General Introduction and Objectives

This course on Abstract Algebra is intended to put on a proper footing basic algebraic structures on which further mathematics can be built. It starts with the basic knowledge of sets and relations through fundamental algebraic structures of groups, rings and fields. Topics on elementary number theory are also treated and the course ends with a discussion on the theory of polynomials and rational functions over any field and in one variable only.

The objectives of this course are as follows. The reader should be able to:

(i) have a working knowledge of the technical language through clear and precise definitions of terms,

(ii) state and prove elementary properties of the algebraic structures which are usually stated in the form of lemmas, propositions and theorems, and

(iii) apply the definitions and properties of the algebraic concepts to solving various problems in abstract algebra.

LECTURE ONE

Sets

Introduction

We shall define what a set is and discuss how to represent a set and its members. We shall examine different types of sets, subsets, equality of sets and the universal set. We shall then see how to form new sets from given ones by taking complements, unions or intersections, of the given sets.

Geometrical representation of sets shall be presented in the form of Venn diagrams which will then be used in solving problems on sets.

Objectives

The reader should be able to

(i) have a working knowledge of the language of sets, and

(ii) represent sets in Venn diagrams with a view to using them to solve problems on sets.

Pre-Test

1. If $A = \{f, g, h, i, j\}$; $B = \{t, u, v\}$; $C = \{7, 8, 9, 10, 11\}$ state whether the following statements are true or false.

(i) $a \in A$ (ii) $f \in A$ (iii) $k \notin A$
(iv) $p \in B$ (v) $s \notin B$ (vi) $a \in B$
(vii) $20 \in C$ (viii) $11 \in C$ (ix) $\{9\} \in C$

3. If $P(X)$ denotes the power set of X, write down the elements of the set $P(X)$, if $X = \{a, b, c\}$.

4. Let A, B and C be sets. Is the following valid?
$A \neq B \ \& \ B \neq C \Rightarrow A \neq C$.

5. Let μ be a universal set. Simplify
(i) $A \cap u$ (ii) $A \cup u$ (iii) $A \cup A'$
(iv) $A \cup A'$ (v) $(A')'$

6. Given that

$$\begin{aligned} A &= \{c, e, g, i, k\} \\ B &= \{c, d, e, f, g, h\} \\ C &= \{b, d, f, h\} \end{aligned}$$

find
(i) $A \cup B$ (ii) $B \cap C$ (iii) $A \cap (B \cup C)$
(iv) $(A \cap B) \cup (A \cap C)$ (v) $A - B$ (vi) $B - A$

7. Show that $A \subset B \Leftrightarrow B' \subset A'$

8. If $C \subseteq A$ and $C \subseteq B$, show that $C \subseteq A \cap B$

9. By using Venn diagrams, show that

(i) $A \cup (B \cap C) = (A \cup B) \cap (\mathcal{A} \cup \mathcal{C})$

(ii) $(A' \cup B')' = A \cap B$

10. In a school of 100 teachers, 50 teach Mathematics, 45 teach Physics and 35 teach Chemistry. 20 teach Mathematics and Physics but none teaches Mathematics and Chemistry. How many teach Chemistry and Physics? How many teach only Physics?

What is a set?
A set is a collection of well-defined objects, which can be distinguished from one another. We shall say 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 or members of the set and the sets may be finite or infinite in number.

Notation
We shall use capital letters $A, B, C, D, \ldots$ to denote sets and lower case letters $a, b, c, d, \ldots$ to denote elements. The elements of a set may be enumerated or defined by stating a concise unambiguous description of its elements. The symbols used for enclosing the elements of a set is a pair of braces $\{ \cdot \}$. For example if a set A consists of the elements a, b, c, d ad e, we write

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

When a set is defined by stating a description of its elements, the symbols ":" or "|" is used to denote "such that".

For example

$$N = \{n : n \text{ is a whole number}\}$$

means that N is the set of all elements n such that n is a whole number, i.e. N is the set of all whole numbers, $N = \{1, 2, 3, 4, 5, \ldots\}$.

If A is a set and a is an element of A, we write $a \in A$ to mean a is a member of A or a is an element of A. If b is not a member of A, we write $b \notin A$.

Example 1

Write out the elements of the set

$$\begin{aligned} X &= \{n | n \text{ is a whole number}, 0 < n < 5\} \\ X &= \{1, 2, 3, 4\}. \end{aligned}$$

Practice Exercises 1.1

1. List the set of all months in the year whose names begin with J.

2. List the set of all the numbers which can be thrown with a die.

3. Write out the elements of the set

$$H = \{x : x^2 - 5x + 6 = 0\}$$

4. Is the set finite or infinite?

   (i) $P = \{p : p \text{ is a triangle}\}$

   (ii) $A = \{a, b, c\}$.

Subsets

When we remove some or all the elements of a set, what remains is called a subset of the set.

Let A and B be any two sets. If every element of B is an element of A, then B is a subset of A. We use the symbol $\subset$ to stand for "is a subset of". Thus $B \subset A$ means B is a subset of A. On the other hand, the symbol $\not\subset$ stands for "is not a subset of". The symbol $\supset$ stands for 'contains'. Thus $A \supset B$ means that A contains B or that B is a subset of A.

If we extend the idea of a subset to include the cases when either none or all the elements of a set A are removed, then A is also a subset of A and the subset which contains no element is called the empty set or the null set. We shall denote the empty set by the symbol ϕ. Note that the empty set is a subset of every set, by definition.

The collection of all the subsets of a set A is called the power set of A and is denoted by $P(A)$.

Equality of Sets

A set A is equal to set B, written as $A = B$ if the two sets contain exactly the same elements. Since every member of A is also a member of B, and vice-versa it follows that if $A = B$, then $A \subset B$ and $B \subset A$. In fact, if $A \subset B$, $B \subset A$, then $A = B$.

Property and Improper Subsets

The symbols $\subset$ and $=$ are combined to form $\subseteq$ which stands for "is a subset of or is equal to". If $B \subset A$ and if in addition, there is at least one element

of A which is not an element of B, then we say that B is a proper subset of A. Otherwise if $A \subseteq B$ and $A \neq B$, then we say that A is an improper subset of B.

The universal set
The set containing all elements under discussion in a particular problem is called the universal set and is denoted by the symbol u. It therefore follows that the universal set is not unique as it changes from problem to problem. It must therefore be defined for each particular problem.

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,

$$A' = A^c = \{x : x \in u \text{ and } x \notin A\}.$$

Example 2:
List all the subsets of the set $\{1, 2, 3, 4\}$.
The subsets are

$$\phi,\ \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\},$$
$$\{1, 2, 3\}, \{2, 3, 4\}, \{1, 3, 4\}, \{1, 2, 4\}, \{1, 2, 3, 4\}.$$

Example 3
If the universal set is $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$,
find A' if $A = \{1, 5, 6, 9\}$ and $A' = \{2, 3, 4, 7, 8, 10\}$.

Practice Exercises 1.2

1. Describe the following set
   $\{x | x$ is a real number, $x^2 + 1 = 0\}$
2. List all the subsets of the set $\{x, y, z\}$
3. If $u = \{1, 2, 3, 4, 5\}$, list the complements of

(i) $\{1,2,3\}$ (ii) $\{5\}$
(iii) $\{1,2,3,4,5\}$ (iv) ϕ

4. If $u = \{1,2,3,4,5,6,7,8\}$ and $A = \{1,2,4,6,8\}$
   find (i) A', (ii) $(A')'$.

5. Show that the number of elements in the power set $P(A)$ is 2^n, where n is the number of elements in A.

Union of Sets
Let A and B be any two sets. Then we define the union, denoted $A \cup B$, of A and B as the set

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

$A \cup B$ is read as "A union B" or "A cup B" because $\cup$ looks like a cup.

Example 4:
Let $A = \{2,4,6,8\}$, $B = \{1,2,7,8\}$, then $A \cup B = \{1,2,4,6,7,8\}$.

Intersections of sets
Let A and B be any 2 sets. Then we define the intersection, denoted by $A \cap B$, of A and B as the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$
$A \cap B$ is read as "A intersection B" or "A cap B" because $\cap$ looks like a cap.
Thus $A \cap B$ consists of elements common to A and B.
If $A \cap B = \phi$ say sets A and B are disjoint.

Example 5:
Let $A = \{2,3,4\}$, $B = \{2,6,9\}$, then $A \cap B = \{2\}$.

Difference of sets
The difference between two sets A and B, denoted by $A - B$, is the set $A - B = \{x : x \in A \text{ and } x \notin B\}$.
Thus $A - B$ consists of elements in A which are not in B.

Example 6:
Let $A = \{a, b, c\}$ and $B = \{a, d\}$. Then $A - B = \{b, c\}$ and $B - A = \{d\}$.

Practice Exercises 1.3

1. Let u be a universal set. Simplify

   (i) $A \cup A$ (ii) A$\cap A$ (iii) $A \cup \phi$
   (iv) $A \cap \phi$ (v) $A \cap \phi$ (vi) $A \cup u$

2. If $X = \{1, 2, 3, 4\}$, $Y = \{3, 4, 5, 6\}$, $Z = \{5, 6, 7, 8\}$
   determine

   (i) $X \cup Y$ (ii) $X \cap Y$ (iii) $X \cup Z$ (iv) $X \cap Z$
   (v) $Y \cup Z$ (vi) $Y \cap Z$ (vii) $X - Y$ (viii) $Y - X$
   (ix) $X - Z$ (x) $Z - X$ (xi) $Y - Z$ (xii) $Z - Y$

Venn diagrams
We use the following diagrams to represent sets geometrically. We represent a universal set by a rectangle while we use circles to represent subsets of this universal set. We assume that the elements lie inside the rectangle and circles. Such a diagram representing subset of a universal set is called a Venn diagram. For example Fig. 1.1 and 1.2 are Venn diagrams with 2 and 3 subsets of a universal set, respectively.

Fig. 1.1 **Fig. 1.2**

Example 7:
Show that for any sets A, B and C,

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Method 1 (Analytical Method)
($\Rightarrow$ means "imply that" or "implies that")

$$\begin{aligned} x \in \text{ L.H.S.} &\Leftrightarrow x \in A \text{ and } x \in B \cup C \\ &\Leftrightarrow x \in A \text{ and } (x \in B \cup C \text{ or } x \in C) \\ &\Leftrightarrow x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ &\Leftrightarrow x \in A \cap B \text{ or } x \in A \cap C \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C) = \text{R.H.S.} \end{aligned}$$

Method II (By Venn diagrams)

From the Venn diagrams in Figs. 1.3 and 1.4

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Example 8:
For any two finite sets A and B, we have

(i) $n(A \cap B) = n(A) + n(B) - n(A \cup B)$

(ii) $n(A \cup B) = n(A) + n(B) - n(A \cap B)$

where $n(X)$ denotes the number of elements in set X.

Fig. 1.5

Put $n(A \cap B) = y$ so that

$$\begin{aligned} n(A) &= x + y \text{ and } n(B) = y + z \\ \Rightarrow \quad n(A) + n(B) &= (x + y) + (y + z) \\ &= (x + y + z) + y \\ &= n(A \cup B) + n(A \cap B) \\ \Rightarrow \quad n(A \cap B) &= n(A) + n(B) - n(A \cup B), \text{ and} \\ n(A \cup B) &= n(A) + n(B) - n(A \cap B). \end{aligned}$$

Example 9:
In an examination all the candidates offered either English or French. If 52% offered French and 65% offered English, what percentage offered both subjects?

.

Fig. 1.6

In the Venn diagram in Fig. 1.6, let

$$\begin{aligned} E &= \{\text{all candidates who offered English}\} \\ F &= \{\text{all candidates who offered French}\} \\ E \cup F &= \{\text{all candidates sitting the examination}\} \end{aligned}$$

Then $E \cup F$ represents 100%.

$$\begin{aligned} (65 - x) + x + (52 - x) &= 100 \\ \Rightarrow \quad x &= 17 \end{aligned}$$

So $E \cap F$ represents 17% which is the percentage of those who offered both subjects.

Example 10:
In a sample of 1000 foodstuff stores taken at an Ibadan market, the following facts emerged.

200 of them stock rice, 240 stock beans,
250 stock gari, 64 stock both beans and rice,
97 stock both rice and gari, while 60 stock beans and gari.

If 430 do not stock rice, do not stock beans and do not stock gari, how many stores stock rice, beans and gari?

Fig. 1.7

In Fig. 1.7, put $R = \{\text{rice stores}\}$, $B = \{\text{beans stores}\}$ and $G = \{\text{gari stores}\}$. Also put $x = n(R \cap B \cap G)$.
Then

$$\begin{aligned} a &= 200 - [(97 - x) + x + 64 - x)] = 39 + x \\ b &= 240 - [(64 - x) + x + (60 - x)] = 116 + x \\ c &= 250 - [(97 - x) + x + (60 - x)] = 93 + x \\ 1000 &= 430 + a + b + c + (64 - x) + (97 - x) + (60 - x) + x \\ &= 430 + 248 + 3x + 221 - 2x \\ &\Rightarrow \quad x = 1000 - 899 = 101. \end{aligned}$$

so, 101 stores stock rice, beans and gari.

Practice Exercises 1.4

1. Prove analytically and by the use of Venn diagrams that for any sets A, B and C.

   (i) $A \cup B = B \cup A$ (ii) $A \cap B = B \cap A$
   (iii) $(A \cup B) \cup C = A \cup (B \cup C)$ (iv) $A \cap (B \cap C) = (A \cap B) \cap C$
   (v) $(A \cap B)' = A' \cup B'$ (vi) $(A \cup B)' = A' \cap B'$
   Note: (v) and (vi) are known as de-Morgan's laws).

2. In a class of 40 students, 32 are good in Mathematics, 24 are good in Physics and 4 do not take Mathematics and Physics. How many are good in Mathematics and Physics as well?

3. In a survey of 100 housewives, 42 had used Omo detergent, 50 had used Surf, 48 had used Drive, 12 had used Omo and Surf, 18 had used Surf and Drive, and 13 had used Drive and Omo. How many housewives had used all three brands of detergent?

4. If A, B and C are any three sets, show that

$$\begin{aligned} n(A) + n(B) + n(C) &= n(A \cup B \cup C) + n(A \cap B) \\ &\quad + n(A \cap C) + n(B \cap C) - n(A \cap B \cap C) \end{aligned}$$

5. Show that

$$\begin{aligned} A \subset B &\Leftrightarrow B' \subset A' \\ &\Leftrightarrow A \cap B = A \\ &\Leftrightarrow A \cup B = B \\ &\Leftrightarrow A - B = \phi \end{aligned}$$

6. Show that A and B are disjoint sets $\Leftrightarrow A - B = A \Leftrightarrow B - A = B$.

Summary
After defining a set and its notation, we have considered various types of sets such as subsets, equal sets, proper and improper subsets, the universal set and complement. We can now form new sets by taking unions, intersections, and differences of sets. The geometrical representation in the form of Venn diagrams is then considered with applications to problems involving determining the number of elements in finite sets.

Post-Test
See Pre-Test at the beginning of the lecture.

References

1. Beachy, J. *Abstract Algebra*, A study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE TWO

Binary Operations

Introduction
We can only add, subtract, multiply or divide *two* numbers at a time. Such operations in which two elements are involved at a time are called binary operations. We shall consider the four binary operations of addition, subtraction, multiplication and division and extend them to any combination or variation of these operations. We shall also consider the operations of union, intersection and difference on sets as well as any combinations of them.

Objectives
At the end of this lecture the reader should be able to do the following:

(i) determine the properties of binary operations with regard to closure, commutativity, associativity, identity, inverse and idempotent elements;

(ii) determine whether a binary operation on a set is distributive over another binary operation on the same set.

Pre-Test

1. Consider $(Z, \otimes)$ where $\otimes$ is defined for all integers a and b in Z as

$$a \otimes b = a + b - ab$$

(i) Evaluate $5 \otimes 7$

(ii) Solve for $x : x \otimes (-6) = 15$
Determine whether or not the following sets and operations, satisfy;

(a) the closure property,

(b) the commutative law,

(c) the associative law

(d) is there an identity element? If there is, find it.

(e) Find, if it exists, an inverse for each element.

2. $(R, \otimes)$ where $a \otimes b = a + b - ab$

3. $(m\mathbb{Z}, +)$

4. $(\mathbb{Z}_{\text{odd}}, +)$

5. $(\mathcal{F}, \cap)$, where $\mathcal{F}$ is the family of sets in a universal set.

6. $S = \{ax + b \in R[x]\}$ under composition

7. $S = \left\{ \dfrac{zx + b}{cx + d} \in R(x) \right\}$ under composition.

8. Obtain an inverse function for each of the following:

$$\text{(i)} \quad f(x) = 3x - 4 \qquad \text{(ii)} \quad g(x) = 3 - 2x$$
$$\text{(iii)} \quad h(x) = \frac{3x - 7}{5x - 3} \qquad \text{(iv)} \quad \phi(x) = \frac{2x}{2 - x}$$

9. Obtain the operation table. Hence, or otherwise, determine an identity element and an inverse for each element, if they exist.

(i) $(\mathbb{Z}_6, \oplus)$ where $a \oplus b$ is the remainder when $a + b$ is divided by 6.

(ii) $\{4, 8, 12, 16\}$ where $a \otimes b$ is the remainder when ab is divided by 20.

(iii) $(\{\phi, A, A^c, u\}, \cup)$

(iv) $\left\{f_1(x) = x, \quad f_2(x) = \dfrac{1}{x}, \quad f_3(x) = 1 - x, \right.$
$\left. f_4(x) = \dfrac{1}{1-x}, \; f_5(x) = \dfrac{x-1}{x}, \; f_6(x) = \dfrac{x}{x-1} \right\}$
under composition.

10. Show whether or not
    (i) $\otimes$ is distributive over $\oplus$ in $(R, \oplus, \otimes)$ if $a \oplus b = a + b + 1$, $a \otimes b = a + b + ab$.
    (iii) $\div$ is distributive over $+$ in $(R^*, +, \div)$
    (iv) $\cup$ is distributive over $\cap$ in $(\mathcal{F}, \cup, \cap)$
    (v) $-$ is distributive over $\cap$ in $(\mathcal{F}, \cap, -)$.

What is a binary operation?
We have been dealing mainly with the rational operations of addition, subtraction, multiplication and division on real numbers. We now want to extend this idea to general, operations on various sets. We add, subtract, multiply or divide two numbers at a time. Therefore any operation, which is defined on a set by taking any two members of the set at a time, is called a binary operation on the set. Thus addition, subtraction multiplication and division are all binary operations on the set of real numbers. Furthermore, union, intersection and difference are binary operations on the family of sets, while addition and composition are also binary operations on the set of functions.

Notation: We shall be using the following notation for some sets.
N: the set of all natural (or counting) numbers.
Z or I: the set of all integers
$Z^+ = I^+ = N$: the set of all positive integers.
mZ: m-multiples of ± 1 including 0.
$Z_{\text{ev}} = 2Z$: the set of all even integers.
Z_{odd}: the set of all odd integers.
$Z_m : \{0, 1, 2, \ldots, m-1\}$
$Z_m^* = Z_m - \{0\}; \{1, 2, \ldots, m-1\}$
Q: the set of all rational numbers.
Q^+: the set of all positive rational numbers.
$Q^* = Q - \{0\}$, the set of all non-zero rational numbers.

R: the set of all real numbers
R^+: the set of all positive real numbers
$R^* = R - \{0\}$; the set of all non-zero real numbers
$\mathcal{F}$: the family of all sets
$R[x]$: the set of all polynomial functions in x with coefficients in R.
$R(x)$: the set of all rational functions in x with coefficients in R.
$(S, *)$: a set S with a binary operation $*$ defined on S.

Example 1:
Obtain the operation table of $(\mathbb{Z}_5^*, \otimes)$ where $a \otimes b$ is the remainder when ab is divided by 5.

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Example 2:
Consider $(Z, \otimes)$ where $a \otimes b = a + b + ab$.
Evaluate: (i) $3 \otimes 8$, (ii) y if $y \otimes 4 = -31$

(i) $3 \otimes 8 = 3 + 8 + 3(8) = 35$

(ii) $-31 = y \otimes 4 = y + 4 + 4y$
$5y = -35$, $y = -7$

Example 3:
If $f(x) = 2x - 1$, $g(x) = 5 - 2x$, find the composition fog

$$\begin{aligned} fog(x) &= f(g(x)) = f(5 - 2x) \\ &= 2(5 - 2x) - 1 = 9 - 10x \end{aligned}$$

Example 4:
If $f(x) = \dfrac{x-3}{2x-1}$, $g(x) = \dfrac{x-1}{x+1}$

evaluate gof

$$\begin{aligned} gof(x) &= g(f(x)) = g\left(\frac{x-3}{2x-1}\right) \\ &= \left(\frac{x-3}{2x-1}-1\right)\Big/\left(\frac{x-3}{2x-1}+1\right) \\ &= \frac{x-3-(2x-1)}{x-3+(2x-1)} = \frac{-x-2}{3x-4} \end{aligned}$$

Example 5:
Define $x * y = \dfrac{x+y}{xy}$ on $\mathbb{R}$ the set of real numbers.
Examine whether $*$ is a binary operation on R.
$0 * y = \dfrac{0+y}{0(y)} = \dfrac{y}{0}$ = undefined number.
Therefore $0 * y$ is not defined and so $*$ is not a binary operation on R.
(Note that a binary operation must be defined on all pairs of the set).

Practice Exercise II.1

1. Evaluate

   (i) $2\square 5$ if $a\square b = 3a + 4b$ in $(N, \square)$

   (ii) fog if $f(x) = 4x - 1$, $g(x) = \frac{1}{2x} + 3$ in $(R[x], o)$

   (iii) $f^2 = fof$ if $f(x) = \dfrac{x-1}{x+1}$ in $(R(x), o)$.

2. Obtain the operation table

   (i) $\left\{f_1(x) = x,\ f_2(x) = \dfrac{x-1}{x+1},\ \ f_3(x) = \dfrac{-1}{x},\ \ f_4(x) = \dfrac{1+x}{1-x}\right\}$ under composition.

   (ii) $(\{-1, 0, 1\}, \times)$

   (iii) $(\{1, 4, 7, 13\}, \otimes)$, where $a \otimes b$ is the remainder when ab is divided by 15.

   (iv) $(\{\phi, A, A^c, u\}, \cap)$

Closure Property

Let $*$ be a binary operation on a set S. If $a*b$ is a member of S for all members a and b in S, then we say that $(S, *)$ is closed or satisfies the closure property.

In the case of numbers and sets the following sets are closed under the stated operations.

$$\begin{array}{l}(N,+) \quad (N,\times) \\ (Z,+), \quad (Z,-), \quad (Z,\times) \\ (Q,+), \quad (Q,-), \quad (Q,\times), \quad (Q^*,\div) \\ (R,+), \ (R,-), \ (R,\times), \ (R^*,\div) \\ (\mathcal{F},\cup), \ (\mathcal{F},\cap), \ (\mathcal{F},-)\end{array}$$

The following are not closed

$$\begin{array}{l}(N,-), \quad (N,\div) \\ (Z^*,\div), \ (Q,\div), \ (Q^+,-), \ (\mathbb{R}^*,\div), \ (R^+,-)\end{array}$$

Example 6:

Is the set closed under the binary operation?

(i) $(Z_{\text{odd}},+)$ (ii) $(mZ,\times)$

(i) Let a and b be any members of Z_{odd}

$$\begin{aligned} a &= 2m+1 \text{ for some } m \in \mathbb{Z}, \text{ and} \\ b &= 2n+1 \text{ for some } n \in \mathbb{Z}. \end{aligned}$$

Then $a+b = 2(m+n+1) \notin Z_{\text{odd}}$. Therefore Z_{odd} is not closed under addition.

(ii) Note that $m\mathbb{Z} = \{km : k \in \mathbb{Z}\}$
Let a and b be any members of $m\mathbb{Z}$. Then
$a = k_1 m$ for some $k_1 \in \mathbb{Z}$
$b = k_2 m$ for some $k_2 \in \mathbb{Z}$
Then $a \times b = (k_1 k_2 m)m$. Since $k_1 k_2 m \in \mathbb{Z}$, it follows that $a \times b \in m\mathbb{Z}$.
Therefore, $m\mathbb{Z}$ is closed under multiplication.

Practice Exercise II.2

Determine whether or not the closure property is satisfied.

1. $(\{0,1\},+)$
2. $(\{-1,0,1\},\times)$
3. $(\{\phi, A, A^c, \mu\},\cap)$
4. $(\mathbb{Z}_6,\oplus)$ where $a\oplus b$ is the remainder when $a+b$ is divided by 6.
5. $(\{2,4,8,12,14,16\},\otimes)$ where $a\otimes b$ is the remainder when ab is divided by 20.
6. $(N,\oplus)$ where $a\oplus b = a+b-2$.
7. $\{f\in R[x] : f(x) = ax+b\}$ under composition.

Remark
To show that a property is not satisfied, it is sufficient to produce just *one* counter-example. However, to show that a property is satisfied, it must be shown for *all* the members and not just for a few of them.

Property of Commutativity
Let $*$ be a binary operation on a set S. If whenever $a*b = b*a$ for *all* pairs of elements a and b in S, we say that $(S,*)$ satisfies the property of commutativity or $(S,*)$ is Abelian (named after Abel, the Mathematician, who first introduced the idea).

In the case of numbers and sets, the following are commutative under the stated operations.

$$\begin{array}{llll}(N,+), & (N,\times), & (Z,+), & (Z,\times)\\ (Q,+), & (Q,\times), & (R,+), & (R,\times)\\ (\mathcal{F},\cup), & (\mathcal{F},\cap) & & \end{array}$$

The following are not commutative

$$\begin{array}{lll}(Z,-), & (Q,-), & (Q^*,\div)\\ (R,-), & (R^*,\div), & (\mathcal{F},-)\end{array}$$

Example 7:
Examine whether the property of commutativity is satisfied.

(i) $(Z, *)$, $a * b = 2a - b$

(ii) $\{f_1(x) = x,\ f_2(x) = -\dfrac{1}{x},\ f_3(x) = \dfrac{1-x}{1+x}$
$f_4(x) = \dfrac{x+1}{x-1}\}$ under composition.

(i) $3 * 4 = 2(3) - 4 = 2$
$4 * 3 = 2(4) - 3 = 5$
Therefore $3 * 4 \neq 4 * 3$ and so $(Z, *)$ is not commutative.

(ii) Obtain the operation table

o	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

The entries in the operation table are symmetrical about the main diagonal. This shows that $f_i o f_j = f_j o f_i$ for all $i \neq j$. Therefore the set is commutative under composition.

Practice Exercise II.3
Determine whether or not $(S, *)$ is commutative

1. $(Z_{\text{ev}}, -)$
2. $(Q, \otimes)$, $a \otimes b = a + b - ab$
3. $\{f \in R[x] : f(x) = ax + b\}$ under composition.

Property of Associativity
Let $*$ be a binary operation on a set S. If whenever $(a * b) * c = a * (b * c)$ for *all* triples of elements a, b and c in$S$, we say that $(S, *)$ satisfies the property of associativity.

In the case of numbers and sets, the following are associative.

$$\begin{array}{llll}(N,+), & (N,\times), & (Z,+), & (Z,\times)\\ (Q,+), & (Q,\times), & (R,+), & (R,\times)\\ (\mathcal{F},\cup), & (\mathcal{F},\cap) & & \end{array}$$

The following are not associative

$$\begin{array}{lll}(Z,-), & (Q,-), & (Q^*,\div)\\ (R,-), & (R^*,\div), & (\mathcal{F},-)\end{array}$$

Example 8:
Examine whether $(Q,\otimes)$, $a\otimes b = a+b-ab$ satisfies the associative property.

$$\begin{aligned}(a\otimes b)\otimes c &= (a+b-ab)\otimes c\\ &= a+b-ab+c-(a+b-ab)c\\ &= a+b+c-ab-ac-bc+abc\\ a\otimes(b\otimes c) &= a\otimes(b+c-bc)\\ &= a+b+c-bc-a(b+c-bc)\\ &= a+b+c-ab-ac-bc+abc\end{aligned}$$

Therefore $(a\otimes b)\otimes c = a\otimes(b\otimes c)$ and so $(Q,\otimes)$ is associative.

Example 9:
Let f, g and h be any functions in a variable x. Show that $(fog)oh = fo(goh)$.
$[(fog)oh](x) = (fog)(h(x)) = f[g(h(x))]$
$[fo(goh)](x) = f(goh)(x) = f[g(h(x))]$
Therefore $(fog)oh = fo(goh)$.

Remark
From Example 9 above, we can conclude that $(R[x], o)$ and $(R(x), o)$ are associative. Also all their subsets are associative under composition.

Practice Exercise II.4
Examine whether the property of associativity is satisfied.

