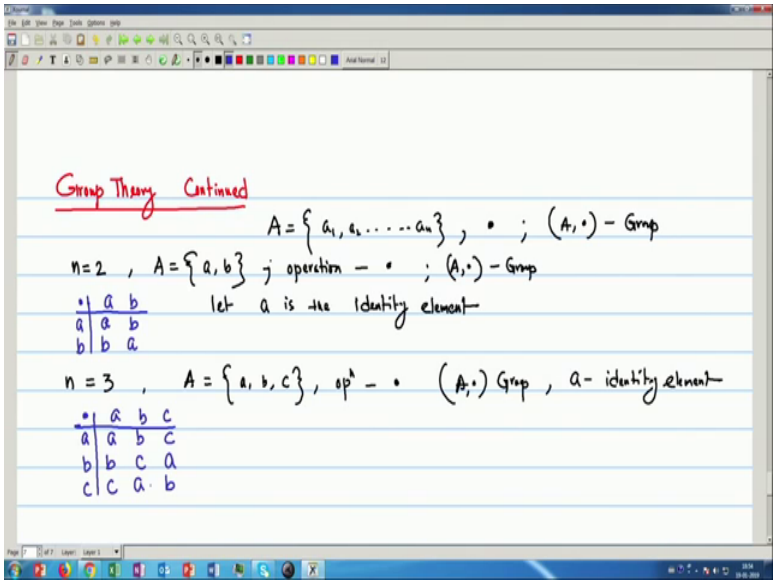
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 50
Algebraic Structures (Contd)

So, we are reading the properties of Group.

(Refer Slide Time: 00:26)



And we identify some more groups; so, Group Theory. See already we have seen that if A is one set. A is one set with n numbers of elements and one operations dot. So, that my A dot is from a group. Then, this elements with the operations can be represented by n by n matrix.

Now and also we have seen that no 2 rows or no 2 columns that are in two elements in a row or no to element column in identical. We have proved that thing. Now say we see if n is equal to 2; if n equal to 2; that means, my set has 2 elements and let this elements are A and B. These are the 2 element sets and we take the operation is operation is dot and A dot form a such that A dot form a group.

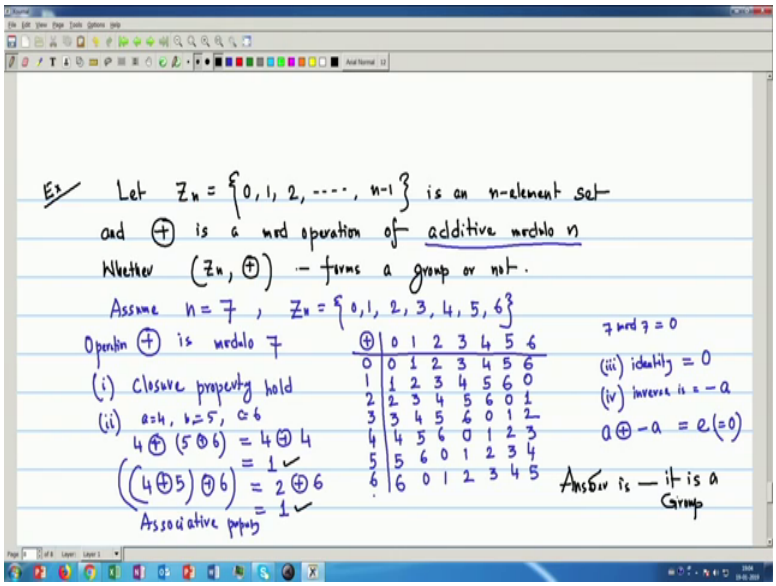
Now if I this will be 2 by 2 matrix and we see that we what will be the elements of the matrix. So, we represent like this now see a dot a; that means, I need a since it is a group it has some identity element and since it has 2 elements only. So, one must be the identity

element. So, let a is the a is the identity element; a is the identity element. So, we can write a dot a is a only. Now since a is identity means a dot b is b only. Now similarly b dot a is b only, since it is commutative that property also we have to seen and now if it is b dot b; then, it is b only. b dot b is the a because otherwise b, b will be the identity, since we have already assumed that is the identity element.

Now, if I continue this thing for n equal to 3. So, if it is n equal to 3 and my set is a b c; the 3 element set. Operation is as usual dot we see and a dot is the group and a is the identity element. Then, if I give then I have 3 elements, I give dot a b c. See a dot a since it is identity a, a dot b; b since it is identity, it is c.

