Reminder:

Let A be a Dedekind ring with quotient field K. Let L/K be a finite Galois extension of degree n with Galois group Γ. Let B be the integral closure of A in L. Consider a maximal ideal $\mathfrak{p} \subset A$ and a prime ideal $\mathfrak{q} \subset B$ over $\mathfrak{p}$, and let $f_{\mathfrak{q}|\mathfrak{p}}$ be the degree of the residue field extension $k(\mathfrak{q})/k(\mathfrak{p})$.

Assumption: The residue field $k(\mathfrak{p})$ is perfect.

$$\begin{array}{ccc} L & B & \mathfrak{q} \\ | & & \\ K & A & \mathfrak{p} \end{array}$$

Definition 6.3.3: The stabilizer of $\mathfrak{q}$ is called the *decomposition group of* $\mathfrak{q}$:

$$\Gamma_{\mathfrak{q}} := \left\{\gamma \in \Gamma \,\middle|\, \forall x \in \mathfrak{q} \colon {}^{\gamma}x \in \mathfrak{q}\right\}.$$

Proposition 6.3.4:

(a) The numbers $e = e_{\mathfrak{q}|\mathfrak{p}}$ and $f = f_{\mathfrak{q}|\mathfrak{p}}$ depend only on $\mathfrak{p}$.

(b) We have $\mathfrak{p}B = \prod_{[\gamma]\in\Gamma/\Gamma_{\mathfrak{q}}} {}^{\gamma}\mathfrak{q}^e$.

(c) We have $n = r \cdot e \cdot f$.

$r = [\Gamma : \Gamma_{\mathfrak{q}}]$

$ef = |\Gamma_{\mathfrak{q}}|.$

Proposition 6.3.6: Set $L' := L^{\Gamma_{\mathfrak{q}}}$ and $B' := B \cap L'$ and $\mathfrak{q}' := \mathfrak{q} \cap B'$.

(a) Then $\mathfrak{q}$ is the unique prime of B above $\mathfrak{q}'$ and $\mathfrak{q}'B = \mathfrak{q}^e$.

(b) We have $e_{\mathfrak{q}|\mathfrak{q}'} = e$ and $f_{\mathfrak{q}|\mathfrak{q}'} = f$ and $e_{\mathfrak{q}'|\mathfrak{p}} = f_{\mathfrak{q}'|\mathfrak{p}} = 1$.

$$\begin{tikzcd}
L \arrow[d, dash, "\Gamma_{\mathfrak{q}}"'] & \supset B \arrow[d, dash] & \supset \mathfrak{q} \arrow[d, dash] \\
L^{\Gamma_{\mathfrak{q}}} = L' \arrow[d, dash] & \supset B' \arrow[d, dash] & \supset \mathfrak{q}' \arrow[d, dash] \\
K & \supset A & \supset \mathfrak{p}
\end{tikzcd}$$

Proof: $\Gamma_{\mathfrak{q}}$ acts transitively on the primes of B above $\mathfrak{q}'$.
It stabilizes $\mathfrak{q}$ $\Rightarrow$ $\mathfrak{q}$ = unique prime above $\mathfrak{q}'$.
$\Rightarrow$ $\mathfrak{q}' \cdot B = \mathfrak{q}^{e_{\mathfrak{q}|\mathfrak{q}'}}$

$$B/\mathfrak{p}B = B/\prod_{[\gamma]\in\Gamma/\Gamma_{\mathfrak{q}}} \gamma\mathfrak{q}^e \cong \bigtimes_{[\gamma]\in\Gamma/\Gamma_{\mathfrak{q}}} B/\gamma\mathfrak{q}^e \qquad e = e_{\mathfrak{q}|\mathfrak{p}}$$

$$B/\mathfrak{q}'B \cong B/\mathfrak{q}^e \quad \Rightarrow \quad e_{\mathfrak{q}|\mathfrak{q}'} = e = e_{\mathfrak{q}|\mathfrak{p}}.$$

