Introduction:
Previously we worked through an example illustrating many of the components of Galois Theory including the Fundamental Theorem. Here I will state and prove the Fundamental Theorem. Supporting definitions and theorems will be presented as needed. When appropriate (and useful) proofs of supporting results will be provided.

The Theorem (Dummit & Foote Version):

Definition: Let $K$ be a finite extension of $F$. Then $K$ is said to be Galois over $F$ (and $K/F$ is a Galois Extension) if $|\text{Aut}(K/F)| = [K:F]$. In this case the group of automorphisms $\text{Aut}(K/F)$ is called the Galois group of $K/F$, denoted $\text{Gal}(K/F)$.

Definition: A polynomial over $F$ is called separable if it has no multiple roots (i.e. all its roots are distinct).

Theorem(s): $K$ is the splitting field over $F$ of a separable polynomial $f(x)$ if and only if $K/F$ is Galois. Further, over a finite field or a field of characteristic zero, every irreducible polynomial is separable. So, in those cases, $K$ is Galois over $F$ if and only if $K$ is the splitting field of an irreducible polynomial over $F$. [This is basically Theorem 3 found at the bottom of this document (proof omitted).]

(Non)Example:

Consider the extension $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$. What is the degree of this extension? Well, we know by closure of multiplication that $\mathbb{Q}(\sqrt{2})$ must contain $\sqrt{4}$. So, a basis of this extension would be $\{1, \sqrt{2}, \sqrt{4}\}$. This means $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 3$. We can also see that $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 3$ because $x^3 - 2$ is irreducible by Eisenstein.

But if we factor the polynomial in $\mathbb{Q}(\sqrt{2})$ we see that $x^3 - 2 = (x - \sqrt{2})(x^2 + \sqrt{2}x + \sqrt{4})$ and if we compute the discriminant of this quadratic we see that it is $\sqrt{4} - 4\sqrt{4}$ which is negative. So the other two roots of this cubic are complex and hence not contained in $\mathbb{Q}(\sqrt{2})$.

This means that any automorphism that of $\mathbb{Q}(\sqrt{2})$ that fixes $\mathbb{Q}$ must take $\sqrt{2}$ to itself since that's the only root available. This completely determines the map on $\mathbb{Q}(\sqrt{2})$ Thus $|\text{Aut}(\mathbb{Q}(\sqrt{2})\setminus\mathbb{Q})| = 1$.

This means that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is NOT Galois. This also means that $\mathbb{Q}(\sqrt{2})$ is not the splitting field of an irreducible polynomial over $\mathbb{Q}$. 
Theorem: (Fundamental Theorem of Galois Theory) Let $K$ be a Galois Extension and set $G = \text{Gal}(K/F)$. Then there is a bijection

$$
\begin{array}{c|c}
\text{Subfields } E \text{ of } K \text{ containing } F & \text{Subgroups } H \text{ of } G \\
\hline
1 & 1 \\
\end{array}
$$

given by the correspondences

$$
\begin{align*}
E & \leftrightarrow \text{The elements of } G \\
\{ \text{The fixed Field of } H \} & \leftrightarrow H
\end{align*}
$$

which are inverse to each other.

Under this correspondence:

1. (Inclusion Reversing) If $E_1, E_2$ correspond to $H_1, H_2$ respectively, then $E_1 \subset E_2$ iff $H_2 \leq H_1$.


$$
\begin{array}{c|c}
K & H \\
\hline
E & G : H \\
\hline
F &
\end{array}
$$

3. $K/E$ is always Galois, with Galois group $\text{Gal}(K/E) = H$:

$$
\begin{array}{c|c}
K & H \\
\hline
E &
\end{array}
$$

4. $E$ is Galois over $F$ if and only if $H$ is a normal subgroup in $G$. If this is the case, then the Galois group is isomorphic to the quotient group: $\text{Gal}(E / F) \cong G / H$.

5. If $E_1, E_2$ correspond to $H_1, H_2$ respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by $H_1$ and $H_2$ and the composite field $E_1E_2$ corresponds to the intersection $H_1 \cap H_2$. Hence, the lattice of subfields of $K$ containing $F$ and the lattice of subgroups of $G$ are “dual” – the lattice diagram for one is the lattice diagram for the other turned upside down.
The Proof: (It's gonna be a big one!)

