Galois Theory Workshop 5

Solvability by radicals and finite fields

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 radical number is algebraic.

2. Draw the diagram of subfields of $\mathbb{F}_{p^{30}}$, for a prime p.

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

   Hint: begin by rereading Example 7.1.12 and Lemma 9.1.6.

4. (i) How many subfields does $\mathbb{F}_{243}$ have?

   (ii) Let K and L be fields of order 125. How many isomorphisms $K \to L$ are there?

   (iii) How many homomorphisms $\mathbb{F}_{27} \to \mathbb{F}_{19683}$ are there?

   (iv) How many homomorphisms $\mathbb{F}_4 \to \mathbb{F}_8$ are there?

5. Stewart's book takes a different approach to radicals (his Sections 8.8 and 15.1). Here you'll show that it's equivalent to the one in the notes.

   A field extension $M : K$ is **radical** if $M = K(\alpha_1, \ldots, \alpha_r)$ for some $r \geq 0$ and $\alpha_1, \ldots, \alpha_r \in M$ with the following property: for each $i \in \{1, \ldots, r\}$, there is some $n \geq 1$ such that
   $$\alpha_i^n \in K(\alpha_1, \ldots, \alpha_{i-1}).$$

   Let's say that a complex number is **Stewart-radical** if it belongs to some subfield M of $\mathbb{C}$ such that $M : \mathbb{Q}$ is radical, and write $\mathbb{Q}^{\mathrm{Stew}}$ for the set of Stewart-radical numbers. Your task is to show that $\mathbb{Q}^{\mathrm{Stew}} = \mathbb{Q}^{\mathrm{rad}}$, that is, Stewart-radical $\iff$ radical.

   (i) Let M_1 and M_2 be subfields of $\mathbb{C}$ that are both radical over $\mathbb{Q}$. Prove that there exists a subfield M of $\mathbb{C}$, also radical over $\mathbb{Q}$, that contains both M_1 and M_2. Deduce that $\mathbb{Q}^{\mathrm{Stew}}$ is a subfield of $\mathbb{C}$.

   (ii) Show that if $\alpha \in \mathbb{C}$ and $n \geq 1$ with $\alpha^n \in \mathbb{Q}^{\mathrm{Stew}}$ then $\alpha \in \mathbb{Q}^{\mathrm{Stew}}$.

   (iii) Deduce that $\mathbb{Q}^{\mathrm{rad}} \subseteq \mathbb{Q}^{\mathrm{Stew}}$.

   (iv) Prove by induction on $r \geq 0$ that if $\alpha_1, \ldots, \alpha_r$ are complex numbers satisfying the condition in the definition of radical extension, then $\mathbb{Q}(\alpha_1, \ldots, \alpha_r) \subseteq \mathbb{Q}^{\mathrm{rad}}$. Deduce that $\mathbb{Q}^{\mathrm{Stew}} = \mathbb{Q}^{\mathrm{rad}}$.

6. Let p be a prime number and $m, n \geq 1$ with $m \mid n$. Work out the Galois correspondence for $\mathbb{F}_{p^n} : \mathbb{F}_{p^m}$. (Most of the work for this was already done in Chapter 10.)

7. Let K be a field and $n \geq 1$. Is $\mathrm{Gal}_K(t^n - 1)$ necessary abelian?

   Hint: reread Lemma 9.1.6 and Example 10.3.2.

8. Prove that the rings $\mathbb{F}_3[t]/\langle t^3 + t^2 - t + 1\rangle$ and $\mathbb{F}_3[t]/\langle t^3 - t + 1\rangle$ are isomorphic. (You are not being asked to *construct* an isomorphism.)

9. Prove that $t^5 - 4t + 2$ is not solvable by radicals over $\mathbb{Q}$.

10. Prove the $\Leftarrow$ direction of Lemma 9.2.4. (This is Exercise 9.2.5.)

11. Find an irreducible polynomial of degree 7 over $\mathbb{Q}$ that is not solvable by radicals.

12. Proposition 10.4.6 describes the subfields of a finite field, with a proof that uses the fundamental theorem of Galois theory. The same result can also be proved directly, as follows.

   (i) Show that if a finite field of order q has a subfield of order r then q is a power of r. Deduce that for a prime p and an integer $n \geq 1$, every subfield of $\mathbb{F}_{p^n}$ has order p^m for some $m \mid n$.

   (ii) Let a and b be positive integers such that $b \mid a$. Prove that $(t^b - 1) \mid (t^a - 1)$ in $\mathbb{Z}[t]$.

   (iii) Let m, n and p be positive integers such that $m \mid n$. Prove that $(t^{p^m} - t) \mid (t^{p^n} - t)$ in $\mathbb{Z}[t]$.

   (iv) Let m and n be positive integers such that $m \mid n$, and let p be a prime. Prove that $t^{p^m} - t$ splits in $\mathbb{F}_{p^n}$, and deduce that $\mathbb{F}_{p^n}$ has a subfield of order p^m.

   (v) By considering the number of roots of $t^{p^m} - t$ in $\mathbb{F}_{p^n}$, show there is only one subfield of $\mathbb{F}_{p^n}$ of order p^m.