PS9 - Galois examples

Math146 - George McNinch

due 2025-04-27 Fri

1 Let p be a prime number and let ζ be a root of $f_p = \dfrac{T^p - 1}{T - 1} \in \mathbf{Q}[T]$ in some extension field of $\mathbf{Q}$. Then we know that $L = \mathbf{Q}(\zeta)$ has $[L : \mathbf{Q}] = p - 1$.

- a. If $i \in \mathbf{Z}$ and $i \not\equiv 0 \pmod p$ explain why ζ^i is a root of f_p.
- b. For $i \in \mathbf{Z}$ with $i \not\equiv 0 \pmod p$ show that there is an automorphism $\phi_i : L \to L$ with the property that $\phi_i(\zeta) = \zeta^i$.
- c. Show for $i, j \in \mathbf{Z}$ with $ij \not\equiv 0 \pmod p$ that $\phi_i = \phi_j$ if and only if $i \equiv j \pmod p$.
- d. Show that the assignment $(\mathbf{Z}/p\mathbf{Z})^\times \to \operatorname{Gal}(L/\mathbf{Q})$ given by $i + p\mathbf{Z} \mapsto \phi_i$ is a well-defined isomorphism of groups.

  Deduce that $\operatorname{Gal}(L/\mathbf{Q})$ is cyclic of order $p - 1$.
- e, If $p = 7$ show that $\operatorname{Gal}(L/\mathbf{Q})$ is generated by ϕ_3.
- f. Again if $p = 7$ find a subgroup $H \subseteq \operatorname{Gal}(L/\mathbf{Q})$ such that $[L^H : \mathbf{Q}] = 3$ and show that $L^H = \mathbf{Q}(\zeta + \zeta^6)$.

  Hint: Note that a typical element of L may be written uniquely in the form

  $$x = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_6\zeta^6$$

  for $a_i \in \mathbf{Q}$. Notice that

  $$\phi_3(x) = a_0 + a_1\zeta^3 + a_2\zeta^6 + a_3\zeta^9 + \cdots + a_6\zeta^{18} = a_0 + a_1\zeta^3 + a_2\zeta^6 + a_3\zeta^2 + \cdots + a_6\zeta^4$$

  Now study $\phi_3^j(x)$ where ϕ_3^j is your generator from e.

2. Observe that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field over $\mathbb{Q}$ of the polynomial $(T^2 - 2)(T^2 - 3)$.

- a Show that $[E : \mathbb{Q}] = 4$ and deduce that $\operatorname{Gal}(L/\mathbf{Q})$ has order 4.
- b. Recall that any group of order 4 is either cyclic or isomorphic to the group

  $$K = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

  Decide whether $\Gamma = \operatorname{Gal}(L/\mathbf{Q})$ is cyclic or is isomorphic to K.
- c. By finding all subgroups of Γ, use the fundamental theorem of Galois theory to list all intermediate fields of the extension $\mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

3. Consider the polynomial $g = T^4 - 3 \in \mathbb{Q}[T]$. According to Eisenstein's criteria, g is irreducible over $\mathbb{Q}$.

   a. Let α be a root of g and let i be a root of $T^2 + 1$. Show that $E = \mathbb{Q}(\alpha, i)$ is a splitting field of g over $\mathbb{Q}$.

   b. Show that $T^2 + 1$ remains irreducible over $\mathbb{Q}(\alpha)$, and conclude that $[E : \mathbb{Q}] = 8$. Deduce that the Galois group $\Gamma = \mathrm{Gal}(E/\mathbb{Q})$ has order 8.

   c. Viewing $E = \mathbb{Q}(i)(\alpha)$ as an extension of $\mathbb{Q}(i)$, show that there is an automorphism $\sigma : E \to E$ for which $\sigma_{|\mathbb{Q}(i)} = \mathrm{id}$ and for which $\sigma(\alpha) = i\alpha$.

   d. Show that $o(\sigma) = 4$ and describe $E^{\langle\sigma\rangle}$ as a primitive extension of $\mathbb{Q}$.

      Hint: Remember that – according to the Fundamental Theorem – $[E : E^{\langle\sigma\rangle}] = |\langle\sigma\rangle| = 4$.

   e. Consider the non-trivial automorphism $\tau_0 : \mathbb{Q}(i) \to \mathbb{Q}(i)$; thus τ_0 is given by "complex conjugation";

      $$\tau_0(a + bi) = \overline{a + bi} = a - bi.$$

      Since E is the splitting field over $\mathbb{Q}(i)$ of g and since $\tau_0 g = g$, our result on automorphisms of splitting fields implies that there is an automorphism

      $$\tau : E \to E$$

      such that $\tau_{|\mathbb{Q}(i)} = \tau_0$ and $\tau(\alpha) = \alpha$.

      Show that $o(\tau) = 2$ and describe $E^{\langle\tau\rangle}$ as a primitive extension of $\mathbb{Q}$.

   f. Explain why $K = E^{\langle\tau\rangle}$ is not a *normal* extension of $\mathbb{Q}$ by exhibiting a polynomial in $\mathbb{Q}[T]$ with a root in K that does not split over K. Deduce that $\langle\tau\rangle$ is not a normal subgroup of Γ and in particular deduce that Γ is not abelian.

   g. Show that $o(\sigma\tau) = 2$ and describe $E^{\langle\sigma\tau\rangle}$ as a primitive extension of $\mathbb{Q}$.

      Hint: Note that the elements $1, \alpha, \alpha^2, \alpha^3$ form a $\mathbb{Q}(i)$-basis for E, so a typical element $x \in E$ may be written uniquely in the form

      $$x = s_0 + s_1\alpha + s_2\alpha^2 + s_3\alpha^3$$

      for $s_i \in \mathbb{Q}(i)$.

      Now, $x \in E^{\langle\sigma\tau\rangle}$ if and only if $\sigma\tau(x) = x$.

      Check that

      $$\sigma\tau(x) = \overline{s_0} + i \cdot \overline{s_1}\alpha - \overline{s_2}\alpha^2 - i \cdot \overline{s_3}\alpha^3$$

      Then check that

      $$(1 + i)\alpha \in E^{\langle\sigma\tau\rangle}.$$