Supplementary Material for MTH 299
Online Edition

Abstract

This document contains supplementary material, such as definitions, explanations, examples, etc., to complement that of the text, "How to Think Like a Mathematician".

Contents

1 Useful Sets and Spaces

Theorem 1.1. $A = B$ is equivalent to $(A \subseteq B$ and $B \subseteq A)$

Definition 1.2. The **power set** of a set, A, is the set which contains all possible subsets of A as its elements. The power set is denoted as

$$\mathcal{P}(A) = \{E \ : \ E \subseteq A\}.$$

Definition 1.3. $\mathbb{P}_n$ is the collection of all (real) polynomials of degree less than or equal to n. That is

$$\mathbb{P}_n = \{p \ : \ p(x) = a_0 + a_1 x + \cdots + a_n x^n, \text{ where } a_0, \ldots, a_n \in \mathbb{R}\}.$$

Definition 1.4. Let $\mathcal{I}$ be any fixed set, and assume that for all $r \in \mathcal{I}$, E_r, is a set. The operations of **union and intersection over a general index set** are defined as

$$\bigcup_{r \in \mathcal{I}} E_r = \{x \ : \ x \in E_r \text{ for at least one } r \in \mathcal{I}\}$$

and

$$\bigcap_{r \in \mathcal{I}} E_r = \{x \ : \ x \in E_r \text{ for all } r \in \mathcal{I}\}.$$

Note, another way to write this is

$$\left(x \in \bigcup_{r \in \mathcal{I}} E_r \right) \iff (\exists\, r_0 \in \mathcal{I} \text{ such that } x \in E_{r_0})$$

and

$$\left(x \in \bigcap_{r \in \mathcal{I}} E_r \right) \iff (\forall\, r \in \mathcal{I},\ x \in E_r).$$

As a notational convenience, when $\mathcal{I}$ is a simple set that can be listed easily, we sometimes write

$$\bigcup_{i=1}^{\infty} E_i = \bigcup_{i \in \mathbb{N}} E_i$$

or

$$\bigcup_{j=5}^{21} E_i = \bigcup_{j \in \{5,6,\ldots,21\}} E_j.$$

Proposition 1.5. Suppose A, B are subsets of a universal set $\mathcal{U}$. Their union and intersection satisfy the so-called "De Morgan's Laws" for sets:

i) $(A \cup B)^c = A^c \cap B^c$, and

ii) $(A \cap B)^c = A^c \cup B^c$.

Remark 1.6. The same results hold for Boolean algebra (propositional logic). State this result and prove it.

Definition 1.7. Let E be a set. A **partition of** E is a collection, $\mathcal{T} \subseteq \mathcal{P}(E)$, such that

$$\forall A_1, A_2 \in \mathcal{T} \text{ such that } A_1 \neq A_2,\ A_1 \cap A_2 = \emptyset$$

and

$$E = \bigcup_{A \in \mathcal{T}} A.$$

(Recall that $\mathcal{P}(E)$ is the power set of E, defined earlier in this section.)

Remark 1.8. It is very useful to simply write out what it means to be a partition in plain words. *A partition of E is a collection of subsets of E such that two things happen: (1) the union over all of the sets in the collection covers all of E and (2) if you take any two distinct subsets in the collection, they have an empty intersection.* So, what you are doing is breaking up E into disjoint pieces and not leaving any piece of E out. This is incredibly useful for many areas of mathematics. You can also think of it as exactly what happens with the hard drive on your computer. The hard drive is one disc, but many people choose to break it up into separate partitions that don't interact with each other.

Remark 1.9. It is very important to note a possible simplification in your proofs involving partitions. Suppose you want to show that $\mathcal{T}$ is a partition. If you first confirm that it is true that all sets in $\mathcal{T}$ are also elements of $\mathcal{P}(E)$, then you have confirmed that $A \subset E$ for all A in $\mathcal{T}$. You may then tell your reader that you only need to check that

$$E \subseteq \bigcup_{A \in \mathcal{T}} A,$$

because the reverse set containment is already true by the previous observation.

