Yale University Department of Mathematics
Math 350 Introduction to Abstract Algebra
Fall Semester 2016

Instructor:	Professor Asher Auel	**Lecture:**	LOM 206
Office:	LOM 210	**Time:**	Mon Wed Fri 10:30 – 11:20 am

Text:	*Abstract Algebra, 3rd ed.*, Dummit and Foote John Wiley & Sons, 2004. ISBN-13: 978-0-471-43334-7.
Web-site:	http://math.yale.edu/~auel/courses/350f16/

Introduction: Abstract Algebra is the study of mathematical structures carrying notions of "multiplication" and/or "addition." Though the rules governing these structures seem familiar from our middle and high school training in algebra, they can manifest themselves in a beautiful variety of different ways. The notion of a group, a structure carrying only multiplication, has its classical origins in the study of roots of polynomial equations and in the study of symmetries of geometrical objects. Today, group theory plays a role in almost all aspects of higher mathematics and has important applications in chemistry, computer science, materials science, physics, and in the modern theory of communications security.

The main topics covered will be (finite) group theory, homomorphisms and isomorphism theorems, subgroups and quotient groups, group actions, the Sylow theorems, ring theory, ideals and quotient rings, Euclidean domains, principle ideal domains, unique factorization domains, module theory, and vector space theory. Time permitting, we will investigate topics such as the reflection groups of platonic solids and the mathematics behind public key cryptography systems such as RSA. This will be a heavily proof-based course with homework requiring a significant investment of time and thought. The course is a must for all students interested in studying higher mathematics, and would be helpful for those considering entering subjects such as computer science and theoretical physics.

Grading: Your final grade will be calculated according to the table at right. 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.

Homework	35 %
Quizzes	10 %
Midterm (Mon 17 Oct)	20 %
Final Exam (Tue 20 Dec)	35 %

Exams: The quizzes will be announced at least a week ahead of time. The midterm exam will take place in-class on Monday 17 October 2016. The final exam will take place 2:00 – 5:30 pm on Tuesday 20 December 2016. Make-up quizzes and exams will only be allowed with a dean's excuse. The use of electronic devices during quizzes and exams will not be allowed.

Homework: You will be assigned a weekly problem set, due in class on Friday. There will be no problem sets due the week of midterm exams. The problem sets will be posted on the course web-site syllabus page the week before they are due. Your lowest problem set score will be dropped from your final grade calculation. *Late or improperly submitted homework 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. *If it's not readable, it won't be graded.* You should strongly consider starting with a rough draft, especially on problems requiring a proof. You will need to show your work on computational problems. 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, bums on the street) 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—just don't do it! You will not learn by copying solutions from others or from the internet! 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, Wolfram Alpha) used beside the text book. Make the process fun, transparent, and honest.

Prerequisites: The official prerequisite is linear algebra, either Math 222 or 225, in in reality, all that is required is a mature mathematical mind, some experience with writing proofs, and the desire to work incredibly hard.

Topics covered: Subject to change.

(1) Basic set theory and notations. Set. Subset. Inclusion. Cardinality. Cartesian product. Function. Domain/codomain. Injection/surjection. Inverse. Equivalence relation. Modular arithmetic. DF 0.1–0.3.

(2) First examples of groups. Cyclic groups. Dihedral groups. Symmetric groups. Quaternion group. Matrix groups. Homomorphism. Isomorphism. DF 1.1–1.6.

(3) Subgroups. Group actions. Lagrange's Theorem. Centralizers. Normalizers. Stabilizers. Kernels. Normal subgroups. Cyclic subgroups. Generating sets. DF 1.7, 2.1–2.5.

(4) Quotient groups. Cosets. Isomorphism theorems. Simple groups. Jordan–Hölder. Alternating group. DF 3.1–3.5

(5) Group actions. Permutation representation. Cayley's theorem. The class equation. Automorphism groups. Sylow's theorem. DF 4.1–4.5.

(6) Direct products. Structure of finitely generated abelian groups. Semidirect products. Classifying groups of small order. p-groups. Nilpotent groups. DF 5.1–5.5, 6.1.

(7) First examples of rings. Fields. Ring of integers. Hamilton quaternions. Rings of functions. Integral domains. Subrings. Ideals. Polynomial rings. Matrix rings. Group rings. Quadratic number rings. Homomorphisms. DF 7.1–7.3.

(8) Subrings. Ideals. Quotient rings. Isomorphism theorems. Ring of fractions. Chinese remainder theorem. DF 7.3–7.6.

(9) Euclidean domains. Principal ideal domains. Unique factorization domains. DF 8.1–8.3.

(10) Polynomial rings. Gauss' lemma. Roots. Irreducibility. Eisenstein's criterion. DF 9.1–9.5.

(11) Modules. Submodules. Quotient modules. Module homomorphisms. Module isomorphism theorems. Generators. Direct sums. Free modules. Tensor products. DF 10.1–10.4.

(12) Modules over a PID. Fundamental theorem. Elementary divisors. Primary decomposition. Invariant subspaces. Rational canonical form. Jordan canonical form. DF 12.1–12.3.

(13) (Optional topic) Public key cryptography systems such as RSA.