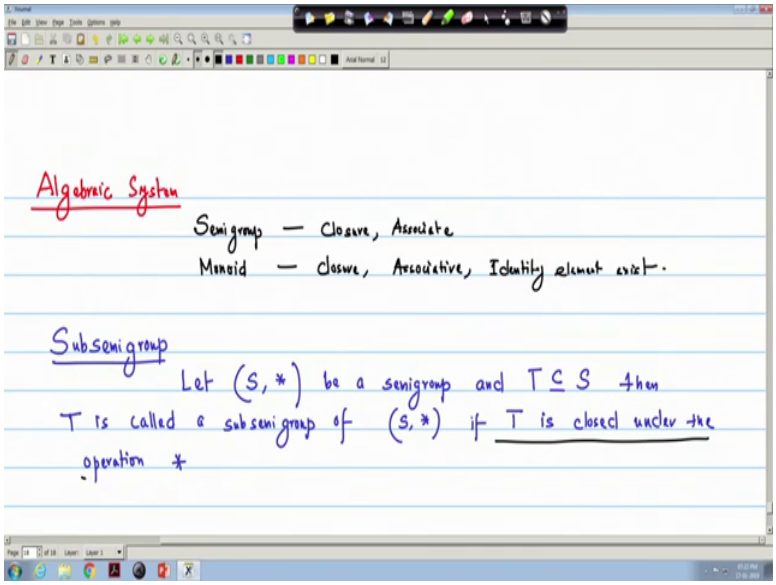
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 48
Algebraic Structures (Contd.)

So, we have read two simple very simple algebraic systems. And some examples also we have seen that how they are satisfying the property particularly we have used the closure, the associative and the identity element.

And then how they are forming the semi groups and the monoid. Now there are some variant or again some subset. Because whatever algebraic system mainly we have defined that it has a non empty set and the operations are operating on this set.

(Refer Slide Time: 01:19)



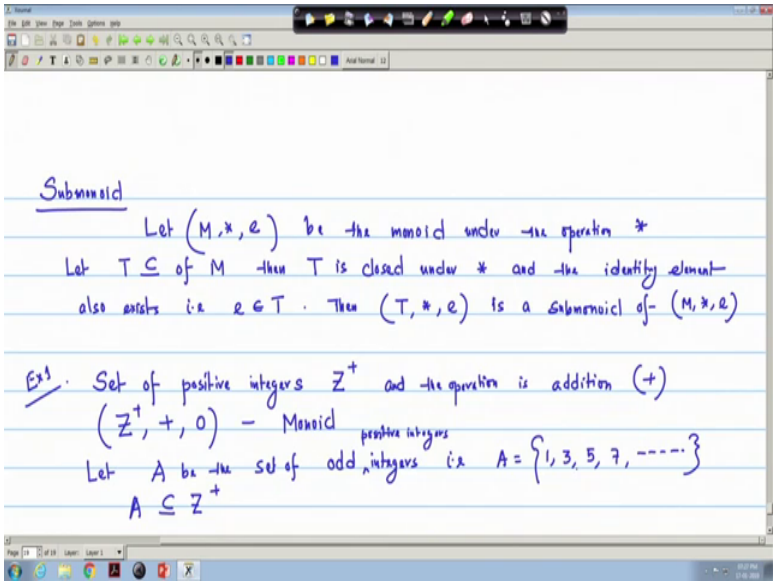
So, how they behave when we will consider a subset of the set? So again algebraic system we will read. And mainly will consider the subset of the set of the algebraic system and then we will try to get them find some more properties. So, first since now we know the we have read the semi group and semi group now if I quickly summarize it has the property of closure and associative ok.

And monid we have seen the closure associative and it has some identity element identity exist I write identity element exist. Now we define a sub semi group because for

both these cases we have considered a set and we have given examples. So, now if how we define it sub semi group or sub monoid. So, first we define a sub semi group.

Let S be the non empty set and star is the operation the a star b a semi group and T is a sub set of S then T is called a sub semi group of S star. If T is closed under the operation star so as the name is sub semigroup only we are taking ones subset of S. And the only condition is that this subset must be closed under the operation star. Now similarly if we define the sub monoid.

