Homework Assignment # 8.

Plan for the next week: Galois correspondence (online lectures 20 and 21, Section 14.2 in DF), maybe start finite fields (online lecture 22, Section 14.3 in DF).

Problems, to be submitted by Thu, March 29th.

Problem 1: Prove the interesting part of Corollary 18.7 form online notes: if $K/L/F$ is a tower of algebraic extensions and K/L and L/F are separable, then K/F is separable (see online notes for a hint). Give a detailed argument.

Problem 2: Let p be a prime, $n \geq 2$ an integer, $f(x) = x^n - p$, and let $K \subset \mathbb{C}$ be the splitting field for $f(x)$ over $\mathbb{Q}$. Recall that $K = \mathbb{Q}(\sqrt[n]{p}, \omega_n)$ where $\omega_n = e^{2\pi i/n}$.

(a) Describe the elements of $\mathrm{Gal}\,(K/\mathbb{Q})$ by their actions on $\sqrt[n]{p}$ and ω_n.

(b) Let $G = \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ where $(\mathbb{Z}/n\mathbb{Z})^\times$ acts on $\mathbb{Z}/n\mathbb{Z}$ by multiplication. Prove that $\mathrm{Gal}\,(K/\mathbb{Q})$ is isomorphic to a subgroup of G and describe an explicit embedding.

(c) (optional) Under which conditions on n and p is this embedding an isomorphism? You are not asked for necessary and sufficient conditions; just the most general sufficient conditions that you can justify.

Problem 3: Let F be a field, let $f(x) \in F[x]$ be an irreducible (over F) separable polynomial of degree n, and let K be a splitting field of $f(x)$.

(a) Prove that $|\mathrm{Gal}\,(K/F)|$ is a multiple of n and divides $n!$

(b) Let $n = 3$. Prove that $\mathrm{Gal}\,(K/F)$ is isomorphic to either $\mathbb{Z}/3\mathbb{Z}$ or S_3.

(c) Let $n = 4$ and assume that $|\mathrm{Gal}\,(K/F)| = 8$. Determine the isomorphism class of $\mathrm{Gal}\,(K/F)$.

Problem 4: Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n, and let K be a splitting field of $f(x)$. Label the roots of $f(x)$ by $1, \ldots, n$ (in some order), and let $\iota : \mathrm{Gal}\,(K/\mathbb{Q}) \to S_n$ be the associated embedding.

(a) Assume $f(x)$ has at least one non-real root. Prove that the complex conjugation is an element of $\mathrm{Gal}\,(K/\mathbb{Q})$ of order 2.

(b) Assume that $f(x)$ has precisely two non-real roots. Prove that the image of the complex conjugation under the embedding ι is a transposition.

(c) Suppose that $n = \deg(f)$ is prime and again assume that $f(x)$ has precisely two non-real roots. Prove that $\mathrm{Gal}\,(K/\mathbb{Q})$ is isomorphic to S_n. **Hint:** $\mathrm{Gal}\,(K/\mathbb{Q})$ must contain an element of order n (why?)

Problem 5: The main goal of this problem is to give a slightly different solution to Problem 4(c) in HW#6. So, let $S = \{n_1, \ldots, n_k\}$ be a finite set of positive integers ≥ 2 and $K = \mathbb{Q}(\sqrt{n_1}, \ldots, \sqrt{n_k})$.

(a) Prove that there exists a subset T of S such that the set $P(T) = \{1\} \cup \{\sqrt{n} : n \text{ is a product of distinct elements of } T\}$ is a basis for $K/\mathbb{Q}$.

(b) Let T be as in (a). Let $\alpha \in K$ be such that $\sigma(\alpha) = \pm\alpha$ for every $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q})$. Prove that $\alpha = q\beta$ for some $\beta \in T$ and $q \in \mathbb{Q}$.

(c) Assume now that $n_1, \ldots, n_k$ are pairwise relatively prime and none of them is a square. Use (b) to give a short proof of the fact that $[K : \mathbb{Q}] = 2^k$.