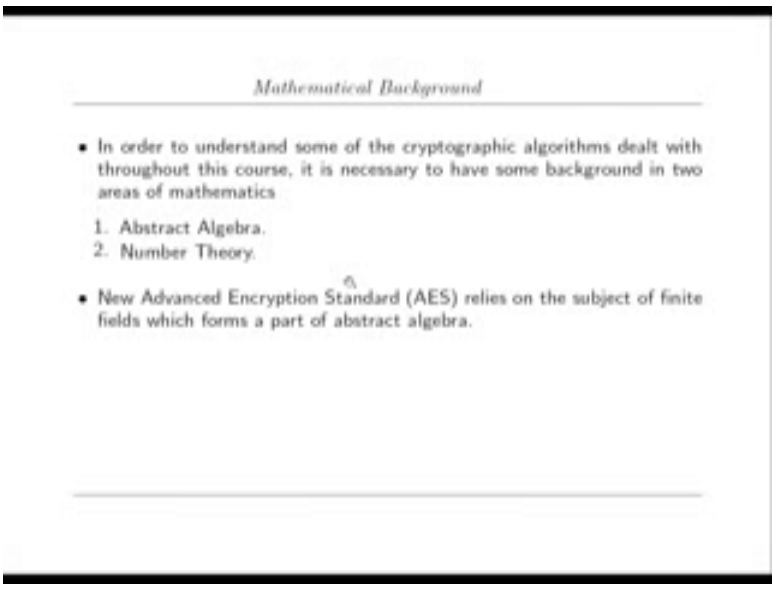
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 12
Mathematical Background

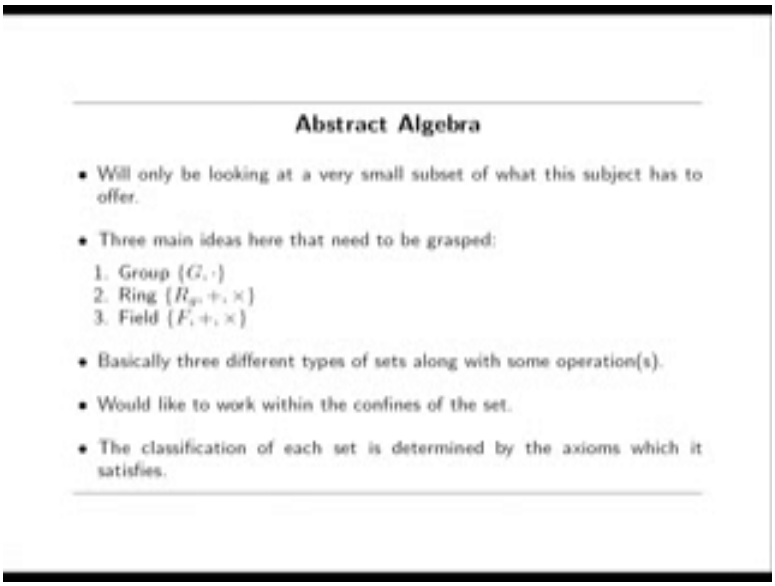
So, we talked about some mathematical background which is required for to understand the cryptographic algorithm, we have seen that for (Refer Time: 00:31) we are using something called primitive polynomial. So, and for AES we need to use some Galois field polynomial, but the Galois field knowledge finite field. So, this mathematical background is required.

(Refer Slide Time: 00:51)



So, in order to understand some cryptographic algorithm dealt with throughout this course, it is necessary to have the background in basically 2 areas like abstract algebra and the number theory. In abstract algebra the polynomial is part of this abstract algebra where we will talk about the finite field theory and also AES is the new encryption standard, advanced encryption standard for block cipher, will discuss this and for that we need to have a knowledge of this finite field and which is a part of the abstract algebra.

(Refer Slide Time: 01:31)



So, we will start with the abstract algebra. So, this is basically algebraic structure, which is deal with something called set and some operation.

