ABEL AND THE INSOLVABILITY OF THE QUINTIC

JIM BROWN

ABSTRACT. In this paper we deal with the insolvability of the quintic from Abel's perspective. We give a brief historical recap of the problem culminating in Abel's proof that a general quintic can not be solved by radicals. Most students of mathematics are familiar with the Galois theory argument that the general quintic is not solvable by radicals. It is our hope that this paper will shed light on the brilliance of Abel that is often overlooked. The modern language of groups and fields is pushed to the background, only to be brought forward in illustrating how Abel's ideas translate into modern language. The student who is not familiar with modern algebra but has the ability to read proofs and abstract mathematics should be able to read this paper and gain an understanding of this beautiful piece of mathematics.

1. Solvable by radicals?

In this paper we will treat Abel's proof that a general quintic is not solvable by radicals, a startling proof when most mathematicians of the day thought it was just a matter of time until someone found a method of solution. We will review not just Abel's proof, but also the history of the problem leading up to Abel's work. This paper does not assume the reader is familiar with modern algebra. Field extensions will be used to help connect the material to modern algebra for those with a knowledge of the subject, but this connection is not essential to understand Abel's proof. However, before we delve into the actual problem we remind the reader what this problem is and what it means for an equation to be solvable by radicals.

Consider the polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

In modern language, we say that $f(x)$ is *solvable by radicals* if the roots of $f(x)$ are in a finite field extension L/K where L is formed by successive field extensions

$$K = K_0 \subset K_1 = K(r_0^{\frac{1}{m_1}}) \subset K_2 = K_1(r_1^{\frac{1}{m_2}}) \subset \cdots \subset L = K_n = K_{n-1}(r_{n-1}^{\frac{1}{m_n}})$$

for integers $m_1, \ldots, m_n$ and elements $r_i \in K_i$.

Let us illustrate this by looking at the quadratic equation

$$f(x) = ax^2 + bx + c$$

for integers a, b, and c. The solutions to the quadratic equation, as is well known to all, are given by

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

2000 *Mathematics Subject Classification.* Primary 01A55.
Key words and phrases. Abel, Insolvability of the quintic.

The solutions are obtained from the normal elementary operations in addition to forming the square root of $b^2 - 4ac$. In this case, $L = \mathbb{Q}(\sqrt{b^2 - 4ac})$. Therefore, a quadratic equation is clearly solvable by radicals.

Similarly, one can see that the general cubic and the general quartic equations are solvable by radicals. For example, the general cubic can be put into the form $f(x) = x^3 + ax - b$ by a linear change of variables. A root of this polynomial is given by

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^2}{27}}} + \sqrt[3]{\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^2}{27}}}.$$

One can see this is a radical solution to $f(x)$ as defined above. In terms of fields, we have

$$\begin{aligned} K_1 &= K\left(\sqrt{\frac{b^2}{4} + \frac{a^2}{27}}\right), \\ K_2 &= K_1\left(\sqrt[3]{\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^2}{27}}}\right), \\ L &= K_3 = K_2\left(\sqrt[3]{\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^2}{27}}}\right), \end{aligned}$$

each of which is attained by adjoining a radical to the previous field where we assume here that K contains the third roots of unity.

Of course Abel and his contemporaries did not have the language of field extensions to work with. To Abel an equation is *solvable by radicals* if the roots are what Abel calls *algebraic functions*. Recall that a rational function is the ratio of two polynomials. Abel defines an algebraic function of the 0^{th} order to be a rational function of the coefficients. For example, $f_0(a,b,c) = \dfrac{a^5 - 4bc}{b^5 - 2c}$ would be a algebraic function of the 0^{th} order. An algebraic function of the 1^{st} order is a function $f_1(f_0^{\frac{1}{m}})$ where f_0 is a algebraic function of the 0^{th} order and f_1 is a rational function of the coefficients and $f_0^{\frac{1}{m}}$ to the 0^{th} order. An example of an algebraic function of the 1^{st} order would be $f_1(a,b,c) = \dfrac{-b + \sqrt{b^2 - 4ac}}{2a}$ where for this example we have $f_0 = b^2 - 4ac$ and $m = 2$. Similarly, we can define an algebraic function of any positive order k to be a function $f_k(f_{k-1}^{\frac{1}{m_k}})$ where f_{k-1} is an algebraic function of order $k-1$, m_k is a positive integer, and f_k is a rational function of the coefficients and $f_{k-1}^{\frac{1}{m_k}}$. We call an algebraic function of some positive order k an *algebraic function.*

2. The quadratic, cubic, and the quartic

The ability to solve quadratic equations dates back to the Babylonians around 4000 years ago. The Babylonians did their mathematics entirely base 60. Of course they did not treat these as abstract equations; their work was entirely word problems. What a nightmare for modern algebra students! Therefore they did not have a formula to solve general quadratic equations, but rather were aware of the method of completing the square in order to solve particular quadratic equations they encountered.

