Université de M'sila
Département de Mathématiques
Matière : Anglais (Master 1 – S1) , Spécialité : Algèbre et Mathématiques Discrètes Prof. L. Zedam

Lecture 1 (S1) : Basic concetpts of Discrete Mahematics (part 1)

I- Mathematics can be broadly classified into two categories :

- **Continuous Mathematics** : It is based upon continuous number line or the real numbers. It is characterized by the fact that between any two numbers, there are almost always an infinite set of numbers. For example, a function in continuous mathematics can be plotted in a smooth curve without breaks.
- **Discrete Mathematics** : It involves distinct values; i.e. between any two points, there are a countable number of points. For example, if we have a finite set of objects, the function can be defined as a list of ordered pairs having these objects, and can be presented as a complete list of those pairs.

II- Topics in Discrete Mathematics:

Although there cannot be a definite number of topics of Discrete Mathematics, the following topics are almost always covered in any study regarding this matter :

- Sets, Relations and Functions
- Mathematical Logic
- Group theory
- Counting Theory
- Probability
- Mathematical Induction and Recurrence Relations
- Graph Theory
- Trees (Mathematical sense)
- Boolean and Many valued Algebra; …..

III- Some basic concepts of Discrete Mahematics:

1- Set : A set is an unordered collection of different elements. A set can be written explicitly by listing its elements using set bracket. If the order of the elements is changed or any element of a set is repeated, it does not make any changes in the set.

Some Example of Sets

- A set of all positive integers
- A set of all the planets in the solar system
- A set of all the states in India
- A set of all the lowercase letters of the alphabet

Specification of sets:
There are four main ways to specify a set:
(1) by listing all its members (list notation);
(2) by stating a property of its elements (predicate notation);
(3) by defining a set of rules which generates (defines) its members (recursive rules).
(4) by stating a characteristic (or indexing) function of its elements (membership function);

The cardinal or the cardinality of a set S, denoted by |S|, is the number of its elements. The number is also referred as the cardinal number. If a set has an infinite number of elements, its cardinality is ∞.

Finite set: A set which contains a finite number of elements is called a finite set.

Infinite set: A set which contains infinite number of elements is called an infinite set.

Subset: A set *X* is a subset of set *Y* (Written as $X \subseteq Y$) if every element of *X* is an element of set *Y*.

Universal Set (universe set): It is a collection of all elements in a particular context or application. All the sets in that context or application are essentially subsets of this universal set.

Empty Set or Null Set: An empty set contains no elements. It is denoted by $\emptyset$. As the number of elements in an empty set is finite, empty set is a finite set. The cardinality of empty set or null set is zero.

Singleton set: Singleton set or unit set contains only one element. A singleton set is denoted by {s}{s}.

Power set: Power set of a set S is the set of all subsets of S including the empty set. The cardinality of a power set of a set S of cardinality *n* is 2^n. Power set is denoted as *P(S).*

Operations on Sets:

- ***Inclusion :*** If all the elements of a set A are also elements of a set B, then we say that A is a ***subset*** of B, and we write: $A \subseteq B$
- Two sets A and B are said to be ***equal*** if and only if they have exactly the same elements. In this case, we simply write: $A = B$
- The ***intersection*** of two sets A and B, written $A \cap B$, is the set of elements that are in A **and** in B.
- The ***union*** of two sets A and B, written $A \cup B$, is the set of elements that are in A **or** in B (or both).
- The ***difference*** of two sets A and B (also known as the ***set-theoretic difference*** of A and B, or the ***relative complement*** of B in A) is the set of elements that are **in** A **but not in** B. This is written $A - B$, or sometimes $A \setminus \mathrm{B}$.
- The ***Symmetric difference*** of sets A and B, denoted $A \vartriangle B$, is the set of all objects that are a member of exactly one of A and B (elements which are in one of the sets, but not in both). For instance, for the sets $\{1, 2, 3\}$ and $\{2, 3, 4\}$, the symmetric difference set is $\{1, 4\}$. It is the set difference of the union and the intersection, $(A \cup B) \setminus (A \cap B)$ or $(A \setminus B) \cup (B \setminus A)$.
- The set of elements that are **not** in a set A is called the ***complement*** of A. It is written A' (or sometimes A^C, or $\bar{A}$).
- ***Cartesian product*** of A and B, denoted $A \times B$, is the set whose elements (or members) are all possible ordered pairs (a, b) where a is an element of A and b is an ele,ent of B. The cartesian product of $\{1, 2\}$ and {red, white} is {(1, red), (1, white), (2, red), (2, white)}.

