MRQ 2017

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet VI: Galois groups, the Galois correspondence and the Fundamental Theorem of Galois Theory (Solutions)

1. **Let F be a field *not* of characteristic 2 and let K be an extension of F of degree 2. Show that K is a Galois extension of F.**

   Solution: We shall first show that K is a normal extension of F. Choose $\alpha \in K \setminus F$. Then $F(\alpha)$ is a subfield of K with $F \subsetneq F(\alpha) \subseteq K$. As $|K : F| = 2$, an application of the Tower Law shows $K = F(\alpha)$. Let $f(X)$ be the minimum polynomial of α over F. Then $\deg f(X) = 2$ and α is a root of $f(X)$ in K. Therefore $f(X)$ factorizes over K as a product of $X - \alpha$ and, necessarily, another linear factor. Hence $f(X)$ splits over K and as $K = F(\alpha)$ is obtained by adjoining a root of $f(X)$, we conclude K is the splitting field of $f(X)$ over F. Hence K is a normal extension of F.

   Now turn to separability. Let $\beta \in K$. If $\beta \in F$, then the minimum polynomial of β over F is $X - \beta$, which has only one root. Otherwise, as $|K : F| = 2$, we conclude, with use of the Tower Law, that $F(\beta) = K$ and the minimum polynomial of β over F is an irreducible quadratic polynomial over F, say $g(X) = X^2 + bX + c$. Then $Dg(X) = 2X + b$ is a non-zero polynomial of degree 1 since F does not have characteristic 2. As $g(X)$ is irreducible, $Dg(X)$ does not divide $g(X)$, so these polynomials are coprime. Hence $g(X)$ has no repeated roots in its splitting field. This shows that K is a separable extension of F.

   These two observations establish that K is a Galois extension of F.

2. **Find an example of field extensions $F \subseteq K \subseteq L$ such that K is a Galois extension of F, L is a Galois extension of K, but L is not a Galois extension of F.**

   [Hint: Consider $\sqrt[4]{2}$.]

   Solution: Take $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt[4]{2})$. The minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $X^2 - 2$, so $|K : F| = |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$. Also $(\sqrt[4]{2})^2 = \sqrt{2}$, so $K \subseteq L$. We know $|L : \mathbb{Q}| = 4$, as the minimum polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $X^4 - 2$, so the Tower Law tells us $|L : K| = 2$.

   By Question 1, both K is a Galois extension of F and L is a Galois extension of K (though separability comes more easily here since the fields concerned have characteristic zero). However, L is not a normal extension of F, since $X^4 - 2$ is irreducible over $F = \mathbb{Q}$ (by Eisenstein's Criterion), this polynomial has a root (namely $\sqrt[4]{2}$) in L, but does not split over L (as two of its roots are non-real complex numbers). Thus L is not a Galois extension of F.

3. **Let n be a natural number and $F = \mathbb{Q}(\sqrt[n]{2})$. Show that $|F : \mathbb{Q}| = n$. Show that $\mathrm{Gal}(F/\mathbb{Q})$ is trivial or cyclic of order 2 according to whether n is odd or even.**

Solution: Let $f(X) = X^n - 2$. Then $f(X)$ is irreducible over $\mathbb{Q}$, so this is the minimum polynomial of $\sqrt[n]{2}$ over $\mathbb{Q}$. Hence

$$|F : \mathbb{Q}| = |\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}| = n.$$

Let $\phi \in \mathrm{Gal}(F/\mathbb{Q})$. Since $F = \mathbb{Q}(\sqrt[n]{2})$, an element of F is a linear combination (with rational coefficients) of powers of $\sqrt[n]{2}$ and therefore the image of this element under ϕ is determined by the value $\sqrt[n]{2}\phi$ (the image of $\sqrt[n]{2}$ under ϕ). Moreover, if we apply ϕ to the formula

$$(\sqrt[n]{2})^n - 2 = 0$$

(that is, $f(\sqrt[n]{2}) = 0$), we obtain

$$(\sqrt[n]{2}\phi)^n - 2 = 0.$$

Hence ϕ maps $\sqrt[n]{2}$ to a root of $f(X)$ in $F = \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{R}$.

Now the roots of $f(X)$ in $\mathbb{C}$ are $\sqrt[n]{2}\,\omega^i$, for $i = 0, 1, \ldots, n-1$, where $\omega = \mathrm{e}^{2\pi i/n}$. Note ω^i is a real number if and only if it equals 1 or -1. Moreover, -1 occurs only when n is even. Hence if n is odd, $\sqrt[n]{2}\phi = \sqrt[n]{2}$ and ϕ is the identity map. Thus $\mathrm{Gal}(F/\mathbb{Q})$ is trivial if n is odd.

If n is even, then $f(X)$ has two roots in $F = \mathbb{Q}(\sqrt[n]{2})$, namely $\pm\sqrt[n]{2}$. Our argument shows us that $|\mathrm{Gal}(F/\mathbb{Q})| \leqslant 2$. Consider one of these two roots α, $\alpha = \pm\sqrt[n]{2}$. Since both $\sqrt[n]{2}$ and α are roots of the irreducible polynomial $f(X)$ over $\mathbb{Q}$, an application of Lemma 3.5 shows there exists a $\mathbb{Q}$-isomorphism $\psi\colon \mathbb{Q}(\sqrt[n]{2}) \to \mathbb{Q}(\alpha)$ such that $\sqrt[n]{2}\psi = \alpha$. Now as $\alpha = \pm\sqrt[n]{2}$, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[n]{2}) = F$ and hence $\psi \in \mathrm{Gal}(F/\mathbb{Q})$. We conclude that when n is even, $|\mathrm{Gal}(F/\mathbb{Q})| = 2$ and therefore the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ is cyclic of order 2.

4. **Let $f(X) = X^4 + 5X^2 + 5$ over $\mathbb{Q}$.**

   (a) Show that $f(X)$ is irreducible over $\mathbb{Q}$.

   (b) Find a splitting field K for $f(X)$ over $\mathbb{Q}$.

   (c) Find an element of order 4 in $\mathrm{Gal}(K/\mathbb{Q})$.

   (d) Describe the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ up to isomorphism.

Solution: (a) $f(X)$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion applied with prime $p = 5$.

