Lecturer: Prof. Madhu Sudan
Teaching Fellow: Jaroslaw Blasiok
Course website: http://madhu.seas.harvard.edu/courses/Fall2016
Staff e-mail: am106-f16-staff@seas.harvard.edu
Time & place: MW 2:30-4, Maxwell-Dworkin G115

Summary

Algebra is the study of operations (such as addition, multiplication, composition) on sets of objects (such as numbers, polynomials, matrices, permutations). In addition to studying specific operations on specific sets, we also abstract properties that such operations commonly satisfy and the implications of these properties, thereby unifying the study of a wide variety of mathematical objects. In addition to being a beautiful subfield of mathematics, algebra has numerous applications in science and engineering. It is extremely useful for studying symmetries of physical objects, and for encoding data and computations to provide properties such as error-correction and privacy.

In this course, we will cover:

- The basics of abstract algebra (groups, rings, fields)
- Algorithmic aspects of algebra: which algebraic problems have (efficient) algorithms, and which do not.
- Applications of algebra to science and engineering

Tentative Topics

1. Introduction (1 lecture)
2. The Integers (2 lectures)
    - General Theory (Gallian Ch. 0): induction, gcds, prime factorization, modular arithmetic
    - Algorithmic Aspects: O notation, complexity of arithmetic, factorization, Euclidean algorithm
3. Group Theory (9 lectures)
    - General Theory (Gallian Chs. 1-11): groups, subgroups, cyclic groups, permutation groups, isomorphism, cosets, products, quotients, homomorphisms, classification of finite abelian groups.
    - Algorithmic Aspects: presentations of groups, undecidability of general group membership, algorithms for permutation groups, complexity of discrete logarithms
    - Applications: symmetry groups, public-key cryptography, equivalence of log-depth circuits and constant-width branching programs, secure function evaluation, solving Rubik's cube, expander graphs.
4. Rings and Fields (9 lectures)
    - General Theory (Gallian Chs. 12-22): rings, integral domains, ideals and quotients, ring homomorphisms, polynomial rings, vector spaces, extension fields, algebraic extensions, finite fields.
    - Algorithmic aspects: polynomial arithmetic, polynomial factorization, polynomial identity testing, irreducibility testing, finite field arithmetic.
    - Applications: error-correcting codes, secret sharing, secure multiparty computation, k-wise independent probability spaces, fast integer multiplication
5. Conclusion (1 lecture)

The above list is overly ambitious for the time we have. We will certainly not be able to cover all of the algorithmic aspects and applications mentioned, but AM 206 students will have the opportunity to explore some of these as part of their "extra assignments".

Prerequisites

The formal prerequisite for the course is (Applied) Math 21ab or equivalent, but general "mathematical maturity" is more important than the specific material in these courses. At times, we will assume familiarity with basic linear algebra as covered in Math 21b, but students who have instead taken a prior proof-based course on a different topic (such as AM 107, Math 101, CS 121, or CS 124) should also be adequately prepared.

Grading

AM 106 students:

- Weekly problem sets: 50% (lowest score dropped)
- Two in-class quizzes: 10% each
- Final exam: 25%
- Class participation: 5%

AM 206 students:

- Weekly problem sets: 50% (lowest score dropped)
- Two (7-8 page) essays on advanced topics of your choice & 1 presentation in the week of November 28, 2016: 5% each
- Two in-class quizzes: 5% each
- Final exam: 20%
- Class participation: 5%

Your class participation grade is based on participation in lecture, but can also be boosted by participation in section and/or coming to office hours or section with questions or comments that show genuine interest in the material (i.e. is not just aimed to help you answer questions on the problem set or exam). Do not be afraid of asking "stupid" questions!

AM206 problem sets will have some more advanced problems substituted in..

Problem Sets & Collaboration Policy

The course will have weekly problem sets, due by 11:59PM *sharp* electronically via Canvas. You are allowed 6 late days for the semester, of which at most 2 can be used on any individual problem set. (1 late day = 24 hours exactly). For any exceptions to these rules, I require a note from your senior tutor.

Students are encouraged to discuss the course material and the homework problems with each other in *small* groups (2-3 people). Discussion of homework problems may include brainstorming and verbally walking through possible solutions, but should not include one person telling the others how to solve the problem. In addition, each person must write up their solutions independently, and these write-ups should not be checked against each other or passed around.

While working on your problem sets, you may not refer to existing solutions, whether from other students, past offerings of this course, materials available on the internet, or elsewhere. All sources of ideas, including the names of any collaborators, must be listed on your homework paper.

Sections

There will be weekly sections, which will be used to clarify difficult points from lecture, review background material, go over previous homework solutions, and sometimes provide interesting supplementary material.

Readings

The handouts for the course will be made available at the <href="http: madhu.seas.harvard.edu="" courses="" fall2016"="">course website. These will be required reading. The recommended text is:

Joseph A. Gallian. Contemporary Abstract Algebra, 9th edition.

It has been ordered at the Coop, and placed on reserve in the libraries. This book will include most of the topics covered in the course, and a lot more too, but it will not cover all the topics in the course. In particular it does not cover some of the applications and the algorithmic discussions. So it is important that you also attend lecture.

Related Courses at Harvard

- Math 122 &123: Algebra I & II. A full-year course in abstract algebra. Because it is longer and assumes more background, Math 122-123 covers a number of topics that we cannot fit in AM 106, such as group representations, modules, and Galois theory. (Students taking AM 206 can study some of these topics for their additional assignments.) On the other hand, it usually does not include the algorithmic aspects and applications of algebra that we will cover in AM 106.
- Math 152: Discrete Mathematics. A seminar-style course covering a variety of related topics in

abstract algebra and discrete mathematics. My guess is that it has significant but not complete overlap with the "general theory" we cover, but that it has not much overlap with the applications and algorithmic issues we cover.

- Computer Science theory (x2x) courses. A number of the applications and algorithmic aspects of algebra that we will cover (and others) also appear scattered in various theoretical computer science courses. In AM 106, we will have time to do a more systematic treatment, in which these applications are integrated with the general study of abstract algebra (rather than taking algebraic facts on faith, or doing a quick "crash course").