HOMEWORK 12, DUE THU APR 29TH

All solutions should be with proofs, you may quote from the book or from previous home works

(1) Let $K \subset L$ be a finite extension of fields and let $K \subset M \subset L$, where M is the set of all elements in L separable over K. We have seen in class that M is a subfield of L.

(a) Show that L is purely inseparable over M. That is, either $L = M$ or characteristic is $p > 0$ and if $a \in L$, then $a^q \in M$ for some $q = p^n$.

(b) Show that the separable degree $[L : K]_s$ divides $[L : K]$. If $\frac{[L:K]}{[L:K]_s} = m > 1$, show that the characteristic of K is a prime p and m is a power of p.

(2) Let $K \subset L$ be a field extension. A map $D : L \to L$ is called a K-derivation, if it is a K-linear map and $D(ab) = aD(b) + bD(a)$ (Leibniz formula) for all $a, b \in L$.

(a) Show that $D(x) = 0$ for all $x \in K$.

(b) If D_1, D_2 are derivations, show that $D_1 + D_2$ is a derivation and aD for $a \in L$ defined as $(aD)(x) = aD(x)$ for $x \in L$ are derivations. Thus, show that $\mathbb{T}$ = set of all derivations form an L-vector space.

(c) Assume L is a finite extension of K. Show that $\mathbb{T} = 0$ if and only if L is a separable extension of K.

(3) A field K is called *perfect* if either its characteristic is zero or it is a prime number p and every element in K has a p^{th} root. Show that, if K is perfect, any finite extension of K is separable.

(4) Let K be a finite field with q elements.

(a) Let $G(X) = X^{q^n} - X \in K[X]$ and let L be the splitting field of G. Show that $[L : K] = n$.

(b) Let $f(X) \in K[X]$ be irreducible. Show that f divides $X^{q^n} - X$ if and only if $\deg f$ divides n.

(c) Show that,

$$X^{q^n} - X = \prod_{d|n} \prod_{f_d \text{ irr}} f_d(X),$$

where $f_d(X) \in K[X]$ are irreducible of degree d and monic in X.

(5) Let $K \subset \overline{K}$ be a fixed inclusion of a field in an algebraic closure. Let $P(X) \in K[X]$ be any polynomial and let $L = K(a_1, \ldots, a_n) \subset \overline{K}$, where a_is are the roots of P, so L is a splitting field. If $\sigma : L \to \overline{K}$ is any homomorphism with $\sigma(x) = x$ for all $x \in K$, show that $\sigma(L) = L$ and thus it is an element of $G(L/K)$ as defined in class.