Mathematical Logic:

Some mathematical statements carry a logical value of being true or false, while some do not. For example, the statement "4+5 = 9" is true, whereas the statement "2 is odd" is false. However, a statement like "$x^2 - 2x = 15$" is neither true nor false, until further information is given concerning x.

Definition: By a truth value we mean a logical value of true or false. A statement which possesses a truth value is called a proposition. Technically, of course, a proposition can be stated in any language, not necessarily mathematical; the only requirement is that the statement must be quantifiable as being true or false.

This leads to the algebra of **Boolean logic**, in which we are dealing with entities whose values can either be 0 (false) or 1 (true). In fact, this reminds us of the binary number system and the underlying structure (on/off switches) of computing machines.

Propositional Logic:

As with numbers, we now treat propositions as mathematical quantities, which can be operated one on another by a selection of proposition operators, or logic operators. The first and simplest operator is analogous to taking the negative of a number.

Definition: Let p denote a proposition. The negation of p is the proposition given by the statement "not p" and whose value is opposite that of p. The negation of p can simply be called not p and is denoted by $\neg p$.

Example: We give two propositions, one in mathematics and another in English, each with its negation.

p : 4 + 5 = 9 q : The earth is flat.
$\neg p$: 4 + 5 6= 9 $\neg q$: The earth is not flat.

Note that each proposition has the opposite truth value from that of its negation; If p is true then $\neg p$ is false, and vice versa.

Logic Operators and Truth Tables

A logic operator can be given by a table which displays the output value for every possible combination of the input values. The truth table for The negation operator, for instance, is given below.

Table 1: Truth table for $\neg$p.

p	$\neg p$
T	F
F	T

A number of logic operators will now be given by their truth tables. In general, the resulting proposition obtained by applying these operators will be called a ***compound proposition*.**

Definition: Let p and q be two propositions. The conjunction p ∧ q and disjunction p ∨ q yield the compound statements p and q, respectively, p or q, and whose values are given according to the following table.

Table 2: Truth tables for p ∧ q and p ∨ q.

p	q	$p \wedge q$	$p \vee q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Example: Suppose p : 4+5 = 9 and q : 2 is odd. Write the statement and find the value of the compound proposition (a) $\neg$p ∧ q (b) p ∨ $\neg$q.

Solution. Note that p has value true and q false. The first statement is false (F ∧ F) and the second true (T ∨ T), and they are given by:

a) $\neg$p ∧ q : 4 + 5 6= 9 and 2 is odd

b) p ∨ $\neg$q : 4 + 5 = 9 or 2 is not odd

Exercise: Suppose p is true and q is false. Determine true or false for each compound proposition below.

a) $\neg p \lor \neg q$

b) $(p \land \neg q) \lor \neg p$

c) $(p \land q) \lor (\neg p \land \neg q)$

d) $(\neg p \lor (q \lor p)) \land (p \land q)$

Example: Construct a truth table to determine the possible output values of the compound proposition given by $(p \lor \neg q) \land (\neg p \lor q)$.

Solution: There are four possible rows. We show the intermediate steps according to the order in which the logic operations apply, as follows.

p	q	$\neg p$	$\neg q$	$p \lor \neg q$	$\neg p \lor q$	$(p \lor \neg q) \land (\neg p \lor q)$
T	T	F	F	T	T	T
T	F	F	T	T	F	F
F	T	T	F	F	T	F
F	F	T	T	T	T	T

Exercise: Construct the truth table for each given compound proposition.

a) $\neg(\neg p \land \neg q)$

b) $\neg p \lor (p \land \neg q)$

c) $(p \land \neg q) \lor (\neg p \lor q)$

d) $(p \lor q) \land (\neg p \land \neg q)$

Definition: The implication $p \rightarrow q$ yields a compound proposition whose truth value is given in Table 3. The statement $p \rightarrow q$ is read if p then q, or sometimes, p implies q. Implication is also called the if-then operator.

Table 3: Truth table for $p \rightarrow q$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Exercise: Suppose $p : 4 + 5 = 9$ and $q : 2$ is odd. Write the statement and determine the value of each compound proposition below.

a) $p \rightarrow q$

b) $q \to p$

c) $\neg p \to q$

d) $\neg q \to \neg p$

Example. Construct the truth table for the proposition $(p \to q) \to r$.

Solution. This is the first time we see a compound proposition involving three propositional variables. The first three columns of the next table show the standard ordering for the eight possibilities of the values of (p, q, r).

p	q	r	$p \to q$	$(p \to q) \to r$
T	T	T	T	T
T	T	F	T	F
T	F	T	F	T
T	F	F	F	T
F	T	T	T	T
F	T	F	T	F
F	F	T	T	T
F	F	F	T	F

Exercise: Construct the truth table for each given compound proposition.

a) $\neg q \to \neg p$

b) $(p \wedge q) \to (p \vee q)$

c) $(p \vee q) \to r$

d) $(\neg p \to q) \wedge (\neg p \to r)$

Definition: The compound propositions $p \leftrightarrow q$ (read p if and only if q, orp iff q) and $p \oplus q$ (read p exclusive or q, or p xor q) are given by their truthtables, respectively, next.

Table 4 Truth tables for $p \leftrightarrow q$ and $p \oplus q$

p	q	$p \leftrightarrow q$	$p \oplus q$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	T	F

In the English language, the exclusive or is often translated p or q but not both, since the table shows that $p \oplus q$ is true when exactly one of them is true, not both. Moreover, a proposition of the form $p \leftrightarrow q$ is called a biconditional statement, and is used to connect two statements whose truth values are the same, i.e., p is true if q is true, and p is false if q is false. Note that these two compound propositions have opposite values for each pair (p,q). To help remember, $p \leftrightarrow q$ is true exclusively when p and q have identical values, whereas $p \oplus q$ is true exactly when p and q have unequal truth-values.

Exercise Suppose that we have the following propositions.

p : It is hot today.
q : It is windy today.
r : It will rain tomorrow.

Translate the following sentences using the variables p, q, r, and the appropriate logic operators.
a) If today is hot and windy, then it will rain tomorrow.
b) Tomorrow will rain if and only if today is not windy.
c) Either today is hot or tomorrow will rain, but not both.
d) If today is neither hot nor windy, then it will not rain tomorrow.

Exercise Construct the truth table for each given compound proposition.

a) $(p \leftrightarrow q) \wedge (p \oplus q)$
b) $(p \leftrightarrow \neg q) \rightarrow (\neg p \oplus \neg q)$
c) $(p \oplus q) \oplus r$
d) $[(\neg p \wedge q) \vee (\neg r \rightarrow p)] \leftrightarrow (r \oplus \neg q)$

Tautology and Contradiction:

Definition: A **tautology** is a compound proposition whose truth table consists of all true values.

Consider the compound proposition $(p \wedge q) \rightarrow p$, whose truth table, displayed below, happens to show all true values. This is an example of a tautology.

p	q	$p \wedge q$	$(p \wedge q) \to p$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

Definition. The counterpart of a tautology is a **contradiction**, i.e., a compound proposition that shows all false values in the truth table.

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

(a) $p \vee \neg p$

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

(b) $p \wedge \neg p$

Note that the negation of a tautology is a contradiction since it is always false, and the negation of a contradiction is a tautology since it is always true.

Incidentally, a compound proposition whose table contains a mix of true and false, like most that we have seen thus far, is called a contingency.

Exercise Identify each compound proposition as a tautology, contradiction, or contingency.

a) $p \to (p \vee q)$
b) $(p \to q) \to q$
c) $(p \leftrightarrow q) \wedge (p \oplus q)$
d) $(p \leftrightarrow \neg q) \to (\neg p \oplus \neg q)$

Definition. By a *premise* we mean a proposition whose value is assumed true. An *argument* is a set of premises $P_1, P_2, \ldots, P_k$, together with another proposition Q which serves as the *conclusion*. The argument is said to be *valid* when the proposition $(P_1 \wedge P_2 \wedge \cdots \wedge P_k) \to Q$ is a tautology.

Example. Assume the following two premises.

P1 : Tomorrow is not Friday.
P2 : If today is not Sunday then tomorrow is Friday.

Therefore, we claim the following conclusion.

Q : Today is Sunday.

Is the above argument valid?

Solution. Let us fix the following propositions.

p : Today is Sunday.
q : Tomorrow is Friday.

The two premises and the conclusion are then represented by, respectively,

P1 : $\neg q$
P2 : $\neg p \to q$
Q : p

We need now study the truth table of the compound proposition

$$(P1 \wedge P2) \to Q : (\neg q \wedge (\neg p \to q)) \to p$$

given below.

p	q	$\neg p$	$\neg q$	$\neg p \to q$	$\neg q \wedge (\neg p \to q)$	$(\neg q \wedge (\neg p \to q)) \to p$
T	T	F	F	T	F	T
T	F	F	T	T	T	T
F	T	T	F	T	F	T
F	F	T	T	F	F	T

The table shows that $(P1 \wedge P2) \to Q$ is indeed a tautology, establishing the validity of the argument.

Example. Assume that every even number is composite. Can we conclude that all odd numbers are prime?

Solution. Let p denote the statement “n is even” and q the statement “n is composite.” Note that the premise is given by $p \to q$, and the conclusion $\neg p \to \neg q$. We look at the truth table, and find a contingency. Hence, the argument is not valid.

p	q	$p \to q$	$\neg p$	$\neg q$	$\neg p \to \neg q$	$(p \to q) \to (\neg p \to \neg q)$
T	T	T	F	F	T	T
T	F	F	F	T	T	T
F	T	T	T	F	F	F
F	F	T	T	T	T	T

Exercise Determine the validity of each given argument.
a) Premises: Today is not Sunday. Today is Sunday if and only if tomorrow is Tuesday. Conclusion: Tomorrow is not Tuesday.
b) Premises: If you like Discrete Mathematics, you will like Calculus. You like neither Discrete Mathematics nor Calculus. Conclusion: If you like Calculus, you will like Discrete Mathematics.
c) Premises: If n is even then n is composite. If n is prime then 2n + 1 is also prime. Conclusion: If 2n + 1 is composite then either n is prime or odd.
d) Premises: Either prime numbers are infinitely many or composites are, but not both. There are infinitely many primes. If composites are finitely many, so are even numbers. Conclusion: Both composites and even numbers are finitely many.

Logical Equivalence

Sometimes it may well be the case that two compound propositions have look-alike truth tables. Can you see, for instance, why the table for $p \oplus q$ is no different that that for $\neg(p \leftrightarrow q)$? Such a relation between two propositions is an important concept and shall be given a special name

Definition. Two propositions are called equivalent to each other if their truth tables are identical. We employ the symbol $\equiv$ to denote this relation. Hence, for example, we have $\neg(p \leftrightarrow q) \equiv p \oplus q$.

