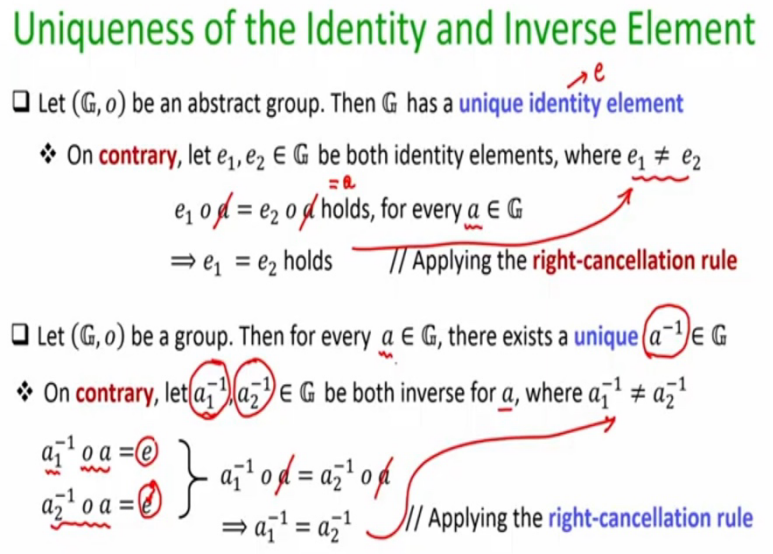
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology, Bangalore

Lecture - 62
Cyclic Groups

(Refer Slide Time: 00:24)

Hello everyone and welcome to this lecture. So, in this lecture, we will continue our discussion on groups and we will introduce a very special class of groups called as cyclic groups.

(Refer Slide Time: 00:32)



Let us first prove that the identity element and inverse element are unique in any group. We first prove for the identity element. Let G be an abstract group. G has to have an identity element because that is one of the group axioms. We now have to prove that it has a *unique* identity element e i.e., G cannot have multiple identity elements. And the proof will be by contradiction.

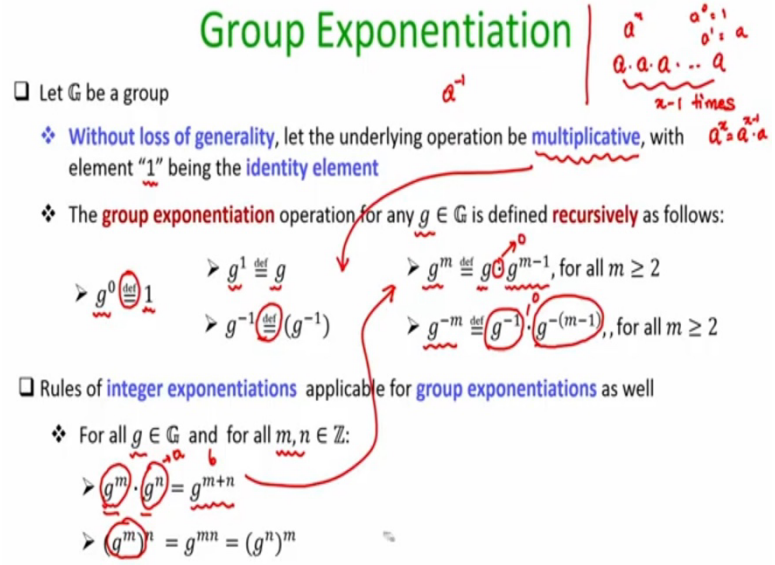
So, on contrary assume that G has 2 distinct group elements e_1 and e_2 and both of them are identity elements. So, the proof by contradiction paradigm tries to arrive at a contradiction, so, let us see what contradiction we can arrive at. Both e_1 and e_2 are identity elements and the following holds from the property of identity elements: you take any element a from the group, the result of $e_1 \circ a$, will be the same as the result of $e_2 \circ a$ and both these answers will be same as a. Since $e_1 \circ a = e_2 \circ a$ we can apply the right cancellation rule and conclude that $e_1 = e_2$ which is a contradiction since we assumed that e_1 and e_2 are distinct elements. Thus, we have shown that every group G has a unique identity element.

We next show that every element a in any abstract group G has a unique inverse element G. You cannot have multiple inverse elements in the group. So, again the proof will be by contradiction. So, on contrary assume that you have multiple inverse elements for this a.

