Finite Fields

We have seen the following:
Definition: For a polynomial f over a field K, the splitting field of f over K is an extension $L : K$ such that f splits over L but not over any proper subfield of L containing K.
Theorem: A splitting field of f over K exists and is unique up to isomorphism. It has degree at most $n!$ where $n = \deg(f)$.

We will prove the following:
Theorem: For every prime number p and an integer $n \geq 1$, there exists a finite field of cardinality p^n, and it is unique up to isomorphism.

1. (Uniqueness) Let K be a finite field. Prove the following.

   (a) $|K| = p^n$ for some prime number p and an integer $n \geq 1$.

   (b) K is a splitting field of $x^{p^n} - x$.

   Conclude that any two finite fields with the same number of elements are isomorphic.

2. (Existence) Let p be a prime number and n be an integer ≥ 1. Let L be a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. Let $K = \{a \in L : a^{p^n} = a\}$.

   (a) Show that $|K| = p^n$.

   (b) Show that K is a field. (So, in fact, $K = L$.)

Next we will prove the following.
Theorem: Any finite subgroup of the multiplicative group of units in a field is cyclic.

The easiest proof uses the *structure theorem for finite abelian groups*, which we will prove later in the semester.

3. Let G be a finite subgroup of K^*, the multiplicative group of units in a field K. The structure theorem says that $G \cong C_{n_1} \times \cdots \times C_{n_r}$ for some natural numbers $n_1, \ldots, n_r$, where C_n denotes the cyclic group of order n.
   Prove that $\gcd(n_i, n_j) = 1$ for any $i \neq j$. Conclude that G is cyclic.