10. EXAMPLES OF GALOIS GROUPS

§10.1. The Fundamental Theorem of Galois Theory

In this chapter we are going to compute the Galois groups of a number of polynomial extensions. We will be building them up from the zeros of the polynomial, so in all these cases the polynomials will be soluble by radicals.

In the course of developing these examples we will be demonstrating some of the fundamental ideas of Galois Theory. These include some remarkable facts contained within the Fundamental Theorem of Galois Theory. We will be proving this theorem in a later chapter, but by seeing it in action first we will come to appreciate it better.

If K is a polynomial extension of a number field F then we can consider the subfields H that lie between them. We can also consider the Galois group G = G(K/F) and its subgroups.

The fundamental theorem shows that there is a 1-1 correspondence between the fields L with F ≤ L ≤ K and the subgroups H with 1 ≤ H ≤ G. This means that there are exactly as many subfields as there are subgroups.

The fixed field of 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 is 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 L1 ≤ L2 then L2# ≤ L1# (the more you have to fix, the fewer automorphisms will do that. And if H1 ≤ H2 then H2* ≤ H1* . 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 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 L1 ≤ L2 ≤ K then [L2:L1] = [L1#:L2#]. Equivalently, if H1 ≤ H2 ≤ G then [H2:H1] = [H1*:H2*].

Finally, polynomial extensions correspond to normal subgroups. If L2 is a polynomial extension of L1 then L2# is a normal subgroup of L1# and vice versa.

§10.2. f(x) = x^4 − x^2 − 2
(1) Factors: x^4 − x^2 − 2 = (x^2 − 2)(x^2 + 1).

(2) Zeros: ±√2, ±i

(3) Splitting field = F = Q[√2, −√2, i, −i] = Q[√2, i] = Q[i][√2].
(4) $|F:Q| = |F:Q[\sqrt{2}]| \times |Q[\sqrt{2}]:Q| = 2 \times 2 = 4.$

(5) The Galois group has order 4.

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

(7) All 4 combinations arise (since $|F : Q| = 4$).

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

<table>
<thead>
<tr>
<th>$\sqrt{2}$</th>
<th>$-\sqrt{2}$</th>
<th>$\sqrt{2}$</th>
<th>$-\sqrt{2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td>$i$</td>
<td>$-i$</td>
<td>$-i$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>order</th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
</table>

(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 $AB$, $\sqrt{2} \rightarrow -\sqrt{2} \rightarrow -\sqrt{2}$ and $i \rightarrow i \rightarrow -i$.]

Under $BA$, $\sqrt{2} \rightarrow \sqrt{2} \rightarrow -\sqrt{2}$ and $i \rightarrow -i \rightarrow -i$.

(12) The completed table is:

| $\sqrt{2}$ | $\sqrt{2}$ | $-\sqrt{2}$ | $\sqrt{2}$ | $-\sqrt{2}$ |
|------------|------------|-------------|------------|
| $i$        | $i$        | $-i$        | $-i$        |

<table>
<thead>
<tr>
<th>order</th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
</table>

The Galois group is thus isomorphic to $\langle A, B | A^2 = B^2, AB = BA \rangle \cong C_2 \times C_2$.

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

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>order</th>
<th>SUBFIELD</th>
<th>degree over Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$K$</td>
<td>4</td>
</tr>
<tr>
<td>$\langle A \rangle$</td>
<td>2</td>
<td>$Q[i]$</td>
<td>2</td>
</tr>
<tr>
<td>$\langle B \rangle$</td>
<td>2</td>
<td>$Q[\sqrt{2}]$</td>
<td>2</td>
</tr>
<tr>
<td>$\langle B \rangle$</td>
<td>2</td>
<td>$Q[i\sqrt{2}]$</td>
<td>2</td>
</tr>
<tr>
<td>$G$</td>
<td>4</td>
<td>$Q$</td>
<td>1</td>
</tr>
</tbody>
</table>

(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:

- $K = Q[x^4 - x^2 - 2 = 0]$;
- $Q[i] = Q[x^2 + 1 = 0]$;
- $Q[\sqrt{2}] = Q[x^2 - 2 = 0]$;
- $Q[i\sqrt{2}] = Q[x^2 + 2 = 0]$.

90
(17) Since we found all the subgroups we can be sure that their fixed fields give us all the possible subfields of $K$. The Galois correspondence can be illustrated as follows:

**SUBFIELDS OF $\mathbb{Q}[x^4 - x^2 - 2 = 0]$**

**SUBGROUPS OF $G(\mathbb{Q}[x^4 - x^2 - 2 = 0]/\mathbb{Q})$**

§10.3. $f(x) = x^3 - 2$

(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 $\omega$ over $\mathbb{Q}$ is $x^2 + x + 1$ and over $\mathbb{Q}[2^{1/3}]$ it is the same.

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

(6) The Galois group has order 6.

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

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

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

<table>
<thead>
<tr>
<th>$2^{1/3}$</th>
<th>$\omega$</th>
<th>$2^{1/3}\omega$</th>
<th>$2^{1/3}\omega^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega^2$</td>
</tr>
<tr>
<td>orders</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>$2^{1/3}$</th>
<th>$A$</th>
<th>$A^2$</th>
<th>$B$</th>
<th>$A^2B$</th>
<th>$AB$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
</tr>
<tr>
<td>orders</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

91
(13) \( BA = A^{-1}B \).
[Under \( BA \to 2^{1/3} \to 2^{1/3}\) and \( \omega \to \omega^2 \to \omega^2 \). This coincides with \( A^2B = A^{-1}B \).]

(14) The Galois group has the presentation \( \langle A, B \mid A^3, B^2, BA = A^{-1}B \rangle \) from which we see that it is isomorphic to \( D_6 \).

(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. Indeed it is. It is \( \mathbb{Q}[x^2 + x + 1 = 0] \).

(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) Since we found all the subgroups we can be sure that their fixed fields give us all the possible subfields of \( K \). The Galois correspondence can be illustrated as follows:

![Diagram showing subgroups and their fixed fields]

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>normal</th>
<th>order</th>
<th>SUBFIELD</th>
<th>poly ext’n</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>\checkmark</td>
<td>1</td>
<td>\mathbb{Q}[x^3 = 2]</td>
<td>\mathbb{Q}[x^3 = 2]</td>
<td>6</td>
</tr>
<tr>
<td>\langle B \rangle</td>
<td></td>
<td>2</td>
<td>\mathbb{Q}[2^{1/3}]</td>
<td>\mathbb{Q}[2^{1/3}]</td>
<td>3</td>
</tr>
<tr>
<td>\langle AB \rangle</td>
<td></td>
<td>2</td>
<td>\mathbb{Q}[2^{1/3} \omega]</td>
<td>\mathbb{Q}[2^{1/3} \omega]</td>
<td>3</td>
</tr>
<tr>
<td>\langle A^2B \rangle</td>
<td></td>
<td>2</td>
<td>\mathbb{Q}[2^{1/3} \omega^2]</td>
<td>\mathbb{Q}[2^{1/3} \omega^2]</td>
<td>3</td>
</tr>
<tr>
<td>\langle A \rangle</td>
<td>\checkmark</td>
<td>3</td>
<td>\mathbb{Q}[\omega]</td>
<td>\mathbb{Q}[x^2 + x + 1 = 0]</td>
<td>2</td>
</tr>
<tr>
<td>G</td>
<td>\checkmark</td>
<td>6</td>
<td>\mathbb{Q}</td>
<td>\mathbb{Q}</td>
<td>1</td>
</tr>
</tbody>
</table>

§10.4. \( f(x) = x^4 - 2 \)
(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 \( |\mathbb{Q}[2^{1/4}]:\mathbb{Q}[2^{1/4}]| = 2 \) with \( \{1, i\} \) as a basis.
(4) Thus $|K:Q| = 8$ and so $G(K/Q)$ has order 8. A suitable basis for $K$ over $Q$ is:

<table>
<thead>
<tr>
<th>1</th>
<th>$2^{1/4}$</th>
<th>$\sqrt{2}$</th>
<th>$2^{3/4}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td>$2^{1/4}$</td>
<td>$\sqrt{2}$</td>
<td>$2^{3/4}$</td>
</tr>
</tbody>
</table>

(5) Every automorphism in $G(K/Q)$ 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:

<table>
<thead>
<tr>
<th>i $\mapsto$</th>
<th>$i$</th>
<th>$i$</th>
<th>$i$</th>
<th>$i$</th>
<th>$-i$</th>
<th>$-i$</th>
<th>$-i$</th>
<th>$-i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{1/4}$</td>
<td>$2^{1/4}$</td>
<td>$-2^{1/4}$</td>
<td>$-2^{1/4}$</td>
<td>$2^{1/4}$</td>
<td>$2^{1/4}$</td>
<td>$-2^{1/4}$</td>
<td>$-2^{1/4}$</td>
<td>$-2^{1/4}$</td>
</tr>
</tbody>
</table>

(6) As before we can name the automorphisms and list their orders. This Galois group is isomorphic to $D_8$.

<table>
<thead>
<tr>
<th>i $\mapsto$</th>
<th>A</th>
<th>A$^2$</th>
<th>A$^3$</th>
<th>B</th>
<th>A$^3$B</th>
<th>A$^2$B</th>
<th>AB</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{1/4}$</td>
<td>$2^{1/4}$</td>
<td>$-2^{1/4}$</td>
<td>$-2^{1/4}$</td>
<td>$2^{1/4}$</td>
<td>$2^{1/4}$</td>
<td>$-2^{1/4}$</td>
<td>$-2^{1/4}$</td>
</tr>
</tbody>
</table>

| 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 $Q$ of degree 2. Clearly it is $Q[i]$. Because the subgroup is normal the fixed field is a polynomial extension. Indeed it is. It is $Q[x^2 + 1 = 0]$.

(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 $Q$. 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 $Q[i, \sqrt{2}]$. This also must be a polynomial extension. It is $Q[(x^2 + 1)(x^2 - 2) = 0]$, that $Q[x^4 - x^2 - 2 = 0]$.

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

(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 $Q[2^{1/4}]$.