The next group to treat quadratic equations was the Arabic algebraists. The most famous of this group of mathematicians being al-Khwārizmi. He felt the need not just to solve the equations, but also to demonstrate their solution geometrically. This was also a popular trend as algebra moved to Europe; mathematicians of the day viewing algebra as inferior to geometry. The quadratic equations encountered by the Arabic algebraists were mostly in terms of bookkeeping problems. In fact, this seems to be the way that algebra was originally transferred to the geometric-minded Europeans.

This is where solvability remained until the 1500's when a group of Italian mathematicians provided solutions to the general cubic and general quartic. The Babylonians did make progress on the solution to the cubic, but their work was mostly lost until the 20th century and certainly not available to the mathematicians of the 16th century. The story of the solution of the cubic, and eventually the quartic, is a well known one. It is the first real instance of a priority fight over a discovery, especially one that turned nasty. Many great mathematicians of the day had tried and failed to find a method of solving the cubic by radicals. One notable example is Fibonacci, who believed the cubic unsolvable by radicals after failing to find a solution himself.

Many modern authors attribute the solution of the cubic to either Cardano or Nicolo Fontana. Fontana is more well know as Tartaglia, the name normally encountered when reading about the cubic. In fact, del Ferro seems to have been the first to solve the cubic. He never published his work, but rather passed his method on to a student before he died. Tartaglia claimed to be the first to solve the cubic. It may be that he did solve it independently of the work of del Ferro, but it is also entirely possible he was influenced by del Ferro's work. It is difficult to trust Tartaglia's claims because at this point in his life he had already published other's work claiming it to be his own several times. Regardless of del Ferro's influence on Tartaglia, it is clear that Tartaglia's solution was more general then del Ferro's. This much is clear due to the fact that Tartaglia defeated del Ferro's student in a mathematical duel, a popular way mathematicians of the day determined their prowess.

Cardano was interested in the solution of the cubic not just for the practical applications it entailed; he also viewed it as a way to out-perform the ancients by solving a problem they were unable to solve. When he learned of Tartaglia's claim to have solved the cubic he was intent on discovering Tartaglia's method. Tartaglia was a poor man and in need of money. Cardano convinced him to share his solution under the agreement that Cardano would not publish the solution. Cardano kept his word until he learned of del Ferro's solution, which he regarded as voiding his agreement with Tartaglia. When Cardano published the solution in his *Great Art*, he attributed it to Tartaglia as well as del Ferro. The mention of del Ferro infuriated Tartaglia, who claimed plagiarism. In fact, Tartaglia did not have the general solution to the cubic. Cardano was able to provide a solution that worked in full generality, allowing his student Ferrari to defeat Tartaglia in a mathematical duel of their own. The method used by all of these mathematicians is the same as used to solve the quadratic equation. They discovered a way to "complete the cube" in order to write the equation in the form $x^3 = a$. The Cardano solution to the equation $x^3 + ax - b = 0$, as given in the previous section, is

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^2}{27}}} + \sqrt[3]{\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^2}{27}}}.$$

Once the cubic had been solved, the quartic soon followed suit. Cardano's student Ferrari was able to solve the quartic by employing the same method as had been used to solve the cubic. Ferrari is able to reduce the quartic to solving a quadratic equation, thereby reducing it to an equation he was already able to solve. We will not state the solution here as it is not as simple to state and is easily found in any standard abstract algebra book, see ([4], Section 14.7) for example.

3. The first "equations" and the first "solutions"

It is often overlooked that the work of the Italian mathematicians on the cubic and the quartic was done without the benefit of modern notation or abstraction. They were still working with word problems, phrasing their cubics in the form:

> "Two men go into business together and have an unknown capital. Their gain is equal to the cube of the tenth part of their capital. If they had made three ducats less, they would have gained an amount exactly equal to their capital. What was their capital and their profit?"

It is of course much easier to state now:

> "What are the roots of the equation $\left(\frac{x}{10}\right)^3 - 3 = x$?"

The 17th century French lawyer and code-breaker Viete was the first to introduce modern notation. He was the first to come to the realization that a symbol can stand for a number and this symbol can be manipulated like a number. We now refer to Viete's "symbols" as variables, but Viete referred to them as species, indicating the entire species of numbers they could represent. It is clear what an extraordinarily powerful problem solving discovery this was. On top of this, he was also the first to consider the idea of coefficients. With these two breakthroughs he was able to begin considering equations of the forms $ax^3 + bx^2 + cx + d = 0$ as opposed to specific word problems as above.

Viete did not believe these discoveries to be his own. Unlike the Italian mathematicians discussed in Section 2 who were very concerned with their priority, Viete believed he had only rediscovered what the ancients must have already known. Though there is no evidence that the ancients did know his methods, Viete could not fathom how the Greeks would have been able to discover their proofs without his methods. One thing Viete was not modest about was the applicability of his methods. He believed that he could find the root of any polynomial by employing his new machinery. Adding fuel to this notion was his ability to solve a contest problem presented by van Roomen that involved finding the roots of a degree 45 polynomial. It so happened that Viete recognized the equation as a trigonometric identity, which he was then able to solve.

