$$[0] = \{b \in \mathbb{Z} \mid b^2 \equiv 0 (\mathrm{mod}\, 5)\} = \{5k \mid k \in \mathbb{Z}\} = A_1$$
$$[1] = \{b \in \mathbb{Z} \mid b^2 \equiv 1 (\mathrm{mod}\, 5)\} = \{5k+1 \mid k \in \mathbb{Z}\} \cup \{5k+4 \mid k \in \mathbb{Z}\} = A_2$$
$$[2] = \{b \in \mathbb{Z} \mid b^2 \equiv 4 (\mathrm{mod}\, 5)\} = \{5k+2 \mid k \in \mathbb{Z}\} \cup \{5k+3 \mid k \in \mathbb{Z}\} = A_3.$$

Hence $\{A_1, A_2, A_3\}$ is the corresponding partition of $\mathbb{Z}$.

Exercises

1. Determine whether the statement is true or false in each of the following cases:
   (i) $60 \equiv -3 (\mathrm{mod}\, 7)$ (ii) $50 \equiv 13 (\mathrm{mod}\, 8)$
   (iii) $8^4 \equiv 2 (\mathrm{mod}\, 13)$ (iv) $3^4 \equiv 1 (\mathrm{mod}\, 5)$
   (v) $6 + 5^2 \equiv 3 + 2 (\mathrm{mod}\, 2)$
2. What is the remainder when $6 \cdot 7^{32} + 7 \cdot 9^{45}$ is divided by 4?
3. Find the remainder when 7^{30} is divided by 4.
4. What is the remainder when $1! + 2! + 3! + \ldots + 50!$ is divided by 16 ?
5. What is the remainder when 4^{119} is divided by 9?

1.4 Functions

As we have already pointed out, the concept of function is of paramount importance in mathematics. Among many other reasons, it helps us to study the relationship between various algebraic structures. To put it in a somewhat naive manner, a function is a rule of correspondence between the elements of two sets. From the literature of mathematics, one may find that the term *function* was first coined around 1694 by the famous German mathematician Leibnitz (1646-1716), in context with the slope of a curve. Later in 1749, Swiss mathematician Euler (1707-1783) defined a function simply as a law governing the interdependence of variable quantities and made extensive use of it. However the present day conception of function is attributed to Dirichlet (1805-1859), who in 1837 proposed the definition of a function as a *rule of correspondence that assigns a unique value of the dependent variable to every permitted value of an independent variable*". We shall shortly see that this idea, in essence, lies at the core of the formal definition of a function.

Given two sets A and B, a *function* (or, *mapping*) f from A to B (written as $f : A \to B$) assigns to each $a \in A$ exactly one $b \in B$; here b is called the value of the function at a or the *image* of a under f, whereas a is called the *preimage* of b

under f and we denote this state of affairs by the notation $f(a) = b$. More formally, a function from A to B may be defined as a particular type of relation as follows:

Definition 1.4.1. For two nonempty sets A and B, a relation f from A into B is called a ***function*** from A into B if

(i) domain of $f = A$ and

(ii) f is *well-defined* (or, *single valued*) in the sense that for all $(a, b), (a', b') \in f$, $a = a'$ implies that $b = b'$, i.e.,

$$a = a' \Longrightarrow f(a) = f(a').$$

If we examine this definition closely, we see that, in order to show that a relation f from A into B is a function, we must prove that the domain of f is A, which means that every element of A has some image in B and further we have to show that f is well-defined, i.e., a single element of A cannot have more than one image in B. Combining these two, we see that $f \subseteq A \times B$ such that for all $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

Remark 1.4.2. Corresponding to every function $f : A \to B$, if we look at the relation from A into B, given by $G(f) = \{(a, f(a)) \mid a \in A\}$, called the *graph* of the function f, it can be easily seen that *every element of A is the first component of one and only one ordered pair in $G(f)$*. In particular, if we take $f : \mathbb{R} \to \mathbb{R}$, then $G(f)$, being a subset of $\mathbb{R} \times \mathbb{R}$, i.e., the Euclidean plane, can be pictorially represented and in usual terminology this representation is called the 'graph of f'. Note that in such a figure, the geometric interpretation of the above character (in italics) of a function is precisely that *each vertical line must intersect the graph (i.e., the diagram) in exactly one point.*

Further, it is worth pointing out, though of pure logical interest, that Definition 1.4.1 enables us to define functions with an empty domain also. Indeed, if $A = \emptyset$ then $\emptyset \times B = \emptyset$, which is clearly a subset of $\emptyset \times B$ and the well-definedness of this function is vacuously satisfied. We however, in the sequel, shall continue to consider functions on nonempty domains only.

For a function $f : A \to B$, the set A is referred to as the ***domain*** of the function and it is denoted by $\mathcal{D}(f)$, whereas the set B is called the ***codomain*** of f. The set $f(A) = \{f(x) : x \in A\}$ is naturally a subset of the codomain B. Some authors prefer to call the set $f(A)$ as the ***range*** of the function f and denote it by $Im(f)$.

Let us now give examples of relations, some of which are functions and some others which are not.

Example 1.4.3. (i) Let A denote the set of names of all those countries that qualified to the finals of the FIFA World Cup Football, Korea-Japan 2002, and B denote the set of names of all the football players of those countries enrolled for this event. Let us define a relation f by associating with each country in A, the name of the captain of its football team from B. Then clearly, $f \subseteq A \times B$ and since every country in A has one (and only one) captain of its football team, so $\mathcal{D}(f) = A$ and f is well-defined. Hence f is a function from A to B.

(ii) Let f be the subset of $\mathbb{Z} \times \mathbb{Z}$ defined by $f = \{(n, 4n-5) : n \in \mathbb{Z}\}$. Then $\mathcal{D}(f) = \{n : n \in \mathbb{Z}\} = \mathbb{Z}$. To show that f is well-defined, let $n = m$ for some $n, m \in \mathbb{Z}$. Then $4n - 5 = 4m - 5$, whence $f(n) = f(m)$ and hence f is well-defined. Consequently, f is a function from $\mathbb{Z}$ to $\mathbb{Z}$.

(iii) Let f be the subset of $\mathbb{Q} \times \mathbb{Z}$ given by $f = \left\{\left(\frac{p}{q}, p+q\right) : p, q \in \mathbb{Z}, q \neq 0\right\}$. Observe that $\mathcal{D}(f) = \left\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\right\} = \mathbb{Q}$. However, f is not well-defined. Indeed, we have $\frac{3}{5} = \frac{9}{15} \in \mathbb{Q}$ and $(\frac{3}{5}, 8), (\frac{9}{15}, 24) \in f$. But, $f(\frac{3}{5}) = 8 \neq 24 = f(\frac{9}{15})$ justifies our claim. Hence f is not a function from $\mathbb{Q}$ to $\mathbb{Z}$.

(iv) Let $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$ and f be a relation from A into B, given by $f = \{(a, 1), (b, 3), (c, 2)\}$. Note that here $\mathcal{D}(f) = \{a, b, c\} \subset A$ and consequently f is not a function from A to B.

Definition 1.4.4. A function $f : A \to A$ is said to be the ***identity function (identity mapping)*** if $f(x) = x$ for all $x \in A$. This function is usually denoted by ι_A.

Definition 1.4.5. A function $f : A \to B$ is said to be a ***constant function*** if $f(A)$ is a singleton subset of B, i.e., under a constant function, every element of the domain set goes to some fixed element in B.

