Main theorems of Galois theory.

So far we have proved the following:

**Theorem 1.** Suppose $E/F$ is a finite extension. Then the following statements are equivalent:

1. $E$ is a splitting field of a separable polynomial over $F$.
2. $|\text{Aut}(E/F)| = [E : F]$.
3. $E/F$ is a Galois extension.
4. $F = \text{Fix}(\text{Aut}(E/F))$.
5. $F = \text{Fix}(G)$ for some finite subgroup $G$ of $\text{Aut}(E)$.

Now we have all the needed tools to prove:

**Theorem 2.** Suppose $E/F$ is a finite Galois extension. Let

$$
\begin{align*}
\{K | F \subseteq K \subseteq E, K \text{ subfield}\} & \quad \{H | H \leq \text{Gal}(E/F)\} \\
K & \quad \Psi \quad \text{Gal}(E/K) \\
\text{Fix}(H) & \quad \Phi \quad \text{Gal}(E/K)
\end{align*}
$$

1. $\Psi$ is well-defined; that means $E/K$ is a Galois extension. And $\Psi$ and $\Phi$ are inverse of each other.
2. These maps give bijections between normal extensions $K/F$ and normal subgroups of $\text{Gal}(E/F)$.
3. If $K/F$ is a normal extension and $F \subseteq K \subseteq E$, then

$$\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K).$$

**Proof.** (1): For any $\alpha \in E$, we have that $m_{\alpha,K}(x)|m_{\alpha,F}(x)$. Hence all the zeros of $m_{\alpha,K}(x)$ are in $E$ and all of them are distinct. Hence $E/K$ is a normal separable extension. Hence $E/K$ is a Galois extension.

We have

$$(\Phi \circ \Psi)(K) = \text{Fix}(\text{Gal}(E/K)) = K,$$
and

$$(\Psi \circ \Phi)(H) = \text{Gal}(E/\text{Fix}(H)) = H.$$  

(2) and (3): Suppose $K/F$ is a normal extension. For any $\alpha \in K$, $m_{\alpha,F}(x)$ has distinct zeros in $E$ as $E/F$ is separable. Hence $K/F$ is a separable extension. Therefore $K/F$ is both normal and separable, which means that it is a Galois extension.

Since $E/F$ and $K/F$ are normal extension, the restriction map $r : \text{Gal}(E/F) \to \text{Gal}(K/F)$ is a well-defined onto group homomorphism. And $\text{ker}(r)$ is clearly $\text{Aut}(E/K) = \text{Gal}(E/K)$. Hence we have that $\Psi(K)$ is a normal subgroup of $\text{Gal}(E/F)$ and

$$\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K).$$

Suppose $H$ is a normal subgroup of $\text{Gal}(E/F)$. Let $K := \text{Fix}(H)$. Suppose $\overline{F}$ is an algebraic closure of $F$ that has $E$ as a subfield. To show $K/F$ is a normal extension, it is enough to show that for any $\widehat{\sigma} \in \text{Aut}(\overline{F}/F)$ we have $\widehat{\sigma}(K) = K$. Notice that, since $\widehat{\sigma}(F) = F$ and $K/F$ is a finite extension, it is enough to show $\widehat{\sigma}(K) \subseteq K$. Since $E/F$ is a normal extension, $\widehat{\sigma}(E) = E$. So the restriction $\sigma$ of $\widehat{\sigma}$ to $E$ gives us an element of $\text{Gal}(E/F)$. We have to show for any $\alpha \in K$,

$$\widehat{\sigma}(\alpha) = \sigma(\alpha) \in \text{Fix}(H).$$

Hence we have to show for any $\tau \in H$, we have

$$\tau(\sigma(\alpha)) \equiv \sigma(\alpha).$$

Notice that since $H$ is a normal subgroup of $\text{Gal}(E/F)$, we have $\sigma^{-1} \circ \tau \circ \sigma \in H$. Therefore

$$(\sigma^{-1} \circ \tau \circ \sigma)(\alpha) = \alpha;$$

and claim follows. \hfill \Box

It is worth pointing out that in the above proof, we showed: if $E/F$ is a separable extension and $K$ is an intermediate subfield, then $K/F$ is a separable extension. Later partially as part of your HW assignment you will strengthen this result by showing that $E/F$ is separable if and only if $E/K$ and $K/F$ are separable. As a consequence of the main theorem of Galois theory, we also see that if $E/F$ is a normal extension, then $E/K$ is normal; but $K/F$ is often not a normal extension. (If all the subgroups of $\text{Gal}(E/F)$ are normal, then for any
intermediate subfield \( K \) we have that \( E/K \) and \( K/F \) are normal extensions; in particular we get this when \( \text{Gal}(E/F) \) is an abelian group.

