Discrete Structure

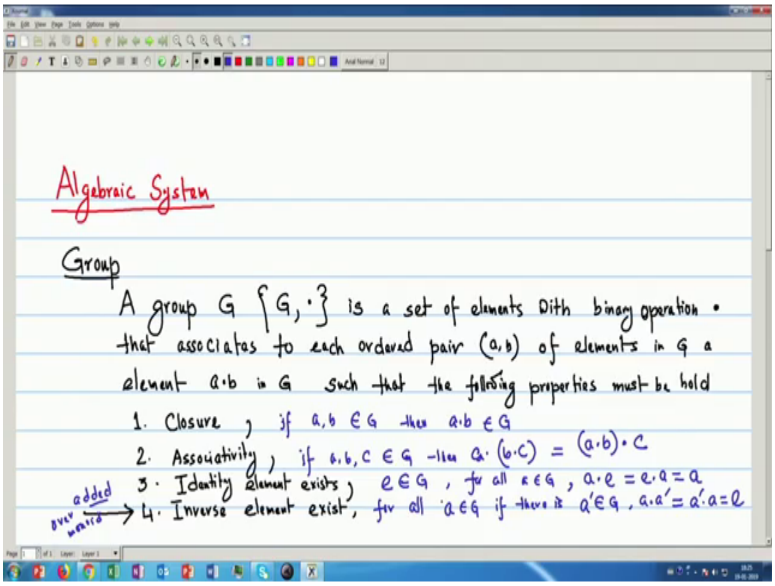
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 49
Algebraic Structures (Contd.)

We are discussing the Algebraic Structures and we have defined the algebraic systems as set of finite set of elements which is non-empty and some binary operations or some unary operations in unit that operates on this set. We have also read some general properties of algebraic systems, and mainly now what we are doing that we are trying to identify or to form to define the different algebraic systems depending on the properties that they satisfy.

We have already read the semi groups and monoids the simplest algebraic systems now today we will read the group which is the most important algebraic systems or we can tell the algebra and which have a number of application arrears in almost all the streams of engineering mathematics in computer science. So, we will read the group today as an algebraic system.

(Refer Slide Time: 01:50)



Algebraic System

Group

A group G $\{G, \cdot\}$ is a set of elements Dith binary operation $\cdot$ that associates to each ordered pair (a, b) of elements in G a element $a \cdot b$ in G such that the following properties must be hold

1. Closure, if $a, b \in G$ then $a \cdot b \in G$
2. Associativity, if $a, b, c \in G$ then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. Identity element exists, $e \in G$, for all $a \in G$, $a \cdot e = e \cdot a = a$
4. Inverse element exist, for all $a \in G$ if there is $a' \in G$, $a \cdot a' = a' \cdot a = e$

Now, if we remember though we have read the general properties of algebraic systems as the closure property, the associative property, the commutative property, the identity and the inverse. Now, the semi group and the monoid that we have defined that mainly they followed or they satisfy the property of closures, then associative and if the identity element it has then it is a monoid otherwise it is a semi group.

Now, group is a you can define that again this is algebraic system which actually satisfies the all three properties that the monoid satisfies; that means, the closure, associativity and the identity element it has. Now, in addition if it has the inverse element then we will tell it this as a group.

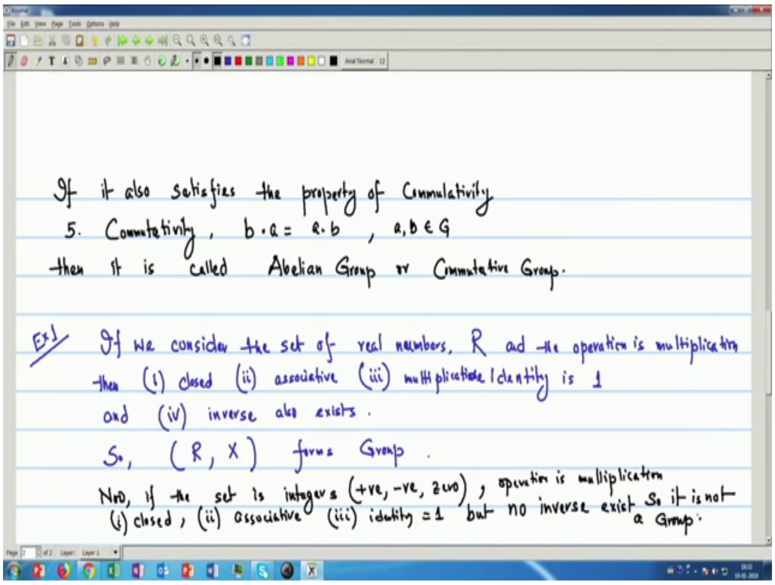
So, we define write in that the a group G we give the notation like that, as if G is the set of element and dot is the operation. So, is a set of elements with binary operation dot that associates to each ordered where a, b of the set G of a element a dot b where dot is the operation that we have defined. So, a dot b and that is also in G; such that the following properties must be hold.

