Abel and the Insolvability of the Quintic: Part 3

The proof for the non-solvability of polynomial equation of degree 5 (or more) by radicals obviously has to proceed via method of contradiction. Abel therefore assumed that such a solution was possible for a quintic and then figured out the most general form of such a solution. At the same time Abel observed that the radical expressions occurring in such a form must themselves be rational expressions of the roots desired. This was a key part which Abel proved for the first time. This result was later termed as the *Theorem of Natural Irrationalities*.

Abel's approach to the proof of this central result proceeds in multiple stages. Abel shows that an algebraic function of order 1 (say $v = f_1(f_0^{1/m}, a, b, c)$) can always be expressed as a linear combination of powers of the radical expression ($u = f_0^{1/m}$) used to generate this function. Also when this is done, it is possible to express the coefficients of this linear combination (as well as the radical u) as rational functions of the original algebraic function (v) and its counterparts. The same procedure can then be carried inductively to algebraic functions of any order. We will rewrite Abel's proof in the modern notation of radical extensions.

Irreducibility of the Polynomial $x^p - a$

We first need to establish the irreducibility of the polynomial $f(x) = x^p - a \in F[x]$ where p is a prime number and $a \in F$ is not a p^{th} power in field F. In order to establish this we first show that the the powers of a are also not p^{th} powers in F. More precisely we show that *if* $k = 1, 2, \ldots, p-1$ *then* a^k *is not a* p^{th} *power in* F.

Clearly on the contrary assume that $a^k = b^p$ for some $b \in F$. Now we note that k and p are coprime so there exists integers m, n such that $mk + np = 1$. And therefore

$$a = a^{mk+\,np} = (a^k)^m a^{np} = b^{mp} a^{np} = (b^m a^n)^p$$

which contradicts the fact that a is not a p^{th} power in F.

Let us now assume that $f(x) = x^p - a$ is reducible in $F[x]$. This means that we have polynomials $g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$. Also without any loss of generality we can assume that $g(x), h(x)$ are monic polynomials (i.e. the coefficients of highest power of x in them is 1). Let K be the splitting field of $f(x)$ over F. Thus $f(x)$ can be factored as a product of linear factors over K. Since the roots of $f(x)$ are p^{th} roots of a which are obtained by multiplying one such root u with the p^{th} roots of unity. It follows that K contains all the roots of the form ωu where ω is any p^{th} root of unity. Let μ_p denote the set of all p^{th} roots of unity. Then we can write

$$f(x) = \prod_{\omega \in \mu_p} (x - \omega u)$$

Clearly both the polynomials $g(x), h(x)$ also split into linear factors over K and the some linear factors of $f(x)$ make up $g(x)$ and remaining ones make up $h(x)$. Thus we can write

$$g(x) = \prod_{\omega \in I}(x - \omega u), h(x) = \prod_{\omega \in J}(x - \omega u)$$

where I, J are sets with $I \cap J = \emptyset, I \cup J = \mu_p$.

Let the constant term of $g(x)$ be denoted by b so that $b \in F$. Now from the above relation we can see that $b = (-u)^k \prod_{\omega \in I} \omega$ where k is the number of elements in I. Since $\omega^p = 1$, it follows that $\{(-1)^k b\}^p = u^{kp} = a^k$. This means that a^k is a p^{th} power in F. This is not possible if $k = 1, 2, \ldots, p-1$. Thus either $k = 0$ or $k = p$. If $k = 0$ then $I = \emptyset$ and $g(x) = 1$. If $k = p$ then $J = \emptyset$ and $h(x) = 1$. Thus we have either $g(x) = 1$ or $h(x) = 1$ and therefore the polynomial $f(x) = x^p - a$ is irreducible over F. We can formally state this as:

Theorem 7: *Let p be a prime number and let a be a member of a field F which is not a p^{th} power in F. Then the polynomial $f(x) = x^p - a$ is irreducible over F.*

Properties of Radical Extension $R = F(u)$

Next we consider a radical extension R of a field F of height 1. This means that there is a prime number p and an element $a \in F$ which is not p^{th} power in F and an element $u \in R$ such that $R = F(u)$ and $u^p = a$. Now each member of R can be expressed as a rational function of u with coefficients in F. It is easy to show that we can express members of R as polynomials in u with coefficients of F. To do this we must show that if $g(u)$ is a polynomial expression in u with coefficients in F, then $1/g(u)$ can also be expressed as a polynomial in u with coefficients in F.

