MA542 Lecture

Timothy Kohl

Boston University

April 2, 2025

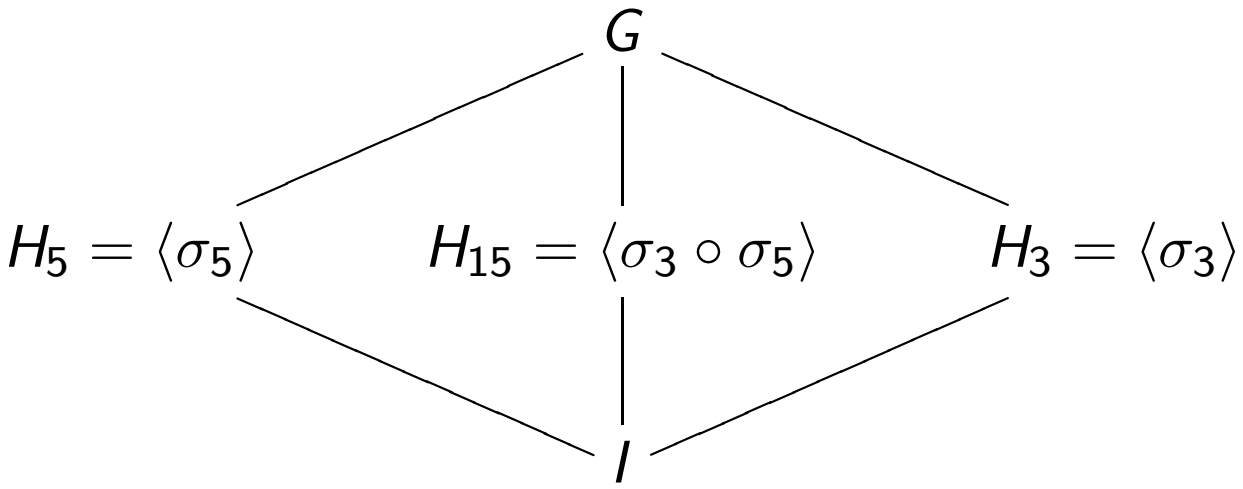
Subgroups and Subfields

Last time, we saw the correspondence

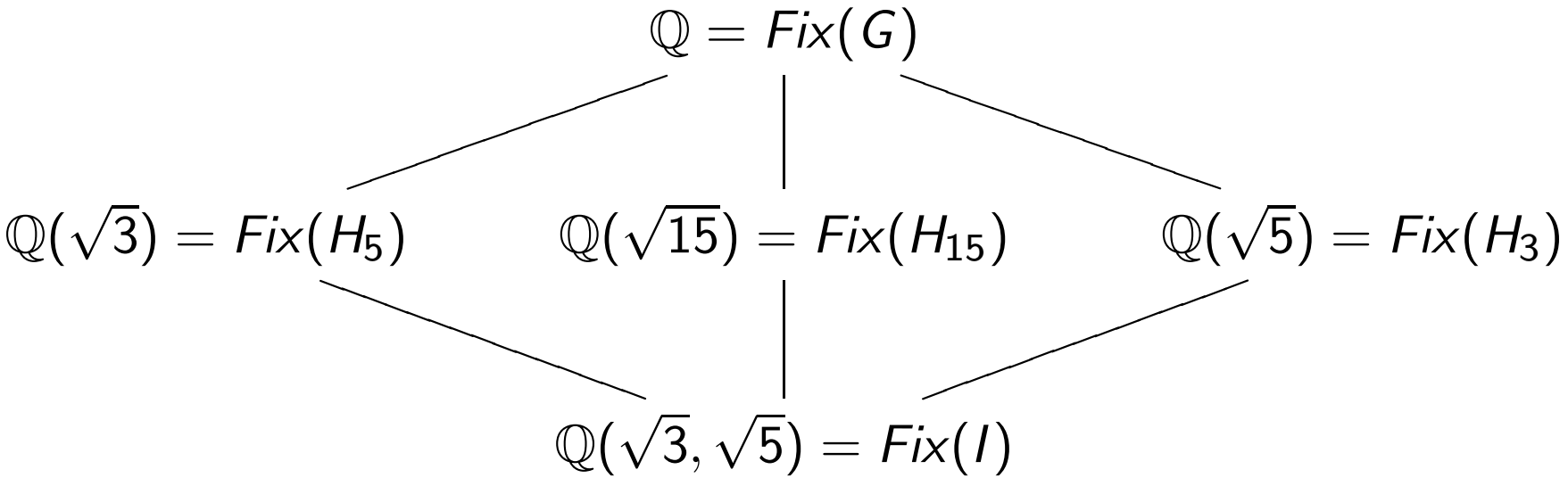
$$\{\textit{subgroups of } G\} \overset{Fix}{\to} \{\textit{subfields of } E \textit{ that contain } F\}$$

