16. Polynomials solvable by radicals (Chapter 18.3)

F - field

Definition 16.1. Let G be a group.
(1) G is called *simple* if the only normal subgroups of G are $\{e\}$ and G.
(2) A *composition series of G* is a sequence

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

of subgroups of G such that for $0 \le i \le n-1$
(i) G_i is a normal subgroup of G_{i+1},
(ii) $G_i \neq G_{i+1}$,
(iii) G_{i+1}/G_i is a simple group.

Although a composition series is not necessarily unique, if

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = G$$

is another composition series of G, then the Jordan-Hölder theorem asserts that $n=m$ and the sets $\{G_{i+1}/G_i\}$ and $\{H_{i+1}/H_i\}$ contain the same groups up to isomorphism. We call the groups G_{i+1}/G_i the *composition factors* of G.
(3) If G is finite, then G is called *solvable* if its composition factors are cyclic groups of prime order.

Example 16.2. (1) Finite abelian groups are solvable (exercise).
(2) Let G be a group and $H \triangleleft G$ a normal subgroup. Then G is solvable if and only if both H and G/H are solvable.
(3) S_n is solvable if and only if $n \le 4$. If $n \ge 5$, then S_n has a composition series $\{e\} \triangleleft A_n \triangleleft S_n$ and A_n is not abelian.
(4) Odd groups are solvable (Feit-Thompson theorem, 1963).

Definition 16.3. Let $F \subseteq E$ be a field extension.

(1) $F \subseteq E$ is called <u>pure</u> if $E = F(\alpha)$ with $\alpha^n \in F$ for some $r \geq 1$.
(2) $F \subseteq E$ is called <u>radical</u> if there is a sequence of extensions $F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = E$ where $E_i \subseteq E_{i+1}$ is pure. They for $1 \leq i \leq r$ we have $E_i = F(\alpha_1, \ldots, \alpha_i)$ and there exist $n_1, \ldots, n_r \geq 1$ such that $\alpha_i^{n_i} \in E_{i-1}$.

<u>Lemma 16.4.</u> Let F be a perfect field. Let
$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = E$$
be a radical extension of F. The there exists a radical extension
$$F = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_s = N$$
of F such that
(i) $E \subseteq N$,
(ii) $F \subseteq N$ is normal, and
(iii) N_i is the splitting field of a polynomial of the form $x^{m_i} - c_i \in N_{i-1}[x]$ for $1 \leq i \leq s$.

<u>Proof</u> For $1 \leq i \leq r$ we have $E_i = E_{i-1}(\alpha_i)$, and α_i is a root of $x^{n_i} - b_i \in E_{i-1}[x]$. Let $n = n_1 \cdots n_r$ and let w be a primitive n-th root of unity. We construct the required extension iteratively. First we construct a field K such that $E_1 \subseteq K$, $F \subseteq K$ is normal, and $F = k_0 \subseteq k_1 \subseteq k_2 = K$, with k_i being the splitting field of a polynomial of the form $x^{n_i} - c_i \in k_{i-1}[x]$. We have a radical extension
$$F = E_0 \subseteq E_0(w) \subseteq E_0(w, \alpha_1) = E_1(w)$$
and $F \subseteq F(w)$ is normal since $F(w)$ is the splitting field of $x^n - 1 \in F[x]$. Since F is perfect, $F \subseteq F(w)$ is Galois and so $E_{G(F(w)/F)} = F$. Set
$$f_1(x) = \prod_{\sigma \in G(F(w)/F)} (x^{n_1} - \sigma(b_1)) = (x - b_1)^{|G(F(w)/F)|} \in F[x], \quad g_1(x) := (x^n - 1) f_1(x) \in F[x].$$
Let K be the splitting field of $g_1(x)$. Then $F \subseteq K$ is normal and hence Galois. Moreover $\alpha_1 \in K$ and so $E_1 \subseteq K$. Finally, by setting k_1 := splitting field of $x^n - 1$ over F, k_2 := splitting field of $x^{n_1} - b_1$ over k_1

we obtain $F=K_0 \subsetneq K_1 \subseteq K_2 = K$ as required.
For the next step we construct a field K' such that $E_2 \subseteq K'$, $F \subseteq K'$ is normal, and $F = K_0' \subseteq K_1' \subseteq K_2' \subseteq \cdots \subseteq K_s' = K'$ with K_i' being the splitting field of a polynomial of the form $x^{m_i} - c_i \in K_{i-1}'[x]$. Set

$$f_2(x) := \prod_{\sigma \in G(K/F)} (x^{n_2} - \sigma(b_2)), \quad g_2(x) := g_1(x) f_2(x).$$

Since $F \subseteq K$ is Galois, $G(K/F) = \{\sigma_1, \dots, \sigma_k\}$ is finite. For any $\tau \in G(K/F)$ we have

$$\{\sigma_1, \dots, \sigma_k\} = \{\tau\sigma_1, \dots, \tau\sigma_k\}. \quad (*)$$

Hence for every $\tau \in G(K/F)$ we have

$$\tau(f(x)) = \tau\Big(\prod_{\sigma \in G(K/F)} (x^{n_2} - \sigma(b_2))\Big) = \prod_{\sigma \in G(K/F)} (x^{n_2} - \tau\sigma(b_2)) \overset{(*)}{=} \prod_{\sigma \in G(K/F)} (x^{n_2} - \sigma(b_2)) = f(x)$$

Hence the coefficients of $f(x)$ belong to $E_{G(K/F)} = F$ (since $F \subseteq K$ is Galois). Hence $f(x) \in F[x]$. Let K' be the splitting field of $g_2(x)$ over F. Then $F \subseteq K'$ is normal and hence Galois. Moreover $\alpha_2 \in K'$ and $E_1 \subseteq K \subseteq K'$ and so $E_2 = E_1(\alpha_2) \subseteq K'$. Finally, by setting $K_1' :=$ splitting field of $x^n - 1$ over F, $K_2' :=$ splitting field of $x^{n_2} - b_1$ over K_1', $K_3' :=$ splitting field of $x^{n_2} - \sigma_1(b_2)$ over K_2', $\dots$, $K_{k+2}' :=$ splitting field of $x^{n_2} - \sigma_k(b_2)$ over K_{k+1}' we obtain $F = K_0' \subseteq K_1' \subseteq K_2' \subseteq \cdots \subseteq K_{k+2}' = K'$ as required.
We continue like this and this construction terminates since r is finite. ∎

Definition 16.5 A polynomial $f(x) \in F[x]$ is *solvable by radicals* if its splitting field is contained in some radical extension of F.

By definition, $f(x) \in F[x]$ is solvable by radicals if and only if each root of f can be expressed using elements of F and a finite sequence of signs $+, -, \cdot, \div, \sqrt[n]{}$.