DUE DATE: MAR. 3, 2016

1. Suppose that $K$ is a field of characteristic zero, and $p(x) \in K[x]$ an irreducible polynomial of degree $d$ over $K$. Let $\alpha_1$, $\alpha_2$, $\ldots$, $\alpha_d$ be the roots of $p(x)$, and $L = K(\alpha_1, \ldots, \alpha_d)$ the field obtained by adjoining all the roots of $p(x)$.

Let $S$ be the set $S = \{\alpha_1, \ldots, \alpha_d\}$ of the roots.

(a) If $\sigma$ is an element of $\mathrm{Aut}(L/K)$ explain why, for any root $\alpha_i \in S$, $\sigma(\alpha_i) \in S$ too, so that the group $G = \mathrm{Aut}(L/K)$ acts on the set $S$.

(b) If $\sigma \in G$, and $\sigma(\alpha_i) = \alpha_i$ for $i = 1, \ldots, d$, explain why $\sigma$ is actually the identity map $\sigma : L \longrightarrow L$ on $L$.

(c) An action of a group $G$ on a set $S$ is the same as a homomorphism $G \longrightarrow \mathrm{Perm}(S)$ from $G$ to the group of permutations of $S$. Explain why the action from part (a) gives an *injective* homomorphism.

(d) Explain why the group $G$ acts *transitively* on $S$. [HINT: Lifting lemma!]

(e) Explain why $G$ can be realized as a subgroup of $S_d$, the symmetric group on $d$ elements, such that the subgroup acts transitively on the set $\{1, \ldots, d\}$.

2. Let $K = \mathbb{Q}$, and $\zeta = e^{2\pi i/7}$. By **H3** Q1, the minimal polynomial of $\zeta$ over $\mathbb{Q}$ is $q(x) = x^6 + x^5 + x^5 + x^3 + x^2 + x + 1 = \frac{x^7-1}{x-1}$.

(a) Show that all other roots of $q(x)$ are powers of $\zeta$, and explain why this shows that $L = \mathbb{Q}(\zeta)$ is the splitting field for $q(x)$.

(b) Let $G = \mathrm{Gal}(L/\mathbb{Q})$. For $\sigma \in G$, explain why $\sigma$ is completely determined by what it does to $\zeta$. (i.e., once you know what $\sigma(\zeta)$ is, you know how $\sigma$ acts on all of $L$.)

(c) Compute the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$. (Keeping in mind part (b) of this question, and part (d) of question 1 may help, but don't get hung up on it if it doesn't.)

(d) Describe the subgroups of $G$, and draw the corresponding diagram of intermediate fields between $\mathbb{Q}$ and $L$.

(e) Compute the Galois groups for the extensions $\mathbb{Q}(\cos(\frac{2\pi}{7}))/\mathbb{Q}$ and $\mathbb{Q}(i\sin(\frac{2\pi}{7}))/\mathbb{Q}$, where $i = \sqrt{-1}$. (NOTE: These are subfields of $L$.)

In the next two problems we will explore some further aspects of the Galois correspondence.

3. Recall that a group $G$ is a product $G = H_1 \times H_2$ if and only if there are *normal* subgroups $H_1 \subset G$ and $H_2 \subset G$ such that $H_1 \cap H_2 = \{e\}$ and $H_1 \cdot H_2$ (the subgroup generated by $H_1$ and $H_2$) is equal to $G$.

Suppose that $K \subseteq L$ is a finite Galois extension, and $M_1$ and $M_2$ are two intermediate fields such that:

1. Both $K \subseteq M_1$ and $K \subseteq M_2$ are Galois extensions.
2. $M_1 \cap M_2 = K$.
3. The smallest subfield of $L$ containing both $M_1$ and $M_2$ is $L$ itself.

(a) If $H_1$ and $H_2$ are the subgroups of $G = \mathrm{Aut}(L/K)$ corresponding to $M_1$ and $M_2$ under the Galois correspondence, show that $G = H_1 \times H_2$.

(b) Conversely, if the Galois group $G$ is a product $G = H_1 \times H_2$, then show that there are two intermediate fields $M_1$ and $M_2$ having properties (1)–(3) above.

(c) Consider again the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ and its intermediate fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. Use (a) to find the Galois group $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. (This justifies the claim about this Galois group from **H6** Q3.)

4. Suppose that $L/K$ is a Galois extension with Galois group $G$, and let $M_1 \subseteq M_2$ be intermediate fields, corresponding to subgroups $H_1$ and $H_2$ of $G$.

(a) What condition on $H_1$ and $H_2$ is equivalent to the condition that "$M_2/M_1$ is a Galois extension"?

(b) Given that this condition on groups holds, what is $\mathrm{Gal}(M_2/M_1)$, i.e., how do you compute $\mathrm{Gal}(M_2/M_1)$ from $H_1$ and $H_2$?