Lior Silberman's Math 422/501: Problem set 6 (due 23/10/2020)

Group actions

1. Let G be a group, let L be a field. Show that the set $\mathrm{Hom}_{\mathrm{Grp}}(G, L^\times) \subset L^G$ is linearly independent over L.

2. Let G be a finite group of automorphisms of a field L, and let $K = \mathrm{Fix}(G)$ be its fixed field. In class we showed that $[L:K] = \#G$.
   (a) Show that the extension L/K is normal.
   Hint: Let $f \in K[x]$ be irreducible, let $\alpha \in L$ be a root, and consider the polynomial $\prod_{\beta \in G\cdot\alpha}(x-\beta)$ where the product is over the G-orbit of α.
   (b) Show that the extension is separable.
   Hint: Count monomorphisms.

3. (The Galois correspondence for finite fields) Fix a prime p.
   (a) Assume that $\mathbb{F}_{p^k}$ embeds in $\mathbb{F}_{p^n}$. Show that $k|n$ and find the degree of this extension.
   (b) Let $k|n$. Show that $\mathbb{F}_{p^n}$ has a unique subfield isomorphic to $\mathbb{F}_{p^k}$, consisting of the fixed points of the map $x \mapsto x^{p^k}$.
   (c) Show that $G = \mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^n})$ is cyclic of order $\left[\mathbb{F}_{p^n} : \mathbb{F}_{p^k}\right]$ and generated by the Frobenius map $x \mapsto x^{p^k}$.
   (d) Using (a),(b),(c) show that the map $H \mapsto \mathrm{Fix}(H)$ induces a bijection between subgroups $H < G$ and intermediate fields $\mathbb{F}_{p^k} \subset F \subset \mathbb{F}_{p^n}$ such that $[\mathbb{F}_{p^n} : F] = \#H$.

Symmetric polynomials

Let R be a ring and let the symmetric group S_n acts on the polynomial ring $R[x_1, \dots, x_n]$ by permuting the variables. Write $R[\underline{x}]^{S_n}$ for the set of fixed points.

4. (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.*

5. (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 $\underline{\beta} \in \mathbb{Z}^n_{\ge 0}$ and $r \in R$ so that the highest term of $q = r\prod_{r=1}^n s_r^{\beta_r}$ is a highest term of p.
   (b) Show that $p - q$ has either fewer highest terms than p or 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

6. (Derivative criterion for separability) Let K be a field.
   (a) Show that the formal derivative $\partial\colon K[[x]] \to K[[x]]$ (see PS2 problem 6(d)) restricts to a K-linear derivation on $K[x]$.
   (b) Let L/K be an extension and let $\alpha \in L$ be a zero of $f \in K[x]$. Show that $(x-\alpha)^2 | f$ in $L[x]$ iff $Df(\alpha) = 0$ iff $(x-\alpha)|Df$ in $L[x]$.
   (*c) Show that $f \in K[x]$ has no repeated roots in any extension iff $(f, Df) = 1$.
   (d) Show that an irreducible $f \in K[x]$ is separable iff $Df \neq 0$.

7. Let $f(x) = x^3 + x + 1$. Over which fields is f separable?

Supplementary problems: More on derivations

Fix a ring R.

A. 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: $(\mathrm{ad}(a))\,(bc) = [(\mathrm{ad}(a))\,(b)]\,c + b\,[(\mathrm{ad}(a))\,(c)]$.

B. 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 $\mathrm{End}_R(A)$.

C. 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.