Fields to Groups and Back Again

Let us fix some finite extension $F \subset K$ of subfields of $C$ and set $G$ to be the Galois Group $\Gamma(K : F)$. We will be interested in intermediate fields $L$, that is, $F \subset L \subset K$, and in subgroups $H$ of $G$. We will describe first a mapping from fields $L$ to groups $H$

**Definition 1** Let $F \subset L \subset K$ be an intermediate field. We define $L^*$, a subgroup of $G$, by

$$L^* = \{ \sigma \in G : \sigma(\alpha) = \alpha \text{ for all } \alpha \in L \}$$  (1)

That is, $L^*$ is those automorphisms of $L$ which fix all elements of $L$.

Why is $L^*$ a subgroup of $G$? Well, suppose $\sigma, \tau$ were two automorphims of $K$ over $F$. Then, as we have discussed before, so is $\sigma\tau$. But further, if $\sigma(\alpha) = \alpha$ and $\tau(\alpha) = \alpha$ for all $\alpha \in L$ then

$$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \alpha$$

for all $\alpha \in L$ and so $\sigma\tau \in L^*$. Similarly $\sigma^{-1} \in L^*$. Finally the identity $e \in L^*$ as $e$ fixes all elements.

We now will describe first a mapping from groups $H$ to fields $L$.

**Definition 2** Let $H \subset G$ be a subgroup of the Galois Group. We define $H^\dagger$, an intermediate field, by

$$H^\dagger = \{ \alpha \in K : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H \}$$  (2)

That is, $H^\dagger$ is those elements of $K$ which are fixed by all automorphisms $\sigma \in H$.

Set $L = H^\dagger$. Why is $L$ an intermediate field? First of all, as all auto- morphisms $\sigma \in \Gamma$ fix all elements $c \in F$, any element $c \in F$ will be fixed by all $\sigma \in H$, so that $F \subset L$. Now suppose $\alpha, \beta \in L$ and take any $\sigma \in H$. As $\sigma(\alpha) = \alpha$ and $\sigma(\beta) = \beta$, we must have $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$. Thus $\alpha + \beta \in L$ and similarly $\alpha\beta, -\alpha, \alpha^{-1} \in L$.

**An Extended Example:** Take ground field $F = Q$ and extension $K = Q(\sqrt{2}, \sqrt{3})$. The four elements of the Galois Group $G$ are $e, \sigma_1, \sigma_2, \sigma_3$ where (as done earlier)

$$e(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$
\[ \sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \]
\[ \sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \]
\[ \sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \]

\( G \) is the Vierergruppe. There are five subgroups (we count the trivial ones here) of \( G \):

\[ \{e\}, H_1 = \{e, \sigma_1\}, H_2 = \{e, \sigma_2\}, H_3 = \{e, \sigma_3\}, \text{ and } G \text{ itself.} \]

Let's start in the “middle” with \( H_1 = \{e, \sigma_1\} \). What is \( H_1^{\dagger} \)? That is, which \( \alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \) are fixed by all \( e, \sigma_1 \). Well, \( e \) is the identity so it fixes everything so we can ignore it. If we think of \( \sigma_1(\alpha) = \alpha \) as an (easy!) equation it is true precisely when \( b = d = 0 \). So \( \alpha \in H_1^{\dagger} \) if and only if we can write \( \alpha = a + c\sqrt{3} \). That is, \( H_1^{\dagger} = \{Q(\sqrt{3})\} \). Similarly, for \( \alpha \in H_2^{\dagger} \) the necessary and sufficient condition is that \( c = d = 0 \) so \( \alpha = a + b\sqrt{2} \) and \( H_2^{\dagger} = \{Q(\sqrt{2})\} \). Similarly, for \( \alpha \in H_3^{\dagger} \) the necessary and sufficient condition is that \( b = c = 0 \) so \( \alpha = a + d\sqrt{6} \) and \( H_3^{\dagger} = \{Q(\sqrt{6})\} \).

