COURSE TITLE

ABSTRACT ALGEBRA

COURSE CODE

MTS 211

ABST1

LECTURE DAYS

	DAYS	TIME	VENUE
1.			
2.			

LECTURES

LEVELS OF PERFORMANCE

Mark Range Point	Grade
70 - 100	A
60 - 69	B
50 - 59	C
45 - 49	D
40 - 44	E
0 - 39	F

CLASSIFICATION OF GRADE

GPA RANGE	GPA RANGE
4.50 - 5.00	Distinction
3.50 - 4.49	Upper Credit
2.50 - 3.49	Lower Credit
1.50 - 2.49	Pass

1.49 and below failure

BASIC OF GRADE POINT AVERAGE (GPA)

Mark Range	% Page
4.50 - 5.00	First Class
3.50 - 4.49	Second Class Upper
2.50 - 3.49	Second Class Upper
1.50 - 2.49	Third Class
1.00 - 1.40	Pass
0.99	Fail

LEVELS OF PERFORMANCE

Mark Range Point	Grade
70 - 100	A
60 - 69	B
50 - 59	C
45 - 49	D
40 - 44	E
0 - 39	F

-JEKEEN HABEEB
MTS

ABSTRACT ALGEBRA

* Basic set theory: Relation, functions (mapping)
* Number theory: binary operations, algebraic structures.
* Groups and rings: binary logic, method of proof.

BASIC CONCEPT

SET THEORY.

A set is any well-defined collection of objects called the element or members of the set. E.g The collection of all students of FUNAAB that take MTS 211 is a set because it is easy to identify members of the collection.

REPRESENTATION OF A SET

There are basically two ways of representing sets. They are:

i. Roaster Method
ii. Rule Method.

ROASTER METHOD

In this method all the elements of set are listed with a comma. seperating one element from the other. This elemnt are enclosed in bruce or bracket.

RULE METHOD: In this method, a set is defined by specifying a property by that element of the set have in common. The set is then describe as follows:

$\therefore A = \{x : P(x)\}$ or $A = \{x \mid P(x)\}$.

The set $B = \{x : x = n^2;$ when n is a natural number less than or equal to 6 $n \leq 6\}$.

$B = \{1, 2 4 6\}$ or $B = \{1^2, 2^2, 4^2, 6^2\}$

FINITE AND INFINITE SET

A set S is said to be finite, if the process of listing the element terminate. Otherwise S is said to be infinite.

NULL OR EMPTY SET: A set which does not have any element is called a null or an empty set is denoted by $\emptyset$

SUBSET: Let A be a set. A set B is called a subset of set A, if every element in B is also found in A.

NUMBER OF SUBSET OF A SET

If a set A contains n number of element, then the number of subset of A is 2^n.

SUPER SET: If A is a subset of B, then B is called a super set of A.

EQUAL SET: Two set are said to be

equal if every element in A also in B and every element in B is also in A. To show that two set A and B are equal, we pick an arbituary element of A and shaw that the element is also in A.

Cardinal Number of a Set

The cardinal number of set A is the number of element in set A denoted by $|A|$ or $n(A)$.

Ex. 1; Find the number of integers in the set $\{1,2,3\cdots,60\}$ that are not divisible by 2 nor 3 nor 5.

COLLECTION OF SET

If element of a set are themselves set, then such a set is said to be a collection or class of set of family of set. If we wish to consider some of the set in a given class of set then we speak of or sub-class or a sub-collection.

POWER SET OF A SET.

If S is any null empty set, then the family of all subset of S is called the power set of S. it's denoted P(S)

INDEXED AND INDEX.

Sometimes, the elements of one set are used to label the element of another set. Let A_i be a non-emp set for each i in a set I.

Let I = set $\{1,2,3,\cdots,n\}$.

Then the set $A_1, A_2, A_3 \cdots A_n$ are called indexed set while the set I called the index. The suffix i in I is called an index. Such a family of set denoted by $\{A_i\}\ i \in I$ is said to be an indexed family of set.

REMARK: The notions of union and interception can be extended to arbituary indexed family of set.

ARBITUARY UNION OF SET

Let $\{A_i\}\ i \in I$ be an indexed family of set, then the arbituary union of the set A_i, denoted by $\bigcup_{i \in I} A_i$ is the set of element that belong to at least one A_i.

ARBITRARY INTERSECTION OF SET

The arbitrary intersection of the set is denoted by $\bigcap A_i$ it is set of element that belong to all A_i. An indexed family of set is said to be disjoint if $\bigcap A_i = \emptyset$

CARTESIAN PRODUCT OF SET

Let A and B be two sets. The cartesian product of A with B denoted by $A \times B$ is the set of all ordered pairs $\{a,b\}$ where a belong to A $a \in A$ and $b \in B$.

Ex. Let $A = \{1,2,3\}$ and $B = \{4,5\}$. Find $A \times B$ and $B \times A$

SOLUTION

$A \times B = \{(1,4),(1,5),(2,4),(2,5),(3,4),(3,5)\}$

$B \times A = \{(4,1),(4,2),(4,3),(5,1),(5,2),(5,3)\}$

Note the following:

i) The element of A+B are ordered pairs

ii) The ordered pair (a,b) is not the same as the set $\{a,b\}$.

iii) Two ordered pair (a,b) and (c,d) are equal if and only if $a = c$ and $b = d$

partition of a set.

Let A be a non-empty set. A collection of non-empty subset $A_1, A_2, \cdots A_n$ is called a partition of the set A if:

i) A equals the U $A = \bigcup_{i=1}$

ii) $A_i \cap A_j$ is empty if $i \neq j$

Ex. Let $A = \{1,2,3,4\}$, then the collection $B = \{(1,2),(3),(4)\}$ is a partition of the set

N.B: They could be other partition of set A

ASSIGNMENT

Obtain other partitions of set A above.

Equivalent set two sets A and B are said to be equivalent if there is a one to one (1-1) correspondence between their elements. This is also expressed by saying that A is equipotent to B.

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

Exam $B = \{1,2,3,4,5\}$.

Then set A is equivalent to Set B. This is so because there is a (1-1) correspondence between element of A and element of B

$a \leftrightarrow 1$, $e \leftrightarrow 2$, $i \leftrightarrow 3$, $o \leftrightarrow 4$

$u \leftrightarrow 5$

COUNTABLY INFINITE SET

An infinite set A is said to be countably infinite (or denumerable) if it is equivalent to the set $\mathbb{N}$ of natural number.