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

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

A typical element of $Q[x^2 + 2]$ can be expressed as a linear combination, over $Q$, 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 $x = a + b2^{1/4} + c\sqrt{2} + d2^{3/4} + ei + f2^{1/4}i + g\sqrt{2}i + h2^{3/4}i$. Then $x^A = a + b2^{1/4}i - c\sqrt{2} - d2^{3/4}i + ei - f2^{1/4} - g\sqrt{2}i + h2^{3/4}$ and so
\(x^{AB} = a - b \sqrt[4]{2}i - c\sqrt{2} + d\sqrt[3]{4}i - ei - f\sqrt{2}/4 + g\sqrt{2}i + h\sqrt{3}/4.\)

If \(x^{AB} = x\) then, equating coefficients of our basis elements, we get:
\[
b = -f, \quad c = e = 0, \quad d = h, \quad \text{and so} \quad x = a + b\sqrt[4]{2}(1 - i) + d\sqrt[3]{4}(1 + i) + g\sqrt{2}i.
\]
So the fixed field is spanned, as a vector space over \(\mathbb{Q}\), by \(1, \sqrt{2}\) and \(\sqrt[3]{4}(1 + i)\). As a field it can be generated by \(\alpha = 2^{1/4}(1 - i)\) since \(\alpha^2 = -2\sqrt{2}i\) and \(\alpha^3 = -2(2^{3/4}(1 + i))\). So the fixed field of the subgroup \(\langle AB \rangle\) is \(\mathbb{Q}[2^{1/4}(1 - i)]\). Similarly, the fixed field of \(\langle A^3B \rangle\) is \(\mathbb{Q}[2^{1/4}(1 + i)]\).

This is the “brute force” method, only to be resorted to as 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.

\[
\begin{array}{cccccccc}
i \rightarrow & 1 & A & A^2 & A^3 & B & A^3B & A^2B & AB \\
2^{1/4} \rightarrow & i & 2^{1/4} & 2^{1/4}i & -2^{1/4} & 2^{1/4} & 2^{1/4} & -2^{1/4} & -2^{1/4} \\
2^{1/2} \rightarrow & 2^{1/2} & -2^{1/2} & 2^{1/2} & -2^{1/2} & 2^{1/2} & -2^{1/2} & 2^{1/2} & -2^{1/2} \\
2^{1/2}i \rightarrow & 2^{1/2}i & 2^{1/2} & 2^{1/2} & -2^{1/2} & 2^{1/2} & 2^{1/2} & 2^{1/2} & 2^{1/2} \\
2^{1/4}i \rightarrow & 2^{1/4}i & -2^{1/4} & 2^{1/4} & 2^{1/4} & 2^{1/4} & -2^{1/4} & 2^{1/4} & -2^{1/4}
\end{array}
\]

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:

![Subfields of Q[x^4 = 2]](image1)

![Subgroups of G(Q[x^4 = 2]/Q)](image2)
Hence, if the element is fixed:

\[ a \Rightarrow a + b \]

Its image under \( AB \) is \( a + b \).

By playing with the automorphism table:

Unfortunately this is a case for brute force. You are quite unlikely to stumble on the answer.

Fixed Field for \( \langle A \rangle \):

Clearly it is \( Q[i] \).

Fixed Field of \( \langle B \rangle \):

(\( B \)) has index 2 in \( G \) and so its fixed field will have degree 4 over \( Q \).

Clearly the fixed field is \( Q[\theta] \).

Fixed Field for \( \langle AB \rangle \):

(\( AB \)) has index 2 in \( G \) and so its fixed field must have degree 2 over \( Q \).

Unfortunately this is a case for brute force. You are quite unlikely to stumble on the answer by playing with the automorphism table.

A typical element of \( Q[x^{20} - 1] = a + b\theta + c\theta^2 + d\theta^3 + ei \phi + gi\theta^2 + hi\theta^3 \). Its image under \( AB \) is \( a + b\theta^2 + c\theta^0 + d\theta^0 - ei - fi\theta^1 - gi\theta^4 - hi\theta \).

\[ a + b\theta^2 + c(-1 - \theta - 0\theta^2 - 0\theta^3) + d\theta - ei - fi\theta^1 - gi(-1 - 0 - 0\theta^2 - 0\theta^3) - hi\theta \]

\[ (a -c) + (d - c)\theta + (b - c)\theta^2 - c\theta^3 + (g - e)i + (g - h)i\theta + (g - f)i\theta^2 + gi\theta^3 \]

Hence, if the element is fixed:
a = a – c so c = 0;
b = d – c = d;
c = b – c so b = 0;
d = –c = 0;
e = g – e so g = 2e;
f = g – h = 2e –h;
g = g – f so f = 0;
h = g = 2e.

So a typical element fixed by AB is \(a + e(i + 2i^2 + 2i^3)\).

So AB fixes \((1 + 20^2 + 20^3)\).

**Check:** \(1 + 20^2 + 20^3 \rightarrow 1 + 20^4 + 20 = 1 + 2(-1 – 0^2 – 0^3) = -(1 + 0^2 + 0^3)\), so
\(i(1 + 20^2 + 20^3)\) will be fixed.

But what if this is rational? Just because it contains an “\(i\)” does not guarantee that it is not. After all \(\theta\) is also non-real. So we need to investigate a little harder.

Now \((1 + 20^2 + 20^3)^2 = 1 + 40^4 + 40 + 40^2 + 40^3 + 8 = 5 + 4(1 + 0 + 0^2 + 0^3 + 0^4) = 5\) so \(1 + 20^2 + 20^3 = \pm \sqrt{5}\). In fact it is \(-\sqrt{5}\) but that does not matter. We have shown that the fixed field corresponding to \(\langle AB \rangle\) is \(\mathbb{Q}[\sqrt{5}i]\) which clearly has the desired degree.

The other fixed fields can be found similarly, but it is a lot of work. Let us try a different set of generators.

Let \(c = \cos(2\pi/5)\), \(s = \sin(2\pi/5)\).

Then \(\mathbb{Q}[x^{20} – 1 = 0] = \mathbb{Q}[0, i] \leq \mathbb{Q}[c, s, i]\) since \(\theta = c + is\). But \(c = (\theta + \theta^{-1})/2\) and \(s = (\theta – \theta^{-1})/(2i)\) so \(\mathbb{Q}[0, i] = \mathbb{Q}[c, s, i]\).

Putting \((c + is)^2 = 1\) and equating imaginary parts gives \(5c^4 – 10c^2s^2 + s^4 = 0\). Putting \(c^2 = 1 – s^2\) gives \(16s^4 – 20s^2 + 5 = 0\). Since \(16x^4 – 20x^2 + 5\) is prime by Eisenstein this is the minimum polynomial of \(s\) over \(\mathbb{Q}\). So \(|\mathbb{Q}[s]:\mathbb{Q}| = 4\). Clearly \(|\mathbb{Q}[s, i]:\mathbb{Q}[s]| = 2\) since quite definitely \(i \not\in \mathbb{Q}[s]\). So \(|\mathbb{Q}[s, i]:\mathbb{Q}| = 8\). But we know that \(|\mathbb{Q}[x^{20} = 1]:\mathbb{Q}| = 8\) so \(\mathbb{Q}[x^{20} = 1] = \mathbb{Q}[s, i]\).

We can find \(s\) precisely by solving \(16x^4 – 20x^2 + 5 = 0\) as a quadratic in \(x^2\).

\[
s^2 = \frac{20 \pm \sqrt{400 – 320}}{32} = \frac{5 \pm \sqrt{5}}{8}\text{ and so }s = \pm \sqrt{\frac{5 \pm \sqrt{5}}{8}}.
\]

Let \(t = \sqrt{\frac{5 \pm \sqrt{5}}{8}}\). The zeros of \(16x^4 – 20x^2 + 5\) are thus \(\pm s, \pm t\).

Now \(st = \sqrt{\frac{5}{4}}\), that is \(t = \sqrt{\frac{5}{4s}}\). So if A maps \(s\) to \(t\) and \(\sqrt{5}\) to \(-\sqrt{5}\) then it maps \(t\) to \(-s\).

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>A</th>
<th>A^2</th>
<th>A^3</th>
<th>B</th>
<th>AB</th>
<th>A^2B</th>
<th>A^3B</th>
</tr>
</thead>
<tbody>
<tr>
<td>order</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>s →</td>
<td>s</td>
<td>s</td>
<td>t</td>
<td>–s</td>
<td>–t</td>
<td>s</td>
<td>–s</td>
<td>–t</td>
</tr>
<tr>
<td>i →</td>
<td>i</td>
<td>i</td>
<td>i</td>
<td>i</td>
<td>–i</td>
<td>–i</td>
<td>–i</td>
<td>–i</td>
</tr>
<tr>
<td>√5 →</td>
<td>√5</td>
<td>–√5</td>
<td>√5</td>
<td>–√5</td>
<td>√5</td>
<td>–√5</td>
<td>√5</td>
<td>–√5</td>
</tr>
<tr>
<td>t →</td>
<td>t</td>
<td>–s</td>
<td>–t</td>
<td>s</td>
<td>t</td>
<td>–s</td>
<td>–t</td>
<td>s</td>
</tr>
</tbody>
</table>
We can now easily find the fixed fields for all of the subgroups of the Galois Group. And since this Galois Group is abelian all of these subfields are polynomial extensions of \( \mathbb{Q} \).

