Math 422/501: Problem set 7 (due 28/9/09)

Splitting fields and normal closures

1. Construct subfields of $\mathbb{C}$ which are splitting fields over $\mathbb{Q}$ for the following polynomials:
   (a) $t^3 - 1$;
   (b) $t^4 + 5t^2 + 6$;
   (c) $t^4 + 7t^2 + 6$;
   (d) $t^6 - 8$.
   Find the degrees of the splitting fields as extensions of $\mathbb{Q}$.

2. Construct a splitting field for the following polynomials over $\mathbb{F}_3$:
   (a) $t^3 + 2t + 1$;
   (b) $t^3 + t^2 + t + 2$.
   (c) Are the two fields isomorphic?

3. Let $f \in K[x]$ and let $\Sigma : K$ be a splitting field for f over K. Let $K \subset M \subset \Sigma$ be an intermediate field. Show that Σ is a splitting field for f over M.

4. Let $f \in K[x]$ have degree n and let $\Sigma : K$ be a splitting field for f over K. Show that $[\Sigma : K] \leq n!$.

Algebraic closures

DEFINITION. A field extension $K \hookrightarrow \bar{K}$ is called an *algebraic closure* if it is algebraic, and if polynomial in $K[x]$ splits in $L[x]$. We also say informally that $\bar{K}$ is an *algebraic closure of* K.

5. Let $K \hookrightarrow L$ be an algebraic extension.
   (a) If K is finite, show that $|L| \leq \aleph_0$.
   (b) If K is infinite, show that $|L| = |K|$.

6. Let $K \hookrightarrow \bar{K}$ be an algebraic closure. Show that every algebraic extension of $\bar{K}$ is isomorphic to $\bar{K}$.

7. (Existence of algebraic closures) Let K be a field, X an infinite set containing K with $|X| > |K|$. Let $0, 1$ denote these elements of $K \subset X$. Let
   $$\mathscr{F} = \{(L, +, \cdot) \mid K \subset L \subset X,\, (L, 0, 1, +, \cdot) \text{ is a field with } K \subset L \text{ an algebraic extension}\}\,.$$
   Note that we are assuming that restricting $+, \cdot$ to K gives the field operations of K.

   (OPT) Show that $\mathscr{F}$ is a set.
   (a) Show that every algebraic extension of K is isomorphic to an element of $\mathscr{F}$.
   (b) Given $(L, +, \cdot)$ and $(L', +', \cdot') \in \mathscr{F}$ say that $(L, +, \cdot) \leq (L', +', \cdot')$ if $L \subseteq L'$, $+ \subseteq +'$, $\cdot \subseteq \cdot'$. Show that this is a transitive relation.
   (c) Let $\bar{K} \in \mathscr{F}$ be maximal with respect to this order. Show that $\bar{K}$ is an algebraic closure of K.
   (d) Show that K has algebraic closures.

8. (Uniqueness of algebraic closures) Let $K \hookrightarrow \bar{K}$ and $K \hookrightarrow L$ be two algebraic closures of K. Show that the two extensions are isomorphic.
Hint: Let $\mathscr{G}$ be the set of K-embeddings intermediate subfields $K \subset M \subset L$ into $\bar{K}$, ordered by inclusion.

Symmetric polynomials

Let R be a ring. Then S_n acts on the polynomial ring $R[x_1, \ldots, x_n]$ by permuting the variables, and we write $R[\underline{x}]^{S_n}$ for the set of fixed points.

9. (Basic structure)
   (a) Show that $R[\underline{x}]^{S_n}$ is a subring of $R[\underline{x}]$, *the ring of symmetric polynomials*.
   (b) For $\alpha \subset [n]$ write $\underline{x}^\alpha$ for the monomial $\prod_{i\in\alpha} x^i$. For $1 \le r \le n$ let
   $$s_r(\underline{x}) = \sum_{\alpha \in \binom{[n]}{r}} \underline{x}^\alpha \in R[\underline{x}]\,.$$
   Show that $s_r(\underline{x}) \in R[\underline{x}]^{S_n}$. These are called the *elementary symmetric polynomials*.

