

4. EXAMPLES OF GALOIS GROUPS

§4.1. Overview of Galois Theory

All fields are assumed to be subfields of \mathbf{C} (though much Galois Theory extends to fields in general). If F is a subfield of K we call K an **extension** of F and we can regard it as a vector space over F whose dimension, called the **degree of the extension**, is written $[K:F]$.

The **Galois group** of the extension, $G(K/F)$, is the group of all field automorphisms (1-1 maps from the field to itself which preserve sums and products) which fix the elements of F , with multiplication of maps as the operation. The **fixed field** of a subgroup of $G(K/F)$ is the set of all elements of K which are fixed by every automorphism in the subgroup.

If $\alpha_1, \dots, \alpha_n \in \mathbf{C}$, $F[\alpha_1, \dots, \alpha_n]$ denotes the smallest subfield which contains F and the α_i . If $\alpha_1, \dots, \alpha_n$ are the zeros of $f(x) \in F[x]$ this field is written as $F[f(x) = 0]$ and such an extension is called a **polynomial extension**.

The **minimum polynomial** of $\alpha \in \mathbf{C}$ over F is the monic polynomial $p(x) \in F[x]$ of smallest degree for which $p(\alpha) = 0$. It is a prime polynomial and its degree, n , is the dimension of $F[\alpha]$ over F . In fact $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ is a basis. Numbers with the same minimum polynomial over F are said to be **algebraic conjugates**, over F . Under an automorphism in $G(K/F)$ every element of K must be mapped to one of its algebraic conjugates.

The Galois group of an extension of a field by a polynomial of degree n is isomorphic to a subgroup of S_n . The degree of the extension itself equals the order of the Galois group over F and there is a 1-1 order-reversing correspondance between the subfields and the subgroups with the index of a subgroup being the degree, over F , of its fixed field and with normal subgroups corresponding to polynomial extensions.

If $A \leq B \leq C$ are fields, $[C:A] / [C:B] = [B:A]$. If X, Y are bases for C over B and B over A then a basis for C over A is $\{\beta\gamma \mid \beta \in X, \gamma \in Y\}$. If B and C are polynomial extensions of A , then $G(C/A) / G(C/B) \cong G(B/A)$.

A **radical extension** is one of the form $F[x^n = a]$, for $a \in F$. Radical extensions have abelian Galois groups and so a field which can be reached from F by a sequence of radical extensions has a soluble Galois group over F . A polynomial is soluble by radicals over F if and only if its Galois group is soluble.

The Galois group of a polynomial extension can be computed readily if the zeros of the polynomial are known and can sometimes be obtained indirectly when they are not.

§4.2. $f(x) = x^4 - x^2 - 2$

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

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

(3) Splitting field = $F = \mathbf{Q}[\sqrt{2}, -\sqrt{2}, i, -i] = \mathbf{Q}[\sqrt{2}, i] = \mathbf{Q}[i][\sqrt{2}]$.

(4) $|\mathbf{F}:\mathbf{Q}| = 4$ [= $|\mathbf{F}:\mathbf{Q}[\sqrt{2}]| \times |\mathbf{Q}[\sqrt{2}]:\mathbf{Q}| = 2 \times 2$]

(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 $|\mathbf{F}:\mathbf{Q}| = 4$]

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

$\sqrt{2} \rightarrow$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$i \rightarrow$	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, $\sqrt{2} \rightarrow -\sqrt{2} \rightarrow -\sqrt{2}$ 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:

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

The Galois group is thus isomorphic to $\langle A, B \mid A^2 = B^2 = AB = BA \rangle \cong V_4$.

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

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

SUBFIELD	degree over \mathbf{Q}	SUBGROUP	order
\mathbf{K}	4	1	1
$\mathbf{Q}[i]$	2	$\langle A \rangle$	2
$\mathbf{Q}[\sqrt{2}]$	2	$\langle B \rangle$	2
$\mathbf{Q}[i\sqrt{2}]$	2	$\langle B \rangle$	2
\mathbf{Q}	1	G	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 $\mathbf{K} = \mathbf{Q}[x^4 - x^2 - 2 = 0]$, $\mathbf{Q}[i] = \mathbf{Q}[x^2 + 1 = 0]$, $\mathbf{Q}[\sqrt{2}] = \mathbf{Q}[x^2 - 2 = 0]$, $\mathbf{Q}[i\sqrt{2}] = \mathbf{Q}[x^2 + 2 = 0]$.

