Content:

Theorem Fundamental Theorem of Galois Theory. Let $F \lhd E$, $G = \mathrm{Gal}(E/F)$.
(1) There is a 1-1 correspondence between the intermediate fields between F and E and subgroups of G. The correspondence is $K \mapsto \mathrm{Gal}(E/K)$ and $H \mapsto E^H$.
(2) If K_1, K_2 are intermediate fields corresponding to H_1 and $H_2 \leq G$, then $K_1 \subseteq K_2 \Leftrightarrow H_2 \leq H_1$.
(3) If the intermediate field K corresponds to $H \leq G$, then $[E:K] = [H:\mathrm{Id}] = |H|$ and $[K:F] = [G:H]$.
(4) $K \lhd E$.
(5) $F \lhd K \Leftrightarrow H \lhd G$, where H is the subgroup corresponding to K. In this case, $\mathrm{Gal}(K/F) \cong G/H$.

Example $p(x) = x^4 - 4x^2 - 1 \in \mathbb{Q}[x]$. Let E be the splitting field for $p(x)$.
(1) $E = \mathbb{Q}(\sqrt{2+\sqrt{5}}, i)$; (2) A basis for E over Q is ; (3) $|\mathrm{Gal}(E/\mathbb{Q})| = 8$;
(4) $\varphi_1 =$; $\varphi_2 =$; $\varphi_3 =$; $\varphi_4 =$; $\varphi_5 =$; $\varphi_6 =$; $\varphi_7 =$; $\varphi_8 =$; (5)

Theorem Fundamental Theorem of Galois Theory. Let $F \lhd E$, $G = \mathrm{Gal}(E/F)$.
(1) There is a 1-1 correspondence between the intermediate fields between F and E and subgroups of G. The correspondence is $K \mapsto \mathrm{Gal}(E/K)$ and $H \mapsto E^H$.
(2) If K_1, K_2 are intermediate fields corresponding to H_1 and $H_2 \leq G$, then $K_1 \subseteq K_2 \Leftrightarrow H_2 \leq H_1$.
(3) If the intermediate field K corresponds to $H \leq G$, then $[E:K] = [H:\mathrm{Id}] = |H|$ and $[K:F] = [G:H]$.
(4) $K \lhd E$.
(5) $F \lhd K \Leftrightarrow H \lhd G$, where H is the subgroup corresponding to K. In this case, $\mathrm{Gal}(K/F) \cong G/H$.

(1) Proof:
See Lecture Notes 4/21/10, Proof for Theorem $*$.

(2) Proof:
Let $H_1 = \mathrm{Gal}(E/K_1)$, $H_2 = \mathrm{Gal}(E/K_2)$.
Assume $K_1 \subseteq K_2$. Need to show $K_1 \subseteq K_2 \Rightarrow \mathrm{Gal}(E/K_2) \subseteq \mathrm{Gal}(E/K_1)$.
Let $\varphi \in \mathrm{Gal}(E/K_2)$. Then $\varphi: E \to E$ and fixes K_2.
Since $K_1 \subseteq K_2$, then φ fixes K_1, hence $\varphi \in \mathrm{Gal}(E/K_1)$.
Since $\mathrm{Gal}(E/K_2) \leq \mathrm{Aut}(E)$, $\mathrm{Gal}(E/K_1) \leq \mathrm{Aut}(E)$, and $\mathrm{Gal}(E/K_2) \subseteq \mathrm{Gal}(E/K_1)$, then $\mathrm{Gal}(E/K_2) \leq \mathrm{Gal}(E/K_1)$. $\therefore H_2 \leq H_1$.

