Thm 12.1.24

\[ F = \text{field}, \quad F[x] \supset f(x) \text{ separable} \]
\[ E = \text{splitting field of } f(x). \]
\[ G = \text{Gal}(E/F). \]

Then \( |G| = [E:F] = n \)

Note: \( n \) need not be \( \deg f(x). \)

Proof: Will argue by induction on \( n \).

(Statement is trivial for \( n = 1 \).

\( f(x) \) has an irreducible factor \( f_i(x) \)
of degree \( k > 1 \). Because \( f \) is separable,
\( f(x) \) has \( k \) distinct zeros in \( \mathbb{E} \), \( x_1, x_2, \ldots, x_k \). For \( i \) with \( 1 \leq i \leq k \) there is \( y_i \in \mathbb{E} \) with \( y_i(x_i) = x_i \).

Let \( K = F(x_1) = F[x_1]/(f(x)) \).

So \( [K : F] = k \).

\( E \) is the splitting field of \( f(x) \in F[x] \subset K[x] \).

By induction \( |H| = m \).

Let \( H = \{ \theta_1, \theta_2, \ldots, \theta_m \} \).

Claim 1: The \( m \) elements \( \{ y_i \cdot \theta_j : 1 \leq i \leq k, 1 \leq j \leq m \} \) of \( \mathbb{G} \)
are all distinct

Claim 2. Each element of \( C \) is one of them.

The theorem follows from these

Proof of claim 1: Suppose \( y_i \theta_j = y_i \theta_j' \).

for some \( i, i', j \) and \( j' \).


\[ y_i \theta_j (\alpha_i) = y_i \theta_j (\alpha_i) \quad \text{since } \theta_j \text{ fixed} \]

\[ = \alpha_i \]

\[ y_i \theta_j (\alpha_i) = \alpha_i \phantom{'} \quad \text{so } i = i' \text{ and } y_i = y_i' \]

\( \Rightarrow \theta_j = \theta_j' \quad \text{so } j = j' \). This proves Claim 1.
Proof of Claim 2: Let $y \in G$. Then

$$\Psi(x_i) = x_i$$

for some $i$.

Let $\Theta = y_i^{-1} y$, so

$$\Theta(x_i) = y_i^{-1} \Psi(x_i) = y_i^{-1} x_i = x_i$$

$\Theta$ fixes $x_i$, so it fixes $K$.

$\Theta \in H$ so $\Theta = \Theta_j$ for some $j$.

$$\Theta = y_i^{-1} y = \Theta_j$$

$$y = y_i; \Theta_j$$

QED
Example: Let $p$ be prime.

$f = \mathbb{Q}[x], \quad b(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + 1$

It is irreducible.

Its zeros are the $p$th roots of 1 other than 1. Let $s$ be one such root. (e.g. $s = e^{2\pi i/p}$)

$k = \mathbb{Q}(s)$. The other zeros of $f$ are powers of $s$. Let $y_k \in G$, with $y_k(s) = s^k$.

The set of these $y_k$'s is a
cyclic 

To see this pick a prime \( p \) that is \( 1 \mod 4 \). Reduce \( \bar{\xi} \) mod \( \xi \).

\( \mathbb{F}_p \) is cyclic. Convince this to show \( G \) is cyclic.

Prop 12.1.26 Let \( f(x) \in \mathbb{F}[x] \) be a

\[ \text{cyclic, separable polynomial of degree } d \text{ with splitting field } \mathbb{E}. \] Then

\[ \text{Gal}(\mathbb{E}/\mathbb{F}) \text{ is isomorphic to a subgroup of } S_d \text{ (symmetric group of letters)} \]
2) \( |G| \) divides \( a! = 15! \).

Proof: \( G \) permutes the roots of \( f(x) \)
and each \( \varphi \in G \) is determined by
how it permutes them. This makes
\( G \), a subgroup of \( S_{15} \). Q.E.D.

E.g. \( F = \mathbb{Q} \) \( f(x) = x^{3} - 2 \) (Day 1 example)
\( G = \text{Gal} \left( E/\mathbb{Q} \right) = S_{3} \).
\( E = \mathbb{Q}(\sqrt{2}, -\sqrt{3}) \)

Definition 12.1.9. An extension \( F \subseteq E \)
is separable if \( E = F(\alpha) \). We say...
Let $E$ be a finite separable extension of $F$. Then it is simple.

Proof: If $F$ is finite, so is $E$ and $E$ is cyclic. Let $\alpha$ be a generator of it. Then $E = F(\alpha)$.

Suppose $F$ is infinite, $E = F(M_1, M_2, \ldots, M_n)$.
Suffice to assume $s = 2$

$E = \mathbb{F} \langle \alpha, \beta \rangle.$

Let $p(x)$ and $q(x)$ be the minimal polynomials of $\alpha$ and $\beta.$

Let $\alpha = x_1, \ldots, x_m$ be the zeros of $p(x)$ and $\beta = \beta_1, \ldots, \beta_n$ of $q(x).$

Let $K$ be the splitting field for $p(x)q(x)$ over $E.$

$\alpha_i, \beta_j \in K$
Consider the quotient

$$
\alpha_i - \alpha_1 \in K \text{ for } 1 \leq i \leq m
$$

\[
\beta_i - \beta_0
\]

And if $F$ is infinite we can pick $u \neq 0 \in F$ not equal to any of the above. Let

$$
\gamma = \alpha, u \beta_1 = \alpha + u \beta_0 \in E = F(\alpha, \beta)
$$

We claim $E = F(\gamma)$.

It suffices to show $\alpha, \beta \in F(\gamma)$. 
Let \( h(x) \) be the minimal polynomial of \( \beta \) over \( F(q) \). Want to show it has degree 1.

Will show \( h(\beta_i) \neq 0 \) for \( 1 \leq i \leq n \).

Let \( h(x) = p(x - u \beta) \in F(q)[x] \) \( h(\beta_i) = p(x - u \beta_i) = p(\alpha_i) = 0 \) so \( h(x) \) (the minimal poly of \( \beta_i \)) divides \( k(x) \).

For \( j > 1 \)
\[
k(\beta_i) = p(x - u \beta_i)
\]
Suppose this is O then
\( x - M^2 \beta_j = \alpha_i \) for some \( i \neq j \).

This means
\[
M = \frac{x - \alpha_i}{\beta_j} = \frac{\alpha_i + M \beta_j - \alpha_i}{\beta_j}.
\]

\( M^2 \beta_j = \alpha_i + M \beta_j - \alpha_i. \)

\[
m(\beta_j - \beta_1) = \alpha_i - \alpha_i.
\]

\[
M = \frac{\alpha_i - \alpha_i}{\beta_j - \beta_1} = \frac{\alpha_i - \alpha_i}{\beta_i - \beta_j}.
\]

But we choose \( \alpha \) not to be this.

**Conclusion**
\( \ker(\beta_i) \neq 0 \) for \( i \leq t \)
\( \ker(\beta_i) = 0 \)
\( h(x) = \beta(x - \alpha x) \)

We know \( h(x) | r(x) \) \( \Rightarrow \)
\( \beta_i \) is the only zero of \( h(x) \).
\( h(x) = x - \beta_i \)
\( h(x) \) is minimal poly of \( B = B_i \) over \( F[x] \).

Hence \( B \subset F[x] \) and
\[ \alpha = \chi_{\mathcal{M}_\mathcal{E}} \mathcal{F}(\mathcal{H}) \]

\( \chi \) generates \( \mathcal{E} \).