Thm 12.1.24 For \( f(x) \in \mathbb{F}[x] \) a separable polynomial with splitting field \( E \), let \( G = \text{Gal}(E/F) \). Then \( |G| = [E:F] = n \)

Proof: Argue by induction on \( n \).

Let \( p(x) \) be an irreducible factor of \( f(x) \) of degree \( k > 1 \). \( p(x) \) has \( k \) distinct zeros in \( E \), \( \alpha_1, \alpha_2, \ldots, \alpha_k \).

Let \( K = F(\alpha_i) \). It contains the other
23. Regard \( f(x) \) as a polynomial over \( K \).
\( E \) is its splitting field. By induction,
\( |H| = m \cdot n/K \), where \( H = \text{Gal} (E/K) \).
Let \( H = E \theta_1, \theta_2, \ldots, \theta_m \). \( S \subset G \).

We also know that for each \( \alpha_i \), there is an element \( \psi \in G \) with \( \psi_i (\alpha_i) = \alpha_i \).

Consider the set \( \{ \psi_i \theta_j : 1 \leq i \leq k, 1 \leq j \leq m \} = S \subset G \).

**Claim 1**. The \( kn = n \) elements in this set are distinct.

**Claim 2**. Each elt of \( G \) is in \( S \).
Claim 1: Suppose \( \psi_i \cdot \theta_j \cdot \psi_{i'} \).

Then \( \psi_i \cdot (\psi_i \cdot \theta_j \cdot \psi_{i'}) = \psi_i \cdot \theta_j \cdot (\psi_i \cdot \psi_{i'}) = \psi_i \cdot \theta_j \cdot (\psi_i \cdot \psi_{i'}) = \psi_i \cdot \theta_j \cdot (\psi_i \cdot \theta_j) \).

So \( i = i' \) and \( \psi_i = \psi_{i'} \).

\( \psi_i^{-1} \cdot (\psi_i \cdot \theta_j \cdot \psi_{i'}) = \psi_i^{-1} \cdot (\psi_i \cdot \theta_j) \cdot \psi_i^{-1} \cdot \psi_{i'} \cdot \psi_i \cdot (\psi_i \cdot \theta_j) \).

\( \theta_j = \theta_{j'} \) at \( j = j' \).

Claim 2: Let \( y \in G_i \). Then \( \psi_i (\lambda_i) = \lambda_i \) for all \( i \).

Let \( \theta = \psi_i^{-1} y \). Then
$\beta(x_i) = y_i^{-1} \psi(x_i) = y_i^{-1} a_i = a_i$

$\Theta$ fixes $K_j$ so $\Theta \in H$ and in some $\Theta_j$.

$\Theta_j = y_i^{-1} \psi$ and $\psi = y_i \Theta_j \in S$.

QED

Example:
Let $S^1$ be a $p$th root of unity for a prime $p$. Let $G = \text{Gal}(\mathbb{Q}(S)/\mathbb{Q})$.

Let $\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \ldots + x^{p-1}$.
The zeros of $\overline{\Phi}_p(x)$ are the nontrivial ($\neq 1$) $p$th roots of unity. $\mathbb{Q}(\zeta)$ is the splitting field for $\overline{\Phi}_p(x)$, so $|G| = p - 1$. Claim $G \cong \mathbb{Z}_{p-1}$. $G$ has elements $\zeta^k$ with $\zeta^k(\zeta) = \zeta^k$ for $1 \leq k \leq p - 1$.

To see this consider the ring $\mathbb{Z}[x]/(\overline{\Phi}_p(x))$. Let $l$ be a prime
\[ l \equiv 1 \mod p. \]
Then $K = \mathbb{Z}[x]/(\overline{\Phi}_p(x))$ is a finite field.
Prop 12.1.26 Let $f(x) \in F[x]$ be a separable polynomial with splitting field $E$. Then

1) $G = \text{Gal}(E/F)$ is isomorphic to a subgroup of $S_n$.
2) $|G|$ divides $n! = |S_n|$.

