Insolvability of General Quintic

Sixuan Lou

February 16, 2018

1 Definitons & Preliminaries

We say a field extension K/k is a *simple radical extension (s.r.e)* if $K = k(\alpha)$ for some $\alpha \in K$ and there exists $n \in \mathbb{N}$ such that $\alpha^n \in k$. If K/k can be built up by a chain of s.r.e's, we say K/k is a *root extension*. That is, there is a chain

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = K$$

where K_{i+1}/K_i is a s.r.e for all $i = 0, \ldots, r-1$.

We say a polynomial $f \in k[x]$ is *solvable by radicals* if there is a root extension L/k in which f splits.

Lemma 1.1. Let K_1/k, K_2/k be two root extensions, then K_1K_2/k is a root extension as well.

Proof. Suppose we have two chains:

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r, \quad k = K'_0 \subseteq K'_1 \subseteq \cdots \subseteq K'_s$$

Observe, for all K', $K_{i+1}K'/K_iK'$ is a simple radical extension. Suppose $K_{i+1} = K_i(\alpha)$, then $K_{i+1}K' = K_iK'(\alpha)$, and $\alpha^n \in K_i \subseteq K_iK'$ for some $n \in \mathbb{Z}^+$. Then the following chain suffices:

$$k = K_0K'_0 \subseteq K_1K'_0 \subseteq K_1K'_1 \subseteq K_2K'_1 \subseteq K_2K'_2 \subseteq K_3K'_2 \subseteq \cdots \subseteq K_rK'_{s-1} \subseteq K_rK'_s$$

□

Let k be a field of characteristic zero.

Lemma 1.2. If ζ is a primitive n-th root of unity, and $x^n - 1$ does not split completely over k, then $k(\zeta)/k$ is Galois and its Galois group embeds into $(\mathbb{Z}/n)^\times$.

Proof. Since ζ is a primitive n-th root of unity, $k(\zeta)$ is the splitting field of $x^n - 1$ over k, so $k(\zeta)/k$ is Galois. Let $\sigma \in \mathrm{Gal}(k(\zeta)/k)$, it maps ζ to another primitive n-th roof of unity, $\zeta^\sigma = \zeta^i$ for some i. The map $\varphi : \mathrm{Gal}(k(\zeta)/k) \to (\mathbb{Z}/n)^\times$ mapping σ to i is a well-defined group homomorphism. It's injective since if $\varphi(\sigma) = 1$, $\zeta^\sigma = \zeta$, and it determines the identity map on $k(\zeta)$. □

Lemma 1.3. If p is an odd prime, then the group $(\mathbb{Z}/p^e)^\times$ is cyclic for all $e \in \mathbb{Z}^+$.

Proof. Observe $\mathbb{Z}/p$ is a field, and finite subgroup of the multiplicative group of a field is cyclic. Let $g \in (\mathbb{Z}/p)^\times$ be a generator. Then $g^{p-1} = 1 + pT$ for some $T \in \mathbb{Z}$, so for $t \in \mathbb{Z}/p$,

$$(g+pt)^{p-1} = 1 + p(T_0 - g^{p-2}t + pT) =: 1 + pu.$$

Observe g^{p-2} is also a primite root of unity, so as t runs through $\mathbb{Z}/p$, the product $g^{p-2}t$ runs through $(\mathbb{Z}/p)^\times$, so in particular there exists some $t \in \mathbb{Z}/p$ such that $(g+pt)^{p-1} = 1 + pu$, where $p \nmid u$. We claim $g + pt$ must be a generator of $(\mathbb{Z}/p^e)^\times$ for all $e \geq 2$. Observe

$$\begin{aligned}
(g+pt)^{p(p-1)} &= (1+pu)^p = 1 + p^2 u_2 && (p \nmid u_2)\\
(g+pt)^{p^2(p-1)} &= (1+p^2u_2)^p = 1 + p^3 u_3 && (p \nmid u_3)\\
&\cdots && (1.1)
\end{aligned}$$