For example, $f : \mathbb{Z} \to \mathbb{Z}$, defined by $f(x) = 0$ for all $x \in \mathbb{Z}$ is a constant function, where $Im(f) = \{0\}$.

Let us now develop the concept of *equality of two functions*. Let $f : X \to Y$ and $g : X \to Y$ be two functions. Clearly, $f, g \subseteq X \times Y$. Suppose $f = g$. Let x be any element of X. Then, $(x, f(x)) \in f = g$ and $(x, g(x)) \in g$. Since g is a function, every element of X can appear once and only once in the first component of the ordered

pairs in g, whence due to its well-definedness, we must have $f(x) = g(x)$. Conversely, assume that $f(x) = g(x)$ for all $x \in X$. Let $(x, y) \in f$. Then $y = f(x) = g(x)$ gives $(x, y) \in g$, whence $f \subseteq g$. In an essentially similar manner, one can show that $g \subseteq f$. Hence it follows that $f = g$. Thus we conclude that two functions $f : X \to Y$ and $g : X \to Y$ are ***equal*** if and only if $f(x) = g(x)$ for all $x \in X$.

For example, let $f : \mathbb{R}^+ \to \mathbb{R}$ be given by $f(x) = 1 + \frac{x}{|x|}$ and $g : \mathbb{R}^+ \to \mathbb{R}$ be given by $g(x) = 2$; then $f = g$.

Definition 1.4.6. Let us consider a function $f : A \to B$. Then,

(a) f is called ***injective*** (or, ***one-one***,)[21] when for all $a_1, a_2 \in A$ if

$$a_1 \neq a_2 \Longrightarrow f(a_1) \neq f(a_2)$$

(i.e., distinct elements of the domain are mapped to distinct images).

(b) f is called ***surjective***[22] (or, ***onto***) if $Im(f) = B$,

(i.e., for every $b \in B$ there exists at least one $a \in A$ such that $f(a) = b$).

(c) f is called ***bijective*** if f is both surjective and injective.

In this case it is often said that there is a ***one-to-one correspondence*** between the elements of the sets A and B.

Remark 1.4.7. A logically equivalent[23] definition of an injective function is as follows: *A function $f : A \to B$ is said to be injective when $f(a_1) = f(a_2)$ in B implies that $a_1 = a_2$ in A, for all $a_1, a_2 \in A$.*

Now let us have a closer look at different types of functions in terms of various examples. Note that there can be functions which are neither injective nor surjective, as we shall show in the following list of examples:

Example 1.4.8. (i) Consider the relation f on $\mathbb{Z}$ defined by $f(n) = |n|$ for all $n \in \mathbb{Z}$. It is easy to see that $\mathcal{D}(f) = \mathbb{Z}$ and f is well-defined. So f is a function. Here $f(2) = |2| = 2 = |-2| = f(-2)$ but $2 \neq -2$. This implies that f is *not*

[21] Some authors prefer to call it ***one-to-one***.

[22] The word "sur" in French means "on".

[23] Note that, A statement of the form "`if 'p' holds then 'q' holds`" is logically equivalent to "`if 'q' does not hold then 'p' does not hold`", and is **not** logically equivalent to "*if 'p' does not hold then 'q' does not hold*". Let us try to explain its significance in terms of a nonmathematical statement. Try to appreciate that your statement like *if it rains then I shall not attend the lecture*, will not be binding on you in case it does not rain, but in the event of your attending the lecture it may be logically concluded that it is not raining.

injective. Since for all $n \in \mathbb{Z}$, $f(n)$ is a nonnegative integer, we see that the negative integers in $\mathbb{Z}$ have no preimage under f, whence f is *not surjective*. Note that, here $f(\mathbb{Z}) = \mathbb{N}_0$. Observe that if we consider $f_1 : \mathbb{Z} \to \mathbb{N}_0$ by stipulating $f_1(n) = |n|$ for all $n \in \mathbb{Z}$, then f_1 becomes a *surjective (onto)* function but *not injective.*

(ii) Refer to Example 1.4.3(ii). Here $f(n) = 4n - 5$ for all $n \in \mathbb{Z}$. Let $n_1, n_2 \in \mathbb{Z}$ and suppose that $f(n_1) = f(n_2)$. Then, $4n_1 - 5 = 4n_2 - 5$, i.e., $n_1 = n_2$. Hence f is an *injective* (*one-one*) function. But f is *not surjective* (*onto*). Indeed, here $10 \in \mathbb{Z}$ has no preimage under f. For otherwise, if $f(n) = 10$ for some $n \in \mathbb{Z}$, it would lead to $4n - 5 = 10$, i.e., $n = \frac{15}{4} \in \mathbb{Z}$, which is impossible.

Observe that, if we consider $f_1 : \mathbb{R} \to \mathbb{R}$ by defining $f_1(x) = 4x - 5$ for all $x \in \mathbb{R}$, then f_1 becomes an example of a function which is both *surjective* and *injective*, and consequently a *bijective* function.

Remark 1.4.9. In particular, if we consider functions from $\mathbb{R} \to \mathbb{R}$, then surjectivity and injectivity of these functions have some interesting geometrical features with reference to their graph, which can be plotted in the Euclidean plane $\mathbb{R} \times \mathbb{R}$.

If $f : \mathbb{R} \to \mathbb{R}$ is an *injective* function, then each horizontal line in $\mathbb{R} \times \mathbb{R}$ can intersect the graph of f in *at most one point*; whereas if f is a *surjective* function, then each horizontal line in $\mathbb{R} \times \mathbb{R}$ must intersect the graph of f in *at least one point.* Finally, if f is *bijective* then each horizontal line must intersect the graph of f in *exactly one point.*

For example, let us consider the graphs of the following functions from $\mathbb{R}$ to $\mathbb{R}$ given by $f(x) = \sqrt[3]{x^2}, g(x) = 2^x, h(x) = x^3 + 3|x|$ and $k(x) = x^3$ (as in Figs. 6a, b, c, d).

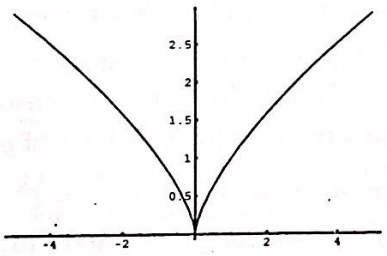


Fig.6a : $f(x) = \sqrt[3]{x^2}$

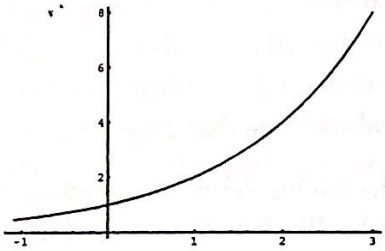


Fig.6b : $g(x) = 2^x$

Applying the above mentioned characteristics, it can be verified that the function f is neither injective nor surjective; the function g is injective but not surjective; the

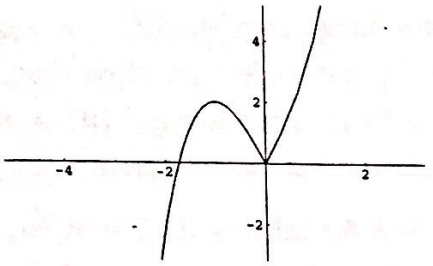


Fig.6c : $h(x) = x^3 + 3|x|$

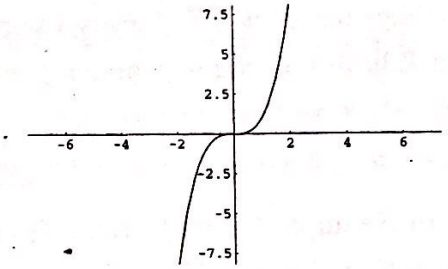
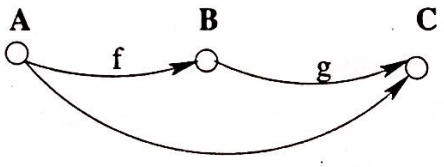


Fig.6d : $k(x) = x^3$

function h is not injective though surjective; finally, the function k is both injective and surjective and hence bijective.

