# The Galois Group

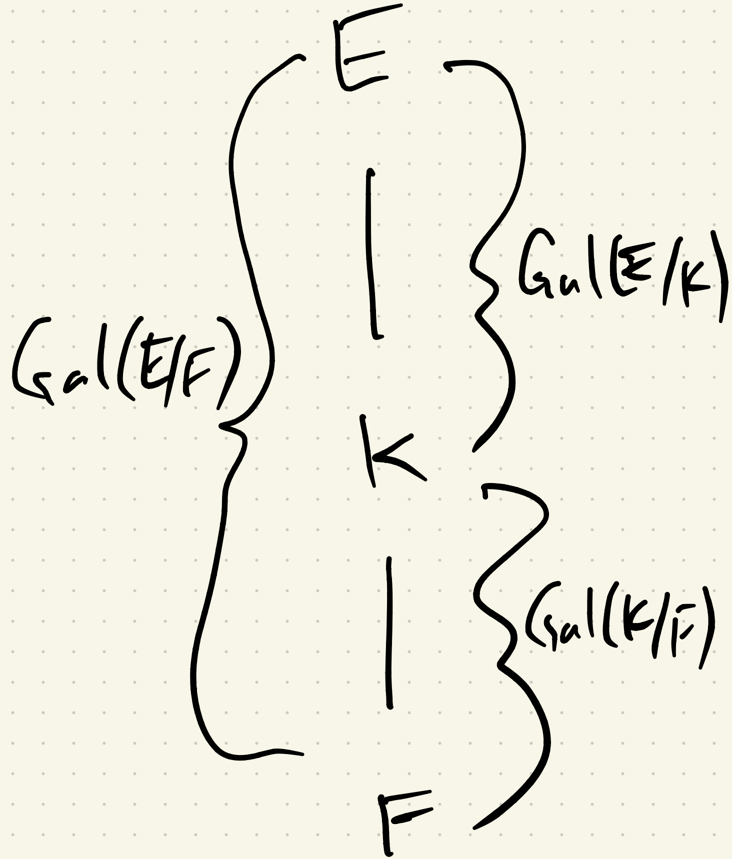
## IV: Relative Galois Theory

## Last time

An explicit computation of a Galois group

# New Stuff

If $F \subseteq K \subseteq E$, how do $\mathrm{Gal}(E/F)$, $\mathrm{Gal}(E/K)$, and $\mathrm{Gal}(K/F)$ relate to each other?



<u>Lemma</u> (Top subextensions are subgroups)

If $F \subseteq K \subseteq E$, then $\mathrm{Gal}(E/K) \leq \mathrm{Gal}(E/F)$.

<u>Pf</u> We need to check $\mathrm{Gal}(E/K) \subseteq \mathrm{Gal}(E/F)$.

Now $\sigma \in \mathrm{Gal}(E/K)$ implies $\sigma \in \mathrm{Aut}(E)$ with $\sigma|_K = \mathrm{id}_K$. Hence $\sigma|_F = (\sigma|_K)|_F = \mathrm{id}_K|_F = \mathrm{id}_F$.

Therefore $\sigma \in \mathrm{Gal}(E/F)$.

$\blacksquare$

Natural question: are "bottom subextensions" also subgroups? **No.**

$$\begin{array}{c} E \\ | \\ K \\ | \\ F \end{array} \qquad K \,|\, F \; \Big\} \; \tau \in \mathrm{Gal}(K/F)$$

If $\tau \in \mathrm{Gal}(K/F)$, do we have $\tau \in \mathrm{Gal}(E/F)$?

Recall $\tau : K \to K$, and hence it isn't defined on all of $E$.

Can we make $\sigma \in Gal(E/F)$ an element of $Gal(K/F)$.

Not immediately: $\sigma$ is a function on $E$, not $K$.

However, we do know $\sigma|_K : K \longrightarrow E$.

In order for $\sigma|_K$ to be an element of $Gal(K/F)$, we need $im(\sigma|_K) = K$.

When does this happen?

**Non-example** Let $E$ be the splitting field for $x^3-2$, and let $K = \mathbb{Q}(\sqrt[3]{2})$.

(Here: $F = \mathbb{Q}$).

