9. EXAMPLES OF GALOIS GROUPS

§9.1. Review of the Fundamental Theorem of Galois Theory

Many books on Galois Theory just present one or two simple examples of constructing Galois groups, such as the classical case of $G(\mathbb{Q}[x^3 = 2]/\mathbb{Q})$, and then move on quickly to the situation where a polynomial is not soluble by radicals, and where you have to calculate the Galois groups indirectly. From the point of view of understanding the fundamental ideas behind Galois Theory in a general sort of way, this is probably quite sufficient.

That's why they often only present Eisenstein's criterion for proving that a polynomial is prime. But I take the view that it is instructive to struggle with lots of examples of Galois groups. One would like to think that one could take any integer polynomial and find its Galois group and its fixed fields. But there's no straightforward algorithm for doing this, even when the polynomial is soluble by radicals and we have its zeros. It often requires a lot of ingenuity.

My philosophy is that is good to require students to wrestle with a number of non-trivial examples. This is why, when I teach a course on Galois Theory, one of the assessment tasks is to be given an integer polynomial (a

different one for each student) and the student has to find its Galois group and to use it to illustrate as much as possible of the theory. A list of such polynomials can be found in one of the appendices.

One of the difficulties is to determine whether or not an example collapses. For example, is $6^{1/3} \in \mathbb{Q}[\sqrt[3]{3+\sqrt{3}}]$? If so then $G(\mathbb{Q}[6^{1/3}, \sqrt[3]{3+\sqrt{3}}]/\mathbb{Q})$, will have order 6. If not it has order 18. It looks quite plausible that $6^{1/3} \notin \mathbb{Q}[\sqrt[3]{3+\sqrt{3}}]$, but it's hard to prove this.

Possibly I've gone overboard. Some of the later examples require a fair amount of ingenuity. You should decide when you have had enough and skip to the next chapter. But if you're given a project, with your own personal polynomial, you may find some inspiration here.

So, in this chapter we are going to compute the Galois groups of a number of polynomial extensions, where the polynomial is soluble by radicals. The first step will be to find the zeros, then the automorphisms. In the next chapter we'll address the case of polynomials that are not soluble by radicals. In those cases we must determine the Galois group indirectly.

In the course of developing these examples we'll be demonstrating some of the fundamental ideas of Galois Theory. These include some remarkable facts contained within the Fundamental Theorem of Galois Theory.

If K = F[f(x) = 0] is a polynomial extension of a number field F then we say that K is the **splitting field** of f(x) over F. (If we don't include the phrase 'over F' then it's assumed that we mean 'over $\mathbb{Q}$'.

We can consider the subfields H that lie between F and K as well as the Galois group G = G(K/F) and its all its subgroups.

The fundamental theorem states that there's a 1-1 correspondence between the fields L with $F \leq L \leq K$ and the subgroups H with $1 \leq H \leq G$. This means that there are exactly as many subfields as there are subgroups.

The **fixed field** of a subgroup H is the set of all elements of K that are fixed by every element of the subgroup H and the **fixing** subgroup of a field L is the set of all automorphisms of K that fix every element of L.

We shall denote the fixed field of H by H^* and the fixing subgroup of L by $L^\#$. It's easy to show that H^* is indeed a subfield and $L^\#$ is a subgroup. The 1-1 correspondence pairs subgroups with their fixed fields and subfields with their fixing subgroup, so that if $H^* = L$ then $L^\# = H$ and L and H correspond.

This 1-1 correspondence is order reversing, meaning that if $L_1 \leq L_2$ then $L_2^\# \leq L_1^\#$ (the more you have to fix, the fewer automorphisms will do that). And if $H_1 \leq H_2$ then $H_2^* \leq H_1^*$. This means that if you draw the traditional type of diagram of the subgroups of G, where you indicate that one subgroup is inside another by

placing the larger subgroup higher up and drawing a line between them, then turning this diagram upside down you get a picture of the subfields.

At the bottom of the subfields is F and it corresponds to the entire Galois group G sitting above all the subgroups. At the top of the subfields is K and this corresponds to the trivial subgroup 1 at the bottom of the subgroups.

The degree of an extension corresponds to the index of the corresponding subgroups.

That is, if $L_1 \le L_2 \le K$ then $|L_2:L_1| = |L_1^{\#}:L_2^{\#}|$.

Equivalently, if $H_1 \le H_2 \le G$ then $|H_2:H_1| = |H_1^{*}:H_2^{*}|$.

Finally, polynomial extensions correspond to normal subgroups. If L_2 is a polynomial extension of L_1 then $L_2^{\#}$ is a normal subgroup of $L_1^{\#}$ and vice versa.

At this stage we will just assume this so-called Fundamental Theorem of Galois Theory. We will prove it in a later chapter. I have found that students are much more motivated in understanding the proof once they have seen it working wonderfully in many particular examples.

§9.2. $f(x) = x^4 - x^2 - 2$

(1) Factors: $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$.

(2) Zeros: $\pm \sqrt{2}, \pm i$

(3) Splitting field: $F = \mathbb{Q}[x^4 - x^2 - 2]$
$= \mathbb{Q}[\sqrt{2}, -\sqrt{2}, i, -i]$
$= \mathbb{Q}[\sqrt{2}, i] = \mathbb{Q}[i][\sqrt{2}]$.

(4) $|F/\mathbb{Q}| = |F/\mathbb{Q}[\sqrt{2}]| \times |\mathbb{Q}[\sqrt{2}]/\mathbb{Q}| = 2 \times 2 = 4$.

(5) The Galois group has order 4.

(6) Possible automorphisms: $i \to \pm i$ and $\sqrt{2} \to \pm \sqrt{2}$, giving four combinations.

(7) All 4 combinations arise (since $|F:\mathbb{Q}| = 4$).

(8) These automorphisms can be summarised in the table:

$\sqrt{2} \to$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\mathbf{i} \to$	I	i	–i	–i
order	1	2	2	2

(9) The first column is the identity automorphism.

(10) Let A, B be the 2nd and 3rd automorphisms. Then AB is the 4th.

(11) AB = BA [Under AB, $\sqrt{2} \to -\sqrt{2} \to -\sqrt{2}$ and $i \to i \to -i$.
Under BA, $\sqrt{2} \to \sqrt{2} \to -\sqrt{2}$ and $i \to -i \to -i$.]

(12) The completed table is:

	1	**A**	**B**	**AB**
$\sqrt{2} \to$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$i \to$	i	i	$-i$	$-i$
order	1	2	2	2

The Galois group is thus:

$$\langle \mathbf{A, B \mid A^2 = B^2, AB = BA} \rangle \cong \mathbf{C_2 \times C_2}.$$

(13) The subgroups of this group, together with their fixed fields are:

SUBGROUP	**order**	**SUBFIELD**	**degree over $\mathbb{Q}$**
G	4	$\mathbb{Q}$	1
$\langle A \rangle$	2	$\mathbb{Q}[i]$	2
$\langle B \rangle$	2	$\mathbb{Q}[\sqrt{2}]$	2
$\langle AB \rangle$	2	$\mathbb{Q}[i\sqrt{2}]$	2
1	1	$\mathbb{Q}[f(x)]$	4

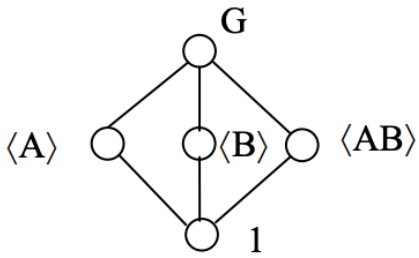
(14) Because we have listed every subgroup we can be confident that we have listed every subfield.

(15) Notice that the degree of each extension is the index of the corresponding subfield.

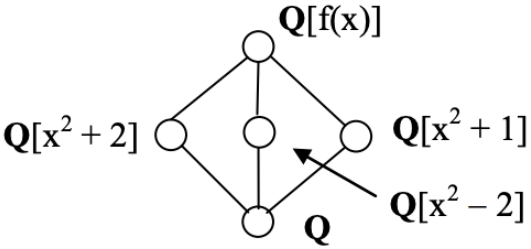
(16) In this group every subgroup is normal, so every subfield must be a polynomial extension. Indeed they are since:

$$\mathbb{Q}[i] = \mathbb{Q}[x^2 + 1];$$
$$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[x^2 - 2];$$
$$\mathbb{Q}[i\sqrt{2}] = \mathbb{Q}[x^2 + 2].$$

(17) The Galois correspondence can be illustrated as follows:



SUBGROUPS OF G(Q[$x^4 - x^2 - 2$]/Q)



SUBFIELDS OF Q[$x^4 - x^2 - 2$]

It might appear from the relative positions of the subgroups and subfields that $\mathbb{Q}[x^2 + 2]$ is the fixed field corresponding to ⟨A⟩, which is not the case. You must remember that the lattice of fixed fields is the same as the lattice of subgroups of the Galois group, *once this has been turned upside down*. It doesn't show up in this

example. However $\langle A \rangle$ corresponds to $\mathbb{Q}[x^2 + 1]$, its fixed field.

Notice too that the circles representing the subgroups and subfields are all white. We use the convention that normal subgroups and polynomial extensions are represented by white circles. Subgroups that are not normal, and fields that are not polynomial extensions, will be represented by black circles. There are none of these in this example.

§9.3. $f(x) = x^3 - 2$

(1) Zeros: $2^{1/3}$, $2^{1/3}\omega$, $2^{1/3}\omega^2$.

(2) Splitting field: $F = \mathbb{Q}[2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2] = \mathbb{Q}[2^{1/}3, \omega]$.

(3) The minimum polynomial of $2^{1/3}$ is $x^3 - 2$.
Thus $|\mathbb{Q}[2^{1/3}]/\mathbb{Q}| = 3$.

(4) The minimum polynomial for ω over $\mathbb{Q}$ is $x^2 + x + 1$ and over $\mathbb{Q}[2^{1/3}]$ it is the same.

(5) $|F/\mathbb{Q}| = |F/\mathbb{Q}[2^{1/3}]| \times |\mathbb{Q}[2^{1/3}]/\mathbb{Q}| = 2 \times 3 = 6$.

(6) The Galois group has order 6.

(7) Possible automorphisms: $2^{1/3} \rightarrow 2^{1/3}$, $2^{1/3}\omega$, $2^{1/3}\omega^2$ and $\omega \rightarrow \omega$ or ω^2, giving six combinations.

(8) All 6 combinations arise. [since $|F:\mathbb{Q}| = 6$]

(9) The automorphisms can be summarised in the table:

$\mathbf{2^{1/3} \rightarrow}$	$2^{1/3}$	$2^{1/3}\omega$	$2^{1/3}\omega^2$	$2^{1/3}$	$2^{1/3}\omega$	$2^{1/3}\omega^2$
$\boldsymbol{\omega \rightarrow}$	ω	ω	ω	ω^2	ω^2	ω^2
orders	1	3	3	2	2	2

(10) Let A be the automorphism which fixes ω and maps $2^{1/3}$ to $2^{1/3}\omega$.

(11) Let B be the automorphism which fixes $2^{1/3}$ and maps ω to ω^2.

(12) We can now express each of the six automorphisms in terms of A, B:

	$\mathbf{1}$	$\mathbf{A}$	$\mathbf{A^2}$	$\mathbf{B}$	$\mathbf{A^2B}$	$\mathbf{AB}$
$\mathbf{2^{1/3} \rightarrow}$	$2^{1/3}$	$2^{1/3}\omega$	$2^{1/3}\omega^2$	$2^{1/3}$	$2^{1/3}\omega$	$2^{1/3}\omega^2$
$\boldsymbol{\omega \rightarrow}$	ω	ω	ω	ω^2	ω^2	ω^2
orders	1	3	3	2	2	2

(13) $BA = A^{-1}B$.
[Under BA $2^{1/3} \rightarrow 2^{1/3} \rightarrow 2^{1/3}\omega$ and $\omega \rightarrow \omega^2 \rightarrow \omega^2$.]

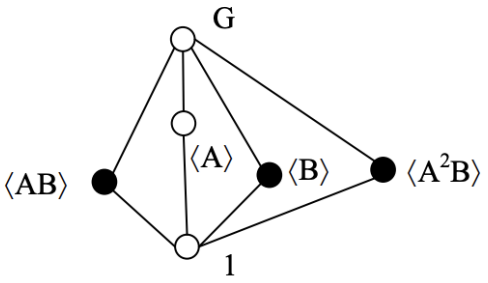
(14) The Galois group is thus:

$$\mathbf{\langle A, B \mid A^3, B^2, BA = A^{-1}B \rangle \cong D_6.}$$

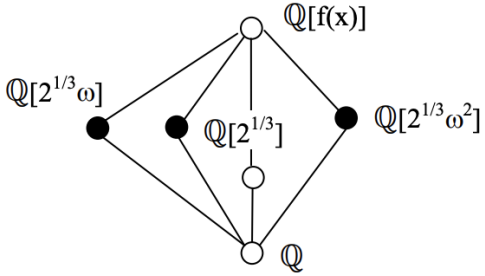
(15) The cyclic subgroup generated by A is a normal subgroup of order 3, that is, of index 2. It's fixed field is thus an extension of $\mathbb{Q}$ of degree 2. Clearly it is $\mathbb{Q}[\omega]$. Because the subgroup is normal the fixed field should be a polynomial extension. It is, in fact, $\mathbb{Q}[x^2 + x + 1 = 0]$.

(16) B fixes $2^{1/3}$ so the fixed field of $\langle B \rangle$ is $\mathbb{Q}[2^{1/3}]$.
AB fixes $2^{1/3}\omega$ so the fixed field of $\langle AB \rangle$ is $\mathbb{Q}[2^{1/3}\omega]$.
A^2B fixes $2^{1/3}\omega^2$ so the fixed field of $\langle A^2B \rangle$ is $\mathbb{Q}[2^{1/3}\omega^2]$.

(17) The Galois correspondence can be illustrated as follows:



SUBGROUPS OF G($\mathbb{Q}[x^3 = 2]/\mathbb{Q}$)



SUBFIELDS OF $\mathbb{Q}[x^3 = 2]$

You can see more clearly, with this example, the fact that the lattices of subgroups and subfields are flipped over relative to one another. You can also see the use of white and black circles.

Often it's more convenient to present this information in a table. We can't see as clearly what is inside what but sometimes the diagrams are too messy.

H≤ G	**◁**	**|H|**	**H***	**poly ext'n**	**deg**
G	√	6	$\mathbb{Q}$	$\mathbb{Q}$	1
⟨A⟩	√	3	$\mathbb{Q}[\omega]$	$\mathbb{Q}[x^2 + x + 1]$	2
⟨B⟩		2	$\mathbb{Q}[2^{1/3}]$		3
⟨AB⟩		2	$\mathbb{Q}[2^{1/3}\omega]$		3
⟨A^2B⟩		2	$\mathbb{Q}[2^{1/3}\omega^2]$		3
1	√	1	$\mathbb{Q}[2^{1/3}, \omega]$	$\mathbb{Q}[x^3 = 2]$	6

§9.4. $f(x) = x^4 - 2$

(1) $K = \mathbb{Q}[x^4 = 2] = \mathbb{Q}[\pm 2^{1/4}, \pm 2^{1/4}i]$
$= \mathbb{Q}[2^{1/4}, i] = \mathbb{Q}[2^{1/4}][i]$

(2) The minimum polynomial of $2^{1/4}$ is $x^4 - 2$.
Thus $|\mathbb{Q}[2^{1/4}]:\mathbb{Q}| = 4$ and $\{1, 2^{1/4}, \sqrt{2}, 2^{3/4}\}$ is a basis for $\mathbb{Q}[2^{1/4}]$ as a vector space over $\mathbb{Q}$.

