This course requires a performance assessment. It covers 4 competencies.

**Introduction**

**Overview**

Abstract Algebra is the axiomatic and rigorous study of the underlying structure of algebra and arithmetic. It covers the knowledge and skills necessary to understand, apply, and prove theorems about numbers, groups, rings, and fields. Topics include the well-ordering principle, equivalence classes, the division algorithm, Euclid's algorithm, prime factorization, greatest common divisor, least common multiple, congruence, the Chinese remainder theorem, modular arithmetic, rings, integral domains, fields, groups, roots of unity, and homomorphisms. Candidates should have completed Linear Algebra before engaging in this course.

**Getting Started**

Welcome to Abstract Algebra! The textbook, *An introduction to abstract algebra with notes to the future teacher*, is non-interactive, so you will need to follow the traditional ritual of reading, doing exercises, and checking the answers in the back of the book. There are also few selected videos to support your learning in some of the more advanced topics. More information on the textbook can be found within the Learning Resources link under "Preparing for Success."

You will demonstrate your competency in this subject area by successfully completing five tasks covering number theory, groups, rings, and fields, each of which you will submit for evaluation in TaskStream.

**Teaching Dispositions Statement**

Please review the [Statement of Teaching Dispositions](#).

**Preparing for Success**

The information in this section is provided to detail the resources available for you to use as you complete this course.

**Learning Resources**

The following learning resources have been selected to help you complete this course successfully.

Access your textbook using this link, which will open in the VitalSource e-reader. For instructions on downloading for use offline on PC, phone, or mobile device, watch: [Vitalsource Bookshelf Video](#) (These instructions are for a different book but apply here).

IMPORTANT NOTE: Answers to odd-numbered questions can be found in the "Selected Answers" section of your textbook (starting on page 395). *Do not immediately look at the answer and then assume you will know how to reproduce the calculation and proof*
methods in your assessments. Instead, give each of these problems serious thought and energy.

If you are interested in obtaining a paper copy of the book, the full reference is:


Pacing Guide
Following the pacing guide will help you complete the course in the suggested timeframe:

Week 1
• Number Theory (sections 1.1, 1.2, and 1.3)

Week 2
• Number Theory and Congruence (sections 1.4 and 2.1)
• Performance Task 1

Week 3
• Rings and Zₙ (sections 2.4 and 2.5)
• Performance Task 2

Week 4
• Fields and Integral Domains (section 2.5)
• Performance Task 3

Week 5
• Groups (section 4.1 and videos)
• Performance Task 4

Week 6
• Homomorphisms (sections 2.6, 4.5, and videos)
• Performance Task 5

Supplemental Activities
There may be times when you feel like you need more information or practice than what has been provided in the course. In addition to consulting with your Course Instructor when you need help, you can access optional and supplemental activities by using the word "supplemental" in the Course Search box. These activities can be enriching, but they are not essential for becoming competent.

**Contact a Course Instructor**

Your Course Instructor is an important resource for you as you progress through your study of the course. Your Course Instructor will help guide your learning, answer questions, and provide valuable information. Be sure to consult your Course Instructor frequently.

**Competencies and Objectives**

This course covers the following competencies and objectives:

**• Competency 210.4.1: Number Theory**

The graduate demonstrates an understanding of important number theory principles, their applications, and proofs.

**Objectives:**

- Apply the division algorithm to find the quotient and remainder in an integer division problem.
- Apply Euclid's algorithm to find the greatest common divisor of two given numbers.
- Find the least common multiple of two given numbers.
- State the well-ordering principle.
- Determine the equivalence class for a given member of a set.

**• Competency 210.4.2: Groups**

The graduate analyzes the characteristics of and proves theorems involving groups.

**Objectives:**

- Determine whether a given mathematical structure is a group by applying the definition of a group.
- Determine the identity of a given group.
- Determine the inverse of a specified element of a given group.
- Determine whether two given groups are isomorphic.
- Define the concept of permutation group.
- Prove a given theorem involving symmetric groups.

