Radical Extensions Are Solvable

Math 552

April 29, 2019

We start with this lemma, which is what we've done in the proof of the fact that the compositum of radical extensions are radical. [It's not exactly the same though.]

Lemma. *Let K_1/F and K_2/F be field extensions such that*

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = K_1$$

and

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = K_2$$

with F_i/F_{i-1} and E_j/E_{j-1} of type A. If $E_j = E_{j-1}[\beta_i]$, then let $F_{m+1} \stackrel{\text{def}}{=} F_m[\beta_1]$ and inductively, $F_{m+j} \stackrel{\text{def}}{=} F_{m+j-1}[\beta_j]$. Then

$$F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m \subseteq F_{m+1} \subseteq \cdots \subseteq F_{m+n} = K_1K_2,$$

with F_i/F_{i-1} type A for $i = 1, \ldots, m+n$.

Proof. Clearly $K_2 = F[\beta_1, \ldots, \beta_n]$, and since $F \subseteq K_1$, we have that $K_1K_2 = K_1[\beta_1, \ldots, \beta_n] = F_m[\beta_1, \ldots, \beta_n] = F_{m+n}$.

Now if β_j is a root of unity, we have then $F_{m+j}/F_{m+j-1} = F_{m+j-1}[\beta_j]/F_{m+j-1}$ is of type A.

If $\beta_j^{n_j} \in E_{j-1}$ for some n_j not divisible by the characteristic of F, then, as $E_{j-1} \subseteq F_{m+j-1}$, we have that F_{m+j}/F_{m+j-1} is of type A.

If $\beta_j^p - \beta_j \in E_{j-1}$, where $p = \text{char}(F)$, then since $E_{j-1} \subseteq F_{m+j-1}$, we have that F_{m+j}/F_{m+j-1} is of type A. $\square$

Now we can proof the main result.

Theorem. *If K/F is radical, then it is solvable.*

Proof. Since K/F is radical, there is a finite extension L/K such that we have a tower

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = L,$$

with F_i/F_{i-1} of type A. Then, for all $\sigma \in \mathrm{Emb}_{L/F}$ we have that $\sigma(F_i)/\sigma(F_{i-1})$ is also of type A [and same subtype, which is a simple exercise]. So, we have that

$$F = \sigma(F_0) \subseteq \sigma(F_1) \subseteq \cdots \subseteq \sigma(F_r) = \sigma(L),$$

and by the lemma, we have that the Galois closure of L/F, namely $L' \stackrel{\text{def}}{=} \prod_{\sigma \in \mathrm{Emb}_{L/F}} \sigma(L)$, has a tower

$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = L'$$

with L_i/L_{i-1} of type A.

Now, let m be the product of all n_i such that $L_i = L_{i-1}[\alpha_i]$ with $\alpha_i^{n_i} \in L_{i-1}$ and n_i not divisible by $\mathrm{char}(F)$ [i.e., L_i/L_{i-1} of type A(ii)]. Then, let ζ be a primitive m-th root of unity and $E \stackrel{\text{def}}{=} F[\zeta]$, $E_i \stackrel{\text{def}}{=} L_i[\zeta]$ for $i = 0, \ldots, s$, and $E_{-1} \stackrel{\text{def}}{=} F$.

We then have that E/F is abelian [and hence Galois], and since L'/F is also Galois, we have that $L'E/F$ is Galois. [Note that $L'E = L'[\zeta]$.]

Now, we have:

$$F = E_{-1} \subseteq E_0 \subseteq E_1 \subseteq \cdots \subseteq E_s = L'E.$$

Then, for $i \geq 1$ we have that E_i/E_{i-1} is of type A [and same subtype as L_i/L_{i-1}, although perhaps $E_i = E_{i-1}$], as $L_{i-1} \subseteq E_{i-1}$, and so is E_0/E_{-1}.

If E_i/E_{i-1} is of type A(i), then it is abelian, and if it is of type A(iii), then it is cyclic.

Now, if E_i/E_{i-1} is of type A(ii), then $E_i = E_{i-1}[\beta_i]$ with $\beta_i^{n_i} \in L_{i-1} \subseteq E_{i-1}$ [and $\mathrm{char}(F) \nmid n_i$]. By definition of m, we have that $n_i \mid m$ and this $\zeta^{m/n_i} \in E_0 \subseteq E_{i-1}$ is a primitive n_i-th root of unity and therefore [by previous theorem on cyclic extensions] we have that E_i/E_{i-1} is *cyclic*.

Therefore, we have that E_i/E_{i-1} is abelian for $i = 0, \ldots, s$. Using Galois correspondence [i.e., the *Fundamental Theorem of Galois Theory*] we get

$$G_s = 1 \leq G_{s-1} \leq G_{s-2} \leq \cdots \leq G_{-1} = \mathrm{Gal}(L'E/F),$$

where $G_i = \mathrm{Gal}(E_s/E_i)$.

Still by the *Fundamental Theorem of Galois Theory*, since E_i/E_{i-1} is abelian [and therefore Galois by definition], we have that $G_i \trianglelefteq G_{i-1}$ and $\mathrm{Gal}(E_i/E_{i-1}) \cong G_{i-1}/G_i$ is abelian, for $i = 0, \ldots, s$. Hence, $\mathrm{Gal}(L'E/F)$ is a solvable group.

Now, since $K \subseteq L \subseteq L' \subseteq L'E$, all finite extensions, and $L'E/F$ is Galois with solvable Galois group, we have that K/F is solvable. $\square$