(3) The minimum polynomial for i over $\mathbb{Q}$ is $x^2 + 1$ and over $\mathbb{Q}[2^{1/4}]$ it is still $x^2 + 1$.
So $|\mathbb{Q}\,[2^{1/4}][i]/\mathbb{Q}[2^{1/4}]| = 2$ with $\{1, i\}$ as a basis..

(4) Thus $|K/\mathbb{Q}| = 8$ and so $G(K/\mathbb{Q})$ has order 8. A suitable basis for K over $\mathbb{Q}$ is:

1	$2^{1/4}$	$\sqrt{2}$	$2^{3/4}$
i	$2^{1/4}$i	$\sqrt{2}$i	$2^{3/4}$i

(5) Every automorphism in $G(K/\mathbb{Q})$ must map i to $\pm$ i and $2^{1/4}$ to one of $\pm 2^{1/4}$, $\pm 2^{1/4}$i. There are 8 automorphisms, described by their effect on these generators:

i $\rightarrow$	i	i	I	i	–i	–i	–i	–i
$\mathbf{2^{1/4}} \rightarrow$	$2^{1/4}$	$2^{1/4}$i	$-2^{1/4}$	$-2^{1/4}$i	$2^{1/4}$	$2^{1/4}$i	$-2^{1/4}$	$-2^{1/4}$i
Orders	1	4	2	4	2	2	2	2

(6) As before we can name the automorphisms and list their orders. This Galois group is:

$$\mathbf{\langle A, B \mid A^4, B^2, BA = A^{-1}B \rangle \cong D_8.}$$

	1	**A**	$\mathbf{A^2}$	$\mathbf{A^3}$	**B**	$\mathbf{A^3B}$	$\mathbf{A^2B}$	**AB**
i $\rightarrow$	i	i	i	i	–i	–i	–i	–i
$\mathbf{2^{1/4}} \rightarrow$	$2^{1/4}$	$2^{1/4}$i	$-2^{1/4}$	$-2^{1/4}$i	$2^{1/4}$	$2^{1/4}$i	$-2^{1/4}$	$-2^{1/4}$i
order	1	4	2	4	2	2	2	2

(7) The cyclic subgroup generated by A is a normal subgroup of order 4, that is, of index 2. It's fixed field is thus an extension of $\mathbb{Q}$ of degree 2. Clearly it is $\mathbb{Q}$[i]. Because the subgroup is normal the fixed field is a polynomial extension. It is $\mathbb{Q}[x^2 + 1]$.

(8) The cyclic subgroup generated by A^2 is another normal subgroup. Since it has index 4 the fixed field must have degree 4 over $\mathbb{Q}$. It must therefore fix something other than i. Of course, it fixes $\sqrt{2}$.
For $(\sqrt{2})^{A^2} = ((2^{1/4})^{A^2})^2 = (-2^{1/4})^2 = \sqrt{2}$.

So the fixed field must be $\mathbb{Q}[i, \sqrt{2}]$. This also must be a polynomial extension. It is on fact

$\mathbb{Q}[(x^2 + 1)(x^2 - 2) = 0]$, that is, $\mathbb{Q}[x^4 - x^2 - 2]$.

(9) There are the subgroups $\langle A^2, B\rangle$ and $\langle A^2, AB\rangle$, of order 4 (index 2). Their fixed fields have degree 2 over $\mathbb{Q}$. The fixed field for $\langle A^2, B\rangle$ is $\mathbb{Q}[\sqrt{2}]$ and for $\langle A^2, AB\rangle$ it's $\mathbb{Q}[\sqrt{2}i]$.

(10) While these are the only normal subgroups of the Galois group, apart from the whole group and the trivial subgroup, there are 4 other subgroups of order 2 (index 4). Their fixed fields will all be extensions of degree 4. What are they?

B fixes $2^{1/4}$ so the fixed field of $\langle B\rangle$ is $\mathbb{Q}[2^{1/4}]$.
A^2B fixes $2^{1/4}i$ so the fixed field of $\langle AB\rangle$ is $\mathbb{Q}[2^{1/4}i]$.

But what does AB fix? Just because it doesn't fix either of the generators $2^{1/4}$ and i doesn't mean it only fixes the rational numbers. Since $\langle AB\rangle$ has index 4 its fixed field must have degree 4 over $\mathbb{Q}$. You can't always find fixed fields by merely inspecting the automorphism table.

A typical element of $\mathbb{Q}[x^4 = 2]$ can be expressed as a linear combination, over $\mathbb{Q}$, of the basis elements 1, $2^{1/4}$, $\sqrt{2}$, $2^{3/4}$, i, $2^{1/4}$i, $\sqrt{2}$i, $2^{3/4}$i.

Let
$x = a + b2^{1/4} + c\sqrt{2} + d2^{3/4} + e\mathrm{i} + f2^{1/4}\mathrm{i} + g\sqrt{2}\mathrm{i} + h2^{3/4}\mathrm{i}$,
where a to h are rational.
Then
$x^{\mathrm{A}} = a + b2^{1/4}\mathrm{i} - c\sqrt{2} - d2^{3/4}\mathrm{i} + e\mathrm{i} - f2^{1/4} - g\sqrt{2}\mathrm{i} + h2^{3/4}$ and so
$x^{\mathrm{AB}} = a - b2^{1/4}\mathrm{i} - c\sqrt{2} + d2^{3/4}\mathrm{i} - e\mathrm{i} - f2^{1/4} + g\sqrt{2}\mathrm{i} + h2^{3/4}$.
If $x^{\mathrm{AB}} = x$ then, equating coefficients of our basis elements, we get:
$b = -f$,
$c = e = 0$,
$d = h$, and so

$$x = a + b2^{1/4}(1 - \mathrm{i}) + d2^{3/4}(1 + \mathrm{i}) + g\sqrt{2}\mathrm{i}.$$

So the fixed field is spanned, as a vector space over $\mathbb{Q}$, by 1, $2^{1/4}(1 - \mathrm{i})$, $\sqrt{2}\mathrm{i}$ and $2^{3/4}(1 + \mathrm{i})$.

As a field it can be generated by $\alpha = 2^{1/4}(1 - \mathrm{i})$ since $\alpha^2 = -2\sqrt{2}\mathrm{i}$ and $\alpha^3 = -2(2^{3/4}(1 + \mathrm{i}))$.

So the fixed field of the subgroup $\langle \mathrm{AB} \rangle$ is $\mathbb{Q}[2^{1/4}(1 - \mathrm{i})]$. Similarly the fixed field of $\langle \mathrm{A}^3\mathrm{B} \rangle$ is $\mathbb{Q}[2^{1/4}(1 + \mathrm{i})]$.

This is the ‘brute force’ method should only be a last resort. Usually you can find the fixed field from the automorphism table, provided you stare at it long enough,

and provided you provide some ancillary rows, for interesting combinations of the generators. In this case we might decide to provide rows to show the effect of the automorphisms on $2^{1/2}$, $2^{1/4}$, $2^{1/2}i$ and $2^{1/4}i$. The entries are obtained by multiplying, or squaring, the entries in the appropriate rows.

	1	**A**	**A²**	**A³**
i →	i	i	i	i
$2^{1/4}$ →	$2^{1/4}$	$2^{1/4}i$	$-2^{1/4}$	$-2^{1/4}i$
$2^{1/2}$ →	$2^{1/2}$	$-2^{1/2}$	$2^{1/2}$	$-2^{1/2}$
$2^{1/2}$i →	$2^{1/2}i$	$-2^{1/2}i$	$2^{1/2}i$	$-2^{1/2}i$
$2^{1/4}$i →	$2^{1/4}i$	$-2^{1/4}$	$-2^{1/4}i$	$2^{1/4}$

	B	**A³B**	**A²B**	**AB**
i →	$-i$	$-i$	$-i$	$-i$
$2^{1/4}$ →	$2^{1/4}$	$2^{1/4}i$	$-2^{1/4}$	$-2^{1/4}i$
$2^{1/2}$ →	$2^{1/2}$	$-2^{1/2}$	$2^{1/2}$	$-2^{1/2}$
$2^{1/2}$i →	$-2^{1/2}i$	$2^{1/2}i$	$-2^{1/2}i$	$2^{1/2}i$
$2^{1/4}$i →	$-2^{1/4}i$	$2^{1/4}$	$2^{1/4}i$	$-2^{1/4}$

Examining the AB column we see that $2^{1/2}i$ is fixed by AB. But, as explained above, the degree of the fixed field over $\mathbb{Q}$ is 4. The degree of $\mathbb{Q}[2^{1/2}i]$ is only 2. We need something else.

Notice that $2^{1/4}$ and $2^{1/4}i$ swap under A^3B. This means that their sum is fixed by A^3B. Now we can check that the degree of $\mathbb{Q}[2^{1/4}(1 + i)]$ over $\mathbb{Q}$ is 4, which is

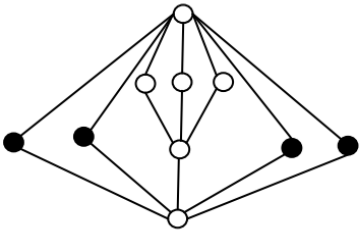
enough. The fixed field of $\langle A^3B \rangle$ is $\mathbb{Q}[2^{1/4}(1 + i)]$. No need for brute force!

In the case of AB, $2^{1/4}$ and $2^{1/4}i$ also swap, but with a sign change in each case. Here it is the difference that is fixed. The fixed field of $\langle AB \rangle$ is $\mathbb{Q}[2^{1/4}(1 – i)]$.

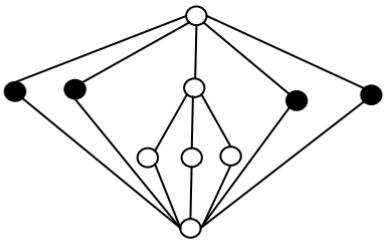
But we found that $2^{1/2}i$ is also fixed by AB. Do we need to throw that in too? No, it must be there already, otherwise the degree would be too big. In fact squaring $2^{1/4}(1 – i)$ gives $–2^{1/2}i$, so $2^{1/2}i$ is already there in

$$\mathbb{Q}[2^{1/4}(1 – i)].$$

(11) Since we considered all the subgroups of the Galois group we can be sure that we have all the subfields. The Galois correspondence can be illustrated as follows:



SUBGROUPS OF G($\mathbb{Q}[x^4 = 2]/\mathbb{Q}$)



SUBFIELDS OF $\mathbb{Q}[x^4 = 2]$

Here it would be very messy to label everything. Instead we list the subgroups and their fixed fields in a table.

$H \leq G$	$\triangleleft$	$\lvert H\rvert$	H^*	poly ext'n	deg
G	√	8	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A\rangle$	√	4	$\mathbb{Q}[i]$	$\mathbb{Q}[x^2 + 1]$	2
$\langle A^2, B\rangle$	√	4	$\mathbb{Q}[\sqrt{2}]$	$\mathbb{Q}[x^2 = 2]$	2
$\langle A^2, AB\rangle$	√	4	$\mathbb{Q}[\sqrt{2}i]$	$\mathbb{Q}[x^2 + 2]$	2
$\langle A^2\rangle$	√	2	$\mathbb{Q}[i, \sqrt{2}]$	$\mathbb{Q}[x^4 - x^2 - 2]$	4
$\langle B\rangle$		2	$\mathbb{Q}[2^{1/4}]$		4
$\langle AB\rangle$		2	$\mathbb{Q}[2^{1/4}(1 - i)]$		4
$\langle A^2B\rangle$		2	$\mathbb{Q}[2^{1/4}i]$		4
$\langle A^3B\rangle$		2	$\mathbb{Q}[2^{1/4}(1 + i)]$		4
1	√	1	$\mathbb{Q}[2^{1/4}, i]$	$\mathbb{Q}[x^4 = 2]$	8

§9.5. $f(x) = x^{20} - 1$

The 20^{th} roots of 1 are $\sigma, \sigma^3, \sigma^7, \sigma^9, \sigma^{11}, \sigma^{13}, \sigma^{17}, \sigma^{19}$ where $\sigma = e^{2\pi i/20}$ so the splitting field is $\mathbb{Q}[x^{20} - 1] = \mathbb{Q}[\sigma]$. Under an automorphism σ maps to σ^r form some r that's coprime to 20.

The automorphism table is:

	1	**A**	**A³**	**A²**	**B**	**AB**	**A³B**	**A²B**
σ →	σ	σ^3	σ^7	σ^9	σ^{11}	σ^{13}	σ^{17}	σ^{19}

and so the Galois group is:

$$\mathbf{G = \langle A, B \mid A^4, B^2, BA = AB\rangle \cong C_4 \times C_2.}$$

The proper non-trivial subgroups are:
Order 4: $\langle A\rangle$, $\langle AB\rangle$, $\langle A^2, B\rangle$
Order 2: $\langle A^2\rangle$, $\langle B\rangle$, $\langle A^2B\rangle$

The fixed field are hard to find directly in terms of powers of σ. Let's try a few supplementary elements of the splitting field.
$\sigma^5 = i$ and $\theta = \sigma^5 = e^{2\pi i/5}$. The algebraic conjugates of θ are θ, θ^2, θ^3 and θ^4.

	1	**A**	**A^3**	**A^2**	**B**	**AB**	**A^3B**	**A^2B**
$\sigma \rightarrow$	σ	σ^3	σ^7	σ^9	σ^{11}	σ^{13}	σ^{17}	σ^{19}
$i \rightarrow$	i	–i	–i	i	–i	i	i	–i
$\theta \rightarrow$	θ	θ^3	θ^2	θ^4	θ	θ^3	θ^2	θ^4

We can see that B fixes θ and since $\langle B\rangle$ has index 4 in *G* and θ has degree 4 over $\mathbb{Q}$, the fixed field of $\langle B\rangle$ is $\mathbb{Q}[\theta]$. Also, $\langle AB\rangle = \{1, AB, A^2, A^3B\}$ and clearly the fixed field of $\langle AB\rangle$ is $\mathbb{Q}[i]$.

To find the other fixed fields we'll obtain a surd form for θ. Let $c = \cos(2\pi/5)$ and
$s = \sin(2\pi/5)$.
Then
$1 = \theta^5 = (c + is)^5$
$= c^5 + 5ic^4s - 10c^3s^2 - 10ic^2s^3 + 5cs^4 + is^5$.

Equating imaginary parts, dividing by *s* and writing $s^2 = 1 - c^2$ we find that $16c^4 - 12c^2 + 1 = 0$.

Hence $c^2 = \dfrac{12 \pm \sqrt{144 - 64}}{32} = \dfrac{3 \pm \sqrt{5}}{8}$,

so $c = \pm\sqrt{\dfrac{3 \pm \sqrt{5}}{8}}$.

Now the same calculations will apply if c is any one of the four values:

$$\cos(2\pi/5),\ \cos(4\pi/5),\ \cos(6\pi/5),\ \cos(8\pi/5).$$

With the help of a calculator we can identify which 'cos' goes with which surd.

We now see that:

$\cos(2\pi/5) = \sqrt{\dfrac{3 - \sqrt{5}}{8}}$, $\cos(4\pi/5) = -\sqrt{\dfrac{3 + \sqrt{5}}{8}}$.

Hence $\theta + \theta^4 = 2\cos(2\pi/5) = \sqrt{\dfrac{3 - \sqrt{5}}{2}}$ and

$$\theta^2 + \theta^3 = 2\cos(4\pi/5) = -\sqrt{\frac{3 + \sqrt{5}}{2}}.$$

Let $c_1 = \theta + \theta^4$ and $c_2 = \theta^2 + \theta^3$.

