MODULE3

INDUCTION, COUNTING AND ALGEBRAIC STRUCTURES

Induction, Counting

Elementary Combinatorics

Mathematical Induction

The simplest and most common form of mathematical induction infers that a statement involving a natural number n (that is, an integer $n \geq 0$ or 1) holds for all values of n. The proof consists of two steps:

1. The **base case** (or **initial case**): prove that the statement holds for 0, or 1.
2. The **induction step** (or **inductive step**, or **step case**): prove that for every n, if the statement holds for n, then it holds for $n+1$. In other words, assume that the statement holds for some arbitrary natural number n, and prove that the statement holds for $n+1$.

The hypothesis in the induction step, that the statement holds for a particular n, is called the **induction hypothesis** or **inductive hypothesis**. To prove the induction step, one assumes the induction hypothesis for n and then uses this assumption to prove that the statement holds for $n+1$.

Authors who prefer to define natural numbers to begin at 0 use that value in the base case; those who define natural numbers to begin at 1 use that value.

Sum of consecutive natural numbers [edit]

Mathematical induction can be used to prove the following statement $P(n)$ for all natural numbers n.

$$P(n):\ \ 0+1+2+\cdots+n=\frac{n(n+1)}{2}.$$

This states a general formula for the sum of the natural numbers less than or equal to a given number; in fact an infinite sequenc

$0=\frac{(0)(0+1)}{2}$, $0+1=\frac{(1)(1+1)}{2}$, $0+1+2=\frac{(2)(2+1)}{2}$, etc.

Proposition. For every $n \in \mathbb{N}$, $0+1+2+\cdots+n=\frac{n(n+1)}{2}$.

Proof. Let $P(n)$ be the statement $0+1+2+\cdots+n=\frac{n(n+1)}{2}$. We give a proof by induction on n.

Base case: Show that the statement holds for the smallest natural number $n=0$.

$P(0)$ is clearly true: $0=\frac{0(0+1)}{2}$.

Induction step: Show that for every $k \geq 0$, if $P(k)$ holds, then $P(k+1)$ also holds.

Assume the induction hypothesis that for a particular k, the single case $n=k$ holds, meaning $P(k)$ is true:

$$0+1+\cdots+k=\frac{k(k+1)}{2}.$$

It follows that:

$$(0+1+2+\cdots+k)+(k+1)=\frac{k(k+1)}{2}+(k+1).$$

Basis of counting:

If X is a set, let us use |X| to denote the number of elements in X.

Two Basic Counting Principles

Two elementary principles act as —building blocks< for all counting problems. The first principle says that the whole is the sum of its parts; it is at once immediate and elementary.

Sum Rule: **The principle of disjunctive counting** :

If a set X is the union of disjoint nonempty subsets S1, ….., Sn, then | X | = | S1 | + | S2 | + ….. + | Sn |.

We emphasize that the subsets S1, S2, …., Sn must have no elements in common. Moreover, since X = S1 U S2 U ……U Sn, each element of X is in exactly one of the subsets Si. In other words, S1, S2, …., Sn is a partition of X.

If the subsets S1, S2, …., Sn were allowed to overlap, then a more profound principle will be needed--the principle of inclusion and exclusion.

Frequently, instead of asking for the number of elements in a set *perse*, some problems ask for how many ways a certain event can happen.

The difference is largely in semantics, for if A is an event, we can let X be the set of ways that A can happen and count the number of elements in X. Nevertheless, let us state the sum rule for counting events.

If E1, ……, En are mutually exclusive events, and E1 can happen e1 ways, E2 happen e2 ways,…. ,En can happen en ways, E1 or E2 or …. or En can happen e1 + e2 + …….. + en ways.

Again we emphasize that mutually exclusive events E1 and E2 mean that E1 or E2 can happen but both cannot happen simultaneously.

The sum rule can also be formulated in terms of choices: If an object can be selected from a reservoir in e1 ways and an object can be selected from a separate reservoir in e2 ways and an object can be selected from a separate reservoir in e2 ways, then the selection of one object from either one reservoir or the other can be made in e1 + e2 ways.