Now, the properties are one that the closure; that means, if a, b belongs to G then a dot b belongs to G. Then associative; that means, if a, b, c belongs to G then a dot b dot c is same as that a dot b dot c. 3 is our identity element; that means there is an element e exists, an elements e belongs to G then for all a belongs to G a dot e equal to e dot a is a only. Now, up to these three properties we have seen and that then if it holds then we call this is monoid.

Now, in addition if the system has some inverse element exists; that means, for all a belongs to G, if there is an element a dash belongs to G such that a dot a dash a dot a dash equal to the a dash dot a is the identity element only. Now, see we have only these properties we have added. This is my added property with monoid, added over monoid and we tell that then this forms a group.

Now, if the group of satisfies the commutative property also then it is called an abelian group or the commutative group as we have defined in form monoid and the semi group.

(Refer Slide Time: 09:37)



If it also satisfies the property of Commulativity

5. Commutativity, $b \cdot a = a \cdot b$, $a, b \in G$

then it is called Abelian Group or Commutative Group.

Ex) If we consider the set of real numbers, R and the operation is multiplication

then (i) closed (ii) associative (iii) multiplicatiode Identity is 1

and (iv) inverse also exists.

So, $(R, \times)$ forms Group.

Now, if the set is integers (+ve, -ve, zero), operation is multiplication

(i) closed, (ii) associative (iii) identity = 1 but no inverse exist So it is not a Group.

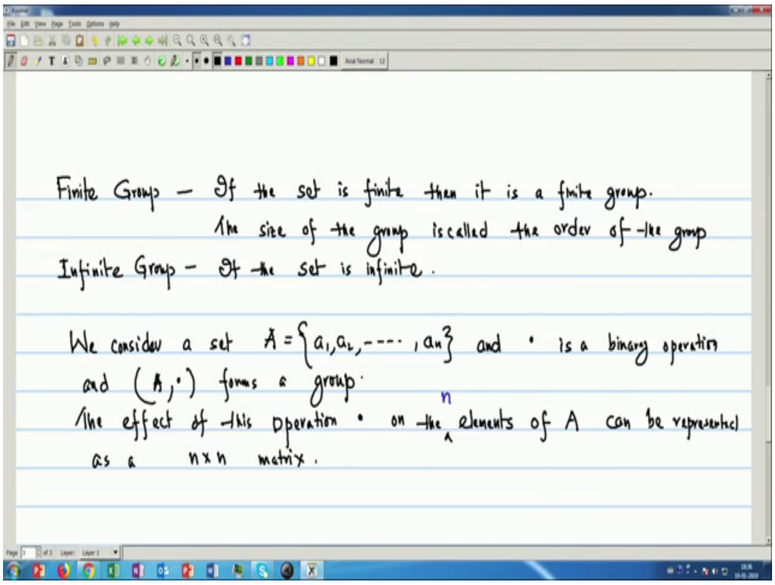
So, if it also satisfies the property of computability; that means, that is the property. I write that 5, that b dot a equal to a dot b for a, b belongs to G then it is a called an abelian group or we can tell this is a commutative group.

Now, we see one simple example that if my set is; one simple example you see if the set is a real number normally we define the denote that is a R and the operation is multiplication then it is the closed, since if I take two real number and if we multiply that is also an element of a the set R. It is associative with real numbers the associative property also holds because in final result is an real number that is also an element of R. So, this is associative.

Then the identity element exists and we know the multiplicative identity is one, multiplicative identity is 1 and now, the inverse also exists. Since it is a real number so, the inverse also exists. So, it forms a group. So, R with multiplication forms an algebraic system, it is a group.

Now, if instead of this R the real number if we consider the set, now if the set is integers again positive, negative, with 0 and the operation is multiplication then it is closed, associative, identity exists that is equal to 1; multiplicative identity 1, but there is no inverse exists since it is the set of integers. So, but no inverse exists; so, it is not a group. So, integers so, it is not a group integers with multiplication as the operation it is not a group.

(Refer Slide Time: 16:00)



Finite Group – If the set is finite then it is a finite group.

The size of the group is called the order of the group

Infinite Group – If the set is infinite.

We consider a set $A = \{a_1, a_2, ----, a_n\}$ and $\cdot$ is a binary operation and $(A, \cdot)$ forms a group.

