Content:

Example	Gal $(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$.
Theorem	Let $p(x) \in F[x]$; deg $p(x) = n$, then Gal$(E/F) \cong$ a subgroup of S_n.
Example	If $\alpha \in \{e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}\}$, then Aut$(E) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$. Is there a bigger field that φ_4 fixes?
Definition	Fixed Field
Proposition	E^S is a subfield of E.
Proposition	$S \subseteq T \Rightarrow E^T \subseteq E^S$.
Example	$S = \{\varphi_4\}$, $E^S = \mathbb{Q}(\alpha + \alpha^4)$, $H = \{\varphi_1, \varphi_4\}$, $E^H = \mathbb{Q}(\alpha + \alpha^4)$.
Theorem	If $S \subseteq$ Aut(E) and $\lvert S\rvert = n$, then $[E:E^S] \geq n$.

Recall Gal$(E/F) \leq$ Aut(E).

Recall $(*)$ Let $p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$, and
$X = \{\alpha | p(\alpha) = 0\} = \{e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}\}$.
If E is a splitting field for $p(x)$, then Aut$(E) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$.

Example (1) Gal$(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ = Aut$(\mathbb{Q}(\sqrt{5})) \cong \mathbb{Z}_2$.
(2) Gal$(\mathbb{Q}(\alpha)/\mathbb{Q})$ = Aut$(\mathbb{Q}(\alpha)) \cong \mathbb{Z}_4$.

Example Gal $(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$.

Proof:
Let $a + bi \in \mathbb{C}$ where $a, b \in \mathbb{R}$. Let $\varphi \in$ Gal$(\mathbb{C}/\mathbb{R})$. Then φ fixes $\mathbb{R}$.
Then $\varphi(a + bi) = a + b\varphi(i)$
Let $f(x) = x^2 + 1 = (x + i)(x - i)$.
Since i is a root of f, then $\varphi(i)$ must be a root of $x^2 + 1$.
So $\varphi(i) = i$ or $\varphi(i) = -i$.

$\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[x]/(x^2 + 1) \cong \mathbb{R}(-i) = \mathbb{C}$.
So $\varphi \in$ Gal$(\mathbb{C}/\mathbb{R})$ where $\varphi(i) = -i$ is an isomorphism.

Theorem Let $p(x) \in F[x]$ and deg $p(x) = n$, and let E be a splitting field of $p(x)$ over F, then Gal$(E/F) \cong$ a subgroup of S_n.

Proof:
Let $X = \{a_1, \ldots, a_n\}$ be the roots of $p(x)$. $E = F(a_1, \ldots, a_n)$.
So any element of Gal(E/F) permutes the roots of $p(x)$.
That is, $\sigma \in \text{Gal}(E/F) \Rightarrow \sigma|_X \in S_X$.
Define φ: Gal$(E/F) \to S_X$ by $\varphi(\sigma) = \sigma|_X$.
φ is a homomorphism. You check.
Let $\sigma, \tau \in \text{Gal}(E/F)$. Let $a \in X$.
$\varphi(\sigma\circ\tau) = \sigma\circ\tau|_X$, where $\sigma\circ\tau|_X : X \to X$
and $\varphi(\sigma)\circ\varphi(\tau) = \sigma|_X \circ \tau|_X$ where $\sigma|_X : X \to X$ and $\tau|_X : X \to X$.
So $\sigma\circ\tau|_X(a) = \sigma(\tau(a)) = (\sigma|_X \circ \tau|_X)(a)$.
Thus $\varphi(\sigma\circ\tau) = \varphi(\sigma)\circ\varphi(\tau)$.
So then Gal $(E/F)/\ker\varphi \cong \varphi(\text{Gal}(E/F) \leq S_X$.
Need to show ker $\varphi = \{\text{Id}_E\}$. Note ker $\varphi = \{\sigma \in \text{Gal}(E/F) | \varphi(\sigma) = \text{Id}_X\}$
Let $\gamma \in \ker\varphi$. Then $\varphi(\gamma) = \text{Id}|_X$.
So γ fixes F and γ fixes a_i $\forall$ i.
By Monday's proposition, $\gamma = \text{Id}_E$. (as $E = F(a_1, \ldots, a_n)$).
Thus ker $\varphi = \{\text{Id}_E\}$.
So Gal $(E/F)/\ker\varphi \cong \varphi(\text{Gal}(E/F) \leq S_X \cong S_n$ (as $|X| = n$).

Example For E referenced in Recall (∗), Aut$(E) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$.

	S_4
$\varphi_1(\alpha) = \alpha$	(1)
$\varphi_2(\alpha) = \alpha^2$	(1243)
$\varphi_3(\alpha) = \alpha^3$	(1342)
$\varphi_4(\alpha) = \alpha^4$	(14)(23)

This is a subgroup of S_4.

New Section Fixed Fields

Example For Aut(E) reference in Recall ($*$), is there a bigger field that φ_4 fixes?
Yes.