1. $(N, *), a * b = \max\{a, b\}$
2. $(N, *), a * b = a^2 b$
3. $(Z, \square), a \square b = a + ab$
4. $(R, \square), a \square b = |a - b|$
5. $(N, \oplus), a \oplus b = a + b - 2$.

Identity and Idempotent Elements

Let $*$ be a binary operation on a set S. If there exists an element $e \in S$ such that

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

for all $a \in S$, then we call e an identity element of $(S, *)$. Note that an identity element keeps all elements of S fixed under the binary operation.

However, if only the equation $a * e = a$ is satisfied for all $a \in S$, we call e a right identity element. Similarly, if only the equation $e * a = a$ is satisfied for all $a \in S$, we call e a left identity element. Therefore an identity element is both a right and left identity elements. Note that if $(S, *)$ is Abelian (i.e. commutative), then $a * e = a$ or $e * a = a$ is sufficient for the definition of an identity element.

Any element a in $(S, *)$ which satisfies

$$a * a = a$$

is called an idempotent (element) in $(S, *)$.

Example 10

(i) 0 is an identity element for $(Z, +)$, $(Q, +)$, $(R, +)$ where 1 is an identity element for $(N, \times), (Z, \times), (Q, \times)$ and $(R, \times)$.

(ii) 0 is the only idempotent element in $(Z, +), (Q, +), (R, +)$ since $x + x = x$ has only one solution $x = 0$; while 0 and 1 are the only idempotent elements in $(Z, \times), (Q, \times)$ and $(R, \times)$ since the equation $x^2 = x$ has only two solutions $x = 0$ or 1.

Example 11
Find

(i) an identity element

(ii) idempotent elements in $(\mathcal{F}, \cup)$, if they exist:

(i) We must solve for X in $(\mathcal{F}, \cup)$ the equation

$$A \cup X = A$$

and obtain $X = \phi$. Since $\phi \in \mathcal{F}$, then ϕ is an identity element in $(\mathcal{F}, \cup)$.
(ii) Since $A \cup A = A$ is true for every set A in $(\mathcal{F}, \cup)$ it follows that every member of $\mathcal{F}$ is an idempotent in $(\mathcal{F}, \cup)$.

Example 12
Determine, if it exists, an identity element in $(\{4, 8, 12, 16\}, \otimes)$, where $a \otimes b$ is the remainder when ab is divided by 20.
Consider the operation table

$\otimes$	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

By inspection, we observe that the row and column beginning with 16 contain the numbers in the set $\{4, 8, 12, 16\}$ in the same order as they are written in the top and at the left side of the table. This shows that

$$4 \times 16 = 4 = 16 \times 4 \qquad 8 \times 16 = 8 = 16 \times 8$$
$$12 \times 16 = 12 = 16 \times 12 \quad 12 \times 16 = 16$$

Hence 16 is an identity element.

Practice Exercise II.5
Obtain an identity element and idempotent elements if they exist in the following sets and operations.

1. $(\mathcal{F}, \cap)$
2. $(Q, \otimes), a \otimes b = a + b - ab$
3. $(Z, *), a * b = 2a - b$
4. $(\{2, 4\}, \otimes),\ a \otimes b$ is the remainder when ab is divided by 6.
5. $(R \times R, *),\ (a_1, b_1) * (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$
6. $(N, *),\ a * b = a^2b$
7. $(\mathbb{Z}, \square),\ a \square b = a + ab$
8. Show that $f(x) = x$ is an identity element as well as an idempotent element in the set of functions in a variable x under composition.

Inverses

Let $(S, *)$ be a set together with a binary operation and suppose that $(S, *)$ has an identity element. Given any element $a \in S$ if there exists an element $x \in S$ such that

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

then we say that a has an inverse and that x is an inverse of a. In the same way, we say that x has an inverse and that a is an inverse of x. An inverse of an element $a \in S$ is usually denoted by a^{-1}.

However, if only the equation $a * x = e$ is satisfied, we call x a right inverse of a. Similarly, if only the equation $x * a = e$ is satisfied, we call x a left inverse of a. Therefore an inverse is both a right and a left inverses.

Note that if $(S, *)$ is commutative then either $a * x = e$ or $x * a = e$ is sufficient to define an inverse of a.

Example 13

(i) $-a$ is an inverse of a in $(R, +)$

(ii) $\frac{1}{a}$ is an inverse of a in$(R^*, \times)$

Example 14
Determine, if possible, an inverse for each element of $(Q, \otimes)$ where

$$a \otimes b = a + b - ab$$

Note that 0 is an identity in $(Q, \otimes)$ (see Question 2 of Practice Exercise II.5). We solve for x in $(Q, \otimes)$ the equations.

$$a \otimes x = 0 = x \otimes a$$

$$a + x - ax = 0,\ x = \frac{a}{a-1}$$

Now $\frac{a}{a-1}$ is not defined only when $a = 1$. Therefore all elements, except 1, each has an inverse in $(Q, \otimes)$ and $a^{-1} = \frac{a}{a-1}$.

Example 15
Obtain an inverse, if it exists, for each element in $(\{4, 8, 12, 16\}, \otimes)$ where $a \otimes b$ is the remainder when ab is divided by 20.

From the operation table in Example 12 and since 16 is an identity element, we check for the entries containing 16 in the operation table.

$$\begin{aligned} 4 \otimes 4 &= 16 \text{ means } 4^{-1} = 4 \\ 8 \otimes 12 &= 16 \text{ means } 8^{-1} = 12 \text{ and } 12^{-1} = 8 \\ 16 \otimes 16 &= 16 \text{ means } 16^{-1} = 16 \end{aligned}$$

Example 16
Find an inverse of the function

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

Solve for x the equation

$$y = \frac{3-x}{x+2}\,, \quad x = \frac{3-2y}{y+1}$$

Therefore, the required inverse function is

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

Practice Exercise II.6
Find an inverse for each element of the set, if it exists.

1. $(Z, \times)$
2. $(Z_{\text{ev}}, -)$
3. $(\mathcal{F}, \cup)$
4. $(\mathcal{F}, .\cap)$
5. $(Z_6, \oplus)$, where $a \oplus b$ is the remainder when $a + b$ is divided by 6.
6. $(Z_5^*, \otimes)$, where $a \otimes b$ is the remainder when ab is divided by 5.
7. $(\{1, 5, 8, 12\}, \otimes)$, where $a \otimes b$ is the remainder where ab is divided by 13.
8. (i) $f(x) = \dfrac{x-3}{5-x}$ (ii) $g(x) = 4x - 1$ under composition.

The Distributive Laws

Let $(S, \oplus, \otimes)$ represent a set S on which two binary operations $\oplus$ and $\otimes$ are defined. For example, we are familiar with the binary operations of addition and multiplication on numbers as well as union and intersection on the family of sets.

Let $(S, \oplus, \otimes)$ be a set together with two binary operations. If

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

and

$$(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$$

for *all* a, b and c in S, then we say that the binary operation $\otimes$ is distributive over the binary operation $\oplus$.

However, if only the equation

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

is satisfied for all a, b and c in S, we say that $\otimes$ is distributive from the left (or is left distributive) over $\oplus$. Similarly if only the equation

$$(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$$

is satisfied for all a, b and c in S, we say that $\otimes$ is a distributive from the right (or is right distributive) over $\oplus$.

Note that if $(S, \otimes)$ is commutative then either of the two equations is sufficient to define the distributive law.

Example 17

(i) In $(R, +, \times)$ we know that $\times$ is distributive over addition, i.e.

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

or

$$a(b + c) = ab + ac$$

i.e. we can open or expand the brackets.

(ii) In $(\mathcal{F}, \cup, \cap)$, we can show analytically or by Venn diagrams that $\cup$ is distributive over $\cap$ and also that $\cap$ is distributive over $\cup$, i.e.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

and

$$A \cap (B \cup C) = A \cap B) \cup (A \cap C)$$

for all sets A, B and C.

Example 18
Test whether $\triangle$ is distributive over $\square$ in $(R, \square, \triangle)$ where

$$a \square b = \frac{1}{2}(a - b) \text{ and } a \triangle b = a^2 b$$

We must test whether

(i) $a \triangle (b \square c) = (a \triangle b) \square (a \triangle c)$

(ii) $(b \square c) \triangle a = (b \triangle a) \square (c \triangle a)$

(i) L.H.S. $= a \triangle \frac{1}{2}(b - c) = \frac{1}{2}a^2(b - c)$
R.H.S. $= a^2 b \square a^2 c = \frac{1}{2}a^2(b - c)$
$\therefore$ L.H.S. $=$ R.H.S.

(ii) L.H.S. $= \frac{1}{2}(b-c)\triangle a = \frac{1}{4}(b-c)^2 a$
R.H.S. $= b^2 a \square c^2 a = \frac{1}{2}(b^2 - c^2)a$
$\therefore$ L.H.S. $\neq$ R.H.S.

Therefore $\triangle$ is distributive from the left and not from the right over $\square$ in $(R, \square, \triangle)$.

Practice Exercise II.7

1. Use Venn diagrams or analytical method, to show whether or not:
   (i) $\cup$ is distributive over - in $(\mathcal{F}, \cup, -)$
   (ii) $\cap$ is distributive over - in $(\mathcal{F}, \cap, -)$
   (iii) $-$ is distributive of $\cup$ in $(\mathcal{F}, \cup, -)$
   (iv) $-$ is distributive over $\cap$ in $(\mathcal{F}, \cap, -)$
2. Test whether $\otimes$ is distributive over $\oplus$ in $(R, \oplus, \otimes)$ if
   (i) $a \oplus b = \frac{1}{3}(a-b)$, $a \otimes b = a^2 b$
   (ii) $a \oplus b = a + b + 1$, $a \otimes b = a + b + ab$.

Summary
We give the definitions and examples of
(i) a binary operation
(ii) closure
(iii) commutativity
(iv) associativity
(v) identity element
(vi) idempotent
(vii) inverse element
(viii) distributive laws.

Post-Test
See Pre-Test at the beginning of this lecture.

References

1. Beachy, J. *Abstract Algebra*, A study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE THREE

Logic

Introduction
Logic can be described as the art of reasoning which enables man to reach valid and reasonable conclusions and decisions. In this lecture, we shall consider that part of logic which enables us to reduce reasoning to an algebra which has fixed and simple rules similar to those in the algebra of sets.

Objectives
The reader should be able to

(i) have a working knowledge of the language of logic,

(ii) represent propositions by truth tables, and

(iii) reduce reasoning to an algebra similar to the algebra of sets.

Pre-Test

1. If p represents the statement, 'Pilots are brave' and q represents the statement 'Mathematicians love music', write out the meaning of the following sentences:
   (i) $\wedge q$, (ii) $\sim p \vee q$, (iii) $\sim p \rightarrow \sim q$

2. Is the conclusion drawn from the following arguments valid?

   All musicians have long hair,

   Some musicians play the piano,

   Therefore all who play the piano have long hair.

3. If p is the statement 'all unlucky women are unmarried', and q is the statement, 'all married women are lucky'. Does $p \Rightarrow q$?

4. If p, q, r are propositions, construct the truth tables for
   (i) $(p \vee q) \wedge r$, (ii) $(p \vee q) \vee (p \vee r)$, (iii) $(p \vee \sim p) \vee (q \vee \sim q)$

5. By constructing truth tables show that

   (i) $(p \wedge q) \wedge (\sim p \wedge \sim q)$ is false

   (ii) $\sim [(p \wedge q) \wedge (\sim p \wedge \sim q)]$ must be true

   (iii) $p \Rightarrow q = \sim (p \wedge \sim q) = \sim p \vee q$.

6. Show that the proposition
   $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$
   is a tautology.

7. Show that
   $(p \vee q \vee r) \wedge (p \vee q \vee \sim r) \wedge (p \vee q \vee s) = p \vee q$

8. Construct the truth tables for each of the following propositions
   (i) $(p \wedge q) \vee (\sim p \wedge \sim q)$, (ii) $p \Rightarrow \sim q$, (iii) $\sim p \Leftrightarrow \sim q$

9. Simplify $(p \wedge \sim q) \Rightarrow q$

10. Show that

    (i) $p \vee \sim p$ is true

    (ii) $p \vee (\sim p \vee q)$ is true, and

    (iii) $(p \Leftrightarrow q) \Rightarrow (p \Rightarrow q)$ is true.

What is logic?
Logic is the art of reasoning in which we seek valid conclusions from given statements which are called hypotheses or premises.

Propositions
A proposition is a statement which is either true or false, but not both. We assign either the truth value T when the proposition is true and the truth value F when it is false. We shall use the letters $a, b, c, d, \ldots, p, q, r, s, \ldots$ to denote propositions.

Example 1
The following statements are propositions

1. All triangles are congruent
2. 20 is less than 100.

Note that No. 1 is a false statement while No. 2 is a true statement.

Example 2
The following statements are not propositions

1. What a beautiful lady she is!
2. It is sensational.

This is because we cannot assign any specific truth value to them.

Combinations of Propositions

The connective 'and'
If we combine two propositions with the connective 'and', then we obtain another proposition called the conjunction of the two given propositions.

When we join two propositions p and q, we can combine their truth values in four ways as shown in Table 3.1

p	q
T	T
T	F
F	T
F	F

Table 3.1

When we join three propositions p, q and r we can combine their truth values in $8 = 2^3$ ways as shown in Table 3.2.

p	q	r
T	T	T
T	T	F
T	F	T
F	T	T
T	F	F
F	T	F
F	F	T
F	F	F

Table 3.2

If we join two proportions p, q by the connective 'and', the compound proposition obtained is called 'p and q' and is denoted by $p \wedge q$ (read as 'p cap q'). Note that $p \wedge q$ is true only when p is true and q is true so that the truth table of $p \wedge q$ is as in Table 3.3.

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

Table 3.3

Example 3
Let $p =$ 'He is good in mathematics' and $q =$ 'He is good in Physics'. Then $p \wedge q$ means 'He is good in Mathematics and Physics'.

The connective 'or'
If we combine two propositions with the connective 'or', then we obtain another proposition called the disjunction of the two given propositions.

If we join two propositions p, q by the connective 'or', the compound proposition obtained is called 'p or q' and is denoted by $p \vee q$ (read as 'p cup p'). Note that if at least one of p, q is true, then $p \vee q$ is true, so that the truth table of $p \vee q$ is as in Table 3.4.

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

Table 3.4

Example 4
Let p = 'He is good in Mathematics' and q = 'He is good in Physics'. Then $p \vee q$ means 'He is good in either Mathematics or Physics'.

Equality of Propositions
Two propositions are equal if they have the same truth values. To prove equality of two propositions, a general method is to construct their truth tables.

Example 5
If p, q and r are propositions, show that $p \wedge (q \wedge r) = (p \wedge q) \wedge r$ (Associative law for $\wedge$).
The truth tables of $p \wedge (q \wedge r)$ and $(p \wedge q) \wedge r$ are shown in Table 3.5

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

Table 3.5

From table 3.5, we conclude that

$$p \wedge (q \wedge r) = (p \wedge \epsilon) \wedge r$$

Example 6
If p, q and r are propositions, show that $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$ (i.e. $\vee$ is distributive over $\wedge$).
The truth tables of $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are shown in Table 3.6.

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

Table 3.6

From Table 3.6, we conclude that

$$p \vee (q \wedge r) = (po \vee q) \wedge (p \vee r)$$

Representation by Venn diagrams
In analogy to sets, where $\cup$ is replaced by $\vee$ and $\cap$ by $\wedge$ we can represent

propositions by Venn diagrams.
For example, $p \vee q$ can be represented as shown in Fig. 3.7.

Fig. 3.7

In Fig. 3.7, the regions a, b, c and d represent the following truth values for $p \vee q$.

Region	Truth Value of $p \vee q$
a	T
b	T
c	T
d	F

Similarly for $p \wedge q$, region a represents T while the regions b, c and d represent F.

Practice Exercise III.1
If p, q and r are propositions, show that

1. $p \vee q = q \vee p$ (commutative law for $\vee$)
2. $p \wedge q = q \wedge p$ (commutative law for $\wedge$)
3. $p \vee (q \vee r) = (p \vee q) \vee r$ (associative law for $\vee$)
4. $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ ($\wedge$ is distributive over $\vee$)
5. $p \wedge (p \vee q) = p$ (Absorption law)
6. $p \vee (p \wedge q) = p$ (Absorption law)
7. $p \wedge p = p$ (Idempotent law for $\wedge$)
8. $p \vee p = p$ (Idempotent law for $\vee$)

Tautology and Fallacy
A proposition which is always true no matter what truth values are assigned to its component propositions is called a Tautology and is denoted by its common truth value T.

A proposition which is always false, no matter what truth values are assigned to its component propositions is called a Fallacy and is denoted by its common truth value F.

Example 7
If p is any proposition, show that
(i) $p \vee F = p$ (ii) $p \vee T = T$
Construct the truth tables of $p \vee F$ and $p \vee T$ as in Table 3.8.

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

Table 3.8

From table 3.8, we conclude that

$$p \vee F = p \text{ and } p \vee t = T.$$

Practice Exercise III.2
If p is any proposition: show that

1. $p \wedge F = F$
2. $p \wedge T = p$

The Negation of a proposition
Let p be a proposition. Then its negation, denoted by $\sim p$, $\bar{p}$ or p' is another proposition which always has the opposite truth value to that of p. In other words, when p is true, $\sim p$ is false while when p is false, $\sim p$ is true.

Example 8
Let p = all men are mad. Then $\sim p$ = some men are not mad or not all men are mad or some men are sane.

Note that $\sim p \neq$ all men are not mad, because you require only 1 sane man to negate proposition p.

Example 9
Show that if p and q are propositions, then

$$\sim (p \vee q) = \sim p \wedge \sim q \text{ (De-Morgan's law)}$$

Construct the truth tables for both sides of the equation in Table 3.9.

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

Table 3.9

From Table 3.9, we conclude that

$$\sim (p \vee q) = \sim p \wedge \sim q.$$

Practice Exercise III.3
If p, q are propositions, show that

1. $p \vee \sim p = T$
2. $p \wedge \sim p = F$
3. $\sim (\sim p) = p$
4. $\sim F = T, \sim T = F$
5. $\sim (p \wedge q) = \sim p \vee \sim q$ (De-Morgan's law)
6. $[(p \vee q) \wedge (p \vee \sim q)] \vee \sim p = T$.

Implication and Equivalence
If p and q are propositions, we can combine them with the connective 'if... then' (which is denoted by $\Rightarrow$) to form a compound proposition. Thus $p \Rightarrow q$ is read as "if p, then q" or "p implies q" or "p is sufficient for q". The proposition $p \Rightarrow q$ has truth values as shown in Table 3.10.

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 3.10

The first two truth values assigned to $p \Rightarrow q$ in Table 3.10 are obvious. Note that when p is false, it does not depend on the truth value of q. If p is false, q can have any truth value without changing the truth value of $p \Rightarrow q$. We therefore assign the truth value T to $p \Rightarrow q$ whenever p is false. In other words, if p is false, then no condition is imposed on q in $p \Rightarrow q$. Whereas if p is true, then q must be true if $p \Rightarrow q$ is to be true; and if p is true and q is false, then $p \Rightarrow q$ must be false.

Illustration to explain the Truth Table for $p \Rightarrow q$

Let p = The figure is an isosceles triangle
q = The figure is a triangle

Then we have

(i) $p \Rightarrow q$ is always true

(ii) $p \Rightarrow \sim q$ is always false

(iii) $\sim p \not\Rightarrow q$ is not always true for the figure could still be a triangle. Thus $\sim p \not\Rightarrow q$ is false and so $\sim p \Rightarrow q$ is true.

(iv) $\sim p \not\Rightarrow \sim q$ is not always true for the figure may not be a triangle. Thus $\sim p \not\Rightarrow \sim q$ is false and so $\sim p \Rightarrow \sim q$ is true.

Equivalence
If p, q are propositions, we can combine them with the connective "if and only if" (which is denoted by $\Leftrightarrow$) to form a compound proposition. Thus $p \Leftrightarrow q$ is read as "p if and only if q" or "p is equivalent to q" or "p is a necessary and sufficient condition for q". Also $p \Leftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$ so that its truth value can be obtained as in Table 3.11.

p	q	$p \Rightarrow q$	$p \Rightarrow p$	$p \Leftrightarrow q$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

Table 3.11

From Table 3.11, we find that $p \Leftrightarrow q$ is true when p, q are both true or both false and is false otherwise.

In the proposition $p \Rightarrow q$, we call $q \Rightarrow p$ the converse proposition to $p \Rightarrow q$, $\sim p \Rightarrow \sim q$ the inverse proposition to $p \Rightarrow q$, and $\sim q \Rightarrow \sim p$ the contrapositive proposition $p \Rightarrow q$.

Example 10
Find the relationship among
$p \Rightarrow q$, $q \Rightarrow p$, $\sim p \Rightarrow \sim q$ and $\sim q \Rightarrow \sim p$.
The truth values are shown in Table 3.12.

p	q	$q \Rightarrow q$	$q \Rightarrow p$	$\sim p$	$\sim q$	$\sim p \Rightarrow \sim q)$	$\sim q \Rightarrow \sim p$
T	T	T	T	F	F	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Table 3.12

From Table 3.12 we conclude that

$$(p \Rightarrow q) = (\sim q \Rightarrow \sim p) \text{ and } (q \Rightarrow p) = (\sim p \Rightarrow \sim q),$$

i.e. a proposition is equal to its contrapositive.
However, there is no relationship among a proposition, its converse and inverse.

Remark
The logic $(p \Rightarrow q) = (\sim q \Rightarrow \sim p)$ is usually employed in proving mathematical statements and it is referred to as proof by contradiction. If the statement

to be proved is $p \Rightarrow q$, then sometimes it is easier to prove its contrapositive $\sim q \Rightarrow \sim p$.

Practice Exercise III.4

1. Show that

   (i) $(p \Rightarrow q) = (\sim p \vee q)$

   (ii) $(p \Rightarrow q) \vee p = (p \wedge q) \Rightarrow q = p \Rightarrow (p \vee q)$

   (iii) $(p \Rightarrow q) \vee q = (p \vee q) \Rightarrow q = p \Rightarrow (p \wedge q)$

   (iv) $(p \Rightarrow q) \wedge q = q$

   (v) $(p \Rightarrow q) \wedge p = p \wedge q$

2. Simplify

   (i) $(p \Leftrightarrow q) \wedge p$ (ii) $(p \wedge q) \Leftrightarrow p$

   (iii) $(p \Leftrightarrow q) \vee p$ (iv) $(p \vee q) \Leftrightarrow q$

Syllogism
A syllogism is a conclusion in logic from two or more given statements.

Example 11
If p = Mary is a female student in Form five, q = All form Five female students are members of the women basket ball team. What conclusion can you draw?

Put m = Mary
F = {Form five female students}
B = {Basket ball team}

Then $m \in F$ and $F \subset B$. The conclusion is that $m \in B$, i.e. Mary is a member of the women basket ball team.

Practice Exercise III.5

1. Consider the statements: A man born and bred in Kaduna claims he is a native of Oyo State of Nigeria. Therefore, Kaduna is in Oyo State of Nigeria. Is the argument valid?

2. Consider the statements: Lagos is the largest city in Nigeria. The Federal Government of Nigeria is based in its largest city. Therefore, Lagos is the capital city of Nigeria. Is the argument valid?

3. Draw a Venn diagram to illustrate the statements: All animals must breathe to live. Dogs are animals. What conclusion can you draw from your diagram?

4. Is the following argument sound? Every rectangle has four sides and four right angles. Therefore a rectangle is a square. Illustrate your answer in a diagram.

5. Consider the following argument. All the members of this class can ride a bicycle. Olu is not a member of this class. Therefore, Olu cannot ride a bicycle. Is the argument valid?

6. Consider the following argument. A crime had been committed. Ali was around the scene of the crime when it was committed. Therefore Ali must have committed the crime. Is the argument valid?

7. The Executive Committee of a Students' Union is divided into subcommittees. Write down each of the following propositions using suitable symbols.

   (a) Past Presidents are not allowed on the social sub-committee.

   (b) All members of the Games subcommittee must be on the Finance sub-committee.

   (c) All members of the Bar sub-committee also serve on the Social sub-committee.

   (d) Every member of the committee must serve in the Games sub-committee or the Bar sub-committee.

What major conclusion can you draw from these propositions?

Algebra of Sets and Propositions

From the above discussion we see that the algebra of propositions is very similar to the algebra of sets. Table 3.13 shows that they are identical apart from the changes in symbols used in both cases.

Algebra of Sets A, B, C	Algebra of Propositions p, q, r
$\cup$	$\vee$
$\cap$	$\wedge$
A'	$\sim p$
u	T
ϕ	F

Table 3.13

Because of the similarities, the methods of simplification for the algebra of sets can be applied in the algebra of propositions.

Example 12

Simplify

$$\begin{aligned}
[(p \vee q) \wedge (p \vee \sim p)] \vee \sim p &= [(p \vee q) \vee \sim p] \wedge [(p \vee \sim q) \vee \sim p], \text{ (distributive law)} \\
&= [(p \vee \sim p) \vee q] \wedge (p \vee \sim p) \vee \sim q], \text{ (commutative law)} \\
&= (T \vee q) \wedge (T \vee \sim q), \text{ (property of complement)} \\
&= T \wedge T, \text{ (property of } T) \\
&= T, \text{ (property of } T)
\end{aligned}$$

Practice Exercise III.6

Simplify

$$[p \wedge (\sim p \vee q)] \vee [q \wedge \sim (p \wedge q)].$$

Summary
We considered in logic

(i) propositions as statements which are either true or false but not both;
(ii) compound propositions using connectives of 'and' and 'or'.
(iii) equality of propositions using truth tables and Venn diagrams.
(iv) negation of propositions
(v) special propositions called Tautology and Fallacy
(vi) syllogism which is making valid conclusions
(vii) the similarity of the algebra of propositions with the algebra of sets.

Post-Test
See Pre-Test III at the beginning of the lecture.

References

1. Beachy, J. *Abstract Algebra*, A study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE FOUR

Switching Algebras

Introduction
We shall see that electrical switching circuits can be reduced to an algebra which is similar to the algebra of sets or propositions. By this, complicated electrical circuits can be simplified.

Objectives
The reader should be able to

(i) represent electrical circuits by closure tables and

(ii) reduce electrical circuits to an algebra similar to the algebra of sets or propositions.

Pre-Test

1. Construct the closure tables for the following circuits:
   (i) $pq + r$ (ii) $(p + q)(p + r)$

2. Show, by constructing closure tables, that

   (i) $p + qr = (p + q)(p + r)$ (+ is distributive over.)

(ii) $p + pq = p$ (absorption law)
Simplify and draw the simplified circuit for Questions 3 to 10.

3. $(p + q)(p + q')$

4. $p'q' + p + q$

5. $(p + q + r)(p + q + r')$

6. $(p + q' + r')(p + qr)$

7. $(p + q + r' + x')(p + q + rx)$

8.

9.

10.

Electrical circuits
When current flows in an electrical circuit, it flows through a switch or switches. When current flows through a switch, then the switch is said to be

closed, but when no current flows, the switch is said to be open. We shall denote switches by the symbols p, q, r, x, etc.

In an electrical circuit, we have two types of arrangements. (see Fig. 4.1).

(a) **(b)**

Fig. 4.1

In (a), we say that the switches p and q are in series. If switch p is open or closed and q is open, then no current will flow in the circuit. If both p and q are closed, then current flows. In (b), we say that the switches are arranged in parallels. If switch p is closed, and q is open, the current flows through the circuit. If both switches are closed, current also flows through the circuit. However no current flows through the circuit when both switches are open. We assign the closure value 1 when a switch is closed and closure value 0 when the switch is open.

Definition

1. We define for a switch p, another switch denoted by p' called the negation of p. If p is closed, then p' is open and vice-versa.

2. When switches p and q are in series, then we denote the circuit by pq as in Fig. 4.1(a).

3. When switches p and q are in parallel we denote the circuit by $p + q$ as in Fig. 4.1(b).

4. A switch which is always closed is denoted by 1.

5. A switch which is always open is denoted by 0.

6. Two circuits are equal if they have the same closure tables.

We can then show that electrical circuits satisfy the same properties as sets and propositions if we identify the operations as in Table 4.2.

	Complement 'Negation'	$\cup, \vee, +$	$\cap, \wedge, \cdot$	$u, T, 1$	$\Phi, F, 0$
Sets	A'	$A \cup B$	$A \cap B$	u	Φ
Propositions (logic)	$\sim p$	$p \vee q$	$p \wedge q$	T	F
Switching circuits	p'	$p + q$	pq	1	0

Table 4.2

If p, q nd r are electrical switches, then the following properties are satisfied.

