Insolubility of the Quintic

Problems from the History of Mathematics

Lecture 11 — February 28, 2018

Brown University

From Quartics to Quintics

Discovery of the cubic formula (as published in *Ars Magna* in 1545) and the quartic formula[1] led many to believe that a solution to the quintic was forthcoming (but perhaps complicated).

This thought prevailed until 1771, when Lagrange published *Reflections on the Algebraic Theory of Equations*. Here, Lagrange analyzed why the methods used to study the quadratic, cubic, and quartic had succeeded. He introduced the resolvent and concluded that old methods would not suffice for the quintic.

Ex: For a cubic with roots α_i and ζ a cube root of 1, define

$$R(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3)^2.$$

[1] The quartic was actually reduced to the cubic before work on the latter was published. This was the work of Lodovico Ferrari, in 1540.

... Or Maybe Not

The first to suggest that the quintic might not be solvable in radicals was Gauss. In his opus *Disquisitiones Arithmeticae* (1799), he writes:

> *Everyone knows that the most eminent geometers have been ineffectual in the search for the general solution of equations higher than the* 4*th degree... and there is little doubt that this problem does not so much defy modern methods of analysis as that it proposes the impossible.*

Coincidentally, 1799 was the year that Paolo Ruffini published the first proof of the insolubility of the quintic. (There was a gap in the proof, though, which we'll discuss later.)

The first full proof appeared in 1814 in the work of Niels Hendrik Abel.

A Modern Proof using Galois Theory

A Galois-Theoretic Proof

While the Abel-Ruffini Theorem is taught in many algebra courses today, the proofs that students see are entirely due to the later work of Galois.

For context, we sketch these ideas now.

Let $f(x) \in k[x]$ be an irreducible polynomial with roots $\alpha_1, \dots \alpha_n$. Let $L = k(\alpha_1, \dots \alpha_n)$ denote the splitting field of $f(x)$.

The Galois group G_f of $f(x)$ is the group of field automorphisms of L that fix k. These automorphisms permute the roots of f and are determined by this action. (This gives an injection $G_f \hookrightarrow S_n$.)

A Galois-Theoretic Proof

The Galois-theoretic approach to the Abel–Ruffini Theorem begins thus:

Theorem (Galois, 1830):

The equation $f(x) = 0$ is solvable by radicals if and only if the Galois group G_f is solvable.

Here, we call a group G solvable if there exists a chain of subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots H_k = G$$

such that

1. $H_i \triangleleft H_{i+1}$ for all i. Here, $A \triangleleft B$ denotes a normal subgroup, one in which $a \in A$ and $b \in B$ implies $bab^{-1} \in A$.
2. the quotient groups H_i / H_{i-1} are abelian for all i.

A Galois-Theoretic Proof

Once we have a correspondence between solvability by radicals and solvable Galois groups, it suffices to show that:

1. the 'generic' polynomial of degree n has Galois group S_n
2. that S_n is not solvable for $n \geq 5$.

Here, (1) follows from work on symmetric polynomials begun by Newton and mastered by the time of Lagrange, Vandermonde, and Ruffini.

But these mathematicians lacked the idea of a *normal subgroup*, which appears for the first time in the work of Galois.[2] Since our definition for solvable groups uses normal subgroups, (2) requires the work of Galois.

[2] The name comes from the Galois correspondence, in which normal subgroups of G_f correspond to normal extensions of the base field k.

The Work of Abel and Ruffini

Abel's Proof

Abel's proof of the insolubility of the quintic breaks into three claims:

1. If $f(x) = 0$ is solvable in radicals, then there exists a radical tower E/k with $L \subset E$. Here, a radical tower is a chain of field extensions

$$k = K_0 \subset K_1 \subset \cdots \subset K_m = E$$

in which K_i is obtained from K_{i-1} by adjoining an mth root.

2. If E/k is a radical tower and $L \subset E$, then L/k is a radical tower.
3. L/k is not a radical tower for $n \geq 5$.

We discuss each one in turn.

Abel's Proof, Step 1

Step 1:

$f(x) = 0$ solvable $\quad \Longrightarrow \quad$ $\exists$ a radical tower E/k with $L \subset E$.

This is the easiest of Abel's three steps, since a closed formula in radicals suggests the exact chain of extensions to consider.

