MA542 Lecture

Timothy Kohl

Boston University

March 31, 2025

Galois Groups

Last time, we introduced the concept of Galois group of an extension.

Definition

Let E be an extension field of F. The Galois Group of E over F, denoted $Gal(E/F)$ is the set of automorphisms $\phi : E \to E$ such that for $c \in F$, one has $\phi(c) = c$.
And for a subgroup $H \leq Gal(E/F)$ the fixed field
$E_H = \{x \in E \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ which is a field which is intermediate between E and F. (depending on H of course).

And as mentioned last time, when $F = \mathbb{Q}$ any automorphism of E fixes $F = \mathbb{Q}$, but when F is larger, one needs to check.

Let's consider the extension $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$, and we begin with the basis of E over $\mathbb{Q}$.

As $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ has basis

$$\{1, \sqrt{3}\}$$

and $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ has basis

$$\{1, \sqrt{5}\}$$

then as $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ contains *both*, and $\mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt{5}) = \mathbb{Q}$ then the following 4 element set is a basis:

$$\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\sqrt{5} = \sqrt{15}\}$$

and so any automorphism is determined by how it acts on these basis 'vectors'.

Given the basis $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ and $\phi \in Gal(E/\mathbb{Q})$ then obviously $\phi(1) = 1$.

Moreover, since $\sqrt{3}^2 = 3$ and $\sqrt{5}^2 = 5$ then $\phi(\sqrt{3})^2 = \phi(3) = 3$ and $\phi(\sqrt{5})^2 = \phi(5) = 5$

i.e. the roots of $x^2 - 3$ must be sent to other roots of $x^2 - 3$ and similarly the roots of $x^2 - 5$ must be sent to other roots of $x^2 - 5$.

As such $\phi(\sqrt{3}) = \pm\sqrt{3}$ and $\phi(\sqrt{5}) = \pm\sqrt{5}$, and we note that we have two choices for $\phi(\sqrt{3})$ and two choices for $\phi(\sqrt{5})$.

We note also, that $\phi(\sqrt{15}) = \phi(\sqrt{3}\sqrt{5}) = \phi(\sqrt{3})\phi(\sqrt{5})$ which means $\phi(\sqrt{15})$ is determined by $\phi(\sqrt{3})$ and $\phi(\sqrt{5})$.

So, for a typical element $a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \in E$ (where $a, b, c, d \in \mathbb{Q}$), we have

$$\phi(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) = a + b\phi(\sqrt{3}) + c\phi(\sqrt{5}) + d\phi(\sqrt{15})$$

where, again $\phi(\sqrt{15}) = \phi(\sqrt{3})\phi(\sqrt{5})$.

So let's determine the elements of $G = Gal(E/\mathbb{Q})$.

Define $\sigma_3 : E \to E$ by

$$\sigma_3(\sqrt{3}) = -\sqrt{3}$$
$$\sigma_3(\sqrt{5}) = \sqrt{5}$$

i.e. σ_3 fixes $\sqrt{5}$, which means also that $\sigma_3(\sqrt{15}) = (-\sqrt{3})\sqrt{5} = -\sqrt{15}$.

Similarly, define $\sigma_5 : E \to E$ by

$$\sigma_5(\sqrt{5}) = -\sqrt{5}$$
$$\sigma_5(\sqrt{3}) = \sqrt{3}$$

i.e. σ_5 fixes $\sqrt{3}$ and also that $\sigma_5(\sqrt{15}) = -\sqrt{15}$.

We have the identity automorphism (always) which fixes every element of E, and as σ_3 and σ_5 are automorphisms, so is their composition $\sigma_3 \circ \sigma_5$ where

$$\begin{aligned}
\sigma_3(\sigma_5(\sqrt{3})) &= \sigma_3(\sqrt{3}) = -\sqrt{3} \\
\sigma_3(\sigma_5(\sqrt{5})) &= \sigma_3(-\sqrt{5}) = -\sigma_3(\sqrt{5}) = -\sqrt{5} \\
\sigma_3(\sigma_5(\sqrt{15})) &= -(-\sqrt{15}) = \sqrt{15}
\end{aligned}$$

So the composition does something a bit different to the particular 'radical' in that it does not send it to is negative.