1. $p + q = q + p$, $pq = qp$ (commutative laws)

2. $p + (q + r) = (p + q) + r$, $p(qr) = (pq)r$ (associative laws)

3. $p + 1 = p$, $p + 0 = p$ (Identity law)

4. $p(q + r) = pq + pr$, $p + qr = (p + q)(p + r)$ (distributive laws)

5. $p(p + q) = p$, $p + pq = p$ (Absorption laws)

6. $p \cdot 0 = 0$, $p + 1 = 1$ (Property of 0 and 1)

7. $p \cdot p = p$, $p + p = p$ (Idemptotent law)

8. $(p + q)' = p'q'$, $(pq)' = p' + q'$ (De-Morgan's laws)

9. $p + p' = 1$, $pp' = 0$, $(p')' = p$, $1' = 0$, $0' = 1$.
(Properties of negation).

Note that we can prove all these properties by constructing closure tables.

Example 1
If p and q are switches, show that

$$p(p+q) = p \ \text{ (Absorption law)}$$

The tables of p and $p(p+q)$ are shown in Table 4.3 from which we conclude that $p(p+q) = p$.

p	q	$p+q$	$p(p+q)$
1	1	1	1
1	0	1	1
0	1	1	0
0	0	0	0

Table 4.3

Example 2
Simplify and draw the simplified circuit.

$$\begin{aligned}
(p'+q')(p+q')(p+q) &= (p'p + p'q' + q'p + q'q')(p+q) \\
&= (0 + p'q' + q'p + q')(p+q) \\
&\qquad\qquad \text{(negation and idempotent)} \\
&= q'(p+q) \text{ (property of 0 and absorption law)} \\
&= q'p + 0 \text{ (negation)} \\
&= q'p \text{ property of 0)}
\end{aligned}$$

Fig. 4.4: The simplified circuit $q'p$.

Example 3
Simplify the circuit in Fig. 4.5 and draw the simplified circuit.

Fig. 4.5

The circuit is given by the expression

$$\begin{aligned}(p+q)(p+r)+r(p+qr) &= pp+pr+qp+qr+rp+rqr \\ &= (p+pr+qp+rp)+(qr+rqr) \text{ (idempotent)} \\ &= p+qr \text{ (absorption law)}\end{aligned}$$

The simplified circuit is shown in Fig. 4.6.

Fig. 4.6

Practice Exercise IV

1. Show that the properties listed for electrical circuits are satisfied. Draw the two equivalent circuits.

2. Simplify and draw the simplified circuit:

   (i) $(p' + q)p$

   (ii) $(p' + q')(p' + q)(p + q)$

   (iii) $(p + q + rst)(p + q + r' + s' + t')$

   (iv) $(p + q + r' + pq)(p'q' + r' + y' + x')$.

Summary

We considered different types of electrical switches such as

(i) open and closed switches

(ii) switches in series and in parallel.

We then consider equal switches through the considerations of their closure tables and observe that the algebra of electrical switches is similar to the algebra of sets and the algebra of propositions.

Post-Test

See Pre-Test at the beginning of the Lecture.

References:

1. Beachy, J. *Abstract Algebra*, A study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE FIVE

Switching Algebras

Introduction
We shall study different types of relations such as reflexive, symmetric, transitive, and equivalence relations. We shall then show that the interesting relations are the equivalence relations which partition the sets on which they are defined into disjoint equivalence classes.

Objectives
The reader should be able to

(i) distinguish different types of relations, and

(ii) use an equivalence relation to partition the set on which it is defined.

Pre-Test

1. Let $T = \{(x, y) \in N^2 | 2x + y = 10\}$ be a relation in the set of natural numbers. Find:
   (a) domain of T (b) range of T (c) T^{-1}.

2. Consider the relation in the set of real numbers defined by

$$f = \{(x, y) \in R^2 | y = 24 - x^2\}$$

(i) Find the domain, range and inverse of f

(ii) Draw on the same axes, the graphs of f and f^{-1}.

3. Let R be the set of real numbers and T_1, T_2 two relations on R, whose graphs are given by

$$\begin{aligned} T_1^* &= \{(x,y) \in R \times R | x^2 + y^2 \leq 169\} \\ T_2^* &= \left\{(x,y) \in R \times R | y \geq \frac{5x}{12}\right\} \end{aligned}$$

Sketch $T_1^* \cap T_2^*$ on the coordinate diagram of $R \times R$.

4. Let $\sim$ be a relation on $Z - (0)$ where Z is the set of integers, defined by $a \sim b$ if $a|b$ (i.e. a divides b) and $b|a$ (i.e. b divides a). Show that $\sim$ is an equivalence relation and determine the equivalence classes of $\sim$.

5. Determine whether the following relation in the set R of real numbers is an equivalence relation.

$$x \text{ is related to } y \text{ if } x \leq y \text{ for } x, y \in R.$$

6. Determine whether the following relation in the set R of real numbers is an equivalence relation

$$x \text{ is related to } y \text{ if } xy = 1 \text{ for } x, y \in R.$$

7. Two relations R and S are defined in the set of integers by

$$\begin{aligned} &mRn \text{ if 3 divides } 2m + n \\ &mSn \text{ if 4 divides } 2m + n \end{aligned}$$

(i) Show that one of these relations is an equivalence relation and the other is not.

(ii) Describe the equivalence classes into which the equivalence relation partitions the integers.

(iii) Determine a subset of the set of integers on which the other relation is an equivalence relation.

8. If T is a relation, prove that $(T^{-1})^{-1} = T$.

9. Let h, g be any relations. Show that

$$(hog)^{-1} = g^{-1}oh^{-1}$$

10. If S and S' are symmetric relations in a set A, show that $S \cap S'$ is also a symmetric relation in A.

Definitions

1. The *Cartesian product* of sets X and Y is the set $X \times Y$ of all ordered pairs (x, y) such that $x \in X$ and $y \in Y$ i.e.

$$X \times Y = \{(x, y) | x \in X, y \in Y\}$$

2. A *relation* is a set of ordered pairs. Thus any subset of $X \times Y$ defines a relation on $X \times Y$. If f is a relation, theh $(x, y) \in f$ is sometimes written as xfy (and read as 'x is in relation f to y').

Remark
Sometimes we distinguish a relation from its defining set of ordered pairs. If R denotes the relation, then R^* denotes the set of ordered pairs, called the *graph* of R.

3. The *domain* of a relation f is the set

$$D(f) = \{x | (x, y) \in f \text{ for some } y\}$$

(the set of all first coordinates).

4. The *range* of f is the set

$$R(f) = \{y : (x, y) \in f \text{ for some } x\}$$

(the set of all second coordinates).

5. The *inverse* of f is the set

$$f^{-1} = \{(y, x) | (x, y) \in f\}$$

6. If f and g are relations such that f and g are both subsets of $X \times Y$, we define the *composition* (or *product*) of f and g as the relation:

$$gof = \{(x, z) | (x, y) \in f \text{ and } (y, z) \in g \text{ for some } y\}$$

Composition of relations may not be commutative as shown by the *Counter-example*. Let $f = \{(1, 2), (3, 4)\}$, $g = \{(0, 1)\}$. Then $fog = \{(0, 2)\}$ while $gof = \phi$. Thus $fog \neq gof$.

7. *Equivalence relations*
An equivalence relation on a set X is any relation $\sim \subseteq X \times X$ such that for all $x, y, z \in X$, we have

(i) $x \sim x$ (Reflexive law)

(ii) $x \sim y$ implies that $y \sim x$ (Symmetric law)

(iii) $x \sim y$ and $y \sim z$ implies that $x \sim z$ (Transitive law)

Note: An equivalence relation satisfies the R, S, T laws.

8. Let $\sim$ be an equivalence relation on a set S, define the *equivalence class* of a as the set of all elements b in S such that $a \sim b$ and denote this set by $[a]$, i.e.

$$[a] = \{b \in S | a \sim b\}$$

The set of all equivalence classes in S is called the *quotient set* of $\sim$ and it is denoted by $S/\sim$.

9. Let Ω be any set, finite or infinite. The set $\{S_\alpha | \alpha \in \Omega\}$ is said to be indexed by Ω and Ω is called an *indexing* set for this set.

10. A family $\{S_\alpha | \alpha \in \Omega\}$, where Ω is an indexing set, of subsets of a set S is said to form a <u>partition</u> of S if

(i) $S = \bigcup_{\alpha \in \Omega} S_\alpha$ and

(ii) for S_α, S_β either $S_\alpha = S_\beta$ or $S_\alpha \cap S_\beta = \phi$.

Example 1
Let $\sim$ be the relation of equality, $=$ on any set S. Then it is easy to check that $\sim$ is an equivalence relation.

Example 2
If $\sim$ is an equivalence relation on a set S, show that the set of all equivalence classes of $\sim$ gives a partition of S.

We show that

(i) $S = \bigcup_{a \in S} [a]$, and

(ii) $[a] \cap [b] \neq \phi \Rightarrow [a] = [b]$.

Solution

(i) Since $[a] \subseteq S$, we have that $\bigcup_{a \in S} [a] \subseteq S$ ...(1)

Also for any $a \in S$, $a \in [a]$

$$\Rightarrow \quad a \in \bigcup_{a \in S} [a] \Rightarrow S \subseteq \bigcup_{a \in S} [a] \qquad \ldots (2)$$

(1) and (2) imply that $S = \bigcup_{a \in S} [a]$

(ii) Now suppose $x \in [a] \cap [b]$, then $x \in [a]$ and $x \in [b]$
i.e. $x \in [b]$ ...(3)
and $b \sim x$ ...(4)
Let $y \in [a]$, then $a \sim y$ which implies that $y \sim a$ ...(5)
since $\sim$ is symmetric. Now (5) and (3) imply
$y \sim x$, by the transitivity of $\sim$,
$\Rightarrow x \sim y$, ...(6)
by the symmetric law. Now (4) and (6) imply $b \sim y$, by the transitive law. This implies

$$y \in [b] \Rightarrow [a] \subseteq [b]$$

By a similar argument, one can show that $[b] \subset [a]$. Hence $[a] = [b]$. Hence the equivalence classes of S give a partition of S.

Example 3
Define a relation $\sim$ on Z, the set of all integers by $x \sim y$ means $m|x-y$, $m \in Z^+$ ($m|x-y$ means "m divides $x-y$"). Show that $\sim$ is an equivalence relation and describe the equivalence classes of $\sim$. [The equivalence classes are denoted by Z_m and are called residue classes of integers modulo m].

Reflexive law: Let $x \in Z$. Since $m|0$, i.e. $m|x-x$, it follows that $x \sim x$. Hence the reflexive law is satisfied.

Symmetric law: Suppose $x \sim y$, show $y \sim x \cdot x \sim y \Rightarrow m|x-y \Rightarrow m|y-x$ since $y-x=-(x-y) \Rightarrow y \sim x$. Hence the symmetric law is satisfied.

Transitive law
Suppose $x \sim y$ and $y \sim z$, show $x \sim z$. Now $x \sim y$ and $y \sim z$ imply $m|x-y$ and $m|y-z$

$$\Rightarrow \quad m|(x-y)+(y-z) \text{ i.e. } m|x-z \Rightarrow z \sim z$$

Hence, the transitive law is satisfied.

Therefore the relation $\sim$ is an equivalence relation. The equivalence classes are
$[0]=\{b \in Z|b=mq \text{ for all } q \in Z\}$
$[1]=\{b \in Z|b=1+mq \text{ for all } q \in Z\}$
$[m-1]=\{b \in Z|b=m-1+mq \text{ for all } q \in Z\}$

Example 4
Let Z^+ denote the set of all positive integers and let a relation $\sim$ on Z^+ be defined by $a \sim b$ if there exists a positive integer n such that $a|b^n$. Show that $\sim$ is both reflexive and transitive on Z^+. By constructing a suitable counter-example, show that this relation is not symmetric

$$a \sim b \Leftrightarrow \text{ there exists } n \in Z^+ \text{ such that } a|b^n.$$

Reflexive law: Show $a \in Z^+ \Rightarrow a \sim a$. Now for $n=l \in Z^+$, we have $a|a^1 \Rightarrow a \sim a$. Hence the reflexive law is satisfied.

Transitive law: Show $a \sim b$ and $b \sim c \Rightarrow a \sim c$. $a \sim b$ and $b \sim c \Rightarrow a|b^n$ and $b|c^m$ for some n, m

$$\begin{aligned} & n, m \in Z^+ \Rightarrow b^n = k_1 a \text{ and } c^m = k_2 b \\ & c^m = k_2 b \Rightarrow c^{mn} = k_2^n b^n = k_2^n k_1 a \\ \Rightarrow \quad & c^{mn} = k_3 a \text{ for } k_3 = k_2^n k_1 \\ \Rightarrow \quad & a|c^{mn} \Rightarrow a \sim c \end{aligned}$$

Hence the transitive law is satisfied.

Symmetric law: Let $a = 2$, $b = 6$. Then

$$6^1 = 3 \times 2 \text{ i.e. } 2|6^1 \Rightarrow 2 \sim 6$$

We shall show that $6 \not\sim 2$. If $6 \sim 2$, then $2^n = 6k$ for $n, k \in Z^+$. But there does not exist any $n \in Z^+$ such that $2^n = 6k$. Hence $6 \not\sim 2$ and the relation $\sim$ is not symmetric.

Practice Exercise V

1. Let $S = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and let $\sim$ be a relation defined on S by

   $$n \sim m \text{ if } m \text{ is a multiple of } n.$$

   Write out members of $\sim$.

2. Define a relation $\sim$ on Z, the set of all integers by $x \sim y$ means $7|x-y$. Show that $\sim$ is an equivalence relation and describe the equivalence classes of $\sim$.

3. Prove that a relation T is symmetric if and only if $T^{-1} = T$.

4. Let f, g, h be any relations. Show that $fo(goh) = (fog)oh$.

Summary
We considered a relation as any subset of the Cartesian product of two sets. We then define the graph, domain, range, and inverse of a relation together with the composition or product of two relations. Finally we consider a special type of relation called an equivalence relation which satisfies the reflexive, symmetric and transitive laws and which partitions the set on which it is defined into a set of disjoint equivalence classes called the quotient set.

Post-Test
See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE SIX

Orders

Introduction
We shall study a special class of relations called partially ordered sets. We shall then consider some of their distinguished elements such as least, greatest, minimal and maximal elements as well as lower and upper bounds of their subsets, and then conclude with some partially ordered sets called totally-ordered and well-ordered sets.

Objectives
The reader should be able to identify:

(i) partially ordered sets (posets)

(ii) least, greatest, minimal and maximal elements of posets,

(iii) lower and upper bounds, greatest lower and least upper bounds of subsets of posets, and

(iv) totally-ordered and well-ordered sets.

Pre-Test

1. Let $\mathcal{F}$ denote the family of all sets in a universal set and let $A \sim B$ mean $A \subset B$.
   Show that $(\mathcal{F}, \subseteq)$ is a partially ordered set.

2. Let $S = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and let $\sim$ be a relation defined on S by

   $$n \sim m \text{ if } m \text{ is a multiple of } n.$$

   Is $(S, \sim)$ a partially ordered set?

3. Let $S = \{1, 2, 3, 4\}$ and let
   $\sim = \{(1,1), (2,2), (3,3), (4,4), (1,2), (1,3), (1,4), (2,4)\}$ such that $(S, \sim)$ is a poset. Find.

   (i) the set of first elements of $(S, \sim)$

   (ii) the set of least elements of $(S, \sim)$

   (iii) the set of minimal element, of $(S, \sim)$

   (iv) the set of maximal elements of $(S, \sim)$

4. If S is partially ordered by $\overset{\alpha}{\sim}$, show that it may contain several minimal elements or none.

5. Let $(R \leq)$ be a poset where R is the set of real numbers. Consider the open interval (a, b) as a subset of R. Find

   (i) the set of lower bounds of (a, b);

   (ii) the set of greatest lower bounds of (a, b);

   (iii) the set of upper bounds of (a, b);

   (iv) the set of least upper bounds of (a, b).

6. Let S be a poset and T be a subset of S.
   Show that if $sup(T)$ exists in S, then it is unique.

7. Show that $(Z, \leq)$ is a totally ordered set where Z is the set of integers.

8. Show that $(S, \leq)$ is a well-ordered set where $S = \{n \in Z; n \geq -100\}$

9. Show that a totally-ordered set can have at most one minimal element which would then be a first element.

10. Let S be a poset and let every subset of S contain a first element. Show that S is totally ordered.

Partially ordered sets

A relation $\sim$ on a set S is said to be *anti-symmetric* if $a \sim b$ and $b \sim a$ imply that $a = b$. A relation $\sim$ on a set S is called a partial order if $\sim$ is reflexive, anti-symmetric and transitive. $(S, \sim)$ is then said to be a *partially ordered set* (or $p \cdot o.$ set or poset) and if $a \sim b$ we write $a \overset{\alpha}{\sim} b$ and read this as "a precedes b" or "b dominates a". If $a \sim b$, and $a \neq b$, we write $a \propto b$ and read this as "a properly precedes b" or "b properly dominates a".

Example 1

(i) Let R denote the set of real numbers and let $a \sim b$ means $a \leq b$. Show that $(R, \leq)$ is a poset

(ii) Let $S = \{1, 2, 4, 6\}$ and let $\sim$ be a relation defined on S by $\sim = \{(2, 4), (3, 6), (4, 5), (5, 5), (6, 3)\}$.
Show that $\sim$ is not antisymmetric.

Solution

(i) *Reflexive law:* Since $a \leq a$ for all $a \in R$, it follows that the relation $\leq$ satisfies the reflexive law.

Anti-symmetric law: If $a \leq b$ and $b \leq a$, then $a = b$. Therefore, the relation $\leq$ is anti-symmetric.

Transitive law: If $a \leq b$ and $b \leq c$, then $a \leq c$. Hence the relation $\leq$ is transitive. Therefore $(R, \leq)$ is a poset.

(ii) *Anti-symmetric law:* Since (3,6) and (6,3) are members of $\sim$ and $6 \neq 3$, it follows that the relation $\sim$ is not anti-symmetric.

Example 2 Let $\mathcal{P}$ denote the set of all propositions, and let $\overset{\alpha}{\sim} q$ mean $p \wedge q = p$. Show that $(\mathcal{P}, \overset{\alpha}{\sim})$ is a partially ordered set.

Solution
Reflexive law:
$p \wedge p = p$ (Idempotent)
$\Rightarrow\ p \overset{\alpha}{\sim} p$. Hence $\overset{\alpha}{\sim}$ is reflexive.

Anti-symmetric law: Let $p \overset{\alpha}{\sim} q$ and $q \overset{\alpha}{\sim} p$. Then $p \wedge q = p$ and $q \wedge p = q$. Now $p \wedge q = q \wedge p$ (commutative law).
$\Rightarrow\ p = q$. Hence $\overset{\alpha}{\sim}$ is antisymmetric.

Transitive law: Let $p \overset{\alpha}{\sim} q$ and $q \overset{\alpha}{\sim} r$.
Then $p \wedge q = p$ and $q \wedge r = q$. Now
$(p \wedge q) \wedge r = p \wedge (q \wedge r)$ (Associative law)

$$\begin{aligned} \Rightarrow\ p \wedge r &= (p \wedge q) \wedge r = p \wedge (q \wedge r) \\ &= p \wedge q = p \Rightarrow p \overset{\alpha}{\sim} r. \end{aligned}$$

Hence $\overset{\alpha}{\sim}$ is transitive.
Hence $(\mathcal{F}, \overset{\alpha}{\sim})$ is a poset.

Least, greatest, minimal and maximal elements
Let $(S, \overset{\alpha}{\sim})$ be a poset. An element a in S is called the *first* or least *element of* S if a precedes every other element of S i.e., $a \overset{\alpha}{\sim} x$ for all $x \in S$. We call b the *last* or *greatest* element of S if b dominates every other element of S, i.e. $y \overset{\alpha}{\sim} b$ for all $y \in S$.

An element c in S is called a *minimal element* if there exists no element in S which properly precedes c.

$$\text{i.e. } x \overset{\alpha}{\sim} c \Rightarrow x = c$$

Similarly, an element d in S is called a *minimal element if there* exists no element of S which properly dominates d.

$$\text{i.e. } d \overset{\alpha}{\sim} y \Rightarrow d = y$$

Example 3
Consider the relation R whose graph is given by $R^* = \{(2,4),(2,5),(4,5),(6,3),(2,2),(3,3),(4,4),(5,5),(6,6)\}$ on the set $S = \{2,3,4,5,6\}$. Find

(i) the set of all first elements of (S,R);

(ii) the set of all last elements of (S,R);

(iii) the set of all minimal elements of (S,R)

(iv) the set of all maximal elements of (S,R).

Note that (S,R) is a poset satisfying the reflexive, antisymmetric and transitive laws.

(i) the set of first element $= \Phi$

(ii) the set of last element $= \phi$

(iii) the set of minimal elements $= \{2,6\}$

(iv) the set of maximal element $= \{3,5\}$

Example 4
If $(S, \overset{\alpha}{\sim})$ is a poset, show that it may contain several maximal elements or none.

We shall solve this problem by giving suitable examples. Let $S = \{1,2,3,4\}$
$\overset{\alpha}{\sim} = \{(1,1),(2,2),(3,3),(4,4),(1,2),(1,3),(1,4)\}$
$\{\text{Maximal elements}\} = \{2,3,4\}$
Let $S = (0,1) = \{x \in R | 0 < x < 1)\}$ and let $\overset{\alpha}{\sim}$ be the relation $\leq$. Then

$$\{\text{Maximal elements}\} = \phi$$

Practice Exercise VI.1

1. Define a relation $\sim$ on Z, the set of all integers by $x \sim y$ means $m|x-y$, $m \in Z^+$.
   ($m|x-y$ means "m divides $x-y$"). Is $(Z,\sim)$ a poset?

2. Let $S = \{1, 2, 3, 4\}$ and let $\underline{\alpha} = \{(1,1), (2,2), (3,3), (4,4), (1,2), (1,3), (1,4)\}$ such that $(S, \underline{\alpha})$ is a partially ordered set.
   Find

   (i) the set of first elements of $(S, \underline{\alpha})$

   (ii) the set of least elements of $(S, \underline{\alpha})$

   (iii) the set of minimal elements of $(S, \underline{\alpha})$

   (iv) the set of maximal elements of $(S, \underline{\alpha})$

3. Let $\mathcal{S}$ denote the set of all electrical switching circuits and let $p\underline{\alpha}q$ mean $pq = p$. Show that $(\mathcal{S}, \underline{\alpha})$ is a partially ordered set.

Greatest lower bounds and Least upper bounds

Let S be a poset and T a subset of S. A *lower bound* on T is an element of S which precedes every element of T. The *greatest lower bound* of T is the lower bound which dominates every lower bound of T.

The greatest lower bound of T is also called the *infimum* of T and is written as

g.l.b. of T or inf(T).

An *upper bound* of a subset T of a poset S is defined as an element of S which dominates every element of T. The *least upper bound* or *supremum* of T is the upper bound which precedes every other upper bound of T. We write this as *l.u.b.* of T or sup(T).

Example 5

Let $(R, \leq)$ be a poset where R is the set of real numbers. Consider the open interval $(0, 1)$ as a subset of R. Find:

(i) the set of lower bounds of (0,1)

(ii) the set of greatest lower bounds of (0,1)

(iii) the set of upper bounds of (0,1), and

(iv) the set of least upper bounds of (0,1).

Solution

(i) Every real number $x \leq 0$ is a lower bound. Therefore the set of lower bounds is the interval $(-\infty, 0)$

(ii) The set of greatest lower bound $= \{0\}$

(iii) Every real number $y \geq 1$ is an upper bound. Hence the set of upper bounds is the interval $[1, \infty]$.

(iv) The set of least upper bounds $= \{1\}$

Example 6
Let S be a poset and let T be a subset of S. Show that if $\inf(T)$ exists in S, then it is unique.

Let $x = \inf(T)$. Then $x \overset{\alpha}{\sim} t$ for all $t \in T$ and if y is any lower bound, then $y \overset{\alpha}{\sim} x$. Now let x' be another $\inf(T)$. Then $x' \overset{\alpha}{\sim} t$ for all $t \in T$ and if y is any lower bound, then $y \overset{\alpha}{\sim} x'$. In particular $x = \inf(T)$ is a lower bound and so putting $y = x$, we have $x \overset{\alpha}{\sim} x'$.

Similarly, $x' = \inf(T)$ is a lower bound and so putting $y = x'$, we have $x' \overset{\alpha}{\sim} x$. Now $x \overset{\alpha}{\sim} x'$ and $x' \overset{\alpha}{\sim} x \Rightarrow x = x'$, by the antisymmetric law. Therefore, $\inf(T)$ is unique.

Totally-ordered and well-ordered sets
Let S be a poset. The elements $a, b \in S$ are said to be comparable if either $a \overset{\alpha}{\sim} b$ or $b \overset{\alpha}{\sim} a$. A set S is said to be totally *ordered* (or *simply ordered* or *linearly ordered* or *chain*) if it is a poset in which any two elements are comparable. A set is said to be *well-ordered* if

(i) S is totally ordered, and

(ii) every subset of S contains a first element.

Example 7
Show that $(N, \leq)$ is a totally ordered set.

Solution
For any $m, n \in N$, we have either $m \leq n$ or $n \leq m$.

Hence N is a totally ordered set.

Example 8
Show that a totally ordered set can have at most one maximal element which would then be a last element.

Solution
Let S be a totally ordered set. We shall show that

(i) if a maximal element exists, it is unique

(ii) there is an example where S has one maximal element, and

(iii) there is an example where S has no maximal element.

(i) If b, b' are maximal elements, then since S is totally ordered, every pair of elements are comparable, i.e.

$$b, b' \in S \Rightarrow \text{ either } b \overset{\alpha}{\sim} b' \text{ or } b' \overset{\alpha}{\sim} b.$$

Since b, b' are maximal elements, either of the cases above is possible only if $b = b'$. Hence if a maximal element exists, it is unique.

(ii) Let $S = \{1, 2, 3\}$
$\overset{\alpha}{\sim} = \{(1,1), (2,2), (3,3), (1,2), (1,3), (2,3)\}$
$(S, \overset{\alpha}{\sim})$ is a totally ordered set.
$\{\text{Maximal elements}\} = \{3\}, 3$ is also the last element.

(iii) Let $S = \{1, 2, 3\}$
$\overset{\alpha}{\sim} = \{(1,1), (2,2), (3,3), (2,1), (3,2), (1,3)\}$
$(S, \overset{\alpha}{\sim})$ is a totally ordered set.
$\{\text{Maximal elements}\} = \phi$

Example 9
Show that $(N, \leq)$ is a well-ordered set.
We have shown in Example 6 above that $(N, \leq)$ is a totally ordered set. Also every subset of N has a first element. Hence N is well-ordered.

Practice Exercise VI.2

1. Let $(R, \leq)$ be a poset where R is the set of real numbers. Consider the closed interval $[a, b]$ as a subset of R. Find for the subset $[a, b]$ the set of

   (i) lower bounds

   (ii) greatest lower bounds

   (iii) upper bounds

   (iv) least upper bounds.

2. Show that $(T, \leq)$ is a well-ordered set where

$$T = \{x \ \in R | x \geq 0\}$$

Summary
We first consider partially ordered sets (posets) which satisfy the reflexive, anti-symmetric and transitive laws. The following special elements of a poset are then studied

(i) least, greatest, minimal and maximal elements

(ii) lower bounds and upper bounds

(iii) greatest lower bounds (infimum, or inf) and least upper bounds (supremum or sup).

Finally we look at totally-ordered and well-ordered sets.

Post-Test
See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE SEVEN

Lattices and Boolean Algebras

Introduction
Objectives
The reader should be able to give the definition, examples and elementary properties of lattices and Boolean algebras.

Pre-Test

1. Show that $(\mathcal{P}, \overset{\alpha}{\sim}, v)$ is a Boolean algebra where $\mathcal{P}$ is the set of all propositions and p
   $stackrel\alpha\sim q$ means $p \vee q = q$.

2. Prove the following properties in a lattice

   (a) $a \wedge a = a$ (each element is idempotent)

   (b) $a \wedge b = b \wedge q$ and $a \vee b = b \vee a$ (commutative law)

   (c) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ and
   $a \vee (b \vee c) = (a \vee b) \vee c$ (associative law)

   (d) $(a \vee b) \wedge a = a$ and $(a \wedge b) \vee a = a$ (Absorption law).

