Abel and the Insolvability of the Quintic: Part 4

We now turn to the goal of this series namely to establish the fact that the general polynomial of degree 5 or higher is not solvable by radicals over its field of coefficients. Here Abel’s argument is quite terse and I have not been able to fully comprehend some parts of it. Also proof of some statements are not provided by Abel because it appeared quite obvious to him. We will provide here a proof which is based on Ruffini’s arguments and its later simplification by Wantzel.

The idea of the proof is to study the field extension $K = \mathbb{C}(x_1, x_2, \ldots, x_n)$ of $F = \mathbb{C}(s_1, s_2, \ldots, s_n)$ with regard to the symmetries under various permutations of the indeterminates $x_i$. Clearly the elements of the base field $F$ are invariant under all the possible permutations of $x_i$. But the elements of field $K$ are invariant only under the identity permutation. We need to analyze the behavior of a radical extension $R$ of $F$ which is contained in $K$ with regard to invariance under the permutations of $x_i$.

**Insolvability of the General Polynomial of Degree $n \geq 5$**

Let the general polynomial of degree $n$ be denoted by $P(x)$ with $x_1, x_2, \ldots, x_n$ as its roots so that

$$P(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$$

where $s_1, s_2, \ldots, s_n$ are the elementary symmetric functions of the roots $x_i$. The base field of the coefficients is $F = \mathbb{C}(s_1, s_2, \ldots, s_n)$ and clearly the splitting field of $P(x)$ over $F$ is $K = \mathbb{C}(x_1, x_2, \ldots, x_n)$.

We start with a very surprising and curious result regarding the behavior of radical expressions with respect to two specific permutations of the $x_i$. In order to define these two permutations it is absolutely important that we have $n \geq 5$. Such permutations don’t exist if $n < 5$.

**Theorem 12:** Let $u, a \in K = \mathbb{C}(x_1, x_2, \ldots, x_n)$ and $p$ be a prime number such that $u^p = a$. Let $n \geq 5$ and let $\sigma, \tau$ be two permutations of $x_i$’s defined as follows:

$$\sigma : x_1 \to x_2 \to x_3 \to x_1, x_i \to x_i \text{ for } i > 3$$

and

$$\tau : x_3 \to x_4 \to x_5 \to x_3, x_i \to x_i \text{ for } i = 1, 2 \text{ and } i > 5$$

If $a$ is invariant under the permutations $\sigma, \tau$ then so is $u$.

Clearly if $a = 0$ then $u = 0$ and the theorem is trivially true in this case. So let $a \neq 0$ so that $u \neq 0$. Now we have $u^p = a$ so that $\sigma(u^p) = \sigma(a) = a$ or $(\sigma(u))^p = a = u^p$. We then have $(\sigma(u)/u)^p = 1$ so that $\sigma(u)/u$ is some $p^{th}$ root of unity, say $\omega_\sigma$ and then we have $\sigma(u) = \omega_\sigma u$. 
Applying the permutation $\sigma$ to this equation we get
\[ \sigma^2(u) = \sigma(\omega_\tau u) = \omega_\sigma \sigma(u) = \omega_\sigma^2 u \]
and similarly $\sigma^3(u) = \omega_\tau^3 u$. But $\sigma^3$ is the identity permutation and hence we get $\omega_\sigma^3 u = u$ so that $\omega_\sigma^3 = 1$.

Following exactly the same reasoning we get $\tau(u) = \omega_\tau u$ where $\omega_\tau$ is some $p^{th}$ root of unity and we have $\omega_\tau^3 = 1$. Now its time to do some permutation algebra. Clearly we have
\[ \sigma \circ \tau : x_1 \rightarrow x_2 \rightarrow x_3 \rightarrow x_4 \rightarrow x_5 \rightarrow x_1, x_i = x_i \text{ for } i > 5 \]
and
\[ \sigma^2 \circ \tau : x_1 \rightarrow x_3 \rightarrow x_4 \rightarrow x_5 \rightarrow x_2 \rightarrow x_1, x_i = x_i \text{ for } i > 5 \]
Again we can see that
\[ (\sigma \circ \tau)u = \omega_\sigma \omega_\tau u, \quad (\sigma^2 \circ \tau)(u) = \omega_\sigma^2 \omega_\tau u \]
Since both $(\sigma \circ \tau)^5$ and $(\sigma^2 \circ \tau)^5$ are identity permutations it follows that
\[ (\omega_\sigma \omega_\tau)^5 = (\omega_\sigma^2 \omega_\tau)^5 = 1 \]
Also we have previously obtained
\[ \omega_\sigma^3 = \omega_\tau^3 = 1 \]
Now it is clear that
\[ \omega_\sigma = (\omega_\sigma^3)^2(\omega_\sigma \omega_\tau)^5(\omega_\tau^2 \omega_\tau)^{-5} = 1 \cdot 1 \cdot 1 = 1 \]
and
\[ \omega_\tau = (\omega_\tau^3)^2 \omega_\tau^5(\omega_\sigma \omega_\tau)^{-5} = 1 \cdot 1 \cdot 1 = 1 \]
We thus have $\sigma(u) = \omega_\sigma u = u, \tau(u) = \omega_\tau u = u$ so that $u$ is invariant under the permutations $\sigma$ and $\tau$.

