MAT 1348: Notes on Set Theory I

Prof. P. J. Scott Winter 2016

1 Sets

Sets are the basis of much of modern mathematics. You are already familiar from your other mathematics courses with some basic sets which mathematicians use. Let's give some examples:

1. *Finite sets*: these are finite collections of distinct elements. The set A with elements $a_1, \cdots, a_n$ is denoted by $A = \{a_1, \cdots, a_n\}$. For example, the set $\{1, 2, 5, 9\}$ consisting of the four numbers 1, 2, 5, and 9, or the set $\{\Box\}$ consisting of one element, $\Box$. Finally, a very important set: the *empty set* (or null set) $\emptyset$, which has no elements at all! The empty set is defined by $\emptyset = \{x \mid \mathbf{F}\} = \{x \mid 0 = 1\}$. You can use any false property $\mathbf{F}$ to define $\emptyset$. **Notation**: Please use $\emptyset$ and do not write $\{\ \}$, which is sometimes ambiguous. The *cardinality* of the finite set $\{a_1, \cdots, a_n\}$ is defined to be n, the number of elements in the set. Notice: we allow sets to be elements of sets. So the set $S = \{\{1, 2\}, \{a, b, c\}\}$ has 2 elements: one is a set of cardinality 2, the other is a set of cardinality 3. But S itself has cardinality 2, since it consists of those two sets shown. The cardinality of $\emptyset$ is defined to be 0, since $\emptyset$ has 0 elements.

2. **Important example** Notice: the set $A = \{\emptyset\}$ has *one* element, namely the empty set itself! So A is not empty and the cardinality of A is 1. Notice $\{\emptyset, \{\emptyset\}\}$ has two elements, so has cardinality 2. Make sure you understand this! We usually write $card(A)$ or $|A|$ for the cardinality of a finite set.[1]

3. *Infinite Sets:* The following basic infinite sets are often used in mathematics:

   (a) $\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$ (the positive integers).

   (b) $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$ (the natural numbers).

   (c) $\mathbb{Z} = \{0, 1, 2, 3, \cdots, -1, -2, -3, \cdots\}$ (the integers).

   (d) $\mathbb{Q} = \{m/n \mid m, n \in \mathbb{Z}, n \neq 0\}$ (the rationals).

   (e) $\mathbb{R}$ = the set of real numbers.

   (f) $\mathbb{C}$ = the set of complex numbers = the set of numbers of the form $a + bi$, where a, b are real numbers and $i = \sqrt{-1}$.

4. Sets of functions used in calculus: for example, the sets of continuous, differentiable or integrable functions $\mathbb{R} \to \mathbb{R}$.

5. Solution sets of linear equations or the set of roots of a polynomial.

Notation: Below we use usual logic notation of Boolean equivalence: $\varphi \equiv \psi$ means $\varphi \leftrightarrow \psi$ is a tautology, i.e. the formulas are logically equivalent.

Definition 1.1 Intuitively, a *set* is a collection of distinct elements which satisfy some common property.

[1] It is possible to talk about the cardinality of infinite sets, but we don't cover that in this course. It is a fascinating subject: see Rosen, Chapter 2.5

- We write $\{x \mid \varphi(x)\}$ for the set of elements x satisfying property $\varphi(x)$.
- Given a set S, we write $a \in S$ to say that *a is an element of set S*.

We will not make too precise for now which "properties" $\varphi(x)$ are legitimate; for the sets we use in this course, the properties φ will be easily described in basic logic.

Equality Principle: *Two sets are equal if and only if they have the same elements.* More formally, given two sets X and Y,

$$X = Y \quad \text{if and only if} \quad (\text{for all elements } a)(a \in X \equiv a \in Y)$$

Hence, the following two sets are equal $\{1, 1, 2\} = \{1, 2\}$, because they have the same elements.[2]

We write $A \neq B$ to say A and B are unequal sets. That means they do not have the same elements. That means there are elements of one set which are not elements of the other set.