Suppose $g + pt$ has order δ in $(\mathbb{Z}/p^e)^\times$, then $(g+pt)^\delta \equiv 1 \bmod p$, so $p - 1 \mid \delta$. Moreover, $\delta \mid \varphi(p^e) = p^{e-1}(p-1)$, so $\delta = p^a(p-1)$ for some $0 \leq a \leq e-1$. However by Equation (1.1), $(g+pt)^{p^a(p-1)} = 1 + p^{a+1}u_{a+1}$ for some $p \nmid u_{a+1}$, so we must have $a + 1 = e$, and $\delta = p^{e-1}(p-1) = \varphi(p^e)$, so $g + pt$ is a generator of $(\mathbb{Z}/p^e)^\times$. □

2 The main result

Theorem 2.1 (Hilbert's Theorem 90 (mult ver.))**.** Let K/k be a cyclic extension of degree n. Let $\sigma \in \mathrm{Gal}(K/k)$ be a generator, then for all $\beta \in K$,

$$N_{K/k}(\beta) = 1 \iff \beta = \frac{\alpha}{\alpha^\sigma} \text{ for some } \alpha \in K^\times$$

Proof.

1. Let $\beta \in K$ with $N_{K/k}(\beta) = 1$ be given. Define

$$\beta_1 = \beta, \quad \beta_{i+1} = \beta\beta_i^\sigma \quad (0 \leq i \leq n-2)$$

Since σ generates $\mathrm{Gal}(K/k)$, the list $\{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\}$ is linearly independent, there exists $\theta \in K$ such that

$$\alpha := \theta + \beta_1\theta^\sigma + \beta_2\theta^{\sigma^2} + \cdots + \beta_{n-1}\theta^{\sigma^{n-1}}$$

α is not zero. Then it is evident that $\alpha/\alpha^\sigma = \beta$ (use the fact that $N_{K/k}(\beta) = 1$).

2. Suppose there exists $\alpha \in K^\times$ such that $\beta = \alpha/\alpha^\sigma$. Then

$$N_{K/k}(\beta) = \prod_{\sigma \in \mathrm{Gal}(K/k)} \beta^\sigma = \prod_{\sigma \in \mathrm{Gal}(K/k)} \frac{\alpha^\sigma}{\alpha^{\sigma^2}} = \frac{N_{K/k}(\alpha)}{N_{K/k}(\alpha)} = 1$$

□

Lemma 2.2. Let k be a field, $n \in N$ with $\operatorname{char} k \nmid n$. Assume $\zeta_n \in k$, then

1. If K/k is a cyclic extension of degree n, K/k is a s.r.e.
2. Given $a \in K$, let α be a root of $x^n - a$, then $k(\alpha)/k$ is cyclic of degree d, for some $d \mid n$, and $\alpha^d \in k$.

Proof. 1. Suppose $\mathrm{Gal}(K/k)$ is generated by σ of order n. Since k contains ζ_n, ζ_n^{-1} is fixed by every automorphism of K/k. So,

$$N_{K/k}(\zeta_n^{-1}) = \prod_{\sigma\in\mathrm{Gal}(K/k)} (\zeta_n^{-1})^\sigma = \prod_{\sigma\in\mathrm{Gal}(K/k)} \zeta_n^{-1} = \zeta_n^{-n} = 1$$

By Hilbert Theorem 90, there exists $\alpha \in K^\times$ such that $\zeta_n^{-1} = \alpha/\alpha^\sigma$, so $\alpha^\sigma = \zeta_n\alpha$. Since σ generates the Galois group, $\{\alpha, \alpha^\sigma, \alpha^{\sigma^2}, \dots, \alpha^{\sigma^{n-1}}\} = \{\alpha, \zeta_n\alpha, \zeta_n^2\alpha, \dots, \zeta_n^{n-1}\alpha\}$ are all n distinct roots of the minimal polynomial m of α over k. So $\deg m = n$, so $K = k(\alpha)$. Furthermore, for every $\sigma \in \mathrm{Gal}(K/k)$,

$$(\alpha^n)^\sigma = (\alpha^\sigma)^n = (\zeta_n\alpha)^n = \alpha^n$$

so $\alpha^n \in k$.