and asked whether there is a correspondence *in the other direction* and if the map *Fix* is injective/surjective/bijective.

Let's revisit the $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ example to explore these questions.



$\downarrow Fix$



For the intermediate field $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$ we can consider $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{3}))$.

A typical element is of the form

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

and for $\sigma \in Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$ it must fix a, b, c, d.

But if $\sigma \in Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{3}))$ then it must fix $\sqrt{3}$ obviously, and since it's an automorphism of $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5}))$ it must be one of the elements $\{I, \sigma_3, \sigma_5, \sigma_5 \circ \sigma_3\}$.

And we know that $\sigma_3(\sqrt{3}) \neq \sqrt{3}$, and $(\sigma_5 \circ \sigma_3)(\sqrt{3}) \neq \sqrt{3}$ which leaves I and σ_5 which both *do* fix $\sqrt{3}$.

So we can equate $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{3})) = \langle \sigma_5 \rangle = H_5$.

And in general we can compute $Gal(\mathbb{Q}(\sqrt{5},\sqrt{3})/K)$ for any field K where $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\sqrt{5},\sqrt{3})$, and each is naturally a subgroup of $Gal(\mathbb{Q}(\sqrt{5},\sqrt{3})/\mathbb{Q})$ which we can identify.

- $Gal(\mathbb{Q}(\sqrt{5},\sqrt{3})/\mathbb{Q}(\sqrt{3})) = \{I, \sigma_5\} = H_5$
- $Gal(\mathbb{Q}(\sqrt{5},\sqrt{3})/\mathbb{Q}(\sqrt{5})) = \{I, \sigma_3\} = H_3$
- $Gal(\mathbb{Q}(\sqrt{5},\sqrt{3})/\mathbb{Q}(\sqrt{15})) = \{I, \sigma_3 \circ \sigma_5\} = H_{15}$
- $Gal(\mathbb{Q}(\sqrt{5},\sqrt{3})/\mathbb{Q}(\sqrt{5},\sqrt{3})) = \{I\}$

So now we have a correspondence going in the other direction:

$$\{\textit{subfields of } E \textit{ that contain } F\} \to \{\textit{subgroups of } G\}$$
$$K \mapsto Gal(E/K)$$

and so the natural question here too is whether this correspondence is one-to-one.

(i.e. Can $Gal(E/K_1) = Gal(E/K_2)$ for intermediate fields $K_1 \neq K_2$.)

The possibility that $H \mapsto Fix(H) = E_H$ and $K \mapsto Gal(E/K)$ being one-to-one is strongly suggested by the following 'bonus' observation we can make.

Specifically, for $E = \mathbb{Q}(\sqrt{5}, \sqrt{3})$, and for each $H \leq G = Gal(E/\mathbb{Q})$ we have

$$Gal(E/E_H) = H$$

which can be verified directly since, for example $H_3 = \{I, \sigma_3\}$ and $E_{H_3} = \mathbb{Q}(\sqrt{5})$ and $Gal(E/\mathbb{Q}(\sqrt{5})$ is exactly $H_3 = \{I, \sigma_3\}$.

This looks 'circular' but that's exactly the point, namely that $H \mapsto E_H \mapsto Gal(E/E_H) = H$!

