1. Basic Notions and Conventions

1.1 **Sets and Elements**.

A *set* is an unordered collection of distinct objects, called the *elements* of the set. These elements can be anything: numbers, letters, people, points, or even subsets of some other set. We will usually use a capital letter for the name of a set, and delineate a given set using curly braces. Thus the statement

$$\text{“Let } S = \{1, 2, 3, 4\},\text{”}$$

defines a set with four elements, and calls this set S. Because sets are not ordered, $S = \{2, 1, 4, 3\}$; and because sets are only sensitive to distinct elements, $S = \{1, 2, 2, 4, 3\}$. The symbol $\in$ is translated as “is an element of”, so that $1 \in S$; to signify that 5 is not in the set S, write $5 \notin S$ (in words: “5 is not an element of the set S”).

The *cardinality* of a set T is the number of elements in T, and we'll use the notation $\#(T)$ for that number. If T has an infinite number of elements, $\#(T) = \infty$; a finite set is a set with a finite cardinality, so that for the set S in the above paragraph, $\#(S) = 4$.

Defining a set in a clear and unambiguous way is an important first step in working with it. If the set is small enough and all the elements are known explicitly, the set can be given as a complete list of its elements: the statement

$$S = \{1, 2, 3, 4\}$$

completely and unambiguously conveys what S is to any reader. For larger sets where there is an obvious pattern, one can use an ellipsis:

$$T = \{1, 2, 3, \ldots, 10\}$$

makes it clear what T is. This even works for infinite sets:

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

clearly defines the integers and the strictly positive integers respectively. How far you can take this “fill in the blank” method for defining a set is subjective — when in doubt, be explicit:

$$S = \{1, 4, 9, \ldots\}$$

may make S clear to some readers and not to others. Better is the more explicit “Let S be the set of squares of the positive integers.” Even more explicit is the use of so-called set-builder notation:

$$S = \{n^2 \,|\, n \in \mathbf{N}\}.$$

One should read this as: “S equals the set of elments of the form n^2 such that $n \in N$.”

Here is a short list of some sets we will use throughout the course:

$\mathbf{N} = \{1, 2, 3, \ldots\}$	the counting numbers;
$\mathbf{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$	the integers;
$\mathbf{Q} = \{a/b \,\vert\, a, b \in \mathbf{Z}, b \neq 0\}$	the rational numbers;
$\mathbf{R}$	the real numbers;
$\mathbf{C} = \{a + bi \,\vert\, a, b \in \mathbf{R}\}$	the set of complex numbers;
$\mathbf{R}^2 = \{(a, b) \,\vert\, a, b \in \mathbf{R}\}$	the set of points in the plane.
$\emptyset$	the *empty set* or *null set*.

The last set listed is the set with no elements.

Once a set is clearly defined, one might expect it to be possible to test if any given object is in that set — this may be easy or quite hard (or even provably impossible). Roughly speaking, to show that element x is in set S, one must either do an exhaustive search of S (only practical if S is a small finite set!) or show that x satisfies all the properties used to define S. To show x is not an element of S, one can again "search and compare" if S is small, or find some defining property of S which x fails to satisfy. For example, if $S = \{n^2 \,\vert\, n \in \mathbf{N}\}$, then showing $64 \in S$ amounts to finding an integer n so that $n^2 = 64$; showing that $27 \notin S$ requires some additional information about S and about the integers — *e.g.,* that there are no squares of integers between 25 and 36. Similarly, it's clear that $\sqrt{2} \in \mathbf{R}$ and that $\sqrt{2} \notin \mathbf{Z}$, but it requires a (not too difficult) proof that $\sqrt{2} \notin \mathbf{Q}$.

1.2 **Subsets**.

Given two sets S and T, we say "S is a *subset* of T" if each element of S is also an element of T; the notation for this is the inclusion relation $S \subset T$ (one can also write $T \supset S$, meaning the same thing). To prove that $S \subset T$, one must show: for every $x \in S$ one has $x \in T$. To show that S is not a subset of T ($S \not\subset T$), usually one must find an element $x \in S$ so that $x \notin T$. For example, let

$$S = \{81, 225, 428\} \text{ and } T = \{n^2 \,\vert\, n \in \mathbf{Z}\}.$$

Then $S \not\subset T$ since $428 \notin T$ (8 is never the last digit of a perfect square!). By convention, we always consider $\emptyset \subset T$ for any set T (since $\emptyset$ contains no elements, the statement "for every $x \in S$, x is also in T" is vacuously true).

