1. Ultimate Aim

Numbers were first used to count things. As such the first numbers that people used were whole positive numbers. One thing that is natural to do is to add two numbers, since that represents counting the total number of objects belonging to two groups.

Becoming quite a bit more sophisticated, one can then ask: "Given that there are three objects in one pile and five objects in both piles, then how many objects are there in the second pile?". Abstracting this question even more, and letting x denote the number of objects in the second pile, we get an equation

$$x + 3 = 5.$$

As soon as one reaches this level of generality, there are obvious problems. What is the solution to the equation

$$x + 3 = 3?$$

It took people a very long time to realise that the right answer is $x = 0$, in other words that we should consider zero as a number. From there it is not such a big leap to consider equations of the form

$$x + 4 = 3,$$

and realise the need for negative numbers. Becoming even more sophisticated, we might consider an equation of the form

$$3x = 9.$$

Once again, as soon as you write this down, some trouble maker is going to ask how to solve

$$3x = 2.$$

The solution, as everyone knows, is to allow fractions (or better we have gone from whole numbers, to the natural numbers, from there to the integers and finally to the rationals). It seems at this stage, that we are finished, since any equation, of the form

$$ax + b = c,$$

where a, b and c are rational numbers, has a unique rational solution (or none exists for obvious reasons). Indeed one can solve this equation, using only the operations of addition, subtraction, multiplication and division, and the rationals are obviously closed under these operations.

However, one often wants to solve quadratic equations, for example

$$x^2 - 5x + 6 = 0.$$

It didn't take people too long to write down an algorithm to find all integer solutions to quadratic equations. In this example we are looking for two numbers whose product is 6 and whose sum is 5.

It turns out to be quite a jump to go from quadratic to cubic equations. In fact problems of this sort were considered so important, that in the late middle ages various Italian cities staged competitions and there were elaborate celebrations when someone found a general method (note that people were reluctant to use negative numbers, so that they preferred to write the equation $x^2 - 5x + 6 = 0$ in the form $x^2 + 6 = 5x$; hence they considered that there were many different types of cubic equations, depending on the sign of the coefficients).

Going back to quadratic equations, two problems arise. First the equation $x^2 = 2$ has no rational solutions. Actually this was not so worrying, as $\sqrt{2}$ may be considered as a real number, and as real numbers represent lengths, real numbers seem quite natural.

However the equation $x^2 = -1$ has no real solution. Again it took quite a while to realise that one ought to add a number i, and call it a solution of this equation. Completing the square, yields a formula for the roots of a quadratic polynomial, the quadratic formula and so it is not hard to see that any quadratic polynomial with complex coefficients has a complex root (the only thing to check is that any complex number has at least one square root.)

From then on, a lot of attention was focused on finding similar formulas for higher degree polynomial equations. Eventually people found such a formula for cubics and quartics. People expected that there would be a similar formula for the roots of a quintic polynomial.

Most of the mathematics that went into this project was mind boggling bad, and almost no progress was made on this problem, until the brilliant French mathematician Galois showed that there is no such formula in general. That is, there are quintic polynomials, with real coefficients, such that there is no formula for the values of the roots, that involves addition, subtraction, multiplication, division, and the operation of taking roots of the coefficients of the quintic (strictly speaking Abel was the first person to exhibit a quintic polynomial with real coefficients which cannot be solved by radicals).

The entire sequence Math 100ABC is devoted to proving his Theorem.

To give some structure to this course, let us look at some of the ideas behind his proof.

But before we do even that, note that there is another natural question raised by this introduction.

Theorem 1.1 (Fundamental Theorem of Algebra)**.** *Let $f(x)$ be a polynomial of degree $n > 0$, with complex coefficients.*

Then the equation

$$f(x) = 0,$$

has at least one complex root.

Even though this result is called the Fundamental Theorem of Algebra, in fact there is no (reasonably uncontrived) proof of this fact, that only uses results of algebra.

Galois' brilliant observation is that the symmetries of the roots of the polynomial $f(x)$ determine the structure of the solutions. For example, consider the equation

$$x^2 + 1 = 0.$$

Solving this equation involves taking a square root. In other words if i is a root of this equation, then so is $-i$. Thus the two roots i and $-i$ are interchangeable and there ought to be a symmetry that reflects this. In fact the symmetry is obvious. In terms of the original polynomial, note that replacing x by $-x$ leaves the polynomial unchanged. One can see this by direct calculation

$$x^2 + 1 \longrightarrow (-x)^2 + 1 = x^2 + 1$$

or by factoring

$$x^2 + 1 = (x + i)(x - i) \longrightarrow (x - i)(x + i) = x^2 + 1.$$

A more sophisticated way to look at this is to realise that there is a symmetry of the complex numbers $z \longrightarrow \bar{z}$ (aka complex conjugation) that leaves the real numbers invariant.

Similarly, consider a cubic equation. If you could solve this equation by taking cube roots then one would expect there to be a symmetry of order three, of the original polynomial equation.

More generally, one might hope that if one can solve an equation, simply by taking repeated roots (and the other standard operations of arithmetic) then that would say a lot about the underlying symmetries of the original polynomial.

In fact Galois wrote down a quintic polynomial whose symmetry group is too large. That is to say that if one can solve a polynomial equation by taking roots, then in fact there are not so many symmetries.

To make all of this argument work will take some effort.

The first order of the day is to study symmetry groups. Since this is a course in abstract algebra, the idea will be to abstract all known examples of symmetries and make up axioms that reflect all these known cases.