Insolvability of Quintic

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

Abstract

The aim of this article is to give a quick but complete proof of Abel's theorem on insolvability of quintic polynomials along a geodesic path. As prerequisites, we assume that the reader is familiar with the notion of quotient rings and first homomorphism theorem. We refer the reader to my article "How to work with quotient rings?" for confidence building.

Definition 1. A field L is said to be an extension field of the field F if there exists an injective homomorphism from F to L. We denote this by L/F. (Note that the notation L/F does **not** denote the 'quotient set'.)

Note that any field F is an extension field of itself. If L is an extension field of F we can view F as a subfield of L.

Ex. 2. Suppose $\sigma : F \to L$ is a non-zero field homomorphism then σ is injective.

If L is an extension field of F then L can be viewed as a vector space over F. We denote the dimension of L over F by $[L : F]$. When this is finite, it is called the degree of the extension L/F.

Definition 3. A field extension L/F is said to be a finite extension if the degree $[L : F] < \infty$.

Example 4. (i) F/F (ii) $\mathbb{C}/\mathbb{R}$

Theorem 5 (Tower Law)**.** *Let $F \subset E \subset L$ be fields. Then $[L : F] = [L : E][E : F]$.*

Proof. If $\{x_i\}_{i\in I}$ is a basis for E/F and $\{y_j\}_{j\in J}$ is a basis for L/E then $\{x_i y_j\}_{(i,j)\in I\times J}$ is a basis for L/F. □

Definition 6. Consider a field extension L/F. Let $S \subset L$. A smallest subring (subfield) which contains S and F is said to be the subring (subfield) generated by S over F and is denoted by $F[S]$ (respectively $F(S)$). If S is finite set, say $S = \{\alpha_1, \ldots, \alpha_k\}$ then $F[S]$ (respectively $F(S)$) is denoted by $F[\alpha_1, \ldots, \alpha_k]$ (respectively $F(\alpha_1, \ldots, \alpha_k)$).

Ex. 7. The field of quotients of $F[S] = F(S)$.

Definition 8. A field extension L/F is said to be finitely generated (over F) if there exists a finite subset S of L such that L is generated by S over F. If $S = \{\alpha_1, \ldots, \alpha_k\}$ then we have $L = F(\alpha_1, \ldots, \alpha_k)$.

Ex. 9. Every finite extension is finitely generated.

Definition 10. Consider a field extension L/F. An element α in L is said to be algebraic over F if there exists a non zero polynomial $p(x) \in F[x]$ for which α is a root. If α is not algebraic over F then we say α is *transcendental* over F.

Question is whether $[F(\alpha : F] < \infty$ or not. If it is finite, say, n, there exists a nontrivial linear combination $\sum_0^n c_j \alpha^j = 0$. This motivates the definition of algebraic elements. I suggest that this be rewritten.

If $L = \mathbb{C}$ and $F = \mathbb{Q}$ then α in C is called an algebraic number or a transcendental number accordingly if α is algebraic or transcendental over $\mathbb{Q}$.

Ex. 11. If the extension L/F is finite, then any element of L is algebraic over F.

Hint: Let $[L : F] = n$. Let α be a element in L. Consider the set of $n + 1$ elements $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ which is linearly dependent.

Theorem 12. *Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F form a subfield K of L.*

Proof. Suppose α and β are algebraic over F. Then $\alpha \pm \beta$, $\alpha\beta$, α/β(for $\beta \neq 0$), are all algebraic. All of these elements lie in the extension $F(\alpha, \beta)$, which is finite over F by the tower law, hence they are algebraic.[1] □

Let L/F be an extension. Consider the evaluation map $\nu_\alpha : F[x] \to L$ defined by $\nu_\alpha(p(x)) = p(\alpha)$. Then ν_α is a ring homomorphism and also a vector space homomorphism.