§4.3. $f(x) = x^3 - 2$

- (1) Zeros: $2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2$.
 (2) Splitting field = $F = \mathbf{Q}[2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2] = \mathbf{Q}[2^{1/3}, \omega]$.
 (3) The minimum polynomial of $2^{1/3}$ is $x^3 - 2$. Thus $|\mathbf{Q}[2^{1/3}]:\mathbf{Q}| = 3$.
 (4) The minimum polynomial for ω over \mathbf{Q} is $x^2 + x + 1$ and over $\mathbf{Q}[2^{1/3}]$ it is the same.
 (5) $|\mathbf{F}:\mathbf{Q}| = 6$ [= $|\mathbf{F}:\mathbf{Q}[2^{1/3}]| \times |\mathbf{Q}[2^{1/3}]:\mathbf{Q}| = 2 \times 3$]
 (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 $|\mathbf{F}:\mathbf{Q}| = 6$]

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

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

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

(11) Let B = 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:

	1	A	A ²	B	A ² B	AB
$2^{1/3} \rightarrow$	$2^{1/3}$	$2^{1/3}\omega$	$2^{1/3}\omega^2$	$2^{1/3}$	$2^{1/3}\omega$	$2^{1/3}\omega^2$
$\omega \rightarrow$	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 $\omega \rightarrow \omega^2 \rightarrow \omega^2$. 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 .

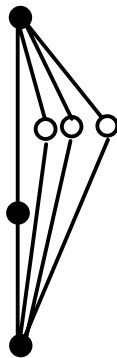
(15) The cyclic subgroup generated by A is a normal subgroup of order 3, that is, of index 2. Its fixed field is thus an extension of \mathbf{Q} of degree 2. Clearly it is $\mathbf{Q}[\omega]$. Because the subgroup is normal the fixed field should be a polynomial extension. Indeed it is. It is $\mathbf{Q}[x^2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

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

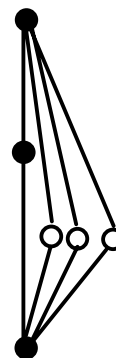
AB fixes $2^{1/3}\omega$ so the fixed field of $\langle AB \rangle$ is $\mathbf{Q}[2^{1/3}\omega]$.

A²B fixes $2^{1/3}\omega^2$ so the fixed field of $\langle A^2B \rangle$ is $\mathbf{Q}[2^{1/3}\omega^2]$.

(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:



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



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

SUBFIELD	poly ext'n	degree over \mathbf{Q}	SUBGROUP	normal	order
$\mathbf{Q}[x^3 = 2]$	\checkmark	6	1	\checkmark	1
$\mathbf{Q}[2^{1/3}]$		3	$\langle B \rangle$		2
$\mathbf{Q}[2^{1/3}\omega]$		3	$\langle AB \rangle$		2
$\mathbf{Q}[2^{1/3}\omega^2]$		3	$\langle A^2B \rangle$		2
$\mathbf{Q}[x^2 + x + 1 = 0]$	\checkmark	2	$\langle A \rangle$	\checkmark	3
\mathbf{Q}	\checkmark	1	G	\checkmark	6

§4.4. $f(x) = x^4 - 2$

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

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

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

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

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

Every automorphism in $G(K/\mathbf{Q})$ 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	$-i$	$-i$	$-i$	$-i$
$2^{1/4} \rightarrow$	$2^{1/4}$	$2^{1/4}i$	$-2^{1/4}$	$-2^{1/4}i$	$2^{1/4}$	$2^{1/4}i$	$-2^{1/4}$	$-2^{1/4}i$

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

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

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

The cyclic subgroup generated by A^2 is another normal subgroup. Since it has index 4 the fixed field must have degree 4 over \mathbf{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 $\mathbf{Q}[i, \sqrt{2}]$. This also must be a polynomial extension. It is $\mathbf{Q}[(x^2 + 1)(x^2 - 2) = 0]$, that $\mathbf{Q}[x^4 - x^2 - 2 = 0]$.

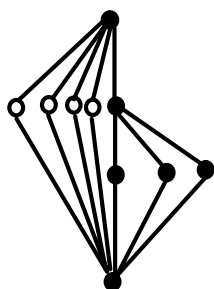
Then there are the subgroups $\langle A^2, B \rangle$ and $\langle A^2, AB \rangle$, both of order 4 (index 2). Their fixed fields will have degree 2 over \mathbf{Q} . The fixed field for $\langle A^2, B \rangle$ is $\mathbf{Q}[\sqrt{2}]$ and for $\langle A^2, AB \rangle$ it is $\mathbf{Q}[\sqrt{2}i]$.

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?

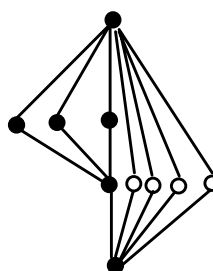
B fixes $2^{1/4}$ so the fixed field of $\langle B \rangle$ is $\mathbf{Q}[2^{1/4}]$.
 A^2B fixes $2^{1/4}i$ so the fixed field of $\langle AB \rangle$ is $\mathbf{Q}[2^{1/4}i]$.