Let a_1^{-1} and a_2^{-1} be two distinct inverse elements. Now, the property of the inverse element is that, if I perform the group operation on the inverse and the element I should get the identity element. So, the result of $a_1^{-1} \circ a$ will be the identity element and the result of $a_2^{-1} \circ a$ will also be the identity element.

Thus $a_1^{-1} \circ a = a_2^{-1} \circ a$ and from the right cancellation rule we conclude that a_1^{-1} is the same as a_2^{-1} which goes against the assumption that a_1^{-1} inverse and a_2^{-1} are distinct. So that shows that, every element in the group has a unique inverse.

(Refer Slide Time: 04:02)



Now, we want to introduce a new operation in the group which we call as, *group exponentiation*. The group operation is still $\circ$, but we will be using that operation $\circ$, multiple times on an element of the group which I can view as a some kind of group exponentiation. So, in the regular arithmetic when I say a^x, it is interpreted as if I want to multiply a with itself $x - 1$ times.

So, I want to abstract out that operation in the context of a group itself. So, imagine you are given an abstract group and without loss of generality, I will now follow the multiplicative notation. This is just for our convenience because we are accustomed to multiplicative notation while discussing exponentiation in the regular arithmetic, so that is why I am using the multiplicative notation.

But whatever I am discussing is true even if my group operation is additive or if it is treated as an abstract operation $\circ$. So, since I am following the multiplicative notation, I will be using 1 for denoting the identity element e, 1 does not mean the numerical 1, remember. And I will use a^{-1} for denoting the inverse of the element a, again a^{-1} need not stand for $\frac{1}{a}$, it depends upon my exact group.

Now, the group exponentiation for any group element is defined recursively as follows. Because in the regular world also, a^x can be defined recursively, so, I define a^0 as 1, in the regular world, and then I define a^1 as a and then I can recursively define a^x as the result of a^{x-1} with a. Similar definition I will now use in the context of an abstract group.

So, I will define g^0 to be the identity element, this is a definition. And I will define g^1 to be the element g itself. Now, I will define g^m to be $g \cdot g^{m-1}$. So, remember g^{m-1} is also a group element because g^{m-1} is further recursively be defined as $g^2 \cdot g^{m-2}$ and g^{m-2} is again recursively defined as $g^{m-3} \cdot g^2$ and so on.

So, g^{m-1} will be a group element and g is a group element and I am following a multiplicative notation. So, this multiplication actually stands for the abstract group operation $\circ$. So, whatever result I will obtain by performing the group operation on the element g and the element g^{m-1} that will be defined as g^m, for every $m \geq 2$.

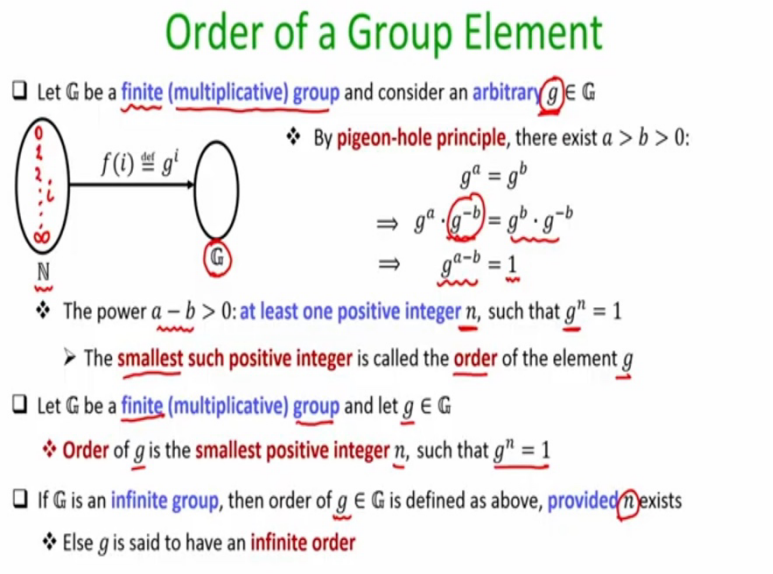
I can define even the negative powers of my group element. So, g^{-1} will actually stand for the multiplicative inverse of my element g and g^{-m} will be recursively defined as follows. I will take the multiplicative inverse of g and I will take $g^{-(m-1)}$ and I will apply the group operation and whatever is the resultant value that will be called as g^{-m}. So, this is the way I defined a group exponentiation assuming that I am following a multiplicative notation, corresponding definition will be there if I am following an additive notation.

