Dartmouth College Department of Mathematics
Math 81/111 Abstract Algebra
Winter 2024

Problem Set # 6 (due via Canvas upload by midnight Monday 26 February)

Notation: The **Galois group** of a polynomial $f(x)$ over a field F is defined to be the F-automorphism group of its splitting field E.

Problems:

1. Let $f(x) \in \mathbb{R}[x]$ be a monic polynomial of degree $n \geq 1$ with discriminant Δ.

(a) Assume that $f(x)$ has no repeated roots and let r_2 be the number of pairs of complex conjugate (nonreal) roots. Prove that the sign of Δ is $(-1)^{r_2}$.

(b) Let $f(x) \in \mathbb{R}[x]$ be a cubic polynomial. Prove that $\Delta \geq 0$ if and only if the roots of $f(x)$ are all real.

2. 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 calculate the Galois group $\mathrm{Gal}(\mathbb{Q}(\gamma, i)/\mathbb{Q})$.

3. 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) $[K : M] = 6$

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

(c) $\mathrm{Gal}(K/M)$ isomorphic to C_6

(d) $\mathrm{Gal}(M/F)$ isomorphic to C_6

4. This problem will show you 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 $\mathbb{Q}$.

5. 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 element of order p and a transposition. Find a composite n and a choice of an n-cycle and a transposition that do not generate S_n. **Hint.** For a general n, you could prove that S_n is generated by (12) and $(12\cdots n)$. What is special about p being prime is that every element of order p in S_p is a p-cycle and every power of a p-cycle is a p-cycle (or the identity), which are facts that you should verify. Up to conjugating (which doesn't affect whether it generates S_p) the subgroup generated by your choice of p-cycle and transposition, you can assume that your transposition is (12), and up to taking powers of your p-cycle, that it starts $(12\cdots)$. What then?

(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.