Proof:

(1) The proof is by induction on $[E:k]$.

If $[E:k]=1$, that is $E=k$ then f is a product of linear factors in $k[x]$ hence $f_\varphi = \varphi_*(f)$ is a product of linear factors in $k'[x]$ and $E^\varphi = k'$, and $\varphi: \underset{k}{E} \to \underset{k'}{E'}$ is the extension of itself.

Assume $[E:k] > 1$ and let $f = p \cdot g$ where p is an irreducible factor of f of largest degree d among all irreducible factor of f. Then $d > 1$. ~~If f is separable~~ We have $f_\varphi = \varphi_*(p)\,\varphi_*(g)$, with $\varphi_*(p) = p_\varphi$ and $\varphi_*(g) = g_\varphi$,

and since f_φ is separable p_φ has exactly d roots $\alpha_1^\varphi, \dots, \alpha_d^\varphi$ all contained in E_φ since E_φ^* is a splitting field of f_φ.

Let $\alpha \in R(p)$. By Lemma II.15 we have for every root α_i^* an extension

$$\hat{\varphi}_i : k(\alpha) \longrightarrow E_*,$$

with $\hat{\varphi}_i(\alpha) = \alpha_i^*$.

Exercise: if $\hat{\varphi} : k(\alpha) \longrightarrow E_*$ is any extension of $\varphi' : k \to k'$ then $\hat{\varphi} = \hat{\varphi}_i$ for some $1 \le i \le d$.

Thus there are precisely d extensions $\hat{\varphi} : k(\alpha) \to E_*$ of $\varphi : k \to k'$, one for each root of p_*. Now fix such an extension

$$\hat{\varphi} : k(\alpha) \longrightarrow k'(\alpha_*), \quad \alpha_* \in \{\alpha_1^*, \dots, \alpha_d^*\}.$$

Then $[E : k(\alpha)] = [E : k]/d < [E : k]$.

Now E is a splitting field of f over $k(\alpha)$ and $\hat{\varphi}_*(f) = f_*$, and E_* is a splitting

field of f_* over $k'(\alpha_*)$. By recurrence $\hat{\varphi}$ has $[E:k(\alpha_1)] = [E:k]/d$ extensions to $E \to E_*$ and as a result $\varphi: k \to k'$ has $[E:k(\alpha)]d = [E:k]$ extensions.

(2) Take $k = k'$, $\varphi = id_k$, $E = E_*$. ∎

Remark: The equality $[E:k] = |Gal(E|k)|$ establishes a relation between two quantities that are both difficult to compute in practice.

The following corollary is very useful

Corollary II.18 (Corol. A-5.7) Let $E|k$ be the splitting field of a separable polynomial $f \in k[x]$ of degree n. If f is irreducible

$$n \mid |Gal(E|k)|.$$

Proof: Let $\alpha \in E$ be a root of f.

Since f is irreducible $[k(\alpha) : k] = n$

which together with

$$|Gal(E/k)| = [E : k] = [E : k(\alpha)]\,[k(\alpha) : k]$$

gives the result. ∎

Pf: Let $\alpha \in E$ be a root of f.

Since f is irreducible $[k(\alpha):k] = n$

which together with

$$|Gal(E|k)| = [E:k] = [E:k(\alpha)][k(\alpha):k]$$

gives the result. ∎

Here is a first nice application of the extension theorem: (Thm. A.5.13)

Corollary II.19 Let p be prime, $n \geq 1$.

Then $Gal(\mathbb{F}_{p^n}|\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$

and a generator is given by the Frobenius automorphism:

$$F_r : \overline{\mathbb{F}}_{p^n} \longrightarrow \overline{\mathbb{F}}_{p^n}$$
$$x \longmapsto x^p.$$

Proof:

(1) $\mathbb{F}_{p^n}$ is a splitting field of the polynomial $X^{p^n-1}-1$; indeed, since the group $\mathbb{F}_{p^n}^{\times}$ has order p^n-1, $x^{p^n-1}=1 \ \forall x \in \mathbb{F}_{p^n}^{\times}$ and thus

$$\mathbb{F}_{p^n} = \{0\} \cup \text{Roots}\left(X^{p^n-1}-1\right)$$

which shows that $\mathbb{F}_{p^n}$ is a splitting field of said polynomial.

