Given E/F field ext $Gal(E/F) = Aut_F(E)$
finite.

$$\{K \mid F \subset K \subset E\} \underset{Gal}{\overset{Fix}{\rightleftarrows}} \{H < Gal(E/F)\}$$

__Def__: E/F is Galois if F is closed (ie. $F = Fix(G)$)

__Lem__: If E/F is a splitting field of some poly and if $f \in F[x]$ irreducible, $\alpha, \beta \in E$ roots of f then $\exists\, \sigma \in Gal(E/F)$ s.t. $\sigma(\alpha) = \beta$

__Today__: separability & Galois correspondence.

__Observation__: if $F \subset E$ field ext, $f, g \in F[x]$
then $\gcd(f,g)$ $\text{lcm}(f,g)$ are same in $F[x]$ & $F[x]$.
(exercise)

__Exercise__: show that for g is irreducible, ($g \mid f$ & $g \mid f'$) if and only if $g^2 \mid f$.
the derivative

__Hint__: consider E a splitting field of f.

Def A poly $f \in F[x]$ has distinct roots if any of the following equiv conditions hold:

- In every splitting field E, f has distinct roots
- In every extension E/F $(x-\alpha)^2 \nmid f$ $\forall \alpha \in E$.
- In every extension E/F $g^2 \nmid f$ any $g \in E[x]$, $\deg g > 0$.
- in some splitting field f has exactly $\deg f$ roots
- f, f' have no common factors.

Def $f \in F[x]$ is separable if each irred factor of f has distinct roots $(x^2+1)(x^2+1)$

Lem $f \in F[x]$ sep $\Rightarrow$ $f \in E[x]$ sep all E/F.

$f = g_1 \cdots g_r$ g_i irred. in E $g_i = h_{i1} h_{i2} \cdots h_{is_i}$

$h_{ij} | g_i$

Remark If f not separable then for some irred factor g, have $\gcd(g, g') \neq 1$ which can only happen if $g' = 0$.

$g = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ actually has form

$g = x^{mp} + \cdots$ every exponent is a mult. of p.

i.e. $g \in F[x^p]$ $\qquad$ $\gcd\{f, 0\} = f$

<u>Consequence</u>: In char 0, every poly is separable.

<u>Def</u> E/F algebraic is called separable if $\forall\, \alpha \in E$ $\min_F \alpha$ is separable.

<u>Lem</u> if $F \subset K \subset E$, E/F sep $\Rightarrow$ E/K & K/F separable.

if $\alpha \in E$ $\quad \min_K \alpha \mid \underset{\text{sep}}{\min_F \alpha}$ ✓

Suppose E/F $\quad G \subseteq \mathrm{Gal}(E/F)$ $\quad F = \mathrm{Fix}\, G$

and $\alpha \in E$ has a finite G orbit. $\Lambda = \{\sigma\alpha \mid \sigma \in G\}$

<u>Lemma</u>. $\underbrace{\prod_{\lambda \in \Lambda} (x - \lambda)}_{f} = \min_F \alpha = h = \sum a_i x^i$

Pf

Clearly $f(\alpha) = 0$. $\qquad$ G acts on $E[x]$ by acting on coeffs.

$E[x]^G = F[x]$

$\min_F \alpha \mid f$ $\qquad \Rightarrow f \in F[x]$

$\overset{\shortparallel}{h}$

$h(\sigma\alpha) = \sum a_i (\sigma\alpha)^i = \sum \sigma(a_i \alpha)^i = \sigma(h(\alpha)) = 0$

in E $(x-\lambda) \mid h$ all λ $\Rightarrow$ $\underbrace{\prod (x-\lambda)}_{= f} \mid h$ $\quad f \mid h$ in $F[x]$

$\square$

$$E[x] = \{ \sum a_i x^i \mid a_i \in E \} = \{ (a_0, a_1, \dots) \mid a_i \in E \text{ \& } a_i = 0 \ i \gg 0 \}$$

$$\sigma(\sum a_i x^i) \equiv \sum \sigma(a_i) x^i$$

$$E[x]^G = E^G[x]$$

__also note:__ f is separable.

Suppose E/F G-Galois finite dim'l.

- will show E/F sep. & normal

  previous lemma $\Rightarrow$ $\alpha \in E$ then $\min_F \alpha = \prod_{\sigma \in G} (x - \sigma\alpha)$ is sep & all roots are in E.

Suppose E/F sep & normal (finite)

- will show E = splitting field for a sep. poly.

  Choose $\alpha_1, \dots, \alpha_n$ generating E over F

  $f = \prod \min_F \alpha_i$ $\quad$ E is splitting field of f

---

Suppose E = splitting field of a sep poly over F

a will show E/F is Galois.

let $G = Gal(E/F)$ WTS $E^G = F$

Induct on $[E:F]$.

- base case $[E:F] = 1$ ✓ ← E splitting field for g
- Induction: choose $\alpha \in E \setminus F$ ^ a root of g consider $E / F(\alpha)$

note E = splitting field of (the same) poly over $F(\alpha)$

$\Rightarrow F(\alpha) = E^{Gal(E/F(\alpha))}$

let $K = E^G$ Claim: $\min_F \alpha = \min_K \alpha$

$\prod_{\lambda \in \Lambda} (x - \lambda)$ // lem :)

$\Lambda = \{ \sigma\alpha \mid \sigma \in G \}$

G acts transitively by lemma

$$K = E^G \subset E^{Gal(E/F(\alpha))} = F(\alpha)$$

$$K(\alpha) = F(\alpha)$$

So $[K(\alpha):F] = [K(\alpha):K][K:F] = [F(\alpha):K][K:F]$

$\quad \| $

$[F(\alpha):F]$

$[\cancel{F(\alpha):K}][K:F] = [F(\alpha):F] = [K(\alpha):K]$

$= [\cancel{F(\alpha):K}]$ $\quad [K:F] = 1$.

$F = K = E^G$ Δ.

<u>Cor</u>: If $E/K/F$ exts w/ E/F Galois then E/K Galois.

<u>Pf</u>: if E/F is splitting field of a sep poly then E/K also.

$\Rightarrow$ $K = E^{Gal(E/K)}$ all intermediate fields K.

i.e. if E/F is Galois (i.e. F "closed")
then any intermediate subfield K is closed also.

$\Rightarrow$ Subgps $\longrightarrow$ subfields
$H \longrightarrow E^H$ is surjective. if Galois

$\Rightarrow$ there are at most a finite set of subfields

$\Rightarrow$ Primitive element (Artin) if E/F Galois then
$E = F(\alpha)$. single element.

$E \cong \frac{F[x]}{(f)}$ splitting $|G| = [E:F]$
$= \deg f$

$G \hookrightarrow S_{\text{root } f}$ $\deg f$ roots.

$|G| = \frac{\deg f}{|\mathrm{Stab}\ \alpha| = (1)}$