Descartes, a much more famous mathematician then Viete, picked up where Viete left off. He further developed Viete's methods and symbols to the point that his works begin to resemble modern mathematics. Descartes was the first to state the fundamental theorem of algebra: a degree n polynomial necessarily has n roots. Descartes did not attempt to prove this statement. He believed all polynomials of degree greater then 4 could be solved with the same methods as had been applied to the quadratic, the cubic, and the quartic. In fact, he left the solution of higher degree equations as an exercise to the reader.

4. The work of Lagrange and Ruffini

No discussion of the history of the insolvability of the quintic would be complete without discussing Langrange's contributions. Lagrange's 1771 paper *Reflections on the Algebraic Theory of Equations* was an immensely important paper. Instead of merely pushing forward and trying to find a solution of the quintic by radicals, Langrange analyzed why the methods used to solve the quadratic, the cubic, and the quartic had succeeded. He concluded that the method that had been used to solve these equations would not work to solve the quintic. His reasoning was as follows. For a cubic with roots $\alpha_1, \alpha_2, \alpha_3$ Langrange considered the resolvent

$$R = (\alpha_1 + \xi_3\alpha_2 + \xi_3^2\alpha_3)^3$$

with ξ_3 a root of the equation $x^3 - 1 = 0$. His novel idea was to consider what effect a permutation of the roots $(\alpha_1, \alpha_2, \alpha_3)$ would have upon the resolvent. For the cubic there are $3! = 6$ different possibilities for the permutation of the roots. However, Lagrange calculated that these permutations only lead to 2 different possible values for the resultant. For instance,

$$(\alpha_1 + \xi_3\alpha_2 + \xi_3^2\alpha_3)^3 = (\alpha_2 + \xi_3\alpha_3 + \xi_3^2\alpha_1)^3.$$

Similarly, when he considered the resolvent of a quartic he found that there are only 3 possible values for R even though there are $4! = 24$ possible permutations of the roots. The key fact here is that the number of possible values for the resolvent is less then the degree of the equation one is trying to solve. This is what allows one to simplify the equation as was done for the quadratic, cubic, and quartic. When Lagrange considered the resolvent of the quintic, he found that there were 6 possible values! Langrange concluded that the methods used before would not generalize to solve the quintic. However, he was still confident that the quintic could be solved by new methods.

Gauss seems to have been the first prominent mathematician to state that he believed the quintic was not solvable. His first statement to this effect was contained in his 1799 doctoral dissertation. He published this thought in his *Disquisitiones Arithmeticae*:

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

It is now widely known that the first serious attempt at proving the insolvability of the quintic was given by the Italian Paolo Ruffini. Ruffini was a doctor by trade, using his evenings to jot down his musings on mathematics. During his lifetime he published 6 versions of his proof, the first in *Teoria Generale delle Equazioni* in

1799 and the last in 1813. The reason he published so many versions is that his proof was not widely accepted. Each version of the proof was written to try and answer criticisms other mathematicians had leveled at his work. Ruffini's writing was notoriously long and difficult to understand. Lagrange, who Ruffini credited as his inspiration, said of Ruffini's work that there is "little in it worthy of attention." One of the few eminent mathematicians who did give Ruffini credit was Cauchy. He wrote to Ruffini praising his work, letting him know he had lectured on Ruffini's work and even generalized some of the results.

In fact there was a gap in Ruffini's proof. Ruffini assumed without proof that all algebraic functions can be expressed in terms of rational functions of the roots of the equation. In modern language, Ruffini failed to show that if L is a field that is contained in a radical tower over a field K, then L itself must necessarily be a radical extension. Later in his life Abel read Ruffini's work, coming to the same conclusions as most had that the work was difficult to read and did not fully demonstrate the insolvability of the quintic.

5. Abel: A biographical sketch

In this section we give a brief biographical sketch of Abel's life. The interested reader is advised to consult [5] for a more thorough treatment of Abel's biography.

Abel was born on August 5, 1802 in Frindoe, Norway. At the time Norway was still part of Denmark, not achieving independence until 1814. Abel grew up poor with many accounts saying his father was a drunk and his mother a woman of "low moral standards." Both of his parents died by the time he was 18 years old, leaving him to care for himself and his younger siblings.

Abel's genius was already apparent during his years in high school. His high school teacher Holmboe recognized his gifts and encouraged him to pursue them. While in high school Abel read works by Lagrange and Cauchy, among others. In fact, Abel read one of Cauchy's papers that was based upon Ruffini's work!

In 1821 Abel entered Royal Frederick's University in Christiania where he continued to excel. During his years at the university Abel believed he had found a general solution to the quintic. However, when pressed for numerical examples by his teachers he soon discovered his solution was not a general one. After this incident Abel set his sights on proving that the quintic was not in fact solvable by radicals. Due to his extraordinary talents, Abel was granted special permission by the university to travel to Berlin and Paris to meet with the great mathematicians of the day. Abel published his proof of the insolvability of the quintic in 1824 in the hope that it would open doors for him during his travels.