But what does AB fix? A typical element of $\mathbf{Q}[x^4 = 2]$ can be expressed as a linear combination, over \mathbf{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 $x^{AB} = a - b2^{1/4}i - c\sqrt{2} + d2^{3/4}i - ei - f2^{1/4} + g\sqrt{2}i + h2^{3/4}$. If $x^{AB} = x$ then, equating coefficients of our basis elements, we get: $b = -f, c = e = 0, d = h$, and so $x = a + b2^{1/4}(1 - i) + d2^{3/4}(1 + i) + g\sqrt{2}i$. So the fixed field is spanned, as a vector space over \mathbf{Q} , by $1, 2^{1/4}(1 - i), \sqrt{2}i$ and $2^{3/4}(1 + i)$. 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 $\mathbf{Q}[2^{1/4}(1 - i)]$. Similarly the fixed field of $\langle A^3B \rangle$ is $\mathbf{Q}[2^{1/4}(1 + i)]$.

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



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



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

SUBFIELD	poly ext'n	degree over \mathbf{Q}	SUBGROUP	normal	order
$\mathbf{Q}[x^4 = 2]$	\checkmark	8	1	\checkmark	1
$\mathbf{Q}[2^{1/4}(1 - i)]$		4	$\langle AB \rangle$		2
$\mathbf{Q}[2^{1/4}(1 + i)]$		4	$\langle A^3B \rangle$		2
$\mathbf{Q}[2^{1/4}i]$		4	$\langle A^2B \rangle$		2
$\mathbf{Q}[2^{1/4}]$		4	$\langle B \rangle$		2
$\mathbf{Q}[x^2 + 1 = 0]$	\checkmark	2	$\langle A \rangle$	\checkmark	4
$\mathbf{Q}[x^2 = 2]$	\checkmark	2	$\langle A^2, B \rangle$	\checkmark	4
$\mathbf{Q}[x^2 + 2 = 0]$	\checkmark	2	$\langle A^2, AB \rangle$	\checkmark	4
$\mathbf{Q}[x^4 - x^2 - 2 = 0]$	\checkmark	4	$\langle A^2 \rangle$	\checkmark	2
\mathbf{Q}	\checkmark	1	G	\checkmark	8

§4.5. $f(x) = x^5 - 2$

$\mathbf{Q}[x^5 - 2 = 0] = \mathbf{Q}[2^{1/5}, \varepsilon]$ where $\varepsilon = e^{2\pi i/5}$. The minimum polynomial of ε over \mathbf{Q} is $x^4 + x^3 + x^2 + x + 1$ and the minimum polynomial of $2^{1/5}$ over $\mathbf{Q}[\varepsilon]$ is $x^5 - 2$. So the Galois group has order 20 and has the presentation:

$$\langle A, B \mid A^5, B^4, BA = A^{-1}B \rangle.$$

The further details are left to the reader.

§4.6. $f(x) = x^4 - 6x^2 + 3$

This is a quadratic in x^2 with zeros $\pm\sqrt{3 \pm \sqrt{6}}$. The splitting field is $\mathbf{Q}[\alpha, \beta]$ where $\alpha = \sqrt{3 + \sqrt{6}}$ and $\beta = \sqrt{3 - \sqrt{6}}$. Since $x^4 - 6x^2 + 3$ is prime by Eisenstein's Theorem $|\mathbf{Q}[\alpha]:\mathbf{Q}| = 4$ and $|\mathbf{Q}[\beta]:\mathbf{Q}| = 4$.

This might suggest that $|\mathbf{K}:\mathbf{Q}| = 16$. 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 β over \mathbf{Q} has degree 4, its minimum polynomial over $\mathbf{Q}[\alpha]$ is a quadratic. For $\alpha\beta = \sqrt{9 - 6} = \sqrt{3}$, so $\beta = \sqrt{3}/\alpha$ and so $\beta^2 - 3/\alpha^2 = 0$.

That would mean that $|\mathbf{Q}[\alpha, \beta]:\mathbf{Q}[\alpha]| = 2$ and hence $|\mathbf{Q}[\alpha, \beta]:\mathbf{Q}| = 8$ provided that $x^2 - 3/\alpha^2$ is the minimum polynomial of β over $\mathbf{Q}[\alpha]$. But is it? Could it be that β already belongs to $\mathbf{Q}[\alpha]$?

Let's suppose that $\beta \in \mathbf{Q}[\alpha]$ and see if this leads to a contradiction. If so, then $\alpha\beta = \sqrt{3} \in \mathbf{Q}[\alpha]$. But $\alpha^2 \in \mathbf{Q}[\alpha]$ and hence $\sqrt{6}$ and $\sqrt{2}$ belong to $\mathbf{Q}[\alpha]$. Clearly this would mean that $\mathbf{Q}[\alpha] = \mathbf{Q}[\sqrt{2}, \sqrt{3}]$. (It is fairly straightforward to show that $\sqrt{3} \notin \mathbf{Q}[\sqrt{2}]$ and hence that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis for $\mathbf{Q}[\alpha]$ over \mathbf{Q} .)