Other examples were given in class. This is a **very** important idea.

General Comprehension Principle[3]: For any element a, $a \in \{x \mid \varphi(x)\} \equiv \varphi(a)$.

This says that any element of a set must satisfy the property φ which defines the set. So it says: if $S = \{x \mid \varphi(x)\}$ is the set of elements x satisfying property $\varphi(x)$, then to say $a \in S$ (that is, to say *a is an element of S*) is the same thing as saying " a has property φ, that is, that $\varphi(a)$ is true."

Example 1.2 Suppose we look at numbers. Let $\varphi(x)$ mean "x is even". Then the even numbers $\mathcal{E}$ are precisely the set of numbers which have property φ, that is: $\mathcal{E} = \{x \mid x \text{ is even}\} = \{x \mid \varphi(x)\}$. Hence $4 \in \mathcal{E}$ means $\varphi(4)$, that is, it means "4 is even". This is the Comprehension Principle.

Example 1.3 Suppose we consider the set of roots of a polynomial p:

$$X = \{x \mid p(x) = 0\} \qquad (\text{here the property } \varphi(x) \text{ is } p(x) = 0).$$

Then to say $r \in X$ just says $p(r) = 0$, i.e. it says that r is a root of p. This is what the Comprehension Principle says in this case.

Which sets exist? We will take the informal principle that sets used in mathematics should exist. We begin with some informal axioms as discussed in class.

Axiom 0. The empty set $\emptyset$ and any finite set of distinct elements exist. In particular, $\{\emptyset\}$ exists. Also, any set $\{a\}$ with a single element a exists. We call this a *singleton* set. Notice a may itself be a set: so what? Still $\{a\}$ is a set of cardinality 1. A *doubleton* is a finite set of two distinct elements, say $\{a, b\}$. Again, a, b are distinct, and may be sets. In this course, we allow ourselves to pick arbitrary elements $a, b, \cdots$ as elements in our finite sets: $a, b, \cdots$ can be integers, rationals, reals, or even infinite sets!. For example, the set $\{\pi, \mathbb{N}\}$ has two elements, the number π and the set $\mathbb{N}$, so it has cardinality 2 !

[2]Note that $\{1, 1, 2\}$ and $\{1, 2\}$ give different *lists* and also different *multisets* in the terminology of computer science, but as *ordinary sets* they are equal, and have exactly 2 distinct elements.

[3]In general, this Principle is too general and is actually inconsistent: this is called Russell's paradox: Rosen, p. 126, # 46. So in practice, mathematicians use a weaker axiom: Zermelo's Comprehension Principle, discussed below.

Axiom 1. The sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ exist.

Axiom 2. (Zermelo's Comprehension Principle) If A is a set, and $\varphi(x)$ is some mathematical property of the variable x (which ranges over A), then $\{x \in A \mid \varphi(x)\}$ exists and is a subset of A. Moreover,

$$a \in \{x \in A \mid \varphi(x)\} \ \equiv \ (a \in A \ \wedge \ \varphi(a) \ )$$

Further axioms of Set-Theory used in everyday mathematics will be discussed below (for example Powersets).

Remark 1.4 (Advanced Theory) More precise treatments of logic and axiomatic set theory start with basic axioms of sets that imply that finite sets (including $\emptyset$ and singletons $\{x\}$) exist, as well as the natural numbers $\mathbb{N}$ (with associated properties of Peano arithmetic) should exist. Then we add axioms for more advanced set-theoretic constructions (like powersets (see below), and unions of indexed families). Using set-theoretic techniques (e.g. equivalence relations) one constructs $\mathbb{Z}$ and $\mathbb{Q}$ from $\mathbb{N}$ and later we construct $\mathbb{C}$ from $\mathbb{R}$. The tricky part is to construct the reals $\mathbb{R}$ from the rationals $\mathbb{Q}$, which involves developing some limiting processes (like Cauchy sequences of rationals) or Dedekind Cuts.