2. Let $a \in k$ be given, let α be a root of $x^n - a$, then $\{\alpha, \zeta_n\alpha, \zeta_n^2\alpha, \dots, \zeta_n^{n-1}\alpha\}$ are n distinct roots of $x^n - a$. Therefore, $k(\alpha)$ is the splitting field of $x^n - a$. Since $x^n - a$ is separable, it follows $k(\alpha)/k$ is Galois and every $\sigma \in \mathrm{Gal}(k(\alpha)/k)$ sends α to $\zeta^i\alpha$ for some i. Define $\begin{pmatrix}\varphi : \mathrm{Gal}(k(\alpha)/k) \to \mathbb{Z}/n \\ \varphi : \sigma \mapsto i\end{pmatrix}$, it is easily seen that φ is an injective group homomorphism, therefore $\mathrm{Gal}(k(\alpha)/k)$ is isomorphic to a subgroup of $\mathbb{Z}/n$, hence $\mathrm{Gal}(k(\alpha)/k) \cong \mathbb{Z}/d$ for some $d \mid n$. Furthermore, for any $\sigma \in \mathrm{Gal}(k(\alpha)/k)$, $\alpha^{\sigma^d} = \zeta_n^{d\varphi(\sigma)}\alpha = \alpha$, so $\zeta_n^{d\varphi(\sigma)} = 1$, so

$$(\alpha^d)^\sigma = (\alpha^\sigma)^d = (\zeta_n^{\varphi(\sigma)})^d\alpha^d = \alpha^d.$$

Hence α^d is fixed by every $\sigma \in \mathrm{Gal}(k(\alpha)/k)$, so $\alpha^d \in k$.

□

Lemma 2.3. Let k be a field, $\mathrm{char}\, k = 0$. Let ζ be a primitive n-th root of unity. Then $k(\zeta)/k$ is a root extension and each factor in the chain is cyclic.

Proof. 1. Suppose $n = p^e$ for some odd prime p. Then $\mathrm{Gal}(k(\zeta)/k)$ is isomorphic to a subgroup of $(\mathbb{Z}/p^e)^\times$, which is cyclic by Lemma 1.3, hence Galois extension is a s.r.e and the Galois group is cyclic.

2. Suppose $n = 2^e$. Then $\mathrm{Gal}(k(\zeta)/k)$ is isomorphic to a subgroup of $(\mathbb{Z}/2^e)^\times$, which is of order $\varphi(2^e) = 2^e - 2^{e-1} = 2^{e-1}$, hence $\mathrm{Gal}(k(\zeta)/k)$ is a 2-group. By first Sylow theorem, there is a subgroup $H \lhd \mathrm{Gal}(k(\zeta)/k)$ of index 2, hence $k(\zeta)^H/k$ is Galois, with Galois group $\mathbb{Z}/2$, which is cyclic. Then we have chain

$$k \subseteq k(\zeta)^H \subseteq k(\zeta)$$

Since $[k(\zeta)^H : k] = 2$, $k(\zeta)/k(\zeta)^H$ is a proper subextension, the claim follows from induction.

3. Suppose $n = p_1^{e_1} \cdots p_r^{e_r}$. Observe $\zeta^{n/p_i^{e_i}}$ is a primitive $p_i^{e_i}$-th root for each i. Suppose there exists i such that $\zeta^{n/p_i^{e_i}}$ is not in k, then we have chain:

$$k \subseteq k(\zeta^{n/p_i^{e_i}}) \subseteq k(\zeta)$$

where the first part may be handled in one of the base case, and the latter part is a proper subextension, hence is handled by the inductive hypothesis.