3. Prove that
   $a \overset{\alpha}{\sim} b \Leftrightarrow a \vee b = b$ in a lattice

4. Complete the following operation tables in a Boolean algebra.

$\vee$	0	1	a	a'
0	0	1	a	a'
1	1			
a	a			
a'	a'			

$\wedge$	0	1	a	a'
0		0		
1	0	1	a	a'
a		a		
a'		a'		

5. Show that 1 is unique in a Boolean algebra.

6. Show that each element in a Boolean algebra has only one complement.

7. Prove in a Boolean algebra that
(i) $a'' = a$ (ii) $0' = 1$, (iii) $(a \vee b)' = a' \wedge b'$

8. Show that $a \overset{\alpha}{\sim} b$ implies $b' \overset{\alpha}{\sim} a'$ in a Boolean algebra.

9. Find the complements of the following in the Boolean algebra of sets where we put $\cup = +$ and $\cap = \cdot$
(a) $(P + Q)(P + R)$ (b) $AH' + AC + BC'$

10. Let S be a set in which two binary operations $\vee$ and $\wedge$ are defined, satisfying
(i) commutative law, (ii) associative law, (iii) idempotent law
(iv) absorption law.
Prove that S is a lattice, relative to a suitably defined order in S.
(**Hint:** Define $a \overset{\alpha}{\sim} b$ if $a \wedge b = a$ or $a \vee b = b$).

Definitions

1. A *lattice* is a system $(S, \overset{\alpha}{\sim}, \wedge, \vee)$ such that $(S, \overset{\alpha}{\sim})$ is a poset in which each pair of elements has a *g.l.b.* or inf denoted by $a \wedge b$ and a *l.u.b.* or sup denoted by $a \vee b$.

2. A lattice is said to be *distributive* if it has the following properties.
$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

3. A lattice is *complemented* if it contains distinct elements 0 and 1 such that $0 \overset{\alpha}{\sim} a \overset{\alpha}{\sim} 1$ for every element a in the lattice, and if each element a has a *complement* a' *with the property* that $a \wedge a' = 0$ and $a \vee a' = 1$.

4. A *Boolean algebra* is a complemented distributive lattice.

Example 1
Show that $(\mathcal{J}, \subseteq, \cup, \cap)$ is a Boolean algebra where $\mathcal{J}$ is the family of all sets in a universal set.

Partially ordered set:- We shall show first that $(\mathcal{J}, \subseteq)$ is a poset.

Reflexive law:- Since $A \subseteq A$ for all $A \epsilon \mathcal{J}$, it follows that $\subseteq$ is reflexive.

Anti-symmetric law: $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$. Thus $\subseteq$ is antisymmetric.

Transitive law:- $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$ therefore $\subseteq$ is transitive.

We shall show next that $A \cap B$ is the inf of A and B and that $A \cup B$ is the sup of A and B.

INF: Since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, it follows that $A \cap B$ is a lower bound of A and B. Also if C is a lower bound, i.e. $C \subseteq A$ and $C \subseteq B$, then we have that $C \subseteq A \cap B$. This implies that $A \cap B$ is g.l.b. of A and B.

SUP: Since $A \subseteq A \cup B$ and $B \subseteq A \cup B$, it follows that $A \cup B$ is an upper bound of A and B. Also if C is an upper bound, i.e. $A \subseteq C$ and $B \subseteq C$, then we have that $A \cup B \subseteq C$. This implies that $A \cup B$ is the l.u.b. of A and B.

Hence $(\mathcal{J}, \subseteq, \cap, \cup)$ is a lattice.

Distributive Law
Since $\cap$ is distributive over $\cup$ and $\cup$ is distributive over $\cap$, it follows that $(\mathcal{J}, \subseteq, \cap, \cup)$ is a distributive lattice.

Complement: The universal set μ and the empty set ϕ satisfy the property

that for any set $A \in \mathcal{J}$, $\phi \subseteq A \subseteq \mu$. Also for any $A \in \mathcal{J}$, we have its complement $A' \in \mathcal{J}$ such that $A \cap A' = \phi$ and $A \cup A' = \mu$. Hence $(\mathcal{J}, \subseteq, \cap, \cup)$ is complemented.

Therefore $(\mathcal{J}, \subseteq, \cap, \cup)$ is a complemented distributive lattice and so it is a Boolean algebra.

We can show that all the other properties satisfied by the Boolean algebra of sets are also satisfied by any Boolean algebra. We give some examples.

Example 2
Prove the following properties in a Boolean algebra $(S, \overset{\alpha}{\sim}, \wedge, \vee)$

(a) $a \vee a = a$ (Idempotent law)

(b) $(a \wedge b) \vee a = a$ (Absorption law)

(c) $a \overset{\alpha}{\sim} b \Rightarrow a \wedge b = a$

(d) $1' = 0$ (Property of complement)

(e) $(a \wedge b)' = a' \vee b'$ (De-Morgan's law)

Solution

(a) Since $(S, \overset{\alpha}{\sim})$ is a poset, it follows that $a \overset{\alpha}{\sim} a$ by the reflexive law. Then a is an upper bound for a and a. Now suppose that c is any upper bound for a and a, then $a \underline{\alpha} c$. Hence a is the least upper bound of a and a, i.e. $a \vee a = a$.

(b) We must show that a is the l.u.b. of $a \wedge b$ and a. Now since $a \wedge b$ is the g.l.b. of a and b, we have that $a \wedge b \overset{\alpha}{\sim} a$. Also by the reflexive law, $a \overset{\alpha}{\sim} a$. Hence a is an upper bound of $a \wedge b$ and a. Let c be any upper bound of $a \wedge b$ and a. Then

$$a \wedge b \overset{\alpha}{\sim} c \text{ and } a \overset{\alpha}{\sim} c$$

Since $a \overset{\alpha}{\sim} c$, it follows that a is the l.u.b. of $a \wedge b$ and a, i.e. $(a \wedge b) \vee a = a$.

(c) First show $a \overset{\alpha}{\sim} b \Rightarrow a \wedge b = a$. Since $a \wedge b$ is the inf of a and b, we have that $a \wedge b \overset{\alpha}{\sim} a$ and $a \wedge b \overset{\alpha}{\sim} b$.
By the reflexive law, $a \overset{\alpha}{\sim} a$. Therefore $a \overset{\alpha}{\sim} a$ and $a \overset{\alpha}{\sim} b$ (given) imply that a is a lower bound of a and b. Therefore $a \overset{\alpha}{\sim} a \wedge b$. Now

$$a \wedge b \overset{\alpha}{\sim} a \text{ and } a \overset{\alpha}{\sim} a \wedge b \Rightarrow a \wedge b = a$$

by antisymmetric law. Finally, we show

$$a \wedge b = a \Rightarrow a \overset{\alpha}{\sim} b.$$

Since a is given as the g.l.b. of a and b it follows that $a \overset{\alpha}{\sim} b$

(d) Any element x satisfying the conditions

$$x \wedge a = 0, \quad x \vee a = 1$$

is called the complement of a. Now consider $1 \wedge 0$, the g.l.b of 1 and 0, $1 \wedge 0 \overset{\alpha}{\sim} 0$. Also since $0 \overset{\alpha}{\sim} a$ for all a, if follows that $0 \overset{\alpha}{\sim} 1 \wedge 0$. Therefore, $1 \wedge 0 \overset{\alpha}{\sim} 0$ and $0 \overset{\alpha}{\sim} 1 \wedge 0$ imply $1 \wedge 0 = 0$, by the antisymmetric law.

Also consider $1 \vee 0$, the l.u.b of 1 and $0.1 \overset{\alpha}{\sim} 1 \vee 0$. Also since $a \overset{\alpha}{\sim} 1$ for all a, it follows that $1 \vee 0 \overset{\alpha}{\sim} 1$. Therefore

$$1 \overset{\alpha}{\sim} 1 \vee 0 \text{ and } 1 \vee 0 \overset{\alpha}{\sim} 1 \text{ imply that } 1 \vee 0 = 1$$

by the antisymmetric law.

Therefore, 0 is the complement of 1.

(e) To prove $(a \wedge b)' = a' \vee b'$, it is sufficient to prove

(i) $(a \wedge b) \wedge (a' \vee b') = 0$, and

(ii) $(a \wedge b) \vee (a' \vee b') = 1$

$$\begin{aligned} \text{(i) L.H.S.} &= [(a \wedge b) \wedge a'] \vee [(a \wedge b) \wedge b'] \quad \text{(distributive law)} \\ &= [(a' \wedge a) \wedge b] \wedge [a \wedge (b \wedge b')] \quad \text{(commutative and associative laws)} \end{aligned}$$

$$
\begin{aligned}
&= (0 \wedge b) \vee (a \wedge 0), \quad \text{(complement)} \\
&= 0 \vee 0 = 0 = \text{R.H.S.} \\
\text{(ii) L.H.S.} &= (a' \vee b') \vee (a \wedge b) \quad \text{(commutative law of } \vee) \\
&= [(a' \vee b') \vee a] \wedge [(a' \vee b') \vee b] \quad \text{(distributive law)} \\
&= [(a \vee a') \vee b'] \wedge [a' \vee (b' \vee b)] \quad \text{(commutative and associative laws)} \\
&= (1 \vee b') \wedge (a' \vee 1), \quad \text{(complement)} \\
&= 1 \wedge 1 = 1 = \text{R.H.S.}
\end{aligned}
$$

Example 3
Show that 0 is unique in a Boolean algebra. 0 satisfies the property

$$0 \overset{\alpha}{\sim} a \text{ for all } a \qquad (i)$$

Now let $0'$ be another element such that

$$0' \overset{\alpha}{\sim} a \text{ for all } a \qquad (ii)$$

Then if we put $a = 0'$ in (i), we have $0 \overset{\alpha}{\sim} 0'$ and if we put $a = 0$ in (ii), we have $0' \overset{\alpha}{\sim} 0$.
Now $0 \overset{\alpha}{\sim} 0'$ and $0' \overset{\alpha}{\sim} 0 \Rightarrow 0 = 0'$, by the antisymmetric law.
Hence 0 is unique.

Practice Exercise

1. Show that $(\zeta, \overset{\alpha}{\sim}, +, \cdot)$ is a Boolean algebra where ζ is the set of all switching circuits and $p \overset{\alpha}{\sim} q$ means $pq = p$.

2. Prove the following properties in a Boolean algebra
   (i) $p.1 = p$ (ii) $p + 0 = p$.

Summary
A partially ordered set in which the operations of infimum and supremum are defined is called a lattice. A Boolean algebra is then defined as a complemented distributive lattice. Properties of a Boolean algebra are then studied and we notice that he algebras of sets, propositions and electrical switching circuits are all examples of a Boolean algebra.

Post-Test Assignments
See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE EIGHT

Mappings

Introduction
We shall consider a class of special relations called mappings. The types of mappings to be considered include one-to-one, onto, bijective, inverse, identity, constant and similarity mappings. Other types are functions and composites of mappings.

Objectives
The reader should be able to define, identify and solve problems involving:

(i) injective, surjective and bijective mappings

(ii) identity and inverse mappings

(iii) functions and composites of mappings

(iv) similarity mappings

Pre-Test

1. Which of the following relations is a mapping?
   When f is a mapping, determine whether it is injective, surjective or bijective.
   When bijective, write down f^{-1}

(i) $X = \{5, 6, 8, 12\}$, $Y = \{a, b, c\}$
$f = \{(5, a), (6, b), (12, c)\}$

(ii) $X = \{a, b, c, d\}$, $Y = \{5, 7, 12, 10\}$
$f = \{(a, 7), (b, 12), (c, 10), (d, 5)\}$

(iii) $X = \{6, 4, 7, 11\}$, $Y = \{a, b, c\}$
$f = \{(6, a), (4, c), (7, b), (11, c)\}$

(iv) $X = Y = \{\text{real numbers}\}$
$f = \{(x, 3x + 5) | x \in X\}$

(v) $X = \{\text{integers}\}$, $Y = \{\text{positive integers}\}$
$f = \{(n, n^2) | n \in X\}$

(vi) $f = \{(x, y) \in R^2 | y = 24 - x^2\}$

2. Let $X = \{a, b, c\}$, $Y = \{d, e, f\}$. Find the number of mappings from X to Y. How many of these are bijections?

3. Show that a surjective mapping of a finite set to itself is bijective.

4. $S = \{a, b, c, d, e\}$. Define a mapping $f : S \to S$ as $f(a) = a$, $f(b) = c$, $f(c) = e$, $f(d) = d$, $f(e) = b$.

   (i) Give a complete description of f^2, f^3 and show that $f^2 = f^{-1}$

   (ii) Let g be another injective mapping on S defined by

   $$g(a) = d, \quad g(c) = \ c, \quad g(e) = e$$

   in which $g(b)$ and $g(d)$ are omitted.
   If $gof = gof$, find the values of $g(b)$ and $g(d)$.

5. Let $f : X \to Y$ and $g : Y \to Z$ be any two surjective mappings. Show that their composite $gof : X \to Z$ is also surjective.

6. Let $f : A \to B$ and $g : B \to C$ be any two mappings such that gof is surjective. Show that g must be surjective but that f need not be surjective. Illustrate your answer by an example.

7. Let $f : A \to B$ and $g : B \to C$ be any two mappings such that gof is bijective. Show that g need not be bijective. Show also that f need not be bijective. Illustrate your answers by examples.

8. Let $f : A \to B$ be a mapping such that $Y \subseteq B$. Show that

$$f[f^{-1}(Y)] \subseteq Y.$$

9. Consider the functions g_1, g_2 and g_3 defined from subsets of the set R of real numbers to R as follows:

$$\begin{aligned} g_1(x) &= \ln(x+1), \;\; x > -1, \;\; x \in R \\ g_2(x) &= \frac{1}{1+x^2}, \;\; x \in R \\ g_3(x) &= \frac{1}{\sqrt{(1-x^2)}}, \;\; -1 < x < 1, \;\; x \in R \end{aligned}$$

   (i) Determine the range for each function

   (ii) Determine the inverse function for each function, if it exists. Otherwise, find a subset of the domain so that g restricted to this subject, would have an inverse.

10. (a) Show that the relation of similarity between posets is an equivalence relation.
    (b) Show that a similarity mapping preserves
    (i) greatest elements, (ii) minimal elements.

Definitions:

1. A relation f is said to be *single-valued* if $(x, y) \in f$ and $(x, z) \in f$ imply $y = z$.

2. A *mapping* is a single-valued relation.
   Thus a mapping is a set of ordered pairs, no two distinct members of which have the same first coordinate.

3. Let f be a mapping with X as its domain and with its range contained in Y. Let $x \in X$, then there is a unique $y \in Y$ such that $(x, y) \in f$. Denote this unique element by $f(x)$ and call it the *image of* x *under* f. We also say that f is a mapping on X into Y and write it as $f : X \to Y$, so that $x_1 = x_2$ implies $f(x_1) = f(x_2)$.

4. Let $f : X \to Y$ be a mapping. Y is called the *codomain* of f, and the range of f i.e. $\{f(x)|x \in X\}$ is also called the *image of* X *under* f. We write $f(X)$ for the range of f.

5. Let $f : X \to Y$ be a mapping such that the codomain Y is a set of numbers then f is called a *function*.

6. A way of representing a mapping is to use a *mapping diagram* or an *arrowgraph*. For example consider the mapping

$$f : \{a, b, c\} \to \{q, r, s, t\}$$

where $f(a) = r$, $f(b) = s$ and $f(c) = r$. Then a mapping diagram or an arrowgraph representing the mapping is shown in Fig. 8.1.

Fig. 8.1: A mapping diagram or an arrow graph.

Example 1
Is f a mapping? If it is, find the range.

(i) $X = \{x, y, z\}$, $Y = \{2, 3, 5, 7\}$ and
$f = \{(x, 2), (y, 5), (z, 3)\}$

(ii) $A = \{1, 2\}$, $B = \{a, b, c, d, e\}$, and
$g = \{(1, a), (2, c), (1, e)\}$

Solution

(i) f is a mapping since no two distinct members of f have the same first coordinate.
Range of $f = \{2, 3, 5\}$.

(ii) g is not a mapping since 1 has two images a and e in Y.

Example 2
If $f : R \to R$ is a function, defined by $f : x \to 3x^2 - 2$

(i) find the image of the point -3 under the function f

(ii) determine the value of f at the point 2 under the function f; and

(iii) evaluate $f(0)$, $f(-1)$ and $f(4)$

(i) $f(-3) = 3(-3)^2 - 2 = 25$

(ii) $f(2) = 3(2^2) - 2) = 10$

(iii) $f(0) = -2$
$f(-1) = 3(-1)^2 - 2 = 1$
$f(4) = 3(4^2) - 2 = 46$

Practice Exercise VIII.1
Is the relation a mapping? If it is, state the domain, codomain and range.

1. $\{(p, 1), (q, 1), (r, 2), (s, 3), (t, 3)\}$
2. $\{(1, a), (1, b), (2, b), (3, c), (4, c)\}$
3. $\{(1, 3), (2, 3), (3, 3), (4, 3)\}$
4. $\{(4, 1), (4, 2), (4, 3)\}$
5. $\{(x, y)|x + y = 5\}$

6. $\{(x, y)|x^2 + y^2 = 1\}$

7. $\{(x, y)|y = 6\}$

8. Find the image of the mapping

$$f : R \times R \to R \times R$$

described by the rule

(i) $(x, y) \to (x + 2y, -y)$ at the point $(4, 2)$

(ii) $(x, y) \to (3x - y, y - x^2)$ at the point $(-2, 5)$

9. Find the range by considering the graph of the function $f : R \to R$ defined by the rule

(i) $f : x \to 3x + 7$

(ii) $f : x \to x^2 + 6$

(iii) $f : x \to (x + 3)(2 - x)$

Note: If f is a function from R to R (R = set of all real numbers), f can be considered as a subset of the plane $R \times R$ and can be represented by its graph on the plane. The x-axis represents the domain while the y-axis represents the codomain of the function. By drawing the graph of the function, we are able to determine the range which is the part of the y-axis that the graph occupies.

10. Which diagram in Fig. 8.2 represents a mapping?
If it is a mapping, state

(a) the domain

(b) the codomain

(c) the images

(d) the range.

(i) (ii)

(iii) (iv)

Fig. 8.2

One-to-one and Onto mappings
A mapping $f : X \to Y$ is said to be *one-to-one or injective or mono* if $f(x_1) = f(x_2)$ in Y implies $x_1 = x_2$ in X.
In other words,

(i) No two distinct members of the domain X have the same image in Y.

(ii) Different elements in the domain X have different images in Y.

(iii) $x_1 \neq x_2$ in X implies $f(x_1) \neq f(x_2)$ in Y.

(iv) If $f : R \to R$ is a function, then any straight line drawn on the graph of the function parallel to the x-axis intersects the curve in not more than one point.

A mapping $f : X \to Y$ is said to be *onto* or *surjective* or *epi* if the range of f is equal to its codomain Y. In other words,

(i) $f(X) = Y$

(ii) Every element in the codomain Y is the image of at least one element in the domain X.

(iii) Given any $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

(iv) If $f : R \to R$ is any function, then the graph of the function occupies the whole of the y-axis i.e. any straight line drawn on the graph parallel to the x-axis intersects the curve in at least one point.

A mapping $f : X \to Y$ is said to be *bijective* (or a bijection) if it is injective and surjective. A bijection between X and Y is called also a one-to-one correspondence between X and Y.

Example 3
Is the mapping one-to-one and onto?

(a) $f : R \to R$, $f : x \mapsto x^2$

(b) $g : R \to R^+ \cup \{0\}$, $g : x \mapsto x^2$

(c) $h : R^+ \to R^+$, $h : x \mapsto x^2$

(a) It is possible to use any of the following three methods.

(i) *By inspection:* Since for example $(-3)^2 = 3^2 = 9$ it follows that f is not one-to-one. Also since the square of a real number is not negative, it follows that the range $f(R)$ is a proper subset of the codomain R. Therefore f is not onto.

(ii) *Analytic method:* Solve the equation $f(x_1) = f(x_2)$ for x_1, x_2, $x_1^2 = x_2^2$ and so $x_1 = \pm x_2$. This shows that x_1 and $-x_1$ have the same image and so f is not one-to-one.

Also given $y \in R$, the equation $f(x) = y$ i.e., $x^2 = y$ does not have a solution if y is negative as $x = \sqrt{y}$ will not be a real number. Therefore f is not onto.

(iii) *Graphical method:* Sketch the graph as shown in Fig. 8.3

Graph of $f(x) = x^2$
Fig. 8.3

Graph of $h(x) = x^2$
Fig 8.4

(a) From the graph, some lines drawn parallel to the x-axis intersects the curve in two points. This shows that the function f is not one-to-one.

From the graph also, observe that the curve does not occupy the whole of the y-axis and some lines drawn parallel to the x-axis do not intersect the curve at all. Hence f is not onto.

(b) Using any method, we conclude that g is not one-to-one.
However, the codomain does not include the negative real numbers, which are represented by the negative y-axis in Fig. 8.3. In this case every straight line drawn parallel to the x-axis intersects the curve in at least one point. Therefore, g is onto.

(c) The function has the graph drawn in Fig. 8.4. Note that the domain and codomain consists of positive real numbers only. Since every line drawn parallel to the x-axis intersects the curve in not more than one point, it follows that h is one-to-one.

Also since every line drawn parallel to the x-axis intersects the curve in at least one point, it follows that h is onto.

Remark: Example 3 shows that the domain and codomain are very important in determining whether a mapping is one-to-one or onto.

Example 4
Let $g : R \to R$ be a mapping, where R is the set of real numbers, defined by

$$g(x) = 5x + 7$$

is g bijective?

If $g(x) = g(y)$, then $5x + 7 = 5y + 7$ which implies that $x = y$. Hence g is injective. Also for any $y \in R$, solve $y = 5x + 7$ for x and obtain

$$x = \frac{y - 7}{5} \in R$$

such that

$$g(x) = \frac{x - 7}{5}$$

Hence g is surjective and so g is bijective. Note that the graphical method can also be used.

Example 5
Show that an injective mapping of a finite set to itself is bijective. Let $f : S \to S$ be an injective mapping, where $S = \{a_1, \ldots, a_n\}$. We must show that f is surjective. We shall employ the method of proof by contradiction. Suppose f is not surjective, it follows that the range $f(S)$ is a proper subset of S. Now it is not possible to map S injectively onto $f(S)$, so it must be that f is surjective.

Identity mappings
An identity mapping is a mapping $f : A \to A$ where the domain is the same set as the codomain which assigns every element of set A onto itself i.e. $f(x) = x$ for every $x \in A$. An identity mapping on a set A is sometimes denoted by 1_A.

Example 6
Determine whether an identity mapping $f : A \to A$ is one-to-one or onto. The mapping is $f(x) = x$ for every $x \in A$. To test whether f is one-to-one, we solve the equation $f(x_1) = f(x_2)$ for x_1, x_2. The equation becomes $x_1 = x_2$. Therefore an identity mapping is one-to-one.

To test whether f is onto, given a in the codomain A, we solve the equation $f(x) = a$ for x. The equation becomes $x = a$. Since a solution exists, we conclude that an identity mapping is onto.

Example 7
Let a, b, c, d be real numbers such that $ad - bc \neq 0$.
Let

$$f : R - \left\{\frac{-d}{c}\right\} \to R - \left\{\frac{a}{c}\right\}$$

be the function defined by

$$f(x) = \frac{ax + b}{cx + d}$$

Is f injective or surjective?

$$y = \frac{ax + b}{cx + d} \Rightarrow x = \frac{b - dy}{cy - a}$$

$$f(x) = \frac{a}{c} - \frac{ad - bc}{c(cx + d)}, \quad x = -\frac{d}{c} - \frac{ad - bc}{c(cy - a)}$$

Hence, the asymptotes of $f(x)$ are

$$f(x) = \frac{a}{c} \text{ and } x = -\frac{d}{c}$$

$f(x)$ cuts the x-axis when $x = -\dfrac{b}{a}$
$f(x)$ cuts the $f(x)$-axis when $f(x) = \dfrac{b}{d}$
The graph of $f(x)$ is shown in Fig. 8.5, depending on whether $ad > bc$ or $ad < bc$

.

Fig. 8.5

From Fig. 8.5, since any vertical or horizontal line cuts the graph in exactly one point, it follows that f is a bijection.

Practice Exercise VIII.2
Determine whether the mapping is
(i) one-to-one (ii) onto

1. $f = \{(p,1),(q,1),(r,2),(s,3),(t,3)\}$ where
   Domain $= \{p,q,r,s,t\}$ ad codomain $= \{1,2,3\}$.
2. $f : R \to R$, $f : x \mapsto \sin x$.
3. $g : R \to R$, $g : x \mapsto 3x + 7$
4. $h : R \to R$, $h : x \mapsto (x-1)(x-2)$
5. $f : R \to [-1,+1]$, $f : x \mapsto \cos x$

Inverse and Composition of Mappings

If $f : X \to Y$ is a mapping, then we can consider its inverse f^{-1} as a relation

$$f^{-1} = \{(f(x), x) | x \in X\}$$

The domain of f^{-1} is the range of f. If f^{-1} is a single-valued relation then f^{-1} becomes a mapping and is called the *inverse mapping* of f.

Let X, Y and Z be any non-empty sets such that $f : X \to Y$ and $g : Y \to Z$ are mappings. Then because the codomain of f is equal to the domain of g, we define the *product* or *composition* of the mappings f and g as a mapping denoted y gof and described by the rule

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

i.e. $gof : X \to Z, \quad gof(x) = g[f(x)]$.

The process of describing the rule of gof explains why the composition of f and g is denoted by gof in the reverse order.

Example 8

Let $f : X \to Y$ and $g : Y \to Z$ be any two mappings. Show that gof is also a mapping.

As relations, the composite gof of relations f and g is a relation. We have to show that gof is a single valued relation. Let

$$(x, z_1) \in gof \text{ and } (z, z_2) \in gof$$

We have to show that $z_1 = z_2$. Now there exists y_1, y_2 such that

$$(x, y_1) \in f \text{ and } (y_1, z_1) \in g$$

$$(x, y_2) \in f \text{ and } (y_2, z_z) \in g$$

Since f is a mapping (and so a single-valued relation), it follows that $(x, y_1) \in f$ and $(x, y_2) \in f \Rightarrow y_1 = y_2 = y$, say.
Therefore, also since g is a mapping,

$$(y, z_1) \in g \text{ and } (y, z_2) \in g \Rightarrow z_1 = z_2$$

Hence gof is a mapping.

Example 9
Let $f : X \to Y$ and $g : Y \to Z$ be any two injective mappings. Show that gof is also injective.
Let $gof(x_1) = gof(x_2)$ in Z; we must show that $x_1 = x_2$. Since g is injective, then

$$g[f(x_1)] = g[f(x_2)] \Rightarrow f(x_1) = f(x_2)$$

Since f is injective, then

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Therefore gof is injective.

Example 10
Let $f : X \to Y$ and $g : Y \to Z$ be two mappings such that gof is injective. Show that f must be injective but that g need not be injective. Illustrate your answer by an example.

Let $f(x_1) = f(x_2)$. To show that f is injective, one must show that $x_1 = x_2$.

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow g[f(x_1)] = g[f(x_2)] \\ &\Rightarrow gof(x_1) = gof(x_2) \end{aligned}$$

Since gof is injective, then $x_1 = x_2$. Hence f is injective.

Consider the following example in Fig. 8.6

.

Fig. 8.6

where

$$\begin{aligned} gof &= \{(a,3),(b,4),(c,1)\} \text{ is injective} \\ f &= \{(a,z),(b,w),(c,x)\} \text{ is injective; but} \\ g &= \{(x,1),(y,1),(z,3),(w,4)\} \text{ is not injective.} \end{aligned}$$

Example 11
Let $f : X \to Y$ be a mapping such that $A \subseteq X$. Show that $f^{-1}[f(A)] \supseteq A$.
Let $a \in A$, we shall show that $a \in f^{-1}[f(A)]$
$a \in A \Rightarrow f(a) \in f(A)$ i.e. $(a, f(a)) \in f$
$\Rightarrow a \in f^{-1}[f(A)] \Rightarrow A \subseteq f^{-1}[f(A)]$.

Practice Exercise VIII.3

1. Find the rules for the mappings
   (a) $f^2 = fof$ (b) $g^2 = gog$
   (c) fog (d) gof
   (e) f^{-1}
   if $f : R \to R$, $f : x \mapsto 3x - 2$
   $g : R \to R$, $g : x \mapsto x^2 - 4x + 1$
   (f) check whether fog and gof are equal or not.

2. Solve the equation $fog(x) = gof(x)$ for values of x where the composites fog and gof coincide.

$$f : x \mapsto x^2 + 2 \qquad g : x \mapsto \sqrt{(3x - 4)}$$

Similar sets and Similarity mappings

Two posets S and T are said to be *similar* if there exists a bijective mapping α from S to T such that a precedes b in S if and only if $\alpha(a)$ precedes $\alpha(b)$ in T. The bijective mapping α is called a similarity mapping from S to T.

Example 12

Show that a similarity mapping preserves maximal elements.