Thus $\sqrt{3 + \sqrt{6}} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ for some $a, b, c, d \in \mathbf{Q}$. 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 \mathbf{Q} and so:

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

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: $a + d = 0$:

$$\begin{aligned} 7a^2 + 2b^2 + 3c^2 &= 3; \\ a(b - c) &= 0; \\ -a^2 + bc &= 1 \end{aligned}$$

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 \mathbf{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: $b + c = 0$:

$$\begin{aligned} a^2 + 5b^2 + 6d^2 &= 3; \\ b(a - d) &= 0; \\ ad - b^2 &= 1. \end{aligned}$$

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 \mathbf{Q} and so has no rational zeros.

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, $\beta \notin \mathbf{Q}[\alpha]$ and hence $|\mathbf{Q}[\alpha, \beta]:\mathbf{Q}| = 8$ (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 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	A^2B	A^2	A^3B	A	A^3	AB
$\alpha \rightarrow$	α	α	$-\alpha$	$-\alpha$	β	β	$-\beta$	$-\beta$
$\beta \rightarrow$	β	$-\beta$	β	$-\beta$	α	$-\alpha$	α	$-\alpha$
order	1	2	2	2	2	4	4	2

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

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

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

SUBFIELD	poly ext'n	degree over \mathbf{Q}	SUBGROUP	normal	order
$\mathbf{Q}[x^4 - 6x^2 + 3]$	$\sqrt{\quad}$	8	1	$\sqrt{\quad}$	1
$\mathbf{Q}[\alpha - \beta]$		4	$\langle AB \rangle$		2
$\mathbf{Q}[\alpha + \beta]$		4	$\langle A^3B \rangle$		2
$\mathbf{Q}[\beta]$		4	$\langle A^2B \rangle$		2
$\mathbf{Q}[\alpha]$		4	$\langle B \rangle$		2
$\mathbf{Q}[\sqrt{2}]$	$\sqrt{\quad}$	2	$\langle A \rangle$	$\sqrt{\quad}$	4
$\mathbf{Q}[\sqrt{6}]$	$\sqrt{\quad}$	2	$\langle A^2, B \rangle$	$\sqrt{\quad}$	4
$\mathbf{Q}[\sqrt{3}]$	$\sqrt{\quad}$	2	$\langle A^2, AB \rangle$	$\sqrt{\quad}$	4
$\mathbf{Q}[\sqrt{2}, \sqrt{3}]$	$\sqrt{\quad}$	4	$\langle A^2 \rangle$	$\sqrt{\quad}$	2
\mathbf{Q}	$\sqrt{\quad}$	1	G	$\sqrt{\quad}$	8

§4.7. $f(x) = x^6 - 18x^3 + 6$

- (1) Zeros: $\alpha, \alpha\omega, \alpha\omega^2, \beta, \beta\omega, \beta\omega^2$ where $\alpha = \sqrt[3]{9 + 5\sqrt{3}}$ and $\beta = \sqrt[3]{9 - 5\sqrt{3}}$.
- (2) Splitting field = $F = \mathbf{Q}[\alpha, \beta, \omega]$.
- (3) $\sqrt{3} = \alpha^3 - 9 \in F$. Also $\beta^3 - 9 = -\sqrt{3}$.
- (4) $\alpha\beta = \sqrt[3]{6}$
- (5) $F = \mathbf{Q}[\alpha, \sqrt[3]{6}, \omega]$.
- (6) $|\mathbf{Q}[\alpha, \sqrt[3]{6}, \omega] : \mathbf{Q}[\alpha, \sqrt[3]{6}]| = 2$.
- (7) $|\mathbf{Q}[\alpha] : \mathbf{Q}| = 6$ (By Eisenstein $x^6 - 18x^3 + 6$ is prime over \mathbf{Q}).

GUESS: Min poly of $\sqrt[3]{6}$ over $\mathbf{Q}[\alpha]$ is $x^6 - 6$ so $[F:\mathbf{Q}]$ has degree 18 over \mathbf{Q} .

SUPPOSE: $\sqrt[3]{6} \in \mathbf{Q}[\alpha]$. (Expect a contradiction.)