(Refer Slide Time: 01:51)

So, abstract algebra. So, in this area we will talk about 3 algebraic structure namely group, ring and finally talk about field; group, ring, field and these are basically algebraic structure on its over a set with an, with 1 or 2 operator. So, let us start with this set. So, what is the set?

(Refer Slide Time: 02:39)

So, let G be a set of element. So, what is a set? Set is basically a, how to define a set? Set it is a collection of well defined object, this is the definition of set. Set is a distinct collection of well defined objects. So, there are 2 things: one is distinct and well defined well defined means so if you define a set, then if you take any element from the universe then we can say definitely whether that element is in the set or not. So, this sense it is well defined. So, it is completely defined, I mean there is no that this, this element could be in the set something like that this type of answer should not be there. Some example of set is say - set of natural number 1, 2, 3, n, up to infinity, this is the set of natural number.

Now, this are distinct element. So, 1 is not repeated twice, this is not a set if we say 1, 1, 2, 3, 3 like this; this is this repetition is not allowed in the set so this is a distinct collection and if I have this set then whether we can say that this 1 by 2 is in the set or not. So, 1 by 2 is not in the natural number, so it is not in the set. So, that sense is this well defined. So, any element if you take from the universe, we can definitely say whether that element belongs to that set or not. So, another could be set of integer I - which is basically coming from minus infinity 1, minus 1, 0, 1, 2 dot dot dot infinity this is the set of all integer, this is the integer set.

And then we have a set of rational number which is basically of the form p by q or p q are coming from integer set. So, this is the way we represent a set, there is 2 way we can

represent a set we can explicitly write all the elements in the set, but if the set is infinity then it is not possible to write, then we lives some type of symbolic notation, so a set is having some property; if it is natural number it has some properties follows the pianos (Refer Time: 06:02) all this. So, like for a rational number any rational number is of this form p by q. So, this is the property set means the element this is the given followed by the property.

So, this is the set of rational number; other than number also there could be another sale like in this room, what is the number of element that set like we are a teacher, some student, chock, board so this collection is also a set. Now similarly see a set of irrational number and set of real number is denoted by R.

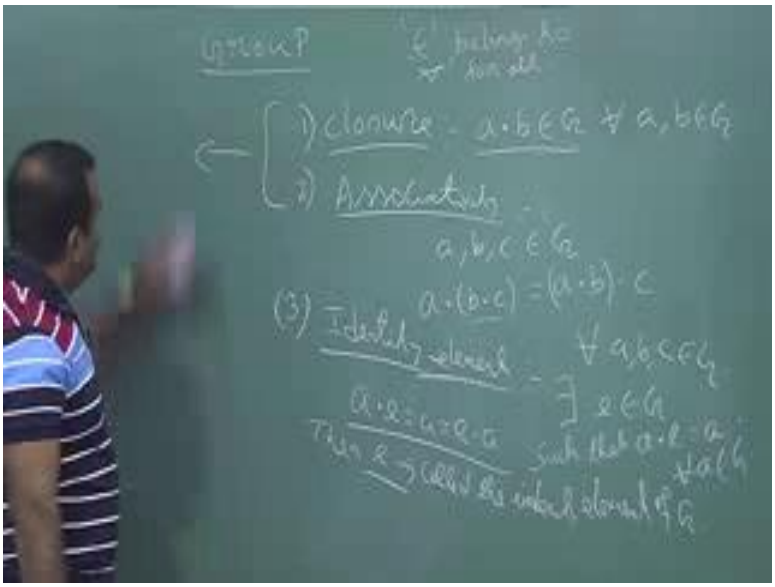
(Refer Slide Time: 07:00)

So, R is denoted by R is the set of real number. Now suppose we are there set G and we have a operated on this set, operator means it is a binary operator; binary operation like binary means it is taking 2 element at a time. So, if a b belongs to G then we can operate this operator a dot b or it could be star this is just a notation, then a star b or we could use plus then a plus b. So, these are all binary operator or binary operation, because it is taking 2 element binary I mean 2 element a b that is why it is say it is binary operator; if it is 3 element then it is ternary operator.

