Homework 8 : Due Wednesday, April 20

Discussion: Let $p_1, p_2, \ldots, p_n$ be distinct prime numbers and let

$$F = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$$

It is natural to believe that $[F : \mathbb{Q}] = 2^n$ and to guess at the potential 2^n many elements of $Gal_{\mathbb{Q}}F$. However, it is far from obvious that things work out so nicely. Is $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$? If it so happened that $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$ and so $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$ would have only 4 elements rather than the 8 you might expect (because if you know what an automorphism does to $\sqrt{2}$ and $\sqrt{3}$, then what it does to $\sqrt{5}$ would be determined). Since $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, we have $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ if and only if $\sqrt{5}$ is a $\mathbb{Q}$-linear combination of $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. You probably believe that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$, but a direct attack would involve writing out an arbitrary such combination and performing some tedious calculations.

Even if you succeed in showing that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ directly through algebraic manipulations, then at the next step you would consider whether $\sqrt{7}$ is a $\mathbb{Q}$-linear combination of $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$. As you can see, this gets out of hand quite rapidly. Although it is possible to make very clever use of elementary tools to solve this problem, we will use Galois theory to show that everything works as you might expect, and also to obtain significantly more information.

Problem 1: Let F be as above.
a. Show that $\mathbb{Q} \prec F$ is a Galois extension.
b. Show that $[F : \mathbb{Q}] = 2^m$ for some m with $0 \leq m \leq n$.
c. Show that $\sigma^2 = id_F$ for all $\sigma \in Gal_{\mathbb{Q}}F$.
d. Show that if a group H has the property that $a^2 = e$ for all $a \in H$, then H is abelian.
e. Conclude that $Gal_{\mathbb{Q}}F$ is an abelian group with $|Gal_{\mathbb{Q}}F| = 2^m$.

Our first major goal is to prove that $m = n$. To do this, we will use the Galois Correspondence to count (or at least bound) the number of fields E with $\mathbb{Q} \prec E \prec F$ satisfying $[E : \mathbb{Q}] = 2$, and compare it to the number of subgroups of $Gal_{\mathbb{Q}}F$ of index 2. We begin with the former.

Problem 2: Let F be as above.
a. Recall that an integer d is squarefree if it is not divisible by p^2 for any prime p. Show that if $c, d \in \mathbb{Z}$ are distinct squarefree numbers with $c, d \geq 2$, then $\mathbb{Q}(\sqrt{c}) \neq \mathbb{Q}(\sqrt{d})$.
b. Show that there exists at least $2^n - 1$ many intermediate fields $\mathbb{Q} \prec E \prec F$ with $[E : \mathbb{Q}] = 2$.

Interlude: Suppose that G is a finite abelian group with the property that every nonidentity element of G has order a fixed prime p. We can view G as a vector space over $\mathbb{Z}/p\mathbb{Z}$ by defining scalar multiplication as $\overline{k} \cdot a = a + a + \cdots + a$ (k times) and noting that this is well-defined because $|a| \in \{1, p\}$. Since scalar multiplication is just repeated addition, it follows that a subset $H \subseteq G$ is a subgroup of G exactly when H is a subspace of G. Furthermore, a mapping from G to another vector space over $\mathbb{Z}/p\mathbb{Z}$ is a group homomorphism exactly when it is a linear transformation.

The reason why it is useful to view G as a vector space space over $\mathbb{Z}/p\mathbb{Z}$ rather than just as an abelian group is because we can use linear algebra. Viewing G as a vector space over $\mathbb{Z}/p\mathbb{Z}$, it follows that G has a basis, say $B = \{b_1, b_2, \ldots, b_k\}$. Using this basis, we conclude that $|G| = p^k$ and in fact $G \cong (\mathbb{Z}/p\mathbb{Z})^k$, where the isomorphism is as vector spaces over $\mathbb{Z}/p\mathbb{Z}$. This implies that $G \cong (\mathbb{Z}/p\mathbb{Z})^k$ as groups as well.

Applying this in our case of $Gal_{\mathbb{Q}}F$ with $p = 2$, we can use Problem 1 to deduce that $k = m$ (because $|(\mathbb{Z}/2\mathbb{Z})^k| = 2^k$ and $2^k = 2^m$ implies $k = m$), hence $Gal_{\mathbb{Q}}F \cong (\mathbb{Z}/2\mathbb{Z})^m$. As mentioned above, we want to think about the number of subgroups of $(\mathbb{Z}/2\mathbb{Z})^m$ of index 2. Now a subgroup of $(\mathbb{Z}/2\mathbb{Z})^m$ has index 2 exactly when it is 2^{m-1} many elements, which is exactly when it is a subspace of dimension $m-1$. We need to count the number of such subspaces, and we do this by examining bases. Every subspace of dimension $m-1$ has a basis of size $m-1$, but there are many such choices so we need to deal with the overcounting.

Problem 3: Let V be a vector space over $\mathbb{Z}/2\mathbb{Z}$ of dimension m.
a. Find the number of $(m-1)$-tuples $(b_1, b_2, \ldots, b_{m-1})$ such that $\{b_1, b_2, \ldots, b_{m-1}\}$ is linearly independent.
b. Suppose that H is a subspace of V of dimension $m-1$. Find the number of $(m-1)$-tuples $(b_1, b_2, \ldots, b_{m-1})$ such that $\{b_1, b_2, \ldots, b_{m-1}\}$ is a basis for H.
c. Prove that there are exactly $2^m - 1$ many subspaces of V of dimension $m-1$.

We are now ready to put all of the pieces together.

Problem 4: Let F be as above.
a. Show that $m = n$, so $|Gal_{\mathbb{Q}}F| = 2^n$ and in fact $Gal_{\mathbb{Q}}F \cong (\mathbb{Z}/2\mathbb{Z})^n$.
b. Show that $\sqrt{p_{i+1}} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_i})$ for all i.
c. Describe the elements of $Gal_{\mathbb{Q}}F$, and explain how you know that they are all automorphisms.
d. Show that $F = \mathbb{Q}(\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n})$.

Problem 5: Let $d_1, d_2, \ldots, d_n \in \mathbb{N}^+$ be distinct squarefree numbers. Show that $\{\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n}\}$ is linearly independent over $\mathbb{Q}$.