- (8) $\mathbf{Q}[\alpha] = \mathbf{Q}[\sqrt{3}, \sqrt[3]{6}]$
- (9) $[F:\mathbf{Q}] = 12$.
- (10) There are 12 automorphisms in the Galois group, mapping $\sqrt[3]{6}$ to $\sqrt[3]{6}, \sqrt[3]{6}\omega$ or $\sqrt[3]{6}\omega^2, \sqrt{3}$ to $\pm\sqrt{3}$ and ω to ω^2 , in all 12 combinations.
- (11) Let θ map $\sqrt[3]{6}$ to $\sqrt[3]{6}\omega$ while fixing $\sqrt{3}$ and ω .
- (12) θ has order 3 and so $\langle\theta\rangle$ has order 3 and index 4.
- (13) The fixed field of $\langle\theta\rangle$ must be $\mathbf{Q}[\sqrt{3}, \omega]$.
- (14) Under $\theta, \alpha \rightarrow \alpha\omega^r$ or $\beta\omega^r$ for some r .
- (15) $\alpha \rightarrow \beta\omega^r$ is impossible. [For then $\alpha \rightarrow \beta\omega^r, \alpha^3 \rightarrow \beta^3$ and so $\sqrt{3} \rightarrow -\sqrt{3}$ C!]
- (16) $\alpha \rightarrow \alpha$ is impossible. [For then $\alpha \in \mathbf{Q}[\sqrt{3}, \omega] \cap \mathbf{R} = \mathbf{Q}[\sqrt{3}]$ C!]
- (17) $\alpha \rightarrow \alpha\omega$ is impossible [For then $\beta \rightarrow \beta$ and so $\beta \in \mathbf{Q}[\sqrt{3}]$ C!]
- (18) $\alpha \rightarrow \alpha\omega^2$.
- (19) $\alpha^2\beta \rightarrow \alpha^2\beta$ [$\alpha^2\beta = \alpha\sqrt[3]{6}$].
- (20) $\alpha^2\beta \in \mathbf{Q}[\sqrt{3}]$ so $\alpha^2\beta = a + b\sqrt{3}$ for some $a, b \in \mathbf{Q}$.
- (21) $54 + 30\sqrt{3} = a^3 + 3b^3\sqrt{3} + 3a^2b\sqrt{3} + 9ab^2$. [Cubing both sides.]
- (22) $a^3 + 9ab^2 = 54$.
- (23) $a^2b + b^3 = 10$.
- (24) There's an automorphism ρ of $\mathbf{Q}[\alpha] = \mathbf{Q}[\sqrt{3}, \sqrt[3]{6}]$ that maps $\sqrt{3}$ to $-\sqrt{3}$, and fixes $\sqrt[3]{6}$. (25) ρ swaps α and β .
- (26) $\alpha\beta^2 = \beta\sqrt[3]{6} = a - b\sqrt{3}$.
- (27) $6 = \alpha^3\beta^3 = a^2 - 3b^2$. [Multiply (20) and (26).]
- (28) $2b^3 + 3b = 5$. [Subtract (27) $\times b$ from (23) and divide by 2.]
- (29) $b = 1, a = 3$.
- (30) $(3 + \sqrt{3})^3 = 6(9 + 5\sqrt{3})$. So $\sqrt[3]{6} \cdot \sqrt[3]{9 + 5\sqrt{3}} = 3 + \sqrt{3}$.
- (31) So in fact $\sqrt[3]{6} \in \mathbf{Q}[\alpha]$.
- (32) $F = \mathbf{Q}[\sqrt[3]{6}, \sqrt{3}, \omega]$ has degree 12 over \mathbf{Q} . The 12 automorphisms are given by:

	1	A^4	A^2	A^3	A	A^5	B	A^2B	A^4B	A^3B	A^5B	AB
$\sqrt[3]{6} \rightarrow$	$\sqrt[3]{6}$	$\sqrt[3]{6}\omega$	$\sqrt[3]{6}\omega^2$	$\sqrt[3]{6}$	$\sqrt[3]{6}\omega$	$\sqrt[3]{6}\omega^2$	$\sqrt[3]{6}$	$\sqrt[3]{6}\omega$	$\sqrt[3]{6}\omega^2$	$\sqrt[3]{6}$	$\sqrt[3]{6}\omega$	$\sqrt[3]{6}\omega^2$
$\sqrt{3} \rightarrow$	$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$\omega \rightarrow$	ω	ω	ω	ω	ω	ω	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2

The Galois group is $\langle A, B \mid A^6 = B^2 = 1, BA = A^{-1}B \rangle \cong D_{24}$.

§4.8. $f(x) = x^6 - 6x^3 + 6$

(1) The zeros are $\alpha, \alpha\omega, \alpha\omega^2, \beta, \beta\omega, \beta\omega^2$ where $\alpha = \sqrt[3]{3 + \sqrt{3}}, \beta = \sqrt[3]{3 - \sqrt{3}}$ and $\alpha\beta = \sqrt[3]{6}$.

(2) Splitting field = $F = \mathbf{Q}[\alpha, \beta, \omega]$.