Product Rule: The principle of sequencing counting

If S1, ….., Sn are **nonempty sets, then the number of elements in the Cartesian product S 1 x S2 x ….. x Sn is the product ∏in=1 |S i |. That is,**

| S1 x S2 x ..... x Sn | = **∏in=1| S i |.**

Observe that there are 5 branches in the first stage corresponding to the 5 elements of S1 and to each of these branches there are 3 branches in the second stage corresponding to the 3 elements of S2 giving a total of 15 branches altogether. Moreover, the Cartesian product S1 x S2 can be partitioned as (a1 x S2) U (a2 x S2) U (a3 x S2) U (a4 x S2) U (a5 x S2), where (ai x S2) = {(ai, b1), (ai i, b2), (ai, b3)}. Thus, for example, (a3 x S2) corresponds to the third branch in the first stage followed by each of the 3 branches in the second stage.

More generally, if a1,….., an are the n distinct elements of S1 and b1,….,bm are the m di stinct elements of S2, then S1 x S2 = Uin =1 (ai x S2).

For if x is an arbitrary element of S1 x S2 , then x = (a, b) where a Î S1 and b Î S2. Thus, a = ai for some i and b = bj for some j. Thus, x = (ai, bj) Î(ai x S2) and theref ore x Î Uni =1(ai x S2).

Conversely, if x Î Uin =1(ai x S2), then x Î (ai x S2) for some i and thus x = (ai, bj) where bj i s some element of S2. Therefore, x Î S1 x S2.

Next observe that (ai x S2) and (aj x S2) are disjoint if i ≠ j since if

x Î (ai x S2) ∩ (aj x S2) then x = (ai, bk) for some k and x = (aj, b1) for some l. Bu t then (ai, bk) = (aj, bl) implies that ai = aj and bk = bl. But since i ≠ j , ai ≠ a j.

Thus, we conclude that S1 x S2 is the disjoint union of the sets (ai x S2). Furthermore |ai x S2| = |S2| since there is obviously a one-to-one correspondence between the sets ai x S2 and

S2, namely, (ai, bj) → bj.

Then by the sum rule |S1 x S2| = ∑nni=1 | ai x S2|

7.(n summands) |S2| + |S2| +…..... + |S2|

8.n |S2|

9.nm.

Therefore, we have proven the product rule for two sets. The general rule follows by m athematical induction.

We can reformulate the product rule in terms of events. If events E1, E2 , …., En ca n happen e1, e2,…., and en ways, respectively, then the sequence of events E1 first,

followed by E2,…., followed by En can happen e1e2 …en ways.

In terms of choices, the product rule is stated thus: If a first object can be chosen e1 w ays, **a second e2 ways , …, and an nth object can be made in e1e2….en ways.**

Pigeon hole principles and its application:

The statement of the *Pigeonhole Principle*:

If m pigeons are put into m pigeonholes, there is an empty hole *iff* there's a hole with more than on e pigeon.
If n > m pigeons are put into m pigeonholes, there's a hole with more than one pigeon.

Example:
Consider a chess board with two of the diagonally opposite corners removed. Is it possible to co ver the board with pieces of domino whose size is exactly two board squares?

Solution

No, it's not possible. Two diagonally opposite squares on a chess board are of the same color. Theref ore, when these are removed, the number of squares of one color exceeds by 2 the number of square s of another color. However, every piece of domino covers exactly two squares and these are of diffe rent colors. Every placement of domino pieces establishes a 1-
1 correspondence between the set of white squares and the set of black squares. If the two sets have different number of elements, then, by the Pigeonhole Principle, no 1-
1 correspondence between the two sets is possible.

Generalizations of the pigeonhole principle
A generalized version of this principle states that, if n discrete objects are to be allocated to m containers, then at least one container must hold no fewer than objects, where is the ceiling function, denoting the smallest integer larger than or equal to x. Similarly, at least one container must hold no more than objects, where is the floor function, denoting the largest integer smaller than or equal to x.
A probabilistic generalization of the pigeonhole principle states that if n pigeons are randomly put into m pigeonholes with uniform probability 1/m, then at least one pigeonhole will hold more than one pigeon with probability

