Math 536 Homework 10
Spring 2008
Due: Friday, April 11

1. Let F be a field of characteristic $\neq 2$.

   (a) Let E be a quadratic extension of F (i.e., $[E : F] = 2$). Show that

   $$S(E) = \{a \in F^* : a \text{ is a square in } E\}$$

   is a subgroup of F^* containing F^{*2} .

   (b) Let E and E' be quadratic extensions of F. Show that there is an F -isomorphism $\phi : E \to E'$ if and only if $S(E) = S(E')$.

   (c) Show that there is an infinite sequence of fields $E_1, E_2, \ldots$ with E_i a quadratic extension of $\mathbb{Q}$ for $i = 1, 2, \ldots$ and such that E_i is not isomorphic to E_j for $i \neq j$.

   (d) Let p be an odd prime. Use part (b) to show that, up to isomorphism, there is exactly one field with p^2 elements.

2. For any prime p, show that $X^p - X - 1$ is irreducible in $\mathbb{Q}[X]$.

3. Construct a splitting field for $X^5 - 2$ over $\mathbb{Q}$. What is its degree over $\mathbb{Q}$?

4. Find a splitting field of $X^{p^m} - 1 \in \mathbb{F}_p[X]$. What is its degree over $\mathbb{F}_p$?

5. (a) Let F be a finite field of characteristic p. Show that the cardinality of F, $|F|$, is a power of p, $|F| = q = p^m$ for some integer $m \geq 1$.

   (b) Show that F is a splitting field for $f(X) = X^q - X$.

   (c) Show that any other finite field with $q = p^m$ elements is isomorphic to F.

6. Let $f(X)$ be an irreducible polynomial in $F[X]$, where F has characteristic $p > 0$. Show that $f(X)$ can be written as $f(X) = g(X^{p^e})$ where $g(X)$ is irreducible and separable. Deduce that every root of $f(X)$ has the same multiplicity p^e in any splitting field.

7. Read the part of section IX.5 on constructions with straightedge and compass (in Knapp) that explains why it is impossible to *double a cube* with straightedge and compass. (This is described on pages 464 – 467.)