UNIVERSITY OF AGRICULTURE, ABEOKUTA,DEPARTMENT OF MATHEMATICS

MTS 211-20011/2012 First Semester Lecture note;

COURSE TITLE:Abstract Algebra

Sets

Definition

A set is a collection of objects which can be distinguished from each other.We shall sat that a set is defined if whenever any object is given, it is possible to decide whether or not it belongs to the set.The objects comprising the set are generally called the elements of the set and they may be finite or infinite in number.

Example:

1. A school constitutes a set and each student or teacher is an element of the set.

2. The whole number $1, 2, 3, ...$ constitutes a set and each whole number is an element of this set.

Capital letters are use to denote sets and small letters $a, b, c, d, ...$ to denote elements.The symbol needed for enclosing the elements of a set is a pair of braces,so that when a set A is specified by listing the elements a, b, c, d and e contained in A,we will write

$$A = \{a, b, c, d, e\}$$

The symbol : or | is used for 'such that'. Example

$N = \{n : n \quad is \quad a \quad whole \quad number\}$ indicates that N is the set of all elements n such that N is a whole number .That is N is the set of all whole number.

Membership of a set :

The element that make up a set are usually called member of that set.We use the symbol $\in$ to stand for 'is a member (element) of' while the symbol $\notin$ stand for 'is not a member (element) of' e.g

If $A = \{a, b, c\}$ then $a \in A, d \notin A$

Finite and Infinite set:

A finite set is one whose members are countable.e.g

1. Consider a set $A = \{n : n \quad is \quad a \quad whole \quad number, 0 < n < 20\}$.

2. Member of a football team.

An infinite set is one whose elements are uncountable,as they are infinitely numerous. e.g

The set N of all whole numbers is an infinite set and we could write it thus:

$N = \{1, 2, 3, ...\}$ with ..., to show it goes on forever.

The set consisting of a single object is called a singleton set.

Subsets:

A set T is called a subset of a set S if every element of T ia also an element of S.We write $T \subseteq S$ or $S \supseteq T$. Observe that this definition implies that every set is a subset of itself.However,if T is a subset of S and $T \neq S$,we say that T is a proper subset of S and then write $T \subset S$ or $S \supset T$.Thus T is a proper subset of S if T is a subset of S and there exist at least one element of S that is not in T.

Two sets S, T are equal if and only if $S \subseteq T$ and $T \subseteq S$

Example:

Kano state,Lagos state,Oyo state is a proper subset of states in Nigeria

Empty set:

A set is said to be empty or null if it contains no elements.If a set S is empty,we write $S = \phi$ or $\{\}$. e.g

$S = \{x|x \in R \quad and \quad x^2 + 1 = 0\} = \phi$ since $x^2 + 1 = 0$ has no real roots.

Empty set ϕ is a subset of every set.

Equality of sets:

Two sets are equal if they have the same elements e.g

$\{a, e, i, o, u\} = \{e, o, u, i, a\}$.

Also we introduce two new symbols namely $\Longrightarrow$ and $\Longleftrightarrow$. e.g

$x \in \{x, y, z\} \Longrightarrow \{x\} \subset \{x, y, z\}$.

This means that the statement on the right hand side must follow from the statement on the left but the statement on the left does not necessarily follow from that on the right.

$\Longrightarrow$ stands for implies and $\Longleftrightarrow$ stands for 'implies and implied by' or 'if and only if'

For any two sets A and B,

If $x \in B \Longrightarrow x \in A$, then $B \subset A$.

$A \subset B$ and $B \subset A \Longrightarrow A = B$.

Universal set :

The set containing all elements under discussion in a particular problem is called the universal set and is denoted by symbol Σ

Complement:

Given a set A,then the set which contains all the elements of the universal set,which are not elements of A is called the complement of A and is denoted by A' or A^c.Thus

$A' = \{x : x \in \Sigma \quad and \quad x \notin A\}$ e.g

$\Sigma = \{1, ..., 8\}$,$A = \{2, 4, 6, 8\}$, $A' = \{1, 3, 5, 7\}$.

Equivalent set:

If to each elements of a set A there corresponds an element of another set B and to each element of B there corresponds an element of A,the element of the two sets are said to be in one-to-one correspondence.The sets are then said to be equivalent.The symbol which expresses this relationship is $\sim$ and $A \sim B$ means that A is equivalent to B.e.g

The sets $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$ are equivalent because we could make the first element of A correspond to the first element of B and so on.

The sets $A = \{a, b, c, d\}$ and $B = \{1, 2, 3, 4, 5\}$ are not equivalent because even through we can pair all the elements of A with some of the elements of

B,the reverse procedure leaves one element without any pair.

Power set:

The family β of all subsets of S is called the power set of S and is denoted by 2^s.

For example

Is $S = \{1, 2, 3\}$,$\beta = \{\phi, S, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{3, 1\}\} = 2^3$.

Definition:

Let Ω be any set .The family or collection of sets S_ω written $\{S_\omega\}_{\omega\in\Omega}$ is said to be indexed by Ω and Ω is called an indexing set for this family.

For example

1. Let $\Omega = N =$ set of all natural number and $S_n = 1 + \frac{1}{2} + ... + \frac{1}{2^n}$.Then the family $\{S_n|n \in N\}$ is indexed by $\Omega = N$.

