Homework Assignment # 9

Plan for the week of Apr 5: On Tuesday we will talk about Galois groups of finite fields (see pages 2 and 3 of online lecture 22, Section 14.3 in DF) and Galois correspondence for cyclotomic fields (Section 14.5 in DF). On Thursday we will talk about cyclic Galois extensions (online lecture 23, beginning of 14.7 in DF).

Here and in all future assignments "online" or "online notes" refers to Algebra-II lectures posted on my Spring 2010 Algebra-II webpage

`http://people.virginia.edu/~mve2x/7752_Spring2010/`

Problems, due by 11:59pm on Friday, April 9th.

Problem 0: Read online Lecture 21 (there are some theorems and examples there which we have not discussed in class and which are relevant to this homework). Also read the last part of Lecture 15 notes posted on collab, starting with "Another proof that $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$".

Problem 1: 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 (this generalizes the result of HW#8.4(c) from $n = 3$ to arbitrary prime n). **Hint:** $\mathrm{Gal}(K/\mathbb{Q})$ must contain an element of order n (why?)

Problem 2: 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 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: DF, Problem 17 on pages 582-583.

Problem 5: 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 $\iota : \mathrm{Gal}(KL/F) \to \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$.

(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 6: 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 (see p. 594 in DF or the end of online Lecture 18 for the definition). 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.

(c) Suppose K/L and L/F are both p-extensions, and let M be the Galois closure of K over F (note: we do not know whether K/F is Galois or not). Prove that M/F is also a p-extension. **Hint:** first use (b) to show that M/L is a p-extension.

(d) Now assume only that L/F is a separable extension with $[L : F]$ a power of p, and let M be the Galois closure of L over F. Prove that $[M : F]$ need not be a power of p.