Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring Semester 2018

Instructor:	Professor Asher Auel	**Lecture:**	LOM 215
Office:	LOM 210	**Time:**	Tue Thu 11:35 am – 12:50 pm
Text:	*Galois Theory, 4th ed.*, Ian Stewart CRC Press, 2015. ISBN-13: 978-1-48-224582-0.		
Web-site:	http://math.yale.edu/~auel/courses/370s18/		

Introduction: The main object of study in Galois theory are roots of single variable polynomials. Many ancient civilizations (Babylonian, Egyptian, Greek, Chinese, Indian, Persian) knew how to solve quadratic equations. Today, most middle schoolers memorize the "quadratic formula" by heart. While various incomplete methods for solving cubic equations were developed in the ancient world, a general "cubic formula" (as well as a "quartic formula") was not known until the 16th century Italian school. It was proven by Ruffini and Abel, that the roots of the general quintic polynomial could not be solvable in terms of nested roots. Galois theory provides a satisfactory explanation for this, as well as to the unsolvability (proved independently in the 19th century) of several classical problems concerning compass and straight-edge constructions (e.g., trisecting the angle, doubling the cube, squaring the circle). More generally, Galois theory is all about symmetries of the roots of polynomials. An essential concept is the field extension generated by the roots of a polynomial. The philosophy of Galois theory has also impacted other branches of higher mathematics (Lie groups, topology, number theory, algebraic geometry, differential equations).

This course will provide a rigorous proof-based modern treatment of the main results of field theory and Galois theory. The main topics covered will be irreducibility of polynomials, Gauss's lemma, field extensions, minimal polynomials, separability, field automorphisms, Galois groups and correspondence, constructions with ruler and straight-edge, theory of finite fields. The grading in Math 370 is very focused on precision and correct details. Problem sets will consist of a mix of computational and proof-based problems.

Grading: Your final grade will be calculated according to the maximum of the following expressions. Notice that more overall emphasis is placed on exams than on weekly homework assignments. On the other hand, completing your weekly homework will be crucial to your success on the exams.

$$20\% \text{ homework} + 25\% \text{ first midterm} + 25\% \text{ second midterm} + 30\% \text{ final}$$
$$20\% \text{ homework} + 15\% \text{ first midterm} + 25\% \text{ second midterm} + 40\% \text{ final}$$
$$20\% \text{ homework} + 25\% \text{ first midterm} + 15\% \text{ second midterm} + 40\% \text{ final}$$

Exams: The midterm exams will take place in-class on Thursday 22 February and Tuesday 10 April. The final exam will take place 2:00 – 5:30 pm on Saturday 05 May. Make-up exams will only be allowed with a dean's excuse. The use of electronic devices during exams will not be allowed.

Homework: There will be weekly problem sets assigned (except for the weeks of the midterm exams), due in class on Thursday. The problem sets will be posted on the course web-site syllabus page the week before they are due. Your lowest problem set score of at least 50% will be dropped from your final grade calculation. Unless submitted with a Dean's excuse, late problem sets turned in within one week of the deadline will be worth only 50% of its score. After one week, problem sets will not be accepted. If you know in advance that you will be unable to submit your homework at the correct time and place, you must make special arrangements ahead of time.

Consider (as you would for any other class) the pieces of paper you turn in as a final copy: written neatly and straight across the page, on clean paper, stapled together, with nice margins, lots of space, and well organized. You might consider taking the opportunity to learn LaTeX.

Group work, honestly: Working with other people on mathematics is not only allowable, but is highly encouraged and fun. You may work with anyone (e.g., other students in the course, students not in the course, tutors) on the rough draft of your problem sets. If done right, you'll learn the material better and more efficiently working in groups. The golden rule is:

> You may work with anyone on *solving* your homework problems,
> but you must *write* up your final draft by yourself.

Writing up the final draft is as important a process as figuring out the problems on scratch paper with your friends. Mathematical writing is very idiosyncratic—it is easy to tell if papers have been copied from others or from the internet—just don't do it! You will not learn, and will engage in academic dishonesty, by copying solutions! Also, if you work with people on a particular assignment, you *must list your collaborators at the top of the paper*, as well as any resources (e.g., Wikipedia) used beside the text book. All claims in your solutions must be fully and rigorously justified. You are free to cite results from lecture, from the book, and within reason, from anywhere else (as long as it doesn't make the problem trivial). Make the process fun, transparent, and honest.

Peer tutor: This course has its own peer tutor, Jason Gaitonde, who will hold office hours twice weekly to help with problem sets, preparing for exams, or reviewing material from lecture. Jason is also available for private meetings and to answer questions via email, so just contact him.

Prerequisites: Previous exposure to linear and abstract algebra is required. For example, the contents of Math 225 Linear Algebra and Matrix Theory and Math 350 Abstract Algebra, are recommended.

Topics covered: Subject to change.

(1) Review of polynomial rings. Euclidean division. Euclidean algorithm for calculating gcd. Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD. Polynomials as functions. Roots as linear factors.

(2) Fundamental Theorem of Algebra. Irreducibility of polynomials. Gauss's Lemma. Eisenstein Criterion. Reduction modulo p. GT 2.2, 3.1–3.6.

(3) Field extensions. Degree. Simple extensions. Algebraic and transcendental extensions. Minimal polynomial. Field automorphisms. GT 4.1–4.3, 5.1–5.4, 6.1–6.2, 17.1.

(4) Ruler and compass constructions. Solvable numbers. GT 7.1–7.4.

(5) Separability. Derivations. Perfect fields. GT 9.3, 17.5.

(6) Linear independence of characters and embeddings (Dedekind's Lemma). Normal closure. GT 10.1, 11.1–11.2.

(7) Galois extensions. The Galois group of a polynomial. Galois correspondence. GT 8.1–8.8, 12.1, 17.6.

(8) Primitive element theorem. Solvable fields. Solving for roots with radicals. GT 13, 14.1–14.3, 15.1–15.3.

(9) Finite fields. Cyclic extensions. GT 19.1–19.2.

(10) Elementary symmetric polynomials. General polynomial. Discriminant. GT 18.2–18.3.

(11) Solving equations of degree at most 4. Calculating Galois groups. Cyclotomic extensions. Proving the Fundamental Theorem of Arithmetic. GT 18.5, 21.5–21.6, 22.1–22.4.

Yale University, Department of Mathematics, 10 Hillhouse Ave, New Haven, CT 06511
E-mail address: asher.auel@yale.edu