Math 603 Assignment 11, 2020-21

Part I. From Gallier–Shatz:

- problem 122
- problem 123
- problem 125
- problem 128
- problem 131, subproblems 1 and 2.

Part II.

1. (a) Let k be a field of characteristic $p > 1$ and let α be an element of an extension field of k such that $[k(\alpha) : k] = p^3$. Consider the family $\mathfrak{F}$ of all fields between k and $k(\alpha)$. Is $\mathfrak{F}$ finite? Either prove that $\mathfrak{F}$ is finite, or prove that $\mathfrak{F}$ is infinite.

(b) Give an example of a field extension E/k such that $[E : k] < \infty$ and there are infinitely many fields between E and k.

2. We say that a field extension E/k is *strongly normal* if for every element $y \in E \smallsetminus k$ (i.e. $y \in E$ and $y \notin k$), there exists a k-linear ring automorphism $\sigma \in \mathrm{Aut}(E/k)$ such that $\sigma(y) \neq y$. Show that if k is an infinite field, then the rational function field $k(x)$ is strongly normal over k. (Hint: For every element $a \in k$, there exists an automorphism $\sigma_a \in \mathrm{Aut}\big(k(x)/k\big)$ such that $\sigma_a(x) = x + a$.)

Part III.
Let k be a field and let E be an extension field of k. Let

$$R_k = \mathrm{End}_k(E, +)$$

be the ring of all endomorphisms of the k-vector space underlying E. We describe a bijection between

- the family $\mathfrak{F}(E/k)$ consisting of all subextension fields F/k of E/k with $[E : F] < \infty$, and
- the family $\mathfrak{A}(E/k)$ consisting subrings of R_k satisfying the conditions in (B) below.

In the notation below, the bijection is

$$F \longmapsto R_F, \qquad R \longmapsto \{y \in E \,|\, T \circ y_L = y_L \circ T \quad \forall T \in R\}.$$

So at least at a formal level this bijection is analogous to the Galois correspondence. In fact one can deduce from it the Galois correspondence. This problem has several parts, (A) and (B0)–(B5), with hints.

Notation/Definition.

i. For every element $y \in E$, denote by y_L the element of R_k which sends any $z \in E$ to yz.

ii. Let S be the subring of R_k consisting of all endomorphisms y_L of $(E, +)$ with $y \in E$.

iii. For every subextension field F/k of E/k, define $R_F := \mathrm{End}_F(E, +)$ be the ring of all endomorphisms of the F-vector space underlying E. Clearly this subring R_F of R_k contains S. Left multiplication by elements of S, i.e. $y \cdot T := y_L \circ T \ \forall\, y \in E, \forall\, T \in R_F$, gives R_F a structure as a vector space over E.

(A) Suppose that F is a subfield of E such that $[E : F] < \infty$. Show that $\dim_E(R_F) = [E : F]$, where the E-vector space structure of R_F is given above in iii.

(B) Suppose that R is a *subring* of R_k (containing 1 by our convention) such that

R is a finite dimensional E-vector subspace of R_k

The last condition means that $y_L \circ T \in R$ for all $y \in E$ and all $T \in$, and there exists elements $T_1, \ldots, T_m \in R$ such that every element of R can be written as a linear combination $\sum_{i=1}^m y_{i,L} \circ T_i$ with $y_1, \ldots, y_m \in E$. Let

$$F := \{y \in E \,|\, T \circ y_L = y_L \circ T \quad \forall\, T \in R\}.$$

It is easily checked that F is a subfield of E containing k; this is part (1) below. Follow the steps below to show that there exists a subextension $[E : F] < \infty$ and $R = R_F$.

(B0) Show that F is a subfield of E containing k. Note that $R \subseteq R_F$ by definition.

(B1) Consider the k-linear map

$$\beta : E \to \mathrm{Hom}_E(R, E), \quad \beta(y)(T) := T(y) \ \ \forall\, y \in E, \forall\, T \in R.$$

and the induced E-linear map

$$\tilde{\beta} : E \otimes_k E \to \mathrm{Hom}_E(R, E), \quad \sum_j (z_j \otimes y_j)(T) := \sum_j z_j\, T(y_j)$$

for all elements $\sum_j (z_j \otimes y_j) \in E \otimes_k E$. Show that the E-linear span of $\beta(E)$ is equal to $\mathrm{Hom}_E(R, E)$; in other words the E-linear map $\tilde{\beta}$ is a surjection, or equivalently $\beta(E)$ contains an E-basis of $\mathrm{Hom}_E(R, E)$. Here the E-module structure of $E \otimes_k E$ is through the first factor of $E \otimes_k E$.

(Hint: Suppose that $\tilde{\beta}(E) \subsetneq \mathrm{Hom}_E(R, E)$. Use basic facts about duals vector spaces to get a contradiction.)

(B2) Conclude from (1) that there exists an E-basis $T_1, \ldots, T_n$ of the E-submodule $R \subseteq R_k$ and elements $y_1, \ldots, y_n \in E$ such that

$$T_i(y_j) = \delta_{ij} \ \ \forall\, i, j = 1, \ldots, n,$$

where $n = \dim_E(R)$.

For such elements $T_1, \ldots, T_n \in R$ and $y_1, \ldots, y_n \in E$, show that

$$T = \sum_{i=1}^{n} T(y_i)_L \circ T_i \quad \forall T \in R.$$

(B3) Use the last displayed equality in (2) to show that for any $i, j = 1, \ldots, n$ and any $y \in E$, we have

$$T_j \circ y_L \circ T_i = T_j(y)_L \circ T_i.$$

Conclude that $T_j(y) \in F$ for all $y \in E$ and all $j = 1, \ldots, n$.

(B4) Given any $y \in E$, consider the element

$$y' := y - \sum_{j=1}^{n} T_j(y) \cdot y_j.$$

Show that $T_i(y') = 0$ for all $i = 1, \ldots, n$. Conclude that $T(y') = 0$ for all $T \in R$, and hence $y' = 0$ because R contains id_E.

(B5) Show that $y_1, \ldots, y_n$ are linearly independent over F, so that $[E : F] = n$ and also that $\dim_E(R_F) = n$. Conclude that $R = R_F$.