2 Logic

2.1 Supplement to Chapter 6 - Statements, Negation of Compound Statements

Definition 2.1. A **compound statement** is a statement composed of one or more given statements, and at least one connective: $\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow$.

For example, $(P \Rightarrow Q) \vee P$ is a compound statement.

Definition 2.2. Two compound statements are **logically equivalent** if they have the same truth table.

Definition 2.3. (see page 54 of textbook) A **conditional statement** is a statement that requires an input to become a statement.

For example, the expression, $P(x)$: "x is even", is to be understood as something that *becomes a statement after* plugging in a value of x. (See pg. 81 of our text for an extremely brief description.) Formally, we need to define the collection of legal values that can be plugged in, which we call the **domain** of the conditional statement. For this problem, we will use the domain $\mathbb{Z}$. For example, $P(2)$ is true, and $P(5)$ is false.

2.2 Supplement to Chapter 7 - Implications

Definition 2.4. Statements of the form **"If statement A is true, then statement B is true."** are called **implications**. Mathematically this is denoted by $A \Rightarrow B$.
In English, this statement can be expressed in the following equivalent ways.

(i) "If A then B"

(ii) "A implies B"

(iii) "A only if B"

(iv) "B if A"

(v) "B whenever A"

(vi) "A is sufficient for B"

(vii) "B is necessary for A"

When is the statement $A \Rightarrow B$ true? For example, is the following statement true: *If pigs could fly, then I am on Mars.*?
Note that "$A \Rightarrow B$" says nothing about whether the statements A, B themselves are true or false. The following cases are possible for the implication $A \Rightarrow B$ to be true.

- A - true and B - true
- A - false and B - false
- A - false and B - true

In other words, if the assumption is false, the conclusion could be anything!

Theorem 2.5. The **negation** of A $\Rightarrow$ B is equivalent to A and (not B).

$$\neg(A \Rightarrow B) \equiv (A \wedge (\neg B))$$

3 Various facts about real numbers, integers, and rationals

Axiom 3.1. Always assume all of the associativity and commutativity and distributivity as you have done since you were six years old.
We will assume the following properties of the integers:

1. closed under addition

2. closed under multiplication

e.g. if $x, y \in \mathbb{Z}$, then so is $(5y^{10} - xy + x^2 - 11) \in \mathbb{Z}$.

Axiom 3.2. We will assume the following properties of the rationals:

1. closed under addition

2. closed under multiplication

3. addition is invertible

4. multiplication is invertible (with the exception of the zero element).

Definition 3.3. The set of **even** integers is the set

$$\text{even integers} \;=\; \{n \in \mathbb{Z} \;:\; n = 2k \text{ for some } k \in \mathbb{Z}\}.$$

An integer is said to be **odd** if it is not even. You can check that the set of odd integers is

$$\text{odd integers} \;=\; \{n \in \mathbb{Z} \;:\; n = 2k + 1 \text{ for some } k \in \mathbb{Z}\}.$$

4 Functions

4.1 Some definitions about functions

Definition 4.1. A **function** from a set X to a set Y is an assignment such for all $x \in X$, there is assigned exactly one element of Y. This assignment can re-use elements of Y for the corresponding values of x. In concise terms, we write

$$f : X \to Y,$$

and for all $x \in X$, $f(x) \in Y$. We call f the function, x the input variable, $f(x)$ the output, X is the domain, and Y is the co-domain.

Remark 4.2. It is very important to note, you cannot assume you have precisely defined a *function* until you have specified *three items*: the domain, the co-domain, and the assignment rule / formula. This is a very frequently confused issue, and it can make things very difficult when investigating properties involving injective, surjective, and bijective.