Definition 1.4.10. Let us consider functions $f : A \to B$ and $g : B \to C$. The ***composition***, $\circ$ of f and g, written $g \circ f$ is the relation from A into C defined as $g \circ f = \Big\{(a, c) : a \in A, c \in C$ and there exists $b \in B$ such that $f(a) = b$ and $g(b) = c\Big\}$(*Fig.7*). Note that $Im\,(f) \subseteq \mathcal{D}(g)$.



g o f

Fig. 7

Let $(g \circ f)(a) = c$. Now, since $c = g(b)$ and $b = f(a)$ for some $b \in B$, we combine them to get $c = g(b) = g\Big(f(a)\Big)$, whence we have $(g \circ f)(a) = g\Big(f(a)\Big)$. We assert that $g \circ f$ is a function from A to C. Towards proving this, first we have to show that $\mathcal{D}(g \circ f) = A$. Let $a \in A$. Now as f is a function from A to B, there exists $b \in B$ such that $f(a) = b$. Again, g is a function from B to C so that there exists $c \in C$ such that $g(b) = c$. Hence, $(g \circ f)(a) = g\Big(f(a)\Big) = g(b) = c$, i.e., $(a, c) \in g \circ f$, whence $a \in \mathcal{D}(g \circ f)$. This proves that $A \subseteq \mathcal{D}(g \circ f)$. As the reverse inclusion is obvious, we conclude that $\mathcal{D}(g \circ f) = A$. Now we justify the well-definedness of $g \circ f$.

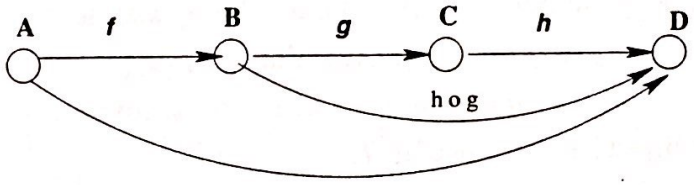
Let $(a_1, c_1), (a_2, c_2) \in g \circ f$ and $a_1 = a_2$ where $a_1, a_2 \in A$ and $c_1, c_2 \in C$. By Definition 1.4.10, there exist $b_1, b_2 \in B$ such that $f(a_1) = b_1, g(b_1) = c_1$ and $f(a_2) = b_2, g(b_2) = c_2$. As f is well-defined and $a_1 = a_2$, we have $b_1 = f(a_1) = f(a_2) = b_2$ and as g is well-defined, we arrive at $c_1 = g(b_1) = g(b_2) = c_2$. Thus $g \circ f$ is well-defined. Consequently, $g \circ f$ is a function from A to C.

Example 1.4.11. Consider the functions $f : \mathbb{Z} \to \mathbb{Q}$ and $g : \mathbb{Q} \to \mathbb{Q}$, given

by $f(x) = \frac{1}{3}x$ for all $x \in \mathbb{Z}$ and $g(x) = x^3$ for all $x \in \mathbb{Q}$. Observe that, here $g \circ f : \mathbb{Z} \to \mathbb{Q}$ is given by $(g \circ f)(x) = g\Big(f(x)\Big) = g\Big(\frac{x}{3}\Big) = \frac{x^3}{27}$ for all $x \in \mathbb{Z}$. But $f \circ g$ is not defined here, as for $\frac{1}{3} \in \mathbb{Q}$, $g(\frac{1}{3}) = \frac{1}{27} \notin \mathbb{Z}$ and hence $f\Big(\frac{1}{27}\Big)$ makes no sense.

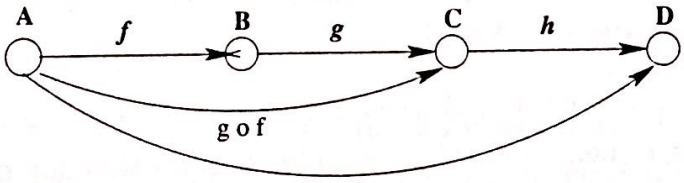
Example 1.4.12. Consider the functions $f : \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$, defined by $f(n) = (-1)^n, n \in \mathbb{Z}$ and $g(n) = 2n, n \in \mathbb{Z}$. Then, $g \circ f : \mathbb{Z} \to \mathbb{Z}$ is given by $(g \circ f)(n) = g\Big(f(n)\Big) = g\Big((-1)^n\Big) = 2(-1)^n$, $n \in \mathbb{Z}$, i.e., $(g \circ f)(n) = 2$ or -2, according as n is even or odd integer. Observe that, here one may define $f \circ g : \mathbb{Z} \to \mathbb{Z}$ by $(f \circ g)(n) = f\Big(g(n)\Big) = f(2n) = (-1)^{2n}$, $n \in \mathbb{Z}$, i.e., $(f \circ g)(n) = 1$ for all $n \in \mathbb{Z}$. This example shows that $g \circ f \neq f \circ g$, in general, even when both are defined; i.e., *composition of functions is noncommutative.*

Let us now discuss some important properties of the composition of functions. Watch the following diagram (Figs. 8a and b) carefully:



(h o g) o f

Fig. 8a



h o (g o f)

Fig. 8b

In fact, we have the following theorem:

Theorem 1.4.13. *Let $f : A \to B$, $g : B \to C$ and $h : C \to D$. Then $h \circ (g \circ f) = (h \circ g) \circ f$, i.e., composition of functions is associative, provided the requisite compositions make sense.*

Proof. Observe that $h \circ (g \circ f) : A \to D$ and $(h \circ g) \circ f : A \to D$. Let $x \in A$. Then $\Big[h \circ (g \circ f)\Big](x) = h\Big((g \circ f)(x)\Big) = h\Big(g(f(x))\Big) = (h \circ g)\Big(f(x)\Big) = \Big[(h \circ g) \circ f\Big](x)$. Since x is any element of A, we conclude that $h \circ (g \circ f) = (h \circ g) \circ f$. □

Theorem 1.4.14. *Suppose that $f : A \to B$ and $g : B \to C$. Then,*

(i) if f and g are both injective, then $g \circ f$ is also so;

(ii) if $g \circ f$ is injective, then f is injective;

(iii) if f and g are both surjective, then $g \circ f$ is also so;

(iv) if $g \circ f$ is surjective, then g is surjective;

(v) if f and g are both bijective, then $g \circ f$ is also so;

(vi) if $g \circ f$ is bijective, then f is injective and g is surjective.

Proof. (i) Let $a, a' \in A$. Suppose that $(g \circ f)(a) = (g \circ f)(a')$. Then, $g\Big(f(a)\Big) = g\Big(f(a')\Big)$ implies that $f(a) = f(a')$, since g is injective. Again, as f is injective, we conclude that $a = a'$. Hence $g \circ f$ is injective.

(ii) If possible, let f be not injective. Then, there exist some $a_1, a_2 \in A$ such that $a_1 \neq a_2$ but $f(a_1) = f(a_2)$. This implies that $g\Big(f(a_1)\Big) = g\Big(f(a_2)\Big)$ as g is well-defined, i.e., $(g \circ f)(a_1) = (g \circ f)(a_2)$ — which contradicts the injectivity of $g \circ f$. Hence if $g \circ f$ is injective, so must be f.