(b) First consider the polynomial

$$g(Y) = Y^2 + 5Y + 5.$$

The roots of $g(Y)$ in $\mathbb{C}$ are

$$\frac{-5 \pm \sqrt{5}}{2} = -\frac{5 + \sqrt{5}}{2} \quad \text{and} \quad -\frac{5 - \sqrt{5}}{2}.$$

Since $f(X) = g(X^2)$, the roots of $f(X)$ are those elements of $\mathbb{C}$ that square to the above roots of $g(Y)$, namely

$$\pm\alpha, \quad \pm\beta$$

where

$$\alpha = \sqrt{\frac{5 + \sqrt{5}}{2}}\, i \qquad \text{and} \qquad \beta = \sqrt{\frac{5 - \sqrt{5}}{2}}\, i. \tag{1}$$

Note

$$\alpha^2 = -\frac{5 + \sqrt{5}}{2},$$

so

$$\sqrt{5} = -5 - 2\alpha^2 \in \mathbb{Q}(\alpha).$$

Also α^2 and β^2 are the two roots of $g(Y)$, so $\alpha^2\beta^2 = 5$ and therefore

$$\beta = -\sqrt{5}/\alpha \in \mathbb{Q}(\alpha)$$

(noting that $\alpha\beta$ is a negative number). [This last observation could also be achieved by explicitly multiplying the formulae (1) for α and β.]

We conclude that

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{\frac{5+\sqrt{5}}{2}}\, i\right)$$

is the splitting field for $f(X)$ over $\mathbb{Q}$ (since it contains the four roots $\pm\alpha$ and $\pm\beta$ and is constructed by adjoing some of these roots).

(c) As K is a finite normal extension of $\mathbb{Q}$ (as the spitting field of $f(X)$), it is a finite Galois extension of $\mathbb{Q}$ and the first part of the Fundamental Theorem of Galois Theory tells us

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K : \mathbb{Q}| = 4$$

(noting that the minimum polynomial of α over $\mathbb{Q}$ is $f(X)$). Furthermore any $\phi \in \mathrm{Gal}(K/\mathbb{Q})$ is determined by its effect on α and must map α to one of the four roots $\pm\alpha$, $\pm\beta$ of $f(X)$ in K. We conclude that each of these choices does indeed determine an element of the Galois group. In particular,

$$\phi\colon \alpha \mapsto \beta$$

determines some element of $\mathrm{Gal}(K/\mathbb{Q})$. As the group has order 4, ϕ is an element of order 2 or 4 (by a corollary of Lagrange's Theorem). Let us calculate ϕ^2.

First

$$\begin{aligned}
\sqrt{5}\phi &= (-5 - 2\alpha^2)\phi \\
&= -5 - 2(\alpha\phi)^2 \\
&= -5 - 2\beta^2 \\
&= -5 + 2\left(\frac{5-\sqrt{5}}{2}\right) \\
&= -\sqrt{5}
\end{aligned}$$

and therefore

$$\beta\phi = (-\sqrt{5}/\alpha)\phi = \sqrt{5}/\beta = -\alpha.$$

Hence

$$\alpha\phi^2 = \beta\phi = -\alpha \neq \alpha.$$

We conclude that $\phi\colon \alpha \mapsto \beta$ determines an element of order 4 in the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

(d) As $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, we conclude

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle\phi\rangle,$$

a cyclic group of order 4.

5. **Let $f(X) = X^8 - 1$ over $\mathbb{Q}$.**

   (a) Factorize $f(X)$ into irreducible polynomials over $\mathbb{Q}$.
   (b) Find a splitting field K for $f(X)$ over $\mathbb{Q}$.
   (c) Determine the elements of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.
   (d) Describe the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ up to isomorphism.

Solution: (a)

$$\begin{aligned} f(X) &= X^8 - 1 \\ &= (X^4 - 1)(X^4 + 1) \\ &= (X^2 - 1)(X^2 + 1)(X^4 + 1) \\ &= (X - 1)(X + 1)(X^2 + 1)(X^4 + 1). \end{aligned} \tag{2}$$

Certainly the linear factors are irreducible over $\mathbb{Q}$, while $X^2 + 1$ is irreducible over $\mathbb{Q}$ since it cannot have any linear factors as its roots are $\pm i \notin \mathbb{Q}$.

Finally consider $X^4 + 1$. If it were factorizable over $\mathbb{Q}$, then it would be factorizable over $\mathbb{Z}$ by Gauss's Lemma. It has no linear factors over $\mathbb{Z}$ as the roots of $X^4 + 1$ are non-real complex numbers. If

$$X^4 + 1 = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$$

is a product of two quadratic factors (which can be assumed to be monic without loss of generality) with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, then

$$\begin{aligned} \alpha + \gamma &= 0, & \alpha\gamma + \beta + \delta &= 0, \\ \alpha\delta + \beta\gamma &= 0, & \beta\delta &= 1. \end{aligned}$$

Hence $\beta = \delta = \pm 1$ and $\alpha = -\gamma$. Therefore

$$\alpha^2 = \beta + \delta = \pm 2,$$

which is impossible. Hence $X^4 + 1$ is irreducible over $\mathbb{Q}$ and Equation (2) above is indeed a factorization of $X^8 - 1$ into irreducible polynomials over $\mathbb{Q}$.

(b) The roots of $X^8 - 1$ in $\mathbb{C}$ are the powers ω^i, for $0 \leqslant i \leqslant 7$, of $\omega = \mathrm{e}^{\pi i/4}$. Hence the splitting field of $X^8 - 1$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\omega) = \mathbb{Q}(\mathrm{e}^{\pi i/4})$.

(c) Our element ω is a root of $X^4 + 1$ (since $\omega^4 = \mathrm{e}^{\pi i} = -1$) and this polynomial is then the minimum polynomial of ω over $\mathbb{Q}$. Hence

$$|K : \mathbb{Q}| = |\mathbb{Q}(\omega) : \mathbb{Q}| = 4.$$

As K is the splitting field of a polynomial over $\mathbb{Q}$, it is a finite Galois extenson and the first part of the Fundamental Theorem of Galois Theory says

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K : \mathbb{Q}| = 4.$$

Furthermore, a $\mathbb{Q}$-automorphism of $K = \mathbb{Q}(\omega)$ is determined by its effect on ω and must map ω to a root of its minimum polynomial. Thus the four elements of $\mathrm{Gal}(K/\mathbb{Q})$ are determined by

$$\begin{aligned} \phi_1 &\colon \omega \mapsto \omega, & \phi_2 &\colon \omega \mapsto \omega^3, \\ \phi_3 &\colon \omega \mapsto \omega^5, & \phi_4 &\colon \omega \mapsto \omega^7. \end{aligned}$$

(Noting that the four roots of $X^4 + 1$ are $\mathrm{e}^{\pi i/4} = \omega$, $\mathrm{e}^{3\pi i/4} = \omega^3$, $\mathrm{e}^{5\pi i/4} = \omega^5$ and $\mathrm{e}^{7\pi i/4} = \omega^7$.)