where $(m)_n$ is the falling factorial $m(m-1)(m-2)...(m-n+1)$. For $n = 0$ and for $n = 1$ (and $m > 0$), that probability is zero; in other words, if there is just one pigeon, there cannot be a conflict. For $n > m$ (more pigeons than pigeonholes) it is one, in which case it coincides with the ordinary pigeonhole principle. But even if the number of pigeons does not exceed the number of pigeonholes ($n \leq m$), due to the random nature of the assignment of pigeons to pigeonholes there is often a substantial chance that clashes will occur. For example, if 2 pigeons are randomly assigned to 4 pigeonholes, there is a 25% chance that at least one pigeonhole will hold more than one pigeon; for 5 pigeons and 10 holes, that probability is 69.76%; and for 10 pigeons and 20 holes it is about 93.45%. If the number of holes stays fixed, there is always a greater probability of a pair when you add more pigeons. This problem is treated at much greater length at birthday paradox.
A further probabilistic generalisation is that when a real-valued random variable X has a finite mean E(X), then the probability is nonzero that X is greater than or equal to E(X), and similarly the probability is nonzero that X is less than or equal to E(X). To see that this implies the standard pigeonhole principle, take any fixed arrangement of n pigeons into m holes and let X be the number of pigeons in a hole chosen uniformly at random. The mean of X is n/m, so if there are more pigeons than holes the mean is greater than one. Therefore, X is sometimes at least 2.
Applications:
The pigeonhole principle arises in computer science. For example, collisions are inevitable in a

hash table because the number of possible keys exceeds the number of indices in the array. No hashing algorithm, no matter how clever, can avoid these collisions. This principle also proves that any general-purpose lossless compression algorithm that makes at least one input file smaller will make some other input file larger. (Otherwise, two files would be compressed to the same smaller file and restoring them would be ambiguous.)
finds that it is not easy to explicitly find in tegers , such that | − | < , where > 0 is a n m C name small positive number and a is some arbitrary irrational number. But if one takes M such that 1/M < e, by the pigeonhole principle there must be n1, n2 {1, 2, ..., M + 1} such that n1a and n2a are in the same integer subdivision of size 1/M (there are only M such subdivisions between consecutive
integers). In particular, we can find n1, n2 such that n1a is in (p + k/M, p + (k + 1)/M), and n2a is in (q + k/M, q + (k + 1)/M), for some p, q integers and k in {0, 1, ..., M − 1}. We can
then easily verify that (n2 − n1)a is in (q − p − 1/M, q − p + 1/M). This implies that [na] < 1/M < e, where = n2 −
n1 or n = n1 − n2. This shows that 0 is a limit point of {[na]}. We can then use
this fact to prove the case for p in (0, 1]: find n such that [na] < 1/M < e; then if p (0, 1/M], we are done. Otherwise in (/ , (+ 1)/], and by setting = sup{ : [ ] < /

C

|[(k + 1)na] − p| < 1/M < e.

A generalized version of this principle states that, if *n* discrete objects are to be allocated to *m* conta iners, then at least one container must hold no fewer than objects, where is the ceiling function, den oting the smallest integer larger than or equal to *x*. Similarly, at least one container must hold no m ore than objects, where is the floor function, denoting the largest integer smaller than or equal to *x*.

A probabilistic generalization of the pigeonhole principle states that if *n* pigeons are randomly put in to *m* pigeonholes with uniform probability 1/*m*, then at least one pigeonhole will hold more than one pigeon with probability

where $(m)_n$ is the falling factorial $m(m-1)(m-2)...(m-n+1)$. For $n = 0$ and for $n = 1$ (and $m > 0$), that probability is zero; in other words, if there is just one pigeon, there cannot be a conflict. For $n > m$ (more pigeons than pigeonholes) it is one, in which case it coincides with the ordinary pigeonhole pri nciple. But even if the number of pigeons does not exceed the number of pigeonholes ($n \leq m$), due to the random nature of the assignment of pigeons to pigeonholes there is often a substantial chance th at clashes will occur. For example, if 2 pigeons are randomly assigned to 4 pigeonholes, there is a 25 % chance that at least one pigeonhole will hold more than one pigeon; for 5 pigeons and 10 holes, th at probability is 69.76%; and for 10 pigeons and 20 holes it is about 93.45%. If the number of holes s tays fixed, there is always a greater probability of a pair when you add more pigeons. This problem i s treated at much greater length at birthday paradox.

A further probabilistic generalisation is that when a real-
valued random variable *X* has a finite mean *E*(*X*), then the probability is nonzero that *X* is greater tha n or equal to *E*(*X*), and similarly the probability is nonzero that *X* is less than or equal to *E*(*X*). To see that this implies the standard pigeonhole principle, take any fixed arrangement of *n* pigeons into *m* holes and let *X* be the number of pigeons in a hole chosen uniformly at random. The mean of *X* is *n*/ *m*, so if there are more pigeons than holes the mean is greater than one. Therefore, *X* is sometimes at least 2.