(3) Note: $\sqrt{3} = \alpha^3 - 3 \in F, \beta^3 - 3 = -\sqrt{3}, \alpha\beta = \sqrt[3]{6}$

(4) $F = \mathbf{Q}[\alpha, \sqrt[3]{6}, \omega]$.

(5) $|\mathbf{Q}[\alpha, \sqrt[3]{6}, \omega] : \mathbf{Q}[\alpha, \sqrt[3]{6}]| = 2$. and $|\mathbf{Q}[\alpha] : \mathbf{Q}| = 6$.

SUPPOSE: $\sqrt[3]{6} \in \mathbf{Q}[\alpha]$.

(6) $\alpha^2\beta = a + b\sqrt{3}$ for some $a, b \in \mathbf{Q}$.

(7) $18 + 6\sqrt{3} = (a + b\sqrt{3})^3 = a^3 + 3b^3\sqrt{3} + 3a^2b\sqrt{3} + 9ab^2$.

(8) $a^3 + 9ab^2 = 18$.

(9) $a^2b + b^3 = 2$.

(10) $\alpha\beta^2 = a - b\sqrt{3}$.

(11) $6 = \alpha^3\beta^3 = a^2 - 3b^2$.

(12) $2b^3 + 3b - 1 = 0$.

(13) $2x^3 + 3x - 1$ has no zeros in \mathbf{Z}_5 so it has no rational zeros. C!

(14) $F = \mathbf{Q}[\alpha, \sqrt[3]{6}, \omega]$ has degree 36 over \mathbf{Q} . Its Galois group has order 36 and is generated by:

	$\alpha \rightarrow$	$\sqrt[3]{6}$	ω	β
A	$\beta\omega$	$\sqrt[3]{6}$	ω	$\alpha\omega^2$
B	α	$\sqrt[3]{6}\omega$	ω	$\beta\omega$
C	α	$\sqrt[3]{6}$	ω^2	β

A: $\alpha \rightarrow \beta\omega, \sqrt[3]{6} \rightarrow \sqrt[3]{6}, \omega \rightarrow \omega$

B: $\alpha \rightarrow \alpha, \sqrt[3]{6} \rightarrow \sqrt[3]{6}\omega, \omega \rightarrow \omega$.

C: $\alpha \rightarrow \alpha, \sqrt[3]{6} \rightarrow \sqrt[3]{6}, \omega \rightarrow \omega^2$

and is $\langle A, B, C \mid A^3, B^3, C^2, D^2, AB = BA, AC = CA^{-1}, AD = DA^{-1}, BC = CBA, BD = DB^{-1}, CD = DC \rangle$.

§4.9. $f(x) = x^{15} - 1$

(1) Zeros: $1, \theta, \theta^2, \dots, \theta^{14}$ where $\theta = e^{2\pi i/15}$

(2) Splitting field: $\mathbf{Q}[\theta]$

(3) 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 $\phi(15) = 8$.

(4) The automorphisms are:

	1	A	A^2	A^3B	A^3	A^2B	AB	B
θ	θ	θ^2	θ^4	θ^7	θ^8	θ^{11}	θ^{13}	θ^{14}
order	1	4	2	4	4	2	4	2

(5) The Galois group is $\langle A, B \mid A^4 = B^2 = 1, BA = AB \rangle$

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

- (1) $(x^3 - 5)(x^5 - 7)$
- (2) Zeros: $5^{1/3}, 5^{1/3}\omega, 5^{1/3}\omega^2, 7^{1/5}, 7^{1/5}\theta, 7^{1/5}\theta^2, 7^{1/5}\theta^3, 7^{1/5}\theta^4, 7^{1/5}\theta^5, 7^{1/5}\theta^6$
where $\omega = e^{2\pi i/3}$ and $\theta = e^{2\pi i/5}$.
- (3) $\mathbf{Q}[\omega, \theta] = \mathbf{Q}[\sigma]$ where $\sigma = e^{2\pi i/15}$.
- (4) Splitting Field: $\mathbf{Q}[5^{1/3}, 7^{1/5}, \sigma]$
- (5) Let r be the degree of $5^{1/3}$ over $\mathbf{Q}[7^{1/5}]$. Then a product of r zeros of $x^3 - 5$ is in $\mathbf{Q}[7^{1/5}]$ and so $5^{r/3} \in \mathbf{Q}[7^{1/5}]$ and $\mathbf{Q}[5^{r/3}] \leq \mathbf{Q}[7^{1/5}]$.
- (6) If $r < 3$ then $\mathbf{Q}[5^{r/3}]$ has degree 3 over \mathbf{Q} , but 3 does not divide 5. Thus $r = 3$.
- (7) Hence $\mathbf{Q}[5^{1/3}, 7^{1/5}]$ has degree 15 over \mathbf{Q} .
- (8) The degree of σ over $\mathbf{Q}[5^{1/3}, 7^{1/5}]$ is the same as its degree over \mathbf{Q} which is $\phi(15) = 8$.
- (9) The degree of the splitting field over \mathbf{Q} is $15 \times 8 = 120$.
- (10) The Galois Group is generated by:

