Dr. Rocca
Email: roccac@wcsu.edu
Site: https://sites.wcsu.edu/roccac/
Telephone: (203) 867-9360

Applied Abstract Algebra
Meeting Time: Day TBA 5:30-8pm
Grading: Standard A-F
Credits: 3
Prerequisite: MAT 375 or Equivalent

Office Hours:

Office hours are on ground this semester. If you need to meet virtually, we can make an appointment to do so via my WebEx Virtual Office: Higgins 101-DV (https://westconn.webex.com/meet/roccac)

Monday: 1:00 pm - 2:00 pm

Tuesday: 1:00 pm - 2:00 pm

Wednesday: None

Thursday: 1:00 pm - 2:00 pm, 3:30 pm - 4:30 pm

Friday: 1:00 pm - 2:00 pm

or by appointment

Course Materials:

For this course you will need:

- "Abstract Algebra: An Introduction, 3rd edition" by Thomas Hungerford
- A notebook which you need to bring to each class.

Course Description and Outcomes:

In this course students will expand their knowledge of Abstract Algebra and its applications. Generally, this course looks at common properties and applications of matrix arithmetic, modular arithmetic, polynomial rings over fields in general and finite fields in particular, and groups over elliptic curves. The specific applications will be focused around algorithms for computer science, information security, and algebraic coding theory.

After completing this course students will be able to

- Clearly define and give examples of common algebraic structures such as groups, rings, integral domains, fields, modules, and vector spaces.
- Explain the properties common to the different algebraic structures as well as properties which distinguish them.
- Demonstrate how we derive fundamental properties from the basic definitions.
- Compare the First Isomorphism Theorems for groups and rings and understand how they compare to the Rank and Nullity Theorem from linear algebra.
- Describe the relation between, irreducible polynomials, maximal ideals, and field extensions.
- Sketch out the general idea of quotient structures built from equivalence relations as a generalization of quotient groups and rings.
- Outline key arguments in the proofs of the First Isomorphism Theorems, Lagrange's Theorem, Cayley's Theorem, and Cauchy's Theorem
- Outline applications of groups, rings, and other structures to computer science, information security, and error correcting codes.

Course Content:

- **Exploration of Algebraic Structures**: For this unit we will focus on the mechanics of the examples we will draw upon for the semester. Some of this will be review of previously encountered ideas such as matrix arithmetic and modular arithmetic, but we will also be looking at polynomials over finite fields and arithmetic on elliptic curves which will likely be new to students. In the text we are using for this class this will pull material from chapters 1, 2, and 4 and from additional handouts.

- **Rings, Integral Domains, and Fields**: In this unit we look at definitions and fundamental properties for rings, integral domains, and fields. Since some of the basic concepts may be familiar to students, we will be placing emphasis on demonstrating understanding of why things work the way they work. Particularly we will be looking at relations between quotient rings and field extensions. In the text we are using for this class this will pull material from chapters 3, 4, 5, 6, and 11.
- **Applications of Rings and Fields**: In this unit we will take what we learned about rings and fields and see how to apply it to performing arithmetic with bytes, information security, and understanding the limitations of geometric constructions. In the text we are using for this class this will pull material from chapters 13, 14, and 15 and from additional handouts.
- **Groups**: In this unit we look at definitions and fundamental properties of groups. Again, some of the basic concepts may be familiar to students, so we will be placing emphasis on demonstrating understanding of why things work the way they work. In the text we are using for this class this will pull material from chapters 7 and 8.
- **Applications of Groups**: In this last unit we look at how we can apply out knowledge of group theory to encryption algorithms defined on elliptic curves and to algebraic coding theory. In the text we are using for this class this will pull material from chapter 16 as well as from additional handouts.

Assessments and Grades:

Your grade in this class will be a weighted average as follows:

- 25% In Class Participation
- 25% Out of Class Assignments
- 25% Comprehensive Ring Theory Exam
- 25% Comprehensive Group Theory Exam

In Class Participation (Quizzes?) (25%): We will begin most classes with discussion of questions related to the previous class to insure we are all staying on top to the material. Preferably this will be an open discussion, but if there is a lack of participation we will have quizzes. We will also occasionally have in class work sheets which you will hand in and will count toward this grade.

Out of Class Assignments (25%): You will need to complete some work out of class. For the most part this will be exercises from the textbook, but for some topics I will pull questions from other sources.

Comprehensive Ring Theory Exam (25%): For this exam you will need to be able to:

- Give definitions of rings, zero divisors, units, integral domains, fields, quotient rings, irreducible polynomials, field extensions, ideals, homomorphisms, isomorphisms, and kernels.
- Give examples of various rings and their properties.
- Explain/discuss the connection between field extensions, quotient rings, and maximal ideals.
- Outline a proof of the First Isomorphism Theorem for Rings.
- Demonstrate how to carrying out arithmetic on bytes of information and the connection to quotient rings.
- Explain arithmetic over finite fields and its use in encryption schemes.
- Explain why there are limitations on geometric constructions with straightedge and compass in the context of field extensions.