(d) We shall determine the order of the elements of the Galois group. First ϕ_1 is the identity map. We consider ϕ_2, ϕ_3 and ϕ_4. Observe

$$\omega\phi_2^2 = (\omega^3)\phi_2 = (\omega\phi_2)^3 = (\omega^3)^3 = \omega^9 = \omega$$

$$\omega\phi_3^2 = (\omega^5)\phi_3 = (\omega\phi_3)^5 = (\omega^5)^5 = \omega^{25} = \omega$$
$$\omega\phi_4^2 = (\omega^7)\phi_4 = (\omega\phi_4)^7 = (\omega^7)^7 = \omega^{49} = \omega,$$

using the fact that $\omega^8 = 1$. Hence ϕ_2, ϕ_3 and ϕ_4 all have order 2 as elements of the group $\mathrm{Gal}(K/\mathbb{Q})$. We conclude

$$\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2,$$

the Klein 4-group.

6. **Describe the Galois group $\mathbf{Gal}(\mathbb{Q}(i+\sqrt{3})/\mathbb{Q})$.**

Solution: First consider the extension $\mathbb{Q}(i+\sqrt{3})$ of $\mathbb{Q}$. Certainly $\mathbb{Q}(i+\sqrt{3}) \subseteq \mathbb{Q}(i,\sqrt{3})$. The degree of the latter is

$$|\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}| = |\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}| \cdot |\mathbb{Q}(\sqrt{3}) : \mathbb{Q}| = 4,$$

since the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is $X^2 - 3$ and the minimum polynomial of i over $\mathbb{Q}(\sqrt{3})$ is $X^2 + 1$. (Note $X^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt{3})$ as it has no roots in this subfield of $\mathbb{R}$.) It now follows

$$|\mathbb{Q}(i+\sqrt{3}) : \mathbb{Q}| = 2 \text{ or } 4,$$

since $i + \sqrt{3} \notin \mathbb{Q}$.

Now if the minimum polynomial of $i+\sqrt{3}$ were a quadratic, then there would exist $p, q \in \mathbb{Q}$ with

$$(i+\sqrt{3})^2 + p(i+\sqrt{3}) + q = 0;$$

that is,

$$2i\sqrt{3} + pi + p\sqrt{3} + (q+2) = 0.$$

This would imply that $\{i\sqrt{3}, i, \sqrt{3}, 1\}$ were linearly dependent over $\mathbb{Q}$, which contradicts our application of the Tower Law when we concluded $|\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}| = 4$. Hence the minimum polynomial of $i + \sqrt{3}$ over $\mathbb{Q}$ has degree 4 and

$$|\mathbb{Q}(i+\sqrt{3}) : \mathbb{Q}| = 4.$$

Therefore

$$\mathbb{Q}(i+\sqrt{3}) = \mathbb{Q}(i,\sqrt{3})$$

and

$$\mathrm{Gal}(\mathbb{Q}(i+\sqrt{3})/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(i,\sqrt{3})/\mathbb{Q}).$$

An element ϕ in the Galois group of $\mathbb{Q}(i,\sqrt{3})$ over $\mathbb{Q}$ is determined by its effect on i and on $\sqrt{3}$. Furthermore, ϕ must map roots of X^2+1 to themselves and roots of X^2-3 to themselves. Hence

$$i\phi = \pm i \qquad \text{and} \qquad \sqrt{3}\phi = \pm\sqrt{3}. \tag{3}$$

Note $\mathbb{Q}(i,\sqrt{3})$ is the splitting field of $(X^2+1)(X^2-3)$ over $\mathbb{Q}$ and so is a normal extension of $\mathbb{Q}$. As we are working in fields of characteristic zero, the Fundamental Theorem of Galois Theory applies and we know

$$|\mathrm{Gal}(\mathbb{Q}(i,\sqrt{3})/\mathbb{Q})| = |\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}| = 4.$$

It then follows that all four choices listed in Equation (3) above do indeed define $\mathbb{Q}$-automorphisms of $\mathbb{Q}(i,\sqrt{3}) = \mathbb{Q}(i+\sqrt{3})$. Hence the four elements of the Galois group are

$$\phi_1 \colon i \mapsto i,\ \sqrt{3} \mapsto \sqrt{3}; \qquad \phi_2 \colon i \mapsto -i,\ \sqrt{3} \mapsto \sqrt{3};$$
$$\phi_3 \colon i \mapsto i,\ \sqrt{3} \mapsto -\sqrt{3}; \qquad \phi_4 \colon i \mapsto -i,\ \sqrt{3} \mapsto -\sqrt{3}.$$

Equivalently, in terms of the single element $i+\sqrt{3}$,

$$\phi_1 \colon i+\sqrt{3} \mapsto i+\sqrt{3}; \qquad \phi_2 \colon i+\sqrt{3} \mapsto -i+\sqrt{3};$$
$$\phi_3 \colon i+\sqrt{3} \mapsto i-\sqrt{3}; \qquad \phi_4 \colon i+\sqrt{3} \mapsto -i-\sqrt{3}.$$

This describes all elements of the Galois group.

If we wish to determine the structure of the Galois group, observe

$$i\phi_2^2 = (-i)\phi_2 = -(i\phi_2) = -(-i) = i,$$
$$\sqrt{3}\phi_3^2 = (-\sqrt{3})\phi_3 = -(\sqrt{3}\phi_3) = -(-\sqrt{3}) = \sqrt{3},$$

and similarly $i\phi_4^2 = i$ and $\sqrt{3}\phi_4^2 = \sqrt{3}$. We conclude ϕ_2^2, ϕ_3^2 and ϕ_4^2 fix all points in $\mathbb{Q}(i+\sqrt{3})$, so are the identity. Hence

$$\mathrm{Gal}(\mathbb{Q}(i+\sqrt{3})/\mathbb{Q}) \cong C_2 \times C_2,$$

the Klein 4-group.

7. **For each of the following field extensions, find the Galois group, find all of its subgroups, and find the subfield corresponding to each subgroup under the Galois correspondence. Determine which of the subfields are normal extensions of the base field.**

   (a) The splitting field of X^3-1 over $\mathbb{Q}$.
   (b) The splitting field of X^3-2 over $\mathbb{Q}$.
   (c) The splitting field of X^4-1 over $\mathbb{Q}$.
   (d) The splitting field of X^5-1 over $\mathbb{Q}$.
   (e) The splitting field of X^6-1 over $\mathbb{Q}$.
   (f) The splitting field of X^6+X^3+1 over $\mathbb{Q}$.
   (g) $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3})$ over $\mathbb{Q}$.
   (h) The splitting field of X^4-2 over $\mathbb{Q}(i)$.

