Grad Algebra (602) / Problem Set 5

1) Complete the proofs of the following assertions from the course:
   a) Let $f : A \to B$ be an isomorphism of $C$-algebras, $a$ and ideal of $A$, and $b := f(a)$. Then $b$ is an ideal of $B$, and $\overline{f} : A/a \to B/b, x(mod\ a) \mapsto f(x)(mod\ b)$ is an isomorphism of $C$-algebras.
   b) Explain how to deduce from this the assertion used in the class: Let $\sigma' : M' \to N'$ be a $K$-isomorphism of subfields of an algebraically closed field extension $L$ of $K$. Then for $x \in L_{0,M'}$ there exists $y \in L_{0,N'}$ such that $\sigma'$ prolongs to a $K$-isomorphism of fields $\sigma'_x : M'(x) \to N'(y)$.

2) Show that the (formal) derivation has the following properties:
   a) Let $A$ be an arbitrary commutative ring with $1_A$, and $A[X]$ the polynomial ring in the variable $X$ over $A$. We define a map $D : A[X] \to A[X]$ by $P(X) = \sum_{i=0}^{n} a_i X^i \mapsto D(P) := \sum_{i=1}^{n} ia_i X^{i-1}$, and call it the (formal) derivation.
   b) The derivation $D$ satisfies the Leibniz rule: $D(PQ) = QD(P) + PD(Q)$.

3) Define inductively: $D^0 = id_{A[X]}$, and $D^{n+1} = D \circ D^n$ for all $n \geq 0$, and set $P^{(n)}(X) := D^n(P)$. For any $A$-algebra $B$, and $a \in B$ and $P(X)$ in $A[X]$ show the following:
   a) $a$ is a root of $P(X)$ in $B$, i.e., $P(a) = 0_B$ in $B$ if and only if $(X - a)$ divides $P(X)$ in the ring $B[X]$.
   b) For $n > 0$ one has: $P(X)$ is divisible by $(X - a)^n$ in $B[X]$ if and only if $P^{(k)}(a) = 0_B$ for $0 \leq k < n$, provided $(n - 1)!$ is not a zero divisor in $B$.

4) Suppose that $A = K$ is a field. Show that the following conditions for $P(X)$ are equivalent:
   i) $P(X)$ is separable.
   ii) All the roots of $P(X)$ in every (finite) field extension $L|K$ are simple.

5) Now suppose that $P(X) \in K[X]$ is irreducible. Show that the following conditions are equivalent:
   i) $P(X)$ is separable.
   ii) $P'(X) \neq 0_{K[X]}$.

6) Try to prove the following generalization of Problem 5 above: A monic polynomial $P(X) = X^n + \ldots + a_0$ in $A[X]$ is separable if and only if the ideal $(P, P')$ generated by $P(X)$ and $P'(X)$ in $A[X]$ is the whole $A[X]$. (Why is this a generalization of Problem 5?) Is the same true for some/all the non-monic polynomials $P(X)$?

7) Let $K$ be either a finite field or a field of characteristic zero. Show the following:
   a) An irreducible polynomial over $K$ is separable.
   b) A polynomial $P(X)$ over $K$ is separable if and only if all the irreducible factors of $P(X)$ are simple, i.e., $P(X)$ is not divisible by the square of any irreducible polynomial.