We are now ready to prove the insolvability of the polynomial $P(x)$ by radicals if $n \geq 5$. We have the precise statement of the theorem as follows:

**Theorem 13:** If $n \geq 5$ then the general polynomial of degree $n$ given by
\[ P(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n \]
is not solvable by radicals over $\mathbb{Q}(s_1, s_2, \ldots, s_n)$ nor over $\mathbb{C}(s_1, s_2, \ldots, s_n)$.

By theorem 6 of [this post](https://paramanand.math/abel-the-theorem-13) it is sufficient to show that the polynomial $P(x)$ is not solvable by radicals over $F = \mathbb{C}(s_1, s_2, \ldots, s_n)$. Let us suppose on the contrary that the polynomial $P(x)$
is solvable by radicals over $F$. This means there is a radical extension $R$ of $F$ which contains a root $x_1$ of $P(x)$. By renumbering of the $x_i$’s it is possible to ascertain that $R$ contains $x_1$ in particular. Now by the theorem of natural irrationalities proved in the last post we can assume that $R$ is contained in $K = \mathbb{C}(x_1, x_2, \ldots, x_n)$. Let the height of $R$ over $F$ be $h$. Clearly $h$ cannot be zero as it would mean $R = F$ and hence every member of $R$ including the root $x_1$ would have to be invariant under all the permutations of the $x_i$’s. Hence $h > 0$. Let $F = R_0 \subseteq R_1 \subseteq R_2 \subseteq \ldots \subseteq R_h = R$ be the tower of radical extensions leading from $F$ to $R$. Here each $R_i$ is a radical extension of height 1 of $R_{i-1}$.

Consider first the radical extension $R_1$ of height 1 over $F$. Clearly we have a member $u \in R_1$ and a prime $p$ such that $R_1 = F(u)$ and $u^p = a \in F$ is not a $p^{th}$ power in $F$. Clearly the element $a \in F$ is invariant under all the permutations of the $x_i$’s and since $n \geq 5$, the element $a$ is invariant under the two permutations $\sigma$ and $\tau$ defined in theorem 12 above. It follows from theorem 12 that the element $u$ is also invariant under $\sigma, \tau$. Since every element of $F$ is also invariant under these two permutations it follows that every element of $F(u) = R_1$ is also invariant under $\sigma, \tau$.

Now considering the field $R_2$ as a radical extension of height 1 over $R_1$ and repeating the same argument we see that every element of $R_2$ is also invariant under $\sigma, \tau$. Continuing this process for each of the fields $R_i$ we finally see that every member of $R_h = R$ is invariant under $\sigma, \tau$. But we have $x_1 \in R$ which is clearly not invariant under $\sigma$ and therefore we obtain a contradiction. It follows that our initial assumption of the solvability of $P(x)$ by radicals over $F$ is wrong and thereby our proof is complete.

**Note:** The treatment of the insolvability of general polynomial of degree 5 or more in this series of posts is taken from the wonderful book *Galois Theory of Algebraic Equations* by Jean-Pierre Tignol. Readers are advised to go through this beautiful book for further development in these topics. This has been the first understandable presentation of Abel's proof I have found in literature and online articles. Most of the Modern Algebra textbooks totally ignore the contributions of Abel or just mention it as a historical note and straightaway jump onto the beautiful theories of Galois. Tignol's book discusses all the historical developments leading upto Galois Theory with the exposition of the contributions from various mathematicians like Gauss, Lagrange, Abel and finally Galois.