Indeed, the 'reverse' composition works too, since for $K = \mathbb{Q}(\sqrt{5})$ we have $H = Gal(E/K) = \{I, \sigma_3\}$, but $E_{H_3} = K$, i.e. $E_{Gal(E/K)} = K$.

More on this soon...

A non-abelian Galois Group

We previously computed $Gal(\sqrt{5}, \sqrt{3})/\mathbb{Q})$ and found that it was isomorphic to the abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

In contrast we consider a Galois group which we shall see is non-abelian.

The field extension we are interested in is $E = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ which is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$.

The group structure of $G = Gal(E/\mathbb{Q})$ is quite different, which will be apparent especially when we look at fixed fields later one.

For $E = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ and $F = \mathbb{Q}$ an automorphism $\phi \in Gal(E/F)$ is again characterized by the fact that 'roots go to roots'.

We need to work with the basis of E as an F-vector space (again $F = \mathbb{Q}$) namely

$$\mathcal{B} = \{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta, \zeta\sqrt[3]{2}, \zeta\sqrt[3]{2}^2\}$$

and $[E : F] = 6$.

Now, since $\sqrt[3]{2} \in \mathcal{B}$ which is a root of $x^3 - 2$ then $\phi(\sqrt[3]{2})$ must also be a root of $x^3 - 2$ in E, and since E is the splitting field of $x^3 - 2$, it actually *contains* the other roots of $x^3 - 2$.

So in particular $\phi(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$.

Moreover, we note that $\phi(\sqrt[3]{2})$ determines $\phi(\sqrt[3]{2}^2)$ by the homomorphism property in that $\phi(\sqrt[3]{2}^2) = \phi(\sqrt[3]{2})^2$, and of course, $\phi(1) = 1$ since $1 \in F$.

The other basis elements to account for are $\phi(\zeta)$, $\phi(\zeta\sqrt[3]{2})$, and $\phi(\zeta\sqrt[3]{2}^2)$.

Since $\phi(\zeta\sqrt[3]{2}) = \phi(\zeta)\phi(\sqrt[3]{2})$ and $\phi(\zeta\sqrt[3]{2}^2) = \phi(\zeta)\phi(\sqrt[3]{2}^2)$ then we need to determine $\phi(\zeta)$.

Since ζ is a root of $\Phi(x) = x^2 + x + 1$ then $\phi(\zeta)$ is also a root of $x^2 + x + 1$, so $\phi(\zeta) = \{\zeta, \zeta^2\}$.

So qualitatively, one has 3 choices for $\phi(\sqrt[3]{2})$ and 2 choices for $\phi(\zeta)$, and this determines ϕ of every basis element in

$$\mathcal{B} = \{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta, \zeta\sqrt[3]{2}, \zeta\sqrt[3]{2}^2\}$$

so $2 \cdot 3$ automorphisms overall, which we can tabulate.

- $\phi(\sqrt[3]{2}) = \sqrt[3]{2} \quad \phi(\zeta) = \zeta$ (i.e. the identity)
- $\phi(\sqrt[3]{2}) = \zeta\sqrt[3]{2} \quad \phi(\zeta) = \zeta$
- $\phi(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2} \quad \phi(\zeta) = \zeta$
- $\phi(\sqrt[3]{2}) = \sqrt[3]{2} \quad \phi(\zeta) = \zeta^2$
- $\phi(\sqrt[3]{2}) = \zeta\sqrt[3]{2} \quad \phi(\zeta) = \zeta^2$
- $\phi(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2} \quad \phi(\zeta) = \zeta^2$

We will label some of these in a way which look a bit arbitrary, but will ultimately make it easier to understand the group structure of $G = Gal(E/F)$.

Let's define x to be the automorphism so that $x(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$ and $x(\zeta) = \zeta$.

Observe that

$$(x \circ x)(\sqrt[3]{2}) = x(\zeta\sqrt[3]{2}) = x(\zeta)x(\sqrt[3]{2}) = \zeta(\zeta\sqrt[3]{2} = \zeta^2\sqrt[3]{2})$$

and $(x \circ x)(\zeta) = x(\zeta) = \zeta$.

i.e. $x^2(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$ and $x^2(\zeta) = \zeta$.