Given any subgroup \(H\) of \(G\) we obtain a unique fixed field \(E = K_H\) by Corollary 3 (below). This shows that the correspondence above is injective from the right to left.

If \(K\) is the splitting field of the separable polynomial \(f(x) \in F[x]\) then we may also view \(f(x)\) as an element of \(E[x]\) for any subfield \(E\) of \(K\) containing \(F\). Then \(K\) is also the splitting field for \(f(x)\) over \(E\), so the extension \(K/E\) is Galois. By Corollary 1, \(E\) is the fixed field of \(\text{Aut}(K/E) \leq G\), showing that every subfield of \(K\) containing \(F\) arises as the fixed field for some subgroup of \(G\). Hence the correspondence above is surjective from right to left and hence a bijection. The correspondences are inverse to each other since the automorphisms fixing \(E\) are precisely \(\text{Aut}(K/E)\) by Corollary 1.

The Galois correspondence is inclusion reversing because any automorphism that fixes a subfield \(F'\) of a field \(K'\) will also fix any subfield \(F_1\) of \(F\). So we have proved part (1). [Note that here I'm using \(F', K', F_1\), to denote an arbitrary sequence of fields.]

If \(E = K_H\) is the fixed field of \(H\), then by Theorem 2 (below) \([K : E] = |H|\) and \([K : F] = |G|\). Taking the quotient gives \([E : F] = |G : H|\). This proves part (2).

Note that the above proof uses another theorem that we haven’t proved. Namely that if we have fields \(F \subseteq K \subseteq L\) then \([L : F] = [L : K] [K : F]\). You can prove this simply by using the basis for \(K\) over \(F\) and the basis for \(L\) over \(K\) to construct a basis for \(L\) over \(F\) (the same way I did when I constructed the splitting field for \(x^4 - 2\) over \(\mathbb{Q}\)).

Corollary 2 (below) says that if \(H\) is a finite subgroup of automorphism of a field \(K\) and \(E\) is the fixed field then \(K/E\) is Galois with Galois group \(H\). This gives us part (3) immediately.

[Part (4) is the long one and it is starting now.]

Now suppose that \(E = K_H\) is the fixed field of the subgroup \(H\). Every \(\sigma \in G = \text{Gal}(K/F)\) when restricted to \(E\) is an embedding \(\sigma|_E\) of \(E\) with the subfield \(\sigma(E)\) of \(K\).

Conversely, let \(\tau: E \to \tau(E) \subseteq \overline{F}\) be any embedding of \(E\) (into a fixed algebraic closure \(\overline{F}\) of \(F\) containing \(K\)) which fixes \(F\).

Then \(\tau(E)\) is in fact contained in \(K\): if \(\alpha \in E\) has minimal polynomial \(m_\alpha(x)\) over \(F\) then \(\tau(\alpha)\) is another root of \(m_\alpha(x)\) and \(K\) contains all of these roots by Theorem 3 (below).

As above \(K\) is the splitting field of \(f(x)\) over \(E\) and so also the splitting field of \(\tau f(x)\) which is the same as \(f(x)\) since \(f(x)\) has coefficients in \(F\) over \(\tau(E)\). Then we can extend \(\tau\) to an isomorphism \(\sigma:\)

\[
\begin{array}{ccc}
\sigma: & K & \to & K \\
& & | & | \\
\tau: & E & \to & \tau(E)
\end{array}
\]
Since $\sigma$ fixes $F$ (because $\tau$ does) it follows that every embedding $\tau$ of $E$ fixing $F$ is a restriction to $E$ of some automorphism $\sigma$ of $K$ fixing $F$. In other words, every embedding of $E$ is of the form $\sigma|_E$ for some $\sigma \in G$.

Two automorphisms $\sigma, \sigma' \in G$ restrict to the same embedding of $E$ if and only if $\sigma'\sigma$ is the identity map on $E$. But then $\sigma'\sigma \in H$ since by Part (3) the automorphisms of $K$ which fix $E$ are precisely the elements in $H$. This means that $\sigma'$ is in the coset $\sigma H$. Thus the distinct embeddings of $E$ are in bijection with the cosets $\sigma H$ of $H$ in $G$. In particular this gives

$$|\text{Emb}(E/F)| = [G : H] = [E : F]$$

where $\text{Emb}(E/F)$ denotes the set of embeddings of $E$ (into a fixed algebraic closure of $F$) which fix $F$. Note that $\text{Emb}(E/F)$ contains the automorphisms $\text{Aut}(E/F)$.

