Homework Assignment # 9.

Plan for the next week: Finite fields (online lecture 22, the end of 13.5 and 14.3 in DF), cyclic Galois extensions (online lecture 23, Section 6.6 in Lang) and Solvability of equation by radicals (briefly, online lecture 24, 14.7 in DF)

Problems, to be submitted by Thu, April 5th.

Problem 1: Let $K \subset \mathbb{C}$ be the splitting field of $f(x) = x^4 - 2$ over $\mathbb{Q}$.

(a) Choose an order on the set of roots of $x^4 - 2$ and describe the associated embedding of $\mathrm{Gal}(K/\mathbb{Q})$ to S_4.

(b) Describe all subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and the corresponding subfields of K.

Problem 2 (practice): DF, Problem 6 on page 582.

Problem 3: Let p and q be distinct primes with $q > p$, and let K/F be a Galois extension of degree pq. Prove that

(a) There exists a field L with $F \subseteq L \subseteq K$ and $[L : F] = q$

(b) There exists a unique field M with $F \subseteq M \subseteq K$ and $[M : F] = p$.

Problem 4: Let p be an odd prime, $\omega = e^{2\pi i/p}$, $K = \mathbb{Q}(\omega)$ and L the unique subfield of K with $[L : \mathbb{Q}] = 2$. As we proved in class, if we let b be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\zeta = \sum_{i=0}^{(p-3)/2} \omega^{b^{2i}}$, then $L = \mathbb{Q}(\zeta)$.

(a) Prove by direct computation that if $p = 5$, then $L = \mathbb{Q}(\sqrt{5})$.

(b) Let S be the set of all elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ representable as squares. Prove that $\zeta = \sum_{s \in S} \omega^s$.

(c) Prove that $-1 \in S$ if and only if $p \equiv 1 \mod 4$

(d) Prove that $\overline{\zeta} = \zeta$ if $p \equiv 1 \mod 4$ and $\overline{\zeta} = -1 - \zeta$ if $p \equiv 3 \mod 4$. Deduce that $L \subset \mathbb{R}$ if and only if $p \equiv 1 \mod 4$.

(e) Let M be the unique subfield of K with $[K : M] = 2$. As proved in class, $M \subset \mathbb{R}$. Now prove that $L \subset \mathbb{R}$ if and only if $p \equiv 1 \mod 4$ just by using this fact and Galois correspondence (do not use an explicit description of L). **Hint:** What is the relationship between the subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ corresponding to L and M depending on p mod 4?

Problem 5: Read (and think about) DF, Problem 17 on pages 582-583. This problem will likely be included in Homework #10.

Problem 6: Let K/F and L/F be Galois extensions.

(a) Prove that the extension KL/F is also Galois and there is a natural embedding $\iota : \text{Gal}\,(KL/F) \to \text{Gal}\,(K/F) \times \text{Gal}\,(L/F)$.

(b) Assume now that K/F and L/F are both finite. Prove that the map ι in (a) is an isomorphism if and only if $K \cap L = F$.

Problem 7: Before doing this problem, read the first half of Section 14.4 in DF (pp. 591-593).

Definition 1: Let L/F be a finite separable extension and let $\overline{F}$ be an algebraic closure of F containing L. A subfield L' of $\overline{F}$ is called **conjugate to** L **over** F if $L' = \sigma(L)$ for some F-embedding of σ into $\overline{F}$. Note that L/F is Galois if and only if L does not have any F-conjugates besides L itself.

Definition 2: A finite extension K/F is called a p**-extension** if K/F is Galois and $Gal(K/F)$ is a p-group.

(a) Let L/F be a separable extension of degree n, and let K be the Galois closure of L over F. Prove that K can be written as a compositum $L_1 L_2 \ldots L_n$ where $L_1, \ldots L_n$ are (not necessarily distinct) conjugates of L over F.

(b) Let K/F and L/F be finite p-extensions. Prove that KL/F is also a p-extension.