Example. Prove the relation $p \to q \equiv \neg p \vee q$.

Solution. We have to create the two tables and arrive at the same results.
To save some space, we will juxtapose the two tables into one as follows.

p	q	$p \to q$	$\neg p$	$\neg p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Note that both final columns show identical entries, justifying the equivalence between the two propositions.

Exercise Verify the equivalence in each of the following statements.

a) $\neg p \wedge q \equiv \neg(p \vee \neg q)$

b) $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

c) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

d) $p \to (q \to r) \equiv q \to (p \to r)$

Exercise Prove that all of the following compound propositions are equivalent one to another.

a) $p \to \neg q$

b) $q \to \neg p$

c) $\neg p \vee \neg q$

d) $\neg(p \wedge q)$

The following theorem lists a few conditional statements which are rather well-known tautologies. They can be used as models for a valid argument, and are sometimes refered to as rules of inference.

Theorem 1. Each of the following propositions is a tautology.

$(p \wedge q) \to p$ $p \to (p \vee q)$

$\neg p \to (p \to q)$ $\neg(p \to q) \to p$

$(p \wedge (p \to q)) \to q$ $(\neg q \wedge (p \to q)) \to \neg p$

$(\neg p \wedge (p \vee q)) \to q$ $((p \to q) \wedge (q \to r)) \to (p \to r)$

Theorem 2. An implication is always equivalent to its contrapositive.

Proof. We show the equivalence $p \to q \equiv \neg q \to \neg p$ by simply producing their respective tables below.

p	q	$p \to q$	$\neg q$	$\neg p$	$\neg q \to \neg p$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

z

Laws of Algebra of Propositions

Identity:

$p \vee p \equiv p$	$p \wedge p \equiv p$	$p \to p \equiv T$	$p \leftrightarrow p \equiv T$
$p \vee T \equiv T$	$p \wedge T \equiv p$	$p \to T \equiv T$	$p \leftrightarrow T \equiv p$
$p \vee F \equiv p$	$p \wedge F \equiv F$	$p \to F \equiv \sim p$	$p \leftrightarrow F \equiv \sim p$
		$T \to p \equiv p$	
		$F \to p \equiv T$	

Commutative:

$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$	$p \to q \neq q \to p$	$p \leftrightarrow q \equiv q \leftrightarrow p$

Complement:

$p \vee \sim p \equiv T$	$p \wedge \sim p \equiv F$	$p \to \sim p \equiv \sim p$	$p \leftrightarrow \sim p \equiv F$
		$\sim p \to p \equiv p$	

Double Negation:

$\sim(\sim p) \equiv p$

Associative:

$p \vee (q \vee r) \equiv (p \vee q) \vee r$

$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

Distributive:

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

De Morgan's:

$\sim(p \vee q) \equiv \sim p \wedge \sim q$

$\sim(p \wedge q) \equiv \sim p \vee \sim q$

Equivalence of Contrapositive:

$p \rightarrow q \equiv \sim q \rightarrow \sim p$

Others:

$p \rightarrow q \equiv \sim p \vee q$

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Techniques of Proof

Proving a mathematical statement is an art of writing. There is no strict convention as to how a proof should look like. However, there are commonly accepted methods of proof, which follow certain laws of logic. We look into a few of these methods, trying wherever possible to communicate in the language of propositions as we have learned it.

Direct Proof and Contrapositive

We will use these numbers to illustrate our first proof technique, called **direct proof**. The technique of direct proof applies to statements in the form of an implication $\mathbf{p \rightarrow q}$. It begins by assuming p and shows, through a succession of implications, that q inevitably follows.

Rules for Direct Proofs

1) From an example x that does not satisfy $p(x)$, we may conclude $\neg p(x)$.

2) From $p(x)$ and $q(x)$, we may conclude $p(x) \wedge q(x)$.

3) From either $p(x)$ or $q(x)$, we may conclude $p(x) \vee q(x)$.

4) From either $q(x)$ or $\neg p(x)$ we may conclude $p(x) \Rightarrow q(x)$.

5) From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$ we may conclude $p(x) \Leftrightarrow q(x)$.

6) From $p(x)$ and $p(x) \Rightarrow q(x)$ we may conclude $q(x)$.

7) From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow r(x)$ we may conclude $p(x) \Rightarrow r(x)$.

8) If we can derive $q(x)$ from the hypothesis that x satisfies $p(x)$, then we may conclude $p(x) \Rightarrow q(x)$.

9) If we can derive $p(x)$ from the hypothesis that x is a (generic) member of our universe U, we may conclude $\forall x \in U(p(x))$.

(Proof by Contraposition) *The statement $p \Rightarrow q$ and the statement $\neg q \Rightarrow \neg p$ are equivalent, and so a proof of one is a proof of the other.*
The statement $\neg q \Rightarrow \neg p$ is called the *contrapositive* of the statement $p \Rightarrow q$. The following example demonstrates the utility of the principle of proof by contraposition.

Lemma *If n is a positive integer with $n^2 > 100$, then $n > 10$.*

Proof: Suppose n is not greater than 10. (Now we use the rule of algebra for inequalities which says that if $x \leq y$ and $c \geq 0$, then $cx \leq cy$.)
Then since $1 \leq n \leq 10$,

$$n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100.$$

Thus n^2 is not greater than 100. Therefore, if n is not greater than 10, n^2 is not greater than 100. proof by contraposition, if $n^2 > 100$, n must be greater than 10.

We adopt Principle rule of inference, called the *contrapositive* rule of inference.

From $\neg q(x) \Rightarrow \neg p(x)$ we may conclude $p(x) \Rightarrow q(x)$.

Example(1): Prove that if x is even then x^2 is also even.

Solution: If we let p denote the statement "x is even" and q the statement "x^2 is even," then we are to prove the proposition $p \to q$.

p : x is even
$\to x = 2n$ for some $n \in Z$ (definition of even numbers)
$\to x^2 = 4n^2$ (by squaring both sides)
$\to x^2 = 2m$ where $m = 2n^2 \in Z$ (since n is integer)
$\to x^2$ is even : q (by definition)

Example(2): Prove that the product of two odd numbers is again odd.

Solution: This statement does not look like an implication, but it really is. Simply let p : x and y are odd and q : xy is odd. The proposition to be proved is essentially $p \to q$.

p : x and y are odd
$\to x = 2n + 1$ and $y = 2m + 1$ with both $m, n \in Z$
$\to xy = (2n + 1)(2m + 1)$
$\to xy = 4nm + 2n + 2m + 1$
$\to xy = 2(2nm + n + m) + 1$
$\to xy = 2k + 1$ where $k = 2nm + n + m \in Z$
$\to$ xy is odd : q

Exercise:
Prove the following statements using direct proof.
a) If x is odd, then x3 is also odd.
b) If x is even, then so is $x^2 - 4x + 2$.
c) The sum of two odd numbers is even.
d) The sum of two rational numbers is again rational.

There are times when direct proof may not be the easiest way to establish $p \to q$. In such cases, the contrapositive of this implication is often a useful substitute for the statement before we attempt to prove it. If you recall, **Theorem 2** states that:
$p \to q \equiv \neg q \to \neg p$

Example(3): Let x be an integer. Prove that if x2 is even then so is x.

Solution. As before, we let p : x2 is even and q : x is even. We wish to prove the validity of $p \rightarrow q$. Direct proof would start with $x^2 = 2n$ and have us show that $x = \sqrt{2n}$ is twice an integer. That would be hard. To circumvent this difficulty, we shall instead prove the equivalent statement $\neg q \rightarrow \neg p$.

$\neg q$: x is odd (the integer x is not even)
$\rightarrow x = 2n + 1$ for some $n \in Z$
$\rightarrow x^2 = 4n^2 + 4n + 1$
$\rightarrow x^2 = 2(2n^2 + 2n) + 1$
$\rightarrow x^2 = 2m + 1$ where $m = 2n^2 + 2n \in Z$
$\rightarrow x^2$ is odd : $\neg p$

At this point it is appropriate to remark that writing a mathematical proof need not be so formal as to represent every statement using p and q. The next example is simply meant to show how our writing style can be more casual for the sake of better readability.

Example(4): Prove that if 2n is an irrational number, then n is too.

Solution. We use contrapositive. Suppose that n is rational. We may write n = a/b for some integers a, b. Then 2n = 2a/b, which shows that 2n is also a rational number. This completes the proof.

Exercise: Prove the following statements using contrapositive.
a) If x^3 is odd, then x is also odd.
b) If $x^2 - 3$ is irrational, so is $x - 3$.
c) If the sum of two integers is odd, then one of them is odd.
d) If the product of two integers is even, then one of them is even.

<u>Mathematical Induction</u>

The technique of mathematical induction applies to a statement involving a predicate and the quantifier ∀ with the domain of positive integers. For example, consider the statement

$1 + 2 + 3 + \cdot \cdot \cdot + n = \frac{n(n+1)}{2}$

for all n ∈ N

Here, the predicate P(n) : 1+2+3+ ・ ・ ・+n = $\frac{n(n+1)}{2}$

claims to hold for all integer values of n ≥ 1. How do we prove such a statement? We need only establish the following two propositions.

1) P(1)

2) P(n) → P(n + 1)

Intuitively, the second statement, with n = 1 says that if P(1) holds, so does P(2). Since P(1) holds, i.e., by (1), then P(2) is true. But by (2) again, since P(2) is true, so is P(3). And again, P(3) implies P(4), then P(5), and on for all P(n), where n ∈ N. Proving (2) is what we call the ***induction step***.

Example 1: Let P be the proposition that the sum of the first n odd numbers Is n^2; that is,

$$P(n): 1 + 3 + 5 + \dots + (2n - 1) = n^2$$

Prove P (for n ≥ 1)

Solution: (The nth odd number is 2n – 1, and the next odd number is 2n +1.) Observe that P(n) is true for n = 1,

(i) n=1; P(1): 2*n-1 = 1^2

(ii) n=k; Assuming P(k) is true,

We add (2k-1)+2 = 2K + 1 to both sides of P(k), obtaining:

$$1 + 3 + 5 + \dots + (2k - 1) + (2k + 1) = k^2 + (2k + 1)$$
$$= (k + 1)^2$$

Which is P(k + 1). That is, P(k + 1) is true whenever P(k) is true. By the principle of mathematical induction, P is true for all n ≥.k.