(Refer Slide Time: 04:53)



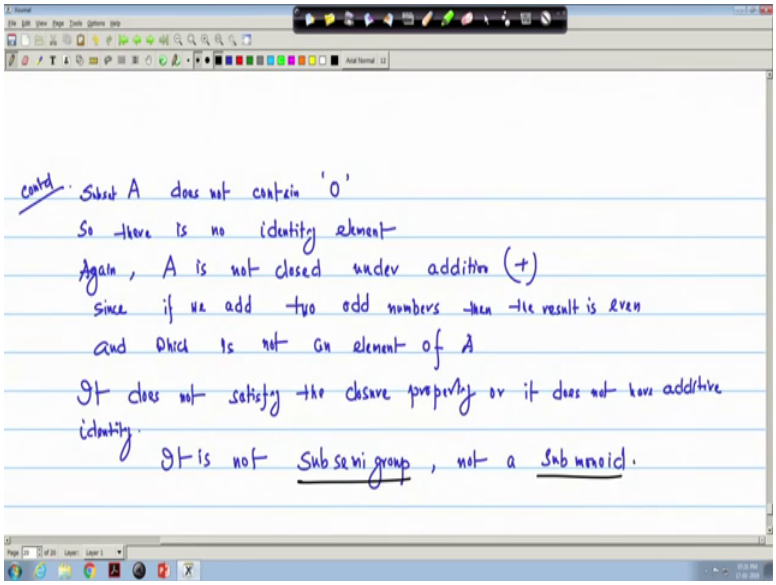
So, again let S star e normally we write M by monoid we give the notation M say M star e be the monoid under operations star the operation star. And let T is a subset of M then T is closed under star and the identity element also exists. That means, e belongs to T. Then we call that then is a sub monoid of M star e.

Now we can take our example of that sub monoid we take that set of integers. consider set of integers set of we take consider set of set of positive integers Z plus and the operation is addition [vocalized-noise. Now already we have seen that Z plus under operation e and my identity element is additive identity is 0 this exists so this is a is a monoid.

Now let a be the set of odd integers set of odd integers. That means, that is A is 1 3 5 7 like that. So, A is a subset of Z plus on set of what positive integers set of odd positive

integers we have taken. Now see if we consider the set A that is on that is only odd integers. So, it does not have any identity element. So, since it does not contain 0.

(Refer Slide Time: 10:43)

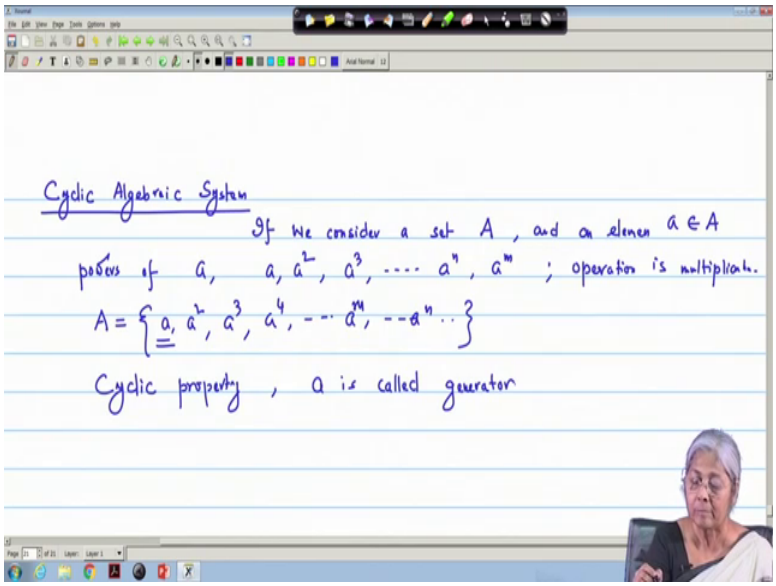


So, a of the subset A as all does not contain 0. So, there is no identity element. Again it is also not closed, again is also not closed under addition. Since if we add 2 odd numbers then the result is even and which is not an element of A.

Since A is the set of odd integers. So, neither it satisfies the closure property not even it has no identity. So, it does not satisfy the closure property or it does not have any identity or some additive identity. The first thing it is not a semi group sub semi group not a is not a sub semi group not also not a sub monoid not a sub monoid.

Now we have seen the defined that a monoid that mainly it holds the property of closure associative property and it has it must have some identity element. Now, it holds some other property like there are some variant of monoid we call that is a cyclic monoid. And it is very important in some real algebraic systems. So, first we define what is we call that cyclic structure so.

