Lecture 22 : Solvability by Radicals

Objectives

(1) Radical extensions.
(2) Solvability by radicals and solvable Galois groups.
(3) A quintic polynomial which is not solvable by radicals.

Keywords and Phrases : Radical extensions, solvable Galois groups, insolvable quintic.

Let F be a field and $f(x) \in F[x]$. If there is a formula for the roots of $f(x)$ which involves the field operations and extraction of roots, then we say $f(x)$ is solvable by radicals over F. This can be made precise in field theory by introducing the notion of a radical extension.

Definition 22.1. *A field extension K/F is called a* **simple radical extension of** F *if $K = F(a)$ where $a^n \in F$ for some positive integer n. We say that K/F is a* **radical extension** *if there is a sequence of field extensions*

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = K$$

such that each F_i is a simple radical extension of F_{i-1} for $1 = 1, 2, \ldots, n$. A polynomial $f(x) \in F[x]$ is called **solvable by radicals over** F *if a splitting field of $f(x)$ over F is contained in a radical extension of F.*

Proposition 22.2. *Let E/F be a separable radical extension. Let $L \supset E$ be the smallest Galois extension of F so that $L \subset F^a$. Then L is a radical extension of F.*

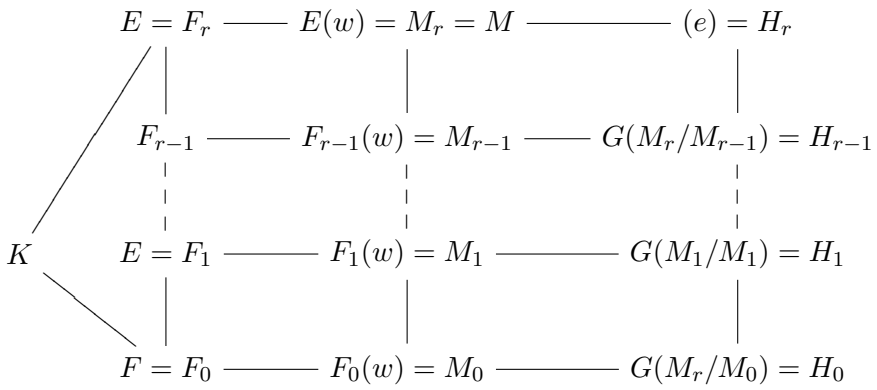
Proof. Since E/F is separable and $[E : F] = n$, there are n F-embedding of E into F^a :

$$\sigma_1, \sigma_2, \ldots, \sigma_n : E \longrightarrow F^a.$$

Then $L = \sigma_1(E)\sigma_2(E)\cdots\sigma_n(E)$ is the smallest Galois extension of F containing E. Indeed, let $E = F(a)$. Then the roots of $f_a(x) = \text{ irr } (a, F)$ in F^a are $\sigma_i(a)$ for $i = 1, 2, \ldots, n$. Hence $L = F(\sigma_1(a), \sigma_2(a), \ldots, \sigma_n(a))$ is the splitting field of $f_a(x)$ over F. Since $\sigma_i(E) \simeq E$, $\sigma_i(E)/F$ is a radical extension for each $i = 1, 2, \ldots, n$. Hence L/F is a radical extension. $\square$

Theorem 22.3. *Suppose char $F = 0$. If $f(x) \in F[x]$ is solvable by radicals then G_f is a solvable group.*

Proof. Let $F = F_0 \subset F_1 \subset \ldots \subset F_r = E$ be a sequence of simple radical extension with $F_i = F_{i-1}(a_i)$ such that $a_i^{n_i} \in F_{i-1}, i = 1, 2, \ldots, r$ and E contains a splitting field K of $f(x)$ over F. We may assume E/F is Galois by the above proposition. Let $n = n_1 n_2 \ldots n_r$ and M be the splitting field of $x^n - 1$ over E.



Let w be a primitive n^{th} root of unity. Then $F(w)$ has primitive n_i^{th} root of unity for $i = 1, 2, \ldots, r$. Since E/F is Galois, E is a splitting field of some polynomial $g(x)$ over F. Then M is a splitting field of $(x^n - 1)g(x)$ over F. Thus M is Galois over F. By the FTGT, $G(K/F) \simeq G(M/F)/G(M/K)$. Hence it is enough to prove that $G(M/F)$ is solvable.

Each M_i/M_{i-1} is a Galois extension. Hence $H_i \triangleright H_{i-1}$ for $i = 1, 2, \ldots r$. Moreover

$$H_{i-1}/H_i \simeq G(M_i/M_{i-1}).$$

Since $M_i = M_{i-1}(a_i)$ where $a_i^{n_i} \in M_{i-1}$ and M_{i-1} has a primitive n_i^{th} root of unity, the group H_{i-1}/H_i is cyclic. Thus $G(M_r/F)$ is a solvable group. Hence G_f is a solvable group. □

We will now construct a quintic $f(x) \in \mathbb{Z}[x]$ which is not solvable by radicals.