	1	**A**	**A^3**	**A^2**	**B**	**AB**	**A^3B**	**A^2B**
$\sigma \to$	σ	σ^3	σ^7	σ^9	σ^{11}	σ^{13}	σ^{17}	σ^{19}
$i \to$	i	–i	–i	i	–i	i	i	–i
$\theta \to$	θ	θ^3	θ^2	θ^4	θ	θ^3	θ^2	θ^4
$c_1 \to$	c_1	c_2	c_2	c_1	c_1	c_2	c_2	c_1
$c_2 \to$	c_2	c_1	c_1	c_2	c_2	c_1	c_1	c_2
$\sqrt{5} \to$	$\sqrt{5}$	$-\sqrt{5}$	$-\sqrt{5}$	$\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$-\sqrt{5}$	$\sqrt{5}$

$H \leq G$	$\triangleleft$	**|H|**	**H***	**poly extn**	**deg**
G	√	8	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A \rangle$	√	4	$\mathbb{Q}[i\sqrt{5}]$	$\mathbb{Q}[x^2 + 5]$	2
$\langle AB \rangle$	√	4	$\mathbb{Q}[i]$	$\mathbb{Q}[x^2 + 1]$	2
$\langle A^2, B \rangle$	√	4	$\mathbb{Q}[\sqrt{5}]$	$\mathbb{Q}[x^2 - 5]$	2
$\langle A^2 \rangle$	√	2	$\mathbb{Q}[i, \sqrt{5}]$	$\mathbb{Q}\ [x^2 + 1)(x^2 - 5)]$	4
$\langle B \rangle$	√	2	$\mathbb{Q}[e^{2\pi i/5}]$	$\mathbb{Q}[x^4 + x^3 + x^2 + x + 1]$	4
$\langle A^2B \rangle$	√	2	$\mathbb{Q}[\cos(2\pi/5)]$	$\mathbb{Q}[x^4 - 3x^2 + 1]$	4
1	√	1	$\mathbb{Q}[x^{20} = 1]$	$\mathbb{Q}[x^{20} = 1]$	8

§9.6. $f(x) = x^{16} - 1$

The splitting field is $\mathbb{Q}[\sigma]$ where $\sigma = e^{2\pi i/16}$. Under an automorphism σ maps to σ^r form some odd r.
The automorphism table is:

	1	**A**	**A^3B**	**A^2B**	**A^2**	**A^3**	**AB**	**B**
$\sigma \to$	σ	σ^3	σ^5	σ^7	σ^9	σ^{11}	σ^{13}	σ^{15}

and so the Galois group is:

$$\mathbf{G = \langle A, B \mid A^4, B^2, BA = AB \rangle \cong C_4 \times C_2.}$$

We won't attempt to find all the fixed fields, but just the one corresponding to $\langle B \rangle$. This time we'll work with powers of σ. Note that B maps σ to σ^{-1} and so it will map each power of σ into its inverse. In fact B is the restriction of the conjugation automorphism to the splitting field.

The splitting field is the end point of the sequence of quadratic extensions:

$$\mathbb{Q} \leq \mathbb{Q}[\sigma^4] \leq \mathbb{Q}[\sigma^2] \leq \mathbb{Q}[\sigma].$$

Note that $\sigma^8 = -1$ and $\sigma^4 = i$.

Each extension has degree 2 and they have bases $\{1, \sigma^4\}$, $\{1, \sigma^2\}$, $\{1, \sigma\}$ respectively. A basis for the splitting field over $\mathbb{Q}$ is the set of all products of these, one from each, that is,

$$1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6, \sigma^7.$$

A typical element is:

$\alpha = a + b\sigma + c\sigma^2 + d\sigma^3 + e\sigma^4 + f\sigma^5 + g\sigma^6 + h\sigma^7.$

Under B this maps to

$$\begin{aligned} &a + b\sigma^{15} + c\sigma^{14} + d\sigma^{13} + e\sigma^{12} + f\sigma^{11} + g\sigma^{10} + h\sigma^9 \\ &= a - b\sigma^7 - c\sigma^6 - d\sigma^5 - e\sigma^4 - f\sigma^3 - g\sigma^2 - h\sigma \\ &= a - h\sigma - g\sigma^2 - f\sigma^3 - e\sigma^4 - d\sigma^5 - c\sigma^6 - b\sigma^7. \end{aligned}$$

If α is fixed by B then, equating coefficients, we have:

$b = -h$,

$c = -g$,

$d = -f$,

$e = 0$.

Hence $\alpha = a + b(\sigma - \sigma^7) + c(\sigma^2 - \sigma^6) + d(\sigma^3 - \sigma^5)$.

The fixed field is thus $\mathbb{Q}[\sigma - \sigma^7, \sigma^2 - \sigma^6, \sigma^3 - \sigma^5]$.
Now $(\sigma - \sigma^7)^2 = \sigma^2 + \sigma^{14} - 2\sigma^8$
$= \sigma^2 - \sigma^6 + 2$ and
$(\sigma - \sigma^7)(\sigma^2 - \sigma^6) = \sigma^3 - \sigma^7 - \sigma^9 + \sigma^{13}$
$= \sigma^3 - \sigma^7 + \sigma - \sigma^5$
so the splitting field is $\mathbb{Q}[\sigma - \sigma^7]$.

§9.7. $f(x) = x^4 - 4x^2 + 10$

This is a quadratic in x^2.

If $f(x) = 0$ then $x^2 = \dfrac{4 \pm \sqrt{16 - 40}}{2} = 2 \pm \sqrt{6}i$.

Hence the zeros of $f(x)$ are $\pm \alpha, \pm \beta$ where $\alpha^2 = 2 + \sqrt{6}i$ and $\beta^2 = 2 - \sqrt{6}i$. Since $(\alpha\beta)^2 = 10$ we may choose α, β so that $\alpha\beta = \sqrt{10}$.

Hence $\mathbb{Q}[f(x)] = \mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\alpha, \sqrt{10}]$.

	1	$\mathbf{A^2}$	**B**	$\mathbf{A^2B}$
$\boldsymbol{\alpha} \rightarrow$	α	$-\alpha$	β	$-\beta$
$\boldsymbol{\sqrt{10}} \rightarrow$	$\sqrt{10}$	$\sqrt{10}$	$\sqrt{10}$	$\sqrt{10}$
$\boldsymbol{\beta} \rightarrow$	β	$-\beta$	α	$-\alpha$
$\boldsymbol{\sqrt{6}i} \rightarrow$	$\sqrt{6}i$	$\sqrt{6}i$	$-\sqrt{6}i$	$-\sqrt{6}i$
orders	1	2	2	2

	A^3B	AB	A	A^3
$\alpha \to$	α	$-\alpha$	β	$-\beta$
$\sqrt{10} \to$	$-\sqrt{10}$	$-\sqrt{10}$	$-\sqrt{10}$	$-\sqrt{10}$
$\beta \to$	$-\beta$	β	$-\alpha$	α
$\sqrt{6}i \to$	$\sqrt{6}i$	$\sqrt{6}i$	$-\sqrt{6}i$	$-\sqrt{6}i$
Orders	2	2	4	4

$$\mathbf{G = \langle A, B \mid A^4, B^2, BA = A^{-1}B \rangle \cong D_8.}$$

The automorphism A doesn't seem to fix anything, but remember that there are more things that might be fixed other than those listed. Since $\langle A \rangle$ has index 2 in the Galois group its fixed field must have degree 2 over $\mathbb{Q}$. What does it fix?

Notice that both $\sqrt{10}$ and $\sqrt{6}i$ simply change their sign under A so their product must be fixed. This is $\sqrt{60}i = 2\sqrt{15}i$. So the fixed field of $\langle A \rangle$ is $\mathbb{Q}[\sqrt{15}i]$.

The fixed field of $\langle B \rangle$ appears to be just $\mathbb{Q}[\sqrt{10}]$, but this isn't big enough. The index of $\langle B \rangle$ is 4 and so we need a fixed field of degree 4. But notice that B swaps α and β so fixes $\alpha\beta$. Unfortunately $\alpha\beta = \sqrt{10}$ and we already have B fixing $\sqrt{10}$. There must be something else.

Of course B fixed $\alpha + \beta$ as well. If this is outside of $\mathbb{Q}[\sqrt{10}]$ we're in business. So what is $\alpha + \beta$?

Now $(\alpha + \beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta$

$= 2 + \sqrt{6}i + 2 - \sqrt{6}i + 2\sqrt{10} = 4 + 2\sqrt{10}$,

so $\alpha + \beta = \pm\sqrt{4 + 2\sqrt{10}}$. It doesn't matter which because in either case this would give B fixing $\sqrt{4 + 2\sqrt{10}}$ and this appears to have degree 4 over $\mathbb{Q}$.

But does it? Suppose that it was $\sqrt{11 + 2\sqrt{10}}$ Since $(1 + \sqrt{10})^2 = 11 + 2\sqrt{10}$ we have:

$$\sqrt{11 + 2\sqrt{10}} = 1 + \sqrt{10}$$

which leaves us with $\mathbb{Q}[\sqrt{10}]$, a subfield whose degree is too small.

Well, suppose that $\sqrt{4 + 2\sqrt{10}} = a + b\sqrt{10}$ for $a, b \in \mathbb{Q}$. Then $a^2 + 10b^2 + 2ab\sqrt{10} = 4 + 2\sqrt{10}$. Since 1, $\sqrt{10}$ are linearly independent over $\mathbb{Q}$ we conclude that:

$$a^2 + 10b^2 = 4 \text{ and } ab = 1.$$

If $a = 0$ this gives $b^2 = \frac{2}{5}$ and so $\sqrt{\frac{2}{5}}$ is rational, which can easily be shown to be false.

Hence $b = \frac{1}{a}$. Substituting into the first equation we get $a^2 + \frac{10}{a^2} = 4$ which means that $a^4 - 4a^2 + 10 = 0$.

This is the same quartic that we began with. But there's one important difference. Our question now is not so much to solve it but rather to determine whether there are any *rational* zeros. Clearly, from what we did earlier, none of the zeros are rational.

So this settles the fact that $\mathbb{Q}[\sqrt{10}, \sqrt{4 + 2\sqrt{10}}\,]$ does, indeed, have degree 4 over $\mathbb{Q}$ and so is the fixed field of $\langle B \rangle$.

But clearly $\mathbb{Q}[\sqrt{10}, \sqrt{4 + 2\sqrt{10}}\,]$ can be simplified to $\mathbb{Q}[\sqrt{4 + 2\sqrt{10}}\,]$.

The fixed field of the other subgroups can now be readily found. They are summarised as follows.

H≤ G	**◁**	**|H|**	**H***	**poly extn**	**deg**
G	√	8	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A \rangle$	√	4	$\mathbb{Q}[\sqrt{15}i]$	$\mathbb{Q}[x^2 + 15]$	2
$\langle A^2 \rangle$	√	2	$\mathbb{Q}[\sqrt{10}, \sqrt{6}i]$	$\mathbb{Q}[(x^2 - 10)(x^2 + 6)]$	4
$\langle B \rangle$		2	$\mathbb{Q}[\sqrt{4 + 2\sqrt{10}}\,]$		4
$\langle AB \rangle$		2	$\mathbb{Q}[\alpha]$		4
$\langle A^2B \rangle$		2	$\mathbb{Q}[\sqrt{6 + 3\sqrt{10}})\,i]$		4
$\langle A^3B \rangle$		2	$\mathbb{Q}[\alpha]$		4
1	√	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[x^4 - 4x^2 + 10]$	8

§9.8. $f(x) = x^4 - 5x^2 + 5$

This polynomial is very similar to the previous one. But watch out! There are important differences. If $f(x) = 0$ then $x^2 = \dfrac{5 \pm \sqrt{25 - 20}}{2} = \dfrac{5 \pm \sqrt{5}}{2}$.

The zeros of $f(x)$ are $\pm\alpha, \pm\beta$ where

$$\alpha^2 = \frac{5+\sqrt{5}}{2} \text{ and}$$

$$\beta^2 = \frac{5-\sqrt{5}}{2}.$$

Since $(\alpha\beta)^2 = \frac{25-5}{4} = 5$ we may choose α, β so that

$$\alpha\beta = \sqrt{5}.$$

Hence $\mathbb{Q}[f(x)] = \mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\alpha, \sqrt{5}]$.
But $\sqrt{5} \in \mathbb{Q}[\alpha]$ so $\mathbb{Q}[f(x)] = \mathbb{Q}[\alpha]$. The automorphisms of $\mathbb{Q}[\alpha]$ are as follows.

	1	$\mathbf{A^2}$	**A**	$\mathbf{A^3}$
$\boldsymbol{\alpha \to}$	α	$-\alpha$	β	$-\beta$
$\boldsymbol{\sqrt{5} \to}$	$\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$-\sqrt{5}$
$\boldsymbol{\beta \to}$	β	$-\beta$	$-\alpha$	α
orders	1	2	2	2

$$\mathbf{G(\mathbb{Q}[x^4 - 5x^2 + 5]/\mathbb{Q}) = \langle A, B \mid A^4 \rangle \cong C_4.}$$

The only proper, non-trivial subgroup is $\langle A^2 \rangle$ and its fixed field is clearly $\mathbb{Q}[\sqrt{5}]$. The fixed fields are as follows.

$\mathbf{H \leq G}$	$\triangleleft$	$\mathbf{\lvert H \rvert}$	**H***	**poly extn**	**deg**
G	$\surd$	4	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A^2 \rangle$	$\surd$	2	$\mathbb{Q}[\sqrt{5}]$	$\mathbb{Q}[(x^2 - 5]$	2
1	$\surd$	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[x^4 - 5x^2 + 5]$	4

§9.9. $f(x) = x^3 - 3x + 1$

And now for something completely different! In this case we could find the zeros using the cubic formula from Chapter 8 but it would be a lot of work to find them and then it would be quite difficult to use them. Instead we'll use an indirect method by observing a rather peculiar property of this polynomial.

Let $f(x) = x^3 - 3x + 1$. If α is a zero of $f(x)$ then so is $\frac{\alpha - 1}{\alpha}$ since

$$f\left(\frac{\alpha - 1}{\alpha}\right) = \left(\frac{\alpha - 1}{\alpha}\right)^3 - 3\left(\frac{\alpha - 1}{\alpha}\right) - 1$$

$$= \frac{(\alpha - 1)^3 - 3\alpha^2(\alpha - 1) - \alpha^3}{\alpha^3}$$

$$= \frac{-\alpha^3 + 3\alpha - 1}{\alpha^3} = 0.$$

The map $\theta(\alpha) = \frac{\alpha - 1}{\alpha}$ maps one zero to another, and it has order 3 and θ^3 is the identity.

So the three zeros of $f(x)$ have the form α, $\theta(\alpha) = \frac{\alpha - 1}{\alpha}$ and $\theta^2(\alpha) = \frac{1}{1 - \alpha}$.

We only need to extend $\mathbb{Q}$ by any one of the three zeros and the other two will automatically be included. Hence if α is any zero then $\mathbb{Q}[f(x) = 0] = \mathbb{Q}[\alpha]$.

It's not difficult to show that $f(x)$ is prime over $\mathbb{Q}$ and so $|\mathbb{Q}[f(x)]/\mathbb{Q}| = 3$. Thus the Galois group is $\mathbf{C}_3$.

§9.10. A Mystery Polynomial

In this case we begin with the Galois group and try to find a suitable polynomial. Is there a polynomial whose Galois group over $\mathbb{Q}$ is cyclic of order 5?

We start by considering $x^{11} - 1$, whose Galois group G will be cyclic of order 10. This group will have a quotient group G/H of order 5 and the fixed field of H will have C_5 as its Galois group.

Now $\mathbb{Q}[x^{11} = 1] = \mathbb{Q}[\varepsilon]$ where $\varepsilon = e^{2\pi i/11}$.
The minimum polynomial of ε over $\mathbb{Q}$ is

$$x^{10} + x^9 + \ldots + x^2 + x + 1$$

so $|\mathbb{Q}[x^{11} - 1]/\mathbb{Q}| = 10$.