Solution:

(a) Observe

$$X^3-1 = (X-1)(X^2+X+1),$$

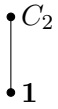
that X^2+X+1 is irreducible over $\mathbb{Q}$ (by Example 1.24(iii) with $p=3$) and that the roots of X^3-1 in $\mathbb{C}$ are $\omega = \mathrm{e}^{2\pi i/3}$, ω^2 and 1. Hence the splitting field of X^3-1 over $\mathbb{Q}$ is $K = \mathbb{Q}(\omega)$. This is a normal separable extension of $\mathbb{Q}$, so the first part of the Fundamental Theorem of Galois Theory tells us

$$|\mathrm{Gal}(K/\mathbb{Q})| = |\mathbb{Q}(\omega) : \mathbb{Q}| = 2.$$

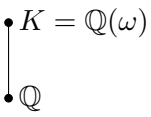
Therefore

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong C_2.$$

This cyclic group has, by Lagrange's Theorem, precisely two subgroups: itself and the trivial subgroup $\mathbf{1}$. The diagram of subgroups is then:



Applying the Galois Correspondence, there are two subfields namely $\mathbb{Q}$ and $K = \mathbb{Q}(\omega)$:



Here $G^* = \mathbb{Q}$ and $\mathbf{1}^* = K$. Finally, as G is abelian, all its subgroups are normal and, correspondingly, all the subfields listed are normal extensions of $\mathbb{Q}$.

(b) The roots of $X^3 - 2$ in $\mathbb{C}$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, where $\omega = \mathrm{e}^{2\pi i/3}$. The splitting field of $X^3 - 2$ over $\mathbb{Q}$ is then $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ and the degree of this extension is

$$|K : \mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})| \cdot |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 6,$$

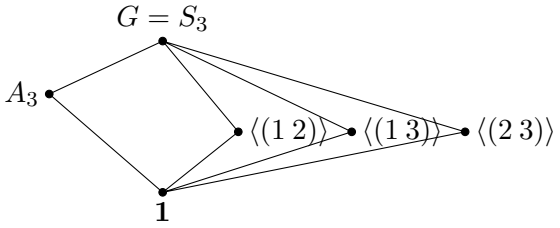
since $X^3 - 2$ is the minimum polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ and $X^2 + X + 1$ is the minimum polynomial of ω over $\mathbb{Q}(\sqrt[3]{2})$.
The Fundamental Theorem of Galois Theory applies (as we are working with a splitting field over a field of characteristic zero), so

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K : \mathbb{Q}| = 6.$$

Furthermore, $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the group of permutations that it induces on the three roots of $X^3 - 2$ in K. Hence, as the group has order 6,

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong S_3.$$

Now S_3 can have subgroups of order 1, 2, 3 and 6, by Lagrange's Theorem. The subgroups of order 2 are cyclic generated by transpositions and the only subgroup of order 3 is $A_3 = \langle(1\ 2\ 3)\rangle$. We conclude the subgroup diagram of S_3 is:



The Galois Correspondence yields the diagram of subfields of K (all of which contain the prime subfield $\mathbb{Q}$). In particular,

$$G^* = S_3^* = \mathbb{Q} \qquad \text{and} \qquad \mathbf{1}^* = K.$$

To determine the other subfields, note that the Fundamental Theorem of Galois Theory tells us

$$|A_3^* : \mathbb{Q}| = \frac{|G|}{|A_3^{**}|} = \frac{|G|}{|A_3|} = 2$$

and

$$|\langle(\alpha\ \beta)\rangle^* : \mathbb{Q}| = \frac{|G|}{|\langle(\alpha\ \beta)\rangle|} = 3$$

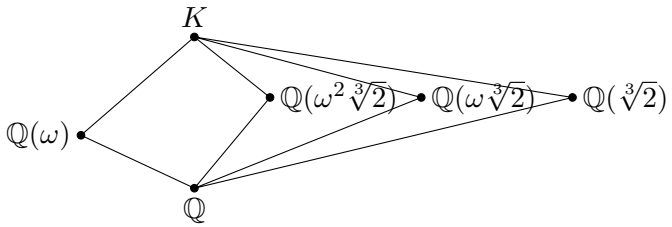
for each transposition $(\alpha\ \beta)$ in S_3. In particular, A_3^* must be the unique subfield of K of degree 2 over $\mathbb{Q}$, so $A_3^* = \mathbb{Q}(\omega)$. The remaining three fields all have degree 3 over $\mathbb{Q}$, so one is certainly $\mathbb{Q}(\sqrt[3]{2})$. However, recall that there are three roots

$$\alpha_1 = \sqrt[3]{2}, \qquad \alpha_2 = \omega\sqrt[3]{2}, \qquad \alpha_3 = \omega^2\sqrt[3]{2}$$

and the three transpositions in S_3 correspond to swapping two of these *and fixing the other*. For example, the transposition (1 3) corresponds to fixing the second root $\alpha_2 = \omega\sqrt[3]{2}$, so the fixed subfield $\langle(1\ 3)\rangle^*$ contains α_2. As $|\mathbb{Q}(\alpha_2) : \mathbb{Q}| = 3$, we conclude $\langle(1\ 3)\rangle^* = \mathbb{Q}(\alpha_2)$. The same argument applies to the other transpositions, so

$$\langle(1\ 2)\rangle^* = \mathbb{Q}(\alpha_3) \qquad \text{and} \qquad \langle(2\ 3)\rangle^* = \mathbb{Q}(\alpha_1).$$

Thus the corresponding diagram of intermediate fields is



Of the subgroups, $\mathbf{1}$, A_3 and S_3 are normal subgroups of S_3 (for example, A_3 has index 2 in S_3, so is normal). The three subgroups of order 2 are not normal in S_3; for example,

$$(1\ 2\ 3)^{-1}\,(1\ 2)\,(1\ 2\ 3) = (2\ 3) \notin \langle(1\ 2)\rangle.$$

Hence $\mathbb{Q}$, $\mathbb{Q}(\omega)$ and K are normal extensions of $\mathbb{Q}$, but $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$ and $\mathbb{Q}(\omega^2\sqrt[3]{2})$ are not.

(c) Observe

$$X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$$

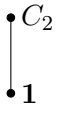
and the four roots of $X^4 - 1$ in $\mathbb{C}$ are ± 1 and $\pm i$. Hence the splitting field of $X^4 - 1$ over $\mathbb{Q}$ is $K = \mathbb{Q}(i)$. We then apply the Fundamental Theorem of Galois Theory to conclude

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K : \mathbb{Q}| = 2,$$

so

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong C_2,$$

a cyclic group of order 2. The subgroup diagram is therefore:



The Galois Correspondence then gives $G^* = \mathbb{Q}$ and $\mathbf{1}^* = K$, each of which is a normal extension of $\mathbb{Q}$, as G is abelian so all its subgroups are normal. The diagram of intermediate fields is:

(d) Observe

$$X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1),$$

that $X^4 + X^3 + X^2 + X + 1$ is irreducible over $\mathbb{Q}$ (by Example 1.24(iii) with $p = 5$), and the roots of $X^5 - 1$ in $\mathbb{C}$ are $\omega = \mathrm{e}^{2\pi i/5}$ and its powers (ω^2, ω^3, ω^4 and 1). Hence the splitting field of $X^5 - 1$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\omega)$ and

$$|K : \mathbb{Q}| = 4.$$

The Fundamental Theorem of Galois Theory then tells us

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K : \mathbb{Q}| = 4.$$

A $\mathbb{Q}$-automorphism of $K = \mathbb{Q}(\omega)$ is determined by its effect on ω and must map ω to one of the four roots of $X^4 + X^3 + X^2 + X + 1$; that is, to ω, ω^2, ω^3 or ω^4. Consider $\phi \in \mathrm{Gal}(K/\mathbb{Q})$ given by

$$\phi\colon \omega \mapsto \omega^2.$$

Observe

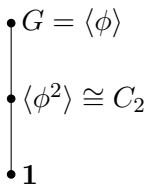
$$\omega\phi^2 = (\omega^2)\phi = (\omega\phi)^2 = (\omega^2)^2 = \omega^4 \neq \omega,$$

so ϕ^2 is not the identity map. We conclude that ϕ is an element of order 4 in the group and

$$G = \mathrm{Gal}(K/\mathbb{Q}) = \langle\phi\rangle \cong C_4,$$

a cyclic group of order 4.

The subgroup diagram of a cyclic group consists of one cyclic subgroup for each divisor of the group order. Hence the subgroups of G are:



When we apply the Galois Correspondence, first

$$G^* = \mathbb{Q} \qquad \text{and} \qquad \mathbf{1}^* = K.$$

The intermediate field $\langle\phi^2\rangle^*$ satisfies

$$|\langle\phi^2\rangle^* : \mathbb{Q}| = \frac{|G|}{|\langle\phi^2\rangle^{**}|} = \frac{|G|}{|\langle\phi^2\rangle|} = 2.$$

Moreover, we calculate

$$(\omega + \omega^4)\phi^2 = \omega\phi^2 + (\omega\phi^2)^4 = \omega^4 + \omega^{16} = \omega + \omega^4$$

and

$$(\omega^2 + \omega^3)\phi^2 = (\omega\phi^2)^2 + (\omega\phi^2)^3 = \omega^8 + \omega^{12} = \omega^2 + \omega^3.$$

Hence both $\omega + \omega^4$ and $\omega^2 + \omega^3$ belong to the fixed field $\langle\phi^2\rangle^*$. Observe

$$\begin{aligned}\big(X - (\omega + \omega^4)\big)\big(X - (\omega^2 + \omega^3)\big) &= X^2 - (\omega + \omega^2 + \omega^3 + \omega^4)X + (\omega + \omega^4)(\omega^2 + \omega^3) \\ &= X^2 - (\omega + \omega^2 + \omega^3 + \omega^4)X + (\omega^3 + \omega^4 + \omega^6 + \omega^7) \\ &= X^2 - (\omega + \omega^2 + \omega^3 + \omega^4)X + (\omega + \omega^2 + \omega^3 + \omega^4) \\ &= X^2 + X - 1,\end{aligned}$$

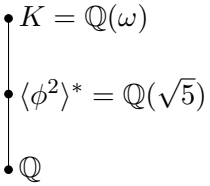
since $1+\omega+\omega^2+\omega^3+\omega^4=0$ as the sum of the roots of X^5-1. Hence $\omega+\omega^4$ and $\omega^2+\omega^3$ are

$$\frac{-1\pm\sqrt{5}}{2}.$$

Therefore

$$\langle\phi^2\rangle^* = \mathbb{Q}(\omega+\omega^4) = \mathbb{Q}\left(\frac{-1+\sqrt{5}}{2}\right) = \mathbb{Q}(\sqrt{5}),$$

noting the latter two fields are equal as one can construct $(-1+\sqrt{5})/2$ from $\sqrt{5}$, and *vice versa*, using field operations and rational numbers. Hence the diagram of subfields is:



As G is abelian, all its subgroups are normal and hence all the above subfields are normal extensions of $\mathbb{Q}$.

(e) Observe that

$$\begin{aligned} X^6-1 &= (X^3-1)(X^3+1) \\ &= (X-1)(X^2+X+1)(X+1)(X^2-X+1) \end{aligned}$$

and the roots of this polynomial are $\omega=\mathrm{e}^{\pi i/3}$ and its powers. Hence the splitting field of X^6-1 over $\mathbb{Q}$ is $\mathbb{Q}(\omega)$ and the degree of the extension is

$$|K:\mathbb{Q}| = |\mathbb{Q}(\omega):\mathbb{Q}| = 2.$$

(Note X^2-X+1 is the minimum polynomial as $\omega^3=-1$ and ω is a root of X^3+1, and $\omega\notin\mathbb{Q}$, so X^2-X+1 is irreducible.) Hence, by the Fundamental Theorem of Galois Theory,

$$|\mathrm{Gal}(K/\mathbb{Q})| = |\mathbb{Q}(\omega):\mathbb{Q}| = 2.$$

Then

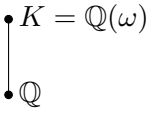
$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong C_2,$$

the subgroup diagram is

and the Galois Correspondence is

$$G^* = \mathbb{Q}, \qquad \mathbf{1}^* = K,$$

with these fields arranged as:



Finally every subgroup of G is normal, as G is abelian, so all the fields listed are normal extensions of $\mathbb{Q}$.

(f) Observe

$$X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1),$$

so the roots of $f(X) = X^6 + X^3 + 1$ are the six ninth roots of 1 that remain when we remove 1, $e^{2\pi/3}$ and $e^{4\pi i/3}$ (the three roots of $X^3 - 1$). Hence the splitting field of $X^6 + X^3 + 1$ is $K = \mathbb{Q}(\omega)$ where $\omega = e^{2\pi i/9}$. (The six roots of $X^6 + X^3 + 1$ are ω, ω^2, ω^4, ω^5, ω^7 and ω^8.)

Observe

$$\begin{aligned} f(X+1) &= (X+1)^6 + (X+1)^3 + 1 \\ &= (X^6 + 6X^5 + 15X^4 + 20X^3 + 15X^2 + 6X + 1) + (X^3 + 3X^2 + 3X + 1) + 1 \\ &= X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3, \end{aligned}$$

which is irreducible over $\mathbb{Q}$, by Eisenstein's Criterion applied with $p = 3$. Hence $f(X)$ is irreducible over $\mathbb{Q}$ and we conclude

$$|K : \mathbb{Q}| = |\mathbb{Q}(\omega) : \mathbb{Q}| = 6.$$

The Fundamental Theorem of Galois Theory applies and shows

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K : \mathbb{Q}| = 6.$$

Moreover any $\mathbb{Q}$-automorphism of $K = \mathbb{Q}(\omega)$ is obtained by its effect on ω and must map ω to one of the six roots of $X^6 + X^3 + 1$. Hence the six elements of the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ are given by

$$\begin{aligned} &\omega \mapsto \omega, && \omega \mapsto \omega^2, \\ &\omega \mapsto \omega^4, && \omega \mapsto \omega^5, \\ &\omega \mapsto \omega^7, && \omega \mapsto \omega^8, \end{aligned}$$

respectively. Consider the element $\phi\colon \omega \mapsto \omega^2$ and its powers:

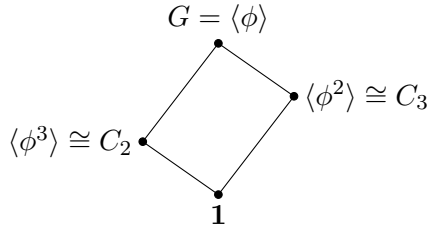
$$\begin{aligned} \omega\phi^2 &= (\omega^2)\phi = (\omega\phi)^2 = (\omega^2)^2 = \omega^4 \neq \omega \\ \omega\phi^3 &= (\omega^4)\phi = (\omega\phi)^4 = (\omega^2)^4 = \omega^8 \neq \omega \\ \omega\phi^6 &= (\omega^8)\phi^3 = (\omega\phi^3)^8 = (\omega^8)^8 = \omega^{64} = \omega \end{aligned}$$

(since $\omega^9 = 1$). Hence ϕ^6 is the identity, but ϕ^2 and ϕ^3 are not. Therefore ϕ is an element of order 6 in the Galois group, so

$$G = \mathrm{Gal}(K/\mathbb{Q}) = \langle\phi\rangle \cong C_6,$$

a cyclic group of order 6.

A cyclic group of order 6 has a unique subgroup of order equal to each divisor of 6, so the diagram of subgroups of the Galois group is:



The Galois Correspondence maps G to $G^* = \mathbb{Q}$ and $\mathbf{1}$ to $\mathbf{1}^* = K$. The intermediate fields $\langle\phi^2\rangle^*$ and $\langle\phi^3\rangle^*$ have degree 2 and 3, respectively, over $\mathbb{Q}$, by the third part of the Fundamental Theorem of Galois Theory. We now determine these fields. First note $\omega^3 = \mathrm{e}^{2\pi/3}$ is a root of X^2+X+1, which is irreducible over $\mathbb{Q}$, so $|\mathbb{Q}(\omega^3) : \mathbb{Q}| = 2$. Therefore

$$\langle\phi^2\rangle^* = \mathbb{Q}(\omega^3).$$

[Indeed, observe

$$(\omega^3)\phi^2 = (\omega\phi^2)^3 = (\omega^4)^3 = \omega^{12} = \omega^3$$

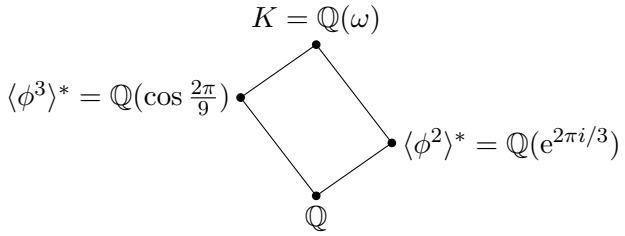
(as $\omega^9 = 1$), so ω^3 does, as claimed, belong to the fixed field $\langle\phi^2\rangle^* = \mathrm{Fix}_K(\langle\phi^2\rangle)$.]
To determine the field $\langle\phi^3\rangle^*$, observe

$$\omega\phi^3 = \omega^8 \qquad \text{and} \qquad (\omega^8)\phi^3 = \omega$$

(since ϕ^3 has order 2). Hence $\omega + \omega^8$ is fixed by ϕ^3, but $\omega + \omega^8 \notin \mathbb{Q}$ (since if it were then there would be an equation $\omega + \omega^8 + p = 0$, with $p \in \mathbb{Q}$, and multiplying by ω gives $1 + p\omega + \omega^2 = 0$, contrary to $\{1, \omega, \omega^2, \ldots, \omega^5\}$ being a basis for $\mathbb{Q}(\omega)$). Therefore $\mathbb{Q}(\omega + \omega^8)$ must be the degree 2 extension of $\mathbb{Q}$ that is fixed by $\langle\phi^3\rangle$. Also $\omega + \omega^8 = \omega + \omega^{-1} = 2\cos\frac{2\pi}{9}$ (as $\omega = \mathrm{e}^{2\pi i/9}$), so

$$\langle\phi^3\rangle = \mathbb{Q}(\omega + \omega^8) = \mathbb{Q}(\cos\tfrac{2\pi}{9}).$$

Hence the diagram of intermediate fields is:



Finally all these fields are normal extensions of $\mathbb{Q}$, since $G = \mathrm{Gal}(K/\mathbb{Q})$ is abelian, so all its subgroups are normal.

(g) Note that the three roots of $X^3 - 5$ in $\mathbb{C}$ are

$$\sqrt[3]{5}, \quad \omega\sqrt[3]{5}, \quad \omega^2\sqrt[3]{5}$$

where

$$\omega = \mathrm{e}^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i.$$

Thus

$$K = \mathbb{Q}(\sqrt[3]{5}, i\sqrt{3}) = \mathbb{Q}(\sqrt[3]{5}, \omega)$$

is the splitting field of $X^3 - 5$ over $\mathbb{Q}$. Also

$$|K : \mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{5}, \omega) : \mathbb{Q}(\sqrt[3]{5})| \cdot |\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}| = 6$$

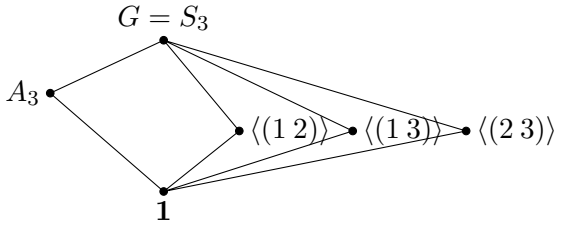
since X^3-5 is the minimum polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$ and X^2+X+1 is the minimum polynomial of ω over $\mathbb{Q}(\sqrt[3]{5})$. Hence, applying the Fundamental Theorem of Galois Theory,

$$|\mathrm{Gal}(K/\mathbb{Q})| = |K : \mathbb{Q}| = 6$$

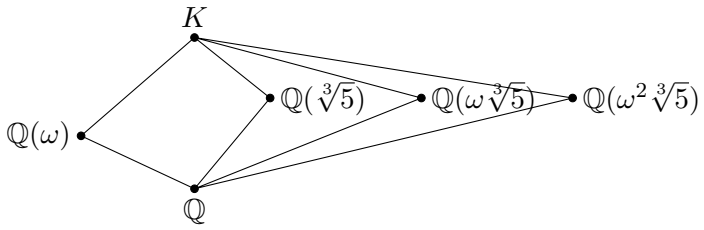
and, since the Galois group is isomorphic to the group of permutations it induces on the three roots of $X^3 - 5$, we conclude