Let $\alpha : S \to T$ be a similarity mapping. Suppose s_0 is a maximal elements of S. We must show that $\alpha(S_0)$ is a maximal element of T. Suppose there exists an element $t \in T$ such that $\alpha(s_0) \overset{\alpha}{\sim} t$. Since α is a bijective mapping, there exists $s \in S$ such that $\alpha(s) = t$. Hence $\alpha(s_0) \underline{\alpha} \alpha(s)$ which implies that $s_0 \circ s$ since α is a similarity mapping. Now $s_0 \overset{\alpha}{\sim} s \Rightarrow s_0 = s$ since s_0 is a maximal element of S. Thus $\alpha(s_0) = \alpha(s) = t$ i.e. $\alpha(s_0)$ is a maximal element of T.

Practice Exercise VIII.3

1. Let B be a subset of a well ordered set A. Suppose $f : A \to B$ is a similarity mapping from A to B. Show that for all $a \in A$, a precedes $f(a)$.

2. Show that a similarity mapping preserves least elements.

Summary

A mapping is defined as a single-valued relation. The domain, codomain, range and mapping diagram or arrow graph are considered. Special mappings are studied such as

(i) functions and their graphical representation
(ii) one-to-one or injective or mono mappings
(iii) onto or surjective or epi mappings
(iv) one-to-one and onto or bijective mappings
(v) identity and constant mappings
(vi) inverses and composition of mappings
(vii) similar sets and similarity mappings

Post-Test

See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE NINE

Groups

Introduction
We shall study certain algebraic structures called groups, as a generalization of familiar sets of numbers with respect to the binary operations of addition and multiplication. We shall consider their simple properties and give examples which will include the symmetric and cyclic groups. We shall also see when a subset of a group is also a group, called a subgroup of the original group with the same binary operation. We shall then conclude by studying homomorphisms of groups which are mappings between groups which preserve the binary operations of the groups.

Objectives
The reader should be able to

(i) prove elementary properties of groups

(ii) show whether a set together with a given binary operation forms a group

(iii) give different examples of a group

(iv) determine subgroups of given groups, and

(v) prove simple properties of homomorphisms of groups.

Pre-Test

1. Let a, b, c be elements of a group $(G, *)$. Show that $b * a = c * a$ implies that $b = c$ (i.e. right cancellation law holds).

2. Show that the inverse of an element of a group $(G, *)$ is unique.

3. Prove that a group $(G, \cdot)$ is Abelian if and only if $(ab)^2 = a^2b^2$ for all a, b in G.

4. If a group $(G, *)$ has $2n$ elements, show that there exists at least one other element x apart from the identity e which satisfies $x * x = e$.

5. (a) Prove that the set of integers modulo 12 that are relatively prime to 12 is a group under multiplication modulo 12.

   (b) Show that the set $\{2, 4, 6, 8\}$ is a group under multiplication modulo 10.

6. (a) If the order of a group G is n, show that $a^n = e$ for all $a \in G$, where e is the identity of G.

   (b) Show that every group of prime order is cyclic. Find all its generators.

7. Show that the following permutations form a cyclic group:
   (1), (1234), (13),(24), (1432).

8. (a) Let H be a non-empty set of a group G. Show that H is a subgroup of G if and only if whenever $a, b \in H$, $ab^{-1} \in H$.

   (b) Show that any subgroup of a cyclic group is cyclic.

9. Show that all the proper subgroups of X_3 are Abelian and cyclic but that S_3 is not Abelian.

10. (a) Let $\alpha : G \to H$ and $\beta : H \to K$ be homomorphisms of groups. Show that $\beta \circ \alpha$ is also a homomorphism.

(b) If $f : G \to H$ is a homomorphism of groups, prove that

(i) the kernel of f is a subgroup of G and that f is a monomorphism if and only if the kernel of f consists of the identity element of G alone.

(ii) if U is a subgroup of G, then $f(U)$ is a subgroup of H, and

(iii) if V is a subgroup of H, then $f^{-1}(V)$ is a subgroup of G.

Semi-groups and Groups
Definition
Let G be a set together with a binary operation $*$:

1. If G is closed with respect to $*$, then $(G, *)$ is called a *groupoid*.
2. A groupoid $(G, *)$ which is associative is called a *semi-group*.
3. A semigroup $(G, *)$ containing an identity element e is called a *monoid*.
4. A monoid $(G, *)$ in which every element has an inverse is called a *group*.

In other words, a group is a set G together with a binary operation $*$ which satisfies the following 4 conditions.

(i) closure, i.e. $a, b \in G \Rightarrow a * b \in G$;

(ii) Associativity, i.e. $a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$.

(iii) Identity law, i.e. there exists $e \in G$ such that for all $a \in G$, $e * a = a * e = a$, and

(iv) Inverse law, i.e. $a \in G$ there exists $b \in G$ such that $a*b = b*a = e$.

5. A group $(G, *)$ with a commutative binary operation is called an *Abelian* or a *commutative* group.

Proposition I
Let a and b be any two elements of a group $(G, *)$.
Show that (i) $(a * b)^{-1} = b^{-1} * a^{-1}$ (ii) $(a^{-1})^{-1} = a$.

Proof

$$\begin{aligned}
\text{(i) } (b^{-1} * a^{-1} * (a * b) &= b^{-1} * [a^{-1} * (a * b)] \text{ (associativity)} \\
&= b^{-1}(*[(a^{-1} * a) * b] \text{ (associativity)} \\
&= b^{-1} * (e * b) \text{ (inverse law)} \\
&= b^{-1} * b \text{ (identity law)} \\
&= e \text{ (inverse law)}
\end{aligned}$$

where e is the identity element of G. Similarly, $(a * b) * (b^{-1} * a^{-1}) = e$. Therefore $b^{-1} * a^{-1}$ is the inverse of $a * b$.

Note: $(a * b)^{-1}$ is not $a^{-1} * b^{-1}$ but $b^{-1} * a^{-1}$.

(ii) $a * a^{-1} = e = a^{-1} * a$ (inverse law)
$\Rightarrow (a^{-1})^{-1} = a$

Proposition 2
Let a, b, c be elements of a group $(G, *)$.
Show that $a * b = a * c$ implies that $b = c$ (i.e. left cancellation law holds).

Proof

$$a * b = a * c$$

Pre-multiply by a^{-1}

$$\begin{aligned}
&a^{-1} * (a * b) = a^{-1} * (a * c) \\
&(a^{-1} * a) * b = (a^{-1} * a) * c \quad \text{(associativity)} \\
&e^{*}b + e * c \quad \text{(inverse law)} \\
&b = c \quad \text{(identity law)}
\end{aligned}$$

Proposition 3
Show that the identity e in a group $(G, *)$ is unique..

Proof
Let e' be another identity element. Then

$a * e = e * a = a$ for all $a \in G$ (1)
$a * e' = e' * a = a$ for all $a \in G$ (2)
Put $a = e'$ in (1) and we have

$$e' * e = e * e' = e' \tag{3}$$

Put $a = e$ in (2) and we have

$$e * e' = e' * e = e \tag{4}$$

(3) and (4) imply that $e = e'$.

Practice Exercise IX.1

1. Let E be any set and let $\cdot$ be a binary operation on E defined by $x \cdot y = x$. Show that $(E, \cdot)$ is a semigroup.

2. Prove that a group $(G, *)$ is Abelian if and only if $(a * b)^{-1} = a^{-1} * b^{-1}$.

3. Let $(G, \cdot)$ be a group with identity element e.
   Let a, b, c and x be members of G.

   (a) If $a.x.b = c$, find x in terms of a, b, c.

   (b) If $ax^2 = b$ and $x^3 = e$, find x in terms of a, b.

4. Let G be a group, 1 the identity of G and $a, b, c, d \in G$ such that

   $$abc = 1 = bcd$$

   Show that $a = d$.

5. Let G be a group and $x, y \in G$ such that

   $$x^2 = y^6 = 1,\ yx = xy^3$$

   Show that $y^2 = 1$ and $xy = yx$.

6. Suppose G is a group, $g, h \in G$ such that $g^3 = h^5 = 1$ and $hg = gh^2$.
   Show that $h = 1$.

Examples of Groups

Example 1:

From our consideration of binary operations in Lecture 2, it is easy to check that

(i) $(N, +)$ is a commutative semigroup

(ii) $(Z, +), (Q, +), (R, +), (Z_{\text{ev}}, +), (mZ, +), (Z_m, +)$ are all Abelian groups.

(iii) $(N, \times)$ and $(Z, \times)$ are commutative monoids and not groups

(iv) $(Q^*, \times)$ and $(R^*, \times)$ are groups.

(v) $(\mathcal{J}, \cup)$ and $(\mathcal{J}, \cap)$ are commutative monoids

(vi) $\{f \in R[x] | f(x) = ax + b, a \neq 0\}$ is a group under composition.

(vii) $(Z, *)$ where $a * b = a + b - ab$, is a commutative monoid.

Example 2:

Verify that the subset $S = \{1, 3, 9, 11\}$ of Z_{16} under multiplication modulo 16 (i.e. $a \otimes b$ is the remainder when xy (ordinary multiplication) is divided by 16) forms a group. [Assume Associativity].

Obtain the operation table of $(S, \otimes)$.

$\otimes$	1	3	9	11
1	1	3	9	11
3	3	9	11	1
9	9	11	1	3
11	11	1	3	9

From the operation table, we find that

(i) the closure property is satisfied

(ii) 1 is the identity element

(iii) $1^{-1} = 1$, $3^{-1} = 11$, $9^{-1} = 9$, $11^{-1} = 3$ (inverse law)

Hence, assuming associativity, we conclude that $(S, \otimes)$ is a group.

Example 3:
Let $(G, *)$ be a group such that every element is its own inverse. Show that G must be Abelian

$$g * g = e \text{ for all } g \in G$$

Let a and b be any two elements of G. The

$$(a * b) * (a * b) = e, \quad (a * b \in G)$$

Premultiply by $b * a$:

$$(b * a) * (a * b) * (a * b) = b * a \qquad \text{(identity law)}$$

By a repeated use of associativity, we have

$$\begin{aligned} b * (a * a) * b * (a * b) &= b * a \\ b * e * b * (a * b) &= b * a \\ (b * b) * (a * b) &= b * a \quad \text{(identity law)} \\ e * (a * b) &= b * a \\ a * b &= b * a \quad \text{(identity law)} \end{aligned}$$

Hence $(G, *)$ is Abelian.

Example 4 **(The Symmetric group)**
A *permutation* on a set T is defined as a bijective mapping from T to itself. From the consideration of mappings in Lecture 8 it is easy to conclude that the set of all permutations on T is a group under composition, called the symmetric group on T or the group of transformations of T and is denoted by S_T. If T is a finite set such that $o(T) = n$, (i.e. the order of T or the number of elements in the set T is n), we denote S_T by S_n and call S_n the symmetric group of degree n or the symmetric group on n letters.

Notation
We may regard an element of S_n as a permutation of the integers $\{1, 2, \ldots, n\}$. Thus, if $\alpha \in S_n$, we may write α as

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix}$$

Note that

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

is the identity element is S_n and the inverse of

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \\ \alpha(1) & \alpha(2) & \alpha(3) & & \alpha(n) \end{pmatrix}$$

is

$$\begin{pmatrix} \alpha(1) & \alpha(2) & \alpha(3) & & \alpha(n) \\ \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

If

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

then $\alpha \circ \beta$ may be easily computed as

$$\alpha \circ \beta = \begin{pmatrix} 3 & 5 & 4 & 2 & 1 \\ \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

by writing the first row of α in the order of the second row of β. Note that since

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \\ 2 & 5 & 1 & 4 & 5 \end{pmatrix}$$

it follows that $\alpha \circ \beta \neq \beta \circ \alpha$ and so S_n is a non-Abelian group.

Let $\{a_1, a_2, \ldots, a_m\} \subseteq \{1, 2, \ldots, n\}$ such that if $\alpha \in S_n$, then $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3, \ldots, \alpha(a_{m-1}) = a_m$, $\alpha(a_m) = a_1$ and $\alpha(j) = j$ if $j \notin \{a_1, \ldots, a_m\}$. Then α is called a cyclic permutation of length m and is written as $(a_1, a_2, \ldots, a_m)$. A transposition in S_n is the permutation which interchanges the numbers i and j and leaves the other elements fixed, i.e. a transposition is a cyclic permutation of order 2. For example (356) is a cycle of length 3 while (24) is a transposition.

Example 5 **(Cyclic groups)**
Let a be an element of a group G. Then we denote by $\langle a \rangle$, the set of all powers of a and their inverses, i.e. $\langle a \rangle = \{a^n : n \in Z\}$ if the operation is multiplication, or $\langle a \rangle = \{na | n \in Z)$ if the operation is addition. *A* group G is said to be a cyclic group if

$$G = \langle a \rangle \text{ for some element } a \in G.$$

For example, $(Z, +)$ is a cyclic group generated by the element 1, i.e.

$$(Z, +) = (\langle 1 \rangle, +)$$

Practice Exercise IX.2

1. Verify that the subset $S = \{1, 3, 5, 7\}$ of Z_8 under multiplication modulo 8 forms a group. (Assume associativity).

2. Test whether the following is a group:
   $(Z, *)$ where $a * b = a + b + ab$.

3. Show that there are six rotations which bring an equilateral triangle into coincidence with itself. Verify that these rotations form a group.

4. Show that an Abelian group consisting of 10 elements is cyclic.

Subgroups
A subset H of a group G is called a subgroup of G if H is also a group under the same binary operation as that in G. When H is a subgroup of G, we write $H \leq G$.

It is easy to see that:

(i) Every subgroup of an Abelian group is Abelian

(ii) $H = G$ and $H = \{e\}$, where e is the identity in G are both subgroups of G called the *trivial* subgroups of G.

If H is a subgroup of G such that $H \neq G$ and $H \neq \{e\}$, then H is called a *proper* subgroup of G.

One way of showing whether a subset H of a group G is a subgroup is the following. It can be shown that H is a subgroup of $(G, +)$ if and only if for every $x, y \in H$, $x - y \in H$; and H is a subgroup of $(G, \cdot)$ if and only if for every $x, y \in H$, $xy^{-1} \in H$.

A way of determining subgroups of *finite* groups is due to Lagrange in a theorem which we state without proof.

THEOREM **(Lagrange):** If H is a subgroup of a finite group G, then the order of H divides the order of G.

Example 6
If $(G, \cdot)$ is a group, show that for any $a \in G$, $\langle a \rangle$ is a subgroup of G.

$$\langle a \rangle = \{a^n | n \in Z)$$

Let $x, y \in \langle a \rangle$. We shall show that $xy^{-1} \in \langle a \rangle$. Now $x, y \in \langle a \rangle$ imply that

$$x = a^n,\ n \in \mathbb{Z} \ \text{ and } \ y = a^m,\ m \in \mathbb{Z}$$

$\Rightarrow \ xy^{-1} = a^{n-m}$. Since $n, m \in \mathbb{Z}$, then $n - m \in \mathbb{Z}$. Therefore $xy^{-1} = a^{n-m} \in \langle a \rangle$. Hence $\langle a \rangle$ is a subgroup of G.

Example 7:
Determine all the subgroups of $(\mathbb{Z}_6, +)$.
By the theorem of Lagrange, the possible subgroups of $\mathbb{Z}_6$ must be of orders 1, 2, 3 or 6. The subgroups of orders 1 and 6 are the trivial subgroups namely.

$$\{0\} \ \text{ and } \ \mathbb{Z}_6$$

Subgroups of order 2
Since the identity must be a member of any subgroup, it follows that a

subgroup of order 2 will be of the form

$$\{0, a\} \text{ for some } a \in \mathbb{Z}_6 - \{0\}$$

Now since the subgroup must be closed, it follows that the only subgroup of order 2 is $\{0, 3\}$.

Subgroups of order 3
A subgroup of order 3 is of the form

$$\{o, a, b\} \text{ for some } a, b \in \mathbb{Z}_6 - \{0\}$$

Now since the subgroup must be closed, it follows that the only subgroup of order 3 is $\{0, 2, 4\}$.
Hence all the subgroups of $(\mathbb{Z}_6, +)$ are

$$\{0\},\ \mathbb{Z}_6,\ \{0, 3\},\ \{0, 2, 4\}$$

Practice Exercise IX.3

1. Find all the subgroups of $S = \{1, 3, 5, 7\}$ under multiplication modulo 8.

2. Determine all the subgroups of $S = \{1, i, -1, -i\}$ where $i^2 = -1$ under ordinary multiplication of complex numbers.

3. Find all the subgroups of the commutative group consisting of10 elements.

4. If H is a subgroup of $(\mathbb{Z}, +)$ show that $H = d\mathbb{Z}$, with $d \geq 0$ and $d \in \mathbb{Z}$.

5. If $G = \langle a, b | a^2 = b^3 = 1, ab = b^2a \rangle$, find all subgroups of G.

6. Let $H \leq G$. Define a relation $\sim$ in G by $a \sim b \Rightarrow ab^{-1} \in H$. Show that $\sim$ is an equivalence relation.

Homomorphisms

Let $(S, *)$ and $(T, \cdot)$ be two sets on which we have binary operations defined. These sets can, therefore, be groupoids, semigroups, monoids or groups. A mapping

$$f : (S, *) \rightarrow (T, \cdot)$$

is called a homomorphism if

$$f(a * b) = f(a) \cdot f(b) \text{ for all } a, b \in S.$$

A homomorphism is called a *monomorphism* if f is injective and is called an *epimorphism*, if f is surjecive. The mapping f is called an *isomorphism* if f is both a monomorphism and an epimorphism, i.e. an isomorphism is a bijective homomorphism.

Let $f : G \rightarrow H$ be a homomorphism from group G to group H. Then the *kernel* of f is a subset of G defined as

$$Ker(f) = \{x \in G | f(x) = e_H\}$$

where e_H is the identity of H.

A homorphism $f : G \rightarrow G$ which maps a group G to itself is called an *endomorpism* while a bijective endomorphism is called an *automorphism*.

Example 8

Let $f : (R, +) \rightarrow (R^*, \cdot)$ be defined by $f(x) = e^x$ for all $x \in R$. Show that f is a monomorphism but not an isomorphism.

To show that f is a homomorphism, we must show that $f(x + y) = f(x) \cdot f(y)$. Now

$$f(x + y) = e^{x+y} = x^x \cdot e^y = f(x) \cdot f(y)$$

Hence f is a homomorphism.

To show that f is injective, one must show that $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

Now,

$$f(x_1) = f(x_2) \quad \Rightarrow \quad e^{x_1} = e^{x_2}$$

$$\Rightarrow \quad e^{x_1 - x_2} = 1$$
$$\Rightarrow \quad x_1 - x_2 = 0$$
$$\Rightarrow \quad x_1 = x_2$$

Hence f is injective and so f is a monomorphism.

To show that f is not an isomorphism, we note that there does not exist any $x \in R$ such that $e^x < 0$. Therefore f is not surjective and so f is not an isomorphism.

it Example 9

Let f be a homomorphism from a group G to a group H such that e_G and e_H are the identity elements of G and H, respectively. Show that

(i) $f(e_G) = e_H$, i.e. f maps identity to identity

(ii) $f(x^{-1}) = [f(x)]^{-1}$ i.e. f maps inverses to inverses.

(iii) G and H have the same cardinal number if f is bijective.

(i) Since $e_G^2 = e_G$, we have
$f(e_G^2) = f(e_G)$
$\Rightarrow \ f(e_G) \cdot f(e_G) = f(e_G)$, (homomorphism)
$\Rightarrow \ f(e_G) \cdot f(e_G) = e_H \cdot f(e_G)$ (identity law in H)
$\Rightarrow \ f(e_G) = e_H$ (right cancellation law in H)

(ii) $x \cdot x^{-1} = e_G$ (inverse law in G)
$\Rightarrow \ f(x \cdot x^{-1}) = f(e_G)$
$\Rightarrow \ f(x) \cdot f(x^{-1}) = e_H$ (homomorphism and (i))
Similarly $f(x^{-1})f(x) = e_H$
Therefore, $[f(x)]^{-1} = f(x^{-1})$

(iii) Since the definition of same cardinal number just means the existence of a bijective mapping and since f is a bijective mapping from G to H, it follows that G and H have the same cardinality.

Practice Exercise IX.4

1. Define $f : (Z, +) \to (Q, +)$ by $f(n) = \dfrac{3n}{4}$. Show that f is a homomorphism.

2. Define $f : (Z, \cdot) \to (Q, \cdot)$ by $f(n) = \dfrac{3n}{4}$. Show that f is not a homomorphism.

3. Define a mapping $f : (R^*, \cdot) \to (R^*, \cdot)$ by $f(x) = |x|$. Show that f is a homomorphism. Find (a) Image of f (b) Kernel of f.

4. Let y be a fixed element in a group $(G, \cdot)$. Define $\alpha : G \to G$ by $\alpha(g) = y^{-1}gy$, for all $g \in G$. Show that α is a homomorphism.

5. Let f be an isomorphism from a group G to a group H. Show that

   (i) $gg' = g'g$ in $G \Leftrightarrow f(g) \cdot f(g') = f(g') \cdot f(g)$

   (ii) G is Abelian $\Leftrightarrow$ H is Abelian

   (iii) $g^k = e_G \Rightarrow [f(g)]^k = e_H$

6. (a) Let G be a cyclic group, G' a group and $f : G \to G'$ a surjective homomorphism. Show that G' must be cyclic.

   (b) Show that the homomorphic image of a cyclic group is cyclic.

   (c) Show that an infinite cyclic group is isomorphic to the additive group of integers.

Summary
Algebraic structures such as groupoids, semigroups, monoids and groups are considered as well as Abelian or commutative groups. Properties of groups are given and examples from numbers, sets, residue classes, symmetric groups and cyclic groups are studied.

Conditions for a subset of a group to be a subgroup are given and Lagrange's theorem is used to determine subgroups of given finite groups.

Mappings between groups which preserve the binary operations of the groups are called homomorphisms. Homomorphisms which are one-to-one or onto or both are studied together with their kernels as well as homomorphism from a group to itself called endomorphism.

Post-Test
See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE TEN

Rings and Fields

Introduction
Numbers have two binary operations which give integers the structure of a ring and real numbers the structure of a field. We shall study sets with two binary operations which give rise to the structure of rings and fields. We shall consider their simple properties and give examples. We shall also see certain subsets of rings, called subrings and ideals with the same binary operations. We shall then conclude by studying homomorphisms of rings which are mappings between rings which preserve the binary operations of the rings.

Objectives
The reader should be able to

(i) prove elementary properties of rings and fields

(ii) show whether a set together with two given binary operations forms a ring or a field

(iii) give different examples of a ring or a field

(iv) determine subrings and ideals of rings

(v) prove simple properties of homomorphisms of rings.

Pre-Test

1. If $(R, +, \cdot)$ is a ring, show that

   (i) $0 \cdot a = 0$ for all a in R;

   (ii) $(-a) \cdot b = -(a \cdot b)$, for all a, b in R

2. (i) Show that $(Z_6, \oplus, \otimes)$ is a commutative ring but not a field.
   (ii) Show that $(Z_{\text{EV}}, +, \cdot)$ is a commutative ring.

3. Two operations $*$ and $\circ$ are defined on the set $\mathcal{R}$ of real numbers by

$$\begin{aligned} x * y &= x + y + 1 \\ x \circ y &= xy + x + y \end{aligned}$$

   Show that $(\mathcal{R}, *, \circ)$ is a field.

4. Prove that the set of numbers $= \{x + y\sqrt{3}\}$, where x and y are rational numbers under addition and multiplication, forms a field.

5. Let $(R, +)$ be a group (not necessarily Abelian) and let $(R, \cdot)$ be a monoid such that the distributive laws hold. Prove that $(R, +, \cdot)$ is a ring, (i.e. show that $(R, +)$ is Abelian).

6. Let S be a set and 2^S the power set of S. Define $+$ and $\cdot$ in 2^S as

$$A + B = (A \cup B) - A \cap B) \text{ and } A \cdot B = A \cap B$$

   Show that $(2^S, +, \cdot)$ is a commutative ring with identity S

7(a) Let $(R, +, \cdot)$ be a ring with identity 1 and let $U(R)$ be the set of invertible elements a in R such that $ab = ba = 1$ for some b in R. Show that $(U(R), \cdot)$ is a group.

(b) Find $U(R)$ in the following rings:

   (i) $(Z, +, \cdot)$

   (ii) $(Z_8, \oplus, \otimes)$

(iii) D = division ring

(iv) F = field.

8(a) Show that a commutative ring $(R, +, \cdot)$ satisfies the cancellation law if and only if it has no proper zero divisors.

(b) Show that a finite integral domain is a field.

(c) Show that $(Z_m, \oplus, \otimes)$ is an integral domain if and only if m is a prime.

9. If $\phi : R \to S$ is a ring homomorphism, show that

(i) $\phi(0_R) = 0_S$

(ii) $\phi(-a) = -\phi(a)$, for all a in R

(iii) if R has an identity 1_R and $\phi(1_R) \neq 0_S$, then

$$\phi(1_R) = 1_{\phi(R)}$$

(iv) $ker(\phi)$ is a subring of R (and an ideal of R)

(v) $\phi(R)$ is a subring of S

(vi) ϕ is a ring monomorphism if and only if $ker(\phi) = \{0_R\}$

10. Let F be a finite field such that $x^3 = 1$ if and only if $x = 1$. If $y \in F$, show that there exists $z \in F$ such that $z^3 = y$.

Definitions of Rings and Fields

1. A *ring* $(R, +, \cdot)$ is a set on which two binary operations, $+$ and $\cdot$, (called addition and multiplication, respectively), are defined such that

(i) $(R, +)$ is an Abelian group;

(ii) $(R, \cdot)$ is a semigroup;

(iii) for all a, b, c in R
$a \cdot (b + c) = a \cdot b + a \cdot c$ (right distributive law)
$(a + b) \cdot c = a \cdot c + b \cdot c$ (left distributive law).

2. A ring $(R, +, \cdot)$ is *commutative* if $(R, \cdot)$ is a commutative semigroup.

3. A ring $(R, +, \cdot)$ is a *ring with identity* if there exists $e \in R$ such that $a \cdot e = e \cdot a = a$ for all $a \in R$. We shall write 0 for the additive identity and 1, for the multiplicative identity.

4. An element a of a ring is said to be an *idempotent* if $a^2 = a$. A ring in which every element is idempotent is called a *Boolean ring*.

5. In a commutative ring $(R^*, +, \cdot)$, if $a, b \in R$ are such that $a \neq 0$, $b \neq 0$ and $ab = 0$, we say that a and b are *proper zero divisors*.

6. A cummutative ring $(R, +, \cdot)$ with identity is called an integral domain if $(R - \{0\}), \cdot)$ satisfies the cancellation laws, or alternatively if it has no proper zero divisors.

7. A ring $(R, +, \cdot)$ such that $(R - \{0\}, \cdot)$ is a group is called a *division ring* or a *skew field*.

8. A commutative division ring is called a *field*. *In other words, a field* $(F, +, \cdot)$ is a set with two binary operations $+$ and $\cdot$ such that

   (i) $(F, +)$ is an Abelian (additive) group

   (ii) $(F - \{0\}, \cdot)$ is an Abelian (multiplicative) group.

   (iii) For all a, b, c in F.

   $$a \cdot (b + c) = a, b + a \cdot c, \quad \text{(distributive law)}$$

   Note that it suffices to have only one distributive law since multiplication is commutative by (ii).

Subrings and Ideals

9. A non-empty subset S of a ring $(R, +, \cdot)$ is called a *subring* of $(R, +, \cdot)$ if $(S, +, \cdot)$ is also a ring. Note that S is a subring of R if and only if for every $a, b \in S$ then $a - b \in S$ and $a \cdot b \in S$.

10. Let A be a non-empty subset of a ring $(R, +, \cdot)$ such that

(i) $(A, +)$ is a subgroup of $(R, +)$;

(ii) for any $a \in A$, and $r \in R$ we have $ra \in A$, and $ar \in A$.

Then A is called an ideal of R.

$\{0\}$ and R are ideals of R and are called the trivial ideals of R. If A is an ideal of R such that $A \neq 0$ and $A \neq R$, then A is called a *proper ideal* of R. A ring without proper ideals is called a *simple ring*.

Note that A is an ideal of R if and only if for every $a, b \in A$ and $r \in R$ then $a - b \in A$, $ra \in A$ and $ar \in A$.

Ring Homomorphisms

11. Let R and S be any two rings. A mapping $\phi : R \to S$ is called a ring *homomorphism* if for all a, b in R we have

$$\phi(a + b) = \phi(a) + \phi(b) \text{ and } \phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

A ring homomorphism which is also $1 - 1$ is called a *ring monomorphism*. A ring homomorphism which is onto called a *ring epimorphism*. A *ring* isomorphism is a bijective ring homomorphism.

If $\phi : R \to S$ is a ring homomorphism, the *kernel* of ϕ is defined as

$$ker(\phi) = \{a \in R | \phi(a) = 0\}$$

Example 1:
From our consideration of binary operations in lectures 2 and 9, it is easy to check that

(i) $(Z, +, \cdot)$ is a commutative ring with identity and also an integral domain.