Suppose we take $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ with $\sigma(\alpha_1) = \alpha_2$ and $\sigma(\alpha_2) = \alpha_3$.

Is $\mathrm{im}(\sigma|_K) = K$? From homework we know $\sigma(\alpha_1) = \alpha_2 \notin \mathbb{Q}(\alpha_1) = K$.

Thm (when restrictions are "nice")

If $F \subseteq K \subseteq E$, where $K$ is the splitting field of $g(x) \in F[x]$ and $E$ is the splitting field of $f(x) \in F[x]$, then for all $\sigma \in Gal(E/F)$ we have $im(\sigma|_K) = K$.

Pf Let $\beta_1, \dots, \beta_m \in K$ be the roots of $g(x)$. We've seen then that $\{\beta_1^{e_1} \cdots \beta_m^{e_m} : 0 \le e_i < \partial(irr_{F(\beta_1,\dots,\beta_{i-1})}(\beta_i))\}$ is an $F$-basis for $K$.

Key fact: $\sigma$ permutes $\{\beta_1, \ldots, \beta_m\}$.

First, let's show $\text{im}(\sigma|_K) \subseteq K$.

Let $k \in K$ be given, so $k = \sum f_{e_1 \cdots e_m} \beta_1^{e_1} \cdots \beta_m^{e_m}$.

Observe

$$\sigma|_K(k) = \sigma\left(\sum f_{e_1 \cdots e_m} \beta_1^{e_1} \cdots \beta_m^{e_m}\right)$$

$$= \sum f_{e_1 \cdots e_m} \underbrace{\sigma(\beta_1)}_{\in K}{}^{e_1} \cdots \underbrace{\sigma(\beta_m)}_{\in K}{}^{e_m} \in K.$$

Hence $\text{im}(\sigma|_K) \subseteq K$. Similar argument resolves "$\supseteq$".

$\blacksquare$

Cor (Restrictions to splitting field are "nice")

If $F \subseteq K \subseteq E$ where $K$ is the splitting field for $g(x) \in F[x]$ and $E$ is the splitting field for $f(x) \in F[x]$, then $\psi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$ given by $\psi(\sigma) = \sigma|_K$ is a homomorphism with $\ker(\psi) = \mathrm{Gal}(E/K)$.

Pf We know $\varphi$ is well-defined. Operation preserving is $\sigma_1\sigma_2|_K = \sigma_1|_K \, \sigma_2|_K$.

Now $\ker(\varphi) = \{\sigma \in \mathrm{Gal}(E/F) : \sigma|_K = \mathrm{id}_K\}$

$$= \{\sigma \in \mathrm{Aut}(E) : \sigma|_K = \mathrm{id}_K\}$$

$$= \mathrm{Gal}(E/K).$$

$\boxed{\text{QED}}$

Cor ( Galois Quotients)

If $F \subseteq K \subseteq E$ where $K$ is the splitting field for seperable $g(x) \in F[x]$ and $E$ is the splitting field for seperable $f(x) \in F[x]$, then $Gal(E/K) \triangleleft Gal(E/F)$ and

$$Gal(E/F)/Gal(E/K) \cong Gal(K/F).$$

Pf We only need to check that $\psi$ from the last result is surjective.

We know $|\mathrm{Gal}(E/F)| = [E:F]$ and

$$|\mathrm{Gal}(K/F)| = [K:F].$$

Observe that $E$ is the splitting field for separable $f(x) \in K[x]$,

and $|\mathrm{Gal}(E/K)| = [E:K]$. So we get

$$|\mathrm{im}(\varphi)| = \left| {\mathrm{Gal}(E/F)} \big/ {\mathrm{Gal}(E/K)} \right| = \frac{|\mathrm{Gal}(E/F)|}{|\mathrm{Gal}(E/K)|} = \frac{[E:F]}{[E:K]}$$

$$= \frac{[E:K][K:F]}{[E:K]} = [K:F] = |\mathrm{Gal}(K/F)| = |\mathrm{codomain}(\varphi)|$$