• **Corollary.** (Milne, Cor.3.5) $\mathbf{E}$ field. For any finite group $G \subset \mathrm{Aut}(\mathbf{E})$, one has $G = \mathrm{Aut}_{\mathbf{E}^G}(\mathbf{E})$.
In particular, if $\mathbf{F} \subset \mathbf{E}$ is a finite degree extension, then $[\mathbf{E} : \mathbf{E}^G] = \#G$.

Let $\mathbf{F} \subset \mathbf{E}$ be an algebraic extension.

• **Definition.** $\mathbf{F} \subset \mathbf{E}$ is called *separable* if the minimum polynomial over $\mathbf{F}$ of every element in $\mathbf{E}$ is separable.

• **Definition.** $\mathbf{F} \subset \mathbf{E}$ is called *normal* if the minimum polynomial over $\mathbf{F}$ of every element in $\mathbf{E}$ splits in $\mathbf{E}[x]$.

In particular, an algebraic extension $\mathbf{F} \subset \mathbf{E}$ is both separable and normal if the minimum polynomial f over $\mathbf{F}$ of every element in $\mathbf{E}$ splits in $\mathbf{E}[x]$ as $f(x) = c(x - \alpha_1) \dots (x - \alpha_n)$, with $c, \alpha_i \in \mathbf{E}$ and $\alpha_i \neq \alpha_j$, for $i \neq j$.

• **Theorem.** (Milne, thm.3.10) *Let $\mathbf{F} \subset \mathbf{E}$ be an extension. Then the following four statements are equivalent:*
(a) $\mathbf{F}$ is the invariant subfield of $Aut_{\mathbf{F}}(\mathbf{E})$;
(b) $\mathbf{F} = \mathbf{E}^G$, for some finite subgroup $G \subset Aut(\mathbf{E})$;
(c) $\mathbf{E}$ is a finite degree separable and normal extension of $\mathbf{F}$;
(d) $\mathbf{E}$ is the splitting field of a separable polynomial in $\mathbf{F}[x]$.

• **Definition.** If an extension $\mathbf{F} \subset \mathbf{E}$ satisfies any of the above statements, then ot is called a *Galois extension* and $G := \mathrm{Aut}_{\mathbf{F}}(\mathbf{E})$ is its *Galois group.*

• **Example.** (see Milne, Example 3.21) $\mathbf{Q} \subset \mathbf{Q}(\zeta_7)$, where ζ_7 is a primitive 7^{th} root of 1.