MA542 Lecture

Timothy Kohl

Boston University

April 7, 2026

Fundamental Theorem of Galois Theory

Let F be a perfect field and let E be a splitting field over F of some polynomial in $F[x]$.

The mapping from the set of subfields of E containing F to the set of subgroups of $Gal(E/F)$ given by $K \mapsto Gal(E/K)$ is a 1-1 correspondence.

Similarly, the mapping from subgroups of $Gal(E/F)$ to sub-fields, given by $H \mapsto E_H = Fix(H)$ is a 1-1 correspondence.

Furthermore for any intermediate field $F \subseteq K \subseteq E$:

(1) $[E : K] = |Gal(E/K)|$ and $[K : F] = [Gal(E/F) : Gal(E/K)]$
(2) $K = E_{Gal(E/K)}$
(3) If H is a subgroup of $Gal(E/F)$ then $H = Gal(E/E_H)$.
(4) If K is the splitting field of some polynomial in $F[x]$ then $Gal(E/K)$ is a normal subgroup of $Gal(E/F)$ and $Gal(K/F) \cong Gal(E/F)/Gal(E/K)$.

Before we can approach the proof of the main theorem, we need a number of foundational facts about splitting fields.

Lemma

Let F be a field and $p(x) \in F[x]$ be irreducible over F, and let α be a zero of $p(x)$ in some extension of F. If $\phi : F \to F'$ is an isomorphism of fields and β is a zero of $\phi(p(x)) \in F'[x]$ in some extension of F' then there is an isomorphism from $F(\alpha) \to F'(\beta)$ that agrees with ϕ on F, and maps α to β.

PROOF:
First, note that if $p(x)$ is irreducible in $F[x]$ then $\phi(p(x))$ is irreducible in $F'[x]$ and so we have an isomorphism

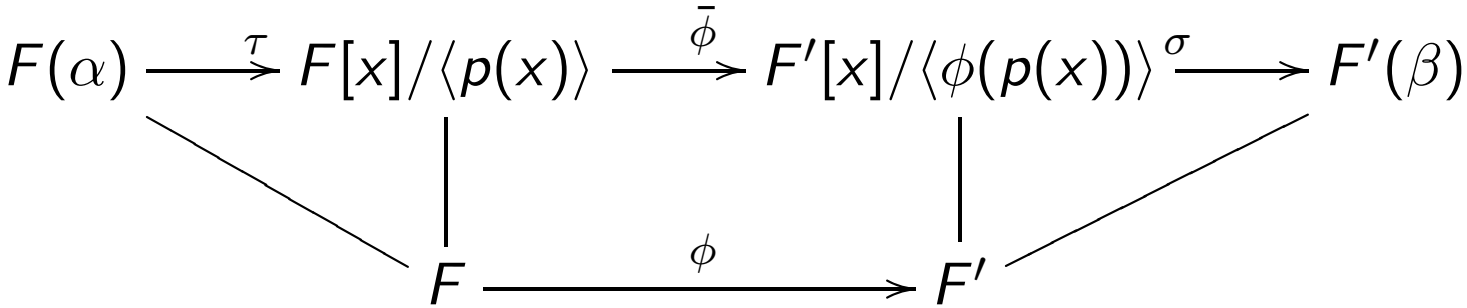
$$F(\alpha) \xrightarrow{\tau} F[x]/\langle p(x)\rangle \xrightarrow{\bar{\phi}} F'[x]/\langle \phi(p(x))\rangle \xrightarrow{\sigma} F'(\beta)$$

where $\bar{\phi}$ is the map $f(x) + \langle p(x)\rangle \mapsto \phi(f(x)) + \langle \phi(p(x))\rangle$, where again $\phi : F \to F'$ is a given isomorphism.

