Theorem  Let $K$ be a field $G=\{\sigma_1, \ldots, \sigma_n\} \leq \text{Aut}(G)$ for distinct $\sigma_1, \ldots, \sigma_n$. Let $F = K^G$. Then

$$[K:F] = n = |G|$$

If last time showed $n \leq [K:F] = m$

Now suppose $n < [K:F]$ Can choose $\alpha_1, \ldots, \alpha_{n+1} \in K$ $F$-linearly independent. Here, system:

$$\begin{align*}
\sigma_1(\alpha_1)X_1 + \sigma_1(\alpha_2)X_2 + \ldots + \sigma_1(\alpha_{n+1})X_{n+1} &= 0 \\
\vdots & & \vdots \\
\sigma_n(\alpha_1)X_1 + \sigma_n(\alpha_2)X_2 + \ldots + \sigma_n(\alpha_{n+1})X_{n+1} &= 0
\end{align*}$$

has nontrivial solution $X_1 = \beta_1, X_2 = \beta_2, \ldots, X_{n+1} = \beta_{n+1}$ by linear algebra. If all $\beta_1, \ldots, \beta_{n+1} \in \mathbb{F}$, then $\sigma(\alpha_1)\beta_1 + \ldots + \sigma(\alpha_{n+1})\beta_{n+1} = 0$ contradicts $F$-linear independence of $\sigma_1 \alpha_1, \ldots, \alpha_{n+1}$ since $\sigma_1 = 1$ is the identity.
at least one $\beta_i \notin F$

Can now assume (renumber) for some $1 \leq r \leq n+1$:
* $\beta_1, \ldots, \beta_r$ nonzero and $\beta_i = 0$ for $i > r$
* no non-trivial solution
  
  $X_1 = \beta'_1, \ldots, X_{n+1} = \beta'_{n+1}$,

so $K$ has fewer than $r$ many nonzero $\beta'_1, \ldots, \beta'_{n+1}$. 

* $\beta_r = 1$, $\beta_i \notin F$

We get, for $1 \leq i \leq n$

$\sigma_i\left(c_{\alpha_i}, \beta_1, \ldots, c_{\alpha_{r-1}}, \beta_{r-1}\right) + \sigma_i\left(c_{\alpha_r}\right) = 0$

Since $\beta_r \notin F$, for one of the $\sigma_i$ ...

say $\sigma_{k_0}$: $\sigma_{k_0}\left(\beta_i\right) \notin \beta_i$

For $1 \leq j \leq n$ we get:

$\sigma_{k_0} \sigma_j\left(c_{\alpha_1}\right) \sigma_{k_0}\left(\beta_1\right) + \ldots + \sigma_{k_0} \sigma_j\left(c_{\alpha_{r-1}}\right) \sigma_{k_0}\left(\beta_{r-1}\right) + \sigma_{k_0} \sigma_j\left(c_{\alpha_r}\right) = 0$

$\sigma_i\left(c_{\alpha_1}\right) \sigma_{k_0}\left(\beta_1\right) + \ldots + \sigma_i\left(c_{\alpha_{r-1}}\right) \sigma_{k_0}\left(\beta_{r-1}\right) + \sigma_i\left(c_{\alpha_r}\right) = 0$
Subtracting $\Box$ from $\Box$

\[
\sigma_i(\alpha_1)(\beta_1 - \sigma_{\mathbb{K}_0}(\beta_1)) + \ldots + \sigma_i(\alpha_{r-1})(\beta_{r-1} - \sigma_{\mathbb{K}_0}(\beta_{r-1})) = 0
\]

We therefore obtain a solution to $\Box$

\[
X_1 = \beta_1 - \sigma_{\mathbb{K}_0}(\beta_1), \ldots, X_{r-1} = \beta_{r-1} - \sigma_{\mathbb{K}_0}(\beta_{r-1})
\]

and $X_r = X_{r+1} = \ldots = X_{n+1} = 0$

But with $X_1 = \beta_1 - \sigma_{\mathbb{K}_0}(\beta_1)$ also not equal to zero.

This contradicts the minimality of the choice of $r$.

$\therefore, n \leq [K:F]\]

$\therefore, n = [K:F]$ and the theorem follows $\square$

To restate the theorem:

**Theorem** $K$ field, $G \leq \text{Aut}(K)$, $G$ finite, then

\[
[K:K^G] = |G|
\]
Remark

1) Let $K/F$ be a finite extension of fields.