(Refer Slide Time: 15:05)

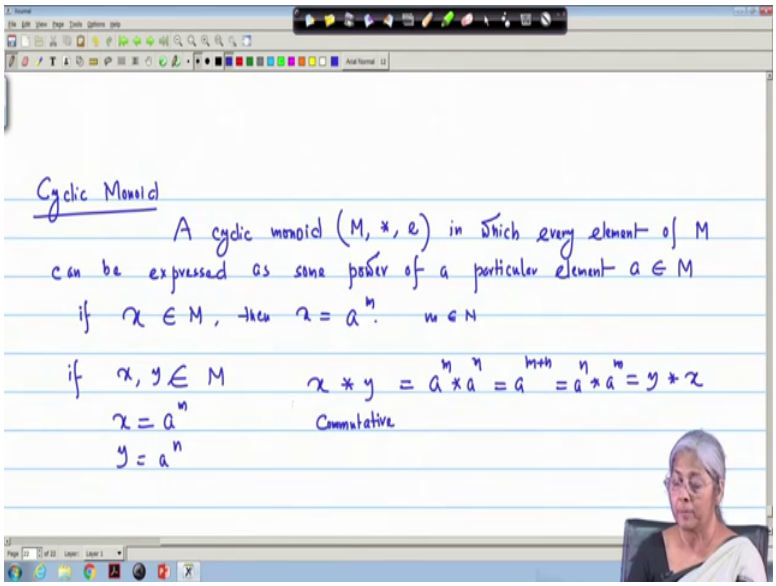


If it is a the cyclic property we can tell see if we can it is as a algebric system it has a set and if there exists one element in the set such that the other all other elements can be generated from by taking the power of that particular element then it is called a cyclic in nature. And that particular element is called the generator of that system the algebra.

Like we tell that if say a if we consider a set A if we consider a set A. And element and then element A belongs to A. Then the all powers of a if we take all the powers of a or a then say a into a square a cube like that; that means, say some a to the power n it a to the power m. And obviously, operations I am taking as the multiplication operation is multiplication.

Now, if the set A contains all these elements say a square a cube a 4 some a to the power n or e to the power n then actually we using this a taking the power we can generate all other elements. So, in that case this is a this is this has some cyclic property this is have some cyclic property. And a is the called the generator general is called the generator. Now we define the cyclic monoid.

(Refer Slide Time: 18:47)



So, we can define the cyclic monoid. So, I can write that a cyclic monoid just now the way we have defined that algebraic system only now algebraic system we are considering a monoid. So, it is M star e in which every element of the set M can be expressed as some power of a particular element that belongs to M also obvious particular element a belongs to M.

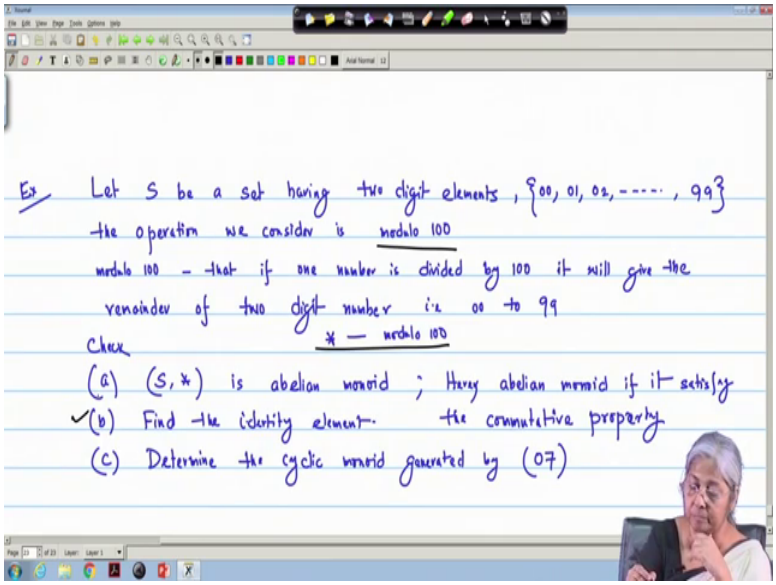
Then I can write that x if x belongs to M then x equal to some a to the power M ok. So, this is my definition of cyclic monoid some power of particular element A such that if x belongs to M the x equal to a to the power M some power and M belongs to some integer. Now if x y 2 elements that are belongs to M. So obviously, we can write that x equal to a to the power M and say y equal to a to the power n.