Let us also observe that the set of intermediate subfields of \( F \subseteq E \) and the set of all subgroups of \( \text{Gal}(E/F) \) are POSets with respect to the inclusion. And \( \Psi \) and \( \Phi \) are order reversing bijections:

if \( K_1 \subseteq K_2 \), then clearly \( \Psi(K_1) \supseteq \Psi(K_2) \); and if \( H_1 \subseteq H_2 \), then clearly \( \Phi(H_1) \supseteq \Phi(H_2) \). Hence we get that

\[
K_1 \subseteq K_2 \Leftrightarrow \Psi(K_1) \supseteq \Psi(K_2), \text{ and } H_1 \subseteq H_2 \Leftrightarrow \Phi(H_1) \supseteq \Phi(H_2).
\]

The following is a non-obvious corollary of the main theorem of Galois theory.

**Theorem 3.** Suppose \( E/F \) is a finite separable extension. Then there are only finitely many intermediate subfields \( F \subseteq K \subseteq E \).

**Proof.** Suppose \( \{\alpha_1, \ldots, \alpha_n\} \) is an \( F \)-basis of \( E \). Let \( L \) be a splitting field of \( f(x) := \prod_{i=1}^{n} m_{\alpha_i,F}(x) \). Since \( E/F \) is a separable extension, \( f(x) \) is a separable polynomial. Hence \( L/F \) is a finite Galois extension. Hence by the main theorem of Galois theory, there are only finitely many intermediate subfields \( F \subseteq K \subseteq L \); and claim follows. \( \square \)

It is worth pointing out that \( L \) in the above proof is the smallest Galois extension of \( F \) that contains \( E \) as a subfield. That is why \( L \) is called the Galois closure of \( E \) over \( F \). When \( E/F \) is not separable, we still can do the above construction; and we get the smallest normal extension of \( F \) that contains \( E \) as a subfield. That is why in general we call \( L \) the normal closure of \( E \) over \( F \).

**Problem 4.** Prove that the finite field extension \( \mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p) \) has infinitely many intermediate subfields.

**Theorem 5.** Suppose \( E/F \) is a finite field extension. Then there are only finitely many intermediate subfields \( F \subseteq K \subseteq E \) if and only if there is \( \alpha \in E \) such that \( E = F[\alpha] \). (In this case \( \alpha \) is called a primitive element and \( E/F \) is called a simple extension.)

**Corollary 6.** Suppose \( E/F \) is a finite separable extension. Then \( E/F \) is a simple extension.

**Proof.** This is an immediate corollary of the previous couple of theorems. \( \square \)
Proof of Theorem 5. (⇒) Since $E/F$ is a finite extension, $E = F[\alpha_1, \ldots, \alpha_n]$ for some $\alpha_i$’s. Using induction on $n$, it is clear that it is enough to prove the case of $n = 2$. So suppose $E = F[\alpha_1, \alpha_2]$.

If $F$ is a finite field, then $E$ is a finite field. And so $E^\times$ is a cyclic group. (Recall that in you have proved the following result in group theory: if $G$ is a finite group and for any positive integer $n$, $|\{g^n = 1 \mid g \in G\}| \leq n$, then $G$ is a cyclic group. Using this result it is immediate that $E^\times$ is cyclic if $E$ is a finite field.) Suppose $E^\times = \langle \alpha \rangle$; and so $E = F[\alpha]$.

