Abel and the Insolvability of the Quintic: Part 1

Introduction

Most of the students come across the solution of linear and quadratic equations in their secondary classes. While the solution of a linear equation $ax + b = 0$ with a, b being rational does not present any difficulties (because the solution x itself turns out to be a rational number), a quadratic equation of the form $ax^2 + bx + c = 0$ (with a, b, c rational) does present significant challenges. For one thing the solution may not be rational and sometimes may not be even real. Usually one encounters the use of square roots to solve such an equation. Fortunately there is a standard formula for solving such equations

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

so that the equation can be solved directly in terms of its *literal* coefficients.

Many mathematicians tried to extend these ideas to solve the equations of third and fourth degrees. Thus during the 16th century Cardano solved the cubic and Ferrari solved the quartic equation. Later in the 18th century Lagrange published his classic work "Reflexions sur la resolution algébrique des equations" in which he unified the existing methods of solving equations upto degree 4. He hoped that unifying all the available approaches into one coherent theory would help in solving higher degree equations. But neither Lagrange nor any other mathematician was able to provide a solution to quintics (equations of degree 5) or higher degree equations. Then in 1824 a young Nowergian mathematician Niels Henrik Abel proved that *it is not possible to solve a quintic equation in the same way as it is possible to solve equations of degree* $2, 3$ *or* 4.

In this series of posts we will study the above mentioned result of Abel and its very tricky and non-obvious proof.

Solution of Algebraic Equations Through Radicals

Before we start onto a discussion of Abel's theorem, it is better to discuss the solution of quadratic and cubic equations and note some similarities in these approaches. Since we have already mentioned the quadratic formula for the solution of a quadratic equation we discuss the solution of cubic equations. In this regard, we follow the approach of Cardano.

Let the cubic equation be given by

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0 \tag{1}$$

By dividing the equation with a_0 we can always assume that the coefficient of x^3 is 1. Hence let's assume the equation is of the form $x^3 + a_1x^2 + a_2x + a_3 = 0$ where a_1, a_2, a_3 are real or complex numbers. What we want here is a formula consisting of a_1, a_2, a_3 through which we can get the solution of the equation by substituting numerical values of a_1, a_2, a_3. Thus what we need is a general formula for expressing the root of the equation in terms of its literal

coefficients. If we assume that α, β, γ are roots of the equation then we get $\alpha + \beta + \gamma = -a_1$ so that

$$(\alpha + a_1/3) + (\beta + a_1/3) + (\gamma + a_1/3) = 0$$

and thus if we put $y = x + a_1/3$ we will get a cubic equation in y whose sum of roots is 0 so that the equation won't have a term containing y^2. Thus by simple linear substitution it is possible to reduce any cubic equation in the form

$$x^3 + ax + b = 0 \tag{2}$$

We will solve this standard form of the cubic equation. Let's the assume that the solution is of the form $x = A + B$ so that

$$x^3 = (A + B)^3 = A^3 + B^3 + 3AB(A + B)$$

which leads to

$$x^3 - 3ABx - (A^3 + B^3) = 0 \tag{3}$$

Comparing this with the original equation (2) we get $3AB = -a, A^3 + B^3 = -b$ so that $A^3B^3 = -a^3/27$. Therefore A^3, B^3 are the roots of $t^2 + bt - (a^3/27) = 0$ i.e.

$$t = \frac{-b \pm \sqrt{b^2 + \dfrac{4a^3}{27}}}{2} = -\frac{b}{2} \pm \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}$$

and thus we get the solution for the cubic as

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

The solution is thus seen to be composed of nested radicals. The square roots are supposed to generate two values and both of them are taken care of in the above formula. Similarly the cube roots are supposed to generate 3 values each and thus the above expression seems to give 9 values of x. However there is a constraint of $AB = -a/3$ which restricts our choices and we get only three values of A, B and hence 3 values of x. If A, B represent one pair of values then the other two pairs are $A\omega, B\omega^2$ and $A\omega^2, B\omega$ where ω is an primitive cube root of unity given by $\omega^2 + \omega + 1 = 0$.