While on his travels Abel met several prominent mathematicians, receiving a chilly reception from most. While in Paris Abel met Legendre and Cauchy, each of which was less then encouraging to Abel. Abel wrote of the French mathematicians he met:

> "monstrous egotists ... uncommonly reserved with respect to foreigners ... Everyone works by himself here, without bothering others. Everyone wants to teach and no one wants to learn."

One of the more influential mathematicians he met was not one of the most famous of his day, but is well known now for the journal that still bears his name:

Crelle. Crelle was very impressed with Abel's work and encouraged him to submit his papers to the journal he was starting. Abel continued for the rest of his life to submit his work to Crelle for publication in his journal.

Towards the end of his life people finally started to recognize the brilliance of Abel's work. Such mathematicians as Gauss and Legendre sang his praises. Unfortunately, Abel was unable to secure a university position even with such mathematicians trying to find him work. He continued his work on the solvability of equations by radicals. In his pursuits he was the first to introduce the notion of "abelian", the notion still bearing his name. He may have finished the work that was ultimately left for Galois had he not stopped working on the solvability of equations in order to pursue competitive work with Jacobi on elliptic functions.

Abel died in poverty on April 6, 1829 of tuberculosis. On the 8th of April Crelle sent word that he had finally found a position for Abel so he would live in poverty no longer.

6. Abel's proof

In this section we present Abel's proof of the insolvability of the quintic by radicals as given in his 1824 paper. The method employed is reductio ad absurdum. Though the proof given in Abel's 1824 paper is very terse; we will fill in the details where appropriate. We are indebted to [5] for Abel's proof as well as the author's comments on the proof.

We begin with the general equation of degree 5

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0 \tag{1}$$

with the assumption that y is expressible in terms of radicals of the coefficients. Abel states that it is clear that one can write

$$y = a_0 + a_1 R^{\frac{1}{p}} + a_2 R^{\frac{2}{p}} + \cdots + a_{p-1} R^{\frac{p-1}{p}}$$

where p is a prime and $a_0, \ldots, a_{p-1}, R$ are all of the same form as y. He presents a proof of this fact in an 1826 paper. We state this result as a theorem and give Abel's proof of this fact.

Theorem 6.1. *Any algebraic function y solving Equation 1 can be written in the form*

$$y = a_0 + a_1 R^{\frac{1}{p}} + a_2 R^{\frac{2}{p}} + \cdots + a_{p-1} R^{\frac{p-1}{p}}$$

with p a prime and $a_0, \ldots, a_{p-1}, R$ are algebraic functions of lower order then y.

Proof. Note that by factoring p and writing radicals to the p as a nested sequence, we can assume p is prime. For example, $\sqrt[6]{\alpha} = \sqrt[3]{\sqrt[2]{\alpha}}$.
Let v be an algebraic function as in the statement of the theorem. By definition we can write $v = \dfrac{F}{G}$ where

$$G = g_0 + g_1 R^{\frac{1}{p}} + g_2 R^{\frac{2}{p}} + \cdots + g_q R^{\frac{q}{p}}$$

for some $q \in \mathbb{N}$ and p prime and similarly for F. Next we consider the substitutions $R^{\frac{1}{p}} \mapsto \xi R^{\frac{1}{p}}, R^{\frac{1}{p}} \mapsto \xi^2 R^{\frac{1}{p}}, \ldots, R^{\frac{1}{p}} \mapsto \xi^{p-1} R^{\frac{1}{p}}$ where $\xi \neq 1$ is a solution to the equation $x^p - 1 = 0$. Note that we have $p-1$ different substitutions so in general we have $p-1$ different values of G, call them $G_1, \ldots, G_{p-1}$. Consider the expression

$$v = \frac{FG_1 G_2 \cdots G_{p-1}}{GG_1 G_2 \cdots G_{p-1}}.$$

We claim that we can write the denominator of v as an algebraic function of the 0^{th} order. To see this, merely multiply out the expression and gather terms:

$$\begin{aligned} GG_1G_2\cdots G_{p-1} &= (g_0 + g_1R^{\frac{1}{p}} + g_2R^{\frac{2}{p}} + \cdots + g_qR^{\frac{q}{p}}) \\ &\quad \times(g_0 + g_1\xi R^{\frac{1}{p}} + g_2\xi^2R^{\frac{2}{p}} + \cdots + g_q\xi^qR^{\frac{q}{p}}) \\ &\quad \times\cdots\times(g_0 + g_1\xi^{p-1}R^{\frac{1}{p}} + g_2\xi^{2(p-1)}R^{\frac{2}{p}} + \cdots + g_q\xi^{q(p-1)}R^{\frac{q}{p}}) \\ &= \text{something with no } R^{\frac{i}{p}} \text{ left with } 0 < i < p \end{aligned}$$

where we have used the fact that

$$\begin{aligned} 1 + \xi + \xi^2 + \cdots + \xi^{p-1} &= \frac{1-\xi^p}{1-\xi} \\ &= 0. \end{aligned}$$

