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

Problem Set # 7 (due in class on Thursday March 28; have a great Spring break!)

Notation: You are not allowed to use FT Theorem 3.10 or its corollaries. But you can use the fundamental theorem of Galois theory as stated in class.

Problems:

1. Let K/F be a Galois extension with Galois group isomorphic to $C_2 \times C_{12}$. How many subextensions of $K/M/F$ are there satisfying:

(a) $[M : F] = 6$

(b) $[M : F] = 9$

(c) $G(K/M)$ isomorphic to C_6

2. Let p be a prime number and S_p the symmetric group on p things.

(a) Prove that an element of S_p has order p if and only if it is a p-cycle.

(b) Prove that S_p is generated by any choice of a p-cycle and a transposition. Find a composite n and a choice of an n-cycle and a transposition that do not generate S_n.

(c) Let $F \subset \mathbb{R}$ be a subfield. Prove that if $f(x) \in F[x]$ is an irreducible polynomial of degree p having $p-2$ real roots, then the Galois group of $f(x)$ over F is isomorphic to S_p.

(d) Let $F \subset \mathbb{R}$ be a subfield. Prove that if $f(x) \in F[x]$ is an irreducible cubic polynomial with $\Delta < 0$, then the Galois group of $f(x)$ over F is isomorphic to S_3.

(e) Prove that the Galois group of the polynomial $x^3 - x - 1$ over $\mathbb{Q}$ is isomorphic to S_3.

(f) Prove that the Galois group of the polynomial $x^5 - x^4 - x^2 - x + 1$ over $\mathbb{Q}$ is isomorphic to S_5. **Hint.** You are allowed to use real analysis (e.g., the intermediate value theorem), but as a challenge, try to find a purely algebraic (possibly computer-aided) way.

3. Let p be an odd prime number. Prove that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a Galois extension and that there is an isomorphism of groups

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$$
$$j \mapsto \left(\varphi_j : \zeta \mapsto \zeta^j\right)$$

Deduce that the Galois group is cyclic of order $p-1$.

4. Let $\gamma = \sqrt{2+\sqrt{2}} \in \mathbb{R}$.

(a) Show that $\mathbb{Q}(\gamma)/\mathbb{Q}$ is Galois with cyclic Galois group.

(b) Show that $\mathbb{Q}(\gamma, i) = \mathbb{Q}(\zeta_{16})$ and that this field is a Galois extension of $\mathbb{Q}$.

5. The 12th roots of unity. Let $\zeta = \zeta_{12}$.

(a) Prove that $x^4 - x^2 + 1$ is the minimal polynomial of ζ over $\mathbb{Q}$ and that the other roots are $\zeta^5, \zeta^7, \zeta^{11}$.

(b) Prove that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension and that there is an isomorphism of groups

$$(\mathbb{Z}/12\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$
$$j \mapsto \left(\varphi_j : \zeta \mapsto \zeta^j\right)$$

Deduce that the Galois group is isomorphic to a Klein four group.