$$e_{\mathfrak{q}|\mathfrak{p}} = e_{\mathfrak{q}|\mathfrak{q}'} \cdot e_{\mathfrak{q}'|\mathfrak{p}} \quad \Rightarrow \quad e_{\mathfrak{q}'|\mathfrak{p}} = 1.$$

$$|\Gamma_{\mathfrak{q}}| = e_{\mathfrak{q}|\mathfrak{q}'} \cdot f_{\mathfrak{q}|\mathfrak{q}'} = e_{\mathfrak{q}|\mathfrak{p}} \cdot f_{\mathfrak{q}|\mathfrak{p}}$$

$$\Rightarrow f_{\mathfrak{q}|\mathfrak{q}'} = f_{\mathfrak{q}|\mathfrak{p}}.$$

$$f_{\mathfrak{q}|\mathfrak{p}} = f_{\mathfrak{q}|\mathfrak{q}'} \cdot f_{\mathfrak{q}'|\mathfrak{p}}$$

$$\Rightarrow f_{\mathfrak{q}'|\mathfrak{p}} = 1.$$

qed

6.4 Inertia group

Next $\Gamma_{\mathfrak{q}}$ acts on the residue field $k(\mathfrak{q}) := B/\mathfrak{q}$ by a natural homomorphism

$$\Gamma_{\mathfrak{q}} \longrightarrow \mathrm{Aut}(k(\mathfrak{q})/k(\mathfrak{p})).$$

Definition 6.4.1: Its kernel is called the *inertia group of* $\mathfrak{q}$:

$$I_{\mathfrak{q}} := \{\gamma \in \Gamma \mid \forall x \in B\colon {}^{\gamma}x \equiv x \bmod \mathfrak{q}\}.$$

Proposition 6.4.2: The extension $k(\mathfrak{q})/k(\mathfrak{p})$ is finite galois and the above homomorphism induces an isomorphism $\Gamma_{\mathfrak{q}}/I_{\mathfrak{q}} \cong \mathrm{Aut}(k(\mathfrak{q})/k(\mathfrak{p}))$.

Proof: Natural injective homo $\Gamma_{\mathfrak{q}}/I_{\mathfrak{q}} \longrightarrow \mathrm{Aut}(k(\mathfrak{q})/k(\mathfrak{p}))$

Replace L/K by $L/L^{\Gamma_{\mathfrak{q}}}$ $\leadsto$ WLOG $\Gamma = \Gamma_{\mathfrak{q}}$.

Take any $\bar{b} \in k(\mathfrak{q})$, lift it to $b \in B$, let $f \in A[X]$ be its min. pol. over K.

Then $f(X) = \prod_{i=1}^{m} (X - b_i)$ for $b_i \in B$ and $b_1 = b$. Let $\bar{f}$ be the image of f in $k(\mathfrak{p})[X]$

$\Rightarrow \bar{f}(\bar{b}) = 0$ and $\bar{f}(X) = \prod_{i=1}^{m} (X - \bar{b}_i) \in k(\mathfrak{p})[X]$.

splits completely in $k(\mathfrak{q})[X]$

So $k(\mathfrak{q})/k(\mathfrak{p})$ is normal, $k(\mathfrak{p})$ perfect $\Big\} \Rightarrow k(\mathfrak{q})/k(\mathfrak{p})$ is galois.

Choose $\bar{b}$ with $k(\mathfrak{q}) = k(\mathfrak{p})(\bar{b})$

$\Rightarrow \forall i\ \exists \gamma \in \Gamma\colon b_i = {}^{\gamma}b \Rightarrow \bar{b}_i = {}^{\gamma}\bar{b}$

$\Rightarrow$ Every conjugate of $\bar{b}$ over $k(\mathfrak{p})$ is $= {}^{\gamma}\bar{b}$ for some $\gamma \in \Gamma$.

$\Rightarrow \Gamma \twoheadrightarrow \mathrm{Aut}(k(\mathfrak{q})/k(\mathfrak{p}))$.

qed.

$I_{\mathfrak q} \triangleleft \Gamma_{\mathfrak q} \Rightarrow L^{I_{\mathfrak q}}/L^{\Gamma_{\mathfrak q}}$ galois with group $\Gamma_{\mathfrak q}/I_{\mathfrak q}$.

