MA542 Lecture

Timothy Kohl

Boston University

April 9, 2025

Corollary

If E is a splitting field for a polynomial in $F[x]$ and K is an intermediate field $F \subsetneq K \subsetneq E$ then $|Gal(E/K)| = [E : K]$.

Proof.

If E is a splitting field for $f(x) \in F[x]$ then we may regard $f(x)$ as an element of $K[x]$ which dies not split in K but does in E so therefore E is a splitting field for $f(x) \in K[x]$, ergo $[E : K] = |Gal(E/K)|$. $\square$

The next major consideration (although not obviously so important initially) is that when E is a splitting field of some $f(x) \in F[x]$ then the fixed field of $Gal(E/F)$ is *exactly* F and nothing larger.

For perspective (and to highlight the importance of E being a splitting field over F), recall that $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{I\}$ which means the fixed field of $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is not just $\mathbb{Q}$ (the base field) but, in fact, all of $\mathbb{Q}(\sqrt[3]{2})$.

And the reason this happens, is precisely due to the fact that $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of *any* $f(x) \in \mathbb{Q}[x]$.

Also note that if E is the splitting field for $f(x) \in F[x]$ then it does **not** mean that $[E : F] = deg(f(x))$, although the degree of $f(x)$ does imply a *bound* on $[E : F] = |Gal(E/F)|$ as we shall see later.

Theorem

If $G = Gal(E/F)$ where E is the splitting field of some $f(x) \in F[x]$ then $E_G = F$.

PROOF: Since we can represent $E = F(\gamma)$ for some primitive element $\gamma \in E$. We can also write $E_G = F(\alpha)$ for some $\alpha \in E_G$ which means $\alpha = h(\gamma)$ for some $h(x) \in F[x]$ where $deg(h(x)) < n = [E : F]$.

Why? Well since $E = F(\gamma) \cong F[x]/\langle p(x)\rangle$ for $p(x) = irr(\gamma, F)$ then a typical element of E corresponds to $h(x) + \langle p(x)\rangle$ where $deg(h(x)) < deg(p(x))$ and $x + \langle p(x)\rangle \leftrightarrow \gamma \in E$.

Now since $\alpha \in E_G$ then since $\alpha = h(\gamma)$ then for all $\sigma \in Gal(E/F)$ we have $\sigma(\alpha) = \sigma(h(\gamma)) = h(\gamma)$ because $\alpha \in E_G$ (the fixed field of $Gal(E/F)$).

PROOF: (continued)
However, $\sigma(h(\gamma)) = h(\sigma(\gamma))$ (since σ is an automorphism and therefore a homomorphism so polynomial combinations of γ go to polynomial combinations of $\sigma(\gamma)$) and so $h(\sigma(\gamma)) = h(\gamma)$ for all $\sigma \in Gal(E/F)$.

But now $\{\sigma(\gamma) \mid \sigma \in Gal(E/F)\}$ is the set of all n roots of $p(x) = irr(\gamma, F)$ so if we let $\tilde{h}(x) = h(x) - h(\gamma)$ then

$$\begin{aligned} \tilde{h}(\sigma(\gamma)) &= h(\sigma(\gamma)) - h(\gamma) \\ &= \sigma(h(\gamma)) - h(\gamma) \\ &= h(\gamma) - h(\gamma) \\ &= 0 \end{aligned}$$

for all $\sigma \in Gal(E/F)$.

This means that $\tilde{h}(x)$ has at least n distinct roots, namely $\{\sigma(\gamma) \mid \sigma \in Gal(E/F)\}$, i.e. $deg(\tilde{h}(x)) \geq n$.

PROOF: (continued)
But this is impossible since $deg(\tilde{h}(x)) = deg(h(x)) < n$ unless $\tilde{h}(x) = 0$ (the constant polynomial) which means $h(x) = h(\gamma) = \alpha$ but since $h(x) \in F[x]$ then we must have $\alpha \in F$.

As such $E_G = F(\alpha) = F$ as claimed. $\square$

If E is the splitting field of some polynomial $f(x) \in F[x]$ then, given any two roots α_1, α_2 of $f(x)$ there is an isomorphism $F(\alpha_1) \cong F(\alpha_2)$ and so for some $\sigma \in Gal(E/F)$ we have $\sigma(\alpha_1) = \alpha_2$.

We now recall an important property of permutation/symmetric groups.