Example(2). Prove that the identity 1+2+3+ ・ ・ ・+n =$\frac{n(n+1)}{2}$ holds for all integers n ≥ 1.

Solution: We let P(n) denote this predicate,

P(n) : 1 + 2 + 3 + ・ ・ ・ + n =$\frac{n(n+1)}{2}$

The statement we are to prove can be represented by ∀n ≥ 1 : P(n). Note that P(5), for instance, stands for the proposition 1+2+3+4+5 = $\frac{5(5+1)}{2}$, whose value is true. This is just an example. We proceed with the two parts of the proof.

1) P(1) is the proposition 1 = [1(1+1)]/2 Obviously then, P(1) is true.

2) Using direct proof, we will show $P(n) \to P(n+1)$. Note first the statement $P(n+1): 1+2+3+\cdots+(n+1) = \frac{(n+1)(n+2)}{2}$, as we proceed.

$$
\begin{aligned}
P(n): 1+2+3+\cdots+n &= \frac{n(n+1)}{2} \\
\to 1+2+3+\cdots+n+(n+1) &= \frac{n(n+1)}{2} + (n+1) \\
\to 1+2+3+\cdots+n+(n+1) &= \frac{n(n+1)+2(n+1)}{2} \\
\to 1+2+3+\cdots+n+(n+1) &= \frac{n^2+3n+2}{2} \\
\to 1+2+3+\cdots+n+(n+1) &= \frac{(n+1)(n+2)}{2} \\
\to P(n+1) &
\end{aligned}
$$

Example 3:

Prove the following proposition (for $n \geq 0$):

$$P(n): 1 + 2 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 1$$

solution :

(i) P(0) : left side =1

Right side $=2^1-1=1$

(ii) Assuming P(k) is true ; n=k

$$P(k): 1 + 2 + 2^2 + 2^3 + \ldots + 2^k = 2^{k+1} - 1$$

We add 2k+1 to both sides of P(k), obtaining

$$
\begin{aligned}
1 + 2 + 2^2 + 2^3 + \ldots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} \\
&= 2(2^{k+1}) - 1 = 2^{k+2} - 1
\end{aligned}
$$

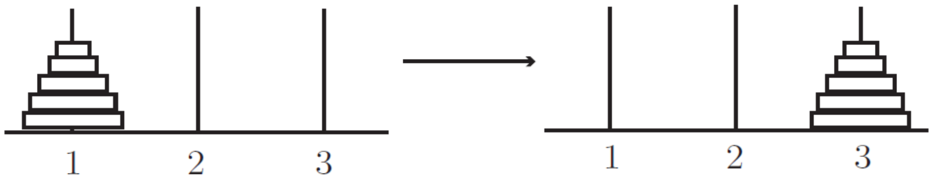
which is P(k +1). That is, P(k +1) is true whenever P(k) is true. By the principle of induction, P(n) is true for all n.

Recursion Equations

Describe the uses you have made of recursion in writing programs. Include as many as you can.

Recall that in the Towers of Hanoi problem we have three pegs numbered 1, 2 and 3, and on one peg we have a stack of n disks, each smaller in diameter than the one below it as in Figure An allowable move consists of removing a disk

Figure.: The Towers of Hanoi



from one peg and sliding it onto another peg so that it is not above another disk of smaller size. We are to determine how many allowable moves are needed to move the disks from one peg to another. Describe the strategy you have used or would use in a recursive program to solve this problem.

For the Tower of Hanoi problem, to solve the problem with no disks you do nothing. To solve the problem of moving all disks to peg 2, we do the following

1. (Recursively) solve the problem of moving $n-1$ disks from peg 1 to peg 3,
2. move disk n to peg 2,
3. (Recursively) solve the problem of moving $n-1$ disks on peg 3 to peg 2.

Thus if $M(n)$ is the number of moves needed to move n disks from peg i to peg j, we have

$$M(n) = 2M(n-1) + 1.$$

This is an example of a **recurrence equation** or **recurrence**. A recurrence equation for a function defined on the set of integers greater than or equal to some number b is one that tells us how to compute the nth value of a function from the $(n-1)$st value or some or all the values preceding n. To completely specify a function on the basis of a recurrence, we have to give enough information about the function to get started. This information is called the *initial condition (or the initial conditions)* (which we also call the *base case*) for the recurrence. In this case we have said that $M(0) = 0$. Using this, we get from the recurrence that $M(1) = 1$, $M(2) = 3$, $M(3) = 7$, $M(4) = 15$, $M(5) = 31$, and are led to guess that $M(n) = 2^n - 1$.

Formally, we write our recurrence and initial condition together as

$$M(n) = \begin{cases} 0 & \text{if } n = 0 \\ 2M(n-1)+1 & \text{otherwise} \end{cases}$$

Example:

Given the recurrence

$$T(n) = rT(n-1) + a,$$

we can substitute the right hand side of the equation $T(n-1) = rT(n-2) + a$ for $T(n-1)$ in our recurrence, and then substitute the similar equations for $T(n-2)$ and $T(n-3)$ to write

$$\begin{aligned}
T(n) &= r(rT(n-2) + a) + a \\
&= r^2T(n-2) + ra + a \\
&= r^2(rT(n-3) + a) + ra + a \\
&= r^3T(n-3) + r^2a + ra + a \\
&= r^3(rT(n-4) + a) + r^2a + ra + a \\
&= r^4T(n-4) + r^3a + r^2a + ra + a
\end{aligned}$$

From this, we can guess that

$$\begin{aligned}
T(n) &= r^nT(0) + a\sum_{i=0}^{n-1} r^i \\
&= r^nb + a\sum_{i=0}^{n-1} r^i.
\end{aligned}$$

$$\begin{aligned}
T(0) &= b \\
T(1) &= rT(0) + a \\
&= rb + a \\
T(2) &= rT(1) + a \\
&= r(rb + a) + a \\
&= r^2b + ra + a \\
T(3) &= rT(2) + a \\
&= r^3b + r^2a + ra + a
\end{aligned}$$

SETS

A set is a collection of objects called the elements or members of the set. The ordering of the elements is not important and repetition of elements is ignored, for example {1, 3, 1, 2, 2, 1} = {1, 2, 3}.

One usually uses capital letters, A,B,X, Y, . . . , to denote sets, and lowercase letters, a, b, x, y, . . ., to denote elements of sets.

Below you'll see just a sampling of items that could be considered as sets:

• The items in a store

• The English alphabet

• Even numbers

A set could have as many entries as you would like. It could have one entry, 10 entries, 15 entries, infinite number of entries, or even have no entries at all! For example, in the above list the English alphabet would have 26 entries, while the set of even numbers would have an infinite number of entries.

Each entry in a set is known as an **element or member**

Sets are written using curly brackets "{" and "}", with their elements listed in between. For example the English alphabet could be written as {a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}

and even numbers could be {0,2,4,6,8,10,...} (Note: the dots at the end indicating that the set goes on infinitely)

Principles:

$\in$ belong to

$\notin$ not belong to

$\subseteq$ subset

$\subset$ proper subset, For example, {a, b} is a proper subset of {a, b, c}, but {a, b, c} is not a proper subset of {a, b, c}.

$\not\subset$ not subset

So we could replace the statement "a is belong to the alphabet" with a $\in$ {alphabet} and replace the statement "3 is not belong to the set of even numbers" with 3 $\notin$ {Even numbers}

Now if we named our sets we could go even further. Give the set consisting of the **alphabet** the name A, and give the set consisting of **even numbers** the name E.We could now write a $\in$ A and 3 $\notin$ E.

Problem

Let A = {2, 3, 4, 5} and C = {1, 2, 3, . . ., 8, 9}, Show that A is a proper subset of C.

Answer

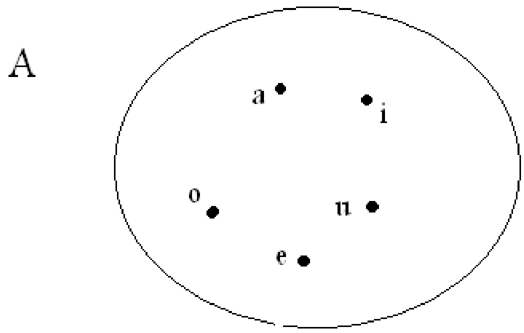
Each element of A belongs to C so A $\subseteq$ C. On the other hand, 1 $\in$ C but 1 $\notin$ A. Hence A $\neq$ C. Therefore A is a proper subset of C.

There are three ways to specify a particular set:

1) By list its members separated by commas and contained in braces{ }, (if it is possible), for example, A= {a,e,i,o,u}

2) By state those properties which characterize the elements in the set, for example, A={x:x is a letter in the English alphabet, x is a vowel}

3) Venn diagram: (A graphical representation of sets).



Example (1)

A={x:x is a letter in the English alphabet, x is a vowel} e ∈ A (e is belong to A)

f ∉ A (f is not belong to A)

Example (2)

X is the set {1,3,5,7,9} 3 ∈ X and 4 ∉X

Example (3)

Let E = {x | x*P*2*P* − 3x + 2 = 0} → (x-2)(x-1)=0 → x=2 & x=1

E = {2, 1}, and 2∈E

Universal set, empty set:

In any application of the theory of sets, the members of all sets under investigation usually belong to some fixed large set called the universal set. For example, in human population studies the universal set consists of all the people in the world. We will let the symbol U denotes the universal set.

The set with no elements is called the empty set or null set and is denoted by ∅ or {}

Subsets:

Every element in a set A is also an element of a set B, then A is called a subset of B. We also say that B contains A. This relationship is written:

A ⊂ B or B ⊃A

If A is not a subset of B, i.e. if at least one element of A dose not belong to B, we write A ⊄ B.

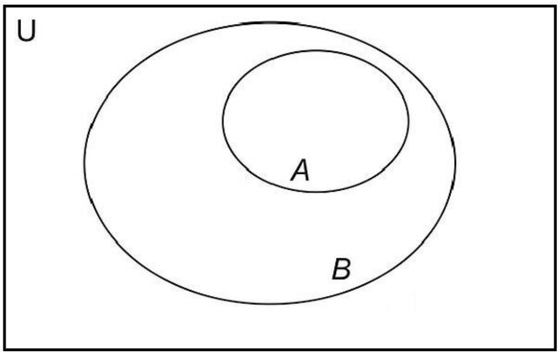
Example :

Consider the sets. A = {1,3,4,5,8,9} B = {1,2,3,5,7} and C ={1,5}

Then C⊂ A and C⊂ B since 1 and 5, the element of C, are also members of A and B.

But B⊄ A since some of its elements, e.g. 2 and 7, do not belong to A. Furthermore, since the elements of A,B and C must also belong to the universal set U, we have that U must at least the set {1,2,3,4,5,7,8,9}.

