Math146 - Review for the final exam

George McNinch

2025-03-31

I. The final exam is *comprehensive*, though it will weight material covered since the second midterm more heavily. The problems and definitions mentioned in this review document *primarily concern the material since the second midterm*; thus, *in preparing for the final exam, you should also study the review material for both midterms, and the midterms themselves.*

The recent material concerns §13 - §16 of the course lecture notes, namely:

perfect fields and separable polynomials, automorphisms of algebraic objects, the Fundamental Theorem of Galois Theory, and the material concerning the insolvability of the quintic.

II. You should be able to give careful statements answering the following questions about definitions:

- separable polynomial
- perfect field
- separable extension of fields; normal extension of fields
- the definition *fixed field* F^H of a subgroup $H \subseteq \mathrm{Aut}(F)$
- the *Galois group* $\mathrm{Gal}(E/F)$ for a field extension $F \subseteq E$.

III. You should know the following statements and examples

- the *Fundamental Theorem of Galois Theory*
- the fact that any finite field is perfect
- a condition for the roots of a polynomial in a splitting field to be distinct
- an example of an irreducible polynomial $q \in F[T]$ of degree > 1 such that q has exactly one root in a splitting field E of q over F.
- an example of a non-abelian Galois group
- a description of the Galois group $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ of the finite field $\mathbf{F}_{p^n}$ for a prime number p
- an example of a field extension $F \subset E$ such that E is *not normal* over F.
- for $a \in K$, describe the roots of $T^n - a \in K[T]$ in a splitting field of f over K

IV. You should be able to write careful solutions to problems similar to the following:

1. Let L_1 and L_2 be splitting fields over K of the polynomial $f \in K[T]$. We have seen before that $L_1 \simeq L_2$. More precisely, there is an isomorphism $\phi : L_1 \to L_2$ for which $\phi(a) = a$ for all $a \in K$.

   Use ϕ to show that there is an isomorphism $\mathrm{Gal}(L_1/K) \xrightarrow{\sim} \mathrm{Gal}(L_2/K)$. (Be sure to show that the mapping you exhibit is in fact an isomorphism).

2. Let ω be a root of $f(T) = \dfrac{T^5 - 1}{T - 1} = T^4 + T^3 + T^2 + T + 1 \in \mathbf{Q}[T]$ in some splitting field of f over $\mathbf{Q}$.

   a. Explain why $\mathbf{Q}(\omega)$ is a normal separable extension of $\mathbf{Q}$.

   b. Describe the group $\mathrm{Gal}(\mathbf{Q}(\omega)/\mathbf{Q})$. What is its *order*? What can you say about its *group structure*?

3. Let K be a finite field and let $a \in K$ be an element for which $f = T^3 - a \in K[T]$is *irreducible.* Let $L = K(\sqrt[3]{a})$ be a splitting field for f over K.

   Using results from the lectures, Prove the following: if $g \in K[T]$ is an irreducible polynomial of degree 3, then g splits over L.

4. Let $K = \mathbf{Q}(X)$ be the field of rational functions over $\mathbf{Q}$. Observe that

$$L = \mathbb{Q}(X)(\sqrt{X}, \sqrt{X+1})$$

   is a splitting field over $\mathbb{Q}(X)$ of the polynomial

$$(T^2 - X)(T^2 - (X + 1)) \in \mathbf{Q}(X)[T] = K[T]).$$

   a Show that $[L : \mathbb{Q}(X)] = 4$ and deduce that $\mathrm{Gal}(L/\mathbf{Q})$ has order 4.

   b. Recall that any group of order 4 is either cyclic or isomorphic to the group

$$\mathscr{K} = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

   Decide whether $\Gamma = \mathrm{Gal}(L/\mathbf{Q})$ is cyclic or is isomorphic to $\mathscr{K}$.

   c. By finding all subgroups of Γ, use the fundamental theorem of Galois theory to list all intermediate fields of the extension $\mathbb{Q}(X) \subseteq L = \mathbb{Q}(X)(\sqrt{X}, \sqrt{X+1})$.

5. For $n \in \mathbf{Z}_{\geq 0}$, let $\mathscr{P}_n = \{f \in K[T] \mid \deg f < n\}$, and note that $\dim_K \mathscr{P}_n = n$.

   Fix a polynomial $g \in K[T]$ of degree ≤ 2, say $g = a_0 + a_1 T + a_2 T^2$ for $a_0, a_1, a_2 \in K$. Show that multiplication by g defines a mapping

$$\lambda_g : \mathscr{P}_n \to \mathscr{P}_{n+2};$$

   Thus $\lambda_g(h) = gh$ for $h \in \mathscr{P}_n$.

   If $n = 3$, find the matrix representing the linear mapping λ_g with respect to the monomial bases of $\mathscr{P}_3$ and $\mathscr{P}_5$.

6. Let L be a splitting field over $\mathbf{Q}$ of the polynomial $T^3 - 7$.

   a. Let $\omega \in L$ be root of $\dfrac{T^7 - 1}{T - 1}$. Show that $\mathrm{Gal}(L/\mathbf{Q}(\omega)$ is cyclic, isomorphic to $\langle \sigma \rangle$. What is the order of this group (i.e. what is the order of σ)?

   b. Let $\alpha \in L$ be a root of $T^3 - 7$. Show that $\mathrm{Gal}(L/\mathbf{Q}(\alpha)$ is cyclic, isomorphic to $\langle \tau \rangle$. What is the order of this group (i.e. what is the order of τ)?

   c. Prove that $\tau\sigma\tau = \sigma^3$ in $\mathrm{Gal}(L/\mathbf{Q})$.