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 $q = p^n$.

Solution. If characteristic is zero, we know every element in L is separable over K and thus $M = L$. So, assume characteristic is $p > 0$. Let $a \in L$ and let $P(X)$ its irreducible polynomial over M. If $\deg P = 1$, then $a \in M$, and we can take $q = p^0$. So assume $M \neq L$ and $a \notin L$, so $\deg P > 1$.Since a can not be separable over M (if separable, it will also be separable over K and then it will be in M), we must have $P'(X) = 0$ and then the non-zero terms aX^r in $P(X)$ must have $p|r$. So, choose $q = p^n$, n largest, such that any non-zero term aX^r in $P(X)$ has $q|r$. Then replacing these terms with $aY^{r/q}$, we get a polynomial $Q(Y) \in M[Y]$ such that $Q(X^q) = P(X)$ and at least one non-zero term in $Q(Y)$ is of the form aY^r with $p \not| r$. Then $Q(Y)$ is a separable polynomial over M and a^q is a root of this and thus $a^q \in M$. □

(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.

Solution. We have seen in class that $[M : K]_s = [M : K]$. So, suffices to show that $[L : M]_s = 1$. That is, there is only one way to map $L \to \overline{K}$ fixing $M \subset \overline{K}$. If $\sigma : L \to \overline{K}$ is a field homomorphism such that $\sigma(x) = x$ for all $x \in M$, for any $a \in L$, we have $a^q \in M$ as in the previous part and $\sigma(a^q) = x \in M$. So, $\sigma(a)^q = x$ and thus, $\sigma(a)$ is some

q^{th} root of $x \in \overline{K}$. But $X^q - x$ has a unique solution in $\overline{K}$ and thus $\sigma(a)$ has only one choice.
For the latter part, we only need to show that $[L : M]$ is a power of p. If $a \in L$ and not in M, we have $[L : M] = [L : M(a)][M(a) : M]$. But $a^q \in M$ will show that $[M(a) : M]$ is a power of p and an easy induction will finish the proof. □

(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 $x \in K$.

Solution. We show first (and you have seen this earlier) that $D(1) = 0$.

$$D(1) = D(1 \cdot 1) = 1D(1) + 1D(1) = 2D(1),$$

and thus $D(1) = 0$.
Next, we use the fact that D is K-linear. If $x \in K$, $D(x) = D(x \cdot 1) = xD(1) = 0$. □

(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.

Solution. This is straightforward. □

(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.

Solution. First, assume that L is a separable extension of K and let $D : L \to L$ be a K-derivation. Let $a \in L$ and $P(X) \in K[X]$ its irreducible polynomial. Since $P(a) = 0$, we have $D(P(a)) = 0$. Using Leibniz formula one easily checks that $D(P(a)) = P'(a)D(a)$ ($P'(X)$ is the derivative of P). Since the extension is separable, $P'(a) \neq 0$ and then $D(a) = 0$.
Conversely, assume that L is not a separable extension. Then, we will show that $\mathbb{T} \neq 0$. This can happen only in characteristic $p > 0$. Let $M \subset L$ be the set of all elements in L separable over K as in the previous problem. We are assuming $M \neq L$ and thus one easily checks that there is

$M \subset F \subset L = F(a)$, $a \notin F, a^p \in F$, for a suitable subfield F. We will show that there is a non-zero F-derivation of L (which is clearly a K-derivation, since $K \subset F$). Notice that $L = F[X]/(X^p - b)$, where $b = a^p \in F$. Any element in L can be written as $A(a)$ for some $A \in F[X]$ and define $D : L \to L$ by $D(A(a)) = A'(a)$ (check that this is well defined) and then $D(a) = 1$ and it is an F-derivation.

□

(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.

Solution. First, notice that if every element in K has a p^{th} root in K, then repeating this, every element has a q^{th} root for $q = p^n$. If a is not separable over K, as in the first problem, its irreducible polynomial $P(X) \in K[X]$ is of the form $P(X) = Q(X^q)$ for some $q = p^n$ and Q is separable over K. Writing $Q(T) = T^m + a_1 T^{m-1} + \cdots + a_m$ we let $a_i = b_i^q$. Then, $Q(X^q) = X^{qm} + b_1^q X^{q(m-1)} + \cdots + b_m^q = (X^m + b_1 X^{m-1} + \cdots + b_m)^q$ and thus $P(X)$ is not irreducible unless $q = 1$, which says that a is in fact 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 $[L : K] = n$.

Solution. Notice that G is separable, since $G' = -1$. Thus it has q^n distinct roots and so L must have at least q^n elements. So, $[L : K] \geq n$. If $M \subset L$ are the set of elements which are root s of G, I claim, it is a field. If a, b are roots of G, then $a^{q^n} = a, b^{q^n} = b$ and then $(a+b)^{q^n} = a^{q^n} + b^{q^n} = a + b$. Similarly, for ab and $1/a$ if $a \neq 0$. So, every element of L satisfies G. If $[L : K] = m > n$, then, since $L - \{0\}$ is a cyclic group of order $q^m - 1$, there is an element $a \in L$ whose order is $q^m - 1$ and then $a^{q^n} \neq a$. □

(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.

Solution. Let $\deg f = n$. Since f is irreducible, $K[X]/(f(X)) = L$ is field and $[L : K] = n$. Thus L has q^n elements and so $a^{q^n} = a$ for any $a \in L$. On the other hand, f has a root $a \in L$ and so $f(a) = 0$ and $a^{q^n} = a$ which says f divides $X^{q^n} - X$, since f is irreducible.
Conversely, assume that f divides $G(X) = X^{q^n} - X$ and let L be the splitting field of G. If a is a root of f, then clearly, $a^{q^n} = a$ and so we have $K \subset K(a) \subset L$. $[K(a) : K] = \deg f$ and $[L : K] = n$ and so $\deg f$ 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.

Solution. This is clear from the previous part. □

(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.

Solution. If σ is as in the problem, $\sigma(a_i)$ must be a root of $P(X)$ and thus must be one of the a_is. So, σ takes each a_i to L and thus, $\sigma(L) \subset L$. But σ is a K-linear map, since $\sigma(x) = x$ for all $x \in K$ and L is a finite dimensional vector space over K and so $\sigma(L) = L$. □