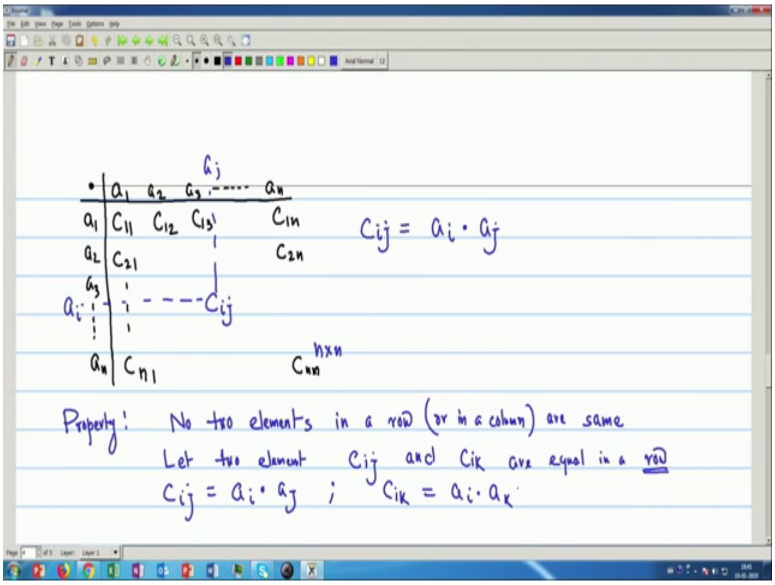
The effect of this operation $\cdot$ on the n elements of A can be represented as a $n \times n$ matrix.

Now, there are some other simple definition of groups we always we read, one is called the finite group, finite and infinite group. If the set is finite then it is a finite group and then the size of the group and in this case if it is a finite group the size of the group is called the order of the group, is called the order of the group. Now, if the set is infinite then it is a finite group. So, simply infinite or finite; it actually depends on whether if the set is finite or infinite. So, if the set is infinite; that means, the set has infinite number of elements.

Now, if you consider a set A say we consider some properties of group we know study. We consider is set A equal to say n number of elements it has and the say we say dot is a binary operation and a dot that means, a set with the binary operation dot forms a group.

Now, the effect of this operation of this operation dot on the elements of or the n number of elements of A that we can represent by a matrix. The elements of A or I can write on the n elements of because n element set so, n elements of a can be represented as a n by n matrix and we will see some properties if it is a group then from directly from the matrix how we can identify some of the properties group properties.

(Refer Slide Time: 20:00)



$$\begin{array}{c|cccccc} & & & & a_j & & \\ \cdot & a_1 & a_2 & a_3 & \cdots & \cdots & a_n \\ \hline a_1 & C_{11} & C_{12} & C_{13} & \vdots & & C_{1n} \\ a_2 & C_{21} & & & \vdots & & C_{2n} \\ a_3 & \vdots & & & \vdots & & \\ a_i & \vdots & \cdots & \cdots & C_{ij} & & \\ \vdots & \vdots & & & & & \\ a_n & C_{n1} & & & & & C_{nn} \end{array}^{n \times n}$$

$$C_{ij} = a_i \cdot a_j$$

Property: No two elements in a row (or in a column) are same

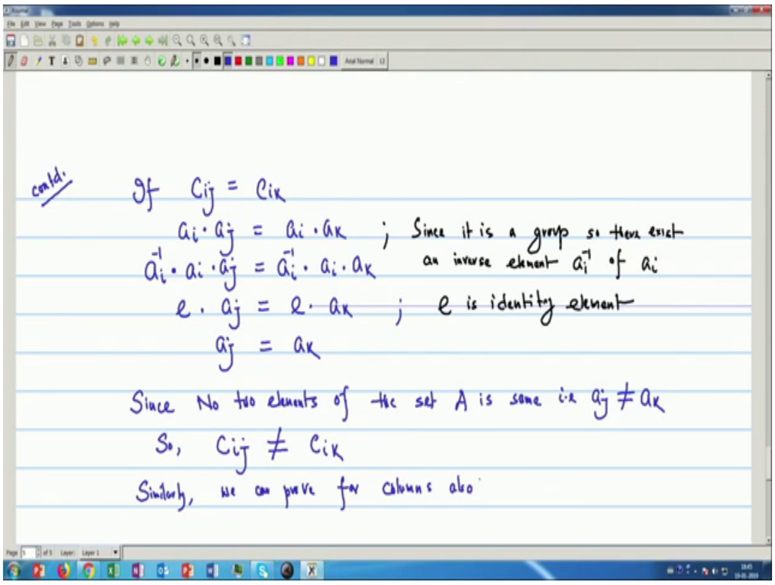
Let two element C_{ij} and C_{ik} are equal in a row

$C_{ij} = a_i \cdot a_j$; $C_{ik} = a_i \cdot a_k$

So, I can write in this way the matrix will be like I can give a 1, a 2, a 3 up to a n. We in the operation we give here and then again a 1, a 2, a 3 and then a n and this is we see this is n by n matrix. If we represent the elements that a 1 dot a 1 that the after operation if we represent this as a C 11, C 12, C 13, C 1 n, similarly 2 1 then I can write that C ij is a i dot a j; that means, if I consider some C ij here some C ij. So, here I will be getting that a i elements a i is here and as if some a j. So, C ij is a i dot a j.

