

## Cartesian Products and Relations

**Definition (Cartesian product)** If  $A$  and  $B$  are sets, the *Cartesian product* of  $A$  and  $B$  is the set

$$A \times B = \{(a, b) : (a \in A) \text{ and } (b \in B)\}.$$

The following points are worth special attention: The Cartesian product of two sets is a set, and the elements of that set are ordered pairs. In each ordered pair, the first component is an element of  $A$ , and the second component is an element of  $B$ .

**Example (Cartesian product)** If  $A = \{\{1, 2\}, \{3\}\}$  and  $B = \{(a, b), (c, d)\}$ , then

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

**Determining  $|A \times B|$ .** If  $A$  and  $B$  are finite sets, then  $|A \times B| = |A| \cdot |B|$  because there are  $|A|$  choices for the first component of each ordered pair and, for each of these,  $|B|$  choices for the second component of the ordered pair.

**Cartesian Product is not commutative** For the sets  $A$  and  $B$  one paragraph above,

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

This example shows that, in general,  $A \times B \neq B \times A$ . The underlying reason is that if  $A$  and  $B$  are non-empty and one set, say  $A$ , contains an element  $x$  which is not in  $B$ , then  $A \times B$  contains an ordered pair with first component equal to  $x$ , but  $B \times A$  contains no such ordered pair. The condition that  $A$  and  $B$  are non-empty is required because of the following Proposition.

**Proposition CPR1.** If  $A$  is a set, then  $A \times \emptyset = \emptyset$  and  $\emptyset \times A = \emptyset$ .

**Proof.**

We argue by contradiction using the definition of Cartesian product: Suppose  $A \times \emptyset \neq \emptyset$  and consider  $(x, y) \in A \times \emptyset$ . Then, by definition of Cartesian product,  $y \in \emptyset$ , a contradiction. Therefore, the set  $A \times \emptyset$  must be empty. The proof that  $\emptyset \times A = \emptyset$  is similar, and is left as an **exercise**. ■

**Proposition CPR2.** If  $A$  and  $B$  are sets,  $A \times B = B \times A$  if and only if  $A = B$ , or  $A = \emptyset$ , or  $B = \emptyset$ .

**Proof.**

( $\Leftarrow$ ) If  $A = B$  then substituting  $B$  for  $A$  gives  $A \times B = A \times A = B \times A$ . If  $A = \emptyset$  or  $B = \emptyset$ , then by Proposition CP1,  $A \times B = \emptyset = B \times A$ .

( $\Rightarrow$ ) Suppose that  $A$  and  $B$  are non-empty sets and  $A \times B = B \times A$ . Let  $x \in A$ . Since  $B \neq \emptyset$ , there exists an element  $y \in B$ , so that  $(x, y) \in A \times B$ . Since  $A \times B = B \times A$ , we have that  $(x, y) \in B \times A$  (too). By the definition of Cartesian product,  $x \in B$ . Therefore,  $A \subseteq B$ . Similarly  $B \subseteq A$ . Thus,  $A = B$ . ■

It is sometimes true that the Cartesian product distributes over other set operations similarly to the distributive law of multiplication over addition.

**Proposition CPR3.** Let  $A, B$  and  $C$  be sets. Then,

(a)  $A \times (B \cap C) = (A \times B) \cap (A \times C)$ ;

(b)  $A \times (B \cup C) = (A \times B) \cup (A \times C)$ ;

(c)  $(A \times B) \cap C = (A \times C) \cap (B \times C)$ ;

(d)  $(A \times B) \cup C = (A \times C) \cup (B \times C)$ .

**Proof.**

We prove part (b) and leave the proofs of the remaining parts as an **exercise**. We have  $(x, y) \in A \times (B \cup C) \Leftrightarrow x \in A$  and  $y \in B \cup C \Leftrightarrow (x \in A)$  and  $(y \in B$  or  $y \in C) \Leftrightarrow [(x \in A)$  and  $(y \in B)]$  or  $[(x \in A)$  and  $(y \in C)]$  (by a distributive law of logic)  $\Leftrightarrow [(x, y) \in A \times B]$  or  $[(x, y) \in A \times C] \Leftrightarrow (x, y) \in (A \times B) \cup (A \times C)$ . ■

**Exercise.** Investigate, and prove or disprove as appropriate, similar statements involving the set operations relative complement  $(A - B)$ , and symmetric difference.

**Definition (relation).** A *relation from a set  $A$  to a set  $B$*  is a subset of  $A \times B$ . A *(binary) relation on  $A$*  is a subset of  $A \times A$ .

It is important to remember that a relation is a set of ordered pairs. There need be no relationship between the components of the ordered pairs; *any* set of ordered pairs is a relation. Usually, however, we choose which ordered pairs belong to the relation so that components are related in some way, so we think of the relation as somehow representing the connection. For example, if  $A = \{Gary, Jing, Keika\}$  and  $B = \{7447, 7448, 7455\}$ , then  $R = \{(Gary, 7448), (Jing, 7447), (Keika, 7455)\}$  is a relation from  $A$  to  $B$  that pairs each UVic Math instructor in set  $A$  and her/his UVic telephone extension in set  $B$ .

**Counting relations.** Since any subset of  $A \times B$  is a relation from  $A$  to  $B$ , it follows that if  $A$  and  $B$  are finite sets then the number of relations from  $A$  to  $B$  is  $2^{|A \times B|} = 2^{|A| \cdot |B|}$ . One way to see this is as the number of subsets of  $A \times B$ . A direct way to count is the same way one counts subsets: observe that for each of the  $|A \times B| = |A| \cdot |B|$  ordered pairs in  $A \times B$  there are two possibilities, either the ordered pair belongs to the relation or it doesn't, so by the rule of product the number of relations from  $A$  to  $B$  is  $2 \cdot 2 \cdot 2 \cdots 2$  ( $|A| \cdot |B|$  twos). Similarly, if  $A$  is a finite set then the number of relations on  $A$  is  $2^{|A| \cdot |A|}$ .

Let  $A = \{1, 2, \dots, 10\}$ . By the above, there are  $2^{100}$  relations on  $A$ . The number of these that contain the pairs  $(1, 1), (2, 2), \dots, (10, 10)$  is  $1^{10} 2^{90} = 2^{90}$ : each of the 10 specified pairs must be in the relation (1 way to do this), and there are two possibilities – in or not – for each of the remaining 90 pairs. Similar reasoning shows that the number of relations on  $A$  that contain none of  $(1, 2), (3, 4), (5, 6)$  is  $2^{97}$ . The number of relations on  $A$  that contain  $(2, 5)$  or  $(7, 9)$  is  $2^{100} - 2^{98}$  (total minus the number that contain neither ordered pair). A different way of counting these gives the equivalent expression  $2^{99} + 2^{99} - 2^{98}$  (the number that contain  $(2, 5)$  plus number that contain  $(7, 9)$  minus the number that contain both). Finally, the number of relations on  $A$  that contain either  $(2, 5)$  or  $(7, 9)$  but not both is  $2^{98} + 2^{98}$  (the number that contain  $(2, 5)$  and not  $(7, 9)$  plus the number that contain  $(7, 9)$  and not  $(2, 5)$ ).

**Example (less than or equal to relation)** The relation  $R$  on the set  $A = \{1, 2, 3\}$  given by

$$R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$$

is the set of all ordered pairs  $(a, b)$  of elements of  $A$  such that  $a \leq b$  and we can think of the set  $R$  as representing the “less than or equal to” relation.