Suppose α is algebraic over F. Then $\ker(\nu_\alpha) \neq 0$. Also, $\ker\nu_\alpha$ is an ideal in $F[x]$. Then there exists a *unique monic irreducible polynomial* (Justify the words in italics.) $p(x)$ such that $\ker \nu_\alpha = \langle p(x) \rangle$. This polynomial $p(x)$ is called the minimal polynomial of α over F and is denoted by $\min(\alpha, F)$. By fundamental homomorphism theorem $F[x]/\langle \min(\alpha, F) \rangle \simeq \text{Image}(\nu_\alpha) = F[\alpha]$. Therefore $F[\alpha] = F(\alpha)$. We have proved the following:

Theorem 13. *Let $\alpha \in L$ be algebraic over F. Then there is a unique monic irreducible polynomial $min(\alpha, F)$ in $F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $min(\alpha, F)$ divides $f(x)$ in $F[x]$. Also $F[x]/\langle min(\alpha, F) \rangle \simeq F(\alpha)$.*

Suppose α is transcendental over F. Then $\ker(\nu_\alpha) = 0$. Therefore $F[x] \simeq F[\alpha]$.

Ex. 14. Let L/F be an extension. If α is algebraic over F then prove that $F(\alpha)/F$ is a finite extension and $[F(\alpha) : F] = \deg(\min(\alpha, F))$. Also, if α is transcendental over F then prove that $F(\alpha)/F$ is not a finite extension. (Hint: If α is algebraic over F then $\{1+I, x+I, \ldots, x^{n-1}+I\}$ is a basis for $F[x]/I$ where $I = \langle \min(\alpha, F) \rangle$ and n is degree of the minimal polynomial.)

[1] Some more explanation will be needed for a beginner.

Theorem 15 (Kronecker)**.** *Let F be a field and $f(x)$ a polynomial in $F[x]$. Then there exists a field extension L of F such that $f(x)$ has a root in L.*

Proof. We may assume that $f(x)$ is an irreducible polynomial over F. The field $L = F[x]/\langle f(x)\rangle$ is an extension of F (why?) and the element $x+ < f(x) >$ a root of $f(x)$ in L.[2] □

Example 16. Consider the polynomial x^2+1 over $\mathbb{R}$. Then it has a root in $\mathbb{R}[x]/\left\langle x^2+1\right\rangle \simeq \mathbb{C}$.

Ex. 17. Let $f(x)$ be a polynomial in $F[x]$. Then show that there exists a field extension which contains all the roots of $f(x)$ over F.

Ex. 18. Let $p_1(x), p_2(x), \ldots, p_k(x)$ be the polynomials in $F[x]$. Then show that there exists a field extension of F which contains all the roots of these polynomials.

Definition 19. Let E/F be a field extension. A polynomial $f(x) \in F[x]$ is said to split in $E[x]$ if $f(x)$ can be written as a product of linear factors in $E[x]$.

Definition 20 (Splitting field of a polynomial $f(x)$ over F)**.** Let $f(x) \in F[x]$. An extension E/F is said to be *a* splitting field of $f(x)$ over F if (i) $f(x)$ splits in $E[x]$, (ii) E is the minimal[3] field such that $f(x)$ splits in $E[x]$.

Theorem 21. *Let $f(x) \in F[x]$. Then there exists a splitting field of $f(x)$ over F. Also it is a finite extension of F.* □

Ex. 22. Find a splitting field of (i) x^2+1 over $\mathbb{Q}, \mathbb{R}$ and (ii) x^2-2 over $\mathbb{Q}, \mathbb{R}$.