Definition

$G \leq S_n$ is a <u>transitive</u> if given any $x, y \in \{1, \ldots, n\}$ there exists $\sigma \in G$ such that $\sigma(x) = y$.

For example if $\sigma = (1, 2, \ldots, n)$ then $\langle \sigma \rangle$ is transitive since $\sigma(i) = i + 1$ and $\sigma^t(i) = i + t$.

Theorem

If E is the splitting field for some $f(x) \in F[x]$ where $n = deg(f(x))$ then $Gal(E/F)$ acts transitively on the set of roots of $f(x)$ and so $Gal(E/F)$ is isomorphic to a transitive subgroup of S_n. (i.e. $[E : F] \leq n!$)

Proof.

If α_1, α_2 are the roots of $f(x)$ then we have an isomorphism $\sigma : F(\alpha_1) \to F(\alpha_2)$ such that $\sigma(x) = x$ for all $x \in F$.

So by the isomorphism extension theorem there exists $\bar{\sigma} : E \to E$ such that $\bar{\sigma}(y) = \sigma(y)$ for $y \in F(\alpha_1)$ i.e. $\bar{\sigma}(\alpha_1) = \alpha_2$ and, moreover, $\bar{\sigma}(x) = \sigma(x) = x$ for all $x \in F$ which means $\bar{\sigma} \in Gal(E/F)$.

So $Gal(E/F)$ acts transitively on $\{\alpha_1, \dots, \alpha_n\}$, the roots of $f(x)$ which makes $Gal(E/F)$ isomorphic to a transitive subgroup of S_n (i.e. the group of permutations of $\{1, \dots, n\}$)
Ergo, for $n = deg(f(x))$, the degree $[E : F] = |Gal(E/F)| \leq n!$. □

So far we've proved that if E/F is a Galois extension, that is E is a splitting field for a polynomial in $F[x]$ that if K is an intermediate field $F \subseteq K \subseteq E$ then

$$\begin{aligned}
[E:K] &= |Gal(E/K)| \\
[K:F] &= [E:F]/[E:K] \\
&= |Gal(E/F)|/|Gal(E/K)| \\
&= |Gal(E/F):Gal(E/K)|
\end{aligned}$$

We also proved that when E/F is a Galois extension then $E_{Gal(E/F)} = F$, that is the fixed field of the Galois group is *exactly* F, *but no larger*.

Concordantly, if K is any intermediate field then E is a Galois extension over K too since if E is the splitting field of $f(x) \in F[x]$ then it's the splitting field of $f(x) \in K[x]$ since if $f(x) \in F[x]$ then $f(x) \in K[x]$.

As such $E_{Gal(E/K)} = K$ and so we have one 'loop' of the correspondence, namely

$$K \mapsto Gal(E/K) \mapsto E_{Gal(E/K)}$$

in that the composition in one direction is the identity:

$$\begin{tikzcd}
\{\text{intermediate fields}\} \arrow[r, bend left=60] & \{\text{subgroups of Gal(E/F)}\} \arrow[l, bend left=60]
\end{tikzcd}$$

For the reverse direction, we start with $H \leq Gal(E/F)$ and show that $H = Gal(E/E_H)$.

First, observe that $E = E_H(\beta)$ for some $\beta \in E$ and consider

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\beta)) \in E[x]$$

and note that $f(x)$ has no repeated factors since if $\sigma_1(\beta) = \sigma_2(\beta)$ for $\sigma_1, \sigma_2 \in H$ then $\sigma_2^{-1}\sigma_1(\beta) = \beta$ which mean $\sigma_2^{-1}\sigma_1$ is the identity on the entire field $E_H = F(\beta)$ so $\sigma_2^{-1}\sigma_1 = I$, and so $\sigma_1 = \sigma_2$.

Now for $\tau \in H$ consider $\tau(f(x)) = \prod_{\sigma \in H}(x - \tau\sigma(\beta))$ which must equal $f(x)$ since, as σ varies over the elements of H, then so does $\tau\sigma$.

But now, $\tau(f(x))$ is also the effect of τ acting on the *coefficients* of $f(x)$ so, degree by degree, each of these coefficients are unchanged by τ so they must lie in E_H.

Thus, $f(x) \in E_H[x]$, and observe now that $f(\beta) = 0$ which means $irr(\beta, E_H) \mid f(x)$.