Comprehensive Group Theory Exam (25%): For this exam you will need to be able to:

- Give definitions of groups, subgroups, normal subgroups, Sylow p-subgroups. quotient groups, cosets, permutations, homomorphisms, isomorphisms, and kernels.
- Give examples of various groups and their properties.
- Outline proofs of First Isomorphism Theorem, Lagrange's Theorem, Cayley's Theorem, and Cauchy's Theorem.

- Explain the uses of groups and permutations in various encryption schemes.
- Explain key points in Algebraic Coding Theory and how they are connected to groups and to matrix operations.

Exam Collaboration: At the start of each exam you will be given 15 minutes during which you can look it over and discuss the exam with your fellow students. During this time you cannot write down anything on the exam, or other paper, and you cannot use your calculator. Once the 15 minutes are up you will need to complete the exam on your own.

Exam Redos: For each unit exam you will be allowed to redo some specific questions in order to earn back up to 40% of the points you lost. Which questions you redo and how many questions you redo will depend on how you did on the exam. Redos are due within one week of when the exams are handed back, you must turn in the original exam stapled on top of the redos, and for each question you redo you must include a sentence or two explaining what you did wrong.

Writing Math Exercise: In order to help you understand what it means to write up mathematics in a neat and professional manner, you are required to complete the ***Exercises in Writing Up Mathematics*** packet. After this is completed, you will be expected to use what you learned when writing up out of class work. This will count as one of your out of class assignments.

Quality of Work Guidelines: All the out of class work you turn in must be neat and professional. Answers must be in complete sentences. The quality of your work on out of class work (assignments, projects, and redos) counts for up to 10% of your grade.

Class Calendar:

Meeting Day (The Day We Meet)	
1/22 Syllabus, matrices, and modular arithmetic	**1**
1/29 Polynomials and elliptic curves	**2**
2/5 Definitions and fundamental properties of rings, integral domains, and fields	**3**
2/12 Homomorphisms and isomorphisms of rings, kernels, and ideals	**4**
2/19 First isomorphism theorem, irreducible polynomials, and field extensions	**5**
2/26 Applications of rings and fields: Arithmetic with bits and bytes, and information security	**6**
3/5 Applications of rings and fields: Information security continued, and geometric constructions	**7**
3/12 Review and Comprehensive Ring Theory Exam	**8**
3/19 Spring Break	

Meeting Day (The Day We Meet)	
3/26 Definitions and fundamental properties of groups (Modular Arithmetic, Matrices, Elliptic Curves, Dihedral Groups, Permutation)	**9**
4/2 Normal subgroups, cosets, and Lagrange's Theorem	**10**
4/9 Homomorphisms, kernels, and the First Isomorphism Theorem	**11**
4/16 Groups as permutations and Cayley's Theorem	**12**
4/23 Cauchy's Theorem and Sylow p-subgroups	**13**
4/30 Applications of groups: Elliptic curves and modular arithmetic in information security	**14**
5/7 Applications of groups: Matrices to algebraic coding	**15**
5/14 Final Exam Week: Comprehensive Group Theory Exam	**16**

Course Outline:

1. Examples of Algebraic Structures
   (a) Matrix Operations
      i. Addition and Multiplication
      ii. Determinants
      iii. Multiplicative Inverses and Zero Divisors
      iv. Matrices as Linear Maps with Null Spaces
   (b) Integers Modulo n and p
      i. Divisibility
      ii. Well Ordering Principle and the Division Algorithm
      iii. Modular Congruence (Clock Math)
      iv. Modular Congruence is an Equivalence Relation
      v. Modular Congruence Respects Arithmetic (exponentiation, multiplication, addition)
      vi. Multiplicative Inverses (Units) and Zero Divisors
   (c) Polynomials with Rational Coefficients
      i. Divisibility
      ii. Remainder and Factor Theorems
      iii. Division Algorithm for Polynomials
      iv. Irreducible Polynomials
      v. Congruence with Polynomials
   (d) Elliptic Curves
      i. Definition and Comments on Discriminants
      ii. Adding on a Curve
      iii. Elliptic Curves Modulo p
2. Rings, Integral Domains, and Fields
   (a) General Definitions
   (b) Properties of All Rings
   (c) Multiplicative Inverses and Zero Divisors
   (d) Orders and Characteristics
      i. Fermat's Little Theorem
      ii. Euler's ϕ-Function and integers modulo pq
   (e) Integral Domains and Fields
   (f) Homomorphisms
      i. General Definition
      ii. Kernels and Ideals
      iii. The First Isomorphism Theorem for Rings
      iv. Isomorphisms
      v. Endomorphisms and Automorphisms
   (g) Field Extensions and Quotient Rings
3. Groups
   (a) General Definitions
   (b) Properties of All Groups
   (c) Orders
   (d) Subgroups and Cosets
      i. Definitions
      ii. Relation to Orders
      iii. Lagrange's Theorem
   (e) Homomorphisms

   i. General Definition
   ii. Kernels and Normal Subgroups
   iii. The First Isomorphism Theorem for Groups
   iv. Isomorphisms
   v. Endomorphisms and Automorphisms
   vi. Permutations and Cayley's Theorem
   vii. Cauchy's Theorem and Sylow p-subgroups
4. Application
   (a) Arithmetic with Bits and Bytes using Galois Fields and Quotient Rings
   (b) Fermat, Factoring, and Primes
      i. Fermat Factorization
      ii. Probabilistic Primality Testing
   (c) One Way Functions and Discrete Logarithms
      i. Chinese Remainder Theorem
      ii. Fast Exponentiation and Multiplication with Numbers and Curves
      iii. RSA, Diffie-Hellman, and ElGamal
   (d) Geometric Constructions
   (e) Algebraic Coding Theory