2. (*) Let $\Omega = \{1, 2, 3, 4, 5\}$ and S_ω=all integral multiples of ω.Thus $S_1 = Z$

   $S_2 = 2Z = \{..., -4, -2, 0, 2, 4, ...\}$

   $S_3 = 3Z = \{..., -6, -3, 0, 3, 6, ...\}$

   $S_\omega = \{..., -2\omega, -\omega, 0, \omega, 2\omega, ...\}\omega \in \Omega$

3. Let $\Omega =$ the set of all English words and $S_\omega = \{x|x \ \ is \ a \ \ letter \ \ in \ \ \omega \in \Omega\}$

   Suppose ω is the word 'fence' then $S_\omega = \{e, f, n, c\}$

4. let $\Omega = \{a, b, c\}$

   $S_a = \{all \quad even \quad integers\}$

   $S_b = \{x \in Z | -10 \leq x \leq 5\}$

   $S_c = \{all \quad integers \quad \geq -5\}$

The last example shows that indexing set may have no direct bearing on the sets being indexed. Ω may just provide a way of distinguishing the set concerned.

Intersection:

Suppose we have two sets S, T.The intersection of S and T is the set of all elements common to both S and T and is denoted by $S \cap T$. Thus $S \cap T = \{x | x \in S \quad and \quad x \in T\}$.Observe that if $T \subset S$, then $S \cap T = T$.Also if $S \cap T = \phi$,we say S and T are disjoint.

If $\Omega = \{\omega\}$ is any indexing set for a family $\{S_\omega\}_{\omega \in \Omega}$ we define the intersection $\cap_{\omega \in \Omega} S_\omega$ of members of this family as the set of all elements common to all the $S_\omega, \omega \in \Omega$.Thus $\cap_{\omega \in \Omega} S_\omega = \{x | x \in S_\omega \quad for \quad each \quad \omega \in \Omega\}$.

For example

Let $S = \{1, 3, 5, 7, 9\}$,$T = \{x \in Z | x^3 - 6x^2 + 11x - 6 = 0\}$.Then $S \cap T = \{1, 3\}$.

Union:

Let S, T be two sets.We define the union of S and T ,written $S \cup T$, as the set of elements which are either in S or T.Thus $S \cup T = \{x | x \in S \quad or \quad x \in T\}$.It follows that $S \cup T = T \cup S$.If Ω is an indexing set for a family $\{S_\omega\}_{\omega \in \Omega}$,then the union $\cup_{\omega \in \Omega} S_\omega$ of the sets S_ω is defined as

$\cup_{\omega\in\Omega}S_\omega = \{x|x \quad is \quad in \quad at \quad least \quad one \quad S_\omega.$

For example

In example (*),$\cup_{\omega\in\Omega}S_\omega = Z$.

Theorem: If S, T are two sets,then

1. $S \cap (T \cap V) = (S \cap T) \cap V$
2. $(S \cup T) \cup V = S \cup (T \cup V)$
3. $S \cap (T \cup V) = (S \cap T) \cup (S \cap V)$
4. $S \cup (T \cap V) = (S \cup T) \cap (S \cup V)$

Proof: (1)-(2) (exercise)

3. Let $x \in L.H.S$,then $x \in S$ and $x \in T \cup V$. This implies that $x \in S$ and $x \in (T \quad or \quad V)$.

i.e $x \in (S \quad and \quad T)$ or $x \in (S \quad and \quad V)$.

i.e $x \in S \cap T$ or $x \in S \cap V$,

i.e $x \in S \cap T \cup x \in S \cap V$

Hence $x \in R.H.S$.

Therefore $S \cap (T \cup V) \subseteq (S \cap T) \cup (S \cap V)$.

Let $x \in R.H.S$,then $x \in S \cap T$ or $x \in S \cap V$.

i.e $x \in (S \quad and \quad T)$ or $x \in (S \quad and \quad V)$

$\implies \quad that \quad x \in S \quad and \quad x \in T \quad or \quad V$

i.e $x \in S \cap (T \cup V)$

Hence $(S \cap T) \cup (S \cap V) \subseteq S \cap (T \cup V)$

Therefore $(S \cap (T \cup) = (S \cap T)n \cup (S \cap V)$

Definition:

A family $\{S_\omega\}_{\omega \in \Omega}$ of subset S_ω of a set S is said to form a partition if

1. $S = \cup_{\omega \in \Omega} S_\omega$ and

2. For any $S_\omega, S_{\omega'}$,either $S_\omega = S_{\omega'}$ or $S_\omega \cap S_{\omega'} = \phi$

i.e $\omega \neq \omega' \implies S_\omega \cap S_{\omega'} = \phi$

Definition:

Let S, T be two sets,we define $S - T$,the difference of S and T (sometimes read 'S minus T) as the set of elements which are in S but not in T.

For example

Let $S = \{1, 2, 3, 4, 7, 10\}$

$T = \{2, 7, 5, 8, 11\}$

$S - T = \{1, 3, 10\}$

Theorem:

1. $A - B \subset A$

2. $(A - B) \cap B = \phi$

Proof:

1. Let $x \in (A - B)$. By definition $x \in A$ and $x \notin B$. In any case $x \in A$,so $(A - B) \subset A$

2. Let $x \in (A - B) \cap B$

Then $x \in A - B$ and $x \in B$ (1)

Now $x \in A - B$ implies that $x \in A$ and $x \notin B$. This contradicts (1).Hence there does not exist any element in $(A - B) \cap B$.