Applications:

The pigeonhole principle arises in computer science. For example, collisions are inevitable in a hash table because the number of possible keys exceeds the number of indices in the array. No hashing algorithm, no matter how clever, can avoid these collisions. This principle also proves that any general-purpose lossless compression algorithm that makes at least one input file smaller will make some other input file larger. (Otherwise, two files would be compressed to the same smaller file and restoring them would be ambiguous.

A notable problem in mathematical analysis is, for a fixed irrational number *a*, to show that the set {[*na*]: *n* is an integer} of fractional parts is dense in [0, 1]. After a moment's thought, one

The principles of Inclusion – Exclusion:

Semigroup: Let S be a non-empty set with a binary operation * defined on it. The algebraicsystem (S, *) is called a semigroup if * is associative.

(i.e) $a*(b*c)=(a*b)*c \quad \forall a,b,c \in S$

Examples:

1. (2Z, +) and (2Z, .)aresemigroups.
2. If S is the set of all $n\times n$ matrices with real entries, then (S, +) and (S, .) are semigroups, where + is matrix addition and . is matrix multiplication.
3. (Z, -) is not a semigroup because ' – ' is not associative, since $2-(3-4)\neq(2-3)-4$

Monoid: A semigroup(M, *) with identity element **e** is called a monoid. Sometimes a monoid is denoted as (M, *, **e**) indicating the fact that **e** is the identity element.

Examples:

1. $(N,\times)$ia a monoid with identity element**1**. But **(N, +)** is not a monoid, since identityf or + is **0**, which is not in **N**.
2. The set of non negative integers $S = N \cup \{0\}$ is the monoid under + and $\times$. (i.e) (S, +) and (S, $\times$) are monoids with identity 0 and 1.

   Let S be the non-empty set and let S^S denote the set of all mappings from S to S. Let . denote the composition of functions operation.

   If $f,g \in S^S$, then f and g are functions from $S \to S$. Their composite $(f \circ g)(x)= f(g(x)) \forall x \in S$. Then $f \circ g$ is a function from $S \to S$ and $f \circ g \in S^S$. We know composition function is associative.

   The identity function $I : S \to S$ defined by $I(x)= x \ \forall x \in S$ is the identity element of S^S. For $(I \circ f)(x)= I(f(x))=f(x) \forall x \in S$ and $(f \circ I)(x)= f(I(x))= f(x) \forall x \in S$

$\therefore I \circ f = f \circ I = f \quad \forall f \in S^S . \therefore (S^S,\circ)$is a monoid with identity I.

Sub semigroups: Let (S, *) be a semigroup and let $T \subseteq S$ closed under *, then (T, *) is called a sub semigroup.

be a noe-empty subset. If T is

Submonoid: Let (M, *) be monoid and **e** be the identity. If T be a non-empty subset of Mand if T is closed under * with $e \in T$, then (T, *) is called a submonoid of (M, *).

Examples:

1. $(N,\times)$ is a semigroup. Let T = 3N then $T \subset S$, if $x, y \in T$ then x = 3r, y = 3s for some positive integers r and s. Now x+y = 3r× 3s = 3(3rs) ∈ 3N = T. ∴ T is closed under×. Hence (T, ×) is a sub semigroup of (N, ×). More generally, if S = mN, where m is afi xed positive integer, then (S, ×) is a sub semigroup.
2. For the semigroup (N, +), (2N, +) is a sub semigroup.
3. (Z, +) is monoid with identity 0. If T = the set of all non-negative integers = {0, 1, 2,3, ...}, then (T, +) is a submonoid with identity 0.

Problems:

1. For any commutative monoid (M, *), prove that the set of all idempotent elements of M forms a submonoid.

   Solution: Given (M, *) be a commutative monoid.L

   et e be its identity element.

   Let S be the set of all idempotent elements of M. (i.e) $S = \{x \in M / x*x = x\}$

Since e*e = e, e is an idempotent element of M.

$\therefore e \in S$ and hence S is non-empty.

Let $a, b \in S$ be any two elements. They are idempotent elements.

∴ a*a = a and b*b = b.

We have to prove a*b is idempotent.

Now (a*b)*(a*b) = a*(b*a)*b [Since * is associative

= a*(a*b)*b [Since * is commutative

= (a*a)*(b*b) [Since * is associative

= a*b

Hence a*b is idempotent and so S is closed under * and $e \in S$.So

(S, *) is a submonoid of (M, *).

2. Show that every finite semigroup has an idempotent element.

Solution: Let (S, *) be a finite semigroup.