The notion of subsets is graphically illustrated below



A is entirely within B so $A \subset B$.

Set of numbers:

Several sets are used so often, they are given special symbols.

N = the set of *natural numbers* or positive integers

Several sets are used so often, they are given special symbols.

N = the set of *natural numbers* or positive integers

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

Z = the set of all integers: . . . ,−2,−1, 0, 1, 2, . . .

$$\mathbb{Z} = \mathbb{N} \cup \{\ldots, -2, -1\}$$

Q = the set of rational numbers

$$\mathbb{Q} = \mathbb{Z} \cup \{\ldots, -1/3, -1/2, 1/2, 1/3, \ldots, 2/3, 2/5, \ldots\}$$

Where $Q = \{ a/b : a , b \in Z, b \neq 0\}$

R = the set of real numbers

$$\mathbb{R} = \mathbb{Q} \cup \{\ldots, -\pi, -\sqrt{2}, \sqrt{2}, \pi, \ldots\}$$

C = the set of complex numbers

$$\mathbb{C} = \mathbb{R} \cup \{i, 1+i, 1-i, \sqrt{2}+\pi i, \ldots\}$$

Where $C=\{ x + iy ; x , y \in R; i = \sqrt{-1}\}$

Observe that $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$.

<u>There Is and For All</u>

A predicate can also become a proposition when prefixed by a quantifier.

There are two quantifiers, i.e.,

$\exists$ read: there is or there exists

$\forall$ read: for all or for every

Example. Let P(x) : $x^2 = 4$ and Q(x) : $x^2 > 0$. Determine true or false.
a) $\exists x \in R : P(x)$
b) $\forall x \in Z : P(x)$
c) $\exists x \in Z : Q(x)$
d) $\forall x \in R : Q(x)$
Solution. Note as follows how each statement is supposed to read.

a) $\exists x \in R : P(x)$ represents the statement "There is a real number x such that $x^2 = 4$." This statement is true because there does exist such a number $x \in R$, e.g., x = 2. (In fact there is another example, x = −2, but producing one example is enough.)

b) $\forall x \in Z : P(x)$ stands for "For all integers x, we have $x^2 = 4$. This is false, for example consider x = 1, which gives "12 = 4." (Sometimes this predicate can be true, e.g., for x = 2, but not always true.)

c) $\exists x \in Z : Q(x)$ is true; just let x = 3, for instance. (In fact, there are abundantly many examples, for as long as x 6= 0.)

d) $\forall x \in R : Q(x)$ is false, for when x = 0 we get "02 > 0" (even though x = 0 is the only instance for which Q(x) becomes false).

Exercise. For each predicate P(x) given below, determine the truth values of $\exists x \in R : P(x)$ and $\forall x \in R : P(x)$.
a) P(x) : $x > 2x$
b) P(x) : $x^4 < -1$
c) P(x) : $3x^2 - 15x + 7c = 0$
d) P(x) : $2x^2 - 9x + 11 > 0$

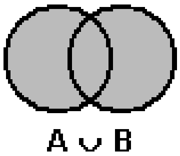
Theorem 1:
For any set A, B, C:
1- $\emptyset \subset A \subset U$.
2- $A \subset A$.
3- If $A \subset B$ and $B \subset C$, then $A \subset C$.
4- $A = B$ if and only if $A \subset B$ and $B \subset A$.

Set operations:

1) UNION:

The *union* of two sets *A* and *B*, denoted by $A \cup B$, is the set of all elements which belong to *A* or to *B*;

$A \cup B = \{ x : x \in A \text{ or } x \in B\}$



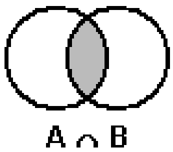
Example

A={1,2,3,4,5} B={5,7,9,11,13} $A \cup B = \{1,2,3,4,5,7,9,11,13\}$

2) INTERSECTION

The *intersection* of two sets *A* and *B*, denoted by $A \cap B$, is the set of elements which belong to both *A* and *B*;

$A \cap B = \{ x : x \in A \text{ and } x \in B\}$.



Example 1

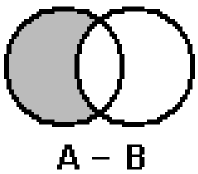
A={1,3,5,7,9} B={2,3,4,5,6} The elements they have in common are 3 and 5

$A \cap B = \{3,5\}$

3) THE DIFFERENCE:

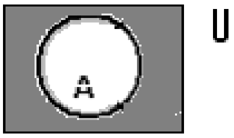
The difference of two sets A\B or A-B is those elements which belong to A but which do not belong to B.

$A \setminus B = \{x : x \in A, x \notin B\}$



4) COMPLEMENT OF SET: Complement of set A*Pc*P or A' , is the set of elements which belong to U but which do not belong to A .

A*Pc*P = {x : x ∈ U, x ∉ A}



Example: let A={1,2,3}

B={3,4}

U={1,2,3,4,5,6}

Find:

A ∪ B = {1, 2, 3, 4}

A ∩ B = {3}

A - B = {1, 2}

A*Pc*P = {4, 5, 6}

5) Symmetric difference of sets

The symmetric difference of sets A and B, denoted by A ⊕ B, consists of those elements which belong to A or B but not to both. That is,

$A \oplus B = (A \cup B)\backslash(A \cap B)$ or $A \oplus B = (A\backslash B) \cup (B\backslash A)$

A ⊕ B

Example: Suppose U = N = {1, 2, 3, . . .} is the universal set.

Let A = {1, 2, 3, 4}, B= {3, 4, 5, 6, 7}, C= {2, 3, 8, 9}, E= {2, 4, 6, 8,. . .}

Then:

$A^c = \{5, 6, 7, \ldots\}$, $B^c = \{1, 2, 8, 9, 10, \ldots\}$, $C^c = \{1,4,5,6,7,10,\ldots\}$ $E^c = \{1, 3, 5, 7, \ldots\}$

$A\backslash B = \{1, 2\}$, $A\backslash C = \{1, 4\}$, $B\backslash C = \{4, 5, 6, 7\}$, $A\backslash E = \{1, 3\}$,

$B\backslash A = \{5, 6, 7\}$, $C\backslash A = \{8, 9\}$, $C\backslash B = \{2, 8, 9\}$, $E\backslash A = \{6, 8, 10, 12, \ldots\}$.

Furthermore:

$A \oplus B = (A\backslash B) \cup (B\backslash A) = \{1, 2, 5, 6, 7\}$, $B \oplus C = \{2, 4, 5, 6, 7, 8, 9\}$,

$A \oplus C = (A\backslash C) \cup (B\backslash C) = \{1, 4, 8, 9\}$, $A \oplus E = \{1, 3, 6, 8, 10, \ldots\}$.

Example. Let $A = \{1, 3, 5, 7\}$, $B = \{0, 1, 2, 3\}$, and $C = \{0, 2\}$. Determine the output of each set operation given below.

a) $A \cup B, A \cup C, B \cup C$
b) $A \cap B, A \cap C, B \cap C$
c) $A - B, A - C, B - C$
d) $A \oplus B, A \oplus C, B \oplus C$

Solution. We refer to the four definitions given above.

a) By definition, $x \in A \cup B$ if and only if $x \in \{1, 3, 5, 7\}$ or $x \in \{0, 1, 2, 3\}$. For this to hold, x can be any one of the elements in either set. Hence, $A \cup B = \{0, 1, 2, 3, 5, 7\}$. Similarly, $A \cup C = \{0, 1, 2, 3, 5, 7\}$ and $B \cup C = \{0, 1, 2, 3\} = B$.

b) Since $x \in A \wedge x \in B$ is true if only if x is a common element of A and B, then we have $A \cap B = \{1, 3\}$. Similarly, $A \cap C = \emptyset$ and $B \cap C = C$.

c) Of the elements in $A = \{1, 3, 5, 7\}$, only 5 and 7 do not belong to B. Hence, $A - B = \{5, 7\}$. Similarly, $A - C = A$ and $B - C = \{1, 3\}$.

d) Note that $x \in \{1, 3, 5, 7\} \oplus x \in \{0, 1, 2, 3\}$ is true exactly when x belongs to one, but not both, of the two sets. So we have $A \oplus B = \{0, 2, 5, 7\}$. Similarly, $A \oplus C = \{0, 1, 2, 3, 5, 7\}$ and $B \oplus C = \{1, 3\}$.

Definition. When $A \cap B = \emptyset$, we say that the two sets A and B are disjoint.

Example. Explain why $A \oplus B = A \cup B$ if A and B are disjoint sets.
Solution. We have $x \in A \oplus B$ exactly when x belongs to A or B but not both. The "both" part may be ignored, since $A \cap B$ is empty in this case. Therefore, $A \oplus B = A \cup B$.

Theorem 2 :
$A \subset B$, $A \cap B = A$, $A \cup B = B$ are equivalent

Theorem 3: (Algebra of sets)

Sets under the above operations satisfy various laws or identities, which are listed below:

1- $A \cup A = A$
$A \cap A = A$

2- $(A \cup B) \cup C = A \cup (B \cup C)$ — Associative laws
$(A \cap B) \cap C = A \cap (B \cap C)$

3- $A \cup B = B \cup A$ — Commutativity
$A \cap B = B \cap A$

4- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ — Distributive laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

5- $A \cup \varnothing = A$ — Identity laws
$A \cap U = A$

6- $A \cup U = U$ — Identity laws
$A \cap \varnothing = \varnothing$

7- $(A^c)^c = A$ — Double complements

8- $A \cup A^c = U$ — Complement intersections and unions

$A \cap A^c = \varnothing$

9- $U^c = \varnothing$
$\varnothing^c = U$

10- $(A \cup B)^c = A^c \cap B^c$ — De Morgan's laws

We discuss two methods of proving equations involving set operations. The first is to break down what it means for an object x to be an element of each side, and the second is to use Venn diagrams. For example, consider the first of De Morgan's laws:

$$(A \cup B)^c = A^c \cap B^c$$

We must prove: 1) $(A \cup B)^c \subset A^c \cap B^c$
2) $A^c \cap B^c \subset (A \cup B)^c$

We first show that $(A \cup B)^c \subset A^c \cap B^c$

Let's pick an element at random $x \in (A \cup B)^c$. We don't know anything about x, it could be a number, a function. All we do know about x, is that:

$x \in (A \cup B)^c$, so
$x \notin A \cup B$

because that's what complement means. Therefore

$x \notin A$ and $x \notin B$,

by pulling apart the union. Applying complements again we get

$x \in A^c$ and $x \in B^c$

Finally, if something is in 2 sets, it must be in their intersection, so

$x \in A^c \cap B^c$

So, any element we pick at random from: $(A \cup B)^c$ is definitely in, $A^c \cap B^c$, so by definition

$(A \cup B)^c \subset A^c \cap B^c$

Next we show that $(A^c \cap B^c) \subset (A \cup B)^c$.