Example 1.5

(i) The set of even numbers is $\mathcal{E} = \{x \in \mathbb{Z} \mid Even(x)\}$ where $Even(x) =$ (for some $y \in \mathbb{Z}$)$(x = 2y)$. Notice that by the Comprehension Principle, $n \in \mathcal{E}$ if and only if n has the property $Even(n)$. This means: $n \in \mathcal{E}$ if and only if $n \in \mathbb{Z} \wedge Even(n)$, which means: $n \in \mathcal{E}$ if and only if n is an even integer.

(ii) Rational numbers are real numbers with finite or repeating decimal expansion, e.g. $\frac{1}{8} = .125$ and $\frac{1}{3} = .33333\ldots$ Hence

$$\mathbb{Q} = \{r \in \mathbb{R} \mid \ r \text{ has a finite or repeating decimal expansion}\}$$

What is the property $\varphi(r)$ defining $\mathbb{Q}$ above? By the Comprehension Principle, why is $\frac{1}{4} \in \mathbb{Q}$?

Definition 1.6 (Subsets) We say A *is a subset of* B, denoted $A \subseteq B$, if *all elements of* A *are elements of* B. Symbolically, this says $\forall a(a \in A \ \rightarrow \ a \in B)$. **Notice:** $A \not\subseteq B$ (A is **not** a subset of B) says: $\neg\forall a(a \in A \ \rightarrow \ a \in B)$, which is equivalent to $\exists a(a \in A \wedge a \notin B)$; i.e. there is some element a which is in A but not in B.

Theorem 1.7 *For any sets* A, B*:*

(i) $\emptyset \subseteq A$.

(ii) $A \subseteq A$.

(iii) $A = B$ *if and only if* $A \subseteq B$ *and* $B \subseteq A$.

Let's see how to prove them: Let x be an arbitrary element.

$$A \subseteq B \quad \text{means} \quad (\text{for all } x)(x \in A \text{ implies } x \in B)$$

Proof. Let P be the statement $x \in A$, Q be the statement $x \in B$, for an arbitrary element x. Then to say $A \subseteq B$ corresponds to saying $P \to Q$ is a tautology (that is, always true, for each element x).

(i). $\emptyset \subseteq A$ translates into:

$$\textit{for each element } x, \quad (x \in \emptyset \to x \in A) \textit{ must be a tautology.} \tag{1}$$

The comprehension principle says: for any element x, $\quad x \in \emptyset \equiv \mathbf{F}$ (i.e. $x \in \emptyset$ is constantly false). Let $P = x \in A$. Then statement (1) becomes the tautology $\mathbf{F} \to P$. Hence $\emptyset \subseteq A$.

(ii). Using the notation above, $A \subseteq A$ becomes the tautology $P \to P$ (for arbitrary elements x).

(iii) Exercise: use the definition. □

We end with an important exercise:

Exercises 1.8 (Important!)

(i) $\{\emptyset\} \subseteq \{\emptyset, \{\emptyset\}\}$ and also $\{\emptyset\} \in \{\emptyset, \{\emptyset\}\}$. Why? Is $\{\emptyset\} \in \emptyset$? Is $\emptyset = \{\emptyset\}$?

(ii) Given two sets $A = \{x \mid \varphi(x)\}$ and $B = \{x \mid \psi(x)\}$, when does $A = B$? Check that $A = B$ if and only if for all x, $\varphi(x) \equiv \psi(x)$, i.e. $\varphi(x) \leftrightarrow \psi(x)$ is a tautology.

2 Boolean Algebras and Powersets

Definition 2.1 Given a set $\mathcal{U}$, the *powerset of* $\mathcal{U}$, denoted $\mathcal{P}(\mathcal{U})$, is the set of all subsets of $\mathcal{U}$. Symbolically $\mathcal{P}(\mathcal{U}) = \{A \mid A \subseteq \mathcal{U}\}$.