COUNTABLE SET

A set A is said to be countable if it is either empty, finite or countably infinite otherwise the set is said to be uncountable

THE INTEGERS

Recall that the set $Z = \{\cdots -3, -2, -1, 1, 2, 3 \cdots\}$ is called the set of integers. Let a and b be 2 integers with $a \neq 0$. We say that a divides b or b is divisible by a or a is a divisor or a factor of b or b is a multiple of a if $b = qa$, if $b = qa$ for some $q \in Z$.

The statement (a divides b) is written as a/b - If a does not divide b, we write this as $a \nmid b$

Example:

1. 66 is divisible by 11 since $66 = 11 \times 6$
2. 16 is a divisor of 128 because $128 = 16 \times$
3. 0 is divisible by every integer because $0 = b \times 0$ for every integer b.

N.B: If a divides b, then $-a$ also divides b because $b = aq = b = (-a)(-q)$. It is therefore sufficient if we consider positive divisor of integers only.

THEOREM

Let $a, b, c \in Z$

1. If a/b and $b \neq 0$, then $|a| \leq |b|$.
2. If a/b and a/c, then $a/b+c$ & $a/b-c$
3. If a/b, then for every x, we have that a/bx
4. If a/b and b/c, then a/c
5. If a/b and b/c, then for any integers x and y, we've that $a/bx+cy$. The expression $bx+cy$ is called a linear combination of b & C.

PRIMES.

Every positive integer greater than 1, by at least two integers i.e 1 and 2. A positive integer $p>1$ is called prime if the only positive integers that divide P are P and 1. If a positive integer $n>1$ is not prime, then n is said to be composite.

Ex: The integers 2, 3, 5, 7 and 11 are prime where as the integers 4, 9, 10 and 21 are composite

REMARK:

1. The integer 2 is the only even number that is prime number.
2. An even number is an integer n which can be expressed as $n=2q$ for some integer q.
3. An odd number m is an integers which can be expressed as $m=2q+1$ for some integer q.
4. The integer 1 has a special status. It is neither prime nor complete
5. ~~Let a and b be any two integers with $b>0$~~

EUCLIDS DIVISION THEOREM OR DIVISION ALGORITH

Let a and b be any two integers with $b>0$ then there exist unique integer q and r such that $a=bq+r$ where $0 \leq r < b$.

REMARK.

1. The theorem above comes the basis of the usual arithmetic process of long division and it is one must important number theory.
2. In the expression $a=bq+r$, bq is largest multiple of a which does not

exceed a, and r is called the least remainder of a when divided by b. The number q is called the quotient. If r=0, then, a=bq, hence a is a multiple of b.

Example2

Let a=23 and b=5. Then $23 = 5 \times 4 + 3$ where $0 < 3 < 5$.

Greatest Common Divisor (g.c.d)

Let a and b be integers. An integer d not equal to 0 is called a common divisor of a and b if d|a and d|b.

An integer d is called the greatest common Divisor (g.c.d) of a and b if

i) d is a common divisor of a and b

ii) c is an integer such that c|a and c|b, c divides a and c divides b, the c must divide d.

REMARK

i) The greatest common divisor of a and b is denoted by (a,b).

ii) If the g.c.d of a and b is 1, then the integers a and b are said to be relatively prime or co-prime i.e, a and b are relatively prime is (a,b)=1.

iii) The g.c.d of a and b is also called the highest common factor (H.C.F).

Example:

1. The g.c.d of 12 and 16 is 4

2. The integer 21 and 85 are relatively prime.

REMARK: We shall now use the division algorithm the compute the g.c.d of the two integers.

Find the g.c.d of 2598 and 1124 by the use of the euclid's.

$2598 = 1124(2) + 350$

$1124 = 350(3) + 74$

$350 = 74(4) + 54$

$74 = 54(1) + 20$

$54 = 20(2) + 14$

$20 = 14(1) + 6$

$14 = 6(2) + 2$

$6 = 2(3) + 0$

When we get to remainder 0, then the last remainder before 0 in the algorithm is the required g.c.d. In this case the required g.c.d is 2.

REMARK

Having obtained the g.c.d, d, of two integers a & b, we can write d as a linear combination of a and b - i.e, we can find two integers s and t:

$d = as + bt$

Ex. Find the g.c.d of 595 and 252 using the euclid's division algorithm and express it in the form $252s + 595t$

SOLUTION

$595 = 252(2) + 91$

$252 = 91(2) + 70$

$91 = 70(1) + 21$

$70 = 21(3) + 7$

$21 = 7(3) + 0$

g.c.d = 7.

$7 = 70 - 3(21)$

Let us find the integers s and t such that $7 = 252s + 595t$.

$7 = 70 - 3(21)$

$21 = 91 - 70(1)$

$70 = 252 - 91(2)$

$7 = 70 - 21(3)$

$= 70 - (91 - 70(1))3$

$= 70 - 3(91) + 3(70)$

$= 4(70) + 3(91)$

$= 4(252 - 91(2)) - 3(91)$

$= 4(252) - 8(91) - 3(91)$

$= 4(252) - 11(91)$

$= 4(252) - 11(595 - 252(2))$

$= 4(252) - 11(595) + 22(252)$

$= 4(252) + 22(252) - 11(595)$

$7 = 26(252) - 11(595)$

compare to $7 = 252(s) + 595t$

$s = 26$ and $t = -11$

$7 = 252(s) + 595(t)$

$= 252(26) + 595(-11)$

N.B

1. If the g.c.d of a and b is 1, then $as + bt = 1$, conversely if $as + bt = 1$ then g.c.d of a & b = 1. Hence, a necessary and sufficient condition for the g.c.d of a & b = 1 is the existence of integers s and t such that $as + bt = 1$

BASIC PROPERTIES OF G.C.D

1. If $c \mid ab$ (c divides ab) and the g.c.d of $a \$ c = 1$, then c divides b, $b \mid c$,
2. If the g.c.d of $a \$ c$ is 1 and g.c.d of $a \$ c$ is 1, then $(a, bc) = 1$.
3. i.e if $a;b = 1$, $a,c = 1$ then $abc = 1$
4. Let k be any integer and a,b be integers where atleast one of a and $b \neq 0$ (ka, kb) $|k(a,b)|$.
5. If $(a,b) = d$, then $(a/d), (b/d) = 1$

LEAST COMMON MULTIPLE (L.C.M).

