MA542 Lecture

Timothy Kohl

Boston University

April 4, 2025

Subgroups and Fixed Fields

D_3 has a much richer subgroup structure than say $\mathbb{Z}_2 \times \mathbb{Z}_2$ and there are some definite contrasts between that case and this one.

Consider first $H = \langle x \rangle = \{1, x, x^2\}$ and $H' = \langle t \rangle = \{1, t\}$.

As $x(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$ but $x(\zeta) = \zeta$ and similarly $t(\sqrt[3]{2}) = \sqrt[3]{2}$ while $t(\zeta) = \zeta^2$ one can deduce that

$$E_H = \mathbb{Q}(\zeta) \text{ and } E_{H'} = \mathbb{Q}(\sqrt[3]{2}).$$

We also note that for $E=\mathbb{Q}(\sqrt[3]{2},\zeta)$ and $E_H=\mathbb{Q}(\zeta)$ that $\{1,\sqrt[3]{2},\sqrt[3]{2}^2\}$ is a $\mathbb{Q}(\zeta)$-basis for E/E_H since

$$a+b\sqrt[3]{2}+c\sqrt[3]{2}^2+d\zeta+e\zeta\sqrt[3]{2}+f\zeta\sqrt[3]{2}^2=$$
$$(a+d\zeta)+(b+e\zeta)\sqrt[3]{2}+(c+f\zeta)\sqrt[3]{2}^2$$

since

$$\mathbb{Q}(\sqrt[3]{2},\zeta)=\mathbb{Q}(\zeta,\sqrt[3]{2})=\mathbb{Q}(\zeta)(\sqrt[3]{2})=\{x+y\sqrt[3]{2}+z\sqrt[3]{2}^2\mid x,y,z\in\mathbb{Q}(\zeta)\}$$

As such

$$Gal(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q}(\zeta)) \leq Gal(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q})$$

and any element in $Gal(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q}(\zeta))$ is an automorphism that fixes ζ and therefore the set of all these is

$$\{I, x, x^2\}$$

which is exactly H.

Thus $Gal(E/E_H) = H$ that is, the Galois group of E over the fixed field of $H \leq Gal(E/F)$ is H itself.

Moreover $[E : E_H] = |H|$.

Similarly for $H' = \{1, t\}$ we have $E_{H'} = \mathbb{Q}(\sqrt[3]{2})$ if we look at $E/E_{H'}$ we have $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}(\sqrt[3]{2})$ which has a $\mathbb{Q}(\sqrt[3]{2})$ basis $\{1, \zeta\}$ since

$$a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\zeta + e\zeta\sqrt[3]{2} + f\zeta\sqrt[3]{2}^2 =$$
$$(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) + (d + e\sqrt[3]{2} + f\sqrt[3]{2}^2)\zeta$$

since $\mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(\sqrt[3]{2})(\zeta) = \{p + q\zeta \mid p, q \in \mathbb{Q}(\sqrt[3]{2})\}$.

As such

$$Gal(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q}(\sqrt[3]{2})) \leq Gal(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q})$$

and any element in $Gal(\mathbb{Q}(\sqrt[3]{2},\zeta)/\mathbb{Q}(\sqrt[3]{2}))$ is an automorphism that fixes $\sqrt[3]{2}$ and therefore the set of all these is

$$\{I, t\}$$

which is exactly H'.

Thus $Gal(E/E_{H'}) = H'$ that is, the Galois group of E over the fixed field of $H' \leq Gal(E/F)$ is H' itself.

Moreover $[E : E_{H'}] = |H'|$.

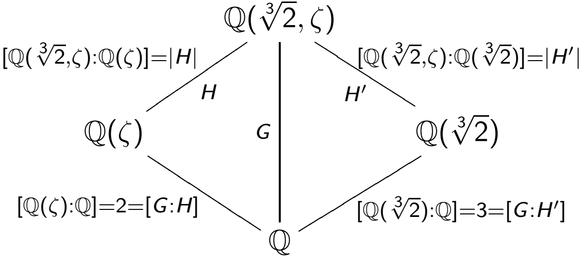
Note also that

$$[G:H]=\frac{|G|}{|H|}=2=[E_H:F]=[\mathbb{Q}(\zeta):\mathbb{Q}]$$

and

$$[G:H']=\frac{|G|}{|H'|}=3=[E_{H'}:F]=[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$$

which is not an accident, but actually an essential feature we wish to highlight.



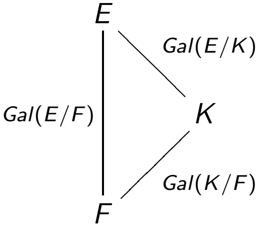
So what about groups associated to the extensions $\mathbb{Q}(\zeta)/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ given the information about the subgroup indices and degrees of these extensions in the diagram?

In general, for E a splitting field over F, with Galois group $Gal(E/F)$ we have, for an intermediate field $F \subseteq K \subseteq E$ that $Gal(E/K) \leq Gal(E/F)$.

But what about $Gal(K/F)$?

More importantly, is it even defined?

And if it is, is it a subgroup of $Gal(E/F)$? (No it isn't!)



This question has some bearing on the fixed fields of different subgroups of $Gal(E/F)$.

