Content:

Theorem	If $S \subseteq \text{Aut}(E)$ and $\lvert S\rvert = n$, then $[E:E^S] \geq n$.
Corollary	If $S \subseteq \text{Aut}(E)$ and $\lvert S\rvert = \infty$, then $[E:E^S] = \infty$.
Theorem	If $G \leq \text{Aut}(E)$, then $[E:E^G] = \lvert G\rvert$.
Corollary	$[E:E^{\text{Gal}(E/F)}] = \lvert\text{Gal}(E/F)\rvert$.
Example	If $G = \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ where α is a primitive 5^{th} root of unity, then $E^G = \mathbb{Q}$.
Example	If $G = \text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}_2$, then $E^G = \mathbb{Q}$.
Example	If $G = \text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\text{Id}\}$, then $E^G = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$.
Definition	Normal Extension

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

Proof: See Lecture Notes 4/7/10

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

Proof: Homework

Let $n \in \mathbb{N}$. Let $T = \{\sigma_1, \ldots, \sigma_n\} \subseteq S$. By part (b), $E^S \subseteq E^T$.
By part (a) E^T and E^S are subfields of E, hence E^S is a subfield of E^T.
If $[E:E^T]$ or $[E^T:E^S]$ is infinite, then $[E:E^S]$ is infinite by Theorem 39 of Extension Fields Part I. Assume both are finite.
Then by Lecture Notes 3/15/10 (Let K/E be an extension and E/F be an extension. If $[K:E]$ and $[E:F]$ are both finite, then $[K:F] = [K:E][E:F]$.) $[E:E^S] = [E:E^T][E^T:E^S]$.
Since $|T| = n$, then by Lecture Notes 4/7/10 (If $S \subseteq \text{Aut}(E)$ and $|S| = n$, then $[E:E^S] \geq n$), we have $[E:E^T] \geq n$. And $[E^T:E^S] \geq 1$ as extension field degrees are always ≥ 1.
Thus $[E:E^S] \geq n$, $\forall\, n \in \mathbb{N}$.
$\therefore$ $[E:E^S] = \infty$.

Theorem If $G \leq \text{Aut}(E)$, then $[E:E^G] = |G|$.

Proof: Similar argument. See handout; very lengthy.

Corollary $[E:E^{\text{Gal}(E/F)}] = |\text{Gal}(E/F)|$.

Example If $G = \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ where α is a primitive 5^{th} root of unity, then $E^G = \mathbb{Q}$.

Proof:
Since $p(x) = x^4 + x^3 + x^2 + x + 1$ has degree 4, and we have shown p is irreducible over Q, then $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$.
And we know $4 = [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):E^G][E^G:\mathbb{Q}]$.
In Lecture Notes 4/5/10, we found that $\text{Aut}(E) \cong \mathbb{Z}_4$,
hence $|\text{Aut}(E)| = |\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = 4$.
Since $|\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = 4$, then $[\mathbb{Q}(\alpha):E^G] = [\mathbb{Q}(\alpha):\mathbb{Q}(\alpha)^{\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})}] = 4$, by the above corollary.
So $[\mathbb{Q}(\alpha)^{\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})}:\mathbb{Q}] = 1$, hence $\mathbb{Q}(\alpha)^{\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})} = \mathbb{Q}$.

Example If $G = \text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}_2$, and $E = \mathbb{Q}(\sqrt{5})$, then $E^G = \mathbb{Q}$.

Proof:
$2 = [\mathbb{Q}(\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{5}):E^G]\ [E^G:\mathbb{Q}]$.
And $\text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}_2$ gives us that $|\text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})| = 2$.
Thus $2 = |\text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{5}):E^G]$ by above corollary.
So $[E^G: \mathbb{Q})] = 1$, hence $E^G = \mathbb{Q}$. $\therefore\ \mathbb{Q} \lhd \mathbb{Q}(\sqrt{5})$.

Example If $G = \text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\text{Id}\}$ and $E = \mathbb{Q}(\sqrt[3]{2})$, then $E^G = \mathbb{Q}(\sqrt[3]{2})^G \neq \mathbb{Q}$.
Thus $[\mathbb{Q}(\sqrt[3]{2}):E^G] = 1$ by above corollary.
So $3 = [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}):E^G][E^G:\mathbb{Q}] \Rightarrow [E^G:\mathbb{Q}] \neq 1$, hence $E^G \neq \mathbb{Q}$.
$\therefore\ \mathbb{Q}$ is not normal in $\mathbb{Q}(\sqrt[3]{2})$.

Definition Let E/F be an extension. We say that E is a *normal extension* of F if $[E:F] < \infty$ and F is the fixed field of Gal (E/F). We write $F \lhd E$.