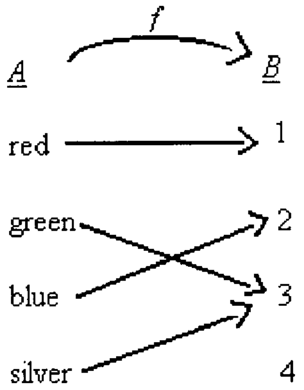
Functions and the Symmetric Groups

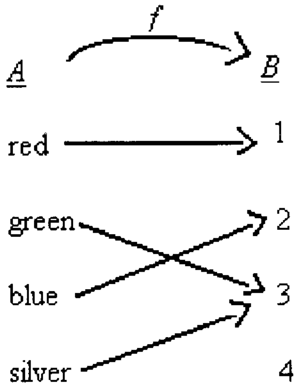
Functions, much like relations, are sets of ordered pairs. Unlike relations, the ordered pairs that constitute a function can have first coordinates from one set and second coordinates from a different set. To add precision, let's give a definition of a function. Let A and B be sets. A function is a set of ordered pairs (x, y) such that $x \in A$ and $y \in B$ with the property that for every particular value that appears in the first coordinate there corresponds one and only one particular second coordinate. For example, let $A = \{$red, green, blue$\}$ and let $B = \{1, 2\}$. The collection of ordered pairs $\{$ (red, 1), (green,1), (blue,2), (green,2)$\}$ is not a function since the particular first coordinate "green" has two different associated second coordinates. We will use the notation $f : A \rightarrow B$ to mean "f is a function whose first coordinates are from set A and whose second coordinates come from set B. A shorter way to interpret this symbol is "f takes A to B". We will also use diagrams such as the following when sets A and B are finite:



This diagram indicates that the function f is the set: $\{$(red,1), (green,3), (blue,2), (silver,3)$\}$. To further refine our vocabulary, we will say that 2 is the image of blue. Notice that we can use the definite article "the" since f is a function (blue can not have any other image). Also, we will say that silver is a pre-image 3. Notice that we can't use the definite article in the preceding sentence since 3 has another pre-image. The set of all pre-images of a function is called the domain of the function. In the above example, the domain of f is the entire set A. The set of all images of a function is called the range of the function. In the above example, the range of f is $\{1,2,3\}$ which is a proper subset of B.

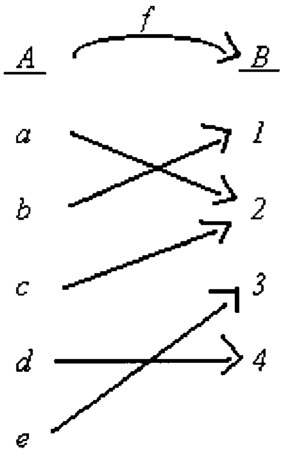
As another example of these terms let f: reals $\rightarrow$ reals be defined by $f(x) = \frac{1}{x^2}$. The domain of f is the set of all real numbers except 0. The range of f is the set of positive reals. The image of 2 is $\frac{1}{4}$. A pre-image of $\frac{1}{9}$ is 3. Another pre-image of $\frac{1}{9}$ is -3.

A function $f : A \to B$ is said to be surjective (or "onto") iff every element in set B has at least one pre-image. Our example:



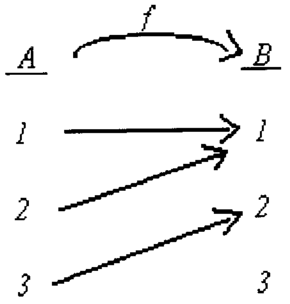
is not a surjective function. 4 has no pre-image. The function f : reals → reals given by $f(x) = x^2$ is also not surjective since -9 has no pre-image (i.e. the equation $x^2 = -9$ has no solution in the real number system). The function f : reals → reals given by $f(x) = x^3$ is surjective. Every real number a has a pre-image because the equation $x^3 = a$ is satisfied by $x = \sqrt[3]{a}$. You should compare the graphs of $y = x^2$ and $y = x^3$.