Now, it turns out that the rules of integer exponentiations that we are aware of are applicable even for group exponentiations. Imagine I am given a group element g and I take arbitrary exponents m and n where m and n could be positive or negative. Now, it turns out that if I take the group element g^m and if I take the group element g^n and perform the group operation then that will give me the same group element g^{m+n}.

And this g^{m+n} can be obtained by recursively following this definition. So, what I am saying is, on your left hand side you have 2 group elements and we are performing the group operation on them. So, we will get one group element call it a and you have g^{m+n} which is another group element whose value I can obtain by following this recursive definition call it b. My claim is $a = b$ i.e., the group elements a and the group elements b are same. So, you can easily follow that.

In the same way, let g^m be a and then if I compute a^n then that will be the same as the element g^{mn}, so g^{mn} also will be some element, call it b. So, $a = b$ and g^{mn} will be the same as the element c^m where $c = g^n$; so all of them will be same. It is easy to verify these rules are applicable even in the context of group exponentiations.

(Refer Slide Time: 10:23)



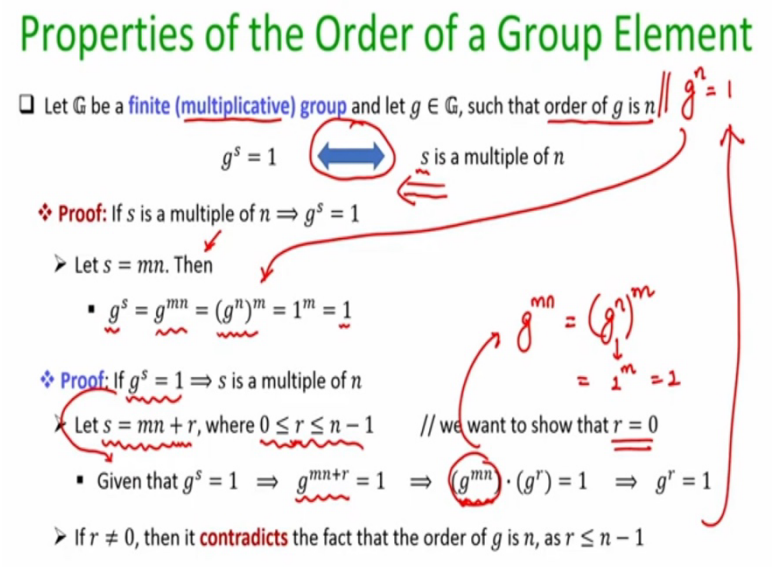
So now, let us define order of a group element. So, imagine you are given a finite group and for convenience, I will be using the multiplicative notation. However, whatever we define here holds for any group. And now consider an arbitrary group element g.

We define a function from the set of natural numbers to the group and my function is the following. The domain will be $\{0, 1, 2, \ldots, \infty\}$ and the co-domain is the group. The way I go from the domain to co-domain is, if I want to map the element i, I go to g^i. Now, it is easy to see that since my group G is a finite group, it will have finite number of elements whereas, my domain is infinitely large then by pigeon hole principle, I know that there exists at least 2 non-zero values a and b such that $a > b$ and both a as well as b get mapped to the same group element, namely $g^a = g^b$. Now, since g^{-b} is also a group element, if we multiply both sides of the equation with g^{-b} then we get $g^{a-b} = g^{b-b} = 1$. Note that 1 is the identity element in multiplicative notation. Since $a > b$, $a - b$ is positive. This in turn implies that there is at least one positive integer n, such that for the element g which I have arbitrarily chosen here, g^n is 1.

Of course, there might be multiple values of n for which g^n will be 1, it depends upon how many (a, b) pairs are there. But at least 1 positive integer n is definitely there such that g^n is the identity element. Among all those positive integers n such that, g^n is equal to the identity element, the smallest positive integer is called as the order of the element g.

So, let G be a finite group and for convenience assume we are following the multiplicative notation and g is a group element then the order of the group element g is the smallest positive integer n such that, g^n is 1. So, the above definition or the order of our group is with respect to a finite group because if the group is infinite and if you are now taking an arbitrary group element then it may not be the case that you can easily find out the n, or whether, at the first place we do not know whether such an n exist or not if my group is infinite. So, in that case I will say that the element g will have an infinite order. But for the finite groups, the smallest positive integer n such that g^n is the identity element, will be treated as the order of the group element g.