(ii) $(Q, +, \cdot)$ and $(\mathcal{R}, +, \cdot)$ are fields

(iii) $(Z_m, \oplus, \otimes)$ is a commutative ring with identity.

Example 2:
If $(R, +, \cdot)$ is a ring, show that

(i) $a \cdot 0 = 0$, for all $a \in R$;

(ii) $a \cdot (-b) = -(a \cdot b)$, for all a, b in R; and

(iii) $(-a) \cdot (-b) = a \cdot b$, for all a, b in R.

(i) Since $(R, +)$ is an Abelian group, then for any $a \in R$. We have

$$\begin{aligned} & a = a + 0 \text{ (identity law)} \\ \Rightarrow\ & a \cdot a = a \cdot (a + 0) \\ \Rightarrow\ & a \cdot a = a \cdot a + \cdot 0 \text{ (distributive law)} \\ \Rightarrow\ & 0 = a \cdot 0 \text{ (cancellation law for } (R, +)) \end{aligned}$$

(ii) Since $(R, +)$ is an Abelian group, we have

$$\begin{aligned} & b + (-b) = 0 \text{ (inverse law)} \\ \Rightarrow\ & a[b + (-b)] = a \cdot 0 = 0 \text{ (by (i) above)} \\ \Rightarrow\ & a \cdot b + a \cdot (-b) = 0 \text{ (distributive law)} \\ \Rightarrow\ & -(a \cdot b) = a \cdot (-b) \text{ (inverse law)} \end{aligned}$$

(iii) $(-a) \cdot (-b) = (-a) \cdot (-b) + 0$ (identity law in $(R, +)$)
$= (-a) \cdot (-b) + a \cdot 0$ (by (i) above)
$= (-a) \cdot (-b) + a[(-b) + b]$ (inverse law)
$= (-a) \cdot (-b) + a \cdot (-b) + a \cdot b$ (distributive law)
$= [(-a) + a] \cdot (-b) + a \cdot b$ (distributive law)
$= 0 \cdot (-b) + a \cdot b$ (inverse law)
$= 0 + a \cdot b$ (by (i) above)
$= a \cdot b$ (identity law)

Example 3
Show that mZ, where m is any fixed integer in Z, is an ideal in the ring $(Z, +, \cdot)$.
If $mq_1, mq_2 \in mZ$, then $mq_1 - mq_2 = m(q_1 - q_2) \in mZ$
Hence mZ is a subgroup of $(Z, +)$. For any $mq \in mZ$, and $n \in Z$.
$n(mq) = m(nq) \in mZ$ and$(mq)n = m(qn) \in mZ$.

Hence mZ is an ideal of Z.

Example 4
Let Z_5 be the set of residue classes of integers modulo 5. Show that $(Z_5, \oplus, \otimes)$ is a field.
$(Z_5, \oplus)$ is an Abelian group. In $(Z_5^*, \otimes)$, closure, associativity and commutativity follow from those of integers. 1 is the multiplicative identity. The multiplicative inverses are.

$$1^{-1} = 1,\ 2^{-1} = 3,\ 3^{-1} = 2,\ 4^{-1} = 4$$

Distributivity follows from that of integers, hence $(Z_5, \oplus, \otimes)$ is a field.

Practice Exercise X

1. Let C be the set of complex numbers,

   $$C = \{x + iy | x, y \in R\}$$

   Show that $(C, +, \cdot)$ is a field.

2. Find all the ideals of Z_4, Z_5 and Z_{12}

3. Show that the set

   $$S = \left\{ \left(\begin{array}{cc} a & b \\ & \\ 0 & 0 \end{array} \right) \middle| a, b \in Z \right\}$$

   is a subring and a right ideal but not a left ideal in the ring $(M_2(Z), +, \cdot)$.

4. Let F be a finite field such that $x^5 = 1$ if and only if $x = 1$. If $y \in F$, show that there exists $x \in F$ such that $x^3 = y$.

5. Show that the set

   $$\left\{ \left(\begin{array}{cc} y & y \\ & \\ -y & x \end{array} \right) \middle| x, y \in R \right\}$$

   is a subring (indeed, a field) of the ring $(M_2(R), +, \cdot)$.

6. Verify whether the following mappings are ring homomorphisms.

   (i) $\phi : R \to R$, $\phi(x) = x + 2$ where R is the ring of real numbers.

   (ii) $\phi : Z \to M_2(Z)$, $\phi(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, where Z is the ring of integers and $M_2(Z)$ is the ring of 2×2 matrices over Z.

   (iii) $\phi : Z \to M_2(Z)$, $\phi(a) = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$

   (iv) $\phi : Z \to M_2(Z)$, $\phi(a) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

7. Let $(B, +, \cdot)$ be a commutative ring with identity, such that $a^2 = a$ for all $a \in B$. Define the operations $\wedge$ and $\vee$ as $a \wedge b = ab$, $a \vee b = a + b + ab$. Show that $(B, \wedge, \vee)$ is a Boolean algebra.

Summary

Different types of rings are considered:

(i) commutative ring
(ii) ring with identity
(iii) Boolean ring
(iv) rings with proper zero divisors
(v) division ring or skew field
(vi) field
(vii) subrings and ideals
(viii) simple ring

Different types of ring homomorphisms are also studied, namely, one-to-one, onto, bijective as well as their kernel

Post-Test

See Pre-Test at the beginning of this Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE ELEVEN

Mathematical Induction

Introduction
To prove a formula which is true for all natural numbers, it is not possible to do this through a case by case verification. We shall study a powerful but simple machinery for achieving such a proof.

Objectives
The reader should be able to use the principle of mathematical induction to prove formulae and statements which are true for all natural numbers.

Pre-Test

1. Show that for all natural numbers n
   (i) $5^{2n} - 1$ is divisible by 24
   (ii) $4^{3n-1} + 2^{3n-1} + 1$ is divisible by 7.
   (iii) 17 divides $3.5^{2n+1} + 2^{3n+1}$
   (iv) 9 divides $2^{2n} - 3n - 1$
2. Prove, by mathematical induction, that for all positive integers n

(i) $\sum_{i=1}^{n} i(i+2) = \frac{1}{6}n(n+1)(2n+7)$

(ii) $\sum_{i=1}^{n}(-1)^i i^2 = \frac{1}{2}(-1)^n n(n+1)$

(iii) $\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2$

(iv) $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$

3. Show that if $(a,b)\cdot(c,d) = (ad+bc, bd)$, then $(an,b)^n = (nab^{n-1}, b^n)$

4. Show that if $p_1, \cdots, p_k$ are any k primes whatever, $k > 1$, there exist integers $\alpha_1, \ldots, \alpha_k$ such that $\alpha_1 p_1 + \cdots + \alpha_k p_k = 1$

5. Let $\{a_1, \ldots, a_n\}$ be a finite set of positive integers. Show that there exists a prime q which is not in $\{a_1, \ldots, a_n\}$.

6. Show that if a, b, c are integers such that $c|ab$ and $(b,c) = 1$, then $c|a$. Hence prove that if p is a prime and $\{a_1, \ldots, a_n\}$ is a set of n integers and if $p|a_1 \ldots a_n$, then p divides at least one of the a_i's.

7. Prove for a natural number n, the Binomial expansion
$$(a+b)^n = \sum_{r=0}^{n} {}^nC_r a^{n-r} b^r$$

8. Prove that $2^n > 1 + n$, for all $n > 1$.

9. Let r and s be natural numbers satisfying $r = s - 1$. Show that for all natural numbers, $n, r^{2n} + 2ns - 1$ is divisible by s^2. Hence show that $2^{40} + 119$ is divisible by 9.

10. If $B = \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix}$ prove that
$B^n = \begin{pmatrix} 2n+1 & 2n \\ -2n & -2n+1 \end{pmatrix}$ for all $n = 1, 2, 3, \ldots$

The Principle of Mathematical Induction

The principle of mathematical induction is a very powerful mathematical tool which is very useful in proving mathematical formulae and statements which are true for all positive integers. It can be stated as follows.

A mathematical formula or statement T_n involving the positive integer n is true for ALL positive integers, if

(i) it is true for T_1 i.e. when $n = 1$, and

(ii) the hypothesis that it is true for any particular n, say $n = r$, is sufficient to ensure that it is also true for $n = r + 1$.

Condition (ii) can be replaced by (ii)$'$ the hypothesis that it is true for all $r < n$ is sufficient to ensure that it is also true for $r = n$.

Example 1:

Show that $10^{3n} - 1$ is divisible by 37 for all natural numbers n.

We shall use the principle of mathematical induction.

When $n = 1$, we have

$$10^{3n} - 1 = 10^3 - 1 = 999 = 27 \times 37$$

Hence $37|10^{3b} - 1$ for $n = 1$.

We shall now assume as an inductive hypothesis that $37|10^{3r} - 1$, for some integer r.

We shall then show that $37|10^{3(r+1)} - 1$

$$\begin{aligned} 10^{3(r+1)} - 1 &= 10^{3r} \cdot 10^3 - 1 \\ &= (10^{3r} - 1)10^3 + (10^3 - 1) \\ & \quad 37|10^{3r} - 1, \text{ by the inductive hypothesis, and} \\ & \quad 37|10^3 - 1, \text{ proved earlier, hence } 37|10^{3(r+1)} - 1 \end{aligned}$$

Thus $37|10^{3n} - 1$ for all positive integers n.

Example 2:

Show that $3^{2n+2} - 8n - 9$ is divisible by 64 for all natural numbers n.

When $n = 1, 3^{2n+2} - 8n - 9 = 3^4 - 8 - 9 = 64$.
Therefore $64|3^{2n+2} - 8n - 9$ when $n = 1$. Now, assume as an inductive hypothesis that for $r < n$, $3^{2r+2} - 8r - 9$ is divisible by 64. We now consider $r = n$.

$$\begin{aligned} 3^{2n+2} - 8n - 9 &= 3^{2(n-1)+2} \cdot 3^2 - 8n - 9 \\ &= 9[3^{2(n-1)+2} - 8(n-1) - 9] + 7n + 9 - 8n - 9 \\ &= 9(64M) + 64n \ \text{(by the inductive hypothesis for } r = n-1) \\ &= 64(9M + n). \end{aligned}$$

Hence 64 divides $3^{2r+2} - 8r - 9$ when $r = n$. Therefore, by the principle of mathematical induction $3^{2n+2} - 8n - 9$ is divisible by 64 for all natural numbers n.

Example 3

Prove by mathematical induction, that

$$\sum_{k=1}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2)$$

When $n = 1$, L.H.S. $= 1(2) = 2$

$$\text{R.H.S.} = \frac{1}{3}(2)(3) = 2 = \text{L.H.S.}$$

Therefore the formula is true for $n = 1$. We now assume as an inductive hypothesis that the formula is true for all $n < r$, i.e.

$$\sum_{k=1}^{r} k(k+1) = \frac{1}{3}r(r+1)(r+2)$$

We now consider $r = n$.

$$\sum_{k=1}^{n} k(k+1) = \sum_{k=1}^{n-1} k(k+1) + n(n+1)$$

$$
\begin{aligned}
&= \frac{1}{3}(n-1)n(n+1) + n(n+1) \\
&\quad \text{(by the inductive hypothesis for } r = n-1) \\
&= \frac{1}{3}n(n+1)[n-1+3] \\
&= \frac{1}{3}n(n+1)(n+2)
\end{aligned}
$$

Hence the formula is true for $r = n$, and so the formula is true for all n.

Practice Exercise XI
Show that for all natural numbers n

1. $11^{2n} - 1$ is divisible by 120
2. 9 divides $5^{2n} + 3n - 1$
3. 5 divides $n^5 - n$
4. 9 divides $(3n+1)7^n - 1$
5. 7 divides $2^{5n+3} + 3^{4n+3}$
6. 3 divides $n^3 + 6n^2 + 8n$
7. 8 divides $5^{2n} - 3^{2n}$
8. 9 divides $10^n + 3.4^{n+2} + 5$
9. 24 divides $2.7^n + 3.5^n - 5$
10. 8 divides $3^{2n} + 7$
11. 6 divides $n(n+1)(2n-1)$
12. 64 divides $7^{2n} + 16n - 1$
13. 15 divides $2^{4n} - 1$
14. 4 divides $3^n - 2n - 1$

15. 14 divides $3^{4n+2} + 5^{2n+1}$

16. 3 divides $7^n + 2$

18. $\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$

18. $\sum_{k=1}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2)$

19. $\sum_{k=1}^{n}(2k-1) = n^2$

20. $\sum_{k=1}^{n}(k^2+1)k! = n(n+1)!$

Summary
Two forms of the principle of mathematical induction are given and various applications are considered.

Post-Test
See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE TWELVE

Divisibility and Euclid's Algorithm

Introduction

This is a section on elementary number theory in which we seek to study in detail the nature of natural numbers and integers. In particular we shall see that integers can be divided into those that are primes and those that are composites. This then introduces the idea of factors and multiples, common and greatest factors, common and least common multiples. Their elementary properties are then studied.

Objectives

The reader should be able to

(i) prove Euclid's Division Algorithm and use it in computing greatest common divisors of any two integers;

(ii) prove the linear property for greatest common divisors and use it to solve for integral solutions of certain linear equations in 2 variables;

(iii) prove the unique factorization theorem and use it in the calculation of least common multiples and greatest common divisors; and

(iv) determine when a natural number is a prime and show that there are infinitely many primes.

Pre-Test

1. Find integers u, v such that $d = ux + vy$ where $d = g.c.d.(x, y)$, $x = 2024$, $y = 1760$.

2(a) Show that if a and b are natural numbers, then

(i) $g.c.d.(a, b) | l.c.m.[a, b]$

(ii) $l.c.m.[a, b] | ab$

(b) Show that $(a, b) \cdot [a, b] = ab$.

3. (i) Let $t > 0$ be an integer such that $t|a$ and $t|b$.
Show that

$$g.c.d.\left(\frac{a}{t}, \frac{b}{t}\right) = \frac{1}{t}\ g.c.d.(a, b)$$

(ii) Let m, x and y be positive integers, show that $l.c.m.[mx, my] = m(l.c.m.[x, y])$.

4. (i) Show that $g.c.d.(a, b) = g.c.d.(a, b + at)$ for any integers a, b and t.
(ii) Show that $l.c.m.[a, b] = g.c.d.(a, b)$ implies $a = b$ for any positive integers a and b.
(iii) If $(x, y) = (x, z)$, is $[x, y] = [x, z]$ for any positive integers, x, y, z? Justify your answer.

5. Find the $l.c.m.[x, y]$, when $x = 426$, $y = 964$.

6. (i) Write down a list of prime numbers less than 50.
(ii) Determine whether or not 2183 is a prime number.
(iii) If $x^2 = y^2 + 2183$, find x and y if x and y are positive integers.

7. (i) If $m = [a, b]$ and $d = (a, b)$, find all the values (in positive integers) of a and b with $a > b$ satisfying the equation $m + 13d = 253$.
(ii) Given $[a, b] = 72$ and $(a, b) = 12$, find a and b.

8. Show that (a, b) is the smallest natural number that can be expressed as $ua + vb$ where u and v are integers.

9. (a) Use the linear property of the g.c.d. to find integers x and y such that
   (i) $9x + 4y = 7$ (ii) $\frac{x}{7} + \frac{y}{15} = \frac{23}{105}$
   (b) If x, y and n are natural numbers, prove that x^n divides y^n if and only if x divides y.

10. (a) If n is an integer such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \quad (p_1 \text{ and } p_2 \text{ are prime numbers}),$$

    show that there exist integers q_1, q_2 such that

$$q_1 p_1^{\alpha_1} + q_2 p_2^{\alpha_2} = 1$$

(b) If C_r, C_s are cyclic groups such that $(r, s) = 1$, show that $C_r \times C_s$ is a cyclic group.

Primes, g.c.d. and l.c.m.
Definition

1. Let n be an integer. An *integral divisor* or *factor* of n is an integer m such that

$$n = mq \text{ for some integer } q.$$

   n is also said to be *divisible* by m or is an *integral multiple* of m. We write $m|n$ to mean m divides n. If $m|n$ and $0 < m < n$, then m is called a *proper divisor* of n.

2. An integer p such that $|p| > 1$ is called a *prime* or a *prime number* if the only divisors of p are ± 1 and $\pm p$. A positive integer $p > 1$ will be called a prime if there is no divisor d of p such that $1 < d < p$.

3. An integer, which is not a prime, is said to be *composite*, i.e. an integer n is composite if $n = mq$ for some $m, q \in Z$, $|m| > 1$, $|q| > 1$.

4. Let a, b be any 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* (g.c.d.) or

highest common factor (h.c.f.) of a and b.
We write

$$d = (a, b) \text{ or } d = g.c.d.(a, b)$$

for the g.c.d. or h.c.f. of a and b.

If d, d' are two g.c.d's of a and b, then $d|d'$ and $d'|d \Rightarrow d' = \pm d$. Therefore we can regard a g.c.d. of two integers as a positive integer.

5. If g.c.d$(a, b) = 1$, we say that a and b are *relatively prime* or *coprime.*

6. Let $a_1, \ldots, a_n$ be non-zero integers. An integer b is called a *common multiple* of the a_i if $a_i|b$ for $i = 1, \ldots, n$. 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 $a_1, \ldots, a_n$ by $[a_1, \ldots, a_n]$.

   We shall now prove theorems which facilitate the computation of g.c.d. and l.c.m.

THEOREM **(Euclid's Division Algorithm**
For any integers a, b such that $b > 0$, there exist unique integers q, r such that

$$a = bq + r, \ 0 \leq r < b$$

[*Note:* q is called the *quotient*, and r, the *remainder*]

Proof: Consider the set

$$S = \{a - bx | x \in Z \text{ and } a - bx \geq 0\}$$

Then $a + b \cdot |a|$ is an element of S (by putting $x = -|a|$).
Hence $S \neq \phi$. Since $S \subseteq N \cup \{0\}, S$ must contain a least element $r \geq 0$, by the well-ordering principle of N. Hence,

$$r = a - bq, \text{ for some } q \in Z$$

i.e. $a = bq + r$.
Since $r \geq 0$, we only need to show $r < b$. Suppose $r \geq b$, then $r - b =$

$a - bq - b = a - b(q+1) \geq 0 \Rightarrow r - b \in S$. But $r - b < r$. This is a contradiction to the fact that r is the least element in S. So it must be that $0 \leq r < b$.

Finally, we show that q, r are unique. Suppose

$$a = bq + r = bq' + r', \;\; 0 \leq r < b, \;\; 0 \leq r' < b$$

Then $b(q' - q) = r - r' \Rightarrow b | r - r'$.
But $|r - r'| < b \Rightarrow r - r' = 0 \Rightarrow r = r'$ and so $q = q'$ also.

By reversing the process of Euclid's Division Algorithm, we obtain the *linear property* for the greatest common divisor.

THEOREM
Let a, b be two non-zero integers such that $d = (a, b)$. Then $d = ua + vb$ for some integers u, v.

Proof: Let $S = \{xa + yb | x, y \in Z\}$. Then S contains a set T of positive integers and by the well-ordering principle, T has a least element $d = ua + vb$, say for some $u, v \in Z$. Now $d > 0$ and so by Euclid's division algorithm, $a = dq + r$, for some $q, r \in Z$, $0 \leq r < d$.
$\Rightarrow \;\; r = a - dq = (1 - qu)a + (-qv)b \Rightarrow r \in S$
$\Rightarrow r = 0$ and so $d | a$.
Similarly it can be shown that $d | b$.
Thus $d |$g.c.d(a, b). Now suppose any other integer c, say, divides a and b.
Then

$$c | ua \text{ and } c | vb \Rightarrow c | ua + vb) \Rightarrow c | d$$

Hence $d = (a, b) = ua + vb$.

Remark: Note that u and v are not unique. In fact it is easy to see that $u + \frac{b}{a}m$ and $v - \frac{a}{d}m$ for any integer m, can also be used.

THEOREM (unique Factorization Theorem, or Fundamental Theorem of Arithmetic).

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

Proof: If n is a prime p, then the theorem is true since p is itself a product with only one factor. On the other hand, if n is composite, then we shall proceed by induction. Let $\{T_m | m \in N\}$ be the set of all composites > 1. Then $T_1 = 4 = 2 \times 2$ and so the theorem is true for $m = 1$. Now assume as an inductive hypothesis that the theorem is true for all $r < n$. Since T_n is composite $T_n = uv$ where $u < T_n$, $v < T_n$. Then by the inductive hypothesis

$$u = p_1 \cdots p_a \text{ and } v = q_1 \cdots q_b$$

$\Rightarrow T_n = p_1 \cdots p_a q_1 \cdots q_b$. Therefore the theorem is true for T_n and so is true for all n.

To prove uniqueness, assume $T_n = p_1 \cdots p_s = q_1 \cdots q_t$ are two prime factorizations of T_n. Since each $p_i | T_n$ we have that $p_i | q_1 \cdots q_t$ which implies that $p_i | q_j$ for some j. Since p_i and q_j are primes, it follows that $p_i = q_{j_i}, i = 1, \ldots, s$. Hence $s \leq t$. Similarly, we can show that $q_j = p_{i_j}, j = 1, \ldots, t$. Hence $t \geq s$. Therefore $t = s$. This proves uniqueness.

THEOREM: There are infinitely many primes.

Proof: Assume that there are a finite number of primes, say k of them $p_1, \ldots, p_k$. Consider the integer

$$s = 1 + p_1, \ldots, p_k$$

Then $p_1 \not| s$ for $i = 1, \ldots, k$. So by the unique factorization theorem, s can be expressed uniquely as a product of positive primes which must be different from the p_i, $i = 1, \ldots, k$. Hence we have constructed at least one new prime different from the p_i, contradicting the assumption that there are k of them. So the number of primes must be infinite.

Example 1: Let m, n, p be integers. Show that

(i) $m|n \Rightarrow m|nq$ for any integer q.

(ii) $m|n$ and $m|p \Rightarrow m|nx + py$ for any integers x, y;

(iii) $m|n$ and $n|m \Rightarrow m = \pm n$;

(iv) $m|n$ and $m > 0 \Rightarrow m \leq n$

(i) $m|n \Rightarrow n = km$ for some integer k. Hence

$$nq = (kq)m \text{ for any integer } q.$$

This implies $m|nq$.

(ii) $m|n \Rightarrow n = k_1 m$ for some integer k_1
$m|p \Rightarrow p = k_2 m$ for some integer k_2
$\Rightarrow \quad nx + py = (k_1 x)m + (k_2 y)m$ for any integers x, y
$\Rightarrow \quad nx + py = (k_1 x + k_2 y)m$
$\Rightarrow \quad m|nx + py.$

(iii) $m|n \Rightarrow n = k_1 m$ for some integer k_1
$n|m \Rightarrow m = k_2 n$ for some integer k_2
$\Rightarrow \quad n = k_1 k_2 n \Rightarrow k_1 k_2 = 1$
$\Rightarrow \quad k_1 = 1 = k_2$ or $k_1 = -1 = k_2$
Hence $n = \pm m$.

(iv) $m|n \Rightarrow n = km$ for some integer k. Since $m > 0$, $n > 0$ we have that $k > 0$. Since $k \geq 1$, it follows that $m \leq n$.

Example 2
Let a and b be integers such that $b.0$ and $a = bq + r$, $0 \leq r < b$ for some integers q, r. Show that $(a, b) = (b, r)$.

Let $d = \text{g.c.d.}(a, b)$. Then $d|a$ and $d|b$. This implies that $d|a - bq$ i.e. $d|r$. Therefore $d|b$ and $d|r$ which implies that

$$d|\text{g.c.d.}(b, r) \tag{1}$$

Let $d' = (b, r)$. Then $d'|b$ and $d'|r$. This implies that $d'|bq + r$ i.e. $d'|a$. Therefore $d'|b$ and $d'|a$ which implies that

$$d'|(a, b) \tag{2}$$

(1) and (2) imply that $d = \pm d'$. Since we take positive integers for g.c.d.'s, we have $d = d'$ and $(a, b) = (b, r)$.

Remark: The result of Example 2 will be used in the computation of g.c.d.'s without factoring into primes, and is very efficient. If we have two integers a and b with $b > 0$, we obtain by a repeated use of the division algorithm

$$\begin{aligned}
a &= d_1 b + r_1 \quad 0 \le r_1 < b \\
b &= d_2 r_1 + r_2, \quad 0 \le r_1 < r_1 \\
r_1 &= d_3 r_2 + r_3 \quad 0 \le r_3 < r_2 \\
&\cdots \\
r_{n-2} &= d_n r_{n-1} + r_n, \quad 0 \le r_n < r_{n-1} \\
r_{n-1} &= d_{n+1} r_n + 0
\end{aligned}$$

Therefore, by Example 2, we have

$$\begin{aligned}
(a, b) &= (b, r_1) = (r_1, r_2) = r_2 r_3) = \cdots = (r_{n-1}, r_n) \\
&= (r_n, 0) = r_n
\end{aligned}$$

Example 3
Find $d = (170, 102)$ and find integers u and v such that $d = 170u + 102v$.
By Euclid's division algorithm, we obtain

$$\begin{aligned}
170 &= 102(1) + 68 \\
102 &= 68(1) + 34 \\
68 &= 34(2)
\end{aligned}$$

Therefore $d = (170, 102) = 34$.
Reversing the above process, we obtain

$$\begin{aligned}
d = 34 &= 102 - 68(1) \\
&= 102 - (170 - 102) \\
&= 102(2) - 170(1)
\end{aligned}$$

Therefore $u = -1, v = 2$.

Example 4
Find all the integral solutions of the equation

$$710x + 68y = 6$$

g.c.d. of 710 and 68 is obtained as

$$d = (710, 68) = 2$$

By reversing the process, we obtain

$$\begin{aligned} & 710(-9) + 68(94) = 2 \\ \Rightarrow \quad & 710(-27) + 68(282) = 6 \end{aligned}$$

Now all solutions of $710x + 68y = 6$ are

$$\begin{aligned} x &= -27 + \frac{68}{d}t = -27 + 34t \in Z \\ y &= 282 - \frac{710}{d}t = 282 - 355t,\ t \in Z \end{aligned}$$

Practice Exercise

1. Find integers u, v such that $d = ux + vy$ where $d = \text{g.c.d.}(x, y)$, for the following pairs of integers.

   (i) $x = 1170,\ \ y = 102$

   (ii) $x = 814,\ \ y = 4078$

   (iii) $x = 18426,\ \ y = 28964$

   (iv) $x = 14288,\ \ y = 6084$

2. Find the l.c.m. $[x, y]$ for the following pairs of integers.

   (i) $x = 170,\ \ y = 102$

   (ii) $x = 814,\ \ y = 78$

   (iii) $x = 288,\ \ y = 84$

(iv) $x = 24, \quad y = 760$

3. Show that if $(a, b) \cdot (c, d) = (ad + bc, bd)$ then

$$(a, b)^n = (nab^{n-1}, b^n)$$

4. Show that if $p_1, \ldots, p_k$ are any k primes whatever, $k > 1$, there exists integers $\alpha_1, \ldots, \alpha_k$ such that

$$\alpha_1 p_1 + \cdots + \alpha_k p_k = 1$$

5. Show that if a, b, c are integers such that $c|ab$ and $(b, c) = 1$, then $c|a$.

Summary
Various concepts about integers are considered such as
(i) factors
(ii) prime and composite numbers
(iii) divisors, common divisors, greatest common divisions (g.c.d) or h.c.f.
(iv) multiples, common multiples and least common multiples (l.c.m.)
(v) relatively prime or coprime numbers
Their properties and examples are given.
The Euclide's Division Algorithm is proved leading to the linear property of the g.c.d. which states that the g.c.d. of two numbers can be expressed as a linear combination of the numbers.
The Unique Factorization Theorem or the Fundamental Theorem of Arithmetic is also proved with application to the proof of the fact that there are infinitely many primes.

Post-Test
See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE THIRTEEN

Congruences

Introduction
The theory of congruences is a mathematical tool designed to further solve divisibility problems in number theory. We shall see how to study the nature of very large natural numbers expressed as powers.

Objectives
The reader should be able to:

(i) be familiar with the language of congruence and residue system;

(ii) show that the set of reduced system of residues forms an Abelian group under multiplication;

(iii) deduce Euler's, Fermat's and Wilson's theorems on congruences;

(iv) solve liner congruences; and

(v) apply congruences to the solution of divisibility problems.

