MAT 373 Modern Algebra I

Department of Mathematics
Southern Connecticut State University

I. Catalog Description

Introduction to the study of algebraic structures and their applications. Topics include elementary number theory, abstract groups, cyclic and permutation groups, homomorphisms, normal subgroups, quotient groups, applications to algebraic coding theory and public-key cryptography, and a brief introduction to rings and fields.

II. Purpose

MAT 373 introduces students to some of the basic ideas of abstract algebra and how they relate to some of the more concrete settings of elementary number theory, geometry, linear codes and public-key cryptography. Upon completion of the course, students should be able to demonstrate satisfactory knowledge of the basic notions of abstract algebra and have a sense of their applicability, and they should be able to construct symbolically accurate and mathematically correct proofs of basic facts pertaining to groups and elementary number theory.

III. Credit

MAT 373 carries 4 semester hours of university credit. It is required of mathematics majors pursuing a B.S. with 7-12 Certification or concentration in Pure Mathematics. It is an elective for the other concentrations in the B.S. in mathematics program.

IV. Prerequisites

The student must have passed MAT 250 and MAT 372 with a C- or better in each.

V. Format

MAT 373 is offered in the lecture-discussion format. Classes will meet for four contact hours per week.

VI. Course Objectives

Upon completion of MAT 373, students should:

(1) Possess a basic but solid knowledge of mathematical objects encountered during their undergraduate math career thus far (such as numbers, matrices, polynomials, functions, sets) and recognize the algebraic similarities they share.

(2) Understand the concept of binary operation on a set and the idea of an algebraic structure (a set endowed with operations that satisfy certain axioms).

(3) Understand the role of basic group theory in elementary number theory, coding theory (linear codes) and cryptography (public-key)

(4) Make connections between groups and familiar geometric objects such as a regular n-gon, tetrahedron, cube and so on (via the dihedral and symmetric groups)

(5) Be able to prove elementary facts about groups and elementary number theory by logically combining definitions and theorems.

(6) Acquire knowledge about the ways to obtain new algebraic structures out of old ones (e.g. sub-structures, quotient structures, direct products)

(7) Learn new ways of denoting familiar objects (e.g. cyclic notation for permutations)

(8) Recognize when two algebraic structures are abstractly "the same" (in other words, internalize the concept of isomorphism)

VII. Outline

I. **Number Theory (about 13 lectures, or** 38%**)**

1. The division algorithm
2. Divisibility
3. The Euclidean Algorithm
4. The Diophantine equation $ax + by = c$
5. The Fundamental Theorem of Arithmetic
6. Congruence and congruence classes
7. Modular Arithmetic
8. Binary and decimal representation of integers
9. Linear congruences and Chinese Remainder Theorem
10. Fermat's Little Theorem and pseudoprimes
11. Wilson's Theorem
12. The structure of $\mathbb{Z}_p$ and $\mathbb{Z}_n$
13. Public-Key Cryptography

II. **Group Theory (about 18 lectures, or** 53%**)**

1. Definitions and examples of groups
2. Basic properties of groups
3. Subgroups and direct products
4. Isomorphisms and homomorphisms
5. Algebraic coding theory (linear codes)

6. The symmetric and alternating groups
7. Congruence and Lagrange's Theorem
8. Normal Subgroups
9. Quotient groups
10. Quotient groups and homomorphisms

III. **Ring Theory (about 3 lectures, or 9%)**

1. Definition and examples of rings and fields.

VIII. Recommended Texts

1. Thomas W. Hungerford, *Abstract Algebra, An Introduction*, 3rd Edition, Brooks/Cole (Cengage), 2016.
2. David M. Burton, *Elementary Number Theory*, 7th Edition, McGraw-Hill Education, 2010.
3. Joseph H. Silverman, *A Friendly Introduction to Number Theory*, 4th Edition, Pearson, 2011.
4. Joseph A. Gallian, *Contemporary Abstract Algebra*, 10th Edition, CRC Press, 2021.

IX. Waiver Policy.

Course credit or waiver by examination are available for this course.

X. Preparation

Prepared and proposed by A. D'Amour and J. Hong, November 2021.