An integer m is called a common multipe of integers $a_1, a_2 \cdots a_n$ if for each a_i $m = a_i \partial_i$ for some integers, the mq is also a common multiple. They are infinitely many common multiple unique and hence there is no greatest integer among common multiple. But there is a unique smallest integer among the common multiple.

An integer $a \$ b$ is denoted by (a,b), For ex 18 is a common multiple of 2,3,6 $\$$ 9 since each of these integers divides 18. Again, 36,72··· are also common multiple of 2,3,6 $\$$ 9 the smallest among them is 18; 18 is the L.C.M

Ex. Find the nos of Z in the set $(1,2,3,\cdots,60)$ that are not divisble by: nor 3 nor 5.

SOLUTION.

Let A denote nos divisible by 2.

B denotes nos divisible by 3

C " " " " 5

$|A| = \left(\frac{60}{2}\right) = 30$, $|B| = \left(\frac{60}{3}\right) = 20$, $|C| = \frac{60}{5} =$

$$|A \cap B| = \frac{60}{2 \times 3} = \frac{60}{6} = 10$$

$$|A \cap C| = \frac{60}{2 \times 5} = 6.$$

$$|B \cap C| = \frac{60}{3 \times 5} = 4$$

$$|A \cap B \cap C| = \frac{60}{2 \times 3 \times 5} = 2.$$

$|A' \cap B' \cap C'| = 60 - (A \cup B \cup C) + [(A \cap B) \cup (A \cap C) \cup (B \cap$

$- A \cap B \cap C$

$= 60 - (30+20+12) + (10+6+4) - 2$

$= 60 - 62 + 20 - 2$

$= 16$

16 numbers are not divisible by 2,3 or 5

UNIQUE FUNDAMENTAL THEOREM OF ARITHMETIC.

Every positive integer, $n > 1$ can be expressed as a product of primes. Futhermore, apart from the order of appearance of one prime factors are unique.

Ex: The prime factorization of 81 is:

$81 = 3 \times 3 \times 3 \times 3 = 3^4$

The prime factorization of 100 is:

$100 = 2^2 \times 5^2$.

Ex: Use prime factorisation to find one G.C.D of 12 and 30.

SOLUTION

$30 = 2^1 \times 3^1 \times 5^1$

$12 = 2 \times 2 \times 3^1$

$2 \times 3 \times 5$

$2^2 \times 3^1 \times 5^0$

∴ the G.C.D (12 and 30)

$2^{\min(2,1)} \times 3^{\min(1,1)} \times 5^{\min(1,0)}$

$= 2^1 \times 3^1 \times 5^0$

$= 6$.

N.B: All primes occuring in the prime factorization of "a" and "b" are to included in both factorization with zero exponents if necessary.

Ex: Use prime factorization to find the L.C.M of 119 and 272.

$272 = 2^4 \times 17^1 \times 7^0$

$119 = 2^0 \times 17^1 \times 7^1$

$(119, 272) = 2^{\max(0,4)} \times 17^{\max(1,1)} \times 7^{\max(0,1)}$

$= 2^4 \times 17^1 \times 7^1$

$= 1904$

CONGRUENCES

If "a" and "b" are integers and "m" is a positive integer, then "a" is set to be congruent to "b" modulo m if $\frac{a-b}{m}$ i.e $m|a-b$.

Symbolically, "b" is expressed as

$a \equiv b \pmod{m}$.

Expression 1 is called the congruence, "m" is called the modulo of the congruence and "b" is called a residue of $a \pmod{m}$.

If "m" does not divide a-b, then "a" and "b" are said to be in congruence mod m. This is written as; $a \not\equiv b \pmod{m}$.

Ex: $83 \equiv 13 \pmod{5}$ because $83 - 13 = 70$ which is divisible by 7, so 13 is the residue and 5 is the modulus of the congruence.

Ex: $3 \equiv -5 \pmod 4$ because $3-(-5)=8$ is divisible by 4.

Ex: $25 \not\equiv 3 \pmod 5$ because $25-3=22$ is not divisible by 5.

REMARK: It is often useful to formulate the congruence as follows.

$a \equiv b \pmod m$ iff $a-b = -mx$ K where K

1. $a \equiv a \pmod m$.
2. $a \equiv b \pmod m$, then $b \equiv a \pmod m$
3. $a \equiv b$ & $b \equiv a \pmod m$, then $a \equiv c \pmod m$

CONGRUENT ARITHMETIC.

Let $a \not\equiv b \pmod m$ and let c be any integer, then

1. $a+c \equiv b+c \pmod m$.
2. $a-c \equiv b-c \pmod m$
3. $ax c \equiv bx c \pmod m$.

If a, b, c and d are integers such that $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then;

4. $a+c \equiv b+d \pmod m$.
5. $a-c \equiv b-d \pmod m$
6. $ac \equiv bd \pmod m$.
7. $a^k \equiv b^k \pmod m$ ∀ +ve integer k

Ex: Since $3 \equiv 5 \pmod 4$ and $21 \equiv$

It follows from (4) above that $24 = 3$

$24 = 3+21 \equiv -5+1 \pmod 4$

$\equiv -4 \pmod 4$

Also, $63 = 3 \times 21 \equiv -5 \times 1 \pmod 4$

$\equiv -5 \pmod 4$ by eqn(6

DIVISION IN CONGRUENCES

Although, we can divide both sides of equation by an integer, this is not true for congruences. For ex: We cannot divide both sides of 30 congruent to $2 \pmod$ by the common factor 2 because 15 is not congruent to $1 \pmod 4$.

More care is needed in dividing a congr through by a common integer.

RESIDUE CLASSES

Let x be an integer and let $m > 0$. The set of all integers congruent to $x \pmod m$ is called the residue class of x. It's denoted by (x) i.e

$(x) = \{a \in z : a$ is congruent to $x \pmod m\}$.

The residue classes $\pmod 4$ are

$(0), (1), (2), \ldots (m-1)$.

