Abel and the Insolvability of the Quintic: Part 2

In the last post we defined the concept of a radical field extension along the lines of the definition of algebraic functions given by Abel. In the current post we will study some properties of such field extensions which will ultimately enable us to study the field extension $\mathbb{C}(x_1, x_2, \ldots, x_n)$ of $\mathbb{C}(s_1, s_2, \ldots, s_n)$ where $s_1, s_2, \ldots, s_n$ are elementary symmetric functions of the indeterminates $x_1, x_2, \ldots, x_n$.

While discussing properties of radical extensions it will be found that at certain times it is useful to let the base field contain all the roots of unity. Abel and his contemporaries always assumed the existence of roots of unity as a given while dealing with solution of algebraic equations.

Properties of Radical Extensions

We first show that in the definition of a radical extension R of F with $R = F(u)$ where $u \in R$ with $u^p \in F$ we may drop the requirement that p be a prime. This is possible if we assume that the base field F contains roots of unity.

Theorem 1: *Let $R \supseteq F$ be a field extension such that $R = F(u)$ where $u \in R$ is such that $u^n \in F$ for some positive integer n. If F contains a primitive n^{th} root of unity then R is a radical extension of F.*

We proceed by induction. Starting with $n = 1$ we see that $u \in F$ so that $R = F$ and clearly R is then a radical extension of height 0 of F. So let's suppose that $n > 1$ and that the result holds for all exponents of u upto $n - 1$.

Let us first suppose that $n = rs$ where r, s are positive integers greater than 1 and less than n. Since we have $u^n = u^{rs} = (u^r)^s$, it follows by the induction hypothesis that $R = F(u)$ is a radical extension of $F(u^r)$ and $F(u^r)$ is a radical extension of F. Hence it follows that R is a radical extension of F.

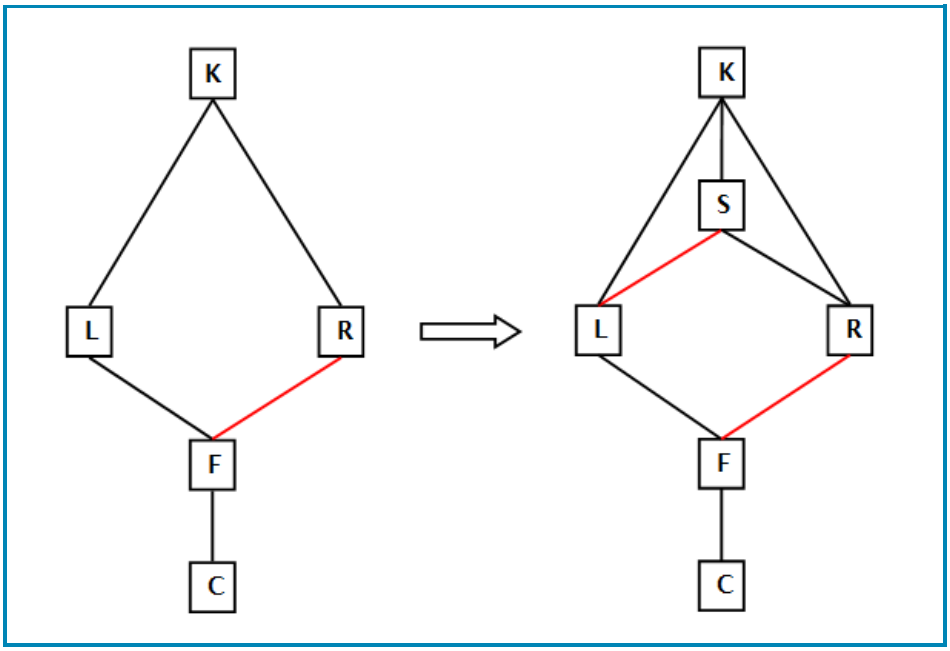
If n is prime then we need to consider two cases: either u^n is an n^{th} power in F or it is not an n^{th} power in F. In the latter case we are done by the definition of a radical extension. So we only need to consider the case that $u^n = a^n$ for some $a \in F$. In this case we may assume that $a \neq 0$ otherwise $u = 0$ and $R = F$ so that R is a radical extension of height 0 of F. Now we have $(u/a)^n = 1$ so that u/a is an n^{th} root of unity. Since F contains a primitive n^{th} root of unity, it contain all the n^{th} roots of unity. Hence $u/a \in F$ so that $u \in F$ and therefore $R = F$ so that R is a radical extension of height 0 of F.

Next we see how we can generate radical extensions based on some given radical extension R of F. The following result discusses the scenario where we have towers of field extensions $F \subseteq R \subseteq K$ and $F \subseteq L \subseteq K$. If R is a radical extension of F then based on it we can create

a radical extension S of L which also includes R.

Theorem 2: *Let fields F, R, L, K be such that $F \subseteq R \subseteq K$ and $F \subseteq L \subseteq K$. Also let us assume that $\mathbb{C} \subseteq F$. If R is a radical extension of F then there is a radical extension S of L which is contained in K and contains R.*

The above theorem can be graphically represented as below:



Here the lines represent containment / field extension with the convention that a field at the top contains the field below. Red lines indicate radical extensions.