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>order</th>
<th>FIXED FIELD</th>
<th>polynomial extension</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \langle A^2 \rangle )</td>
<td>2</td>
<td>( \mathbb{Q}[i, \sqrt{5}] )</td>
<td>( \mathbb{Q}[(x^2 + 1)(x^2 - 5)] )</td>
<td>4</td>
</tr>
<tr>
<td>( \langle B \rangle )</td>
<td>2</td>
<td>( \mathbb{Q}[s] )</td>
<td>( \mathbb{Q}[16x^4 - 20x^2 + 5] )</td>
<td>4</td>
</tr>
<tr>
<td>( \langle A^2B \rangle )</td>
<td>2</td>
<td>( \mathbb{Q}[is] )</td>
<td>( \mathbb{Q}[16x^4 + 20x^2 + 5] )</td>
<td>4</td>
</tr>
<tr>
<td>( \langle A \rangle )</td>
<td>4</td>
<td>( \mathbb{Q}[i] )</td>
<td>( \mathbb{Q}[x^2 + 1] )</td>
<td>2</td>
</tr>
<tr>
<td>( \langle AB \rangle )</td>
<td>4</td>
<td>( \mathbb{Q}[\sqrt{5}] )</td>
<td>( \mathbb{Q}[x^2 + 5] )</td>
<td>2</td>
</tr>
<tr>
<td>( \langle A^2, B \rangle )</td>
<td>4</td>
<td>( \mathbb{Q}[\sqrt{5}] )</td>
<td>( \mathbb{Q}[x^2 - 5] )</td>
<td>2</td>
</tr>
<tr>
<td>( G )</td>
<td>8</td>
<td>( \mathbb{Q} )</td>
<td>( \mathbb{Q}[x] )</td>
<td>1</td>
</tr>
</tbody>
</table>

\[ \section{10.6. \ f(x) = x^3 - 3x + 1} \]

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

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

\[
f\left(\frac{\alpha - 1}{\alpha}\right) = \left(\frac{\alpha - 1}{\alpha}\right)^3 - 3\left(\frac{\alpha - 1}{\alpha}\right) - 1 = \frac{(\alpha - 1)^3 - 3\alpha^2(\alpha - 1) - \alpha^3}{\alpha^3} = -\alpha^3 + 3\alpha - 1 = 0.
\]

The map \( F(\alpha) = \frac{\alpha - 1}{\alpha} \) maps one zero to another, and it has order 3. \( F^3 \) is the identity. So the three zeros of \( f(x) \) have the form \( \alpha, F(\alpha) = \frac{\alpha - 1}{\alpha} \) and \( F^2(\alpha) = \frac{1}{1 - \alpha} \). We only need to extend \( \mathbb{Q} \) by one of the three zeros and the other two will automatically be included. Hence if \( \alpha \) is any zero \( \mathbb{Q}[f(x) = 0] = \mathbb{Q}[\alpha] \).

It is not difficult to show that \( f(x) \) is prime over \( \mathbb{Q} \) and so \( |\mathbb{Q}[f(x)]| = 3 \). Thus the Galois group is cyclic of order 3.

\[ \section{10.7. A Mystery Polynomial} \]

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 \( \varepsilon \) over \( \mathbb{Q} \) is \( x^{10} + x^9 + ... + x^2 + x + 1 \) so \( |\mathbb{Q}[x^{11} - 1]/\mathbb{Q}| = 10 \).

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

\[
\varepsilon \rightarrow \begin{array}{cccccccccc}
\varepsilon & \varepsilon^2 & \varepsilon^4 & \varepsilon^8 & \varepsilon^5 & \varepsilon^10 & \varepsilon^9 & \varepsilon^7 & \varepsilon^3 & \varepsilon^6 \\
\end{array}
\]

order 1 10 5 10 5 2 5 10 5 10

97
Now $C_5$ is a quotient group of $C_{10}$. We simply have to factor out by $\langle A^5 \rangle$. Then $G(K/Q) \cong C_5$ 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 $Q[x^{11} - 1]$. It is not difficult to see these are spanned by $\epsilon + \epsilon^{-1}, \epsilon^2 + \epsilon^{-2}, \epsilon^3 + \epsilon^{-3}, \epsilon^4 + \epsilon^{-4}$ and $\epsilon^5 + \epsilon^{-5}$. These are respectively $2\cos(2\pi/11), 2\cos(4\pi/11), 2\cos(6\pi/11), 2\cos(8\pi/11)$ and $2\cos(10\pi/11)$. These are the zeros of some polynomial of degree 5, but which one? In fact it has very simple integer coefficients.

Let $\epsilon$ be any non-real 11th root of 1, let $\epsilon_r = \epsilon^r + \epsilon^{-r}$ for $r = 1, 2, 3, 4, 5$.

Hence $\epsilon_1 = x$, $\epsilon_2 = x^2 - 2$, $\epsilon_3 = x^3 - 3x$, $\epsilon_4 = x^4 - 6 - 4(x^2 - 2) = x^4 - 4x^2 + 2$ and $\epsilon_5 = x^5 - 10x - 5(x^3 - 3) = x^5 - 5x^3 + 5x$.

But $\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5$ is the sum of all the 11th roots of 1, except 1 and so is $-1$. So $(x^5 - 5x^3 + 5x) + (x^4 - 4x^2 + 2) + (x^3 - 3) + (x^2 - 2) + x + 1 = 0$. 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 $\epsilon$. Since $\epsilon$ can be any one of the five non-real 11th 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 $Q[x^4 + x^4 - 4x^3 - 3x^2 + 3x + 1]$ over $Q$ is $C_5$.

**EXERCISES FOR CHAPTER 10**

For each of exercises 1 to 6 find the Galois group, $G$, of its splitting field over $Q$. Describe each automorphism in $G$ by its effect on a set of generators for the splitting field. Find the subgroups of $G$ and the corresponding fixed fields. Identify which subgroups are normal in $G$ and which subfields of the splitting field are polynomial extensions of $Q$.

**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:** $f(x) = x^6 + 3x^3 - 1$.
Exercise 7: Let $\theta = e^{2\pi i/7}$ and for $r = 1, 2, 3$ let $\alpha_r = 0^r + 0^{6r}$.

Let $f(x) = (x - \alpha_1) (x - \alpha_2) (x - \alpha_3)$.

(i) Find $f(x)$ and show that it is a rational polynomial.

(ii) Find $G(\mathbb{Q}[f(x) = 0]/\mathbb{Q})$.

Exercise 8: $f(x) = x^4 - 6x^2 + 3$

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

Exercise 10: $f(x) = x^6 - 6x^3 + 6$

Exercise 11: $f(x) = x^{15} - 1$

Exercise 12: $f(x) = x^8 - 5x^5 - 7x^3 + 35$

Exercise 13: $f(x) = x^{30} - 30x^{15} + 216$

Exercise 14: $f(x) = x^6 + 6x^4 + 12x^2 + 6$

SOLUTIONS FOR CHAPTER 10

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:

| $\sqrt{5}$ | $\sqrt{5}$ | $\sqrt{5}$ | $-\sqrt{5}$ | $-\sqrt{5}$ |
| $\sqrt{2}i$ | $\sqrt{2}i$ | $-\sqrt{2}i$ | $\sqrt{2}i$ | $-\sqrt{2}i$ |

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

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

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>normal</th>
<th>order</th>
<th>SUBFIELD</th>
<th>poly ext’n</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\sqrt{\cdot}$</td>
<td>1</td>
<td>$\mathbb{Q}[x^2 - 3x^2 - 10]$</td>
<td>$\mathbb{Q}[x^2 - 3x^2 - 10]$</td>
<td>4</td>
</tr>
<tr>
<td>$\langle A \rangle$</td>
<td>$\sqrt{\cdot}$</td>
<td>2</td>
<td>$\mathbb{Q}[\sqrt{5}]$</td>
<td>$\mathbb{Q}[x^2 - 5]$</td>
<td>2</td>
</tr>
<tr>
<td>$\langle B \rangle$</td>
<td>$\sqrt{\cdot}$</td>
<td>2</td>
<td>$\mathbb{Q}[\sqrt{2}i]$</td>
<td>$\mathbb{Q}[x^2 + 2]$</td>
<td>2</td>
</tr>
<tr>
<td>$\langle AB \rangle$</td>
<td>$\sqrt{\cdot}$</td>
<td>2</td>
<td>$\mathbb{Q}[\sqrt{10}i]$</td>
<td>$\mathbb{Q}[x^2 + 10]$</td>
<td>2</td>
</tr>
<tr>
<td>$G$</td>
<td>$\sqrt{\cdot}$</td>
<td>4</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}$</td>
<td>1</td>
</tr>
</tbody>
</table>

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 $3^2 = 9 \mod 10$, $\mathbb{Z}_{10}^\# \cong C_4$.

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

Let $\alpha = e^{2\pi i/10}$ and let A be the automorphism that takes $\alpha$ to $\alpha^3$. This generates the Galois group. $A^2$ takes $\alpha$ to $\alpha^9 = \alpha^{-1}$ and fixes $\alpha + \alpha^{-1} = 2\cos(2\pi/10) = 2\cos(\pi/5)$.

Since $(A^2)$ 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 \( c^5 + 5ic^4s - 10c^3s^2 - 10ic^2s^3 + is^5 = -1 \).

Equating real parts we get \( 5c^4s - 10c^2s^2 + s^4 = 0 \).

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

\[ \therefore \quad 5c^4 - 10c^2(1 - c^2) + (1 - c^2)^2 = 0. \]

\[ \therefore \quad 16c^4 - 12c^2 + 1 = 0. \]

\[ \therefore \quad c^2 = \frac{12 \pm \sqrt{80}}{32} = \frac{3 \pm \sqrt{5}}{8}. \]

It is not difficult to reject \( \frac{3 - \sqrt{5}}{8} \) so \( c^2 = \frac{3 + \sqrt{5}}{8} \).

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 \( \cos(\pi/5) = \frac{1 + \sqrt{5}}{4} \) and so its minimum polynomial is \((4x - 1)^2 - 5 = x^2 - \frac{1}{2}x - \frac{1}{4}\).

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 cannot possibly be the minimum polynomial.

The zeros of \( x^8 + x^6 + x^4 + x^2 + 1 \) are \( \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^7, \alpha^8 \) and \( \alpha^9 \) (not \( \alpha^5 = -1 \)).

Now \( \alpha^2, \alpha^4, \alpha^6 \) and \( \alpha^8 \) are 5th 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 \( \alpha \). We do not need to check that it is prime because we know from the Galois groups that \( \mathbb{Q}[\alpha] \) must have degree 4 over \( \mathbb{Q} \).

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

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>normal</th>
<th>order</th>
<th>SUBFIELD</th>
<th>poly ext’n</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \langle A^2 \rangle )</td>
<td>( \sqrt )</td>
<td>2</td>
<td>( \mathbb{Q}[\cos(\pi/5)] )</td>
<td>( \mathbb{Q}[x^4 - x^3 + x^2 - x + 1] )</td>
<td>4</td>
</tr>
<tr>
<td>G</td>
<td>( \sqrt )</td>
<td>4</td>
<td>( \mathbb{Q} )</td>
<td>( \mathbb{Q} )</td>
<td>1</td>
</tr>
</tbody>
</table>

**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 \( \pm \sqrt{\frac{-3 \pm 3\sqrt{3}i}{2}} \).

Hence \( \mathbb{Q}[x^6 - 27] = \mathbb{Q}[^{\sqrt{3}}, \alpha, \beta] \) where \( \alpha = \sqrt{\frac{-3 + 3\sqrt{3}i}{2}} \) and \( \beta = \sqrt{\frac{-3 - 3\sqrt{3}i}{2}} \).