**Infix notation for relations.** If  $R$  is a relation on  $A$  and  $(a, b) \in R$ , we sometimes use the infix notation  $aRb$  and say “ $a$  is related to  $b$  (under  $R$ )”. If  $a$  is not related to  $b$  under  $R$ , we sometimes use the infix notation with a slash through the  $R$ .

**Example (subset relation, infix notation).** Let  $B = \{a, b, c\}$  and let  $\mathcal{S}$  be the relation on  $\mathcal{P}(B)$  (the *power set* of  $B$ , i.e. the set of all subsets of  $B$ ) defined by  $X \mathcal{S} Y \Leftrightarrow X \subseteq Y$ . That is, a subset  $X$  of  $B$  is related to a subset  $Y$  of  $B$  under  $\mathcal{S}$  exactly when  $X$  is a subset of  $Y$ . The symbol  $\mathcal{S}$  can be regarded as a synonym for the symbol  $\subseteq$  or, alternatively, the symbol  $\subseteq$  could be regarded as the name of the set of all ordered pairs  $(X, Y)$  where  $X, Y \in \mathcal{P}(B)$  and  $X$  is a subset of  $Y$ .

**Example (recursively defined relations).** Relations are sets (of ordered pairs), and thus can sometimes be defined recursively. For example, let  $D$  be the relation on  $\mathbf{Z}^+$  (the positive integers) defined by:

BASIS:  $1 R 5$ ;

RECURSION: For all  $x, y \in \mathbf{Z}^+$ , if  $x R y$  then  $(x + 1) R (y + 5)$ .

After generating a few terms, it is not difficult to guess and prove that

$R = \{(a, b) \in \mathbf{Z}^+ \times \mathbf{Z}^+ : b = 5a\}$ . The statement to be proved is  $P(a)$ : *An ordered pair  $(a, b)$  belongs to  $R$  if and only if  $b = 5a$ .*

We first prove by induction on  $a$  that *if  $a \in \mathbf{Z}^+$  and  $b = 5a$ , then  $(a, b) \in R$* :

BASIS ( $a = 1$ ):  $(1, 5) \in R$  by definition of  $R$ . Thus, the statement is true for  $a = 1$ .

INDUCTION HYPOTHESIS: For some  $k \geq 1$ , suppose that if  $n = 5k$  then  $(k, n) \in R$ .

INDUCTION STEP: Suppose  $m = 5(k + 1)$ . Then  $m - 5 = 5k$ , so by the induction hypothesis  $(k, m - 5) \in R$ . By the definition of  $R$ ,  $(k, m - 5) \in R \Rightarrow (k + 1, m - 5 + 5) \in R$ . Thus, if  $m = 5(k + 1)$ , then  $(k + 1, m) \in R$ .

Therefore, by induction, for all  $a \in \mathbf{Z}^+$ , if  $a \in \mathbf{Z}^+$  and  $b = 5a$ , then  $(a, b) \in R$ .

To complete the proof, we show by induction on  $a$  that *if  $(a, b) \in R$  then  $b = 5a$* :

BASIS ( $a = 1$ ): By definition of  $R$ , the only ordered pair in  $R$  with first component equal to 1 is  $(1, 5)$ . Since  $5 = 5 \cdot 1$ , the statement is true for  $a = 1$ .

INDUCTION HYPOTHESIS: For some  $k \geq 1$ , suppose that if  $(k, n) \in R$ , then  $n = 5k$ .

INDUCTION STEP: Suppose  $(k + 1, m) \in R$ . By definition of  $R$ , this can happen only if  $(k, m - 5) \in R$ . By the induction hypothesis,  $m - 5 = 5k$ . Hence  $m = 5k + 5 = 5(k + 1)$ . Thus, if  $(k + 1, m) \in R$ , then  $m = 5(k + 1)$ .

Therefore, by induction, for all  $a \in \mathbf{Z}^+$ , if  $(a, b) \in R$  then  $b = 5a$ .

For a more difficult example, consider the relation  $S$  on  $\mathbf{Z}^+$  defined by:

BASIS:  $(1, 2), (1, 3) \in S$ ;

RECURSION: For all  $x, y \in \mathbf{Z}^+$ , if  $(x, y) \in S$  then  $(x + 1, y + 2), (x + 1, y + 3) \in S$ .

**Exercise:** Prove by induction that  $S = \{(k, n) \in \mathbf{Z}^+ \times \mathbf{Z}^+ : 2k \leq n \leq 3k\}$ .

## Functions

**Definition (function).** A *function* from a set  $A$  to a set  $B$  is a relation  $f$  from  $A$  to  $B$  with the property that for every element  $a \in A$  there exists one and only one element  $b \in B$  such that  $(a, b) \in f$ .

**Definition (image, value, preimage).** If  $f$  is a function from  $A$  to  $B$ , then we use the notation  $f : A \rightarrow B$ . From the definition of a function if  $f : A \rightarrow B$ , then  $f$  can be viewed as an assignment, to each element  $a \in A$ , of a unique element  $b$  in  $B$ . If  $(a, b) \in f$ , then we denote the assignment of  $b$  to  $a$  by writing  $b = f(a)$  and calling  $b$  *the image of  $a$  under  $f$* , or the *value of  $f$  at  $(a)$* ; the element  $a$  is called a *preimage* of  $b$ . (Note that it is a preimage rather than *the* preimage; more than one element of  $A$  could map to  $b$ .)

It is common usage to say “ $f$  maps  $A$  to  $B$ ”. This expression arises from the usual arrow diagram where each element of  $A$  is joined by an arrow to the element of  $B$  assigned to it. Unfortunately, this tends to lead to the confusion that the elements of  $A$  are somehow assigned to the elements of  $B$ , *which is backwards!* It is the elements of  $B$  that are assigned to the elements of  $A$ .

It is important to keep the following facts straight. Every element of  $A$  has some element of  $B$  assigned to it. No element of  $A$  is assigned more than one element of  $B$ , each is assigned *exactly one*. There is no guarantee that different elements of  $A$  are assigned different elements of  $B$ . When we say that each element of  $A$  is assigned a unique element of  $B$ , we mean that each element of  $A$  is assigned one and only one element of  $B$ . This does *not* mean that if  $a_1 \neq a_2$ , then  $f(a_1) \neq f(a_2)$ ; it is quite possible that  $f(a_1) = f(a_2)$  (We have a special name for functions with the property that  $a_1 \neq a_2$  implies  $f(a_1) \neq f(a_2)$ : 1-1.) There is no guarantee that any particular element of  $B$  is assigned to any element of  $A$ . (We have a special name for functions with the property that every element of  $B$  is the image of at least one element of  $A$ : onto.)

**Definition (domain, inputs, codomain, range).** Before we can talk about functions, we need names for the objects we want to talk about:

- The set  $A$  is called the *domain*, and the elements of  $A$  are called *inputs* to  $f$  (so the domain is where the inputs live).
- The set  $B$  is called the *codomain*.
- The subset of  $B$  consisting of the elements which are values of  $f$  (i.e., are assigned to some element in  $A$ ) is called the *range of  $f$* . (Think: the values of  $f$  range over the elements in this set.) The range of  $f$  is the set  $f(A) = \{b : b \in B \text{ and } b = f(a) \text{ for some } a \in A\}$ .