The Galois Group thus has order 10 and, being the Galois group of a Type I radical extension, it's abelian. It must therefore be cyclic. In fact it can be generated by the automorphism which maps ε to ε^2. The automorphisms can be listed as follows:

	1	**A**	$\mathbf{A^2}$	$\mathbf{A^3}$	$\mathbf{A^4}$	$\mathbf{A^5}$	$\mathbf{A^6}$	$\mathbf{A^7}$	$\mathbf{A^8}$	$\mathbf{A^9}$
$\boldsymbol{\varepsilon \rightarrow}$	ε	ε^2	ε^4	ε^8	ε^5	ε^{10}	ε^9	ε^7	ε^3	ε^6
order	1	10	5	10	5	2	5	10	5	10

Now $\mathbf{C}_5$ is a quotient group of $\mathbf{C}_{10}$.
We simply have to factor out by $\langle A^5 \rangle$.
Then $G(K/\mathbb{Q}) \cong \mathbf{C}_5$ where K is the fixed field of A^5.

So, what does A^5 fix? Notice that A^5 is the restriction of the conjugation automorphism.
So A^5 fixes the real numbers in $\mathbb{Q}[x^{11} - 1]$.

It's not difficult to see these are spanned by:

$\varepsilon + \varepsilon^{-1}$, $\varepsilon^2 + \varepsilon^{-2}$, $\varepsilon^3 + \varepsilon^{-3}$, $\varepsilon^4 + \varepsilon^{-4}$ and $\varepsilon^5 + \varepsilon^{-5}$.

These are respectively:
$2\cos(2\pi/11)$, $2\cos(4\pi/11)$, $2\cos(6\pi/11)$, $2\cos(8\pi/11)$ and $2\cos(10\pi/11)$. They are the zeros of some polynomial of degree 5, but which one? In fact it has very simple integer coefficients.

Let ε be any non-real 11^{th} root of 1,
let $\varepsilon_r = \varepsilon^r + \varepsilon^{-r}$ for $r = 1, 2, 3, 4, 5$.
Let $x = \varepsilon_1 = \varepsilon + \varepsilon^{-1}$.
Then $x^2 = \varepsilon^2 + \varepsilon^{-2} + 2 = \varepsilon_2 + 2$.

$x^3 = \varepsilon^3 + 3\varepsilon + 3\varepsilon^{-1} + \varepsilon^{-3} = 3\varepsilon_1 + \varepsilon_3$.

$x^4 = \varepsilon^4 + 4\varepsilon^2 + 6 + 4\varepsilon^{-2} + \varepsilon^{-4} = 6 + 4\varepsilon_2 + \varepsilon_4$,

and $x^5 = \varepsilon^5 + 5\varepsilon^3 + 10\varepsilon + 10\varepsilon^{-1} + 5\varepsilon^{-3} + \varepsilon^{-5}$

$= 10\varepsilon_1 + 5\varepsilon_3 + \varepsilon_5$.

Hence $\varepsilon_1 = x$,

$\varepsilon_2 = x^2 - 2$,

$\varepsilon_3 = x^3 - 3x$,

$\varepsilon_4 = x^4 - 6 - 4(x^2 - 2) = x^4 - 4x^2 + 2$

and $\varepsilon_5 = x^5 - 10x - 5(x^3 - 3x) = x^5 - 5x^3 + 5x$.

But $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5$ is the sum of all the 11^{th} roots of 1, except 1 and so is -1.

So $(x^5 - 5x^3 + 5x) + (x^4 - 4x^2 + 2) + (x^3 - 3x) + (x^2 - 2) + x + 1 = 0$.

This gives $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0$.
This is prime mod 2 and so is the minimum polynomial of ε. Since ε can be any one of the five non-real 11^{th} roots of 1, the zeros of this polynomial are:
$2\cos(2\pi/11)$, $2\cos(4\pi/11)$, $2\cos(6\pi/11)$ and $2\cos(8\pi/11)$.

So the Galois group of $\mathbb{Q}[x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1]$ over $\mathbb{Q}$ is isomorphic to $\mathbf{C}_5$.

Have you had enough? If so, skip to the next chapter. We're now going to present some even harder examples. But you might want to come back to these, especially if you have to do a project to find the Galois group of your own personal polynomial. You might find some useful ideas.

§9.11. $f(x) = x^6 - 6x^3 + 6$

The zeros of $x^6 - 6x^3 + 6$ are α, $\alpha\omega$, $\alpha\omega^2$, β, $\beta\omega$, $\beta\omega^2$ where $\alpha = \sqrt[3]{3 + \sqrt{3}}$ and $\beta = \sqrt[3]{3 - \sqrt{3}}$. The splitting field is $F = \mathbb{Q}[\alpha, \beta, \omega]$. Note that $\sqrt{3} = \alpha^3 - 3 \in F$, $\beta^3 - 3 = -\sqrt{3}$ and $\alpha\beta = 6^{1/3}$. So $F = \mathbb{Q}[\alpha, 6^{1/3}, \omega]$.

Now $|\mathbb{Q}[\alpha, 6^{1/3}, \omega]/\mathbb{Q}[\alpha, 6^{1/3}]| = 2$. and $|\mathbb{Q}[\alpha]/\mathbb{Q}| = 6$.
Suppose that $6^{1/3} \notin \mathbb{Q}[\sqrt[3]{3 + \sqrt{3}}]$.

Then $\mathbb{Q}[\alpha, 6^{1/3}]:\mathbb{Q}[\alpha]| = 3$, in which case
$|\mathbb{Q}[\alpha, 6^{1/3}]/\mathbb{Q}| = 18$ and $|\mathbb{Q}[f(x)]/\mathbb{Q}| = 36$.

$F = \mathbb{Q}[\alpha, 6^{1/3}, \omega]$ has degree 36 over $\mathbb{Q}$. Its Galois group has order 36 and is as follows:

	A	**B**	**C**	**D**
$\alpha\rightarrow$	$\alpha\omega$	α	β	α
$\mathbf{6^{1/3}}\rightarrow$	$6^{1/3}$	$6^{1/3}\omega$	$6^{1/3}$	$6^{1/3}$
$\omega\rightarrow$	ω	ω	ω	ω^2
$\beta\rightarrow$	$\beta\omega^2$	$\beta\omega$	α	β

The group is $\langle$A, B, C | A, B, C, D | A^3, B^3, C^2, D^2, BA = AB, CA = A^{-1}C, DA = A^{-1}D,

CB = BCA, DB = $B^{=1}$D, DC = CD$\rangle$.

We won't calculate the subgroups and their fixed fields. We'll finish by showing that our assumption that $6^{1/3} \notin \mathbb{Q}[\alpha]$ is justified. This is quite hard.

Suppose that $6^{1/3} \in \mathbb{Q}[\alpha]$. Now $\mathbb{Q}[\alpha]$ has as a basis over $\mathbb{Q}$ $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$ and hence, under our assumption, $6^{1/3} = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\alpha^5$ for some rational numbers *a*, *b*, *c*, *d*, *e*, *f*.

Under A, $6^{1/3}$ this maps to

$a + b\alpha\omega + c\alpha^2\omega^2 + d\alpha^3 + e\alpha^4\omega + f\alpha^5\omega^2$

$= a + b\alpha\omega - c\alpha^2 - c\alpha^2\omega + d\alpha^3 + e\alpha^4\omega - f\alpha^5 - f\alpha^5\omega.$

But this has to be either $6^{1/3}$, $6^{1/3}\omega$ or $6^{1/3}\omega^2$. This is all going on in $\mathbb{Q}[\alpha, \omega]$ which has a basis$\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \omega, \alpha\omega, \alpha^2\omega, \alpha^3\omega, \alpha^4\omega, \alpha^5\omega\}$ over $\mathbb{Q}$.

Case 1: $6^{1/3} \to 6^{1/3}$: Then

$a + b\alpha\omega - c\alpha^2 - c\alpha^2\omega + d\alpha^3 + e\alpha^4\omega - f\alpha^5 - f\alpha^5\omega$

$= a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\alpha^5$

and, equating corresponding coefficients, we get

$b = c = e = f = 0$ and $6^{1/3} = a + d\alpha^3 \in \mathbb{Q}[\sqrt{3}]$, a contradiction by considering dimensions. (Remember that $\alpha^3 = 3 + \sqrt{3}$.)

Case 2: $6^{1/3} \to 6^{1/3}\omega$: Then

$a + b\alpha\omega - c\alpha^2 - c\alpha^2\omega + d\alpha^3 + e\alpha^4\omega - f\alpha^5 - f\alpha^5\omega$

$= a\omega + b\alpha\omega + c\alpha^2\omega + d\alpha^3\omega + e\alpha^4\omega + f\alpha^5\omega$

and, equating corresponding coefficients, we get

$a = c = d = f = 0$ and $6^{1/3} = b\alpha + e\alpha^4$

$= \alpha(b + e\alpha^3)$

$= \alpha(b + 3e + e\sqrt{3})$

$= \alpha(g + e\sqrt{3})$

where $g = b + 3e \in \mathbb{Q}$.

Cubing, $6 = (3 + \sqrt{3})(g + e\sqrt{3})^3$

$= (3 + \sqrt{3})(g^3 + 3g^2e\sqrt{3} + 9ge^2 + 3e^3\sqrt{3})$

$= (3g^3 + 27ge^2 + 9g^2e + 9e^3)$

$+ (9g^2e + 9e^3 + g^3 + 9ge^2)\sqrt{3}$.

Since 1, $\sqrt{3}$ are linearly independent over $\mathbb{Q}$:

$3g^3 + 27ge^2 + 9g^2e + 9e^3 = 6$ and

$9g^2e + 9e^3 + g^3 + 9ge^2 = 0$.

If $e = 0$ then $g^3 = 2$, a contradiction. So $e \neq 0$.

Let $x = g/e \in \mathbb{Q}$.

Then from the second equation $x^3 + 9x^2 + 9x + 9 = 0$. Eisenstein is no good.

Mod 5 this polynomial becomes $x^3 - x^2 - x - 1$. Since this has no zeros in $\mathbb{Z}_5$, the cubic $x^3 + 9x^2 + 9x + 0$ is prime over $\mathbb{Q}$ and hence has no rational zeros, a contradiction.

Case 3: $6^{1/3} \to 6^{1/3}\omega^2$: Then

$$a + b\alpha\omega - c\alpha^2 - c\alpha^2\omega + d\alpha^3 + e\alpha^4\omega - f\alpha^5 - f\alpha^5\omega$$
$$= a\omega^2 + b\alpha\omega^2 + c\alpha^2\omega^2 + d\alpha^3\omega^2 + e\alpha^4\omega^2 + f\alpha^5\omega^2$$
$$= -a - a\omega - b\alpha - b\alpha\omega - c\alpha^2 - c\alpha^2\omega - d\alpha^3 - d\alpha^3\omega - e\alpha^4 - e\alpha^4\omega - f\alpha^5 - f\alpha^5\omega$$

and, equating corresponding coefficients, we get
$a = b = d = e = 0$ and so

$$6^{1/3} = c\alpha^2 + f\alpha^5 = \alpha^2(c + f\alpha^3)$$
$$= \alpha^2(c + 3f + f\sqrt{3})$$
$$= \alpha^2(g + f\sqrt{3}) \text{ where}$$
$$g = c + 3f.$$

Cubing, $6 = (12 + 6\sqrt{3})(g + f\sqrt{3})^3$

$$= (12 + 6\sqrt{3})(g^3 + 3g^2f\sqrt{3} + 9gf^2 + 3f^3\sqrt{3})$$
$$= (12g^3 + 108gf^2 + 54g^2f + 54f^3) + (36g^2f + 36f^3 + 6g^3 + 54gf^2)\sqrt{3}.$$

Since $1, \sqrt{3}$ are linearly independent over $\mathbb{Q}$,
$12g^3 + 108gf^2 + 54g^2f + 54f^3 = 6$ and
$36g^2f + 36f^3 + 6g^3 + 54gf^2 = 0$ and so dividing by 6
$6g^2f + 6f^3 + g^3 + 9gf^2 = 0$.
If $f = 0$ then $g^3 = ½$, a contradiction. So $f \neq 0$.
Let $x = g/f \in \mathbb{Q}$.
Then from the last equation $x^3 + 6x^2 + 9x + 6 = 0$.

This is prime over $\mathbb{Q}$ by Eisenstein and so has no rational zeros, a contradiction.

So we have shown that, indeed, $6^{1/3} \notin \mathbb{Q}[\alpha]$

§9.12. $f(x) = x^6 + 6x^4 + 12x^2 + 6$

By Eisenstein's Theorem $x^6 + 6x^4 + 12x^2 + 6$ is prime over $\mathbb{Q}$. Moreover, as it is a cubic in x^2, it's clearly soluble by radicals. Put $y = x^2$.
Then $f(x) = g(y) = y^3 + 6y^2 + 12y + 6 = (y + 2)^3 - 2$.
The zeros of $g(y)$ are $2^{1/3} - 2$, $2^{1/3}\omega - 2$ and $2^{1/3}\omega^2 - 2$ and so the zeros of $f(x)$ are $\pm \alpha, \pm \beta, \pm \gamma$ where
$\alpha^2 = 2^{1/3} - 2$,
$\beta^2 = 2^{1/3}\omega - 2$ and
$\gamma^2 = 2^{1/3}\omega^2 - 2$.

The splitting field of $f(x)$ is $K = \mathbb{Q}[\alpha, \beta, \gamma]$.
This clearly contains $\alpha^2 + 2 = 2^{1/3}$ and $\omega = \dfrac{\alpha^2 - 2}{\beta^2 - 2}$ so contains $\mathbb{Q}[2^{1/3}, \omega] = \mathbb{Q}[x^3 - 2]$.

This has degree 6 over $\mathbb{Q}$.

Now $|K: \mathbb{Q}[x^3 - 2]| = 8$.
(A basis is $\{1, \alpha, \beta, \gamma, \alpha\beta, \beta\gamma, \alpha\gamma, \alpha\beta\gamma\}$.)
Hence $|K/\mathbb{Q}| = 48$. This means that $|G(K/\mathbb{Q})| = 48$.

Each automorphism of $\mathbb{Q}[x^3 = 2]$ permutes α^2, β^2, γ^2 in one of 6 ways.
For each of these there are 8 elements of K.

For example if $2^{1/3} \to 2^{1/3}\omega$ and $\omega \to \omega$ then
$\alpha^2 \to \beta^2$, $\beta^2 \to \gamma^2$ and $\gamma^2 \to \alpha^2$.

Hence $\alpha \to \pm\beta$, $\beta \to \pm\gamma$ and $\gamma \to \pm\alpha$. Less obvious is the fact that K contains $\sqrt{6}i$. But note that the product of the zeros is $-(\alpha\beta\gamma)^2 = 6$.

We can describe the 8 elements of *K* that extend the above automorphism of $\mathbb{Q}[x^3 = 2]$ in the following table.

$\alpha \to$	β	$-\beta$	β	β
$\beta \to$	γ	γ	$-\gamma$	γ
$\gamma \to$	α	α	α	$-\alpha$
$\mathbf{2^{1/3}} \to$	$2^{1/3}\omega$	$2^{1/3}\omega$	$2^{1/3}\omega$	$2^{1/3}\omega$
$\boldsymbol{\omega} \to$	ω	ω	ω	ω
$\mathbf{\sqrt{6}i} \to$	$\sqrt{6}i$	$-\sqrt{6}i$	$-\sqrt{6}i$	$-\sqrt{6}i$

$\alpha \to$	$-\beta$	$-\beta$	β	$-\beta$
$\beta \to$	$-\gamma$	γ	$-\gamma$	$-\gamma$
$\gamma \to$	α	$-\alpha$	$-\alpha$	$-\alpha$
$\mathbf{2^{1/3}} \to$	$2^{1/3}\omega$	$2^{1/3}\omega$	$2^{1/3}\omega$	$2^{1/3}\omega$
$\boldsymbol{\omega} \to$	ω	ω	ω	ω
$\mathbf{\sqrt{6}i} \to$	$\sqrt{6}i$	$\sqrt{6}i$	$\sqrt{6}i$	$-\sqrt{6}i$

I won't write out all 48 automorphisms, let alone describe the Galois group and the Galois correspondence. But let's look at some instances of fixed fields and fixing subgroups.

