LAGRANGE'S SOLUTION TO THE QUARTIC

DAVID SMYTH

1. Lagrange's Solution to the Quartic

Lagrange actually proved the fundamental theorem on symmetric functions in the course of developing a more systematic approach to solving polynomial equations. In this lecture, we'll see how Lagrange made use of the theorem to give a solution to the general quartic equation. Lagrange's solution begins with the following observation, which tells you how to turn an arbitrary function into a symmetric function.

Lemma 1.1. *Let $f_1 \in k[\alpha_1, \dots, \alpha_n]$ be any polynomial, and let $f_1, \dots, f_k$ be the orbit of f_1 under the action of S_n, i.e. the set of all functions you get by acting on f_1 with elements of S_n. If $s(x_1, \dots, x_k)$ is any symmetric function in k variables, then $s(f_1, \dots, f_k)$ is a symmetric function in $\alpha_1, \dots, \alpha_n$.*

Example 1.2. *Let $f_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \in k[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$. One can easily check that the orbit of f_1 is:*

$$\begin{aligned} f_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ f_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ f_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) \end{aligned}$$

According to the theorem, any symmetric function of f_1, f_2, f_3 must give a symmetric function of the α_i. In particular, one can verify by inspection that $f_1 + f_2 + f_3, f_1f_2 + f_1f_3 + f_2f_3, f_1f_2f_3$ are all symmetric in $\alpha_1, \dots, \alpha_4$. It follows of course that they can be expressed as polynomials in the elementary symmetric functions, and indeed one can easily check:

$$\begin{aligned} f_1 + f_2 + f_3 &= 2s_2(\alpha_1, \dots, \alpha_4) \\ f_1f_2 + f_1f_3 + f_2f_3 &= (Exercise!) \\ f_1f_2f_3 &= (Exercise!) \end{aligned}$$

How does Lagrange use this to solve the quartic polynomial? Given an equation

$$f(x) = x^4 + a_2x + a_3 + a_4 = 0,$$

Lagrange starts by assuming that $f(x)$ has 4 distinct roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. (It is not true of course that all degree 4 polynomials have 4 distinct roots - this extra assumption is a weakness of Lagrange's method, and later in the course we will have the technical machinery to get around it.) As we discussed in the last lecture, these roots must satisfy the four equations:

$$s_1(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = \alpha_1+\alpha_2+\alpha_3+\alpha_4 = -a_1 = 0.$$
$$s_2(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = a_2$$
$$s_3(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = -a_3$$
$$s_4(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = a_4$$

Thus, we are given three complex numbers a_2, a_3, a_4, and we want to find four complex numbers $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ satisfying the above equations. Though we don't know what $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ are, Lagrange begins by defining f_1, f_2, f_3 to be the expressions in Example 1.2. In other words, we have used four unknown complex numbers to define three more unknown complex numbers. The key point, however, is that we have a way to find formulas for f_1, f_2, f_3 in terms of a_2, a_3, a_4. Here comes Lagrange's stroke of genius - consider the cubic polynomial:

$$(x-f_1)(x-f_2)(x-f_3) = x^3-(f_1+f_2+f_3)x^2+(f_1f_2+f_1f_3+f_2f_3)x-f_1f_1f_3$$

As we argued in Example 1.2, the coefficients of this polynomial are symmetric functions in $\alpha_1,\alpha_2,\alpha_3,\alpha_4$. By the fundamental theorem of symmetric functions, we can therefore write the coefficients of this function as polynomials in a_2, a_3, a_4. But this means that we can use our solution for the cubic to solve for f_1, f_2, f_3 in terms of a_2, a_3, a_4! Needless to say, actually writing down the formula would be a rather tedious affair, but the key point is that we know one exists.