Then I can write that x star y that is a to the power M into a to the power n is a to the power M plus n is a to the power n into a to the power M this is y star x this star is the multiplication we are writing. So; that means, it is competitive in nature x star y we get y star x it is commutative. Now we see this is this is cyclic monoid.

Now there are in real life we use there are many applications in GL algebra that actually it satisfies this property of cyclic monoid. We see one of the examples that our module operation is very popular in many algebra that and many application areas like coding theory cryptography and that is actually it holds it satisfies or any system under this

modulo operation this becomes algebraic systems like cyclic monoid we take one example of that take one example.

(Refer Slide Time: 22:39)



So, let S be n a set having 2 digit elements; that means, 00, 01, 02 in this way up to 99. Although we write 00 is 00 1 is 1, but just for symmetry we are writing this way. Now the operation we consider is modulo 100. That means, what is this operation the module 100 is if I take one element or some number if I divide it by 100 we will be taking only the remainder.

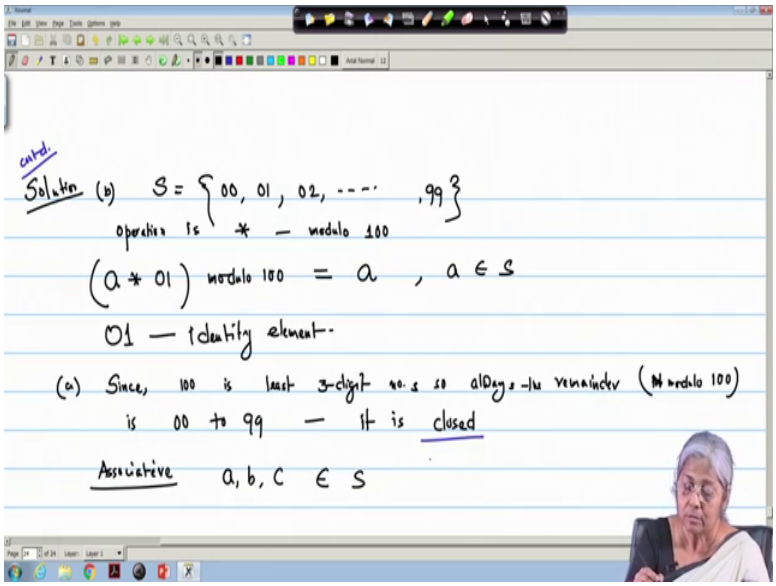
Since 100 is 3 digit number the least 3 digit number. So, though if I take the remainder the remainder can be only up to 99; that means, it is closed. So, this is modulo operation; that means, it tells that modulo 100 is the operation that if one number is divided by 100 it will give will consider the remainder with the remainder of 2 digit numbers 2 digit numbers. That means, again 000 to 999.

So, now, the we have to check that we will check the first is if S star is abelian monoid . Here abelian here abelian monoid abelian means it is commutative abelian monoid if it satisfy the commutative property. If it is commutative property it satisfied then it is a abelian or commutative monoid commutative property.

So, we have to check whether S star is an abelian monoid. Then find the identity element and we see the cyclic monoid generated by determine the cyclic monoid generated by

say some numbers 07. So, with this example and; obviously, here with this example we see there some more properties of the monoid and this star here we consider the star is the operation of means the modulo 100. Star is the operation modulo 100 for this example ok. So, first we see now what is the identity element better we see them b first.

(Refer Slide Time: 28:39)

