Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2018

Problem Set # 6 (due in class on Thursday March 8)

Notation: Recall that C_n denotes an abstract cyclic group of order n written multiplicatively. Remember, the Galois group of a polynomial over a field F is defined to be the F-automorphism group of its splitting field.

Reading: GT 8, 9.1-9.2.

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. Compute the Galois group of the polynomial $f(x) = x^3 - 4x + 2 \in \mathbb{Q}[x]$. You cannot use any advanced theorems, like the Galois correspondence or the fact that splitting fields are Galois.

3. Let F be a field and $f(x) \in F[x]$ a monic polynomial of degree n. Let K be the spitting field of f over F, so that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ over K.

(a) Prove that $\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \in F$. This is called the **discriminant** $\Delta(f)$ of f. **Hint.** Remember the Vandermonde determinant? Did you do this for $n = 2, 3$?

(b) Prove that $\Delta(f) = 0$ if and only if $f(x)$ has a repeated root in K.

(c) Prove that if Δ is not a square in F then $[K : F]$ is even.

4. Let $F \subset \mathbb{R}$ be a subfield and $f(x) \in F[x]$ a cubic polynomial with discriminant Δ.

(a) You know that $\Delta = 0$ if and only if $f(x)$ has a repeated root. Prove that in this case, all the roots of $f(x)$ are in F.

(b) Prove that $\Delta > 0$ if and only if all the roots of $f(x)$ are real.

(c) Prove that $\Delta < 0$ if and only if $f(x)$ a single real root and a pair of complex conjugate roots.

Try to think of what these conditions mean for polynomials of higher odd degree (e.g., degree 5).

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 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 with all but two of its roots being real, then the Galois group of $f(x)$ over F is isomorphic to S_p. You can assume that the splitting field of $f(x)$ is a Galois extension.

(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.