Homework 10, Math 702 – Frank Thorne (thorne@math.sc.edu)

You are welcome and encouraged to collaborate, but please write up your own solutions.
Due Monday, March 26, 2018.

1. Let K be the splitting field of $x^p - 2$ over $\mathbb{Q}$, for p an odd prime. Compute:
   (a) The degree $[K : \mathbb{Q}]$;
   (b) The Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Describe this as an abstract group as succinctly as possible, and also describe the group elements explicitly as automorphisms of K.
   (c) The corresponding lattices of subfields of K and subgroups of $\mathrm{Gal}(K/\mathbb{Q})$. Which subfields of K are Galois over $\mathbb{Q}$?

2. Same problem, where K is the splitting field of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$.

3. Same problem, where $K = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$. In addition, determine a polynomial over $\mathbb{Q}$ for which K is the splitting field.

4. Suppose that F is any field of characteristic $\neq 2$, and that K/F is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4-group. Prove that K/F is a *biquadratic extension* of the form $K = F(\sqrt{D}, \sqrt{D'})$ where $D, D' \in F$ and none of D, D', or DD' is a square in F.

   (Note: The choices of D and D' will not be uniquely determined.)

5. (Bonus.)
   (a) Let K/F be a cyclic extension of degree n (i.e., a Galois extension whose Galois group is cyclic), with Galois group generated by σ.
   The **norm** of an element $\alpha \in F$ is defined to be
   $$N_{K/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha).$$
   Suppose that $N_{K/F}(\alpha) = 1$. Prove **Hilbert's Theorem 90**: α is of the form $\frac{\beta}{\sigma\beta}$ for some $\beta \in K$.
   Possible hint. Take β of the form
   $$\beta = \theta + \alpha\sigma(\theta) + (\alpha\sigma\alpha)\sigma^2(\theta) + \cdots + (\alpha\sigma\alpha \ldots \sigma^{n-2}\alpha)\sigma^{n-1}(\theta)$$
   for some $\theta \in K$. (Why can this be assumed to be nonzero.........?)
   (b) Applying Hilbert's Theorem 90 to the extension $\mathbb{Q}(i)/\mathbb{Q}$, prove that the rational solutions to $a^2 + b^2 = 1$ can be taken of the form
   $$a = \frac{s^2 - t^2}{s^2 + t^2}, \quad b = \frac{2st}{s^2 + t^2}$$
   for some $s, t \in \mathbb{Q}$. Deduce a parametrization of the side lengths of all right triangles with integer side lengths.
   (c) Continuing the previous solution, suppose that $D \in \mathbb{Z}$ is not a perfect square. Determine all rational solutions to the equation $a^2 + Db^2 = 1$.