2- Relation: Whenever sets are being discussed, the relationship between the elements of the sets is the next thing that comes up. **Relations** may exist between objects of the same set or between objects of two or more sets.

A binary relation R from a set X to a set Y (written as xRy or R(x,y)) is a subset of the Cartesian product X×Y. If the ordered pair of R is reversed, the relation also changes.

Generally an n-ary relation R between sets $A_1,\dots,$ and A_n is a subset of the n-ary product $A_1\times\cdots\times A_n$

If $X=Y$, then R is called a binary relation on X. If $A_1= A_2\dots= A_n$, then R is called an n-ary relation on X.

- The **domain** of R, denoted by *Dom(R)*, is the set $\{x \mid (x,y) \in R$ for some y in$B\}$;
- The **range** of R, denoted by *Rang(R),* is the set $\{y \mid (x,y) \in R$ for some x in$A\}$.

Some properties of the relations on a set X: reflexivity, irreflexivity, symmetry, asymmetry , anti-symmetry, transitivity, …… .

Particular classes of relations: oreder relaion, preorder relation, pseudo order relation, tolerance relation, equivalence relation, … .

3- Function : A function or a mapping (defined as f: X→Y) is a relationship from elements of one set X to elements of another set Y (X and Y are non-empty sets). X is called Domain and Y is called Codomain of function '*f*'. Function 'f' is a relation on X and Y such that for each x∈X, there exists a unique y∈Y such that (x,y)∈R. 'X' is called pre-image and 'Y' is called image of function f. **A function can be one to one or many to one but not one to many.**

A function f:A→B is surjective (onto) if the image of f equals its range. Equivalently, for every b∈B, there exists some a∈A such that f(a)=b. This means that for any y in B, there exists some x in A such that y=f(x).

A function f:A→B is injective or one-to-one function if for every b∈B, there exists at most one a∈A such that f(a)=b. This means a function **f** is injective if $a_1 \neq a_2$ implies f(a1)≠f(a2).

A function f:A→B is bijective or one-to-one correspondent if and only if **f** is both injective and surjective.

The inverse of a one-to-one corresponding function $f{:}A\to B$, is the function $g{:}B\to A$, holding the following property : $f(x)=y \Leftrightarrow g(y)=x$. The function f is called **invertible**, if its inverse function g exists.

Université de M'sila
Département de Mathématiques
Matière : Anglais (Master 1 – S1) , Spécialité : Algèbre et Mathématiques Discrètes Prof. L. Zedam

Lecture 2 (S1) : Basic concetpts of Discrete Mahematics (part 2)

4- Graph: The graph theory is the study of *graphs*, which are mathematical structures used to model pairwise relations between objects. A graph in this context is made up of *vertices*, *nodes*, or *points* which are connected by *edges*, *arcs*, or *lines*. A graph may be *undirected*, meaning that there is no distinction between the two vertices associated with each edge, or its edges may be *directed* from one vertex to another; see Graph (discrete mathematics) for more detailed definitions and for other variations in the types of graph that are commonly considered. Graphs are one of the prime objects of study in discrete mathematics.

A graph is an ordered pair *G* = (*V*, *E*) comprising a set *V* of *vertices* or *nodes* or *points* together with a set *E* of *edges* or *arcs* or *lines*, which are 2-element subsets of *V* (i.e. an edge is associated with two vertices, and that association takes the form of the unordered pair comprising those two vertices). To avoid ambiguity, this type of graph may be described precisely as undirected and simple.

The vertices belonging to an edge are called the *ends* or *end vertices* of the edge. A vertex may exist in a graph and not belong to an edge.

V and *E* are usually taken to be finite, and many of the well-known results are not true (or are rather different) for infinite graphs because many of the arguments fail in the infinite case. The *order* of a graph is |*V*|, its number of vertices. The *size* of a graph is |*E*|, its number of edges. The *degree* or *valency* of a vertex is the number of edges that connect to it, where an edge that connects a vertex to itself (a loop) is counted twice.

5- Number Theory: number theory, or in older term **"arithmetic"**, is a branch of pure mathematics devoted primarily to the study of the integers. It is sometimes called "The Queen of Mathematics" because of its foundational place in the discipline. Prime numbers (A prime number is a number p whose only factors are 1 and p) and prime factorization are especially important in number theory, as well as the properties of objects made by the integers (e.g., rational numbers) or defined as generalizations of the integers, e.g., algebraic integers (algebraic numbers).

