**Algebraic number theory (Spring 2013), Homework 6**

Frank Thorne, thorne@math.sc.edu

**Due Friday, April 19**

Recall that starred (*) exercises may involve background beyond what is assumed in this course.

1. (5 points) Prove that any finite subgroup of the unit circle is cyclic.
2. (5 points) Determine the unit group $\mathcal{O}_K^\times$ for all imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$.
3. (7 points) Determine the fundamental unit in $\mathbb{Q}(\sqrt{D})$ for each positive $D \leq 10$.
4. (5 points) Compute the Galois group of $\mathbb{Q}(\zeta_8)$, and find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_8)$.
5. (5 points) Compute the Galois group of $\mathbb{Q}(\zeta_{11})$, and find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{11})$.
6. (3 points) Describe explicitly the splitting of all primes in the extension $\mathbb{Q}(\zeta_{11})$.
7. (12 points) Let $f(x)$ be a cubic polynomial such that the splitting field $K$ of $f(x)$ over $\mathbb{Q}$ has degree 6.

   Enumerate all possible splitting types of primes in $K$. There will *not* be that many. You should find examples for all splitting types you claim can occur, and prove that other splitting types can't occur.
8. (20 points) Let $m$ and $n$ be distinct squarefree integers not equal to 1.

   (a) Prove that $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is Galois over $\mathbb{Q}$ with Galois group $\mathbb{Z}/2 \times \mathbb{Z}/2$. Does this field have any quadratic subfields other than $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{n})$?

   (b) Suppose $p$ ramifies in both $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{n})$. What happens in $K$? Find an example.

   (c) Suppose $p$ splits in both of these fields. What happens in $K$? Find an example.

   (d) Suppose $p$ is inert in both of these fields. What happens in $K$? Find an example.

   (e) Suppose the splitting behavior of $p$ is different in both of these fields. What happens in $K$? Find an example.

   (f) (*David Zureick-Brown's favorite algebraic number theory problem*) Does there exist an irreducible polynomial which is reducible mod every prime?