(iii) Let $c \in C$. Then there exists $b \in B$ such that $g(b) = c$ (as g is surjective). Again, as f is also surjective, there exists $a \in A$ such that $f(a) = b$. Thus, $(g \circ f)(a) = g\Big(f(a)\Big) = g(b) = c$. Hence $g \circ f$ is a surjective function.

(iv) Let $c \in C$. Since $g \circ f : A \to C$ is surjective, there exists some $a \in A$ such that $(g \circ f)(a) = c$, i.e., $g\Big(f(a)\Big) = c$. This implies that for $c \in C$, there exists $f(a) \in B$ such that $f(a)$ is a preimage of c in B under g. Since c is an arbitrary element of C, we conclude that g is surjective.

(v) This follows as an immediate consequence of part (i) and (iii) put together.

(vi) Follows from (ii) and (iv). □

Recall the identity function as given in Definition 1.4.4. We leave it to the reader to verify that this function is bijective; furthermore, if $f : A \to B$ be any function and $\iota_A : A \to A$ and $\iota_B : B \to B$ be identity functions respectively on A and B then, $f \circ \iota_A = f = \iota_B \circ f$.

Now, for a function $f : A \to A$, let us give the following recursive definition:

$$\begin{aligned} f^0(a) &= a. \\ f^1(a) &= f(a). \\ f^{n+1}(a) &= (f \circ f^n)(a) \text{ for all } a \in A, n \in \mathbb{N}. \end{aligned}$$

It is interesting to observe that if A is a finite set and $f : A \to A$ is an injective function on A then, f is automatically surjective. Towards proving this assertion, let us first prove the following lemma:

Lemma 1.4.15. [24] *Let A be any set and $f : A \to A$ be an injective function. Then $f^n : A \to A$ is an injective function for all integers $n \geq 1$.*

Proof. If possible, let there be some integer, say $n > 1$ such that f^n is not injective. Assume further that k be the smallest such positive integer. So f^k is not injective, whence there must exist some $a, b \in A$ such that $a \neq b$ but yet $f^k(a) = f^k(b)$. But this implies that $f\left(f^{k-1}(a)\right) = f\left(f^{k-1}(b)\right)$ which in turn gives that $f^{k-1}(a) = f^{k-1}(b)$ since f is injective. By the choice of the integer k, we have that f^{k-1} is injective and hence we get $a = b$, which is a contradiction. So, our initial assumption was wrong and consequently, f^n is injective for all $n \geq 1$. □

Theorem 1.4.16. *For any finite set A, if $f : A \to A$ is injective, then f is surjective also and hence is bijective.*

Proof. Let $a \in A$. Now as $f^n : A \to A$, we have that $f^n(a) \in A$ for all $n \geq 1$. This indicates that $\{a, f(a), f^2(a) \ldots\} \subseteq A$. Since A is finite, there must exist positive integers r and s such that $r > s$ and $f^r(a) = f^s(a)$. But this means $f^s\left(f^{r-s}(a)\right) = f^s(a)$, which gives that $f^{r-s}(a) = a$, since by virtue of the Lemma 1.4.15 we have that f^s is injective. Call $a' = f^{r-s-1}(a) \in A$. Then $f(a') = f\left(f^{r-s-1}(a)\right) = f^{r-s}(a) = a$ shows that f is a surjective function and consequently a bijective function. □

Definition 1.4.17. Consider a function $f : A \to B$. Then f is called

(i) ***left invertible*** if there exists $g : B \to A$ such that, $g \circ f = \iota_A$ and then g is called a ***left inverse*** of f,

(ii) ***right invertible*** if there exists $h : B \to A$ such that, $f \circ h = \iota_B$ and then h is called a ***right inverse*** of f,

(iii) ***invertible*** if f is both left and right invertible.

[24] Though a proof of this result follows from Theorem 1.4.14(i), we prefer to give an independent proof here.

Example 1.4.18. (i) Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n + 1$ for all $n \in \mathbb{N}$ and $g : \mathbb{N} \to \mathbb{N}$ be defined by $g(1) = 1$ and $g(n) = n - 1$ for all $n(> 1) \in \mathbb{N}$. Hence $(g \circ f)(n) = g\Big(f(n)\Big) = g(n + 1) = n + 1 - 1 = n$ for all $n \in \mathbb{N}$, so that $g \circ f = \iota_{\mathbb{N}}$, whence g is a *left inverse* of f. Observe that here $(f \circ g)(1) = f\Big(g(1)\Big) = f(1) = 2$ and so $f \circ g \neq \iota_{\mathbb{N}}$ so that g *is not a right inverse of* f.

(ii) Let $f : \mathbb{Z} \to E_0^+$ be defined by $f(x) = |x| + x$ for all $x \in \mathbb{Z}$, where E_0^+ is the set of nonnegative even integers and let $g : E_0^+ \to \mathbb{Z}$ be defined by $g(x) = \frac{x}{2}$ for all $x \in E_0^+$. Then $(f \circ g)(x) = f\big(g(x)\big) = f\big(g(2n)\big)$ [as $x \in E_0^+, x = 2n$ for some nonnegative integer n] $= f(n) = |n| + n = 2n = x$. Hence g *is a right inverse of* f. Observe that, here $(g \circ f)(-1) = g\Big(f(-1)\Big) = g(0) = 0$ and hence $g \circ f \neq \iota_{\mathbb{Z}}$ so that g *is not a left inverse of* f.

(iii) Consider the function $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = 3x + 4$ for all $x \in \mathbb{R}$ and the function $g : \mathbb{R} \to \mathbb{R}$, defined by $g(x) = \frac{x-4}{3}$ for all $x \in \mathbb{R}$. It is now a routine exercise to see that here both $g \circ f = f \circ g = \iota_{\mathbb{R}}$. Hence f is invertible and g is both a left as well as right inverse of f.

The above examples establish clearly that a function may or may not have a left (right) inverse. However, example (iii) shows that left and right inverses of the function f are the same. This is not a stray incident. In fact, whenever a function f is invertible, then its right and left inverses are the same. Indeed, let $f : A \to B$ be invertible and assume further that g be a left inverse and h be a right inverse of f. Then by definition we have $g \circ f = \iota_A$ and $f \circ h = \iota_B$. Now, $g = g \circ \iota_B = g \circ (f \circ h) = (g \circ f) \circ h = \iota_A \circ h = h$. This also justifies that inverse of a function, if exists, is unique and hence it is denoted by f^{-1}. Furthermore, observe that a function $f : A \to B$ is invertible if its inverse relation f^{-1} is a function from B to A.

Now since the existence of left (right) inverse of a function is not guaranteed, it would be useful to characterize those functions that admit left (right) inverse. This is presented in the following theorem.

Theorem 1.4.19. *Let us consider* $f : A \to B$. *Then,*

(i) f *is left invertible if and only if* f *is injective,*

(ii) f *is right invertible if and only if* f *is surjective and*

(iii) f *is invertible if and only if* f *is bijective.*

Proof. (i) Suppose f is left invertible. Then there exists $g : B \to A$ such that $g \circ f = \iota_A$. Now to prove the injectivity of f, let us assume $f(a) = f(b)$ for some $a, b \in A$. Then we have, $g\big(f(a)\big) = g\big(f(b)\big)$ by well-definedness of the function g, whence $(g \circ f)(a) = (g \circ f)(b)$ and this implies that $\iota_A(a) = \iota_A(b)$, i.e., $a = b$. Thus f is injective.