Note that \( \sqrt{\frac{-3 + 3\sqrt{3}i}{2}} \) and \( \sqrt{\frac{-3 - 3\sqrt{3}i}{2}} \) are not uniquely defined because there are two square roots in each case. But \( (\alpha\beta)^2 = 9 \) (this is the product of the zeros of \( x^4 + 3x^2 + 9 \)) and we choose \( \alpha, \beta \) so that \( \alpha\beta = 3 \).

Hence \( \mathbb{Q}[x^6 - 27] = \mathbb{Q}[^{\sqrt{3}}, \alpha] \).

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 $\beta$ are:

<table>
<thead>
<tr>
<th></th>
<th>I</th>
<th>A</th>
<th>B</th>
<th>AB</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha \rightarrow$</td>
<td>$\alpha$</td>
<td>$-\alpha$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
</tr>
<tr>
<td>$\beta \rightarrow$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
<td>$\alpha$</td>
<td>$-\alpha$</td>
</tr>
<tr>
<td>$\sqrt{3} \rightarrow$</td>
<td>$\sqrt{3}$</td>
<td>$-\sqrt{3}$</td>
<td>$\sqrt{3}$</td>
<td>$-\sqrt{3}$</td>
</tr>
<tr>
<td>$\sqrt{3}i \rightarrow$</td>
<td>$\sqrt{3}i$</td>
<td>$-\sqrt{3}i$</td>
<td>$\sqrt{3}i$</td>
<td>$-\sqrt{3}i$</td>
</tr>
<tr>
<td>$i \rightarrow$</td>
<td>$i$</td>
<td>$-i$</td>
<td>$i$</td>
<td>$i$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>normal</th>
<th>order</th>
<th>SUBFIELD</th>
<th>poly ext’n</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\sqrt{1}$</td>
<td>1</td>
<td>$Q[x^6 - 27]$</td>
<td>$Q[x^6 - 27]$</td>
<td>4</td>
</tr>
<tr>
<td>$\langle A \rangle$</td>
<td>$\sqrt{1}$</td>
<td>2</td>
<td>$Q[\sqrt{3}i]$</td>
<td>$Q[x^2 + 3]$</td>
<td>2</td>
</tr>
<tr>
<td>$\langle B \rangle$</td>
<td>$\sqrt{1}$</td>
<td>2</td>
<td>$Q[\sqrt{3}]$</td>
<td>$Q[x^2 - 3]$</td>
<td>2</td>
</tr>
<tr>
<td>$\langle AB \rangle$</td>
<td>$\sqrt{1}$</td>
<td>2</td>
<td>$Q[i]$</td>
<td>$Q[x^2 + 1]$</td>
<td>2</td>
</tr>
<tr>
<td>G</td>
<td>$\sqrt{1}$</td>
<td>4</td>
<td>$Q$</td>
<td>$Q$</td>
<td>1</td>
</tr>
</tbody>
</table>

**Exercise 4:** $Q[x^{24} = 1] = Q[\alpha]$ where $\alpha = e^{2\pi i/24}$.

Under an automorphism in $G(Q[x^{24} = 1]/Q)$ $\alpha \rightarrow \alpha^r$ where $r$ is coprime with 24.

Thus $G(Q[x^{24} = 1]/Q) \cong Z_{24}^\#$, the group of units of the ring $Z_{24}$.

$Z_{24}^\# = \{1, 5, 7, 11, 13, 17, 19, 23\} = \{\pm 1, \pm 5, \pm 7, \pm 11\}$.

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

Let A be the automorphism that maps $\alpha$ to $\alpha^5$.

Let B be the automorphism that maps $\alpha$ to $\alpha^7$.

Then AB maps $\alpha$ to $\alpha^{11}$.

Let C be the automorphism that maps $\alpha$ to $\alpha^{-1}$.

<table>
<thead>
<tr>
<th></th>
<th>I</th>
<th>A</th>
<th>B</th>
<th>AB</th>
<th>C</th>
<th>AC</th>
<th>BC</th>
<th>ABC</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha \rightarrow$</td>
<td>$\alpha$</td>
<td>$\alpha^5$</td>
<td>$\alpha^7$</td>
<td>$\alpha^{11}$</td>
<td>$\alpha^{-1}$</td>
<td>$\alpha^{-5}$</td>
<td>$\alpha^{-7}$</td>
<td>$\alpha^{-11}$</td>
</tr>
</tbody>
</table>

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 $\alpha^5$ to $\alpha^{25} = \alpha$). But is $Q[\alpha + \alpha^5]$ the whole of the fixed field? ABC clearly fixes $\alpha + \alpha^{-11}$ and we might be tempted to say that $Q[\alpha + \alpha^{-11}]$ 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 is 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 $\alpha^4 = e^{2\pi i/6} = \frac{1 + \sqrt{3}i}{2}$ the splitting field contains $\sqrt{3}i$ and hence $\sqrt{3}$. Since $\alpha^3 = \frac{1 + i}{\sqrt{2}}$ 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 $Q[x^{24} - 1] = Q[i, \sqrt{2}, \sqrt{3}]$. Various powers of $\alpha$ can be expressed in terms of these generators as follows.

<table>
<thead>
<tr>
<th>$\alpha^3$</th>
<th>$\alpha^4$</th>
<th>$\alpha^5$</th>
<th>$\alpha^6$</th>
<th>$\alpha^9$</th>
<th>$\alpha^{12}$</th>
<th>$\alpha^{15}$</th>
<th>$\alpha^{16}$</th>
<th>$\alpha^{18}$</th>
<th>$\alpha^{20}$</th>
<th>$\alpha^{21}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1 + i}{\sqrt{2}}$</td>
<td>$\frac{1 + \sqrt{3}i}{2}$</td>
<td>$i$</td>
<td>$-1 + \sqrt{3}i$</td>
<td>$\frac{-1 + i}{\sqrt{2}}$</td>
<td>$-1$</td>
<td>$-1 - i$</td>
<td>$\frac{-1 - \sqrt{3}i}{2}$</td>
<td>$-i$</td>
<td>$1 - \sqrt{3}i$</td>
<td>$\frac{1 - i}{\sqrt{2}}$</td>
</tr>
</tbody>
</table>
The effect of the automorphisms on these new generators is as follows.

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>normal</th>
<th>order</th>
<th>SUBFIELD</th>
<th>poly ext’n</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>√</td>
<td>1</td>
<td>(\mathbb{Q}[x^{24} - 1])</td>
<td>(\mathbb{Q}[x^{24} - 1])</td>
<td>8</td>
</tr>
<tr>
<td>\langle A \rangle</td>
<td>√</td>
<td>2</td>
<td>(\mathbb{Q}[i, \sqrt{6}])</td>
<td>(\mathbb{Q}[x^2 + 1(x^2 - 6)])</td>
<td>4</td>
</tr>
<tr>
<td>\langle B \rangle</td>
<td>√</td>
<td>2</td>
<td>(\mathbb{Q}[\sqrt{2}, i\sqrt{3}])</td>
<td>(\mathbb{Q}[x^2 + 2(x^2 - 3)])</td>
<td>4</td>
</tr>
<tr>
<td>\langle AB \rangle</td>
<td>√</td>
<td>2</td>
<td>(\mathbb{Q}[i\sqrt{2}, \sqrt{3}])</td>
<td>(\mathbb{Q}[x^2 - 2(x^2 - 3)])</td>
<td>4</td>
</tr>
<tr>
<td>\langle C \rangle</td>
<td>√</td>
<td>2</td>
<td>(\mathbb{Q}[\sqrt{2}, \sqrt{3}])</td>
<td>(\mathbb{Q}[x^2 + 2(x^2 - 3)])</td>
<td>4</td>
</tr>
<tr>
<td>\langle AC \rangle</td>
<td>√</td>
<td>2</td>
<td>(\mathbb{Q}[i\sqrt{2}, i\sqrt{3}])</td>
<td>(\mathbb{Q}[x^2 + 2(x^2 - 3)])</td>
<td>4</td>
</tr>
<tr>
<td>\langle BC \rangle</td>
<td>√</td>
<td>2</td>
<td>(\mathbb{Q}[i, \sqrt{2}])</td>
<td>(\mathbb{Q}[x^2 + 1(x^2 - 2)])</td>
<td>4</td>
</tr>
<tr>
<td>\langle ABC \rangle</td>
<td>√</td>
<td>2</td>
<td>(\mathbb{Q}[i\sqrt{2}, \sqrt{3}])</td>
<td>(\mathbb{Q}[x^2 + 2(x^2 - 3)])</td>
<td>4</td>
</tr>
<tr>
<td>\langle A, B \rangle</td>
<td>√</td>
<td>4</td>
<td>(\mathbb{Q}[i\sqrt{6}])</td>
<td>(\mathbb{Q}[x^2 + 6])</td>
<td>2</td>
</tr>
<tr>
<td>\langle A, C \rangle</td>
<td>√</td>
<td>4</td>
<td>(\mathbb{Q}[\sqrt{6}])</td>
<td>(\mathbb{Q}[x^2 - 6])</td>
<td>2</td>
</tr>
<tr>
<td>\langle A, BC \rangle</td>
<td>√</td>
<td>4</td>
<td>(\mathbb{Q}[i])</td>
<td>(\mathbb{Q}[x^2 + 1])</td>
<td>2</td>
</tr>
<tr>
<td>\langle B, C \rangle</td>
<td>√</td>
<td>4</td>
<td>(\mathbb{Q}[\sqrt{2}])</td>
<td>(\mathbb{Q}[x^2 - 2])</td>
<td>2</td>
</tr>
<tr>
<td>\langle B, AC \rangle</td>
<td>√</td>
<td>4</td>
<td>(\mathbb{Q}[i\sqrt{3}])</td>
<td>(\mathbb{Q}[x^2 + 3])</td>
<td>2</td>
</tr>
<tr>
<td>\langle AC, BC \rangle</td>
<td>√</td>
<td>4</td>
<td>(\mathbb{Q}[i\sqrt{2}])</td>
<td>(\mathbb{Q}[x^2 + 2])</td>
<td>2</td>
</tr>
<tr>
<td>\langle C, AB \rangle</td>
<td>√</td>
<td>4</td>
<td>(\mathbb{Q}[\sqrt{3}])</td>
<td>(\mathbb{Q}[x^2 - 3])</td>
<td>2</td>
</tr>
<tr>
<td>G</td>
<td>√</td>
<td>8</td>
<td>(\mathbb{Q})</td>
<td>(\mathbb{Q})</td>
<td>1</td>
</tr>
</tbody>
</table>

Exercise 5: If \(x^4 + 3x^2 - 1 = 0\) then \(x^2 = \frac{-3 \pm \sqrt{9 + 4}}{2} = \frac{-3 \pm 3\sqrt{13}}{2}\).