**• Competency 210.4.3: Rings**

The graduate demonstrates understanding of the characteristics of and proves theorems involving rings.
Objectives:

- Determine whether a given ideal is a principal, maximal, or prime ideal.
- Apply the Euclidean algorithm for polynomials to determine the greatest common divisor for two given polynomial functions.
- Determine the reducibility of a given polynomial.
- Apply the definition of "ring" to determine whether a given mathematical structure is a ring.
- Find the characteristic of a given ring.
- Find the additive inverse for a given number, mod n.
- Find the multiplicative inverse for a given number, mod n.

• Competency 210.4.4: Fields

The graduate demonstrates understanding of the characteristics of and proves theorems involving fields and subfields.

Objectives:

- Define the term "subfield."
- Apply the definition of "field" to determine whether a given mathematical structure is a field.

Well-Ordering Principle and Equivalence Class

The foundational well-ordering principle and the notion of equivalence class are the first tools used in abstract algebra. The following section on induction and equivalence relations will cover topics relating to number theory and will also introduce the new concept of an equivalence class.

Read Section 1.1 and do exercises 1, 7, 9.

Integer Arithmetic and the Division Algorithm

Section 1.2 begins by listing the arithmetic properties of the integers. Make note of the names of these properties; they will come up many times throughout the course.

Arithmetic Properties of the Integers

1. Addition and multiplication are **associative**. For any integers \(a, b, \text{ and } c\), \(a + (b + c) = (a + b) + c\) and \(a(bc) = (ab)c\).
2. Addition and multiplication are **commutative**. For any integers \(a \text{ and } b\), \(a + b = b + a\) and \(ab = ba\).
3. There exists a unique **additive identity** 0 such that \(0 + x = x\) for any integer \(x\).
4. There exists a unique **multiplicative identity** 1 such that \(1 \cdot x = x\) for any integer \(x\).
5. Every integer \(x\) has an **additive inverse** \(-x\) such that \(x + (-x) = 0\).
6. Addition and multiplication satisfy the **distributive law**: For any integers \(x, y,\)
and $z$; $x(y + z) = xy + xz$.

When we add two integers, we get another integer. This means the integers are "closed" under addition. The integers are also closed under multiplication.

Each arithmetic property of the integers is phrased in terms of addition and multiplication. The word "subtraction" is not used. Instead of subtracting an integer, we can use the additive inverse (property 5). For example, the additive inverse of 5 is -5. Instead of subtracting 5 from an integer, we can instead add -5.

There is no multiplicative inverse property for the integers. In the real numbers, the multiplicative inverse of 5 is 1/5, but this is not an integer. When we divide one integer by another, we get a rational number, but we do not necessarily get an integer. Therefore, the integers are not closed under division. Instead of dividing integers, we have the very important Division Algorithm.

Succeed by reading the directions for each activity and following them carefully.

Read Section 1.2 and do exercises 1, 5, 7, 9.

Read the "To the Teacher" material following the exercises for 1.2 to see why the Division Algorithm is called an "algorithm."

**Greatest Common Divisors and Euclid's Algorithm**

Euclid's Algorithm is a step-by-step process for finding the greatest common divisor $\gcd(a, b)$ of two given integers $a$ and $b$. Step 1 of Euclid's Algorithm is the Division Algorithm from section 1.2. In section 1.3, Euclid's Algorithm is described following Proposition 6 and demonstrated in Examples 3, 4, and 5.

Euclid's Algorithm can also be used to find integers $m$ and $n$ such that: $\gcd(a, b) = am + bn$. This important process is demonstrated in Examples 4 and 5 and you are asked to try it in Exercises 10 and 11.

Proposition 7 tells us Euclid's Algorithm can also be used to find the least common multiple $\text{lcm}(a, b)$.

Read Section 1.3 and do exercises 5, 7, 8, 10, 11.