Conversely, suppose f is injective. We have to show that f is left invertible. Towards this, we construct a function $g : B \to A$ which becomes the left inverse of f. Since $f : A \to B$ is injective, observe that, for any element $b \in B$, either there is no preimage in A or there exists a unique preimage, say $a_b \in A$, so that $f(a_b) = b$. Let us choose arbitrarily some element $a_0 \in A$ and fix it. We now define $g : B \to A$ by

$$\begin{aligned} g(b) &= a_0, \quad \text{if } b \text{ has no preimage under } f \\ &= a_b, \quad \text{if } a_b \text{ is the unique preimage of } b \text{ under } f, \text{ i.e., } f(a_b) = b \end{aligned}$$

for all $b \in B$. Clearly, $\mathcal{D}(g) = B$. We leave it to the reader to verify that g is well-defined. (Observe that this requires injectivity of f). We now show that $g \circ f = \iota_A$. Let $a_1 \in A$ and $f(a_1) = b_1$ for some $b_1 \in B$. Then by definition of g, $g(b_1) = a_1$. So, $(g \circ f)(a_1) = g\Big(f(a_1)\Big) = g(b_1) = a_1 = \iota_A(a_1)$. Since a_1 is any element of A, we conclude that $g \circ f = \iota_A$.

(ii) Suppose f is right invertible. Then there exists $h : B \to A$ such that $f \circ h = \iota_B$. Let $b \in B$. Then $h(b) \in A$. Suppose $h(b) = a \in A$. Then, $b = \iota_B(b) = (f \circ h)(b) = f\Big(h(b)\Big) = f(a)$. This shows that f is a surjective function.

Conversely, suppose f is surjective. Let $b \in B$. By surjectivity of f, there must exist some $a \in A$ such that $f(a) = b$. Let us consider the set of all preimages of b, say $A_b = \{a \in A : f(a) = b\}$. Then clearly $A_b \neq \emptyset$. Let us choose[25] $a_b \in A_b$ for each $b \in B$. [Note that such a choice is made arbitrarily, but once it is made, the elements chosen are fixed for the rest of the discussion.] Now, define $h_1 : B \to A$ such that $h_1(b) = a_b$ for all $b \in B$. It can be justified that h_1 is a function from B to A (though the verification of well-definedness is highly nontrivial). We assert that h_1 is the right inverse of f. Indeed, let $b \in B$; then $(f \circ h_1)(b) = f\big(h_1(b)\big) = f(a_b) = b = \iota_B(b)$ and hence $f \circ h_1 = \iota_B$ proves our claim.

(iii) It follows directly from (i) and (ii) above. □

[25] To an analytic mind, the permission of making such a 'choice' may surely pose a question. Indeed, this is done by virtue of the so called *Axiom of choice* which lies at the very foundation of the theory of sets. We introduce it in brief, in Appendix B.

Two sets A and B are said to be ***cardinally equivalent*** (or, ***equipotent***) written as $A \sim B$ if there exists a bijective function from A onto B. Note that the identity function on any set is bijective; also bijective functions are invertible and the inverse function is also bijective; furthermore, the composition of two bijective functions, when definable is bijective. In view of these facts, it follows that '$\sim$' is an equivalence relation among nonempty subsets of some universal set. If $A \sim B$, then A, B belong to the same equivalence class under '$\sim$' and we sometimes denote it by writing $|A| = |B|$. It can be easily seen that if both A and B are finite sets, then $|A| = |B|$ if and only if A and B have the same number of elements. If however A, B are infinite sets and $A \sim B$, then they are said to have the same ***cardinal number.*** We merely comment here that not all infinite sets have the same cardinal number[26] and take this opportunity to state (without proof) a classical theorem of this area, due to Schröder-Bernstein, which goes as follows:

Let A and B be two sets. If $A \sim Y$ for some subset Y of B and $B \sim X$ for some subset X of A, then $A \sim B$.

Now, let $f : A \to B$ and $A' \subseteq A$. Then the function f induces a function from A' to B in a natural way as the following definition shows:

Definition 1.4.20. Let $f : A \to B$ and $\emptyset \neq A' \subseteq A$. The ***restriction*** of f to A', written as $f\big|_{A'}$ is defined to be $f\big|_{A'} = \left\{\left(a', f(a')\right) : a' \in A'\right\}$. Observe that $f\big|_{A'}$ has actually the same rule of correspondence as f except that its domain is a subset of that of f.

Definition 1.4.21. Let $f : A \to B$ and $A \subseteq A'$. A function $g : A' \to B$ is called an ***extension*** of f to A' if $g\big|_{A} = f$.

Note that a function may have more than one extension.

Example 1.4.22. (i) Suppose $A = \{a \in \mathbb{R} : a > 0\}$. Let $f : A \to \mathbb{R}$ be given by $f(a) = \frac{|a|}{a}$; $a \in A$. Observe that, $g : \mathbb{R} \to \mathbb{R}$ defined by $g(a) = 1$, for all $a \in \mathbb{R}$, is an extension of f to $\mathbb{R}$, since $g\big|_{A} = f$.

(ii) Let $f : \mathbb{R} \to \mathbb{R}_1$ where $\mathbb{R}_1 = \{x \in \mathbb{R} : -1 \leq x \leq 1\}$ be given by $f(x) = \sin x$ for all $x \in \mathbb{R}$. Suppose $A = \{x \in \mathbb{R} : -\frac{\pi}{2} \leq x \leq \frac{\pi}{2}\}$. Then the function $g : A \to \mathbb{R}_1$ given by $g(x) = \sin x$, for all $x \in A$ is a restriction of f to A.

[26] The cardinal number of $\mathbb{N}$ happens to be the same as that of $\mathbb{Q}$ but $\mathbb{R}$ has a different cardinal number.

A word of caution regarding another usage of the notation f^{-1}, which is usually used to denote the unique inverse of a bijective function f, is necessary.

Suppose $f : A \to B$ be a function. Let Q be a nonempty subset of B. Then the set $f^{-1}(Q) = \{a \in A : f(a) \in Q\}$ is called the ***inverse image*** of Q under f and $f^{-1}(Q) \subseteq A$. It must be clearly understood from the definition of inverse image, here $f^{-1} : B \to A$ may not exist, and so $f^{-1}(Q)$ is to be understood as the set of preimages of the elements of Q under f. If $P \subseteq A$, then the set $f(P) = \{f(a) : a \in P\} \subseteq B$ and $f(P)$ is called the ***image*** (or, ***direct image***) of P under f. Let X, Y be two nonempty subsets of A. It is interesting to see that $f(X \cap Y) \neq f(X) \cap f(Y)$, in general.

Indeed, let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$ for all, $x \in \mathbb{R}$. Consider X to be the set of all nonnegative integers and Y to be the set of all nonpositive integers. Then, clearly $X, Y \subseteq \mathbb{R}$ and $X \cap Y = \{0\}$. Further, $f(X \cap Y) = f(\{0\}) = \{0\}$, whereas $f(X) = f(Y) = \left\{n^2 : n \in \mathbb{N} \cup \{0\}\right\}$, and hence $f(X) \cap f(Y) = f(X) \neq \{0\}$ proves our claim. However, such an equality holds good for all subsets X, Y of the domain of the function f if and only if f is injective. [See Worked Out Exercise 1.4.8(v)].