The case \( \{e\}^{\dagger} \) is always the same, since the identity preserves everything \( \{e\}^{\dagger} = K \). Finally, what about \( G^{\dagger} \). That is, which \( \alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \) are fixed by all \( e, \sigma_1, \sigma_2, \sigma_3 \). To be fixed by \( \sigma_1 \) forces \( b = d = 0 \), to be fixed by \( \sigma_2 \) forces \( c = d = 0 \), to be fixed by \( \sigma_3 \) is now redundant as it forces \( b = c = 0 \). So all of \( b, c, d \) must be zero but \( a \) can be an arbitrary rational and so \( G^{\dagger} = \{Q\} \).

Now set

\[ L_1 = Q(\sqrt{2}), L_2 = Q(\sqrt{3}), L_3 = Q(\sqrt{6}) \]

and consider the groups associated (via \( * \)) with the fields \( Q, L_1, L_2, L_3, K \).

The easiest is \( Q^{*} = G \), which is to say that all \( \sigma \in G \) fix all \( \alpha \in Q \) which is true as \( G \) was defined as all automorphisms \( \sigma \) of \( K \) which fix all \( \alpha \in Q \).

How about \( L_1^{*} \)? Clearly \( e \in L_1^{*} \) as \( e \) fixes everything. Also \( \sigma_2 \in L_1^{*} \) as \( \sigma_2(a + b\sqrt{2}) = a + b\sqrt{2} \). But \( \sigma_1, \sigma_3 \notin L_1^{*} \) as they send \( \sqrt{2} \) to \( -\sqrt{2} \). So \( L_1^{*} = \{e, \sigma_2\} \).

How about \( L_2^{*} \)? Clearly \( e \in L_2^{*} \) as \( e \) fixes everything. Also \( \sigma_1 \in L_2^{*} \) as \( \sigma_1(a + c\sqrt{3}) = a + c\sqrt{3} \). But \( \sigma_2, \sigma_3 \notin L_2^{*} \) as they send \( \sqrt{3} \) to \( -\sqrt{3} \). So \( L_2^{*} = \{e, \sigma_1\} \).

How about \( L_3^{*} \)? Clearly \( e \in L_3^{*} \) as \( e \) fixes everything. Also \( \sigma_3 \in L_3^{*} \) as \( \sigma_3(a + d\sqrt{6}) = a + d\sqrt{6} \). But \( \sigma_1, \sigma_2 \notin L_3^{*} \) as they send \( \sqrt{6} \) to \( -\sqrt{6} \). So \( L_3^{*} = \{e, \sigma_3\} \).

Finally, how about \( K^{*} \). Clearly \( e \in K^{*} \) as \( e \) fixes everything. But the other \( \sigma_1, \sigma_2, \sigma_3 \) do not fix everything and so are not in \( K^{*} \). Thus \( K^{*} = \{e\} \).

We can put this all in tabular form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>( K = Q(\sqrt{2}, \sqrt{3}) )</td>
<td>( {e} )</td>
</tr>
<tr>
<td>( L_1 = Q(\sqrt{2}) )</td>
<td>( H_2 = {e, \sigma_2} )</td>
</tr>
<tr>
<td>( L_2 = Q(\sqrt{3}) )</td>
<td>( H_1 = {e, \sigma_1} )</td>
</tr>
<tr>
<td>( L_3 = Q(\sqrt{6}) )</td>
<td>( H_3 = {e, \sigma_3} )</td>
</tr>
<tr>
<td>( Q )</td>
<td>( G = {e, \sigma_1, \sigma_2, \sigma_3} )</td>
</tr>
</tbody>
</table>
We see we have a one-to-one correspondence. We can go from fields to
groups by applying \( \ast \). And we can go from groups to fields by applying \( \dagger \).
And \( \dagger \) and \( \ast \) are inverses as maps, if we apply one and then the other we get back where we started.