The extension $E/F$ will be Galois if and only if $|\text{Aut}(E/F)| = [E : F]$. By the equality above, this will be the case if and only if each of the embeddings of $E$ is actually an automorphism of $E$, i.e. if and only if $\sigma(E) = E$ for every $\sigma \in G$.

If $\sigma \in G$, then the subgroup of $G$ fixing the field $\sigma(E)$ is the group $\sigma H\sigma^{-1}$, i.e., $\sigma(E) = K_{\sigma H\sigma^{-1}}$.

To see this, observe that if $\sigma(\alpha) \in \sigma(E)$ then $(\sigma h \sigma^{-1})(\sigma(\alpha)) = \sigma(h(\alpha)) = \sigma(\alpha)$ for every $h$ in $H$, since $h$ fixes $\alpha \in E$. This shows that $\sigma h \sigma^{-1}$ fixes $\sigma(E)$. On the other hand, the group fixing $\sigma(E)$ has order equal to the degree of $K$ over $\sigma(E)$. But this is the same as the degree of $K$ over $E$ since $E$ and $\sigma(E)$ are isomorphic. So, the order of this group is the same as $H$. Hence $\sigma H\sigma^{-1}$ is precisely the group fixing $\sigma(E)$ since we have shown one containment and their orders are the same (the orders of $H$ and $\sigma H\sigma^{-1}$ are the same because they are conjugates).

Because of the bijective nature of the Galois correspondence already proved, we know that two subfields of $K$ containing $F$ are equal if and only if their fixing subgroups are equal in $G$. Hence $\sigma(E) = E$ for all $\sigma \in G$ if and only if $H = \sigma H \sigma^{-1}$ for all $\sigma \in G$. In other words, $E$ is Galois over $F$ if and only if $H$ is a normal subgroup of $G$.

We have already identified the embeddings of $E$ over $F$ as the set of cosets of $H$ in $G$ and when $H$ is normal in $G$ seen that the embeddings are automorphisms. It follows that in this case the group of cosets $G/H$ is identified with the group of automorphisms of the Galois extension $E/F$ by the definition of the group operation (composition of automorphisms). Hence $G/H \cong \text{Gal}(E/F)$ when $H$ is normal in $G$, which completes the proof of Part (4).

Finally, suppose that $H_1$ is the subgroup of the elements of $G$ fixing the subfield $E_1$ and $H_2$ is the subgroup of elements of $G$ fixing the subfield $E_2$. Any element in $H_1 \cap H_2$ fixes both $E_1$ and $E_2$, hence fixes every element in the composite $E_1 E_2$, since the elements in this field are algebraic combinations of the elements of $E_1$ and $E_2$.

Conversely, if an automorphism $\sigma$ fixes the composite $E_1 E_2$, then in particular $\sigma$ fixes $E_1$, i.e., $\sigma \in H_1$ and $\sigma$ fixes $E_2$, i.e., $\sigma \in H_2$, hence $\sigma \in H_1 \cap H_2$. Similarly, the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by $H_1$ and $H_2$, completing the proof of the Fundamental Theorem of Galois Theory!
**Selected Supporting Theorems and Proofs**

Theorem 1: (Linearity independence of automorphisms). Let $\sigma_1, \sigma_2, ..., \sigma_n$ be distinct automorphisms of a field $F$. Then they are linearly independent as functions on $F$.

Comments: This is a special case of Corollary 8 from Section 14.2 of Dummit & Foote. In Section 14 they develop theory about characters. I think this is more generality than needed. So my proof below (which is really for Theorem 7) is specific to automorphisms. This should be enough to get the theorems that are needed to support the Fundamental Theorem.

Proof: Let $\sigma_1, \sigma_2, ..., \sigma_n$ be distinct automorphisms of a field $F$. Suppose these automorphisms are linearly dependent. Of all the possible non-trivial linear combinations that equal the zero map, choose the one with the smallest number, $m$, of nonzero coefficients $c_i$. We can assume (by renumbering if needed) that the $m$ nonzero coefficients are $c_1, c_2, ..., c_m$.