**Example (function, domain, codomain, range, image, preimage).** Let  $A$  be the set of all faculty and students at UVic, and let  $B$  be the set of all amounts of money in dollars and cents. Let  $f$  be the relation from  $A$  to  $B$  where  $(a, b) \in f \Leftrightarrow$  person  $a \in A$  owes amount  $b$  to the library. Since for every person  $a \in A$  there is a unique amount of money that s/he owes to the library (possibly \$0),  $f$  is a function. The domain of  $f$  is  $A$ , its codomain is  $B$ , and its range is the set of all amounts of money that are owed (each by at least one person). If  $(\text{Gary}, \$1.59) \in f$ , then  $f(\text{Gary}) = \$1.59$ , the image of Gary

is \$1.59, a pre-image of \$1.59 is Gary, and the amount \$1.59 belongs to the range of  $f$ . (Note: any person who owes \$1.59 to the library is also a pre-image of \$1.59.)

The above example demonstrates a function which can not be defined by “giving a formula” for  $f(a)$ . In the definition of function  $A$  and  $B$  are just sets – there don’t have to be any numbers anywhere – so it may be very difficult to give a formula.

**Example (function, domain, codomain, range, image, preimage).** Let  $f : \mathbf{R} \rightarrow \mathbf{R}$  defined by  $f(x) = 2\lceil x \rceil$ . (Recall that, for a real number  $x$ , *the ceiling of  $x$* , denoted  $\lceil x \rceil$  is the smallest integer which is greater than or equal to  $x$ . Hence  $f$  is a function.) The domain of  $f$  is the set  $\mathbf{R}$  of real numbers. The codomain is also the set of real numbers. The range of  $f$  is the set of even integers: since  $\lceil x \rceil$  is an integer,  $f(x) = 2\lceil x \rceil$  is an even integer. Thus, the range is a subset of the even integers. To see that every even integer  $2t$ , ( $t \in \mathbf{Z}$ ) is a value of  $f$ , observe that for  $t \in \mathbf{Z}$ ,  $f(t) = 2\lceil t \rceil = 2t$ .

**Exercises.** We leave as an exercise for the reader to determine the range of the function  $g : \mathbf{R} \rightarrow \mathbf{R}$  defined by  $g(x) = \lfloor x \rfloor^2$ . (Recall that for a real number  $x$ , *the floor of  $x$* , denoted  $\lfloor x \rfloor$  is the largest integer which is less than or equal to  $x$ .) For more exercises, find the range of  $h : \mathbf{R} \rightarrow \mathbf{R}$  defined by  $h(x) = \lfloor 2x \rfloor$ , and show that the range of  $\ell : \mathbf{Z} \rightarrow \mathbf{Z}$  defined by  $\ell(n) = n^2 + 4n + 4$  is  $\{k^2 : k \in \mathbf{N}\} = \{0^2, 1^2, 2^2, \dots\}$ .

**Counting functions.** Let  $A$  and  $B$  be finite sets, say  $A = \{a_1, a_2, \dots, a_m\}$  and  $B = \{b_1, b_2, \dots, b_n\}$ . We count the number of functions from  $A$  to  $B$ . By the definition of function, for each  $a \in A$  there is exactly one  $b \in B$  such that  $(a, b) \in f$ . Thus, there are  $n$  choices for the element to be paired with  $a_1$ ,  $n$  choices for the element to be paired with  $a_2$ , and so on. In general, for each choice for  $a$  there are  $n = |B|$  choices for the element  $b$  such that  $(a, b) \in f$ . By the rule of product, the number of functions from  $A$  to  $B$  is therefore  $n \times n \times \dots \times n$  ( $m$  terms, all equal to  $n$ ), which equals  $n^m$  (or  $|B|^{|A|}$ ).

**Definition (image of a set, preimage of a set).** The notions of image and preimage can be generalized to sets. Suppose  $f : A \rightarrow B$  is a function. If  $A_1 \subseteq A$ , then *the image of  $A_1$  under  $f$*  is the set

$$f(A_1) = \{b \in B : b = f(a) \text{ for some } a \in A_1\}.$$

That is,  $f(A_1)$  is the set whose elements are the images under  $f$  of the elements in  $A_1$ . If  $B_1 \subseteq B$ , then *the preimage of  $B_1$  under  $f$*  is the set

$$f^{-1}(B_1) = \{a \in A : f(a) \in B_1\}.$$

That is,  $f^{-1}(B_1)$  is the set of elements in  $A$  whose image under  $f$  is in  $B_1$ .

**Example (image of a set, preimage of a set).** Let  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{a, b, c, d\}$  and  $f : A \rightarrow B$  be given by

$$f = \{(1, d), (2, a), (3, c), (4, a), (5, c)\}.$$

Then  $f(\{1, 2, 3\}) = \{d, a, c\}$ , and  $f^{-1}(\{d, a, c\}) = \{1, 2, 3, 4, 5\}$ . Notice that this shows that if  $f(A_1) = B_1$  then it need not be the case that  $f^{-1}(B_1) = A_1$ ; it is however, true that if  $f(A_1) = B_1$ , then  $f^{-1}(B_1) \subseteq A_1$ . (To see this, let  $y \in B_1$ . then  $y = f(x)$  for some  $x \in A_1$ . Hence  $x \in f^{-1}(B_1)$ .) We leave it as an **exercise** to prove that equality occurs, that is  $f^{-1}(f(A_1)) = A_1$ , if and only if there is no element  $a \in A - A_1$  such that  $f(a) \in f(A_1)$ . As a further **exercise**, prove that for  $B_1 \subseteq B$  we have  $f(f^{-1}(B_1)) \subseteq B_1$ ,

with equality if and only if  $B_1$  is a subset of the range of  $f$  (that is, every element of  $B_1$  is the image of some element of  $A$ ).

Observe that if  $f : A \rightarrow B$  is a function then, by definition of function  $f^{-1}(B) = A$  and  $f(A)$  is the range of  $f$  (which is a subset of  $B$ ). Let  $B_1 \subseteq B$ . By definition of preimage of a subset of the codomain we have  $f^{-1}(B_1) = \emptyset$  if and only if there is no element  $x \in A$  with  $f(x) \in B_1$ . Thus  $f^{-1}(\emptyset) = \emptyset$  and, in the example above  $f^{-1}(\{b\}) = \emptyset$ .

**Example (finding the range).** Let  $f : \mathbf{R} \rightarrow \mathbf{Z}$  be defined by  $f(x) = \lceil 2x \rceil + \lfloor 2x \rfloor$ . To determine the range of  $f$ , we begin by testing a few values of  $x$ :

- $f(0) = 0$ ;
- If  $x \in (0, 1/2)$ , then  $2x \in (0, 1)$  so  $\lceil 2x \rceil = 1$  and  $\lfloor 2x \rfloor = 0$ , hence  $f(x) = 1$ ;
- $f(1/2) = 2$ ;
- If  $x \in (1/2, 1)$  then  $2x \in (1, 2)$   $\lceil 2x \rceil = 2$  and  $\lfloor 2x \rfloor = 1$ , hence  $f(x) = 3$ ;
- $f(1) = 4$ ;
- If  $x \in (1, 3/2)$ , then  $2x \in (2, 3)$  so  $\lceil 2x \rceil = 3$  and  $\lfloor 2x \rfloor = 2$ , hence  $f(x) = 5$ .
- $f(3/2) = 6$ .

