Galois Theory Workshop 4

From splitting fields to the fundamental theorem

There are more questions here than you'll have time for in the workshop. I suggest you start from the beginning and do whatever you do in the time, without hurrying. Keep the other ones for practice another day.

In all questions, you're strongly encouraged to use results from the notes—and this will make your life much easier!

1. Let $M : K$ be a field extension. Let $0 \neq f \in K[t]$, and let $\alpha \in M$ be a roof of f; then $f(t) = (t - \alpha)g(t)$ for some $g(t) \in K(\alpha)[t]$. Prove that

   $$M \text{ is a splitting field of } g \text{ over } K(\alpha) \iff M \text{ is a splitting field of } f \text{ over } K.$$

   You can do this without using any results on the existence or uniqueness of splitting fields.

2. Let K be a field and let $f \in K[t]$ be an irreducible polynomial.
   (i) Prove that the order of $\mathrm{Gal}_K(f)$ is divisible by the number of distinct roots of f in its splitting field.
   (ii) Deduce that if $\mathrm{char}\, K = 0$ then $\deg(f)$ divides $|\,\mathrm{Gal}_K(f)|$.

3. Let $M : K$ be a finite normal separable field extension. Let H be a subgroup of $G = \mathrm{Gal}(M : K)$. Prove that H is a normal subgroup of G if and only if $\mathrm{Fix}(H)$ is a normal extension of K, and that if these conditions hold then $G/H \cong \mathrm{Gal}(\mathrm{Fix}(H) : K)$.

   Can be done very quickly using the fundamental theorem.

4. Prove that every field extension of degree 2 is normal.

   This should remind you of the fact that every subgroup of index 2 is normal.

5. Show that any automorphism of a field M is an automorphism over the prime subfield of M.

6. Show by example that for field extensions $M : L : K$,

   $$M : L \text{ and } L : K \text{ normal} \not\Rightarrow M : K \text{ normal}.$$

   Hint: start by trying the simplest possible examples.

7. (i) Let K be a field and let f and g be nonzero polynomials over K. Put $L = \mathrm{SF}_K(g)$. Show that $\mathrm{SF}_L(f)$ and $\mathrm{SF}_K(fg)$ are isomorphic over K.
   (ii) Let f and g be nonzero polynomials over $\mathbb{Q}$. Prove that $\mathrm{SF}_{\mathbb{Q}}(fg)$ is the compositum of $\mathrm{SF}_{\mathbb{Q}}(f)$ and $\mathrm{SF}_{\mathbb{Q}}(g)$, where all three splitting fields are viewed as subfields of $\mathbb{C}$.

8. Let $0 \neq f \in \mathbb{Q}[t]$ with distinct complex roots $\alpha_1, \ldots, \alpha_k$. Prove that $\sum_{i=1}^{n} \alpha_i^{10}$ is rational. (Hint: Corollary 8.2.7.)

9. Say whether each of the following statements is true or false.
   (i) Let $M : K$ be a field extension of degree 10. Then it is not possible to find extensions $M : L_2 : L_1 : K$ that are all nontrivial.
   (ii) Let $f(t) \in K[t]$ be an irreducible polynomial of degree n. Then $[\mathrm{SF}_K(f) : K] \leq n$.
   (iii) Let $M : K$ be a field extension and $\alpha, \beta \in M$. Then $[K(\alpha\beta) : K] \leq [K(\alpha, \beta) : K]$.

(iv) Let $(x, y) \in \mathbb{R}^2$ and suppose that x and y each have an annihilating polynomial of degree 4 over $\mathbb{Q}$. Then (x, y) is constructible by ruler and compass from $(0, 0)$ and $(1, 0)$.

(v) For all nontrivial finite field extensions $M : \mathbb{Q}$, the Galois group $\mathrm{Gal}(M : \mathbb{Q})$ is nontrivial.

(vi) For all finite extensions $M : K$ and $M' : K'$, every isomorphism $\psi \colon K \to K'$ can be extended to a homomorphism $\varphi \colon M \to M'$.

(vii) A regular 1020-sided polygon can be constructed by ruler and compass, given two points in the plane.

(viii) Let $f \in \mathbb{Q}[t]$ and let $S = \mathrm{SF}_{\mathbb{Q}}(f)$. Then the splitting field of f over $\mathbb{Q}(\sqrt[3]{2})$ is $S(\sqrt[3]{2})$.

(ix) Let f be a polynomial over a field K and let $\theta, \varphi \in \mathrm{Gal}_K(f)$. If $\theta(\alpha) = \varphi(\alpha)$ for all roots α of f in the splitting field of f, then $\theta = \varphi$.

(x) The Galois group of $(t^4 - 2t^3 + t^2 - 4t + 1)^3$ over $\mathbb{Q}$ is solvable.

10. Let $L : K$ be an algebraic extension. Prove that $L : K$ is normal if and only if it has the following property: for every extension $M : L$, the field L is a union of conjugacy classes in M over K.