Let $a \in S$, then by closure $a, a^2, a^3, a^4, ...$ are all elements of S.

Since S is finite, these elements are not all different. So we have repetitions.L

et $a^m = a^r$, *where* $r > m$. Let r = m+n.

$\therefore\ a^m = a^r = a^{m+n}$

Then $a^m * a^n = a^{m+n} * a^n \Rightarrow a^{m+n} = a^{m+2n}$

And $a^{m+n} * a^n = a^{m+2n} * a^n \Rightarrow a^{m+2n} = a^{m+3n}$ and so on.

$\therefore a^m = a^{m+n} = a^{m+2n} = a^{m+3n} = ... = a^{m+mn}$

Since $a^m = a^{m+mn}$

We have $a^{nm} = a^{nm+mn}$ [Replacing m by nm]

$= a^{nm} * a^{mn}$

This proves that a^{mn} is an idempotent element of S.

$\therefore$ Every finite semigroup has an idempotent element.

3. Show that the set of all invertible elements of a monoid form a group under the sameo peration as that of the monoid.

Solution: Let (M, *) be a monoid having the identity e.

Let G be the set of all invertible elements of M.

Since $e^{-1} = e$, we have $e \in G$. So G is non- empty. Further inverse is unique.

Let $a, b \in G$, then a and b have inverse. Let a^{-1}, b^{-1} be their inverses.We have to prove that $a * b \in G$.

S we have to prove that it is invertible.

Now consider $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1}$

$= a*(e)*a^{-1}$

$= a*a^{-1}$

$= e$

And $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b$

$= b^{-1}*(e)*b$

$= b^{-1}*b = e$

$\therefore b^{-1}*a^{-1}$ is the inverse of a*b.(i.e) a*b i

s invertible.

Hence $a * b \in G$. So G is closed under *.

Associativity: Since G is a subset of M, associativity is inherited in G.

Identity: $e \in G$ is the identity. Since a*e = e*a = a, $\forall\, a \in G$.

Inverse: Let $a \in G$ be any element. So 'a' is invertible.

$\therefore a*a^{-1} = a^{-1}*a = e \Rightarrow (a^{-1})^{-1}*a^{-1} = a^{-1}*(a^{-1})^{-1} = e$ [Since $(a^{-1})^{-1} = a$

Since a^{-1} is invertible and so $a^{-1} \in G$.

Hence inverse exists for every $a \in S$. So (G,*) is a group.

4. If **Z_6** is the set of equivalence classes generated by the equivalence relation"Congru ence modulo 6", prove that $(Z_6, \times_6)$ is a monoid where the operation $\times_6$ on Z_6 is defined as $[j] \times_6 [k] = [(j \times k) \bmod 6]$ for any $[j], [k] \in Z_6$.

Solution: We know $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$. We shall form the composition table.

$\times_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

$\therefore$ Z_6 is closed under $\times_6$.

Associativity: Since $[a] \times_6 [b] \times_6 [c] = [a] \times_6 [bc]$

$= [a(bc) \bmod 6]$

$\times_6$ depends on associativity of usual multiplication. $\therefore$ $\times_6$ is associative.

Identity: From the table we find, $[1] \times_6 [a] = [a]$ for all $[a] \in Z_6$.

$\therefore$ [1] is the identity element. Hence $(Z_6, \times_6)$ is a monoid.

Homomorphism: Homomorphism is a structure preserving map between two algebraics ystems of same type. Homomorphisms of semigroups and monoids are useful in the econ omical design of sequential machines and in formal languages.

Homomorphism of semigroups: Let (S, *) and (T, **.**) be two semigroups. A mapping $f : S \to T$ is called homomorphism if $f(a*b) = f(a).f(b) \quad \forall a,b \in S$.

The homomorphism of semigroups f is called a monomorphism if f is one-one.

f is called epimorphism if f is onto.

f is called an isomorphism if f is one-one and onto.

If f is an isomorphism of S onto T, we say S is isomorphic to T as semigroups.

Example: Consider the semigroups (N, +) amd (Z_m, $+_m$). Define $f : N \to Z_m$ by $f(a) = [a]$ then $f(a+b) = [a+b] = [a] +_m [b] = f(a) +_m f(b)$.

$\therefore$ f is a semigroup homomorphism.

Monoid Homomorphism: Let (M,*) be a monoid with identity e and (T, .) be a monoid with identity e'. A mapping $f : M \to T$ is called a homomorphism of monoids if $f(a*b) = f(a).f(b) \quad \forall a,b \in M$ and $f(e) = e'$.

