24. Solvability of equations by radicals and solvability of Galois groups

The goal of this lecture is to prove the following theorem:

**Theorem 24.1.** Let $F$ be a field of characteristic zero, $f(x) \in F[x]$ and $K$ a splitting field for $f(x)$ over $F$. Then the equation $f(x) = 0$ is solvable by radicals $\iff$ $\text{Gal}(K/F)$ is solvable.

Informally, the equation $f(x) = 0$ is solvable by radicals if the roots of $f(x)$ can be obtained from $F$ using four arithmetic operations and taking roots (of arbitrary degree). The formal definition of solvability by radicals will be given later.

24.1. Some preparations. We start with a simple observation:

**Observation 24.2.** Let $G$ be a finite group. Then $G$ is solvable if and only if $G$ has a chain of subgroups $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\}$ where $G_{i+1} \triangleleft G_i$ and $G_i/G_{i+1}$ is cyclic.

**Proof.** By a standard argument any finite group $G$ has a descending chain $\{G_i\}$ where $G_{i+1} \triangleleft G_i$ and each quotient $G_i/G_{i+1}$ simple. So, for each $i$ either

(i) $G_i/G_{i+1}$ is cyclic of prime order or

(ii) $G_i/G_{i+1}$ is non-abelian simple

If (i) occurs for all $i$, then each $G_i/G_{i+1}$ is solvable, so $G$ is solvable by Algebra-I. If (ii) occurs for some $i$, then $G_i/G_{i+1}$ is not solvable, whence $G$ is not solvable. $\square$

**Definition.** A finite extension $K/F$ is called cyclic if $K/F$ is Galois and $\text{Gal}(K/F)$ is cyclic.

The following is a slight reformulation of Kummer’s Theorem (Theorem 23.6).

**Theorem.** Let $F$ be a field containing primitive $n^{\text{th}}$ root of unity for some $n$, and let $K/F$ be a finite extension. The following are equivalent:

(a) $K/F$ is cyclic with $[K : F] \mid n$

(b) $K = F(\sqrt[n]{a})$ for some $a \in F$.

**Definition.** Let $F$ be a field of characteristic zero.
(a) Let $K/F$ be a finite extension. We will say that $K/F$ is a root extension if there is a chain of subfields $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ where for $0 \leq i \leq n - 1$ we have $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$ and $n_i \in \mathbb{N}$.

(b) Let $f(x) \in F[x]$. We say that the equation $f(x) = 0$ is solvable by radicals if a splitting field of $f(x)$ over $F$ is contained in some root extension of $F$.

**Lemma 24.3.** Assume that $M/F$ is a root extension and let $L$ be the Galois closure of $M$ over $F$. Then $L/F$ is also a root extension.

*Proof.* Exercise. The main idea is to use Problem 1(a) in HW#10 which asserts that $L$ is the compositum of all Galois conjugates of $K$. \qed

### 24.2. Proof of the Main Theorem.

**Proof of Theorem 24.1.** Proofs in both directions are fairly similar, so we will only do the forward direction. Thus we are given that there is a root extension $M/F$ s.t. $K \subseteq M$. Let $L$ be the Galois closure of $M$ over $F$. Then $F \subseteq K \subseteq L$ with $L/F$ and $K/F$ both Galois, so by Proposition 21.3 $\text{Gal}(K/F)$ is a quotient of $\text{Gal}(L/F)$. Thus, to prove that $\text{Gal}(K/F)$ is solvable,

it is enough to show that $\text{Gal}(L/F)$ is solvable.

By Lemma 24.3 $L$ is a root extension, so there exist subfields $F = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_s = L$ s.t. $L_{i+1} = L_i(\sqrt[n_i]{a_i})$ for some $a_i \in L_i$ and $n_i \in \mathbb{N}$.

**Easy case:** $F$ contains primitive $n_i$th root of unity for each $i$. Then by Kummer’s Theorem $L_{i+1}/L_i$ is cyclic (in particular, Galois). Let $G_i = \text{Gal}(L/L_i)$ and $G = \text{Gal}(L/F)$.

$$F = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_s = L$$

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_s = \{1\}$$

By Proposition 21.3 applied to the triple $L_i \subseteq L_{i+1} \subseteq L$ we get that $G_{i+1} \trianglelefteq G_i$ and $G_i/G_{i+1} \cong \text{Gal}(L_{i+1}/L_i)$ is cyclic. Thus by Observation 24.2 $G$ is solvable.

**General case:** Since $\text{char } F = 0$, for each $n \in \mathbb{N}$ the algebraic closure of $F$ contains primitive $n$th root of unity, call it $\zeta_n$ (choose one).

Let $E = F(\zeta_{n_1}, \ldots, \zeta_{n_s})$. The extension $E/F$ is Galois since the Galois conjugates of a root of unity are its powers. In fact, it is not hard to show that $E = F(\zeta_n)$, where $n = LCM(n_1, \ldots, n_s)$ and $\text{Gal}(E/F) \cong \mathbb{Z}_n^*$, so in particular $\text{Gal}(E/F)$ is abelian.
Since $E/F$ and $L/F$ are both Galois, by Problem 4 in HW#9 $EL/F$ is also Galois. Consider the chain of subfields

$$E = EL_0 \subseteq EL_1 \subseteq \ldots \subseteq EL_s = EL$$

Note that $EL_{i+1} = EL_i(\sqrt[n]{a_i})$. Since $EL_i$ contains $\zeta_{n_i}$, by Kummer’s theorem the extension $EL_{i+1}/EL_i$ is cyclic.

Applying the argument from the easy case to (***)) and using the fact that $EL/E$ is Galois (as $EL/F$ is Galois), we deduce that $\text{Gal}(EL/E)$ is solvable. Using Proposition 21.3 again, we get that

$$\text{Gal}(EL/E) \cong \frac{\text{Gal}(EL/F)}{\text{Gal}(E/F)}.$$ 

Since $\text{Gal}(E/F)$ is abelian (hence also solvable), we get that $\text{Gal}(EL/F)$ is solvable.

Finally (again by Proposition 21.3), $\text{Gal}(L/F)$ is a quotient of $\text{Gal}(EL/F)$, hence also solvable. \qed