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

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

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 \(i, \sqrt{13}, \alpha\) and \(\beta\) are:

| \(\alpha \rightarrow\) | \(\alpha\) | \(-\alpha\) | \(\beta\) | \(-\beta\) | \(\alpha\) | \(-\alpha\) | \(\beta\) | \(-\beta\) |
| \(\beta \rightarrow\) | \(\beta\) | \(-\beta\) | \(\alpha\) | \(-\alpha\) | \(\beta\) | \(-\beta\) | \(\alpha\) | \(-\alpha\) |
| \(\sqrt{13}\) | \(\sqrt{13}\) | \(-\sqrt{13}\) | \(-\sqrt{13}\) | \(\sqrt{13}\) | \(\sqrt{13}\) | \(-\sqrt{13}\) | \(-\sqrt{13}\) |

Now \(\theta_2^2 = \theta_3^2 = \theta_4^2 = \theta_5^2 = \theta_6^2 = \theta_7^2 = \theta_8^2 = 0_2\).
Let $\theta_7 = A$. Then $A^2 = 2, A^3 = 0_8$.
Let $\theta_3 = B$.
We can express all 8 automorphisms in terms of $A, B$.

<table>
<thead>
<tr>
<th></th>
<th>$A^2$</th>
<th>$B$</th>
<th>$A^3B$</th>
<th>$AB$</th>
<th>$A^2B$</th>
<th>$A$</th>
<th>$A^3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i \to$</td>
<td>$i$</td>
<td>$i$</td>
<td>$i$</td>
<td>$-i$</td>
<td>$-i$</td>
<td>$-i$</td>
<td>$-i$</td>
</tr>
<tr>
<td>$\alpha \to$</td>
<td>$\alpha$</td>
<td>$-\alpha$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
<td>$\alpha$</td>
<td>$-\alpha$</td>
<td>$\beta$</td>
</tr>
<tr>
<td>$\beta \to$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
<td>$\alpha$</td>
<td>$-\alpha$</td>
<td>$\beta$</td>
<td>$-\alpha$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>$\sqrt{13} \to$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$-\sqrt{13}$</td>
<td>$-\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$-\sqrt{13}$</td>
<td>$-\sqrt{13}$</td>
</tr>
<tr>
<td>$\sqrt{13i} \to$</td>
<td>$\sqrt{13i}$</td>
<td>$\sqrt{13i}$</td>
<td>$-\sqrt{13i}$</td>
<td>$-\sqrt{13i}$</td>
<td>$-\sqrt{13i}$</td>
<td>$\sqrt{13i}$</td>
<td>$\sqrt{13i}$</td>
</tr>
</tbody>
</table>

Now $BA = A^3B = A^{-1}B$.
So $G(Q[x^4 + 3x^2 - 1] / Q) = \langle A, B | A^4 = B^2 = 1, BA = A^{-1}B \rangle \cong D_8$.
The subgroups of the Galois group and the corresponding fields are given in the following table:

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>normal</th>
<th>order</th>
<th>SUBFIELD</th>
<th>poly ext'n</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>$\sqrt{1}$</td>
<td>$1$</td>
<td>$Q[x^4 + 3x^2 - 1]$</td>
<td>$Q[x^4 + 3x^2 - 1]$</td>
<td>$8$</td>
</tr>
<tr>
<td>$\langle A^2 \rangle$</td>
<td>$\sqrt{1}$</td>
<td>$2$</td>
<td>$Q[i, \sqrt{13}]$</td>
<td>$Q[(x^2 + 1)(x^2 - 1)]$</td>
<td>$4$</td>
</tr>
<tr>
<td>$\langle B \rangle$</td>
<td>$2$</td>
<td>$4$</td>
<td>$Q[\alpha + \beta]$</td>
<td>$4$</td>
<td></td>
</tr>
<tr>
<td>$\langle AB \rangle$</td>
<td>$2$</td>
<td>$Q[\alpha]$</td>
<td>$4$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\langle A^3B \rangle$</td>
<td>$2$</td>
<td>$Q[\sqrt{13}(\alpha + \beta)]$</td>
<td>$4$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\langle A'B \rangle$</td>
<td>$2$</td>
<td>$Q[\beta]$</td>
<td>$4$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\langle A \rangle$</td>
<td>$\sqrt{1}$</td>
<td>$4$</td>
<td>$Q[\sqrt{13}i]$</td>
<td>$Q[x^2 + 3]$</td>
<td>$2$</td>
</tr>
<tr>
<td>$G$</td>
<td>$\sqrt{1}$</td>
<td>$8$</td>
<td>$Q$</td>
<td>$\sqrt{1}$</td>
<td>$1$</td>
</tr>
</tbody>
</table>

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

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

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

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

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

Hence $Q[x^6 + 3x^3 - 1 = 0] = Q[\alpha, \beta, \omega]$ where $\alpha = \left(\frac{-3 + \sqrt{13}}{2}\right)^{1/3}$ and $\beta = -\left(\frac{-3 + \sqrt{13}}{2}\right)^{1/3}$.

Now $\alpha \beta = \left(\frac{9 - 13}{4}\right)^{1/3} = -1$.
Hence $Q[x^6 + 3x^3 - 1 = 0] = Q[\alpha, \beta, \omega]$.

The automorphisms, and the effect on $\omega, \sqrt{13}, \alpha$ and $\beta$ are:

<table>
<thead>
<tr>
<th></th>
<th>$\theta_2$</th>
<th>$\theta_3$</th>
<th>$\theta_4$</th>
<th>$\theta_5$</th>
<th>$\theta_6$</th>
<th>$\theta_7$</th>
<th>$\theta_8$</th>
<th>$\theta_9$</th>
<th>$\theta_{10}$</th>
<th>$\theta_{11}$</th>
<th>$\theta_{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega^2$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>$\alpha \omega$</td>
<td>$\alpha \omega^2$</td>
<td>$\beta$</td>
<td>$\beta \omega$</td>
<td>$\beta \omega^2$</td>
<td>$\alpha$</td>
<td>$\alpha \omega$</td>
<td>$\alpha \omega^2$</td>
<td>$\beta$</td>
<td>$\beta \omega$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>$\beta \omega^2$</td>
<td>$\beta \omega$</td>
<td>$\alpha$</td>
<td>$\alpha \omega^2$</td>
<td>$\alpha \omega$</td>
<td>$\beta$</td>
<td>$\beta \omega^2$</td>
<td>$\beta \omega$</td>
<td>$\alpha$</td>
<td>$\alpha \omega^2$</td>
<td>$\alpha \omega$</td>
</tr>
<tr>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
<td>$\sqrt{13}$</td>
</tr>
</tbody>
</table>

Now $\theta_2^2 = \theta_3, \theta_2^3 = 1, \theta_4^2 = \theta_5^2 = \theta_6^2 = \theta_7^2 = \theta_8^2 = \theta_9^2 = \theta_{10}^2 = 1, \theta_{11}^2 = \theta_2, \theta_{12}^2 = \theta_3$. 

103
Let $\theta_1 = A$. Then $A^2 = \theta_2$, $A^3 = \theta_{10}$, $A^4 = \theta_3$, $A^5 = \theta_{12}$, $A^6 = 1$.
Let $\theta_4 = B$.

We can express all 12 automorphisms in terms of $A$, $B$.

<table>
<thead>
<tr>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
<th>$\omega \rightarrow$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>$A^2$</td>
<td>$A^4$</td>
<td>$B$</td>
<td>$A^2B$</td>
<td>$A^4B$</td>
<td>$A^6B$</td>
<td>$A^4$</td>
<td>$A$</td>
<td>$A^5$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
<td>$\alpha \rightarrow$</td>
</tr>
<tr>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
<td>$\beta \rightarrow$</td>
</tr>
<tr>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
<td>$\sqrt{13} \rightarrow$</td>
</tr>
<tr>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
<td>$\sqrt{3i} \rightarrow$</td>
</tr>
</tbody>
</table>

Now $BA = A^3B = A^{-1}B$.
So $G(Q[x^6+3x^3-1=0]/Q) = \langle A, B | A^6 = B^2 = 1, BA = A^{-1}B \rangle \cong D_{12}$.