Set $F_i = K^\text{Aut}(K/F)$

By previous theorem

$[K:F] = [K:F_i][F_i:F] = |\text{Aut}(K/F)|[F:F_i]$

Thus

$[K:F] = |\text{Aut}(K/F)|$

(Exercise: Show $\text{Aut}(K/F)$ is finite)

Further, we see

$|\text{Aut}(K/F)| = [K:F]$

iff $F = K^\text{Aut}(K/F)$

Conclusion: $K/F$ is Galois $\iff F = K^\text{Aut}(K/F)$

2) Now let $G$ be any finite subgroup of $\text{Aut}(K)$, $K$ a field and set $F = K^G$. Then $G \leq \text{Aut}(K/F)$. (Easy).

By previous theorem and remark 1,


$: G = \text{Aut}(K/F)$ and

$K/K^G$ is Galois

Consequently, if $\sigma \in \text{Aut}(K)$ and $\sigma(\lambda) = \lambda$ for all $\lambda \in F$,

$F = K^G$, then $\sigma \in G$, for all finite subgroups $G$ of $\text{Aut}(K)$.
3) Let \( G, H \) both be finite subgroups of \( \text{Aut}(K) \). Suppose \( K^G = K^H \). By (2)
\[ G = \text{Aut}(K/K^G) = \text{Aut}(K/K^H) = H. \]
Consequentially, distinct finite subgroups of \( \text{Aut}(K) \) have distinct fixed subfields of \( K \).

**Theorem**

1) A finite extension of fields is Galois \( \iff \) \( K \) is the splitting field of some separable polynomial \( F[x] \).

2) If \( K/F \) is a Galois extension, then every irreducible polynomial in \( F[x] \) with one root in \( K \) is separable and has all of its roots in \( K \).

**Proof**

We have already proven that the splitting field of a separable polynomial is a Galois extension. Now, assume that \( K/F \) is Galois, and take \( G := \text{Gal}(K/F) \). Choose \( \alpha \in K \). Let \( \alpha_1, \alpha_2, ..., \alpha_r \) be the distinct elements of \( \{ \sigma(\alpha) \mid \sigma \in G \} \).

Set \( f(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_r) \in K[x] \).

Note \( f(x) \) is separable. Next, for \( \tau \in G \), have a ring automorphism \( K[x] \xrightarrow{\tau} K[x] \)
\[ a_nx^n + ... + a_0 \mapsto \tau(a_n)x^n + ... + \tau(a_0) \]
And for \( \tau \in G \), \( \tau(f(x)) = \tau(x - \alpha_1, \tau(x - \alpha_2, ..., \tau(x - \alpha_r) = (x - \tau(\alpha_1), ..., (x - \tau(\alpha_r)) \]
\[ = f(\tau(x)) \]
Since \( \tau \) permutes the roots of \( f(x) \).
Then \( \tau(b_i) = b_i \), \( \tau(b_0) = b_0 \) since \( \tau: f(x) \mapsto f(x) \).

Since \( \tau \) is arbitrary, we can conclude \( b_1, \ldots, b_0 \in F \).

\( \therefore \ f(x) \in F[x] \).

Now let \( p(x) = \prod_{i=1}^{r} (x - \alpha_i) \in F[x] \). We know \( p(x) \mid f(x) \).

However, we've also proved that \( \alpha_1, \ldots, \alpha_r \) are the distinct roots of \( p(x) \) (since \( \tau \) permutes the roots of \( p(x) \in F[x] \)).

\[ \therefore \ (x - \alpha_i) \mid p(x) \text{ in } K[x] \text{ for all } 1 \leq i \leq r \]

\[ \therefore \ (x - \alpha_1) \ldots (x - \alpha_r) \mid p(x) \text{ by unique factorization} \]

\[ \therefore \ f(x) \mid p(x) \text{ and so } f(x) = p(x) \]

Part (2) of the theorem follows.

To finish part (1) of the theorem, suppose \( K/F \) is Galois. Since \( K/F \) is finite, we can write:

\[ K = F(\omega_1, \ldots, \omega_s) \text{ for } \omega_1, \ldots, \omega_s \text{ algebraic over } F \]

Let \( q_1(x), \ldots, q_s(x) \) for \( 1 \leq i \leq s \) be the distinct minimal polynomials for \( \omega_1, \ldots, \omega_s \). By above, the \( q_1(x), \ldots, q_s(x) \) are separable. Also, there are no common roots for the \( q_1(x), \ldots, q_s(x) \).

\[ \therefore \ K \text{ is the splitting field for the separable polynomial } q(x) = q_1(x) \ldots q_s(x) \in F[x] \]

Part (1) follows. Theorem follows \( \square \)

**Def** Let \( K/F \) be a Galois extension. Let \( \sigma \in \text{Gal}(K/F) \). Then the elements \( \sigma(\alpha) \) for \( \sigma \in \text{Gal}(K/F) \) are called **Galois conjugates** of \( \alpha \).