Therefore $(A - B) \cap B = \phi$.

Theorem:

1. $\Sigma' = \phi, \phi' = \Sigma$

2. $(S')' = S$

3. $(S \cup T)' = S' \cap T'$

4. $(S \cap T)' = S' \cup T'$

(3) and (4) are known as De Morgan's law.

Proof.

3. Let $x \in (S \cup T)'$ then $x \notin (S \cup T)$. i.e $x \notin (S \quad or \quad T)$.Then clearly $x \in S'$ and $x \in T'$ which means that $x \in S' \cap T'$ i.e $(S \cup T)' \subseteq S' \cap T'$. Similarly let $x \in S' \cap T'$,then $x \in S'$ and $x \in T'$. i.e $x \notin S$ and $x \notin T$. Hence x cannot be in $S \cup T$,since it is neither in S nor in T. i.e $x \in (S \cup T)'$.

Therefore $S' \cap T' \subseteq (S \cup T)'$.

Therefore $(S \cup T)' = S' \cap T'$.

Definition: Let S, T be two sets.The symmetric difference of S and T is defined as $(S \cup T) - (S \cap T)$ and written as $S \triangle T$.

Definition: Let $\{S_\omega\}_{\omega \in \Omega}$ be a family of sets indexed by Ω. The disjoint union or set sum of S_ω is define as $\cup_{\omega \in \Omega} \{S_\omega \times \{\omega\}\}$ and written as $\vee_{\omega \in \Omega} S_\omega$. If sets S_ω are disjoint then $\vee_{\omega \in \Omega} S_\omega$ and $\cup_{\omega \in \Omega} S_\omega$ have the same number of elements.

For example.

1. Let $\Omega = \{1, 2\}, S_1 = \{a, b\}, S_2 = \{c, d\}$

Then $S_1 \vee S_2 = \{(a, 1), (b, 1), (c, 2), (d, 2)\}$

2. Let $\Omega = \{a, b, c\}$

$S_a = \{1, 2, 3, 6, 8, 10\}, S_b = \{2, 4, 6, 7, 9\}, S_c = \{4, 11, 6, 1, 3, 18\}$

Then $S_a \vee S_b \vee S_c = (S_a \times \{a\}) \cup (S_b \times \{b\}) \cup (S_c \times \{c\})$. Note that $S_a \cup S_b \cup S_c$ has 11 elements but $S_a \vee S_b \vee S_c$ has 17 elements.

Definition: The cartesian product (or product set) of S and T written as $S \times T$ is the set of all ordered pair (a, b) such that $a \in S$ and $b \in T$.

If S or T is a null set,then so is $S \times T$.If S has s elements and T has t elements,$S \times T$ has st elements. If either S or T is infinite and the other is non-empty,then $S \times T$ is infinite.

For example

Let $S = \{c, d\}, T = \{4, 7, 9\}$ then $S \times T = \{(c, 4), (c, 7), (c, 9), (d, 4), (d, 7), (d, 9)\}$.

Hence $S \times T$ has 6 elements.

Definition: The cartesian product $S_1 \times ... \times S_n$ of n sets $S_1, ...S_n$ as the set of all n-tuples $(\alpha_1, ..., \alpha_n)$ where $\alpha_i \in S_i, i = 1, 2, ..., n$ with the understanding that $(\alpha_1, ..., \alpha_n) = (\alpha'_1, ..., \alpha'_n)$ if and only if $\alpha_i = \alpha'_i$.

For example

The Euclidean 3-space $= R \times R \times R = \{(a, b, c) | a, b, c \in R\}$.

Definition: An open sentence in a single variable x is an expression of the form $p(x)$ such that when x is replaced by a specific value like a,then $p(aP$ is either true or false.

An open sentence in two variables x, y is an expression of the form $p(x, y)$ such that whenever x, y are given specific values a, b say,then $p(a, b)$ is either true or false.

For example

1. x divides y is an open sentence in x and y $p(2, 4)$ is rue but $p(3, 5)$ is false.

2. $x - y = 4$ is an open sentence in two variables $p(12, 8)$ is true but $p(9, 6)$ is false.

Definition: Let S and T be two sets. A propositional function defined on $S \times T$ is an open sentence $p(x, y)$ where x takes in S and y in T.

Definition: Let S, T be two sets.A relation $\sim$ from S to T is given by a triple $(S, T, p(x, y))$ where $p(x, y)$ is a propositional function on $S \times T$.

If $p(a, b)$ is true,write $a \sim b$ (to be read a is in relation to b). Otherwise write $a \sim b$. If $\sim$ is a relation from S to T,we may write it as $\sim: S \longrightarrow T$ and $b =\sim (a)$ where $a \in S, b \in T$ and $p(a, b)$ is true. If $\sim= (S, S, p(x, y))$ we say that $\sim$ is a relation on S.

Definition: Let $\sim$ be a relation from a set S to a set T.The domain D of $\sim$ is the subset of S consisting of first co-ordinate elements of $\sim^*$. i.e

$D = \{a|(a, b) \in\sim^*\}$.

The range F of $\sim$ is the subset of T consisting of second co-ordinate elements of $\sim^*$ i.e

$F = \{b|(a, b) \in\sim^*\}$.

