Homework 9 **Math 5591H**

Due by Tuesday, April 2

A1. Let L/F be an extension and let $f \in F[x]$.

(a) If K is a spitting field of f over F and $K \supseteq L$, prove that K is a splitting field of f over L.

(b) Give an example where K is a splitting field of f over L, but is not a splitting field of f over F.

A2. Let F be a field of characteristic p and let $f \in F[x]$ be irreducible.

(a) Prove that $f(x) = g(x^{p^k})$ for some separable irreducible $g \in F[x]$ and some integer $k \geq 0$.

(b) Prove that in its splitting field, $f(x) = c(x - \alpha_1)^{p^k} \cdots (x - \alpha_d)^{p^k}$ for some distinct $\alpha_1, \ldots, \alpha_d$.

13.5.5. Let p be a prime integer, let $a \in \mathbb{F}_p$, $a \neq 0$, and let $f = x^p - x + a \in \mathbb{F}_p[x]$. Prove that the splitting field K of f is obtained by adjoining a single root of f. Prove that f is separable and irreducible over $\mathbb{F}_p$. (*Hint:* Show that if α is a root of f, then $\alpha + b$ is a root of f for every $b \in \mathbb{F}_p$. Deduce that f has p roots. To prove that f is irreducible, show that for every root α' of f there is an automorphism of $K/\mathbb{F}_p$ that maps α to α' and so, $m_{\alpha'} = m_\alpha$.)

A3. (a) Let $n = p^r m$ where p is prime and $p \nmid m$. Prove that $\Phi_n(x) = \Phi_{pm}(x^{p^{r-1}})$. (*Hint:* You may use induction and the formula that expresses Φ_n in terms of Φ_d with $d \mid n$, or you may just compare the roots of the polynomials $\Phi_n(x)$ and $\Phi_{pm}(x^{p^{r-1}})$.)

(b) Deduce that if $n = p_1^{r_1} \cdots p_k^{r_k}$ is the prime factorization of n, then $\Phi_n(x) = \Phi_d(x^q)$, where $d = p_1 \cdots p_k$ and $q = p_1^{r_1 - 1} \cdots p_k^{r_k - 1}$.

13.6.10. Let ϕ denote the Frobenius automorphism of $\mathbb{F}_{p^n}$, $\phi(\alpha) = \alpha^p$. Prove that the order of ϕ (as an element of the group of automorphisms of $\mathbb{F}_{p^n}$) is n.

14.3.4. Construct the field $\mathbb{F}_{16}$ and find a generator of its multiplicative group.

A4. (a) Find all irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$.

(b) Determine the number of irreducible polynomials of degree 4 in $\mathbb{F}_3[x]$.