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

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

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>normal</th>
<th>order</th>
<th>SUBFIELD</th>
<th>poly ext’n</th>
<th>deg</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>$\sqrt{}$</td>
<td>$1$</td>
<td>$Q[f(x)]$</td>
<td>$Q[f(x)]$</td>
<td>$12$</td>
</tr>
<tr>
<td>$\langle A^3 \rangle$</td>
<td>$\sqrt{}$</td>
<td>$2$</td>
<td>$Q[\alpha + \beta, \sqrt{39i}]$</td>
<td>$Q[(x^3+3x+3)(x^2+39)]$</td>
<td>$6$</td>
</tr>
<tr>
<td>$\langle B \rangle$</td>
<td>$\sqrt{}$</td>
<td>$2$</td>
<td>$Q[\alpha + \beta, \sqrt{3i}]$</td>
<td>$Q[(x^3+3x+3)(x^2+39)]$</td>
<td>$6$</td>
</tr>
<tr>
<td>$\langle AB \rangle$</td>
<td>$\sqrt{}$</td>
<td>$2$</td>
<td>$Q[\alpha, \sqrt{13}]$</td>
<td>$Q[(x^3+3x+3)(x^2+39)]$</td>
<td>$6$</td>
</tr>
<tr>
<td>$\langle A^2B \rangle$</td>
<td>$\sqrt{}$</td>
<td>$2$</td>
<td>$Q[\alpha, \sqrt{13}]$</td>
<td>$Q[(x^3+3x+3)(x^2+39)]$</td>
<td>$6$</td>
</tr>
<tr>
<td>$\langle A^4B \rangle$</td>
<td>$\sqrt{}$</td>
<td>$2$</td>
<td>$Q[\alpha, \sqrt{13}]$</td>
<td>$Q[(x^3+3x+3)(x^2+39)]$</td>
<td>$6$</td>
</tr>
<tr>
<td>$\langle A \rangle$</td>
<td>$\sqrt{}$</td>
<td>$12$</td>
<td>$Q$</td>
<td>$\sqrt{}$</td>
<td>$1$</td>
</tr>
</tbody>
</table>

Exercise 7:
(i) $\sum \alpha_j = 0 + 0^2 + 0^3 + 0^4 + 0^5 + 0^6 = -1$,
\begin{align*}
\Sigma \alpha_j & = (0 + 0^6) (0^2 + 0^5) + (0 + 0^6) (0^3 + 0^4) + (0^2 + 0^5) (0^3 + 0^4) \\
& = 0^3 + 0^6 + 0^8 + 0^{11} + 0^4 + 0^5 + 0^9 + 0^{10} + 0^5 + 0^6 + 0^8 + 0^9 \\
& = 0^3 + 0^6 + 0 + 0^4 + 0^5 + 0^2 + 0^3 + 0^5 + 0^3 + 0^5 + 0 + 0^2 \\
& = 2(0 + 0^2 + 0^3 + 0^4 + 0^5 + 0^6) = -2, \\
\alpha_1 \alpha_2 \alpha_3 & = (0 + 0^6) (0^2 + 0^5) (0^3 + 0^4) \\
& = 0^3 + 0^7 + 0^9 + 0^{10} + 0^11 + 0^{12} + 0^{14} + 0^{15} \\
& = 0^6 + 1 + 0^2 + 0^3 + 0^4 + 0^5 + 1 + 0 = 1.
\end{align*}
Hence \( f(x) = x^3 + x^2 - 2x - 1 \).

(ii) The zeros of \( f(x) \) are \( 0 + 0^6, 0^2 + 0^5 \) and \( 0^3 + 0^4 \). Under an automorphism of \( \mathbb{Q}[\theta] \), \( \theta \) maps to \( \theta^r \) for \( r = 1, 2, 3, 4, 5, 6 \). However restricted to \( \mathbb{Q}[x^3 + x^2 - 2x - 1] \) these collapse to three automorphisms.

<table>
<thead>
<tr>
<th>0 + 0^6 \mapsto 0 + 0^5</th>
<th>( A )</th>
<th>( A^2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0^2 + 0^5 \mapsto 0^3 + 0^4</td>
<td>0^3 + 0^4</td>
<td>0^2 + 0^5</td>
</tr>
</tbody>
</table>

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

**Exercise 8:**

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

The splitting field is \( \mathbb{Q}[\alpha, \beta] \) where

\[ \alpha = \sqrt{3} + \sqrt{6} \quad \text{and} \quad \beta = \sqrt{3} - \sqrt{6}. \]

Since \( x^4 - 6x^2 + 3 \) is prime by Eisenstein’s Theorem

\[ |\mathbb{Q}[\alpha]:\mathbb{Q}| = 4 \quad \text{and} \quad |\mathbb{Q}[\beta]:\mathbb{Q}| = 4. \]

This might suggest that \( |K:\mathbb{Q}| = 16 \). But that would require the Galois group, necessarily a subgroup of \( S_4 \), to have order 16 and this doesn’t divide 24. The explanation is that while the minimum polynomial of \( \beta \) 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 \( \beta \) over \( \mathbb{Q}[\alpha] \). But is it? Could it be that \( \beta \) 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 is 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 \( \sqrt{3} + \sqrt{6} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \) for some \( a, b, c, d \in \mathbb{Q} \). 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:

\[
\begin{align*}
    a^2 + 2b^2 + 3c^2 + 6d^2 &= 3; \\
    ab + cd &= 0; \\
    ac + bd &= 0; \\
    ad + bc &= 1. 
\end{align*}
\]

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

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

**Case I: a + d = 0:**

\[
\begin{align*}
    7a^2 + 2b^2 + 3c^2 &= 3; \\
    a(b - c) &= 0; \\
    -a^2 + bc &= 1. 
\end{align*}
\]
Case IA: \( a = 0 \): Here we have \( 2b^2 + 3c^2 = 3 \) and \( bc = 1 \) and so \( 2b^4 - 3b^2 + 3 = 0 \). 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 \( b = c \) and so \( 7a^2 + 5b^2 = 3 \) and \( a^2 + b^2 = 1 \). Thus \( 2a^2 = -2 \), a contradiction.

Case II: \( b + c = 0 \):
\[
a^2 + 5b^2 + 6d^2 = 3;
\]
\[
b(a - d) = 0;
\]
\[
ad - b^2 = 1.
\]

Case IIA: \( b = 0 \): Then \( a^2 + 6d^2 = 3 \) and \( ad = 1 \) and so \( 2a^4 = -2 \), a contradiction.

Case IIB: \( b \neq 0 \): Then \( a = d \) and so \( 7a^2 + 5b^2 = 3 \) 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, \( \beta \not\in \mathbb{Q}[\alpha] \) and hence \( [\mathbb{Q}[\alpha, \beta]:\mathbb{Q}] = 8 \) (consistent with the Galois group being a subgroup of \( S_4 \)). The only subgroup of \( S_4 \) with order 8 is \( D_8 \) so the Galois group here must be \( D_8 \). But if we wish to examine the connection between the subgroups and fixed fields we need to list the automorphisms. Now while \( \alpha \) can map to any one of the four possibilities \( \pm \alpha, \pm \beta \), once \( \alpha^0 \) has been chosen we must map \( \beta \) to \( \pm \sqrt[3]{3}/\alpha^0 \). Thus if \( \alpha \) maps to \( \pm \alpha, \beta \) must map to \( \pm \beta \) and if \( \alpha \) maps to \( \pm \beta \), \( \beta \) must map to \( \pm \alpha \). The eight automorphisms are given by the following table:

<table>
<thead>
<tr>
<th>( \alpha ) ( \to )</th>
<th>1</th>
<th>B</th>
<th>( A^2B )</th>
<th>( A^2 )</th>
<th>( A^3B )</th>
<th>A</th>
<th>( A^3 )</th>
<th>AB</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha )</td>
<td>( \alpha )</td>
<td>( -\alpha )</td>
<td>( -\alpha )</td>
<td>( \beta )</td>
<td>( \beta )</td>
<td>( -\beta )</td>
<td>( -\beta )</td>
<td></td>
</tr>
<tr>
<td>( \beta )</td>
<td>( -\beta )</td>
<td>( \beta )</td>
<td>( -\beta )</td>
<td>( \alpha )</td>
<td>( -\alpha )</td>
<td>( \alpha )</td>
<td>( -\alpha )</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>( \sqrt{3} ) ( \to )</th>
<th>1</th>
<th>B</th>
<th>( A^2B )</th>
<th>( A^2 )</th>
<th>( A^3B )</th>
<th>A</th>
<th>( A^3 )</th>
<th>AB</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sqrt{3} )</td>
<td>( \sqrt{3} )</td>
<td>( -\sqrt{3} )</td>
<td>( -\sqrt{3} )</td>
<td>( \sqrt{3} )</td>
<td>( -\sqrt{3} )</td>
<td>( -\sqrt{3} )</td>
<td>( \sqrt{3} )</td>
<td></td>
</tr>
<tr>
<td>( \sqrt{6} )</td>
<td>( \sqrt{6} )</td>
<td>( \sqrt{6} )</td>
<td>( \sqrt{6} )</td>
<td>( -\sqrt{6} )</td>
<td>( -\sqrt{6} )</td>
<td>( -\sqrt{6} )</td>
<td>( -\sqrt{6} )</td>
<td></td>
</tr>
<tr>
<td>( \sqrt{2} )</td>
<td>( \sqrt{2} )</td>
<td>( -\sqrt{2} )</td>
<td>( -\sqrt{2} )</td>
<td>( \sqrt{2} )</td>
<td>( \sqrt{2} )</td>
<td>( -\sqrt{2} )</td>
<td>( -\sqrt{2} )</td>
<td></td>
</tr>
</tbody>
</table>

The Galois group is thus \( \langle A, B \mid A^4 = B^2 = 1, BA = A^{-1}B \rangle \). The subgroups and the corresponding fixed fields are given by the following table.

<table>
<thead>
<tr>
<th>SUBGROUP</th>
<th>normal</th>
<th>order</th>
<th>SUBFIELD</th>
<th>poly ext’n</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \sqrt{\ } )</td>
<td>1</td>
<td>( \mathbb{Q}[x^4 - 6x^2 + 3] )</td>
<td>( \mathbb{Q}[x^4 - 6x^2 + 3] )</td>
<td>8</td>
</tr>
<tr>
<td>( \langle AB \rangle )</td>
<td>2</td>
<td>( \mathbb{Q}[\alpha - \beta] )</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \langle A^2B \rangle )</td>
<td>2</td>
<td>( \mathbb{Q}[\alpha + \beta] )</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \langle A^2B \rangle )</td>
<td>2</td>
<td>( \mathbb{Q}[\beta] )</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \langle B \rangle )</td>
<td>2</td>
<td>( \mathbb{Q}[\alpha] )</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \langle A \rangle )</td>
<td>( \sqrt{\ } )</td>
<td>4</td>
<td>( \mathbb{Q}[\sqrt{2}] )</td>
<td>( \mathbb{Q}[x^2 - 2] )</td>
<td>2</td>
</tr>
</tbody>
</table>
Exercise 9:

The zeros of the polynomial \( f(x) = x^6 - 18x^3 + 6 \) (a quadratic in \( x^3 \)) are:
\[ \alpha, \alpha \omega, \omega \alpha^2, \beta, \beta \omega, \omega \beta^2 \text{ where } \alpha = \frac{1}{\sqrt[3]{9}} + 5\sqrt[3]{3} \text{ and } \beta = \frac{1}{\sqrt[3]{9}} - 5\sqrt[3]{3}, \text{ both of which are positive.} \]

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

Also \( \omega \beta = \frac{1}{\sqrt[3]{6}} \) so \( F = \mathbb{Q}[\alpha, \ \frac{1}{\sqrt[3]{6}}, \ \omega] \).

