z} = k_{\mathfrak{p}}$. Hence we can assume without loss of generality, that $Q = Z_{\mathfrak{P}}$ and $\mathfrak{p} = \mathfrak{P}_Z$. (*) ⌈$\mathrm{Gal}(k_{\mathfrak{P}}, k_{\mathfrak{p}})$ only depends on $k_{\mathfrak{P}}, k_{\mathfrak{p}}$, not on $\mathfrak{P}$ or $\mathfrak{p}$.⌋

By definition, $\sigma_{\mathfrak{P}}$ factors

$$\begin{tikzcd}
D_{\mathfrak{P}} \arrow[r, "\sigma_{\mathfrak{P}}"] \arrow[d] & \mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, k_{\mathfrak{P}}) = \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \\
D_{\mathfrak{P}}/I_{\mathfrak{P}} \arrow[ur, dashed, "\overline{\sigma_{\mathfrak{P}}}"'] &
\end{tikzcd}$$

and we only need to show surjectivity.

Let $\vartheta \in k_{\mathfrak{P}}$ s.t. $k_{\mathfrak{p}}(\vartheta) = k_{\mathfrak{P}}$ and let $z \in B$ a lift of ϑ, i.e.,

$$\vartheta = z \mod \mathfrak{P}.$$

Let P be the minimal polynomial of z over Q. We have seen (in the discussion of stability of Dedekind property under finite separable extensions) that $P \in A[X]$. Moreover, we know that the roots of P are exactly the Galois conjugates

$$\{\sigma z : \sigma \in \mathrm{Gal}(K/Q) = D_{\mathfrak{P}}\}.$$

Let $\eta \in Gal(k_\beta / k_p)$, then η is completely determined by $\eta(\vartheta)$. But $\eta(\vartheta)$ is a root of P mod p, whose roots are exactly $\{\sigma_\beta(\vartheta) : \sigma \in D_\beta\}$.

$$P = X^d + a_{d-1}X^{d-1} + \dots + a_0 \Rightarrow \overline{P}(\mu(\vartheta)) = \mu(\vartheta)^d + \bar{a}_{d-1}\mu(\vartheta)^{d-1} + \dots + \bar{a}_0$$

$$= \mu(\vartheta^d + \bar{a}_{d-1}\vartheta^{d-1} + \dots + \bar{a}_0) = \mu(P(z) \bmod \beta) = 0$$

o.t.o.h., $P(X) = \prod_{\sigma \in D_\beta} (X - \sigma(z)) \Rightarrow P(X) \bmod \beta \overset{\nearrow}{=} \prod_{\sigma \in D_\beta} (X - \sigma_\beta(z))$

well-def. since $\sigma_\beta(z) = \sigma(z) \bmod \beta$

In particular, there is $\sigma \in D_\beta$ s.t.

$$\eta(\vartheta) = \sigma_\beta(\vartheta),$$

i.e., $\bullet_\beta$ is surjective.

(iii) $f_p = |Gal(k_\beta / k_p)| = \left| {D_\beta}/{I_\beta} \right| = \dfrac{e_p f_p}{|I_\beta|}$. $\boxed{\Xi}$

<u>Remark</u>: we call $D_\beta / I_\beta \longrightarrow Gal(k_\beta / k_p)$, $\sigma I_\beta \longmapsto \sigma_\beta$ the <u>canonical isomorphism</u>.

<u>Corollary</u>

$p \in Spec(A)^\times$ is unramified iff for some $\beta \in Spec_p(B)$ we have $I_\beta = \{id_K\}$. In that case

$$D_\beta \cong Gal(k_\beta / k_p)$$

Recall: As $k_{\mathfrak{p}}$ is finite, $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is cyclic with generator

$$\mathrm{frob}_{|k_{\mathfrak{p}}|} : \vartheta \in k_{\mathfrak{P}} \longmapsto \vartheta^{|k_{\mathfrak{p}}|}$$

⌜**Proof:** Check that $\sigma := \mathrm{frob}_{|k_{\mathfrak{p}}|}$ is a $k_{\mathfrak{p}}$-linear automorphism of $k_{\mathfrak{P}}$.

$k_{\mathfrak{P}}^{\sigma} = k_{\mathfrak{p}}$ since for $x \neq 0$ we have $\sigma x = x \Leftrightarrow x^{|k_{\mathfrak{p}}|-1} - 1 = 0$, which has at most $|k_{\mathfrak{p}}|-1$ roots and every element of $k_{\mathfrak{p}} - \{0\}$ is indeed a root.