Let's see how these automorphisms act globally.

We can show that these are distinct automorphisms:

$$
\begin{aligned}
I(a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}) &= \boxed{a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}} \\
\sigma_3(a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}) &= a+b\sigma_3(\sqrt{3})+c\sigma_3(\sqrt{5})+d\sigma_3(\sqrt{15}) \\
&= \boxed{a-b\sqrt{3}+c\sqrt{5}-d\sqrt{15}} \\
\sigma_5(a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}) &= a+b\sigma_5(\sqrt{3})+c\sigma_5(\sqrt{5})+d\sigma_5(\sqrt{15}) \\
&= \boxed{a+b\sqrt{3}-c\sqrt{5}-d\sqrt{15}} \\
(\sigma_3\circ\sigma_5)(a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}) &= \boxed{a-b\sqrt{3}-c\sqrt{5}+d\sqrt{15}}
\end{aligned}
$$

As to whether these are *all* the elements of the Galois group, we again point out that any automorphism is determined by what happens to $\sqrt{3}$ and $\sqrt{5}$, so the Galois group at least *contains* $\{I, \sigma_3, \sigma_5, \sigma_3 \circ \sigma_5\}$.

Again, since the Galois group is a group, it must be closed, so if it contains σ_3 and σ_5, it contains $\sigma_3 \circ \sigma_5$ which, as we've just seen, is a distinct automorphism itself.

What about the composition $\sigma_5 \circ \sigma_3$?

By direct computation we have

$$\begin{aligned}(\sigma_5 \circ \sigma_3)(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= \sigma_5(\sigma_3(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15})) \\ &= \sigma_5(a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15})) \\ &= a - b\sqrt{3} - c\sqrt{5} + d\sqrt{15}\end{aligned}$$

and so we see that $\sigma_5 \circ \sigma_3 = \sigma_3 \circ \sigma_5$.

And, of course, $\sigma_3 \circ I = I \circ \sigma_3 = \sigma_3$ and $\sigma_5 \circ I = I \circ \sigma_5 = \sigma_5$, and obviously $I \circ I = I$.

Also, since $\sigma_3(\sigma_3(\sqrt{3})) = \sigma_3(-\sqrt{3}) = -\sigma_3(\sqrt{3}) = -(-\sqrt{3}) = \sqrt{3}$ we have that

$$\sigma_3 \circ \sigma_3 = I \text{ and } \sigma_5 \circ \sigma_5 = I$$

which means $\sigma_3^2 = I$ and $\sigma_5^2 = I$, and since σ_3 and σ_5 commute, we have that $(\sigma_3 \circ \sigma_5)^2 = I$ as well.

So we have that $G = Gal(E/\mathbb{Q}) = \{I, \sigma_3, \sigma_5, \sigma_3 \circ \sigma_5\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

That is, it is isomorphic to the so-called Klein 4-group V.

Now, let's consider the fixed fields of the different subgroups of G.

Since $G = \{I, \sigma_3, \sigma_5, \sigma_3 \circ \sigma_5\}$, where all non-identity elements have order 2, the (proper) subgroups are

$$H_3 = \{I, \sigma_3\}$$
$$H_5 = \{I, \sigma_5\}$$
$$H_{15} = \{I, \sigma_5 \circ \sigma_3\}$$

and if $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ then E_{H_3}, for example, is the subfield fixed by the identity and σ_3.

Now I fixes all of E and if

$$x = a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}$$

then $\sigma_3(x) = x$ implies $b = 0$ *and* $d = 0$. Why?

Well $\sigma_3(\sqrt{15}) = -\sqrt{15}$ since $\sqrt{15} = \sqrt{3}\sqrt{5}$.

So $E_{H_3} = \{a + c\sqrt{5} \mid a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{5})$.