If g_0 is a polynomial, we are done. If it contains further radicals we can repeat the process until their are no radicals left, leaving us with a g_0 that is simply a rational function of the coefficients, i.e., an algebraic function of the 0^{th} order.
Using this fact, we can write

$$v = \frac{F}{G} = \frac{FG_1G_2\cdots G_{p-1}}{GG_1G_2\cdots G_{p-1}} = f_0 + f_1R^{\frac{1}{p}} + \cdots f_qR^{\frac{q}{p}}$$

as an algebraic function of order k for some positive integer k where we have absorbed the rational function $GG_1G_2\cdots G_{p-1}$ into the numerator and the f_i and R are algebraic functions of order $k-1$. We can assume $q < p$ for if not we could write $p = n_1q + m_1$ and so $R^{\frac{q}{p}} = R^{m_1}R^{\frac{n_1}{p}}$. We can then absorb the R^{m_1} into the coefficients f_i. □

To see an example of Theorem 6.1 we can consider the cubic $y^3 + ay - b = 0$ again. Cardano's solution can be written in the form

$$y_0 = R^{\frac{1}{3}} + a_2R^{\frac{2}{3}}$$

where

$$R = \frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}$$

and

$$a_2 = -\frac{a}{3R}.$$

Note that Theorem 6.1 can be stated in modern language as follows.

Theorem 6.2. *Assume that $x^p - R \in F[x]$ is irreducible and that α is a root. Let β be an element of $F(\alpha)$ with $\beta \notin F$. Then there is a $\gamma \in F(\alpha)$ such that $\gamma^p \in F$ and*

$$\beta = a_0 + \gamma + a_2\gamma^2 + \cdots + a_{p-1}\gamma^{p-1}$$

where $a_0, a_2, \ldots, a_{p-1} \in F$.

Theorem 6.3. *The general equation of degree 5*

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0 \tag{2}$$

is not solvable by radicals.

Proof. Suppose such a solution y_0 exists. Theorem 6.1 shows that we can write

$$y_0 = a_0 + a_1 R^{\frac{1}{p}} + a_2 R^{\frac{2}{p}} + \cdots + a_{p-1} R^{\frac{p-1}{p}} \tag{3}$$

with p a prime and $a_0, \ldots, a_{p-1}, R$ are all algebraic functions of lower order then y_0. Note that we can assume $a_1 = 1$ by replacing $R^{\frac{1}{p}}$ by $\left(\frac{R}{a_1^p}\right)^{\frac{1}{p}}$ if necessary. Therefore assume our solution is of the form

$$y_0 = a_0 + R^{\frac{1}{p}} + a_2 R^{\frac{2}{p}} + \cdots + a_{p-1} R^{\frac{p-1}{p}}. \tag{4}$$

We can assume that it is impossible to express $R^{\frac{1}{p}}$ as a rational function in $a_0, a_1, \ldots, a_{p-1}, R$ and the coefficients of Equation 2. Subsituting Equation 4 into Equation 2, we obtain an expression

$$b_0 + b_1 R^{\frac{1}{p}} + b_2 R^{\frac{2}{p}} + \cdots + b_{p-1} R^{\frac{p-1}{p}} = 0$$

where the b_i are polynomials in the a_j's and R and rational functions of the coefficients of Equation 2.

Claim 6.4. It must be the case that b_0, b_1, $\ldots$, b_{p-1} are all 0.

Proof. Let $z = R^{\frac{1}{p}}$. We have the following simultaneous equations

$$z^p - R = 0 \quad \text{and} \quad b_0 + b_1 z + b_2 z^2 + \cdots + b_{p-1} z^{p-1} = 0.$$

If we assume that the b_i are not all 0 then we must have some nonzero solution to the system of equations. Suppose there are k such values that are simultaneous solutions. We can find an equation

$$c_0 + c_1 z + \cdots + c_k z^k \tag{5}$$

that has these k values as its roots where the c_i are rational functions of R, b_0, b_1, $\ldots$, b_{p-1}. Since it shares the k roots with $z^p - R = 0$, we know that the roots of Equation 5 must be of the form ξz for ξ a root of the equation $x^p - 1 = 0$. Upon substituting the simultaneous solutions $xi_i z$ into the equation

$$b_0 + b_1 z + b_2 z^2 + \cdots + b_{p-1} z^{p-1} = 0$$

we obtain k simultaneous equations

$$\begin{aligned} c_0 + c_1 z + \cdots + c_k z^k &= 0 \\ c_0 + \xi_1 c_1 z + \cdots \xi_1^k c_k z^k &= 0 \\ &\vdots \\ c_0 + \xi_{k-1} c_1 z + \cdots \xi_{k-1}^k c_k z^k &= 0. \end{aligned}$$

If we treat each power of z as a separate unknown, then we have k simultaneous equations to determine k unknowns. Therefore we can always find z as a rational function of $c_0, c_1, \ldots, c_k$. Since the c_i's are themselves rational functions of the coefficients of Equation 2 along with $a_0, a_1, \ldots, a_{p-1}$ and R, this shows that we can express $R^{\frac{1}{p}}$ as such a rational function. However, we assumed this was not possible, giving us our contradiction. Thus it must be that $b_i = 0$ for all $i = 0, \ldots, p-1$. □

Note that Claim 6.4 can be written in modern language as follows.