(Refer Slide Time: 15:00)



So now, let us discuss some interesting properties of the order of a group element. So again, I will stick to the multiplicative notation. So, imagine you are given an element g and it is given to you that its order is n; that means, I know that g^n is 1 then my claim is the following. If you have g^s also giving you the identity element then that is possible if and only if, s is a multiple of n that means, s is completely divisible by n.

Of course, for $s = n$ this claim is true, but my claim is that, if at all there is any other s such that g^s gives you the identity element then s has to be a multiple of n. So, I have to prove 2 implications here. So, let us first prove the implication in one direction. Assume s is a multiple of n. So, I want to prove that if s is a multiple of n then this direction implication is true.

I want to prove that g^s will give me the identity element given that g^n is the identity element since the order of g is n. Since s is a multiple of n we can write down that s is some mn where,

m is some integer. Then what can I say about g^s, as per my group exponentiation rules, it is same as g^{mn}.

And g^{mn} I can break down as the group element g^n being raised to the power m. But since g^n is the identity element this is the same as the identity element raised to the power m and identity element raised to power m means, I am operating the identity element with itself, several types, namely m times which will give me again the identity element namely 1. So that proves the implication in one direction.

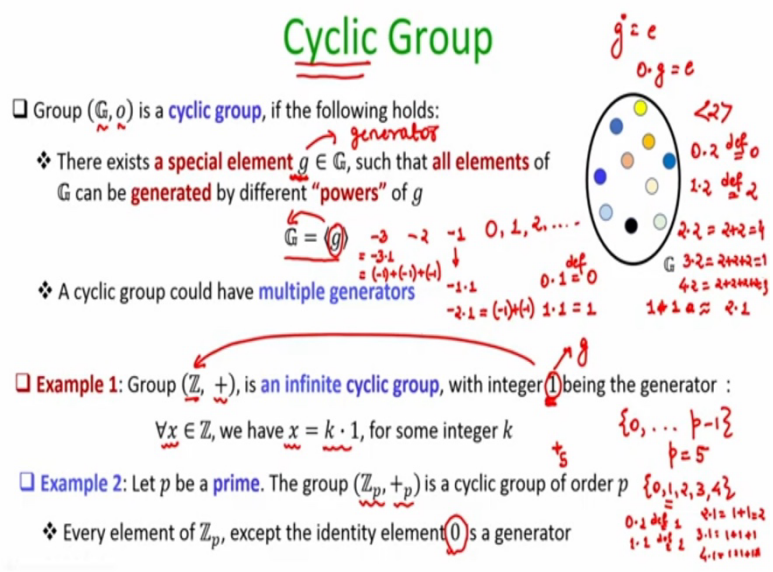
Now, let us prove the implication in the other direction. I want to prove that if there is some exponent s, such that g^s is 1 then, definitely s has to be a multiple of n. So, again I will give a direct proof here. So, I can always write down my exponent s, as some quotient time n plus a remainder where, the remainder will be in the range 0 to $n - 1$. And my goal is to show that s is completely divisible by n, namely, I want to show that my remainder r is 0.

Now, again I am giving a direct proof. So, I am assuming my premise to be true, since my premise is true that means g^s is 1 and now, I am writing down the value of s in terms of the quotient and the remainder to get g^{mn+r}. Now, I can rewrite g^{mn+r} and break it as per the rules of group exponentiation like $(g^m)^n$; I can write it out as the result of group operation being performed on $g^{mn}$and element g^r and my right hand side is the identity element.

Now, I can further apply the rules of the group exponentiation and say that g^{mn} is same as the element g^n being raised to power m and g^n is the identity element. So, this gives me 1^m which is 1. That means, this is identity element or 1 and 1 multiplied with g^r will be giving me the element g^r itself, so, I get g^r is equal to identity element.

So, remember that my range of r is 0 to $n - 1$. So, my conclusion now is the following, since g^r is equal to identity element r has to be 0 because if r is not 0 and if it is strictly less than n then I get a contradiction to the fact that n is the smallest positive integer for which g^n was identity element. So that shows the implication in the other direction as well.

(Refer Slide Time: 19:41)



So, now, let us define what we call as *cyclic group*. Let G be a group with some abstract operation $\circ$. It may or may not be a finite group. The specialty of the group is that it has an element g which we call as a generator. It is called a generator because when you take different powers of this generator, again by power I mean group exponentiation, you will get **all** the elements of your group. That means, this element g has the capacity to generate all the elements of your group by performing the group exponentiation on this generator.