For example

$S = \{1,3,4,7,8\}$,$T = \{1,2,3,4,5,6,7,8,9,10\}$

Let $\sim = (S,T,p(x,y))$ where $p(x,y)$ means $y = 2x$.

Then $\sim * = \{(1,2),(3,6),(4,8)\}$.

$D = \{1,3,4\}, F = \{2,6,8\}$.

Definition: A relation $\sim$ on a set S is said to be reflexive if $a \sim a$ for all $a \in S$ i.e $(a,a) \in \sim^*$ for all $a \in S$.

(**) For example

Let $S = N$,the set of all natural numbers.For $a,b \in N$,let $a \sim b$ means a divides b.Then a divides a for all $a \in N$ and so $\sim$ is reflexive.

Definition: A relation $\sim$ on a set S is said to be symmetric if $a \sim b$ implies that $b \sim a$ for all $a,b \in S$. i.e $(a,b) \in \sim^*$ implies that $(b,a) \in \sim^*$ for all $a,b \in S$.

For example

In the example (**) above,$\sim$ is not symmetric,since a divides b does not necessarily imply that b divides a.

e.g 2|6 but 6 does not divide 2.

Definition: A relation $\sim$ on a set S is said to be transitive if $a \sim b$ and $b \sim c$ imply that $a \sin c$. i.e $(a,b) \in \sim^*, (b,c) \in \sim^*$ imply that $(a,c) \in \sim^*$.

e.g In the example (**) above,$\sim$ is transitive,since a divides b and b divides c imply that a divides c.

Definition: A relation $\sim$ on a set S is called an equivalence relation if $\sim$ is reflexive,symmetric and transitive.

For eaxample

Let $S = Z$. Define $a \sim b$ by 5 divides $(a - b)$. Then $\sim$ is an equivalence relation.

Proof.

5 divides $(a - b)$ implies that $(a - b) = 5k$ for some $k \in Z$ i.e $a = 5k + b$.

So $a \sim a$ since $a = 5k + a$ for some $k = 0 \in Z$ i.e $\sim$ is reflexive.

Now $a \sim b$ implies that $a = 5k + b$. i.e $b = a + 5k'$ where $k' = -k$ also in Z.Hence $a \sim b$ implies $b \sim a$ ie.$\sim$ is symmetric.

Now $a \sim b$,$b \sim c$ all imply that $a = 5k_1 + b, b = 5k_2 + c$ respectively for some $k_1, k - 2 \in Z$ i.e $b = a - 5k - 1$ and $a - 5k - 1 = 5k_2 + c$ i.e $a = 5(k_1 + k_2) + c$. Now $k_1 + k_2 = k \in Z$.Hence $a = 5k + c$ for $k \in Z$.

Thus $a \sim b, b \sim c$ imply $a \sim c$. Hence $\sim$ is transitive.

Therefore $\sim$ is an equivalence relation.

Definition: Let $\sim$ be an equivalence relation on a set S. foe $a \in S$, we define equivalence class of a as the set of all elements b in S such that $a \sim b$ and denote this set by $[a]$.The set of all equivalence classes in S is called the quotient set of $\sim$ and written $s/\sim$.

For example

In the example (**) above,

$[0] = \{b \in Z | b = 5k \quad for \quad all \quad k \in Z\} = \{..., -10, -5, 0, 5, ...\}$

$[1] = \{b \in Z | b = 1 + 5k \quad for \quad all \quad k \in Z\} = \{..., -9, -4, 1, 6, 11, ...\}$

.

.

.

$[4]=\{b\in Z|b=4+5k, \quad for \quad all \quad k\in Z\}=\{...,-6,-1,4,9,14,...\}$

of course $[5]=[0]$

The equivalence classes above are called residue classes modulo 5.In general case where 5 is replaced by an arbitrary positive integer m,then the equivalence classes are called residue classes modulo m and are given by $[0],[1],...,[m-1]$.

Theorem: If $\sim$ is an equivalence relation on a set S,then the set of equivalence classes of $\sim$ gives a partition of S.Conversely,given any partition of S,there exists an equivalence relation $\sim$ on S such that the set of equivalence classes of r is the given partition.

Natural Numbers

Let N be a non-empty set.Assume the following axioms on N.

1. There exists an injective map $\alpha : N \longrightarrow N$;the image $\alpha(a)$ of $a\in N$ is denote a^* and is called the successor of a.

2. The successors form a proper subset of N.

3. (Axioms of induction): Let S be any subset of N which contains a non-successor and such that $a\in S \Longrightarrow a^*\in S$. Then $S=N$.

The first principle of Mathematical Induction

Let T_n be a statement concerning natural members n.Assuming that T_1 is true and that the truth of T_r implies the truth of T_{r^*},then T_n is true for every $n \in N$.

Proof

Suppose S is the subset of elements $r \in N$ for which T_r is true.Then $1 \in S$ and $t \in S \Longrightarrow t^* \in S$.So by the induction axioms $S = N$.Hence the result.