Now, b dot a it is b only. Now, b dot b; b dot b I write it is c and b dot c, it is a and c dot a again c, then c dot b already b dot c is a. So, c dot b is a and c dot c is b. So, I get that the first row is a, b, c; then b, c, a and then c, a, b. So, with only 3 elements, but no 2 row and in the row no 2 elements in the row or column are equal. So, it holds the property, we have read ok. Now, we read one examples that see one example of group.

(Refer Slide Time: 05:30)



So, let Zn equal to 0, 1, 2 upto n minus 1; that means, there are n elements set Zn is an n-element set and we denote this operation is a modulo operation is a mod operation of additive modulo n and then, will say whether it forms a this set whether we check, whether Zn with modulo operation; whether this forms a group or not ok. Let we consider or we assume n equal to 7; that means, my Zn is 0, 2, 3, 4, 5, 6 since I will be

taking modulo 7 that my operation is operation is modulo 7. If you remember that modulo 7 means the number we if we divide by 7, we will be taking the reminder it will give that.

So, if you divide by 7 the reminder can be from 0 to 6 and that is my set. So, if I draw the group operation or the effect of this modulo operation on the set Zn in matrix notation just now what we have read. So, it will be the give 0, 1, 2 this is my modulo 7 because my set is upto 6. There are as upto 6 elements. Now if I because it is additive modulo, mod operation this a additive modulo n additive modulo n; that means, every time we will add and will be dividing by 7 and taking the reminder. That means 0 plus 0 divided by 7. Obviously, it will be 0 then 0 plus 1. So, since 0 is my identity element. So, I will be getting 1, 2, 3, 4, 5, 6 because all are less than 7. Now, since it is for I 1 plus 0 is becomes 1.

Because 1 divided by 7 reminder is my 1 modulo 7 is 1, 2; then, this because 3, 4, 5, 6. Now, 6 plus 1 is 7 and if I 7 modulo 7 if I take that becomes 0 because reminder 0. So, I give here 0. Now, 2 plus 0 is 2; 3, 4, 5, 6. Now again, 5 plus 2, 7; 7 modulo 7 becomes 0. Now, 6 plus 2, 8; 8 modulo 7 becomes 1. Similarly, we can fill up 3, 4, 5, 6, again 7 become 0; 8 becomes 1; 9 becomes 2. Then, 4, 5, 6, 7 becomes 0; 8 becomes 1; 2 this becomes 3. 5, 6 then 0, 1, 2, 3, 4; now, this 6 and now it becomes 4, 6, 6 12; 12 modulo 7 is 5. Now, we see we once you got the or the effects are the operations of modulo 7 of the set Zn; then, we see that my if I study then my matrix element are only 0 two 6.

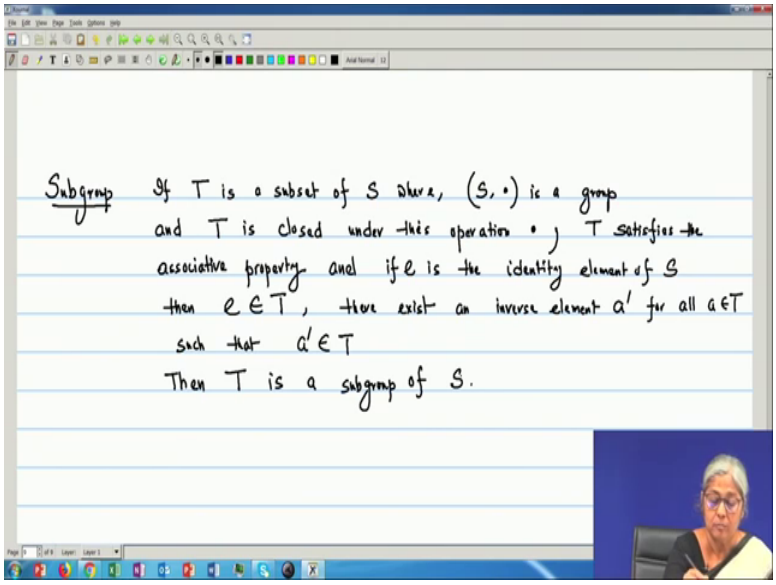
So, first thing is that it is, it holds a closure property. So, the closure property holds because my matrix elements are also elements are from lies between 0 to 6. Now, associative since it is addition. So, if I take any we can take a is 4, 5, 6; that means, a equal to 4; b is 5 and c is 6. So, I can take 4, 6 this is equal to 5, 6 11. So, this is this became 11 modulo 7; 11 modulo 7 is 4 and 4 modulo 4 8.