Proposition 6.4.3: Set $L'' := L^{I_\mathfrak{q}}$ and $B'' := B \cap L''$ and $\mathfrak{q}'' := \mathfrak{q} \cap B''$.

(a) Then $\mathfrak{q}'B'' = \mathfrak{q}''$ and $\mathfrak{q}''B = \mathfrak{q}^e$.

(b) We have $|I_\mathfrak{q}| = e$ and $[\Gamma_\mathfrak{q} : I_\mathfrak{q}] = f$ and $[\Gamma : \Gamma_\mathfrak{q}] = r$.

(c) We have $e_{\mathfrak{q}|\mathfrak{q}''} = e$ and $f_{\mathfrak{q}|\mathfrak{q}''} = e_{\mathfrak{q}''|\cancel{\mathfrak{p}}\,\mathfrak{q}'} = 1$ and $f_{\mathfrak{q}''|\cancel{\mathfrak{p}}\,\mathfrak{q}'} = f$.

$$\begin{array}{llllll}
 & L & B & \mathfrak q & r & e \quad f \\
I_{\mathfrak q} & | & | & | & 1, & e, \ 1 \\
 & L^{I_{\mathfrak q}} = L'' & B'' & \mathfrak q'' & & \\
\Gamma_{\mathfrak q}/I_{\mathfrak q} & | & | & | & 1, & 1, \ f \\
 & L^{\Gamma_{\mathfrak q}} = L' & B' & \mathfrak q' & & \\
 & | & | & | & r & \\
 & K & A & \mathfrak p & &
\end{array}$$

$\Gamma_{\mathfrak q}$, Γ

Proof: WLOG: $\Gamma = \Gamma_{\mathfrak q}$

$\Gamma_{\mathfrak q}/I_{\mathfrak q} \xrightarrow{\sim} \underbrace{\mathrm{Gal}(k(\mathfrak q)/k(\mathfrak p))}_{\text{order} = f}$

$\Gamma_{\mathfrak q}/I_{\mathfrak q} \cong \mathrm{Gal}(L''/L')$

$\Rightarrow$ the inertia group of $\mathfrak q''$ is trivial.

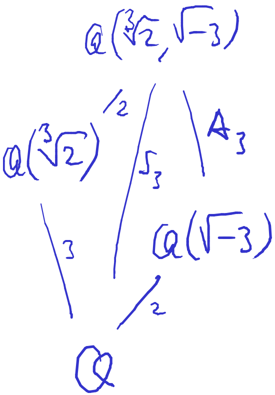
$f = |\Gamma_{\mathfrak q}/I_{\mathfrak q}| = |\mathrm{Gal}(L''/L')| = 1 \cdot e_{\mathfrak q''|\mathfrak q'} \cdot \underbrace{f_{\mathfrak q''|\mathfrak q'}}_{f}$

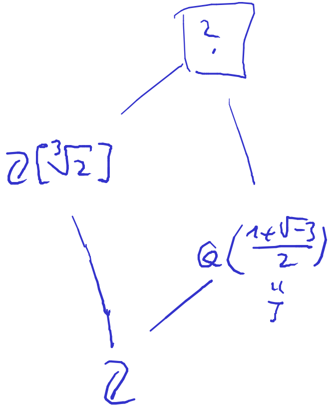
$\Rightarrow e_{\mathfrak q''|\mathfrak q'} = 1$

6.4.2 for L/L'' $\Rightarrow$ $k(\mathfrak q) = k(\mathfrak q'')$

qed.

Example:



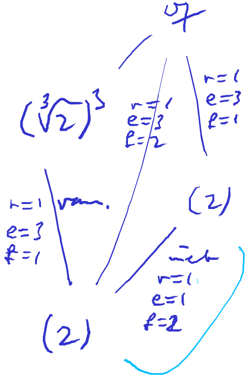


$y^2+y+1=0$

x^2+x^2+1

$\Gamma_q = \Gamma$.

$I_q = A_3$.