Here are some familiar and not-so-familiar examples:

odd 1, 3, 5, 7, 9, 11, . . . even 2, 4, 6, 8, 10, . . . square 1, 4, 9, 16, 25, 36, . . . cube 1, 8, 27, 64, 125, . . . prime 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, . . . composite 4, 6, 8, 9, 10, 12, 14, 15, . . . 1 (modulo 4) 1, 5, 9, 13, 17, 21, 25, . . . 3 (modulo 4) 3, 7, 11, 15, 19, 23, . . . triangular 1, 3, 6, 10, 15, 21, . . . perfect 6, 28, 496, . . . Fibonacci 1, 1, 2, 3, 5, 8, 13, 21, . . .

Integers can be considered either in themselves or as solutions to equations (Diophantine geometry). Questions in number theory are often best understood through the study of analytical objects (e.g., the Riemann zeta function) that encode properties of the integers, primes or other number-theoretic objects in some fashion (analytic number theory). One may also study real numbers in relation to rational numbers, e.g., as approximated by the latter (Diophantine approximation).

An *algebraic number* is any complex number that is a solution to some polynomial equation $f(x)=0$ with rational coefficients; for example, every solution x of $x^3 +(11/5)x^2 +9=0$ is an algebraic number. Fields of algebraic numbers are also called *algebraic number fields*, or shortly *number fields*. Algebraic number theory studies algebraic number fields. Thus, analytic and algebraic number theory can and do overlap: the former is defined by its methods, the latter by its objects of study.

6- Algebraic curve: an algebraic curve over a field ***K*** is an equation of the form $f(x,y) = 0$, where $f(x,y)$ is a polynomial in ***x*** and ***y*** with coefficients in ***K***. In other words: is the set of points on the Euclidean plane whose coordinates are zeros of some polynomial of two variables. A nonsingular algebraic curve is an algebraic curve over ***K*** which has no singular points over ***K***. A point on an algebraic curve is simply a solution of the equation of the curve. A ***K***-rational point is a point *(x,y)* on the curve, where ***x*** and ***y*** are in the field ***K***.

Above we have considered curves defined over a field ***K***. If the coefficients of the defining equation of the curve are in ***R***, we shall call real (algebraic) curves. When the coefficients of the defining equation are in ***C*** we speak of a complex (algebraic) curve.

7- Combinatorics: is the mathematics of counting and arranging. Of course, most people know how to count, but combinatorics is often concerned with how things are arranged. In this context, an **arrangement** is a way of objects could be grouped.

8- Permutation: a permutation is an arrangement of objects with regard to order. For a given finite set S. A permutation of S is a one-to-one mapping of S onto itself.
To specify a particular permutation we list the elements of ***A*** and, under them, show where each element is sent by the one-to-one mapping. For example, if A = {a, b, c} a possible permutation σ would be σ $=\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$. By the permutation σ, ***a*** is sent to ***b***, ***b*** is sent to ***c***, and ***c*** is sent to ***a***. The condition that the mapping be one-to-one means that no two elements of ***A*** are sent by the mapping into the same element of ***A***.

If ***S*** is a set of ***n*** distinct objects, then the number of permutations of those objects is ***n***! (***n*** factorial)

Université de M'sila
Département de Mathématiques
Matière : Anglais (Master 1 – S1) , Spécialité : Algèbre et Mathématiques Discrètes **Prof. L. Zedam**

Lecture 3 (S1) : Finite Fields, Polynomial.

1- Finite Fields :

A **finite field** or **Galois field** (so-named in honor of Évariste Galois) is a field that contains a finite number of elements. As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules. The most common examples of finite fields are given by the integers mod p when p is a prime number.

A finite field is a finite set on which the four operations multiplication, addition, subtraction and division (excluding division by zero) are defined, satisfying the rules of arithmetic known as the field axioms. The simplest examples of finite fields are the prime fields: for each prime number p, the field GF(p) (also denoted $\mathbf{Z}/p\mathbf{Z}$, $\mathbb{F}_p$, or $\mathbf{F}_p$) of order (that is, size) p is easily constructed as the integers modulo p.

The elements of a prime field may be represented by integers in the range $0, \ldots, p-1$. The sum, the difference and the product are computed by taking the remainder by p of the integer result. The multiplicative inverse of an element may be computed by using the extended Euclidean algorithm (see Extended Euclidean algorithm § Modular integers).

The number of elements of a finite field is called its *order*. A finite field of order q exists if and only if the order q is a prime power p^k (where p is a prime number and k is a positive integer). All fields of a given order are isomorphic. In a field of order p^k, adding p copies of any element always results in zero; that is, the characteristic of the field is p.

