Solvability by radicals

Zijian Yao

December 8, 2013

For now all our discussion happens in characteristic 0.

Definition 1. Let E/F be a finite, separable extension, let K be the Galois closure of E/F, the extension E/F is said to be solvable if $Gal(K/F)$ is a solvable group. In particular, if E/F is Galois, then E/F is solvable if its Galois group is solvable.

Remark: this is equivalent as saying that there exists solvable Galois extension L/F such that $F \subset E \subset L$. This is because, we have tower of extensions $F \subset E \subset K \subset L$, where $Gal(L/F)/Gal(L/K) \sim Gal(K/F)$, then by properties of solvable groups this is clear.

Definition 2. $\alpha \in F$ is expressible by radical roots if there exists $F \subset E_1 \subset E_2 \subset ... \subset E_s = E$ such that $\alpha \in E$ and $E_{i+1} = E_i(\sqrt[n_i]{\alpha_i})$, where $\sqrt[n_i]{\alpha_i}$ denote a root of polynomial $x^{n_i} - \alpha_i$, $\alpha_i \in F_i$. We say a polynomial $f(x) \in F[x]$ is solvable by radicals if all roots of $f(x)$ are expressible by radicals.

Definition 3. Let L/F be a finite, separable extension, we say L/F is solvable by radicals if there is a finite extension E/F, such that $L \subset E$, and E admits tower $F \subset E_1 \subset E_2 \subset ... \subset E_s = E$ such that and $E_{i+1} = E_i(\sqrt[n_i]{\alpha_i})$ for some $\alpha_i \in E_i$.

Lemma 4. *Let E/F be solvable, and E'/F is some extension, where E, E' belongs to some algebraically closed field. Then EE'/E' is solvable.*

Proof. Let K be the Galois closure of E/F, then KE' is Galois over E', and $Gal(KE'/E') < Gal(K/F)$, so KE'/E' is solvable. Therefore EE'/E' is solvable.

Lemma 5. *Let $M/E/F$ be tower of finite extensions, let E/F and M/E be solvable, then M/F is solvable.*

Proof. Let K be the Galois closure of E/F, then KM is solvable over K. Let L be the Galois closure of KM over K. Consider any embedding σ of L fixing F into some algebraic closure of F, then $\sigma K = K$, so σL is solvable over K. Let N be the composite of all such σL, then N is Galois over F. Therefore, $Gal(N/K) < \prod_\sigma Gal(\sigma L/K)$. So $Gal(N/K)$ is solvable group, thus $Gal(N/F)$ is solvable.

Recall we have the following proposition,

Proposition 6. *Let F be field, $n \in \mathbb{N}$, assume $\zeta_n \in F$, where ζ_n is the primitive n-th root of unity. Then*

(1). $F(\sqrt[n]{a})/F$ is cyclic of degree $d \mid n$, where $a \in F$.

(2). If E/F is cyclic of degree n, then there is $a \in F$ such that $E = F(\sqrt[n]{a})$

Theorem 7 (Galois). *Let E/F be separable extension, then E/F is solvable if and only if it is solvable by radicals.*

Proof. (1). First assume E/F is solvable, let K be the Galois closure of E/F, let $n = [K : F]$, and $m = \prod p_i$ where $p_i \mid n$. Let ζ be a primitive m-th root of unity and consider $F(\zeta)$. Clearly $F(\zeta)/F$ is abelian. Consider the lift of K over $F(\zeta)$, $KF(\zeta)/F$ is solvable.Let Galois group of $K(\zeta)/F(\zeta)$ be G, solvable. Let $1 = G_0 \lhd G_1 \lhd ... \lhd G_s = G$ be the composition series, where successive pairs G_{i+1}/G_i is cyclic of prime order. The Galois correspondence tells us that each $F_i/F(\zeta)$ is Galois, and therefore F_i/F_{i+1} is Galois with Galois group G_{i+1}/G_i, which is cyclic of prime order. Hence there is some $a_{i+1} \in F_{i+1}$ such that $F_i = F_{i+1}(\sqrt[p_{i+1}]{a_{i+1}})$, so the extension $K(\zeta)/F$ is solvable by radicals, thus E/F is solvable by radicals.

(2). For the converse direction. assume E/F is solvable by radicals. Let σ be an embedding of E in its algebraic closure, then $\sigma E/F$ is solvable by radicals. Let K be the Galois closure of E/F, so K is the composite of all such σE's. Hence K is solvable by radicals over F. Let $n = [K : F]$, and $m = \prod p_i$ where $p_i \mid n$, let ζ be a primitive m-th root of unity.

Since K/F is solvable radicals, there is a tower of fields $F = F_0 \subset F_1 \subset ... \subset F_l$ where $K \subset F_l$, and each successive pair is radical extension $F_i = F_{i-1}(\alpha_i)$. Consider the closure L of F_l over F. L is the composite of all embedded $\sigma_j F_l(\zeta)$.

So $L = F(\zeta, \sigma_j \alpha_i) = F(\zeta)(\sigma_j \alpha_i)$. We join the elements $\{\alpha_1, ..., \alpha_l, \sigma_1\alpha_1, ..., \sigma_1\alpha_l, ..., \sigma_s\alpha_l\}$ to $F(\zeta)$ one by one, then each successive pair is a radical extension, thus cyclic Galois. We know L/F_i' and L/F_{i+1}' are Galois with Galois group G_i and G_{i+1}, then $G_{i+1} \lhd G_i$ and the quotient is cyclic.

This shows L/F is solvable. So E/F is solvable.

Corollary 8 (Galois's Theorem). *The polynomial $f(x)$ can be solved by radicals if and only if its Galois group is solvable.*

Theorem 9. *In general, polynomials over some field of degree greater or equal to 5 is not solvable by radicals.*

Recall we have elementary symmetric functions $s_1, s_2, ..., s_n$ of indeterminants $f_n = x_1, ..., x_n$. We know that the general polynomial $x^n - s_1X^{n-1} + s_2x^{n-2} - .... + (-1)^n s_n$ over the field $F(s_1, s_2, ...s_n)$ is separable with Galois group S_n. We view the s_i over the field F as indeterminants. By this we mean,the roots of f_n, namely $x_1, ..., x_n$ have no polynomial relations among them. So over the field $F(s_1, ..., s_n)$, the polynomial is *not solvable by radicals.*

Here we gave an explicit construction of a family of polynomials over $\mathbb{Q}$ that is no solvable by radicals. Let p be a prime great or equal to 5. Choose a positive even integer m and even integers $n_1 < n_2 < ... < n_{p-2}$.

Construct $g(x) = (x^2 + m)(x - n_1)...(x - n_{p-2})$ and let $f(x) = g(x) - \frac{2}{n}$ where n is large enough such that $2/n < |all\, local\, extrema|$. Check this works.

Theorem 10. *For each $n \in \mathbb{N}$, there are infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ with s_n being its Galois group.*

For characteristic p case, we modify our definitions slightly.

1. It is obtained by adjoining a root of unity.

2. It is obtained by adjoining a root of a polynomial $x^n - a$ with $p \nmid n$

3. It is obtained by adjoining a root of an equation $x^p - x - a$ with a in previous field.