Based on these computations, it seems reasonable to guess that the range of  $f$  is  $\mathbf{Z}$ . We prove that this is the case. First, observe that  $f(x)$  is an integer for every  $x \in \mathbf{R}$ , so  $f(\mathbf{R}) \subseteq \mathbf{Z}$ . To show the opposite inclusion, let  $y \in \mathbf{Z}$ . We must find  $x \in \mathbf{R}$  such that  $f(x) = y$ . If  $y$  is even, say  $y = 2t, t \in \mathbf{Z}$ , then  $f(t/2) = \lceil 2t/2 \rceil + \lfloor 2t/2 \rfloor = 2t = y$ . If  $y$  is odd, say  $y = 2t + 1, t \in \mathbf{Z}$ , then for any  $x \in (t/2, t/2 + 1/2)$  we have  $2x \in (t, t + 1)$ , hence  $f(x) = (t + 1) + t = 2t + 1 = y$ . Hence the range of  $f$  is  $\mathbf{Z}$ . As an **exercise**, show that the image of the set  $\mathbf{N}$  of natural numbers is  $f(\mathbf{N}) = \{4n : n \in \mathbf{N}\}$ .

**Example (finding preimages).** Let  $g : \mathbf{R} \rightarrow \mathbf{Z}$  be defined by  $g(x) = \lfloor 3x \rfloor$ . We determine the preimage of  $\{-1, 1\}$  and of  $T = \{2n : n \in \mathbf{N}\}$ . To determine  $g^{-1}(\{-1, 1\})$  we need to figure out the preimages of each element of  $\{-1, 1\}$ . We have  $g(x) = -1 \Leftrightarrow \lfloor 3x \rfloor = -1 \Leftrightarrow 3x \in [-1, 0) \Leftrightarrow x \in [-1/3, 0)$ . Similarly,  $g(x) = 1 \Leftrightarrow x \in [1/3, 2/3)$ . Thus,  $g^{-1}(\{-1, 1\}) = [-1/3, 0) \cup [1/3, 2/3)$ . The set  $g^{-1}(T)$  can be determined in the same way. For  $n \in \mathbf{N}$  we have  $g(x) = 2n \Leftrightarrow \lfloor 3x \rfloor = 2n \Leftrightarrow 3x \in [2n, 2n + 1) \Leftrightarrow x \in [2n/3, (2n + 1)/3)$ . Therefore,  $g^{-1}(T) = \bigcup_{n=0}^{\infty} [2n/3, (2n + 1)/3) = [0, 1/3) \cup [2/3, 1) \cup [4/3, 5/3) \cup [3, 7/3) \cup \dots$

**Theorem F1.** Let  $f : A \rightarrow B$  be a function,  $A_1, A_2 \subseteq A$  and  $B_1, B_2 \subseteq B$ . Then

- (a)  $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$ ;
- (b)  $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$ .
- (c)  $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$ .
- (d)  $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$ .

**Proof.**

We prove (b) and leave the others as exercises. Let  $y \in f(A_1 \cap A_2)$ . then  $y = f(x)$  for some  $x \in A_1 \cap A_2$ . Since  $x \in A_1 \cap A_2$  if and only if  $x \in A_1$  and  $x \in A_2$ , we have  $y = f(x)$  for some  $x \in A_1$  and  $y = f(x)$  for some  $x \in A_2$ . Therefore,  $y \in f(A_1)$  and  $y \in f(A_2)$ , i.e.  $y \in f(A_1) \cap f(A_2)$ . ■

To see that strict containment can occur in part (b) of Theorem F1, consider the function  $f : \{1, 2, 3\} \rightarrow \{1, 2\}$  where  $f = \{(1, 1), (2, 1), (3, 2)\}$ . Take  $A_1 = \{1, 3\}$  and  $A_2 = \{2, 3\}$ . Then  $f(A_1 \cap A_2) = f(\{3\}) = \{2\}$  whereas  $f(A_1) \cap f(A_2) = \{1, 2\} \cap \{1, 2\} = \{1, 2\}$ .

**Definition (equality of functions).** Two functions  $f : A \rightarrow B$  and  $g : A \rightarrow B$  are *equal* if  $f(x) = g(x)$  for every  $x \in A$ . If  $f$  and  $g$  are equal, we write  $f = g$ .

There is a subtle point hidden in the definition of equality of functions. For two functions to be equal, they must have the same domain, the same codomain, and give the same value for the same input. Thus, technically, the function  $f : \mathbf{Z} \rightarrow \mathbf{Z}$  defined by  $f(x) = |x|$  is not equal to the function  $g : \mathbf{Z} \rightarrow \mathbf{N}$  defined by  $g(x) = |x|$  because these two functions do not have the same codomain.

**Definition (restriction of a function, extension of a function).** Let  $f : A \rightarrow B$  be a function. For  $X \subseteq A$ , the *restriction of  $f$  to  $X$*  is the function  $f|_X : X \rightarrow B$  defined by  $f|_X(x) = f(x)$  for all  $x \in X$ . If  $A' \supseteq A$ , an *extension of  $f$  to  $A'$*  is any function  $g : A' \rightarrow B$  for which  $g(x) = f(x)$  for every  $x \in A$ .

The restriction of a function  $f : A \rightarrow B$  is the new function obtained by restricting the allowed inputs for  $f$  to a subset of its domain  $A$ . An extension of  $f$  is any function that is identical to  $f$  on the inputs in  $A$ , and is also defined for the inputs in  $A' - A$ . Observe that  $f$  can, and probably does, have more than one extension. This is why we say *an* extension, rather than *the* extension. Observe that if  $g$  is an extension of  $f$ , then  $g|_A = f$ .

**Example (restriction).** Let  $f : \mathbf{R} \rightarrow \mathbf{Z}$  be defined by  $f(x) = 2[x] - [x]$ . The restriction  $f|_{\mathbf{Z}}$  of  $f$  to the integers is the function  $f|_{\mathbf{Z}} : \mathbf{Z} \rightarrow \mathbf{Z}$  where  $f|_{\mathbf{Z}}(n) = n$  for all  $n \in \mathbf{Z}$  (because if  $n$  is an integer then  $[x] = [n] = n$ ).

**Counting restrictions and extensions.** Let  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{s, t, u, v, w, x, y, z\}$  and  $f : A \rightarrow B$  be  $f = \{(1, t), (2, x), (3, x), (4, s), (5, t)\}$ . The number of extensions of  $f$  to a function from  $\{1, 2, \dots, 9\}$  to  $B$  is  $8^4$ , since there are 8 choices for the image of each of 6, 7, 8 and 9 (in an extension the images of 1, 2, 3, 4 and 5 must be the same as for  $f$ ). The range of  $f$  is  $R = \{s, t, x\}$ , and the number of subsets  $A' \subseteq A$  such that  $f|_{A'}$  also has range  $R$  is  $1 \cdot 3 \cdot 3$ , since  $A'$  must contain 4 (since  $f^{-1}(\{s\}) = \{4\}$ ), must contain at least one of 1 and 5 (since  $f^{-1}(\{t\}) = \{1, 5\}$ ) must contain at least one of 2 and 3 (since  $f^{-1}(\{x\}) = \{2, 3\}$ ).

**Definition (converse of a relation).** Let  $R$  be a relation from  $A$  to  $B$ . The converse of  $R$  is the relation  $R^c$  from  $B$  to  $A$  defined by  $R^c = \{(b, a) : (a, b) \in R\}$ . (This is the relation obtained by reversing the components of each ordered pair in  $R$ .)

**Motivating question.** Suppose  $f : A \rightarrow B$  is a function. Then, by definition,  $f$  is relation from  $A$  to  $B$ . It is natural to wonder when the converse relation,  $f^c$ , is a function (from  $B$  to  $A$ ).