Axiom 3. Power Sets] Given any set $\mathcal{U}$, the powerset $\mathcal{P}(\mathcal{U})$ exists, with all the structure described below.

The powerset of a set is a typical example of a Boolean Algebra. An abstract boolean algebra is a tuple

$$\mathcal{B} = (B, \wedge, \vee, \overline{\ }, \mathbf{F}, \mathbf{T})$$

satisfying the equations we wrote for Boolean algebras. In the case of the powerset,

$$\mathcal{P}(\mathcal{U}) = (\mathcal{P}(\mathcal{U}), \cap, \cup, \overline{\ }, \emptyset, \mathcal{U})$$

the operations are *intersection* , *union* , and *complement* of subsets as given by:

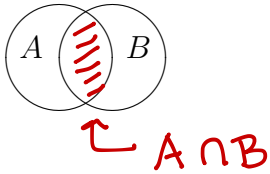
$$\begin{array}{rcll} A \cap B & = & \{x \in \mathcal{U} \mid (x \in A) \wedge (x \in B)\} & (\textit{intersection}) \\ A \cup B & = & \{x \in \mathcal{U} \mid (x \in A) \vee (x \in B)\} & (\textit{union}) \\ \overline{A} & = & \{x \in \mathcal{U} \mid x \notin A\} & (\textit{complement}) \end{array}$$

where $x \notin A$ means $\neg(x \in A)$. The equations of boolean algebras again are given in the notes on propositional calculus. But here is the table of Boolean Algebra laws from earlier in the course, now translated into the set theory language. Let $A, B, C \subseteq \mathcal{U}$ be subsets of a big set $\mathcal{U}$.

$(A \cup \neg A) = \mathcal{U}$	$(A \cap \neg A) = \emptyset$	Negation Laws
$(\emptyset \cup A) = A$	$(\mathcal{U} \cap A) = A$	Unit Laws
$(A \cup A) = A$	$(A \cap A) = A$	Idempotent Laws
$\overline{\overline{A}} = A$	$\overline{\overline{A}} = A$	Double Complement Law
$(A \cup B) = (B \cup A)$	$(A \cap B) = (B \cap A)$	Commutative Laws
$((A \cup B) \cup C) = (A \cup (B \cup C))$	$((A \cap B) \cap C) = (A \cap (B \cap C))$	Associative Laws
$(A \cup (B \cap C)) = (A \cup B) \cap (A \cup C)$	$(A \cap (B \cup C)) = (A \cap B) \cup (A \cap C)$	Distributive Laws
$\overline{(A \cap B)} = (\overline{A} \cup \overline{B})$	$\overline{(A \cup B)} = (\overline{A} \cap \overline{B})$	De Morgan's Laws

Venn and Hasse Diagrams

We draw pictures of sets in various ways (described in class). *For example:*



$A \cap B$ is the region of intersection

Examples 2.2

(i) $\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$ (this has 4 elements).

(ii) $\mathcal{P}(\{0,1,2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$ (this has 8 elements).

In class we drew the above powersets as *Hasse Diagrams*: this means we put the smallest subset ($= \emptyset$) at the bottom, the whole set at the top, and we draw a vertical (or oblique) line to mean "subset":

$$\begin{array}{l} B \\ | \quad \leftarrow \text{means } A \subseteq B \\ A \end{array}$$

In class I showed how $\mathcal{P}(\{0,1\})$ is a diamond shaped graph. whereas $\mathcal{P}(\{0,1,2\})$ is a graph with 8 nodes and 12 edges: bottom node is the empty set, then above them are all the singleton subsets, then above them are all the doubleton subsets, then at the top is the whole set $\{0,1,2\}$. Draw it yourself.

Example 2.3 (Proving Set Equations by Propositional Calculus) Given a Boolean algebra of sets, say $\mathcal{P}(\mathcal{U})$, we need to be able to prove the Boolean algebra equations.