Now suppose $\zeta^{n/p_i^{e_i}} \in k$ for all i, then we claim their product

$$\prod_i \zeta^{n/p_i^{e_i}}$$

is a primitive n-th root of unity, since the smallest power that takes it to unity is exactly n (each pair p_i, p_j is coprime). Therefore, in this case, $k(\zeta) = k$, this case is vacuous.

This finishes the proof. □

Lemma 2.4. Let ℓ/k be a root extension, then there is a Galois extension L/k that contains ℓ and such that L/k is a root extension where each step is a cyclic s.r.e.

Proof. Suppose ℓ/k has chain:

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = \ell$$

Let K be the Galois closure of ℓ over k. Given $\sigma \in \mathrm{Gal}(K/k)$, we claim ℓ^σ is a root extension, with chain:

$$k = K_0^\sigma \subseteq K_1^\sigma \subseteq \cdots \subseteq K_r^\sigma = \ell$$

Given $i = 0, \ldots, r-1$, suppose $K_{i+1} = K_i(\alpha)$, then

$$K_{i+1}^\sigma = (K_i(\alpha))^\sigma = \left\{ \frac{f^\sigma(\alpha^\sigma)}{g^\sigma(\alpha^\sigma)} : f, g \in K_i[x] \right\} = K_i^\sigma(\alpha^\sigma)$$

Suppose $\alpha^n \in K_i$, then $(\alpha^\sigma)^n = (\alpha^n)^\sigma \in K_i^\sigma$. Since finite composite of root extension is a root extension, $L := \prod_{\sigma \in \mathrm{Gal}(K/k)} \ell^\sigma$ is a root extension over k. We claim L in fact is the Galois closure K.

Since each σ is an automorphism of K, $\ell^\sigma \subseteq K$, hence the composite $L \subseteq K$. Conversely, let $\tau \in \mathrm{Gal}(K/k)$ be given, since $\mathrm{Gal}(K/k)$ is a group,

$$L^\tau = (\prod_{\sigma \in \mathrm{Gal}(K/k)} \ell^\sigma)^\tau = \prod_{\sigma \in \mathrm{Gal}(K/k)} \ell^{\sigma\tau} = \prod_{\sigma \in \mathrm{Gal}(K/k)} \ell^\sigma = L$$

Thus every $\tau \in \mathrm{Gal}(K/k)$ fixes L, it follows that L/k is Galois, and definition of the Galois closure, $K \subseteq L$, hence $K = L$. Therefore, we have obtained a Galois root extension L/k. Suppose, it is equipped with chain:

$$k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = L$$

Suppose $L_{i+1} = L_i(\alpha_{i+1})$ for some $\alpha_{i+1} \in L_{i+1}$ $(0 \le i \le n-1)$, and suppose $\alpha_i^{n_i} \in L_{i-1}$ $(1 \le i \le n)$. Let $E_0 = L_0$, $E_i = L_i(\zeta_{n_1}, \ldots, \zeta_{n_i})$, and consider the chain:

$$\begin{tikzcd}
k = L_0 \arrow[d, hook] & E_1 \arrow[d, hook] & E_2 \arrow[d, hook] & \cdots & E_{s-1} \arrow[d, hook] & E_s \\
E_0(\zeta_{n_1}) \arrow[ur, hook] & E_1(\zeta_{n_2}) \arrow[ur, hook] & E_2(\zeta_{n_3}) \arrow[ur, hook] & \cdots \arrow[ur, hook] & E_{s-1}(\zeta_{n_s}) \arrow[ur, hook] &
\end{tikzcd}$$

Lemma 2.3 ensures each $E_i(\zeta_{i+1})/E_i$ is a root extension and each factor is cyclic $(0 \le i \le n-1)$, Lemma 2.2 ensures each $E_{i+1}/E_i(\zeta_{n_{i+1}})$ is a cyclic s.r.e $(0 \le i \le n-1)$. Therefore E_s/k is a root extension in which each factor is a cyclic s.r.e. □

Theorem 2.5. $f \in k[x]$ is solvable by radicals if and only if the Galois group of f is solvable.

