Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2019

Problem Set # 9 (due in class on Thursday April 18)

Problems:

1. Let K/F be a Galois extension with group S_3.

(a) Prove that there exists an irreducible polynomial $f(x) \in F[x]$ of degree 6 whose splitting field is K.

(b) Assume that the characteristic of F is not 2. Prove that there exists an irreducible polynomial $f(x) \in F[x]$ of degree 3 whose splitting field is K.
Remark. The cubic is more intuitive than the sextic, though slightly harder to prove.

2. More about prime cyclotomic extensions (your midterm preparation might help).

(a) In the cases $p = 5$ and $p = 7$, compute simple generators for each subfield, prove that each is normal over $\mathbb{Q}$, express each as the splitting field of an irreducible polynomial over $\mathbb{Q}$, and draw the lattices of subfields and subgroups of the Galois group.

(b) Find a Galois extension $L/\mathbb{Q}$ whose Galois group is cyclic of order 5 and an irreducible polynomial of degree 5 over $\mathbb{Q}$ whose splitting field is L. **Hint.** Feel free to use the computer for help on the last part.

3. Let $L/\mathbb{Q}$ be a Galois extension whose Galois group is cyclic of order 4. Prove that its unique quadratic subextension $K/\mathbb{Q}$ is real (i.e., $K = \mathbb{Q}(\sqrt{d})$ with $d > 0$). **Hint.** Complex conjugation.

4. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible quartic polynomial and $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x)$. Let $G \subset S_4$ be the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$. Prove that $K/\mathbb{Q}$ has no nontrivial intermediate subfields if and only if $G = A_4$ or $G = S_4$.

5. This problem will guide you through an example of a tower of extensions $K/L/F$, with K/F radical but L/F not radical. Let $K = \mathbb{Q}(\zeta_7)$ and $L = \mathbb{Q}(\zeta_7 + \overline{\zeta}_7)$.

(a) Prove that $K/\mathbb{Q}$ is radical.

(b) Prove that $L/\mathbb{Q}$ is not radical. **Warning.** A simple extension $F(\alpha)$ can be radical even if α is not an nth root of anything in F (try to think of an example).

(c) Write down a polynomial of degree 3 over $\mathbb{Q}$ that is solvable by radicals but whose splitting field is not a radical extension of $\mathbb{Q}$.