Definition:

(a). Define $'+' : N \times N \longrightarrow N$ such that for $m, n \in N, m_n$ satisfies

1. $m + 1 = m^*$

2. $m + n^* = (m + n)^*$ (b). $'.' : N \times N \longrightarrow N$ such that for $m, n \in N, m, n$ satisfies

1. $m.1 = n$

2. $m.n^* = m.n + m$

Theorem: The following laws are satisfied by the $^{(}+^{)}$ and $^{(}.^{)}$ defined on N. For all $m, n, q \in N$,we have

1. $m + n = n + m; mn = nm$ (Commutative law)

2. $m + (n + q) = (m + n) + q; m(nq) = (mn)q$ (associative law)

3. $m + q = n + q \Longrightarrow m = n; mq = nq \Longrightarrow m = n$ (cancelation law)

4. $m.(n + p) = m.n + m.p$ (distributive law)

Thus $(N, +), (N, .)$ are commutative semi groups.

proof.

2. Let m, n be fixed natural numbers and T_q the assertion that $m+(n+q) = (m+n)+q$ for all $q \in N$.Now T_1 is true by the definition above,since $m+(n+1) = m+n^* = (m+n)^* = (m+n)+1$

We now assume that T_r is true and show that T_{r^*} holds i.e

$m+(n+r)^* = (m+n)+r^*$.Now by the definition above (a-(2))

$m+(n+r^*) = m+(n+r)^* = (m+(n+r))^*$ and also

$(m+n)+r^* = ((m+n)+r)^*$ so that the truth of T_r implies the truth of T_{r^*}

So, T_r is true for all $n \in N$.

Example:

17 divides $(3 \times 5^{2n+1} + 2^{3n+1})$ for any $n \in N$.

proof

let T_n be the statement that 17 divides $3 \times 5^{2n+1} + 2^{3n=1}$. Obviously T_1 holds since

$3 \times 5^3 + 2^4 = 5^2 \times 17 - 2 \times 17 = 23 \times 17$

Now assume T_r holds .We prove that T_{r+1} holds

$3 \times 5^{2(r+1)+1} + 2^{3(r+1)+1}$

$= 5^2(3 \times 5^{2r+1} + 2^{3r+1}) - 2^{2r+1}(5^2 - 8)$

$= 5^2(3 \times 5^{2r+1} + 2^{3r+1}) - 2^{2r+1}) \times 17$

Since T_r holds,$17/(3 \times 5^{2r=1} + 2^{3r+1})$ and so T_{r+1} holds.

Second principle of Mathematical induction

Let T_r be a statement about a natural number r,if for each r,the truth of T_q

for all $q < r$ implies the truth of T_r,then T_n is true for all n.

proof

Let S be the set of natural numbers,such that T_s is not true.If $S \neq \phi$,then by the well-ordering principle (every non-empty subset of N has a first or least element is known as well-ordering principle of N) for N,S has a least element r,say T_r is not true but T_s is true for all $s < r$,contradicting our induction hypothesis. So $S = \phi$. So T_n is true for all $n \in N$.

Integers

Definition: Consider the set $N \times N$,the cartesian product of N by itself. Define a relation on $N \times N$ by $(a, b) \sim (c, d)$ if and only if $a + d = b + c$

Definition: The set I of equivalence classes $[a, b]$ of relation $\sim$ defined above is called the set of integers.

Positive integers

N can be identified with a subset of I as follows:

Define a mapping $\phi : (N, +) \longrightarrow (I, +)$ by $n \longrightarrow [n^*, 1]$.

ϕ is well=defined since $a = b \Longrightarrow a + 1 = b + 1$ i.e $[a^*, 1] = [b^*, 1]$.

ϕ is injective since $[a^*, 1] = [b^*, 1] \Longrightarrow a = b$. So ϕ is an injective homomorphism $N \longrightarrow I$. The elements in the image of N under ϕ are called positive integers.

The Zero integers

For any $a, b \in N$,$[a, a] = [b, b]$ and $[a, b] = [c, b]$ if and only if $c = a$.Also for any $a, c, d \in N$, $[a, a] + [c, d] = [c, d] + [a, a] = [c, d]$.hence $[a, a]$ for any $n \in N$,the zero integer denoted by 0 i.e $[a, a]$ for any $a \in N$ is the identity element of $(I, +)$.

Negative integers

Let I be the set of all $[a, b] \in I$ such that $a < b$. Now for $a, b \in N$, $[a, b] + [b, a] = [a + b, b + a] = [r, r] = 0$ for any $r \in N$. Thus $[b, a]$ is the additive inverse of $[a, b]$.We denote this element by $-[a, b]$.

Definition: Let $n \in I$. The absolute values of a written $|a|$ is defined by $|a| = \{^{a \quad if \quad a \geq 0}_{a \quad if \quad a<0}$

Thus $|a| = 0$ if and only if $a = 0$ and $|a| \in T_=$ if $a \neq 0$.The following laws holds, for $a, b \in I$.

1. $-|a| \leq a \leq |a|$ any $a \in I$

2. $|ab| = |a||b|$

3. $|a| - |b| \leq |a + b| \leq |a| + |b|$

4. $|a| - |b| \leq |a - b| \leq |a| + |b|$.

Divisibility and Primes

Definition: Let b be an integer.An integral divisor or factor of b is an integer a such that $b = ac$ for some integer c. b is also said to be divisible by a or an integral multiple of a. We write $a|b$ if a divides b.If $a|b$ and $0 < a < b$,then a is called a proper divisor of b.