Then $c_1\sigma_1 + c_2\sigma_2 + ... + c_m\sigma_m = 0$ and so for any $g$ in the multiplicative group $F^\times$ we have:

$$c_1\sigma_1(g) + c_2\sigma_2(g) + ... + c_m\sigma_m(g) = 0.$$  

Now, let $g_0 \in F^\times$ be such that $\sigma_1(g_0) \neq \sigma_m(g_0)$. Such a thing exists because our automorphisms are distinct. Now,

$$c_1\sigma_1(g_0g) + c_2\sigma_2(g_0g) + ... + c_m\sigma_m(g_0g) = 0.$$  

Since these are homomorphisms,

(1)  \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \q
Theorem 2: [Degree of Extension = Order of Automorphism Group] Let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of the automorphisms of a field $K$ and let $F$ be the fixed field of $G$.

Then $[K : F] = n = |G|$. (This is Theorem 9 from 14.2 of Dummit & Foote.)

Proof: I’ll rule out both $n > [K : F]$ and $n < [K : F]$.

Suppose first that $n > [K : F]$. Let $\omega_1, \omega_2, \ldots, \omega_m$ be a basis for $K$ over $F$, where $m < n$. Then the system

$$\begin{align*}
\sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \ldots + \sigma_n(\omega_1)x_n &= 0 \\
\sigma_1(\omega_2)x_1 + \sigma_2(\omega_2)x_2 + \ldots + \sigma_n(\omega_2)x_n &= 0 \\
&\vdots \\
\sigma_1(\omega_m)x_1 + \sigma_2(\omega_m)x_2 + \ldots + \sigma_n(\omega_m)x_n &= 0
\end{align*}$$

has a non-trivial solution (unknowns $> \text{equations}$). Let, $\beta_1, \ldots, \beta_n$ be a non-trivial solution.

Now, let $a_1, a_2, \ldots, a_m$ be arbitrary elements of $F$. These elements are fixed by all of the automorphisms in $G$. So, we can 1) multiply the $i$th equation by $a_i$, 2) move these coefficients inside the map, and 3) substitute the solution $\beta_1, \beta_2, \ldots, \beta_n$ to get:

$$\begin{align*}
\sigma_1(a_1 \omega_1)\beta_1 + \sigma_2(a_1 \omega_1)\beta_2 + \ldots + \sigma_n(a_1 \omega_1)\beta_n &= 0 \\
\sigma_1(a_2 \omega_2)\beta_1 + \sigma_2(a_2 \omega_2)\beta_2 + \ldots + \sigma_n(a_2 \omega_2)\beta_n &= 0 \\
&\vdots \\
\sigma_1(a_m \omega_m)\beta_1 + \sigma_2(a_m \omega_m)\beta_2 + \ldots + \sigma_n(a_m \omega_m)\beta_n &= 0
\end{align*}$$

Let’s add these together and do some factoring and homomorphism-ing:

$$\begin{align*}
\sigma_1(a_1 \omega_1)\beta_1 + \sigma_1(a_2 \omega_2)\beta_1 + \ldots + \sigma_n(a_m \omega_m)\beta_1 + \sigma_2(a_1 \omega_1)\beta_2 + \sigma_2(a_2 \omega_2)\beta_2 + \ldots + \sigma_n(a_m \omega_m)\beta_2 + \ldots + \\
\sigma_n(a_1 \omega_1)\beta_n + \sigma_n(a_2 \omega_2)\beta_n + \ldots + \sigma_n(a_m \omega_m)\beta_n &= 0
\end{align*}$$

$$\begin{align*}
\sigma_1(a_1 \omega_1 + a_2 \omega_2 + \ldots + a_m \omega_m)\beta_1 + \sigma_2(a_1 \omega_1 + a_2 \omega_2 + \ldots + a_m \omega_m)\beta_2 + \ldots + \sigma_n(a_1 \omega_1 + a_2 \omega_2 + \ldots + a_m \omega_m)\beta_n &= 0.
\end{align*}$$

But $a_1, a_2, \ldots, a_m$ were arbitrary, so $a_1 \omega_1 + a_2 \omega_2 + \ldots + a_m \omega_m$ is an arbitrary element of $K$. Thus, the linear combination $\beta_1\sigma_1 + \beta_2\sigma_2 + \ldots + \beta_n\sigma_n$ is equivalent to the zero map. But, the above theorem assures us that $\sigma_1, \sigma_2, \ldots, \sigma_n$ is an linearly independent set. This gives us a contradiction. So we cannot have $n > [K : F]$. Note that so far, we haven’t used the fact that the elements $\sigma_1, \sigma_2, \ldots, \sigma_n$ form a group!

