MAT 347
Computing Galois groups
Arpil 1, 2016

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

0.1 Discriminants

1. Explain how we can think of G as a subgroup of S_n.

2. 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 $D \in F$.

3. 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.

4. 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.

5. For any $f(x)$, can you write D in terms of the coefficients of $f(x)$?

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

7. Suppose that $f(x)$ is an irreducible cubic polynomial with only one real root. Show that its Galois group is S_3.

0.2 A quintic polynomial

Now we consider the polynomial $f(x) = x^5 - 6x + 3$. We will show that is Galois group is S_5 and thus it is not solvable by radicals. As above let K denote the splitting field and G the Galois group.

8. Prove that $f(x)$ is irreducible.

9. Let α be any root of $f(x)$. Use the tower $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$ to deduce that $5|[K : F]$.

10. Prove that G contains an element of order 5.

11. Prove that G contains a 5-cycle.

12. Prove (using calculus) that $f(x)$ has exactly three real roots. Deduce that G contains a transposition.

13. Prove that $G = S_5$.

14. Suppose that an irreducible degree 5 polynomial has one real root and its discriminant is a square (in $\mathbb{Q}$). Can you conclude that its Galois group is A_5?