Which subgroup fixes $\mathbb{Q}[\alpha]$? Since $\mathbb{Q}[\alpha]$ has degree 6 over $\mathbb{Q}$ the subgroup, which we'll call H, must have order 8. The elements of H must either fix β^2 and γ^2 or they must swap them. Restricted to $\mathbb{Q}[x^3 = 2]$ they must fix $2^{1/3}$.

	1	**B**	**A^2B**	**A^2**	**A^3B**	**A**	**A^3**	**AB**
$\alpha \rightarrow$	α	α	α	α	α	α	α	α
$\beta \rightarrow$	β	$-\beta$	β	$-\beta$	γ	$-\gamma$	γ	$-\gamma$
$\gamma \rightarrow$	γ	γ	$-\gamma$	$-\gamma$	β	β	$-\beta$	$-\beta$
$2^{1/3} \rightarrow$	$2^{1/3}$	$2^{1/3}$	$2^{1/3}$	$2^{1/3}$	$2^{1/3}$	$2^{1/3}$	$2^{1/3}$	$2^{1/3}$
$\omega \rightarrow$	ω	ω	ω	ω	ω^2	ω^2	ω^2	ω^2
$\sqrt{6}i \rightarrow$	$\sqrt{6}i$	$-\sqrt{6}i$	$-\sqrt{6}i$	$\sqrt{6}i$	$\sqrt{6}i$	$-\sqrt{6}i$	$-\sqrt{6}i$	$\sqrt{6}i$
orders	1	2	2	2	2	4	4	2

It's easily checked that this group is

$$\langle \mathbf{A, B \mid A^4 = B^2 = 1, BA = A^{-1}B} \rangle,$$

the dihedral group $\mathbf{D}_8$. Since $\mathbb{Q}[\alpha]$ is not a polynomial extension of $\mathbb{Q}$ (it doesn't contain the algebraic conjugates β and γ) H is not a normal subgroup of G.

Now let's go in the other direction.
Let C be the automorphism that maps

$\alpha \to -\gamma$,
$\beta \to \gamma$,
$\gamma \to \alpha$.
This has order 6 and so if F is its fixed field then
|K/F| = 6. Hence *F* has degree 8 over $\mathbb{Q}$.

From a previous table C can be described as follows.

	C
$\boldsymbol{\alpha \to}$	$-\beta$
$\boldsymbol{\beta \to}$	γ
$\boldsymbol{\gamma \to}$	α
$\boldsymbol{2^{1/3} \to}$	$2^{1/3}\omega$
$\boldsymbol{\omega \to}$	ω
$\boldsymbol{\sqrt{6}i \to}$	$-\sqrt{6}i$

Apart from ω there is nothing else that is obviously fixed by C.
We have to do a bit of work. A basis for K over $\mathbb{Q}[x^3 = 2]$ is: $\{1, \alpha, \beta, \gamma, \alpha\beta, \beta\gamma, \alpha\gamma, \alpha\beta\gamma\}$.

Suppose $a + b\alpha + c\beta + d\gamma + e\alpha\beta + f\beta\gamma + g\alpha\gamma + h\alpha\beta\gamma$ is fixed by C, where *a*, *b*, ..., *h* are in $\mathbb{Q}[x^3 = 2]$. To simplify things let's suppose these coefficients are in $\mathbb{Q}$.
$a + b\alpha + c\beta + d\gamma + e\alpha\beta + f\beta\gamma + g\alpha\gamma + h\alpha\beta\gamma$
$= a - b\beta + c\gamma + d\alpha - e\beta\gamma + f\alpha\gamma - g\alpha\beta - h\alpha\beta\gamma$.
Equating corresponding coefficients we get
$b = c = d = h = 0$ and $e = -f = -g$.

So $X = \alpha\beta - \beta\gamma - \alpha\gamma$ is fixed by C.

We can see how this works. C sends each term to the next and the last to the first. We can adapt this to get $Y = (\alpha\beta - \beta\gamma\omega - \alpha\gamma\omega^2)2^{1/3}$ and $Z = (\alpha\beta - \beta\gamma\omega^2 - \alpha\gamma\omega)2^{2/3}$ in the fixed field.

F has degree 4 over $\mathbb{Q}[\omega]$ with a basis $\{1, X, Y, Z\}$ and hence has degree 8 over $\mathbb{Q}$ as we expected.

Now you may be worried that what we have described might not be a field. After all, where is XY? With some painstaking calculations we can show that all is well. For example $XY = 6\omega - \omega^2 Z + 2Y$.

§9.13. $f(x) = x^8 - 5x^4 - 7x^3 + 35$

$f(x) = x^8 - 5x^5 - 7x^3 + 35$ factorises as $(x^3 - 5)(x^5 - 7)$. The zeros are therefore:

$5^{1/3}$,
$5^{1/3}\omega$,
$5^{1/3}\omega^2$,
$7^{1/5}$,
$7^{1/5}\theta$,
$7^{1/5}\theta^2$,
$7^{1/5}\theta^3$,
$7^{1/5}\theta^4$,
$7^{1/5}\theta^5$,
$7^{1/5}\theta^6$ where $\omega = e^{2\pi i/3}$ and $\theta = e^{2\pi i/5}$.

Now $\mathbb{Q}[\omega, \theta] = \mathbb{Q}[\sigma]$ where $\sigma = e^{2\pi i/15}$.
The splitting field is $\mathbb{Q}[5^{1/3}, 7^{1/5}, \sigma]$.
Let r be the degree of $5^{1/3}$ over $\mathbb{Q}[7^{1/5}]$.
Then a product of r zeros of $x^3 - 5$ is in $\mathbb{Q}[7^{1/5}]$
and so $5^{r/3} \in \mathbb{Q}[7^{1/5}]$ and $\mathbb{Q}[5^{r/3}] \leq \mathbb{Q}[7^{1/5}]$.

If $r < 3$ then $\mathbb{Q}[5^{r/3}]$ has degree 3 over $\mathbb{Q}$, but 3 doesn't divide 5. Thus $r = 3$ and so $\mathbb{Q}[5^{1/3}, 7^{1/5}]$ has degree 15 over $\mathbb{Q}$.

The degree of σ over $\mathbb{Q}[5^{1/3}, 7^{1/5}]$ is the same as its degree over $\mathbb{Q}$ which is $\varphi(15) = 8$. The degree of the splitting field over $\mathbb{Q}$ is thus $15 \times 8 = 120$.

The Galois Group is generated by:

	A	**B**	**C**	**D**
$\mathbf{5^{1/3}\rightarrow}$	$5^{1/3}\sigma^5$	$5^{1/3}$	$5^{1/3}$	$5^{1/3}$
$\mathbf{7^{1/5}\rightarrow}$	$7^{1/5}$	$7^{1/5}\sigma^3$	$7^{1/5}$	$7^{1/5}$
$\boldsymbol{\sigma\rightarrow}$	σ	σ	σ^2	σ^{-1}

and the Galois group is:
$\mathbf{\langle A, B, C, D \mid A^3 = B^5 = C^4 = D^2 = 1, BA = AB, CA = A^{-1}C, DA = A^{-1}D, CB = B^3C, DB = B^{-1}D, DC = CD\rangle.}$
As this is a large group I'll omit the the subgroups and fixed fields.

§9.14. $\mathbf{f(x) = x^{30} - 30x^{15} + 216}$

$f(x) = x^{30} - 30x^{15} + 216$ factorises as $(x^{15} - 12)(x^{15} - 18)$ and so, if $\theta = e^{2\pi i/15}$, its zeros are:

$12^{1/15}\theta^n$, and $18^{1/15}\theta^n$ for $n = 0, 1, 2, \ldots, 14$.

The splitting field is $\mathbb{Q}[12^{1/15}, 18^{1/15}, \theta]$.
Now $2^{1/3} = \dfrac{(12^{1/15})^2}{18^{1/15}}$ so the splitting field is:

$$\mathbb{Q}[12^{1/15}, 2^{1/3}, \theta].$$

Let r be the degree of $12^{1/15}$ over $\mathbb{Q}[2^{1/3}]$.
Then a product of r zeros of $x^{15} - 12$ is in $\mathbb{Q}[2^{1/3}]$.
Hence $12^{r/15} \in \mathbb{Q}[2^{1/3}]$ and so $12^{r/15} = a + b2^{1/3} + c2^{2/3}$ for some $a, b, c \in \mathbb{Q}$.

Under the automorphism of $\mathbb{Q}[2^{1/3}, \omega]$ that maps $2^{1/3} \to 2^{1/3}\omega$ and fixes ω, $12^{r/15}$ must map to $12^{r/15}\theta^t$ for some t.

Thus 3 divides t and $12^{r/15} = 2^{s/3}(m/n)$ for some coprime integers m, n. So $12^r n^{15} = 2^s m^{15}$. Hence 15 divides r and so $r = 15$.
The degree of $\mathbb{Q}[12^{1/15}, 2^{1/3}, \theta]$ over $\mathbb{Q}$ is:

$$15 \times 3 \times 8 = 360.$$

The Galois group is generated by:

	A	**B**	**C**	**D**
$\mathbf{12^{1/15} \to}$	$12^{1/15}\theta$	$12^{1/15}$	$12^{1/15}$	$12^{1/15}$
$\mathbf{2^{1/3} \to}$	$2^{1/3}$	$2^{1/3}\theta^5$	$2^{1/3}$	$2^{1/3}$
$\mathbf{\theta \to}$	θ	θ	θ^2	θ^{-1}

The Galois group is thus:
$\langle \mathbf{A, B, C, D \mid A^{15} = B^3 = C^4 = D^2 \mid BA = AB, CA = A^8C, DA = A^{-1}D, CB = B^{-1}C, DB = B^{-1}D, DC = CD} \rangle$**.**

EXERCISES FOR CHAPTER 9

For Exercises 1 – 10 do the following.

(A) find the zeros of f(x);

(B) find the splitting field $\mathbb{Q}[f(x)]$ in the form:

$$\mathbb{Q}[\alpha_1, \alpha_2, ..., \alpha_k];$$

(C) find automorphisms of $\mathbb{Q}[f(x)]$ by describing their effects on the generators α_i.

(D) find a presentation of the Galois group

$$G = G(\mathbb{Q}[f(x)]/\mathbb{Q});$$

(E) where possible describe G as a cyclic or dihedral group or a direct product of these;

(F) find all the subgroups of G and all the corresponding fixed fields and identify the normal subgroups and write their fixed field explicitly as a polynomial extension.

Exercise 1: $f(x) = x^4 - 3x^2 - 10$.

Exercise 2: $f(x) = x^8 + x^6 + x^4 + x^2 + 1$.

Exercise 3: $f(x) = x^6 - 27$.

Exercise 4: $f(x) = x^{24} - 1$.

Exercise 5: $f(x) = x^4 + 3x^2 - 1$.

Exercise 6: $f(x) = x^4 - 6x^2 + 3$.

Exercise 7: $f(x) = x^4 - 6x^2 + 25$.

Exercise 8: $f(x) = x^6 + 3x^3 - 1$.

Exercise 9: $f(x) = x^6 - 18x^3 + 6$.

Exercise 10: $f(x) = x^{15} - 1$.

Exercise 11: Let $\theta = e^{2\pi i/7}$ and for $r = 1, 2, 3$ let

$$\alpha_r = \theta^r + \theta^{6r}.$$

Let $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.
(i) Show that $f(x)$ is a rational polynomial.
(ii) Find $G(\mathbb{Q}[f(x)]/\mathbb{Q})$.

SOLUTIONS FOR CHAPTER 9

Exercise 1: $x^4 - 3x^2 - 10 = (x^2 - 5)(x^2 + 2)$.
So $\mathbb{Q}[x^2 - 3x^2 - 10] = \mathbb{Q}[\sqrt{5}, \sqrt{2}i]$.
The automorphisms, and the effect on these generators, are:

	1	**A**	**B**	**AB**
$\sqrt{5} \rightarrow$	$\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$-\sqrt{5}$
$\sqrt{2}i \rightarrow$	$\sqrt{2}i$	$-\sqrt{2}i$	$\sqrt{2}i$	$-\sqrt{2}i$
orders	1	2	2	2

Hence $G(\mathbb{Q}[x^2 - 3x^2 - 10]/\mathbb{Q})$
$\cong \langle \mathbf{A, B \mid A^2 = B^2 = 1, BA = AB} \rangle \cong \mathbf{C_2 \times C_2}$.

The subgroups are 1, $\langle A \rangle$, $\langle B \rangle$ and G. The corresponding subfields are given by the following table.

$H \leq G$	$\triangleleft$	**$\lvert H \rvert$**	**H***	**poly extn**	**deg**
G	$\surd$	4	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A \rangle$	$\surd$	2	$\mathbb{Q}[\sqrt{5}]$	$\mathbb{Q}[x^2 - 5]$	2
$\langle B \rangle$	$\surd$	2	$\mathbb{Q}[\sqrt{2}\, i]$	$\mathbb{Q}[x^2 + 2]$	2
$\langle AB \rangle$	$\surd$	2	$\mathbb{Q}[\sqrt{10}\, i]$	$\mathbb{Q}[x^2 + 10]$	2
1	$\surd$	1	$\mathbb{Q}[\sqrt{5}, \sqrt{2}i]$	$\mathbb{Q}[f(x)]$	4

Exercise 2: $(x^2 - 1)(x^8 + x^6 + x^4 + x^2 + 1)$

$= (x^2)^5 - 1 = x^{10} - 1.$

Hence $\mathbb{Q}[x^8 + x^6 + x^4 + x^2 + 1] = \mathbb{Q}[x^{10} - 1] \cong \mathbb{Z}_{10}^{\#}$.

$\mathbb{Z}_{10}^{\#} = \{1, 3, 7, 9\}$. Since $3^2 = 9 \bmod 10$, $\mathbb{Z}_{10}^{\#} \cong C_4$.

Hence $G(\mathbb{Q}[x^8 + x^6 + x^4 + x^2 + 1 = 0]/\mathbb{Q}) \cong \mathbf{C_4}$.

Let $\alpha = e^{2\pi i/10}$ and let A be the automorphism that takes α to α^3. This generates the Galois group.

A^2 takes α to $\alpha^9 = \alpha^{-1}$ and fixes

$\alpha + \alpha^{-1} = 2\cos(2\pi/10) = 2\cos(\pi/5)$.

Since $\langle A^2 \rangle$ has index 2 in the Galois group the fixed field has degree 2 over $\mathbb{Q}$.

We need to check that $2\cos(\pi/5)$ is not rational.

Let $c = \cos(\pi/5)$ and $s = \sin(\pi/5)$.

Then $(c + is)^5 = \cos(\pi) + i \sin(\pi) = -1$.

Hence $c^5 + 5ic^4s - 10c^3s^2 - 10ic^2s^3 + is^4 = -1$.

Equating real parts we get $5c^4s - 10c^2s^3 + s^5 = 0$.

Since $s \neq 0$ this gives $5c^4 - 10c^2s^2 + s^4 = 0$.

Hence $5c^4 - 10c^2(1 - c^2) + (1 - c^2)^2 = 0$.