This follows a very similar way. Firstly, we pick an element at random from the first set, $x \in (A^c \cap B^c)$

Using what we know about intersections, that means

$x \in A^c$ and $x \in B^c$

Now, using what we know about complements,

$x \notin A$ and $x \notin B$.

If something is in neither A nor B, it can't be in their union, so

$x \notin A \cup B$,

And finally

$\therefore \quad x \in (A \cup B)^c$

We have prove that every element of $(A \cup B)^c$ belongs to $A^c \cap B^c$ and that every element of $A^c \cap B^c$ belongs to $A \cup B)^c$. Together, these inclusions prove that the sets have the same elements, i.e. that $(A \cup B)^c = A^c \cap B^c$

Power set

The power set of some set S, denoted P(S), is the set of all subsets of S (including S itself and the empty set)

Example 1: Let A = { 1,2 3}

Power set of set A = P(A) = [{1},{2},{3},{1,2},{1,3},{2,3},{},A]

Example 2: P({0,1})={{},{0},{1},{0,1}}

Classes of sets: Collection of subset of a set with some properties

Example: Suppose A = { 1,2 3} , let X be the class of subsets of A which contain exactly two elements of A. Then

class X = [{1,2},{1,3},{2,3}]

Cardinality

Definition. The cardinality of a set A, denoted by |A|, is the number of elements in A, if finite.

Hence for example, |{a, b, c}| = 3 and |∅| = 0.

The cardinality of the power set

Theorem: If |A| = n then |P(A)| = 2^n (Every set with n elements has 2^n subsets)

Example

write the answers to the following questions.

1. $|\{1,2,3,4,5,6,7,8,9,0\}|$
2. $|P(\{1,2,3\})|$
3. $P(\{0,1,2\})$
4. $P(\{1\})$

Solution:

1. 10
2. $2^3=8$
3. $\{\{\},\{0\},\{1\},\{2\},\{0,1\},\{0,1,2\},\{0,2\},\{1,2\}\}$
4. $\{\{\},\{1\}\}$

<u>Definition.</u> Two sets A and B are identical, in which case we write A=B,when the following proposition holds for every element x.

$x \in A \leftrightarrow x \in B$

Now if we associate two propositions with these two sets,

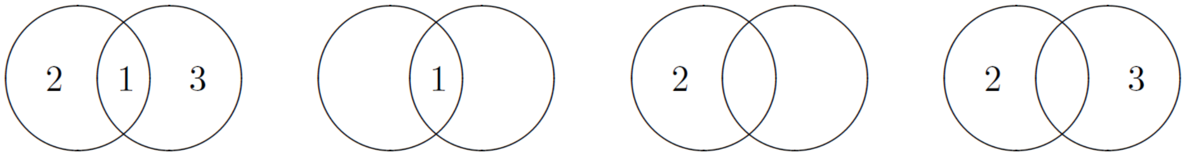
$p : x \in A$

$q : x \in B$

then we see that the four labels respectively correspond to the four rows of (p,q) values in the following truth table.

			$A \cup B$	$A \cap B$	$A - B$	$A \oplus B$
	p	q	$p \vee q$	$p \wedge q$	$p \wedge \neg q$	$p \oplus q$
1	T	T	T	T	F	F
2	T	F	T	F	T	T
3	F	T	T	F	F	T
4	F	F	F	F	F	F

Note that the table includes the truth values of the four set operations ∪,∩,−, and ⊕. These give their Venn diagrams below, showing the regions where each resulting set contains its elements, i.e., where the truth value is true.



$A \cup B$ $A \cap B$ $A - B$ $A \oplus B$

With Venn diagrams, we are able to give intuitive proofs to certain set identities. It is convincing enough, for instance, to deduce that $(A - B) \cup (A \cap B) = A$ since both consist of regions 1 and 2 in the diagrams. The next theorem is another example.

Theorem . Let A and B be any two sets. Then
$A \oplus B = (A - B) \cup (B - A)$
Proof. The proof is an easy visualization with Venn diagrams. Or, if you prefer truth tables to Venn diagrams, we may let $p : x \in A$ and $q : x \in B$ as before, and note that $(A - B) \cup (B - A)$ is given by the proposition $(p \wedge \neg q) \vee (q \wedge \neg p)$. The truth table below show that $(p \wedge \neg q) \vee (q \wedge \neg p) \equiv p \oplus q$, which defines the set $A \oplus B$. ▽

p	q	$\neg p$	$\neg q$	$p \wedge \neg q$	$q \wedge \neg p$	$(p \wedge \neg q) \vee (q \wedge \neg p)$
T	T	F	F	F	F	F
T	F	F	T	T	F	T
F	T	T	F	F	T	T
F	F	T	T	F	F	F

Exercise. Use truth table to establish the set identity
$A \oplus B = (A \cup B) - (A \cap B)$

Exercise. Use Venn diagrams to find the resulting set identical to each one given below.
a) $(A \cap B) \oplus (A - B)$
b) $(A - (A - B)) \oplus B$
c) $(A \cup B) \oplus (A \cap B)$
d) $(A \cup B) \oplus (A \oplus B)$

Definition. If A and B are two given sets, the direct product $A \times B$, read A cross B, is defined by $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$.
For example, if $A = \{1, 2\}$ and $B = \{3, 4\}$ then
$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
$B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2)\}$

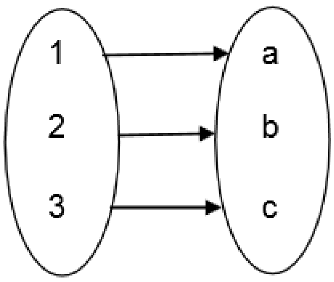
Relations

The language of set theory plays a fundamental role in much of modern mathematics. We will study the idea of relations between elements of two sets.

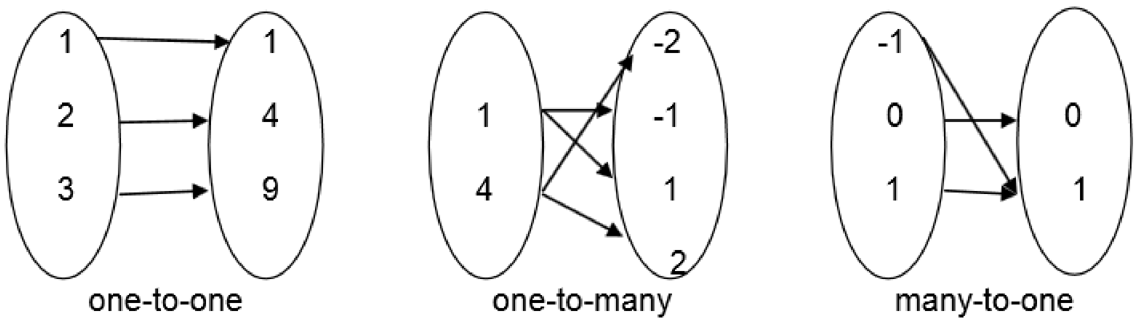
A **relation** is a set of ordered pairs. For example: (1, a), (2, b), (3, c). The set of first elements is called the domain: {1, 2, 3} and the set of second elements is called the range: {a, b, c}.

Relations can be represented on arrow diagrams

Example:



The three main types of relations are shown in the following arrow diagrams



Binary Relations

There are many relations in mathematics :"less than" , "is parallel to ","is a subset of", etc. These relations consider the existence or nonexistence of a certain connection between pairs of objects taken in a definite order. We define a relation simply in terms of ordered pairs of objects

Definition. Let A and B be two sets. A relation R from A to B means a subset R $\subseteq A \times B$.

Product sets:

Consider two arbitrary sets A and B. The set of all ordered pairs (a,b) where $a \in A$ and $b \in B$ is called the product, or cartesian product, of A and B.

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

Example: Let A = {1,2} and B = {a ,b ,c} then
A × B = {(1,a), (1,b),(1,c),(2,a),(2,b),(2,c)}
Also, A × A = {(1, 1), (1, 2), (2, 1), (2, 2)}
The order in which the sets are considered is important, so A×B ≠ B ×A.Let A and B be sets. A binary relation, R, from A to B is a subset of A×B. If (x,y) ∈R, we say that x is R-related to y and denote this by xRy if (x,y) ∉R, we write x Ř y and say that x is not R-related to y .
if R is a relation from A to A ,i.e. R is a subset of A × A, then we say that R is a relation on A.

The **domain** of a relation R is the set of all first elements of the ordered pairs which belong to R, and the **range** of R is the set of second elements

Example 1:
Let A = {1, 2, 3, 4}. Define a relation R on A by writing (x, y) ∈ R if x < y. Then R = {(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)}.

Example 2:
let A = {1,2,3} and R = {(1,2),(1,3),(3,2)}. Then R is a relation on A since it is a subset of A×A with respect to this relation:
1R2, 1R3, 3R2 but (1,1)∉R & (2,1)∉R
The domain of R is {1,3} and
The range of R is {2,3}

Example 3:
Let A = {1, 2, 3}. Define a relation R on A by writing (x, y) ∈ R , such that a≥b, list the element of R
aRb ↔ a≥b , a,b∈A
∴ R = {(1,1),(2,1), (2,2), (3,1), (3,2), (3,3)}

Definition. By the *inverse* of a relation $R \subseteq A \times B$, we mean the relation from B to A given by $R^{-1} = \{(b,a) \mid (a,b) \in R\}$.

For example, the inverse of $R = \{(1,0),(5,5),(9,-2)\} \subseteq \mathbb{N} \times \mathbb{Z}$ is the relation $R^{-1} = \{(0,1),(5,5),(-2,9)\} \subseteq \mathbb{Z} \times \mathbb{N}$.

Properties of relations:

Let R be a relation on the set A

1) Reflexive : R is reflexive if : $\forall$ a $\in$A $\rightarrow$ aRa or (a,a) $\in$ R ; $\forall$ a, b $\in$A. . Thus R is not reflexive if there exists a $\in$ A such that (a, a) $\notin$ R.

2) Symmetric : aRb $\rightarrow$ bRa $\forall$ a,b $\in$A. if whenever $(a, b) \in R$ then $(b, a) \in R$. Thus R is not symmetric if there exists $a, b \in A$ such that $(a, b) \in R$ but $(b, a) \notin R$.

