Math 5286 Honors fundamental structures of algebra– 2nd semester
Spring 2019, Vic Reiner
Final exam - Due by 5pm on Wednesday May 8
(in my VinH 107 mailbox, or under my VinH 256 office door, or emailed as PDF.)

Instructions: There are 4 problems. This is an open book, open library, open notes, open web, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult.

1. (35 points total, 5 points each part) True or False?
True assertions must be proven, and false assertions must be disproven.

(a) The polynomial $f(x) = x^3 + x^2 - 4x + 1$ in $\mathbb{Q}[x]$ is irreducible, and its splitting field $\mathbb{K} = \mathrm{split}_{\mathbb{Q}}(f(x))$ over $\mathbb{Q}$ has Galois group $G(\mathbb{K}/\mathbb{Q}) \cong S_3$.

(b) Every irreducible cubic polynomial $f(x)$ in $\mathbb{Q}[x]$ that has only one real root will have splitting field $\mathbb{K} = \mathrm{split}_{\mathbb{Q}}(f(x))$ with Galois group $G(\mathbb{K}/\mathbb{Q}) \cong S_3$.

(c) In a tower of fields $\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3$, if both $\mathbb{F}_2/\mathbb{F}_1$ and $\mathbb{F}_3/\mathbb{F}_2$ are Galois, then $\mathbb{F}_3/\mathbb{F}_1$ will also be Galois.

(d) For all $n = 2, 3, 4, \ldots$, the symmetric group S_n is generated by any transposition (i, j) together with any n-cycle $(i_1, i_2, \cdots, i_n)$.

(e) There are exactly seven strictly intermediate subfields $\mathbb{K}$ with $\mathbb{Q} \subsetneq \mathbb{K} \subsetneq \mathbb{Q}(\zeta_{37})$, where $\zeta_{37} = e^{\frac{2\pi i}{37}}$.

(f) Not all of the intermediate subfields $\mathbb{Q} \subsetneq \mathbb{K} \subsetneq \mathbb{Q}(\zeta_{37})$ will have $\mathbb{K}/\mathbb{Q}$ Galois.

(g) Consider two $\mathbb{R}[x]$-modules V_1, V_2 in which as sets, both $V_1 = \mathbb{R}^2$ and $V_2 = \mathbb{R}^2$, but where $x(v) = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] v$ for v in V_1, while $x(v) = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right] v$ for v in V_2. Then V_1, V_2 contain the same number of R-submodules.

2. (20 points total) Let $R \subset S$ where R is a principal ideal domain and S is a unique factorization domain (for example, $R = \mathbb{Z} \subset \mathbb{Z}[x] = S$).

Given two elements a, b in R, show that if r is any GCD (greatest common divisor) for a, b in R, and s is any GCD for a, b in S, then r, s are associates in S, that is, $s = ur$ for some unit u in $S^\times$.

3. (20 points total; 5 points each part)

(a) Prove that $f(x) = x^4 - 80$ is irreducible in $\mathbb{Q}[x]$.

(b) Let $\mathbb{K} = \text{split}_{\mathbb{Q}}(f(x)) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ where the α_i are the four roots of $f(x)$. Write down the entire Galois group $G := G(\mathbb{K}/\mathbb{Q})$ as a subgroup of the symmetric group S_4 permuting these four roots, and identify G up to isomorphism as one of the transitive subgroups of S_4 discussed in lecture.

(c) How many intermediate subfields $\mathbb{L}$ are there with $\mathbb{Q} \subsetneq \mathbb{L} \subsetneq \mathbb{K}$? Explain.

(d) How many intermediate subfields $\mathbb{L}$ with $\mathbb{Q} \subsetneq \mathbb{L} \subsetneq \mathbb{K}$ have $\mathbb{L}/\mathbb{Q}$ Galois? Explain.

4. (25 points total; 5 points each part)

(a) Let $\mathbb{F}$ be a field of characteristic zero, and $\mathbb{K}/\mathbb{F}$ a field extension with $[\mathbb{K} : \mathbb{F}]$ finite. Prove there are only finitely many intermediate subfields $\mathbb{L}$ with $\mathbb{F} \subsetneq \mathbb{L} \subsetneq \mathbb{K}$.

Now for the rest of this problem, assume that $\mathbb{F}$ is a field of characteristic 2, and the cardinality $|\mathbb{F}|$ is infinite. As an example, one might have $\mathbb{F} = \mathbb{F}_2(u)$, the field of rational functions in a variable u with $\mathbb{F}_2$ coefficients.

(b) For the field extension

$$\mathbb{K} := \mathbb{F}(x, y) \supsetneq \mathbb{F}(x^2, y^2) =: \hat{\mathbb{F}},$$

calculate the extension degree $[\mathbb{K} : \hat{\mathbb{F}}]$. Here $\mathbb{F}(x, y)$ is the field of rational functions $\frac{f(x,y)}{g(x,y)}$ in two variables x, y with coefficients in $\mathbb{F}$, and $\mathbb{F}(x^2, y^2)$ is the subfield of rational functions of the form $\frac{f(x^2,y^2)}{g(x^2,y^2)}$.

(c) Show that there are infinitely many intermediate subfields $\mathbb{L}$ with $\hat{\mathbb{F}} \subsetneq \mathbb{L} \subsetneq \mathbb{K}$ (in contrast to part (a) of this problem).

(d) Show that there does **not** exist γ in $\mathbb{K}$ for which $\mathbb{K} = \hat{\mathbb{F}}(\gamma)$.
(This shows why characteristic zero is needed in the Primitive Element Theorem.)

(e) Show that if we re-define $\mathbb{K} = \mathbb{F}(x_1, x_2, \ldots) \supsetneq \mathbb{F}(x_1^2, x_2^2, \ldots) = \hat{\mathbb{F}}$, where there are infinitely many variables in the list $x_1, x_2, \ldots$, then $\mathbb{K}$ is an algebraic extension of $\hat{\mathbb{F}}$, but there do not exist elements in $\mathbb{K}$ whose degrees over $\hat{\mathbb{F}}$ are arbitrarily large. Show that, in fact, every element of $\mathbb{K}$ has degree at most two over $\hat{\mathbb{F}}$.
(This shows why assuming characteristic zero was needed in Artin's Lemma 16.5.3.)