Proof:
We know $\varphi_4(\alpha) = \alpha^4$; $\varphi_4(\alpha^2) = \alpha^3$; $\varphi_4(\alpha^3) = \alpha^2$; $\varphi_4(\alpha^4) = \alpha$.
We also have $\varphi_4(\alpha + \alpha^4) = \alpha^4 + \alpha$, and $\varphi_4(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^2$.
Let $K = \mathbb{Q}(\alpha + \alpha^4)$.
Then $\mathbb{Q} \subseteq \mathbb{Q}(\alpha + \alpha^4) \subseteq \mathbb{Q}(\alpha)$.
Since φ_4 fixes $\mathbb{Q}$ and φ_4 fixes $\alpha + \alpha^4$, then φ_4 fixes K.
And since $\alpha + \alpha^4$, $= e^{\frac{2n\pi i}{5}} + e^{\frac{8n\pi i}{5}} = e^{\frac{2n\pi i}{5}} + e^{\left(2\pi - \frac{2\pi}{5}\right)ni} = \alpha + \overline{\alpha} = 2\cos^{2\pi}/_{5} \notin \mathbb{Q}$,
then $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha + \alpha^4)$.

Is there a bigger field than K that φ_4 fixes? No.

Proof:
Suppose $\exists$ L, a field fixed by φ_4 such that $K \subsetneq L \subseteq \mathbb{Q}(\alpha)$.
We know $4 = [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(\alpha + \alpha^4)]\ [\mathbb{Q}(\alpha + \alpha^4):\mathbb{Q}]$.
So then $4 = [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):L]\ [L: \mathbb{Q}(\alpha + \alpha^4)]\ [\mathbb{Q}(\alpha + \alpha^4):\mathbb{Q}]$.
Since $\alpha + \alpha^4 \notin$ Q, then $[\mathbb{Q}(\alpha + \alpha^4):\mathbb{Q}] \neq 1$, hence $[\mathbb{Q}(\alpha + \alpha^4):\mathbb{Q}] > 1$.
And since $K \subsetneq L$, then $[L: \mathbb{Q}(\alpha + \alpha^4)] \neq 1$, hence $[L: \mathbb{Q}(\alpha + \alpha^4)] > 1$.
Thus, $[\mathbb{Q}(\alpha):L] = 1$, hence $\mathbb{Q}(\alpha) = L$.
Thus, φ_4 fixes all elements in $\mathbb{Q}(\alpha)$.
But this is a contradiction as $\varphi_4(\alpha) \neq \alpha$.
So there is no bigger field than K that φ_4 fixes.

Definition Let S be a subset of Aut(E).
The *fixed field* of S is the set $E^S = \{x \in E \mid \varphi(x) = x\ \forall\ \varphi \in S\}$.

Example If $S = \{\varphi_4\}$, then $E^S = \mathbb{Q}(\alpha + \alpha^4)$.

Proposition E^S is a subfield of E.

Proof:
Clearly $E^S \subseteq E$. Let $\varphi \in S$.
$0 \in E^S$ and $1 \in E^S$ as $\varphi(0) = 0$ and $\varphi(1) = 1$ by homomorphism properties, so $E^S \neq \emptyset$.
Let $a, b \in E^S$. Then by homomorphism properties we have
$\varphi(a - b) = \varphi(a) - \varphi(b) = a - b$, $\varphi(ab) = \varphi(a)\varphi(b) = ab$, and $\varphi(a^{-1}) = \varphi(a)^{-1} = a^{-1}$.
Since φ was arbitrary, then $a - b$, ab, and $a^{-1} \in E^S$.
Hence E^S is a subfield of E.

Proposition $S \subseteq T \Rightarrow E^T \subseteq E^S$.

Proof:
Let $a \in E^T$. Let $\sigma \in S$. Since $S \subseteq T$, then $\sigma \in T$. Thus $\sigma(a) = a$.
Hence $a \in E^S$.

Example $S = \{\varphi_4\}$, $E^S = \mathbb{Q}(\alpha + \alpha^4)$, $H = \{\varphi_1, \varphi_4\}$, $E^H = \mathbb{Q}(\alpha + \alpha^4)$.
So $S = \{\varphi_4\} \subsetneq \{\varphi_1, \varphi_4\} = H$, and $E^H = \mathbb{Q}(\alpha + \alpha^4) = E^S$.

Note $[E:E^S] = [\mathbb{Q}(\alpha):\mathbb{Q}(\alpha + \alpha^4)]$.
$4 = [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(\alpha + \alpha^4)]\ [\mathbb{Q}(\alpha + \alpha^4):\mathbb{Q}]$.
We know $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha + \alpha^4)] \neq 1$ as $\alpha \notin \mathbb{Q}(\alpha + \alpha^4)$ and φ_4 does not fix α, but φ_4 fixes everything in $\mathbb{Q}(\alpha + \alpha^4)$.
And, clearly $[\mathbb{Q}(\alpha + \alpha^4):\mathbb{Q}] \neq 1$. Thus, $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha + \alpha^4)] = 2$.

