For $n \equiv 2$ (4) $\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{n/2})$.

Example 6.5.5: Consider the cyclotomic field $L := \mathbb{Q}(\mu_n)$ for $n \not\equiv 2 \bmod (4)$.

✓ (a) A rational prime p is ramified in $\mathcal{O}_L$ if and only if $p|n$.

✓ (b) For any $p \nmid n$ the Frobenius substitution at p corresponds to the residue class of p under the isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

✓ (c) A rational prime p is totally split in $\mathcal{O}_L$ if and only if $p \equiv 1 \bmod (n)$.

(d) If $n = p^\nu$ for a prime p, then p is totally ramified in $\mathcal{O}_L$.

$\mathcal{O}_L = \mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/(\Phi_n(X))$ for ζ primitive n-th root of 1.

$\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$

(b) $\forall p$: $\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{F}_p[X]/(\Phi_n(X))$

Case $p \nmid n$: $\Phi_n \mid X^n - 1$ = separable over $\mathbb{F}_p$. ⇒ all irred. factors simple

⇒ p unramified in $\mathcal{O}_L$.

⇒ $\mu_n(\overline{\mathbb{F}}_p)$ = cyclic of order n.

⇒ ζ mod any $\mathfrak{p} < \mathcal{O}_L$ above p has order n.

$\kappa(\mathfrak{p}) = \mathbb{F}_p(\bar\zeta)$ $\quad \bar\zeta$ residue class of ζ.

$\mathrm{Frob}_p(\bar\zeta) = \bar\zeta^p$

⇒ $\mathrm{Frob}_{\mathfrak{p}|p}(\zeta) = \zeta^p$.

⇒ (b).

(c) for $p \nmid n$ follows from (b).

Case $p | n$ ⇒ Write $n = p^\nu m$, $p \nmid m$.

$$\Rightarrow \Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$$

$$= \prod_{\substack{0 \le \lambda \le \nu \\ e|m}} (X^{p^\lambda e} - 1)^{\mu(p^{\nu-\lambda} \cdot \frac{m}{e})}, \qquad \mu(p^{\nu-\lambda}\cdot\tfrac{m}{e}) = \mu(p^{\nu-\lambda}) \cdot \mu(\tfrac{m}{e})$$

For fixed $e|m$ get: $\mu(p^{\nu-\lambda}) = \begin{cases} 1 & \nu = \lambda \\ -1 & \nu-1 = \lambda \\ 0 & \nu-2 \ge \lambda \end{cases}$

$$(X^{p^\nu e} - 1)^{\mu(\frac{m}{e})} \cdot (X^{p^{\nu-1} e} - 1)^{-\mu(\frac{m}{e})}$$

$$\equiv (X^e - 1)^{p^\nu \cdot \mu(\frac{m}{e})} \cdot (X^e - 1)^{-p^{\nu-1} \cdot \mu(\frac{m}{e})}$$

$$= (X^e - 1)^{\mu(\frac{m}{e}) \cdot (p^\nu - p^{\nu-1})}$$

$$\Rightarrow \Phi_n(X) \equiv \Big[\prod_{e|m} (X^e - 1)^{\mu(\frac{m}{e})}\Big]^{p^\nu - p^{\nu-1}} \bmod (p)$$

$$= \Phi_m(X)^{p^\nu - p^{\nu-1}}.$$

⇒ $\forall \mathfrak{p}|p$: $e_{\mathfrak{p}|p} = p^\nu - p^{\nu-1} > 1$ because $p^\nu > 2$.

⇒ p is ramified in $\mathcal{O}_L$.

(d) $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p^\nu\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$

$\cup$

$I_\mathfrak{p} \longleftrightarrow (\mathbb{Z}/p^\nu\mathbb{Z})^\times \times 1$.

6.6 Relative norm

Now we return to the situation that L/K is finite separable of degree n.

Definition 6.6.1: The *relative norm* of a fractional ideal $\mathfrak{b}$ of B is the A-submodule

$$\mathrm{Nm}_{L/K}(\mathfrak{b}) := \big(\{\mathrm{Nm}_{L/K}(y) \mid y \in \mathfrak{b}\}\big) \subset K.$$

Proposition 6.6.2:

(a) This is a fractional ideal of A.

(b) If $\mathfrak{b} \subset B$ then $\mathrm{Nm}_{L/K}(\mathfrak{b}) \subset \mathfrak{b} \cap A$.

(c) For any $y \in L^\times$ we have $\mathrm{Nm}_{L/K}((y)) = (\mathrm{Nm}_{L/K}(y))$. $\Leftarrow$ multiplicativity of $\mathrm{Nm}_{L/K}$.

Proof: (a) $\exists\, b, c \in B \setminus \{0\}$: $b \cdot B \subset \mathfrak{b} \subset \frac{1}{c} \cdot B$.

$\forall x \in B$: $\mathrm{Nm}_{L/K}(x) \in A$.