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

- (11) The Galois Group is $\langle A, B, C, D \mid A^3 = B^5 = C^4 = D^2 = 1, BA = AB, CA = A^{-1}C, DA = A^{-1}D, CB = B^3C, DB = B^{-1}D, DC = CD \rangle$

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

- (1) $(x^{15} - 12)(x^{15} - 18)$
- (2) Zeros: $12^{1/15}\theta^n, 18^{1/15}\theta^n$ for $n = 0, 1, 2, \dots, 14$.
- (3) Splitting field: $\mathbf{Q}[12^{1/15}, 18^{1/15}, \theta]$
- (4) $2^{1/3} = \frac{(12^{1/15})^2}{18^{1/15}}$ so splitting field = $\mathbf{Q}[12^{1/15}, 2^{1/3}, \theta]$
- (4) Let r = degree of $12^{1/15}$ over $\mathbf{Q}[2^{1/3}]$. Then a product of r zeros of $x^{15} - 12$ is in $\mathbf{Q}[2^{1/3}]$.
- (5) Hence $12^{r/15} \in \mathbf{Q}[2^{1/3}]$
- (6) Thus $12^{r/15} = a + b2^{1/3} + c2^{2/3}$ for some $a, b, c \in \mathbf{Q}$.
- (7) Under the automorphism of $\mathbf{Q}[2^{1/3}, \omega]$ that maps $2^{1/3} \rightarrow 2^{1/3}\omega$ and fixes ω , $12^{r/15}$ must map to $12^{r/15}\theta^t$ for some t .
- (8) Thus $3|t$ and $12^{r/15} = 2^{s/3}(m/n)$ for some coprime integers m, n .
- (9) $12^r n^{15} = 2^s m^{15}$
- (10) $15 \mid r$, so $r = 15$ [comparing factors of 3]
- (10) The degree of $\mathbf{Q}[12^{1/15}, 2^{1/3}, \theta]$ over \mathbf{Q} is $15 \times 3 \times 8 = 360$.
- (11) The Galois group is generated by:

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

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

§4.12. $f(x) = x^3 - 3x + 1$

Here it is much more difficult to find the zeros (even with the cubic formula). But there is a way of finding the Galois group indirectly in this case due to a curious property of this polynomial.

$$\text{Let } f(x) = x^3 - 3x + 1. \text{ If } \alpha \text{ is a zero of } f(x) \text{ then so is } 1 - \frac{1}{\alpha} \text{ for } f\left(1 - \frac{1}{\alpha}\right) = \left(1 - \frac{1}{\alpha}\right)^3 - 3\left(1 - \frac{1}{\alpha}\right) - 1 = \frac{(\alpha - 1)^3 - 3\alpha^2(\alpha - 1) - \alpha^3}{\alpha^3} = \frac{-\alpha^3 + 3\alpha - 1}{\alpha^3} = 0.$$

The map $\alpha \rightarrow 1 - \frac{1}{\alpha}$ has order 3 and so the three zeros of $f(x)$ have the form $\alpha, \alpha^f, \alpha^{f^2}$ and so if α is any zero $\mathbf{Q}[f(x) = 0] = \mathbf{Q}[\alpha]$. It is not difficult to show that $f(x)$ is prime over \mathbf{Q} and so $|\mathbf{Q}[f(x) = 0]: \mathbf{Q}| = 3$. Thus the Galois group is cyclic of order 3.

§4.13. $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$

Is there a polynomial whose Galois group over \mathbf{Q} is cyclic of order 5? Now $\mathbf{Q}[x^{11} = 1] = \mathbf{Q}[\varepsilon]$ where $\varepsilon = e^{2\pi i/11}$. Its minimum polynomial over \mathbf{Q} is $x^{10} + x^9 + \dots + x^2 + x + 1$ and so $|\mathbf{Q}[x^{11} = 1]: \mathbf{Q}| = 10$. 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 can be generated by the automorphism which maps ε to ε^2 . The automorphisms can be listed as follows:

	1	A	A ²	A ³	A ⁴	A ⁵	A ⁶	A ⁷	A ⁸	A ⁹
$\varepsilon \rightarrow$	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 C_5 is a subgroup of this Galois group, but all that would mean is that $G(\mathbf{Q}[x^{11} = 1]: F)$ is isomorphic to C_5 where F is the fixed field of A^2 . (By the way, what is that?).