Suppose $F$ is infinite and $E = F[\alpha_1, \alpha_2]$. Consider the family of intermediate subfields $\{F[\alpha_1 + c\alpha_2] \mid c \in F\}$. Since there are only finitely many intermediate subfields and $F$ is infinite, there are $c, c' \in F$ such that $c \neq c'$ and $K := F[\alpha_1 + c\alpha_2] = F[\alpha_1 + c'\alpha_2]$. Therefore $K$ contains $(\alpha_1 + c\alpha_2) - (\alpha_1 + c'\alpha_2) = (c - c')\alpha_2$. Since $F \subseteq K$ and $c - c' \in F^\times$, we deduce that $\alpha_2 \in K$. And so $\alpha_1 \in K$. Thus $K = F[\alpha_1, \alpha_2] = E$, which implies $E = F[\alpha_1 + c\alpha_2]$ is a simple extension.

(⇐) Suppose $E = F[\alpha]$. For an intermediate subfield $F \subseteq K \subseteq F$, let $g(x) := m_{\alpha,K}(x)$. Notice that $m_{\alpha,F}(\alpha) = 0$ and $m_{\alpha,F}(x) \in K[x]$; and so $g(x)|m_{\alpha,F}(x)$. Hence there are only finitely many possibilities for $g(x)$. Next we show that $g(x)$ uniquely determines $K$; and so there are only finitely many possibilities for $K$. Let $K'$ be the intermediate subfield generated by the coefficients of $g(x)$. So $K' \subseteq K$, $g(x) \in K'[x]$, and $g(x)$ is irreducible in $K[x]$. Thus $g(x)$ is irreducible in $K'[x]$. As $g(\alpha) = 0$, we deduce that $g(x) = m_{\alpha,K'}(x)$. Hence

$$[K'[\alpha] : K'] = \deg m_{\alpha,K'}(x) = \deg g(x) = \deg m_{\alpha,K}(x) = [K[\alpha] : K].$$

On the other hand, $K'[\alpha] \supseteq F[\alpha] = E$ and $K[\alpha] \supseteq F[\alpha] = E$. Therefore we have

$$[E : K] = [E : K'] = [E : K][K : K'],$$

which implies that $K = K'$; and so $g(x)$ uniquely determines $K$. □

Now that we have seen how strong separability condition can be, we investigate it in a more depth. Notice that since any algebraic extension of $F$ can be embedded in $\overline{F}$ where $\overline{F}$ is an algebraic closure of $F$ and $\overline{F}/F$ is a normal extension, we have:

$\overline{F}/F$ is Galois ⇔ $\overline{F}/F$ is separable ⇔ any algebraic extension $E/F$ is separable.

Next we want to find the precise condition on $F$ so that $\overline{F}/F$ is separable. To
this end, we need to come up a mechanism to determine if a given irreducible polynomial has multiple zeros or not. We start with a lemma.

**Lemma 7.** Suppose $E/F$ is a field extension and $f, g \in F[x]$. Then $\gcd(f, g)$ in $F[x]$ is the same as $\gcd(f, g)$ in $E[x]$ up to a multiplication by an element of $E^\times$.

**Proof.** Suppose $q(x) = \gcd(f(x), g(x))$ in $F[x]$. Therefore there are $r(x), s(x) \in F[x]$ such that $r(x)f(x) + s(x)g(x) = q(x)$; and so

$$r(x)(f(x)/q(x)) + s(x)(g(x)/q(x)) = 1.$$  

This implies that $\gcd(f(x)/q(x), g(x)/q(x)) = 1$ in $E[x]$. Thus $\gcd(f(x), g(x)) = q(x)$ in $E[x]$; and claim follows. \qed

In the next lecture we will prove:

**Lemma 8.** (1) $f(x) \in F[x]$ does not have multiple zeros if and only if

$$\gcd(f(x), f'(x)) = 1.$$  

(2) Suppose $f(x)$ is irreducible in $F[x]$. Then there is an irreducible separable polynomial $g(x) \in F[x]$ and a positive integer $k$ such that $f(x) = g(x^{p^k})$ where

$$p = \begin{cases} \text{char}(F) & \text{if char}(F) \neq 0, \\ 1 & \text{otherwise}. \end{cases}$$  

In particular, if char$(F) = 0$, then any polynomial in $F[x]$ is separable.