MAT 1348: Notes on Set Theory I

Prof. P. J. Scott Winter 2015

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.

1. *Finite sets*: these are finite collections of distinct elements. The set with elements $a_1, \cdots, a_n$ is denoted by $\{a_1, \cdots, a_n\}$. 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 $\emptyset$, 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 to define $\emptyset$.

2. The following basic infinite sets:

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

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

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

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

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

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

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

Notation: Below we use usual logic notation: $\varphi \equiv \psi$ means $\models \varphi \leftrightarrow \psi$, i.e. $\varphi \leftrightarrow \psi$ is a tautology.

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

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

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 predicate 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 two collections $\{1, 1, 2\} = \{1, 2\}$, because they have the same elements. [1] Other examples were given in class.

Comprehension Principle: 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.

[1] 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.

Example 1.2 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. that r is a root of p. This is just what the Comprehension Principle says.

Which sets exist? We will take the informal principle that sets used in mathematics exist. So for example:

Axiom 0. The sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ exist.

Axiom 1. The empty set $\emptyset$ and any finite set of distinct elements exist.

Given a set $\mathcal{U}$, we write $\{x \in \mathcal{U} \mid \varphi(x)\}$ for the collection of those elements x in $\mathcal{U}$ satisfying $\varphi(x)$. Sets in mathematics can usually be taken to be in this form: they are typically subsets (or sets of subsets, or sets of sets of subsets ...) of some underlying set $\mathcal{U}$. We will describe this in more detail in many examples below and in class.

Example 1.3

(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 1.4 (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 (for all a)$(a \in A$ implies $a \in B)$.

Theorem 1.5 *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 we have a tautology: $\models P \to Q$ (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 1.6 (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, there's a tautology $\models \varphi(x) \leftrightarrow \psi(x)$.

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 2. 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:

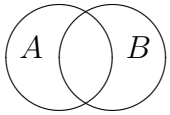
$$\begin{array}{rcll} A \cap B & = & \{x \in \mathcal{U} \mid (x \in A) \wedge (x \in B)\} & (\textit{intersection}) \\ A \cup B & = & \{x \in \mathcal{U} \mid (x \in A) \vee (x \in B)\} & (\textit{union}) \\ \overline{A} & = & \{x \in \mathcal{U} \mid x \notin A\} & (\textit{complement}) \end{array}$$

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?

Let x 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 $\models (P \wedge Q) \leftrightarrow (Q \wedge P)$.

Similarly, as an exercise, check that the de Morgan law for Sets $\overline{A} \cap \overline{B} = \overline{A \cup B}$ becomes the de Morgan tautology in Logic, where $P = (x \in A)$ and $Q = (x \in B)$, as above:

$$\models (\neg P \wedge \neg Q) \leftrightarrow \neg(P \vee Q)$$

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

One of the most important concepts in mathematics is that of *function*. Functions are everywhere in mathematics: calculus is all about properties of differentiation and integration of functions, linear algebra studies linear functions (matrices), etc.

Definition 4.1 (Functions) 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 another notation, as follows.

Let $f = (A, R, B)$ be a function; we often write $f : A \to B$ for this function, where we understand $f(x) = y$ means $(x, y) \in R$. This is well-defined: for each input x, there is a unique output $y = f(x)$ determined by the relation R. This notation leads to the following ideas.

In computer science and many parts of mathematics, it is convenient to have a slightly more "algorithmic" view of functions. In this view, a function $f : A \to B$, sometimes written $A \xrightarrow{f} B$, is thought of as a machine or algorithm: it takes inputs $x \in A$, it applies the algorithm or computation instructions determined by the recipe for f, and then outputs $y = f(x) \in B$. This is often written as $x \mapsto f(x)$, which shows how the mapping works on elements.

In class we give many examples and discuss functions in detail. For example, the many kinds of functions you have seen in calculus, and in linear algebra. In algebra and calculus there are polynomial functions and *rational functions* $f(x) = \frac{p(x)}{q(x)}$, for polynomials $p(x)$ and $q(x)$, where $q(x) \neq 0$. In computer science, there are many algorithms which give functions. Indeed, any computer program can be considered as a function from inputs to outputs. Logic is full of functions. For example, there are 16 Boolean functions $\{\mathbf{T}, \mathbf{F}\}^2 \to \{\mathbf{T}, \mathbf{F}\}$. (among them are the usual Boolean Connectives: conjunction, disjunction, implication, and their negations and converses, etc. Exercise: write down all 16 functions in a big table). The algorithm we gave for finding the truth table of a formula has as input a formula φ, and as output the truth table of φ.

More to come in Part II.