LECTURE 1

September 6, 2023

- Meetings: MWF 9:30 AM R S174
- Student Hours: M 3:00 PM-4:00 PM via Zoom
- Text: Abstract Algebra, Judson
- Evaluation:
  - Assignments: 30%
  - Midterm: 30%
  - Final: 40%

What is algebra? Studies the operations between objects in sets such as

- Addition on numbers.
- Multiplication between numbers.
- Matrix multiplication.
- Addition modulo n
- and others...

A set G is called a group if it is enclosed with an operation that satisfies certain properties. Groups are the main subject of MATH 3021. This class is indeed a proof-based course, so MATH 1200 or equivalent is required to complete this course. It is important to be fluent in proof-writing and be familiar with proof methods (contradiction, induction, etc.).

We will be having a look at some review material from MATH 1200 first, before getting into the integers.

1. MATH 1200 Review

1.1. Set Notations.

Definition 1.1.1. A *set* is an unordered collection of objects.

Example 1.1.2. The following are examples of sets.

- Empty set: $\emptyset$
- Set of natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$
- Set of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$
- Set of rational numbers $\mathbb{Q} = \left\{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N}\right\}$.
- Set of real numbers $\mathbb{R}$
- Set of points in the plane $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$
- Set of complex numbers $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$.
- $\mathcal{M}_n(\mathbb{R})$ denotes the set of all $n \times n$ matrices with real entries.
- $\mathbb{R}^{\mathbb{R}}$ denotes all functions $f : \mathbb{R} \to \mathbb{R}$.

NOTATION 1.1.3. Let A be a set, and let x be an object. We say that x is an element of A and write $x \in A$. If x is not an element of A, we write $x \notin A$.

NOTATION 1.1.4. Let A be a set. We denote the cardinality of the set A by $|A|$, which denotes the number of elements in the set A.

EXAMPLE 1.1.5. If $A = \emptyset$ and $B = \{1, 3, 5\}$, then $|A| = 0$, and $|B| = 3$.

NOTATION 1.1.6. For sets A and B, we say that A is a subset of B and write $A \subset B$, if every element in A is in B. We also say that A is a proper subset of B and write $A \subsetneq B$ if $A \subset B$ but $A \neq B$.

EXAMPLE 1.1.7. $\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

NOTATION 1.1.8. For sets A and B, we have the following set operations

- $A \cup B$ for the union of two sets.
- $A \cap B$ for the intersection of two sets.
- $A \setminus B$ for the difference of A from B.
- $A \times B = \{(a, b) : a \in A, b \in B\}$ for the Cartesian product of the two sets.

1.2. Functions.

DEFINITION 1.2.1. Let X and Y be sets. A function $f : X \to Y$ is a rule that assigns to every $x \in X$ to a unique $f(x) \in Y$. We call X the domain and Y the codomain of f.

NOTATION 1.2.2. Let X and Y be sets and let $f : X \to Y$ be a function. The graph of f we denote it by

$$\mathrm{gr}(f) = \{(x, f(x)) : x \in X\} \subset X \times Y$$

EXAMPLE 1.2.3. Let X be a set. We denote the identity function by $id_X : X \to X$ and is a function such that for all $x \in X$, $id_X(x) = x$.

EXAMPLE 1.2.4. Let X and Y be sets, let $f : X \to Y$ be a function, and suppose $y_0 \in Y$ is arbitrary. Then $f(x) = y_0$ always.

DEFINITION 1.2.5. Let X and Y be nonempty sets, and let $f : X \to Y$ be a function.

- The function f is said to be *one-to-one* if for all $x_1, x_2 \in X$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.
- The function f is said to be *onto* if for all $y \in Y$, there exists an $x \in X$ such that $f(x) = y$.
- The function f is said to be a *bijection* if it is both one-to-one and onto.

EXAMPLE 1.2.6. The following are examples that describes one-to-one, onto, and bijection:

- Let $f : \mathbb{R} \to \mathbb{R}$ be a function with $f(x) = e^x$. Then f is one-to-one, but it is not onto.

- Let $f : \mathbb{R} \to [0, \infty)$ be a function with $f(x) = x^2$. Then f is onto, but it is not one-to-one.
- Let $f : (0, \infty) \to \mathbb{R}$ be a function with $f(x) = \ln(x)$. Then f is both one-to-one and onto, therefore it is a bijection.

Definition 1.2.7. Let X and Y be sets, let $f : X \to Y$ be a function, and let $A \subset X$. We define the *image of A under f* by

$$f(A) = \{y \in Y : \exists x \in A : f(x) = y\} = \{f(x) : x \in A\} \subset Y$$

In particular, $f(X)$ is called the range of f.

Remark 1.2.8. The range and the codomain may not necessarily be the same.

Example 1.2.9. Suppose we let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$. The codomain is $\mathbb{R}$ while the range is $f(\mathbb{R}) = [0, \infty)$.

Notation 1.2.10. Let X, Y and Z be sets, let $f : X \to Y$ and $g : Y \to Z$ be functions. We define the composition of $g \circ f$ as the function $g \circ f : X \to Z$.

Example 1.2.11. Take $f : (0, \infty) \to \mathbb{R}$ with $f(x) = \sqrt{x} - x^2$ and $g : \mathbb{R} \to (0, \infty)$ given by $g(x) = e^x$. Then

$$g(f(x)) = e^{\sqrt{x} - x^2} : (0, \infty) \to (0, \infty)$$

Remark 1.2.12. If X is a set and $f, g : X \to X$, then $g \circ f$ and $f \circ g$ exists, but are not necessarily the same.

Example 1.2.13. Let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2 + 1$ and $g : \mathbb{R} \to \mathbb{R}$ with $g(x) = x + 1$. Then

$$f(g(x)) = (x+1)^2 + 1 \quad g(f(x)) = x^2 + 2$$

Definition 1.2.14. Let X and Y be sets and let $f : X \to Y$ be a function. We say that f is *invertible* if there exists a $g : Y \to X$ such that $f \circ g = id_Y(y)$ and $g \circ f = id_X$. If such a g exists, then denote it by f^{-1} and call it the inverse of f.

Example 1.2.15. Take $f : \mathbb{R} \to (0, \infty)$ given by $f(x) = e^x$. Its inverse is the natural logarithm $g : (0, \infty) \to \mathbb{R}$ with $g(x) = \ln(x)$. Then $f(g(x)) = y$ and $g(f(x)) = x$.

Proposition 1.3. *Let X and Y be sets. The function f is invertible if and only if it is a bijection.*

1.4. Equivalence Relations.

Definition 1.4.1. Let X be a nonempty set. A binary relation "$\sim$" on X is called an *equivalence relation* if the following properties hold:

- (Reflexivity) For all $x \in X$, $x \sim x$.
- (Symmetry) For all $x, y \in X$, if $x \sim y$, then $y \sim x$.
- (Transitivity) For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

Example 1.4.2. Let $n \in \mathbb{N}$ and let $x, y \in \mathbb{Z}$. We say that x is congruent to y modulo n and write $x \equiv y \bmod n$ if $x - y$ is an integer multiple of n, i.e. $n \mid x - y$. We will show next time that congruence modulo is a relation.