But C_5 is also a quotient group of C_{10} . We simply have to factor out by $\langle A^5 \rangle$. Then $G(K/\mathbf{Q}) \cong C_5$ 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 $\mathbf{Q}[x^{11} = 1]$.

It's not difficult to see these are spanned by $\varepsilon + \varepsilon^{10}, \varepsilon^2 + \varepsilon^9, \varepsilon^3 + \varepsilon^8, \varepsilon^4 + \varepsilon^7$ and $\varepsilon^5 + \varepsilon^6$. 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.

If $f(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5$ is the monic quintic with the above real numbers as its zeros, its coefficients can be found by $a_r =$ the sum of all products taken r at a time.

The sum is easy, it's $a_1 = \varepsilon + \varepsilon^{10} + \varepsilon^2 + \varepsilon^9 + \varepsilon^3 + \varepsilon^8 + \varepsilon^4 + \varepsilon^7 + \varepsilon^5 + \varepsilon^6 = -1$. (Remember that $1 + \varepsilon + \varepsilon^2 + \dots + \varepsilon^{10} = 0$.)

The sum of product taken two at a time is:

$$a_2 = (\varepsilon + \varepsilon^{10})(\varepsilon^2 + \varepsilon^9) + (\varepsilon + \varepsilon^{10})(\varepsilon^3 + \varepsilon^8) + \dots + (\varepsilon^4 + \varepsilon^7)(\varepsilon^5 + \varepsilon^6).$$

Now there are 10 such products, yielding 40 products in all. Note that none of these products is 1 since the inverse of each power of ε is in the same term. And since this

expression is fixed by the automorphism A , it must contain each of the 10 non-trivial powers of ϵ the same number of times. So $a_2 = 4(\epsilon + \epsilon^2 + \dots + \epsilon^{10}) = -4$.

When it comes to the sum of products three at a time, we have 10 such products, each with 8 terms, or 80 terms in all. Each of $\epsilon, \epsilon^2, \dots, \epsilon^{10}$ must occur an equal number of times so the expression must be of the form:

$$a_3 = k + \frac{80 - k}{10} (\epsilon + \epsilon^2 + \dots + \epsilon^{10}) = \frac{11k - 80}{10}.$$

Now each product $\epsilon^i \epsilon^j \epsilon^k$ has the form $a^{\pm 1} b^{\pm 1} c^{\pm 1}$ where $a, b, c \in \{\epsilon, \epsilon^2, \epsilon^3, \epsilon^4, \epsilon^5\}$ so for it to equal 1 we must either have the product of two of a, b, c being equal to the third or the product of all three being 1. Whenever we have $ab = c$ there will be two corresponding products equal to 1: abc^{-1} and $a^{-1}b^{-1}c$ and whenever we have $abc = 1$ we will have the two corresponding products abc and $a^{-1}b^{-1}c^{-1}$.

So the number k is simply twice the number of instances of solutions to the equations $x + y = z \pmod{11}$ or $x + y + z = 0 \pmod{11}$ with x, y, z being different elements of the set $\{1, 2, 3, 4, 5\}$. The solutions are: $1 + 2 = 3$; $1 + 3 = 4$; $1 + 4 = 5$; $2 + 3 = 5$; $2 + 4 = 5$.

Hence $k = 10$ and so $a_3 = 3$.

With a_4 there are 5 products, each with 16 terms, making again 80 products of ϵ 's.

So $a_4 = k + \frac{80 - k}{10} (\epsilon + \epsilon^2 + \dots + \epsilon^{10}) = \frac{11k - 80}{10}$, where k is the number of solutions to the equations:

$$\begin{aligned} x + y &= z + w \pmod{11}, \\ x + y + z &= w \pmod{11} \text{ and} \\ x + y + z + w &= 0 \pmod{11} \end{aligned}$$

where x, y, z, w are different elements of the set $\{1, 2, 3, 4, 5\}$.

These solutions are:

$$\begin{aligned} 1 + 4 &= 2 + 3; \\ 2 + 4 &= 1 + 5; \\ 3 + 4 &= 2 + 5; \\ 3 + 4 + 5 &= 1; \\ 1 + 2 + 3 + 5 &= 0. \end{aligned}$$

Hence $k = 10$ and $a_4 = 3$.

Finally for a_5 there is one product with 32 terms. So $a_5 = (11k - 32)/10$ where k is the number of solutions to the equations $u + v = x + y + z \pmod{11}$, $v = x + y + z + u \pmod{11}$ and $x + y + z + u + v = 0 \pmod{11}$ where x, y, z, u, v are the distinct elements of $\{1, 2, 3, 4, 5\}$. The only solutions to any of these equations is $1 + 3 + 4 + 5 = 2$ and so $k = 2$. Hence $a_5 = -1$.

So the polynomial is $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$. This must therefore have C_5 as its Galois group over \mathbf{Q} .