A group that has a generator g is called cyclic and is represented by the notation $G = \langle g \rangle$. This notation basically says that g can act as a seed and reproduce the entire set G by computing different powers of this generator. Of course, a cyclic group can have more than one generator. However, we require a group to have only one generator for it to be cyclic.

Before proceeding further, let us see some examples of a cyclic group. So, consider the infinite group, namely the group based on the set of integers with respect to the plus operation. My claim is that the integer 1 constitutes your generator.

This is because if you take different powers of this element 1, it will give you all the elements of your set of integers. So, let us see whether we can generate any arbitrary integer x by computing some power of this element x. And indeed, it is easy to verify that you take any integer x, it will be some $k \cdot 1$ for some integer k. So, for instance, if you want to generate, say, the element 0 from this element 1, then I know that $0 \cdot 1 = 0$ from the definition of group exponentiation.

Since we defined g^0 to be the identity element when using the multiplicative notation, in the additive notation this will mean that, if we add g, 0 number of times that will give me the identity element for any g. So, I am now treating g as 1, so that means, $0 \cdot 1$ will generate the element 1 whereas, if you want to generate the integer 1 then it is same as you perform 1^1.

1^1 in the additive notation will be treated as $1 \cdot 1$ and that will give you 1. If you want to generate the element 2 through the element 1 then that is same as performing the operation plus on the element 1 that will give you 2. So, this can be treated as 2 times 1 and so on. So that means, all the values are now in the positive side can be generated by the element 1 and in the same way you can generate the negative elements as 1. So, for instance, if you want to generate -1 then, -1 can be interpreted as if you want to perform $-1 \cdot 1$.

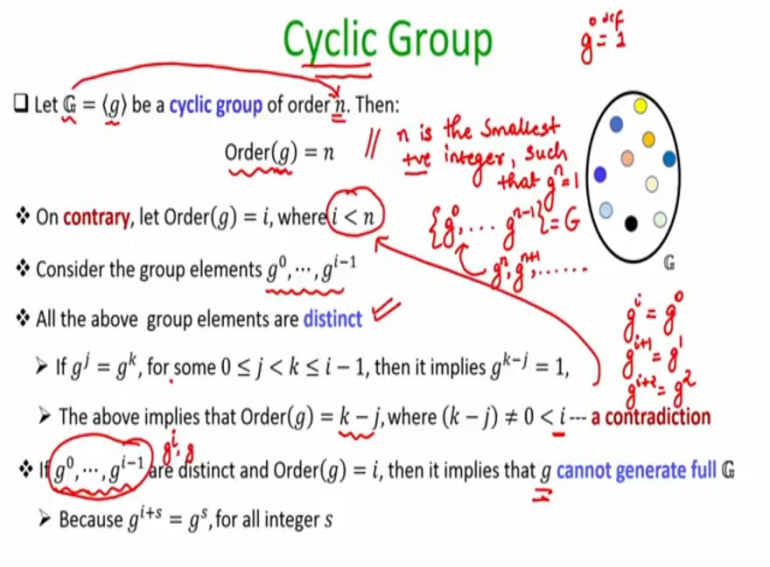
-2 can be interpreted as $-2 \cdot 1$. So, $-2 \cdot 1$ is nothing but the additive inverse of 1 namely, -1 being added to itself 2 times. In the same way you want to generate -3 that is same as $-3 \cdot 1$ and $-3 \cdot 1$ is nothing but -1 being added to itself 3 times. That is the definition of group exponentiation for the additive notation. So that shows that even though this group is infinite it is having a generator, namely the element 1.

So this is an example of an infinite cyclic group. Now, let us take an example of a finite cyclic group. Let p be a prime and now if I consider the set of all integers modulo p, namely the set 0 to $p - 1$ and if my operation is $+_p$ then my claim is that, this group is a cyclic group and in fact has multiple generators. In fact, all the elements except the identity element 0 will be a generator for this group.

Let's verify this by taking p = 5. Then, the set here is $\{0, 1, 2, 3, 4\}$ and my operation is $+_5$. Now, you can check here that I can generate all the elements through 1. So, 0 can be generated through 1 because $0 \cdot 1$ is defined to be 0, namely the identity element. $1 \cdot 1$ is also defined to be the element itself. And now $2 \cdot 1$ is basically (1 + 1 modulo 5) and (1 + 1 modulo 50) is 2. $3 \cdot 1$ will be (1 + 1 + 1 modulo 5) which will be 3, and $4 \cdot 1$ will be 1 + 1 + 1 + 1 which is 4 modulo 5 which is 4.

