Mathematical Thinking I
Course Notes
Fall 2023

David Lyons
Mathematical Sciences
Lebanon Valley College

last update: July 10, 2023

Mathematical Thinking I
Course Notes

Fall 2023

David Lyons
Mathematical Sciences
Lebanon Valley College

Contents

1 Some Essential Mathematical Vocabulary

1.1 Sets and Functions

A ***set*** is a collection of objects called the ***elements*** or ***members*** of the set. Given an object x and a set A, exactly one of two things is true: either x is an element of A, denoted $x \in A$, or x is not an element of A, denoted $x \notin A$.

To denote a set that contains a small number of elements, we list the elements, separated by commas, and enclosed in curly brackets. For example, the set $A = \{x, y, z\}$ contains elements x, y, z, and contains no other objects. In this notation, the order in which the objects are listed does not matter. Redundancy also does not matter: the same object may be listed more than once. For example, we may write the following.

$$A = \{x, y, z\} = \{y, z, x\} = \{y, x, y, z\}$$

Another way to denote a set is the notation $\{x \colon x \text{ satisfies condition } C\}$, where the colon ":" is pronounced "such that". For example, the *closed unit interval* of the real line is the set $\{x \colon 0 \le x \le 1\}$.

The set that contains no elements is called the ***empty set***, denoted $\emptyset$.

We write $A \subseteq B$ to indicate that every element in the set A is also in the set B, and we write $A \not\subseteq B$ to indicate that there is at least one element in A that is not an element in B.

The ***intersection*** of sets A, B, denoted $A \cap B$, is the set

$$A \cap B = \{x \colon x \in A \text{ and } x \in B\}.$$

The ***union*** of sets A, B, denoted $A \cup B$, is the set

$$A \cup B = \{x \colon x \in A \text{ or } x \in B\}$$

where the word "or" means "one or the other or both".

The set

$$A \setminus B = \{x \colon x \in A \text{ and } x \notin B\}$$

(also sometimes denoted $A - B$) is called the ***difference of set*** A ***minus set*** B, or just "A minus B" for short.

Given objects x, y, an ordered list of the form (x, y) is called an ***ordered pair***. To say that the pair is ordered means that the pairs (x, y) and (y, x) are different if $x \neq y$. The object x is called the ***first entry*** (or the ***left entry***) of the ordered pair (x, y), and the object y is called the ***second entry*** (or the ***right entry***). The set of all ordered pairs of the form (a, b), where a is an element of set A and b is an element of set B, is called the ***(Cartesian) product*** of the set A with the set B, denoted $A \times B$.

$$A \times B = \{(a, b) \colon a \in A \text{ and } b \in B\}$$

A ***function*** f ***from a set*** S ***to a set*** T, denoted $f \colon S \to T$, is a subset of $S \times T$ with the property that every element s in S is the left entry of exactly one element in f. We write $f(s) = t$ or $s \xmapsto{f} t$ to indicate that (s, t) is the element of f whose left entry is s. The set S is called the ***domain*** of f and the set T is called the ***codomain*** of f. Two functions are ***equal*** if they have the same domain, the same codomain, and contain the same elements.

Given an element $s_0 \in S$, we refer to $f(s_0)$ as the ***image of*** s_0 ***under*** f. Given an element $t_0 \in T$, we call the set $\{s \in S \colon f(s) = t_0\}$ the ***preimage of*** t_0 ***under*** f.

The function $f \colon S \to T$ is called ***one-to-one*** or ***injective*** if, for every $t \in T$, the preimage of t under f has at most 1 element. A function $f \colon S \to T$ is called ***onto*** or ***surjective*** if, for every $t \in T$, the preimage of t has at least one element. A function is called ***bijective***, or a ***one-to-one correspondence***, if it is both injective and surjective.

Given functions $f \colon S \to T$ and $g \colon T \to U$, the function $g \circ f \colon S \to U$, called the ***composition*** of g with f, is defined by $(g \circ f)(s) = g(f(s))$ for all $s \in S$.

Given a set S, the function $f \colon S \to S$ defined by $f(s) = s$ for every $s \in S$ is called the ***identity function on*** S. The identity function on S is sometimes denoted I_S, Id_S, or $\mathbb{1}_S$, and the subscript S may be omitted when the context is clear.