We have pointed out earlier, that a function may neither be surjective nor injective. However, before finishing this section, we would like to point out that any function from a set A into another set B is a composition of an injective function, a bijective function and a surjective function.

Suppose $f : A \longrightarrow B$ be a function. Define a binary relation ρ on the set A by

$$x \,\rho\, y \text{ if and only if } f(x) = f(y).$$

Then it is easy to verify that ρ is an equivalence relation on A. The set of all equivalence classes under this relation is given by $\{a\rho \mid a \in A\}$ and is called the ***quotient set*** of A by ρ. Let us denote it by A/ρ. Define the function $g : A \longrightarrow A/\rho$ by $g(a) = a\rho$ for all $a \in A$. Clearly g is a surjective.

Next consider the function $h : A/\rho \longrightarrow f(A)$ defined by $h(a\rho) = f(a)$. We first verify that h is well-defined. Indeed, for $a, b \in A$ with $a\rho = b\rho$, we have $a \,\rho\, b$ and so by definition of ρ we get $f(a) = f(b)$, i.e., $h(a\rho) = h(b\rho)$. Thus h is well-defined. Now we show that h is a bijective function. Let $a, b \in A$ such that $h(a\rho) = h(b\rho)$. Then $f(a) = f(b)$ and so $a \,\rho\, b$, i.e., $a\rho = b\rho$. Thus h is one-to-one. Again for any $c \in f(A)$, we have there exists $a \in A$ such that $f(a) = c$. So $c = h(a\rho)$ and hence h is onto. Therefore h is bijective.

Finally, define the inclusion map $i : f(A) \longrightarrow B$ by $i(c) = c$ for all $c \in B$ (note that $f(A) \subseteq B$). No doubt i is an injective function. Now for any $a \in A$, we have

$$(i \circ h \circ g)(a) = (i \circ h)(g(a)) = (i \circ h)(a\rho) = i\big(h(a\rho)\big) = i\big(f(a)\big) = f(a).$$

Thus we get

$$\begin{array}{ccc} A & \xrightarrow{g} & A/\rho \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle h} \\ B & \xleftarrow{i} & f(A) \end{array}$$

that is, $f = i \circ h \circ g$ where i is injective, h is bijective and g is surjective as we required.

Going ahead of ourselves, we would like to point out that this result plays the key role in the isomorphism theorems of groups and rings as we shall see in subsequent relevant chapters.

Worked Out Exercises

◊ **Exercise 1.4.1.** Determine and justify which of the following sets are functions from A to B:

(a) $f = \{(1,2),(1,3),(2,3),(3,4)\}$; $A = \{1,2,3\}, B = \{1,2,3,4\}$.
(b) $f = \{(a,b),(b,c),(c,d),(d,a)\}$; $A = B = \{a,b,c,d\}$.
(c) $f = \{(a,b),(b,c),(c,d)\}$; $A = B = \{a,b,c,d\}$.

Solution. (a) Here f is not a function, as image of $1(\in A)$ under f (i.e., $f(1)$) is not unique, (observe that $f(1) = 2$ and $f(1) = 3$ as well), whence the well-definedness of f is lost.

(b) Here domain of f is $\{a,b,c,d\} = A$. Further, it can easily be seen that f is well-defined, i.e., no element of A has more than one image under f. Consequently, f is a function from A to A.

(c) In this case, f is not a function from A to A. Indeed, the domain of this relation f is $\{a,b,c\} \subset A$.

◊ **Exercise 1.4.2.** Let $f, g : \mathbb{R} \to \mathbb{R}$ be two functions, given by $f(x) = |x| + x$ for all $x \in \mathbb{R}$ and $g(x) = |x| - x$, for all $x \in \mathbb{R}$. Find $f \circ g$ and $g \circ f$.

Solution. Here, $f(x) = |x| + x$.

$$\text{i.e.,}\quad f(x) = 2x \quad \text{if } x \geq 0$$
$$= 0 \quad \text{if } x < 0$$
$$\text{and}\quad g(x) = -2x \quad \text{if } x < 0$$
$$= 0 \quad \text{if } x \geq 0.$$

Now, let $x \geq 0$; then, $(f \circ g)(x) = f\Big(g(x)\Big) = f(0) = 0$
and $(g \circ f)(x) = g\Big(f(x)\Big) = g(2x) = 0.$

Again, let $x < 0$; then, $(f \circ g)(x) = f\Big(g(x)\Big) = f(-2x) = -4x$
and $(g \circ f)(x) = g\Big(f(x)\Big) = g(0) = 0.$

Consequently, we have $(g \circ f)(x) = 0$ for all $x \in \mathbb{R}$ and

$$f \circ g(x) = 0, \quad \text{if } x \geq 0$$
$$= -4x, \quad \text{if } x < 0.$$

◊ **Exercise 1.4.3.** Let $f, g : A \to B$ and $h, t : B \to C$ be functions. Prove that

(i) if $h \circ f = t \circ f$ and f is surjective, then $h = t$ and

(ii) if $h \circ f = h \circ g$ and h is injective, then $f = g$.

Solution. (i) Let $b \in B$. Since f is surjective, there exists some $a \in A$ such that $f(a) = b$. Now, $h(b) = h\Big(f(a)\Big) = (h \circ f)(a) = (t \circ f)(a) = t\Big(f(a)\Big) = t(b)$. Since this holds good for all $b \in B$, we conclude that $h = t$.

(ii) Let $a \in A$. Since $h \circ f = h \circ g$ we have, $(h \circ f)(a) = (h \circ g)(a)$, i.e., $h\Big(f(a)\Big) = h\Big(g(a)\Big)$. Now as h is injective, this gives $f(a) = g(a)$. Since a is an arbitrary element of A, we conclude that $f = g$.

◊ **Exercise 1.4.4.** For each of the function $f : \mathbb{Z} \to \mathbb{Z}$ given below, find:

(i) a left inverse of f, if it exists.

(a) $f(x) = 2x$;

(b) $f(x) = \frac{x}{2}$, if x is even;
$= 7$, if x is odd.

(ii) a right inverse of f, if it exists.

(a) $f(x) = x - 5$

(b) $f(x) = 2x$

Solution. (i) Recall that a function has a left inverse if and only if it is injective.

(a) Injectivity of f is immediate. Hence f has a left inverse. Let $g : \mathbb{Z} \to \mathbb{Z}$ be defined as

$$g(x) = \begin{cases} \frac{x}{2} & \text{when } x \text{ is even} \\ 1 & \text{when } x \text{ is odd.} \end{cases}$$

Now, $(g \circ f)(x) = g\Big(f(x)\Big) = g(2x) = x = i_{\mathbb{Z}}(x)$, whence $g \circ f = i_{\mathbb{Z}}$ and so g is a left inverse of f.

(b) Observe that here, $f(3) = 7 = f(5)$ though $3 \neq 5$. This indicates that f is not injective and so f has no left inverse.

(ii) Recall that a function has a right inverse if and only if it is surjective.

(a) Note that for any $n \in \mathbb{Z}$, we have $n + 5 \in \mathbb{Z}$ so that $f(n+5) = n + 5 - 5 = n$, whence f is surjective and so f has a right inverse. Let us define $g : \mathbb{Z} \to \mathbb{Z}$ by $g(x) = x + 5$ for all $x \in \mathbb{Z}$. Then, $(f \circ g)(x) = f\Big(g(x)\Big) = f(x+5) = x + 5 - 5 = x = i_{\mathbb{Z}}(x)$, whence $f \circ g = i_{\mathbb{Z}}$ shows that g is a right inverse of f.