To show that two sets S and T are equal, one usually shows the two inclusions $S \subset T$ and $T \subset S$. There are sometimes some shortcuts. For example, if S and T are finite sets with the same cardinality, and one has shown that $S \subset T$, then $S = T$ is clear. Note that this won't work for infinite sets: $\mathbf{Z} \subset \mathbf{Q}$, but $\mathbf{Z} \neq \mathbf{Q}$.

Exercise. Given any set S, the *power set of* S is the set of subsets of S:

$$\mathcal{P}(S) = \{U \,\vert\, U \subset S\}.$$

For example, $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Write out $\mathcal{P}(\{a, b, c\})$. Determine (with proof) the cardinality of $\mathcal{P}(S)$ if S has n elements.

1.3 **Set Operations**.

Let S and T be subsets of some given *universal set* U. The *union* of S and T, written $S \cup T$, is the set of all objects which belong to either S or T:

$$S \cup T = \{x \,\vert\, x \in S \text{ or } x \in T\}.$$

For example, $\{a, b, c, d, e\} \cup \{a, c, e, f, h\} = \{a, b, c, d, e, f, h\}$.

The *intersection* of S and T, written $S \cap T$ is the set of elements common to both S and T:

$$S \cap T = \{x \,\vert\, x \in S \text{ and } x \in T\}.$$

For the specific S and T defined above, $S \cap T = \{a, c, e\}$. Two sets are said to be disjoint if their intersection is the empty set.

If X, Y, and Z are three sets, the following statements should be pretty clear: $X \cup Y = Y \cup X$; $X \cap Y = Y \cap X$; $(X \cup Y) \cup Z = X \cup (Y \cup Z)$; and $(X \cap Y) \cap Z = X \cap (Y \cap Z)$ (because of these equalities, we usually just write $X \cup Y \cup Z$ and $X \cap Y \cap Z$ for the last two sets).

Exercise. Show by giving an counterexample that in general $(X \cup Y) \cap Z \neq X \cup (Y \cap Z)$.

Exercise. If $S \cup T = T$, show that $S \subset T$. What similar statement can be made about intersections? If $S \cup T = S \cap T$, how are S and T related?

The *complement* of S (in U) is the set of all elements (of U) which are not in S. There isn't a standard notation for this — we'll use S':

$$S' = \{x \in U \,|\, x \notin S\}.$$

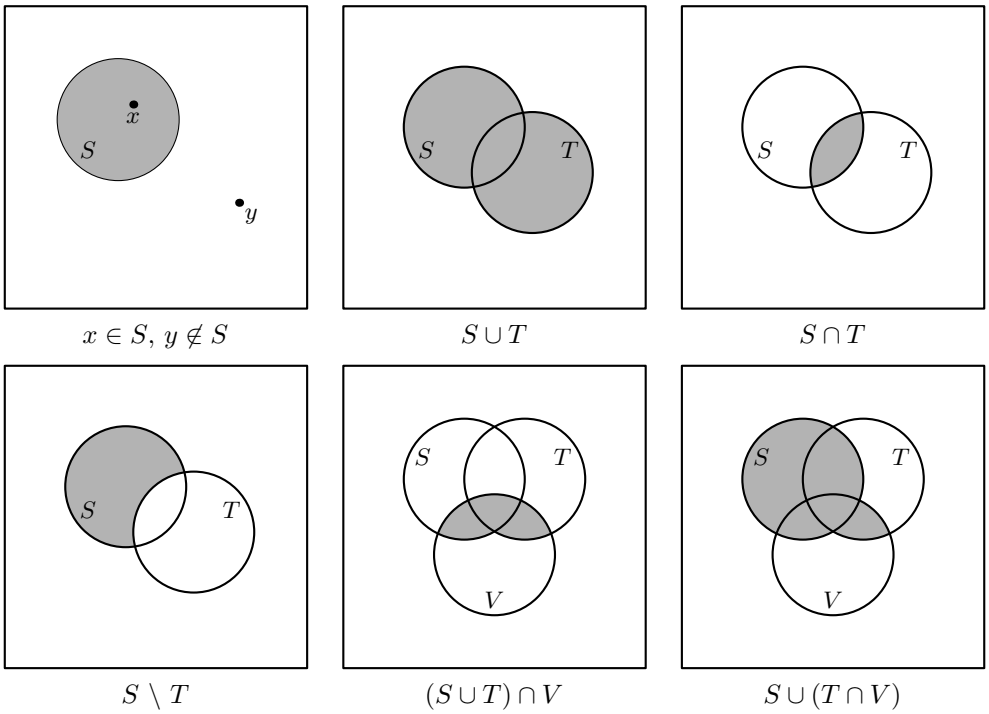
More generally, define the set-theoretic difference $S \setminus T$ to be those elements of S which are not in T:

$$S \setminus T = \{x \in S \,|\, x \notin T\} = S \cap T'.$$

Exercise. If X, Y, and Z are given subsets of a universal set U, prove: (1) that $(X \cup Y)' = X' \cap Y'$; and (2) that $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$.

1.4 **Venn Diagrams**.

Venn diagrams provide a way to picture some set theory arithmetic. Sets are indicated by closed regions and elements of these sets are represented by points shaded inside these regions. See the examples below:



$x \in S,\ y \notin S$ | $S \cup T$ | $S \cap T$

$S \setminus T$ | $(S \cup T) \cap V$ | $S \cup (T \cap V)$

1.5 **Cartesian Products**.

Given two sets S and T, we define a new set called the *Cartesian product of S and T*, written $S \times T$. The elements of this set are ordered pairs of objects, the first entry being from S and the second entry being from T:

$$S \times T = \{(x, y) \,|\, x \in S, y \in T\}.$$

For example, if $S = \{1, 2, 3\}$ and $T = \{a, b\}$, then

$$S \times T = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Note that $S \times T$ and $T \times S$ are different sets.

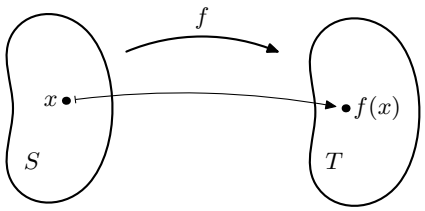
A familiar example of Cartesian products occurs in analytic geometry. $\mathbf{R} \times \mathbf{R}$ is usually written $\mathbf{R}^2$ is and represented by points in the (coördinatized) Euclidean plane: a point P corresponds to the element $(a, b) \in \mathbf{R}^2$ if the point projects onto the number a on the horizontal axis, and onto the number b on the vertical axis.

Exercise. Using the plane to represent $\mathbf{R} \times \mathbf{R}$ in this way, sketch the following sets:(1) $\mathbf{R} \times \mathbf{Z}$; (2) $\{(x, y) \,|\, x = -y\}$.

Of course, we can take the Cartesian product of more than two sets: $S \times T \times U = \{(s, t, u) \,|\, s \in S, t \in T, u \in U\}$; we usually identify this with the sets $(S \times T) \times U$ and $S \times (T \times U)$. When taking the Cartesian product of S with itself n times, we usually write S^n in place of $S \times S \times \ldots \times S$. A typical element of S^n is called an *ordered n-tuple*.

1.6 **Functions**.

A *function* f from a set S to a set T is a way of associating to each element $x \in S$ a particular element $f(x) \in T$. S is called the *domain* of f and T is called the *codomain* of f. This data can be expressed succinctly by $f : S \to T$ or $S \xrightarrow{f} T$, and can be pictured as in the diagram:



Two functions $f : S \to T$ and $g : S \to T$ are equal if $f(x) = g(x)$ for each $x \in S$ — keep in mind that this involves the domain: the functions $f(x) = \sin(\pi x)$ and $g(x) = 0$ are certainly different if our domain is $\mathbf{R}$, but if we restrict our domain to $\mathbf{Z}$, then $f = g$.

