Galois' theorem on polynomial equations

In 1829 Galois[1] proved the non-existence of a general formula for finding the roots of a polynomial of degree at least 5. This result, along with answers (also provided by Galois) to a pair of geometrical problems open since the time of the Greek civilisation[2] are justifiably considered as the crowning achievements of the mathematical concepts whose development began in earnest in the late 1700s, mainly in France, and which nowadays go under the rubric of 'abstract algebra'.

To get a feeling for Galois' theorem, you first of all have to understand what people meant by a 'formula' for the roots of a polynomial equation. Let's therefore give a precise definition :

DEFINITION 1 : Let

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0, \quad a_i \in \mathbf{C}, \quad a_n \neq 0,$$

be a general polynomial of degree n. By general, we mean that the coefficients a_i are unspecified and should be considered as arbitrary complex numbers.

[1]The same result was proven almost simoultaneously by the Norwegian mathematician Abel. I don't know how similar his methods were to those of Galois, but in any case it is Galois' proof which has had the greatest subsequent impact

[2]The problems in question are concerned with the possibility or not of performing the following constructions with a straightedge and compass : (i) trisecting a given angle (ii) 'squaring' a given cube, i.e.: constructing a cube whose volume is twice that of a given cube. It turns out in both cases that the constructions are impossible. By the way, it is worth noting that a third similar-sounding problem was left unsolved by the Greeks, namely whether one can 'square the circle', that is, construct a square whose area is equal to that of a given circle. The answer yet again turns out to be NO, and this was first proven by the German mathematician Lindemann (1870s ?). More precsiely, Lindemann proved the fantastic theorem that the real number π is a so-called *transcendental number*. A real number x is said to be *transcendental* if it is not a root of any polynomial with integer coefficients (otherwise x is said to be *algebraic*). The following facts were already known to Galois and his contemporaries : (a) the set of algebraic numbers is closed under addition, multiplication and inversion (in the language of abstract algebra, the algebraic numbers form a *field*) (b) the squarability of the circle is equivalent to the constructibility of the positive real number x such that $x^2 = \pi$ (c) all constructible numbers are algebraic. From (a), (b) and (c) it clearly follows that the squarability of the circle would imply the algebraicity of π. Hence, Lindemann's proof that π is in fact transcendental was the last piece of the jigsaw. Nowadays, there are several different proofs of this fact, but all of them require methods which are not purely algebraic, specifically the methods of advanced calculus, otherwise known as 'mathematical analysis'.

By a *formula* for the roots of $p(z)$ we mean a finite expression formed by combining sums, products, quotients and m^{th} roots, for any $m > 0$, of the coefficients a_i, which is valid for any assignment of values to these coefficients.

For example, for $n = 2$, we all know that such a formula exists, namely

$$\frac{1}{2a_0}\left(-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}\right).$$

Less well-known, and a lot more complicated, is a formula for $n = 3$, which I wrote down on the blackboard one day. There is even a formula for $n = 4$. In fact, all three formulas were known by the 14th century, the first (it is speculated) as far back as around 2000 BC. For hundreds of years it was assumed by most mathematicians that formulas also existed for all $n \geq 5$ and that the only reason they had not been found was because they were probably very complicated indeed. Hence the results of Galois and Abel had yet another characteristic which justifies their description as 'revolutionary', namely they were unexpected.

To explain Galois' ideas we have to introduce some notions from abstract group theory.

DEFINITION 2 : Let G be a group, $x, y \in G$. The group element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted $[x, y]$, i.e.:

$$[x, y] := x^{-1}y^{-1}xy.$$

Notice that $[x, y] = 1$ if and only if x and y commute, that is iff $xy = yx$.

DEFINITION 3 : Let G be a group, X a subset of G. The *subgroup* of G *generated by* X is the smallest subgroup of G containing X. It is denoted $< X >$.

The following is a more explicit description :

Proposition 1 *$< X >$ is the subgroup of G consisting of all group elements which can be expressed as a product of elements from X, that is all $g \in G$ of the form*

$$g = x_1x_2 \cdots x_n,$$

where each $x_i \in X$, with repititions allowed, and $n \geq 0$ ($n = 0 \Rightarrow g = 1$).

