# Carleton University
# School of Mathematics and Statistics

## MATH 2108 Abstract Algebra I and MATH 3101 Algebraic Structures with Computer Applications

## Winter 2024

**Instructor**: Daniel Panario
Email: daniel@math.carleton.ca
http://www.math.carleton.ca/∼daniel

**Day and time of course:** Tuesdays and Thursdays 11:35 - 12:55.
**Room:** in Southam Hall 317.

**Office hours:** Thursdays 10:05 - 10:55 in HP4372.

**Textbook:** "*Elements of Modern Algebra*" by J. Gilbert and L. Gilbert, 8th edition.

**Prerequisites:** (1) MATH 2152 or MATH 2107; and (2) MATH 1800 (MATH 1800 may be taken concurrently); or COMP 1805 or permission of the School.

**Course Objective:** This course introduces students to algebraic structures such as groups, rings, and fields, and their applications to automata theory and cryptography.

**Evaluation:** Five tests in tutorials (50%), and a final exam (50%).

The best 4 out of the 5 tests will be considered for the final grade. Each test contributes 12.5% of the final marks. No make up, early or delayed, tests will be given. Missed tests count as zero.

You must pass the term work in order to pass the course (that is, 25% of the 50% on tests). If you have a passing term mark (50% in total for the five tests) and you do better in the final exam, then I will count the final exam for 100% of the course.

**Tutorials:** Thursday 8:35 - 9:25 am in Southam Hall 317.
**Teaching assistant**: TBA.
Tutorials begin on Thursday January 18, 2024.

**Tests:** There will be five tests on January 25, February 8 and 29, and March 14 and 28. Tests are in tutorial; each test is worth 12.5% of the final mark (best 4 out of 5).

**Final Exam:** This is a three hour closed-book exam scheduled by the University that will take place sometime during the examination period.

### Academic Accommodation

You may need special arrangements to meet your academic obligations during the term. For an accommodation request the processes are as follows:

Pregnancy obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website.

Religious obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website.

Academic accommodations for students with disabilities: The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send me your Letter of Accommodation at the beginning of the term, and no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with me to ensure accommodation arrangements are made. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable).

## Tentative lecture schedule

This weekly outline is subject to change depending on the progress of the course. The sections are from the textbook.

| Week | Dates | Sections | Topics |
|---|---|---|---|
| 1 | Jan. 9-11 | 1.1-1.4; 1.7 | Introduction. Revision of sets, mappings, composition, binary operations and relations. |
| 2 | Jan. 16-18 | Course notes | Monoids, automota and formal languages. |
| 3 | Jan. 23-25 | 2.3-2.4 | Divisibility, primes, gcd, unique factorization. **Test 1.** |
| 4 | Jan. 30 - Feb. 1 | 2.5-2.6 | Congruence of integers, Chinese remainder theorem, congruence classes. |
| 5 | Feb. 6-8 | 2.8; 3.1 | Introduction to cryptography, RSA. Groups, examples. **Test 2.** |
| 6 | Feb. 13-15 | 3.2-3.3 | Properties of group elements, subgroups, cyclic groups and subgroups. |
| | Feb. 20-22 | | Winter break, no classes. |
| 7 | Feb. 27-29 | 3.4-3.6 | Generators, infinite and finite cyclic groups, order of elements. Isomorphisms, homomorphisms, kernel, image. **Test 3.** |
| 8 | Mar. 5-7 | 4.1-4.2 | Permutation groups, cycles, transpositions, alternating groups, Cayley's theorem. |
| 9 | Mar. 12-14 | 4.4-4.5 | Cosets, Lagrange's theorem, normal subgroups. **Test 4.** |
| 10 | Mar. 19-21 | 4.6; 5.1-5.2 | Quotient groups, homomorphism theorem. Rings, $\mathbb{Z}_n$, integral domains and fields. |
| 11 | Mar. 26-28 | 6.1-6.2; 6.4 | Ideals and quotient rings; maximal ideals and fields. **Test 5.** |
| 12 | Apr. 2-4 | 8.1-8.3 | Ring of polynomials, extended Euclidean algorithm, factorization of polynomials. |
| 13 | Apr. 9 | 8.6; course notes | Algebraic extensions; AES (the Advanced Encryption Standard). Course review. |