Section 0. Sets and Relations

NOTE. Mathematics is the study of ideas, not of numbers!!! The idea from modern algebra which is the focus of most of this class is that of a *group* (this class could easily be called *group theory*). We will often use numbers to give examples of groups, but the topics covered by modern algebra are the abstract ideas of groups, rings, and fields.

Note. As commented in the text on page 1, it is impossible to define all objects in mathematics. This is because we can only define new objects in terms of old objects—at some point we must have foundational objects which are known to us through intuition. One such object is a *set* of *elements*.

Note/Definition. A *set* is a collection of objects called *elements*. The elements of a set appear in no particular order. Also, an object is either in a set or not—it does not appear in a set a repeated number of times, for example. Therefore, we would write the set with elements $5, 3, 2+3, 2$, and $5-2$ as any one of the following: $\{5,3,2\}$, $\{5,2,3\}$, $\{3,5,2\}$, $\{3,2,5\}$, $\{2,5,3\}$, or $\{2,3,5\}$.

Notation. If a is an element of set S then we write "$a \in S$." If S is the set with no elements, we write $S = \varnothing$, the empty set or null set.

Definition 0.1. A set B is a *subset* of set A, denoted $B \subseteq A$ or $A \supseteq B$, if every element $b \in B$ is also an element of A. If B is a subset of A and $A \neq B$ (that is, A and B are different sets), then we write $B \subset A$ (or $B \subsetneq A$) or $A \supset B$ (or $A \supsetneq B$).

Note. Vacuously, for any set B, $\varnothing \subseteq B$

Note. We can show two sets A and B are equal, $A = B$, by showing (1) $A \subseteq B$ and (2) $B \subseteq A$.

Definition 0.2. If A is any set, then A itself is the *improper subset* of set A. All other subset of A are *proper subsets*. The set $\varnothing$ is the *trivial subset* of A.

Note. In axiomatic set theory, we need to have a *universal set*. All sets we discuss are then subsets of this known universal set. Subsets of the universal set can then be defined using a "characterizing property." For example, we can let the universal set be the set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ and define set A as

$$S = \{x \in \mathbb{N} \mid x^2 \leq 100\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

Notation. Several sets of numbers which we are interested in include:

1. The Natural Numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$,
2. The Whole Numbers $\mathbb{W} = \{0, 1, 2, 3, \ldots\}$,
3. The Integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ (the letter $\mathbb{Z}$ is used for the German *zahlen* for "number"),
4. The Rational Numbers $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$,
5. The Real Numbers $\mathbb{R}$, and
6. The Complex Numbers $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$.

Note. Some subsets of the above sets of real numbers are important. In particular, we have:

- The positive integers, rationals, and reals, denoted $\mathbb{Z}^+$, $\mathbb{Q}^+$, and $\mathbb{R}^+$, respectively.
- The nonzero integers, nonzero rationals, nonzero reals, and nonzero complex numbers, denoted $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$, respectively.

Notice. We have $\mathbb{Z}^* \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$ and $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Definition 0.4. Let A and B be sets. The set $A \times B = \{(a, b) \mid a \in A, b \in B\}$ is the *Cartesian Product* of A and B.

Example. If $A = \{1, 2, 3\}$ and $B = \{a, b\}$ then

$$A \times B = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}.$$

Definition 0.7. A *relation* between sets A and B is a subset $\mathcal{R}$ of $A \times B$. If $(a, b) \in \mathcal{R}$ we say a is related to b, denoted $a \,\mathcal{R}\, b$.

Example. Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$. Suppose $\mathcal{R} = \{(1, a), (2, a), (3, b)\}$. Then we have $1 \,\mathcal{R}\, a$, $2 \,\mathcal{R}\, a$, and $3 \,\mathcal{R}\, b$.

Definition 0.10. A *function* ϕ mapping set X into set Y is a relation between X and Y such that each $x \in X$ appears as the first member of exactly one ordered pair $(x, y) \in \phi$. We may also call a function a *map* or *mapping* of X into Y. We write $\phi : X \to Y$ and for $(x, y) \in \phi$ we write $\phi(x) = y$. The *domain* of ϕ is the set X and the *codomain* of ϕ is Y. The *range* of ϕ is the set $\phi[X] = \{\phi(x) \mid x \in X\}$.

Note. We use square brackets when applying a function to a set. The idea of a codomain is to tell the type of object which ϕ gives out. For example, if we treat multiplication of a column vector of dimension n be an $m \times n$ matrix, then we get an m dimensional vector. So the codomain is $\mathbb{R}^m$ (though the range may be a proper subset of $\mathbb{R}^m$).

Definition 0.12. A function $\phi : X \to Y$ is *one to one* (or an *injection*) if $\phi(x_1) = \phi(x_2)$ implies $x_1 = x_2$. The function ϕ is *onto* Y (or a *surjection*) if the range of ϕ is Y. A function that is both one to one and onto is called a *one-to-one correspondence* (or a *bijection*) between the domain and codomain.

Exercise 0.12. Let $A = \{1, 2, 3\}$ and $B = \{2, 4, 6\}$ Which of these are functions? If a function, which is one to one and which is onto B?
(a) $\{(1, 4), (2, 4), (3, 6)\}$ — A function.
(b) $\{(1, 6), (1, 2), (1, 4)\}$ — Not a function.
(c) $\{(2, 2), (1, 6), (3, 4)\}$ — A function, one to one and onto B.

Definition 0.13. Two sets X and Y have the *same cardinality* if there exists a one to one function mapping X onto Y (that is, if there is a one-to-one correspondence between X and Y).