Theorem 6.5. *Let $f(x) \in F[x]$ be an irreducible polynomial of degree p over the field F and let $K = F[x]/(f(x))$. Let $\theta = x (\mathrm{mod}\, f(x)) \in K$. Then the elements $1, \theta, \theta^2, \ldots, \theta^{p-1}$ are a basis for K as a vector space over F.*

Abel now observes that if y_0 is a solution to Equation 2, then so are the values y_i where the values y_i are obtained from y_0 by making the substitution $R^{\frac{1}{p}} \mapsto \xi^i R^{\frac{1}{p}}$ for ξ as above. One can see that these y_i are still solutions by making the substitution into Equation 2. One will once again get an expression

$$b_0 + b_1 R^{\frac{1}{p}} + b_2 R^{\frac{2}{p}} + \cdots + b_{p-1} R^{\frac{p-1}{p}}$$

as before, only this time we will also have powers of ξ multiplying the b_i. However, we showed above that all the b_i are necessarily 0, so we still get that this sum is 0.

Observe that since we are looking at a quintic, it must be that $p \leq 5$. We can also restrict to the case that the roots are distinct. If we have a quintic polynomial $f(x)$ with a repeated root α, then we can write $f(x) = (x - \alpha)^2 g(x)$ where $g(x)$ is a polynomial of degree 3. Then showing that the roots of $f(x)$ are expressible by radicals is the same as showing that $(x - \alpha) g(x)$ has roots that are expressible as radicals. However, this is a polynomial of degree 4, a problem that has already been solved. Therefore we have the following equations

$$y_0 = a_0 + R^{\frac{1}{p}} + a_2 R^{\frac{2}{p}} + \cdots + a_{p-1} R^{\frac{p-1}{p}} \tag{6}$$

$$y_1 = a_0 + \xi R^{\frac{1}{p}} + a_2 \xi^2 R^{\frac{2}{p}} + \cdots + a_{p-1} \xi^{p-1} R^{\frac{p-1}{p}} \tag{7}$$

$$\vdots$$

$$y_{p-1} = a_0 + \xi^{p-1} R^{\frac{1}{p}} + a_2 \xi^{p-2} R^{\frac{2}{p}} + \cdots + a_{p-1} \xi R^{\frac{p-1}{p}}. \tag{8}$$

Consider now the sum $y_0 + y_1 + \cdots + y_{p-1}$. This sum is given by

$$\begin{aligned} y_0 + y_1 + \cdots + y_{p-1} = p a_0 + (1 + \xi + \cdots + \xi^{p-1}) R^{\frac{1}{p}} \\ + a_2 (1 + \xi + \cdots + \xi^{p-1}) R^{\frac{2}{p}} + \cdots \\ + a_{p-1} (1 + \xi + \cdots + \xi^{p-1}) R^{\frac{p-1}{p}}. \end{aligned}$$

Recalling the definition of ξ, we see that

$$a_0 = \frac{1}{p}(y_0 + y_1 + \cdots + y_{p-1}).$$

Similarly, to find an expression for y_1, we multiply Equation 6 by 1, Equation 7 by ξ^{p-1}, etc. until multiplying Equation 8 by ξ and add them up. In this case we get

$$\begin{aligned} y_0 + \xi^{p-1} y_1 + \xi^{p-2} y_2 + \cdots + \xi y_{p-1} = (1 + \xi + \cdots + \xi^{p-1}) a_0 \\ p \xi^p R^{\frac{1}{p}} + a_2 \xi^p (1 + \xi + \cdots + \xi^{p-1}) R^{\frac{2}{p}} + \cdots \\ + a_{p-1} \xi^p (1 + \xi + \cdots + \xi^{p-1}) R^{\frac{p-1}{p}}. \end{aligned}$$

Therefore, we have

$$R^{\frac{1}{p}} = \frac{1}{p}(y_0 + \xi^{p-1} y_1 + \cdots + \xi y_{p-1}). \tag{9}$$

Following the same reasoning we also obtain

$$\begin{aligned} a_2 R^{\frac{2}{p}} &= \frac{1}{p}(y_0 + \xi^{p-2} y_1 + \cdots + \xi^2 y_{p-1}) \\ &\vdots \\ a_{p-1} R^{\frac{p-1}{p}} &= \frac{1}{p}(y_0 + \xi y_1 + \cdots + \xi^{p-1} y_{p-1}). \end{aligned}$$

Using these equations we see that $a_0, \ldots, a_{p-1}$, R, and $R^{\frac{1}{p}}$ are all rational functions in the roots of Equation 2. Let us consider one of these quantities, say R. Then as we did with y_0 above, we can write

$$R = r_0 + S^{\frac{1}{q}} + r_2 S^{\frac{2}{q}} + \cdots + r_{q-1} S^{\frac{q-1}{q}}. \tag{10}$$