Given a function $f \colon S \to T$, if there is a function $g \colon T \to S$ such that $g \circ f = \mathbb{1}_S$ and $f \circ g = \mathbb{1}_T$, then f is said to be ***invertible***. The function g is called the ***inverse*** of f, and we write $g = f^{-1}$.

More on images and preimages. Let $f \colon S \to T$ be a function. Given a set $U \subseteq S$, the ***image of*** U ***under*** f, denoted $f(U)$, is the set

$$f(U) = \{f(u) \colon u \in U\}.$$

Given a set $V \subseteq T$, the ***preimage of*** V ***under*** f, denoted $f^{-1}(V)$, is the set

$$f^{-1}(V) = \{u \colon f(u) \in V\}.$$

When $V = \{t_0\}$ is a set with only one element, we write $f^{-1}(t_0)$ for the preimage set $f^{-1}(\{t_0\})$.

CAUTION about terminology. The collection of symbols "f^{-1}" is used in several different ways (this is called *overloading* of terminology).

- "f^{-1}" denotes the inverse of the invertible function f. Depending on f, the inverse function may or may not exist.
- "$f^{-1}(V)$" denotes the inverse image of a subset V of the codomain T. This set is *always* defined for any $f \colon S \to T$ and for any $V \subseteq T$.
- "$f^{-1}(t_0)$" can mean *two* different things:
  - the image of t_0 under the function $f^{-1} \colon T \to S$, defined when f is invertible, but not defined otherwise, or
  - the preimage set $f^{-1}(t_0) = \{s \in S \colon f(s) = t_0\}$, defined for every $f \colon S \to T$ and every t_0 in T

Exercises for 1.1

1. Which of these are correct (one, both, or neither)? Discuss.
$$b \subseteq \{a, b, c\}, \qquad b \in \{a, b, c\}$$

2. Which of these are correct (one, both, or neither)? Discuss.
$$\emptyset \subseteq \{a, b, c\}, \qquad \emptyset \in \{a, b, c\}$$

3. Are any of the following things the same? Discuss.
$$\{0\}, \qquad \{\emptyset\}, \qquad \emptyset, \qquad \{\}$$

4. Write out all of the subsets of $\{x, y, z\}$.

5. Write out all of the functions from $\{x, y, z\}$ to $\{A, B\}$. Which are injective? Which are surjective? Which are bijective?

6. Write out all of the functions from $\{A, B\}$ to $\{x, y, z\}$. Which are injective? Which are surjective? Which are bijective? For each of your functions $f\colon \{A, B\} \to \{x, y, z\}$, write out $f^{-1}(x)$ and $f^{-1}(\{x, y\})$.

7. Write out all of the functions from $\{x, y, z\}$ to $\{x, y, z\}$. Which are injective? Which are surjective? Which are bijective?

8. Consider the functions $f, g\colon \{x, y, z\} \to \{a, b, c\}$ given by $f(x) = b$, $f(y) = a$, $f(z) = c$ and $g(x) = a$, $g(y) = a$, and $g(z) = c$. One of the two things below has two possible meanings, and one has only one possible meaning. Which is which? And what are those meanings? Discuss.
$$f^{-1}(a), \qquad g^{-1}(a)$$

9. Show, by examples, that the number of elements in the preimage of a point can be 0, 1, 2, any positive integer n, or infinite.

10. Suppose that a function f is bijective. Show that f is invertible.

11. Suppose that a function f is invertible. Show that f is bijective.

12. Suppose the function f is invertible and that $g = f^{-1}$. Show that $f = g^{-1}$.

13. Suppose that f and g are both invertible, and that the composition $g \circ f$ is defined. Show that $g \circ f$ is invertible and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. This fact is referred to as the "shoes and socks" property.

14. Let $f\colon S \to T$ be a function. Prove the following.
    (i) If $f^{-1}(t_0) \cap f^{-1}(t_1) \neq \emptyset$, then $f^{-1}(t_0) = f^{-1}(t_1)$.
    (ii) For any s in S, there is a t in T such that $s \in f^{-1}(t_0)$.
    (iii) Conclude that every element of S is an element of exactly one preimage set under f.