Note that since $u^p = a$, powers of p in $g(u)$ which are greater than $(p-1)$ can be replaced with lower powers of p and members of F. Thus we can assume that $g(u)$ has no powers of u greater than $(p-1)$. Let $g(x) \in F[x]$ be the corresponding polynomial. Then the degree of $g(x)$ can be at most $(p-1)$. Also the polynomial $f(x) = x^p - a$ is irreducible over F. It follows that both the polynomials $f(x)$ and $g(x)$ are relatively prime to each other. Hence there exist polynomials $a(x), b(x) \in F[x]$ such that $f(x)a(x) + g(x)b(x) = 1$. Now putting $x = u$ and noting that $f(u) = 0$ we get $g(u)b(u) = 1$ so that $b(u) = 1/g(u)$. Thus we have been able to express $1/g(u)$ as a polynomial $b(u)$.

It follows now that any rational expression $h(u)/g(u) \in F(u) = R$ can be expressed as polynomial in u with coefficients in F. Note further that degree of such a polynomial can always be made less than p by using the relation $u^p = a$. We have thus shown that any member $v \in F(u) = R$ can be expressed in the form

$$v = a_0 + a_1 u + a_2 u^2 + \cdots + a_{p-1} u^{p-1}$$

where $a_0, a_1, \ldots, a_{p-1} \in F$. We will further establish that this expression of v in terms of u is unique. Clearly if we have

$$v = a_0 + a_1 u + a_2 u^2 + \cdots + a_{p-1} u^{p-1} = b_0 + b_1 u + b_2 u^2 + \cdots + b_{p-1} u^{p-1}$$

then u is the root of a polynomial $g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{p-1}x^{p-1} \in F[x]$ where $c_i = a_i - b_i$. Clearly the degree of $g(x)$ is at most $(p-1)$ and u is a root of an irreducible polynomial $f(x) = x^p - a$ of degree p. Hence we must have $g(x) = 0$ identically and therefore $c_i = 0$ for all i. Thus $a_i = b_i$ and therefore the expression of v in terms of u is unique. What we have proved so far is that:

Theorem 8: *Let R be a radical extension of a field F of height 1 so that $R = F(u)$ where $u \in R$ is such that $u^p = a \in F$ where p is a prime number and a is not a p^{th} power in F. Then every element $v \in R$ can be expressed as a linear combination*

$$v = a_0 + a_1u + a_2u^2 + \cdots + a_{p-1}u^{p-1}$$

where $a_0, a_1, \ldots, a_{p-1} \in F$ in a unique manner.

Abel goes further and states that if in the above result $v \notin F$ then we can choose a suitable $u \in R$ such that the coefficient a_1 can be made unity. This we state as a theorem next:

Theorem 9: *Let R be a radical extension of a field F of height 1. Let $v \in R$ and $v \notin F$. Then an element $u \in R$ can be chosen such that $R = F(u)$ and a prime number p can be found with $u^p \in F$ and u^p not being a p^{th} power in F such that*

$$v = a_0 + u + a_2u^2 + \cdots + a_{p-1}u^{p-1}$$

where $a_0, a_2, \ldots, a_{p-1} \in F$ and this expression for v in terms of u is unique.

Let $R = F(u')$ where $u' \in R$ is such that $u'^p = a' \in F$ and a' is not a p^{th} power in F. Also we have a unique expression for v in terms of u' as

$$v = a'_0 + a'_1u' + \cdots + a'_{p-1}u'^{p-1}$$

where $a'_i \in F$. Since $v \notin F$ it follows that one of the coefficients $a'_1, a'_2, \ldots, a'_{p-1}$ must be non-zero. Let the first such non-zero coefficient be a'_k.