For example, if $A, B, C \in \mathcal{P}(\mathcal{U})$ (so A, B, C are subsets of $\mathcal{U}$), consider some Boolean algebra equations, like commutativity of intersection: $A \cap B = B \cap A$ and De Morgan's Law: $\overline{A} \cap \overline{B} = \overline{A \cup B}$. How do we prove them? Translate to propositional calculus and check you get a tautology!

For example, to show $A \cap B = B \cap A$, let $x \in \mathcal{U}$ be an arbitrary element. We have to show $x \in A \cap B$ if and only if $x \in B \cap A$. This means we must show:

$$(x \in A) \wedge (x \in B) \quad \text{if and only if} \quad (x \in B) \wedge (x \in A) \tag{2}$$

Let $P = (x \in A)$ and $Q = (x \in B)$. Then (2) becomes the tautology $(P \wedge Q) \leftrightarrow (Q \wedge P)$. That is, we know $P \wedge Q \equiv Q \wedge P$, hence (2) holds.

Similarly, as an exercise, check that the following de Morgan law for Sets $\overline{A} \cap \overline{B} = \overline{A \cup B}$ translates into the similar de Morgan tautology in Logic, by letting $P = (x \in A)$ and $Q = (x \in B)$. Hence, check the above de Morgan law becomes

$$(\neg P \wedge \neg Q) \leftrightarrow \neg(P \vee Q) \quad \text{the de Morgan propositional tautology}$$

3 Cartesian Products and Relations

Axiom 3: Given two sets A and B, we can form their *cartesian product*

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

where (a, b) is the *ordered pair* of the two elements a and b.

Important Notice: in an ordered pair (a, b), a is the *first* element of the ordered pair, and b is the second element. Notice $(a, b) \neq (b, a)$. In fact we define $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. This is *definitely different* than the case of the doubleton set $\{a, b\}$, since by definition of equality of sets, we know $\{a, b\} = \{b, a\}$. Why?

In class I draw pictures of sets $A \times B$ using the x-y axes: let A lie on the x axis, B on the y-axis, and elements of $A \times B$ are ordered pairs in the plane determined by these two sets.

Examples 3.1

(i) $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 2)\}$ (It has 6 elements).

(ii) (Euclidean 2-dimensional space) $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the set of ordered pairs of real numbers.

(iii) (Euclidean n-dimensional space) $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$ (n times) is the set of n-tuples of real numbers. (This is a generalization of $\mathbb{R}^2$ using ordered n-tuples of real numbers, instead of just ordered pairs).

Definition 3.2 (Relations) A *binary relation between sets A and B* is a subset $R \subseteq A \times B$. An *n-ary relation on sets $A_1, \cdots, A_n$* is a subset $R \subseteq A_1 \times \cdots \times A_n$.

As a special case when all the sets A_i are equal, a binary *relation* or *predicate* on a set A is a subset $R \subseteq A \times A$. More generally, an *n-ary relation or predicate on a set A* is a subset $R \subseteq A \times A \times \cdots \times A$ (n-times).

So a binary relation is a set of ordered pairs of elements; an n-ary relation is a set of n-tuples of elements.

Notation: Mathematicians often write aRb or $R(a, b)$ to say $(a, b) \in R$, i.e. that the pair (a, b) is in the relation R.

4 Functions

This is one of the most important concepts in mathematics. Functions are everywhere in mathematics: calculus is all about properties of differentiation and integration of functions, linear algebra studies linear functions (e.g. matrices), analysis and topology study many kinds of continuous or smooth functions. In algebra, we study structure-preserving homomorphisms for a wide range of structures (groups, rings, boolean algebras, etc.) In computer science we often consider algorithms or programs as describing functions from inputs to outputs.