End User Agreement:

General Expectations: As a student in this class you are expected to:

- attend class and take notes,
- actively read material in each section, taking notes,
- review your notes on a regular basis,
- check your university email every day,
- check the class site **at least** every other day,
- begin studying for exams in a timely fashion,
- ask questions early and often,
- attend office hours,
- seek help in the math clinic, and
- complete assignments and readings on time.

Assignment Guidelines: (These apply to **all out of class work**.)

- Work done outside of class must always look neat, legible, and professional, adhering to given guidelines. Work must be very neatly written or preferably typed. The quality of your work will be factored into your grade, up to 10%. In extreme cases work may be rejected and then counted as late.
- An assignment is considered late after I have handed it back or gone over it in class. Late assignments are accepted but may receive at most 75% credit. Late assignments go to the absolute bottom of the stack of papers to be graded; **all on time work is graded before any late work.**
- If you work on an assignment as part of a group, then there may be no more than three individuals in the group and all your names must be on the assignment. You should hand in only one copy of the work.
- All work must be submitted in the manner directed.

Email Etiquette Guidelines: When sending an email you must include the course number and semester in the subject line. For example, if you are taking MAT 314 in Fall 1592 then the the subject line should begin with "[MAT 314 Fall 1592]." Also, you should always begin with a salutation such as "Dear Dr. Rocca" and end with a closing such as "Sincerely, I. Newton."

Technology Use: You are free to use technology in the classroom to support the learning of the content, i.e. for note taking, recording, taking pictures of the board etc.. Technology use will be restricted if it becomes disruptive, a distraction, or invades others privacy.

Exam Makeup Policy: To qualify for a makeup exam you must have a valid reason for missing the exam and, if at all possible, let me know ahead of time that you are missing the exam. You will need to meet with me in order to arrange a time for the make up exam. If you do not have a valid reason, do not give prior notice when possible, or simply do not show up for an exam, you are not entitled to a makeup and will not be given one. If you fail to show up for your makeup exam, you will not be given a second opportunity.

The 2% Exception: If a class has any quiz or class work which is ultimately worth no more then 2% of your final grade can not be made up.

Time on Task: As a 3 credit class you should expect to average 8.0 hours of work a week including class time. Some weeks you may get away with less and some may require more.

Attendance: Unless otherwise stated, there is no specific policy for attendance in this course. However, if you have **three consecutive unexcused absences** within the first half of the semester I am required to report to the University that you have **stopped attending**.

Academic Honesty: If on any assignment, quiz, or exam you turn in someone else's work, regardless of the source, as if it were your own you will receive a zero on that assignment, quiz, or exam. If you are caught doing this three times you will receive an F in the course and the Dean will be informed of your academic dishonesty.
(https://www.wcsu.edu/faculty-handbook/2019-2020/policies-pertaining-to-students/academic-honesty-policy/)

Accommodations: If you have need of an accommodation for testing or note taking, please visit AccessAbility Services, located in the HAAS Library room 406 (http://www.wcsu.edu/accessability).

You and Your Grades:

- "A" (Exceptional) range 90% to 100%:
  The student has demonstrated significant mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve standard formulaic exercises and most nonstandard problems which require deeper insight.
- "B" (Good) range 80% to 90%:
  The student has demonstrated mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve standard formulaic exercises and some nonstandard problems which require deeper insight.
- "C" (Adequate) range 70% to 80%:
  The student has demonstrated adequate mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve most standard formulaic exercises but struggles with nonstandard problems which require deeper insight.
- "D" (Inadequate) range 60% to 70%:
  The student has demonstrated inadequate or incomplete mastery of the appropriate knowledge and skills relevant to the course. The student is able to solve some standard formulaic exercises but few if any nonstandard problems which require deeper insight.
- "F" (Unacceptable) below 60%:
  The student has demonstrated essentially no mastery of the appropriate knowledge and skills relevant to the course. The student is unable to solve most standard formulaic exercises and essentially no nonstandard problems which require deeper insight.

Inspire Your Professors:

What to do:

- Show up, on time, ready to learn.
- Ask, and try to answer, questions.
- Put in the time and do the scut work.
- Seek help when you need it, utilize the resources available to you.
- Be an active participant in class and in your own education.
- Be curious about everything and be here to learn.

What not to do:

- Don't ask "What is this good for?"
- Don't ask "Did I miss anything?"
- Don't say "I don't get *it*."
- Don't fiddle with your phone or computer.
- Don't wander in late and rush out early.
- Try not to repeat questions that have just been asked and answered, sometimes multiple times.
- Don't just grub for points.
- Don't be a passive passenger to your own education.