3) Transitive : aRb $\wedge$ bRc $\rightarrow$ aRc. that is, if whenever $(a, b), (b, c) \in R$ then $(a, c) \in R$. Thus R is not transitive if there exist $a, b, c \in R$ such that $(a, b), (b, c) \in R$ but $(a, c) \notin R$.

4) Equivalence relation : it is Reflexive & Symmetric & Transitive. That is, R is an equivalence relation on S if it has the following three properties:

a - For every $a \in S$, aRa.

b- If aRb, then bRa.

c- If aRb and bRc, then aRc.

5) Irreflexive : $\forall$ a $\in$A (a,a) $\notin$ R

6) AntiSymmetric : if aRb and bRa $\rightarrow$ a=b

the relations $\geq,\leq$ and $\subseteq$ are antisymmetric

Example : Consider the relation of C of set inclusion on any collection of sets:

1) A $\subset$ A for any set, so $\subset$ is reflexive

2) A $\subset$ B dose not imply B $\subset$ A, so $\subset$ is not symmetric

3) If A $\subset$ B and B $\subset$ C then A $\subset$ C, so $\subset$ is transitive

4) $\subset$ is reflexive, not symmetric & transitive, so $\subset$ is not equivalence relations

5) A $\subset$ A, so $\subset$ is not Irreflexive

6) If A $\subset$ B and B $\subset$ A then A = B, so $\subset$ is anti-symmetric

Example : If A ={1,2,3} and R={(1,1),(1,2),(2,1),(2,3)}

Is R equivalence relation ?

1) 2 is in A but (2,2) $\notin$ R, so R is not reflexive

2) (2,3) $\in$ R but (3,2) $\notin$ R, so R is not symmetric

3) (1,2) $\in$ R and (2,3) $\in$ R but (1,3) $\notin$ R, so R is not transitive

So R is not Equivalence relation

Example : What is the properties of the relation

1) a=a for any element $a \in A$, so = is reflexive
2) If a = b then b = a, so = is symmetric
3) If a = b and b = c then a = c, so = is tra-nsitive
4)R is (reflexive + symmetric + transitive), so = is equivalence
5) If a = b and b = a then a = b, so = is anti-symmetric

The adjective binary indicates that there are two sets involved. Since we are not interested in studying relations with more than two sets, from now on we agree that the term relation always refers to a binary relation. Since relations are sets, with two relations R and S we are allowed to operate on them, e.g., using the operator union or intersection. We now introduce a new set operator which is customized to relations.

Definition. Suppose that $R \subseteq A \times B$ and $S \subseteq B \times C$ are two relations.
Then $S \circ R$ is the relation from A to C given by
$S \circ R = \{(a, c) \mid (a, b) \in R \wedge (b, c) \in S\}$
The notation $S \circ R$ is read R circle S (yes, right to left!) and we refer to this set operation as the composition of R with S.

Example. Let A = {1, 2, 3, 4}, B = {x, y, z}, and C = {4, 5, 9}. Consider two relations R and S given below, and find the elements of the relation $S \circ R \subseteq A \times C$.
$R = \{(1, y), (1, z), (2, x), (2, y), (4, z)\} \subseteq A \times B$
$S = \{(x, 4), (x, 9), (y, 5), (z, 5), (z, 9)\} \subseteq B \times C$
Solution. The first element $(1, y) \in R$ matches with the element $(y, 5) \in S$, resulting in the new element $(1, 5) \in S \circ R$. Next, $(1, z) \in R$ and $(z, 5) \in S$ yield the same (1, 5), whereas (1, z) and (z, 9) give (1, 9). In all, seven elements are composed in this manner which make up the resulting set.
$S \circ R = \{(1, 5), (1, 9), (2, 4), (2, 5), (2, 9), (4, 5), (4, 9)\}$

Composition of relations:

Let A, B, C be sets and let :

$R : A \rightarrow B$ $(R \subset A \times B)$

$S : B \rightarrow C$ $(S \subset B \times C)$

There is a relation from A to C denoted by

$R \circ S$ (composition of R and S) : $A \rightarrow C$

$R \circ S = \{(a,c) : \exists\, b \in B \text{ for which } (a,b) \in R \text{ and } (b,c) \in S\}$

Example : let $A = \{1,2,3,4\}$

$B = \{a, b, c, d\}$

$C = \{x, y, z\}$

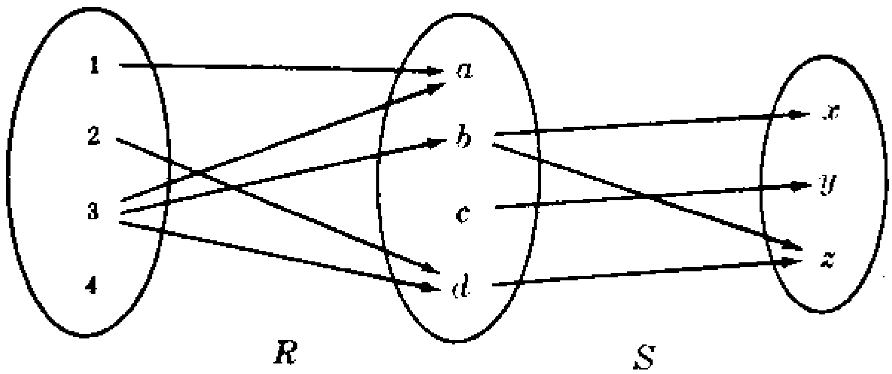
$R = \{(1,a),(2,d),(3,a),(3,d),(3,b)\}$

$S = \{(b,x),(b,z),(c,y),(d,z)\}$

Find $R \circ S$?

Solution :

1) The first way by arrow form



There is an arrow (path) from 2 to d which is followed by an arrow from d to z

2Rd and dSz $\Rightarrow$ $2(R \circ S)$ z and $3(R\circ S)x$ and $3(R\circ S)z$

So $R \circ S = \{(3,x),(3,z),(2,z)\}$

2) The second way by matrix:

$$MR = \begin{array}{c|cccc} & a & b & c & d \\ \hline 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 \\ 3 & 1 & 1 & 0 & 1 \\ 4 & 0 & 0 & 0 & 0 \end{array} \qquad MS = \begin{array}{c|ccc} & x & y & z \\ \hline a & 0 & 0 & 0 \\ b & 1 & 0 & 1 \\ c & 0 & 1 & 0 \\ d & 0 & 0 & 1 \end{array}$$

$R \circ S = M_R \cdot M_S =$

$$\begin{array}{c|ccc} & x & y & z \\ \hline 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 1 & 0 & 2 \\ 4 & 0 & 0 & 0 \end{array}$$

$R \circ S = \{(2,z),(3,x),(3,z)\}$

Definition. By the *inverse of a relation* $R \subseteq A \times B$, we mean the relation from B to A given by $R^{-1} = \{(b, a) \mid (a, b) \in R\}$. For example, the inverse of $R = \{(1, 0), (5, 5), (9,-2)\} \subseteq N \times Z$ is the relation $R^{-1} = \{(0, 1), (5, 5), (-2, 9)\} \subseteq Z \times N$.

Definition. Given a set A, we define the identity relation on A to be the special relation $A^0 = \{(a, a) \mid a \in A\}$. Any relation R on A is then called:

1) ***Reflexive*** if $A^0 \subseteq R$.
2) ***Symmetric*** if $R^{-1} = R$.
3) ***Anti-symmetric*** if $R \cap R^{-1} \subseteq A^0$.
4) ***Transitive*** if $R^2 \subseteq R$.

Example. Let A = {1, 2, 3, 4}. For each relation $R \subseteq A \times A$ given below, determine whether R is reflexive, symmetric, anti-symmetric, or transitive.

a) R = {(1, 1), (1, 2), (2, 1), (2, 2), (2, 4), (3, 3), (4, 2)}
b) R = {(1, 1), (1, 3), (2, 2), (2, 4), (3, 1), (3, 3), (4, 2), (4, 4)}
c) $R = \{(a, b) \in A \times A \mid a \leq b\}$

Solution. We note that A^0 = {(1, 1), (2, 2), (3, 3), (4, 4)}.
1) R is symmetric since $R^{-1} = R$ but not reflexive as $(4, 4) \notin R$. Antisymmetric is false, e.g., $(1, 2) \in R \cap R^{-1}$. So is transitive false, because the composition of (4, 2) with (2, 4) yields $(4, 4) \notin R$.
2) You can check that R is reflexive, symmetric, and transitive. Only antisymmetric is false.
3) R is reflexive since $a \leq a$ for all $a \in A$. Now if $a \neq b$, either $a < b$ or $b < a$ but never both. It follows that R is anti-symmetric, but not symmetric. Lastly, R is transitive for if $a \leq b$ and $b \leq c$, then $a \leq c$.

Theorem . Let R be a relation on a set A. Then
1) R is reflexive if and only if $\forall a \in A : (a, a) \in R$.
2) R is symmetric if and only if $\forall a, b \in A : (a, b) \in R \rightarrow (b, a) \in R$.
3) R is anti-symmetric if and only if $(a, b) \in R \rightarrow (b, a) \notin R$ for all $a, b \in A$ with $a \neq b$.
4) R is transitive if and only if $(a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R$ for all a, b, c $\in A$.

Equivalence Relations

Definition. A relation R on a set A is an *equivalence relation* if R is reflexive, symmetric, and transitive. If R is an equivalence relation, for each $a \in A$ we define the *equivalence class* of a to be the set $[a] = \{x \in A \mid (a, x) \in R\}$.

Example. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $R = \{(a, b) \in A \times A \mid a + b \text{ is even}\}$. Show that R is an equivalence relation and find all the equivalence classes of A under this relation.

Solution. We have $R = \{(1,1), (1,3), (1,5), (2,2), (2,4), (2,6), (3,1), (3,3), (3,5), (4,2), (4,4), (4,6), (5,1), (5,3), (5,5), (6,2), (6,4), (6,6)\}$ and note that R is reflexive, symmetric, and transitive. The equivalence classes are

$$[1] = \{1,3,5\} \qquad [2] = \{2,4,6\} \qquad [3] = \{1,3,5\}$$
$$[4] = \{2,4,6\} \qquad [5] = \{1,3,5\} \qquad [6] = \{2,4,6\}$$

Hence there are only two distinct classes, i.e., {1, 3, 5} and {2, 4, 6}

Theorem Let R be an equivalence relation on a set A. For any $a, b \in A$, the following four propositions are equivalent one to another.

$$a \in [b] \quad \leftrightarrow \quad b \in [a] \quad \leftrightarrow \quad (a, b) \in R \quad \leftrightarrow \quad [a] = [b]$$

Moreover, if $(a, b) \notin R$ then $[a] \cap [b] = \emptyset$.