Therefore $\langle \sigma \rangle$ is a cyclic subgroup of $\mathrm{Gal}(k_{\mathfrak{P}}|k_{\mathfrak{p}})$ and it suffices to show that σ has order $f_{\mathfrak{p}}$.

Let $i \in \mathbb{N}$ s.t. $\sigma^i = \mathrm{id}_{k_{\mathfrak{P}}}$, i.e., $\forall x \in k_{\mathfrak{P}}$ $x^{|k_{\mathfrak{p}}|^i} = \sigma^i(x) = x$. Then for all $x \in k_{\mathfrak{P}} - \{0\}$ we have

$$x^{|k_{\mathfrak{p}}|^i - 1} - 1 = 0$$

and thus $|k_{\mathfrak{p}}|^i \geq |k_{\mathfrak{P}}|$. Thus $i \geq f_{\mathfrak{p}}$.

$\blacksquare$ ⌟

Definition:

Let $\mathfrak{P} \in \mathrm{Spec}(\mathcal{B})^*$, then the Frobenius $\left(\frac{K|\mathbb{Q}}{\mathfrak{P}}\right) \in D_{\mathfrak{P}}/I_{\mathfrak{P}}$ at $\mathfrak{P}$ is the preimage of $\mathrm{frob}_{|k_{\mathfrak{p}}|}$ under the canonical isomorphism.

Exercises: Suppose $\mathfrak{P} \cap A$ is unramified in K.

(a) $\left(\frac{K/\mathbb{Q}}{\mathfrak{P}}\right) \in D_{\mathfrak{P}}$ is the unique element $\sigma \in D_{\mathfrak{P}}$ such that

$$\forall z \in B \quad \sigma z \equiv z^{|k_{\mathfrak{p}}|} \mod \mathfrak{P}.$$

(b) If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then

$$\sigma \left(\frac{K/\mathbb{Q}}{\mathfrak{P}}\right) \sigma^{-1} = \left(\frac{K/\mathbb{Q}}{\sigma(\mathfrak{P})}\right).$$

(c) The set of Frobenius elements at primes above $\mathfrak{P} \cap A$ is a single conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$.

We denote it by $\left(\frac{K/\mathbb{Q}}{\mathfrak{P} \cap A}\right)$.

Applications to cyclotomic fields

Thm

Let $\zeta_n \in \mathbb{C}$ a primitive n-th root of unity and $K = \mathbb{Q}(\zeta_n)$.

(a) If p ramifies in K, then $p \mid n$ (in fact iff, proven later).

(b) $K/\mathbb{Q}$ is Galois of degree $\varphi(n)$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Pf: Let $P = P_{\min, \zeta_n, \mathbb{Q}} \in \mathbb{Z}[X]$ $(P \mid X^n - 1)$ and $d = \deg P$.

We will show that $n^d \in \mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}} = (D_K)$, thus proving (a) ($p$ ramified $\Leftrightarrow p \mid D_K \Rightarrow p \mid n^d \Rightarrow p \mid n$)

Note: $X^n - 1 = P \cdot G$ for some $G \in \mathbb{Z}[X]$.

$$\Rightarrow n X^{n-1} = P'(X) G(X) + P(X) G'(X)$$

$$\Rightarrow n \zeta_n^{n-1} = P'(\zeta_n) G(\zeta_n)$$

$$\Rightarrow \mathrm{Nr}(P'(\zeta_n)) \mid \mathrm{Nr}(n \zeta_n^{n-1}) = n^d \quad (\text{since } \zeta_n^{n-1} \in \mathcal{O}_K^\times)$$

Sheet 6, Ex. 3c: $\mathrm{Nr}(P'(\zeta_n)) \in (\mathrm{disc}_{K|\mathbb{Q}}(\zeta_n)) \subseteq \mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}}$

$$\Rightarrow n^d \in \mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}} \Rightarrow (a).$$

For (b) we show

(i) $K/\mathbb{Q}$ Galois

(ii) $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

(iii) $\mathrm{Gal}(K/\mathbb{Q}) \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

<u>Claim:</u>

$K/\mathbb{Q}$ is Galois

$P \mid X^n - 1 \Rightarrow$ roots of P are n-th roots of unity, i.e., of the form ζ_n^l for $l \in \mathbb{Z}$.