Let $u = a'_ku'^k$ so that $u^p = a'^p_ka'^k$. Since $k \in \{1, 2, \ldots, p-1\}$ it follows that a'^k is not a p^{th} power in F and hence u^p is also not a p^{th} power in F. Now it is clear that $F(u) \subseteq R$ and thus we need to prove that $R \subseteq F(u)$. This can be achieved if we show that every member of R can be expressed as a rational function of u. We will show that in fact we can express every member of R as a polynomial in u with coefficients in F. Note that every element of R can be expressed as a polynomial in u' so it makes sense to first express powers of u' in terms of u.

If $i \in \{1, 2, \ldots, p-1\}$ then $u^i = a'^i_ku'^{ik}$. As i varies from $1, 2, \ldots, p-1$, so does $ik \pmod p$ (but in a different order) and hence we can write $ik = pm + j$ where m is an integer and $j \in \{1, 2, \ldots, p-1\}$. Thus $u^i = a'^i_ka'^mu'^j$. Since the correspondence between i and j is one to one, it follows that we can express every power of u' as $u'^j = \{a'^i_ka'^m\}^{-1}u^i$ i.e. as a multiple of a power of u. It thus follows that every member of R can be expressed as a polynomial in u with coefficients in F. By the irreducibility of $(x^p - u^p)$ over F it follows that

such an expression in unique. Also note that by the way we have chosen u the coefficient of u in this expression for v is 1 and hence we can write

$$v = a_0 + u + a_2u^2 + \cdots + a_{p-1}u^{p-1}$$

in a unique fashion.

Next Abel uses a very ingenious argument and shows the dependence of the coefficients a_0, a_2, a_{p-1} on v in a very direct manner by expressing them as rational functions of v and its counterparts (or "conjugates"). In fact the radical u also gets expressed in the same manner in terms of v. This we state below:

Theorem 10: *Let R be a radical extension of F with $u \in R$ and a prime p such that $u^p = a \in F$ is not a p^{th} power in F and $R = F(u)$. Also assume that F contains a primitive p^{th} root of unity ζ. Let $v \in R - F$ be a root of a polynomial $f(x) \in F[x]$ and let*

$$v = a_0 + u + a_2u^2 + \cdots + a_{p-1}u^{p-1}$$

be the unique expression of v in terms of u. Then R contains p roots of $f(x)$ and $u, a_0, a_2, \ldots, a_{p-1}$ are rational expressions of these p roots of $f(x)$ with coefficients in $\mathbb{Q}(\zeta)$.

Let $g(y) = f(a_0 + y + a_2y^2 + \cdots + a_{p-1}y^{p-1}) \in F[y]$ be a polynomial. Then the fact that $f(v) = 0$ implies that $g(u) = 0$ so that u is a root of $g(x)$. At the same time u is also a root of $h(x) = x^p - a$. Since $h(x)$ is irreducible it follows that $h(x)$ divides $g(x)$ and hence every root of $h(x)$ is a root of $g(x)$. Now the roots of $h(x)$ are of the form ζ^iu where $i = 0, 1, 2, \ldots, p-1$, it follows that $g(\zeta^iu) = 0$. Let

$$v_i = a_0 + a_1\zeta^iu + a_2\zeta^{2i}u^2 + \cdots + a_{p-1}\zeta^{(p-1)i}u^{p-1}$$

with $a_1 = 1$ so that $v = v_0$ and each v_i is a root of $f(x)$. Since each $v_i \in R$ it follows that R contains p roots of $f(x)$. Now we can see that

$$\sum_{i=0}^{p-1}\zeta^{-ik}v_i = \sum_{j=0}^{p-1}\left(\sum_{i=0}^{p-1}\zeta^{(j-k)i}\right)a_ju^j$$