So $16c^4 - 12c^2 + 1 = 0$.

Therefore $c^2 = \dfrac{12 \pm \sqrt{80}}{32} = \dfrac{3 \pm \sqrt{5}}{8}$

It's not difficult to reject $\dfrac{3 - \sqrt{5}}{8}$ so $c^2 = \dfrac{3 + \sqrt{5}}{8}$.

Since $\sqrt{5}$ is irrational, so is c^2 and hence c.

The fixed field that corresponds to $\langle A^2 \rangle$ must therefore be $\mathbb{Q}[\cos(\pi/5)]$.

Now it might seem that the minimum polynomial of $\cos(\pi/5)$ is $(8x^2 - 3)^2 - 5$, but if so then the degree of $\mathbb{Q}[\cos(\pi/5)]$ would be 4. Yet it has to be 2 since the index of $\langle A^2 \rangle$ in the Galois group is only 2.

This is resolved when we observe that:

$$\left(\frac{1+\sqrt{5}}{4}\right)^2 = \frac{3+\sqrt{5}}{8} = c^2.$$

So $\cos(\pi/5) = \dfrac{1+\sqrt{5}}{4}$

Its minimum polynomial is $(4x - 1)^2 - 5$ made monic, is therefore $x^2 - \frac{1}{2}x - \frac{1}{4}$.

One thing remains to be resolved.
We showed that $\alpha = e^{\pi i/5}$ is a zero of $x^8 + x^6 + x^4 + x^2 + 1$, but since the degree of $\mathbb{Q}[f(x)]$ over $\mathbb{Q}$ is 4 this can't possibly be the minimum polynomial.

The zeros of $x^8 + x^6 + x^4 + x^2 + 1$ are α, α^2, α^3, α^4, α^6, α^7, α^8 and α^9 (not $\alpha^5 = -1$).
Now α^2, α^4, α^6 and α^8 are 5^{th} roots of 1 and hence are the zeros of $x^4 + x^3 + x^2 + x + 1$. Dividing $x^8 + x^6 + x^4 + x^2 + 1$ by $x^4 + x^3 + x^2 + x + 1$ we get $x^4 - x^3 + x^2 - x + 1$ and this must be the minimum polynomial of α. We don't need to check that it's prime because we know from the Galois groups that $\mathbb{Q}[\alpha]$ must have degree 4 over $\mathbb{Q}$.

The Galois group is $\langle A \mid A^4 \rangle \cong \mathbf{C}_4$.

The subgroups of the Galois group and the corresponding fields are given as follows:

$H \leq G$	$\triangleleft$	$\lvert H\rvert$	H^*	poly extn	deg
G	$\surd$	4	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A^2 \rangle$	$\surd$	2	$\mathbb{Q}[\cos(\pi/5)]$	$\mathbb{Q}[4x^2 - 2x - 1]$	2
1	$\surd$	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	4

Exercise 3: $x^6 - 27 = (x^2 - 3)(x^4 + 3x^2 + 9)$.
The zeros of $x^2 - 3$ are $\pm\sqrt{3}$ and the zeros of $x^4 + 3x^2 + 9$ are $\pm\sqrt{\dfrac{-3 \pm 3\sqrt{3}i}{2}}$.
Hence $\mathbb{Q}[x^6 - 27] = \mathbb{Q}[\sqrt{3}, \alpha, \beta]$ where
$\alpha = \sqrt{\dfrac{-3 + 3\sqrt{3}i}{2}}$ and $\beta = \sqrt{\dfrac{-3 - 3\sqrt{3}i}{2}}$.
Note that $\sqrt{\dfrac{-3 + 3\sqrt{3}i}{2}}$ and $\sqrt{\dfrac{-3 - 3\sqrt{3}i}{2}}$ are not uniquely defined because, for a start, there are two square roots of $\sqrt{3}i$.

But $(\alpha\beta)^2 = 9$ (the product of the zeros of $x^4 + 3x^2 + 9$) and we choose α, β so that $\alpha\beta = 3$.

Hence $\mathbb{Q}[x^6 - 27] = \mathbb{Q}[\alpha, \sqrt{3}]$.
Now $(\alpha + \beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta = -3 + 6 = 3$,
so $\alpha + \beta = \pm\sqrt{3}$.

The automorphisms, and the effect on these generators, as well as β are:

	1	**A**	**B**	**AB**
α →	α	−α	β	−β
√3 →	√3	−√3	√3	−√3
β →	β	−β	α	−α
√3i →	√3i	√3i	−√3i	−√3i
i →	i	−i	−i	I
orders	1	2	2	2

The Galois group is $\langle \mathbf{A, B \mid A^2, B^2, BA = AB} \rangle \cong \mathbf{C_2 \times C_2}$. The subgroups of the Galois group and the corresponding fields are as follows:

H≤ G	**◁**	**|H|**	**H***	**poly extn**	**deg**
G	√	4	$\mathbb{Q}$	$\mathbb{Q}$	1
⟨A⟩	√	2	$\mathbb{Q}[\sqrt{3}i]$	$\mathbb{Q}[x^2 + 3]$	2
⟨B⟩	√	2	$\mathbb{Q}[\sqrt{3}]$	$\mathbb{Q}[x^2 - 3]$	2
⟨AB⟩	√	2	$\mathbb{Q}[i]$	$\mathbb{Q}[x^2 + 1]$	2
1	√	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	4

Exercise 4: $\mathbb{Q}[x^{24} = 1] = \mathbb{Q}[\alpha]$ where $\alpha = e^{2\pi i/24}$.
Under an automorphism in $G(\mathbb{Q}[x^{24} = 1]/\mathbb{Q})$ $\alpha \to \alpha^r$ where r is coprime with 24.
Thus $G(\mathbb{Q}[x^{24} = 1]/\mathbb{Q}) \cong \mathbb{Z}_{24}^{\#}$, the group of units of the ring $\mathbb{Z}_{24}$.

Now $\mathbb{Z}_{24}^{\#} = \{1, 5, 7, 11, 13, 17, 19, 23\}$
$= \{\pm 1, \pm 5, \pm 7, \pm 11\}$.

Mod 24 the square of each of these is 1 so
$G(\mathbb{Q}[x^{24} = 1]/\mathbb{Q}) \cong \mathbf{C_2 \times C_2 \times C_2}$.

Let A be the automorphism that maps α to α^5.
Let B be the automorphism that maps α to α^7.
Then AB maps α to α^{11}.
Let C be the automorphism that maps α to α^{-1}.

	1	**A**	**B**	**AB**	**C**	**AC**	**BC**	**ABC**
$\alpha \rightarrow$	α	α^5	α^7	α^{11}	α^{-1}	α^{-5}	α^{-7}	α^{-11}
orders	1	2	2	2	2	2	2	2

In finding the fixed fields it is easy to find numbers fixed by the automorphisms but we have to be careful that we have found enough to generate the fixed field. For example A clearly fixes $\alpha + \alpha^5$ (since it maps α^5 to $\alpha^{25} = \alpha$). But is $\mathbb{Q}[\alpha + \alpha^5]$ the whole of the fixed field?

ABC clearly fixes $\alpha + \alpha^{-11}$ and we might be tempted to say that $\mathbb{Q}[\alpha + \alpha^{-11}]$ is the fixed field of ABC until we realise that $\alpha^{12} = -1$ and so $\alpha + \alpha^{-11} = \alpha + \alpha^{13} = \alpha - \alpha = 0$. It's important to make sure that the degree of our subfield is right.

Things are a lot easier in this example if we find simpler generators for the splitting field. Since $\alpha^6 = i$, the

splitting field contains i. Since $\alpha^4 = e^{2\pi i/6} = \dfrac{1+\sqrt{3}i}{2}$ the splitting field contains $\sqrt{3}i$ and hence $\sqrt{3}$.

Since $\alpha^3 = \dfrac{1+i}{\sqrt{2}}$ the splitting field contains $\sqrt{2}$.

Now we know that the degree of the splitting field is 8, the order of the Galois group, so clearly $\mathbb{Q}[x^{24}-1] = \mathbb{Q}[i, \sqrt{2}, \sqrt{3}]$. Various powers of α can be expressed in terms of these generators as follows.

α^3	α^4	α^6	α^8	α^9	α^{12}
$\dfrac{1+i}{\sqrt{2}}$	$\dfrac{1+\sqrt{3}i}{2}$	i	$\dfrac{-1+\sqrt{3}i}{2}$	$\dfrac{-1+i}{\sqrt{2}}$	-1

α^{15}	α^{16}	α^{18}	α^{20}	α^{21}
$\dfrac{-1-i}{\sqrt{2}}$	$\dfrac{-1-\sqrt{3}i}{2}$	$-i$	$\dfrac{1-\sqrt{3}i}{2}$	$\dfrac{1-i}{\sqrt{2}}$

The effect of the automorphisms on these new generators is as follows.

	1	**A**	**B**	**AB**	**C**	**AC**	**BC**	**ABC**
$\alpha \rightarrow$	α	α^5	α^7	α^{11}	α^{-1}	α^{-5}	α^{-7}	α^{-11}
$\mathbf{i} \rightarrow$	i	i	$-i$	$-i$	$-i$	$-i$	i	$-i$
$\sqrt{2} \rightarrow$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3} \rightarrow$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$

It's now easy to find the fixed fields of all the subgroups of the splitting field.

$H \leq G$	$\triangleleft$	$\lvert H\rvert$	H^*	poly extn	deg
G	√	8	$\mathbb{Q}$	$\mathbb{Q}$	1
⟨A, B⟩	√	4	$\mathbb{Q}[i\sqrt{6}]$	$\mathbb{Q}[x^2 + 6]$	2
⟨A, C⟩	√	4	$\mathbb{Q}[\sqrt{6}]$	$\mathbb{Q}[x^2 - 6]$	2
⟨B, C⟩	√	4	$\mathbb{Q}[\sqrt{2}]$	$\mathbb{Q}[x^2 - 2]$	2
⟨A, BC⟩	√	4	$\mathbb{Q}[i]$	$\mathbb{Q}[x^2 + 1]$	2
⟨B, AC⟩	√	4	$\mathbb{Q}[i\sqrt{3}]$	$\mathbb{Q}[x^2 + 3]$	2
⟨AC, BC⟩	√	4	$\mathbb{Q}[i\sqrt{2}]$	$\mathbb{Q}[x^2 + 2]$	2
⟨C, AB⟩	√	4	$\mathbb{Q}[\sqrt{3}]$	$\mathbb{Q}[x^2 - 3]$	2
⟨A⟩	√	2	$\mathbb{Q}[i, \sqrt{6}]$	$\mathbb{Q}[(x^2 + 1)(x^2 - 6)]$	4
⟨B⟩	√	2	$\mathbb{Q}[\sqrt{2}, i\sqrt{3}]$	$\mathbb{Q}[(x^2 - 2)(x^2 + 3)]$	4
⟨AB⟩	√	2	$\mathbb{Q}[i\sqrt{2}, \sqrt{3}]$	$\mathbb{Q}[(x^2 + 2)(x^2 - 3)]$	4
⟨C⟩	√	2	$\mathbb{Q}[\sqrt{2}, \sqrt{3}]$	$\mathbb{Q}[(x^2 - 2)(x^2 - 3)]$	4
⟨AC⟩	√	2	$\mathbb{Q}[i\sqrt{2}, i\sqrt{3}]$	$\mathbb{Q}[(x^2 + 2)(x^2 + 3)]$	4
⟨BC⟩	√	2	$\mathbb{Q}[i, \sqrt{2}]$	$\mathbb{Q}[(x^2 + 1)(x^2 - 2)]$	4
⟨ABC⟩	√	2	$\mathbb{Q}[i\sqrt{2}, \sqrt{3}]$	$\mathbb{Q}[(x^2 + 2)(x^2 - 3)]$	4
1	√	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	8

Exercise 5: If $x^4 + 3x^2 - 1 = 0$ then

$$x^2 = \frac{-3 \pm \sqrt{9 + 4}}{2} = \frac{-3 \pm \sqrt{13}}{2}.$$

So the zeros of $x^4 + 3x^2 - 1$ are $\pm\sqrt{\dfrac{-3 \pm \sqrt{13}}{2}}$.

Hence $\mathbb{Q}[x^4 + 3x^2 - 1 = 0] = \mathbb{Q}[\alpha, \beta]$ where $\alpha = \sqrt{\frac{-3 + \sqrt{13}}{2}}$ and $\beta = \sqrt{\frac{3 + \sqrt{13}}{2}}\,i$.

Now $\alpha\beta = \sqrt{\frac{13 - 9}{4}}\,i = i$.

Hence $\mathbb{Q}[x^4 + 3x^2 - 1 = 0] = \mathbb{Q}[i, \alpha]$.

The automorphisms, and the effect on i, $\sqrt{13}$, α and β are:

	1	$\mathbf{A^2}$	**B**	$\mathbf{A^2B}$
i $\rightarrow$	i	i	i	i
$\boldsymbol{\alpha} \rightarrow$	α	$-\alpha$	β	$-\beta$
$\boldsymbol{\beta} \rightarrow$	β	$-\beta$	α	$-\alpha$
$\boldsymbol{\sqrt{13}} \rightarrow$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$
orders	1	2	2	2

	AB	$\mathbf{A^3B}$	**A**	$\mathbf{A^3}$
i $\rightarrow$	$-i$	$-i$	$-i$	$-i$
$\boldsymbol{\alpha} \rightarrow$	α	$-\alpha$	β	$-\beta$
$\boldsymbol{\beta} \rightarrow$	$-\beta$	β	$-\alpha$	α
$\boldsymbol{\sqrt{13}} \rightarrow$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$
orders	2	2	4	4

Now $BA = A^3B = A^{-1}B$.

So $G(\mathbb{Q}[x^4 + 3x^2 - 1 = 0]/\mathbb{Q})$

$= \langle \mathbf{A, B \mid A^4 = B^2 = 1, BA = A^{-1}B} \rangle \cong \mathbf{D_8}$.

The subgroups of the Galois group and the corresponding fields are given in the following table.

$H \leq G$	$\triangleleft$	$\lvert H\rvert$	H^*	poly extn	deg
G	√	8	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A \rangle$	√	4	$\mathbb{Q}[\sqrt{13}\, i]$	$\mathbb{Q}[x^2 + 13]$	2
$\langle A^2 \rangle$	√	2	$\mathbb{Q}[i, \sqrt{13}]$	$\mathbb{Q}[(x^2 + 1)(x^2 - 13)]$	4
$\langle B \rangle$		2	$\mathbb{Q}[\alpha + \beta]$		4
$\langle AB \rangle$		2	$\mathbb{Q}[\alpha]$		4
$\langle A^2B \rangle$		2	$\mathbb{Q}[\sqrt{13}(\alpha + \beta)]$		4
$\langle A^3B \rangle$		2	$\mathbb{Q}[\beta]$		4
1	√	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	8

To justify the fixed fields we need to check that α, β, $\alpha + \beta$ and $\sqrt{13}(\alpha + \beta)$ have degree 4 over $\mathbb{Q}$.

Since $\sqrt{13} = 2\alpha^2 + 3$, $\mathbb{Q}[\sqrt{13}] \leq \mathbb{Q}[\alpha]$.
But $\alpha \notin \mathbb{Q}[\sqrt{13}]$ (why?) so $|\mathbb{Q}[\alpha]/\mathbb{Q}| = 4$.
Similarly $|\mathbb{Q}[\beta]/\mathbb{Q}| = 4$.

