Math 210B Homework 8

Question 1. Let E/F be an algebraic extension. Recall that the set of all elements in E which are separable over F is a subfield of E containing F, called the *maximal separable subextension* in E/F. In characteristic zero, this coincides with E itself.

On the other hand, in characteristic $p > 0$, an element $a \in E$ is called *purely inseparable* over F if $a^{p^n} \in F$ for some $n \geq 0$. A finite extension E/F is called *purely inseparable* if all elements in E are purely inseparable over F.

(a) Show that if $a \in E$ is separable and purely inseparable over F, then $a \in F$.

(b) Show that a finite extension E of F is purely inseparable over the maximal separable subextension in E/F. That is, any algebraic extension E/F decomposes as E/L and L/F with E/L purely inseparable and L/F separable.

Question 2.

(a) Show that any finite extension of a finite field is normal.

(b) Show that any finite extension of a finite field is separable.

Question 3. Show that in a finite field F with q elements, every $x \in F$ is a root of $X^q = X$. ("Recall by anticipation" that any finite subgroup of the units $F^\times$ of a field must be cyclic.)

Question 4. Let p be a prime number and $n \geq 1$. Let $q = p^n$. Fix $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$. Let $\mathbb{F}_q$ be the set of roots of the polynomial $T^q - T$ in $\overline{\mathbb{F}}_p$.

(a) Compute the derivative of the polynomial $T^q - T \in \mathbb{F}_p[T]$.

(b) Show that $\mathbb{F}_q$ has exactly q elements.

(c) Show that $\mathbb{F}_q$ is a subfield of $\overline{\mathbb{F}}_p$. [Hint: Frobenius.]

(d) Show that there exists exactly one finite field for every number $q = p^n$.

Question 5. Prove that the polynomial $X^4 + 1$ is reducible in $\mathbb{F}_p[X]$ for every prime p.

* * *

Question 6. Let p be a prime integer, $n, m \geq 0$. Find the smallest k such that the finite field $\mathbb{F}_{p^k}$ contains two subfields isomorphic to $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$.

Question 7. First explain why $\mathbb{F}_3[X]/(X^2-2)$ is isomorphic to $\mathbb{F}_3[X]/(X^2-2X-1)$. Then find an explicit isomorphism:

$$\phi : \mathbb{F}_3[X]/(X^2-2) \longrightarrow \mathbb{F}_3[X]/(X^2-2X-1). \tag{1}$$

Question 8. Show that for any finite field $\mathbb{F}_q$ and $n \in \mathbb{N}$ there is an irreducible polynomial over $\mathbb{F}_q$ of degree n.

Question 9.

(a) Find the degree of the splitting field of the polynomial X^7-1 over the finite field $\mathbb{F}_5$.

(b) Find the degree of the splitting field of the polynomial $X^{171}-1$ over the finite field $\mathbb{F}_7$.

Question 10. Let E/F and K/F be two finite field extensions of F contained in a larger extension L, and consider the composite field $M = EK$ inside L. Show that if E/F is separable then so is M/K.