The homomorphism of monoids f is called

(i) a monomorphism if f is one-one
(ii) an epimorphism if f is onto
(iii) an isomorphism if f is one-one and onto.

Theorem 1: Let (S,*) be a semigroup and (T, .) be an algebraic system. Ifo $f : S \to T$ is an nto homomorphism, then (T, .) is also a semigroup.

Proof: Given (S,*) is a semigroup and $f : S \to T$ is an onto homomorphism.

(i.e) $f(a*b) = f(a).f(b)$

To prove (T, .) is a semigroup, we have to prove (**.**) is associative.

Let $x, y, z \in T$ be any three elements. Since f is onto, we can find pre images $a,b,c \in S$ such that $f(a) = x, \; f(b) = y, \; f(c) = z$

Now $f[a*(b*c)] = f(a).f(b*c) = f(a).(f(b).f(c)) = x.(y.z)$and
$f[(a*b)*c] = f(a*b).f(c) = (f(a).f(b)).f(c) = (x.y).z$

Since $a*(b*c) = (a*b)*c$, $f[a*(b*c)] = f[(a*b)*c]$.

$\therefore \; x.(y.z) = (x.y).z, \forall \; x, y, z \in T$.

Hence (T, .) is a semigroup.

Theorem 2: Let (S, *) and (T, .) be semigroups and $g : S \to T$ be a homomorphism. If $a \in S$ is an idempotent element. Prove that $g(a)$is an idempotent element of T.

Proof: Given $g : S \to T$ is a homomorphism of semigroups and $a \in S$ is an idempotent element.

$\therefore$ a*a = a $\Rightarrow g(a*a) = g(a) \Rightarrow g(a).g(a) = g(a)$ [Since g is a homomorphism

$\therefore \; g(a)$ is an idempotent element of T.

Theorem 3: If (M, *) is a monoid having identity e and g is an epimorphism from (M, *) toa n algebraic system (T, .), then (T, .) is a monoid.

Proof: Given (M, *) is a monoid with identity e.

$\therefore$ (M, *) is a semigroup and($g : M \to T$ is an epimorphism.

i.e) an onto homomorphism.

$\therefore$ (T, .) is also a semigroup. [By theorem 1

We have to only prove (T, .) has identity.

Let $a \in M$ be any element and $e \in M$ is the identity.

$\therefore\ a*e = a = e*a$

Now $a*e = a \Rightarrow g(a*e) = g(a) \Rightarrow g(a).g(e) = g(a)$ and
$e*a = a \Rightarrow g(e*a) = g(a) \Rightarrow g(e).g(a) = g(a)$

$g(a).g(e) = g(e).g(a) = g(a) \Rightarrow g(e)$ is the identity of (T, .) and hence (T, .) is a monoid.

Theorem 4: Let (S, *) , (T, .) and $(V, \oplus)$ be semigroups and $g : S \to T, h : T \to V$ be semigroup homomorphism such that their composite $h \circ g : S \to V$ is defined. Prove that $h \circ g$ is a semigroup homomorphism of (S, *) to $(V, \oplus)$.

Proof: Given $g : S \to T, h : T \to V$ are semigroup homomorphisms.

We have to prove $h \circ g : S \to V$ is a homomorphism. L

et $a, b \in S$ be any two elements.

$$\therefore\ (h \circ g)(a*b) = h(g(a*b)) = h(g(a).g(b)) = h(g(a)) \oplus h(g(b))$$
$$= (h.g)(a) \oplus (h.g)(b)$$

$\therefore\ h \circ g$ is a homomorphism of semigroups.

Theorem 7: Show that monoid homomorphism preserves the property of invertibility.

Proof: Let (M, *) and (M', .) be two monoids with identity e and e' respectively.

Let $g : M \to M'$ be a homomorphism.

Let $a \in M$ be an element with inverse a^{-1}.

We have to prove $g(a^{-1}) = [g(a)]^{-1}$. Since a^{-1} is the inverse of a, we have
$a*a^{-1} = a^{-1}*a = e$.

Now $a*a^{-1} = e \Rightarrow g(a*a^{-1}) = g(e) = e' \Rightarrow g(a).g(a^{-1}) = e'$

Similarly, $a^{-1}*a = e \Rightarrow g(a^{-1}*a) = g(e) = e' \Rightarrow g(a^{-1}).g(a) = e'$

$g(a^{-1}) = (g(a))^{-1}$

.