To specify a function $f : S \to T$, one needs a way of knowing what $f(x)$ is for each $x \in S$. The most familiar examples occur when S is a set of numbers or vectors, and f is given by a formula. For example:

$$f : \mathbf{R} \to \mathbf{R}, \quad f(x) = 3x^2 - x \cos 2x,$$

or

$$g : \mathbf{R}^3 \to \mathbf{R}^2, \quad g((x, y, z)) = (x - 2y, y + 3z).$$

Even when the domain and the codomain are sets of numbers, a function need not be given by a nice arithmetic formula as above. For example, let $f : \mathbf{N} \to \{0, 1, 2\}$ be defined by the rule: $f(n) =$ the

remainder upon division of n by 3. This defines f completely and without ambiguity. One can be more explicit:

$$f(n) = \begin{cases} 0, & \text{if } n/3 \text{ is an integer;} \\ 1, & \text{if } (n-1)/3 \text{ is an integer;} \\ 2, & \text{if } (n-2)/3 \text{ is an integer.} \end{cases}$$

(One can obtain a more compact description of this f using the *greatest integer function*: $\lfloor n \rfloor$ = the largest integer less than or equal to n. Then

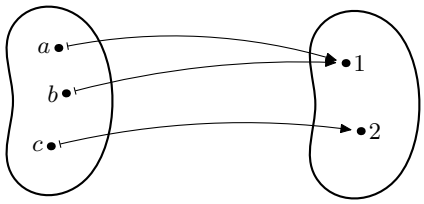
$$f(n) = n - \lfloor \frac{n}{3} \rfloor$$

for any integer n.)

The most explicit way to specify a function is to give a complete list of its values — this is only do-able when the domain is a finite set, and only practical when the domain is small. For example, we can define $f : \{a, b, c\} \to \{1, 2\}$ using a table:

x	a	b	c
$f(x)$	1	2	3

or some sort of diagram,



or by the subset of pairs

$$\{(s, f(s)) \,|\, s \in S\} = \{(a, 1), (b, 1), (c, 2)\} \subset \{a, b, c\} \times \{1, 2\}.$$

Given $f : S \to T$ and $x \in S$, we say that $y \in T$ is the *image* of x if $f(x) = y$. Each element of the domain has an image, and the collection of all such images is called the *image of* f (or sometimes, the *range*):

$$\text{Im}(f) = \{f(x) \,|\, x \in S\} \subset T.$$

In general, the image of f need not be all of the codomain T, and it is possible in general for a given $y \in T$ to be the image of many different x's in S.

A function f is said to be *surjective* or *onto* if the image of f is all of the codomain T. To prove that a given f=20 is surjective, one must take each $t \in T$ and find some $s \in S$ so that $f(s) = t$. To show f is not surjective one usually finds a particular t for which they can prove that the equation $f(x) = t$ has no solution $x \in S$. For example, let $f : \mathbf{R} \to \mathbf{R}$ be given by the formula $f(x) = x^2$. This f is not surjective: the image of f is precisely the non-negative real numbers — in particular, there does not exist an $x \in \mathbf{R}$ such that $f(x) = -1$. On the other hand, the function $g : \mathbf{R} \to \mathbf{R}$ given by $g(x) = 2x - 3$ is surjective: one can check that given any $t \in \mathbf{R}$, the equations $g(x) = t$ is solvable by letting $x = (t + 3)/2$.

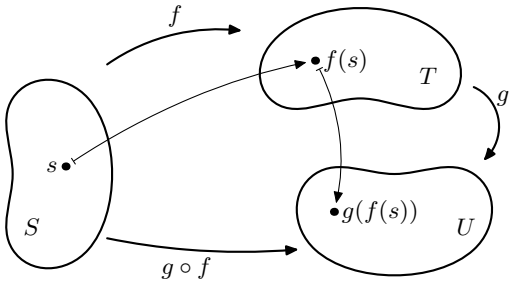
A function $f : S \to T$ is said to be *injective* or = *one-to-one* if any $t \in T$ which is in $\text{Im}(f)$ is the image of exactly one $s \in S$. To prove that a given function is injective, one typically supposes that for two elements $s_1, s_2 \in S$, one has $f(s_1) = f(s_2)$ — then uses the properties of f to show this implies $s_1 = s_2$. For example, $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$ is not injective since $f(1) = f(-1)$. On the other hand, $g : \mathbf{R} \to \mathbf{R}$, given by $g(x) = 2x - 3$ is injective: the equation $g(s_1) = g(s_2)$ will reduce to $s_1 = s_2$.

Exercise. How many functions $f : \{1, 2, 3\} \to \{a, b\}$ are there? How many such functions can be injective? How many can be surjective? What generalizations can you make?