**Example ( $f^c$  not a function).** Let  $A = \{1, 2, 3\}$ ,  $B = \{a, b, c, d\}$ , and  $f = \{(1, a), (2, b), (3, c)\}$ . Then,  $f^c = \{(a, 1), (b, 2), (c, 3)\}$  is not a function because it contains no ordered pair with first component equal to  $d$ . (Equivalently, the preimage of some 1-element subset of  $B$  is the empty set.) The same situation will arise for any function  $f$  from a set  $A$  to a set  $B$  where the range is a proper subset of the codomain. Hence, for  $f^c$  to have a chance at being a function, it must be true that  $f(A) = B$ . (These are called *onto* functions.)

**Example ( $f^c$  not a function).** Let  $A = \{1, 2, 3\}$ ,  $B = \{a, b\}$ , and  $f = \{(1, a), (2, b), (3, b)\}$ . Then,  $f^c = \{(a, 1), (b, 2), (b, 3)\}$  is not a function because it contains two ordered pairs with first component equal to  $b$ . The same situation will arise for any function  $f$  from a set  $A$  to a set  $B$  where some two elements of  $A$  have the same image. (That is, there exist  $a_1, a_2 \in A$  where  $a_1 \neq a_2$  but  $f(a_1) = f(a_2)$ ). Equivalently, the preimage of some 1-element subset of  $B$  contains two or more elements.) Hence, for  $f^c$  to have a chance at being a function, it must be true that if  $a_1, a_2 \in A$  and  $a_1 \neq a_2$ , then  $f(a_1) \neq f(a_2)$ . (These are called 1-1 functions.)

We will develop some results about the functions with the properties suggested by the two examples above, and after that we will return to the question of when the converse of a function from  $A$  to  $B$  is a function from  $B$  to  $A$ .

**Definition (1-1 function).** A function  $f : A \rightarrow B$  is called *one-to-one* (1-1, or injective, or an injection) if  $f(x) = f(y)$  implies  $x = y$ , for all  $x, y \in A$ . (That is,  $f$  is 1-1 if and only if different elements of  $A$  have different images in  $B$ . Equivalently,  $f$  is 1-1 if and only if every element of  $B$  is the image under  $f$  of at most one element of  $A$ .)

**Proposition F2.** If  $A$  and  $B$  are finite sets and  $f : A \rightarrow B$  is a 1-1 function, then  $|A| \leq |B|$ .

**Proof.**

Suppose  $|A| = m$ . If no two elements of  $A$  have the same image under  $f$ , then the range of  $f$  contains exactly  $m$  elements. Since the range of  $f$  is a subset of  $B$ , we have  $|A| = m \leq |B|$ . ■

**Proving 1-1.** To prove a function  $f$  is 1-1, start with “Assume  $f(x) = f(y)$ .” and then argue, using what you are given about  $f$ , that  $x = y$  (the last clause is ...  $x = y$ . Therefore  $f$  is 1-1.) Equivalently, you could prove the contrapositive: start with “Assume  $x \neq y$ .” and argue until you can conclude with “Then  $f(x) \neq f(y)$ .”.

**Example (proving a function is 1-1).** Let  $f : \mathbf{Z} \rightarrow \mathbf{N}$  be defined by  $f(x) = 5x - 7$ . We prove  $f$  is 1-1. Assume  $f(x) = f(y)$ . Then  $5x - 7 = 5y - 7$ . In turn, this implies  $5x = 5y$  and  $x = y$ . Therefore  $f$  is 1-1.

**Disproving 1-1.** To prove that a function  $f$  is not 1-1, find distinct elements  $x$  and  $y$  in the domain so that  $f(x) = f(y)$ . By doing this, you have demonstrated that the implication  $(f(x) = f(y)) \rightarrow (x = y)$  is False, and so  $f(x) = f(y)$  implies  $x = y$ , for all  $x, y \in A$ , is False.

**Example (proving a function is not 1-1).** Let  $f : \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$  be defined by  $f(1) = 1$ , and for  $n \geq 2$ ,  $f(n)$  is the largest prime factor of  $n$ . Computing a few values of  $f$  yields  $f(2) = 2$ ,  $f(3) = 3$ , and  $f(4) = 2$ . Since  $f(4) = f(2)$  and  $4 \neq 2$ , the function  $f$  is not 1-1.

**Advice about investigating functions re: 1-1.** If it is not possible to easily identify elements  $x$  and  $y$  in the domain so that  $f(x) = f(y)$ , then start trying to prove that  $f$  is 1-1. If  $f$  isn't 1-1, then the proof will break down at some point, and this will lead to the required  $x$  elements. For example, let  $f : \mathbf{R} \rightarrow \mathbf{R}$  be  $f(x) = x^2 - 14x + 57 = (x - 7)^2 + 8$ . Now,  $f(x) = f(y) \Rightarrow (x - 7)^2 + 8 = (y - 7)^2 + 8 \Leftrightarrow (x - 7)^2 = (y - 7)^2$ . To prove  $f$  is

1-1, it is necessary to obtain  $x = y$ , but the last equality gives  $x - 7 = \pm(y - 7)$ , which leads to  $x = y$  or  $y = -x - 14$ . The last of these equations gives the elements  $x$  and  $y$  required to show  $f$  is not 1-1: Choose  $x = 0$  (say) and  $y = -0 - 14 = -14$ . Then  $x \neq y$ , and  $f(x) = 57 = f(y)$  (check the arithmetic!), so  $f$  is not 1-1.

**Counting 1-1 functions.** Suppose  $|A| = m$  and  $|B| = n$ . We count the number of 1-1 functions from  $A$  to  $B$ . By Proposition F2, if  $m > n$  there are none. Assume  $m \leq n$ . Suppose  $A = \{a_1, a_2, \dots, a_m\}$ . There are  $n$  choices for the image of  $a_1$  and, for each of these there are  $n - 1$  choices for the image of  $a_2$ ,  $n - 2$  choices for the image of  $a_3$ , and so on until, finally, there are  $n - (m - 1) = n - m + 1$  choices for the image of  $a_m$ . Thus, by the rule of product, the number of 1-1 functions from  $A$  to  $B$  is  $n(n - 1) \cdots (n - m + 1) = n! / (n - m)!$ .

One to one functions allow us to describe a situation when equality holds in theorem F1 (b).

**Proposition F3.** Let  $f : A \rightarrow B$  be a 1-1 function and  $A_1, A_2 \subseteq A$ . Then  $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ .

**Proof.**

By Theorem F1 (b),  $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$ . Thus, it remains to prove the opposite inclusion. Suppose  $f$  is 1-1, and let  $y \in f(A_1) \cap f(A_2)$ . Then  $y = f(x_1)$  for some  $x_1 \in A_1$  and  $y = f(x_2)$  for some  $x_2 \in A_2$ . Since  $f$  is 1-1,  $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ . Hence,  $y = f(x)$  for some  $x \in A_1 \cap A_2$ , that is,  $y \in f(A_1 \cap A_2)$ . Thus,  $f(A_1 \cap A_2) \supseteq f(A_1) \cap f(A_2)$ , as required. ■

Compare the part of the argument where the property that  $f$  is 1-1 was used to the paragraph following Theorem F1. To see that the converse of Proposition F3 is false, consider  $f : \mathbf{Z} \rightarrow \mathbf{Z}$  where  $f(n) = 0$  for all  $n \in \mathbf{Z}$ .

