More on Galois actions, splitting, and ramification

PS 5 posted to web/Localc

Review: decomposition and inertia groups

. L/K extension of number fields.

Galois with group $G = \mathrm{Gal}(L/K)$

$\# G = [L:K] = n$

$\mathfrak{p} \subset \mathcal{O}_K$ nonzero prime ideal

G acts transitively on set of prime ideals of $\mathcal{O}_L$ above $\mathfrak{p}$

if $\mathfrak{q}$ = one of these primes, we define

decomposition group $G_{\mathfrak{q}} := \mathrm{Stab}_G(\mathfrak{q}) = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$

$G_{\mathfrak{q}} \to \mathrm{Gal}\left(\mathcal{O}_L/\mathfrak{q} \,/\, \mathcal{O}_K/\mathfrak{p}\right)$ (will be surjective)

inertia group $I_{\mathfrak{q}} = \mathrm{Ker}(\text{this map})$

Decomposition mod inertia as the residual Galois group

Reminder: if $\mathbb{F}_q$ is a finite field and $\mathbb{F}_{q^f}$ an extension of $\mathbb{F}_q$, then $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ is cyclic of order f, generated by $x \mapsto x^q$.

Prop $G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} \,/\, \mathcal{O}_K/\mathfrak{p})$ is surjective, so

$G_{\mathfrak{q}}/I_{\mathfrak{q}} \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} \,/\, \mathcal{O}_K/\mathfrak{p})$

Pf Suppose first that $G = G_{\mathfrak{q}}$. Pick $\bar{\alpha} \in \mathcal{O}_L/\mathfrak{q}$ a primitive ele. Say min poly is $\bar{g} \in \mathcal{O}_K/\mathfrak{p}\,[x]$. Lift $\bar{\alpha}$ to $\alpha \in \mathcal{O}_L$, let equal actually m $f \in \mathcal{O}_K(x)$ be its min poly. Then $f(\alpha) = 0 = \bar{f}(\bar{\alpha})$, so $g \mid \bar{f}$. Over $\mathcal{O}_L$, f splits into linear factors, so $\bar{g}$ splits over $\mathcal{O}_L/\mathfrak{q}$)

Say $\bar{\sigma} \in \mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} \,/\, \mathcal{O}_K/\mathfrak{p})$. $\bar{\sigma}(\bar{\alpha})$ is a root of $\bar{g}$ in $\mathcal{O}_L/\mathfrak{p}$), so $\exists\, \bar{\beta}$ the same root β of f. Pick $\sigma \in G$ moving α to β.

The Frobenius element of a prime ideal $\mathfrak{q}$

$L \quad \mathfrak{q}$
$|$
$K \quad \mathfrak{p}$

$$G_{\mathfrak{q}}/I_{\mathfrak{q}} \cong Gal\left(\mathcal{O}_L/\mathfrak{q} \,\Big/\, \mathcal{O}_K/\mathfrak{p}\right)$$

$$\underline{x \mapsto x^q} \quad \underline{\text{Frobenius automorphism}}$$

Define a <u>Frobenius element</u> for $\mathfrak{q}$ to be any preimage of this generator in $G_{\mathfrak{q}}$.

Note: $e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p}) = \# G_{\mathfrak{q}}$ and $f(\mathfrak{q}/\mathfrak{p}) = (G_{\mathfrak{q}} : I_{\mathfrak{q}})$

hence $e(\mathfrak{q}/\mathfrak{p}) = \# I_{\mathfrak{q}}$.

Hence iff $\mathfrak{q}/\mathfrak{p}$ unramified, there is <u>one</u> Frobenius element for $\mathfrak{q}$

This element is <u>not</u> well-defined as a function of $\mathfrak{p}$

(<u>unless</u> G <u>abelian</u>) but its conjugacy class is.

The Chebotarëv density theorem

(≈ Dirichlet's theorem on primes in arithmetic progression)

L/K Galois extension of # fields, group $= G$

For each unramified prime $\mathfrak{p}$ of $\mathcal{O}_K$, each $\mathfrak{q} \subset \mathcal{O}_L$ above $\mathfrak{p}$, consider $\mathrm{Frob}_{\mathfrak{q}}$ = Frobenius element of G for $\mathfrak{q}$.

Theorem (Chebotarëv)

Each element of G occurs as $\mathrm{Frob}_{\mathfrak{q}}$ for infinitely many $\mathfrak{q}$

(Cor: $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_m)$, recover Dirichlet's theorem)

A corollary about splitting

Cor There are infinitely many primes of $\mathcal{O}_K$ which split completely in $\mathcal{O}_L$.

Cor If $L \neq K$ there are infinitely many primes in $\mathcal{O}_K$ which do not split completely in L

A related comment about ramification

For $K = \mathbb{Q}$, $L \neq K$, there <u>must be</u> a ramified prime (HW)

For $K \neq \mathbb{Q}$, $L \neq K$, it can happen that no prime ramifies (HW)

Decomposition and inertia fields

$Z_{\mathfrak{q}}$ = fixed field of $G_{\mathfrak{q}}$

$\mathfrak{q}$ only prime of L above $\mathfrak{q} \cap Z_{\mathfrak{q}}$

fundamental identity for $\mathfrak{q}_1 \dots \mathfrak{q}_r / \mathfrak{p}$

so residue field of $\mathfrak{p}$ = residue field of $\mathfrak{q} \cap Z_{\mathfrak{q}}$

$$\begin{array}{ccl}
L & \mathfrak{q} & \\
| & & \Big\} \; ef = [L : Z_{\mathfrak{q}}] \\
T_{\mathfrak{q}} & & \\
| & & \\
Z_{\mathfrak{q}} & \mathfrak{q} \cap Z_{\mathfrak{q}} & \\
| & & \Big\} \; e = f = 1 \\
K & \mathfrak{p} &
\end{array}$$

Π

$efr = n$

$r = (G : G_{\mathfrak{q}})$

$n/r = [L : Z_{\mathfrak{q}}]$

$T_{\mathfrak{q}}$ = fixed field of $I_{\mathfrak{q}}$

$L - T_{\mathfrak{q}} - Z_{\mathfrak{q}} - K$

$$\begin{array}{cl}
\mathfrak{q} & \\
 & \Big\} \; e = e(\mathfrak{q}/\mathfrak{p}),\ f = 1 \\
\mathfrak{q} \cap T_{\mathfrak{q}} & \\
 & \Big\} \; e = 1,\ f = f(\mathfrak{q}/\mathfrak{p}) \\
\mathfrak{q} \cap Z_{\mathfrak{q}} & \\
 & \Big\} \; e = f = 1 \\
\mathfrak{p} &
\end{array}$$

Intermediate behavior of primes

Intermediate behavior of primes

Revisiting the cyclotomic case

$p \neq 2$ odd primes $\quad p^* = (-1)^{\frac{p-1}{2}} p$

q totally split in $\mathbb{Q}(\sqrt{p^*}) \iff [G : G_{\mathfrak{q}}] = \text{even}.$

cyclic

for $\mathfrak{q}$ a prime of $\mathbb{Q}(\zeta_p)$ above q

$\iff$ q splits into an even number of primes in $\mathbb{Q}(\zeta_p)$