Proof. Suppose $f \in k[x]$ is solvable by radicals, then there exists a root extension ℓ/k such that f splits over ℓ. By Lemma 2.4, there is a Galois root extension L/k containing ℓ and each factor is cyclic. This precisely means that L/k is a solvable extension. Let K denote the Galois group of f, we have chain of extensions $L/K/k$, and by the fundamental theorem, $\operatorname{Gal}(K/k) \cong \operatorname{Gal}(L/k)/\operatorname{Gal}(L/K)$. Since quotient of a solvable group is solvable, it follows K/k is solvable.

Conversely, suppose $\operatorname{Gal}(K/k)$ is solvable, we have a solvable filtration:

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_{r-1} \lhd G_r = G$$

Let K be the splitting field of f over k, then by fundamental theorem, we have chain of fixed fields:

$$K = K^{G_0} \supseteq K^{G_1} \supseteq \cdots \supseteq K^{G_{r-1}} \supseteq K^{G_r} = k$$

and for each i, the factor

$$\operatorname{Gal}(K^{G_i}/K^{G_{i+1}}) \cong \frac{\operatorname{Gal}(K/K^{G_{i+1}})}{\operatorname{Gal}(K/K^{G_i})} \cong \frac{G_{i+1}}{G_i} \cong \mathbb{Z}/n_i$$

is cyclic. Define $E_0 = K^{G_r}$, $E_i = K^{G_{r-i}}(\zeta_{n_{r-1}}, \ldots, \zeta_{n_{r-i}})$ and consider the chain:

$$\begin{tikzcd}
k = E_0 \arrow[d, hook] & E_1 \arrow[d, hook] & E_2 \arrow[d, hook] & \cdots & E_{r-1} \arrow[d, hook] & E_r \\
E_0(\zeta_{n_{r-1}}) \arrow[ur, hook] & E_1(\zeta_{n_{r-2}}) \arrow[ur, hook] & E_2(\zeta_{n_{r-3}}) \arrow[ur, hook] & \cdots \arrow[ur, hook] & E_{r-1}(\zeta_{n_1}) \arrow[ur, hook] &
\end{tikzcd}$$

Lemma 2.3 ensures each $E_i(\zeta_{n_{r-i-1}})/E_i$ is a root extension and each factor is cyclic $(0 \le i \le r-1)$, Lemma 2.2 ensures each $E_{i+1}/E_i(\zeta_{n_{r-i-1}})$ is a cyclic s.r.e $(0 \le i \le r-1)$. Therefore E_r/k is a root extension in which each factor is a cyclic s.r.e. Hence f can be solved by radicals. □

Corollary 2.6. $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ has roots cannot be expressed by radicals.

Proof. Notice f is irreducible by Eisenstein. Let K be the splitting field of f over $\mathbb{Q}$, then $5 \mid [K : \mathbb{Q}] = |\operatorname{Gal}(K/\mathbb{Q})|$. Since we have an injection $\operatorname{Gal}(K/\mathbb{Q}) \hookrightarrow S_5$ by permuting the roots, $\operatorname{Gal}(K/\mathbb{Q})$ contains a 5-cycle. Notice f has at least 3 real roots (by mean value theorem) and f' has exactly 2 roots, it follows that f has exactly 3 real roots. Therefore there is a 2-cycle in $\operatorname{Gal}(K/\mathbb{Q})$ given by conjugating the complex roots.

Since 2-cycle and 5-cycle generates S_5, the injection is a surjection, $\operatorname{Gal}(K/\mathbb{Q}) \cong S_5$. However, S_5 is not solvable (A_5 is not solvable), it follows that f cannot be solved by radicals. □