MAT 347
Computing Galois groups
March 31, 2020

A quintic polynomial

Consider the polynomial $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. We will show that the Galois group is S_5 and thus by our theorem from class (Thm. 10.20 in the notes) the polynomial f is not solvable by radicals! Let $K \subset \mathbb{C}$ denote the splitting field and $G := \mathrm{Gal}(K/\mathbb{Q})$.

1. Prove that $f(x)$ is irreducible and hence that $f(x)$ has 5 distinct roots in K.
2. Explain how we can think of G as a subgroup of S_5. (Hint: remember group actions.)
3. Let $\alpha \in K$ be any root of $f(x)$. Use the tower $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$ to deduce that $5 \mid [K : \mathbb{Q}]$.
4. Prove that G contains an element of order 5. (Hint: remember some group theory.)
5. Prove that G contains a 5-cycle.
6. Prove (using calculus) that $f(x)$ has exactly three real roots. Deduce that G contains a transposition. (Hint: consider complex conjugation... why does it stabilize K?)
7. Prove that $G \cong S_5$. (Hint: show using the previous two parts that G has to contain all transpositions.)

Optional: can you find any other quintic polynomials over $\mathbb{Q}$ with Galois group S_5?

Discriminants

Let $f(x) \in F[x]$ be a separable polynomial of degree n and let K be its splitting field. Let $\alpha_1, \ldots, \alpha_n \in K$ be the roots of $f(x)$. Our goal is to understand the Galois group G of $f(x)$ which is defined to be $G := \mathrm{Gal}(K/F)$.

8. Let
$$D := \prod_{i<j} (\alpha_i - \alpha_j)^2$$
be the *discriminant* of $f(x)$. Use the fundamental theorem of Galois theory to prove that $D \in F$. (Incidentally, why is $D \neq 0$?)

9. Prove that the Galois group of $f(x)$ is contained in A_n if and only if D is the square of an element of F. (Hint: consider the action of G on $D^{1/2} \in K$ and remember the definition of the sign of a permutation...)

10. Suppose that $f(x) = x^2 + bx + c$ is a quadratic polynomial. Show that $D = b^2 - 4c$. Explain what happens if D is a square of an element of F.

11. For any $f(x)$, can you write D in terms of the coefficients of $f(x)$? (This has to do with symmetric polynomials...; look up section 14.6 in the book if you get stuck.)

12. Let $f(x)$ be an irreducible cubic polynomial. Show that the Galois group is either S_3 or A_3.

13. Suppose that $f(x) \in \mathbb{Q}[x]$ is an irreducible cubic polynomial with only one real root. Show that its Galois group is S_3.

14. Give an example of an irreducible cubic polynomial in $\mathbb{Q}[x]$ that has Galois group A_3.