Solutions 12

Galois extensions and Galois correspondence

1. Consider the polynomial $f(x) = x^2 - 2$. Determine the Galois group of $K/\mathbb{Q}$, where K is the splitting field. The same question as above for

$$g(x) = (x^2 - 2)(x^2 - 3).$$

Then, via the Galois correspondence, give the factorisation of g over each intermediate field $\mathbb{Q} \subset L \subset K$.

Solution : The splitting field is $K = \mathbb{Q}(\sqrt{2})$. This is an extension of degree 2 of $\mathbb{Q}$, so the Galois group has order 2, and $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. (The two elements are the identity and the automorphism that is constant on rationals and $\sqrt{2} \to -\sqrt{2}$.)

In the second case, the splitting field is $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then the Galois group has order 4, and is therefore isomorphic to either the cyclic group $\mathbb{Z}/4\mathbb{Z}$ or the Klein four-group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since its elements are the automorphisms

$$\sigma_1 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \sigma_2 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \sigma_3 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \qquad \sigma_4 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

and all the non-identity automorphisms have order 2, the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Then the intermediate fields corresponding to the fixed fields of the subgroups $\langle \sigma_i \rangle$, for $i = 2, 3, 4$, are, respectively

$$\mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{6}).$$

The corresponding factorisations are $(x^2 - 2)(x - \sqrt{3})(x + \sqrt{3}), (x - \sqrt{2})(x + \sqrt{2})(x^2 - 3)$, and $(x^2 - 2)(x^2 - 3)$.

2. Let $q = p^n$ be the n-th power of a prime p. Show that the extension $\mathbb{F}_q/\mathbb{F}_p$ is Galois and that its Galois group is the cyclic group C_n generated by the Frobenius endomorphism $\Phi_p(x) = x^p$. Prove that the Main Theorem of Galois theory is true for this extension.

Solution : Denote by H the finite group generated by the Frobenius endomorphism, i.e. $H = \langle \Phi_p \rangle$. The fixed field $\mathbb{F}_q^H$ consists of all $x \in \mathbb{F}_q$ such that $x^p = x$, i.e. $\mathbb{F}_q^H = \mathbb{F}_p$. It follows that $\mathbb{F}_q/\mathbb{F}_p$ is a Galois extension and that H is its Galois group. Hence $H \simeq C_n$.

We show there is a bijective correspondence between subgroups of H and intermediate fields of $\mathbb{F}_p \subset \mathbb{F}_q$. The subgroups of C_n are exactly the subgroups isomorphic to C_d for each d that divides n. In particular, here, they are all $\langle \Phi_p^d \rangle$ for $d|n$. On the other hand, we know that the subfields of $\mathbb{F}_q$ are exactly $\mathbb{F}_{p^d}$ for $d|n$. We see now easily that the fixed field of $\langle \Phi_p^d \rangle$ is $\mathbb{F}_{p^d}$ and that conversely the Galois extension $\mathbb{F}_q/\mathbb{F}_{p^d}$ has Galois group $\langle \Phi_p^d \rangle$, for each $d|n$.

3. Set $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ for $\omega = e^{2\pi i/3}$. Show that $K/\mathbb{Q}$ is Galois and that its Galois group is isomorphic to S_3. Describe the Galois correspondence for this particular example.

   Solution : The extension $K/\mathbb{Q}$ is Galois as one sees that K is the splitting field for $(x^3-2)(x^2+x+1)$ over $\mathbb{Q}$. The Galois group $G = \mathrm{Aut}_{\mathbb{Q}}K$ has order $[K:\mathbb{Q}] = 6$, and its elements are given by

$$\sigma_1 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega \end{cases} \qquad \sigma_2 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \\ \omega \mapsto \omega \end{cases} \qquad \sigma_3 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2 \\ \omega \mapsto \omega \end{cases}$$

$$\sigma_4 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega^2 \end{cases} \qquad \sigma_5 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \\ \omega \mapsto \omega^2 \end{cases} \qquad \sigma_6 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2 \\ \omega \mapsto \omega^2 \end{cases}$$

   Note G acts on the subset of roots $\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$. One can check directly that this action is faithful. Hence the permutation representation $G \to S_3$ gives an isomorphism between G and S_3.

