Math 306, Spring 2012
Homework 7 Solutions

(1) We say that a field L is *algebraically closed* if every $f \in L[x]$ splits over L. We know, for example, that $\mathbb{C}$ is algebraically closed. We say that $L\colon K$ is an *algebraic closure* of K if $L\colon K$ is algebraic and L is algebraically closed. Prove that the following are equivalent about an extension $L\colon K$.
  (a) The extension $L\colon K$ is an algebraic closure of K;
  (b) The extension $L\colon K$ is algebraic, and every irreducible $f \in K[x]$ splits over L;
  (c) The extension $L\colon K$ is algebraic, and if $L'\colon L$ is algebraic then $L = L'$.

Solution: (1 implies 2) Suppose that $L\colon K$ is an algebraic closure. By definition it is algebraic. Let $f \in K[x]$ be irreducible. Then $f \in L[x]$ so it splits by assumption. Hence f splits over L.

(2 implies 3) Suppose that $L'\colon L$ is algebraic. Clearly $L \subseteq L'$. Let $\alpha \in L'$. Since $L'\colon K$ is algebraic, there is an irreducible polynomial $m \in K[x]$ that has α as a zero. By assumption m splits over L. Therefore $\alpha \in L$, so $L' \subseteq L$.

(3 implies 1) We know that $L\colon K$ is algebraic. Let $f \in L[x]$. Let L' be the splitting field of f over L. Then $L'\colon L$ is algebraic. By assumption we have $L = L'$. Hence f splits over L.

(2) Construct the normal closures N for the following extensions.
  (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})\colon \mathbb{Q}$
  (b) $\mathbb{Q}(\sqrt[5]{3})\colon \mathbb{Q}$
  (c) $\mathbb{Z}_3(t)\colon \mathbb{Z}_3$, where t is an indeterminate.

Solution:
  (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
  (b) $\mathbb{Q}(\sqrt[5]{3}, e^{2\pi i/5})$
  (c) $\mathbb{Z}_3(t)$

(3) For each of these algebraic extensions, find the normal closure M and determine an appropriate collection S for which M is the splitting field over K (this means that each polynomial in the collection splits in M).
  (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)\colon \mathbb{Q}$
  (b) $\mathbb{Q}(e^{2\pi i/3}, e^{2\pi i/5}, e^{2\pi i/7}, e^{2\pi i/11}, \ldots)\colon \mathbb{Q}$
  (c) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}, \ldots)\colon \mathbb{Q}$

Solution:
  (a) The normal closure is $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$ and $S = \{x^2 - 2, x^2 - 3, x^2 - 5, x^2 - 7, \ldots\}$
  (b) The normal closure is $\mathbb{Q}(e^{2\pi i/3}, e^{2\pi i/5}, e^{2\pi i/7}, e^{2\pi i/11}, \ldots)$ and the corresponding S is given by $S = \{x^3 - 1, x^5 - 1, x^7 - 1, x^{11} - 1, \ldots\}$.
  (c) The normal closure is $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, e^{2\pi i/3}, \sqrt[5]{2}, e^{2\pi i/5}, \ldots)$ and $S = \{x^2 - 2, x^3 - 2, x^5 - 2, \ldots\}$.

(4) Each of the following statements is false. Disprove each of them by providing a counterexample or a counterproof.
  (a) Every finite extension is separable.
  (b) Every normal extension $L\colon K$ is the splitting field of some polynomial $f \in K[x]$.
  (c) For all fields K, if $f \in K[x]$ and $Df = 0$, then $f = 0$.
  (d) Every separable extension is normal.
  (e) Every normal extension is separable.

Solution:
  (a) Consider $\mathbb{Z}_2(u)(t)\colon \mathbb{Z}_2(u)$, where t is a root of $x^2 - u \in \mathbb{Z}_2(u)[x]$. This finite extension is not separable.
  (b) The extension $\mathbb{Q}(t)\colon \mathbb{Q}$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$.
  (c) Let $K = \mathbb{Z}_2$. Then $f = x^2$ is not zero but $Df = 0$.
  (d) The extension $\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}$ is separable but not normal.

(e) The extension $\mathbb{Z}_2(u)(t)\colon \mathbb{Z}_2(u)$, where t is a root of $x^2 - u \in \mathbb{Z}_2(u)[x]$, is normal but not separable.