So, 8 modulo 8 modulo 7 is 1. Now, if I take 4 modulo 5; then modulo 6. So, 4, 5 this becomes 9 modulo 7 is 2; 2 modulo 6 plus 6 modulo 7; that means, 8 modulo 7 that is also 1. So, I have it this is equal. So, it forms a associative property. So, it holds associative property. Now, the 3 is identity element identity since it is additive modulo 7. So, identity exist and equal to 0 and inverse, this is that since it is additive.

So, inverse is sum minus a since it is additive modulo 0. So, we can take that if I take we will be getting some a and minus a is equal to the identity element e; that means, e minus a 0, this will be my and it is my identity equal to 0. So, inverse exist. So, it forms a group. So, it is a group no service.

So, my answer is it is a group. So, additive modulo 7 or additive now, we can generalise that additive modulo n on the set Zn 0, 1 to n minus 1 in n element that it will be a it always forms a group. Now, we see another property of group already we have defined the sub semi group sub monoid and similarly we can define the subgroup.

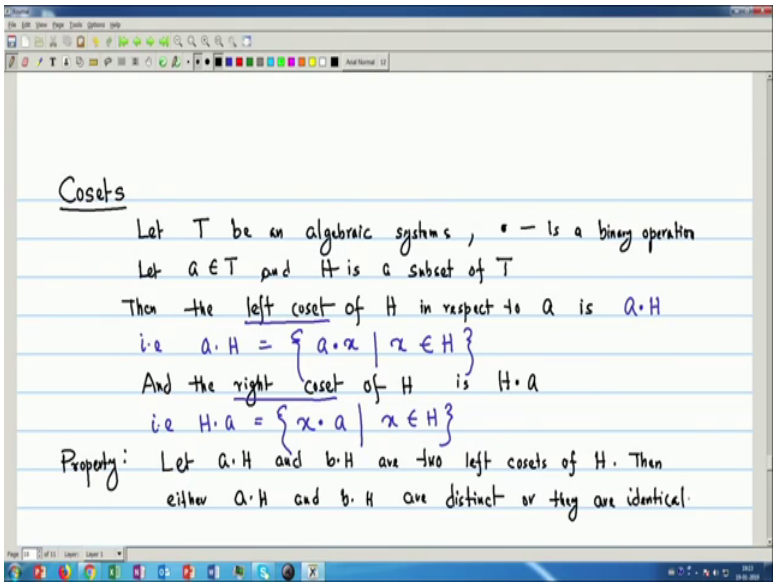
(Refer Slide Time: 16:00)



So, we will define similar way we can define the subgroup, if you remember that if T is a subset of S; where say S is dot is a group and T is closed under the operation dot T satisfies the associative property or and now the 2 property that identity and the inverse element that and the if e is the identity element of S since it is a group. So, it has some identity element; then e belongs to, then e belongs to T.

Then, if e belongs to T and about the inverse that there exist an inverse element a dash for all a belongs to T such that a dash also belongs to T. Then, T is a subgroup of S; T is a subgroup of S. Now, we read two properties; we actually define and then we will a give a theorem on this that it is called the Cosets and the Lagranges theorem on this.

(Refer Slide Time: 19:31)

