K : field, $\quad H \overset{\text{subgroup}}{\leq} Aut(K)$.

<u>Def</u> $Fix(H) = \{ \alpha \in K : \varphi(\alpha) = \alpha \ \forall \varphi \in H \}$ - the subfield fixed by H

<u>Lemma</u> $Fix(H)$ is a field.

<u>Proof</u> $\alpha, \beta \in Fix(H) \Rightarrow \alpha+\beta, \alpha\beta, \alpha^{-1} \in Fix(H)$.

If K/F is an extension, $H \leq Aut(K/F)$ $(\forall \varphi \in H, \ \varphi(a) = a \ \forall a \in F)$

Then $F \subseteq Fix(H)$.

<u>Fundamental Galois Theorem</u> (short version)

Let K/F be a Galois extension.

Then the mappings: $L \longmapsto Gal(K/L)$ between
$Fix(H) \longleftarrow H$

subextensions of K/F and subgroups of $Gal(K/F)$ are inverses of each other, and so they define a 1-1 correspondence between subextensions of K/F and subgroups of $Gal(K/F)$.

$K/F \qquad G = Gal(K/F)$

$L/F \Rightarrow K/L$ is Galois, $Gal(K/L) = H \leq G$.

$H \leq G \Rightarrow Fix(H) \supseteq F, \quad Fix(H) = L/F$.

Proposition Let K be a field. Let $G \leq Aut(K)$. Let $F = Fix(G)$, Let $|G| = n < \infty$. Then $[K:F] = n$ so K/F is Galois.

since $|Aut(K/F)| \geq |G| = [K:F]$.

Proof Let $\alpha_1, \dots, \alpha_m$ be a basis of K over F. To prove: $m = n$.

Let $G = \{\varphi_1, \dots, \varphi_n\}$.

① Assume that $n > m$. Consider:

$$\begin{cases} \varphi_1(\alpha_1)x_1 + \cdots + \varphi_n(\alpha_1)x_n = 0 \\ \vdots \qquad\qquad \vdots \\ \varphi_1(\alpha_m)x_1 + \cdots + \varphi_n(\alpha_m)x_n = 0 \end{cases}$$

m eqns, n variables over K $\Rightarrow$ there is a nonzero solution $\overbrace{\beta_1, \dots, \beta_n}^{\text{not all } 0}$.

That is, $$\begin{cases} \varphi_1(\alpha_1)\beta_1 + \cdots + \varphi_n(\alpha_1)\beta_n = 0 \\ \vdots \qquad\qquad \vdots \\ \varphi_1(\alpha_m)\beta_1 + \cdots + \varphi_n(\alpha_m)\beta_n = 0 \end{cases}$$

$\forall \alpha \in K, \quad \alpha = \sum_{i=1}^{m} a_i \alpha_i$, so $\sum a_i \cdot$ equalities

implies $\varphi_1(\alpha)\beta_1 + \cdots + \varphi_n(\alpha)\beta_n = 0 \quad \forall \alpha \in K$

(so $\beta_1 \varphi_1 + \cdots + \beta_n \varphi_n = 0$, $\{\varphi_i\}$ are lin. dep-nt)

Choose a minimal linear dependence equality for $\{\varphi_i\}$. We may assume that this is

$$(*) \qquad \beta_1 \varphi_1 + \cdots + \beta_K \varphi_K = 0, \quad \beta_1, \ldots, \beta_K \neq 0, \quad K \text{ is minimal such.}$$

Let $\alpha_0 \in K$ s.t. $\varphi_1(\alpha_0) \neq \varphi_2(\alpha_0)$. Then $\forall \alpha \in K$,

$$\beta_1 \varphi_1(\alpha_0 \alpha) + \cdots + \beta_K \varphi_K(\alpha_0 \alpha) = 0$$

$$\beta_1 \varphi_1(\alpha_0) \varphi_1(\alpha) + \cdots + \beta_K \varphi_K(\alpha_0) \varphi_K(\alpha) = 0$$

$$(**) \qquad \text{So } \beta_1 \varphi_1(\alpha_0) \varphi_1 + \cdots + \beta_K \varphi_K(\alpha_0) \varphi_K = 0$$

Then $(**) - \varphi_1(\alpha_0)\, (*)$

$$= \beta_2 \underbrace{(\varphi_2(\alpha_0) - \varphi_1(\alpha_0))}_{\neq 0} \varphi_2 + \cdots + \beta_K (\varphi_K(\alpha_0) - \varphi_1(\alpha_0)) \varphi_K = 0$$

this nontrivial lin. comb of φ_i with $< K$ terms, contradiction.