Definition 4.3. If $f : X \to Y$ is a function, we define the **graph** of f to be the set

$$graph(f) := \{(x, y) \in X \times Y \mid y = f(x)\}.$$

Definition 4.4. If $f : X \to Y$ is a function, we define the **range of** f to be the set

$$\text{range}(f) = \{y \in Y \ : \ y = f(x) \text{ for some } x \in X\}.$$

Definition 4.5. Assume that f is a function, $f : X \to Y$. We say the **image** of A under f is $f(A)$, and it is defined as

$$f(A) = \{y \in Y \ : \ y = f(x) \text{ for some } x \in A\}.$$

Definition 4.6. Assume that f and g are both functions, $f : X \to \mathbb{R}$ and $g : X \to \mathbb{R}$. We define the addition $f + g$ as the new function,

$$(f + g)(x) = f(x) + g(x).$$

Definition 4.7. Assume that $f : X \to Y$ is a function. We say that it is **injective** (or **one–to–one**) if

$$\text{for all } x_1, x_2 \in X, \ f(x_1) = f(x_2) \text{ implies } x_1 = x_2.$$

Definition 4.8. A function $f : X \to Y$ is **surjective** if for all $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

Definition 4.9. A function, $f : X \to Y$, for X and Y both subsets of $\mathbb{R}$, is said to be **increasing** if and only if it holds that

$$x_1, x_2 \in X \text{ and } x_1 \le x_2 \implies f(x_1) \le f(x_2).$$

We say f is **strictly increasing** if the above implication holds with $x_1 < x_2$ implies $f(x_1) < f(x_2)$.

Lemma 4.10. The following functions are strictly increasing:

(i) $f : [0, \infty) \to [0, \infty)$, $f(x) = x^2$. (Note the restricted domain!)

(ii) $f : [0, \infty) \to [0, \infty)$, $f(x) = x^{1/2}$.

(iii) $f : [0, \infty) \to [0, \infty)$, $f(x) = x^p$, where $p > 0$ is a real number.

(iv) $f : \mathbb{R} \to (0, \infty)$, $f(x) = e^x$.

(v) $f : (0, \infty) \to (0, \infty)$, $f(x) = \ln(x)$.

4.2 Some frequently used functions

Definition 4.11. A polynomial of degree n or less is a function that can be expressed as $p(x) = \sum_{i=0}^{n} a_i x^i$ where $a_i \in \mathbb{R}$ for $i \in \{0, 1, \ldots, n\}$.

Definition 4.12. Take $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{i=0}^{n} b_i x^i$ where $a_i, b_i, c \in \mathbb{R}$ for $i \in \{0, 1, \ldots, n\}$ then:

(a) $(p + q)(x) := \sum_{i=0}^{n} (a_i + b_i) x^i$

(b) $(cp)(x) := \sum_{i=0}^{n} (c \cdot a_i) x^i$

Definition 4.13. $\mathbb{P}_n$ is the collection of all (real) polynomials of degree less than or equal to n. That is

$$\mathbb{P}_n = \{p \ : \ p(x) = a_0 + a_1 x + \cdots + a_n x^n, \text{ where } a_0, \ldots, a_n \in \mathbb{R}\}.$$

Definition 4.14. The absolute value of a real number, x, is defined as

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

You can think of $|\cdot|$ as a function (here we use the dot, "$\cdot$", as a placeholder), $|\cdot| : \mathbb{R} \to \mathbb{R}$, given by the assignment rule listed in the previous sentence.

Definition 4.15. The maximum of two real numbers x and y can be defined as:

$$\max\{x, y\} = \begin{cases} x & \text{if } x \geq y \\ y & \text{if } x < y. \end{cases}$$

This can be expanded to 3 or more entries $\max\{x, y, z\}$ intuitively.

Definition 4.16. The minimum of two real numbers x and y can be defined as:

$$\min\{x, y\} = \begin{cases} x & \text{if } x \leq y \\ y & \text{if } x > y. \end{cases}$$

This can be expanded to three or more entries $\min\{x, y, z\}$ intuitively.