DEFINITION 4 : Let G be a group. Let X be the subset of G consisting of all the commutators, i.e.:

$$X = \{[x, y] : x, y \in G\}.$$

The subgroup generated by X is called the *commutator subgroup* of G and is denoted G'.

Intuitively, the size of the commutator subgroup G' measures 'how far' the group G is from being abelian. For example, we have

Proposition 2 *G is abelian iff $G' = \{1\}$.*

For a deeper analysis we introduce a descending chain

$$G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$$

of subgroups of a group G, defined inductively as follows :

$$G_0 := G, \qquad G_n := G'_{n-1}, \text{ for } n \geq 1.$$

This chain of subgroups is called the *lower central series* of G. The group G is said to be *soluble* if $G_n = \{1\}$ for some n, and the least such n for which this is the case is called the *solubility length* of G. For example, Proposition 2 says that the groups of solubility length 1 are the abelian groups. Even groups of solubility length 2 can look very 'unabelian' in certain respects, but nevertheless the concept of solubility has proved useful as a bridge between the simplest kinds of groups (the abelian ones) and general abstract groups. But it is far from the case that all groups are soluble, and the most important example is given by

Theorem 3 *The group S_n is soluble for $n \leq 4$ and insoluble for $n \geq 5$.*

A proof of this result should be possible to find in most textbooks on group theory, though not necessarily in one place ! The interesting part is the insolubility of S_n for all $n \geq 5$ (solubility for $n \leq 4$ may be verified by a direct computation). I don't intend to give a complete proof of this fact here, but in order to help you in your search through the literature I will outline the main steps. First, we need some preparatory stuff :

Let $\sigma \in S_n$, for some fixed n. Recall that σ can be written uniquely as a product of disjoint cycles. Now moreover, every cycle can be written as a product of transpositions, though these will no longer be disjoint. For example, you may verify that

$$(a_1 \cdots a_k) = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_k).$$

Neither is the representation of a cycle as a product of transpositions unique. For example, in S_3 we have

$$(123) = (12)(13) = (13)(23) = (23)(12) = (13)(12)(13)(12) = \ldots \tag{1}$$

Hence, we have the result that every permutation can be written as a product of not necessarily disjoint transpositions, and such a representation is not unique. As the example in (1) shows, even the NUMBER of transpositions in the representation of a given permutation is not uniquely determined. However it turns out that the following is true

Lemma 4 *No permutation can be written both as a product of an even number of transpositions and as a product of an odd number of transpositions.*

Moreover, it's easy to see that the set of permutations which can be written as a product of an even number of transpositions is closed under multiplication and inversion. For if $\sigma = \tau_1 \cdots \tau_{2k}$ and $\sigma^* = \tau_1^* \cdots \tau_{2l}^*$ then

$$\begin{aligned} \sigma\sigma^* &= \tau_1 \cdots \tau_{2k} \tau_1^* \cdots \tau_{2l}^*, \\ \text{and } \sigma^{-1} &= \tau_{2k} \cdots \tau_1. \end{aligned}$$

This gives the first half of the next lemma

Lemma 5 *Fix $n > 0$. Denote by A_n the set of those permutations $\sigma \in S_n$ which can be written as the product of an even number of transpositions. Then A_n is a subgroup of S_n. Moreover, $o(A_n) = \frac{1}{2}n!$ and so $[S_n : A_n] = 2$.*

The group A_n is called the *alternating group* on n letters. The connection to matters of solubility is now provided by

Proposition 6 *(i) For every $n > 0$ we have that $S_n' = A_n$.*
(ii) For every $n \geq 5$, $A_n' = A_n$.

It is now easy to see that Proposition 6 implies Theorem 3.

There remains now just one question to be answered, namely 'What the hell does all this have to do with Galois' theorem ?' Good question ! Well, the answer is provided by the following

Theorem (Galois) *If there exists a general formula for the roots of a polynomial of degree n, then the group S_n must be soluble.*

To even sketch the proof of this remarkably insightful theorem would require the introduction of a whole plethora of new concepts from abstract algebra, and so I will leave the task to whoever teaches you the course 'Algebraiska Strukturer' next year. It suffices to say here that these ideas (some due to Galois himself and others to various of his predecessors) have had a profound impact on the development of that branch of mathematics called 'algebra', undiminished in importance to this day.