As above, we consider the substitutions $S^{\frac{1}{q}} \mapsto \varsigma^i S^{\frac{1}{q}}$ with ς a root of

$$x^{q-1} + x^{q-2} + \cdots + x + 1 = 0.$$

Using the same arguments, we get that $r_0, \ldots, r_{q-1}$, S, and $S^{\frac{1}{q}}$ are all rational functions of the different values of R under these substitutions. However, we know that the different values of R are all rational functions of $y_0, y_1, \ldots, y_{p-1}$. Therefore, it must be that the functions $r_0, \ldots, r_{q-1}$, S, and $S^{\frac{1}{q}}$ are rational functions of $y_0, y_1, \ldots, y_{p-1}$ as well. Following this line of reasoning we can conclude that the irrational functions in the expression for y are all rational functions of the roots of Equation 2.

Let us now consider irrational functions of the form $R^{\frac{1}{p}}$ with R a rational function of the coefficients of Equation 2. At this point Abel is starting from the beginning with R an algebraic function of the 0^{th} order. We now relabel the roots of Equation 2 to be $y_0, y_1, \ldots, y_4$. Write $r = R^{\frac{1}{p}}$, so in particular we have that r is a rational function of the roots $y_0, y_1, \ldots, y_4$ (see argument surrounding Equation 10) and R is a symmetric function of these roots (R is rational in the coefficients, so in particular it is symmetric in the roots). Since we are looking at the solution of a general quintic, we can consider the y_i as independent variables. Since R is a symmetric function in the y_i it remains unchanged under permutations of the y_i. Since $f(x) = x^p - R$ is an irreducible polynomial, we have that r takes on p different values under permutations of the roots. Observing that there are 5! different permutations of the roots $y_0, y_1, \ldots, y_4$, the work of Lagrange gives that p must be a divisor of 5!. (In modern terms this is just Lagrange's theorem on the order of a subgroup dividing the order of the group.) Since p is prime, we must have that $p = 2, 3$ or 5. Abel uses the following theorem due to Cauchy.

Theorem 6.6. *([2]) The number of values a function of n variables can take under permutations of the variables cannot be lower than the largest prime number $p \leq n$ without becoming equal to 2.*

What this says for the case of the quintic is that $p = 2$ or 5. Suppose that $p = 5$. The function $r = R^{\frac{1}{5}}$ has 5 different values. Abel states without proof that this means that r can be put in the form

$$R^{\frac{1}{5}} = r = \alpha_0 + \alpha_1 y_0 + \alpha_2 y_0^2 + \alpha_3 y_0^3 + \alpha_4 y_0^4 \tag{11}$$

with the α_i being symmetric functions of $y_0, y_1, \ldots, y_4$. Abel published a proof of this fact in a later article, but we omit that proof here due to its lack of availability.

Two versions of this "proof" are given in [5], with the first being completely bogus and the second still unconvincing. Recall that the various roots of Equation 1 are formed from by making the substitution $R^{\frac{1}{5}} \mapsto \xi^i R^{\frac{1}{5}}$ for ξ a fifth root of unity. Multiplying both sides of Equation 11 by ξ which amounts to taking $R^{\frac{1}{5}}$ to $\xi R^{\frac{1}{5}}$ and hence y_0 to y_1 we obtain

$$\alpha_0 + \alpha_1 y_1 + \alpha_2 y_1^2 + \alpha_3 y_1^3 + \alpha_4 y_1^4 = \xi\alpha_0 + \xi\alpha_1 y_0 + \xi\alpha_2 y_0^2 + \xi\alpha_3 y_0^3 + \xi\alpha_4 y_0^4.$$

This equation implies either $\xi = 1$ or y_0 and y_1 are not algebraically independent $(y_1 = \xi y_0)$, both of which we assumed were not true. Therefore we must have $p = 2$.

Let $r = R^{\frac{1}{2}}$. Note that r must have two different values of opposite sign. Abel again uses a result due to Cauchy that states one can write

$$r = sS^{\frac{1}{2}}$$

where

$$S^{\frac{1}{2}} = (y_0 - y_1)(y_0 - y_2)\cdots(y_1 - y_2)\cdots(y_3 - y_4)$$

and s is a symmetric function.