(Conjugacy over K defines an equivalence relation on M, and a 'conjugacy class in M over K' means an equivalence class of this equivalence relation.)

This should remind you of the fact that a subgroup is normal if and only if it is a union of conjugacy classes in the group-theoretic sense.

11. Look back at Example 1.2.8. There I claimed that the Galois group of an irreducible cubic f over $\mathbb{Q}$ is given by a very strange formula. Here you'll prove it.

Write $\alpha_1, \alpha_2, \alpha_3$ for the complex roots of f, and put

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

(i) Show that $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to A_3 or S_3.

(ii) Show that $\delta \neq 0$.

(iii) Show that $\theta(\delta) = \pm\delta$ for all $\theta \in \mathrm{Gal}_{\mathbb{Q}}(f)$.

(iv) Show that

$$G \cong \begin{cases} A_3 & \text{if } \delta \in \mathbb{Q}, \\ S_3 & \text{otherwise.} \end{cases}$$

(Hint: for the second case, warm up by doing q. 8 first.)

(v) Define

$$\Delta = \delta^2 = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

(This is called the **discriminant** of f.) It is tedious but straightforward to check that if we write

$$B = -(\alpha_1 + \alpha_2 + \alpha_3), \qquad C = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \qquad D = -\alpha_1\alpha_2\alpha_3$$

then

$$\Delta = -27D^2 + 18BCD - 4C^3 - 4B^3D + B^2C^2.$$

I'm not asking you to do this check, but convince yourself that you could do it if need be. Also, this identity implies that $\Delta \in \mathbb{Q}$, but which result from Chapter 8 also implies that $\Delta \in \mathbb{Q}$, with zero calculation?

(vi) Deduce that if we write $f(t)$ as $t^3 + bt^2 + ct + d$ then

$$\mathrm{Gal}_{\mathbb{Q}}(f) \cong \begin{cases} A_3 & \text{if } \sqrt{-27d^2 + 18bcd - 4c^3 - 4b^3d + b^2c^2} \in \mathbb{Q}, \\ S_3 & \text{otherwise.} \end{cases}$$

(vii) Find the Galois group of $t^3 - 3t - 1$.

12. Work through the details of the Galois correspondence for $t^4 - 2t^2 + 9 \in \mathbb{Q}[t]$.

    A hint: if you find yourself handling the square roots of a non-real complex number z, don't just call them $\pm\sqrt{z}$, which is arguably illegitimate anyway (Warning 9.1.1). Instead, put them in the form $x + yi$ with $x, y \in \mathbb{R}$.

13. Let p be a prime. Prove that $\mathrm{Gal}_{\mathbb{Q}}(t^p - 1) \cong C_{p-1}$.

    Hint: begin by rereading Example 7.1.13. Then find an isomorphism between $\mathrm{Gal}_{\mathbb{Q}}(t^p - 1)$ and the multiplicative group of $\mathbb{F}_p$.

14. Let $n \geq 1$. A **primitive nth root of unity** is an element of order n of the multiplicative group $\mathbb{C}^\times$. Equivalently, it is a complex number α such that n is the least positive integer satisfying $\alpha^n = 1$. The **nth cyclotomic polynomial** is

$$\Phi_n(t) = \prod_{\alpha} (t - \alpha),$$

    where the product is over all primitive nth roots of unity α.

    The coefficients of Φ_n are complex numbers. In this question, you'll show that they're actually integers.

    (i) Show that when p is prime, $\Phi_p(t) = t^{p-1} + \cdots + t + 1$ (as in Example 3.3.16).

    (ii) Calculate Φ_n for $n = 1, \ldots, 7$.

    (iii) By considering $\theta_* \Phi_n$ for $\theta \in \mathrm{Gal}_{\mathbb{Q}}(t^n - 1)$, prove that $\Phi_n \in \mathbb{Q}[t]$.

    (iv) Show that $\prod_{d|n} \Phi_d(t) = t^n - 1$, where the product is over all positive integers d dividing n.

    If you did Introduction to Number Theory, you'll know about the Euler function φ. The degree of Φ_n is $\varphi(n)$, and taking degrees on each side of the equation between polynomials $\prod_{d|n} \Phi_d = t^n - 1$ gives an equation between numbers that you may already know: $\sum_{d|n} \varphi(d) = n$.

    (v) Use Gauss's lemma on primitive polynomials to show that whenever $f, g \in \mathbb{Q}[t]$ are monic polynomials such that $fg \in \mathbb{Z}[t]$, then $f, g \in \mathbb{Z}[t]$. (The two usages of 'primitive' in this question are unrelated.)

    (vi) Put together the previous parts to conclude that $\Phi_n \in \mathbb{Z}[t]$.

    One can go further and show that every cyclotomic polynomial Φ_n is irreducible over $\mathbb{Q}$. This is harder. Another way to say it is that the primitive nth roots of unity are all conjugate to one another over $\mathbb{Q}$.