(b) Observe that for $5 \in \mathbb{Z}$, there does not exist any $x \in \mathbb{Z}$ such that $f(x) = 2x = 5$. Hence f is not surjective. So f has no right inverse.

◊ **Exercise 1.4.5.** Let $|X| = n$. Prove that there can be $n!$ different bijective functions on X.

Solution. Let $f : X \to X$ be a bijective function. For simplicity, let $X = \{a_1, a_2, \ldots, a_n\}$. Now, a bijective function f on X is to be defined by choosing the images of $a_1, a_2, \ldots, a_n$ under f. Suppose we choose it in the order $f(a_1), f(a_2), \ldots, f(a_n)$. Then $f(a_1)$ can be chosen in n ways and once it is chosen, then $f(a_2)$ can be chosen in $(n-1)$ ways, ... etc.; in general $f(a_k)$ can be chosen in $n - (k-1)$ ways for all $1 \leq k \leq n$. Thus, f has $n(n-1)(n-2)\ldots 2 \cdot 1 = n!$ choices. Hence the number of bijective functions that can be defined on X is $n!$.

♦ **Exercise 1.4.6.** Let A and B be two finite sets with $|A| = 5$ and $|B| = 3$. Show that the number of surjective functions from A onto B is 150.

Solution. Observe that since the set B has 3 elements and in a surjective function codomain is the same as range, if we find the number of different possible partitions of the set A into three subsets and assign to each such subset one element of B in all possible manners, then each such assignment will be a surjective function of A onto B. Now as $|A| = 5$, the number of different partitions of A into 3 subsets is given

by $\phi(5,3)$, which can be calculated to be equal to 25 [refer to Worked Out Exercise 1.2.7]. Again each of these partitions (into three subsets) can be assigned to three elements of B in 3! ways. Hence total number of possible surjective functions is $25 \times 3! = 25 \times 6 = 150$.

◊ **Exercise 1.4.7.** Let $f : X \to Y$ be a function. Then prove that

(i) if f is injective and $A, B \subseteq X$ then, $f(A \setminus B) \subseteq f(A) \setminus f(B)$;

(ii) if $A, B \subseteq Y$ then, $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$

Solution. (i) Let $x \in f(A \setminus B)$. Then $x = f(a)$ for some $a \in A$ such that $a \notin B$. Now, $a \in A$ implies that $f(a) \in f(A)$. Suppose $f(a) \in f(B)$. Then $f(a) = f(b)$ for some $b \in B$. But since f is injective $f(a) = f(b)$ implies that $a = b$ so that $a \in B$, which is a contradiction. Hence $f(a) \notin f(B)$. This implies that $x = f(a) \in f(A) \setminus f(B)$. Consequently, $f(A \setminus B) \subseteq f(A) \setminus f(B)$.

(ii) Let $x \in f^{-1}(A) \setminus f^{-1}(B) \iff x \in f^{-1}(A)$ and $x \notin f^{-1}(B) \iff f(x) \in A$ and $f(x) \notin B \iff f(x) \in A \setminus B \iff x \in f^{-1}(A \setminus B)$. Hence we have $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

♦ **Exercise 1.4.8.** Either prove the following statements or give counter examples to disprove:

(i) The set $\mathbb{R}$ is equipotent with $\mathbb{R}^+$.

(ii) The set $\mathbb{R}$ is equipotent with $S = \{x \in \mathbb{R} : 0 < x < 1\}$

(iii) If $X = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ and $Y = \{x \in \mathbb{R} : 0 < x < 1\}$, then X and Y have the same cardinal number.

(iv) Let A, B and C be nonempty sets and $f : A \to B$, $g : B \to C$ are functions.

(a) if $g \circ f : A \to C$ is injective, then g is also injective.

(b) if $g \circ f : A \to C$ is surjective, then f is also surjective.

(v) Let $f : X \to Y$ be a function. Then f is injective if and only if $f(A \cap B) = f(A) \cap f(B)$ for all nonempty subsets A and B of X.

Solution. (i) **True.** Define $f : \mathbb{R} \to \mathbb{R}^+$ by $f(x) = e^x$ for all $x \in \mathbb{R}$. Check that f is a bijective function from $\mathbb{R}$ onto $\mathbb{R}^+$.

(ii) **True.** Define $f : S \to \mathbb{R}$ by $f(x) = \tan \pi(x - \frac{1}{2})$ for all $x \in S$. Check that f is a bijective function from S onto $\mathbb{R}$.

(iii) **True.** Let $P = \{x \in \mathbb{R} : \frac{1}{4} \leq x \leq \frac{3}{4}\}$. Then $P \subseteq Y$. Let us define $f : X \to P$ by $f(x) = \frac{x}{2} + \frac{1}{4}$. Check that f is injective. Now let $x \in P$. Let $y = 2x - \frac{1}{2}$. Now, as $\frac{1}{4} \leq x \leq \frac{3}{4}$, we see that $0 \leq 2x - \frac{1}{2} \leq 1$ and hence $y \in X$. Observe that, $f(y) = \frac{y}{2} + \frac{1}{4} = \frac{1}{2}(2x - \frac{1}{2}) + \frac{1}{4} = x$, whence f is surjective also and consequently a bijective function. Therefore $X \sim P$. Again, $Y \subseteq X$ and $Y \sim Y$. Now apply the Schröeder-Bernstein theorem to see that $X \sim Y$.

(iv) (a) **False.** Indeed, let $f, g : \mathbb{R} \to \mathbb{R}$ be defined by, $f(x) = e^x$ and $g(x) = x^2$ for all $x \in \mathbb{R}$. Note that, here $(g \circ f)(x) = g\Big(f(x)\Big) = g(e^x) = e^{2x}$ for all $x \in \mathbb{R}$, which is injective; but g is not injective as $-5 \neq 5$ but $g(-5) = (-5)^2 = 25 = (5)^2 = g(5)$.

(b) **False.** For example, let $A = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$; let $f : \mathbb{N} \to \mathbb{N}$ be given by $f(n) = 5n$, for all $n \in \mathbb{N}$ and let $g : \mathbb{N} \to A$ be given by $g(n) = \omega^n$, for all $n \in \mathbb{N}$. Observe that $(g \circ f)(n) = g\Big(f(n)\Big) = g(5n) = \omega^{5n}$ for all $n \in \mathbb{N}$. Clearly, $g \circ f : \mathbb{N} \to A$ is a surjective function but f is not.

(v) **True.** Suppose f is injective and A, B be nonempty subsets of X. Let $y \in f(A \cap B)$; i.e., $y = f(x)$ for some $x \in A \cap B$. But as then $x \in A$ so, $y = f(x) \in f(A)$ and a similar argument shows that $y \in f(B)$, whence $y \in f(A) \cap f(B)$ and we get, $f(A \cap B) \subseteq f(A) \cap f(B)$. Now, let $y \in f(A) \cap f(B)$. Then $y \in f(A)$ and $y \in f(B)$ i.e., $y = f(a)$ for some $a \in A$ and $y = f(b)$ for some $b \in B$. Now, as f is injective and $f(a) = f(b)$, we conclude $a = b$, whence $a \in A \cap B$ so that $y = f(a) \in f(A \cap B)$. Hence, $f(A) \cap f(B) \subseteq f(A \cap B)$. Consequently, $f(A \cap B) = f(A) \cap f(B)$.

