IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728. Volume 5, Issue 1 (Jan. - Feb. 2013), PP 29-30
www.iosrjournals.org

Solvability of Polynomials and Galois Group

[1]YahayaShagaiya Daniel, [2]Bako Sunday Samuel, [3]Isaac KatukaJatau
[1,2,3]Department of Mathematical Science, Kaduna State University, Nigeria

Abstract: *Solution of polynomial plays fundamental role in the solution of characteristics differential equation to many physical problems. It has been found that Galois Theory can be used to determine the solvability of polynomials over a field by radicals. That is ''if a polynomial is solvable by radicals, then the automorphism group of its splitting field must be a solvable group.'' Field theory is connected with Group theory.*

Keywords: *solvable group, field, polynomial, radicals.*

I. Introduction

We first need some definitions about field extensions. A field F is an extension field of a field K. Provided that $K \subseteq F$, the operations of K are those of F restricted to $K.F$will be an extension of a field K and E an intermediate field. A field F is said to be a finite dimensional extension of a field K provide$[F:K]$ is finite. Similarly, F is said to be an infinite dimensional extension of K if $[F:K]$ is infinite see Fraleigh [1].

Let $u \in F$ then u is said to be algebraic over K provided that u is a root of some non zeropolynomial$f \in K[x]$. The element u is said to be transcendental over K if u is not a root of any non zero$f \in K[x]$.Furthermore, we say that F is an algebraic extension of K provided every element of F is algebraic over K; on the other hand, F is a transcendental extension provided there exists at least one element of F is a transcendental over K see J.S Milne[3].

For an algebraic element $u \in K[x]$ of degree $n \geq 1$ is called the irreducible or minimal polynomial of u provided f meet the conditions.

1. $f(u) = 0$
2. $g(u) = 0$if and only if f divides g where $g(x) \in K[x]$.

Suppose that K is a finite normal extension of the field F, which is of characteristics zero. There is a one-to-one order reversing correspondence between fields E with $F \subseteq E \subseteq K$ and the subgroups $H$of $Gal(\frac{K}{F})$. We can describe this correspondence by two maps that are inverses of one another: namely, we have

$$E \mapsto Gal(\frac{K}{E})$$

And

$$H \mapsto Fix(H)$$

Now, an intermediate field E is a normal extension of F if and only if the Galois group $Gal(\frac{K}{E})$is a normal subgroup of$Gal(\frac{K}{F})$. Furthermore, see Hungerford [2] the Galois group $Gal(\frac{K}{F})$ is isomorphic to

$$Gal(\frac{K}{F}) \Big/ Gal(\frac{K}{E})$$

We now have the theory in place to prove that the general fifth degree polynomial equation cannot be solved by radicals. A radical extension of a field F is a simple algebraic extension $F(\beta)$where $\beta^2 \epsilon F$, for some integer $n \geq 2$. A sequence of radical extensions: see Surjeet Singh, QaziZameeruddin [4]

$$F = F_0 \subset F_1 = F_0(\beta_1) \subset F_2 = F_1(\beta_2) \ldots F_N = F_{N-1}(\beta_N)$$

Where at each stage $\beta_i^{n_i} \in F_{i-1}$ is called a root tower over F and the last field F_N is an extension of F by radicals. If $f \in F[x]$ has a splitting field contained in an extension of F by radicals, we say that f is solvable by radicals.

Definition

A polynomial $f(x)$ in $F[x]$ is solvable by radicals over F if all its roots are in $F(\alpha_1, \alpha_2, \ldots \alpha_n)$, where for each i, $\alpha_i^{K_i}$ is in $F(\alpha_1, \alpha_2, \ldots \alpha_{i-1})$, for some positive integerK_i. See Fraleigh[1]

Definition

Let K be a field, let$f(x) \in K[x]$, and let F be a splitting field for $f(x)$over K. Then $Gal\left(\frac{F}{K}\right)$ is called the Galois group of $f(x)$over K, or the Galois group of the equation $f(x) = 0$ over K.

Theorem
Let $f(x)$ be a polynomial over a field K of characteristic zero. The equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of $f(x)$ over K is solvable.

Proposition
If H is a subgroup of $sym(p)$ containing both a transposition and the $p - cycle$then $H = sym(p)$. Here P denotes a prime.

Proof
Assume that the transposition is (12). The notation of the $p - cycle$ can be cycled so that it read $(1ab \ldots)$; taking an appropriate power, we can assume the $p - cycle$ is $(q2cd \ldots)$, and we may as well reliable the last elements in order.

First $(12)(123 \ldots p) = (23 \ldots p)$ is in H. Then $(23 \ldots p)(12)(23 \ldots p)^{-1} = (13)$ is in H, as are $(23 \ldots p)^{k}(12)(23 \ldots p)^{-k} = (1, k+1)$. Hence $(12)(13), \ldots, (1k), \ldots (1p)$ are all in H. Then $(1k)(1j)(1k) = (kj)$ is in H for all $k$and j. Any cycle $(abc \ldots l) = (al) \ldots (ac)(ab)$ is now also is a product of disjoint cycles, and all the cycles are in H, we have $sym(p) = H$.

Theorem
The general equation of degree 5 or higher is not solvable by radicals. This is true, in particular, over the field Q.

Example 1
Any Abelian group G is solvable. Now $G > e$ is a normal series of G and its only factor group is $\frac{G}{e}$, which being isomorphic to G is commutative. See J.S Milne[3]

Example 2
Consider the series $S_3 > A_3 > 1$ its factor groups are $\frac{S_3}{A_3}$ and A_3 which are of orders 2 and 3 respectively. Since any group of prime order is commutative, it follows that both the factor groups are commutative. Hence S_3 is solvable. See (Surjeet Singh, QaziZameeruddin[4])

Example 3
Consider $S_4 > A_4 > V_4 > 1$,
a subnormal series of S_4, where $V_4 = \{I, (12)(34), (13)(24), (14)(23)\}$. Its factor groups are $\frac{S_4}{A_4}$, $\frac{A_4}{V_4}$, and V_4 which are of order 2, 3 and 4 respectively.

Example 4
The group S_5 is not solvable, for since A_5 is simple, the series $1 < A_5 < S_5$ is a composition series, and $\frac{A_5}{1}$, which is isomorphic to A_5, is not abelian.

II. Conclusion

The fact in (examples above) is closely connected with the fact that a polynomial equation of degree 5 see (Surjeet, Singh, QaziZameeruddin [4]) is not in general solvable by radicals, but a polynomial equation of degree ≤ 4 is. See Hungerford [2]

We can see Group theory is connected with field theory using this ideal of Galois Theory. The general fifth degree polynomial equation in one indeterminate is not solvable by radicals over the field of rational numbers and polynomial equations of degree≤ 4 are solvable by radicals.

References

[1] Fraleigh, John 2003: *A first Course in Abstract Algebrs*, Addison Wesely Publishing Co. Inc. United States of America.

[2] Hungerfor, W. Thomas, 1990 *Abstract Algebra, An Introduction*saunders college Publishing, clevelard state University.

[3] J.S Milne,2011 *Fields and Galois Theory*, New Zealand

[4] 4.Surjeet Singh, QaziZameeruddin*ModernAlgebra*Vikas Publishing House PVT LTD New Delhi