If we observe carefully we find that the solution ultimately requires the use of roots of unity as well as a series of nested radicals. We thus say that a *general* cubic equation (by *general* we mean an equation with literal coefficients) can be *solved by radicals*. The solution of a general quartic equation is also composed of a series of nested radicals and roots of unity so that a quartic equation is also solvable by radicals.

However all attempts to solve equations of higher degrees met with failure and some people started suspecting that the problem itself is insoluble. While equations like $x^5 - 2 = 0$ did have a solution in terms of radicals namely $x = \sqrt[5]{2}$ no such solution was forthcoming for a

general quintic. While investigating this problem Abel tried to think of most general form of a solution by radicals and then figured out that such a solution for a quintic equation led to a contradiction. This way by a very long and clever argument he established in 1824 that a general quintic could not be solved by radicals.

Before we present Abel's proof it is better to describe the concept of "solvability by radicals" in a slightly more formal manner. To do that we need to understand the technicality of radicals appearing in the solution of cubic and quadratic equations. Thus for example if we consider a quadratic equation $x^2 + ax + b = 0$ and its solution $x = (-a \pm \sqrt{a^2 - 4b})/2$ we see that apart from the expression composed of the coefficients a, b and algebraic operations $+, -, \times, /$ we also need a square root operation to generate new quantities like $\sqrt{a^2 - 4b}$. The idea of a square root is handled very smartly by proposing the existence of a quantity u such that $u^2 = a^2 - 4b$ and allowing the quantity u to be operated with existing quantities a, b using the usual algebraic operation of $+, -, \times, /$ and following the standard algebraical rules of these operations.

In effect we are starting with a field containing rational expressions in a, b and then proposing a new element u and making rational expressions in u, a, b. Also whenever possible we replace u^2 and higher powers of u by rational expressions in a, b, u so that any rational expression in u, a, b is of the form $Au + B$ where A, B are rational expressions in a, b. While dealing with a rational expression it is obvious that the coefficients must include rational numbers and to account for the roots of unity we propose that the coefficients in these rational expressions can be complex numbers. The field of rational expressions in literals a, b with complex coefficients is denoted by $\mathbb{C}(a, b)$. When viewed in this way we see that the field of rational functions in u, a, b i.e. $\mathbb{C}(u, a, b)$ includes $\mathbb{C}(a, b)$ and many other new elements of the form $Au + B$ with $A \neq 0$. We thus say that the field $\mathbb{C}(u, a, b)$ is an extension of the field $\mathbb{C}(a, b)$.

Radical Extensions

It is to be noted that if $(a^2 - 4b)$ is a perfect square (i.e. square of some quantity in $\mathbb{C}(a, b)$) so that $u \in \mathbb{C}(a, b)$ then there is no field extension and we have $\mathbb{C}(u, a, b) = \mathbb{C}(a, b)$. Hence for the concept of field extensions to work it is necessary to posit a further constraint that there is no member $u \in \mathbb{C}(a, b)$ such that $u^2 = a^2 - 4b$. Such a quantity u is then called a *radical* and the corresponding field extension $\mathbb{C}(u, a, b)$ is called a *radical extension* of the field $\mathbb{C}(a, b)$.

More formally we say that *a field R is a radical extension of height 1 of a field F, if there exist $u \in R, a \in F$ and a prime number p such that $u^p = a$ and there is no member in F whose p^{th} power is a and every member of R is a rational expression in u and members of F.*

In the above case we write $R = F(u)$. Unless otherwise stated the base field F will be assumed to be a field of rational expressions in a finite number of literals with complex coefficients i.e. $F = \mathbb{C}(x_1, x_2, \ldots, x_n)$. For completeness we say that R is a radical extension

of F of height 0 if $R = F$.

