Homework #6

Throughout the following, q is a power of the prime number p, $\mathbb{F}_q$ denotes a field with q elements, and $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$.

1. (a) Let $1 \leq j \leq p-1$. Show that p divides the binomial coefficient $\binom{p}{j}$, and therefore $\binom{p}{j} = 0$ in $\mathbb{F}_q$.
(b) Show that if $x, y \in \overline{\mathbb{F}}_q$ and $n \geq 1$, then $(x+y)^{q^n} = x^{q^n} + y^{q^n}$.

2. Show that the polynomial $X^{q^n} - X$ has q^n distinct roots in $\overline{\mathbb{F}}_q$.

3. Show that $\{\, x \in \overline{\mathbb{F}}_q \,|\, x^{q^n} = x \,\}$ is a field with q^n elements.

4. (a) Let $F \subset \overline{\mathbb{F}}_q$ be a field with q^n elements and let $F^\times$ denote the nonzero elements of F. Show that $x^{q^n - 1} = 1$ for all $x \in F^\times$.
(b) Show that $F \subseteq \{\, x \in \overline{\mathbb{F}}_q \,|\, x^{q^n} = x \,\}$, hence these sets are equal since they have the same cardinality.
(c) Show that for each $n \geq 1$, there is exactly one subfield of $\overline{\mathbb{F}}_q$ with q^n elements. We'll denote it by $\mathbb{F}_{q^n}$.

5. (a) $\mathbb{F}_{q^n}^\times$ is cyclic. Why?
(b) Show that there exists $\alpha \in \mathbb{F}_{q^n}$ such that $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. (This is a special case of the *Primitive Element Theorem.*)
(c) Let $n \geq 1$. Show that there is an irreducible polynomial $f(X) \in \mathbb{F}_q[X]$ of degree n.

6. (a) Let σ be a field automorphism of $\overline{\mathbb{F}}_q$. Show that $\sigma(\mathbb{F}_{q^n}) = \mathbb{F}_{q^n}$. (*Hint:* use problem 3.) (This part says that the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is *normal.*)
(b) Let $\phi(x) = x^q$ for all $x \in \mathbb{F}_{q^n}$. Show that ϕ is a field automorphism of $\mathbb{F}_{q^n}$. (*Remark:* ϕ is called the *Frobenius* map.)
(c) Show that ϕ has order n in the group of automorphisms of $\mathbb{F}_{q^n}$.
(d) Let $d|n$. Show that $x \in \mathbb{F}_{q^d}$ if and only if $\phi^d(x) = x$. (This is a special case of the Galois correspondence between subfields and subgroups, since ϕ^d fixes x if and only if the subgroup generated by ϕ^d fixes x.)