19. Finding polynomials with large Galois group

Our big Theorem is only useful if we can find polynomials $f(x)$ such that the automorphism group of the splitting field is S_n. We know one such example: Put $K = \mathbb{C}(r_1, r_2, \ldots, r_n)$ and let F_0 be the field of S_n symmetric functions. (See Problem 14.1.) On this worksheet, we will build some other examples.

I'd like to emphasize that, if you choose a degree n polynomial with integer coefficients at random, it's splitting field is highly likely to be S_n It can be hard to **prove** that the Galois group is S_n, but it is almost always true that the Galois group is S_n.

A criterion better suited to computers

Let $f(x)$ be a polynomial with rational coefficients, let let L be the splitting field of $f(x)$ over $\mathbb{Q}$ and let θ_1, θ_2, $\ldots$, θ_n be the roots of $f(x)$ in L. Let H be a subgroup of S_n and let $g(x_1, x_2, \ldots, x_n)$ be any polynomial with rational coefficients. Set

$$\rho_H = \sum_{w \in S_n} g(\theta_{w(1)}, \theta_{w(2)}, \ldots, \theta_{w(n)}).$$

Problem 19.1. Suppose that $\mathrm{Aut}(L/\mathbb{Q})$, acting on $\{\theta_1, \theta_2, \ldots, \theta_n\}$, is contained in H.

(1) Show that the $\mathrm{Aut}(L/\mathbb{Q})$-orbit of ρ_H is just $\{\rho_H\}$.
(2) Show that ρ_H is a rational number.

Problem 19.2. Let H_1, H_2, $\ldots$, H_M be a list of subgroups of S_n such that every subgroup of S_n, other than S_n itself, is contained in one of the H_i. Suppose that all the numbers ρ_{H_i} are irrational. Deduce that, in this case, $\mathrm{Aut}(L/\mathbb{Q}) = S_n$.

For S_5, such a list of subgroups given by all conjugates of the following subgroups: A_5, S_4, $S_3 \times S_2$ and the 20 element group of permutations of $\mathbb{Z}_5$ of the form $x \mapsto ax + b$.

Testing whether ρ_{H_i} is irrational may sound very hard, but it isn't, due to a result we weren't able to cover: If $f(x)$ is a monic polynomial with integer coefficients, and $g(x_1, x_2, \ldots, x_n)$ has integer coefficients, then ρ_H will be what is called an ***algebraic integer***. This implies that ρ_H will be rational if and only if it is an integer. Computers have no problem numerically computing ρ_H with enough accuracy to see whether or not it is an integer.

A criterion for hand computation

The following problems return from the Homework!

Problem 19.3. Let G be a group of permutations of X. Define i and j in X to be ***switchable*** G contains the transposition which switches i and j; also define each i to be switchable with itself.

(1) Show that being switchable is an equivalence relation.
(2) Let $g \in G$ and let i and j be in X. Show that, if i and j are switchable, then so are $g(i)$ and $g(j)$.
(3) Suppose that $\#(X)$ is prime, and that G acts on X with a single orbit. Show that either every two elements of X are switchable, or else that every element is only switchable with itself.
(4) Let p be a prime and let G be a group of permutations of $\{1, 2, \ldots, p\}$ which has a single orbit and contains a transposition. Show that G is the entire group S_p.

Let p be a prime integer. Let $f(x)$ be a polynomial of degree p with rational coefficients, let L be the splitting field of $f(x)$ over $\mathbb{Q}$ and let θ_1, θ_2, $\ldots$, θ_p be the roots of $f(x)$ in L. Suppose that: (1) $f(x)$ is irreducible over $\mathbb{Q}$ and (2) $f(x)$ has exactly two roots not in $\mathbb{R}$, and all the other roots are in $\mathbb{R}$.

Problem 19.4. Under these conditions, show that

(1) The group $\mathrm{Aut}(L/\mathbb{Q})$ acts on $\{\theta_1, \theta_2, \ldots, \theta_p\}$ with a single orbit.
(2) The group $\mathrm{Aut}(L/\mathbb{Q})$, acting on $\{\theta_1, \theta_2, \ldots, \theta_p\}$, contains a transposition.
(3) We have $\mathrm{Aut}(L/\mathbb{Q}) = S_p$.

I generated three quintics at random, and this criterion applied to the third one I tried: $x^5 + 6x^4 - 3x^3 + 3x^2 + 5x - 3$ is irreducible and its roots are -6.51168, -0.878148, 0.468019 and $0.460907 \pm 0.953175i$.