10. (Generation) Define the *height* of a monomial $\prod_{i=1}^n x_i^{\alpha_i}$ to be $\sum_{i=1}^n i\alpha_i$. Define the *height* of $p \in R[\underline{x}]$ to be the maximal height of a monomial appearing in p.
   (a) Given $p \in R[\underline{x}]^{S_n}$ find $\underline{\beta} \in \mathbb{Z}_{\ge 0}^n$ and $r \in R$ so that $q = r\prod_{r=1}^n s_r^{\beta_r}$ has the same highest term as p.
   (b) Show that $p - q$ has smaller height than p.
   (c) Show that every symmetric polynomial can be written as a polynomial of equal or smaller degree in the elementary symmetric polynomials.

Derivatives, derivations and separability

11. For a Laurent series $f = \sum_{i\ge i_0} a_i x^i \in R((x))$ over a ring R define its *formal derivative* to be the Laurent series $Df = \sum_{i\ge i_0} i a_i x^{i-1}$.
   (a) Show that D is R-linear: that $D(\alpha f + \beta g) = \alpha Df + \beta Dg$ for $\alpha, \beta \in R$ and $f, g \in R((x))$.
   (b) Show that D is a *derivation*: that $D(fg) = Df \cdot g + f \cdot Dg$ (this is called the *Leibnitz rule*).
   (c) Show that $D(f^k) = k \cdot f^{k-1} \cdot Df$ for all $k \ge 0$.
   (d) Show that if f is a polynomial then Df is a polynomial as well, that is that D restricts to a map $R[x] \to R[x]$.

12. (Derivative criterion for separability) Let K be a field.
   (a) Let $\alpha \in K$ be a zero of $f \in K[x]$. Show that $(x-\alpha)^2 | f$ iff $Df(\alpha) = 0$ iff $(x-\alpha) | Df$.
   (b) Let $\varphi\colon K \to L$ be an extension of fields, and let $f, g \in K[x]$. Let $(f, g) = (h)$ as ideals of $K[x]$, $(\varphi(f), \varphi(g)) = (h')$ as ideals of $L[x]$. Taking h, h' monic show that $h = \varphi(h')$.
   (c) Show that $f \in K[x]$ is has no repeated roots in any extension (is *separable)* iff $(f, Df) = 1$.
   (d) Show that an irreducible $f \in K[x]$ is separable iff $Df = 0$.

Optional problems

A. Construct an embedding $K(x) \hookrightarrow K((x))$ and show that D restricts to a map $K(x) \to K(x)$.

For the rest fix a ring R.

B. Let A be an R-algebra, and consider the map $A \times A \to A$ given by the *commutator bracket* $[a,b] = ab - ba$, .
   (a) Show $(A, [\cdot,\cdot])$ is a *Lie algebra,* that is that the commutator is R-bi-linear and anti-symmetric, and satisfies the *Jacobi identity* $[a,[b,c]] + [b,[c,a]] + [c,[a,b]] = 0$.
   (c) Show that for a fixed $a \in A$ the map $b \mapsto [a,b]$ is an element $\mathrm{ad}(a) \in \mathrm{End}_R(A)$.
   (d) Show that $\mathrm{ad}(a)$ is a derivation: $(\mathrm{ad}(a))(bc) = [(\mathrm{ad}(a))(b)]\,c + b\,[(\mathrm{ad}(a))(c)]$.

C. Let A be an R-algebra. Let $\mathrm{Der}_R(A) = \{D \in \mathrm{End}_R(A) \mid D \text{ is a derivation}\}$.
   (a) Show that $\mathrm{Der}_R(A) \subset \mathrm{End}_R(A)$ is an R-submodule.
   (b) Give an example showing that $\mathrm{Der}_R(A)$ need not be an R-subalgebra (that is, closed under multiplication=composition).
   (c) Show that $\mathrm{Der}_R(A)$ is closed under the commutator bracket of $\mathrm{End}_R(A)$.

D. Let A an R-algebra. Show that the map $\mathrm{ad}\colon A \to \mathrm{Der}_R(A)$ is a map of Lie algebras, that is a map of R-modules respecting the brackets.