$\equiv$ → congruent to

ARITHMETIC OF RESIDUE CLASSES

Addition & multiplication are defined for residue classes (mod m) as follows:

$(a)+(b) = (a+b)$ and

$(a)+(b) = (a \times b)$

Ex: Consider the residue classes (mod 4) i.e (0), (1), (2), (3). Then their addition is as follows:

$(0+1) = 1$

$(0+2) = 2$

$(0+3) = 3$

$(1+1) = 2$

$(1+2) = 3$

$(1+3) = 0$

$(2+2) = 0$

$(2 \times 3) = 2$.

REMARK: when m is small, we can easily write down their addition and multiplication tables. The foll. shows addition and multiplication table residue classes (mod 4)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Integers modulo n

The integers modulo n denoted by Z_n reflects to the set $Z_n = \{0, 1, 2, \cdots, n-1\}$: where addition & multiplication are defined by the arithmetic modulo n or, in other words, the corresponding operations for the residue classes.

Ex: The tables above may be viewed as the addition and multiplication tables for Z_4. This means that there is no essentials difference between the arithmetic of Z_n and that of the residue classes modulo n

SOLUTIONS OF CONGRUENCES

A polynomial congruence of degree n is can expression of the form $f(x) = a_n x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0 \equiv 0$ (modulo n) if a_n is not congruent to 0 modulo n.

$21 \equiv 5 \bmod 8$

Any value of x which satisfies the congruence is called its solution.

REMARK

If an integer u is a solution of $f(x) \equiv 0$ modulo n and $v \equiv u$ modulo n, then v is also a solution of the congruence.

LINEAR CONGRUENCE

An expression of a form: $ax \equiv b$ modulo n; where a is not congruent to 0 modulo m is called linear congruence modulo n. Any value for x which satisfies * above is called a solution of the congruence.

Ex: Consider the congruence $3x \equiv 5 \bmod 8$ If we put $x = 7$, we find that $3 \times 7 \equiv 5 \bmod 8$ is true. Hence $x = 7$ is a solution. Also, all integers congruent to 7 mod 8 are also solutions.

The standard practice of writing the solution is $x \equiv 7 \bmod 8$ because 7 belongs to the set of least residues mod 8.

Guide I to solving linear congruences

1. Let $ax \equiv b \bmod m$ be a linear congruence ... of a and m.

If the g.c.d is 1, then solve the congruence $ax \equiv 1 \bmod m$ as follo... Find s and t such that $as + mt = ...$ then multiply eqn(1) by b to get $a(sb) + m(tb) = b$

then $x = sb$ is a solution. If sb is ... we obtain the least positive solution

Ex: Solve the congruence $290x \equiv 5 \bmod ...$

SOLUTION

We find the gcd of 290 and 357, w... is 1. So we ... $290x \equiv$

this solution is obtained by finding s and t such that $290s + 357t = 1$ with the help of reversing the procedur... of long division we obtain $s = -16$ an... $t = 13$. Therefore $290(-16) + 357(13) = ...$ multiply by 5 to get $290(-80) + 357$ $(65) = 5$. Hence $s = -80$ is a solution that is, $s \equiv -80 \bmod 357$

$\therefore s \equiv 277 \bmod 357$

GUIDE II to solving Linear Congruen...

Let $ax \equiv b \bmod m$. If the g.c.d of a and m is not equal to 1. Suppose the g.c.d is d and that d de...

d/b

b, then we first divide the congruence through by d to get the simplest form $a_1 x \equiv b_1 \bmod m_1$. In this new form, the g.c.d of a_1 and m_1 is 1 then we proceed as in case of guide I

N.B: There will be d number of solution. After getting the first solution x_0, the other solutions are obtained as follows:

$x_0 + 1(m/d), x_0 + 2(m/d), \cdots, x_0 + d-1(\frac{m}{d})$

Ex: Solve the congruence $345x \equiv 15 \pmod{912}$

Solve $66x \equiv 111 \pmod{237}$

RELATIONS

Let A and B be two non-empty set. A relation from A to B is a subset of the cartesian product $A \times B$. Suppose that r is a relation from A-B, then r is a set of ordered pairs (a, b); where $a \in A$ belongs $b \in B$. Every such ordered pair is written as $a\,r\,b$ and read as "a is related to b". Recall that the cartesian product $A \times B$ is equal to $\{(x, y) : x \in A, y \in B\}$. Let A $= (1, 2, 5)$ and $B = (2, 4)$. Then A class B $A \times B = [(1,2), (1,4), (2,2), (2,4), (5,2), (5,4)]$ Suppose we consider the relationship of $<$, then we find some ordered pairs are related which some are not. Hence by definition of relations we have $r = \{(1,2), (1,4), (2,4)\}$ If r is a relation from a set A to itself, then r is said to be a relation of A.

DOMAIN & RANGE OF A RELATION

Let r be a relation A to B. Then the set $\{a \in A : (a, b) \in r, b \in B\}$ is called the DOMAIN of the relation, it is denoted by Dom(R). The set $\{b \in B : (a, b) \in R,$ ... range of the relation R, it is denoted by Ran(R)

Ex. Let $A = \{2, 3, 4\}$, $B = \{3, 4, 5\}$. Find the Dom(R) and Ran(R) if r is the relation given by $a\,r\,b$ if $a < b$

$A \times B = \{(2,3), (2,4), (2,5), (3,3), (3,4), (3,5), (4,3), (4,4)$

$r = \{(2,3), (2,4), (2,5), (3,4), (3,5), (4,5)\}$

$Dom(r) = \{2, 3, 4\}$

$Ran(r) = \{3, 4, 5\}$.

INVERSE RELATION

Let r be a relation for A-B. The inverse of r is the relation from B to A which consists the reversal of the order of the pairs in r, denoted by r^{-1}. Thus $r^{-1} = \{(b, a) : b \in B, a \in A\}$.

Ex. Let $A = \{2, 3, 5\}$ and $B = \{6, 8, 10\}$. Find r^{-1} if r is the relation given by $a\,r\,b$ if a/b

$A \times B = \{(2,6), (2,8), (2,10), (3,6), (3,8), (3,10), (5,6), (5,8)$

$r = \{(2,6), (2,8), (2,10), (3,6), (5,10)\}$

$r^{-1} = \{(6,2), (8,2), (10,2), (6,3), (10,5)\}$

REFLEXIVE RELATION

A relative of r on a set A is called reflexive if every $a \in A$ is related to itself.