Examples

$4|12$,

$-5|25$

$1| \quad all \quad (integer)$

Theorem: If

1. $a|b$,then $a|bc$ for any integer c

2. If $a|c$ then $a|bx + cy$ for any integers x, y.

3. If $a|b$ and $b|a$,then $a = \pm b$

4. If $a|b$ and $a > 0, b > 0$ then $a \leq b$.

proof

2. $a|b, a|c \implies b = ar$ and $c = as$ for some $r, s \in Z$, $bx + cy = arx + asy = a(rx + ry)$

So $a|(bx + cy)$

Definition: An integer p such that $|p| > 1$ is called a prime or a prime number if the only divisor of p are ± 1 and $\pm p$.

$p > 1$ is a prime if there is no divisor d of p such that $1 < d < p$.An integer a which is not a prime is said to be composite.

Example

1. $5, 7, 13$ are primes

2. $24 = 8 \times 3$ is composite.

Theorem: (Division Algorithm)

For any integers $a, b, b > 0$ there exist unique integers q, r such that $a = bq + r, 0 \leq r \leq b$

Proof.

Consider the set $S = \{a - bx | x \in Z \quad and \quad a - bx \geq 0\}$. $S \neq \phi$ since for instance either $a - b|a| \quad or \quad a + b|a| \in S$. By definition of S,either $0 \in S$, in which case 0 is the least element of S or all elements in S are in N in which case S has to contain a least element by well-ordering principle for N.In any case,S must contain a least element $r \geq 0$. Now,by definition of S, $r = a - bq$ for some $q \in Z$ and so,$a = bq + r$,Since $r \geq 0$,we only have to show $r < b$. Suppose $r \geq b$,then $r - b = a = a - bq - b = a - b(q+1) \geq 0$.However,$a - bq - b < a - bq$,contrary our choice of q such that r is the least element in S. So $0 \leq r < b$.

We now show that q, r are unique.Suppose $a = bq + r = bq' + r'$ where $0 \leq r < b$ and $0 \leq r' < b$.Then $b(q' - q) = r - r'$. So $b|(r - r')$. But $|r - r'| < |b|$. So $r - r' = 0$ i.e $r = r'$.Hence $q = q'$ also.

Definition: In the expression $a = bq = r, q$ is called the quotient and r the remainder.

Definition: Let a, b be two integers.A common divisor of a and b is an integer d such that $d|a$ and $d|b$.Suppose that every common divisor of a and b

also divides d,then d is called the greatest common divisor or highest common factor of a and b written (g.c.d) or (h.c.f) respectively.

We also write $d = (a, b)$. observe that if d, d' are two gcd's of a, b,then $d' = \pm d$.Therefore a g.c.d of two integers is a non-negative integer .

If $(a, b) = 1$,we say that a and b are relatively prime.

Examples:

1. $(18, 42) = 6$

2. $(15, 7) = 1$.so that 15 and 7 are relatively prime.

Theorem: If a, b be two non-zero integers,then $d = (a, b)$ exists.Moreover $d = ua + vb$ for some integers u, v.In general if $d = (a_1, ..., a_n)$ is the h.c.f of n non-zero integers $\{a_i\}$,then $d = \sum_{i=1}^{n} x_i a - i$ for some integers $x_i \in Z$.

proof.

Let $S = \{xa + yb | x, y \in Z\}$. Then S contains a set T of positive integers and by well-ordering principles T has a least element $d = ua + vb$,say for some belongs to Z. Now $a = qd + r$ for some integers q, r where $0 \leq r < d$. So $r = a - qd = (1 - qu)a + (-qv)b$, so that $r \in S$.Hence $r = 0$ and so $a|a$.

Similarly it can be shown that $d|b$.Now suppose any other integer c,say ,divides both a and d. Then $c|ua$ and $c|vb$,so that $c|(ua + vb)$ i.e $c|d$. Therefore $d = ua + vb$ is the h.c.f of a and b.

Example

1. Find $d = (1824, 760)$

Solution

$1824 = 760 \times 2 + 304$

$760 = 304 \times 2 + 152$

$304 = 152 \times 2$

Thus $d = (1824, 760) = 152$

2. Find integers u, v such that $d = ua + vb$ in the example above.

Solution

$152 = 760 - 304 \times 2$

$= 769 - (1824 - 760 \times 2)2$

$= 760 \times 5 - 1824 \times 2$

$= 5b - 2a$

where $a = 1824, b = 760$

So $u = -2, v = 5$

Theorem (**)

1. $(ca, cb) = c(a, b)$ for any positive integer c

2. If $t|a, t|b$ and $t > 0$,then $(\frac{a}{t}, \frac{b}{t}) = \frac{1}{t}(a, b)$

If $d = (a, b)$ then $(\frac{a}{d}, \frac{b}{d}) = 1$

3. $(b, a) = (a, -b) = (a, b + at)$ for any $t \in Z$.

Theorem (***)

If a, b, c are integers and $c|ab, (b, c) = 1$, then $c|a$.

Corollary:

Let p be a prime and $\{a-1, ..., a_n\}$ a set of n integers.If p divides $a_1 a_2 ... a_n$,then p divides at least one of the a_i.

Theorem: Unique factorization theorem or fundamental theorem of Arithmetic:

Every positive integer $n > 1$ can be expressed as a positive prime uniquely,except for the order of prime factors.

proof

We use the second principle of induction.Let T_n be the statement that a given integer $n > 1$ can be expressed as a product of positive primes.

