CAS MA394 APPLIED ABSTRACT ALGEBRA

Fall 2025

Frank Yang
Professor Tom Enkosky
TTh 2:00 – 3:15

Contents

1 Lecture 1 – 1/20

Definition 1.1. A **set** is a well-defined collection of objects; that is, it is defined in such a manner that we can determine for any given object whether or not it belonsgs to the set. The objects that belond to a set are called its **elements** or **members**. We denote them with capital letters such as A or X.

- If a is an element of a set A, we write $a \in A$.
- The set without any elements its the **empty set**, denoted $\emptyset$ or $\{\}$.
- If A and B are sets and every element of A is in B, then A is a **subset** of B, denoted $A \subseteq B$.
- If $A \subset B$ and $B \subset A$, then $A = B$.
- If $A \subset B$ and $A \neq B$, then A is a **proper subset** of B, denoted $A \subset B$.

Some standard sets include:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$, the set of natural numbers (positive integers).
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of integers.
- $\mathbb{Q} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\}$, the set of rational numbers.
- $\mathbb{R} = (-\infty, \infty)$, the set of real numbers.
- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$, the set of complex numbers.

We can also build new sets from old sets.

- The **union** of two sets A and B is the set of elements that are in A or B (or both), denoted $A \cup B$.
$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$
- The **intersection** of two sets A and B is the set of elements that are in both A and B, denoted $A \cap B$.
$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$
- The **complement** of a set A (with respect to a universal set U) is the set of elements in U that are not in A, denoted $A', A^c, \bar{A}$.
$$A' = \{x : x \in U \text{ and } x \notin A\}.$$
- The **difference** of two sets A and B is the set of elements that are in A but not in B, denoted $A \setminus B$ or $A - B$.
$$A \setminus B = A \cap B' = \{x : x \in A \text{ and } x \notin B\}.$$

Definition 1.2. De Morgan's Laws state that for any two sets A and B,

$$(A \cup B)' = A' \cap B'$$
$$(A \cap B)' = A' \cup B'.$$

Definition 1.3. The **Cartesian product** of two sets A and B is the set of ordered pairs (a, b) where $a \in A$ and $b \in B$, denoted $A \times B$.

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

An example of a Cartesian product is $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$, the set of all points in the plane.

Definition 1.4. A **relation** R from a set A to a set B is a subset of the Cartesian product $A \times B$.

Example 1.5. Let $A = \{0, 1, 2, 3\}, B = \{0, 1, 2, 3\}$. Then $A \times B = \{(a, b) : a, b \in A\}$. If we say that R is the set $\{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)\} \subset A \times B$, then R is a relation from A to B.The relation R can be interpreted as "is less than", since for each $(a, b) \in R$, we have $a < b$.

Definition 1.6. We define a mapping or function $f \subset A \times B$ from a set A to a set B as a special type of relation where each $a \in A$ has a unique $b \in B$ such that $(a, b) \in f$. We denote this by $f : A \to B$ or $A \xrightarrow{f} B$. The set A is called the **domain** of f and $f(A) = \{f(a) : a \in A\} \subset B$ is called the range or **image** of f.

2 Lecture 2 – 1/21

Definition 2.1. If $f : A \to B$ is a map and the image of f is B, i.e., $f(A) = B$, then f is called **onto** or **surjective**. In other words, if there exists an $a \in A$ for every $b \in B$ such that $f(a) = b$, then f is onto.

Definition 2.2. A map is **one-to-one** or **injective** if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$. Equivalently, a function is one-to-one if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

Definition 2.3. A map $f : A \to B$ is a **bijection** if it is both one-to-one and onto.

Definition 2.4. Given two functions, we can construct a new function by using the range of the first function as the domain of the second function. Let $f : A \to B$ and $g : B \to C$ be mappings. Define a new map $g \circ f : A \to C$ called the **composition** of f and g from A to C, by $g \circ f(x) = g(f(x))$.

- If S is any set, we use id_S or id to denote the **identity mapping** from S to itself, or $id(s) = s$ for all $s \in S$.
- A map $g : B \to A$ is an **inverse mapping** of $f : A \to B$ if $g \circ f = id_A$ and $f \circ g = id_B$; in other words, the inverse function of a function simply "undoes" the function.
- A map is said to be **invertible** if it has an inverse. We write f^{-1} to denote the inverse of f.

3 Lecture 3 – 1/22

Definition 3.1. An **equivalence relation** on a set X is a relation $R \subset X \times X$ such that

- $(x, x) \in R$ for all $x \in X$ (reflexive property),
- $(x, y) \in R$ implies $(y, x) \in R$ (symmetric property),
- $(x, y) \in R$ and $(y, z) \in R$ imply $(x, z) \in R$ (transitive property).

Given an equivalence relation R on a set X, we usually write $x \sim y$ instead of $(x, y) \in \mathbb{R}$. If the equivalence relation already has an associated notation such as $=, \cong, \equiv$, we use that notation instead.