A function $f : A \to B$ is said to be injective (or one-to-one) iff every image has one and only one pre-image. Consider the following:

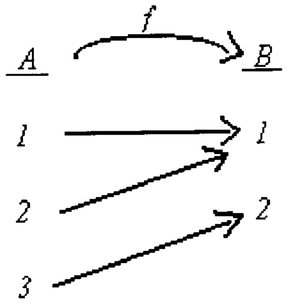


This function is not injective since the image value 2 has two pre-images, a and c. The function f : reals → reals given by $f(x) = x^2$ is not injective. The image value 4 possesses both 2 and -2 as pre-images. The function f : reals → reals given by $f(x) = x^3$ is injective. For each image value a, its only pre-image is $\sqrt[3]{a}$.

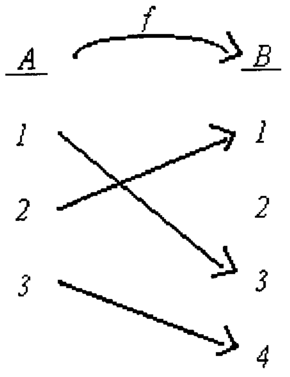
Consider the following examples:



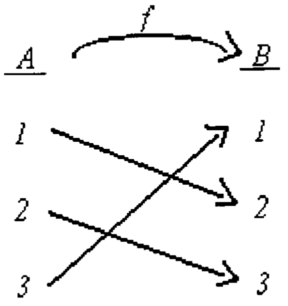
Neither injective nor surjective.



Surjective but not injective.



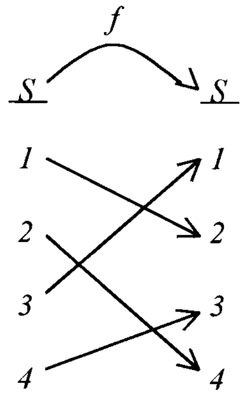
Injective but not surjective.



Both injective and surjective.
(A function which has both properties is said to be bijective.)

If f : reals → reals can be easily graphed, two simple tests exist for the properties discussed. If every horizontal line intersects the graph at least once then the function is surjective. If no horizontal line intersects the graph more than once, then the function is injective.

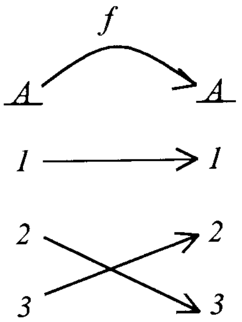
A bijective function whose domain and range is the same finite set is called a permutation. For example, let $S = \{1, 2, 3, 4\}$ and let $f : S \to S$ be defined by:



This function is a permutation of the set S. A popular way to denote this function is $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{smallmatrix}\right)$. In this notation, the domain is the first row and the range is the second. The notation implies $f(1) = 2$, $f(2) = 4$, $f(3) = 1$ and $f(4) = 3$. Normally, the first row is always given its natural order from the smallest integer to the largest integer. How many permutations are there of the set $\{1, 2, 3, 4\}$? We know $f(1)$ can be any of the four elements in S. Once 1 is linked to a specific member of S, $f(2)$ can be any of the remaining three elements. Similar logic can be used to deduce that there will be two choices for $f(3)$ and only one choice for $f(4)$. Therefore there are 4! permutations of S (or any other four element set). In fact, if a set contains n elements then there are $n!$ permutations of that set. We will return to the topic of permutations after a brief departure.

In Calculus you examined composite functions. The function $h(x) = cos(ln\, x)$ is an example of a composite function. If $f(x) = cos\, x$ and $g(x) = ln\, x$, then $h(x) = f\big(g(x)\big)$. Given a particular value for x, how do we compute $f\big(g(x)\big)$? Suppose we wish to compute $f\big(g(4)\big)$ or, equivalently, $h(4)$. As you know from prior mathematics courses, $g(4) = ln\, 4$ must be computed first. $ln\, 4$ is approximately 1.3863. As a result, $f\big(g(4)\big)$ becomes $f(1.3863) = cos(1.3863)$ which is approximately .1835. Notice that there are two distinct transitions: $4 \to 1.3863 \to .1835$. Notice also that for 4 to be in the domain of $h(x)$ it is not sufficient for 4 to be in the domain of $g(x)$. Additionally, the image of 4 with respect to the g function must be in the domain of the f function. You should realize that the way we compute composite functions is to begin with the function denoted on the right. In other words, to compute $f\big(g(x)\big)$ for a particular choice of x, we must begin with the g function.