Consider now irrational functions of the form

$$\left(d_0 + d_1 R_1^{\frac{1}{n_1}} + d_2 R_2^{\frac{1}{n_2}} + \cdots\right)^{\frac{1}{m}} \tag{12}$$

with the d_i and the R_i being rational functions of the coefficients of Equation 2 and hence symmetric functions of the roots $y_0, y_1, \ldots, y_4$. Note that what we are doing here is considering a radical of a sum of algebraic functions of order 1. Applying what we have just done to each $R_i^{\frac{1}{n_i}}$, it must be the case that $n_1 = n_2 = \cdots = 2$, $R_1 = s_1^2 S$, $R_2 = s_2^2 S$, etc. with each s_i a symmetric function. We can write Equation 12 as

$$(e_0 + e_1 S^{\frac{1}{2}})^{\frac{1}{m}}. \tag{13}$$

Set

$$r_0 = (e_0 + e_1 S^{\frac{1}{2}})^{\frac{1}{m}},$$

and

$$r_1 = (e_0 - e_1 S^{\frac{1}{2}})^{\frac{1}{m}}.$$

Upon multiplying r_0 and r_1 we obtain

$$r_0 r_1 = (e_0^2 - e_1^2 S)^{\frac{1}{m}}.$$

Suppose that $r_0 r_1$ is not a symmetric function. Then applying Theorem 6.6 we must have $m = 2$. However, this cannot be the case as then r_0 would have 4 different values, being a square root of terms involving a square root. As we observed above, the only possible values under Theorem 6.6 are 2 or 5. Therefore it must be the case that $r_0 r_1$ is a symmetric function.

Set $v = r_0 r_1$ and

$$z = r_0 + r_1 = (e_0 + e_1 S^{\frac{1}{2}})^{\frac{1}{m}} + v(e_0 + e_1 S^{\frac{1}{2}})^{-\frac{1}{m}}.$$

We have eliminated the possibility that $m = 2$, so it must be the case that $m = 5$ since m is necessarily a prime number. Since z takes on 5 values, we can use the same reasoning as in Equation 11 to write

$$\begin{aligned} z &= \alpha_0 + \alpha_1 y + \alpha_2 y^2 + \alpha_3 y^3 + \alpha_4 y^4 \\ &= (e_0 + e_1 S^{\frac{1}{2}})^{\frac{1}{5}} + v(e_0 + e_1 S^{\frac{1}{2}})^{-\frac{1}{5}} \end{aligned} \tag{14}$$

where the α_i are symmetric functions of the roots y_i and thus rational functions of the coefficients of Equation 2.

The next step in Abel's argument is not clear to me. He states:

> Combining this equation with the proposed equation, we can express y in terms of a rational function of z, a, b, c, d, and e. Now such a function is always reducible to the form
>
> $$y = A_0 + R^{\frac{1}{5}} + A_2 R^{\frac{2}{5}} + A_3 R^{\frac{3}{5}} + A_4 R^{\frac{4}{5}} \tag{15}$$
>
> with the A_i and R are functions of the form $e_0 + e_1 S^{\frac{1}{2}}$, e_0, e_1 and S being rational functions of a, b, c, d, and e.

For the second part to get the A_i and R of the correct form, he is using the same type of arguments as used in establishing Theorem 6.1 and then the arguments used in establishing Equation 13. It is possible that he means that one can express y in terms of an algebraic function of z, a, b, c, d and e. This would make sense because Equation 14 is a quartic, which we know is solvable by radicals. However, this is not what he states. It is also then not clear that one gets the desired form for the A_i's and R.

Assuming what Abel says is valid, the proof can be concluded as follows. Using the expression in Equation 15 for y we obtain

$$R^{\frac{1}{5}} = \frac{1}{5}(y_0 + \xi^4 y_1 + \xi^3 y_2 + \xi^2 y_3 + \xi y_4) \tag{16}$$

$$= (e_0 + e_1 S^{\frac{1}{2}})^{\frac{1}{5}} \tag{17}$$

where we have used the same reasoning as that used to arrive at Equation 9. However, we see that Equation 16 has 120 possible values under permutation of the roots y_i, where as Equation 17 has only 10 possible values. This gives the contradiction to the assumption that Equation 2 is solvable by radicals. □

We end by briefly translating the last part of Abel's argument into modern language. Let $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n = L$ be the tower of field extensions given by the fact that we are assuming Equation 1 is solvable by radicals. What Abel is showing is that K_1 is necessarily a quadratic extension of K and that no further extension is possible, which gives the contradiction he needs.

References

[1] N. Abel, *Oeuvres Complètes*, Two Volumes, (L. Sylow and S. Lie, ed.), Grondahl and Son, Christiana, 1881.
[2] A. Cauchy, *Mémoire sur le nombre des valuers qu'une fonction peut acquérir* (1815), Oeuvres Compléte d'Augustin Cauchy, (Paris:Gauthier-Villars, 1905), series II, 1:62-90.
[3] H. Dörrie, *100 Great Problems of Elementary Mathematics*, Dover Publications Inc., New York, 1965.
[4] D. Dummitt and R. Foote, *Abstract Algebra*, Second Edition, John Wiley and Sons, Inc., New York, 1999.
[5] P. Pesic, *Abel's Proof*, The MIT Press, Cambridge, Massachusetts (2003).
[6] M. Rosen, *Niels Hendrik Abel and Equations of the Fifth Degree*, Amer. Math. Monthly 102, 495-505 (1995).

Department of Mathematics, The Ohio State University, Columbus, OH 43210
E-mail address: jimlb@math.ohio-state.edu