Now, we identify some properties that each element here since it is a group. So, each element has an inverse. So, now, you give a property of a group that give a property that, no two elements in a row or in a column is same. Now, how we can show that thing? See if I have two elements say assume the two elements are same. So, let two elements C ij and C ik are equal or same in a row. We consider that in a row two elements are same. Now what is C ij? Now, C ij is a i dot a j and C ik is a i dot k.

(Refer Slide Time: 24:21)



contd.

If $C_{ij} = C_{ik}$

$a_i \cdot a_j = a_i \cdot a_k$; Since it is a group so there exist an inverse element a_i^{-1} of a_i

$a_i^{-1} \cdot a_i \cdot a_j = a_i^{-1} \cdot a_i \cdot a_k$

$e \cdot a_j = e \cdot a_k$; e is identity element

$a_j = a_k$

Since No two elements of the set A is same i.e $a_j \neq a_k$

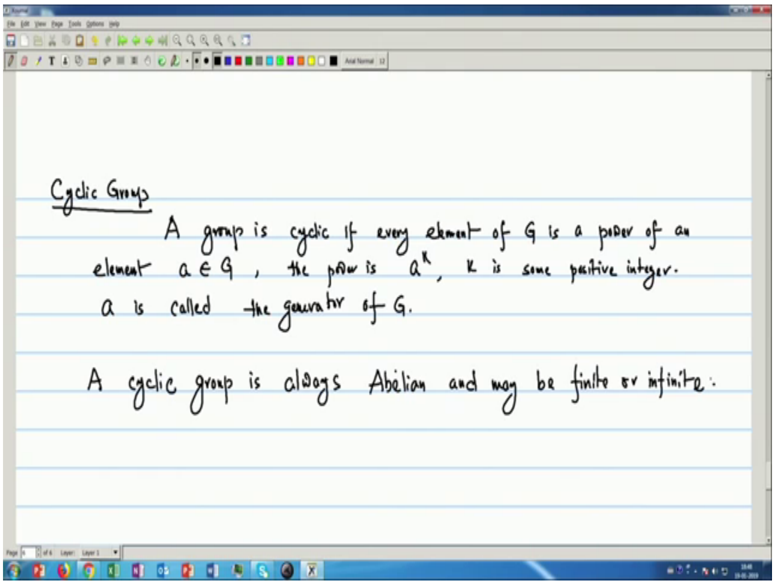
So, $C_{ij} \neq C_{ik}$

Similarly, we can prove for columns also.

Now, if we assume that C ij and C ik are same. Then now if C ij equals C ik; that means, a i dot a k, sorry a i dot a j is a i dot a k. Now, since it is a group so, there exists one inverse element and let these inverse element is for a i is a i inverse. So, we write since it is a group. So, there exist an inverse element of a i. So, I can write a i inverse dot a i dot a j is in both side we do the operation dot, then a i inverse a i is the identity element. So, e dot a j is e dot a k. Since this e is same element e dot a j is e dot a k, we know e dot a j is is a j only and e dot a k is a k only because that is my e is my identity element; e is identity element. So, then a j equal to a k.

Now, since it is a set, so, no two elements this a j and a k are same. So, since no two elements of the set a is same; that means, a i, a j not equal to a k. So, C ij not equal to C ik. So, no and similarly we can proof that for columns also, no two elements in a column are same. So, similarly we can proof for columns also.

(Refer Slide Time: 28:35)



Cyclic Groups

A group is cyclic if every element of G is a power of an element $a \in G$, the power is a^k, k is some positive integer.
a is called the generator of G.

A cyclic group is always Abelian and may be finite or infinite.

Now, as we have defined a cyclic monoid, here also we can define the cyclic group. The definition is same. The group is cyclic is a power of an element say a belongs to G and here a is called the and say the power is like, the power is a to the power K, where K is some integer positive integer and a is called the generator G.

Now, in property of a cyclic group is already we have this thing we have seen for monoid and here also it is same that a cyclic group is always commutative in nature; and maybe finite or infinite. So, we have read some on the definition of group, some properties of group and we will be continuing the group properties and some examples in our next lecture.