Theorem 23. *Let $\theta : F \to F'$ be an isomorphism of fields. Then we can extend θ to an isomorphism $\overline{\theta} : F[x] \to F'[x]$. For, if $f(x) = a_0 + a_1x + \ldots + a_nx^n$ define, $\overline{\theta}(f(x)) = \theta(f)(x)$, where $\theta(f)(x) = \theta(a_0) + \theta(a_1)x + \ldots + \theta(a_n)x^n$.*

$$\begin{array}{ccc} F[x] & \xrightarrow{\overline{\theta}} & F'[x] \\ \big/ & & \big/ \\ F & \xrightarrow{\theta} & F' \end{array}$$

Let $p(x) \in F[x]$ be irreducible, and let $\theta(p)(x) \in F'[x]$. Let α and β be roots of $p(x)$ and $\theta(p)(x)$ respectively, then there is a unique isomorphism $\theta_1 : F(\alpha) \to F'(\beta)$ extending θ with $\theta_1(\alpha) = \beta$.

Proof. $\overline{\theta}$ is an ring isomorphism(It is routine verification). Now, $\phi : F[x]/\langle p(x)\rangle \to F'[x]/\langle \theta(p)(x)\rangle$ defined by $\phi(g + \langle p\rangle) = \overline{\theta}(g) + \langle \theta(p)\rangle$ is an isomorphism (verify!). Note that $\theta(p)(x)$ is also an irreducible polynomial over F'. Since α and β be roots of $p(x)$ and $\theta(p)(x)$ respectively, then we have $F(\alpha) \simeq F[x]/\langle p(x)\rangle \simeq F'[x]/\langle \theta(p)(x)\rangle \simeq F'(\beta)$. That is there exists a unique(?) isomorphism θ_1 from $F(\alpha)$ to $F'(\beta)$ extending θ with $\theta_1(\alpha) = \beta$. □

[2] Write down a detailed proof. Explicitly mention where $p(x)$ goes to in the quotient and show how the coset of x is a zero, as we did in the class.

[3] Explain what minimality means here.

Ex. 24. Let E be a splitting field of an irreducible polynomial $p(x) \in F[x]$. Let α be a root of $p(x)$ in E. Then the number of embeddings (that is an injective homomorphism which is an identity on F) from $F(\alpha)$ to E is number of distinct roots of the polynomial $p(x)$.

Theorem 25. *Let F and F' be fields. Let θ be an isomorphism from F to F'. Let E and E' be splitting fields of $f(x)$ and $\theta(f)(x)$ over F and F' respectively then there exists an isomorphism from E to E'.*

Proof. Proof by strong[4] induction on $[E : F]$. Induction hypothesis: Suppose L/K is a splitting field of $g(x)$ over K, $\theta\colon K \simeq K'$ is an isomorphism from K to K' and L' is a splitting field of $\theta(g)(x)$ over K'. Then there exists an isomorphism from L to L' extending θ.[5]

If $[E : F] = 1$ then there is nothing to prove. So assume that this result is true for all $k < n$ where $n > 1$. Let $[E : F] = n$. Let $p(x)$ be an irreducible factor of $f(x)$. Let α be a root of $p(x)$ in E. Extend the isomorphism θ from F to F' to an isomorphism $\overline{\theta}$ from $F[x]$ to $F'[x]$. Now, $\phi : F[x]/\langle p(x)\rangle \to F'[x]/\langle \theta(p)(x)\rangle$ defined by $\phi(g + \langle p\rangle) = \overline{\theta}(g) + \langle \theta(p)\rangle$ is an isomorphism. Note that $\theta(p)(x)$ is also an irreducible polynomial over F'. Let β be a root of $\theta(p)(x)$ in E'. Then $F(\alpha) \simeq F[x]/\langle p(x)\rangle \simeq F'[x]/\langle \theta(p)(x)\rangle \simeq F'(\beta)$. That is there exists an isomorphism θ_1 from $F(\alpha)$ to $F'(\beta)$ extending θ. [6] Note that $[F(\alpha) : F] > 1$, $[E : F(\alpha)] < n$ and further $E = E(\alpha)$ and $E' = E'(\beta)$ are splitting fields of $f(x)$ and $\theta(f)(x)$ over $F(\alpha)$, $F'(\beta)$ respectively[7] By induction hypothesis there exists an isomorphism ψ from E to E' which is extension of θ_1. Hence the theorem follows. □