   The intermediate fields of $K/\mathbb{Q}$ are $\mathbb{Q}(\omega)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\omega)$, $\mathbb{Q}(\sqrt[3]{2}\omega^2)$ and the corresponding subgroups are those generated by the 3-cycle and the three transpositions respectively.

4. In this exercise, we give a proof of the Fundamental Theorem of Algebra using Galois theory.
   Let K be a finite field extension of $\mathbb{R}$.

   (a) Assume that $K/\mathbb{R}$ is a Galois extension. Show that there is a chain of fields

$$\mathbb{R} \subset K_1 \subset \cdots \subset K_n = K$$

   with $[K_{i+1}:K_i] = 2$, for $1 \leqslant i \leqslant n-1$, and $[K_1:\mathbb{R}]$ odd.
   Solution : By assumption, $K/\mathbb{R}$ is a Galois extension and denote by G its Galois group. Write the order of G as $|G| = 2^n m$, where m is an odd natural number.
   By Sylow, there exists a subgroup $G_1 < G$ of order $|G_1| = 2^n$. Under the Galois correspondence, there is then an intermediate field K_1 such that

$$[K_1:\mathbb{R}] = [G:G_1] = m.$$

Now repeat the process with the subgroup G_1 of order 2^n. There is a chain of normal subgroups

$$G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1$$

such that each G_l has order 2^{n-l+1}. By Galois correspondence, it corresponds to a chain of intermediate fields

$$K_1 \subset \cdots \subset K_n$$

with $[K_{i+1} : K_i] = 2$.

(b) Recall that if $[K : \mathbb{R}] = 2$, then K is isomorphic to $\mathbb{C}$.

Solution : There exists an element $\alpha \in K$ that is not a real. Then we may set $K = \mathbb{R}(\alpha)$. The irreducible polynomial for α must be of the form

$$f(x) = x^2 + ax + b = \left(x + \frac{a}{2}\right)^2 - \frac{\Delta}{4}.$$

Moreover, the discriminant Δ must be strictly negative, since f is irreducible. Hence, via successive substitutions,

$$K \;=\; \mathbb{R}[x]/(f(x)) \;\simeq\; \mathbb{R}[y]/\left(y^2 - \frac{\Delta}{4}\right) \;\simeq\; \mathbb{R}[z]/(z^2+1) \;\simeq\; \mathbb{C}.$$

(c) Show that if $[K : \mathbb{R}]$ is odd, then $K = \mathbb{R}$.

Solution : There exists an element $\alpha \in K$ that is not a real. The irreducible polynomial for α has degree exactly $[\mathbb{R}(\alpha) : \mathbb{R}]$. Because this degree divides $[K : \mathbb{R}]$, it must be odd. By the Intermediate Value Theorem, the irreducible polynomial must have a real zero. But since the polynomial is by definition irreducible, it must be of degree 1 and $\alpha \in \mathbb{R}$.

(d) Conclude that K is either $\mathbb{R}$ or $\mathbb{C}$.

Solution : The finite extension K is contained in a Galois extension k of $\mathbb{R}$. In particular, for the chain of fields

$$\mathbb{R} \subset K_1 \subset \cdots \subset K_n = k,$$

we conclude from subquestions (b) and (c) that $K_1 = \mathbb{R}$ and, if $n > 1$, $k = K_2 = \mathbb{C}$, since there can be no extension of degree two over $\mathbb{C}$. In fact, assume there was : let $\alpha \in K$ that is not a complex value and $[K : \mathbb{C}] = 2$. But then by the quadratic formula, we know explicitly that the minimal polynomial for α has complex roots, contradicting the irreducibility of the polynomial over $\mathbb{C}$.