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong S_3,$$

the symmetric group of degree 3.
We now proceed as in part (b). The diagram of subgroups is:



The Galois correspondence determines intermediate fields: First $G^* = \mathbb{Q}$ and $\mathbf{1}^* = K$. The intermediate field A_3^* is a degree 2 normal extension of $\mathbb{Q}$, so must equal $\mathbb{Q}(i\sqrt{3})$. The three subfields $\langle(1\,2)\rangle^*$, $\langle(1\,3)\rangle^*$ and $\langle(2\,3)\rangle^*$ are degree 3 extensions of $\mathbb{Q}$ that are not normal extensions. Moreover as we use transpositions of two of the three roots, in each case the fixed field includes the other of the three roots. We conclude that these three subfields of degree 3 are therefore $\mathbb{Q}(\sqrt[3]{5})$, $\mathbb{Q}(\omega\sqrt[3]{5})$ and $\mathbb{Q}(\omega^2\sqrt[3]{5})$. The diagram of subfields is:



As noted *en route*, K, $\mathbb{Q}(i\sqrt{3})$ and $\mathbb{Q}$ are normal extensions of $\mathbb{Q}$; the other three are not.

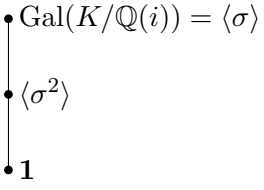
(h) We make use of the work completed in Example 6.13 in the lecture notes. It has been established there that the splitting field of $X^4 - 2$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[4]{2}, i)$, the Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$ (the dihedral group of order 8) generated by σ and τ given by

$$\sigma\colon \sqrt[4]{2} \mapsto i\sqrt[4]{2}, \quad i \mapsto i$$
$$\tau\colon \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad i \mapsto -i,$$

and that $\langle\sigma\rangle^* = \mathbb{Q}(i)$ under the Galois Correspondence between the subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and the subfields of K. Furthermore,

$$\mathrm{Gal}(K/\mathbb{Q}(i)) = \mathbb{Q}(i)^* = \langle\sigma\rangle^{**} = \langle\sigma\rangle.$$

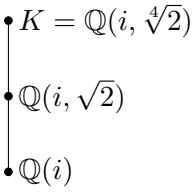
Note that K is also the splitting field of $X^4 - 2$ over $\mathbb{Q}(i)$, so we have determined the Galois group of $X^4 - 2$ over $\mathbb{Q}(i)$ is cyclic of order 4, generated by σ. The diagram of subgroups of subgroups of $\mathrm{Gal}(K/\mathbb{Q}(i))$ is then:



Under the Galois Correspondence between subgroups of $\mathrm{Gal}(K/\mathbb{Q}(i))$ and fields intermediate between K and $\mathbb{Q}(i)$,

$$\langle\sigma\rangle^* = \mathbb{Q}(i), \qquad \mathbf{1}^* = K$$

and $\langle\sigma^2\rangle^*$ is a degree 2 extension of $\mathbb{Q}(i)$. Note σ^2 maps $\sqrt[4]{2}$ to $-\sqrt[4]{2}$ and hence fixes $\sqrt{2} = (\sqrt[4]{2})^2$. Thus $\sqrt{2} \in \langle\sigma^2\rangle^*$ and we conclude therefore that $\langle\sigma^2\rangle^* = \mathbb{Q}(i, \sqrt{2})$. Hence the diagram of intermediate fields is:



Since $\mathrm{Gal}(K/\mathbb{Q}(i)) \cong C_4$, all subgroups are normal and hence each of the above intermediate fields is a normal extension of $\mathbb{Q}(i)$.

8. **Let $f(X) = X^5 - 5X^4 + 5$ over some finite field F. For each of the following groups G either find a finite field F such that the Galois group of $f(X)$ over F is isomorphic to G, or prove that no such field F exists.**

   (a) The trivial group 1.

   (b) The Klein 4-group $V_4 \cong C_2 \times C_2$.

   (c) The cyclic group C_5 of order 5.

   (d) The cyclic group C_6 of order 6.

   (e) The cyclic group C_{10} of order 10.

   (f) The symmetric group S_5 of degree 5.

Solution:

(a) Take $F = \mathbb{F}_5$. Then $f(X) = X^5$ over F, which splits over F. So the splitting field is F and the Galois group $\mathrm{Gal}(F/F)$ is trivial, as required.

(b) If K is the splitting field of $f(X)$ over F (with F of characteristic p for some prime p), then K is a finite field, so $\mathrm{Gal}(K/\mathbb{F}_p)$ is cyclic. Hence $\mathrm{Gal}(K/F)$ is also cyclic (it is the subgroup F^* of $\mathrm{Gal}(K/\mathbb{F}_p)$ under the Galois Correspondence).

Thus there is no choice of F such that $\mathrm{Gal}(K/F)$ is isomorphic to the Klein 4-group.

(c) Take $F = \mathbb{F}_3$. Then $f(X) = X^5 + X^4 + 2$ over $\mathbb{F}_3$. Note

$$f(0) = 2, \quad f(1) = 1, \quad f(2) = 2,$$

so $f(X)$ has no roots, hence no linear factors, in $\mathbb{F}_3$. Therefore if $f(X)$ were reducible over $\mathbb{F}_3$, then it would be a product of a quadratic and a cubic polynomial. Suppose

$$X^5 + X^4 + 2 = (X^3 + \alpha X^2 + \beta X + \gamma)(X^2 + \delta X + \varepsilon),$$

where $\alpha, \beta, \gamma, \delta, \varepsilon \in \mathbb{F}_3$. Then

$$\begin{aligned} \alpha + \delta &= 1, & \alpha\delta + \beta + \varepsilon &= 0, \\ \alpha\varepsilon + \beta\delta + \gamma &= 0, & \beta\varepsilon + \gamma\delta &= 0, \\ & & \gamma\varepsilon &= 2. \end{aligned}$$

Hence $\{\gamma, \varepsilon\} = \{1, 2\}$, so $\gamma = -\varepsilon$. The equation from the X-coefficient then tells us $\beta = \delta$. Note $\beta = \delta \neq 0$, because otherwise the X^4-coefficient would require $\varepsilon = 0$. Then $\beta\delta = \beta^2 = 1$ and the X^2-coefficient equation becomes

$$\gamma(1 - \alpha) = -1 = 2,$$

so $1 - \alpha = \varepsilon$. The X^4-coefficient then gives $\delta = 1 - \alpha = \varepsilon$. Hence the X^3-coefficient now gives

$$\beta(\alpha + 2) = 0.$$

This forces $\alpha = 1$, which yields the contradiction $\beta = \delta = \varepsilon = 0$.