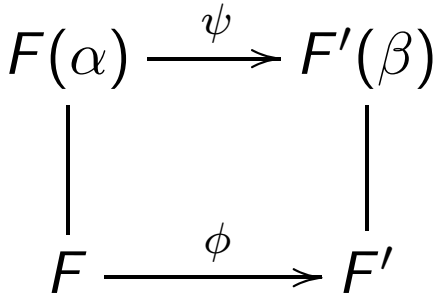
PROOF: (continued)
So with $\tau : F(\alpha) \to F[x]/\langle p(x)\rangle$ and $\sigma : F'[x]/\langle \phi(p(x))\rangle \to F'(\beta)$ we have that

$$\psi = \sigma \circ \bar{\phi} \circ \tau : F(\alpha) \to F'(\beta)$$

is an isomorphism



such that $\psi(c) = \phi(c)$ for all $c \in F$.



The principal consequence of this is what is termed the 'isomorphism extension theorem'.

Theorem

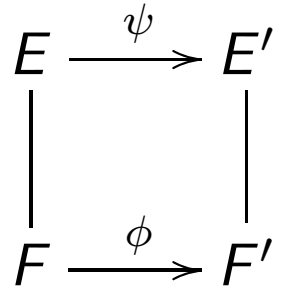
Let ϕ be an isomorphism from a field F to a field F' and let $f(x) \in F[x]$. If E is a splitting field of $f(x)$ over F and E' is a splitting field for $\phi(f(x))$ over F' then there is an isomorphism $\psi : E \to E'$ such that $\psi(c) = \phi(c)$ for $c \in F$.

$$\begin{array}{ccc} E & \xrightarrow{\psi} & E' \\ | & & | \\ F & \xrightarrow{\phi} & F' \end{array}$$

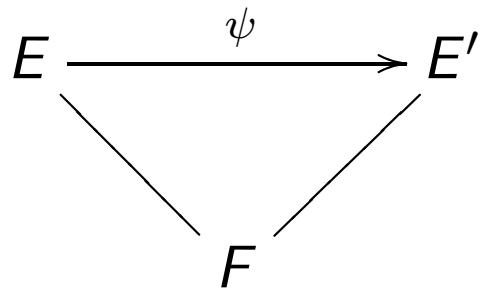
Proof.

Use induction on $n = deg(f(x))$ together with the previous lemma. $\square$

So with the above theorem:



if $F = F'$ with $\phi = Id$ then we deduce that any two splitting fields of $f(x)$ over F are isomorphic!



However, we shall use this result again later on to deduce a different important fact.

Theorem

Let $p(x) \in F[x]$ be an irreducible polynomial with splitting field E/F and let $\beta \in E$ be such that $g(\beta) = 0$ for some $g(x) \in F[x]$.

If $\tilde{\beta}$ is another root of $g(x)$ (in some extension field $\tilde{E}/E$) then, in fact, $\tilde{\beta} \in E$.

PROOF: Since E is the splitting field for $p(x)$, then if $\alpha_1, \ldots, \alpha_n$ are the roots of $p(x)$ then $E = F(\alpha_1, \ldots, \alpha_n)$.

Now let $g(x) \in F[x]$ have the root $\beta \in E$, then without loss of generality, we can assume that $g(x)$ is irreducible.

Let $\tilde{E} \supseteq E$ be the splitting field for $g(x)$ which contains the *other* root $\tilde{\beta}$.

By earlier work, there is a unique isomorphism $\sigma : F(\beta) \to F(\tilde{\beta})$ with $\sigma(\beta) = \tilde{\beta}$ and $\sigma(x) = x$ for $x \in F$.

So now E is the splitting field for $p(x)$ over $F(\beta)$ and $E(\tilde{\beta}) = F(\alpha_1, \ldots, \alpha_n, \tilde{\beta})$ is a splitting field for $p(x)$ over $F(\tilde{\beta})$

So one can extend the isomorphism $\sigma : F(\beta) \to F(\tilde{\beta})$ to an isomorphism $\tau : E = E(\beta) \to E(\tilde{\beta})$ where $\tau(\beta) = \tilde{\beta}$.

But now τ extends σ which is the identity on F so τ is the identity on F too.

Thus τ permutes $\{\alpha_1, \ldots, \alpha_n\}$ since it must take a root of $p(x)$ to another root of $p(x)$.