Theorem If $S \subseteq \text{Aut}(E)$ and $|S| = n$, then $[E:E^S] \geq n$.

Proof:
Let $S = \{\sigma_1, \sigma_2, \ldots, \sigma_n\} \subseteq \text{Aut(E)}$. Then $|S| = n$.
Suppose $[E:E^S] = r < n$.
Then there is a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_r\} \subseteq E$ for E over E^S.
Consider the following homogeneous system of equations in E.
$\sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n = 0$
$\sigma_1(\alpha_2)x_1 + \cdots + \sigma_n(\alpha_2)x_n = 0$
$\vdots$
$\sigma_1(\alpha_r)x_1 + \cdots + \sigma_n(\alpha_r)x_n = 0$
This is a homogeneous system with r equations and n unknowns.
Since $r < n$, there is a nontrivial solution to this system. Choose a nontrivial solution $(c_1, \ldots, c_k, 0, \ldots, 0)$ that has the smallest number, k, of nonzero components. By reindexing the α_i's, we may assume that the nonzero terms come first. Substituting our solution into the system of equations above gives:
$\sigma_1(\alpha_1)c_1 + \cdots + \sigma_k(\alpha_1)c_k = 0$
$\sigma_1(\alpha_2)c_1 + \cdots + \sigma_k(\alpha_2)c_k = 0$
$\vdots$
$\sigma_1(\alpha_r)c_1 + \cdots + \sigma_k(\alpha_r)c_k = 0$

Let $\beta \in E$. Then $\beta = b_1\alpha_1 + \cdots + b_r\alpha_r$, where $b_i \in E^S$.
Let $\sigma_i \in S$.
Since σ_i fixes elements of E^S, we have
$\sigma_i(\beta) = \sigma_i(b_1)\sigma_i(\alpha_1) + \cdots + \sigma_i(b_r)\sigma_i(\alpha_r)$
$= b_1\sigma_i(\alpha_1) + \cdots + b_r\sigma_i(\alpha_r)$.
And now we multiply the first equation in the previous system by b_1, the 2nd one by b_2, and so on, and add the resulting columns.
$b_1\sigma_1(\alpha_1)c_1 + \cdots + b_1\sigma_k(\alpha_1)c_k = 0$
$b_2\sigma_1(\alpha_2)c_1 + \cdots + b_2\sigma_k(\alpha_2)c_k = 0$
$\vdots$
$b_r\sigma_1(\alpha_r)c_1 + \cdots + b_r\sigma_k(\alpha_r)c_k = 0$

$\sigma_1(\beta)c_1 + \cdots + \sigma_k(\beta)c_k = 0$ $(**)$
(Since each column gives a sum of $(b_1\sigma_i(\alpha_1) + \cdots + b_r\sigma_i(\alpha_r))c_i$.)
Since β was arbitrary, then $(**)$ holds for each $\beta \in E$.
And note that c_i were chosen so that there is no shorter relation of this form for which $(**)$ holds.
We will now construct a shorter relation than $(**)$.
But, first note, $k \neq 1$. Otherwise, $\sigma_1(\beta) = 0$ $\forall$ $\beta \in E$, but σ_1 fixes $E^S \subseteq E$.
So $k > 1$. Thus $\sigma_1 \neq \sigma_k$, hence $\exists$ $\gamma \in$ E such that $\sigma_1(\gamma) \neq \sigma_k(\gamma)$.
For arbitrary $\beta \in E$, we have $\beta\gamma \in E$.
So $0 = \sigma_1(\beta\gamma)c_1 + \cdots + \sigma_k(\beta\gamma)c_k = \sigma_1(\beta)\sigma_1(\gamma)c_1 + \cdots + \sigma_k(\beta)\sigma_k(\gamma)c_k$.
And $\sigma_k(\gamma)(\sigma_1(\beta)c_1 + \cdots + \sigma_k(\beta)c_k) - \sigma_1(\beta)\sigma_1(\gamma)c_1 + \cdots + \sigma_k(\beta)\sigma_k(\gamma)c_k$
$= \sigma_1(\beta)(\sigma_k(\gamma) - \sigma_1(\gamma))c_1 + \sigma_2(\beta)(\sigma_k(\gamma) - \sigma_2(\gamma))c_2 + \cdots + \sigma_k(\beta)(\sigma_k(\gamma) - \sigma_k(\gamma))c_k = 0$.
Notice that the coefficient of c_1 is not 0, but the coefficient of c_k is 0.
So, we can rewrite the preceding equation as
$\sigma_1(\beta)d_1c_1 + \cdots + \sigma_{k-1}(\beta)d_{k-1}c_{k-1} = 0$, where $d_i = \sigma_k(\gamma) - \sigma_i(\gamma)$ for each i.
But this is a contradiction as there is no shorter relation of the form $(**)$ which holds.
$\therefore$ $[E:E^S] \geq n$.