28. KUMMER'S THEOREM AND GALOIS'S CRITERION FOR RADICAL EXTENSIONS

On the previous worksheet 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 28.1 through 28.4: 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 whose Galois group is cyclic of order n and let g generate $\mathrm{Gal}(L/K)$.

Problem 28.1. 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 28.2. Let $J \subseteq \mathbb{Z}/n\mathbb{Z}$ be $\{j : L_j \neq (0)\}$.

(1) Show that J is a subgroup of $\mathbb{Z}/n\mathbb{Z}$.
(2) Show that $J = \mathbb{Z}/n\mathbb{Z}$. (Hint: All subgroups of $\mathbb{Z}/n\mathbb{Z}$ are of the form $d\mathbb{Z}/n\mathbb{Z}$ for some divisor d of n. Think about $g^{n/d}$.)
(3) Show that $\dim_K L_j = 1$

Problem 28.3. 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 28.4. Let $\alpha \in L_1$ and put $\theta = \alpha^n$. Show that $L = K(\theta^{1/n})$.

You have now proved:

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 28.5. Let L/K be a ~~solvable extension~~ Galois extension with solvable Galois group of order N. Suppose that $N \neq 0$ in K and that K contains a primitive N-th root of unity. Show that there is a chain of subfields $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$ such that $K_{j+1} = K_j(\theta_j^{1/d_j})$ for some $\theta_j \in K_j$ and some d_j dividing N.

We are now ready to prove

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

We have already shown that, if a radical formula for θ exists, then $\mathrm{Gal}(K/\mathbb{Q})$ is solvable. We now prove the converse:

Problem 28.6. Let K be a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q})$ solvable of order N.

(1) Show that there is a solvable extension L of $\mathbb{Q}$ that contains both K and a primitive N-th root of unity.
(2) Finish the proof of Galois's criterion.