If n is a prime p,then the theorem holds since p is itself a product with only one factor .Otherwise n is composite and therefore has the form $n = ab$ where $a < n, b < n$,Assume that T_r is true for $r < n$,then $a = p_1, ...,_u$, say, and $b = q_1, ..., q_v$ So $n = ab = P_1, ...p_u q_1, ..., q_v$.Thus T_n is true.

We now prove uniqueness. Suppose $n = P_1, ...p_k = q_1, ..., q_j$ are two prime factorizations of n.

Since $P_1|n$,then $P_1|(q_1, ..., q_j)$ and by the corollary above,$P_1|q_j$ for some j.Since both p_1, q_j are primes,we have $P_1 = q_j$.So by cancelation law,we can cancel out P_1, q_j from both sides to have $P_2, ..., p_k = p_1 q_2 ... q_{j-1} q_{j+1} ... q_1$.

If we repeat the process successively with $p_2, p_3, ., .., p_k$ the L.H.S involving the P_i will become 1 and so also with the R.H.S.Hence $l = m$ and every P_i is equal to some q_j.

Corollary: Every integer $n > 1$ can be written in the form $n = P_1^{x_1} ... P_i^{x_i}$ where P_i's are distinct primes and the $\{a_i\}$ are positive integers ≥ 1.

Definition: Let $a_1, ..., a_n$ be non-zero integers.An integer b is called a common multiple of the $\{a_i\}$ if $a_i|b$ for $i = 1, 2, ..., n$. b is called the least common multiple (l.c.m) of the $\{a_i\}$ if b is a common multiple of the $\{a_i\}$ and given any other common multiple c of the $\{a_i\}$,then $b|c$.We denote the l.c.m of the set $\{a_i\}, i = 1, 2, ..., m$ by $[a_1, ..., a_m]$.

For example

l.c.m of 6 and 15 is 30.

Theorem: There are finitely many primes.

Proof.

Suppose there were k of them, say $p_1, ..., p_k$.Consider the integer $1+p_1...p_k = s$.Then $P_i \neq s$ for $i = 1, 2, ..., k$. So if a prime q divides s, q must be distinct from $\{p-i\}$.Now s is either a prime,in which case it is distinct from the p_i,or it is composite, in which case it has a prime factor distinct from the $\}p-i\}$. In either case,we have a prime,different from the $\{p_i\}$,contradicting the fact that there were k of them.So their number must be infinite.

Congruencies

Definition: The equivalence classes of R are called the residue classes of R modulo n.If $b \in [a], b$ is called a residue of a modulo n or b is said to be congruent to a modulo n.

A set $T = \{a_1, ..., a_n\}$ of integers is called a complete residue system modulo n if T contains exactly one integer each from the residue classes modulo n. i.e given any $x \in Z$,there exists one and only one a_i such that $x \equiv a_i(modulon)$.

Let m be some fixed positive integer.Let $a, b \in Z$;then we say that a is congruent to b (modulo m) if and only if $a - b$ is divisible by m.i.e for $k \in Z$ we have $a - b = km$.

Example

1. $\{0, 1, 2, 3, ..., n - 1\}$ is a complete residue system $modn$

2. For $n = 7, \{0, 1, 2, 3, 4, 5, 6\}, \{14, 15, 16, ..., 20\}$ are complete residue systems $mod7$.

Theorem: Let a, b, c, d, n be integers.

1. If $a \equiv b(modn)$ and $c \equiv d(modn0$,then $ra + tc \equiv rb + td(modn)$ where r, t are integers.

2. If $a \equiv b(modn)$ and $c \equiv d(modn)$,then $ac \equiv bd(modn)$

3. If $a \equiv b(modn), c/n$ and $c > 0$,then $a \equiv b(modc)$

4. Let $f(x)$ be a polynomial in $Z[x]$,suppose that $a \equiv b(modn)$,then $f(a) \equiv f(b)(modn)$

5. Suppose that $n_1, ..., n_s$ are integers,then $a \equiv b(modn_i)$ for each i,if and only if $a \equiv b(mod[n_1, ..., n_s])$

Theorem: Let a, c, d, n be integers,$d = (c, n)$.Then $ca \equiv cb(modn)$ if and only if $a \equiv b(mod\frac{n}{d})$.Thus if $d = 1$,then $a \equiv b(modn)$.

Definition: A reduced residue modulo n is a set $V = \{a_1, ...a_s\}$ of integers such that $(a_i, n) = 1$ for each i, a_i does not congruent to $a_j(modn)$ for $i \neq j$ and such that every integer y with $(y, n) = 1$ is congruent modulo n to some members a_i of set V.

Note that if $a \equiv b(modn)$,then $(a, n) \equiv (b, n)$.

Binary operation

The rule by which we combine any two elements of a set to produce a third element is what is we shall call a law of composition or an operation.If any law of composition (*) is such that for all $a, b \in S, a * b$ defines a unique element $c \in S$, we say that the law of composition (*) is closed and (*) is an operation.Clearly $\cap, \cup, \times, +$ are all binary operations which we are familiar with.

Rules of binary operation

1. Closure:

   Let S be a set.An operation * on S is a binary operation if for every pair of elements $a, b \in S.a * b$ is in S.Then S is closed with respect to the binary operation *.