Conversely, suppose that $f(A \cap B) = f(A) \cap f(B)$ for all subsets A and B of X. Suppose that f is not injective. Then there must exist some $x, y \in X$ such that $x \neq y$ but $f(x) = f(y)$. Consider $A = \{x\}$ and $B = \{y\}$. Then $A \cap B = \emptyset$ and so $f(A \cap B) = \emptyset$. However, observe that $f(A) \cap f(B) = \{f(x)\} \neq \emptyset$. This gives $f(A \cap B) \neq f(A) \cap f(B)$, a contradiction. Hence f is injective.

Exercises

1. Determine which of the following sets are functions from A to B. Justify your answer.
   (a) $f = \{(a,b),(a,c),(b,d),(c,a)\}$; $A = \{a,b,c\}$, $B = \{a,b,c,d\}$.
   (b) $f = \{(1,3),(2,2),(3,4)\}$; $A = \{1,2,3\}$ $B = \{1,2,3,4\}$.
   (c) $f = \{(a,p),(b,p),(c,q),(d,r)\}$; $A = \{a,b,c,d\}$ $B = \{p,q,r\}$.
   (d) $f = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid b = a+5\}$; $X = Y = \mathbb{Z}$.
   (e) $f = \{(a,b) \in \mathbb{R} \times \mathbb{R} \mid b = \sqrt{a}\}$; $X = Y = \mathbb{R}$.

   In case any of the above sets are functions, determine their nature as to injectivity, surjectivity or bijectivity.
2. If $A = \{a,b\}$ and $b = \{1,2\}$, find all the relations from A into B. Detect which of these relations are functions from A to B.
3. Show that the following functions are neither injective nor surjective.
   (a) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = |x|$, $x \in \mathbb{R}$.
   (b) $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \cos x$, $x \in \mathbb{R}$.
4. Show that the following functions are injective but not surjective.
   (a) $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 2x$, $x \in \mathbb{Z}$.
   (b) $f : \mathbb{N} \to \mathbb{N}$ given by $f(x) = 2x + 5$, $x \in \mathbb{N}$.
5. Show that the following functions are surjective but not injective.
   (a) $f : \mathbb{Z} \to 2\mathbb{N}_0$ given by $f(x) = 2|x|$, $x \in \mathbb{Z}$.
   (b) $f : \mathbb{Z} \to \{1,-1\}$ given by $f(x) = (-1)^x$, $x \in \mathbb{Z}$.
6. Determine which of the following functions are surjective, injective or bijective.
   (a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = |x|x$, for all $x \in \mathbb{R}$;
   (b) $f : \mathbb{R}^+ \to \mathbb{R}^+$ defined by $f(x) = \sqrt{x}$, for all $x \in \mathbb{R}^+$;
   (c) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = |x| + x$, for all $x \in \mathbb{R}$;
   (d) $f : \mathbb{Z} \to \mathbb{Q}$ defined by $f(x) = 2^x$, for all $x \in \mathbb{R}$;
   (e) $f : \mathbb{R}^* \to \mathbb{R}^*$ defined by $f(x) = \frac{1}{x}$, for all $x \in \mathbb{R}^*$;
   (f) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x - 7$, for all $x \in \mathbb{R}$;
   (g) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 - 3x + 4$, for all $x \in \mathbb{R}$.
7. Let A be a finite set and let $f : A \to B$ be a surjective function. Show that the number of elements of B cannot be greater than that of A.
8. Suppose f and g are two functions from $\mathbb{R}$ into $\mathbb{R}$ such that $f \circ g = g \circ f$. Does it necessarily imply that $f = g$? Justify your answer.
9. Let $X = \{a,b,c\}$. Find all possible bijective functions from X into itself.
10. Let $f : A \to B$. Give suitable examples to show that the inverse relation $f^* = \{(y,x) \in B \times A : (x,y) \in f\}$ need not always be a function. Prove that f^* is a function from $Im(f)$ into A if and only if f is injective.

11. Let $f : A \to B$ be a bijective function. Prove that

    (a) inverse of f is a unique function which is also bijective;

    (b) $(f^{-1})^{-1} = f$, where f^{-1} denotes the unique inverse of f;

    (c) if further, $g : B \to C$ is another bijective function, then show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

12. Find whether the following functions are bijective; if so, find their inverse.

    (a) Let $S = \{x \in \mathbb{R} : -1 < x < 1\}$ and $f : \mathbb{R} \to S$ be defined by $f(x) = \dfrac{x}{1+|x|}$;

    (b) Let $P = \{x \in \mathbb{R} : 0 < x < 1\}$ and $f : P \to \mathbb{R}$ be defined by $f(x) = \dfrac{2x-1}{1-|2x-1|}$.

13. † (a) Prove that the set of all integers is equipotent with the set of all rational numbers.

    (b) Prove that $3\mathbb{Z}$ and $5\mathbb{Z}$ are equipotent.

14. Let X and Y be nonempty sets and $f : X \to Y$ be a function of X into Y. If $A, A_1, A_2, A_\alpha \subseteq X$ and $B, B_1, B_2, B_\alpha \subseteq Y$ for all $\alpha \in \Gamma$ (where Γ is an index set), then prove the following:

    (i) $f(\emptyset) = \emptyset$, $f^{-1}(\emptyset) = \emptyset$, $f(X) \subseteq Y$, $f^{-1}(Y) = X$;

    (ii) $A_1 \subseteq A_2 \Longrightarrow f(A_1) \subseteq f(A_2)$, $B_1 \subseteq B_2 \Longrightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$;

    (iii) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$, $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$;

    (iv) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;

    (v) $f(\bigcup\limits_{\alpha\in\Gamma} A_\alpha) = \bigcup\limits_{\alpha\in\Gamma} f(A_\alpha)$, $f^{-1}(\bigcup\limits_{\alpha\in\Gamma} B_\alpha) = \bigcup\limits_{\alpha\in\Gamma} f^{-1}(B_\alpha)$;

    (vi) $f(\bigcap\limits_{\alpha\in\Gamma} A_\alpha) \subseteq \bigcap\limits_{\alpha\in\Gamma} f(A_\alpha)$, $f^{-1}(\bigcap\limits_{\alpha\in\Gamma} B_\alpha) = \bigcap\limits_{\alpha\in\Gamma} f^{-1}(B_\alpha)$;

    (vii) $f^{-1}(B') = \{f^{-1}(B)\}'$; where B' is the complement of B in Y;

    (viii) $A \subseteq f^{-1}(f(A))$, $f(f^{-1}(B)) \subseteq B$;

    (ix) f is injective $\Longleftrightarrow$ $A = f^{-1}(f(A))$ is true for all $A \subseteq X$;

    (x) f is surjective $\Longleftrightarrow$ $f(f^{-1}(B)) = B$ is true for all $B \subseteq Y$;

    (xi) f is surjective $\Longleftrightarrow$ $\{f(A)\}' \subseteq f(A')$ is true for all $A \subseteq X$;

15. Let A be a nonempty set and ρ be a relation on A. Let B denote the set of all ρ-equivalent classes. Prove that there exists a surjective function from A onto B.

    [*This function is called the* ***canonical surjection*** *and the set B is called the* ***quotient set*** *of A determined by ρ and is denoted by A/ρ.*]

16. (a) Let $f, g : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 3x^2 - 5$ and $g(x) = \dfrac{x}{x^2+1}$. Find $f \circ g$ and $g \circ f$.

    (b) Find $f^{-1}\big(\{70\}\big)$, $f\big(f^{-1}(\{70\})\big)$.

    (c) Show that $g^{-1}\big(g(\{2,3\})\big) \neq \{2,3\}$.