(2) Assume $m > n$. The proof is similar, but swap roles of m and n (n equations in m variables). Get a nonzero solution $\beta_1, \ldots, \beta_m$ s.t.

$$\begin{cases} \varphi_1(\alpha_1) + \cdots + \varphi_1(\alpha_m) \beta_m = 0 \\ \vdots \qquad\qquad \vdots \\ \varphi_n(\alpha_1) + \cdots + \varphi_n(\alpha_m) \beta_m = 0 \end{cases}$$

assume this is minimal such id with all nonzero coeffs

$$\left\{ \begin{array}{l} \vdots \qquad\qquad \vdots \\ \varphi_n(\alpha_1) + \cdots + \varphi_n(\alpha_m)\beta_m = 0 \end{array} \right.$$

assume this is minimal such id with all nonzero coeffs

That is, $\forall \varphi \in G, \quad \beta_1 \varphi(\alpha_1) + \cdots + \beta_k \varphi(\alpha_k) = 0 \quad (*)$

Assume wlog $\beta_1 \neq 0$. Divide by β_1, assume $\beta_1 = 1$.

then $\varphi(\beta_1) = \beta_1 \quad \forall \varphi \in G$.

If all $\beta_i \in F$, then $\varphi(\alpha_1\beta_1 + \cdots + \alpha_k\beta_k) = 0 \quad \forall \varphi \in G$.

in particular, if $\varphi = id$, then $\alpha_1\beta_1 + \cdots + \alpha_k\beta_k = 0$, which contradicts the fact that $\{\alpha_i\}$ is a basis.

Assume $\beta_2 \notin F$. let $\psi \in G$ s.t. $\psi(\beta_2) \neq \beta_2$.

then $\psi(*) = \psi(\beta_1) \cdot (\psi \circ \varphi)(\alpha_1) + \cdots + \psi(\beta_k) \cdot (\psi \circ \varphi)(\alpha_k) = 0 \quad \forall \varphi \in G$.

$\{\psi \circ \varphi : \varphi \in G\} = G$, so we get

$(**) \quad \psi(\beta_1) \cdot \varphi(\alpha_1) + \cdots + \psi(\beta_k) \cdot \varphi(\alpha_k) = 0 \quad \forall \varphi \in G$

Then $(**) - (*) = (\underbrace{\psi(\beta_2) - \beta_2}_{\neq 0})\varphi(\alpha_2) + \cdots + (\psi(\beta_k) - \beta_k)\varphi(\alpha_k) = 0$

Again, we get a smaller nontrivial zero linear combination, contradiction.

So $m = n$. $\square$

Proof of Galois Theorem

$$\begin{array}{ccc} L & \longleftrightarrow & H \\ \rotatebox{90}{$\subseteq$} & & \rotatebox{90}{$\leq$} \\ K & & G \end{array}$$

① L/F subext of K/F $\rightsquigarrow$ $H = Gal(K/L)$ $\rightsquigarrow$ $\tilde{L} = Fix(H)$

L is fixed by H, so $L \subseteq \tilde{L}$.

$|H| = [K : L]$ since K/L is Galois.

also, $|H| = [K : \tilde{L}]$ by propn.

So $\tilde{L} = L$.

② $H \leq G \rightsquigarrow L = Fix(H) \rightsquigarrow \tilde{H} = Gal(K/L)$

Since $G = Gal(K/F)$, G fixes F, so $F \subseteq L$.

So L/F is a subextension of K/F.

$H \leq \tilde{H}$ since H fixes L and $\tilde{H} = \{\varphi \in G : \varphi \text{ fixes } L\}$

If $|H| = n$ then $[K : L] = n$ by proposition, and $|\tilde{H}| = n$ since K/L is Galois. So $\hat{H} = H$. $\square$