15. Suppose that S is finite and that $f\colon S \to S$ is one-to-one. Show that f is onto.

16. Show the previous statement fails if S is not assumed to be finite.

1.2 Integers, divisibility, primes

The set
$$\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$
of all the whole numbers is called the ***integers***. We say that an integer a ***divides*** an integer b, written $a|b$, if $b = ak$ for some integer k. If $a|b$, we say that b is ***divisible*** by a, and we say a is a ***divisor*** of b. We write $a \nmid b$ to indicate that a does not divide b. Given a positive integer m, we say integers a, b are ***equivalent modulo*** m, written $a \equiv b \pmod{m}$, if $m|(a-b)$. An integer $p > 1$ whose only positive divisors are 1 and p is called ***prime***. Here are two important facts about divisibility and primes.

> (1.2.1) **The Division Algorithm.** *Let m be a positive integer. For each integer n there are unique integers q, r that satisfy*
> $$n = mq + r, \qquad 0 \leq r < m.$$
> *The number q is called the **quotient** and the number r is called the **remainder** for **dividing** n **by** m.*

> (1.2.2) **The Fundamental Theorem of Arithmetic.** *Every positive integer n can be written as a product of primes. Further, this prime factorization is unique. That means that if $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ for primes p_i, q_j, then $k = \ell$ and there is a rearrangement of the subscripts for which $p_i = q_i$ for $1 \leq i \leq k$.*

Modular Arithmetic

We write $\mathbf{Z}_m$ to denote the set
$$\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$$
of possible remainders obtained when dividing by a positive integer by m. The function $\mathbf{Z} \to \mathbf{Z}_m$ that sends an input n to its remainder when dividing by m is called "reducing mod m". Sometimes we write $n \,\mathrm{MOD}\, m$ or $n \,\%\, m$, pronounced "n modulo m" or simply "n mod m", to denote this remainder.

We define operations $a +_m b$ and $a \cdot_m b$ for elements a, b in $\mathbf{Z}_m$ by
$$\begin{aligned} a +_m b &= (a+b) \,\mathrm{MOD}\, m \\ a \cdot_m b &= (ab) \,\mathrm{MOD}\, m \end{aligned}$$

The operations $+_m$, $\cdot_m$ are called ***addition modulo*** m and ***multiplication modulo*** m, respectively. The set $\mathbf{Z}_m$ is sometimes called the "m-hour clock" and the operations $+_m, \cdot_m$ are called "clock arithmetic" or "arithmetic modulo m".

Exercises for 1.2

1. Let p be prime and suppose that $p|(ab)$ for some integers a, b. Show that it must be the case that $p|a$ or $p|b$ (or both).

2. Explain why there are infinitely many primes. Hint: Suppose there are only finitely many primes, say $p_1, \ldots, p_n$. Consider $s = p_1 p_2 \cdots p_n + 1$. Explain why s is not divisible by any of the primes, and why this is a contradiction.

3. Let $m > 1$ be a positive integer.

   (a) Show that $a \equiv b \pmod{m}$ if and only if $a \,\mathrm{MOD}\, m = b \,\mathrm{MOD}\, m$. This means that the following two statements hold.

      (i) If $a \equiv b \pmod{m}$, then $a \,\mathrm{MOD}\, m = b \,\mathrm{MOD}\, m$.

      (ii) If $a \,\mathrm{MOD}\, m = b \,\mathrm{MOD}\, m$, then $a \equiv b \pmod{m}$.

   (b) Show that $a \equiv a \pmod{m}$ for every integer a. (This is called the *reflexive* property of equivalence modulo m.)

   (c) Show that if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$. (This is called the *symmetric* property of equivalence modulo m.)

   (d) Show that if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$. (This is called the *transitive* property of equivalence modulo m.)

   (e) Show that if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then

      i. $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$, and

      ii. $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

   (f) Let m be a prime. Let a be a nonzero element of $\mathbf{Z}_m$ and let b be any element of $\mathbf{Z}_m$. Show that there exists some x in $\mathbf{Z}_m$ such that $ax \equiv b \pmod{m}$. Hint: consider the function $\mu_a \colon \mathbf{Z}_m \to \mathbf{Z}_m$ given by $n \to an \,\mathrm{MOD}\, m$. Show that μ_a is one-to-one and onto.