Definition 4.17. The ceiling function $\lceil x \rceil$ is a function from $\mathbb{R} \to \mathbb{Z}$ defined by

$$\lceil x \rceil := \min\{z \in \mathbb{Z} \mid n \geq x\}$$

5 Real Analysis

5.1 A few properties of the real numbers

Axiom 5.1. The real numbers are endowed with a number of properties that we will take for granted. Below, we name a few of them:

1. The **Archimedean property** says that if $x \in \mathbb{R}$, then there exists an $N \in \mathbb{N}$ such that $x < N$. That is, if you are challenged with a real number, then you can find a larger integer.

2. If $x, y \in \mathbb{R}$, then one, and only one of the following cases can happen:

   - Case I: $x < y$,
   - Case II: $x = y$,
   - Case III: $x > y$.

3. Additive and multiplicative properties:

   (a) $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{R}$.
   (b) $a + b = b + a$ for all $a, b \in \mathbb{R}$.
   (c) $a + 0 = a$ for all $a \in \mathbb{R}$.
   (d) For each $a \in \mathbb{R}$, there exists a unique $-a \in \mathbb{R}$, with $a + (-a) = 0$.
   (e) $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{R}$.
   (f) $ab = ba$ for any $a, b \in \mathbb{R}$.
   (g) $a \cdot 1 = a$ for any $a \in \mathbb{R}$.
   (h) For each $a \neq 0$, there exists a unique $a^{-1} \in \mathbb{R}$, with $aa^{-1} = 1$.
   (i) $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{R}$.

4. Ordered properties:

   (a) If $a, b \in \mathbb{R}$, then $a \leq b$ or $b \leq a$.
   (b) If $a \leq b$ and $b \leq c$, then $a \leq c$.
   (c) For any $x, y, c \in \mathbb{R}$, if $x \leq y$ then $x + c \leq y + c$.
   (d) If $a \leq b$, and $0 \leq c$, then $ac \leq bc$.

Remark 5.2. Assume the following property of the power function. If $b \geq a \geq 0$ and $t > 0$ then

1. $a^t \leq b^t$, and

2. if also $a > 0$ and $b > 0$, then $a^{-t} \geq b^{-t}$.

For example, you know well from previous classes that if $0 < a \leq b$, then $a^{1/3} \leq b^{1/3}$, $a^{-1} \geq b^{-1}$, $a^{79} \leq b^{79}$, and so on.

5.2 Properties of subsets of the real numbers

Definition 5.3. A set, $E \subseteq \mathbb{R}$, is said to be **bounded** if there exists an $M \in \mathbb{R}$ such that

$$|x| \leq M \text{ for all } x \in E.$$

Definition 5.4. We say the set $A \subseteq \mathbb{R}$, is **open**, if for all $x \in A$, there exists an $r > 0$, such that the interval $(x - r, x + r) \subseteq A$.

Definition 5.5. We say a set $C \subseteq \mathbb{R}$ is **closed**, if its complement, $C^c \subseteq \mathbb{R}$ is open. (Recall, the complement is defined via the shorthand notation, $C^c = \mathbb{R} \setminus C$.)

5.3 Sequences of real numbers

A **sequence** of real numbers is an ordered list $\{a_n\}_{n \in \mathbb{N}}$. Formally, a sequence is a function $a : \mathbb{N} \to \mathbb{R}$, but think of them as simply a list.

Definition 5.6. We say a sequence $\{a_n\}_{n \in \mathbb{N}}$ **converges to the real number** $L \in \mathbb{R}$ if for every $\epsilon > 0$, there exists an $N \in \mathbb{N}$, such that for all $n \geq N$, we have $|a_n - L| < \epsilon$.

We will refer to this definition as the "ϵ-N" definition of convergence.

Definition 5.7. We say a sequence **converges** if there exists an $L \in \mathbb{R}$, such that the sequence converges to L.

Definition 5.8. We say a sequence, $\{a_n\}_{n \in \mathbb{N}}$, is **bounded** if there exists a real number, say M, such that for all $n \in \mathbb{N}$,

$$|a_n| \leq M$$

Note this is the same thing as saying the set

$$E = \bigcup_{n \in \mathbb{N}} \{a_n\}$$

is a bounded subset of $\mathbb{R}$.