If we now consider $x^3 = (x^2 \circ x)$ then

$$x^3(\zeta) = \zeta$$

and

$$x^3(\sqrt[3]{2}) = x^2(x(\sqrt[3]{2})) = x^2(\zeta\sqrt[3]{2}) = x^2(\zeta)x^2(\sqrt[3]{2}) = \zeta\zeta^2\sqrt[3]{2} = \sqrt[3]{2}$$

which means $x^3 = I$.

Another automorphism we focus on we will call 't' which we define by $t(\zeta) = \zeta^2$ and $t(\sqrt[3]{2}) = \sqrt[3]{2}$.

We note that $t^2 = (t \circ t)$ acts as follows

$$(t \circ t)(\zeta) = t(t(\zeta)) = t(\zeta^2) = t(\zeta)^2 = \zeta^4 = \zeta$$

and similarly

$$(t \circ t)(\sqrt[3]{2}) = t(t(\sqrt[3]{2})) = t(\sqrt[3]{2}) = \sqrt[3]{2}$$

so $t^2 = I$.

We can therefore present the list earlier, in terms of these elements I, x, x^2, t as well as $tx = (t \circ x)$ and $tx^2 = (t \circ x^2)$

	$I(\sqrt[3]{2}) = \sqrt[3]{2}$	$I(\zeta) = \zeta$
	$x(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$	$x(\zeta) = \zeta$
	$x^2(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$	$x^2(\zeta) = \zeta$
	$t(\sqrt[3]{2}) = \sqrt[3]{2}$	$t(\zeta) = \zeta^2$
	$tx(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$	$tx(\zeta) = \zeta^2$
	$tx^2(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$	$tx^2(\zeta) = \zeta^2$

so

$$G = \{I, x, x^2, t, tx, tx^2\}$$

(as a set) but what is its group structure?

We already saw that $|x| = 3$ and $|t| = 2$.

We note also that

$$xt(\sqrt[3]{2}) = x(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$$
$$xt(\zeta) = x(\zeta^2) = \zeta^2$$

which is exactly the same as tx^2.

So $xt = tx^{-1}$ which, since $|t| = 2$ (and therefore $t = t^{-1}$) means that $txt^{-1} = x^{-1}$ and thus $tx^2t^{-1} = x^{-2}$, that is $x^2t = tx$.

In particular this demonstrates that G is indeed closed (as it must be) and that it is clearly a non-abelian group, and since it has six elements, implies that it is isomorphic to D_3, which is, of course, isomorphic to the symmetric group S_3.

Let's consider the group table for G.

$\circ$	I	x	x^2	t	tx	tx^2
I	I	x	x^2	t	tx	tx^2
x	x	x^2	I	tx^2	t	tx
x^2	x^2	I	x	tx	tx^2	t
t	t	tx	tx^2	I	x	x^2
tx	tx	tx^2	t	x^2	I	x
tx^2	tx^2	t	tx	x	x	I

which is, of course, the group table for D_3 although when presented geometrically, 'x' corresponds to a 120° rotation, 'x^2' a 240° rotation etc.

Note also that $|t| = |tx| = |tx^2| = 2$ and $|x| = |x^2| = 3$ and $|I| = 1$ of course.

Appendix: Group Presentations

Let's consider the 'x' and 't' notation we used.

In particular we have a so-called 'finite presentation' of G, in terms of 'generators' and 'relations'.

For perspective, consider the group defined as follows:

$$\begin{aligned}\langle x \rangle &= \{x^i \mid i \in \mathbb{Z}\} \\ &= \{\dots, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, \dots\}\end{aligned}$$

where $x^i * x^j = x^{i+j}$ and so the identity is $1 = x^0$.

We see that $\langle x \rangle \cong \mathbb{Z}$ in that it's an infinite cyclic group.