SYMMETRIC RELATION

A relation r on a set A is called symmetric if bra whenever arb

TRANSITIVE RELATION

A relation r on a set A is called transitive if arb and brc imply arc

EQUIVALENCE RELATION

A relation on a set A is called an equivalence relation or and RST relation if R-Reflexive, S-Symmetric & T-Transitive.

Ex. Let Z be the set of integers. The relation r defined on Z by arb iff $a-b$ is divisible by 3 is an equivalent relation.

Let us show it ; (R.S.T)

Reflexivity: Let $a \in Z$, then $a-a=0=3\times0$ e $a=a$ meaning a is relating to itself and or is reflexing

ymettry: Let $a,b \in Z$, suppose arb. We must that brq. Now we have $a-b=3K$ where $K \in Z$. Thus $-(a-b)=-3K$

$b-a=3p$ where $p=-K$, so bra as required. Hence r is symmetric

Transitivity: Let $a,b,c \in Z$ such that $a \in b$ and $b \in c$. we must show that $a \in c$. We have $a-b=3K_1$ ....(1)

$b-c=3K_2$ ....(2). Adding eqn (1) & (2)

$a-b+b-c=3K_1+3K_2$

$a-c=3(K_1+K_2)$

$a-c=3T$ where $(K_1+K_2)=T$

where, hence arc ∴ I

therefore r is transitive. We therefore conclude r is an equivalence relation

EQUIVALENCE CLASSES

Let r be an equivalence relation on a set A. If $a,b \in A$ such that $a \in b$, then a and b are said to be equivalent w.r.t r. The set of all elements of A that are equivalence to a relation constitute the equivalent class of a. It is denoted by $[a]$. i.e $[a]=\{b \in A : bra\}$. The collection of all equivalence classes of element of A under an equivalence relation r is denoted by A/r.

Ex. Let us obtain the equivalent classes in our example of equivalent relation above:

Recall that $[a]=\{x\in Z: xra\}=\{x\in Z: x-a|3\}=\{x\in Z: x-a=3K, K\in Z\}=\{x\in Z: x=3K+a\}$

$[0]=\{x\in z: x=3K+0\}=\{x\in z: x=3K\}$

$=\{0,3,-3,6,-6\ldots\}$ $K=0,1,-1,2,-1\ldots$

$[1]=\{x\in z: x=3K+1\}=\{x\in z: x=3K+1\}$

$=\{1,4,-2,7,-5\ldots\}$

$[2]=\{x\in z: x=3K+2\}$

$=\{2,5,-1,8,-4\ldots\}$.

$[3]=\{x\in z: x=3K+3\}$

$=\{3,6,0,9,-3\ldots\}$.

$[4]=\{x\in z: x=3K+4\}$

$=\{4,7,1,10,-2\ldots\}$.

$[5]=\{x\in z: x=3K+5\}$

$=\{5,8,2,11,-1\ldots\}$

$[6]=\{x\in z: x=3K+6\}$

$\{6,9,3,12,0\ldots\}$

Observe that for all intergers $n\geq 3$ the equivalence class for n will be the same as one of the above classes we obtained classes. So, the required equivalent classes are $[0]$, $[1]$, $[2]$, and $[$

PROPERTIES OF FIRST CLASSES

REMARK: Let Z be the set of integers and let r be an equivalent relation on defined by arb iff $a-b/n$. Then the distinct equivalence classes are $[0]$, $[$ $[n-1]$. These equivalence classes partit the set of integers.

PROPERTIES OF EQUIVALENCE CLASSES

Let A be a non-empty set, r be an equ lence relation on A. Let $a,b\in A$. the the foll. hold:

1. $a\in[a]$
2. If $b\in[a]$, then $[b]=[a]$
3. $[a]=[b]$ iff arb
4. Either $[a]\cap[b]=\phi$ or $[a]=[b]$

PARTIAL ORDER RELATION

Relation r on a non-empty set A called a partial order if r is reflex transitive and satisfies the anti-symmetric property given by:

If $a,b\in A$ are members A such that arb then $a=b$.

A set A having a partial order is called a partially ordered set (POSET).

Ex. The relation of $\leq$ is partial order on the set of Z. Hence $(Z, \leq)$ is a POSET

FUNCTIONS

Let A and B be two non-empty set. A function $f: A \to B$ is a set of ordered pairs with the property that for each elements $x \in A$, there is a unique $y \in B$ such that $(x, y) \in f$. Put in another language, a function f from a set A to set B is a rule which assigns to each $x \in A$ a unique $y \in B$.

The statement "f is a function from A to B" is usually represented by $f: A \to B$'

B! There may be some elements of B which are not associated with any element A. But every element of A must be associated with only one element of B.

Ex. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{0, 1, 2, 3, 5, 9, 12, 13\}$. Then:

1. $f = \{(1,1), (2,0), (3,7), (4,9), (5,12)\}$ is a function $f: A \to B$ because every element of a as a unique associates in B

2. $f = \{(1,3), (2,3), (3,5), (4,9), (5,9)\}$ is a function $A \to B$

Notice that the 2nd component is the ordered pair may be repeated in a functio

3. $f = \{(1,1), (2,3), (4,7), (5,12)\}$ is not a function from $A \to B$ because 3 is not mapped to any thing.

4. $f = \{(1,1), (2,3), (3,5), (3,7), (4,9), (5,12)\}$ is not a function from A to B because the element 3 is has two different associates in

DEFINITION

Let $f: A \to B$, then the $\{A\}$ is called the domain of f. It's denoted by dom (F). Its members are the first co-ordinates of the ordered pairs belonging to f. The $\{B\}$ is called the codomain of f. The range of f is a subset of the co-domain which consis of members of B that have associates i A. Let $x \in A$ and $y \in B$ be that unique element of B associated of x. Then y is called image. The element x is calle is called the pre-image (y) Ide write this as $y = f(x)$. The element x is the

independent variable while y is dependent variable. Other terms such as transformation mapping, correspondence are synonyms for the word formation

ONE TO ONE FUNCTION

A function from a set $A \to B$ is called a one to one function or an injective function if no two elements of A have the same image in B. In other words, f is 1-1 if for all elements $x, y \in A$ such that $f(x) = f(y)$ implies $x = y$

MANY TO ONE FUNCTION

A function $f: A \to B$ is called many to one function if two or more different element in A have the same image in B.