Corollary 26 (Uniqueness of Splitting Fields)**.** *If $f(x) \in F[x]$, then any two splitting fields of $f(x)$ over F are isomorphic by an isomorphism which is identity on F.* □

Definition 27. A field extension E/F is called normal extension if an irreducible polynomial $p(x) \in F[x]$ has a root in E then $p(x)$ splits in E

Theorem 28. *Let E/F by an finite extension. Then E/F is a normal extension iff E is the splitting field of some polynomial $p(x) \in F[x]$.*

Proof. Let E/F be a normal extension. Since E/F is a finite extension, we let $E = F(\alpha_1, \cdots, \alpha_k)$. Take $p(x) = \prod_{i=1}^{n} \min(\alpha_i, F)$. Then E is the splitting field of $p(x)$ over F (Why?).

Reason: $\alpha_i \in E$ is a root of the irreducible polynomial $\min(\alpha_i, F)$. Since E/F is normal, all roots of $\min(\alpha_i, F)$ lies in E. So, $p(x)$ splits in $E[x]$. Clearly it the smallest field which contains all α_i's.

For the converse part, assume that E is the splitting field of some $p(x) \in F[x]$. Let $g(x) \in F[x]$ be an irreducible polynomial and let α be a root of $g(x)$ in E. Let $\beta \neq \alpha$ be another root of $g(x)$.

We claim $\beta \in E$. Note that $F[\alpha] \simeq F[\beta]$. Since E is the splitting field of $p(x)$ over F, we have $E[\alpha]$ is the splitting field of $p(x)$ over $F[\alpha]$ (Why?) and $E[\beta]$ is the splitting field of

[4] In my opinion, it is weak form, as the hypothesis is stronger than the one in the standard induction, but the conclusion is the same!

[5] Note the change. This is crucial.

[6] Note the change.

[7] Perhaps, this needs explanation, as we found in the classroom.

$p(x)$ over $F[\beta]$. Now, $F[\alpha] \simeq F[\beta] \implies E[\alpha] \simeq E[\beta]$. But $E[\alpha] = E$ so that $E \approx E[\beta]$. Thus $[E : E] = [E[\beta] : E]$ establishes our claim $\beta \in E$. Hence $g(x)$ splits in $E[x]$.

This last paragraph needs careful rewriting. Where does β live? Say that $\theta\colon F[\alpha] \to F[\beta]$ is an isomorphism. Let $\theta_1\colon E[\alpha] \to E[\beta]$ be its extension etc. Also, in the last part, in stead of relying upon $E[\alpha] = E$ etc, argue carefully with the tower law. □

Definition 29. Let E/F be a field extension. The Galois group of E over F is defined by $\mathrm{Gal}(E/F) = \{\sigma : \sigma \text{ is an automorphism of } E \text{ such that } \sigma/_F = \mathrm{id}\}$. Verify that $\mathrm{Gal}(E/F)$ is a subgroup of the group of all automorphisms of E.

If $f(x) \in F[x]$ has splitting field E, then the Galois group of $f(x)$ is $\mathrm{Gal}(E/F)$.

Ex. 30. Let $f(x) \in F[x]$ and let E/F be an extension field. If $\sigma \in \mathrm{Gal}(E/F)$ then σ permutes the roots of $f(x)$ (in E)[8]. That is, if $\alpha \in E$ is a root of $f(x)$, then show that $\sigma(\alpha)$ is also a root of $f(x)$.

