Let $p \in \mathbb{P}$ throughout this problem set. Let $n \in \mathbb{N}$. We will write $\mathbb{F}_{p^n}$ for the finite field of $p^n$ elements constructed in Theorem 21 in the lectures.

1. The following are to be performed only with a straightedge and a compass. Prove your answers.
   (a) Is it possible to trisect an angle of $90^\circ$?
   (b) Is it possible to construct a square whose area equals that of a circle of unit radius?
   (c) Is it possible to construct the roots of $ax^2 + bx + c$ where $a, b, c$ are constructible numbers?

2. Show that if $E$ is a finite field, then $E \cong \mathbb{F}_{p^n}$ for some $p \in \mathbb{P}$ and $n \in \mathbb{N}$.

3. Let $\alpha$ and $\beta \in \mathbb{F}_2$ be zeroes of $x^3 + x^2 + 1$ and $x^3 + x + 1 \in \mathbb{F}_2[x]$ respectively. Show that $\mathbb{F}_2(\alpha) = \mathbb{F}_2(\beta)$.

4. Show that every irreducible polynomial in $\mathbb{F}_p$ is a divisor of $x^{p^n} - x$ for some $n \in \mathbb{N}$.

5. Let $K$ be a field, not necessarily finite. Show that if $G$ is any finite multiplicative subgroup of the multiplicative group $K^\times$, then $G$ is cyclic. In particular, this shows that $\mathbb{F}_{p^n}^\times$ is cyclic. [Hint: use the Fundamental Theorem of Finitely Generated Abelian Group from Math 113.]

6. Let $K$ be a field, not necessarily finite. Let $\text{char}(K) = p \neq 0$.
   (a) Show that the set $K^p = \{\alpha^p \mid \alpha \in K\}$ is a subfield of $K$.
   (b) Let $K^p \leq L \leq K$. Show that if $[L : K^p] < \infty$, then $[L : K^p] = p^n$ for some $n \in \mathbb{N}$.

Date: April 25, 2009 (Version 1.1); due: May 1, 2009.