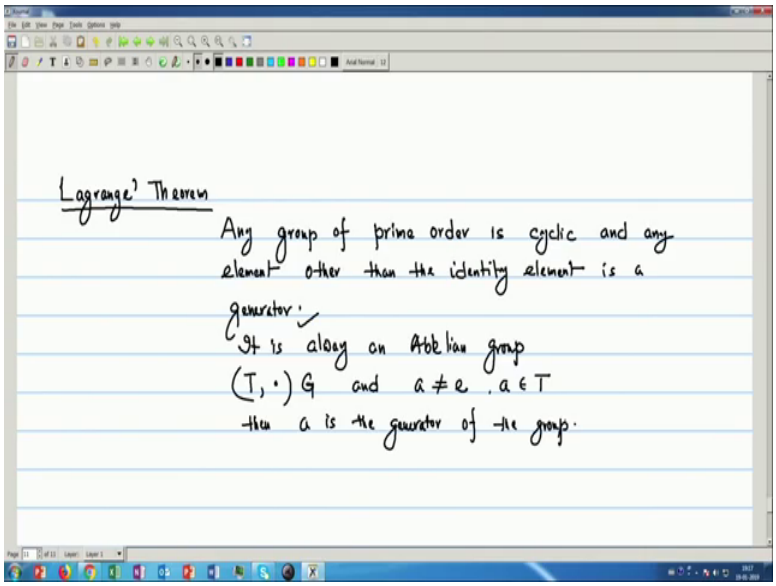


So, first we will define Cosets. So, let T be an algebraic systems and dot is the one is a binary operation. Now, let a belongs to T and H is a subset of T; then the left coset of H is defined as and always the coset is defined with respect to one element of T the original set here it is T. So, let us left coset of H in respect to a is a dot H; a is a dot H that is I can write a dot since H is a sub set. So, I can write a dot H equal to all the elements a dot x, where that all x belongs to all x belongs to H and dot is the binary operation that we have chosen.

Now, similarly the right coset of H in respect to a is H dot a that is we can write H dot a again since for all x element a and x belongs to H. So, this is the 2 things the left coset the left coset and the right coset of H; H, where H is a sub set of T. Now, we give a property on this one property we write on cosets.

So, let a dot H and b dot H are set two left cosets of H or some time we call cosets of H. Then, either a dot H and b dot H are distinct or they are identical and we can easily prove this property from earlier matrix representation and that what we have identified some property that no 2 elements in the row or in the column, they are equal and another thing we always remember that since it is a set. So, it is a distinct element; also if they are they either will be distinct or they are identical if they are not.

(Refer Slide Time: 25:21)

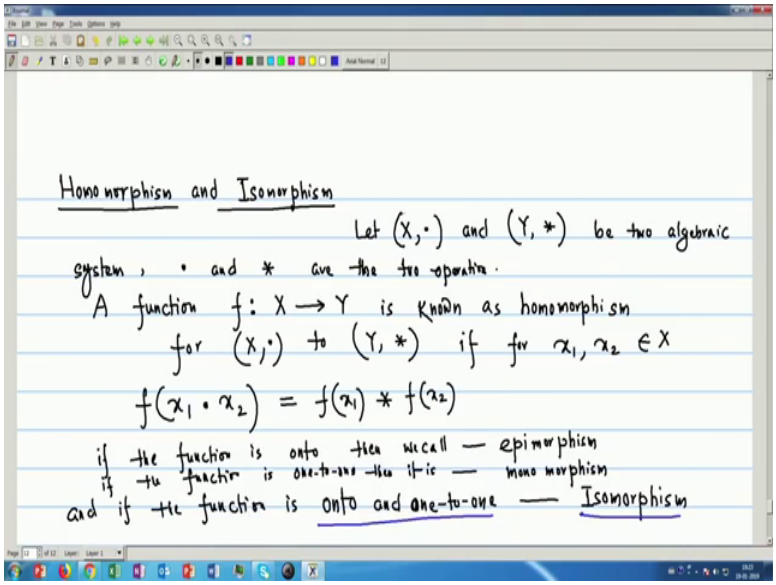


Now, we read the Lagrange's Theorem. Now, Lagrange's theorem tells about a of the property of the order of a group. If you remember the order we have defined that the size of a group and the group must be finite otherwise there is no concept of a size. So, it can write that any group the any group of prime order. So, it tells about the order and any group of prime order is cyclic and any element other than the identity element is a generator of that group, since it is a cyclic group. So, it has some generator and other than identity element every element any element can be the generator that means that is if we take the power of that particular element, it will generate the or it will produce the other elements.

So, this is very important when we will study some algebraic systems. Another thing is always that this is it also forms a Abelian group that it also follows it also follows the commutivity; that means, it is always an Abelian group. So, we can write that any T dot is a group and a not equal to the identity, then an a belongs to T. Then, a is the generator of the group. So, we have read the definition of group and the some properties and some theorems related to the order of the group. Now, since we have started our discussion with the algebraic structure and we have defined like that we have a set and operation defined on it and if you remember then that some relations on this function that gives you the algebraic structure.