Proof. We have $(a, b) \in R$ if and only if $b \in [a]$. Since R is symmetric, $(a, b) \in R$ if and only if $(b, a) \in R$. This yields the equivalence among the first three. Moreover, since $a \in [a]$, then $[a] = [b]$ implies $a \in [b]$. Conversely, if $(a, b) \in R$ then $x \in [a]$ implies $(a, x) \in R$ and $(b, x) \in R$ by transitivity. Hence, $x \in [b]$ and $[a] \subseteq [b]$. By a symmetrical argument, then $[a] = [b]$.

To see the last claim, we show its contrapositive: let $x \in [a] \cap [b]$. Since $(a, x) \in R$ and $(b, x) \in R$, then $(a, b) \in R$, by symmetry and transitivity. $\triangledown$

Functions

We consider again the concept of a relation from a set A to another, possibly different, set B. The familiar notion of a function which is normally taught in Calculus can now be presented as a binary relation.

Definition. Let A and B be two given sets. The relation $f \subseteq A \times B$ is a *function* from A to B if there is a unique element $(a, b) \in f$ for every $a \in A$. In such a case, we write $f : A \to B$. The element $b \in B$ for which $(a, b) \in f$ will be denoted by $b = f(a)$. Thus $f = \{(a, f(a)) \mid a \in A\}$.

A **function f** is a rule that assigns to each element x in a set D exactly one element, called f(x), in a set R.

The range R is the set of all possible values of f(x), when x varies over the entire **domain D**.

The functions we consider have the domain and range as subsets of the real numbers. The real numbers are denoted $(\infty, -\infty)$ or R.

We often use y = f(x) as dependent variable (it's called dependent) because it depends on the value of x (denoted as independent variable).

Example 1:

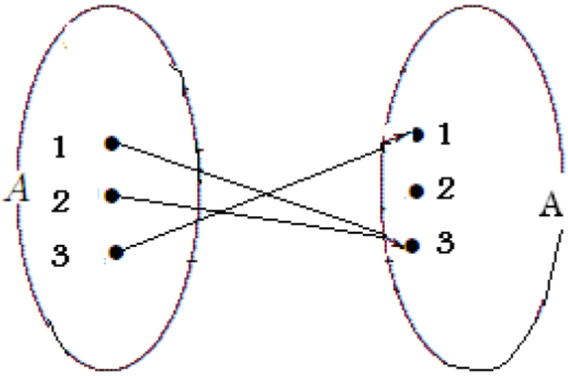
Consider the function $f(x) = x3$, i.e., f assigns to each real number its cube. Then the image of 2 is 8, and so we may write $f(2) = 8$.

Example2 :

consider the following relation on the set A={1,2,3}

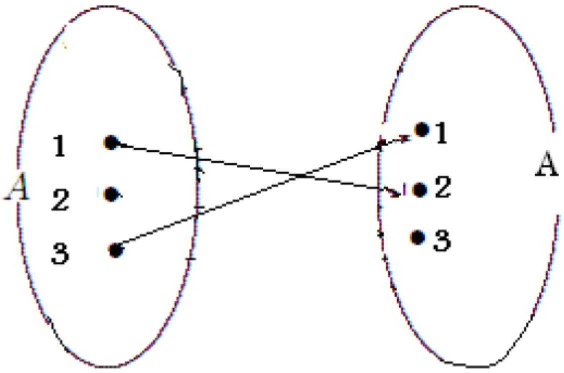
F = {(1,3),(2,3),(3,1)}

F is a function



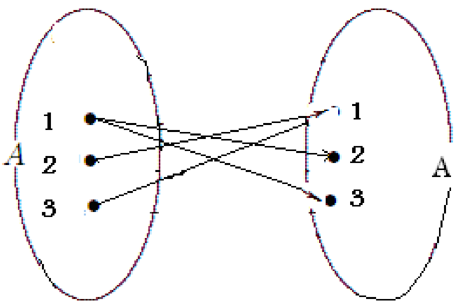
G = {1,2},(3,1)}

G is not a function from A to A



H = {(1,3),(2,1),(1,2),(3,1)}

H is not a function

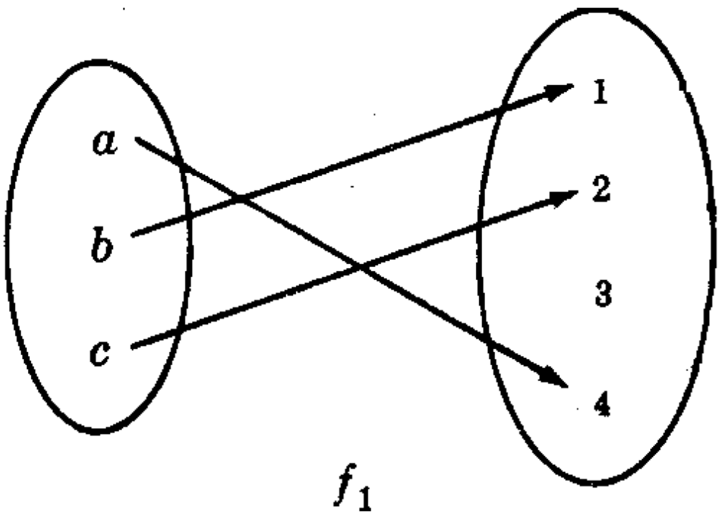


Definition. A function $f : A \to B$ is *one-to-one* or *injective* if every $b \in B$ corresponds to at most one element $(a, b) \in f$. And f is *onto* or *surjective* when $f(A) = B$. If f is both injective and surjective, then we say that f is *bijective*. The noun *bijection* stands for a bijective function. Similarly, an *injection* (*surjection*) stands for an injective (surjective) function. The term *one-to-one correspondence* is a synonym for bijection.

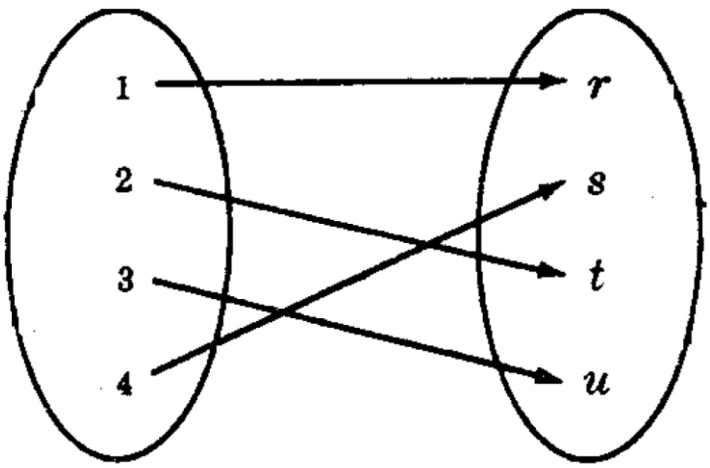
EXAMPLE Consider the function $f : \mathbb{N} \to \mathbb{N} : x \mapsto x$. This is one-to-one and onto.

EXAMPLE Consider the function $f : \mathbb{N} \to \mathbb{Z} : x \mapsto x$. This is one-to-one but not onto.

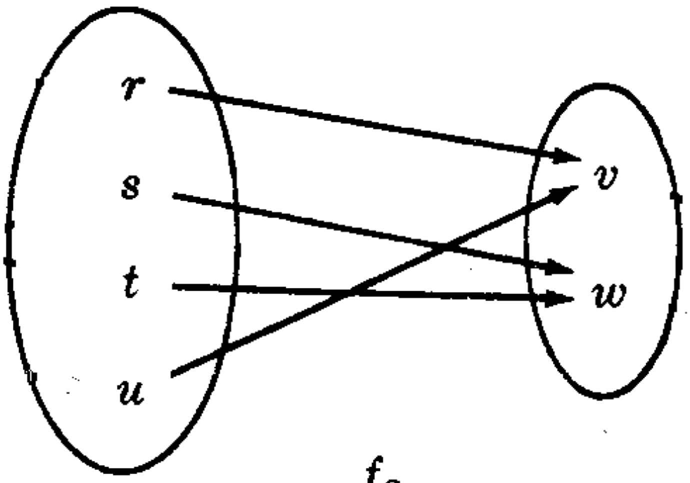
EXAMPLE Consider the function $f : \mathbb{Z} \to \mathbb{N} \cup \{0\} : x \mapsto |x|$. This is onto but not one-to-one.



one to one but not onto (3 ∈ B but it is not the image under f1)



both one to one & onto
(or one to one correspondence between A and B)

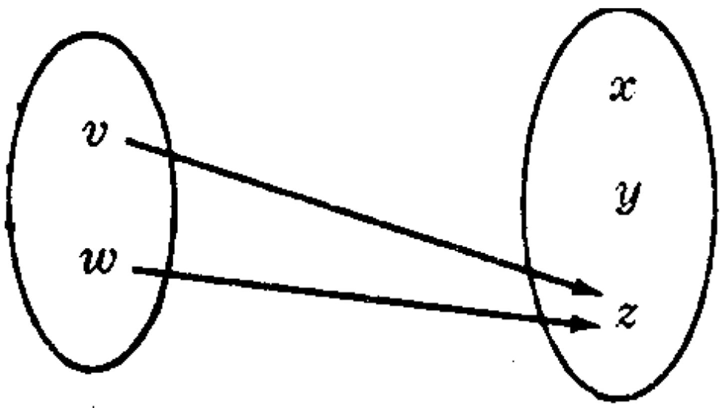


f_3

not one to one & onto

Theorem : A function $f: A \to B$ is invertible if and only if f is both one-to-one and onto. If $f: A \to B$ is one-to-one and onto, then f is called a *one-to-one correspondence* between A and B. This terminology comes from the fact that each element of A will then correspond to a unique element of B and vice versa.

Some texts use the terms *injective* for a one-to-one function, *surjective* for an onto function, and *bijective* for a one-to-one correspondence.



not one to one & not onto

Theorem : A function $f: A \to B$ is invertible if and only if f is both one-to-one and onto. If $f: A \to B$ is one-to-one and onto, then f is called a *one-to-one correspondence* between A and B. This terminology comes from the fact that each element of A will then correspond to a unique element of B and vice versa.

Some texts use the terms *injective* for a one-to-one function, *surjective* for an onto function, and *bijective* for a one-to-one correspondence.

Let $f: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 2x - 3$.
Now f is one-to-one and onto; hence f has an inverse function f^{-1}.
Find a formula for f^{-1}.
Let y be the image of x under the function f: $y = f(x) = 2x - 3$

Consequently, x will be the image of y under the inverse function f^{-1}.