Example 3.2. Let $X = \{1, 2, 3, 4\}$. A set R that is reflexive, symmetric, and transitive (and thus an equivalence relation) is $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)\}$.

Definition 3.3. A **partition** P of a set X is a collection of nonempty sets $X_1, X_2, \ldots, X_n$ such that $X_i \cap X_j = \emptyset$ and $\bigcup_i X_i = X$. Let $\sim$ be an equivalence relation on a set X and let $x \in X$. Then $[x] = \{y \in X : x \sim y\}$ is called the **equivalence class** of x.

Example 3.4. Let $\mathbb{Z}$ be partitioned into $A = \{\text{even integers}\}$ and $B = \{\text{odd integers}\}$.
$A \cap B = \emptyset$ and $A \cup B - \mathbb{Z} \implies A, B$ partition the integers. Define a relation $\sim$ on $\mathbb{Z}$ where $x \sim y \iff x, y$ both even or both odd.
Every $a \in A$ is equivalent to every other $a' \in A$ and every $b \in B$ is equivalent to every other $b' \in B$.

4 Lecture 4 – 1/27

4.1 Mathematical Induction

Definition 4.1. First Principle of Mathematical Induction: Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer $n_0 \in \mathbb{N}$. If for all integers k with $k \geq n_0$, $S(k)$ implies that $S(k+1)$ is true, then $S(n)$ is true for all integers $n \geq n_0$.

Example 4.2. For all $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.
The base case is $n = 1$:, then $1 = \frac{1(1+1)}{2} = 1$, so the base case holds.
Inductive hypothesis: Assume $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for some n.
Inductive step: We want to show that the statement is true for $n + 1$. Consider $1 + 2 + 3 + \cdots + n + (n + 1) = \frac{n(n+1)}{2} + (n + 1) = (n + 1)(\frac{n}{2} + 1) = (n + 1)(\frac{n+2}{2}) = \frac{(n+1)((n+1)+1)}{2}$.

Example 4.3. Prove that

$$\frac{1}{2\,\frac{1}{6}} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

for $n \in \mathbb{N}$.
Base: $n = 1$, then $\frac{1}{1\cdot 2} = \frac{1}{2}$, so the base case holds.
Inductive hypothesis: Assume $\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ for some n.
Inductive step: We want to show that the statement is true for $n + 1$. Consider

$$\begin{aligned}
\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} + \frac{1}{(n+1)(n+2)} &= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n(n+2)+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} \\
&= \frac{n+1}{n+2}.
\end{aligned}$$

Therefore the statement is true for all n.

4.2 The Division Algorithm

Definition 4.4. Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.

- Let a and b be integers. If $b = ak$ for some integer k, we write $a|b$.
- An integer d is called a **common divisor** of a and b if $d|a$ and $d|b$.
- The **greatest common divisor** of a and b is a positive integer d such that d is a common divisor of a and b, and if d' is any other common divisor of a and b, then $d'|d$. We write $d = gcd(a, b)$.
- We say that two integers a and b are relatively prime if $gcd(a, b) = 1$.

Proof of the *gcd* theorem uses the division algorithm:

$$\begin{aligned}
a &= q_1 b + r_1 \ , 0 \leq r_1 < b \\
b &= q_2 r_1 + r_2 \ , 0 \leq r_2 < r_1, r_1 \neq 0 \\
r_1 &= q_3 r_2 + r_3 \ , 0 \leq r_3 < r_2, r_2 \neq 0 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \ , 0 \leq r_n < r_{n-1}, r_{n-1} \neq 0 \\
r_{n-1} &= q_{n+1} r_n + 0.
\end{aligned}$$

The first non-zero remainder is $r_n|gcd(a, b)$, or a common divisor. To show that it's the greatest common divisor, suppose $d = as' + bt'$ for some $s', t' \in \mathbb{Z}$ where $d = gcd(a, b)$. Then if $a = q_1 b + r_1$ and $b = q_2 r_1 + 0$, if $d > r$, but d is a common divisor, then $a - q_1 b = r_1$. Thus $d|a, d_b \implies d|r_1$, therefor d can't be bigger than r_1.

Example 4.5. Let $a = 23, b = 3$. Since $23 = 1 \cdot 3 + 20$, we have $q = 1$ and $r = 20$ which is not valid since r is not less than b. We also have $23 = 8 \cdot 3 - 1$, so $q = 8$ and $r = -1$ is not valid since r is not nonnegative.
The only valid one is $23 = 3 \cdot 7 + 2$, so $q = 7$ and $r = 2$. There is no other way to write $23 = 3 \cdot q + r$ where $0 \leq r < 3$.