What if now we impose a 'relation' that x needs to satisfy? (i.e. an equation)

$$\langle x \mid x^3 = 1 \rangle$$

which means that the elements

$$\{\dots, x^{-4}, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, x^4, \dots\}$$

are not all distinct anymore since $x^3 = 1$ implies $x^4 = x$, $x^5 = x^2$, $x^6 = 1$ etc, and similarly $x^{-1} = x^2$, $x^{-2} = x$ etc.

Indeed, $\langle x \mid x^3 = 1 \rangle$ is finite, and consists of $\{1, x, x^2\}$ where we still say $x^i * x^j = x^{i+j}$ but where we superimpose the relation $x^3 = 1$ which implies that

$$\langle x \mid x^3 = 1 \rangle \cong \mathbb{Z}_3$$

More generally, a finite presentation of a group is one given

$$\langle x_1, x_2, \ldots, x_n \mid \text{equations in the } x_i \rangle$$

namely the set of all possible products of powers of the 'generators' $x_1, \ldots, x_n$ with the relations imposed on them.

For example,

$$\langle x, y \mid xy = yx \rangle$$

consists of all powers of x and y we can write down, where if one has $x^i * x^j$ one simply writes it as x^{i+j} etc.

The one relation here, $xy = yx$ basically says x and y commute with each other so that, for example

$$x^3y^2x^5y^7 = x^3x^5y^2y^7 = x^8y^9$$

which means that, as a set

$$\langle x, y \mid xy = yx \rangle = \{x^i y^j \mid i, j \in \mathbb{Z}\}$$

where the multiplication is based on adding exponents, where again we assume x and y commute, and therefore any *powers* of x and y commute.

As such we find that

$$\langle x, y \mid xy = yx \rangle \cong \mathbb{Z} \times \mathbb{Z}$$

where $x^i y^j \mapsto (i, j)$.

Note, the condition $xy = yx$ can be written as $xyx^{-1}y^{-1} = 1$, namely $[x, y] = 1$ where $[x, y]$ is the so-called 'commutator'.

A natural question to ask is, what if we *don't* impose the $xy = yx$ relation?

If we have $G = \langle x, y \rangle$ then literally we have the collection of all *words* we can write involving powers of x and y where the only rule that holds is that two powers of the same symbol next to each other are combined by adding their exponents.

i.e. $(x^3y^5x^{-3})(x^5y^3) = x^3y^5x^2y^3$

This is an example of what's known as a 'free group' and, with two or more generators, it's a *vastly* more complicated object, and not just because it's non-abelian or that it's infinite.

Note, however, that by imposing relations, we frequently end up with finite groups, if not necessariy abelian, which is where our Galois group example comes in.

Recall that our Galois group for $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}$ is

$$G = \{1, x, x^2, t, tx, tx^2\}$$

where $|x| = 3$ and $|t| = 1$ and where, for example $xt = tx^2$ and $x^2t = tx$.

This is equivalent to the presentation

$$\langle x, t \mid x^3 = 1, t^2 = 1, xt = tx^{-1} \rangle$$

which gives us enough information to show that this groups has six elements, is non-abelian (evident from the relation $xt = tx^{-1}$) and we can show therefore that it is isomorphic to D_3.

What's kind of nice about this, is that it generalizes quite easily.

For $n \geq 3$ one can show that

$$\langle x, t \mid x^n = 1, t^2 = 1, xt = tx^{-1} \rangle$$

consists of the elements $\{1, x, \ldots, x^{n-1}, t, tx, \ldots, tx^{n-1}\}$ and is isomorphic to D_n, and all one does is change the 'n' to change the flavor of dihedral group one gets!

One thing kind of interesting that comes from group presentations is determining whether the resulting group is infinite, finite, or even (non-obviously) trivial.

For example,

$$\langle x, y \mid x^3 = 1, y^2 = 1, y^3 = x^2 \rangle$$

is actually the trivial group (in disguise!).

Why? Well, since $y^3 = x^2$ and $y^2 = 1$ this means $y = x^2$, and so $y^2 = (x^2)^2 = x^4 = x$ since $x^3 = 1$.

But $y^2 = 1$ so $x = 1$, and so $y = x^2 = 1^2 = 1$ and so $y = 1$, thus all powers of x and y 'collapse' down to the identity!