Does this always work? No. But it works in important cases and that
will be the substance of the major theorem of Galois Theory. Indeed, not
to keep you in suspense, here is that theorem. The normal extensions are precisely those extensions for which the correspondence works!

**Theorem 0.1 The Galois Correspondence Theorem** Let \( F \subset K \) be subfields of \( C \) with \( K : F \) a normal extension. Set \( G = \Gamma(K : F) \). Then there is a bijection between the intermediate fields \( L \), meaning that \( F \subset L \subset K \) and the subgroups \( H \) of \( G \). (We include \( L = F \), \( L = K \) as intermediate fields and we include \( \{e\} \) and \( G \) itself as subgroups.) The bijection is given by \( \ast \) and \( \dagger \) as previously defined. That is, \( H = L \ast \) if and only if \( L = H \dagger \). Thus

\[
(L^\ast)^\dagger = L \text{ and } (H^\dagger)^\ast = H
\]

Furthermore, the correspondence reverses containment, making \( L \) bigger
makes \( H = L^\ast \) smaller and making \( H \) bigger makes \( L = H^\dagger \) smaller. The
field \( F \) is associated with all of \( G \) while the field \( K \) is associated with \( \{e\} \).
Setting \( n = [K : F] \) we have \( n = |G| \). Further the sizes are connected, when
\( H = L^\ast \)

\[
[K : L] = |H|
\]

or, equivalently,

\[
[L : F] = |G/H|
\]

A Powerful Application: In the listing for \( K = Q(\sqrt{2}, \sqrt{3}) \) above as
\( G \) has only four elements it doesn’t take too much work (try it!) to show
that \( \{e\}, H_1, H_2, H_3, G \) are the only subgroups. It is not at all clear that
we have listed all of the subfields of \( K \). How do we know there isn’t some
other weird intermediate field between \( Q \) and \( K \)? After all, these are infinite
sets so we can’t try everything. On the other side, however, we are dealing
with finite groups \( G = \Gamma(K : F) \). These can only have a finite number of
subgroups \( H \) and by some (perhaps laborious) effort we can list them all.
The Galois Correspondence Theorem then allows us to give a complete
list of the intermediate fields \( L \).

A Cautionary Example: Let the ground field \( F = Q \) and the extension
field \( K = Q(2^{1/3}) \). Any automorphism \( \sigma : K \to K \) must send \( 2^{1/3} \) to a root
of \( x^3 - 2 \) but \( 2^{1/3} \) is the only root of \( x^3 - 2 \) in \( K \), as the other roots are
not real. Thus we must have \( \sigma(2^{1/3}) = 2^{1/3} \) and so \( \sigma \) must be the identity.
That is, \( G = \Gamma(K : Q) = \{e\} \). As \( [K : Q] = 3 \) there are no intermediate
diagonals except for \( Q \) and \( K \) themselves. So \( Q^\ast = \{e\} \) and \( K^\ast = \{e\} \). As every
element is fixed by \( e \), \( \{e\}^\ast = K \). So in this case we do not get a bijection
between subgroups of the Galois Group and intermediate fields.

For any extension \( K : F \) the following “easy” result is one part of 3, the
main part of the Galois Correspondence Theorem, Theorem 0.1.
Theorem 0.2 Let $F \subset K$ be subfields of $C$. Then for any intermediate field $L$

$$L \subset (L^*)^\dagger$$

(6)

and for any subgroup $H$

$$H \subset (H^\dagger)^*$$

(7)

Proof: $L^*$ is those automorphisms $\sigma$ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in L$. That is, all $\sigma \in L^*$ fix all $\alpha \in L$. That is, all $\alpha \in L$ are fixed by all $\sigma \in L^*$ and hence all $\alpha \in L$ belong to $(L^*)^\dagger$. Similarly, $H^\dagger$ is those $\alpha \in K$ such that $\sigma(\alpha) = \alpha$ for all $\sigma \in H$. That is, all $\sigma \in H$ fix all $\alpha \in H^\dagger$. That is, all $\sigma \in H$ are in $(H^\dagger)^*$. 