2. Commutative property:

   Let $(S, *)$ be a set S together with a binary operation * on S. The binary operation * on S is said to satisfy the commutative law or property if for every pair a, b in S,$a * b = b * a$

3. Associative property:

   Let $(S, *)$ be a set S together with a binary operation * on S.The binary operation * on S is said to satisfy the associative law or property if for every triple $a, b, c \in S$, $(a * b) * c = a * (b * c)$

Example:

1. (a) i $(N, +), (Z, +), (R, +)$ is closed with respect to addition

ii Addition on N, Z, R is commutative

iii Addition on N, Z, R is associative

(b) i $(N, \times), (Z, \times), (R, \times)$ is closed with respect to multiplication

ii Multiplication on N is commutative

iii Multiplication on N is associative

(c) $(N, -), (Z, -), (R, -)$

(i) N is not closed with respect to subtraction

e.g $2, 3 \in N$ but $2 - 3 = -1 \notin N$

Z is closed with respect to subtraction

R is closed with respect to subtraction

ii Subtraction on N is not commutative

e.g $2, 3 \in N$ but $1 = 3 - 2 \neq 2 - 3 = -1$

Likewise subtraction on Z, R is not commutative.

iii Subtraction on N, Z, R is not associative

(d) $(Z^*, \div), Z^* - Z\ \{0\}, (R^*, \div), R^* = R\ \{0\}$

i Z^*, R^* is not closed with respect to division.

ii Division on Z^*, R^* is not commutative.

e.g $2, 3 \in Z^*, R^*$ but $2 \div 3 \neq 3 \div 2$

iii Division on Z^*, R^* is not associative e.g $2, 3, 5 \in Z^*, R^*$ but $\frac{2}{15} = (2 \div 3) \div 5 \neq 2 \div (3 \div 5) = \frac{10}{3}$

Example 2:

A binary operation $\otimes$ on the set R of real numbers is defined as

$$a \bigotimes b = a + b - 3ab$$

for every pair $a, b \in R$,show that

(a) the operation $\otimes$ on R is commutative

(b) the operation $\otimes$ on R is associative. Solution

(a) Show that $a \bigotimes b = b \bigotimes a$ for every pair $a, b \in R$

$L.H.S = a \bigotimes b = a + b - 3ab = b + a - 3ba = b \bigotimes a = R.H.S$

Hence $\otimes$ on R is commutative.

(b) Show that $(a \bigotimes b) \bigotimes c = a \bigotimes (b \bigotimes c)$ for every $a, b, c \in R$.

$L.H.S = (a + b - 3ab) \bigotimes c$

$= (a + b - 3ab) + c - 3(a + b - 3ab)c$

$= a + b + c - 3ab - 3ac - 3bc + 9abc$

$R.H.S = a \bigotimes (b + c - 3bc)$

$= a + (b + c - 3bc) - 3a(b + c - 3bc)$

$= a + b + c - 3ab - 3ac - 3bc + 9abc$

$= L.H.S$

Hence $\otimes$ on R is associative.

4. Identity:

   Let $(S,*)$ be a set S together with a binary operation * on S.If there is an element $e \in S$ such that

   $$e * a = a * e = a$$

   ,for all $a \in S$,then e is called an identity on set S with respect to the binary operation *

5. Inverses:

   Let $(S,*)$ be a set S together with a binary operation * on S,having an identity e.If a and b are elements in S such that

   $$a * b = b * a = e$$

   then a is called the inverse of b and b is called the inverse of a in $(S,*)$.Denote the inverse of a by a^{-1}.Thus $b = a^{-1}$ and $a = b^{-1}$.

   Example:

   In $(R, \bigotimes)$ where $a \bigotimes b = a + b - 3ab$ for all $a, b \in R$ determine:

   (a) an identity if it exists,

   (b) numbers which have an inverses.

   Solution

   (a) Solve for e,the equation $a \bigotimes e = a$

   $\Longrightarrow a + e - 3ae = a$

$\Longrightarrow (1-3a)e = 0 \Longrightarrow e = 0$

Hence 0 is the identity in $(R, \bigotimes)$

(b) Given a,solve for b,the equation $a \bigotimes b = 0$

$\Longrightarrow a + b - 3ab = 0$

$\Longrightarrow b(1-3a) = -a \Longrightarrow b(3a-1) = a$

$\Longrightarrow b = \frac{a}{3a-1}$,if $a \neq \frac{1}{3}$

$\Longrightarrow a^{-1} = \frac{a}{3a-1}$,if $a \neq \frac{1}{3}$

Hence all numbers,except $\frac{1}{3}$,have inverses in $(R, \bigotimes)$

6. Distributive law:

   Let $(S, *, o)$ be a set S together with two binary operations * and o on S.If for every $a, b, c \in S$,

$$a * (boc) = (a * b)o(a * c)$$

then we say that $*$ is left distributive over o.

If $(aob) * c = (a * c)o(b * c)$ then we say that $*$ is a right distributive over o.

If $*$ is both left distributive and right distributive over o,then $*$ is distributive over o.

Example:

Consider $(R.*, \bigotimes)$ where $a * b = ab$ and $a \bigotimes b = a + b + ab$ for all $a, b \in R$.

(a) Is * distributive over $\bigotimes$?

(b) Is $\otimes$ distributive over *?

Solution

(Excersise)