Galois Theory Workshop 4

The fundamental theorem of Galois theory

There are more questions here than you're likely to have time for in the workshop. I suggest you start from the beginning and do whatever you do in the time, without hurrying, then 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. 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.

2. 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.

3. Work through the details of the Galois correspondence for the polynomial $t^3 - 2$ over $\mathbb{Q}$. By 'work through the details', I mean that you should do all the things I did for $t^4 - 2$ in Section 8.3 of the notes. Example 7.1.15 gets you started.

4. 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.

5. 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.

6. Let $M : K$ be a field extension and let S be any subset of $\mathrm{Gal}(M : K)$. Write

   $$\mathrm{Fix}(S) = \{\alpha \in M : \varphi(\alpha) = \varphi \text{ for all } \varphi \in S\}.$$

   (In the notes, I only defined Fix for sub*groups* of $\mathrm{Gal}(M : K)$.)

   (i) Prove that $\mathrm{Fix}(S)$ is a subfield of M. (Hint: you can reduce work by using what you know about equalizers.)

   (ii) Prove that $\mathrm{Fix}(S) = \mathrm{Fix}(\langle S \rangle)$, where $\langle S \rangle$ is the subgroup of $\mathrm{Gal}(M : K)$ generated by S.

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

8. Work through the details of the Galois correspondence for $t^4 - 2t^2 + 9 \in \mathbb{Q}[t]$ (in the same sense as in question 3).

   A hint: it's arguably illegitimate to use the notation '$\sqrt{z}$' when z is a complex number, since z has two square roots and there's no systematic way to decide which one $\sqrt{z}$ should denote. The only exception is when $z \in \mathbb{R}^+$, in which case the convention is that $\sqrt{z}$ denotes the nonnegative square root. If you find yourself handling the square roots of a complex number not in $\mathbb{R}^+$, it may help you to put them in the form $x + yi$ with $x, y \in \mathbb{R}$.

9. 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 of polynomials $\prod_{d|n} \Phi_d = t^n - 1$ gives an equation of numbers you may already be familiar with: $\sum_{d|n} \varphi(d) = n$.

(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 $\mathbb{Q}$.