In a finite field of order q, the polynomial $X^q - X$ has all q elements of the finite field as roots. The non-zero elements of a finite field form a multiplicative group. This group is cyclic, so all non-zero elements can be expressed as powers of a single element called a primitive element of the field (in general there will be several primitive elements for a given field.)

A field has, by definition, a commutative multiplication operation. A more general algebraic structure that satisfies all the other axioms of a field but isn't required to have a commutative multiplication is called a division ring (or sometimes *skewfield*). A finite division ring is a finite field by Wedderburn's little theorem. This result shows that the finiteness condition in the definition of a finite field can have algebraic consequences.

Finite fields are fundamental in a number of areas of mathematics and computer science, including Number theory, Algebraic geometry, Galois theory, Finite geometry, Cryptography and Coding theory.

2- **Polynomial:** In mathematics, a **polynomial** is an expression consisting of variables and coefficients which only employs the operations of addition, subtraction, multiplication, and non-negative integer exponents. An example of a polynomial of a single variable x is $x^2 - 4x + 7$. An example in three variables is $x^3 + 2xyz^2 - yz + 1$.

Defenition : A polynomial is an expression that can be built from constants and symbols called indeterminates or variables by means of addition, multiplication and exponentiation to a non-negative power. Two such expressions that may be transformed, one to the other, by applying the usual properties of commutativity, associativity and distributivity of addition and multiplication are considered as defining the same polynomial.

A polynomial in a single indeterminate *x* can always be written (or rewritten) in the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

where $a_0, \ldots, a_n$ are constants and x is the indeterminate. The word "indeterminate" means that x does not represent any value, although any value may be substituted for it. The mapping that associates the result of this substitution to the substituted value is a function, called a *polynomial function*.

This can be expressed more concisely by using summation notation:

$$\sum_{i=0}^{n} a_i x^i$$

The word *polynomial* joins two diverse roots, the Greek *poly*, meaning "many," and the Latin *nomen*, or name. It was derived from the term *binomial* by replacing the Latin root *bi-* with the Greek *poly-*. The word *polynomial* was first used in the 17th century.

Polynomials appear in a wide variety of areas of mathematics and science. For example, they are used to form polynomial equations, which encode a wide range of problems, from elementary word problems to complicated problems in the sciences; they are used to define **polynomial functions**, which appear in settings ranging from basic chemistry and physics to economics and social science; they are used in calculus and numerical analysis to approximate other functions. In advanced mathematics, polynomials are used to construct polynomial rings and algebraic varieties, central concepts in algebra and algebraic geometry.

Université de M'sila
Département de Mathématiques
Matière : Anglais (Master 1 – S1) , Spécialité : Algèbre et Mathématiques Discrètes **Prof. L. Zedam**

Lecture 4 (S1) : Groups and Rings.

1- Groups: In mathematics, a **group** is an algebraic structure consisting of a set of elements equipped with an operation that combines any two elements to form a third element. The operation satisfies four conditions called the group axioms, namely closure, associativity, identity and invertibility. One of the most familiar examples of a group is the set of integers together with the addition operation, but the abstract formalization of the group axioms, detached as it is from the concrete nature of any particular group and its operation, applies much more widely. It allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics.

Definition. A group is a set, G, together with an operation • (called the group law of G) that combines any two elements a and b to form another element, denoted a • b or ab. To qualify as a group, the set and operation, (G, •), must satisfy four requirements known as the group axioms:[5]
Closure: For all a, b in G, the result of the operation, a • b, is also in G.
Associativity: For all a, b and c in G, (a • b) • c = a • (b • c).
Identity element: There exists an element e in G, such that for every element a in G, the equation e • a = a • e = a holds. Such an element is unique (see below), and thus one speaks of the identity element.
Inverse element: For each a in G, there exists an element b in G such that a • b = b • a = e, where e is the identity element.

Elementary consequences of the group axioms: Basic facts about all groups that can be obtained directly from the group axioms are commonly subsumed under *elementary group theory*.[24] For example, repeated applications of the associativity axiom show that the unambiguity of $a \bullet b \bullet c = (a \bullet b) \bullet c = a \bullet (b \bullet c)$ generalizes to more than three factors. Because this implies that parentheses can be inserted anywhere within such a series of terms, parentheses are usually omitted.