**Definition (onto function).** A function  $f : A \rightarrow B$  is called *onto* (or surjective, or a surjection) if for every element  $b \in B$  there is an element  $a \in A$  such that  $f(a) = b$ . (That is,  $f$  is onto if and only if every element of  $B$  is the image under  $f$  of some element of  $A$ . Equivalently,  $f$  is onto if and only if every element of  $B$  is the image under  $f$  of at least one element of  $A$ .)

**Proposition F4.** If  $A$  and  $B$  are finite sets and  $f : A \rightarrow B$  is an onto function, then  $|A| \geq |B|$ .

**Proof.**

Suppose  $f$  is onto. Then every element of  $B$  has at least one preimage. By the definition of function, each element of  $A$  is a preimage for a unique element of  $B$ . Thus,  $|A| = \sum_{b \in B} |f^{-1}(\{b\})| \geq \sum_{b \in B} 1 = |B|$ . ■

**Proving onto.** To prove that a function is onto you must argue that for every  $b \in B$  (equivalently, an arbitrarily chosen  $b \in B$ ) there is an  $a \in A$  such that  $f(a) = b$ . Thus, the first line of the proof is “Let  $b \in B$ . We must find  $a \in A$  such that  $f(a) = b$ .”. What you do next depends on the description of  $f$  and of the set  $B$ . Usually, you “solve”  $f(a) = b$  for  $a$  in terms of  $b$  (as written it gives  $b$  in terms of  $a$ ). Then, you verify that what you have is an element of  $A$ . Finally, you substitute this back into  $f$  and show that it gives  $b$ . The last line of the proof is “Hence if  $a = \dots$ , then  $f(a) = \dots = b$ , and so  $f$  is onto.”.

**Example (proving onto).** We show that the function  $f : \mathbf{R}^+ \rightarrow \mathbf{R}^+$  defined by  $f(x) = -9 + (x + 3)^3$  is onto. Let  $y \in \mathbf{R}^+$ . Then  $f(x) = y \Leftrightarrow -9 + (x + 3)^3 = y \Leftrightarrow (x + 3)^3 = y + 9 \Leftrightarrow x + 3 = \pm\sqrt[3]{y + 9}$ . Since  $x \in \mathbf{R}^+$ ,  $x + 3 > 0$  and we can disregard the negative square root to obtain  $x = -3 + \sqrt[3]{y + 9}$ . We must verify that this  $x$  belongs to the domain. Since  $y \in \mathbf{R}^+$  we have  $y + 9 > 9$  and  $\sqrt[3]{y + 9} > 3$ . Therefore  $-3 + \sqrt[3]{y + 9} \in \mathbf{R}^+$ . Hence, if  $x = -3 + \sqrt[3]{y + 9}$ , then  $f(x) = -9 + ((-3 + \sqrt[3]{y + 9}) + 3)^3 = -9 + (\sqrt[3]{y + 9})^3 = y$ , and so  $f$  is onto.

**Disproving onto.** To prove that a function is not onto you must find an element  $b \in B$  which is not  $f(a)$  for any  $a \in A$ . How you do this depends on  $f$ . In general, it is useful to try to prove that  $f$  is onto as above. If it isn't onto, then you will reach a point where either you can't solve for  $a$  in terms of  $b$ , or you will succeed in doing this but the only possibilities you find are not elements of  $A$ . In either case you are done. What you are doing is assuming that  $f$  is onto and showing that leads to (logically implies) a contradiction. Since only a False statement logically implies a contradiction, it must be that the assumption that  $f$  is onto is False.

**Example (disproving onto).** Consider the function  $f : \mathbf{R} \rightarrow \mathbf{R}$  defined by  $f(x) = (x - 2)^2 - 10$ . Let  $y \in \mathbf{R}$ . Then  $f(x) = y \Leftrightarrow (x - 2)^2 - 10 = y \Leftrightarrow (x - 2)^2 = y + 10$ . If  $y$  is chosen so that  $y + 10 < 0$  (say  $y = -11$ ) then there is no real number  $x$  so that  $(x - 2)^2 = y + 10$  because  $(x - 2)^2 \geq 0$  for all real numbers  $x$ . Thus, there is no  $x \in \mathbf{R}$  so that  $f(x) = -11$ , so  $f$  is not onto.

**Example (disproving onto).** Consider the function  $f : \mathbf{Z} \rightarrow \mathbf{Z}$  defined by  $f(n) = 2n + 3$ . Let  $y \in \mathbf{Z}$ . Then  $f(n) = y \Leftrightarrow 2n + 3 = y \Leftrightarrow n = (y - 3)/2$ . But  $(y - 3)/2 \notin \mathbf{Z}$  for all  $y \in \mathbf{Z}$ : In particular if  $y = 0$  then  $(y - 3)/2 = -3/2$ . We now have that if  $f(n) = 0$ , then  $n = -3/2$ . Thus, there is no  $n \in \mathbf{Z}$  such that  $f(n) = 0$ , so  $f$  is not onto.

**Onto depends on the codomain.** Observe that the function  $f$  in the example above is onto as a function from  $\mathbf{R}$  to  $\mathbf{R}$ . **Exercise:** What about from  $\mathbf{Q}$  to  $\mathbf{Q}$ ?

For finite sets  $A$  and  $B$ , it has been straightforward to count the number of functions from  $A$  to  $B$ , and also the number of 1-1 functions from  $A$  to  $B$ . We do not presently have the techniques necessary to count the number of onto functions from  $A$  to  $B$ . This will have to wait until we have covered the Principle of Inclusion and Exclusion, later on. However, we state and use the result now.

**Fact F5.** Let  $A$  and  $B$  be sets with  $|A| = m$  and  $|B| = n$ . Then, the number of onto functions from  $A$  to  $B$  is  $\sum_{k=0}^n (-1)^k \binom{n}{k} (n - k)^m$ .

**Example (counting using onto functions).** We count the number of ways that a collection of 5 labelled (distinguishable) containers can hold a collection of 8 labelled (distinguishable) balls, if no container is left empty. This is the same as the number of functions from the set of balls onto the the set of containers ( $f(b)$  is the container that holds ball  $b$ ), which is  $\sum_{k=0}^5 (-1)^k \binom{5}{k} (5 - k)^8 = \binom{5}{0} 5^8 - \binom{5}{1} 4^8 + \binom{5}{2} 3^8 - \binom{5}{3} 2^8 + \binom{5}{4} 1^8 - \binom{5}{5} 0^8 = 126000$ . The number of ways in which the first 3 containers hold the first 5 balls and the last 2 containers hold the last 3 balls (and, still, no container is left empty) equals the number of functions from a set of 5 labelled balls to the a set of 3 labelled containers, times the

number of functions from a set of 3 labelled balls to the a set of 2 labelled containers. This is  $\left(\sum_{k=0}^3 (-1)^k \binom{3}{k} (3-k)^5\right) \left(\sum_{k=0}^2 (-1)^k \binom{2}{k} (2-k)^3\right) = 864$ .

**Corollary F6.** Let  $A$  and  $B$  be finite sets. If  $f : A \rightarrow B$  is both 1-1 and onto, then  $|A| = |B|$ .

**Proof.**

Since  $f$  is 1-1, we have  $|A| \leq |B|$  by Proposition F2. Since  $f$  is onto, we have  $|A| \geq |B|$  by Proposition F4. The result now follows. ■

**Definition (1-1 correspondence).** A function  $f : A \rightarrow B$  is called a *1-1 correspondence* (or bijective, or a bijection) if it is both 1-1 and onto.