However, $deg(irr(\beta, E_H)) = [E : E_H]$ and $deg(f(x)) = |H|$ so $[E : E_H] \leq |H|$. But since, obviously $H \leq Gal(E/E_H)$ then $|H| \leq |Gal(E/E_H)| = [E : E_H]$ so $|H| = |Gal(E/E_H)|$ and so $H = Gal(E/E_H)$.

So now, we've demonstrated that the composition in the other direction is the identity.

That is, for $H \leq Gal(E/F)$, we have $Gal(E/E_H) = |H|$.

$$
\begin{tikzcd}
\{\text{intermediate fields}\} \arrow[r, bend right=90] & \{\text{subgroups of Gal(E/F)}\} \arrow[l, bend right=90]
\end{tikzcd}
$$

And so there is a bijection between these two collections.

Now what about $H \triangleleft Gal(E/F)$ versus not?

If $K = E_H$ then for $\sigma \in Gal(E/F)$ we have that $\sigma(K)$ is another intermediate field.

$$\begin{tikzcd}[arrows=dash] & E & \\ K \arrow[ur] & & \sigma(K) \arrow[ul] \\ & F \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Proposition

$Gal(E/\sigma(K)) = \sigma H \sigma^{-1}$

Proof.

Let $\tau \in H$ then for $k \in K = E_H$ we have $\sigma(k) \in \sigma(K)$ and so $(\sigma\tau\sigma^{-1})(\sigma(k)) = \sigma\tau(k) = \sigma(k)$ since $\tau \in H = Gal(E/K)$.

Thus $\sigma H \sigma^{-1} \leq Gal(E/\sigma(K))$ but $K \cong \sigma(K)$ so $[E : \sigma(K)] = [E : K]$ and $[E : \sigma(K)] = |Gal(E/\sigma(K))| = |H|$ and $|\sigma H \sigma^{-1}| = |H|$ so since $|H| = |Gal(E/K)| = |Gal(E/\sigma(K)|$ then $\sigma H \sigma^{-1} = Gal(E/\sigma(K))$. $\square$

Corollary

$H \triangleleft Gal(E/F)$ iff $\sigma(K) = K$ for all $\sigma \in Gal(E/F)$.

Corollary

$H \triangleleft G = Gal(E/F)$ iff $K = E_H$ is a splitting field over F and $Gal(E_H/F) \cong Gal(E/F)/H$, that is $Gal(E_H/F) \cong Gal(E/F)/Gal(E/E_H)$.

PROOF: $E_H = F(\beta)$ for some $\beta \in E_H$ and $[E : E_H] = [G : H]$.

Also observe that, since $\sigma(E_H) = E_H$ for all $\sigma \in G$ then $\sigma(\beta)$ is a root of $irr(\beta, F)$ for all $\sigma \in G$.

But $\sigma_1(\beta) = \sigma_2(\beta)$ iff $\sigma_2^{-1}\sigma_1(\beta) = \beta$ iff $\sigma_2^{-1}\sigma$ fixes all of E_H, i.e. $\sigma_2^{-1}\sigma_1 \in H$ which means $\sigma_1 H = \sigma_2 H$.

PROOF (continued):
Conversely, if $\sigma_1 H = \sigma_2 H$ then $\sigma_1(\beta) = \sigma_2(\beta)$ i.e. $\sigma_1(\beta) = \sigma_2(\beta)$ iff $\sigma_1 H = \sigma_2 H$.

So.. if $m = [G : H]$ and $\{\sigma_1, \ldots, \sigma_m\}$ are a set of distinct coset representatives of H in G then $\{\sigma_1(\beta), \ldots, \sigma_m(\beta)\}$ are a set of $m = [G : H] = [E_H : F] = [F(\beta) : F]$ roots of $irr(\beta, F)$ so they are *all* the roots of $irr(\beta, F)$.

Thus, $F(\beta)$ contains *all* the roots of $irr(\beta, F)$ so it is the splitting field of $irr(\beta, F)$ since $[F(\beta) : F] = deg(irr(\beta, F))$.

What this also shows is that $G/H = \{\sigma_1 H, \ldots, \sigma_m H\}$ (which is a group since $H \triangleleft G$) is a group of distinct automorphisms of $F(\beta) = E_H$ so it may be regarded as $Gal(E_H/F)$.
i.e.

$$Gal(E/F)/Gal(E/E_H) \cong Gal(E_H/F)$$

□