Definition 4.1 (Functions-as-Rules) Given two sets A and B, a *function* $f : A \to B$ *or* $A \xrightarrow{f} B$ is a rule or formal procedure which assigns to each input $x \in A$ a specific output $f(x) \in B$. Here, for each input $x \in A$, the output is *unique*, in the sense that one input x must have exactly one corresponding output $f(x)$. (Of course, all the outputs can be the same element of B, if the function f is a constant function. But the main thing is, each input must lead to exactly one output.) We write $x \mapsto f(x)$ for the action of f on input elements x. We say:

- A is the *domain of* f
- B is the *codomain of* f
- The set $f(A) = \{f(x) \in B \mid x \in A\}$ is the *range of* f. Notice that $f(A) \subseteq B$, i.e. the range of f is a subset of B.

An alternative to the above view is the purely set-theoretic view of functions. We identify a function with its graph (a relation). This becomes the following:

Definition 4.2 (Functions-as-Relations) A *function* from A to B is a binary relation $R \subseteq A \times B$ satisfying:

(i) (*Functionality*) For all $x \in A$, $y \in B$, $y' \in B$

$$(x, y) \in R \ \wedge \ (x, y') \in R \quad \text{implies} \quad y = y'$$

(ii) (*Totality*) For all $x \in A$ there exists a $y \in B$ such that $(x, y) \in R$.

We call the elements $x \in A$ *inputs* and the elements $y \in B$ for which $(x, y) \in R$ (for some x) *outputs*. The set A is called the *domain* of the function R. The set B is called the *codomain* of the function R. The set of outputs is called the *image* or *range* of the function; it is a subset of B.

So a function from A to B is a relation satisfying: for all inputs x, there is a *unique* output y such that $(x, y) \in R$. We often write a function as a triple (A, R, B) where A is the domain, B is the codomain, and R is the relation determining the function. It is also convenient to introduce the standard notation (functions-as-rules) above, as follows. Let $f = (A, R, B)$ be a function; we write $f : A \to B$ for this function, where we understand $f(x) = y$ means $(x, y) \in R$. This is well-defined: why?

5 Algebra of functions

When are two functions equal? When they have exactly the same values for all inputs.

Definition 5.1 (Equality of functions) *Let $f, g : A \to B$ be two functions. We say*

$$f = g \quad \textit{iff} \quad \forall x \in A(\ f(x) = g(x)\ ).$$

Examples 5.2 (identity functions, composition)

1. For any set A, the *identity function* $id_A : A \to A$ satisfies $id_A(x) = x$.
2. Given functions $A \xrightarrow{f} B \xrightarrow{g} C$, their *composite* $g \circ f : A \to C$ is given by:

   $$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in A$$

   That is, $g \circ f$ is the function $x \mapsto g(f(x))$.

Proposition 5.3 (Laws of composition)

1. *For all functions $f : A \to B$, $f \circ id_A = f = id_B \circ f$.*
2. *For all functions $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, $h \circ (g \circ f) = (h \circ g) \circ f$.*

Finally, a slightly advanced topic we will need later in the course. We can form the set of all functions between two sets:

Proposition 5.4 (Existence of Function Spaces) *For any sets A, B, we can form*

$$B^A = \{f \mid f : A \to B\}$$

In addition, there is an "evaluation" function: $ev : B^A \times A \longrightarrow B$ given by $ev(f, a) = f(a)$, for all $f \in B^A$ and $a \in A$.

Remark 5.5 (Advanced) For those who want to know how to prove the above Proposition in axiomatic set theory, notice it is a special case of Zermelo's Comprehension axiom. Once we know the Powerset and Cartesian product axioms: for then $P(A \times B)$ exists, so using the relation-view of functions, and the Comprehension Axiom:

$$B^A = \{R \in P(A \times B) \mid \text{the relation } R \text{ is a function from } A \text{ to } B\} = \{R \in P(A \times B) \mid \varphi(R)\}$$

where the formula $\varphi(R)$ is easy to write in logic, using quantifiers.