You have now proved:

**The Fundamental Theorem of Galois theory** Let $L/K$ be a Galois extension with Galois group $G$. The maps $\mathrm{Stab}$ and $\mathrm{Fix}$ are inverse bijections between the set of subgroups of $G$ and the set of intermediate fields $F$ with $K \subseteq F \subseteq L$. Moreover, if $F_1 \subseteq F_2$, then $\mathrm{Stab}(F_1) \supseteq \mathrm{Stab}(F_2)$ and $[\mathrm{Stab}(F_1) : \mathrm{Stab}(F_2)] = [F_2 : F_1]$. If $H_1 \subseteq H_2$ then $\mathrm{Fix}(H_1) \supseteq \mathrm{Fix}(H_2)$ and $[\mathrm{Fix}(H_1) : \mathrm{Fix}(H_2)] = [H_2 : H_1]$.

We proceed to corollaries and related results.

**Problem 26.1.** Let $L/K$ be a Galois extension with Galois group $G$. Let $H$ be a subgroup of $G$ with corresponding subfield $F$.

(1) For $\sigma \in G$, show that the subfield $\sigma(F)$ corresponds to the subgroup $\sigma H \sigma^{-1}$.
(2) Show that the following are equivalent:
  - The extension $F/K$ is Galois.
  - For all $\theta \in F$ and all $\sigma \in G$, we have $\sigma(\theta) \in F$.
  - For all $\theta \in F$ and all $\sigma \in G$, we have $\theta \in \sigma(F)$.
  - The subgroup $H$ of $G$ is normal.
(3) Suppose that the above conditions hold. Show that $\mathrm{Gal}(F/K) \cong G/H$.

**Problem 26.2.** Let's do an old QR problem! Let $\zeta \in \mathbb{C}$ be a root of unity. Show that $2^{1/3} \not\in \mathbb{Q}(\zeta)$.

**Problem 26.3.** Let $K$ be a field and let $L_1, L_2, \dots, L_r$ be finite Galois extensions of $K$.

(1) Show that there is a Galois extension $M$ of $K$ such that all of the $L_j$ embed into $M$ and the $L_j$ generate $M$ as a field. (Hint: Take the splitting field of an appropriate polynomial.)
(2) Show that $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of $\prod \mathrm{Gal}(L_j/K)$.

**Problem 26.4.** Let $L/K$ be a Galois extension with Galois group $G$. Suppose that $G$ is a 2-group.

(1) Show that there a chain of subfields $K = K_0 \subset K_1 \subset \cdots \subset K_N = L$ with $[K_{j+1} : K_j] = 2$.
(2) Suppose that the characteristic of $K$ is not 2. Show that, in the preceeding chain, we can find elements $\phi_j \in K_j$ such that $K_{j+1} \cong K_j(\sqrt{\phi_j})$.
(3) (**Characterization of constructible numbers**) Let $\theta$ be algebraic over $\mathbb{Q}$ and let $L$ be the Galois closure of $\mathbb{Q}(\theta)$. Show that $\theta$ is constructible[1] if and only if $[L : \mathbb{Q}]$ is a power of 2.
(4) (**Gauss's construction of the 17-gon**) Show that a primitive 17-th root of unity is constructible.

**Problem 26.5.** The following problem is on the homework, check that everyone can solve it: Let $K$ be an infinite field, let $V$ be a finite dimensional $K$-vector space and let $H_1, H_2, \dots, H_N$ be finitely many proper $K$-subspaces of $V$. Show that there is an element of $V$ not in any $H_j$.

**Problem 26.6.** Let $L/K$ be a Galois extension.

(1) Show that there are only finitely many fields $F$ with $K \subseteq F \subseteq L$.
(2) Assume furthermore that $K$ is infinite. For every $F$ with $K \subseteq F \subseteq L$, show that there is an element $\theta \in F$ which is not in $F'$ for any $K \subseteq F' \subsetneq F$.
(3) (**The primitive element theorem**) Let $K$ be an infinite field and let $L$ be a separable extension of finite degree. Then there is $\theta \in L$ such that $L = K(\theta)$.

**Remark.** Given a finite degree field extension $L/K$, an element $\theta$ of $L$ such that $L = K(\theta)$ is called **primitive**. We have just show that separable extensions of infinite fields have primitive elements. It is also true that, if $L$ and $K$ are finite, then $L$ has a primitive element; the simplest proof I know is that the multiplicative group $L^{\times}$ will be cyclic and a generator for this group clearly must be primitive. The simplest example of an extension without a primitive element is $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$: Every element $\theta$ of $\mathbb{F}_p(x, y)$ has $\theta^p \in \mathbb{F}_p(x^p, y^p)$, so any such element only generates an extension of degree $p$ inside this degree $p^2$ extension.

[1] To make this problem easier, I will allow you to take square roots of negative, and more generally of complex numbers, when discussing constructibility.