6320-001 - SPRING 2021 - WEEK 10 (3/23, 3/25)

1. This week in 6320

3/23 – More on algebraic closures; finite fields.
3/25 – Separability, field automorphisms, Galois extensions.

2. Comments and suggested reading

Dummit and Foote, 13.4, 13.5, 14.1, 14.3

3. Preview of next week

(This is subject to change depending on how far we get this week!)
The fundamental theorem of Galois theory (14.2), cyclotomic fields (parts of 13.3, 13.6, 14.5).

4. Homework

Due Tuesday, *March 30*, at 11:59pm on Gradescope
All solutions must be typeset using TeX and submitted via Gradescope; handwritten or late submissions will not be accepted. All exercises and problems submitted must start with the statement of the exercise or problem.

You may work in groups, but you must write up your final solutions individually. Any instances of academic misconduct will be taken very seriously.

Justify your answers carefully!

4.1. **Exercises.** *Complete and turn in ALL exercises*:
Grading scale (for each part of an exercise):
3 points – A correct, clearly written solution
2 points – Right idea, but a minor mistake or not clearly argued
1 point – Some progress but multiple minor mistakes or a major mistake
0 points – Nothing written, totally incorrect, or no substantive progress made towards a solution.

Exercise 1. (**DF** 14.3- Exercise 1). Factor $x^8 - x$ into irreducibles in $\mathbb{Z}[x]$ and $\mathbb{F}_2[x]$.

Exercise 2.

(1) Find two distinct irreducible degree 3 monic polynomials $f(x)$ and $g(x)$ in $\mathbb{F}_3[x]$.
(2) For your f and g as in (1), exhibit an explicit isomorphism

$$\mathbb{F}_3[x]/(f(x)) \xrightarrow{\sim} \mathbb{F}_3[x]/(g(x)).$$

Exercise 3. Let K be a field of characteristic p, and let $a \in K$.

(1) Show $f(x) = x^p - x - a$ is separable.
(2) Show that if α is a root of $f(x) = x^p - x - a$, and $k \in \mathbb{F}_p$, then $\alpha + k$ is also a root of $f(x)$.
(3) If f is irreducible, deduce that $L = K[x]/f(x)$ is a splitting field of f, and show that $\mathrm{Aut}(L/K) \cong \mathbb{F}_p$ (as a group under addition).

Exercise 4.

(1) For k a field, and $a, b, c, d \in k$ such that $ad - bc \neq 0$, show that there exists a unique automorphism of $k(t)$ fixing k and sending t to $\frac{at+b}{ct+d}$.
(2) Show that the there is a group homomorphism $\mathrm{PGL}_2(k) \hookrightarrow \mathrm{Aut}(k(t)/k)$ sending the equivalence class of
$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}$$
to the automorphism described in part (1).
(3) Give a simple description of the fixed field of the automorphism $t \mapsto t+1$ of $k(t)$. **Hint: your answer will depend on the characteristic.**

Exercise 5. Let p be a prime number, let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$, let $K = \overline{\mathbb{F}_p}(s,t)$ (= $\mathrm{Frac}(\overline{\mathbb{F}_p}[s,t])$) and let $L = K(s^{1/p}, t^{1/p})$ (by which we mean any splitting field of $(x^p - s)(x^p - t)$).

(1) Show that $[L : K] = p^2$.
(2) Show that $|\mathrm{Aut}(L/K)| = 1$.
(3) Show there are infinitely many intermediate field extensions
$$K \subsetneq M \subsetneq L.$$

4.2. **Problems.** *Attempt as many as you have time for, but only turn in one (of your choice).*
Grading scale (for the problem you turn in):
10 points - A correct, complete, and clearly written solution.
8 points - Right idea, but one or two minor mistakes or not clearly argued.
5 points - Some progress but several minor mistakes or a major mistake.
0 points - Nothing written, totally incorrect, or no substantive progress made.
Revision policy: *If you score at least 5 points on the problem you turn in then you will be allowed to submit* **one** *revision to your solution before the final exam (May 3, 10:30am). If the revision is correct, complete, and clearly written then your mark will change to 9 points. This policy only applies to the problem you submit, not to the exercises in the previous section.*

Problem 1 A field extension L/K is *simple* if there exists $\alpha \in L$ such that $L = K(\alpha)$. Such an α is called a *primitive element* for L/K. In this problem, you will prove

The Primitive Element Theorem: A finite extension L/K is simple if and only if it admits only finitely many intermediary extensions $K \subseteq M \subseteq L$.

Remarks: Note that Exercise 5 gave an example of a finite extension with infinitely many subextensions; the primitive element theorem then implies that this is also an example of a finite extension that is not simple. On the other hand, the fundamental theorem of Galois theory will imply that for any finite *separable* extension, there are only finitely many subextensions. Thus, as a consequence, any finite extension of a perfect field (in particular, a characteristic zero field) is simple.

Proof of the primitive element theorem:

(1) Show that if a finite extension L/K admits a primitive element (i.e. $L = K(\alpha)$ for some $\alpha \in L$), then there are only finitely many intermediary extensions. **Hint: for $K \subseteq M \subseteq L$, show that the coefficients of the minimal polynomial of α over M generate M/K.**
(2) Show that if K is a finite field, then *every* finite extension L/K is simple and admits only finitely many intermediary extensions.
(3) Show that if L/K is a finite extension with only finitely many intermediary extensions, K is infinite, and $\alpha, \beta \in L$, then there exists $k \in K$ such that $K(\alpha, \beta) = K(\alpha + k\beta)$.
(4) Conclude.