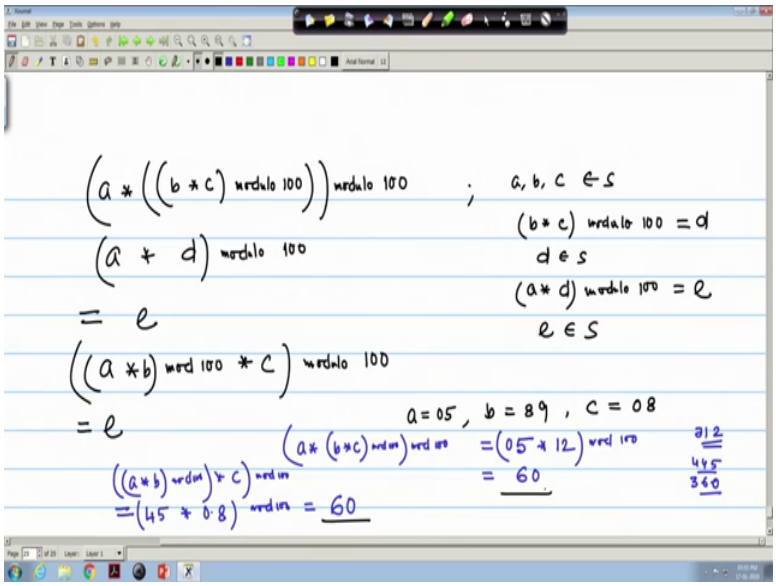


Since my set is S is 00, 01, 02, like 99 to all two digit numbers. And my operation is star which is we take that modulo 100 this multiplication and then we take the module 100. So, 0 so if I take the multiply with 01; that means, if I take a two digit number we multiply with 01 and divide it by 100 take the remainder; that means, module 100 will be getting a only.

Since a star 01 is a and that is it and a belongs to S; that means, a is a 2 digit number. So, 01 is my is my identity this is my identity element. Now if we call so this is actually my b answer of b. Now we check whether it is the first question was what is the what is the abelian monoid? That means, whether it is a commutative or not? So, first thing is it will be closed it has some identity we have to see whether it is associative or not it has identity.

Since 100 is least three digit numbers. So, always the remainder; that means, some number modulo 10 I take the n modulo 100 n modulo 100 is 00 to 99. So, it is closed then whether it is associative or not it is closed. Let us check the associative property? So, if we consider 3 elements a, b, c of two digit numbers belongs to S.

(Refer Slide Time: 32:37)



Now since it is closed so if I consider say first a star b star c modulo 100 and then again this is modulo 100. That means, I am taking first I am considering I am multiplying b and c and all my a, b, c two digit numbers. So, since it is closed so b star c modulo 100 again it will be giving a it will be giving another two digit number say d. So, let b star c modulo 100 is d.

Obviously, d belongs to S because it is closed. So, this becomes now a star d modulo 100 and say b star c modulo d and let the a star modulo a star d modulo 100 is e. So, say my result is e here all that e is also belongs to S. Now, we see that since it is associative property. So, first I do the a star b a star b modulo 100 and star c modulo 100. Now since we are getting this a star be modulo 100 we are taking the last two digit numbers last only the remainder.

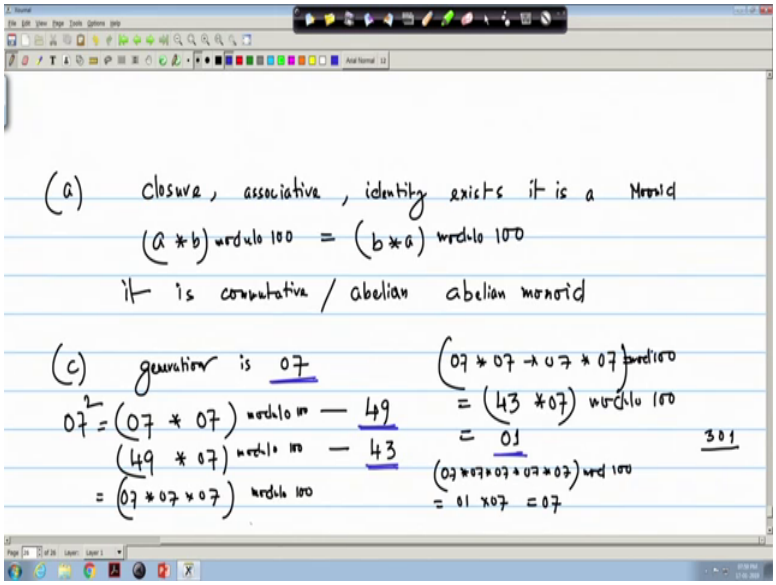
And again that is multiplying with c we are getting taking the remainder when divided by 100. Obviously, we will be getting and again remainder nice last two digit numbers it will be e only. We take some examples that say I get now a is a is 0 5 I take b is 8 9 and we see de we check then if I multiply a star b ok. I should take another value say c equal to 0 8.