(2) Now $\dim(\mathbb{F}_{p^n}/\mathbb{F}_p)=n$ and $X^{p^n-1}-1$ is separable hence by Thm.

$$|\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|=n.$$

(3) Clearly $Fr \in \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Let's show it has order n: assume $1 \le k \le n$ is its order. Then $Fr^k = Id_{\mathbb{F}_{p^n}}$.

— II-22 —

But $\mathrm{Fr}^k(x) = x^{p^k}$, so every $x \in \mathbb{F}_{p^n}$ is a root of $X^{p^k} - X = 0$ and hence $p^n \leq p^k$ which implies $k = n$. ∎

Next we turn to an example where the Galois group of a polynomial is as big as possible.

Thm II.20. Let p be a prime number and $f \in \mathbb{Q}[X]$ a polynomial of degree p (with splitting field E). Assume that f is irreducible and has exactly $p-2$ real roots. Then $\mathrm{Gal}(E/\mathbb{Q}) \simeq S_p$.

We will need the following input from finite group theory:

Lemma II.21 (Cauchy) Let G be a finite group and p a prime with $p \mid |G|$. Then G contains an element of order p.

Proof: Consider

$$\Gamma_p = \{(g_1, \dots, g_p) \in G^p : g_1 \cdots g_p = e\}.$$

The symmetric group S_p acts on G^p via $\tau(g_1, \dots, g_p) = (g_{\tau(1)}, \dots, g_{\tau(p)})$, $\tau \in S_p$. Let $\sigma = (1, 2, \dots, p)$, that is a p-cycle and $C_p := \{\sigma^i : 0 \le i \le p-1\} < S_p$ the cyclic subgroup of order p generated by σ. We claim that C_p preserves Γ_p:

Indeed if $g_1 \cdots g_p = e$ then

$$(g_1 \cdots g_i)^{-1} g_1 \cdots g_p = g_{i+1} \cdots g_p g_1 \cdots g_i = e$$

but $\sigma^i(g_1, \ldots, g_p) = (g_{i+1}, g_{i+2}, \ldots g_p, g_1 \cdots g_i)$.

Now Γ_p is a disjoint union of C_p-orbits and since p is prime such an orbit has either cardinality 1 or p. Let

$$\Gamma_p = \bigsqcup_{i=1}^{r} \mathcal{O}_i \bigsqcup \bigsqcup_{j=r+1}^{\ell} \mathcal{O}_j$$

where $|\mathcal{O}_i| = p \quad 1 \le i \le r$

$$|\mathcal{O}_j| = 1 \quad \text{for } j \le \ell.$$

Thus $|\Gamma_p| = r \cdot p + (\ell - r) \cdot 1$

~~Neither since that~~ Observe that

~~$|\Gamma_p| = |G|^{p-1}$~~ $(e, \ldots, e) \in \Gamma_p$

gives an orbit of cardinality 1, hence

$l - r \geq 1$. On the other hand

$|\Gamma_p| = |G|^{p-1}$ hence $p \mid |\Gamma_p|$, which implies $l - r \geq 2$; that is there is $(h, \ldots, h) \in \Gamma_p$ with $h \neq e$ which proves the lemma. □

Proof of Thm 2.20

Let $\mathbb{Q} \subset E \subset \mathbb{C}$ be a splitting field of f and $R(f) = \{\alpha_1, \ldots, \alpha_p\}$ numbered in such a way that $\{\alpha_2, \ldots, \alpha_p\} \subset \mathbb{R}$.