The idea of the proof is that we adjoin the radicals u which are used in creation of R from F to the field L to create a radical extension S. This will naturally contain R and be contained in K because all such radicals are part of K. We carry this idea in a formal fashion in the proof that follows.

We use induction on the height of radical extension R of F. Let h be this height. If $h = 0$, then $R = F$ and we can take $S = L$ which contains $R = F$ and is contained in K and clearly S is a radical extension of L of height 0. So we have verified the theorem in case $h = 0$. Now we assume that the result holds for all radical extensions R of F with height less than h.

Since R is a radical extension of F of height h, it follows that 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. This means that we have a member $u \in R$ such that $R = R_1(u)$ and $u^p \in R_1$ where p is a certain prime and u^p is not a p^{th} power in R_1.

Clearly by the induction hypothesis we have a radical extension S_1 of L which contains R_1 and is contained in K. Now $u^p \in S_1$ and since S_1 contains $\mathbb{C}$ and thus all the roots of unity we can use Theorem 1 above to deduce that $S = S_1(u)$ is a radical extension of S_1 and hence of L.

Clearly since $u \in R \subseteq K$ and $S_1 \subseteq K$ therefore $S = S_1(u) \subseteq K$. Also $R_1 \subseteq S_1 \subseteq S$ and $u \in S$ so that $R = R_1(u) \subseteq S$. Thus we have found a radical extension S of L which contains R and is contained in K.

The above result is so useful in combining multiple radical extensions to create one radical extension. We have the following result in this connection:

Theorem 3: *Let $\mathbb{C} \subseteq F \subseteq K$ be a field extension and let each of the elements $v_1, v_2, \ldots, v_n$ in K lie in a radical extension of F contained in K. Then there is a single radical extension of F contained in K which contains all the elements $v_1, v_2, \ldots, v_n$.*

Clearly if $n = 1$ the result holds. So let us suppose that there is a single radical extension L of F which contains all the elements $v_1, v_2, \ldots, v_{n-1}$. Also let R be the radical extension of F which contains v_n. Using Theorem 2 we can see that there is a radical extension S of L which contains R and thus we see that S is a radical extension of F which contains all the elements $v_1, v_2, \ldots, v_n$.

Roots of Unity and Radicals

Note that the above results are dependent on the fact that the base field F contains roots of unity. However if this is not the case then we have a remarkable result which shows that all the roots of unity can be obtained via radical extensions. This was established by Gauss using his theory of periods. We establish this result along the lines of Gauss using induction.

Theorem 4: *If n is a positive integer and F is a field then the n^{th} roots of unity lie in a radical extension of F.*

We need to establish this only for the primitive n^{th} roots of unity as the other roots are their powers. For $n = 1$ the result is trivial and hence let $n > 1$. Let us assume that all k^{th} roots of unity lie in a radical extension of F for all $k = 1, 2, \ldots, n - 1$.

Clearly if n is composite, say $n = rs$ with r, s being positive integers greater than 1 and less than n and ζ is a primitive n^{th} root of unity then ζ^r is an s^{th} root of unity and hence by induction hypothesis lies in a radical extension R_1 of F. Again by the induction hypothesis we can find a radical extension of R_2 of R_1 which contains all r^{th} roots of unity. Now $\zeta^r \in R_1 \subseteq R_2$ and R_2 contains all r^{th} roots of unity therefore by theorem 1, $R_2(\zeta)$ is a radical extension of R_2 and hence of F which contains the primitive n^{th} root ζ.

If n is prime then the argument is a bit tricky but Gauss uses the technique of Lagrange resolvents. As usual let g be a primitive root of n and let ζ be a primitive n^{th} root of unity. We set $\zeta_i = \zeta^{g^i}$. Then $\zeta_0, \zeta_1, \zeta_2, \ldots, \zeta_{n-2}$ are the $(n-1)$ primitive n^{th} roots of unity. Let ω be an $(n-1)^{\text{th}}$ root of unity other than 1 and we form the Lagrange resolvent

$$t(\omega) = \zeta_0 + \omega\zeta_1 + \omega^2\zeta_2 + \cdots + \omega^{n-2}\zeta_{n-2}$$

and then we can see that the cyclic permutation of $\zeta_0, \zeta_1, \ldots, \zeta_{n-2}, \zeta_0$ in that order changes the expression $t(\omega)$ into $\omega^{-1}t(\omega)$. It follows that the expression $\{t(\omega)\}^{n-1}$ remains invariant by the application of this permutation.