INTO FUNCTION

A function $f: A \to B$ is called into if there exist one element in B which is not image of any element in A i.e, the range of f is a proper subset of the co-domain.

ONTO FUNCTION

A function $f: A \to B$ is called onto or Subjective if every element of B is an image of an element in A i.e the range of $f = B$.

REMARK: In order to check whether a function $f: A \to B$ is onto or not, write x in terms of y and see if $\forall y \in B$, $\exists x \in A$ such that $f(x) = y$.

BIJECTIVE FUNCTION

A function $f: A \to B$ is called bijecti if f is both 1-1 and onto.

COMPOSITION OF FUNCTIONS

Let $f: A \to B$ and $g: B \to C$. The co position of f with g, denoted by gof, results in a new function f $A \to C$ and it's given by $(gof)x = g(f(x)) \; \forall \; x \in A$. Hence the composition (gof) first apply $f: A \to$ and then employs $g: B \to C$. In other words, the range of f becomes the domain of g. Similar definition applies for fog.

Ex. Let $A = \{1, 2, 3\}$, $B = \{a, b\}$, $C = \{$ $s\}$ and $f: A \to B$ be defined by $f(1)$ $f(2) = a$, $f(3) = b$ and let $g: B \to C$ b defined by $g(a) = s$, $g(b) = r$.

$gof(3) = g(f(3))$
$= g(b)$
$= r$

Find $(gof)(1), (gof)(2), (gof)(3)$

$(gof)(1) = g(f(1))$ * $gof(2) = g(f(2))$

$= g(a)$ $= g(q)$

$= 5$ $= 5$

Ex. Let R be set of $\mathbb{R}$ and let $f: R \to R$, $g: R \to R$ be defined by $f(x) = x+2$ and $g(x) = x^2 \; \forall \; x \in R$ obtain a formula for gof and fog.

$(gof)(x) = g(f(x))$

$= g(x+2)$

$= (x+2)^2$

$(fog)(x) = f(g(x))$

$= f(x^2)$

$= x^2+2$

INVERSE OF A FUNCTION

Let ~~x be a~~ function $f: A \to B$, then the function which reverses the rule of f is called the inverse of f, denoted by f^{-1}.

i.e $f^{-1}: B \to A$, thus $f(x) = y$ iff $x = f^{-1}(y)$

REMARK

1. Not all functions have inverses. A condition for a function $f: A \to B$ to have an inverse is that f is bijective.

2. A function which as an inverse is said to be invertible

BINARY OPERATIONS

Let G be a non-empty set. A binary operation on G is a function that assigns each ordered pair of element ~~(x^2+5x+4)~~ of G to a unique element of G. The symbols $+, \cdot, *$ e.t.c are used to denote binary operations on a set. This property of having "the product of" two element of G to be in G is called the closure property, and we say that the set G is closed with respect to the binary operation. The operation of subtraction is not a binary operation on the set of natural numbers because it is not closed with respect to subtraction. A binary operation on a set G is also called a composition: for a finite set G having a binary operation (*) we can define the operation by means of a table called the composition table. Let G be a set within distinct element, to construct a composition table for G, the element of G are arranged horizontally in a row called the "INITIAL ROW"

Also the element are again arranged vertically in a column called the INITIAL COLUMN". The (i, j)th position in the table is determined by the intersection of the ith and jth column. For example, Let $G = \{a, b, c\}$. Define the operation (*) on G by the following table:

*	a	b	c
a	c	b	a
b	a	a	a
c	b	b	b

ALGEBRAIC STRUCTURE

A non-empty set together with one or more binary operation is called an ALGEBRAIC STRUCTURE.

For Ex. $(N, +), (Z, +), (R, +x)$ are some examples of algebraic structure.

LAWS OF BINARY OPERATION

ASSOCIATIVE LAW

A binary operation * on a non-empty set G is said to be associative if for every a, b, c in G, will have

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

CUMMULATIVE LAW

A binary operation * on a non-en set G is said to be cummutative if for every $a, b, c \in G$, we have

$$a * b = b * a$$

IDENTITY ELEMENT

An element e in a set G is call the Identity Element with respect a binary operation * if for eve element $a \in G$ we have

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

N.B: That the identity element an algebraic structure if it exist Unique

INVERSE ELEMENT

Let G be a set which has an ident element e with respect to the binar operation *. Let $a \in G$ if there ex an element $b \in G$ such that

$a * b = e * a = e$, then b is calle the Inverse of a with respect to *

DISTRIBUTIVE BINARY OPERATION

Let G be non-empty set with two binary operations · and *, the operation "·" is said to be distributive over "*" if:

$a \cdot (b * c) = (a \cdot b) * (a \cdot c)$ and $(b * c) \cdot a = (b \cdot a) * (c \cdot a)$ $\forall a, b, c$

IDEMPOTENT ELEMENT

Let G be a non-empty set with a binary operation *. An element $a \in G$ is called an IDENPOTENT ELEMENT if $a * a = a$.

GROUPS

Let $(G, *)$ be an algebraic structure where * is a binary operation on G. Then the set G is said to be a group w.r.t * if the following holds;

1. G is closed w.r.t *
2. G is associative w.r.t *
3. G has an identity element.
4. Every element of G has an inverse w.r.t *.

REMARK

1. We may not mention the axiom 1 above when defining a group because it is just a consequence on definition on binary operation
2. If $(G, *)$ satisfies axiom 1 and axiom 2 only, then $(G, *)$ is called a semi-group.
3. If $(G, *)$ satisfies axiom 1, axiom 2 and 3 only, then $(G, *)$ is called a monoid.
4. A group $(G, *)$ is said to be "abelion" if $a * b = b * a$ $\forall a, b \in G$
5. A group ~~$(G, *)$~~ with the binary operation of addition is called an "Additive Group". A group with the binary operation of multiplication is called a "Multiplicative Group".

Examples:

1. The set $\mathbb{R} \to \mathbb{R}$ is a group w.r.t. Addition
2. The set $\mathbb{R}^*$ of non-zero $\mathbb{R}$ is a group w.r.t Multiplication.
3. The set $G = \{1, -1, i, -i\}$ is a group w.r.t Multiplication. This is the group of the 4th roots of unity

*	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-i	1
-i	-i	i	1	-1

4. The integers mod n forms a group w.r.t addition
5. Let X be a non-empty set and let G

be the set of all Bijective mappings from $x \xrightarrow{X \to X} x$ to x then G is a group w.r.t composition of mappings.