Pre-Test

1. What remainder does 12^{120} leave upon division by 13?

2. What remainder does 25^{25} leave upon division by 21?

3. Show that $2^{32} - 1$ is divisible by 257.

4. Find the remainder when 4^{53} is divided by 17.

5. Show that
$$2^{5n+3} + 3^{4n+3} \equiv 0 \pmod 7$$
for all positive integers n.

6. If p is a prime number, show that
$$(x + y)^p \equiv x^p + y^p \pmod p$$
for all integers x, y.

7. Solve the following linear congruences:

   (i) $32x \equiv 1 (\text{mod } 17)$;

   (ii) $225x \equiv 153 (\text{mod } 261)$

8. Solve by inspection the linear congruences
(i) $5x \equiv 3 (\text{mod } 7)$ (ii) $4x \equiv 7 (\text{mod } 10)$

9. If p is prime, $p \neq 2$ and n is any integer, show that $a^2 \equiv 1 (\text{mod } p^n)$ $\Rightarrow a \equiv 1 (\text{mod } p^n)$ or $a \equiv -1 (\text{mod } p^n)$.

10. If m is an integer, show that $m^2 \equiv 0, 1$ or $4 (\text{mod } 8)$. Hence prove that there is no integer $m \equiv 7 (\text{mod } 8)$ which is expressible as a sum of 3 squares.

Definition of Congruence
We showed in lecture 5 that the relation $\sim$ defined on the set Z of integers as
$$a \sim b \text{ means } m|a - b$$
gives rise to an equivalence relation which partitions Z into disjoint equivalence classes, denoted Z_m, and called the set of residue classes of integers modulo m.

Let $[a]$ denote the residue class of a, i.e. $[a] \in Z_m$, then an element b in $[a]$ is called a *residue of a, modulo m* or b in $[a]$ is said to be *congruent to a, modulo m,* and we denote this by writing $b \equiv a(\text{mod } m)$,
i.e. $b \equiv a(\text{mod}m)$ means $m|b-a$ or $m|a-b$.
Then $b \equiv a(\text{mod}m)$ is a congruence.

Example 1
Let $a_i \equiv b_i(\text{mod } m)$ for $i = 1, \ldots, q$. Show that

$$\sum_{i=1}^{q} a_i \equiv \sum_{i=1}^{q} b_i \text{ (mod } m)$$

$a_i \equiv b_i \text{ (mod } m)$ means $m|a_i - b_1$.

$$\Rightarrow \quad m \left| \sum_{i=1}^{q} (a_i - b_i) \Rightarrow m \right| \left(\sum_{i=1}^{q} a_i - \sum_{i=1}^{q} b_i \right).$$

Therefore in the language of congruence,

$$\sum_{i=1}^{q} a_i \equiv \sum_{i=1}^{q} b_i (\text{mod } m)$$

Example 2
Let a, b, c, d and n be integers such that $d = \text{g.c.d.}(c, n)$. Then

$$ca \equiv cb(\text{mod } n) \Leftrightarrow a \equiv b \left(\text{mod } \frac{n}{d} \right)$$

Thus if $d = 1$, then $ca \equiv cb(\text{mod } n) \Leftrightarrow a \equiv b(\text{mod } n)$
$\Rightarrow$: $ca \equiv cb(\text{mod } n) \Rightarrow cb - ca = nk$ for some $k \in Z$
i.e. $\left(\frac{c}{d}\right)(b-a) = \left(\frac{n}{d}\right)k$. Note that since $d = (c, n)$, $\frac{c}{d}$ and $\frac{n}{d}$ are integers.
Hence

$$\frac{n}{d} \left| \left(\frac{c}{d}\right)(b-a) \right.$$

Also, $d = (c, n) \Rightarrow \left(\frac{n}{d} \; \frac{c}{d}\right) = 1$. Hence

$$\frac{n}{d} \left| \left(\frac{c}{d}\right)(b-a) \Rightarrow \frac{n}{d} \right| b - a \Rightarrow a \equiv b \left(\text{mod } \frac{n}{d} \right)$$

$\Leftarrow$: $a \equiv b \left(\text{mod } \frac{n}{d}\right) \Rightarrow \frac{n}{d} | a - b \Rightarrow |d(a-b)$.
Since $c = kd$ for some $k \in \mathbb{Z}$, $n|c(a-b)$.
i.e. $ca \equiv cb(\text{mod } n)$.

Practice Exercise III.1
Show that

1. $a \equiv b(\text{mod } m) \Rightarrow ac \equiv bc(\text{mod } m)$, for any $c \in \mathbb{Z}$.
2. $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m) \Rightarrow ac \equiv bd(\text{mod } m)$
3. $a \equiv b(\text{mod } m_i)$, $i = 1, \ldots, s \Leftrightarrow a \equiv b(\text{mod}[m_1, \ldots, m_s])$
4. $a \equiv b(\text{mod } m) \Rightarrow a^k \equiv b^k(\text{mod } m)$, $k > 1$.
5. $a \equiv b(\text{mod } m), c|m$ and $c > 0 \Rightarrow a >\equiv b(\text{mod } c)$
6. if p is prime and $(c, p) = 1$.
   $a \equiv b(\text{mod } p^2) \Leftrightarrow ac \equiv bc(\text{mod } p^2)$
7. $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m) \Rightarrow ra + sc \equiv rb + sd(\text{mod } m)$ where r, s are integers.

Residue systems and congruences
A set $T = \{a_1, \ldots, a_n\}$ of integers is called a *complete residue system modulo* n if T contains exactly one integer each from the residue classes modulo n such that

(i) $a_i \not\equiv a_j(\text{mod } n)$ for $i \neq j$, and

(ii) given any integer $x \in \mathbb{Z}$, there exists one and only one a_i such that $x \equiv a_i(\text{mod } n)$.

Example 3
In $\mathbb{Z}_5$, the following are complete residue systems modulo 5,
$\{0, 1, 2, 3, 4\}, \{5, 6, 7, 8, 9\}$ and $\{15, 16, 17, 18, 19\}$.
A reduced residue system modulo n is a set $V = \{a_1, \ldots, a_s\}$ of integers such that

(i) $a_i \not\equiv a_j (\text{mod } n)$, if $i \neq j$,

(ii) $(a_i, n) \equiv 1$ for each i, and

(iii) given any integer y, with $(y, n) = 1$, then $y \equiv a_k$ for some $a_k \in V$.

Proposition
Let $b \in \mathbb{Z}$, $n \in \mathbb{Z}^+$ such that $(b, n) = 1$. Suppose $\{a_1, \ldots, a_n\}$ is a complete residue system modulo n, then $\{ba_1, \ldots, ba_n\}$ is a complete residue system modulo n. Furthermore, suppose $\{a_1, \ldots, a_s\}$ is a reduced residue system modulo n then $\{ba_1, \ldots, ba_s\}$ is a reduced residue system modulo n.

Proof. Let $S = \{a_1, \ldots, a_n\}$. Then $a_i \not\equiv a_j \pmod{n}$ if $i \neq j$. Now consider the set $T = \{ba_1, \ldots, ba_n\}$. Then since $(b, n) = 1$.
Example 2 shows that

$$ba_i \equiv ba_j (\text{mod } n) \Leftrightarrow a_i \equiv a_j (\text{mod } n)$$

Hence $a_i \not\equiv a_j (\text{mod } n)$ if $i \neq j \Leftrightarrow ba_i \not\equiv ba_j (\text{mod} n)$ if $i \neq j$. Hence the set T is a complete residue system modulo n (since there are n distinct classes).

Now let $U = \{a_1, \ldots, a_s\}$ be a reduced residue system modulo n. Then we have

(i) $a_i \not\equiv a_j (\text{mod } n)$ if $i \neq j$

(ii) $(a_i, n) = 1$ for each i; and

(iii) for any integer y such that $(y, n) = 1$, we have that $y \equiv a_k$ for some $a_k \in U$.

Next consider the set $V = \{ba_1, \ldots, ba_s\}$. Then as before since $(b, n) = 1$, $ba_i \not\equiv ba_j (\text{mod } n)$ if $i \neq j \Leftrightarrow a_i \not\equiv a_j (\text{mod } n)$ if $i \neq j$. Also since $(b, n) = 1$ and $(a_i, n) = 1$, we have that $(ba_i, n) = 1$ for each i. Finally suppose $y \in \mathbb{Z}$ such that $(y, n) = 1$. We must show that y
$equiv ba_k (\text{mod } n)$ for some $ba_k \in V$. Now $(ba_i, n) = 1 \Rightarrow ba_i \equiv a_j (\text{mod } n)$ for some $a_j \in U$, by (iii) above. Since $ba_i \not\equiv ba_j$ if $i \neq j$ and $a_i \not\equiv a_j$, if $i \neq j$, we have that each $a_i \equiv ba_k$ for some $ba_k \in V$. Now $(y, n) = 1 \Rightarrow y = a_i$ for some $a_i \in U$ by (iii) above $\Rightarrow y \equiv ba_k (\text{mod } n)$ for some $ba_k \in V$. This

proves that V is also a reduced residue system modulo n.

Notation. If $\Phi(n)$ denotes the set of a reduced system of residues modulo n, then we denote $|\Phi(n)| = \phi(n)$ and call the number $\phi(n)$ Euler's *phi-function* or the *totient*.

Proposition
$(\Phi(n), \cdot)$ is an Abelian group.

Proof.
Let $\Phi(n) = \{a_1, \ldots, a_{\phi(n)}\}$.

Closure:
$(a_i, n) = 1,\ (a_j, n) = 1 \Rightarrow (a_i a_j, n) = 1$.
This implies that $a_i, a_j \in \Phi(n) \Rightarrow a_i a_j \in \Phi(n)$.

Commutativity: This follows from the commutativity in $\mathbb{Z}$.
Associativity: This follows from the associativity in $\mathbb{Z}$.
Identity: Since $(1, n) = 1$, it follows that 1 lies in one of the classes in $\Phi(n)$. Also

$$a_i \cdot 1 = a_i \text{ for all } i = 1, \ldots, \phi(n).$$

Hence 1 is the identity.
Inverse. Let $a_i \in \Phi(n)$. Since $(a_i, n) = 1$, then by the linear property of the g.c.d.

$$1 = sa_i + tn \Rightarrow sa_i \equiv 1 (\text{mod } n).$$

Hence the inverse of class a_i is a class s. Thus $(\Phi(n), \cdot)$ is an Abelian group.

Corollary: $(\mathbb{Z}_p, +, \cdot)$ is a field for any prime p.

Proof. $(\mathbb{Z}_p, +)$ is an Abelian group. Now $\mathbb{Z}_p^* = \Phi(p)$ and so $(\mathbb{Z}_p^*, \cdot)$ is an Abelian group from the last proposition. Since distributivity of $\cdot$ holds over $+$, we conclude that $(\mathbb{Z}_p, +, \cdot)$ is a field.

Theorem **(Euler).** Let $n \in \mathbb{Z}^+$. If $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 (\text{mod } n)$.

Proof. $(a, n) = 1 \Rightarrow a \equiv a_k (\text{mod } n)$ where $a_k \in \Phi(n)$, i.e. $[a] = [a_k]$. Now $\langle [a] \rangle$ is the cyclic subgroup of $\Phi(n)$ generated by class $[a]$. By Lagrange's theorem, the order of a subgroup divides the order of the group. If we denote the order of $[a]$ by q, then $q|\phi(n) \Rightarrow \phi(n) = k, q$. Now

$$\begin{aligned} [a]^q = [1] &\Rightarrow ([a]^q)^k = [a]^{\phi(n)} = [1] \\ &\Rightarrow a^{\phi(n)} \equiv 1 \ (\text{mod } n). \end{aligned}$$

Corollary **(Fermat).** If p is a prime and a is an integer such that $p \not| a$, then

$$a^{p-1} \equiv 1 (\text{mod } p).$$

Proof. By Euler's theorem, $a^{\phi(p)} \equiv 1 (\text{mod } p)$.
However, $\Phi(p) = \{1, 2, \ldots, p-1\}$ and so $\phi(p) = p - 1$.
Hence $a^{p-1} \equiv 1 (\text{mod } p)$.

Corollary. Let p be a prime and a any integer.
Then $a^p \equiv a (\text{mod } p)$.

Proof. From Fermat's theorem, if $p \not| a$, then

$$a^{p-1} \equiv 1 (\text{mod } p) \Rightarrow a^p \equiv a (\text{mod } p)$$

If $p|a$ then $a^p \equiv 0 (\text{mod } p)$ and $a \equiv 0 (\text{mod } p)$

$$\Rightarrow \quad a^p \equiv a (\text{mod } p)$$

Hence for all $a, a^p \equiv a (\text{mod } p)$.

Theorem **(Wilson).** Let p be a prime. Then $(p-1)! \equiv -1 (\text{mod } p)$.

Proof. If $p = 2$, $1 \equiv -1 (\text{mod} 2)$ and the theorem is true. If $p = 3, 2 \equiv -1 (\text{mod} 3)$ and the theorem is also true. For $p > 3$, p is odd. Consider the subset T of $\Phi(p) = \{1, \ldots, p-1\}$, given by $T = \{2, \ldots, p-2\}$. Since $(\phi(p), \cdot)$ is an Abelian group it follows that every member of $\Phi(p)$ has a multiplicative

inverse. Now, since $1 \cdot 1 = 1(\text{mod } p)$ it follows that [1] is the inverse of [1]. Also since

$$(p-1)(p-1) = p^2 - 2p + 1 \equiv 1(\text{mod } p)$$

it follows that $[p-1)$ is its own inverse. Thus every member of T has its inverse in T.
Next we shall show that no member of T is its own inverse. Indeed,

$$i^2 \equiv 1(\text{mod } p) \Rightarrow p|(i+1)(i-1)$$

$\Rightarrow$ $p|i+1$ or $p|i-1$
$\Rightarrow$ $i+1 \equiv 0(\text{mod } p)$ or $i-1 \equiv 0(\text{mod } p)$
$\Rightarrow$ $i \equiv -1$ or $p-1(\text{mod } p)$ or $i \equiv 1(\text{mod } p)$.

Thus only classes 1 and $p-1$ are the only members of $\Phi(n)$ which are their own inverses. Now the number of elements in T is $p-3$, which is even since p is odd, and so members of T pair themselves up in such a way that

$$ij \equiv 1(\text{mod } p),\ i \neq j,\ i, j \in T$$

Hence $2(3)\cdots(p-2) \equiv 1(\text{mod } p)$
$\Rightarrow$ $2(3)\cdots(p-2)(p-1) \equiv p-1(\text{mod } p)$
$\Rightarrow$ $(p-1)! \equiv -1(\text{mod } p)$.

Example 5

(i) What remainder does 2^{50} leave upon division by 105?

(ii) Show that $7^{100} - 1$ is divisible by 100.

(i) The problem is the same as solving the congruence for $x : 2^{50} \equiv x(\text{ mod } 105)$. Since $105 = 3 \times 5 \times 7$, we shall first prove the congruence modulo 3,5 and 7 separately.
Now, $2^2 \equiv 1(\text{mod } 3) \Rightarrow (2^2)^{25} \equiv 1^{25}(\text{mod } 3) \Rightarrow \quad 2^{50} \equiv 1(\text{mod } 3)$ or $2^{50} \equiv 4(\text{mod } 3)$ (1)
Also $2^2 \equiv -1(\text{mod } 5) \Rightarrow (2^2)^{25} \equiv (-1)^{25}(\text{mod } 5)$
$\Rightarrow \quad 2^{50} \equiv -1(\text{mod } 5) \Rightarrow 2^{50} \equiv 4(\text{mod } 5)$ (2)

Finally, $2^3 \equiv 1(\text{mod } 7) \Rightarrow (2^3)^{16} \equiv 1^{16}(\text{mod } 7)$
$\Rightarrow \quad 2^{48} \equiv 1(\text{mod } 7) \Rightarrow 2^{50} \equiv 4(\text{mod } 7)$ (3)
(1), (2) and (3) imply that

$$2^{50} \equiv 4(\text{mod } 105) \text{ since } 105 = \text{l.c.m. } [3,5,7)$$

Hence the required remainder is 4.

(ii) We wish to show that $7^{100} \equiv 1(\text{mod } 100)$.
Now, $7 \equiv -1(\text{mod } 4)$.
$\Rightarrow 7^{100} \equiv (-1)^{100}(\text{mod } 4)$ i.e. $7^{100} \equiv 1(\text{mod } 4$ (1)
Also $7^2 \equiv -1(\text{mod } 25)$
Hence $(7^2)^{50} \equiv (-1)^{50}(\text{mod } 25)$ i.e. $7^{100} \equiv 1(\text{mod } 25)$ (2)
(1) and (2) show that

$$2^{100} \equiv 1(\text{mod } 100) \text{ since } 100 = \text{l.c.m. } [4,25)$$

Example 6.
What remainder does $2^{35} \times 14^{40}$ leave upon division by 11?

$$\begin{aligned}
2^{35} \times 14^{40} &\equiv (2^5)^7 \times 3^{40}(\text{mod } 11), \text{ since } 14 \equiv 3(\text{mod } 11) \\
&\equiv (-1)^7 \times 9^{20}(\text{mod } 11), \text{ since } 2^5 \equiv -1(\text{mod } 11) \\
&\equiv -1 \times (-2)^{20}(\text{mod } 11) \\
&\equiv -1 \times (-32)^4(\text{mod } 11) \\
&\equiv -1 \times (1)^4(\text{mod } 11) \\
&\equiv -1(\text{mod } 11) \\
&\equiv 10(\text{mod } 11)
\end{aligned}$$

Hence the required remainder is 10.

Practice XIII.2

1. What remainder does 128^6 leave upon division by 9?
2. Show that $6^{130} + 27$ is divisible by 49.

Linear Congruences

1. If $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is a polynomial in x with integral coefficients, then the congruence $f(x) \equiv 0(\text{mod } m)$ is said to be of *degree* n if $a_n \not\equiv 0(\text{mod } n)$.

2. An integer c is called a *solution* of the congruence $f(x) \equiv 0(\text{mod } m)$ if $f(c) \equiv 0(\text{mod } m)$.

3. A congruence of degree 1 is called a *linear congruence*. A linear congruence therefore, has the form

$$ax \equiv b(\text{mod } m), \quad \text{with } a \not\equiv 0(\text{mod } m)$$

Proposition

If c is a solution of $f(x) \equiv 0(\text{mod } m)$, then every integer congruent to c modulo m is also a solution.

Proof. $d \equiv c(\text{mod } m) \Rightarrow d^i \equiv c^i(\text{mod } m)$

$\Rightarrow \; a_id^i \equiv a_ic^i(\text{mod } m) \Rightarrow \sum_{i=1}^{n} a_id^i \equiv \sum_{i=1}^{n} a_ic^i(\text{mod } m)$

$\Rightarrow \; \sum_{i=0}^{n} a_id^i \equiv 0(\text{mod } m)$, since $\sum a_ic^i \equiv 0(\text{mod } m)$

i.e. $f(d) \equiv 0(\text{ mod } m)$ or d is a solution of the congruence $f(x) \equiv 0(\text{ mod } m)$

Remark. Whenever a solution of a congruence exists, there are an infinite number of solutions which correspond with all the integers in the residue class of a particular solution.

Proposition. Let $a \in \mathbb{Z}$, $n \in \mathbb{Z}^+$ such that $(a, n) = 1$. Then the linear congruence $ax \equiv b(\text{mod } n)$ has integral solutions which form a residue class modulo n and these are all the solutions.

Proof. Since $(a, n) = 1$, we have by Euler's theorem that $a^{\phi(n)} \equiv 1(\text{mod } n)$. This implies that

$$a^{\phi(n)} \cdot b \equiv b(\text{mod } n) \text{ i.e. } a \cdot (a^{\phi(n)-1} \cdot b) \equiv b(\text{mod } n).$$

Hence $x_1 = a^{\phi(n)-1}, b$ is a solution of $ax \equiv b(\text{mod } n)$. Suppose y is any other solution of $ax \equiv b(\text{mod } n)$. Then $ax_1 - ay \equiv 0(\text{mod } n)$, i.e. $n|a(x_1 - y)$ and since $(a, n) = 1$, we have $n|x_1 - y$, i.e. $x_1 \equiv y(\text{mod } n)$. Hence all elements in the class $[x_1]$ are the only solutions of the linear congruence $a \equiv b(\text{ mod } n)$.

Algorithm for solving linear congruences
A way of solving linear congruences is to use the linear property for the g.c.d. which states that if $d = (x, y)$, then d can be expressed as

$$d = ux + vy,$$

where u and v are integers.
In the congruence $ax \equiv b(\text{mod } n)$, $x = a$, $y = n$ and $d = (a, n) = 1$.
Then

$$\begin{aligned} 1 &= ua + vn \\ \Rightarrow b &= a(ub) + (vb)n \\ \Rightarrow \quad a(ub) &\equiv b(\text{mod } n) \end{aligned}$$

$\Rightarrow$ ub is a solution of $ax \equiv b(\text{mod } n)$, $(a, n) = 1$, and all solutions consist of all integers congruent to ub modulo n, i.e. the solutions are the integers x satisfying $x \equiv ub(\text{mod } n)$.

To solve linear congruences

$ax \equiv b(\text{mod } n)$ where $(a, n) = d \neq 1$ and $d|b$ one proceeds as follows. Since $d|a$, $d|b$ and $d|n$, then $n|ax - n \Rightarrow \frac{n}{d} \Big| \frac{a}{d}x - \frac{b}{d}$ such that

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\text{mod}\frac{n}{d}\right) \qquad (*)$$

Now $(a, n) = d \Rightarrow \left(\frac{a}{d}, \frac{n}{d}\right) = 1$. We can then use the method using the linear property of the g.c.d. discussed above, to solve the congruence $(*)$. Let x_0 be such a solution

$$x \equiv x_0\left(\text{mod } \frac{n}{d}\right), x \equiv x_0 + l\left(\frac{n}{d}\right) \text{ mod } \left(\frac{n}{d}\right),\ l = 0, 1, \ldots, d-1$$

Hence the original congruence $ax \equiv b(\text{mod } m)$ where $(a, n) = d$ has d distinct classes of solutions.

$$x \equiv x_0 + l\left(\frac{n}{d}\right)(\text{mod } n),\ l = 0, 1, \ldots, d-1$$

However, if the modulus n is small, we can always solve congruences by inspection using the relevant part of the multiplication table for $\mathbb{Z}_n$.

The solution of simultaneous linear congruences is contained in the following.

Theorem **(Chinese remainder theorem)**

Let $n_1, n_2, \ldots, n_m$ be pairwise relatively prime positive integers, $a_1, \ldots, a_m$ any integers such that $(a_k, n_k) = 1$ for each k and $b_1, \ldots, b_m$ any integers. Then the m linear congruences $a_k x \equiv b_k(\text{mod } n_k)$ have a unique solution modulo $n_1 \cdot n_2 \ldots n_m$.

Example 7. Solve the linear congruence $6x \equiv 20(\text{mod } 17)$
$6x \equiv 20(\text{mod } 17) \Rightarrow 6x \equiv 3(\text{mod } 17)$ since $20 \equiv 3(\text{mod } 17)$.
Since $(6, 17) = 1$, the linear property gives

$$\begin{aligned} & 6(3) - 17 = 1 \Rightarrow 6(3)(3) - 17(3) = 3 \\ \Rightarrow\ & 6(9) \equiv 3(\text{mod } 17). \end{aligned}$$

Hence the solution is $x \equiv 9(\text{mod } 17)$.

Example 8. Solve the linear congruence $66x \equiv 111(\text{mod } 237)$. Since $(66, 237) = 3$ and $3|111$, the congruence has 3 distinct classes of solutions.

$$66x \equiv 111(\text{mod } 237) \Rightarrow 22x \equiv 37(\text{mod } 79)$$

Since $(22, 79) = 1$, the linear property gives

$$\begin{aligned} & 22(18) - 79(5) = 1 \Rightarrow 22(18)37 - 79(5)37 = 37 \\ \Rightarrow\ & 22(666) \equiv 37(\text{mod } 79) \end{aligned}$$

Hence $x \equiv 666(\text{mod } 79)$ s a solution of $22x \equiv 37(\text{mod } 79)$ i.e. $x \equiv 34(\text{mod } 79)$, $x \equiv 113(\text{mod } 79)$ and $x \equiv 192(\text{mod } 79)$.

Hence the solutions of the given congruence are $x \equiv 34(\text{mod } 237)$, $x \equiv 113(\text{mod } 237)$ and $x \equiv 192(\text{mod } 237)$.

Example 9. Solve, by inspection, for x,

(i) $3x \equiv 2(\text{mod } 11)$

(ii) $6x \equiv 3(\text{mod } 9)$

(i)

$\times$	0	1	2	3	4	5	6	7	8	9	10
3	0	3	6	9	1	4	7	10	2	5	8

From the part of the multiplication table for $\mathbb{Z}_{11}$.

$$x \equiv 8(\text{mod } 11)$$

(ii)

$\times$	0	1	2	3	4	5	6	7	8
6	0	3	0	6	3	0	6	3	3

From the part of the multiplication table for $\mathbb{Z}_9$ the solutions are $x \equiv 2(\text{mod } 9)$, $x \equiv 5(\text{mod } 9)$ and $x \equiv 8(\text{mod } 9)$.

Practice Exercise XIII.3
Solve the linear congruences

1. $3x \equiv 30(\text{mod } 37)$
2. $111x \equiv 75(\text{mod } 321)$
3. $256x \equiv 179(\text{mod } 337)$
4. $3x \equiv 1(\text{mod } 5)$ and $2x \equiv 3(\text{mod } 7)$.

Summary
Properties of congruences, complete and reduced residue systems are studied. In particular, Euler's, Fermat's and Wilson's theorems on congruences are given with applications. Next, linear congruences are considered together with algorithms for solving them as well as Chinese remainder theorem and applications.

Post-Test
See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE FOURTEEN

Polynomials

Introduction
We shall consider the set $R[x]$ of all polynomials in a variable x and with coefficients in R, a commutative ring with identity. Then $R[x]$ becomes a commutative ring with identity under the operations of addition and multiplication.

We shall be especially concerned with the cases when R is a field such as $Q, \Re, \mathbb{C}$ and $\mathbb{Z}_p$. In this connection, we shall consider

1. reducible and irreducible polynomials
2. zeroes of polynomials
3. factorization of polynomials
4. the division algorithm for polynomials, and
5. g.c.d. or h.c.f. of polynomials.

Objectives
The reader should be able to find, with respect to a given field or coefficients.

(i) reducible and irreducible polynomials

(ii) zeroes of polynomials

(iii) factorization of polynomials

(iv) the remainder when a polynomial is divided by another polynomial, and

(v) g.c.d. or h.c.f. of given polynomials.

Pre-Test

1. Verify whether the polynomial is reducible or irreducible. If it is reducible, obtain the factors

   (i) $x^2 + a^2$ in $\Re[x], \mathbb{C}[x]$

   (ii) $x^2 + 3x + 1$ in $Q[x], \Re[x]$.

2. Factorize

   (i) $2x^3 - 3x^2 - 3x + 2$, over Q

   (ii) $4x^4 - 12x^3 - 3x^2 + 8x + 3$, over $\Re$

   (iii) $x^4 + 4x^3 + 10x + 7$, over $\mathbb{Z}_{11}$

3. Find the remainder in $Q[x]$ when $16x^5 + 2x^2 + 5$ is divided by $2x - 1$.

4. When the polynomial $h(x)$ is divided by $x - 2$, the remainder is 1 and when $h(x)$ is divided by $x+3$, the remainder is 5. What is the remainder when $h(x)$ is divided by $(x - 2)(x + 3)$?

5. When a certain quadratic function in x is divided by $x - 1$, $x - 2$ and $x - 3$ the remainders are r, $2r$ and $4r$, respectively. Find, in terms of r, the remainder when the expression is divided by $x - 4$.

6. By considering the polynomial $2x^3-2x$ over $\mathbb{Z}_4$, show that a polynomial of degree n over a commutative ring with identity may have more than n roots.

7. Find the remainder when $x^5+x^4+x^3+x^2+x+1$ is divided by $4x^2+3x+2$ in $\mathbb{Z}_{11}[x]$.

8. Find the g.c.d. $d(x)$ of $a(x) = x^5 + x^4 + x^3 + x^2 + x + 1$, $b(x) = 4x^2 + 3x + 2$ in $\mathbb{Z}_n[x]$ and find polynomials $r(x)$ and $s(x)$ such that $d(x) = a(x)r(x) + b(x)s(x)$.
[You may use the result of Question 7 above].

9. Find the remainder when $x^6+3x^5+4x^2-3x+2$ is divided by $3x^2+2x-3$ in $\mathbb{Z}_5[x]$.

10. Find the g.c.d. $d(x)$, of $a(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$, $b(x) = 3x^2 + 2x - 3$ in $Z_5[x]$ and find polynomials $r(x)$ and $s(x)$ such that $d(x) = a(x)r(x) + b(x)s(x)$.
[You may use the result of Question 9 above].