Using induction we now define radical extension with arbitrary height h where h is a positive integer. *A field R is said to be a radical extension of height h of a field F, if there is another field R_1 such that R is a radical extension of height 1 of R_1 and R_1 is a radical extension of height $h-1$ of base field F*. Thus a radical extention R of height h of base field F can be viewed as tower of radical extensions $F = R_0, R_1, R_2, \ldots, R_h = R$ such that each R_i is a radical extension of height 1 of R_{i-1}.

Since each radical extension of height 1 involves an element a in base field and a prime p such that a is not a p^{th} power in base field and a quantity u in the extension field such that $u^p = a$, it follows that the existence of a radical extension $R = R_h$ of height h of base field $F = R_0$ implies the existence of h prime numbers $p_1, p_2, \ldots, p_h$ and elements $a_1 \in R_0, a_2 \in R_1, \cdots, a_h \in R_{h-1}$ and $b_1 \in R_1, b_2 \in R_2, \cdots, b_h \in R_h$ such that a_i is not a p_i^{th} power in R_{i-1} and $b_i^{p_i} = a_i$. This is the way we express the concept of a nested radical in a formal fashion. Each level of nesting increases height of radical extension by 1. From the definition above it is obvious that the property of "being a radical extension" is a transitive one in the sense that if a field R is a radical extension of field F and field L is a radical extension of field R, then L is also a radical extension of F.

If we observe the solution of cubic equation $x^3 + ax + b = 0$ given above by Cardano, then we can see that it involves a square root $\sqrt{(b^2/4) + (a^3/27)} = u$ which can be said to lie in a radical extension of $\mathbb{C}(a, b)$ of height 1 as we have $u^2 \in \mathbb{C}(a, b)$ and for sure the expression $(b^2/4) + (a^3/27)$ is not a perfect square of any rational expression in $\mathbb{C}(a, b)$. If we call this radical extension $R_1 = \mathbb{C}(u, a, b)$ then we can see that we need another radical extension of R_1, say R_2, to handle the cube roots involved in the formula for x. In fact we need two radical extensions R_2 and R_3 such that $u_1 \in R_2$ and $u_2 \in R_3$ such that $u_1^3 = -(b/2) + u \in R_1$ and $u_2^3 = -(b/2) - u \in R_1$. We will later see that we can find a single radical extension R' of R_1 which contains $x = u_1 + u_2$.

Let us now define formally the concept of solvability of a polynomial equation by radicals. Let $P(x)$ be a polynomial with coefficients in a field F. Then $P(x)$ is said to be *solvable by radicals over F* if there is a radical extension of F which contains a root of $P(x)$. Using the quadratic formula we can say that the polynomial $x^2 + ax + b$ is solvable by radicals over $\mathbb{Q}(a, b)$. Similarly from Cardano's formulas it is obvious that polynomial $x^3 + ax + b$ is solvable by radicals over $\mathbb{Q}(a, b)$.

Abel did not have this terminology or notation of radical extensions but he used expressions like $R^{1/p}$ to denote radical quantities and was able to put forth his long argument without the use of a sufficiently general notation. Parallel to the concept of radical extensions of height h, Abel defined the concept of algebraic functions of order k.

An algebraic function of order 0 is a rational expression of the coefficients of the given

polynomial equation. The coefficients used to make this rational expression are complex numbers. Suppose we are dealing with a cubic equation $x^3+ax^2+bx+c=0$. Then an algebraic function of order 0 is a rational function $f_0(a,b,c)$ with complex coefficients. Next an algebraic function of order 1 is a rational function of the form $f_1(f_0^{1/m},a,b,c)$ where f_0 is an algebraic function of order 0 and m is a positive integer which can be assumed to be prime. This way Abel introduced radicals of type $f_0^{1/m}$. This process can be carried on inductively to define an algebraic function of order k. This shows the sheer brilliance of a young genius who solved a famous long standing problem which daunted the likes of Gauss and Lagrange.

