1 Review

Let $L \mid K$ be a field extension. Write $\mathrm{Aut}_K(L)$ for the group of K-linear field isomorphisms $L \to L$.
If $G \subseteq \mathrm{Aut}_K(L)$ is a subgroup then we let $L^G = \{a \in L : g(a) = a \text{ for all } g \in G\}$.

The field extension $L \mid K$ is *finite* is $[L : K] = \dim_K(L) < \infty$.
The field extension $L \mid K$ is *Galois* if $L^{\mathrm{Aut}_K(L)}$ is equal to the image of K in L.
For finite Galois extensions the *Galois group* $\mathrm{Gal}(L \mid K) = \mathrm{Aut}_K(L)$ is finite.

For finite field extensions $L \mid K$, the following properties are equivalent:

(a) $L \mid K$ is a Galois extension.
(b) L is the splitting field of a separable polynomial over K.
(c) The extension $L \mid K$ is normal and separable.

Theorem (*Artin's lemma*)**.** Let K be a field and let $G \subseteq \mathrm{Aut}(K)$ be a finite subgroup.
Then $K \mid K^G$ is a finite Galois extension and $G = \mathrm{Aut}_{K^G}(K)$.

2 The fundamental theorem of Galois theory

If $\iota : K \hookrightarrow L$ is a field extension, then an *intermediate field* is a subfield of L containing $\iota(K)$.
As explained last time, if $L \mid K$ is finite Galois and M is an intermediate field then $L \mid M$ is also Galois.

Our first goal today is to prove the following fundamental theorem:

Theorem. Let $\iota : K \hookrightarrow L$ be a finite Galois extension.

(i) The map $M \mapsto \mathrm{Gal}(L \mid M)$ is a bijection

$$\{\text{subfields } M \text{ of } L \text{ containing } \iota(K)\} \mapsto \{\text{subgroups of } \mathrm{Gal}(L \mid K)\}.$$

Its inverse is given by the map $H \mapsto L^H$ where H is a subgroup of $\mathrm{Gal}(L \mid K)$.

(ii) Let M be a subfield of L containing $\iota(K)$. Then

$$[L : M] = |\mathrm{Gal}(L \mid M)| \quad \text{and} \quad [M : K] = \frac{|\mathrm{Gal}(L \mid K)|}{|\mathrm{Gal}(L \mid M)|}.$$

(iii) Let M be a subfield of L containing $\iota(K)$.
Then $M \mid K$ is a Galois extension if and only if $\mathrm{Gal}(L \mid M)$ is a normal subgroup of $\mathrm{Gal}(L \mid K)$.
When this holds, we have $\gamma(M) = M$ for all $\gamma \in \mathrm{Gal}(L \mid K)$ and there is a unique isomorphism

$$I_M : \mathrm{Gal}(L \mid K)/\mathrm{Gal}(L \mid M) \xrightarrow{\sim} \mathrm{Gal}(M \mid K)$$

sending the image of $\gamma \in \mathrm{Gal}(L \mid K)$ in $\mathrm{Gal}(L \mid K)/\mathrm{Gal}(L \mid M)$ to its restriction $\gamma\big|_M$.

Proof. For part (i) we need to prove that

$$M = L^{\mathrm{Gal}(L|M)} \qquad \text{and} \qquad \mathrm{Gal}(L \mid L^H) = H$$

for any intermediate field M and any subgroup $H \subseteq \mathrm{Gal}(L \mid K)$.

We have $M = L^{\mathrm{Gal}(L|M)}$ since $L \mid M$ is a Galois extension.
We have $\mathrm{Gal}(L \mid L^H) = H$ by Artin's lemma.

In part (ii), we have $[L : M] = |\mathrm{Gal}(L \mid M)|$ as $L \mid M$ is a splitting field of a separable $P(x) \in M[x]$.
The second identity in part (ii) holds that $[M : K][L : M] = [L : K] = |\mathrm{Gal}(L \mid L)|$.

For part (iii), suppose that M is an intermediate field and that $M \mid K$ is a Galois extension.
Then $M \mid K$ is a splitting extension for some $P(x) \in K[x]$.