A function $f : S \to T$ which is both injective and surjective possesses an *inverse function* $f^{-1} : T \to S$, defined as follows. Given a particular $t \in T$, we know that since f is surjective, there is an $s \in S$ so that $f(s) = t$; furthermore, since f is injective, there is only one such s, and so defining $f^{-1}(t) = s$ makes sense. It's easy to check that f^{-1} is injective and surjective.

Suppose now that $f : S \to T$ and $g : T \to U$ are two given functions. Given an $s \in S$, we have $f(s) \in T$, and so $g(f(s)) \in U$ makes sense. We can thus define a new function, called the *composition of f and g*:

$$g \circ f : S \to U, \quad g \circ f(s) = g(f(s)).$$



In general $f \circ g$ won't make sense.

Exercise. What condition on T would give sense to $f \circ g$?

Composition of functions is an *associative* operation: if $f : S \to T$, $g : T \to U$, and $h : U \to V$, then both $(h \circ g) \circ f$ and $h \circ (g \circ f)$ make sense as functions from S to V. In fact, they are the same function, as the follow computation shows (watch the parentheses carefully!):

$$((h \circ g) \circ f)(s) = (h \circ g)(f(s)) = h(g(f(s)));$$

$$(h \circ (g \circ f))(s) = h((g \circ f)(s)) = h(g(f(s)))$$

1.7 **Binary Operations**.

A *binary operation* on a set S is a rule which tells one how to

combine two elements of S and get an element of S — thus one can think of a binary operation as a function $F : S \times S \to S$. Ordinarily we will use 'infix' notation to emphasize that we are working with an operation on a set. For example, additon is a binary operation on the integers $\mathbf{Z}$, and to add the integers 6 and 7 we write $6 + 7$ instead of $+(6, 7)$. Multiplication is also a binary operation on $\mathbf{Z}$, and one most properly writes 6×7 — but often the multiplication symbol is dropped, as in $(6)(7)$. Subtraction is also a binary operation on $\mathbf{Z}$, but division is not: $3 \div 4$ is not in $\mathbf{Z}$, and $3 \div 0$ doesn't make any sense at all.

Specifying a binary operation $\star$ on a set S amounts to specifying the corresponding function $S \times S \xrightarrow{\star} S$. This can sometimes be done using explicit formulas. For example, we can define an operation $\star$ on the set $\mathbf{Z}$ by the rule

$$m \star n = mn - 2m - n + 1,$$

where the right hand side of this equation is computed using ordinary arithmetic in the integers (so that $3 \star 4 = 3$).

If the set S is small enough, one can use a table to represent a binary operation $\star$. For example, let $S = \{a, b, c\}$ and consider the following table:

$\star$	a	b	c
a	b	c	b
b	a	b	b
c	a	a	c

One reads off the value of $a \star c$ by finding the entry in the a'th row and the c'th column (so that $a \star c = b$).

Note that in this example $a \star c \neq c \star a$: the operation $\star$ is not *commutative*. An operation $*$ is said to be commutative on or *abelian* on a set S if $x * y = y * x$ for all $x, y \in S$. For example, usual addition $(+)$ is commutative (on $\mathbf{Z}$ or $\mathbf{R}$), but subtraction $(-)$ is not commutative, since (for example) $1 - 2 \neq 2 - 1$.

A binary operation $*$ on a set S is said to be *associative* if, for any $x, y, z \in S$, $x * (y * z) = (x * y) * z$. Thus when $*$ is associative, the expression $x * y * z$ makes sense without parentheses. Usual addition and multiplication are associative operations; subtraction is not. The operation $\star$ defined by the table above is not associative, since (for example)

$$a \star (a \star c) = a \star b = c \quad (a \star a) \star c = b \star b = b.$$

Exercise. How can one see easily from the operation table whether or not the operation is abelian?

Exercise. How many binary operations are possible on the set $\{a, b\}$? How many of these operations are commutative?

Exercise. Let $S = \{a, b\}$, and let $\mathcal{F} = \{f : S \to S\}$ be the set of all functions from S to itself. Define the binary operation $\circ$ on $\mathcal{F}$ to be composition of functions. Write out the operation table.

Exercise. Let $S = \{a, b\}$ and let $\mathcal{P} = \mathcal{P}(S)$ be the power set of S. Determine the table for the operation on $\mathcal{P}$ given by $\cup$ (union).