ICTP 2018 Summer School: Galois Theory mini-projects

1) Consider irreducible $f(x) \in \mathbb{Z}[x]$ and see what Galois groups you get for these polynomials. This is a computational project that will require coding (Sage, the MAGMA calculator?) and experimenting. Consider $f(x)$ by degree d. Why is there nothing to do for $d = 2$? For $d = 3$ how will you order your irreducible polynomials? You could look at $f(x) = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}$ or maybe $f(x) = x^3 + bx + c$ where $b, c \in \mathbb{Z}$. Two natural ways to do this are:

- You look in a box with $0 \leq |a|, |b|, |c| \leq X$ and gather data for various large X.
- Order the polynomials by discriminant up to some large X. How do you know you have checked *all* irreducible $f(x)$ with discriminant less than X?

Are there other ways to organize the polynomials? There are only two subgroups of S_3 with order a multiple of 3, so your answer will be either $\mathbb{Z}/3$ or S_3. How often does each occur?

After this try higher degrees. You will need to determine the transitive subgroups of S_d for small d. What does your data suggest happens for $d = 4$, e.g., how often is the Galois group A_4?

This is a project where you will *not* prove anything. Rather you'll simply trust that whatever software you use is accurately computing Galois groups and gather data and make a conjecture.

2) This is a more theoretical project. The goal is for small d to list the transitive subgroups of S_d and exhibit *with proof* a polynomial $f(x) \in \mathbb{Z}[x]$ with Galois group each of these transitive subgroups. For $d = 4$ think about the polynomials $f(x) = x^4 + ax^2 + b$. Which Galois groups can you get with these?

A more general question is the *Inverse Galois Problem*. Which finite groups G can you exhibit, with proof, as a Galois Group over $\mathbb{Q}$? Start with the cyclic groups. This problem is one of the outstanding unsolved problems in the field.

Here is a fact that might be helpful:

Fact Let $f(x) \in \mathbb{Z}[x]$ be irreducible of degree d with discriminant D. Let p be a prime and suppose $p \nmid D$. Suppose that mod p we have that $f(x)$ factors to $\prod_{i=1}^{k} f_i(x)^{e_i}$ where $f_i(x)$ has degree d_i. Then all $e_i = 1$. If $G \subseteq S_d$ is the Galois group of $f(x)$, then G contains an element of S_d that is a product of k disjoint cycles, the ith one having length d_i.

This Fact helps show that certain structures are in G. For instance $f(x) = x^3 + x - 1$ is irreducible (why?) and has discriminant $D = -31$. Mod 2 it is irreducible and mod 3 it factors as $(x-2)(x^2+2x+2)$. In this case G contains a 3-cycle and a transposition. Since G has elements of order 2 and 3 its order must be a multiple of 6 so $G = S_3$. Using this Fact, and some understanding of types of elements that generate S_d, you can show S_d is a Galois group over $\mathbb{Q}$.