Suppose now that $n < [K : F]$. Then there are more than $n$ linearly independent (over $F$) elements in $K$. Let $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ be linearly independent. Then the system

$$\begin{align*}
\sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \ldots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\
\sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \ldots + \sigma_2(\alpha_{n+1})x_{n+1} &= 0 \\
&\vdots \\
\sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \ldots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0
\end{align*}$$

has a nontrivial solution (unknowns $> \text{equations}$). Let, $\beta_1, \beta_2, \ldots, \beta_n$ be a non-trivial solution.
If all of the $\beta_i$'s were elements of $F$, then substituting into the first equation and bringing the $\beta_i$'s inside the maps (they are fixed by these automorphisms) we get:

$$\sigma_1(\alpha_1\beta_1) + \sigma_1(\alpha_2\beta_2) + \ldots + \sigma_1(\alpha_n\beta_n) = 0$$

$$\sigma_1(\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots + \alpha_n\beta_n) = 0$$

And since $\sigma_1$ is 1-1, this means that $\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots + \alpha_n\beta_n = 0$. But this contradicts the fact that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are linearly independent. Thus at least one of the $\beta_i$'s is not in $F$.

Now, among all the non-trivial solutions to the system above, choose the one with the fewest, $r$, non-zero values. Then by renumbering if needed, we can assume that $\beta_1, \beta_2, \ldots, \beta_r$ are non-zero. Note that a multiple of any solution is also a solution, so we may assume that $\beta_r = 1$. (Note since at least one of the $\beta_i$'s must not be in $F$, $r > 1$.) Suppose that $\beta_1$ is not in $F$. Let's rewrite our system with these things in mind (substituting in this solution):

$$\sigma_1(\alpha_1\beta_1 + \ldots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) = 0$$

$$\sigma_2(\alpha_1\beta_1 + \ldots + \sigma_2(\alpha_{r-1})\beta_{r-1} + \sigma_2(\alpha_r) = 0$$

$$\vdots$$

$$\sigma_n(\alpha_1\beta_1 + \ldots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) = 0$$

More briefly:

$$(3) \quad \sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0 \quad \text{for } i = 1, 2, \ldots, n.$$ 

Now, since $\beta_1$ is not in $F$, there is at least one $1 < \eta < n$ for which $\sigma(\beta_1) \neq \beta_1$. Let's apply this map to all of our equations in the system above to get:

$$\sigma_j[\sigma_i(\alpha_1)\beta_1 + \ldots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r)] = 0 \quad \text{for } i = 1, 2, \ldots, n.$$ 

or (composing and homomorphism-ing):

$$\sigma_j \circ \sigma_i(\alpha_1) \sigma_i(\beta_1) + \ldots + \sigma_j \circ \sigma_i(\alpha_{r-1}) \sigma_i(\beta_{r-1}) + \sigma_j \circ \sigma_i(\alpha_r) = 0 \quad \text{for } i = 1, 2, \ldots, n.$$ 

But since $G$ is a group, the elements $\sigma_1 \circ \sigma_1, \ldots, \sigma_n \circ \sigma_n$ are just the elements $\sigma_1, \ldots, \sigma_n$ in some order. So we are just looking at the system:

$$(4) \quad \sigma_i(\alpha_1) \sigma_i(\beta_1) + \ldots + \sigma_i(\alpha_{r-1}) \sigma_i(\beta_{r-1}) + \sigma_i(\alpha_r) = 0 \quad \text{for } i = 1, 2, \ldots, n.$$ 

Let's do some subtracting! Subtracting (4) from (3) we get:

$$\sigma_i(\alpha_1)\beta_1 - \sigma_i(\alpha_1) \sigma_i(\beta_1) + \ldots + \sigma_i(\alpha_{r-1}) \beta_{r-1} - \sigma_i(\alpha_{r-1}) \sigma_i(\beta_{r-1}) + \sigma_i(\alpha_r) - \sigma_i(\alpha_r) = 0 \quad \text{for } i = 1, \ldots, n.$$ 