Since $(\alpha + \beta)^2 = -3 + 2i$, $\mathbb{Q}[i] \leq \mathbb{Q}[\alpha + \beta]$.
But $\alpha + \beta \notin \mathbb{Q}[i]$ so $|\mathbb{Q}[\alpha + \beta]/\mathbb{Q}| = 4$.
Since $(\sqrt{13}(\alpha + \beta))^2 = -39 + 26i$, $\mathbb{Q}[i] \leq \mathbb{Q}[\sqrt{13}(\alpha + \beta)]$.
But $\sqrt{13}(\alpha + \beta) \notin \mathbb{Q}[i]$ so $|\mathbb{Q}[\sqrt{13}(\alpha + \beta)]/\mathbb{Q}| = 4$.

Exercise 6:
The polynomial $f(x) = x^4 - 6x^2 + 3$ is a quadratic in x^2 with zeros $\pm\sqrt{3 \pm \sqrt{6}}$.

The splitting field is $\mathbb{Q}[\alpha, \beta]$ where:

$$\alpha = \sqrt{3 + \sqrt{6}} \text{ and } \beta = \sqrt{3 - \sqrt{6}}\,.$$

Since $x^4 - 6x^2 + 3$ is prime by Eisenstein's Theorem

$$|\mathbb{Q}[\alpha]/\mathbb{Q}| = 4 \text{ and } |\mathbb{Q}[\beta]/\mathbb{Q}| = 4.$$

This might suggest that $|\mathbb{Q}[\alpha, \beta]/\mathbb{Q}| = 16$. But that would require the Galois group, necessarily a subgroup of $\mathbf{S}_4$, to have order 16 and this doesn't divide 24. The explanation is that while the minimum polynomial of β over $\mathbb{Q}$ has degree 4, its minimum polynomial over $\mathbb{Q}[\alpha]$ is a quadratic. Note that $\alpha\beta = \sqrt{9 - 6} = \sqrt{3}$, so $\beta = \sqrt{3}/\alpha$ and so $\beta^2 - 3/\alpha^2 = 0$.

That would mean that $|\mathbb{Q}[\alpha, \beta]/\mathbb{Q}[\alpha]| = 2$ and hence $|\mathbb{Q}[\alpha, \beta]/\mathbb{Q}| = 8$ provided that $x^2 - 3/\alpha^2$ is the minimum polynomial of β over $\mathbb{Q}[\alpha]$. But is it? Could it be that β already belongs to $\mathbb{Q}[\alpha]$? Let's suppose that $\beta \in \mathbb{Q}[\alpha]$ and see if this leads to a contradiction.

If so, then $\alpha\beta = \sqrt{3} \in \mathbb{Q}[\alpha]$. But $\alpha^2 \in \mathbb{Q}[\alpha]$ and hence $\sqrt{6}$ and $\sqrt{2}$ belong to $\mathbb{Q}[\alpha]$.

Clearly this would mean that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. (It's fairly straightforward to show that $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ and hence that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$).

Thus, based on our assumption,

$\sqrt{3 + \sqrt{6}} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ for some rational numbers a, b, c, d.

Squaring:

$$3 + \sqrt{6} = a^2 + 2b^2 + 3c^2 + 6d^2 + 2ab\sqrt{2} + 2ac\sqrt{3} + 2ad\sqrt{6} + 2bc\sqrt{6} + 2bd\sqrt{12} + 2cd\sqrt{18}$$
$$= a^2 + 2b^2 + 3c^2 + 6d^2 + (2ab + 6cd)\sqrt{2} + (2ac + 4bd)\sqrt{3} + (2ad + 2bc)\sqrt{6}.$$

We can equate corresponding coefficients since 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ are linearly independent over $\mathbb{Q}$ and so:

$$a^2 + 2b^2 + 3c^2 + 6d^2 = 3;$$
$$ab + cd = 0;$$
$$ac + bd = 0;$$
$$ad + bc = 1.$$

We have to show that this system of non-linear equations has no rational zeros.

Suppose there is a solution for a, b, c, d rational.

Adding the middle two we get $(a + d)(b + c) = 0$.

Case I: $a + d = 0$: The system reduces to the following:

$$7a^2 + 2b^2 + 3c^2 = 3;$$
$$a(b - c) = 0;$$
$$-a^2 + bc = 1$$

Case IA: $a = 0$: Here we have $2b^2 + 3c^2 = 3$ and $bc = 1$ and so c = 1/b. The first equation becomes:

$2b^2 + 3/b^2 = 3$, which simplifies to $2b^4 + 3b^2 - 3 = 0$.

By Eisenstein's Theorem $2x^4 + 3x^2 - 3$ is prime over $\mathbb{Q}$ and so has no rational zeros. So this case leads to a contradiction.

Case IB: $a \neq 0$: Then $b = c$ from the middle equation and so $7a^2 + 5b^2 = 3$ and $b^2 - a^2 = 1$. Adding, 7 times to second to the first we get $12b^2 = 10$, or $b^2 = 5/6$. But $\sqrt{\frac{5}{6}}$ is irrational, so again we get a contradiction.

Case II: $b + c = 0$: In this case the system reduces to:

$$a^2 + 5b^2 + 6d^2 = 3;$$
$$b(a - d) = 0;$$
$$ad - b^2 = 1.$$

Case IIA: $b = 0$: Then $a^2 + 6d^2 = 3$ and $ad = 1$ and so $a^4 - 3a^2 + 6 = 0$. But, by Eisenstein's Theorem $x^4 - 3x^2 + 6$ is prime over $\mathbb{Q}$ and so has no rational zeros.

Case IIB: $b \neq 0$: Then $a = d$ and so:

$$7a^2 + 5b^2 = 3 \text{ and } a^2 - b^2 = 1.$$

From this we conclude that $12a^2 = 8$ which is not possible if a is rational.

So, in fact, $\beta \notin \mathbb{Q}[\alpha]$ and hence $|\mathbb{Q}[\alpha, \beta]/\mathbb{Q}| = 8$ (consistent with the Galois group being a subgroup of $\mathbf{S}_4$). The only subgroups of $\mathbf{S}_4$ with order 8 are those isomorphic to $\mathbf{D}_8$ so the Galois group here must be $\mathbf{D}_8$. But if we wish to examine the connection between the subgroups and fixed fields we need to list the automorphisms. Now while α can map to any one of the four possibilities $\pm\alpha$, $\pm\beta$, once α^θ has been chosen we must map β to $\pm\sqrt{3}/\alpha^\theta$. Thus if α maps to $\pm\alpha$, β must map

to $\pm\beta$ and if α maps to $\pm\beta$, β must map to $\pm\alpha$. The eight automorphisms are given by the following table:

	1	**B**	$\mathbf{A^2B}$	$\mathbf{A^2}$	$\mathbf{A^3B}$	**A**	$\mathbf{A^3}$	**AB**
$\boldsymbol{\alpha\rightarrow}$	α	α	$-\alpha$	$-\alpha$	β	β	$-\beta$	$-\beta$
$\boldsymbol{\beta\rightarrow}$	β	$-\beta$	β	$-\beta$	α	$-\alpha$	α	$-\alpha$
order	1	2	2	2	2	4	4	2

So the Galois group is $\langle \mathbf{A, B \mid A^4, B^2, BA = A^{-1}B} \rangle \cong \mathbf{D_8}$.

We can use the relationships $\alpha\beta = \sqrt{3}$ and $\alpha^2 = 3 + \sqrt{6}$ to produce additional rows to the table:

	1	**B**	$\mathbf{A^2B}$	$\mathbf{A^2}$	$\mathbf{A^3B}$	**A**	$\mathbf{A^3}$	**AB**
$\boldsymbol{\sqrt{3}\rightarrow}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$
$\boldsymbol{\sqrt{6}\rightarrow}$	$\sqrt{6}$	$\sqrt{6}$	$\sqrt{6}$	$\sqrt{6}$	$-\sqrt{6}$	$-\sqrt{6}$	$-\sqrt{6}$	$-\sqrt{6}$
$\boldsymbol{\sqrt{2}\rightarrow}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$

The Galois group is thus:

$$\langle \mathbf{A, B \mid A^4 = B^2 = 1, BA = A^{-1}B} \rangle \cong \mathbf{D_8}.$$

The subgroups and the corresponding fixed fields are given by the following table.

H≤ G	$\triangleleft$	**|H|**	**H***	**poly extn**	**deg**
G	$\surd$	8	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A \rangle$	$\surd$	4	$\mathbb{Q}[\sqrt{2}]$	$\mathbb{Q}[x^2 - 2]$	2
$\langle A^2, B \rangle$	$\surd$	4	$\mathbb{Q}[\sqrt{6}]$	$\mathbb{Q}[x^2 - 6]$	2

$\langle A^2, AB\rangle$	√	4	$\mathbb{Q}[\sqrt{3}]$	$\mathbb{Q}[x^2 - 3]$	2
$\langle A^2\rangle$	√	2	$\mathbb{Q}[\sqrt{2}, \sqrt{3}]$	$\mathbb{Q}[(x^2 - 2)(x^2 - 3)]$	4
$\langle B\rangle$		2	$\mathbb{Q}[\alpha]$		4
$\langle A^2B\rangle$		2	$\mathbb{Q}[\beta]$		4
$\langle AB\rangle$		2	$\mathbb{Q}[\alpha - \beta]$		4
$\langle A^3B\rangle$		2	$\mathbb{Q}[\alpha + \beta]$		4
1	√	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	8

Exercise 7:

If $f(x) = 0$ then $x^2 = \dfrac{6 \pm \sqrt{36 - 100}}{2} = 3 \pm 4i$.

The zeros of $f(x)$ are $\pm\alpha, \pm\beta$ where:

$$\alpha^2 = 3 + 4i \text{ and } \beta^2 = 3 - 4i.$$

Since $(\alpha\beta)^2 = 25$ we may choose α, β so that $\alpha\beta = 5$.
Hence $\mathbb{Q}[f(x)] = \mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\alpha]$.

Now it appears that $\mathbb{Q}[\alpha]$ has degree 4 over $\mathbb{Q}$, although attempts to prove that $x^2 - 6x^2 + 25$ is prime don't seem to be successful.

Let's proceed on the assumption that $x^2 - 6x^2 + 25$ is the minimum polynomial of α.

The automorphisms of $\mathbb{Q}[\alpha]$ would be as follows.

	1	**A**	**B**	**AB**
$\boldsymbol{\alpha \to}$	α	$-\alpha$	β	$-\beta$
$\mathbf{i} \to$	i	i	–i	–i
$\boldsymbol{\beta \to}$	β	β	α	α
orders	1	2	2	2

This would give $G(\mathbb{Q}[f(x)]/\mathbb{Q})$
$= \langle A, B \mid A^2, B^2, BA = AB \rangle \cong \mathbf{C}_2 \times \mathbf{C}_2$.

Now $(\alpha + \beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta = 16$ so $\alpha + \beta = \pm 4$. Alarm bells should be starting to ring! The fixed field of $\langle B \rangle$ would appear to be $\mathbb{Q}[\alpha + \beta]$ but this is just $\mathbb{Q}$.

If $\alpha + \beta = 4$ and $\alpha\beta = 5$ then $\alpha(4 - \alpha) = 5$ and so α satisfies a quadratic!

It must be that $x^4 - 6x^2 + 25$ factorises over $\mathbb{Q}$. In fact $x^4 - 6x^2 + 25 = (x^2 - 2x + 5)(x^2 + 2x + 5)$ and the zeros are $\pm 1 \pm 2i$.

Hence $\mathbb{Q}[x^4 - 6x^2 + 25] = \mathbb{Q}[i]$ and the Galois group is

$$\langle \mathbf{A} \mid \mathbf{A^2} \rangle \cong \mathbf{C_2}.$$

The fixed fields are as follows.

H≤ G	**◁**	**|H|**	**H***	**poly extn**	**deg**
G	√	2	$\mathbb{Q}$	$\mathbb{Q}$	1
1	√	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	2

Exercise 8: If $x^6 + 3x^3 - 1 = 0$ then $x^3 = \dfrac{-3 \pm \sqrt{13}}{2}$.

So the zeros of $x^6 + 3x^3 - 1$ are
$\left(\dfrac{-3 \pm \sqrt{13}}{2}\right)^{1/3}$, $\left(\dfrac{-3 \pm \sqrt{13}}{2}\right)^{1/3}\omega$ and $\left(\dfrac{-3 \pm \sqrt{13}}{2}\right)^{1/3}\omega^2$.

Hence $\mathbb{Q}[x^6 + 3x^3 - 1] = \mathbb{Q}[\alpha, \beta, \omega]$ where
$\alpha = \left(\dfrac{-3 + \sqrt{13}}{2}\right)^{1/3}$ and $\beta = -\left(\dfrac{3 + \sqrt{13}}{2}\right)^{1/3}$.

Now $\alpha\beta = \left(\dfrac{9 - 13}{4}\right)^{1/3} = -1$.

Hence $\mathbb{Q}[x^6 + 3x^3 - 1] = \mathbb{Q}[\alpha, \omega]$.

The automorphisms are as follows.

	1	$\mathbf{A^2}$	$\mathbf{A^4}$	**B**	$\mathbf{A^2B}$	$\mathbf{A^4B}$
$\alpha \rightarrow$	α	$\alpha\omega$	$\alpha\omega^2$	β	$\beta\omega$	$\beta\omega^2$
$\omega \rightarrow$	ω	ω	ω	ω	ω	ω
$\beta \rightarrow$	β	$\beta\omega^2$	$\beta\omega$	α	$\alpha\omega^2$	$\alpha\omega$
$\sqrt{13} \rightarrow$	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$
orders	1	3	3	2	2	2

	$\mathbf{A^3B}$	**AB**	$\mathbf{A^5B}$	$\mathbf{A^3}$	**A**	$\mathbf{A^5}$
$\alpha \rightarrow$	α	$\alpha\omega$	$\alpha\omega^2$	β	$\beta\omega$	$\beta\omega^2$
$\omega \rightarrow$	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2
$\beta \rightarrow$	β	$\beta\omega^2$	$\beta\omega$	α	$\alpha\omega^2$	$\alpha\omega$
$\sqrt{13} \rightarrow$	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$
orders	2	2	2	2	6	6

Now $BA = A^5B = A^{-1}B$.
So $G(\mathbb{Q}[x^6 + 3x^3 - 1]/\mathbb{Q})$
$= \langle \mathbf{A, B \mid A^6 = B^2 = 1, BA = A^{-1}B} \rangle \cong \mathbf{D_{12}}$.

Since $\omega = \dfrac{-1 + \sqrt{3}\mathrm{i}}{2}$ it would be interesting to see the effect of these automorphisms on $\sqrt{3}\mathrm{i}$.

	1	$\mathbf{A^2}$	$\mathbf{A^4}$	**B**	$\mathbf{A^2B}$	$\mathbf{A^4B}$
$\alpha \to$	α	$\alpha\omega$	$\alpha\omega^2$	β	$\beta\omega$	$\beta\omega^2$
$\omega \to$	ω	ω	ω	ω	ω	ω
$\beta \to$	β	$\beta\omega^2$	$\beta\omega$	α	$\alpha\omega^2$	$\alpha\omega$
$\sqrt{13} \to$	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$
$\sqrt{3}\mathrm{i} \to$	$\sqrt{3}\mathrm{i}$	$\sqrt{3}\mathrm{i}$	$\sqrt{3}\mathrm{i}$	$\sqrt{3}\mathrm{i}$	$\sqrt{3}\mathrm{i}$	$\sqrt{3}\mathrm{i}$

	$\mathbf{A^3B}$	**AB**	$\mathbf{A^5B}$	$\mathbf{A^3}$	**A**	$\mathbf{A^5}$
$\alpha \to$	α	$\alpha\omega$	$\alpha\omega^2$	β	$\beta\omega$	$\beta\omega^2$
$\omega \to$	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2
$\beta \to$	β	$\beta\omega^2$	$\beta\omega$	α	$\alpha\omega^2$	$\alpha\omega$
$\sqrt{13} \to$	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$	$-\sqrt{13}$
$\sqrt{3}\mathrm{i} \to$	$-\sqrt{3}\mathrm{i}$	$-\sqrt{3}\mathrm{i}$	$-\sqrt{3}\mathrm{i}$	$-\sqrt{3}\mathrm{i}$	$-\sqrt{3}\mathrm{i}$	$-\sqrt{3}\mathrm{i}$

Now $\alpha + \beta$ is a zero of $x^3 + 3x + 3$, and so are $\alpha\omega + \beta\omega^2$ and $\alpha\omega^2 + \beta\omega$. All three are fixed by A^3.
Hence the fixed field of A^3 contains $\mathbb{Q}[x^3 + 3x + 3]$.
It also contains $\mathbb{Q}[\sqrt{39}\mathrm{i}] = \mathbb{Q}[x^2 + 39]$.
Hence the fixed field is $\mathbb{Q}[(x^3 + 3x + 3)(x^2 + 39)]$.

