The Abel-Ruffini Theorem

Jay Havaldar

We all remember the quadratic equation.

$$x = \frac{-b \pm \sqrt{b^2 + 4ac}}{2a}$$

In general, any quadratic equation with integer coefficients is **solvable by radicals**, meaning that the answer can be computed in a finite number of steps using only the $+, -, \times, \div$ operations and also taking nth roots. Though the formulas get longer and longer, the same is true for cubic and quartic polynomials.

The quartic formula.

But something incredible happens when you hit 5: it turns out that there is no such formula. Proving this result took literally hundreds of years and ended with the birth of modern algebra in the 1800s. I'm going to be going through the proof in pretty rigorous detail, and hopefully you and I will both learn something at the end of the day. I will assume for the purposes of this proof that you know basic group theory and algebra (the first couple paragraphs on Wikipedia should do).

Solvable Groups We first start with group theory. Though the two seem pretty unrelated at first, group theory is actually intimately connected with solving algebraic equations. We will start with proving a theorem about groups; namely, that for $n \geq 5$, the symmetric group S_n is not solvable.

Definition: S_n is the **symmetric group** on n letters, and it describes the permutations you can do on n elements. Multiplication in this group is simply composition of operations.

Definition: Suppose we have an element x in some group G. Then we define the operation **conjugation** by another element $g \in G$ as the multiplication operation $g\ x\ g^{-1}$.

Definition: A subgroup N of a group G is said to be **normal** if it is preserved under conjugation by any member of G. In other words, for any $g \in G$, we have that $gNg^{-1} = N$; conjugation sends elements of N to other elements of N.

The normal subgroups are very important in group theory, because we can ``divide'' only by normal subgroups to obtain a quotient group:

Definition: Suppose we have a group G with a normal subgroup N. The quotient group $\frac{G}{N}$ refers to all cosets of the form aN for $a \in G$. We can think of this with analogy to the ``modulo'' operation; elements in $G$ are sent to the same ``bucket'' in $\frac{G}{N}$ if they differ by an element $n \in N$. Multiplication is defined as follows: $(aN)(bN) = (abN)$.

Now, we define what it means for a group to be solvable:

Definition: Let G be a group. We call G **solvable** if and only if there exists a sequence of subgroups:

$$G = H_0 \supset H_1 \supset H_2 \supset ... \supset H_m = e$$

such that H_i is a normal subgroup of H_{i-1}, and the quotient group $\frac{H_{i-1}}{H_i}$ is abelian.

We will prove our theorem in two parts. First, we consider what conditions we need in order to make sure a quotient group is abelian.

Theorem: Let G be a group with normal subgroup H. Then $\frac{G}{H}$ is abelian if and only if H contains all elements of G of the form:

$$xyx^{-1}y^{-1}$$

Proof: First, we assume $\frac{G}{H}$ is abelian. Let us refer to f as the ``canonical'' homomorphism; the mapping that sends an element in G to its natural element in $\frac{G}{H}$. This mapping is a homomorphism due to the way that we defined multiplication in the quotient group. So we have:

$$f(xyx^{-1}y^{-1}) = f(x)\ f(y)\ f(x^{-1})\ f(y^{-1})$$

By hypothesis, $\frac{G}{H}$ is abelian; so multiplication can be done in any order. It is evident, then, that the right hand side is the identity; and so, the left hand side is an element of H.

Conversely, let us assume H contains all elements of the form $xyx^{-1}y^{-1}$. Then, let's take any two elements in $\frac{G}{H}$, called a, b. We must have $a = f(x)$ for some $x \in G$, and similarly $b = f(y)$ for some $y \in G$. By hypothesis, then, H contains $xyx^{-1}y^{-1}$. We already know that:

$$f(xyx^{-1}y^{-1}) = f(x)\ f(y)\ f(x^{-1})\ f(y^{-1}) = e$$

But this means that:

$$f(xyx^{-1}y^{-1}) = a\ b\ a^{-1}\ b^{-1} = e$$
$$ab = ba$$

And so indeed, $\frac{G}{H}$ must be abelian.

(Before this point it may be helpful to review permutations and how to multiply cycles; my convention is multiplying right to left.)

Moving forward, we prove an intermediate lemma.

Lemma Take H, N subgroups of S_n, $n \geq 5$ with $N \subset H$ and N normal in H, with $\frac{H}{N}$ abelian as we want here. Then suppose that H contains every 3-cycle; we claim that N also contains every 3-cycle.

To prove this, take an arbitrary pair of cycles $\sigma = (abc)$ and $\tau = (cdf)$, with a, b, c, d, f as 5 distinct letters. This construction will make sense in just a minute, and you could reverse engineer it from the following calculation. We know from earllier that if the quotient group is abelian, then N must necessarily contain $\sigma\tau\sigma^{-1}\tau^{-1}$. Computing that element, we have:

$$\begin{aligned}\sigma\tau\sigma^{-1}\tau^{-1} &= (abc)(cdf)(cba)(fdc)\\ &= (cad)\end{aligned}$$

It is evident that if H contains **all** possible 3-cycles, then by a similar construction we can proof that N contains all of the 3-cycles as well, since our choice of 5 letters was arbitrary.

Note that this is **not** the case if we only have 4 letters to choose from. In that case, the product becomes a transposition (2-cycle):

$$\begin{aligned}\sigma\tau\sigma^{-1}\tau^{-1} &= (abc)(bcd)(cba)(dcb)\\ &= (cb)\end{aligned}$$

And in the degenerate case of 3 letters to choose from:

$$\begin{aligned}\sigma\tau\sigma^{-1}\tau^{-1} &= (abc)(abc)(cba)(cba)\\ &= (e)\end{aligned}$$

Earlier we showed that if $\frac{H}{N}$ is abelian, then N contains all the elements of the form $xyx^{-1}y^{-1}$, where $x, y \in H$. So, in the case where H contains all the 3-cycles, we know N contains all the 3-cycles as well.

Now, we can complete the proof with a simple argument. Since S_n contains all 3-cycles for $n \geq 5$, then H_1 must also contain all 3-cycles, and so on. But then, the trivial group would contain all 3-cycles; so we are done.

So we've proved that S_n is not a solvable group for $n \geq 5$. But what does any of this have to do with algebraic formulas? We'll find out in the next part!