HW #1, DUE 1-13

MATH 505A

1. Let F be a finite field. Show that F has the structure of a finite-dimensional vector space over $\mathbb{Z}_p$ for some prime p and deduce that the order of F is p^n for some positive integer n.

2. Continuing, show that F is the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$.

3. Conversely, let p^n be a power of a prime p. We know that the map sending x to x^p defines a field homomorphism from any field K of characteristic p to itself. Use this to show that the set S of roots of the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$ inside the splitting field F_n of this polynomial over $\mathbb{Z}_p$ itself forms a field, so that $S = F_n$. Show also that all roots of this polynomial are distinct. Finally, show that the Galois group of F_n over $\mathbb{Z}_p$ is cyclic of order n.

4. Now we know for every prime power p^n there is a unique field F_n up to isomorphism of order p^n. Using the classification of finite abelian groups from last quarter, show that the multiplicative group F_n^* of F_n is cyclic.

5. Deduce for any positive integer m that there is an irreducible monic polynomial of degree m over F_n.