The last term is zero, so we get:

$$\sigma_i(\alpha_1)[\beta_1 - \sigma_i(\beta_1)] + \ldots + \sigma_i(\alpha_{r-1})[\beta_{r-1} - \sigma_i(\beta_{r-1})] = 0 \quad \text{for } i = 1, \ldots, n.$$ 

But since $\beta_1 - \sigma_i(\beta_1) \neq 0, \beta_1 - \sigma_i(\beta_1), \ldots, \beta_{r-1} - \sigma_i(\beta_{r-1})$ is a non-trivial solution to our original system that has fewer than $r$ non-zero values. Contradiction!!!

Thus we must conclude that $[ K : F ] = n = |G|$. BooYah!
Corollary 1 (Inequality used to prove the next Corollary). Let $K/F$ be a finite extension. Then $|\text{Aut}(K/F)| \leq [K : F]$ with equality if and only if $F$ is the fixed field of $\text{Aut}(K/F)$. Put another way, $K/F$ is Galois iff $F$ is the fixed field of $\text{Aut}(K/F)$.

Illustrative Example: Note that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is finite. But, $|\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| < [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. So, $\mathbb{Q}$ is not the fixed field of $\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. In fact, since $|\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 1$, the fixed field of $\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is all of $\mathbb{Q}(\sqrt{2})$.

Proof of Corollary: Let $F_1$ be the fixed field of $\text{Aut}(K/F)$, so that $F \subseteq F_1 \subseteq K$. By the previous Theorem, $[K : F_1] = |\text{Aut}(K/F)|$. Hence $[K : F] = |\text{Aut}(K/F)| [F_1 : F]$. Done!

Note, that the above proof uses another theorem that we haven’t proved. Namely that if we have fields $F \subseteq K \subseteq L$ then $[L : F] = [L : K] [K : F]$. You can prove this simply by using the basis for $K$ over $F$ and the basis for $L$ over $K$ to construct a basis for $L$ over $F$ (the same way I did when I constructed the splitting field for $x^4 - 2$ over $\mathbb{Q}$).

Corollary 2: (Used to prove the next corollary) Let $G$ be a finite subgroup of automorphisms of a field $K$ and let $F$ be the fixed field. Then every automorphism of $K$ fixing $F$ is contained in $G$. In other words, $G = \text{Aut}(K/F)$, so that $K/F$ is Galois with Galois group $G$.

Proof: By definition, $F$ is fixed by all the elements of $G$ so we have $G \leq \text{Aut}(K/F)$. The question is whether there are any automorphisms of $K$ fixing $F$ that are not in $G$ – i.e. whether this containment is proper.

We know that $|G| \leq |\text{Aut}(K/F)|$. By our second theorem, we have that $|G| = [K : F]$, and by the above corollary, $|\text{Aut}(K/F)| \leq [K : F]$. This means that $[K : F] = |G| \leq |\text{Aut}(K/F)| \leq [K : F]$. So $|G| = |\text{Aut}(K/F)|$ and since $G$ is finite we must have that $G = \text{Aut}(K/F)$.

Corollary 3: If $G_1$ and $G_2$ are distinct finite subgroups of automorphisms of a field $K$, then their fixed fields are also distinct.

Proof: Suppose that $F_1$ is the fixed field of $G_1$ and $F_2$ is the fixed field of $G_2$. If $F_1 = F_2$ then by definition, $F_1$ is fixed by $G_2$. By the previous corollary, any automorphism fixing $F_1$ is contained in $G_1$, hence $G_2 \leq G_1$. Similarly $G_1 \leq G_2$ and so $G_1 = G_2$.

Theorem 3 (Theorem 13 from Dummit & Foote): The extension $K/F$ is Galois if and only if $K$ is the splitting field of a separable polynomial over $F$. Furthermore, if this is the case then every irreducible polynomial with coefficients in $F$ which has a root in $K$ is separable and has all its roots in $K$ (so in particular $K/F$ is a separable extension).

Proof: [Omitted: Too much new background theory needed.]