Theorem 31. *If $f(x) \in F[x]$ has n distinct roots in its splitting field E, then Gal(E/F) is isomorphic to a subgroup of the symmetric group S_n.*

Proof. Let $X = \{\alpha_1, \ldots, \alpha_n\}$ be the set of all the roots of $f(x)$ in E. By the previous exercise if $\sigma \in \mathrm{Gal}(E/F)$, then $\sigma(X) = X$. The map from $\mathrm{Gal}(E/F)$ to S_X defined by $\sigma \mapsto \sigma/X$ is easily seen to be a homomorphism and it is an injection(why?). Finally $S_X \simeq S_n$. □

Ex. 32. Find the Galois groups (i) of $x^2 + 1$ over $\mathbb{R}$, (ii) of $x^3 - 1$ over $\mathbb{Q}$, (iii) of $x^3 - 2$ over $\mathbb{Q}$, and (iv) $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where ζ is the primitive pth root of unity and p a prime.

Theorem 33. *Let E be the splitting field of $f(x) \in F[x]$ and if $f(x)$ has simple roots (the roots of $f(x)$ are all distinct) then $|\mathrm{Gal}\,(E/F)| = [E : F]$.*

Proof. Proof by strong[9] induction on $[E : F]$. Induction hypothesis: Suppose L/K is the splitting field of $g(x)$ over K, all the roots of $g(x)$ in L are distinct, $\theta K \simeq K'$ is an isomorphism from K to K' and L' is the splitting field of $\theta(g)(x)$ over K'. Then θ has exactly $[L : K]$ number of extensions from L to L'.

If $[E : F] = 1$ then $E = F$ and there is only one extension of σ, namely, σ itself. If $[E : F] > 1$, let $p(x)$ be an irreducible factor of $f(x)$, then $\deg p(x) > 1$. Let α be a root of $p(x)$ in E. Then by Exercise 24 the number of embeddings from $F(\alpha)$ to E is equal to the degree of $p(x)$. Since $E = E(\alpha)$ is the splitting field of $f(x)$ over $F(\alpha)$ and $[E : F(\alpha)] < [E : F]$, by induction for each embedding θ [10]of $F(\alpha)$ to E we can get $[E : F(\alpha)] = [E : F]/\deg p(x)$ number of extensions of θ[11]. Therefore we get at least $[E : F]$ number of automorphisms which are identity on F. But any element in $\mathrm{Gal}(E/F)$ is an embedding from $F(\alpha)$ to E[12] so $|\mathrm{Gal}\,(E/F)| = [E : F]$. □

[8] Inserted: in E

[9] Same as the last remark on this issue!

[10] Inserted the map θ.

[11] Used the notation θ

[12] Perhaps, better to explain this, as this caused problems in the class.

Definition 34 (Radical extension)**.** An extension R/F is said to be a radical extension if there exists a finite number of tower of fields $F = R_0 \subseteq R_1 \subseteq R_2 \subseteq \ldots \subseteq R_k = R$ such that for each i $R_{i+1} = R_i(\alpha_i)$, with $\alpha_i^{n_i} \in R_i$ for some positive integer n_i. If n_i's are all prime then R/F is said to be prime radical extension.

If $R = F(\alpha)$ with $\alpha^n \in F$ and F contains the nth root of unity, then R is the splitting field of $x^n - \alpha^n$ over F.

Ex. 35. Any radical extension of F is a finite extension. (Hint: If $R = F(\alpha)$ with $\alpha^n \in F$, then α is a root of the polynomial $x^n - \alpha^n$ over F.)

Ex. 36. If R/F is a radical extension then R/F is a prime radical extension.(Hint: If $\alpha^n \in F$ and $n = pm$, where p is a prime, then there is a tower of fields $F \subseteq F(\alpha^m) \subseteq F(\alpha)$.)

Ex. 37. If R/F is a radical extension containing an extension E/F, then E/F is also radical extension.[13]

Ex. 38. If L/E and E/F are radical extensions, then L/F is also a radical extension.

Ex. 39. Prove that any splitting field E/F of $f(x) \in F[x]$ containing a radical extension R/F is itself a radical extension.

Definition 40. If $f(x) \in F[x]$, then $f(x)$ is solvable by radicals over F if there is a radical extension R/F which contains the splitting field E of $f(x)$ over F.