Conversely, assume $H_2 \leq H_1$. Need to show $H_2 \leq H_1 \Rightarrow E^{H_1} \subseteq E^{H_2}$.
Clearly $H_2 \subseteq H_1$. By Galois Theory II Homework #1(b), we have shown $E^{H_1} \subseteq E^{H_2}$. So $E^{\mathrm{Gal}(E/K_1)} \subseteq E^{\mathrm{Gal}(E/K_2)}$.
By (1) of this theorem $K_1 = E^{H_1}$ and $K_2 = E^{H_2}$. Thus $K_1 = E^{\mathrm{Gal}(E/K_1)} \subseteq E^{\mathrm{Gal}(E/K_2)} = K_2$ as desired.

(3) Proof:
If K corresponds to H, then $K = E^H$. So $[E:K] = [E:E^H] = |H|$.
Since $F \lhd E$, then $E^G = F$. Thus $[E:F] = [E:E^G] = |G|$.
$[K:F] = \dfrac{[E:F]}{[E:K]} = \dfrac{|G|}{|H|} = [G:H]$ (by Lagrange's Theorem).

(4) Proof:
Homework

(5) Proof:
Assume $F \lhd K$. Define θ: $\mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$ by $\sigma \mapsto \sigma|_K$.
Composition is preserved, so it is a homomorphism.
We need to be worried about whether it lands in K.
But we have shown in ** that if $H \lhd G$, then $\sigma(K) = K$.
Thus $\sigma|_K \in \mathrm{Gal}(K/F)$. Clearly θ is a homomorphism.
We want to show $H = \mathrm{Gal}(E/K)$ is the kernel of G.
$\sigma \in \ker \varphi \Leftrightarrow \sigma|_K = \mathrm{Id}_K \Leftrightarrow \sigma$ fixes $K \Leftrightarrow \sigma \in \mathrm{Gal}(E/K)$.
So $\ker \theta = \mathrm{Gal}(E/K)$
We want to show onto.
Since $F \lhd E$,
E is a splitting field for some separable polynomial $f \in F[x]$.
So E is a splitting field for f over K.
Thus, any automorphism of K can be extended to E.
(i.e. $\forall\, \gamma \in \mathrm{Gal}(K/F)\ \exists\, \sigma \in \mathrm{Gal}(E/F)$ such that $\sigma|_K = \gamma$.)

Note From this theorem, we have

F	$\mathrm{Gal}(E/F)$
$\lvert\ [K:F] = m = [\mathrm{Gal}(E/F):\mathrm{Gal}(E/K)]$	$\lvert$
K	$\mathrm{Gal}(E/K)$
$\lvert\ [E:K] = n = [\mathrm{Gal}(E/K):\mathrm{Gal}(E/E)]$	$\lvert$
E	$\mathrm{Gal}(E/E)$

Example $p(x) = x^4 - 4x^2 - 1 \in \mathbb{Q}[x]$. Let E be the splitting field for $p(x)$.

(1) $E = \mathbb{Q}(\sqrt{2+\sqrt{5}}, i)$.

Proof:

$x^2 = 2 \pm \sqrt{5}$, so $x = \pm\sqrt{2 \pm \sqrt{5}}$.

$E = \mathbb{Q}(\sqrt{2+\sqrt{5}}, \sqrt{2-\sqrt{5}})$. Let $\alpha = \sqrt{2+\sqrt{5}}$, $\beta = \sqrt{2-\sqrt{5}}$.

Since $\alpha\beta = i$, then $\beta = \alpha^{-1}i$, hence $E = \mathbb{Q}(\alpha, i)$.

(2) A basis for E over $\mathbb{Q}$ is $\{1, i, \alpha, \alpha^2, \alpha^3, \alpha i, \alpha^2 i, \alpha^3 i\}$;

Proof:

We know $[\mathbb{Q}(\alpha, i):\mathbb{Q}] = [\mathbb{Q}(\alpha, i):\mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha):\mathbb{Q}]$.

Since $p(x)$ is irreducible over $\mathbb{Q}$ and deg $p = 4$, then $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$.

Since $f(x) = x^2 + 1$ is irreducible over $\mathbb{Q}(\alpha)$

and deg $f = 2$, then $[\mathbb{Q}(\alpha, i):\mathbb{Q}(\alpha)] = 2$.