Factors and zeroes of polynomials
Definitions

1. Let R be a commutative ring with identity and x an indeterminate. A *polynomial form* in x with coefficients in R is an expression

$$a(x) = \sum_{i=0}^{n} a_i x^i, \quad \text{where } a_i \in R,\ 0 \leq i \leq n.$$

When n is a variable, $a(x)$ is called a *polynomial function.* We shall use 'a polynomial' to describe either a polynomial form or a polynomial function. If $a_n \neq 0$, then $a(x)$ is called a polynomial of *degree* n, and a_n is said to be the *leading coefficient* of $a(x)$. a_0 is usually referred to as the *constant term* of $a(x)$. A *constant polynomial* is a polynomial of the form.

$$a_0 + 0x + \cdots + 0x^n = a_0 \in R$$

2. We define addition $+$ and multiplication $-$ on the set $R[x]$ of all polynomials in x over R as follows.

If

$$a(x) = \sum_{i=0}^{m} a_i x^i, \quad b(x) = \sum_{i=0}^{n} b_i x^i \text{ and } n > m, \text{ define}$$

$$a(x) + b(x) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} b_i x^i$$

$$a(x), b(x) = \sum_{i=0}^{m+n} c_i x^i, \text{ where } c_i = \sum_{j=0}^{i} a_j b_{i-j}, \ 0 \leq i \leq m+n$$

Then $R[x]$ becomes a commutative rind with identity.

3. A polynomial $a(x) = \sum_{i=0}^{n} \alpha_i x^i$ of degree n in $R[x]$ such that $a_n = 1$ is called a *monic* polynomial.

4. Let $a(x), b(x)$ be polynomials in $F[x]$, where F is a field. $a(x)$ is said to *divide* $b(x)$ if there exists a non-zero polynomial $c(x)$ such that

$$b(x) = a(x) \cdot c(x).$$

$a(x)$ is also called a *factor* of $b(x)$ and we write $a(x)|b(x)$ to mean $a(x)$ divides $b(x)$.

5. A polynomial $a(x) \in F[x]$ is said to be *irreducible* over F if $a(x)$ cannot be expressed as a product $b(x) - c(x)$ of two polynomials each of degree lower than that of $a(x)$, i.e. $0 < \deg b(x) < \deg a(x)$ and $0 < \deg c(x) < \deg a(x)$. Otherwise, $a(x)$ is said to be *reducible*. Irreducible polynomials in $F[x]$ correspond to primes in Z.

6. An element $u \in F$ is called a *zero* of a polynomial $a(x) \in F[x]$ if $a(u) = 0$.

Example 1. $x^2 + 1$ is irreducible in $\Re[x]$ while it is reducible in $\mathbb{C}[x]$, where $\mathbb{C}$ is the field of complex numbers, since

$$x^2 + 1 = (x + i)(x - i)$$

THEOREM **(Division Algorithm).** Let

$$a(x) = \sum_{i=0}^{n} a_i x^i, \quad b(x) = \sum_{i=0}^{m} b_i x^i$$

be two polynomials in $F[x]$ such that $a_n \neq 0$, $b_m \neq 0$, $m > 0$. Then there exist unique polynomials $q(x)$, $r(x)$ in $F[x]$ such that

$$a(x) = b(x) \cdot q(x) + r(x), \quad \text{where} \quad \deg r(x) < \deg b(x).$$

Proof. Let $T = \{a(x) - b(x) \cdot c(x) | c(x) \in F[x]\}$. Since the degrees of members of $F[x]$ are non-negative integers, it follows that the degrees of polynomials in T are non-negative integers and must have a least element which is either 0 or some positive integer (by the well-ordering principle for N). Let $r(x)$ denote the polynomial of least degree in T.
Then

$$a(x) = b(x) \cdot q(x) + r(x), \text{ say.}$$

We show next that $\deg r(x) < \deg b(x)$. Suppose that $\deg r(x) = s$, then

$$r(x) = \sum_{i=0}^{s} d_i x^i, \text{ say with } d_s \neq 0.$$

Thus we must show that $s < m$. Suppose, on the contrary, that $s \geq m$. Then

$$a(x) - q(x) \cdot b(x) - \frac{d_s}{b_m} x^{s-m} \cdot b(x) = r(x) - \frac{d_s}{b_m} x^{s-m} b(x)$$

is a polynomial having degree less than s.

Also

$$a(x) - q(x) \cdot b(x) - \frac{d_s}{b_m} x^{s-m} \cdot b(x) = a(x) - b(x) \left[q(x) + \frac{d_s}{b_m} x^{s-m} \right]$$

is a member of T. This is a contradiction to $r(x)$ being the polynomial of least degree in T. Hence it must be that $s < m$, i.e.

$$\deg r(x) < \deg b(x)$$

To complete the proof of the division algorithm, we must show that $q(x), r(x)$ are unique. Suppose that we have $q'(x), r'(x)$ such that

$$\begin{aligned} a(x) &= b(x) \cdot q(x) + r(x),\ \deg r(x) < \deg b(x) \\ &= b(x) \cdot q'(x) + r'(x),\ \deg r'(x) < \deg b(x) \end{aligned}$$

Then

$$b(x)[q(x) - q'(x)] = r'(x) - r(x)$$

Since $\deg[r'(x) - r(x)] < \deg b(x)$, we have that

$$\deg(b(x)[q(x) - q'(x)]) < \deg b(x)$$

But $\deg(b(x)[q(x) - q'(x)]) \geq m$, since

$$\deg[q(x) - q'(x)] \geq 0.$$

Hence, this can only happen if $r'(x) - r(x) = 0$ and $q(x) - q'(x) = 0$. That is if $r'(x) = r(x)$ and $q'(x) = q(x)$.

Corollary **(Factor Theorem)**
An element $u \in F$ is a zero of a polynomial $a(x) \in F[x]$ if and only if $x - u$ is a factor of $a(x)$.

Proof. $\Rightarrow$: Suppose $u \in F$ is a zero of $a(x) \in F[x]$. Hence $a(u) = 0$. By the division algorithm.

$$a(x) = (x - u) \cdot q(x) + r$$

Put $x = u$ and use the fact that $a(u) = 0$, we have $r = 0$. Hence $a(x) = (x - u)q(x)$ and so $(x - u)$ is a factor of $a(x)$.
$\Leftarrow$: If $x - u$ is a factor of $a(x)$, then

$$a(x) = (x - u) \cdot q(x),\ \text{for some } q(x) \in F[x].$$

Put $x = u$, $a(u) = 0 \Rightarrow u$ is a zero of $a(x)$.

Corollary **(Remainder Theorem)**
If $f(x) \in F(x)$ is divided by $ax + b$, then the remainder is $f\left(\frac{-b}{a}\right)$.

Corollary. Let $a(x) \in F[x]$ be a polynomial of degree n. Then $a(x)$ has at most n zeroes in F.

Theorem **(Fundamental Theorem of Algebra)**
Every polynomial function of the n-th degree in $C[z]$ can be factorized into exactly n linear factors in $C[z]$. Thus every polynomial in $C[z]$ is reducible in $C[z]$.

Corollary. Every polynomial in $\Re[x]$ can be resolved into a product of factors in $\Re[x]$, where each factor is either linear or quadratic . Thus every polynomial $f(x)$ in $\Re[x]$ of degree ≥ 3 is reducible in $\Re[x]$.

Rational Root Theorem
If p/q, expressed in its lowest terms is a rational root of the polynomial in $Q[x]$.

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdot + a_1 x + a_0, \ (a_n \neq 0)$$

where $a_i \in \mathbb{Z}$, then p and q satisfy

(i) p is a factor of the constant term a_0, and

(ii) q is a factor of the leading coefficient a_n.

Quadratic Functions over Q
$f(x) = ax^2 + bx + c, \ a \neq 0$
$D = b^2 - 4ac$ is called the discriminant of $f(x)$.

(i) If $D \geq 0$ and is a perfect square, then $f(x)$ has zeroes in Q and is reducible in $Q[x]$.

(ii) If $D > 0$ and is not a perfect square, then $f(x)$ is not reducible in $Q[x]$, has zeroes in $\Re$ and is therefore reducible in $\Re[x]$.

(iii) If $D < 0$, then $f(x)$ is not reducible in $Q[x]$ or $\mathcal{R}[x]$, has zeroes on $\mathbb{C}$ and is therefore reducible in $\mathbb{C}[x]$.

Example 2
A polynomial $T(x)$ in $\Re[x]$ is such that when it is divided by $x-1$, $x+1$ and $x+2$, the remainders are 3,1 and 6, respectively. Find the remainder when $T(x)$ is divided by $(x^2-1)(x+2)$.

By the division algorithm,

$$T(x) = (x^2-1)(x+2)q(x) + a_2x^2 + a_1x + a_0$$

since the degree of the remainder should be less than $\deg(x^2-1)(x+2) = 3$.

$$T(1) = a_2 + a_1 + a_0 = 3 \tag{1}$$

$$T(-1) = a_2 - a_1 + a_0 = 1 \tag{2}$$

$$T(-2) = 4a_2 - 2a_1 + a_0 = 6 \tag{3}$$

Solving (1), (2) and (3), we obtain

$$a_0 = 0 \qquad a_1 = 1 \qquad a_2 = 2$$

Therefore the required remainder is

$$2x^2 + x.$$

Example 3
Find the remainder in $Q(x)$ when $5x^4 + 11x + 5$ is divided by $x - 2$.

$$\begin{aligned} \text{Put } f(x) &= 5x^4 + 11x^2 + 5 \\ f(2) &= 5(2)^4 + 11(2)^2 + 5 = 129 \end{aligned}$$

G.c.d. of polynomials
Let $a(x), b(x)$ be polynomials in $F[x]$, where F is a field. A *common divisor* of $a(x)$ and $b(x)$ is a polynomial $d(x) \in F[x]$ such that $\tilde{d}(x)|a(x)$ and $\tilde{d}(x)|b(x)$. Suppose that every common divisor of $a(x)$ and $b(x)$ also divides $d(x)$, then $d(x)$ is called the greatest common divisor (g.c.d.) or *highest common factor* (h.c.f.) of $a(x)$ and $b(x)$. We write $d(x) = (a(x), b(x))$ for the g.c.d. or h.c.f. of $a(x)$ and $b(x)$ and we require it to be a monic polynomial. This ensures that the g.c.d. is unique.

Let $a(x), b(x)$ be two non-zero polynomials. Suppose $\deg b(x) < \deg a(x)$. Then by a repeated use of the division algorithm, we have

$$\begin{array}{lcl} a(x) & = & b(x) \cdot q(x) + r(x),\ \deg r(x) < \deg b(x) \\ b(x) & = & r(x) \cdot q_1(x) + r_1(x), \deg r_1(x) < \deg r(x) \\ r(x) & = & r_1(x) \cdot q_2(x) + r_2(x),\ \deg r_2(x) < \deg r_1(x) \\ \vdots & \vdots & \vdots \\ r_{k-2}(x) & = & r_{k-1}(x) q_k(x) + r_k(x),\ \deg r_k(x) < \deg r_{k-1}(x) \\ r_{k-1}(x) & = & r_k(x) \cdot q_{k+1}(x) \end{array}$$

In the same way as for numbers, we have

$$\begin{array}{rcl} (a(x), b(x)) & = & (b(x), r(x)) = (r(x), r_1(x)) \\ & & = \cdots = (r_{k-2}(x), r_{k-1}(x)) = (r_{k-1}(x), r_k(x)) = a_k^{-1} r_k(x) \end{array}$$

where a_k is the leading coefficient of $r_k(x)$. Note that $a_k^{-1} r_k(x)$ is a monic polynomials, as required.

By reversing the above process, we obtain polynomials $r(x)$, $s(x)$ such that

$$d(x) = r(x) \cdot a(x) + s(x) \cdot b(x)$$

We also have the following facts which are analogues of those in the theory of numbers.

1. In $F[x]$, let $p(x)$ be an irreducible polynomial over F. Suppose that $p(x)$ divides $a(x) \cdot b(x)$, then either $p(x)$ divides $a(x)$ or $p(x)$ divides $b(x)$.

2. Unique Factorisation Theorem. Let $a(x) \in F[x]$ be a polynomial of degree $n \geq 1$. Suppose that

   $$a(x) = p_1(x) \cdots p_s(x) = q_1(x) \cdots q_t(x)$$

   are two decompositions of $a(x)$ into irreducible factors of degree ≥ 1, then $s = t$ and the $p(x)$'s are the $q(x)$'s in some order or they differ from the $q(x)$'s by constant factors.

Example 4

(a) Find the remainder when $x^6+3x^5+4x^2-3x+2$ is divided by $3x^2+2x-3$ in $Z_7[x]$.

(b) Find the g.c.d., $d(x)$, of $a(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $b(x) = 3x^2 + 2x - 3$ in $\mathbb{Z}_7[x]$ and find polynomials $r(x)$ and $s(x)$ such that $d(x) = a(x) \cdot r(x) + b(x) \cdot s(x)$.

(a) Use the method of long division and note that in Z_7, we have

$$2 \times 4 = 1, \quad 3 \times 5 = 1, \quad 6 \times 6 = 1, \quad -6 = +1$$

$$\begin{array}{rl} & 5x^4 + 5x^2 - x \\ \underline{3x^2 + 2x - 3} \mid & x^6 + 3x^5 + 4x^2 - 3x + 2 \\ & \underline{x^6 + 3x^5 - x^4} \\ & \qquad x^4 + 4x^2 \\ & \qquad \underline{x^4 + 3x^3 - x^2} \\ & \qquad\quad -3x^3 + 5x^2 - 3x \\ & \qquad\quad \underline{-3x^3 - 2x^2 + 3x} \\ & \qquad\qquad -6x + 2 = x + 2 \end{array}$$

Hence the required remainder is $x + 2$.

(b) From part (a) above

$$a(x) = b(x) \cdot (5x^4 + 5x^2 - x) + x + 2 \tag{1}$$

Next divide $b(x) = 3x^2 + 2x - 3$ by $r(x) = x + 2$.

$$\begin{array}{rl} & 3x - 4 \\ \underline{x + 2} \mid & 3x^2 + 2x - 3 \\ & \underline{3x^2 + 6x} \\ & \qquad -4x - 3 \\ & \qquad \underline{-4x - 1} \\ & \qquad\quad -2 = 5 \end{array}$$

Hence $b(x) = (x + 2)(3x - 4) + 5$ (2)
and $x + 2 = 5(3x + 6)$.
Hence $d(x) = \text{g.c.d. } (a(x), b(x)) = 5^{-1}5 = 1$, since the g.c.d. has to be a monic polynomial.

By reversing the above process, start with equation (2) and then consider equation (1).

$$\begin{aligned} 1 &= 3(3x^2+2x-3) - 3(x+2)\cdot(3x-4) \\ &= 3(3x^2+2x-3) - 3(3x-4)\cdot[(x^6+3x^5+4x^2-3x+2) \\ &\qquad -(3x^2+2x-3)\cdot(5x^4+5x^2-x)] \\ &= (3x^2+2x-3)[3+3(3x-4)(5x^4+5x^2-x)] \\ &\qquad -3(3x-4)(x^6+3x^5+4x^2-3x+2) \end{aligned}$$

Hence

$$\begin{aligned} r(x) &= -3(3x-4) = -2x+5 = 5x+5 \\ s(x) &= 3+3(3x-4)(5x^4+5x^2-x) \\ &= 3x^5+3x^4+3x^3+x^2+5x+3 \end{aligned}$$

Practice Exercise XIV

1. Verify whether the polynomial is reducible or irreducible. If it is reducible, obtain the factors.
   (i) $5x^2-49$ in $Q[x]$, $\mathbb{R}[x]$
   (ii) $5x^2+2x+6$ in $\Re[x]$, $\mathbb{C}[x]$
2. Factorize
   (i) x^3-7x+6 over Q
   (ii) x^3-2x^2+4x+7 over $\Re$, $\mathbb{C}$.
3. Find the values of a and b if the function
   $$3x^4+ax^3+12x^2+bx+4$$
   (i) is exactly divisible by $(x-1)$, and
   (ii) leaves remainder 19 when divided by $(x+2)$.

4. Find a polynomial in x of the second degree which takes the values $\frac{1}{p}$, $\frac{1}{p+1}, \frac{1}{p+2}$ if x takes the values of 0,1,2, respectively. Show that its value is $\dfrac{p+2}{p(p+1)}$ when $x = p+2$.

Summary

Polynomials are first defined in terms of

(i) the indeterminate or variable
(ii) the coefficients from any ring or field
(iii) the degree
(iv) the constant term and the leading term.

Different polynomials are also considered such as

(a) constant polynomial
(b) monic polynomial
(c) reducible and irreducible polynomials with respect to the underlying field.

Addition and multiplication are defined which turns $F[x]$ into a commutative ring with identity if F is a field.

The following concepts are studied

1. Division algorithm and its application to the expression of the g.c.d. of two polynomials as a linear combination of the polynomials.
2. Factor and Remainder Theorems with applications to the factorization of polynomials.
3. Rational Root Theorem
4. Fundamental Theorem of Algebra
5. Factors and divisors; common factor and common divisors; h.c.f. and g.c.d. of polynomials.

Post-Test

See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.

LECTURE FIFTEEN

Rational Functions

Introduction
We shall consider the set $F(x)$ of all rational functions in a variable x and with coefficients in a field F. We shall show that every rational function can be expressed as a sum of a polynomial and a proper rational function. Also we shall see how certain rational functions can be split into a sum of partial fractions, which are useful in:

(i) integration of rational functions in calculus.

(ii) finding polynomial approximations to rational functions, and

(iii) finding the turning values of rational functions.

Objectives
The reader should be able to:

(i) express a rational function as a sum of a polynomial and a proper rational function; and

(ii) resolve certain rational functions into a sum of partial fractions.

Pre-Test
Resolve into partial fractions over the field of real numbers

1. $\dfrac{1}{a^2 - x^2}$ 2. $\dfrac{2(6r+1)}{(4r^2-1)(2r+3)}$

3. $\dfrac{3x^2}{1+x^3}$ 4. $\dfrac{2x^3}{x^2 - 5x + 6}$

Express in partial fractions with constant numerators only over the field of real numbers.

5. $\dfrac{x+3}{(2x-1)^2(x+2)}$ 6. $\dfrac{x^2 - 4x + 5}{(3x-1)^3(x+3)}$

Split into partial fractions with constant numerators only over the field of complex numbers

7. $\dfrac{z - 1 + 2i}{z^2 + 1}$ 8. $\dfrac{z^7}{(z - 3i)^2}$

Resolve into two partial proper fractions

9. $\dfrac{3x^2 + 4}{(x^5 + x^4 + x^3 + x^2 + x + 1)(4x^2 + 3x + 2)}$ over Z_{11}

10. $\dfrac{3x^2 + 5}{(x^6 + 3x^5 + 4x^2 - 3x + 2)(3x^2 + 2x - 3)}$ over Z_5.

Definition

A *rational function* in a variable x over a field F is an expression of the form

$$\frac{f(x)}{g(x)}, \quad g(x) \neq 0$$

where $f(x)$ and $g(x)$ are two distinct polynomial functions in $F[x]$. The polynomials $f(x)$ and $g(x)$ are distinct in the sense that one is not a constant multiple of the other. We shall denote by $F(x)$, the set of all rational functions in a variable x with coefficients in the field F.

A rational function is not defined for values for x satisfying $g(x) = 0$. We can always reduce any rational function in $F(x)$ to its simplest form by dividing the numerator and the denominator by any common factor of degree ≥ 1.

Proper rational functions

A rational function $f(x)/g(x) < F(x)$ such that $\deg f(x) < \deg g(x)$ is called a *proper* rational function. If however, $\deg f(x) \geq \deg g(x)$, then we can

divide $f(x)$ by $g(x)$, and by the division algorithm discussed in lecture 14, we can find unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = g(x) \cdot q(x) + r(x)$$

or

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

where $\deg r(x) < \deg g(x)$. Hence it follows that any rational function can be expressed as a sum of a polynomial function (possibly the zero polynomial) and a proper rational function.

Partial Fractions

Theorem. Consider the rational function $a(x)/b(x)$ in $F(x)$ such that $b(x) = g(x) \cdot h(x)$. If g.c.d. $(g(x), h(x)) = 1$, then

$$\frac{a(x)}{g(x) \cdot h(x)} = c(x) + \frac{r(x)}{g(x)} + \frac{s(x)}{h(x)}$$

where $c(x), r(x)$ and $s(x)$ are polynomials in $f[x]$, $\deg r(x) < degg(x)$ and $\deg s(x) < \deg h(x)$.

Proof. $(g(x), h(x)) = 1$ implies that there exists $u(x)$ and $v(x)$ in $F[x]$ such that

$$\begin{aligned} 1 &= u(x)g(x) + v(x)h(x) \\ \Rightarrow\ a(x) &= a(x)u(x)g(x) + a(x)v(x)h(x) \\ \Rightarrow\ \frac{a(x)}{g(x) \cdot h(x)} &= \frac{a(x)u(x)}{h(x)} + \frac{a(x)v(x)}{g(x)} \\ &= c(x) + \frac{s(x)}{h(x)} + \frac{r(x)}{g(x)} \end{aligned}$$

using the division algorithm, where $\deg s(x) < \deg h(x)$ and $\deg r(x) < \deg g(x)$.

Corollary
If $\deg a(x) < \deg b(x)$, then

$$\frac{a(x)}{f(x) \cdot h(x)} = \frac{x(s)}{h(x)} + \frac{r(x)}{g(x)}$$

where $\deg s(x) < \deg h(x)$, $\deg r(x) < \deg g(x)$.

Remark. The Theorem and Corollary show that a proper rational function of the form $a(x)/g(x) \cdot h(x)$ in $F(x)$ where $g(x)$ and $h(x)$ doe not have any common factor of degree ≥ 1, can be split into two proper rational functions in $F(x)$. One refers to this property as the *splitting* or *resolution* of a proper rational function into *proper fractions.*

Proposition (Cover-up Rule)

$$\frac{cx + d}{(x - a) + (x - b)} = \frac{A}{x - a} + \frac{B}{x - b},\ a \neq b$$

where

$$A = \frac{ac + d}{a - b} \qquad B = \frac{bc + d}{b - a}$$

Proof. $cx + d = \dfrac{ca + d}{a - b}(x - b) + \dfrac{cb + d}{b - a}(x - a)$.
Then divide by $(x - a)(x - b)$.

Remark. The cover-up rule is a rule for obtaining the constants A and B. For example to obtain A, we cover up the factor $(x - a)$ in the original rational function and then substitute $x = a$ in the remaining part. The rule can be generalised to any number of linear factors in the denominator, which are relatively prime.

Proposition

(i) $\dfrac{ax + b}{(x - c)^2} = \dfrac{a}{x - c} + \dfrac{ac + d}{(x - c)^2}$

(ii) $\dfrac{ax^2+bx+c}{(x-d)^3} = \dfrac{a}{x-d} + \dfrac{b+2ad}{(x-d)^2} + \dfrac{ad^2+bd+c}{(x-d)^3}$

Proof.

(i) $ax+b = a(x-c)+(ac+b)$
Then divide by $(x-c)^2$.

(ii) $ax^2+bx+c = a(x-d)^2+(b+2ad)(x-d)+ads^2+bd+c$.
Then divide by $(x-d)^3$.

Remark. The Proposition shows that we can split a proper rational functions, where the denominator consists of a repeated linear factor, into a sum of partial fractions with constant numerators only.

Example 1
Resolve into two partial fractions over the field $\mathbb{Z}_7$

$$\frac{3x^2+5}{(3x^3+2x-3)(x^6+3x^5+4x^2-3x+2)}$$

From Example 4 in Lecture 14, we have
g.c.d. $(3x^2+2x-3,\ x^6+3x^5+4x^2-3x+2) = 1$ and

$1 = (5x+5)(x^6+3x^5+4x^2-3x+2)+(3x^5+3x^4|3x^3+x^2+5x+3)\times(3x^3+2x-3)$

$$\begin{aligned}
\Rightarrow\ & \frac{3x^2+5}{3x^2+2x-3)(x^6+3x^5+4x^2-3x+2)} \\
= & \frac{(5x+5)(3x^2+5)}{3x^2+2x-3} + \frac{(3x^5+3x^4+3x^3+x^2+5x+3)(3x^2+5)}{x^6+3x^5+4x^2-3x+2} \\
= & \frac{x^3+x^2+4x+4}{3x^2+2x-3} + \frac{2x^7+2x^6+3x^5+4x^4+2x^3+4x+1}{x^6+3x^5+4x^2-3x+2} \\
= & \frac{4x+2}{3x^2+2x-3} + \frac{x^5+4x^4+x^3+2x+2}{x^6+3x^5+4x^2-3x+2}
\end{aligned}$$

Example 2
Split into partial fractions over the field of real numbers.

$$\frac{2}{x(x+1)(x+2)} = \frac{A}{x} + \frac{B}{x+1} + \frac{C}{x+2}$$

where, by the cover-up rule

$A = \dfrac{2}{1(2)} = 1$ (by covering x and putting $x = 0$)

$B = \dfrac{2}{-1(1)} = -2$ (by covering $x + 1$ and putting $x = -1$)

$C = \dfrac{2}{-2(-1)} = 1$ (by covering $x + 2$ and putting $x = -2$).

Example 3. Express in partial fractions with constant numerators only over the field of real numbers.

$$\frac{x^3 + 5x^2 + 4x + 5}{(x-1)(x^2-1)}$$

Notice that the rational fraction is not a proper one. So we use the division algorithm to obtain

$$\frac{x^3 + 5x^2 + 4x + 5}{(x-1)(x^2-1)} = 1 + \frac{6x^2 + 5x + 4}{(x-1)^2(x+1)} = 1 + \frac{f(x)}{(x-1)^2} + \frac{A}{x+1}$$

where by the cover-up rule

$$\begin{aligned} A &= \frac{6 - 5 + 4}{(-2)^2} = \frac{5}{4} \\ &\Rightarrow \quad 6x^2 + 5x + 4 = (x+1) \cdot f(x) + A(x-1)^2 \\ &\Rightarrow \quad (x+1) \cdot f(x) = 6x^2 + 5x + 4 - \frac{5}{4}(x-1)^2 \\ &\qquad\qquad = \frac{1}{4}(19x + 11)(x+1) \\ &\Rightarrow \quad f(x) = \frac{1}{4}(19x + 11) \end{aligned}$$

Now,

$$\frac{f(x)}{(x-1)^2} = \frac{19x + 11}{4(x-1)^2} = \frac{19}{4(x-1)} + \frac{15}{2(x-1)^2}$$

$$\Rightarrow \quad \frac{6x^2 + 5x + 4}{(x-1)^2(x+2)} = 1 + \frac{19}{4(x-1(} + \frac{15}{2(x-1)^2} + \frac{5}{4(x+1)}$$

Example 4
Resolve into partial fractions over the field of complex numbers

$$\frac{z^5}{z^2+a^2},\ (a \text{ is a real number})$$

By the division algorithm,

$$\begin{aligned}\frac{z^5}{z^2+a^2} &= z^3 - a^2 z + \frac{a^4 z}{z^2+a^2} \\ \frac{a^4 z}{z^2+a^2} &= \frac{a^4 z}{(z+ai)(z-ai)} \\ &= \frac{A}{z+ai} + \frac{B}{z-ai}\end{aligned}$$

where by the cover-up rule

$$\begin{aligned}A &= \frac{a^4(-ai)}{-2ai} = \frac{a^4}{2} \\ B &= \frac{a^4(ai)}{2ai} = \frac{a^4}{2} \\ &\Rightarrow \frac{x^5}{z^2+a^2} = z^3 - a^2 z + \frac{a^4}{2(z+ai)} + \frac{a^4}{2(z-ai)}\end{aligned}$$

Practice Exercise XV
Express in partial fractions.

1. $\dfrac{2x^2 - x + 1}{x^2 - x - 2}$ over $\Re$
2. $\dfrac{x-1}{(x+1)(x^2+1)}$ over $\Re$
3. $\dfrac{9}{(x-1)(7x+2)^2}$ over $\Re$
4. $\dfrac{z-3i}{z^3-1}$ over $\mathbb{C}$

5. $\dfrac{z-1}{(z+1)(z^2+1)}$ over $\mathbb{C}$.

Summary
We have considered rational functions over any field. A rational function can be expressed as a sum of a polynomial function and a proper rational function using the division algorithm for polynomials. Next we have studied proper rational functions with denominator as a product of relatively prime polynomials. Then such a proper rational function can be resolved or split into partial fractions each of which is a proper rational function.
In the special case when the denominator of the rational function consists of relatively prime linear factors, we have found that the splitting into partial fractions can be easily done using the cover-up rule.

Post-Test
See Pre-Test at the beginning of the Lecture.

References

1. Beachy, J. *Abstract Algebra*, A Study Guide for Beginners, 2000.

2. Clark, W.E. *Elementary Abstract Algebra*, Revised Dec. 2001.

3. Connell, E.H. *Elements of Abstract and Linear Algebra*, 2004.

4. Ilori, S.A. and O. Akinyele, *Elementary Abstract and Linear Algebra*, Ibadan University Press, Reprinted 2006.