Proof: $G$ permutes the $n$ roots of $f(x)$. Let $R = \{x_1, x_2, \ldots, x_n\}$ be the product $G \circ E$, determined by its action on $R$. 
Def 12.1.29 A field extension $F \subseteq E$ is simple if $E = F(\alpha)$. Such an $\alpha$ is primitive.

12.1.30 Primitive Element Theorem

Let $E$ be a finite separable extension of $F$. Then it is simple.

Proof If $F$ is finite, then $E$ is also finite. Hence $E^*$ is cyclic. Let $\alpha$ be a generator of it. Then $E = F(\alpha)$.

Suppose $F$ is infinite.
\[ E = F(\alpha_1, \alpha_2, \ldots, \alpha_m) \]. It suffices to consider the case \( m = 2 \). Indeed, we know \( F(\alpha_1, \alpha_2) = F(\alpha) \) for some \( \alpha \).

Then \( F(\alpha_1, \alpha_2, \alpha_3) = F(\alpha_1, \alpha_2)(\alpha_3) = F(\alpha)(\alpha_3) = F(\alpha, \alpha_3) = F(\alpha') \).

\[ \text{etc.} \]

Let \( E = F(\alpha, B) \).

Let \( \alpha \) have min. poly \( f(\alpha) \) with roots \( \alpha_1, \alpha_2, \ldots, \alpha_m \).

Let \( B \) be \( \max \{ q(\beta) \mid \beta \in \mathbb{B} \} \).

Let \( K \) be the splitting field for \( p(x)q(x) \), so \( \alpha_1, \alpha_2, \beta_1, \beta_2 \in K \).
Consider the quotient
$$\frac{x_i - x_j}{\beta_i - \beta_j} \in K \quad \text{for} \quad 1 \leq i \leq m \quad \text{and} \quad 1 \leq j \leq n.$$ 

Let \( n \neq 0 \in F \) not equal to any of the above.

Let \( y = \alpha_1 + n \beta_1 \in E \) since \( \alpha_1, \beta_1 \in E \) and \( \alpha_1 = \beta \in E \) and \( n \in F \).

We \( E = F(\alpha_1, \beta_1) = F(y) \).

It suffices to show \( \alpha_1, \beta_1 \in F(y) \).

Let \( h(x) \) be the min. poly. of \( \beta_1 \) over \( F(y) \).

(want to show it has degree 1, i.e. \( \beta_1 \in F(y) \).)
Recall \( q(x) \) is the min poly of \( \beta_i \) over \( \mathbb{F} \).

\( h(x) \) divides \( q(x) \). It has a factor \( x - \beta_j \) for some \( j \). We'll show \( h(\beta_j) \neq 0 \) if \( j \neq 1 \). This will imply \( h(x) = x - \beta_1 \) and \( \beta_1 \in \mathbb{F}(x) \).

Consider \( r(x) = \beta(x - \alpha \beta) \in \mathbb{F}(x)[x] \).

Then

\[
x(\beta_j) = \alpha (x - \alpha \beta_j) = \alpha (x_j) = 0
\]

This means \( h(x) \) (the min poly for \( \beta_i \) over \( \mathbb{F}(x) \))
divides \( k(x) \). It suffices to show \( k(\beta_j) \neq 0 \) for \( j \geq 1 \).

If \( k(\beta_j) = p(y - m\beta_j) = 0 \) then \( y - m\beta_j \) is a root of \( p(x) \), and
\[
y - m\beta_j = \alpha_i \quad \text{for some} \quad i > 1
\]

so
\[
m = \frac{y - \alpha_i}{\beta_j} = \frac{\alpha_1 + m\beta_j - \alpha_i}{\beta_j}
\]

\text{Solve for } m

\[
m = \frac{\alpha_1 - \alpha_i}{\beta_j - \beta_i}
\]

\text{CONTRADICTION}

QED