Now \( |\mathbb{Q}[\alpha, \ \frac{1}{\sqrt[3]{6}}, \ \omega] : \mathbb{Q}[\alpha, \ \frac{1}{\sqrt[3]{6}}]| = 2 \) 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 \( \frac{1}{\sqrt[3]{6}} \) over \( \mathbb{Q}[\alpha] \) to be \( x^6 - 6 \), in which case \( |F: \mathbb{Q}| = 18 \).

Suppose that \( \frac{1}{\sqrt[3]{6}} \in \mathbb{Q}[\alpha] \). We expect to get a contradiction. Since \( \sqrt[3]{3} \in \mathbb{Q}[\alpha] \) we may conclude that \( \mathbb{Q}[\sqrt[3]{3}, \ \frac{1}{\sqrt[3]{6}}] \subseteq \mathbb{Q}[\alpha] \) but since they both have degree 6 over \( \mathbb{Q} \) it follows that \( \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt[3]{3}, \ \frac{1}{\sqrt[3]{6}}] \). Then \( |F : \mathbb{Q}| = 12 \).

There are 12 automorphisms in the Galois group \( G \) of \( F \) over \( \mathbb{Q} \), mapping \( \frac{1}{\sqrt[3]{6}} \) to \( \frac{1}{\sqrt[3]{6}} \), \( \sqrt[3]{6} \omega \) or \( \frac{1}{\sqrt[3]{6}} \omega^2 \), \( \sqrt[3]{3} \) to \( \pm \sqrt[3]{3} \) and \( \omega \) to \( \omega^2 \), in all 12 combinations. Let \( \theta \) map \( \frac{1}{\sqrt[3]{6}} \) to \( \sqrt[3]{6} \omega \) while fixing both \( \sqrt[3]{3} \) and \( \omega \). Then \( \theta \) has order 3 and so \( \langle \theta \rangle \) has order 3 and index 4 in \( G \).

The fixed field of \( \langle \theta \rangle \) must be \( \mathbb{Q}[\sqrt[3]{3}, \omega] \). Under \( \theta \), \( \alpha \to \alpha \omega^r \) 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 \( \sqrt[3]{3} \to -\sqrt[3]{3} \), a contradiction.]

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

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

The only possibility remaining is that \( \alpha \to \alpha \omega^2 \) under \( \theta \). Then \( \alpha^2 \beta \to \alpha^2 \beta \) since \( \alpha^2 \beta = \alpha \sqrt[3]{6} \). But \( \alpha^2 \beta \in \mathbb{Q}[\sqrt[3]{3}] \) so \( \alpha^2 \beta = a + b \sqrt[3]{3} \) for some \( a, b \in \mathbb{Q} \).

Cubing we get \( 54 + 30 \sqrt[3]{3} = a^3 + 3b^3 \sqrt[3]{3} + 3a^2 b \sqrt[3]{3} + 9ab^2 \). Hence
\[ a^3 + 9ab^2 = 54 \text{ and } a^2 b + b^3 = 10. \]

There is an automorphism \( \rho \) of \( \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt[3]{3}, \ \frac{1}{\sqrt[3]{6}}] \) that maps \( \sqrt[3]{3} \to -\sqrt[3]{3} \) and fixes \( \frac{1}{\sqrt[3]{6}} \). Clearly \( \rho \) swaps \( \alpha \) and \( \beta \). Now \( \alpha \beta^2 = \beta \sqrt[3]{6} = a - b \sqrt[3]{3} \). Hence
\[ 6 = \alpha^3 \beta^3 = a^2 - 3b^2 \text{ whence } 6b = a^2 b - 3b^3. \]

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 \( \alpha \) and \( \beta \) are positive, \( a = 3 \). Hence \( \sqrt[3]{6} = \alpha \beta = (\alpha^2 \beta) / \alpha = \frac{3 + \sqrt[3]{3}}{\alpha} \in \mathbb{Q}[\alpha, \ \sqrt[3]{3}] = \mathbb{Q}[\alpha] \).

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

Now \( \alpha \sqrt[3]{6} = \sqrt[3]{(9 + 5 \sqrt[3]{3})} \sqrt[3]{6} = \sqrt[3]{54 + 30 \sqrt[3]{3}} = 3 + \sqrt[3]{3} \) 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, suppose that it is true. Either you will get a contradiction, in which case it is false, or you will get some
specific information that enables you to show that it is true. Of course your proof that it is true must not 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:

\[
\begin{array}{cccccccccccc}
\sqrt[3]{3} & \sqrt[3]{3} & \sqrt[3]{3} & -\sqrt[3]{3} & -\sqrt[3]{3} & \sqrt[3]{3} & \sqrt[3]{3} & -\sqrt[3]{3} & -\sqrt[3]{3} & \sqrt[3]{3} & \sqrt[3]{3} & -\sqrt[3]{3} & -\sqrt[3]{3} \\
\omega & \omega & \omega & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 \\
i & i & i & i & -i & -i & -i & -i & -i & -i & i & i & i \\
\end{array}
\]

The Galois group is \( \langle A, B \mid A^6 = B^2 = 1, BA = A^{-1}B \rangle \cong D_{12} \).

### Exercise 10:

The zeros of \( x^6 - 6x^3 + 6 \) are \( \alpha, \alpha\omega, \alpha\omega^2, \beta, \beta\omega, \beta\omega^2 \) where \( \alpha = \sqrt[3]{3} + \sqrt[3]{3} \) and \( \beta = \sqrt[3]{3} - \sqrt[3]{3} \). The splitting field is \( F = \mathbb{Q}[\alpha, \beta, \omega] \). Note that \( \sqrt[3]{3} = \alpha^3 - 3 \in F \), \( \beta^3 - 3 = -\sqrt[3]{3} \) 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 \( |\mathbb{Q}[\alpha] : \mathbb{Q}| = 6 \). It seems likely that \( \mathbb{Q}[\alpha, 6^{1/3}] : \mathbb{Q}[\alpha] = 3 \), in which case \( |\mathbb{Q}[\alpha, 6^{1/3}] : \mathbb{Q}| = 18 \) and \( |\mathbb{Q}[f(x)] : \mathbb{Q}| = 36 \). Let us assume this and return to consider the possibility that \( 6^{1/3} \in \mathbb{Q}[\alpha] \) later. (Remember what happened in the last exercise.)

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

\[
\begin{array}{ccc}
\alpha & 6^{1/3} & \omega & \beta = 6^{1/3}/\omega \\
\alpha\omega & 6^{1/3} & \omega & \beta\omega^2 \\
\alpha & 6^{1/3} & \omega & \beta \\
\end{array}
\]
and is \(\langle A, B, C \mid A, B, C, D \rangle \) where \(A = A^3, B^3, C^2, D^2, AB = BA, CA = A^{-1}C, DA = A^{-1}D, CB = BCA, BD = DB^{-1}, CD = DC\).

We won’t calculate the subgroups and their fixed fields. We will finish by considering the possibility that \(6^{1/3} \in Q[\alpha]\). If it is, then we will need to rethink our Galois group.

Suppose that \(6^{1/3} \in Q[\alpha]\). Now \(Q[\alpha]\) has as a basis over \(Q\) \(\{1, \alpha, \alpha^2, \alpha^4, \alpha^5\}\) and hence \(6^{1/3} = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\alpha^5\) for some \(a, b, c, d, e, f \in Q\).

Under A this maps to

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

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 \(Q[\alpha, \omega]\) which has a basis \(\{1, \alpha, \alpha^2, \alpha^4, \alpha^5, \omega, \alpha\omega, \alpha^2\omega, \alpha^3\omega, \alpha^4\omega, \alpha^5\omega\} \) over \(Q\).

**Case 1:** \(6^{1/3} \rightarrow 6^{1/3}\omega\): Then

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

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

**Case 2:** \(6^{1/3} \rightarrow 6^{1/3}\omega^2\): Then

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

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

and equating corresponding coefficients we get \(a = c = d = f = 0\) and \(6^{1/3} = b\alpha + e\alpha^4\)

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

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

Where \(g = b + 3e \in Q\).

Cubing, \(6\) is linearly independent over \(Q\),

\[3g^3 + 27g^2e + 9ge^2 + 3e^3 = 6\]

\[9g^2e + 9e^3 + g^3 + 9ge^2 = 0.\]

If \(e = 0\) then \(g^3 = 2\), a contradiction. So \(e \neq 0\). Let \(x = g/e \in Q\). Then the second equation \(x^3 + 9x^2 + 9x + 9 = 0\).

Mod 5 this polynomial becomes \(x^3 - x^2 - x - 1\). Since this has no zeros in \(Z_5\), the cubic \(x^3 + 9x^2 + 9x + 0\) is prime over \(Q\) and hence has no rational zeros, a contradiction.

**Case 3:** \(6^{1/3} \rightarrow 6^{1/3}\omega^2\): Then

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

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

and equating corresponding coefficients we get \(a = b = d = e = 0\) and \(6^{1/3} = c\alpha^2 + f\alpha^5\)

\[= \alpha^2(c + f\sqrt[3]{3})\]

\[= \alpha^2(g + f\sqrt[3]{3})\]

Where \(g = c + 3f\).

Cubing, \(6\) is linearly independent over \(Q\),

\[(12 + 6\sqrt[3]{3})(g + f\sqrt[3]{3})^3\]

\[= (12 + 6\sqrt[3]{3})(3g^3 + 3g^2f\sqrt[3]{3} + 9gf^2 + 3f^3\sqrt[3]{3})\]
As this is a large group we will omit the finding of the subgroups and fixed fields.

The degree of 5

Exercise 12:

If \( f = 0 \) then \( g^3 = \frac{1}{2} \), a contradiction. So \( f \neq 0 \). Let \( x = \frac{g}{f} \in Q \).

Then from the last equation \( x^3 + 6x^2 + 9x + 6 = 0 \).