So, if I take say a star b star c and this modulo 100 is there always. So, then it is I get 5 and if I multiply these 8 and 89 this will be get getting only 12 because divided by 100

modulo; that means, remainder will be 12 so this is 12. Now if I take this modulo 100 it will be only 60. Now if I do the other way that a star b modulo 100 star c modulo 100.

Then I will get a star b is 5 and 89. So, that will be 4 45 remainder is 45 only 45 and here it is 6 because my sorry c is 8 c is 8. So, if I take modulo 100. So, 8 into 45 this is 36. So, I will be getting only the two digits. So, this is also if I divide by 100 it will be giving him my the 60. So, I see that it is also 60 it is also 60; that means, associative property holds.

(Refer Slide Time: 38:01)



So, what I get that first thing is that for my a part that I see that the system defined here is closure property it holds associative. It has already we have seen identity 0 1 identity exists so it is a it is a monoid. Now here we see that if a star b module 100; obviously, is b star a module 100.

So, it is commutative; that means, it is abelian commutative or abelian. So, it is abelian monoid. Now c part it is generated by generator is 0 7 generator given is generator is 0 7. So, if I 0 7 0 7 modulo 100 since it is only two digits so I will get 49.

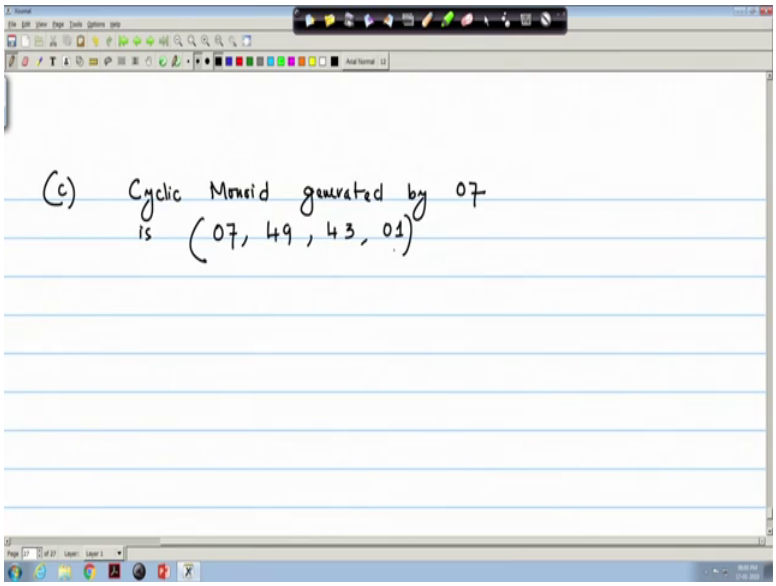
So, if it is 49 star 0 7; that means, it is 0 7 square if I write in this way. Then again if it is 0 7 cube I get the 49 into 0 7 modulo 10 modulo 10 sorry modulo 100 we are taking two digit numbers. So, it will be will get it is 43. Now again if I get 0 7 I write here 49 means

actually this is 0 7 I can write this same thing as the it is as 0 7 star 0 7 star 0 7 that I am taking power 3 modulo 100.

Now in this now if it is already 43. So, if I write 0 7 star 0 7 star 0 7. So, actually this will be this is modulo 100 is actually forty 3 star 0 7 module 100 and this becomes 0 1 because if I multiply. So, 3 0 1 divided by 100 means it will give you 0 1. So, now, again if I multiplies 0 7 star 0 7 another power if I increase either it was 4 I will be getting. Since now I got the identity element 0 1.

So obviously, I will be getting 0 1 into 0 7. So, since already I got so it is 0 7 so it is cyclic in nature. So, what I got first the generator is 0 7. The second it is generating 49 then 43 then again 0 1 and now it will repeat. So, the cyclic the monoid we get a right the c part.

(Refer Slide Time: 42:15)



The cyclic monoid generated by 0 7 is I should write 0 7 then 49 then 43 then 0 1 and it will repeat. So, we read monoid and then that there is some other properties that one monoid can hold. And these type of we can we can see. And we can check that error there are the general properties that we read that again some algebraic system how they hold.

Like we are just now we have seen the abelian monoid that means it satisfies the commutativity. Similarly it can be abelian semi group. So, if the semi group satisfies the

commutative property it will be the abelian thing. So, next lecture will again we will identify some more algebraic systems of the larger algebraic systems and how they satisfy the properties.