Example 41. If $f(x) = x^2 + bx + c \in \mathbb{Q}[x]$[14], define $F = \mathbb{Q}(b, c)$ and $E = F(\sqrt{b^2 - 4c})$. Then E is the splitting field of $f(x)$ over F and also E/F is a radical extension; therefore, $f(x)$ is solvable by radicals over F.

Theorem 42. *Let F be a field of characteristic 0 and let E/F be a radical extension. Then there exists an extension R/F such that (i) $E \subseteq R$, (ii) R is radical over F, (iii) R is normal over F.*

Proof. Since E/F is a radical extension there exists a radical tower $F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_r = E$. We prove the theorem by induction on r. If $r = 0$ then there is nothing to prove. So assume that the result is true for all $k < r$. Using induction hypothesis for $r - 1$, we have a radical extension L/E_{r-1} such that (i) $E_{r-1} \subseteq L$, (ii) L/F is radical and (iii) L/F is normal. Since L/F is normal there exists a polynomial $g(x) \in F[x]$ such that L is the splitting field of $g(x)$ over F. Note that, $E_r = E_{r-1}(a)$ with $a^n = b \in E_{r-1}$. Let $f(x) = min(a, L)$ and K is the splitting field of $f(x)$ over L. Then (i) $E = E_r \subseteq K$, (ii) K radical over L, and (iii) K is the splitting field of the polynomial $f(x)g(x)$ over F and hence K/F is normal.[15]

Reasons: (i) Since $a \in K$ and $E_{r-1} \subseteq L \subseteq K$, we have $E_r \subseteq K$.

(ii) Since $K = L(\alpha_1 = a, \alpha_2, \ldots, \alpha_k)$, where α_i's are all roots of $f(x)$ in L and $f(x)$ divides $x^n - b$, we have $\alpha_i^n \in L$.

[13] Is this clear?

[14] Note the polynomial ring.

[15] A diagram as drawn in the class may be of help.

(iii) Since $g(x)$ splits in L and $f(x)$ splits in K, $L \subseteq K$, we have $f(x)g(x)$ splits in K. Let K_1 be the splitting field of $f(x)g(x)$ over F then $K_1 \subseteq K$. Since L is the splitting field of $g(x)$ over F we have $L \subseteq K_1$ and also since K is the splitting field of $f(x)$ over L, we have $K \subseteq K_1$. Hence $K = K_1$. □

Corollary 43. *Let F be a field of characteristic 0 and let E/F be a radical extension. Then there exists an extension R/F such that (i) $E \subseteq R$, (ii) R is prime radical over F, (iii) R is normal over F.* □

Corollary 44. *Let F be a field of characteristic 0 and let E/F be a radical extension. Then there exists an extension R/F such that*

(i) $E \subseteq R$,

(ii) R is normal over F

(iii) R/F is a prime radical extension such that $F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_r = R$ with the properties

(a) for each j we have $E_j = E_{j-1}(\alpha_j)$, $\alpha_j^{p_j} \in E_{j-1}$, where p_j is a prime and

(b) if α_j is not a p_jth root of unity, then E_{j-1} contains the p_j th root of unity. □

Definition 45 (Solvable group)**.** A group G is said to be solvable if there exists a finite sequence of subgroups of G such that (i) $\{e\} = G_k \subseteq G_{k-1} \subseteq \ldots \subseteq G_0 = G$ with each G_{i+1} a normal subgroup of G_i and (ii) G_i/G_{i+1} is an abelian group,

Ex. 46. Subgroup of a solvable group is solvable and also homomorphic image of a solvable group is solvable.

Theorem 47. *Let $f(x) \in F[x]$ be solvable by radicals over a field F of characteristic 0, and let E/F be its splitting field. Then $\mathrm{Gal}\,(E/F)$ is a solvable group.*

Proof. With out loss of generality we can assume that E/F is a prime radical extension such that $F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_r = E$ with the properties

(1) for each j we have $E_j = E_{j-1}(\alpha_j)$, $\alpha_j^{p_j} \in E_{j-1}$, where p_j is a prime and

(2) if α_j is not a p_jth root of unity, then E_{j-1} contains the p_j th root of unity.

