<u>Theorem</u> Let L be a splitting extension of K.

Then, for any irr. poly $f \in K[x]$

L contains one root of f $\Leftrightarrow$ L contains all the roots of f.

<u>Proof</u>: Assume L is a splitting field of an irr. poly $g(x) \in K[x]$.

Then $L = K(\alpha_1, \cdots, \alpha_m)$, where $\alpha_1, \cdots, \alpha_m$ are the roots of $g(x)$.

Let $f \in K[x]$ be irr, and $\alpha\ \beta$ are roots of f.

Then $L = K(\alpha_1, \cdots, \alpha_m)$

$L(\alpha) = K(\alpha_1, \cdots, \alpha_m)(\alpha) = K(\alpha)(\alpha_1, \cdots, \alpha_m)$

$L(\beta) = K(\alpha_1, \cdots, \alpha_m)(\beta) = K(\beta)(\alpha_1, \cdots, \alpha_m)$,

Since $K(\alpha) \cong K[x]/_{(f)} \cong K(\beta)$, $\xrightarrow{\hat{\sim}}$ we have

$(K(\alpha))(\alpha_1) \cong K(\alpha)[x]/_{(g)} \overset{\wedge}{\cong} K(\beta)[x]/_{(\hat{g})} \cong K(\beta)(\hat{\alpha}_1)$.

g irr in $K[\alpha]$?

and $[K(\alpha)(\alpha_1) : K(\alpha)] = [K(\beta)(\hat{\alpha}_1) : K(\beta)]$. Recursively,

$K(\alpha_1, \cdots, \alpha_j)(\alpha) \cong K(\alpha)(\alpha_1, \cdots, \alpha_j) \cong K(\beta)(\hat{\alpha}_1, \cdots, \hat{\alpha}_j) \cong K(\hat{\alpha}_1, \cdots, \hat{\alpha}_j)(\beta)$.

In particular, $L(\alpha) \cong L(\beta)$, and $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$

So $[L(\beta):L][L:K] = [L(\beta):K] = [L(\beta):K(\beta)][K(\beta):K] = [L(\alpha):K(\alpha)][K(\alpha):K] = [L(\alpha):K]$

$= [L(\alpha):L][L:K] \Rightarrow [L(\beta):L] = [L(\alpha):L]$ and $\alpha \in L \Leftrightarrow \beta \in L$. $\square$

<u>Def</u>: An algebraic extension E/F is called a <u>normal</u> extension if

for each irr. poly $f(x) \in F[x]$, whenever E contains one root of $f(x)$, E contains all roots of $f(x)$.

<u>Cor</u>: An alg. extension is normal iff it is a splitting field of some polynomial.

Let E/F: finite field extension. $Gal(E:F)$

G acts on E, has orbits on E.

For $\underset{Gal(L:F)}{\underline{F<L}}\overset{Gal(E:L)}{<E}$, and $\sigma \in G$. $F = F^\sigma < L^\sigma < E^\sigma = E$. $L^\sigma = L$?

$Gal(E:F)$.

<u>Lemma</u>: Let L be a field with $F < L < E$.

L is fixed by $Gal(E:F)$ setwise $\Leftrightarrow$ $Gal(E:L) \lhd Gal(E:F)$ .... $Gal(E:L) < Gal(E:F)$ is obvious.

<u>Proof</u>: Suppose L is fixed by $Gal(E:F)$.

Then each elt of $Gal(E:F)$ induces an automorphism of L, and hence $Gal(E:F)$ acts on L natually.

The kernal of the action is $Gal(E:L)$, so $Gal(E:L) \lhd Gal(E:F)$.

Conversely, suppose $Gal(E:L) \lhd Gal(E:F)$.

For any $\alpha \in L$ and $g \in Gal(E:F)$.

Claim: $\alpha^g \in L$.

Let $\beta = \alpha^g$, then for any $h \in Gal(E:L)$, $\beta^{hg^{-1}} = \alpha^{ghg^{-1}} = \alpha$, as $ghg^{-1} \in Gal(E:L)$.

Hence $\beta = \alpha^{gh^{-1}} = (\alpha^g)^{h^{-1}} = \beta^{h^{-1}}$, i.e. $\beta^h = \beta$. so $\beta \in L$, i.e. $\alpha^g \in L$ and L is fixed pointwisely by $Gal(E:F)$. $\square$

Theorem: Let $F < L < E$, then $Gal(E:L) \lhd Gal(E:F) \Leftrightarrow L$ is a splitting extension of F.

(L is a normal extension of F).

Proof: Assume $Gal(E:L) \lhd Gal(E:F)$.

Let $f \in F[x]$ be irr. and β a root of f s.t. $\beta \in L$.

Let β' be a root of f. Then there is $\sigma \in Gal(E:F)$ s.t. $\beta' = \beta^\sigma$.

For any $h \in Gal(E:L)$, $\beta'^h = \beta^{\sigma h} = \beta^{\sigma h \sigma^{-1} \sigma} = \beta^\sigma = \beta'$.

so $\beta' \in L$, and L is a splitting field of f.

Conversely. Let L be a splitting extension of F.

Then, for any $\alpha \in L$ and $\sigma \in Gal(E:F)$, $\alpha^\sigma \in L$ (since σ fixes $f(x) \in F[x]$)

i.e. L is fixed by $Gal(E:F)$ setwise.

By lemma, $Gal(E:L) \lhd Gal(E:F)$. $\square$

Eg. Let $w = \frac{-1+\sqrt{3}i}{2}$, a root of x^2+x+1.

Let $\mathbb{Q} < \underset{L}{\underset{\shortparallel}{\mathbb{Q}(w)}} < \underset{E}{\underset{\shortparallel}{\mathbb{Q}(2^{\frac{1}{3}}, w)}}$.

Then $\mathbb{Q}(w)$ is the splitting field of x^2+x+1.

$\mathbb{Q}(2^{\frac{1}{3}}, w)$ is the splitting field of x^3-2.

$Gal(L:\mathbb{Q}) = \mathbb{Z}_2$.

$Gal(E:L) = \mathbb{Z}_3$. $\langle 2^{\frac{1}{3}} \mapsto w 2^{\frac{1}{3}} \rangle$.

$Gal(E:\mathbb{Q}) = \underset{\triangle}{S_3} = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$.

Eg. Let $f(x) = x^5 - 7$.

$Gal(f)_{\mathbb{Q}} = Gal(E:\mathbb{Q})$ where E is a splitting field of f over $\mathbb{Q}$.

Find $Gal(E:\mathbb{Q}) = ?$

$\cong \mathbb{Z}_5 \rtimes \mathbb{Z}_4$.