

## More on Galois actions, splitting, and ramification

ps 5 posted to web/Calc

## Review: decomposition and inertia groups

$L/K$  extension of number fields.

Galois with group  $G = \text{Gal}(L/K)$   
 $\#G = [L:K] = n$

$\mathfrak{p} \subset \mathcal{O}_K$  <sup>nonzero</sup> prime ideal

$G$  acts transitively on set of prime ideals of  $\mathcal{O}_L$  above  $\mathfrak{p}$   
if  $\mathfrak{q} = \text{one of these primes}$ , we define

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

$G_{\mathfrak{q}} \rightarrow \text{Gal}(\mathcal{O}_L/\mathfrak{q} / \mathcal{O}_K/(\mathfrak{p}))$  (will be surjective)

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

# 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  $\text{Gal}(\mathbb{F}_q^f/\mathbb{F}_q)$  is cyclic of order  $f$ , generated by  $x \mapsto x^q$

prop  $G_{\mathbb{F}} \rightarrow \text{Gal}(\mathcal{O}_L/\mathfrak{f}/\mathcal{O}_K/\mathfrak{p})$  is surjective, so

$$G_{\mathbb{F}}/\Gamma_{\mathfrak{f}} \cong \text{Gal}(\mathcal{O}_L/\mathfrak{f}/\mathcal{O}_K/\mathfrak{p})$$

pf suppose first that  $G = G_{\mathbb{F}}$ . Pick  $\bar{\alpha} \in \mathcal{O}_L/\mathfrak{f}$  a primitive element. Say min poly is  $\bar{g} \in \mathcal{O}_K/\mathfrak{p}(x)$ . Lift  $\bar{\alpha}$  to  $\alpha \in \mathcal{O}_L$ , let  $f \in \mathcal{O}_K(x)$  be its min poly. Then  $f(\alpha) = 0 = F(\bar{\alpha})$ , so  $\bar{g} \mid f$ .

Over  $\mathcal{O}_L$ ,  $f$  splits into linear factors, so  $\bar{g}$  splits over  $\mathcal{O}_L/\mathfrak{f}$ .

So  $\bar{\sigma} \in \text{Gal}(\mathcal{O}_L/\mathfrak{f}/\mathcal{O}_K/\mathfrak{p})$   $\bar{\sigma}(\bar{\alpha})$  is a root of  $\bar{g}$  in  $\mathcal{O}_L/\mathfrak{p}$ , so is  $\bar{\beta}$  to some root  $\beta$  of  $f$ . Pick  $\sigma \in G$  mapping  $\alpha$  to  $\beta$ .

# The Frobenius element<sup>s</sup> of a prime ideal $\mathfrak{q}$ $\subset \mathfrak{p}$

$$G_{\mathfrak{q}/\mathbb{I}_{\mathfrak{q}}} \cong \text{Gal}(\mathcal{O}_{K/\mathfrak{q}} / \mathcal{O}_{K/\mathfrak{p}})$$

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

Define a Frobenius element for  $\mathfrak{q}$  to be any preimage of this generator in  $G_{\mathfrak{q}/\mathbb{I}_{\mathfrak{q}}}$ .

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

hence  $e(\mathfrak{q}, \mathfrak{p}) = \# \mathbb{I}_{\mathfrak{q}}$ .

When  $\# \mathbb{I}_{\mathfrak{q}} \nmid \# G_{\mathfrak{q}/\mathbb{I}_{\mathfrak{q}}}$  unramified, there is one Frobenius element for  $\mathfrak{q}$ .

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

(unless G abelian) but its conjugacy class is.

The Chebotarëv density theorem ( $\approx$  Dirichlet's theorem  
on primes in arithmetic  
progression)

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

For each unramified prime  $p$  of  $O_K$ , each  $g \in G$  above  $p$ ,  
consider  $\text{Frob}_g =$  Frobenius element of  $f$  for  $g$ .

Theorem (Chebotarëv)

Each element of  $G$  occurs as  $\text{Frob}_g$  for infinitely  
many  $g$

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

## A corollary about splitting

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

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

## A related comment about ramification

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

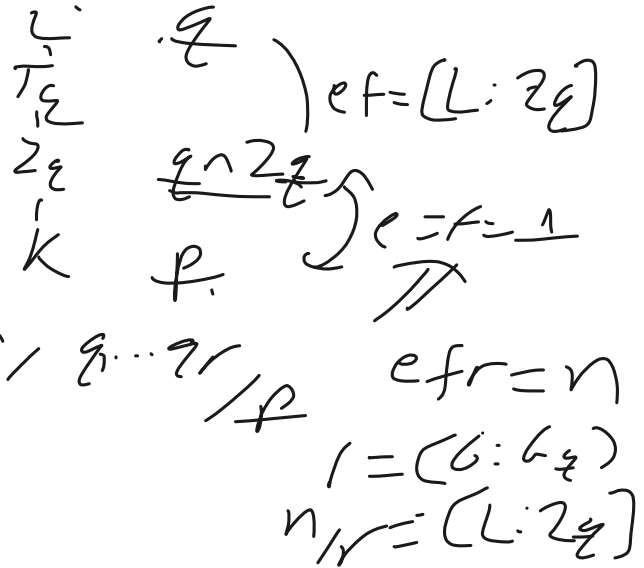
For  $K \neq \mathbb{Q}$ ,  $L \neq K$ , it can happen that no prime ramifies (HW)

# Decomposition and inertia fields

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

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

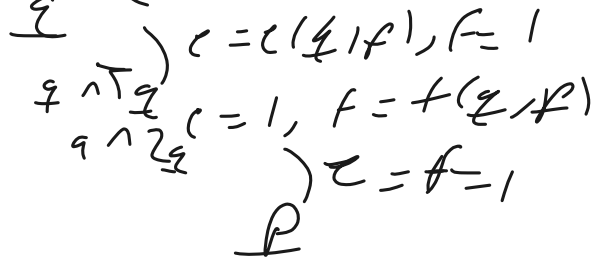
fundamental identity for  $\mathfrak{q} \dots \mathfrak{q}_r$   
 so residue field of  $\mathfrak{p}$  = residue field of  $\mathfrak{q} \cap Z_{\mathfrak{q}}$



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

$L$

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





# Intermediate behavior of primes

# Intermediate behavior of primes

# Revisiting the cyclotomic case

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

$q$  totally split in  $\mathbb{Q}(\sqrt{p^*}) \iff \left[ \frac{\mathbb{Q}(\zeta_p)}{\mathbb{Q}} \right] = \text{even}$   
 for  $q$  a prime of  $\mathbb{Q}(\zeta_p)$  above  $q$

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