$\Rightarrow$ roots of P lie in K

$\Rightarrow [\times \zeta_n]_{K/\mathbb{Q}}$ is diagonalizable over K.

Claim:

Gal(K/Q) injects into $(\mathbb{Z}/n\mathbb{Z})^\times$

Any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is uniquely determined by $\sigma(\zeta_n)$. Moreover, $\sigma(\zeta_n)^n - 1 = 0$, thus

$$\forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})\ \exists j(\sigma) \in \mathbb{N}\quad \sigma(\zeta_n) = \zeta_n^{j(\sigma)}.$$

Moreover, for all $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$

$$\zeta_n^{j(\sigma\circ\tau)} = (\sigma\circ\tau)(\zeta_n) = \sigma\left(\zeta_n^{j(\tau)}\right) = \sigma(\zeta_n)^{j(\tau)} = \zeta_n^{j(\sigma)j(\tau)}$$

$$\Rightarrow n \mid j(\sigma\circ\tau) - j(\sigma)j(\tau)$$

and therefore $\bar{j} : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathbb{Z}/n\mathbb{Z}$ is multiplicative.

$$\sigma \longmapsto j(\sigma) \bmod (n)$$

Also, $\zeta_n = (\sigma^{-1}\circ\sigma)(\zeta_n) = \zeta_n^{j(\sigma^{-1})j(\sigma)} \Rightarrow \bar{j}(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$

As σ is uniquely determined by $\bar{j}(\sigma)$, $\bar{j}$ is injective.

This proves $\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

Claim:

$\forall p \nmid n \ \exists \sigma \in \mathrm{Gal}(K|\mathbb{Q}) \ \bar{j}(\sigma) \equiv p \mod (n)$ (i.e., $\bar{j}$ is onto)

$p \nmid n \Rightarrow p$ unramified $\Rightarrow \sigma_p = \left(\frac{K|\mathbb{Q}}{p}\right) \in \mathrm{Gal}(K|\mathbb{Q})$ well-defined (Gal$(K/\mathbb{Q})$ is abelian).

We show that $\bar{j}(\sigma_p) \equiv p \mod (n)$.

Let $\mathfrak{P} \in \mathrm{Spec}_p(\mathcal{O}_K)$, then

$$\forall x \in \mathcal{O}_K \ \ \sigma_p(x) \equiv x^p \mod \mathfrak{P}.$$

Choose $j \equiv \bar{j}(\sigma_p) \mod n$, then

$$\zeta_n^j = \sigma_p(\zeta_n) = \zeta_n^p \mod \mathfrak{P} \quad (*)$$

Let $F = X^n - 1 \in \mathbb{Z}[X]$. Then $\left(F = \prod_{\ell=0}^{n-1} (\zeta_n^\ell - X)\right)$.

$$n \zeta_n^{p(n-1)} = F'(\zeta_n^p) = -\prod_{\ell \not\equiv p\,(n)} (\zeta_n^\ell - \zeta_n^p) \notin \mathfrak{P}$$

as ($\zeta_n \in \mathcal{O}_K^\times$ implies) $n\zeta_n^{p(n-1)} \in \mathfrak{P} \Leftrightarrow n \in \mathfrak{P} \cap \mathbb{Z} = (p)$

Therefore $\ell \not\equiv p \mod (n) \Rightarrow \zeta_n^p \not\equiv \zeta_n^\ell \mod \mathfrak{P}$ and thus $j \equiv p \mod n$.

$\blacksquare$

Theorem:

Let $K = \mathbb{Q}(\zeta_n)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ and p ramifies in K iff $p \mid n$.

Proof: Exercise.

Definition (Artin Symbol)

Let $p \in \operatorname{Spec}(A)^\times$ unramified in K. The Frobenius $\left(\frac{K/\mathbb{Q}}{p}\right)$ at p is the conjugacy class in $\operatorname{Gal}(K/\mathbb{Q})$ of the Frobenius at $\mathfrak{P}$ for any $\mathfrak{P} \in \operatorname{Spec}_p(B)$.

Thm (Chebotarev)

Let $K/\mathbb{Q}$ #-field. Then $\left\langle \left(\frac{K/\mathbb{Q}}{p}\right) : p \in \operatorname{Spec}(A)^\times \text{ unramified} \right\rangle = \operatorname{Gal}(K/\mathbb{Q})$.