By the definitions of 1-1 and onto, a function  $f$  is a 1-1 correspondence if and only if every element of  $B$  is the image of exactly one element of  $A$  under  $f$ . To determine if a function is a 1-1 correspondence, use the methods discussed above to check whether it is 1-1 and onto. (Of course, you can stop once it fails to have one of these properties.)

Corollary F6 is an important counting principle. It says that if two finite collections of objects can be put into 1-1 correspondence, then there are the same number of objects in each collection. For example, there is a 1-1 correspondence between the subsets of  $A = \{a_1, a_2, \dots, a_n\}$  and the set  $B$  of binary sequences  $b_1 b_2 \dots b_n$  of length  $n$ : It is given by the function  $f : \mathcal{P}(A) \rightarrow B$  defined by  $f(X)$  is the binary sequence  $b_1 b_2 \dots b_n$  where for  $i = 1, 2, \dots, n$ ,

$$b_i = \begin{cases} 1 & \text{if } a_i \in X \\ 0 & \text{if } a_i \notin X. \end{cases}$$

To see that  $f$  is 1-1, note that if  $f(X) = f(Y)$  then the definition of  $f$  implies that  $X$  and  $Y$  contain exactly the same elements. To see that  $f$  is onto, let  $b_1 b_2 \dots b_n \in B$  and construct  $X \in \mathcal{P}(A)$  by the rule  $a_i \in X \Leftrightarrow b_i = 1$ . It follows from the definition of  $f$  that  $f(X) = b_1 b_2 \dots b_n$ . Hence, the number of subsets of  $A$  equals the number of binary sequences of length  $n$ , which equals  $2^n$  (two choices for each position).

**Exercises.** Suppose that  $|A| = |B|$ . Prove:

- (a) If  $f : A \rightarrow B$  is a 1-1 function, then it is a 1-1 correspondence (i.e.  $f$  is also onto).
- (b) If  $f : A \rightarrow B$  is an onto function, then it is a 1-1 correspondence (i.e.  $f$  is also 1-1).

**Proposition F7.** Let  $f : A \rightarrow B$  be a function.

- (a) If  $f$  is 1-1, then any restriction of  $f$  to a subset  $A_1 \subseteq A$  is 1-1.
- (b) If  $f$  is onto, then for any  $A' \supseteq A$ , any extension of  $f$  to a function  $g : A' \rightarrow B$  is onto.

**Proof.**

(a): Let  $x, y \in A_1$  and suppose  $f(x) = f(y)$ . Since  $A_1 \subseteq A$ , we have  $x, y \in A$ . Since  $f$  is 1-1,  $f(x) = f(y)$ . Therefore  $f|_{A_1}$  is 1-1.

(b): Let  $b \in B$ . Since  $f$  is onto, there exists  $x \in A$  such that  $f(x) = b$ . ■

**Definition (composition of functions).** Let  $A, B$  and  $C$  be sets, and  $f : A \rightarrow B$  and  $g : B \rightarrow C$  be functions. The *composition of  $f$  and  $g$*  (or the composite function) is the function  $(g \circ f) : A \rightarrow C$  defined by

$(g \circ f)(a) = g(f(a))$  for every element  $a$  in  $A$ .

**Function composition is not commutative.** In general, order matters. For  $f$  and  $g$  as above, the composition of  $f$  and  $g$  is usually not the same as the composition of  $g$  and  $f$ . For example, let  $f : \mathbf{Z} \rightarrow \mathbf{Z}$  be defined by  $f(x) = x^2$  and  $g : \mathbf{Z} \rightarrow \mathbf{Z}$  be defined by  $g(x) = x + 3$ . Then,

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 3$$

and

$$(f \circ g)(x) = f(g(x)) = f(x + 3) = (x + 3)^2 = x^2 + 6x + 9.$$

Since  $(g \circ f)(0) = 3$  and  $(f \circ g)(0) = 9$ , we have  $g \circ f \neq f \circ g$ . It is also possible that, depending on the sets  $A, B$  and  $C$ , the function  $g \circ f$  is defined but the function  $f \circ g$  is not. We leave it as an **exercise** to find an example that demonstrates this.

**Definition (identity function on a set).** The *identity function on the set  $X$*  is the function  $1_X : X \rightarrow X$  defined by  $1_X(x) = x$  for every element  $x$  of  $X$ .

The integer 0 is an identity element with respect to addition of real numbers:  $x + 0 = 0 + x = x$  for all  $x \in \mathbf{R}$ . Similarly, 1 is an identity with respect to multiplication of nonzero real numbers:  $1 \cdot x = x \cdot 1 = x$  for all  $x \in \mathbf{R} - \{0\}$ . The identity function on a set acts in a similar way with respect to function composition.

**Proposition F8.** Let  $A$  and  $B$  be sets and  $f : A \rightarrow B$  be a function. Then

- (a)  $f \circ 1_A = f$ , and
- (b)  $1_B \circ f = f$ .

**Proof.**

We prove (a) and leave (b) as an **exercise**. Let  $x \in A$ . Then,  $f \circ 1_A(x) = f(1_A(x)) = f(x)$ . Hence,  $f \circ 1_A = f$ . ■

Even though function composition is not commutative, it is associative. We now prove this.

**Proposition F9.** Let  $A, B, C$ , and  $D$  be sets and  $f : A \rightarrow B$ ,  $g : B \rightarrow C$ , and  $h : C \rightarrow D$  be functions. Then  $h \circ (g \circ f) = (h \circ g) \circ f$ .

**Proof.**

By definition of function composition, both  $h \circ (g \circ f)$  and  $(h \circ g) \circ f$  are functions from  $A$  to  $D$ , so they have the same domain and codomain. Let  $x \in A$ . Then,

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x),$$

as required. ■

**Proposition F10.** Let  $A, B$  and  $C$  be sets and  $g : A \rightarrow B$  and  $f : B \rightarrow C$  be functions. Then,

- (a) If  $f$  and  $g$  are 1-1, then  $g \circ f$  is 1-1.
- (b) If  $f$  and  $g$  are onto, then  $g \circ f$  is onto.
- (c) If  $f$  and  $g$  are 1-1 correspondences, then  $g \circ f$  is a 1-1 correspondence.

**Proof.**

We prove (a) and leave the proof of (b) for an exercise. Statement (c) is an immediate consequence of (a) and (b).

Suppose  $(g \circ f)(x) = (g \circ f)(y)$ . Then  $g(f(x)) = g(f(y))$ . Since  $g$  is 1-1,  $f(x) = f(y)$ . Since  $f$  is 1-1,  $x = y$ . therefore,  $g \circ f$  is 1-1. ■

**Exercises:** find examples to demonstrate that the converse of each statement in proposition F10 is false, but the following statement is true: If  $f \circ g$  is a 1-1 correspondence, then  $f$  is 1-1 and  $g$  is onto (but  $f$  need not be onto and  $g$  need not be 1-1). Also, find an example to demonstrate that the converse of the above implication is False (never mind the part in brackets).

We now return to the question of when the converse of a function is itself a function.

**Proposition F11.** Let  $f : A \rightarrow B$  be a function. Then  $f^c$  is a function if and only if  $f$  is 1-1 and onto.

**Proof.**

( $\Rightarrow$ ) Suppose  $f^c$  is a function. By the definition of function, for every  $b \in B$   $f^c$  contains exactly one ordered pair with first component equal to  $b$ . Thus, for every  $b \in B$   $f$  contains exactly one ordered pair with second component equal to  $b$ . That is,  $f$  is 1-1 and onto.