Similarly, for

$$H_5 = \{I, \sigma_5\}$$

we note that since

$$\sigma_5(\sqrt{5}) = -\sqrt{5}$$
$$\sigma_5(\sqrt{3}) = \sqrt{3}$$
$$\sigma_5(\sqrt{15}) = -\sqrt{15}$$

then we find that for

$$x = a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}$$

one has $\sigma_5(x) = x$ only if $c = 0$ and $d = 0$, so

$$E_{H_5} = \{a + b\sqrt{3}\} = \mathbb{Q}(\sqrt{3})$$

and similarly, for $H_{15} = \{I, \sigma_5 \circ \sigma_3\}$ one can show that

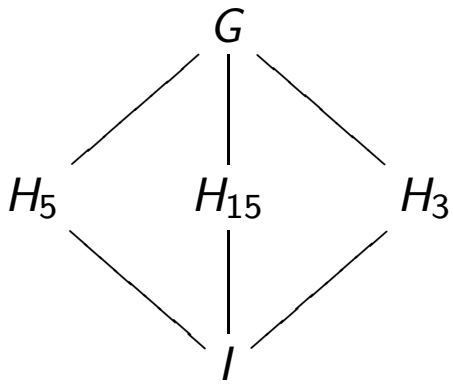
$$E_{H_{15}} = \{a + d\sqrt{15}\} = \mathbb{Q}(\sqrt{15})$$

For completeness sake, we note two relatively obvious facts:

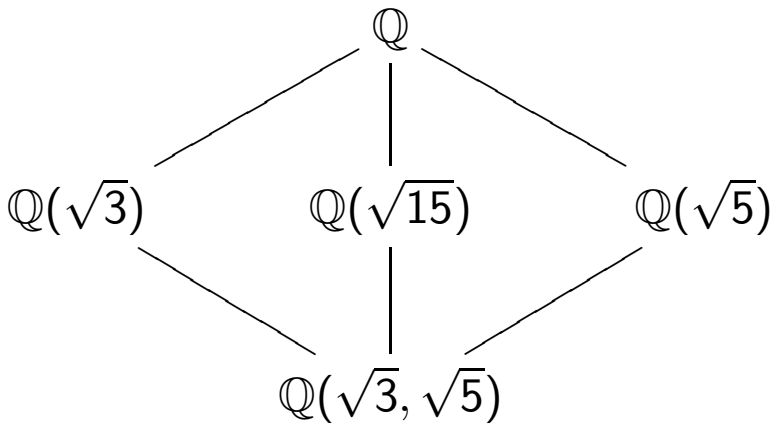
$$E_I = E \text{ and } E_G = \mathbb{Q}$$

and what we end up with is a correspondence between subgroups of G and subfields of E (that contain the base field $\mathbb{Q}$) which we can diagram.

We start with the 'lattice of subgroups of G'



and we can take each subgroup $H \leq G$, and put in its place the corresponding fixed field E_H



which looks a bit odd since the 'bigger' or 'top level' field $\mathbb{Q}(\sqrt{3},\sqrt{5})$ is on the bottom, while the base field $\mathbb{Q}$ is *on top*.

This 'inversion' is actually not that surprising.

If, for example, $H_1 \leq H_2 \leq G$ where $G = Gal(E/F)$ then for $x \in E_{H_2}$ we have that $\sigma(x) = x$ for all $\sigma \in H_2$, which includes all the elements of H_1 and so $x \in E_{H_1}$ automatically.

That is,

$$H_1 \leq H_2 \leftrightarrow E_{H_2} \subseteq E_{H_1}$$

which, again, makes sense since the *smaller* the subgroup of G the *more* it will fix.

(i.e. An element fixed by 2 automorphisms may not necessarily be fixed by 3 automorphisms.)

If for a subgroup $H \leq G$ (where $G = Gal(E/F)$) we define $Fix(H) = E_H$ then this gives a correspondence

$$\{subgroups\ of\ G\} \overset{Fix}{\to} \{subfields\ of\ E\ that\ contain\ F\}$$

which makes one wonder if there is a correspondence *in the other direction*?

(And also, is the map *Fix* one-to-one, or onto?)

We will explore this using the example we just worked out, next time.