This is prime over \( Q \) by Eisenstein and so has no rational zeros, a contradiction.

Exercise 11:

The zeros of \( x^{15} - 1 \) are 1, 0, \( \theta^2, \ldots, \theta^{14} \), and 0 where \( \theta = e^{2\pi i/15} \). The splitting field is \( Q[\theta] \).

Under an automorphism \( \theta \) can only map to \( \theta^r \) where \( r \) is coprime with 15. Moreover all such possibilities arise. So the Galois group has order \( \varphi(15) = 8 \). The automorphisms are:

\[
\begin{array}{cccccccc}
0 & \mapsto & 0 & 0^2 & 0^4 & 0^7 & 0^8 & 0^{11} & 0^{13} & 0^{14} \\
1 & \mapsto & 1 & 4 & 2 & 4 & 4 & 2 & 4 & 2 \\
\end{array}
\]

The Galois group is \( \langle A, B | A^3 = B^2 = 1, BA = AB \rangle \cong C_4 \times C_2 \).

Exercise 12:

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

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

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

\( 5^{1/3} \in Q[7^{1/5}] \) and \( Q[5^{1/3}] \leq Q[7^{1/5}] \).

If \( r < 3 \) then \( Q[5^{1/3}] \) has degree 3 over \( Q \), but 3 does not divide 5. Thus \( r = 3 \) and so \( Q[5^{1/3}, 7^{1/5}] \) has degree 15 over \( Q \).

The degree of \( \sigma \) over \( Q[5^{1/3}, 7^{1/5}] \) is the same as its degree over \( Q \) which is \( \varphi(15) = 8 \).

The degree of the splitting field over \( Q \) is thus \( 15 \times 8 = 120 \).

The Galois Group is generated by:

\[
\begin{array}{cccc}
5^{1/3} & 5^{1/5} & 5^{1/5} & 5^{1/5} \\
7^{1/5} & 7^{1/5} \sigma^3 & 7^{1/5} \sigma^3 & 7^{1/5} \sigma^3 \\
\sigma & \sigma & \sigma^2 & \sigma^{-1} \\
\end{array}
\]

and the Galois group is:

\( \langle A, B, C, D | A^4 = B^4 = C^4 = D^2 = 1, BA = AB, CA = A^{-1}C, DA = A^{-1}D, CB = B^3C, DB = B^3D, DC = CD \rangle \).

As this is a large group we will omit the finding of the subgroups and fixed fields.
Exercise 13:

\[ f(x) = x^{30} - 30x^{15} + 216 \text{ factorises as } (x^{15} - 12)(x^{15} - 18) \text{ and so its zeros are: } \]
\[ 12^{1/15}0^6, 18^{1/15}0^8 \text{ for } n = 0, 1, 2, \ldots, 14. \]

The splitting field is \( \mathbb{Q}[12^{1/15}, 18^{1/15}, 0] \).

Now \( 2^{1/3} = \frac{(12^{1/15})^2}{18^{1/15}} \) so the splitting field is \( \mathbb{Q}[2^{1/15}, 2^{1/3}, 0] \). 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 \( 12^{6/15} \in \mathbb{Q}[2^{1/3}] \) and so \( 12^{6/15} = a + b2^{1/3} + c2^{2/3} \) for some \( a, b, c \in \mathbb{Q} \). Under the automorphism of \( \mathbb{Q}[2^{1/3}, \omega] \) that maps \( 2^{1/3} \to 2^{1/3} \alpha \) and fixes \( \omega \), \( 12^{1/15} \) must map to \( 12^{6/15} \beta \) for some \( \beta \).

Thus \( 3 \beta \) and \( 12^{1/15} = 2^{6/3} (m/n) \) for some coprime integers \( m, n \). So \( 12^{1/15} = 2^m m^{15} \).

Hence 15 divides \( r \) and so \( r = 15 \). The degree of \( \mathbb{Q}[12^{1/15}, 2^{1/3}, 0] \) over \( \mathbb{Q} \) is \( 15 \times 3 \times 8 = 360 \).

The Galois group is generated by:

\[
\begin{array}{cccc}
12^{1/15} & 12^{1/15} & 12^{1/15} & 12^{1/15} \\
2^{1/3} & 2^{1/3} & 0^5 & 2^{1/3} \\
0 & 0 & 0^2 & 0^{-1} \\
\end{array}
\]

The Galois group is \( \langle A, B, C, D | A^{15} = B^3 = C^4 = D^2 | BA = AB, CA = A^8 C, DA = A^{-1} D, CB = B^{-1} C, DB = B^{-1} D, DC = CD \rangle \).

Exercise 14:

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 is 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 \( \omega = \frac{\alpha^2 - 2}{\beta^2 - 2} \) so contains \( \mathbb{Q}[2^{1/3}, \omega] = \mathbb{Q}[x^3 - 2] \). This has degree 6 over \( \mathbb{Q} \). \( |K:Q| \cdot (x^3 - 2) = 8 \).

(A basis is \( \{1, \alpha, \beta, \gamma, \alpha \beta, \beta \gamma, \alpha \gamma, \alpha \beta \gamma\} \). Hence \( |K:Q| \cdot (x^3 - 2) = 48 \). This means that \( |K:Q| \cdot (x^3 - 2) = 48 \).

Each automorphism of \( \mathbb{Q}[x^3 - 2] \) permutes \( \alpha^2, \beta^2, \gamma^2 \) in one of 6 ways. For each of these there are 8 elements of \( K \). For example if \( 2^{1/3} \to 2^{1/3} \alpha \) 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 \( \sqrt{6i} \). 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.

\[
\begin{array}{cccccccc}
\alpha & \beta & -\beta & \beta & -\beta & \beta & -\beta & \beta \\
-\beta & \gamma & \gamma & -\gamma & \gamma & -\gamma & \gamma & -\gamma \\
\gamma & \alpha & \alpha & -\alpha & \alpha & -\alpha & -\alpha & -\alpha \\
2^{1/3} & 2^{1/3} \omega & 2^{1/3} \omega & 2^{1/3} \omega & 2^{1/3} \omega & 2^{1/3} \omega & 2^{1/3} \omega & 2^{1/3} \omega \\
\omega & \omega & \omega & \omega & \omega & \omega & \omega & \omega \\
\sqrt{6i} & -\sqrt{6i} & -\sqrt{6i} & \sqrt{6i} & \sqrt{6i} & \sqrt{6i} & \sqrt{6i} & -\sqrt{6i} \\
\end{array}
\]

We will not write out all 48 automorphisms, let alone describe the Galois group and the Galois correspondence. But let us look at some instances of fixed fields and fixing subgroups.
Which subgroup fixes $Q[\alpha]$? Since $Q[\alpha]$ has degree 6 over $Q$ the subgroup, which we will call $H$, must have order 8. The elements of $H$ must either fix $\beta^2$ and $\gamma^2$ or they must swap them. Restricted to $Q[x^3 = 2]$ they must fix $2^{1/3}$.

<table>
<thead>
<tr>
<th>$\alpha \rightarrow$</th>
<th>1</th>
<th>B</th>
<th>$A^2$B</th>
<th>$A^2$</th>
<th>$A^3$B</th>
<th>A</th>
<th>$A^4$</th>
<th>AB</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta \rightarrow$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
<td>$\gamma$</td>
<td>$-\gamma$</td>
<td>$\gamma$</td>
<td>$-\gamma$</td>
</tr>
<tr>
<td>$\gamma \rightarrow$</td>
<td>$\gamma$</td>
<td>$-\gamma$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
<td>$-\beta$</td>
<td>$-\beta$</td>
</tr>
<tr>
<td>$2^{1/3} \rightarrow$</td>
<td>$2^{1/3}$</td>
<td>$2^{1/3}$</td>
<td>$2^{1/3}$</td>
<td>$2^{1/3}$</td>
<td>$2^{1/3}$</td>
<td>$2^{1/3}$</td>
<td>$2^{1/3}$</td>
<td>$2^{1/3}$</td>
</tr>
<tr>
<td>$\omega \rightarrow$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
</tr>
<tr>
<td>$\sqrt{6}i \rightarrow$</td>
<td>$\sqrt{6}i$</td>
<td>$-\sqrt{6}i$</td>
<td>$-\sqrt{6}i$</td>
<td>$\sqrt{6}i$</td>
<td>$\sqrt{6}i$</td>
<td>$-\sqrt{6}i$</td>
<td>$-\sqrt{6}i$</td>
<td>$\sqrt{6}i$</td>
</tr>
</tbody>
</table>

It is easily checked that this group is $\langle A, B \mid A^4 = B^2 = 1, BA = A^{-1}B \rangle$, the dihedral group $D_8$. Since $Q[\alpha]$ is not a polynomial extension of $Q$ (it does not contain the algebraic conjugates $\beta$ and $\gamma$) $H$ is not a normal subgroup of $G$.

Now let us have an example going in the other direction. Let $C$ be the automorphism that maps $\alpha \rightarrow -\gamma$, $\beta \rightarrow \gamma$, $\gamma \rightarrow \alpha$. This has order 6 and so if $F$ is its fixed field then $|K:F| = 6$. Hence $F$ has degree 8 over $Q$.

Now from a previous table $C$ can be described as follows.

\[
\begin{array}{c|c}
C & \\
\hline
\alpha & -\beta \\
\beta & \gamma \\
\gamma & \alpha \\
2^{1/3} & 2^{1/3} \omega \\
\omega & \omega \\
\sqrt{6}i & -\sqrt{6}i \\
\end{array}
\]

Apart from $\omega$ there is nothing else that is obviously fixed by $C$. We have to do a bit of work. A basis for $K$ over $Q[x^3 = 2]$ 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 $Q[x^3 = 2]$. To simplify things let us suppose these coefficients are in $Q$.

\[
a + b \alpha + c \beta + d \gamma + e \alpha \beta + f \beta \gamma + g \alpha \gamma + h \alpha \beta \gamma = a - b \beta + c \gamma + d \alpha - e \beta \gamma + f \alpha \gamma - g \alpha \beta - h \alpha \beta \gamma.
\]

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 $Q[\omega]$ with a basis \{1, $X$, $Y$, $Z$\} and hence has degree 8 over $Q$ 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 $XY = 6\omega - \omega^2 Z + 2Y$.  

\[112\]