Note. The idea of the cardinality of a set is that the cardinality (or more precisely, the "cardinal number") represents the size of the set. If the set is finite we can simply define the cardinality as the number of elements in the set. However, surprisingly there are different levels of infinity! The smallest level of infinity is the cardinality of $\mathbb{N}$ and is denoted $\aleph_0$ ("aleph nought"). We denote the cardinality of set A as $|A|$ and we have

$$\aleph_0 = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| \neq |\mathbb{R}| = |\mathbb{C}|.$$

A set of cardinality $\aleph_0$ is called *countable*. So $\mathbb{R}$ is not countable and the real

numbers form an infinite set that is larger than the infinite set $\mathbb{N}$. The details of these ideas are due to Georg Cantor in the late 19th century. These topics are studied in Analysis 1 (MATH 4217/5217).

Definition 0.16. A *partition* of a set S is a collection of nonempty subsets of S such that every element of S is in exactly one of the subsets.

Note. Sets A and B are *disjoint* if $A \cap B = \varnothing$. So the nonempty subsets of S which partition S (called the *cells* of the partition) are disjoint.

Example. We can define a partition of $\mathbb{Z}$ as follows. Define $A_0 = \{x \in \mathbb{Z} \mid 3 \text{ divides } x\}$, $A_1 = \{x \in \mathbb{Z} \mid 3 \text{ divides } x+2\}$, and $A_2 = \{x \in \mathbb{Z} \mid 3 \text{ divides } x+1\}$. Then A_0, A_1, and A_2 are the cells of a partitioning of $\mathbb{Z}$. We have $A_0 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $A_1 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$, and $A_2 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Definition 0.18. An *equivalence relation* $\mathcal{R}$ on a set S is a relation on S such that for all $x, y, z \in S$, we have

(1) $\mathcal{R}$ is *reflexive*: $x \mathcal{R} x$,

(2) $\mathcal{R}$ is *symmetric*: If $x \mathcal{R} y$ then $y \mathcal{R} x$, and

(3) $\mathcal{R}$ is *transitive*: If $x \mathcal{R} y$ and $y \mathcal{R} z$, then $x \mathcal{R} z$.

Example 0.20. Let $n \in \mathbb{N}$ Then for any $z \in \mathbb{Z}$, there are unique integers q and r such that $z = nq + r$ and $0 \leq r < n$. This is the Division Algorithm for $\mathbb{Z}$ and is explained in more detail in Section I.6 (see page 60). For such z and n, the number r is the *remainder* which results when z is divided by n. For a given $n \in \mathbb{N}$, there are n possible remainders which result as z ranges over all values in $\mathbb{Z}$ (namely, the remainders are $0, 1, 2, \ldots, n-1$). All $a \in \mathbb{Z}$ which yield a given value of r make up a *residue class modulo* n of $\mathbb{Z}$. In the previous example, A_0 is the residue class modulo 3 associated with remainder 0 modulo 3, A_1 is associated with reminder 1 modulo 3, and A_2 is associated with remainder 2 modulo 3. If two elements $a, b \in \mathbb{Z}$ occur in the same residue class modulo n, then we say a is *congruent* to b modulo n, denoted $a \cong b \pmod{n}$. For example, all even integers are congruent modulo 2 and all odd integers are congruent modulo 2. In fact, congruence modulo n (for given n) is an equivalence relation on $\mathbb{Z}$. Addition modulo n leads to consideration of the set of n equivalence classes on $\mathbb{Z}$ denoted $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Theorem 0.22. Equivalence Relations and Partitions.
Let S be a nonempty set and let $\sim$ be an equivalence relation on S. Then $\sim$ yields a partition of S into equivalence classes where for each $a \in S$ we define $\overline{a} = \{x \in S \mid x \sim a\}$. Also, each partition of S gives rise to an equivalence relation $\sim$ on S where $a \sim b$ if and only if a and b are in the same cell of the partition.

Note. The concept of using an equivalence relation to partition a set is a common one. In particular, we will use it in the proof of Lagrange's Theorem in Section I.10.

Note. You should recall the properties of logic and truth tables from your Mathematical Reasoning class (MATH 2800). Here, we use the symbol $\sim$ to mean negation when placed over a symbol (so $\tilde{p}$ is "not p"):

p	q	$p \cap q$	$p \cup q$	$p \Rightarrow q$	$\tilde{p}$	$\tilde{q}$	$\tilde{p} \cap \tilde{q}$	$\tilde{p} \cup \tilde{q}$	$\tilde{q} \Rightarrow \tilde{p}$
T	T	T	T	T	F	F	F	F	T
T	F	F	T	F	F	T	F	T	F
F	T	F	T	T	T	F	F	T	T
F	F	F	F	T	T	T	T	T	T

Notice that $\widetilde{(p \cap q)} = (\tilde{p} \cup \tilde{q})$, $\widetilde{(p \cup q)} = (\tilde{p} \cup \tilde{q})$, and $(p \Rightarrow q) = (\tilde{q} \Rightarrow \tilde{p})$. Here, by equality, we mean that the same truth values for p and q yield the same truth values on both sides of the equations.

Note. It is often useful to swap a statement for its contrapositive. For example, a function ϕ is one to one if $(\phi(x_1) = \phi(x_2)) \Rightarrow (x_1 = x_2)$. The contrapositive of this definition is $(x_1 \neq x_2) \Rightarrow (\phi(x_1) \neq \phi(x_2))$. So a function is one to one when different input values for a function imply different output values. This is why we can test the graph of $y = f(x)$ in the Cartesian plane for one-to-one-ness with the horizontal line test.

Revised: 1/22/2013