Solve for x in terms of y in the above equation: $x = (y + 3)/2$

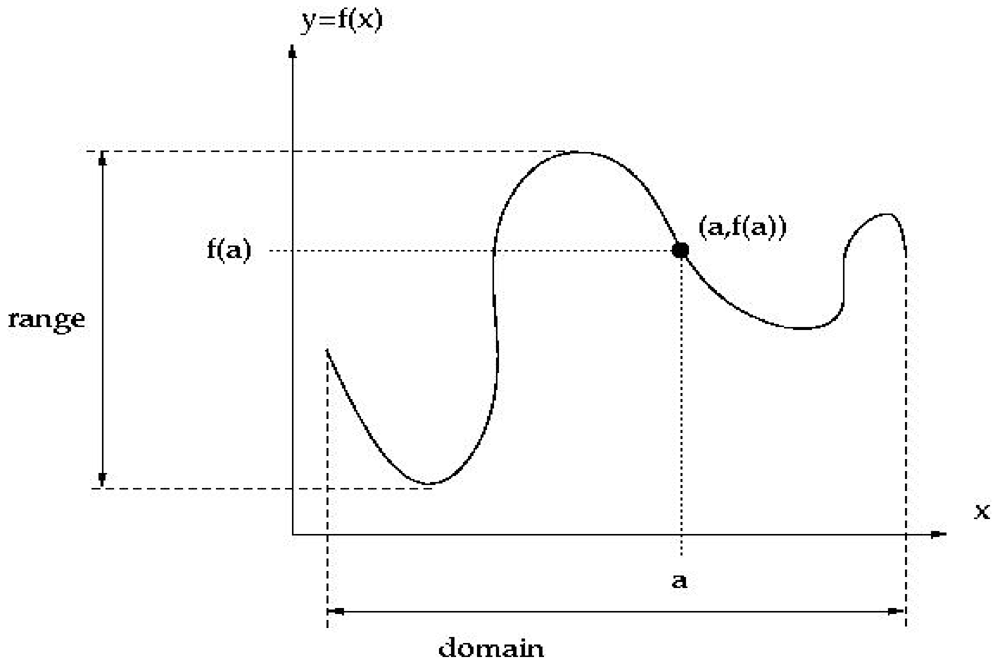
Then $f^{-1}(y) = (y + 3)/2$. Replace y by x to obtain

$$f^{-1}(x) = \frac{x + 3}{2}$$

which is the formula for f^{-1} using the usual independent variable x.

Graph of y = f(x):

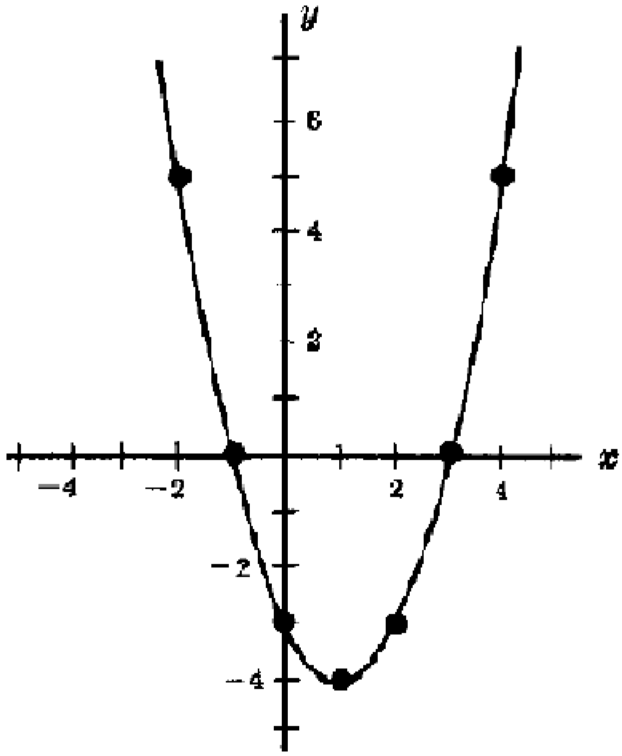
A graph of y = f(x) pictorially represents the relationship between ordered pairs, where the first element in the pair
is the domain, the second element the range: {(x,f(x))|x∈ D } read: “the set of ordered pairs (x; f(x)) such that x is an element of D which is the domain."



Example:

Graph of $f(x) = x^2 - 2x - 3$

x	$f(x)$
-2	5
-1	0
0	-3
1	-4
2	-3
3	0
4	5



RECURSIVELY DEFINED FUNCTIONS

A function is said to be *recursively defined* if the function definition refers to itself. In order for the definition not to be circular, the function definition must have the following two properties:

(1) There must be certain arguments, called *base values*, for which the function does not refer to itself.
(2) Each time the function does refer to itself,

A recursive function with these two properties is said to be *well-defined*.

The following examples should help clarify these ideas.

Factorial Function

The product of the positive integers from 1 to n, inclusive, is called "n factorial" and is usually denoted by $n!$.

That is, $$n! = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$$

It is also convenient to define $0! = 1$, so that the function is defined for all nonnegative integers. Thus:

$0! = 1$, $1! = 1$, $2! = 2\cdot 1 = 2$, $3! = 3\cdot 2\cdot 1 = 6$, $4! = 4\cdot 3\cdot 2\cdot 1 = 24$

$5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$, $6! = 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1 = 720$

And so on. Observe that

$$5! = 5 \cdot 4! = 5 \cdot 24 = 120 \quad \text{and} \quad 6! = 6 \cdot 5! = 6 \cdot 120 = 720$$

This is true for every positive integer n; that is,

$$n! = n \cdot (n-1)!$$

Definition (Factorial Function):

(a) If $n = 0$, then $n! = 1$.
(b) If $n > 0$, then $n! = n \cdot (n-1)!$

Observe that the above definition of $n!$ is recursive, since it refers to itself when it uses $(n-1)!$. However:

(1) The value of $n!$ is explicitly given when $n = 0$ (thus 0 is a base value).
(2) The value of $n!$ for arbitrary n is defined in terms of a smaller value of n which is closer to the base value 0.

EXAMPLE Figure shows the nine steps to calculate 4! using the recursive definition.

Step 1. This defines 4! in terms of 3!, so we must postpone evaluating 4! until we evaluate 3. This postponement is indicated by indenting the next step.

Step 2. Here 3! is defined in terms of 2!, so we must postpone evaluating 3! until we evaluate 2!.

Step 3. This defines 2! in terms of 1!.

Step 4. This defines 1! in terms of 0!.

Step 5. This step can explicitly evaluate 0!, since 0 is the base value of the recursive definition.

Steps 6 to 9. We backtrack, using 0! to find 1!, using 1! to find 2!, using 2! to find 3!, and finally using 3! to find 4!. This backtracking is indicated by the "reverse" indention.

Observe that we backtrack in the reverse order of the original postponed evaluations.

(1) $4! = 4 \cdot 3!$

(2) $3! = 3 \cdot 2!$

(3) $2! = 2 \cdot 1!$

(4) $1! = 1 \cdot 0!$

(5) $0! = 1$

(6) $1! = 1 \cdot 1 = 1$

(7) $2! = 2 \cdot 1 = 2$

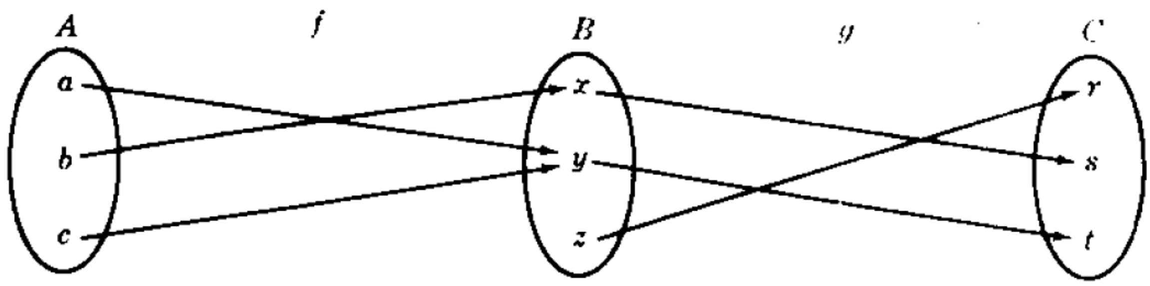
(8) $3! = 3 \cdot 2 = 6$

(9) $4! = 4 \cdot 6 = 24$

Composition of function:

Let $f:A \to B$ and $g:B \to C$, to find the composition function $gof:A \to C$

$(gof)(a) = g(f(a)) = g(y) = t$
$(gof)(b) = g(f(b)) = g(x) = s$
$(gof)(c) = g(f(c)) = g(y) = t$



Example

Let $f(x) = 2x + 3$ and $g(x) = \dfrac{5x+1}{2x-3}$. Determine $(g \circ f)(x)$ and $(f \circ g)(x)$.

Solution

By definition, $(g \circ f)(x) = g(f(x))$.

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(2x+3) \\ &= \frac{5(2x+3)+1}{2(2x+3)-3} \\ &= \frac{10x+16}{4x+3}\end{aligned}$$

By definition, $(f \circ g)(x) = f(g(x))$.

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f\left(\frac{5x+1}{2x-3}\right) \\ &= 2\left(\frac{5x+1}{2x-3}\right) + 3 \\ &= \frac{10x+2}{2x-3} + \frac{3(2x-3)}{2x-3} \\ &= \frac{10x+2+6x-9}{2x-3} \\ &= \frac{16x-7}{2x-3}\end{aligned}$$

Example. Let $A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$, and $C = \{4, 5, 9\}$. Consider two relations R and S given below, and find the elements of the relation $S \circ R \subseteq A \times C$.

$$R = \{(1, y), (1, z), (2, x), (2, y), (4, z)\} \subseteq A \times B$$
$$S = \{(x, 4), (x, 9), (y, 5), (z, 5), (z, 9)\} \subseteq B \times C$$

Solution. The first element $(1, y) \in R$ *matches* with the element $(y, 5) \in S$, resulting in the new element $(1, 5) \in S \circ R$. Next, $(1, z) \in R$ and $(z, 5) \in S$ yield the same $(1, 5)$, whereas $(1, z)$ and $(z, 9)$ give $(1, 9)$. In all, seven elements are composed in this manner which make up the resulting set.

$$S \circ R = \{(1, 5), (1, 9), (2, 4), (2, 5), (2, 9), (4, 5), (4, 9)\}$$