$H \leq G$	$\triangleleft$	$\lvert H\rvert$	H^*	poly extn	deg
G	$\surd$	12	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A\rangle$	$\surd$	6	$\mathbb{Q}[\sqrt{13}\,i]$	$\mathbb{Q}[x^2 + 13]$	2
$\langle A^2\rangle$	$\surd$	3	$\mathbb{Q}[i, \sqrt{13}]$	$\mathbb{Q}[(x^2 + 1)(x^2 - 13)]$	4
$\langle A^3\rangle$	$\surd$	2	$\mathbb{Q}[\alpha + \beta, \sqrt{39}i]$	$\mathbb{Q}[(x^3 + 3x + 3)(x^2 + 39)]$	6
$\langle B\rangle$		2	$\mathbb{Q}[\alpha + \beta, \sqrt{3}i]$		6
$\langle AB\rangle$		2	$\mathbb{Q}[i\beta]$		6
$\langle A^2B\rangle$		2	$\mathbb{Q}[\sqrt{13}(\alpha + \beta)]$		6
$\langle A^3B\rangle$		2	$\mathbb{Q}[i\alpha, \sqrt{13}]$		6
$\langle A^4B\rangle$		2	$\mathbb{Q}[\omega]$		6
$\langle A^5B\rangle$		2	$\mathbb{Q}[\sqrt{13}]$		6
1	$\surd$	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	12

Exercise 9:
The zeros of the polynomial $f(x) = x^6 - 18x^3 + 6$ (quadratic in x^3) are: α, $\alpha\omega$, $\alpha\omega^2$, β, $\beta\omega$, $\beta\omega^2$ where:
$\alpha = \sqrt[3]{9 + 5\sqrt{3}}$ and $\beta = \sqrt[3]{9 - 5\sqrt{3}}$, both of which are positive.

The splitting field is $F = \mathbb{Q}[\alpha, \beta, \omega]$.
Now $\sqrt{3} = \alpha^3 - 9 \in F$ and $\beta^3 - 9 = -\sqrt{3}$.
Also $\alpha\beta = \sqrt[3]{6}$ so $F = \mathbb{Q}[\alpha, \sqrt[3]{6}, \omega]$.

Now $|\mathbb{Q}[\alpha, \sqrt[3]{6}, \omega]/\mathbb{Q}[\alpha, \sqrt[3]{6}]| = 2$ and $|\mathbb{Q}[\alpha]/\mathbb{Q}| = 6$.
(By Eisenstein $x^6 - 18x^3 + 6$ is prime over $\mathbb{Q}$).

We expect the minimum polynomial of $\sqrt[3]{6}$ over $\mathbb{Q}[\alpha]$ to be $x^6 - 6$, in which case $|F:\mathbb{Q}|$ would be 18.

Suppose that $\sqrt[3]{6} \in \mathbb{Q}[\alpha]$. We expect to get a contradiction.

Since $\sqrt{3} \in \mathbb{Q}[\alpha]$ we may conclude that:
$\mathbb{Q}[\sqrt{3}, \sqrt[3]{6}\,] \leq \mathbb{Q}[\alpha]$ but since they both have degree 6 over $\mathbb{Q}$ it follows that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}, \sqrt[3]{6}\,]$. Then $|F/\mathbb{Q}| = 12$.

There are 12 automorphisms in the Galois group G of F over $\mathbb{Q}$, mapping:

$$\sqrt[3]{6} \to \sqrt[3]{6}\,,\ \sqrt[3]{6}\,\omega \text{ or } \sqrt[3]{6}\,\omega^2,$$
$$\sqrt{3} \to \sqrt{3} \text{ or } -\sqrt{3} \text{ and}$$
$$\omega \to \omega \text{ or } \omega^2,$$

in all 12 combinations.

Let θ map $\sqrt[3]{6}$ to $\sqrt[3]{6}\,\omega$ while fixing both $\sqrt{3}$ and ω.
Then θ has order 3, so $\langle\theta\rangle$ has order 3 and index 4 in G.
The fixed field of $\langle\theta\rangle$ must be $\mathbb{Q}[\sqrt{3}, \omega]$.

Under θ, $\alpha \to \alpha\omega^r$ or $\beta\omega^r$ for some r.
Now $\alpha \to \beta\omega^r$ is impossible. [For then $\alpha \to \beta\omega^r$, $\alpha^3 \to \beta^3$ and so $\sqrt{3} \to -\sqrt{3}$, a contradiction.]

But $\alpha \to \alpha$ is also impossible.
[For then $\alpha \in \mathbb{Q}[\sqrt{3}, \omega] \cap \mathbb{R} = \mathbb{Q}[\sqrt{3}]$, a contradiction.]

And $\alpha \to \alpha\omega$ is impossible too.
[For then $\beta \to \beta$ and so $\beta \in \mathbb{Q}[\sqrt{3}]$, a contradiction.]

The only possibility remaining is that $\alpha \to \alpha\omega^2$ under θ.
Then $\alpha^2\beta \to \alpha^2\beta$ since $\alpha^2\beta = \alpha\sqrt[3]{6}$.

But $\alpha^2\beta \in \mathbb{Q}[\sqrt{3}]$ so $\alpha^2\beta = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$.

Cubing we get $54 + 30\sqrt{3} = a^3 + 3b^3\sqrt{3} + 3a^2b\sqrt{3} + 9ab^2$.
Hence

$$a^3 + 9ab^2 = 54 \text{ and}$$
$$a^2b + b^3 = 10.$$

There's an automorphism ρ of $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{3}, \sqrt[3]{6}]$ that maps $\sqrt{3}$ to $-\sqrt{3}$, and fixes $\sqrt[3]{6}$.
Clearly ρ swaps α and β.
Now $\alpha\beta^2 = \beta\sqrt[3]{6} = a - b\sqrt{3}$.
Hence $6 = \alpha^3\beta^3 = a^2 - 3b^2$ whence $6b = a^2b - 3b^3$.

It follows that $6b = 10 - b^3 - 3b^3$. Thus

$$2b^3 + 3b - 5 = (b - 1)(2b^2 + 2b + 5) = 0.$$

The quadratic has no real zeros so $b = 1$ and hence

$$a = \pm 3.$$

In fact, since both α and β are positive, $a = 3$.

Hence $\sqrt[3]{6} = \alpha\beta = (\alpha^2\beta)/\alpha = \dfrac{3 + \sqrt{3}}{\alpha} \in \mathbb{Q}[\alpha, \sqrt{3}] = \mathbb{Q}[\alpha]$.

Of course this is based on the assumption that we have ended up with, so we appear to have a circular

argument. But our analysis has thrown up specific numbers and suggests that we evaluate:

$$(3 + \sqrt{3})^3 = 27 + 27\sqrt{3} + 27 + 3\sqrt{3} = 54 + 30\sqrt{3}.$$

Now $\alpha\sqrt[3]{6} = \sqrt[3]{(9+5\sqrt{3})(6)} = \sqrt[3]{54+30\sqrt{3}} = 3 + \sqrt{3}$ so in fact it *is* the case that $\sqrt[3]{6} \in \mathbb{Q}[\alpha]$.

A useful technique, if you are not sure whether something true or false, is suppose that it's true. Either you'll get a contradiction, in which case it is false, or you will get some specific information that might enable you to show that it is true.

Of course your proof that it's true mustn't rely on the assumption that it is true. It must be able to stand independently.

So $F = \mathbb{Q}[\sqrt[3]{6}, \sqrt{3}, \omega]$ and this has degree 12 over $\mathbb{Q}$.
The 12 automorphisms are given by:

	1	$\mathbf{A^4}$	$\mathbf{A^2}$	$\mathbf{A^3}$	**A**	$\mathbf{A^5}$
$\mathbf{6^{1/3}\rightarrow}$	$6^{1/3}$	$6^{1/3}\omega$	$6^{1/3}\omega^2$	$6^{1/3}$	$6^{1/3}\omega$	$6^{1/3}\omega^2$
$\mathbf{\sqrt{3}\rightarrow}$	$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$\mathbf{\omega\rightarrow}$	ω	ω	ω	ω	ω	ω
$\mathbf{i\rightarrow}$	i	i	i	–i	–i	–i
orders	1	3	3	2	6	6

	B	**A^2B**	**A^4B**	**A^3B**	**A^5B**	**AB**
$6^{1/3}\rightarrow$	$6^{1/3}$	$6^{1/3}\omega$	$6^{1/3}\omega^2$	$6^{1/3}$	$6^{1/3}\omega$	$6^{1/3}\omega^2$
$\sqrt{3}\rightarrow$	$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$\omega\rightarrow$	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2
$i\rightarrow$	$-i$	$-i$	$-i$	i	i	i
Orders	2	2	2	2	2	2

The Galois group is:

$$\langle A, B \mid A^6 = B^2 = 1, BA = A^{-1}B\rangle \cong D_{12}.$$

$H \leq G$	**$\triangleleft$**	**$\lvert H\rvert$**	**H***	**poly extn**	**deg**
G	$\surd$	12	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A\rangle$	$\surd$	6	$\mathbb{Q}[\omega]$	$\mathbb{Q}[x^2 + x + 1]$	2
$\langle A^2, B\rangle$	$\surd$	6	$\mathbb{Q}[\sqrt{3}]$	$\mathbb{Q}[x^2 - 3]$	2
$\langle A^2, AB\rangle$	$\surd$	6	$\mathbb{Q}[i]$	$\mathbb{Q}[x^2 + 1]$	2
$\langle A^3, B\rangle$		4	$\mathbb{Q}[6^{1/3}]$		3
$\langle A^3, AB\rangle$		4	$\mathbb{Q}[6^{1/3}\omega]$		3
$\langle A^3, A^2B\rangle$		4	$\mathbb{Q}[6^{1/3}\omega^2]$		3
$\langle A^2\rangle$	$\surd$	3	$\mathbb{Q}[\sqrt{3}, i]$	$\mathbb{Q}[(x^2 + 1)$ $(x^2 - 3)]$	4
$\langle A^3\rangle$	$\surd$	2	$\mathbb{Q}[6^{1/3}, \omega]$	$\mathbb{Q}[x^3 = 6]$	6
$\langle B\rangle$		2	$\mathbb{Q}[6^{1/3}, \sqrt{3}]$		6
$\langle AB\rangle$		2	$\mathbb{Q}[6^{1/3}\omega, i]$		6
$\langle A^2B\rangle$		2	$\mathbb{Q}[6^{1/3}\omega^2, \sqrt{3}]$		6
$\langle A^3B\rangle$		2	$\mathbb{Q}[6^{1/3}, i]$		6
$\langle A^4B\rangle$		2	$\mathbb{Q}[6^{1/3}\omega, \sqrt{3}]$		6
$\langle A^5B\rangle$		2	$\mathbb{Q}[6^{1/3}\omega^2, i]$		6
1	$\surd$	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	12

Exercise 10:
The zeros of $x^{15} - 1$ are $1, \theta, \theta^2, \ldots, \theta^{14}$ where $\theta = e^{2\pi i/15}$.
The splitting field is $\mathbb{Q}[\theta]$.
Under an automorphism θ can only map to θ^r where r is coprime with 15. Moreover all such possibilities arise. So the Galois group has order $\varphi(15) = 8$.

The automorphisms are:

	1	**A**	**A^2**	**A^3B**	**A^3**	**A^2B**	**AB**	**B**
$\theta \rightarrow$	θ	θ^2	θ^4	θ^7	θ^8	θ^{11}	θ^{13}	θ^{14}
order	1	4	2	4	4	2	4	2

The Galois group is:
$\langle \mathbf{A, B \mid A^4 = B^2 = 1, BA = AB} \rangle \cong \mathbf{C_4 \times C_2}$.

$H \leq G$	**$\triangleleft$**	**$\lvert H \rvert$**	**H***	**poly extn**	**deg**
G	√	12	$\mathbb{Q}$	$\mathbb{Q}$	1
$\langle A \rangle$	√	4			2
$\langle AB \rangle$	√	4			2
$\langle A^2, B \rangle$	√	4			2
$\langle A^2 \rangle$	√	2	$\mathbb{Q}[\omega]$		4
$\langle B \rangle$	√	2			4
$\langle A^2B \rangle$	√	2			4
1	√	1	$\mathbb{Q}[f(x)]$	$\mathbb{Q}[f(x)]$	8

Exercise 11:

(i) $\Sigma\alpha_i = \theta + \theta^2 + \theta^3 + \theta^4 + \theta^5 + \theta^6 = -1,$

$\Sigma\alpha_i\alpha_j = (\theta + \theta^6)(\theta^2 + \theta^5) + (\theta + \theta^6)(\theta^3 + \theta^4)$
$+ (\theta^2 + \theta^5)(\theta^3 + \theta^4)$

$= \theta^3 + \theta^6 + \theta^8 + \theta^{11} + \theta^4 + \theta^5 + \theta^9 + \theta^{10} + \theta^5 + \theta^6$
$+ \theta^8 + \theta^9$

$= \theta^3 + \theta^6 + \theta + \theta^4 + \theta^4 + \theta^5 + \theta^2 + \theta^3 + \theta^5 + \theta^6$
$+ \theta + \theta^2$

$= 2(\theta + \theta^2 + \theta^3 + \theta^4 + \theta^5 + \theta^6) = -2,$

$\alpha_1\alpha_2\alpha_3 = (\theta + \theta^6)(\theta^2 + \theta^5)(\theta^3 + \theta^4)$

$= \theta^6 + \theta^7 + \theta^9 + \theta^{10} + \theta^{11} + \theta^{12} + \theta^{14} + \theta^{15}$

$= \theta^6 + 1 + \theta^2 + \theta^3 + \theta^4 + \theta^5 + 1 + \theta = 1.$

Hence $f(x) = x^3 + x^2 - 2x - 1$.

(ii) The zeros of $f(x)$ are $= \theta + \theta^6$, $\theta^2 + \theta^5$ and $\theta^3 + \theta^4$. Under an automorphism of $\mathbb{Q}[\theta]$, θ maps to θ^r for r = 1, 2, 3, 4, 5, 6. However, restricted to $\mathbb{Q}[x^3 + x^2 - 2x - 1]$, these collapse to three automorphisms.

	1	**A**	**A²**
$\theta + \theta^6 \rightarrow$	$\theta + \theta^6$	$\theta^2 + \theta^5$	$\theta^3 + \theta^4$
$\theta^2 + \theta^5 \rightarrow$	$\theta^2 + \theta^5$	$\theta^3 + \theta^4$	$\theta^2 + \theta^5$
$\theta^3 + \theta^4 \rightarrow$	$\theta^3 + \theta^4$	$\theta + \theta^6$	$\theta^2 + \theta^5$

Hence $G(\mathbb{Q}[x^3 + x^2 - 2x - 1]/\mathbb{Q}) \cong \mathbf{C_3}$.