6 Linear Algebra

Definition 6.1. A set V is a vector space over the reals, $\mathbb{R}$, if it satisfies the following axioms. For each of the following, assume $u, v, w \in V$ are "vectors", and $a, b \in \mathbb{R}$ are "scalars":

(i) Closure of addition: $v + w \in V$, that is "+" is a function such that $+ : V \times V \to V$.

(ii) Closure of scalar multiplication: $av \in V$, that is "multiplication" is a function with "multiplication" $: \mathbb{R} \times V \to V$.

(iii) Associativity of addition: $u + (v + w) = (u + v) + w$.

(iv) Commutativity of addition: $u + v = v + u$.

(v) Identity element of addition: There exists an element $0 \in V$, called the zero vector, such that $v + 0 = v$ for all $v \in V$.

(vi) Inverse elements of addition: For every $v \in V$, there exists an element $-v \in V$, called the additive inverse of v, such that $v + (-v) = 0$.

(vii) Compatibility of scalar multiplication with scalar multiplication: $a(bv) = (ab)v$.

(viii) Identity element of scalar multiplication: $1v = v$, where $1 \in \mathbb{R}$ denotes the multiplicative identity.

(ix) Distributivity of scalar multiplication with respect to vector addition: $a(u + v) = au + av$.

(x) Distributivity of scalar multiplication with respect to addition of real numbers: $(a + b)v = av + bv$.

Remark 6.2. The classical vector space to keep in mind is Euclidean space, $\mathbb{R}^n$.

Remark 6.3. The set, $\mathbb{R}^2$, is a vector space over $\mathbb{R}$ under the following definitions for vector addition and scalar multiplication:

$$x + y := (x_1 + y_1, x_2 + y_2)$$

and

$$\lambda x := (\lambda x_1, \lambda x_2),$$

where $x = (x_1, x_2) \in \mathbb{R}^2$, $y = (y_1, y_2) \in \mathbb{R}^2$, and $\lambda \in \mathbb{R}$. It is tedious, but easy to check that this is true by verifying items (i)–(x).
Similarly, the set, $\mathbb{R}^d$, is a vector space with the same component-wise addition and scalar multiplication rules. For example, you should be working with $\mathbb{R}^3$ as a vector space in your MTH 234 class (if not yet, then soon).

In the case of subsets, many of these are automatically inherited from the overlying vector space. The following definition and upcoming proposition elaborate on this idea.

Definition 6.4. If V is a vector space, and $W \subseteq V$ is a subset of V, and W is a vector space with respect to the operations in V, then W is called a **subspace** of V.

Proposition 6.5. If V is a vector space, and $W \subseteq V$ is a non-empty subset, then W is a subspace of V if it satisfies the following two properties:

1. Closure under addition: if $u, v \in W$, then $u + v \in W$, and
2. Closure under scalar multiplication: if c is a scalar, and $u \in W$, then $cu \in W$.

Definition 6.6. If V and W are vector spaces over the reals, $\mathbb{R}$, and $L : V \to W$, then L is a **linear map** (also called a linear function) if and only if L satisfies

i) Additivity: $L(u + v) = L(u) + L(v)$, for all $u, v \in V$, and

ii) Scalar multiplication: $L(au) = aL(u)$, for all scalars $a \in \mathbb{R}$, and $u \in V$.

Definition 6.7. Matrix-vector multiplication in $\mathbb{R}^2$ is defined for a matrix, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and an element, $x \in \mathbb{R}^2$, with $x = (x_1, x_2)$. The formula which defines matrix multiplication is

$$Ax := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} := (ax_1 + bx_2, cx_1 + dx_2).$$

Here, we require that $a, b, c, d \in \mathbb{R}$.

Proposition 6.8. If we define the space of all 2×2 matrices

$$V = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a, b, c, d \in \mathbb{R} \right\},$$

with the addition operation as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix},$$

and the scalar multiplication operation, for $\lambda \in \mathbb{R}$, as

$$\lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix},$$

then V is a vector space over $\mathbb{R}$.