(5) Suppose that $L\colon K$ is an algebraic extension. Prove that there is a greatest intermediate field M for which $M\colon K$ is normal (assume there is at least one such M). In your proof, you should give a definition of the notion of "greatest".

Solution: For all α in some indexing set I, let M_α be an intermediate subfield of $L\colon K$ which is normal over K. Certainly I is nonempty because K is normal over itself. Let M be the intersection of all subfields of L that contain all the M_α. We claim that M is also normal over K. For each $\alpha \in I$, let $S_\alpha \subseteq K[x]$ be a collection of polynomial for which M_α is the splitting field. Let N be the splitting field of $S = \bigcup_{\alpha \in I} S_\alpha$. We will show that $M = N$. Certainly N contains all the M_α by the minimality of M_α. Therefore N contains M by the minimality of M. But certainly the polynomials of S split over M, so by the minimality of N we have $N \subseteq M$. Therefore $N = M$ and M is normal over K.

(6) Let $L\colon K$ be an algebraic field extension and let M_1 and M_2 be intermediate fields normal over K. Define $K(M_1, M_2)$ to be the smallest subfield of L containing both M_1 and M_2. Prove that both $K(M_1, M_2)\colon K$ and $M_1 \cap M_2\colon K$ are normal extensions.

Solution: The proof of the first part is practically identical to the proof of the last problem. Now let $f \in K[x]$ be irreducible with a root α in $M_1 \cap M_2$. Then $\alpha \in M_1$. Since $M_1\colon K$ is normal, all the roots of f lie in M_1. Similarly, all the roots of f lie in M_2. Therefore $M_1 \cap M_2$ contains all the roots of f, and is therefore normal over K.

(7) Suppose that f is a polynomial in $K[x]$ of degree n and either $\operatorname{char} K = 0$ or $\operatorname{char} K > n$. Suppose that $\alpha \in K$. Prove that

$$f = f(\alpha) + Df(\alpha)(x-\alpha) + \frac{D^2 f(\alpha)}{2!}(x-\alpha)^2 + \cdots + \frac{D^n f(\alpha)}{n!}(x-\alpha)^n.$$

(Hint: Proceed by induction on n, using the following fact: If f has degree $k+1$, then α is a root of the polynomial $f - f(\alpha)$, so $f - f(\alpha) = (x-\alpha)g$, for some g of degree k.)

Solution: Certainly the statement is true when $n = 0$, in which case f is just a constant function, so $f = f(\alpha)$. Suppose that the statement is true for any polynomial of degree k. Let $f \in K[x]$ with degree $k+1$. Then α is a root of the polynomial $f - f(\alpha)$, so $f - f(\alpha) = (x-\alpha)g$, for some g of degree k. By the induction hypothesis, we know that

$$g = g(\alpha) + Dg(\alpha)(x-\alpha) + \frac{D^2 g(\alpha)}{2!}(x-\alpha)^2 + \cdots + \frac{D^k g(\alpha)}{k!}(x-\alpha)^k.$$

Therefore

$$f = f(\alpha) + g(\alpha)(x-\alpha) + Dg(\alpha)(x-\alpha)^2 + \frac{D^2 g(\alpha)}{2!}(x-\alpha)^3 + \cdots + \frac{D^k g(\alpha)}{k!}(x-\alpha)^{k+1}.$$

It suffices to show that, for all $i = 1, \ldots, k$, we have $\frac{D^i g(\alpha)}{i!} = \frac{D^{i+1} f(\alpha)}{(i+1)!}$, or $(i+1)D^i g(\alpha) = D^{i+1} f(\alpha)$. We claim that, for all $i \in \{1, \ldots, k\}$, we have $D^{i+1} f = (i+1)D^i g + (x-\alpha)D^{i+1} g$. We proceed by induction. Clearly since $f = f(\alpha) + (x-\alpha)g$, we have $Df = g + (x-\alpha)Df$, so the statement is true for $i = 0$. Assume that, for some $j \in \{0, \ldots, k-1\}$, we have $D^{j+1} f = (j+1)D^j g + (x-\alpha)D^{j+1} g$. Hence

$$\begin{aligned} D^{j+2} f &= (j+1)D^{j+1} g + D^{j+1} g + (x-\alpha)D^{j+2} g \\ &= (j+2)D^{j+1} g + (x-\alpha)D^{j+2} g. \end{aligned}$$

Hence the equation is true for all i. Therefore $D^{i+1} f(\alpha) = (i+1)D^i g(\alpha)$, as desired.