Since $\beta \in E = F(\alpha_1, \ldots, \alpha_n)$ then $\beta = h(\alpha_1, \ldots, \alpha_n)$ for some polynomial $h(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$.

Then

$$\tilde{\beta} = \tau(\beta) = \tau(h(\alpha_1, \ldots, \alpha_n)) = h(\tau(\alpha_1), \ldots, \tau(\alpha_n))$$

where now $\tau(\alpha_i) \in E$ so $h(\tau(\alpha_1), \ldots, \tau(\alpha_n)) \in E$ as well.
i.e. $\tilde{\beta} \in E$ after all. □

This phenomenon is given the following definition.

Definition

An extension E/F is called a normal extension if for each $\beta \in E$ all the roots of $irr(\beta, F)$ lie in E as well.

As such, for Galois theory, we are interested in separable, normal extensions E/F.

Now consider E/F a splitting field for some $p(x) \in F[x]$.
What we wish to show is that:

- $\sigma(a) = a$ for all $\sigma \in Gal(E/F)$ iff $a \in F$
- $[E : F] = |Gal(E/F)|$.

Once these facts are established, the rest of the fundamental theorem of Galois theory will follow.

And although we are studying splitting fields of the form $E = F(\alpha_1, \ldots, \alpha_n)$ we shall make extensive use of the primitive element theorem which means that $E = F(\alpha_1, \ldots, \alpha_n) = F(\gamma)$ for a 'primitive element' $\gamma \in E$.

The advantage of this is that the basis of $F(\gamma)$ is simply $\{1, \gamma, \ldots, \gamma^{n-1}\}$ where $[F(\gamma) : F] = n$.

This allows us to simplify and streamline the different technical facts which make up the fundamental theorem.

Throughout this discussion and all that follows, we will assume all fields are perfect.

Theorem

If E is a splitting field for some $f(x) \in F[x]$ then $|Gal(E/F)| = [E : F]$.

PROOF: Let $\gamma \in E$ be a primitive element, so that $E = F(\gamma)$ and let $p(x) = irr(\gamma, F)$.

If $\{\gamma_1, \ldots, \gamma_n\}$ are all the distinct roots of $p(x)$ (where say $\gamma = \gamma_1$) then these all lie in E since E is a splitting field for *a* polynomial so it contains the roots of $p(x) = irr(\gamma, F)$, but since $E = F(\gamma)$ then E is the splitting field of $p(x) = irr(\gamma, F)$ itself.

Moreover, if we consider any of the other roots γ_i where $q_i(x) = irr(\gamma_i, F)$, then since $I = \{g(x) \in F[x] \mid g(\gamma_i) = 0\} = \langle q_i(x) \rangle$ and $p(x) \in I$ we have that $q_i(x) \mid p(x)$, but both $p(x)$ and $q_i(x)$ are irreducible so they must be associates, however since $p(x)$ and $q_i(x)$ are monic, they must, in fact, be equal.

As such $F(\gamma_1) = F(\gamma_i)$ for $i = 1, \ldots, n$.

PROOF: (continued) And since $F(\gamma_1) = F(\gamma_i)$ then certainly $F(\gamma_1) \cong F(\gamma_i)$ for each $\gamma_i \in S = \{\gamma_1, \ldots, \gamma_n\}$.

Therefore we may define isomorphisms $\sigma_i : F(\gamma_1) \to F(\gamma_i)$ induced by letting $\sigma_i(\gamma_1) = \gamma_i$ and $\sigma_i(x) = x$ for $x \in F$.

But as $F(\gamma_i) = E$ for each $\gamma_i \in S$ then these $\sigma_i \in Gal(E/F)$, so $|Gal(E/F)| \geq |S| = n$.

So $Gal(E/F)$ contains $\{\sigma_1, \ldots, \sigma_n\}$ and if $\tau \in Gal(E/F)$ then $\tau(\gamma_1) = \tau(\gamma)$ is some other root of $irr(\gamma, F)$, but this means $\tau(\gamma_1) \in S$ so $\tau = \sigma_i$ for some i.

As such $|Gal(E/F)| = n$ exactly. □