Let's consider other subgroups.

$H'' = \langle tx \rangle = \{I, tx\}$ which implies $E_{H''} = \mathbb{Q}(\zeta\sqrt[3]{2})$

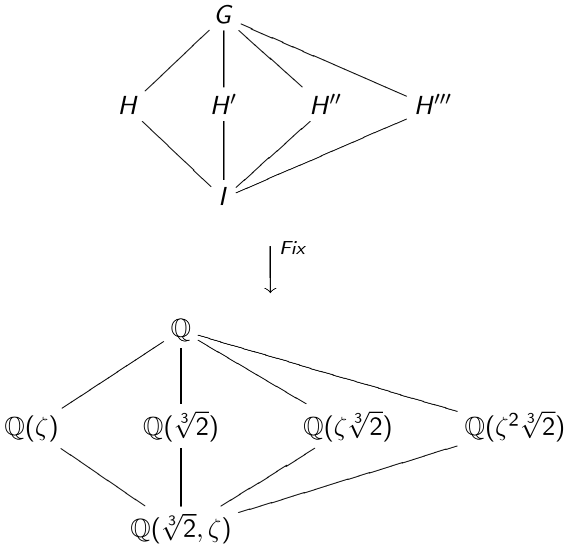
$H''' = \langle tx^2 \rangle = \{I, tx^2\}$ which implies $E_{H'''} = \mathbb{Q}(\zeta^2\sqrt[3]{2})$

and we observe that here too:

$$[E : E_{H''}] = |H''|$$
$$[E : E_{H'''}] = |H'''|$$
$$[G : H''] = 3 = [E_{H''} : F] = [\mathbb{Q}(\zeta\sqrt[3]{2}) : \mathbb{Q}]$$
$$[G : H'''] = 3 = [E_{H'''} : F] = [\mathbb{Q}(\zeta^2\sqrt[3]{2}) : \mathbb{Q}]$$

and, of course I (the trivial subgroup) where $E_{\{I\}} = \mathbb{Q}(\sqrt[3]{2}, \zeta) = E$ so that $[G : \{I\}] = 6 = [E : F]$.

We start with the 'lattice of subgroups of G' and by taking '*Fix*' of each subgroup yield the (inverted) lattice of subfields of $\mathbb{Q}(\sqrt[3]{2},\zeta)$.



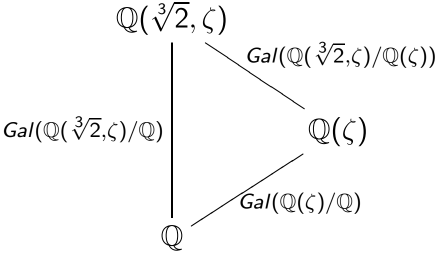
Further Observations:

For $H = \{1, x, x^2\}$ with $E_H = \mathbb{Q}(\zeta)$ we have $Gal(E/E_H)$ as mentioned earlier.

If we consider $Gal(E_H/F) = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ we observe that since ζ is a root of $x^2 + x + 1$ (with the other being ζ^2) then $\mathbb{Q}(\zeta)$ is the splitting field for $x^2 + x + 1 \in \mathbb{Q}[x]$.

Moreover, $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{Id, T\}$ where Id is the identity and $T(\zeta) = \zeta^2$ since the root ζ must get sent to another root (of $x^2 + x + 1$) by an automorphism, and these are all the $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\zeta)$.

And $|Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.



So how do the groups here relate to each other?

We have that $Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}(\zeta)) \leq Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q})$ but what about $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$?

In contrast, for

$$H' = \{1, t\}$$

with $E_{H'} = \mathbb{Q}(\sqrt[3]{2})$ if we look to compute $Gal(E_{H'}/F) = Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ we know, from earlier, that

$$Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{I\}$$

which is because $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of $x^3 - 2 = irr(\sqrt[3]{2}, \mathbb{Q})$, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] > |Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})|$.

So what is the distinction between H and H', which makes E_H a splitting field over $\mathbb{Q}$ while $E_{H'}$ is not a splitting field?

The key difference is that

$$H = \{I, x, x^2\} \triangleleft G = Gal(E/F)$$

but $H' = \{I, t\} \not\triangleleft G$.

In particular, consider $G/H = \{I \cdot H, t \cdot H\}$ and observe that in the coset

$$I \cdot H = \{I, x, x^2\}$$

every element acts trivially on ζ (and therefore trivially as a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta)$) and in the coset

$$t \cdot H = \{t, tx, tx^2\}$$

we have $t(\zeta) = \zeta^2$ and $tx(\zeta) = t(\zeta) = \zeta^2$ and $tx^2(\zeta) = t(\zeta) = \zeta^2$.

So every coset element acts as the automorphism $T \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ we saw earlier, which is the non-trivial element of $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$.

So we can assert that

$$G/H = \{I \cdot H, t \cdot H\} \cong \{Id, T\} = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$$

via the homomorphism $I \cdot H \mapsto Id$ and $t \cdot H \mapsto T$ which is obviously an isomorphism.

$$H \triangleleft G \rightarrow Gal(E_H/F) \cong Gal(E/F)/Gal(E/E_H)$$

which is a basic fact we shall see is fundamental to 'Galois Theory' as we shall develop in generality later on.