Clearly $M \hookrightarrow L$ is a homomorphism of K-extensions $M \mid K \to L \mid K$.
But if $\gamma \in \mathrm{Gal}(L \mid K)$ then $\gamma\big|_M$ is another homomorphism of K-extensions $M \mid K \to L \mid K$.

By a theorem proved in Lecture 16, the images of these homomorphisms must coincide.
As the image of one homomorphism is M while the other is $\gamma(M)$, we have $M = \gamma(M)$.

Thus the restriction operation $\gamma \mapsto \gamma\big|_M$ is a homomorphism $\mathrm{Gal}(L \mid K) \to \mathrm{Gal}(M \mid K)$.
The kernel of this homomorphism is $\mathrm{Gal}(L \mid M)$ so this subgroup is normal in $\mathrm{Gal}(L \mid K)$.

Now, conversely, suppose that $\mathrm{Gal}(L \mid M)$ is a normal subgroup of $\mathrm{Gal}(L \mid K)$.
Let $\gamma \in \mathrm{Gal}(L \mid K)$. We compute from the definitions that

$$\begin{aligned}
\mathrm{Gal}(L \mid \gamma(M)) &= \{\mu \in \mathrm{Gal}(L \mid K) : \mu(m) = m \text{ for all } m \in \gamma(M)\} \\
&= \{\mu \in \mathrm{Gal}(L \mid K) : \mu \circ \gamma(m) = \gamma(m) \text{ for all } m \in M\} \\
&= \{\mu \in \mathrm{Gal}(L \mid K) : \gamma^{-1} \circ \mu \circ \gamma(m) = m \text{ for all } m \in M\} \\
&= \{\gamma \circ \mu \circ \gamma^{-1} : \mu \in \mathrm{Gal}(L \mid M)\} \\
&= \mathrm{Gal}(L \mid M).
\end{aligned}$$

Thus $\gamma(M) = L^{\mathrm{Gal}(L|\gamma(M))} = L^{\mathrm{Gal}(L|M)} = M$.

Thus $\gamma \mapsto \gamma\big|_M$ is again a homomorphism $\mathrm{Gal}(L \mid K) \to \mathrm{Aut}_K(M)$.
Let $H \subseteq \mathrm{Aut}_K(M)$ be the image of this homomorphism.

Then part (ii) tells us that $|H| = [M : K]$.
On the other hand, by Artin's lemma, we know that $[M : M^H] = |H| = [M : K]$.
Hence $[M^H : K] = \frac{[M:K]}{[M:M^H]} = 1$ so $M^H = K$ and therefore also $M^{\mathrm{Aut}_K(M)} = K$.

Thus $M \mid K$ is a Galois extension so by part (i) we must have $H = \mathrm{Aut}_K(M)$.
This means that our homomorphism $\mathrm{Gal}(L \mid K) \to \mathrm{Aut}_K(M) = \mathrm{Gal}(M \mid K)$ is surjective.
The kernel of this map is $\mathrm{Gal}(L \mid M)$ so passing to the quotient gives the desired homomorphism I_M. □

Here is an another characterization of Galois extensions, which was established in the previous argument.

Corollary. Let $\iota : K \hookrightarrow L$ be a Galois extension and suppose $M \subseteq L$ be an intermediate field.
Then $M \mid K$ is a Galois extension if and only if all homomorphisms of K-extensions

$$M \mid K \to L \mid K$$

have the same image, which must be M.

Proof. Suppose that all homomorphisms of K-extensions $M \mid K \to L \mid K$ have M as their image.
Then for all $\gamma \in \mathrm{Gal}(L \mid K)$ we have $\gamma(M) = M$ so restriction defines a homomorphism

$$\mathrm{Gal}(L \mid K) \to \mathrm{Aut}_K(M)$$

whose kernel is $\mathrm{Gal}(L \mid M)$. Thus $\mathrm{Gal}(L \mid M)$ is a normal subgroup of $\mathrm{Gal}(L \mid K)$ so $M \mid K$ is Galois.