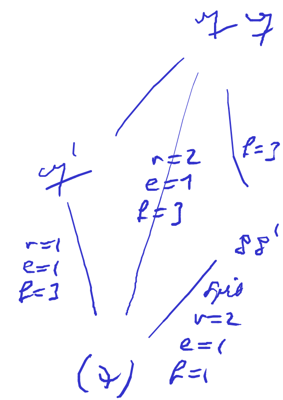


Frob ≠ 1.

Frob$_{q|(7)}$
"
3-cycle.

$\Gamma_q = A_3$

$I_q = 1$



$\mathfrak{p}\mathfrak{p}'$

$\mathfrak{p} \neq \mathfrak{p}'$

x^3-2 irred over $\mathbb{F}_7$

$[\gamma] \longmapsto$ Frobenius

$\Gamma_{\mathfrak{q}}/I_{\mathfrak{q}} \cong \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$

6.5 Frobenius

Keeping L/K galois with group Γ, we now assume that $k(\mathfrak{p})$ is finite. Then $k(\mathfrak{q})/k(\mathfrak{p})$ is finite galois, and its Galois group is generated by the Frobenius automorphism $x \mapsto x^{|k(\mathfrak{p})|}$.

Proposition 6.5.1: (a) There exists $\gamma \in \Gamma_{\mathfrak{q}}$ that acts on $k(\mathfrak{q})$ through $x \mapsto x^{|k(\mathfrak{p})|}$.

(b) The coset $\gamma I_{\mathfrak{q}}$ is uniquely determined by $\mathfrak{q}$.

Frob. subst. Frob. aut.

$$\begin{tikzcd} L \arrow[d, dash] & \supset B \arrow[d, dash] & \mathfrak{q} \arrow[d, dash] & k(\mathfrak{q}) \arrow[d, dash] \\ K & \supset A & \mathfrak{p} & k(\mathfrak{p}) \end{tikzcd}$$

Definition 6.5.2: Any such γ is called a *Frobenius substitution at* $\mathfrak{q}$ and denoted by $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$.

$I_{\mathfrak{q}} = 1$

Proposition 6.5.3: If $\mathfrak{q}$ is unramified over $\mathfrak{p}$, then in addition:

(a) The element $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ is uniquely determined by $\mathfrak{q}$.

(c) The conjugacy class of $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ in Γ is uniquely determined by $\mathfrak{p}$.

(d) If Γ is abelian, then $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ is uniquely determined by $\mathfrak{p}$.

$$\begin{array}{cccc} L & B & \mathfrak{q} & \gamma\mathfrak{q} \\ | & | & | & / \\ K & A & \mathfrak{p} & \end{array}$$

Proof: The primes of B above $\mathfrak{p}$ are the $\gamma\mathfrak{q}$ for $\gamma \in \Gamma$

$\Rightarrow \Gamma_{\gamma\mathfrak{q}} = {}^{\gamma}\Gamma_{\mathfrak{q}}$

$$\boxed{\mathrm{Frob}_{\gamma\mathfrak{q}|\mathfrak{p}} = {}^{\gamma}\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}}$$

Let $\delta := \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ i.e. $\delta \in \Gamma$ with $\forall x \in B: \delta x \equiv x^{p^s}$ mod $\mathfrak{q}$.

Let $p^s := |k(\mathfrak{p})|$

$\Rightarrow \gamma\delta x \equiv \gamma x^{p^s}$ mod $\gamma\mathfrak{q}$.

$\Rightarrow \forall y \in B: \; x = \gamma^{-1} y \Rightarrow \gamma\delta\gamma^{-1} y \equiv \gamma\gamma^{-1} y^{p^s} = y^{p^s}$ mod $\gamma\mathfrak{q}$.

$\Rightarrow \gamma\delta\gamma^{-1} = \mathrm{Frob}_{\gamma\mathfrak{q}|\mathfrak{p}}$.

qed.

Caution 6.5.4: Do not confuse the Frobenius substitution $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \in \Gamma_{\mathfrak{q}}$ with the Frobenius automorphism $x \mapsto x^{|k(\mathfrak{p})|}$ of $k(\mathfrak{q})$.

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 $\mathcal{O}_L$.