Abel's Proof, Step 2

Step 2:

If E/k is a radical tower and $L \subset E$, then L/k is a radical tower.

Roughly, one moves from a radical tower for E/k to one for L/k by intersecting intermediate fields with L.

Step 2 is interesting from a historic perspective because the critical gap in Ruffini's 1799 (incomplete) proof of the Abel–Ruffini theorem amounts to the omission of this step. Ruffini assumes that the 'obvious' radical tower E/k constructed in Step 1 is already L, and goes no further.

Ex: Consider $f(x) = x^3 - 15x - 20$. Following Cardano's formula, the roots of $f(x)$ are given as linear combinations of the cube roots

$$\sqrt[3]{10 \pm 5i}.$$

Since the only roots of $f(x)$ are real, the splitting field L is real. Then L is not large enough to contain its radical tower.

Abel's Proof, Step 3

Step 3:

In the generic case, L/k is not a radical tower for degree $n \geq 5$.

The proof comes in two parts. In the first, we fix a radical tower

$$k = K_0 \subset K_1 \subset \cdots \subset K_m = L$$

and prove that $K_1 = k(\sqrt{\Delta})$, where Δ is the discriminant of f:

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Proof: Suppose that $K_1 = k(\theta)$, in which $\theta^p = t \in k$. Fix $\tau \in G_f$. Then $\tau(\theta)^p = \theta^p$, so $\tau(\theta) = \zeta_p \theta$ for some pth root of unity ζ_p.

If τ is a transposition, then $\theta = \tau(\tau(\theta)) = \zeta_p^2 \theta$, so either $p = 2$ or K_1 is fixed by all transpositions in G_f. Since transpositions generate S_n, the second option implies that K_1 is fixed by G_f, a contradiction.

Abel's Proof, Step 3

Thus $p = 2$ and $\tau(\theta) = \pm\theta$ for all $\tau \in S_n$. We have $\tau(\theta) = \theta$ for each 3-cycle in S_n, so θ is fixed by A_n, the alternating group. But A_n is a maximal subgroup, so it is exactly the stabilizer.

It follows that $\theta/\sqrt{\Delta}$ is fixed by each automorphism, so $\theta/\sqrt{\Delta} \in k$. In other words, $K_1 = k(\sqrt{\Delta})$.

Note: By the Galois correspondence,

building a tower from k up to L

$\longleftrightarrow$ repeatedly quotienting $G_f = S_n$ down to $\{e\}$.

The first part of Step 3 corresponds to the quotient $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$. Since A_n is simple for $n \geq 5$, we expect that K_1 has no radical extension.

Abel's Proof, Step 3

Final Claim:

K_1 has no radical extension in L in the case $n \geq 5$.

Proof: Suppose that $K_2 = K_1(\beta)$, in which $\beta^q = b \in K_1$. Let $\tau \in A_n$. Then $\tau(\beta^q) = \beta^q$, so $\tau(\beta) = \zeta_q \beta$ with ζ_q a qth root of unity.

If τ is a 3-cycle, $\beta = \tau^3(\beta) = \zeta_q^3 \beta$. Thus $q = 3$ or β is fixed by each 3-cycle of A_n. But 3-cycles generate A_n, so the second case implies that β is fixed by all of A_n and that $\beta \in K_1$. Thus $q = 3$.

But 5-cycles also generate A_n (for $n \geq 5$), so $q = 5$ by the same logic. This is a contradiction. □

Abel's Later Work

Much of Abel's work following his proof of the insolubility of the quintic was to find conditions on equations that guarantee a solution in radicals.

One of his results is the following:

Theorem (Abel):

Let $f(x) \in k[x]$ and suppose that $\alpha_1, \ldots, \alpha_n$ are its roots in L/k. Suppose that α_i is a rational function in α_1, ie. $\alpha_i = R_i(\alpha_1)$ and that

$$R_i(R_j(\alpha_1)) = R_j(R_i(\alpha_1))$$

for each i, j. Then $f(x) = 0$ is solvable in radicals.

In the language of Galois theory, this translates to the conditions

$$L = k(\alpha_1) \qquad \text{and} \qquad G_f \text{ is abelian.}$$

This theorem is perhaps the reason that Abel's name became attached to commutative groups.

Questions?