Algebraic system is a set with the operation and then in addition if you consider some relations on this, then it will give algebraic structure. So, now, when we define the algebraic structures; so the relation between the one algebraic system to another algebraic system is very important and that we define with something call the Homomorphism and the another some other variety of Homomorphism.

(Refer Slide Time: 29:48)



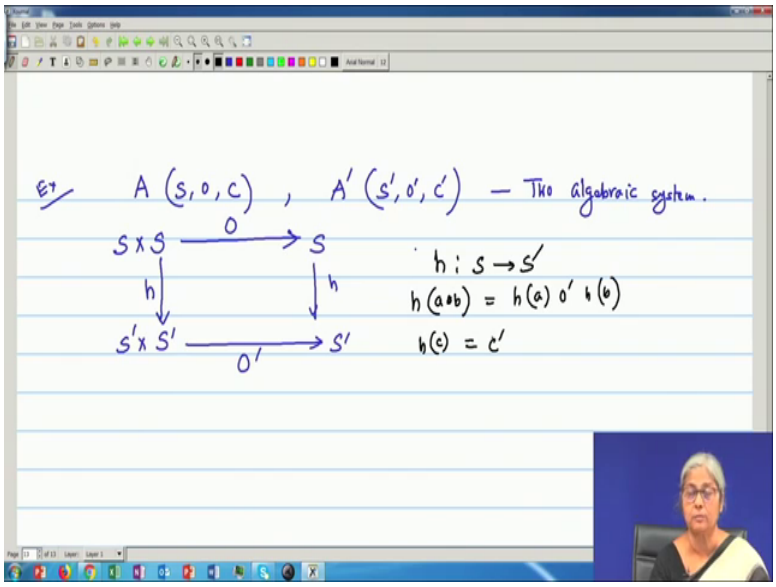
So, we define the mainly the two there are other varieties also the Homomorphism and another important is the Isomorphism. Homomorphism and Isomorphism the we will. So, that if two algebraic systems are isomorphic, then they are structurally similar.

So, homomorphism and isomorphism of it will give the definition that let since it gives a relation between 2 algebraic system. So, I consider 2 algebraic system X dot and say Y star; these are the two algebraic system and dot and star are the two operations. Now, a function if from one algebraic system from X to Y is known or is called Homomorphism right, we can write X is for X dot to Y star, if for sum x 1, x 2 belongs to x, we can write that the properties that f of x 1 f of x 1 dot x 2 the operations defined on x, this is equal to f of x 1 operations defined on y and f of x 2.

So, the function is these; then, we call that this is these two are homomorphism between X and Y and here on we can tell since it is a function. So, you know that if the function is onto, then the term is epimorphism. Then we then we call epimorphism.

If the function is one-to-one; then it is monomorphism; then it is monomorphism and if the function is one-to-one and onto; onto and one-to-one, then it is Isomorphism. So, now, it is clear that if it is onto and one-to-one; that means, they are structurally two algebraic systems, they are same or they are structurally similar; then we can tell that this is they are structurally similar in the algebraic system and they are isomorphic to each other.

(Refer Slide Time: 35:22)



We can we can take or we write in a different way that if we write that take one example that if A on S, O, C and one A dash S dash, O dash, C dash; these are two algebraic systems, then just with this thing we can write we graphically you can tell that if I take this as S; this is my O; S dash sorry S cross S to S and if I give say some homomorphic thing homomorphism say S dash. So, this becomes S dash by S dash, this is something O dash. So, this becomes S dash and again, this gives a h. So that means, here h is h is I can write h is S to S dash and h some 2 elements if I consider a dot b is h a, h a dash, h b dash the way we have defined and if I consider some constant, then that constant is h c equal to c dash.

So, this is the general definition homomorphism and it will graphically it will show in this nature. So, the way we started that actually the study of algebraic structures. So, in this lecture we have reads some algebraic systems like semi group monoid group and then, the how that form the relation between or the how from one algebraic system to

another algebraic system, we can get by applying some function and based on that the nature of the function whether it is onto one-to-one or onto and one-to-one, we get the whether the homomorphism that becomes the epimorphism or monomorphism or the isomorphism. So, mainly our focus is on isomorphic thing whether two algebraic systems are structurally similar or not. That means, whether they are isomorphic or not.

So, with this we complete this lecture here and in the next lecture, we will again study some more algebraic systems which a practically utility and they are used in other different streams of Computer Science and Mathematics.