Clearly if $j \neq k$ then ζ^{j-k} is a primitive p^{th} root of unity and hence the sum with index i on the right side above vanishes. If $j = k$ then the same sum evaluates to p. It follows that

$$\sum_{i=0}^{p-1}\zeta^{-ik}v_i = pa_ku^k$$

for all $k = 0, 1, 2, \ldots, p-1$. Putting $k = 1$ and noting that $a_1 = 1$ we see that u is expressed as a rational function of the roots v_i with coefficients in $\mathbb{Q}(\zeta)$ and then

$$a_k = \frac{\displaystyle\sum_{i=0}^{p-1}\zeta^{-ik}v_i}{pu^k}$$

which shows that a_k is also expressed as a rational function of the roots v_i with coefficients in $\mathbb{Q}(\zeta)$.

Also note the usefulness of the fact that $a_1 = 1$ in the above derivation. Without this it would not have been possible to express u in terms of v_i. Therefore the theorem 9 is significant which allows us to make the coefficient $a_1 = 1$.

We are now ready to prove the famous result of Abel namely:

Theorem of Natural Irrationalities

Let $F = \mathbb{C}(s_1, s_2, \ldots, s_n)$ and $K = \mathbb{C}(x_1, x_2, \ldots, x_n)$ where x_i are n indeterminates and the s_i are their elementary symmetric functions. Thus K represents the field of rational functions in n indeterminates with complex coefficients and F represents the field of *symmetric* rational functions of the same n indeterminates with complex coefficients. Clearly $F \subseteq K$. With this notation we have the following theorem:

Theorem 11: *If an element $v \in K$ lies in a radical extension of F, then K contains a radical extension of F which contains v.*

The theorem says that if we wish to express any of x_i in a radical extension of the base field F then all the intermediate fields in this tower of radical extensions are also contained in K. Note that the theorem crucially depends on the fact that the base field contains root of unity. The theorem is false if we replace field $\mathbb{C}$ with $\mathbb{Q}$. The term "natural irrationalities" refers to the fact that the irrationalities (i.e. radicals) used in expressing v can be assumed to lie in K rather than some external field.

We will use induction on the height h of the radical extension R of F which contains $v \in K$. If $h = 0$ then $R = F$ and then there is nothing to prove. So let $h > 0$. Also let us assume as the induction hypothesis that any element of K which is contained in a radical extension of F height less than h then it is contained in a radical extension of F which lies in K.

Let $v \in K$ be contained in a radical extension R of F of height h. Then we have a radical extension R_1 of F of height $(h-1)$ and R is a radical extension of height 1 of R_1. If $v \in R_1$ then the proof is done by induction hypothesis. So let $v \in R - R_1$. We have an element $u \in R$ and a prime p such that $R = R_1(u)$ and $u^p \in R_1$ with u^p not being a p^{th} power in R_1. Then by theorem 9 we can express v as

$$v = a_0 + u + a_2 u^2 + \cdots + a_{p-1} u^{p-1}$$

where $a_0, a_2, \ldots, a_{p-1} \in R_1$.

Since $v \in K$ it follows that v is a root of a polynomial with coefficients in F and hence in R_1 (clearly v and its images under various permutations of x_i will be the roots of this polynomial). Now by theorem 10, we can deduce that $u, a_0, a_2, \ldots, a_{p-1}$ are rational functions of these

roots and hence lie in K. At the same time u^p and the coefficients a_i lie in R_1 which is a radical extension of F of height $(h-1)$. Therefore by induction hypothesis each of $u^p, a_0, a_2, \ldots, a_{p-1}$ lies in a radical extension of F contained in K. By theorem 3 of the last post there is a single radical extension of F, say R', which contains all these elements and is itself contained in K. Since $u^p \in R'$ therefore $R'(u)$ is radical extension of R' and hence a radical extension of F. Since $u \in K$ therefore $R'(u) \subseteq K$ and thus we have a radical extension of F which contains v and is contained in K.

Using this theorem we will prove in the next post that the general polynomial of degree 5 or higher is not solvable by radicals over the field of its coefficients.

By Paramanand Singh
Friday, January 3, 2014

Labels: Algebra