Thus, $[\mathbb{Q}(\alpha, i):\mathbb{Q}] = 8$.

And elements of $\mathbb{Q}(\alpha)$ look like $c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3$ where $c_i \in \mathbb{Q}$.

Thus elements of $\mathbb{Q}(\alpha, i)$ look like

$c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + i(c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3)$

(3) $|\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})| = 8$;

Proof:

Since E is a splitting field for a separable polynomial over $\mathbb{Q}$,

then $\mathbb{Q} \lhd E$.

So $|\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})| = [\mathbb{Q}(\alpha, i):\mathbb{Q}] = 8$.

(4) Description of the automorphisms of E over $\mathbb{Q}$.

Since $x^2 + 1 = (x + i)(x - i) \in \mathbb{Q}(\alpha, i)[x]$, then $\forall\ \varphi \in \mathrm{Gal}(E/\mathbb{Q})$, $\varphi(i) = \pm i$. Since $p(x) = (x + \alpha)(x - \alpha)(x + \beta)(x - \beta) \in \mathbb{Q}(\alpha)[x]$, then $\forall\ \varphi \in \mathrm{Gal}(E/\mathbb{Q})$, $\varphi(\alpha) = \pm\alpha, \pm\beta$. Thus there are at most 8 automorphisms. Since $|\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})| = 8$, then there are exactly 8.

(5) Description of automorphisms as permutations of S_n.

	$\varphi_i(\alpha)=$	$\varphi_i(-\alpha)=$	$\varphi_i(\beta)=$	$\varphi_i(-\beta)=$	
$\varphi_1 = \mathrm{Id};$	α	$-\alpha$	β	$-\beta$	(1)
$\varphi_2(i) = i, \varphi_2(\alpha) = -\alpha;$	$-\alpha$	α	$-\beta$	β	(12)(34)
$\varphi_3(i) = i, \varphi_3(\alpha) = \beta;$	β	$-\beta$	α	$-\alpha$	(13)(24)
$\varphi_4(i) = i, \varphi_4(\alpha) = -\beta;$	$-\beta$	β	$-\alpha$	α	(14)(23)
$\varphi_5(i) = -i, \varphi_5(\alpha) = \alpha;$	α	$-\alpha$	$-\beta$	β	(34)
$\varphi_6(i) = -i, \varphi_6(\alpha) = -\alpha;$	$-\alpha$	α	β	$-\beta$	(12)
$\varphi_7(i) = -i, \varphi_7(\alpha) = \beta;$	β	$-\beta$	$-\alpha$	α	(1324)
$\varphi_8(i) = -i, \varphi_8(\alpha) = -\beta.$	$-\beta$	β	α	$-\alpha$	(1423)

Proof:
Since $\alpha\beta = i$, then
$\varphi_2(\beta) = \varphi_2(\alpha^{-1}i) = \varphi_2(\alpha)^{-1}\varphi_2(i) = (-\alpha)^{-1}i = -(\alpha^{-1}i) = -\beta.$
$\varphi_3(\beta) = \varphi_3(\alpha^{-1}i) = \varphi_3(\alpha)^{-1}\varphi_3(i) = \beta^{-1}i = \alpha.$
$\varphi_5(\beta) = \varphi_5(\alpha^{-1}i) = \varphi_5(\alpha)^{-1}\varphi_5(i) = \alpha^{-1}(-i) = -(\alpha^{-1}i) = -\beta.$
The rest follow.

Since$|\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})| = 8$, then $\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_8, D_8$, or Q_8.
Since (1324)(14)(23) = (14)(23) and (14)(23)(1324) = (12)((34), then $\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ is not abelian which rules out $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_8$.
Since $\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ has 5 elements of order 2,
then $\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q}) \ncong Q_8$.
Thus $\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q}) \cong D_8$.