Once we have solved for f_1, f_2, f_3, it is easy to see that we can solve for $\alpha_1,\alpha_2,\alpha_3,\alpha_4$. Indeed, using the equation

$$\alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0,$$

we see that

$$f_1 = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4) = -(\alpha_1+\alpha_2)^2,$$

and we conclude that

$$\alpha_1+\alpha_2 = \sqrt{-f_1},$$
$$\alpha_3+\alpha_4 = -\sqrt{-f_1}.$$

Similarly, we have

$$\alpha_1+\alpha_3 = \sqrt{-f_2},$$
$$\alpha_2+\alpha_4 = -\sqrt{-f_2},$$
$$\alpha_1+\alpha_4 = \sqrt{-f_3},$$
$$\alpha_2+\alpha_3 = -\sqrt{-f_3}.$$

From here, one can solve for each of the α_i individually. For example,

$$\alpha_1 = \frac{(\alpha_1+\alpha_2)+(\alpha_1+\alpha_3)-(\alpha_2+\alpha_3)}{2} = \frac{\sqrt{-f_1}+\sqrt{-f_2}+\sqrt{-f_3}}{2}.$$

We have solved the quartic!

Now, let us step back from the particulars of this example, and consider Lagrange's overall strategy. If we are trying to solve a polynomial of degree n, Lagrange's strategy is to find a function of the roots $f_1(\alpha_1,\dots,\alpha_n)$ whose orbit $f_1,\dots,f_k$ under S_n is less than n. Assuming we know how to solve equations of degree less than n, we can solve for $f_1, \ldots, f_k$ by considering the polynomial

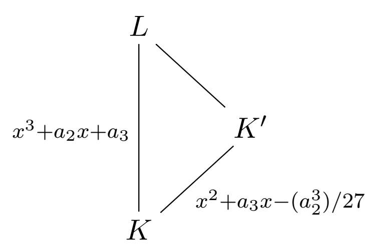
$$\prod_{i=1}^{k}(x - f_i).$$

As in the example of the quartic, the fundamental theorem of symmetric functions implies that the coefficients of this polynomial will be polynomials in the original coefficients $a_1, \ldots, a_n$, so we can solve.

Of course, as someone pointed out in class, if we take the orbit of f_1 to be too small, e.g. if we simply take f_1 to be a symmetric function, then knowing the value of f_1 won't help us much in our quest to solve for the α_i's. The idea, therefore, is to find a function which has a small enough orbit that you can solve for it, but is also a useful bridge to solving for the α_i's. In fact, Lagrange spent the last years of his life looking for a function $f(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ which would allow him to solve the quintic. Alas, we now know that solving the quintic is impossible.

Let us now step back and consider the overall idea of Galois Theory. The problem with polynomials is that they are really not very transparent. When we solved the cubic in Lecture 1, we found that we could essentially reduce the cubic equation to a quadratic equation. In some sense, therefore, there was a quadratic equation "hidden" inside the cubic equation. Similarly, Lagrange found a cubic equation "hidden" inside a quartic equation. We need to switch to a kind of mathematical structure in which this hidden structure becomes more transparent.

In the following weeks, we will see how to associate to any polynomial $f(x) \in K[x]$ a certain algebraic object L/K, called a field extension. While the field extension contains, in some sense, all the relevant information about f , it is much easier to deal with. For example, the fact that solving the cubic involves a hidden quadratic equation, will appear as the fact the associated field extension L/K has an intermediate extension associated to a quadratic equation, i.e. we have a picture like this:



Thus, the problem of solving polynomials will be reduced to understanding the structure of field extensions, especially the problem of understanding all the intermediate field extensions of a given field extension. This problem, in turn, will turn out to be solvable in terms of pure group theory. Associated to a field extension L/K, we will define a certain group $G(L/K)$ called the Galois group of the extension. Subfields will correspond to subgroups/quotients of the Galois group, just as Lagrange's intermediate cubic equation was found by finding a homomorphism $S_4 \to S_3$. This will give us a very pretty answer to our original problem!