**Congruence and the Chinese Remainder Theorem**

A congruence is a statement of the form $a \equiv b \mod m$ where $a$, $b$, and $m$ are integers.

When we write $a \equiv b \mod m$, the "mod $m$" describes the symbol "\equiv" and tells us "$a$ and $b$ are equivalent mod $m$" which means $a-b$ is a multiple of $m$. This is Definition 1 of section 2.1.
For example, 10 ? 2 mod 8 (because 10 - 2 = 8).

We can add, subtract, or multiply each side of a congruence by an integer, but we cannot necessarily divide:

- If we add 4 to each side of 10 ? 2 mod 8, we get 14 ? 6 mod 8 which is a true statement (because 14 – 6 = 8).
- If we multiply each side of 10 ? 2 mod 8 by 3, we get 30 ? 6 mod 8 which is a true statement (because 30 – 6 = 24).
- If we divide each side of 10 ? 2 mod 8 by 2, we get 5 ? 1 mod 8 which is NOT a true statement.

In section 2.1, you will learn how to solve congruences of the form \( ax \equiv b \mod m \) for any given integers \( a, b, \) and \( m \). As you read section 2.1, you should note how to do the following:

- determine whether \( ax \equiv b \mod m \) has a solution,
- find all solutions for \( ax \equiv b \mod m \) given one solution, and
- find a solution for \( ax \equiv b \mod m \) (if it has a solution) using Euclid's Algorithm.

You will also learn how to solve a set of congruences using the Chinese Remainder Theorem.

Read Section 2.1 and do exercises 5, 9, 11, 13, 14, 17, 18, 19.

Performance Task 1
Complete and submit Task 1 to TaskStream. If you do not pass, meet with your Course Instructor.

The Ring \( \mathbb{Z}_m \)

In the previous section, you learned about the equivalence relation given by \( a \equiv b \mod m \) for integers \( a \) and \( b \). The set of equivalences classes for this relation is denoted \( \mathbb{Z}_m \). The elements of \( \mathbb{Z}_m \) are denoted \([x]_m\) where \( x \) is an integer from 0 to \( m-1 \) (this notation was introduced in Section 2.1). Each element \([x]_m\) is an equivalence class of integers that have the same integer remainder as \( x \) when divided by \( m \).

For example, \( \mathbb{Z}_7 = \{[0], [1], [2], [3], [4], [5], [6]\} \). The element \([5]_7\) represents the infinite set of integers of the form 5 plus an integer multiple of 7. That is:

\[ [5]_7 = \{\ldots -9, -2, 5, 12, 19, 26, \ldots \} \]

or, more formally:

\[ [5]_7 = \{y: y = 5 + 7q \text{ for some integer } q\} \]

Modular addition, \([+]\), and modular multiplication, \([\ast]\), are defined for elements of \( a \) and \( b \) of \( \mathbb{Z}_m \) in terms of integer addition and multiplication as follows:
In section 2.4 it is shown that these operations are "well-defined" on the set $Z_m$ (Proposition 1). It is also shown that the set $Z_m$ with these operations has the same arithmetic properties (listed in section 1.2) as the integers themselves.

Read section 2.4 and do exercises 1, 3, 5, 6, 7, 11, 13.

Read the "To the Teacher" material following the exercises for 2.4 to explore the arithmetic differences between $Z_m$ and the integers $Z$.

**Rings**

A "ring" is a structure that shares many of the same arithmetic properties as the integers (listed in 1.2). The formal definition of a "ring" is given as Definition 1 of section 1.5. The integers $Z$, the rational numbers $Q$, and the real numbers $R$ are listed as "familiar" examples of rings along with $Z_m$ from section 1.4. Other examples include sets of polynomials, sets of matrices, and the even integers.

Read section 2.5 pages 82, 83, and 84 and do exercises 1, 3, 5.