Example 4.6. Use the Division Algorithm to find $gcd(2520, 378)$.

$$\begin{aligned}
2520 &= 378(6) + 252 \\
378 &= 252(1) + 126 \\
252 &= 126(2) + 0
\end{aligned}$$

The last non-zero remainder is the gcd, so $gcd(2520, 378) = 126$.

5 Lecture 5 – 1/28

Theorem 5.1. Let p be an integer such that $p > 1$. We say that p is a **prime number**, or simply p is **prime**, if the only positive divisors of p are 1 and p itself. An integer greater than 1 that is not prime is called a **composite number**.

Lemma. Euclid. Let a and b be integers and p be a prime number. If $p|ab$, then either $p|a$ or $p|b$. Suppose $p|ab$ and suppose $p \nmid a$. Then $gcd(a, p) = 1$. Thus there exist integers s, t such that $as + pt = 1$. Multiplying both sides by b gives $abs + ptb = b$. Since $p|ab$ and $p|ptb$, we have $p|b$.

Theorem 5.2. There exist an infinite number of primes.
Assume $p_1, p_2, \cdots, p_n$ are all the primes. Let $N = p_1 p_2 \cdots p_n + 1$. Then N is either prime or composite. If N is prime, then there exists a prime not in our list. If N is composite, then it has a prime divisor p. Since p divides N and p divides $p_1 p_2 \cdots p_n$, p must also divide their difference, which is 1. This is a contradiction since no prime divides 1. Thus there exists a prime not in our list.

5.1 3.1 Integer Equivalence Classes and Symmetries

$\mathbb{Z}_n = \{[0], [1], [2], \cdots, [n-1]\}$ where arithmetic is mod n and the equivalence classes are $a \equiv b (mod\ n)$ if $n|a - b$.

Example 5.3. $\mathbb{Z}_6$:
$[0] = \{0, \pm 6, \pm 12, \pm 18 \cdots\} = [6] = [-12]$ all have a remainder of 0 when divided by 6.
$[1] = \{1, \pm 5, \pm 11, \pm 17 \cdots\} = [7] = [-11]$ all have a remainder of 1 when divided by 6.
$\vdots$

6 Lecture 6 – 1/29

Definition 6.1. Let $\mathbb{Z}_n$ be the set of equivalence classes of the integers *mod n* and $a, b, c \in \mathbb{Z}_n$.

1. Addition and multiplication are commutative. $ab \equiv ba$ and $a + b \equiv b + a$.
2. Addition and multiplication are associate. $(ab)c \equiv a(bc)$ and $(a + b) + c \equiv a + (b + c)$.
3. There are both additive and multiplicative identities. $0 \in \mathbb{Z}_n$ has the property $a + 0 \equiv a$ and $1 \in \mathbb{Z}_n$ has the property $a \cdot 1 \equiv a$.
4. Multiplication distributes over addition. $a(b + c) \equiv ab + ac$.
5. For every integer a there is an additive inverse $-a$. $a + (n - a) \equiv (n - a) + a \equiv n \equiv 0$.
6. Let a be a nonzero integer. Then $gcd(a, n) = 1$ if and only if there exists a multiplicative b inverse for $a(mod\ n)$.

Definition 6.2. A **symmetry** of a geometric figure is a rearrangement of the figure preserving the arrangement of its sides and vertices as well as its distances and angles. A map from the plane to itself preserving the symmetry of an object is called a **rigid motion**.

6.1 3.2 Definitions and Examples

Definition 6.3. A **binary operation** or **law of composition** on a set G is a function $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$, or ab in G, called the composition of a and b.

Definition 6.4. A **group** is a set G together with a law of composition $\circ$ that satisfies the following axioms:

- The law of composition is **associative**; that is, for all $a, b, c \in G$, we have $(a \circ b) \circ c = a \circ (b \circ c)$.
- There exists an **identity element** e in G such that for all $a \in G$, we have $e \circ a = a \circ e = a$.
- For each element $a \in G$, there exists an **inverse element** $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

A group with the property that $a \circ b = b \circ a$ for all $a, b \in G$ is called an **abelian group** or **commutative group**. Groups not satisfying this property are called **nonabelian** or **non-commutative**.

7 Lecture 7 – 2/3

The identity element in a group G is unique; that is, there exists only one element $e \in G$ such that $eg = ge = g$ for all $g \in G$.
If g is any element in a group G, then the inverse of g, denoted by g^{-1}, is unique.
Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.
Let G be a group. For any $a \in G$, $(a^{-1})^{-1} = a$.
Let G be a group and a and b be any two elements in G. Then the equations $ax = b$ and $xa = b$ have unique solutions in G.
If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

Theorem 7.1. In a group, the usual law of exponents hold; that is, for all $g, h \in G$,

1. $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$.
2. $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$.
3. $(gh)^n = (h^{-1}g^{-1})^{-n}$ for all $n \in \mathbb{Z}$. Furthermore, if G is abelian, then $(gh)^n = g^n h^n$.