Let, for each j, $G_j := \mathrm{Gal}\,(E/E_j)$. Then $\{e\} = G_r \subseteq G_{r-1} \subseteq \ldots \subseteq G_0 = \mathrm{Gal}(E/F)$. Consider the map $\varphi_j : \mathrm{Gal}\,(E/E_{j-1}) \to \mathrm{Gal}\,(E_j/E_{j-1})$ defined by $\sigma \mapsto \sigma \mid_{E_j}$. Now we claim that $\sigma \mid_{E_j} \in \mathrm{Gal}\,(E_j/E_{j-1})$. Since $E_j = E_{j-1}(\alpha_j)$ is the splitting field of the polynomial $x^{p_j} - \beta_j$ over E_{j-1}, where $\alpha_j^{p_j} = \beta_j \in E_{j-1}$. Then E_j/E_{j-1} is a normal extension therefore all the roots of $x^{p_j} - \beta_j$ belongs to E_j. Since $\sigma(\alpha_j)$ is a root of $x^{p_j} - \beta_j$, $\sigma(\alpha_j) \in E_j$. Thus $\sigma \mid_{E_j} \in \mathrm{Gal}\,(E_j/E_{j-1})$. So φ_j is well-defined. It is easily seen that φ_j is group homomorphism. Also φ_j is onto. (Why?) $\ker(\varphi_j) = \{\sigma \in G_{j-1} : \sigma \mid_{E_j} = id.\} = G_j = \mathrm{Gal}\,(E/E_j)$. By fundamental theorem of homomorphism $G_{j-1}/G_j \simeq \mathrm{Gal}\,(E_j/E_{j-1})$, which is a cyclic group (verify!). Hence the theorem follows. □

Ex. 48. The polynomial $x^5 - 6x + 3 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ and it has exactly three real roots and two complex roots in $\mathbb{C}$. (Hint: Use Eisenstein's criterion for irreducibility, intermediate value theorem to say there are at least 3 real roots and Rolle's theorem to conclude that there are at most 3 real roots.)

Theorem 49 (Abel)**.** *There exists a quintic polynomial $f(x) \in \mathbb{Q}[x]$ that is not solvable by radicals.*

Proof. Consider the polynomial $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}$ and it has exactly three real roots and two complex roots in $\mathbb{C}$. Let $E/\mathbb{Q}$ be the splitting field of $f(x)$ contained in $\mathbb{C}$, and let G=Gal$(E/\mathbb{Q})$. If α is a root of $f(x)$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$=5, and so

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 5[E : \mathbb{Q}(\alpha)].$$

By Theorem 33 $|G| = [E : \mathbb{Q}]$ is divisible by 5. Regarding G as a group of permutations on the 5 roots, we note that G contains a 5-cycle (it contains an element of order 5, by Cauchy's theorem, and the only elements of order 5 in S_5 are 5-cycles). The restriction of complex conjugation, call it σ, for σ interchanges the two complex roots while it fixes the three real roots. S_5 is generated by any transposition and any 5-cycle (thanks to group theory), so that G=Gal$(E/\mathbb{Q})\simeq S_5$ is not a solvable group (thanks to group theory) and Theorem 47 shows that $f(x)$ is not solvable by radicals. □

Theorem 50. *Now the crucial point is that the Galois group* Gal (f) *of the polynomial* $f(x)$ *is a homomorphic image of* Gal (R/F) *which is solvable. Hence we conclude that there exist polynomials which are not solvable by radicals.*

Acknowledgement. This set of notes (of a course of lectures given by me in MTTS 2009) was prepared by Thiru R. Venkatesh. I thank him for this as well as his help while lecturing on this material.