(8) Suppose that f is a polynomial in $K[x]$ of degree n and either $\operatorname{char} K = 0$ or $\operatorname{char} K > n$. Prove that α is a root of multiplicity r iff

$$f(\alpha) = Df(\alpha) = \cdots = D^{r-1} f(\alpha) = 0$$

and $D^r f(\alpha) \neq 0$. (Hint: Proceed by induction on r.)

Solution: Suppose that α has multiplicity r. Then $f = (x-\alpha)^r g$ for some $g \in K[x]$ with $g(\alpha) \neq 0$. For all i, we have

$$D^i f = \sum_{j=0}^{i} \binom{i}{j} D^j (x-\alpha)^r D^{i-j} g.$$

Now $D^j (x-\alpha)^r = r(r-1)\cdots(r+1-j)x^{r-j}$. Hence $D^i f(\alpha) = 0$ if $i \leq r$ and

$$D^r f = \sum_{j=0}^{r} \binom{r}{j} D^j (x-\alpha)^r D^{r-j} g.$$

Therefore $D^r f(\alpha) = (r+1)! g(\alpha) \neq 0$.

To prove the converse, proceed by induction on r. Certainly the statement is true if $r = 1$. In this case $f(\alpha) = 0$ and $Df(\alpha) \neq 0$. Then $f = (x-\alpha)g$ for some $g \in K[x]$ and $Df = g + (x-\alpha)Dg$, so $g(\alpha) = Df(\alpha) \neq 0$, so f has multiplicity 1. Suppose that the statement is true for $r = k$. Suppose that

$$f(\alpha) = Df(\alpha) = \cdots = D^{k-1} f(\alpha) = 0 \quad \text{and} \quad D^k f(\alpha) \neq 0.$$

Then for all $i \in \mathbb{Z}_{\geq 1}$, we have

$$D^i f = i D^{i-1} g + (x-\alpha) D^i g$$

(see the previous problem). Hence for $i = 1, \ldots, k-1$, we have $g(\alpha) = Dg(\alpha) = \cdots = D^{k-2} g(\alpha)$ and $D^{k-1} g(\alpha) \neq 0$. By induction we know that g has a root α of multiplicity $k-1$. Since $f = (x-\alpha)g$, we know that f has a root α of multiplicity k.

(9) (a) Show that, if $f \in K[x]$ is irreducible and the characteristic of K is p for some prime p, then f is inseparable iff $f = a_0 + a_1^p + \cdots + a_n x^{np}$ for some $n \in \mathbb{Z}_{\geq 1}$ and $a_0, \ldots, a_n \in K$.

(b) Suppose that $L\colon K$ is a field extension and $\operatorname{char} K = p > 0$. If $[L\colon K]$ is coprime to p, then prove that $L\colon K$ is separable.

(c) We say that a field K is *perfect* if every irreducible $f \in K[x]$ is separable. Prove that any algebraic extension of a perfect field is also perfect.

Solution:

(a) If f is inseparable, then there is $m \in K[x]$ with $\deg m \geq$ such that $m | f$ and $m | Df$. But f is irreducible, so f and m are associates, so $f | Df$, so $Df = 0$ and f has the form given above. Conversely is obvious: take $m = f$.

(b) Suppose that $L\colon K$ is inseparable. Then there is an $\alpha \in L$ whose minimal polynomial is of the form $f = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np}$, for some $n \in \mathbb{Z}_{\geq 1}$ and $a_0, \ldots, a_n \in K$. Since f is irreducible, we know that $K(\alpha)\colon K$ has degree np. Therefore $[L\colon K]$ is divisible by np, and hence divisible by p (we are assuming that the extension is finite), contradicting the fact that $[L\colon K]$ is coprime to p.

(c) Let $L\colon K$ be an algebraic extension and let K be perfect. Let $f \in L[x]$ be irreducible with splitting field M. Consider a root $\alpha_1 \in M$ of f. Hence f is the minimum polynomial of α_1 over L. Since $L\colon K$ is algebraic, we know that α_1 is algebraic over K. Let g be the minimum polynomial of α_1 over K. Then $f | g$. Since K is perfect, the polynomial g is separable, so $g = (x-\alpha_1)\cdots(x-\alpha_n)$ in $M[x]$, where all the α_i are distinct. Then f splits in $M[x]$ into a product of distinct linear factors as well, so f is separable. Therefore L is perfect.