~~Now the complex conjugation $\varepsilon : \mathbb{C} \to \mathbb{C}$~~

~~$z \mapsto \bar{z}$~~

~~fixes $\alpha_3, \ldots, \alpha_p$ and interchanges α_1, α_2.~~

~~Thus $\varepsilon(E) = E$ and~~

Using lemma II.7 we consider $Gal(E/\mathbb{Q})$ as a subgroup of S_p.

Notice that the complex conjugation $\varepsilon : \mathbb{C} \to \mathbb{C}, z \mapsto \bar{z}$, fixes $\alpha_3, \ldots, \alpha_p$ and interchanges α_1, α_2. Since $E = \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ this implies $\varepsilon(E) = E$ and that $\varepsilon|_E \in Gal(E/\mathbb{Q}) < S_p$ is the transposition (12).

Since f is irreducible, Corollary II.18 implies $p \mid |Gal(E/\mathbb{Q})|$ and by Cauchy's theorem (lemma II.21) $Gal(E/\mathbb{Q})$ contains an element η of order p. Thus η is a p-cycle (exercise) and since p is prime, a transposition and a p-cycle generate S_p (exercise). ∎

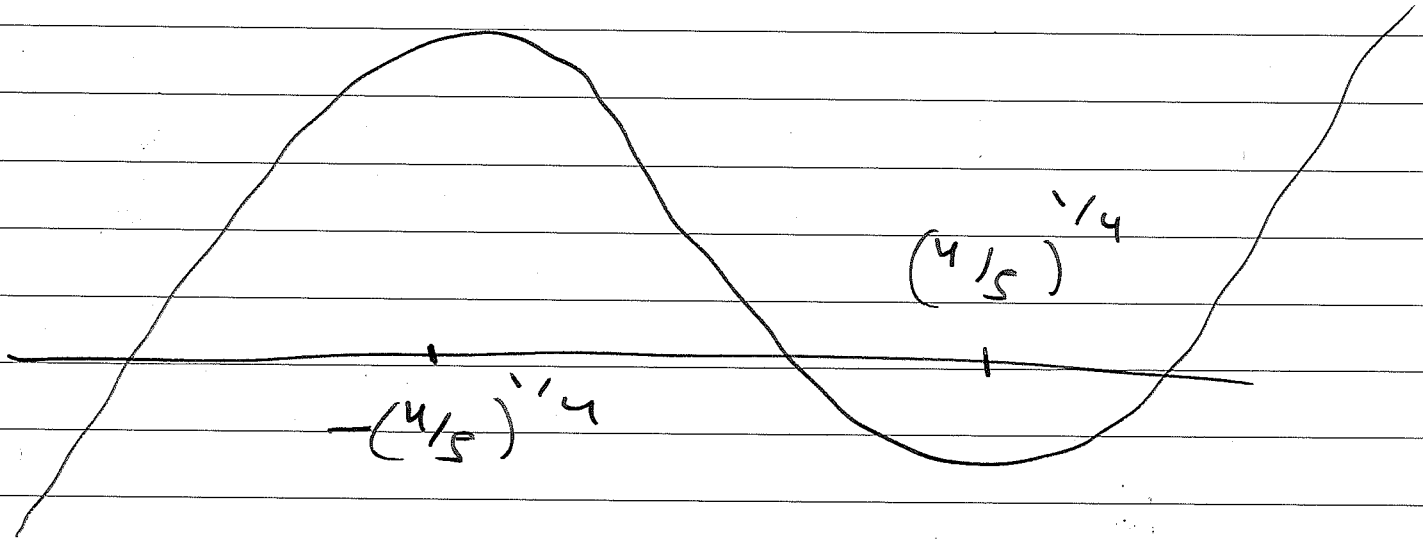
Corollary II.22 The Galois group of $x^5 - 4x + 2$ is isomorphic to S_5.

Proof: By Eisenstein's criterion

$$x^5 - 4x + 2 \in \mathbb{Q}[x]$$

is irreducible.

By computing local extrema, we see that the graph of f has the following shape:



Thus f has exactly $3 = 5 - 2$ real zeros and the theorem II.20. applies. ∎