Uniqueness of identity element and inverses: Two important consequences of the group axioms are the uniqueness of the identity element and the uniqueness of inverse elements. There can be only one identity element in a group, and each element in a group has exactly one inverse element. Thus, it is customary to speak of *the* identity, and *the* inverse of an element.
To prove the uniqueness of an inverse element of a, suppose that a has two inverses, denoted b and c, in a group $(G, \bullet)$. Then

$$\begin{aligned} b &= b \bullet e && \text{as } e \text{ is the identity element} \\ &= b \bullet (a \bullet c) && \text{because } c \text{ is an inverse of } a, \text{ so } e = a \bullet c \\ &= (b \bullet a) \bullet c && \text{by associativity, which allows to rearrange the parentheses} \\ &= e \bullet c && \text{since } b \text{ is an inverse of } a, \text{ i.e. } b \bullet a = e \\ &= c && \text{for } e \text{ is the identity element} \end{aligned}$$

The two extremal terms b and c are equal, since they are connected by a chain of equalities. In other words, there is only one inverse element of a. Similarly, to prove that the identity element of a group is unique, assume G is a group with two identity elements e and f. Then $e = e \bullet f = f$, hence e and f are equal.

Division: In groups, the invertibility of the group action means that division is possible: given elements a and b of the group G, there is exactly one solution x in G to the equation $x \bullet a = b$. In fact, right multiplication of the equation by a^{-1} gives the solution $x = x \bullet a \bullet a^{-1} = b \bullet a^{-1}$. Similarly there is exactly one solution y in G to the equation $a \bullet y = b$, namely $y = a^{-1} \bullet b$. If the • operation is commutative, we get that $x = y$. If not, x may be different from y.

2- Rings: Rings are one of the fundamental algebraic structures used in abstract algebra. It consists of a set equipped with two binary operations that generalize the arithmetic operations of addition and multiplication. Through this generalization, theorems from arithmetic are extended to non-numerical objects such as polynomials, series, matrices and functions.

Definition. A ring is a set R equipped with binary operations[1] + and · satisfying the following three sets of axioms, called the ring axioms.

1. R is an abelian group under addition, meaning that
   - $(a + b) + c = a + (b + c)$ for all a, b, c in R (+ is associative).
   - $a + b = b + a$ for all a, b in R (+ is commutative).
   - There is an element 0 in R such that $a + 0 = a$ for all a in R (0 is the additive identity).
   - For each a in R there exists $-a$ in R such that $a + (-a) = 0$ ($-a$ is the additive inverse of a).
2. R is a monoid under multiplication, meaning that:
   - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in R (· is associative).
   - There is an element 1 in R such that $a \cdot 1 = a$ and $1 \cdot a = a$ for all a in R (1 is the multiplicative identity).[5]
3. Multiplication is distributive with respect to addition:
   - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all a, b, c in R (left distributivity).
   - $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all a, b, c in R (right distributivity).

The conceptualization of rings started in the 1870s and completed in the 1920s. Key contributors include Dedekind, Hilbert, Fraenkel, and Noether.

Dedekind: The study of rings originated from the theory of polynomial rings and the theory of algebraic integers.[7] In 1871, Richard Dedekind defined the concept of the ring of integers of a number field.[8] In this context, he introduced the terms "ideal" (inspired by Ernst Kummer's notion of ideal number) and "module" and studied their properties. But Dedekind did not use the term "ring" and did not define the concept of a ring in a general setting.

Hilbert: The term "Zahlring" (number ring) was coined by David Hilbert in 1892 and published in 1897.[9] In 19th century German, the word "Ring" could mean "association", which is still used today in English in a limited sense (e.g., spy ring),[10] so if that were the etymology then it would be similar to the way "group" entered mathematics by being a non-technical word for "collection of related things". According to Harvey Cohn, Hilbert used the term for a ring that had the property of "circling directly back" to an element of itself.[11] Specifically, in a ring of algebraic integers, all high powers of an algebraic integer can be written as an integral combination of a fixed set of lower powers, and thus the powers "cycle back". For instance, if $a^3 - 4a + 1 = 0$ then $a^3 = 4a - 1$, $a^4 = 4a^2 - a$, $a^5 = -a^2 + 16a - 4$, $a^6 = 16a^2 - 8a + 1$, $a^7 = -8a^2 + 65a - 16$, and so on; in general, a^n is going to be an integral linear combination of 1, a, and a^2.

Fraenkel and Noether: The first axiomatic definition of a ring was given by Adolf Fraenkel in 1914,[12][13] but his axioms were stricter than those in the modern definition. For instance, he required every non-zero-divisor to have a multiplicative inverse.[14] In 1921, Emmy Noether gave the modern axiomatic definition of (commutative) ring and developed the foundations of commutative ring theory in her monumental paper *Idealtheorie in Ringbereichen*.[15]