**Performance Task 2**

In Task 2, you are asked to prove six of the eight properties of a ring. The other two proofs are provided in the attachment "Proof of Properties 2 and 6." The two given proofs are intended as a guide to demonstrate the level of detail required for the proofs in Task 2. You are also asked to verify four of the properties with examples in parts 3a, 4a, 5a, and 6a. Note there are ten parts in all to Task 2 (six proofs with four examples).

Complete and submit Task 2 to TaskStream. If you do not pass, meet with your Course Instructor.

**Integral Domains and Fields**

Integral domains and fields are special rings. It is important to know the differences between them and how to determine whether a particular mathematical structure satisfies the conditions of them.

Read section 2.5 pages 85, 86, and 87 and do exercises 7, 10, 11, 15, 16.

Reflect on how knowing the difference between integral domains and fields helps you better understand basic properties of arithmetic, especially the relationship between integers and rational numbers.

**Performance Task 3**

Complete and submit Task 3 to TaskStream. If you do not pass, meet with your Course Instructor.

**The Complex Numbers**
Read section 2.6 and do exercises 1, 3, 5, 10, 11, 16, 17.

Read the "To the Teacher" material following the exercises for 2.6. Pay special attention to Euler’s extension of the exponential function to the complex domain.

Watch Roots of Unity by DaveAcademy.

Groups

You have studied two important abstract structures, rings and fields. In this section we will study an additional abstract structure, groups. Whereas rings and fields have two binary operations (addition and multiplication), a group has only one binary operation. Because there is only one operation, the definition is a group is easier to state than the definition of a ring. However, this easier definition with fewer properties means there is a wider array of examples of groups as compared to rings. Examples of groups include the integers with addition, the nonzero reals with multiplication, and the complex numbers with addition to name just a few. In addition to these familiar examples, there are many new and unusual examples of groups such as the "group of parade commands" in Example 4 of section 4.1.

Read section 4.1 and do exercises 1, 3, 5, 7, 11, 15, 19.

Watch Proof of exercise 2 (20 minutes) and Proof of the left and right cancellation laws for groups (9 minutes).

Performance Task 4
Complete and submit Task 4 to TaskStream. If you do not pass, meet with your Course Instructor.

Homomorphisms and Isomorphisms

Read section 4.5 (skip examples 6 and 7) and do exercises 1, 4, 5, 10, 11, 12.

Watch Homomorphisms (Abstract Algebra) by Socratica.

Performance Task 5
Complete and submit Task 5 to TaskStream. If you do not pass, meet with your Course Instructor.

Connections

Abstract Algebra has close connections to several other subjects you have studied.

- **Functions and polynomials:** The sets of functions you studied in calculus are examples of integral domains. In particular, the set of polynomials with real coefficients (or integer coefficients) forms an integral domain. Remember, an integral domain means that the set of polynomials (with the usual addition and multiplication of polynomials) has the same arithmetic properties as the integers. This means we can define the “gcd” for two polynomials and use the Euclidean Algorithm for polynomials just like we did for integers. You can explore this topic by reading sections 3.1 and 3.2.
• **Solving equations**: You know the quadratic equation for solving quadratic equations, but do you know how to solve cubics and quartic equations? A method for solving these is given in section 3.6. Abstract Algebra not only helps us solve equations, it can also be used to prove that there is no formula analogous to the quadratic equation for solving equations of fifth degree or higher. You can explore this topic in section 6.5.

• **Geometry**: The symmetries of geometric objects (such as regular polygons) are examples of finite groups. You can explore this topic by reading section 4.2. Abstract Algebra also applies to compass and ruler constructions. Using Abstract Algebra, we can prove that certain constructions are not possible. You can explore this topic by reading section 6.3.

• **Linear Algebra**: As you learned, sets of matrices are examples of rings. Vector fields also arise in Abstract Algebra. You can explore field extensions and vector spaces over fields by reading sections 6.1 and 6.2.

**Final Steps**

Congratulations on completing the activities in this course! The content of this course has prepared you to complete the course's assessments. If you have not already completed the assessments, schedule and complete your assessments now.