Proposition 22.4. *A subgroup of S_5 containing a 5-cycle and a transposition is S_5.*

Proof. By renumbering we may assume G contains $\sigma = (12)$ and $\tau = (12345)$. Then G has $\tau(12)\tau^{-1} = (23), \tau(23)\tau^{-1} = (34), \tau(34)\tau^{-1} = (45)$. It is easy to show that $\langle (12), (23), (34), (45) \rangle = S_5$. □

Any irreducible quintic $f(x) \in \mathbb{Q}[x]$ which has exactly 3 real roots is the polynomial we are looking for. G_f has an element of order 5 and the conjugation automorphism gives an element of order 2 in G_f. The polynomial $x(x^2-4)(x^2+4) = x^5 - 16x = g(x)$ has exactly 3 real roots $0, 2, -2$. Since $g(-1) = 15, g(1) = -15$, $f(x) = g(x) + 2 = x^5 - 16x + 2$ have exactly 3 real roots and it is irreducible over $\mathbb{Q}$, Thus $f(x) = 0$ is not solvable by radicals over $\mathbb{Q}$.

Theorem 22.5 (Galois)**.** *Suppose F is a field of characteristic zero and $f(x) \in F[x]$. If G_f solvable then $f(x)$ is solvable by radicals over F.*

$$
\begin{array}{ccc}
L = K(w) & \text{———} & (e) = H_k = G(L/E) \\
\Big| & & \Big| \\
E_{k-1} = L^{H_{k-1}} & \text{———} & H_{k-1} \\
\vdots & & \vdots \\
E_1 = L^{H_1} & \text{———} & H_1 \\
\Big| & & \Big| \\
E = L^{H_0} = F(w) & \text{———} & H_0 = G(L/E)
\end{array}
$$

Proof. Let K be a splitting field of $f(x)$ over F and $[K : F] = n$. Let L be a splitting field of $x^n - 1$ over K and w be a primitive n^{th} root of unity over K. Then $L = K(w)$. Put $E = F(w)$. Then L is a splitting field of $f(x)$ over E. Since $H = G(L/E)$ embeds into $G(K/F)$, H is also a solvable group. It is enough to show $f(x)$ is solvable by radicals over E. Consider an abelian series for H.

$$H = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_k = (1)$$

By refining this we may assume H_i/H_{i+1} is cyclic of order p_{i+1} for $i = 0, 1, \ldots, k-1$ where $p_1, p_2, \ldots, p_k$ are primes numbers. Let $E_i = L^{H_i}$ for $1, 2 \ldots k$. Then $[E_i : E_{i-1}] = |H_{i-1}/H_i| = p_i$. Since E_{i-1} has a primitive p_i^{th}

root of unity for $i = 1, 2, \ldots, k$, E_i/E_{i-1} is a simple radical extension. Hence L/F is a radical extension. Thus $f(x)$ is solvable by radicals over F. $\square$

Example 22.6. In this example we show that a splitting field of E over a field F of a polynomial $f(x) \in F[x]$ solvable by radicals need not be a radical extension of F. Consider the polynomial $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$. Let E be a splitting field of $f(x)$ over $\mathbb{Q}$. We argue that E is not a radical extension of $\mathbb{Q}$. Reducing $f(x)$ modulo 2, we see that the reduced polynomial has no root in $\mathbb{F}_2$. Hence $f(x)$ is irreducible over $\mathbb{Q}$. The discriminant of $f(x)$ is 81. Hence $G_f = A_3$ and therefore $f(x)$ is solvable by radicals by Galois' theorem. Suppose that $E/\mathbb{Q}$ is a radical extension. Since $[E : \mathbb{Q}] = 3$, there is no proper intermediate subfield of $E/\mathbb{Q}$. So $E = \mathbb{Q}(a)$ where $a^n \in \mathbb{Q}$, for some n. Let $g(x) =$ irr $(a, \mathbb{Q})$. Then E is a splitting field of $g(x)$. Moreover $g(x) \mid x^n - a^n$. Hence any root r of $g(x)$ satisfies $r^n = a^n$. Since $f(x)$ is a real root, we may assume that $E = \mathbb{Q}(r)$. Hence r/a is a real n^{th} root of unity. Hence $r = \pm a$. Hence $g(x)$ has only two roots. This is a contradiction as $g(x)$ is a separable cubic polynomial.