In conclusion, $f(X)$ is irreducible over $\mathbb{F}_3$. Let α be a root of $f(X)$ in some extension. Then $|\mathbb{F}_3(\alpha) : \mathbb{F}_3| = 5$. Hence $\mathbb{F}_3(\alpha) = \mathbb{F}_{3^5}$, which is a normal extension of $\mathbb{F}_3$ as this finite field is constructed as the splitting field of $X^{3^5} - X$. Therefore $f(X)$ splits in $\mathbb{F}_{3^5}$, so $K = \mathbb{F}_{3^5} = \mathbb{F}_3(\alpha)$ is the splitting field of $f(X)$ over $\mathbb{F}_3$.
Thus the Galois group of $f(X)$ over $\mathbb{F}_3$ is

$$\mathrm{Gal}(K/\mathbb{F}_3) = \mathrm{Gal}(\mathbb{F}_{3^5}/\mathbb{F}_3) \cong C_5,$$

cyclic of order 5.

(d) Take $F = \mathbb{F}_2$. Then $f(X) = X^5 + X^4 + 1$ over $\mathbb{F}_2$. Observe

$$(X^2 + X + 1)(X^3 + X + 1) = X^5 + X^4 + 1.$$

Hence $X^5 + X^4 + 1$ is reducible over $\mathbb{F}_2$, but note that $X^2 + X + 1$ and $X^3 + X + 1$ are irreducible over $\mathbb{F}_2$ (having no roots in $\mathbb{F}_2$, hence no linear factors). Therefore the splitting field of $X^2 + X + 1$ over $\mathbb{F}_2$ is $\mathbb{F}_4$ and the splitting field of $X^3 + X + 1$ over $\mathbb{F}_2$ is $\mathbb{F}_8$. (Here we use the fact that finite fields are normal extensions of their prime subfield, so once we adjoin a single root, we have constructed the splitting field.) Therefore the splitting field K is the smallest field containing both $\mathbb{F}_4$ and $\mathbb{F}_8$. As $|\mathbb{F}_4 : \mathbb{F}_2| = 2$ and $|\mathbb{F}_8 : \mathbb{F}_2| = 3$, we conclude that $|K : \mathbb{F}_2| = 6$; that is, $K = \mathbb{F}_{2^6}$.
Hence the Galois group of $f(X)$ over $\mathbb{F}_2$ is

$$\mathrm{Gal}(K/\mathbb{F}_2) = \mathrm{Gal}(\mathbb{F}_{2^6}/\mathbb{F}_2) \cong C_6.$$

(e) Note that the Galois group of $f(X)$ over a field F is isomorphic to some subgroup of the symmetric group S_5 of degree 5. There are no permutations of order 10 in S_5 since the order of a permutation is the lowest common multiple of the cycle lengths. Hence there is no choice of F such that the Galois group of $f(X)$ over F is cyclic of order 10.

(f) As we noted in (b), the Galois group of $f(X)$ over a finite field F must be cyclic. Hence there is no choice of F such that the Galois group is isomorphic to S_5.

9. **Let $f(X)$ be an irreducible polynomial over the finite field $\mathbb{F}_p$ (where p is a prime number). Show that if α is a root of $f(X)$ in some extension field, then $\mathbb{F}_p(\alpha)$ is a splitting field for $f(X)$ over $\mathbb{F}_p$.**

In each of the following cases, let α be a root of $f(X)$. Show that $f(X)$ is irreducible over $\mathbb{F}_p$ and express the roots of $f(X)$ as polynomials in α of degree less than the degree of $f(X)$ [that is, express the roots in terms of our standard basis for the usual extension $\mathbb{F}_p(\alpha)$ over $\mathbb{F}_p$]:

(a) $f(X) = X^2 + 1$, $p = 7$;

(b) $f(X) = X^3 + 2X^2 + X + 1$, $p = 3$.

Solution: Let α be a root of $f(X)$. Then $\mathbb{F}_p(\alpha)$ is a finite extension of $\mathbb{F}_p$, so is isomorphic to some finite field $\mathbb{F}_{p^n}$. This is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$, so $\mathbb{F}_p(\alpha)$ is a normal extension of $\mathbb{F}_p$. Hence, since $f(X)$ is an irreducible polynomial over $\mathbb{F}_p$ with one root in $\mathbb{F}_p(\alpha)$, $f(X)$ necessarily splits over $\mathbb{F}_p(\alpha)$. In conclusion, as we have adjoined the roots of $f(X)$, $\mathbb{F}_p(\alpha)$ is the splitting field of $f(X)$ over $\mathbb{F}_p$.

(a) Consider $f(X) = X^2 + 1$ over $\mathbb{F}_7$. Observe

$$\begin{aligned} f(0) &= 1, & f(1) &= 2, \\ f(2) &= 5, & f(3) &= 3, \\ f(4) &= 3, & f(5) &= 5, \\ f(6) &= 2. \end{aligned}$$

Hence $f(X)$ has no roots in $\mathbb{F}_7$, so no linear factors, and therefore is irreducible over $\mathbb{F}_7$.

Adjoin a root α to $\mathbb{F}_7$ to form the splitting field $\mathbb{F}_7(\alpha)$ of $f(X)$ over $\mathbb{F}_7$. Note that the sum of the roots is 0, so the other root is

$$-\alpha = 6\alpha.$$

(b) Consider $f(X) = X^3 + 2X^2 + X + 1$ over $\mathbb{F}_3$. Observe

$$f(0) = 1, \qquad f(1) = 2, \qquad f(2) = 1,$$

so $f(X)$ has no roots, and hence no linear factors, over $\mathbb{F}_3$. Thus $f(X)$ is irreducible over $\mathbb{F}_3$.

Adjoin a root α to $\mathbb{F}_3$ to form the splitting field $K = \mathbb{F}_3(\alpha)$ over $\mathbb{F}_3$. Note $|K : \mathbb{F}_3| = 3$, so $K \cong \mathbb{F}_{27}$ and

$$\mathrm{Gal}(K/\mathbb{F}_3) = \langle \gamma \rangle$$

is cyclic of order 3 generated by the Frobenius automorphism γ. Since γ permutes the roots of $f(X)$, the roots of $f(X)$ in K must be α, $\alpha\gamma = \alpha^3$ and $\alpha\gamma^2$.

As α is a root of $f(X)$,

$$\alpha\gamma = \alpha^3 = -2\alpha^2 - \alpha - 1 = \alpha^2 + 2\alpha + 2.$$

Rather than calculate $\alpha\gamma^2$ (which is a longer calculation), we shall exploit the fact that the X^2-coefficient of $f(X)$ tells us that the sum of the roots is 1. Hence the third root is

$$1 - \alpha - (\alpha^2 + 2\alpha + 2) = 2\alpha^2 + 2.$$

In conclusion, the three roots of $f(X)$ in the splitting field $\mathbb{F}_3(\alpha)$ are

$$\alpha, \qquad \alpha^2 + 2\alpha + 2, \qquad 2\alpha^2 + 2.$$