Now note that if we calculate the expression $\{t(\omega)\}^{n-1}$ it will involve multiplying the various ζ's and since these are primitive n^{th} roots of unity thier products will also be expressed as an n^{th} root of unity. It follows that the expression $\{t(\omega)\}^{n-1}$ can be expressed in the form of a linear combination of the ζ's where the coefficients will be certain polynomials in ω. Thus we have

$$\{t(\omega)\}^{n-1} = a_0\zeta_0 + a_1\zeta_1 + \cdots + a_{n-2}\zeta_{n-2}$$

where a_i are polynomials in ω. Now we apply the cyclic permutation of the ζ's to the above expression and note that doing so does not change the LHS. Thus we get

$$\begin{aligned}\{t(\omega)\}^{n-1} &= a_0\zeta_0 + a_1\zeta_1 + \cdots + a_{n-2}\zeta_{n-2}\\ &= a_0\zeta_1 + a_1\zeta_2 + \cdots + a_{n-2}\zeta_0\\ &= a_0\zeta_2 + a_1\zeta_3 + \cdots + a_{n-2}\zeta_1\\ &= \cdots\\ &= a_0\zeta_{n-2} + a_1\zeta_0 + \cdots + a_{n-2}\zeta_{n-3}\end{aligned}$$

Adding these equations we get

$$(n-1)\{t(\omega)\}^{n-1} = \left(\sum_{i=0}^{n-2} a_i\right)\left(\sum_{i=0}^{n-2}\zeta_i\right)$$

and since the ζ's sum to -1 it follows that expression $\{t(\omega)\}^{n-1}$ is a polynomial in ω. By induction hypothesis the $(n-1)^{\text{th}}$ root ω lies in a radical extension R_1 of F and hence the expression $\{t(\omega)\}^{n-1}$ also lies in R_1. It follows by theorem 1 that $R_1(t(\omega))$ is a radical extension of R_1 and hence of F. Considering all the $(n-1)^{\text{th}}$ roots of unity it is clear that we can find a radical extension R_2 of F which contains all such expression $t(\omega)$. It can now be easily checked that

$$\zeta_i = \frac{1}{n-1}\sum_{\omega}\omega^{-i}t(\omega)$$

and therefore $\zeta_i \in R_2$. Thus we see that the primitive n^{th} root ζ lies in a radical extension of F. This completes the proof.

We next want to prove an important result regarding solvability of polynomials over a field. If $P(x)$ is a polynomial over field F and $L \supseteq F$ is a field extension then $P(x)$ can also be regarded as a polynomial over field L. We will establish that if $P(x)$ is solvable by radicals over F then it is also solvable by radicals over L. This also shows that if $P(x)$ is not solvable by radicals over L then it is not solvable by radicals over F. Thus in case we are trying to establish non-solvability by radicals of some polynomial then it does not harm to extend the field of coefficients. Thus it makes sense to always enlarge the field of coefficients to include roots of unity and thereby all the complex numbers. By doing this we achieve a lot of simplicity (via the use of theorems 1, 2, 3 above) in our proofs without losing any generality. We first

prove a preliminary result.

Theorem 5: *Let $F \subseteq L$ be a field extension. If R is a radical extension of F then there is a radical extension S of L such that R can be identified with a subfield of S.*

This result should be contrasted with theorem 2 as it does away with the requirement that base field F should contain $\mathbb{C}$.

Again as usual the proof will be by induction on the height h of R over F. If $h = 0$ then $R = F$ and we can take $S = L$ which contains $R = F$. If $h = 1$ so that $R = F(u)$ with $u^p = a \in F$ not being a p^{th} power in F. Now consider the polynomial $P(x) = x^p - a$. It is a polynomial over F as well as over L. Hence there is a splitting field $K \supseteq L$ which contains all the roots of $P(x)$. Since u is a root of this polynomial we can identify this u with some member of K. Since $K \supseteq L \supseteq F$ it follows that K contains all the rational expressions in u with coefficients in F. In this sense $K \supseteq R = F(u)$.

If a is not a p^{th} power in L, then $L(u)$ is a radical extension of L of height 1 and clearly it contains both F and u and therefore $R = F(u)$. We thus have a radical extension of L which contains R.

If a is a p^{th} power in L say $a = b^p$ with $b \in L$ then we have $u^p = b^p$ so that $(u/b)^p = 1$ so that u/b is a p^{th} root of unity. Clearly via theorem 4 there is a radical extension S of L which contains u/b and hence contains u. Clearly then S contains F and u and therefore $R = F(u)$. This completes the proof when R is a radical extension of height $h = 1$ of F.

If $h > 1$, 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. By induction hypothesis we may assume that there is a radical extension S_1 of L which contains R_1. Now we have scenario that $R_1 \subseteq S_1$ and R is a radical extension of R_1 of height 1. Clearly from the proof for height $h = 1$ we can see that there is a radical extension S of S_1 and hence of L which contains R.

We now come to the final result of this post which shows that solvability by radicals of a polynomial is not affected by extending the field of coefficients.

Theorem 6: *Let $P(x)$ be a polynomial over field F. If $P(x)$ is solvable by radicals over F then it is also solvable by radicals over any field extension $L \supseteq F$.*

Let R be a radical extension of F containing a root r of $P(x)$. Clearly by theorem 5, the field R can be assumed to be contained in some radical extension S of L and hence $r \in S$. It thus follows that the radical extension S of L contains a root r of $P(x)$ and hence $P(x)$ is solvable by radicals over L.

We have covered the groundwork regarding radical extensions and these results will be used in

the next post to establish the fundamental theorem of *natural irrationalities* which was first proved by Abel.

By Paramanand Singh
Thursday, January 2, 2014

Labels: Algebra