In the same way 2 is also a generator, you can generate all the elements through 2. So, $0 \cdot 2$ will be defined as 0, $1 \cdot 2$ will be defined as 2 itself, $2 \cdot 2$ will be $2 + 2$ modulo 5 which is 4, $3 \cdot 2$ will be $2 + 2 + 2$, you get 6 but you have to do operations modulo 5, so, you will get 1 and then, $4 \cdot 2$ will be $2 + 2 + 2 + 2$ which is 8 modulo 5 which is 3. So, 2 is also a generator since we were able to generate all elements in the group. Similarly, you can check that 3 and 4 are also generators.

(Refer Slide Time: 27:32)



So, now, let us derive some interesting properties for cyclic groups. So, imagine G is a cyclic group and suppose the order of G is n. So that means, now I am considering a finite cyclic group since the group has a well-defined order. Let n be the number of elements and say g is one of the generators. Then my claim is that the order of the generator is n. What does that mean?

So, this means that n is the smallest positive integer such that g^n is equal to the identity element. So, assume I follow the multiplicative notation. So, the order of G is equal to n means, g^n is 1 and n is the smallest such positive integer. By the way in the definition of order of an element, why I am focusing on positive integer, because if I do not put a restriction on positive integer then clearly g^0 is always defined to be the identity element. So that is why I am interested in the smallest positive power for which g^n will be 1.

So, now, let us prove this statement regarding the order of the generator. So, the proof will be by contradiction. So, on contrary assume that the order of the G is not n, but some positive integer i where i is strictly less than n. So, now, what can I say about the elements

$g^0, g^1, \ldots, g^{i-1}$; of course, they are group elements because we have the closure property being satisfied. But apart from being group elements, my claim is that, all these i elements are distinct. Again, this can be proved by contradiction. So, on contrary assume that the j-th power of g and k-th power of g produce the same group element, where k is some power higher than j and both j-th power and k-th power are strictly less than equal to $i - 1$.

Now, if that is the case then I come to the conclusion that g^{k-j} is the identity element. How do I get this? By multiplying both the sides of this equation by g^{-j}. But then that means that the order of G is $(k-j)$. Why $k - j$? Because since, k is strictly greater than j then $k - j$ is positive and that means $k - j$ is not 0 and $k - j$ is strictly less than i.

Which is a contradiction to my assumption that, order of g is i, so that shows that indeed, the statement that all this i distinct powers of g are going to give me distinct group elements is true. But, if these i powers of g are giving me the distinct elements then how come at the first place g is a generator. Because if g is a generator then it has to generate all the n elements of the group. Right now I have generated only i elements of the group, by raising g or by computing i distinct powers of g and i is strictly less than n.

How do I generate the remaining elements of the group? You might be wondering, why can't I go for the higher powers. The problem is that if you go to the higher powers, you start getting the elements which you have already generated through the first i powers of your generator. Namely g^i, will give you the same element as g^0. g^{i+1} will give you the same element g^1, g^{i+2} will give you the same element as g^2 and so on.

So that means, once you have computed the first i powers of g the next powers of g will start giving you the elements which you had already generated; you would not be getting any extra or any new elements of the group. And that goes against the assumption that my g was a generator for the whole group. If it was a generator for the whole group then it should have the capability to generate all the n elements, not just i elements. So that is why the order of my generator g has to be the same as the order of the finite group or the whole group which is n.

And that shows that, why we are calling this group as a cyclic group because if g is the generator then by raising g to different powers from 0 to $n - 1$, I will be getting the entire

group. Now, once I start computing the higher powers of g, namely g^n, g^{n+1} and so on, I would not be getting anything extra. I will start getting the same elements which I have generated by computing $g^0, g^1 \ldots g^{n-1}$. In that sense, it is a cyclic group; cyclic in the sense, you can arrange the elements of the group in a cycle. And that cycle can be completed by raising g or the generator to different powers in the range 0 to $n - 1$.

So that brings me to the end of today's lecture. Just to summarize, today we saw some more properties of groups. We discussed about the order of the group, we discussed the properties of the order of the group, we discussed about the order of a group element. And we also discussed about cyclic groups and derived some properties regarding the order of the generator of a cyclic group. Thank you.