The symbol S_3 stands for the set of all permutations on a set with three elements endowed with a binary operation that students sometimes find confusing. S_3 is called the symmetric group on three symbols. First, let's construct the elements of S_3 and find convenient names for them. As we pointed out earlier, S_3 must have $3! = 6$ elements. If these permutations are used on the particular set $A = \{1, 2, 3\}$, they can be written $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ and $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$. Recall that $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, for example, is symbolic for:



This notation is unwieldy in any context but particularly so when creating a group table. We will use an alternative notation called "cycle" notation. Cycle notation plays a large role later in this text. Consider again $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$. We will rename this function (23). Notice that we don't use a comma between the elements. Cycle notation is read left to right until you arrive at the last element. At that point, you "recycle" and take the last element back to the first element. Therefore, (23) can be read: "2 is taken to 3 by this function" and "3 is taken to 2 by this function". What about 1? In cycle notation, an unused element is assumed to have itself as its image. What could (132) mean? It means: "1 is taken to 3 and 3 is taken to 2 and 2 is taken to 1". That's the same as our $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$. How can we name $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ in this notation? We will name it e. A full renaming of the elements in S_3 is:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e$$

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (12)$$

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (13)$$

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (23)$$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (123)$$

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (132)$$

How do we induce a binary operation on this set? We use composition of functions in the same way it is used in Calculus! Let's try to compute $(23)\bigstar(13)$. Let's call the resulting function f. What is $f(1)$? As we reviewed earlier, the function on the right, namely (13), must be applied to 1 first. This function transforms 1into 3 as the notation indicates. Then, the function on the left, namely (23), is applied to 3. 3 is transformed into 2. Therefore, this two-step procedure results in $f(1) = 2$. Similarly, $f(2) = 3$ and $f(3) = 1$. $\therefore$ $(23)\bigstar(13) = \begin{pmatrix}1\,2\,3\\2\,3\,1\end{pmatrix} = (123)$

Let's try one more example of composition.

$$[(13)\bigstar(12\,3)](1) = 2[1 \to 2 \to 2]$$
$$[(13)\bigstar(123)](2) = 1[2 \to 3 \to 1]$$
$$[(13)\bigstar(123)](3) = 3[3 \to 1 \to 3]$$
$$\therefore\ (13)\bigstar(123) = \begin{pmatrix}1\,2\,3\\2\,1\,3\end{pmatrix} = (12)$$

Using this operator, we can complete the following table for S_3:

S_3	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)

This table is clearly closed and e acts as an identity. You should check that every element possesses an inverse. There would by $6^3 = 216$ equations to check in order to be satisfied that this operation is associative. This table represents a group!

Notation is even trickier for S_4 and other symmetric groups. Does (13)(24) represent $\begin{pmatrix}1\,2\,3\,4\\3\,2\,1\,4\end{pmatrix}\bigstar\begin{pmatrix}1\,2\,3\,4\\1\,4\,3\,2\end{pmatrix}$ or does (13)(24) represent the single function $\begin{pmatrix}1\,2\,3\,4\\3\,4\,1\,2\end{pmatrix}$? It turns out that both are possible since they are equal in S_4. S_4 has 24 elements and some of them, like $\begin{pmatrix}1\,2\,3\,4\\3\,4\,1\,2\end{pmatrix}$, can not be represented as a single cycle. You should make a card for S_3. You should try to name all 24 elements in S_4. Creating an S_4 table might be very instructive. S_4 is named the symmetric group on 4 symbols. For each n, there exists a group S_n. $o(S_n) = n!\ \forall n$.