6. Let $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \sqrt{(-1)} & 0 \\ 0 & -\sqrt{(-1)} \end{bmatrix}, \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{bmatrix} \right\}$.

is group w.r.t Multiplication of matrices This group is called a "QUATERION GROUP".

7. The Set $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ is a group under multiplication of matrices and it is called the "KLEIN FOUR" group.

DEFINITION

Let $(G, *)$ be a group.

1. The no. of element in G is called the order of G.

2. Let $a \in G$, the smallest positive integer m, if its exists, such that $a^m = e$ where e is the identity element of G, is called the order of $a \in G$

For Ex: Let $G = \{1, -1, i, -i\}$.

ASSIGNMENT

i. Find the no of integers $S = \{1,2,3,4,$ which are not divisible by two nor b three nor by five.

ii. Solve $66x \equiv 111 \bmod 237$

ELEMENTARY PROPERTIES OF A GRO

Let $(G*)$ be a group and let a, b, c, be elements of G. Then the foll. hol

1. $a * b = a * c$ implies $b = c$ (left cancellation law).

2. $b * a = c * a$ implies $b = c$ (Right Cancellation law).

3. The identity element $e \in G$ is unig

4. The inverse of every $a \in G$ is uni

5. The equation $a * x = b$ has a unique solution given by $x = a^{-1} * b$.

6. The equation $y * a = b$ has a unique so given by $y = b * a^{-1}$

7. $(a^{-1})^{-1} = a$

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

SUB GROUP.

Let $(G*)$ be a group A non-empty subs

S of G is called a subgroup of $(G*)$ If $(S, *)$ is also a group.

Ex. Let $(G*)$ be a group. Then the sets G and $\{e\}$ are sub group of $[G, \cdot)$ where e is the identity element of $(G*)$. These are called Improper or trivial subgroup of $(G*)$.

2. The multiplicative group $S = \{1, -1\}$ is a sub group of the multiplicative group $G = \{1, -1, i, -i\}$.

THEOREM

A non-empty subset S of a group $(G*)$ is a subgroup iff the following hold.

1. $x * y \in S \ \forall \ x, y \in S$
2. $x^{-1} \in S \ \forall \ x \in S$.

REMARK

The theorem above gives the necessary and sufficient condition for a subset of a group to be a sub group

The theorem above is equivalent to the following theorem.

THEOREM

A non-empty subset s of G group $(G*)$ is a sub group of $(G*)$ Iff

$x * y^{-1} \in S \ \forall \ x \in S$.

ILLUSTRATION

Investigate whether the set $S = \{z \in \hat{C} : |z| = 1\}$ is a sub group of C^*, the multiplicative group of non-zero complex number.

SOLUTION

Let $z_1 \& z_2 \in S$ then the $|z_1| = 1, |z_2| = 1$.

Consider $|z_1 \times z_2| = |z_1| \times |z_2| = |x| = 1$ so $z_1 \times z_2 \in S$. Next consider $|z_1^{-1}| = |z_1|^{-1}$

$= \frac{1}{|z_1|} = \frac{1}{1} = 1$. So $z_1 \in S$. We therefore conclude that S is a subgroup of C^*

COSET

Let H be a sub-group of a group G^* and let $a \in G$ the set $a * A = \{a * h \in H\}$ is called left coset generated by a and H Similarly, the $H * a = \{h * a : h \in H\}$ is called a RIGHT COSET generated by a & H The element a is called a real presentaton of $a * H$ and $H * a$.

REMARK

Cleanly $a * H$ and $H * a$ subset of G. Let e be the identity element of G. Then

e is also in H. Hence $e*H = \{e*h : h \in H\}$ =H and $H*e = \{h*e : h \in H\} = H$. Therefore H is both a left closet and right coset

If G is an abellion group, then $H*a = a*H$. Hence every left coset of an abellion group is also a right coset.

DEFINITION

Let H be a subgroup of a G* the nos distinct right (left) coset of $H \in G$ is called Index of $H \in G$. it's denoted by $(G:H)$.

Ex. Let $G = \{\dots, -3, 2, -1, 0, 1, 2, 3, \dots\}$ be the additive group of integers. Let H be the sub-group of G obtained by multiplying every element of G by 3. Then

$H = 3 \times Z = 3Z = \{\dots -9, -6, -3, 0, 3, 6, 9 \dots\}$

Let us consider the right coset of $H \in G$

$H+0 = \{\dots -9, -6, -3, 0, 3, 6, 9 \dots\}$.

$H+1 = \{\dots -8, -5, -2, 1, 4, 7, 10 \dots\}$

$H+2 = \{\dots -7, -4, -1, 2, 5, 8, 11 \dots\}$

$H+3 = \{\dots -6, -3, 0, 3, 6, 9, 12 \dots\}$

$H+4 = \{\dots -5, -2, 1, 4, 7, 10, 13 \dots\}$

Continuing like this, we see that the distinct coset of $H \in G$ are $H+0, H+1, H+2$, The union of this coset gives G. Her the index $H \in G$ is 3.

ASSIGNMENT

Read up on permutation group, Cyc groups and Normal Sub-group.

HOMORPHISMS OF GROUPS.

Let $(G*)$ and $(H \cdot)$ be two gro

A function $f: G \to H$ is called a Homomorphism if $f(x*y) = f(x) \cdot f$ $\forall x, y \in G$.

A Homomorphism is called an Isomorp if it is both an onto and 1-1 functi

If $f: G \to H$ is an isomorphism, we that G and H are isomorphic. We this as $G \cong H$

An ISOMORPHISM from a group G-G called an AUTOMORPHISM.

Ex. Let G be the additive group of re and Let H be the multiplicative group o positive real nos. Consider the functi $f: G \to H$ defined by $f(x) = 5^x \forall x \in$ Investigate whether f is a homomorphi

$f(x+y) = f(x) \times f(y)$

Let $x, y \in G$. Then $f(x+y) = 5^{x+y}$

$= 5^x \times 5^y = f(x) \times f(y)$.

Hence f is homomorphism.

A Homomorphism is called an epimorph-ism if it is a subjective function or onto.

A Homorporphism is called a monomorphism if it is a 1-1 function or injective function.

EXERCISES.