   (g) Suppose that m is not prime. Show that there exist nonzero elements a, b in $\mathbf{Z}_m$ for which there exists *no* x in $\mathbf{Z}_m$ such that $ax \equiv b \pmod{m}$.

1.3 Linear and Exponential Growth

The two most basic growth patterns are the following.

$$a, a+d, a+2d, a+3d, \ldots, a+nd, \ldots$$

$$a, ar, ar^2, ar^3, \ldots, ar^n, \ldots$$

In both patterns, the constant a is called the ***initial term***. The first pattern is called an ***arithmetic sequence***[1] with ***common difference*** d. An arithmetic sequence is said to have ***linear*** growth because it is the sequence of values

$$L(0), L(1), L(2), \ldots$$

of the linear function $L(t) = a + dt$. The second pattern is called a ***geometric sequence*** with ***common ratio*** r (where $r > 0$ and $r \neq 1$). A geometric sequence is said to have ***exponential*** growth because it is the sequence of values

$$E(0), E(1), E(2), \ldots$$

of the exponential function $E(t) = ar^t$.

Finite arithmetic and geometric sums. Exercises at the end of this subsection outline the proofs of the following formulas.

$$a + (a+d) + (a+2d) + \cdots + (a+nd) = \frac{(n+1)(2a+nd)}{2} \tag{1.3.1}$$

$$a + ar + ar^2 + \cdots + ar^n = a\left(\frac{1-r^{n+1}}{1-r}\right) \tag{1.3.2}$$

Infinite geometric sums. An infinite sum of the form

$$a + ar + ar^2 + ar^3 + \cdots$$

is called an ***infinite geometric series***, and is defined to mean the limit (if the limit exists) $\lim\limits_{n\to\infty} s_n$, where $s_1, s_2, s_3, \ldots$ is sequence of finite sums

$$\begin{aligned}
s_0 &= a \\
s_1 &= a + ar \\
s_2 &= a + ar + ar^2 \\
&\vdots \\
s_n &= a + ar + ar^2 + \cdots + ar^n \\
&\vdots
\end{aligned}$$

If $|r| < 1$, then $|r|^n \to 0$ as $n \to \infty$. Using properties of limits from calculus, we have

$$a\left(\frac{1-r^{n+1}}{1-r}\right) \to a\left(\frac{1}{1-r}\right)$$

as $n \to \infty$. Putting this together with (1.3.2) above is the justification for the following formula.

$$a + ar + ar^2 + ar^3 + \cdots = a\left(\frac{1}{1-r}\right) \qquad \text{for } |r| < 1 \tag{1.3.3}$$

[1] The emphasis is on the third syllable "met" when the word "arithmetic" is used as an adjective rather than a noun. For example: "Addition is an operation of a · rith′ · metic. Repeated addition creates an arith · met′ · ic sequence."

Exercises for 1.3

1. Fill in the missing terms of the following arithmetic and geometric sequences. Identify the initial term and the common difference or common ratio for each.

   (a) $5, 2, -1, \_\_, \_\_, \_\_, \ldots$

   (b) $5, 2, 0.8, \_\_, \_\_, \_\_, \ldots$

   (c) $\_\_, 2, \_\_, 5, \_\_, 8, \ldots$

   (d) $\_\_, 2, \_\_, 4, \_\_, 8, \ldots$

2. Find the sum of the first 100 positive integers.

3. Find the given sums of terms of arithmetic and geometric sequences.

   (a) $2 + 5 + 8 + 11 + \cdots + 302$

   (b) $2 + 5 + 8 + 11 + \cdots + 1571$

   (c) $2 + 6 + 18 + 54 + \cdots + 2(3^{100})$

   (d) $2 + 6 + 18 + 54 + \cdots + 9565938$

4. Prove (1.3.1). Hint: Write the sum in reverse order $L(n) + L(n-1) + \cdots + L(1) + L(0)$ directly beneath $L(0) + L(1) + \cdots + L(n)$, in such a way that the terms are aligned vertically. Notice that each vertically aligned pair has the form $L(k)$ and $L(n-k)$, and that $L(k) + L(n-k) = 2a + nd$ (the k's cancel!). Now go from there.

5. Prove (1.3.2). Hint: Let s be the desired sum $a + ar + ar^2 + \cdots + ar^n$. Examine the expansion of $s - rs$ (many terms cancel!). Simplify and solve for s.