Dartmouth College Department of Mathematics
Math 81/111 Field and Galois Theory
Winter 2026
Final Exam Review

Directions: The final exam will take place on Monday, March 16, at 3 pm in Kemeny 307. You will have 3 hours to complete the exam. No electronic devices will be allowed. No notes, external resources, nor textbooks will be allowed to be used while you are working on the exam. However, you are allowed to bring one handwritten 2-sided 3×5 inch index card (or equivalently sized sheet of paper) to refer to during the exam. Unless stated, you will need to write your thoughts/proofs/justifications to get full credit. Below, extra practice problems listed are from: *Abstract Algebra, 3rd Edition* by Dummit and Foote (DF) and *Galois Theory, 4th Edition* by Stewart (GT).

Topics covered:

- Fields. Field extensions. Finite extensions. Degree. Tower law. Algebraic and transcendental extensions. Finitely generated fields. Quadratic formula. Compositum of extensions. GT 4.2, 4.5–4.7, 6.1–6.4, 6.6–6.9, 6.11–6.13, 16.9, 17.2, 17.6, 18.1, 18.9. DF 13.2 # 5, 8–11, 13–14, 18.
- Polynomial rings $F[x]$ and $\mathbb{Z}[x]$. Euclidean division. Euclidean algorithm. Irreducible polynomials. Ideal theory. Unique factorization. DF 13.2 # 17.
- Irreducibility criteria. Reduction modulo p. Quadratic and cubic polynomials and their discriminants (formulas provided). Gauss's lemma. Primitive polynomials. Eisenstein criterion. Irreducible polynomials over $\mathbb{F}_p$. GT 3.4–3.6, 3.8, 18.12. DF 13.1 #1–3, 7–8.
- Classification of simple extensions. Minimal polynomial. GT 5.1–5.4, 5.6–5.8, 17.7–17.12. DF 13.2 #3–4; 14.2 #1–2; 14.4 #6.
- Splitting fields. GT 9.1–9.2, 9.7. DF 13.4 # 1–6; 14.2 #3; 14.6 #48.
- Compass and straightedge. Constructable points. Quadratic closure. GT 7.4–7.5, 7.12, 7.15–7.19.
- Field automorphisms. The group $\mathrm{Aut}_F K$ for a field extension K/F. The bound $|\mathrm{Aut}_F K| \leq [K : F]$ for a finite extension K/F. Examples of towers $K/E/F$ where an F-automorphism of E does not lift to an F-automorphism of K (e.g., $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$). DF 13.1 #4; 14.1 #1–6.
- Galois extensions. Galois iff normal and separable. Finite Galois iff splitting field of separable polynomial. Galois correspondence. Normal subgroups of the Galois group. GT 10.1–10.3, 11.3–11.4, 11.6, 12.1–12.7, 13.1–13.11, 22.1, 22.6, 22.7. DF 14.2 # 4–8, 10–16.
- Galois perspective on quadratic, cubic, and quartic polynomials and their splitting fields. Discriminant. Cubic resolvant. Classification of Galois groups of quartic polynomials. GT 18.5, 18.10, 22.7. DF 14.6 #2–19.

- Normality. A finite extension is normal iff it is the splitting field of a polynomial. Transitivity (or lack thereof) properties in towers. Normal closure. GT 9.5–9.6, 9.8, 11.2. DF 14.4 #1, 5.
- Separability. Various conditions for separability of a polynomial (specifically, an irreducible polynomial), including involving the discriminant, multiplicities of roots in a splitting field, and the formal derivative. Separability of elements in a field extension. Perfect fields (i.e., characteristic zero or characteristic p and Frobenius is surjective). Every irreducible polynomial, hence every finite extension, is separable over a perfect field. DF 13.5 #5, 7.
- Roots of unity. Cyclotomic polynomials $\Phi_n(x)$. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has degree $\phi(n)$ and is Galois with group $(\mathbb{Z}/n\mathbb{Z})^\times$. Trigonometric algebraic numbers $\cos(2\pi/n)$ and $\sin(2\pi/n)$. GT 21.2–21.9, 21.13–15. DF 13.6 #1–6, 8, 10; 14.5 #1, 3, 7–10.
- Finite fields. Classification in terms of number of elements $q = p^n$. Frobenius automorphism generates the Galois group of extensions of finite fields. Construction as the splitting field of $x^q - x$. Simple generators of finite fields. GT 19.1–19.5, 19.7–19.9. DF 13.5 #2–5, 8; 14.3 #1, 4–6.
- Embeddings. If E/F is finite and L/F is arbitrary, then the set of F-embeddings $\mathrm{Hom}_F(E, L)$ satisfied the bound $|\mathrm{Hom}_F(E, L)| \leq [E : F]$. The set $\mathrm{Hom}_F(F(\alpha), L)$ is in bijection with the set of roots of the minimal polynomial of α over F that are contained in L. The automorphism group $\mathrm{Aut}_F K$ acts transitively on the roots of any irreducible polynomial over F that splits completely over K. GT 10.4, 11.1. DF 14.4 #2.
- Solvability by radicals. Review of solvable groups. Radical extensions. Solvability by radicals of polynomials. Normal closure of a radical extension is radical. Subextensions of radical extensions are not necessarily radical. Radical Galois extensions have solvable Galois group. Polynomials solvable by radicals have solvable Galois group (but not necessarily radical splitting fields). GT 14.1–14.7, 14.10, 15.1–15.10. DF 14.7 #1–6.
- Calculating Galois groups of polynomials over $\mathbb{Q}$. Complex conjugation always restricts to an element of the Galois group. Cycle type of complex conjugation in terms of number of complex conjugate pairs of roots. Dedekind's theorem on cycle types of elements of the Galois group in terms of factorization of the polynomial modulo p. DF 14.8 # 1, 3, 5.

True/False Practice:

1. Besides the additional problems in GT and Dummit and Foote (DF) listed above, you can practice on the following True/False problems covering a range of topics. See (often with a grain of salt or an eye-roll) GT Exercises 1.14, 2.9, 3.9, 4.10, 5.9, 6.16, 7.21, 8.12, 9.9, 10.5, 11.7, 12.8, 13.12, 14.13, 15.12, 16.11, 17.13, 19.12, 21.25, 22.9.