( $\Leftarrow$ ) Suppose  $f$  is 1-1 and onto. Then, for every  $b \in B$   $f$  contains exactly one ordered pair with second component equal to  $b$ . This means that for every  $b \in B$   $f^c$  contains exactly one ordered pair with first component equal to  $b$ . That is,  $f^c$  is a function. ■

Suppose  $f$  is a 1-1 and onto function. Then, by Proposition F11,  $f^c$  is a function. Since  $(f^c)^c = f$  and  $f$  is a function, Proposition F11 implies that the function  $f^c$  is (also) 1-1 and onto.

In the arithmetic of real numbers, the inverse of  $x$  is  $-x$  because  $x + (-x)$  equals the additive identity, zero. For  $x \neq 0$ , the multiplicative inverse of  $x$  is  $1/x$  because  $x \cdot (1/x)$  equals the multiplicative identity, one. The inverse of a function is analogous, and is defined below.

**Definition (invertible function).** A function  $f : A \rightarrow B$  is called *invertible* if there exists a function  $g : B \rightarrow A$  such that  $g \circ f = 1_A$  and  $f \circ g = 1_B$ .

Suppose  $f : A \rightarrow B$  is a 1-1 correspondence. Then, by Proposition F11,  $f^c$  is a function. Consider the composite function  $f^c \circ f$ . For  $a \in A$  we have  $(f^c \circ f)(a) = f^c(f(a)) = a$ , by definition of converse. Thus,  $f^c \circ f = 1_A$ . Similarly, for  $b \in B$  we have  $(f \circ f^c)(b) = f^c(f(b)) = b$ . Thus,  $f \circ f^c = 1_B$ . Therefore, a 1-1 and onto function is invertible.

**Proposition F12.** Suppose  $f : A \rightarrow B$  is invertible. Then the function  $g$  such that  $g \circ f = 1_A$  and  $f \circ g = 1_B$  is unique.

**Proof.** Suppose  $g : B \rightarrow A$  and  $h : B \rightarrow A$  are functions such that  $g \circ f = 1_A$  and  $f \circ g = 1_B$  and  $h \circ f = 1_A$  and  $f \circ h = 1_B$ . We need to show  $g = h$ . Let  $b \in B$ . Then  $g(b) = g(1_B(b)) = (g \circ 1_B)(b) = (g \circ (f \circ h))(b) = ((g \circ f) \circ h)(b) = (1_A \circ h)(b) = 1_A(h(b)) = h(b)$ . Thus,  $g = h$ . This completes the proof. ■

**Definition (inverse).** Let  $f : A \rightarrow B$  be an invertible function. The *inverse of  $f$*  is the unique function  $g$  such that  $g \circ f = 1_A$  and  $f \circ g = 1_B$ . It is customary to denote the inverse of  $f$  by  $f^{-1}$ .

In the case where  $f : A \rightarrow B$  is 1-1 and onto, we have above that  $f$  is invertible and  $f^c = f^{-1}$ .

Do not confuse the notation for the inverse of a function, (which exists only sometimes) and the notation for the preimage of a subset of the codomain (which always exists). They use the same symbols, but the former of these is a function and the latter is a set. It should be clear from the context which object is under discussion.

**Proposition F13.** Let  $f : A \rightarrow B$  be a function. Then,  $f$  is invertible if and only if it is 1-1 and onto.

**Proof.**

( $\Leftarrow$ ) Suppose  $f$  is 1-1 and onto. We have noted above that in this case  $f$  is invertible and  $f^c = f^{-1}$ .

( $\Rightarrow$ ) Suppose that  $f$  is invertible. Then, there is a function  $f^{-1} : B \rightarrow A$  such that  $f^{-1} \circ f = 1_A$  and  $f \circ f^{-1} = 1_B$ .

Suppose  $f(x) = f(y)$ . Then  $f^{-1}(f(x)) = f^{-1}(f(y))$ . The LHS of this equation is  $(f^{-1} \circ f)(x) = 1_A(x) = x$  and the RHS is  $(f^{-1} \circ f)(y) = 1_A(y) = y$ . Thus,  $x = y$ , and  $f$  is 1-1.

Let  $b \in B$ . Since  $f^{-1}$  is a function, there exists  $a \in A$  such that  $f^{-1}(b) = a$ . By definition of inverse function, we have  $f(a) = f(f^{-1}(b)) = (f \circ f^{-1})(b) = 1_B(b) = b$ . Therefore  $f$  is onto. This completes the proof. ■

Combining Propositions F12 and F13 gives that if  $f$  is an invertible function, then  $f^{-1} = f^c$ . By definition of converse, this means that  $f^{-1}$  has the property that, for  $a \in A$  and  $b \in B$ ,  $f(a) = b \Leftrightarrow f^{-1}(b) = a$ . (Compare this to the last paragraph in the proof of Proposition F13.) Some (inverse) functions are defined in exactly this way – for example for  $x \in \mathbf{R}^+$  and  $y \in \mathbf{R}$ , we have  $\log_{10}(x) = y \Leftrightarrow 10^y = x$

**Proving  $f$  is invertible and finding the inverse.** There are two ways to prove that a function  $f : A \rightarrow B$  is invertible. One way is to write down the right function  $g : B \rightarrow A$  and then check that  $g \circ f = 1_A$  and  $f \circ g = 1_B$ . Another way is to use Proposition F13 and check if  $f$  is 1-1 and onto. In the proof that  $f$  is onto, one starts with "Let  $y \in B$  and suppose  $f(x) = y$ ." and ultimately derives "Then  $x = g(y)$ ." By our discussion in the previous paragraph,  $g$  is the inverse function. Thus, a description of the inverse function is a byproduct of the proof that  $f$  is onto.

Notice that the definition of an invertible function is symmetric in  $f$  and  $g$  (a.k.a.  $f^{-1}$ ). Thus, if  $f$  is invertible, so is  $f^{-1}$  and  $(f^{-1})^{-1} = f$ .

**Example (proving  $f$  is invertible and finding  $f^{-1}$ ).** Let  $f : \mathbf{R}^+ \rightarrow \mathbf{R}$  be defined by  $f(x) = 2\ln(x) - 7$ . We show that  $f$  is invertible and find  $f^{-1}$ . Suppose  $f(a) = f(b)$ . Then, we have  $2\ln(a) - 7 = 2\ln(b) - 7 \Leftrightarrow 2\ln(a) = 2\ln(b) \Leftrightarrow \ln(a) = \ln(b) \Leftrightarrow e^{\ln(a)} = e^{\ln(b)} \Leftrightarrow a = b$ , since the exponential and logarithm functions are inverses. Thus,  $f$  is 1-1. Now, suppose  $y \in \mathbf{R}$ . Then,  $f(x) = y \Leftrightarrow 2\ln(x) - 7 = y \Leftrightarrow \ln(x) = (y + 7)/2 \Leftrightarrow x = e^{(y+7)/2}$ . For  $y \in \mathbf{R}$  the quantity  $e^{(y+7)/2} \in \mathbf{R}^+$ , the domain of  $f$ . Hence, if  $x = e^{(y+7)/2}$  then  $f(x) = f(e^{(y+7)/2}) = 2\ln(e^{(y+7)/2}) - 7 = 2(y + 7)/2 - 7 = y$ , so  $f$  is onto. Moreover  $f^{-1} : \mathbf{R} \rightarrow \mathbf{R}^+$  is described by  $f^{-1}(y) = e^{(y+7)/2}$ .