$\Rightarrow 0 \neq \mathrm{Nm}_{L/K}(b) \subset \mathrm{Nm}_{L/K}(\mathfrak{b}) \subset \frac{1}{\mathrm{Nm}_{L/K}(c)} \cdot A$.

(b) If $\mathfrak{b} \subset B \Rightarrow \forall b \in \mathfrak{b}$: $\underbrace{\mathrm{Nm}_{L/K}(b)}_{\in K} = \prod_{\sigma \in \Sigma} \sigma b = \underbrace{b}_{\in L} \cdot \underbrace{\Big(\prod_{\sigma \in \Sigma \setminus \{id\}} \sigma b\Big)}$ $\Rightarrow \in L$, integral over $A \Rightarrow \in B$.

$\Sigma = \mathrm{Hom}_K(L, \bar{K})$.

$\Rightarrow \mathrm{Nm}_{L/K}(b) \in bB \subset \mathfrak{b}$.

qed.

$$\mathrm{Nm}_{L/K}(z\mathfrak{b}) = \mathrm{Nm}_{L/K}(z)\cdot\mathrm{Nm}_{L/K}(\mathfrak{b}).$$

$\Downarrow$

Lemma:

(a) For any $z \in L^\times$ we have $\mathrm{Nm}_{L/K}(z\mathfrak{b}) = \mathrm{Nm}_{L/K}(z)\,\mathrm{Nm}_{L/K}(\mathfrak{b})$.

(b) Suppose that $\mathfrak{b} \subset B$ and take $x \in \mathrm{Nm}_{L/K}(\mathfrak{b}) \smallsetminus \{0\}$ and $y \in \mathfrak{b}$ such that $\mathfrak{b} = (x, y)$. Then $\mathrm{Nm}_{L/K}(\mathfrak{b}) = (x, \mathrm{Nm}_{L/K}(y))$.

$\subset A$

Proof: (a) ✓

(b) "$\supset$" clear.

Consider $bx + cy \in \mathfrak{b}$ with $b, c \in B$.

$$\Rightarrow \mathrm{Nm}_{L/K}(bx+cy) = \prod_{\sigma\in\Sigma}\left(\sigma b \cdot x + \sigma c \cdot \sigma y\right) = [\text{smth}]\cdot x + \prod_{\sigma\in\Sigma}\sigma c\,\sigma y$$

integral over A

integral over A in K.

$\Rightarrow \in A$.

$\mathrm{Nm}_{L/K}(c)\cdot\mathrm{Nm}_{L/K}(y)$

$\in A$.

qed.

Proposition 6.6.3: For any two fractional ideals $\mathfrak{b}, \mathfrak{b}'$ of B we have

$$\mathrm{Nm}_{L/K}(\mathfrak{b}\mathfrak{b}') \;=\; \mathrm{Nm}_{L/K}(\mathfrak{b}) \cdot \mathrm{Nm}_{L/K}(\mathfrak{b}').$$

Proof: "$\supset$" clear.

Lemma $\langle a \rangle \Rightarrow$ WLOG $\mathfrak{b}, \mathfrak{b}' < B$.

Pick $z \in \mathfrak{b} \setminus \{0\}$, $z' \in \mathfrak{b}' \setminus \{0\}$ $\Rightarrow zz' \in \mathfrak{b}\mathfrak{b}'$

$\Rightarrow x := \underbrace{\mathrm{Nm}_{L/K}(z)}_{\in A} \cdot \underbrace{\mathrm{Nm}_{L/K}(z')}_{\in A} \in \mathrm{Nm}_{L/K}(\mathfrak{b}) \cap \mathrm{Nm}_{L/K}(\mathfrak{b}') \setminus \{0\}$

$\in \mathrm{Nm}_{L/K}(\mathfrak{b}\mathfrak{b}') \setminus \{0\}$

Write: $\mathfrak{b} = (x, y)$, $\mathfrak{b}' = (x, y')$ $\xRightarrow{\text{Lemma } \langle b \rangle}$ $\mathrm{Nm}_{L/K}(\mathfrak{b}) = (x, \mathrm{Nm}(y))$, $\mathrm{Nm}(\mathfrak{b}') = (x, \mathrm{Nm}(y'))$

$\mathfrak{b}\mathfrak{b}' = (x^2, xy, xy', yy')$

$= \langle x, yy' \rangle$

$\Rightarrow \mathrm{Nm}_{L/K}\langle \mathfrak{b}\mathfrak{b}' \rangle = \langle x, \mathrm{Nm}(yy') \rangle$

$\Rightarrow \mathrm{Nm}(\mathfrak{b}) \cdot \mathrm{Nm}(\mathfrak{b}') = \langle x^2, x\mathrm{Nm}(y), x \cdot \mathrm{Nm}(y'), \mathrm{Nm}(yy') \rangle$

$= \langle x, \mathrm{Nm}(yy') \rangle$.

qed.

Proposition 6.6.4: For any fractional ideal $\mathfrak{c}$ of C we have

$$\mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{c})) \;=\; \mathrm{Nm}_{M/K}(\mathfrak{c}).$$