The General Polynomial Equation

In what follows we will focus on the solution of the general polynomial equation of degree n given by

$$x^n-s_1x^{n-1}+\cdots+(-1)^{n-1}s_{n-1}x+(-1)^ns_n=(x-x_1)(x-x_2)\cdots(x-x_n)$$

where the literals (aka indeterminates) $x_1,x_2,\ldots,x_n$ are the n distinct roots and $s_1,s_2,\ldots s_n$ are the elementary symmetric polynomials in roots x_i.

The field of rational expressions in $s_1,s_2,\ldots,s_n$ (i.e. coefficients of the polynomial equation) will be denoted by $\mathbb{C}(s_1,s_2,\ldots,s_n)$ and the field of rational expressions in the roots x_i will be denoted by $\mathbb{C}(x_1,x_2,\ldots,x_n)$. It is then then clear that $\mathbb{C}(s_1,s_2,\ldots,x_n)$ represents the field of *symmetric* rational expressions in literals $x_1,x_2,\ldots,x_n$. It thus follows that $\mathbb{C}(s_1,s_2,\ldots,s_n)$ is a proper subfield of $\mathbb{C}(x_1,x_2,\ldots,x_n)$.

In this notation the problem of "solving the general polynomial equation by radicals" is equivalent to finding whether there exists a radical extension R of $\mathbb{C}(s_1,s_2,\ldots,s_n)$ which contains $x_1,x_2,\ldots,x_n$ and thus contains $\mathbb{C}(x_1,x_2,\ldots,x_n)$. When $n=1,2,3,4$ it is known that such a radical extension exists. Abel showed that when $n\geq 5$ no such radical extension R exists.

Ruffini's Work on Solvability of Equations

When the problem is formulated in this manner it becomes almost obvious that before we can solve this problem it is absolutely necessary to study the properties of radical extensions of field $\mathbb{C}(s_1,s_2,\ldots,s_n)$. Since this base field contains all symmetric rational functions of $x_1,x_2,\ldots,x_n$ but the field of rational expressions in roots x_i contains many asymmetric rational functions of the roots too we need to study how far the properties of symmetry can be carried off through a radical extension. Thus the problem is intimately related to the invariance of the members of a radical extension under a permutation of roots x_i.

Towards the end of 18th century, an Italian mathematician Paolo Ruffini studied the problem of solvability of general polynomial equations along the lines of considerations of invariance of expressions under permutations of its variables and published the first controversial proof of insolvability of quintic by radicals. Most of his peers did not understand his long (more than 500 pages) proof but Cauchy was able to notice the gems contained in his paper. There were some gaps in Ruffini's proof but his approach was essentially correct. Few years later Abel filled

in these gaps and provided a correct proof.

Abel's fundamental idea was that if the root of an equation could be expressed as a radical expression in the coefficients of the polynomial then each such radical expression itself must be a rational function of the roots. Thus in case of a quadratic equation $x^2+ax+b=0$ the radical expression $\sqrt{a^2-4b}$ is either x_1-x_2 or x_2-x_1. This is a significant step in Abel's and Ruffini's proof and Ruffini assumed this without any proof. Abel provided a rigorous and detailed proof of this key step and generalized some of the results obtained by Ruffini and Cauchy on the number of values taken by a function under permutation of its variables. Using these results and assuming the most general radical expression for a root of the equation he was able to arrive at a contradiction. Abel's argument to obtain the desired contradiction is however very complicated and we will follow a simplified approach by Ruffini in these posts.

In the next post we will study various properties of radical extensions which are necessary to understand the arguments put forth by both Abel and Ruffini to solve the historically famous problem of solvability of algebraic equation by radicals.

By Paramanand Singh
Saturday, December 7, 2013

Labels: Algebra