Conversely, if $M \mid K$ is a Galois extension then we saw above that $\gamma(M) = M$ for all $\gamma \in \mathrm{Gal}(L \mid K)$. □

Corollary. Let $\iota : K \hookrightarrow L$ be a finite separable field extension.
Then there are only finitely many intermediate fields between L and $\iota(K)$.

Proof. After replacing L with a splitting field we may assume that $L \mid K$ is a finite Galois extension.
Then $\mathrm{Gal}(L \mid K)$ is a finite group with finitely many subgroups.
These subgroups are in bijection with the intermediate fields. □

3 Miscellaneous results

Lemma. Let $L \mid K$ be a finite Galois extension. Choose $\alpha \in L$.
Then the minimal polynomial of α over K is

$$P(x) = \prod_{\beta \in \mathrm{Orb}(\mathrm{Gal}(L|K),\alpha)} (x - \beta).$$

Proof. Let $m_\alpha(x) \in K$ be the minimal polynomial of α over K.
We showed in Lecture 17 that $P(x) \in K[x]$ and so $m_\alpha(x) \mid P(x)$.
Thus it suffices to prove that $P(x)$ is irreducible over K.

Suppose for contradiction that $P(x)$ is reducible.
Let $P(x) = Q(x)T(x)$ for two non-constant polynomials $Q(x), T(x) \in K[x]$.
Note that if $\rho \in L$ and $Q(\rho) = 0$, then for any $\gamma \in \mathrm{Gal}(L \mid K)$, we have

$$\gamma(Q(\rho)) = Q(\gamma(\rho)) = \gamma(0) = 0$$

and thus the roots of $Q(x)$ in L are stable under the action of $\mathrm{Gal}(L \mid K)$.

Now note that $Q(x)$ has a root in L, since $P(x)$ splits in L and $Q(x) \mid P(x)$.

Thus the set of the roots of $P(x)$ contains a subset stable under $\mathrm{Gal}(L \mid K)$ with cardinality less than

$$\deg(P(x)) = |\mathrm{Orb}(\mathrm{Gal}(L \mid K), \alpha)|.$$

This contradicts the fact that the set of roots of $P(x)$ is the orbit of α under $\mathrm{Gal}(L \mid K)$. □

Theorem (Primitive element theorem)**.** Let $L \mid K$ be a finite separable extension of fields.
Then $L = K(\alpha)$ for some $\alpha \in L$, so $L \mid K$ is a simple extension.

Proof. When K is a finite field, L is also a finite field, so the result follows as $L \setminus \{0\}$ is a cyclic group. (The last fact is left as an exercise.)

Suppose that K is an infinite field.
Since L is a finite extension of K, L is generated over K by a finite number of elements.
By induction, it is enough to prove that L is generated by one element if it is generated by two elements.

To this end suppose that $L = K(\beta, \gamma)$.
For each $d \in K$ we consider the intermediate field $K(\beta + d\gamma)$.

By the last corollary above, there are only finitely many intermediate fields.
(This is the part of the argument that uses the assumption that $L \mid K$ is finite and separable.)
Since K is infinite, we may thus find $d_1, d_2 \in K$ such that $d_1 \neq d_2$ and $K(\beta + d_1\gamma) = K(\beta + d_2\gamma)$.

Every element of $K(\beta + d_2\gamma)$ can be expressed as a polynomial in $\beta + d_2\gamma$ with coefficients in K.
Thus $\beta + d_1\gamma = P(\beta + d_2\gamma)$ for some $P(x) \in K[x]$, and for this polynomial we have

$$\boxed{\gamma = \frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}} \quad \text{and} \quad \boxed{\beta = (\beta + d_2\gamma) - d_2\frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}}.$$

This shows that $\{\beta, \gamma\} \subset K(\beta + d_2\gamma) \subseteq K(\beta, \gamma)$ so in fact $K(\beta, \gamma) = K(\beta + d_2\gamma)$.
Thus if L is generated by two elements over K then it actually is a simple extension.
By iteration, we conclude that $L \mid K$ is simple whenever it is finite and separable. □