23. Kummer's theorem and Galois's criterion for radical extensions

We showed that, if we adjoin elements to a field by taking m-th roots, we will never leave the solvable fields. On this worksheet, we will prove a converse.

Here is the set up for problems 23.1 through 23.4: Let K be a field where $n \neq 0$ and let $\zeta \in K$ be a primitive n-th root of unity. Let L/K be a Galois extension with $\mathrm{Gal}(L/K) \cong C_n$ and let g generate $\mathrm{Gal}(L/K)$.

Problem 23.1. Show that, as a K-vector space, L splits up as $\bigoplus_{j=0}^{n-1} L_j$ where $L_j := \{x \in L : g(x) = \zeta^j x\}$.

Problem 23.2. With notation as in the previous problems, let $\alpha \in L_j$ and $\beta \in L_k$. Show that $\alpha\beta \in L_{j+k}$.

Problem 23.3. Suppose for the sake of contradiction that, for some j, we have $\dim L_j \geq 2$.
(1) Show that $L_0 \supsetneq K$.
(2) Deduce a contradiction, and conclude that $\dim L_j = 1$ for all $j \in \mathbb{Z}/n\mathbb{Z}$.

Problem 23.4. Let $\alpha \in L_1$ and put $\theta = \alpha^n$. Show that $L = K(\alpha) \cong K[x]/(x^n - \theta)K[x]$.

> **Theorem (Kummer's Theorem):** Let K be a field where $n \neq 0$ and suppose that K contains a primitive n-th root of unity. Let L/K be a Galois extension whose Galois group is cyclic of order n. Then $L = K(\theta^{1/n})$ for some $\theta \in K$.

Problem 23.5. Let L/F be a Galois extension with solvable Galois group of order N. Suppose that $N \neq 0$ in F and $x^N - 1$ splits in F. Show that there is a chain of subfields $F = K_0 \subset K_1 \subset \cdots \subset K_r = L$ where $K_{j+1} = K_j(\theta_j^{1/d_j})$ for some $\theta_j \in K_j$ and some d_j dividing N.

Problem 23.6. Let L/F be a Galois extension with solvable Galois group of order N. Suppose that $N \neq 0$ in F. Show that there is a chain of subfields $F \subseteq K_0 \subset K_1 \subset \cdots \subset K_r \supseteq L$ where $K_0 = F(\zeta_N)$ and $K_{j+1} = K_j(\theta_j^{1/d_j})$ for some $\theta_j \in K_j$ and some d_j dividing N. (See diagram below.) You have proved:

$$\begin{tikzcd}
 & & K_r = K_{r-1}(\theta_{r-1}^{1/d_{r-1}}) \arrow[d, dash] \\
 & & \vdots \arrow[d, dash] \\
 & & K_1 = K_0(\theta_0^{1/d_0}) \arrow[d, dash] \\
L \arrow[uuurr, dash] & & K_0 = F(\zeta_N) \\
 & F \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

> **Theorem (Galois's characterization of equations solvable by radicals):** Let θ be algebraic over $\mathbb{Q}$ and let L be the Galois closure of $\mathbb{Q}(\theta)$. There is a formula for θ using $+$, $-$, $\times$, $\div$, $\sqrt[d]{\ }$ if and only if $\mathrm{Gal}(L/\mathbb{Q})$ is solvable.

Finally, we apply this to study constructible numbers again:

Problem 23.7. Let F be a field of characteristic $\neq 2$. Let L/F be a Galois extension with Galois group of order 2^r. Show that there is a chain of fields $F = K_0 \subset K_1 \subset \cdots \subset K_r = L$ such that $K_{i+1} = K_i(\sqrt{\theta_i})$ for $\theta_i \in K_i$. You have proved:

> **Theorem:** Let θ be algebraic over $\mathbb{Q}$ and let L be the Galois closure of $\mathbb{Q}(\theta)$. There is a formula for θ using $+$, $-$, $\times$, $\div$, $\sqrt{\ }$ if and only if $\mathrm{Gal}(L/\mathbb{Q})$ is a 2-group.