Let G be the multiplicative group of +ve real numbers and H be the additive group of real numbers investigate whether the mapping $f: G \to H$ defined by $f(x) = \text{Log } x \ \forall \ x \in G$ is an Isomorphism

DEFINITION

Let (G^*) be a group with identity element e and let $(H, \circ)$ is another group with identity element e_2. Suppose $f: G \to H$ is a homomorphism. The set $\{x \in G : f(x) = e_2\}$ is called the kernel of f it is denoted as ker (f). The set $\{y \in H : y = f(x)$ for some $x \in G\}$ is called the Image of f is denoted by Im (m).

RINGS

An algebraic structure $(R, +, \times)$ having two binary operations of additions and multiplication is called a ring if the foll axioms hold:

1. $(A+B) \in R \ \forall \ A, B \in R$.
2. $(A+B)+C = A+(B+C) \in R$.
3. $A+B = B+A \ \forall \ A, B \in R$
4. There exist an element $0 \in R \ \exists \ A+0 = 0+A = A \ \forall \ A, B \in R$
5. For each $A \in R$ there exist $-A \in R \ni A+(-A) =$
6. $A \times B \in R \ \forall \ A, B \in R$
7. $(A \times B) \times C = A \times (B \times C) \ \forall \ A, B, C \in R$.
8. $A \times (B+C) = (A \times B) + (A \times C) \ \forall \ A, B, C \in R$.
9. $(B+C) \times A = (B \times A) + (C \times A) \ \forall \ A, B, C \in R$.

REMARK.

1. A ring R is called commutative if $A \times B = B \times A \ \forall \ A, B \in$
2. An element e is a ring R is called an unit (or identity) element. If $e \times A = A \times e \ \forall \ A \in R$. A unit element e (if it exist) in a ring R is generally denoted by 1. A ring R is called a ring with unity if it has a unit element.

Ex:

1. The set Z of integers w.r.t ordinary

addition and multiplication is a commutative ring with unit 1.

2. The set $2\mathbb{Z}$ of even integers w.r.t ordinary addition and multiplication is a commutative ring without unity because there is no even integer e such that $e \times y = y \times e = y$ $\forall$ even integer y

3. The set $Z_n = \{0, 1, 2, 3 \cdots n-1\}$ w.r.t addition and multiplication (mod n) is a non-commutative ring.

RING WITH ZERO DIVISOR

If a and b are non-zero elements of a ring R such that $a \times b = 0$, then a and b are called the divisors of zero or zero divisors. A particular a is called a left divisor of zero and b is called a right divisor of zero.

In a commutative ring R, every left zero divisor is also a right zero divisor, thus there is no distinction between left and right zero divisor in a commutative ring.

Example:

1. The ring of integers $\mathbb{Z}$ has no zero divisor because there are no two non-zero integers where product is zero.

2. The ring $M_2(\mathbb{Z})$ seen earlier is a ring with zero divisors

Consider the matrices $A = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} \\ \end{pmatrix}$

Then $A \times B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Also $B \times A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

so A and B are zero divisors

INTEGRAL DOMAIN

A ring R is called an integral domain if it is commutative.

2. It is without zero divisors.

3. In other words, a commutative ring is called an integral domain if whenever $a, b \in R$ such that $A \times B = 0$, then either $A = 0$ or $B = 0$

Ex.

1. The ring of integers is an integral dom

2. The ring of real numbers is an integral dom

DEFINITION

A ring F containing atleast two elements is a field if:

1. It is commutative

2. It has a unit element

3. Every non-zero element of F has a multiplicative inverse in F.

Ex. The ring of rational numbers $(\mathbb{Q}, +, \times)$ is a fi

2. The ring of real numbers $(\mathbb{R}, +, \times)$ is a fie

3. The ring of complex nos $(\mathbb{C}, +, \times)$ is a fiel

THEOREM

Every field is an integral domain

Proof

Let F be a field. Clearly, F is commutative. It remains to show that F has no zero divisors. Let $a, b \in F$ such that $a \times b = 0$. We must show that either $a = 0$ or $b = 0$ ... *

Suppose $a \neq 0$, then we must show that $b = 0$. Since $a \neq 0$, it has a multiplicative inverse (a^{-1}) in F. Multiply both sides on the left of eqn (*) by (a^{-1})

$$(a^{-1}) \times (a \times b) = (a^{-1}) \times 0$$

$$(a^{-1} \times a)b = 0 \Rightarrow a^{-1} \times (a) = 1$$

$$1 \times b = 0, \quad b = 0$$

Similarly, suppose $b \neq 0$, we must show that $a = 0$. Since $b \neq 0$, b has multiplicative inverse $b \in F$. Multiply both sides of * on the right to get;

$$(a \times b) \times b^{-1} = 0 \times b^{-1}$$

$$a \times (b \times b^{-1}) = b^{-1}$$

$$a \times 1 = 0$$

So F has no zero divisor. Therefore, F is an integral domain.

REMARK; The converse of the theorem above is not true. That is, not every integral domain is a field.

THEOREM

Every finite integral domain is a field

DEFINITION

Let R be a ring, the smallest positive integer n (if it exist) $\exists\, n \times a = 0\ \forall$ $a \in R$ is called a characteristic on the ring. If no such integer exist, then the characteristic of R is 0.

Ex. Let Z_n be the ring of integers mod n. The characteristic of Z_n is n. For instance consider $Z_5 = \{0, 1, 2, 3, 4\}$. The characteristic of Z_5 is 5 because $Z_5 \bmod 5 = 0$

DEFINITION

A ring R with unit element is called a division ring or a skew field if every non-zero element of R has a multiplicative inverse. If a division R is commutative, then R is a field. Note that a skew field has no zero divisors.

THEOREM

Let R be a division ring. Then the non-zero element of R form a group under multi-

phzation.

PROOF:

Let P be the set of non-zero element of R. Let $a, b \in P$. We must show that $axb \in P$. If has no zero divisor, then $axb \neq 0$. So $axb \in P$ and P is closed w.r.t multiplication. Since a^{-1} of each, ~~non-zero element of~~ $a \in R$, then $a^{-1} \in P$. Every element in P has an inverse in P. Again, the unit element of $R \in P$ since it is non-zero. Clearly P is associative w.r.t multiplication. Therefore P is a group w.r.t multiplication

ASSIGNMENT

Read up ~~Submang~~ Sub rings., Ring homomorphism and Ideals.