So, will define a group which is the algebraic structure over a set so for that we need to take a set which is non empty, let G be a non empty set; that means, G is non empty set

and we have a binary operator dot, it could be star also, it could be plus also anyway. So, suppose you have a binary operator dot and we say this is a group if you satisfy the 4 properties or 4 axioms we can say.

(Refer Slide Time: 09:00)



So, first property is closure property. So, closure property is telling us if you take any 2 elements a b from this set, then if you operate under this operator then that must belongs to again that is it. So, this is telling a star b must belong to G for all a b belongs to G. So, we will use this symbol as belongs to and this is for all, these are the standard notation is will use this, but just to recap. If a star b so this is the closure property so; that means, we have this set, if you take any element of this set a b, now if you operate this a dot b then it will be again an element in the set this is G and this is the closer property and this much true for every a b.

Then the second property is associativity or Associate property. associativity property is telling we take 3 element from this set a, b, c, then this must satisfy a dot b, this is a binary operator so we have to take 2 element at a time, so we first take these 2, then operate up on that. So, this is if it is closer property satisfying then this will be belongs to G, then this is another element and this is another element so we can operate this. So, this must give us a dot, b dot c and if it is true for all a b c belongs to G then we say that associativity is satisfying. So, now, if this 2 property satisfy for a set along with this then we call G along with this operator is a semi group; if this just this to property satisfied

one is closer property another one is associativity property, but we are looking for a group.

Now, third property is existence of identity element. So, identity element means, this is our set G. So, here in this set there must be an element which is referred as e such that. So, there exists a and this is unit e, there exists e belongs to G such that a dot e is equal to a this is true for all a belongs to G; this must true for all a belongs to G and this operator can be done in any site like a dot e is equal to a and it should be e dot a. So, if such element exists; now we can prove if this exists then this must be unique.

So, if we have such element and then that element is called identity element of the group then e is called the and it is unique identity element of the group G, so far we do not know the group, so far we have this set. So, e is called the identity element if we have this property.

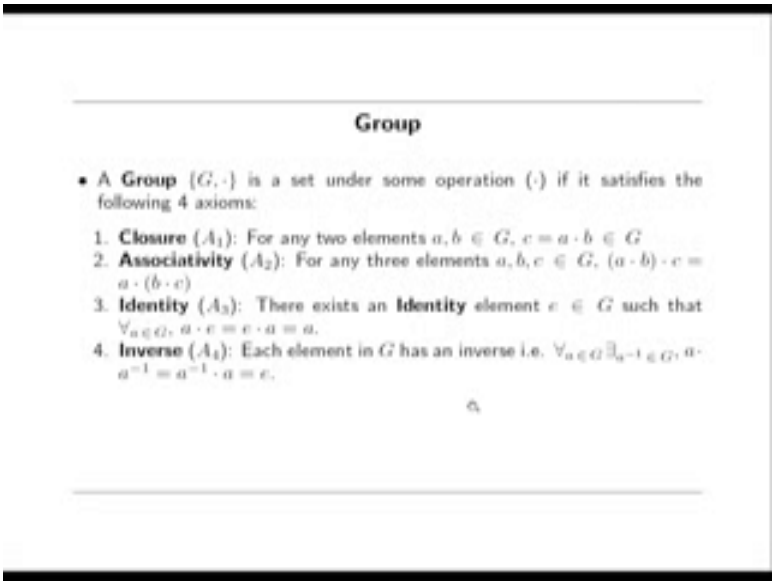
(Refer Slide Time: 14:00)

And the last property for group is property number 4 is basically existence of inverse. So, each element should have inverse. So, what do you mean by inverse? So, for a given element for every element, for a given element there must exist be an element b; such that a dot b must with the identity. So, this is this must be for every element. So, we have a group G we take a element a, so there must be element b. So, b is usually referred if this is true, b is referred by a inverse like this. If this is in multiplicative cells or additive cells b is referred by b is equal to minus a; anyway we will talk about that, but inverse is

like this a inverse. So, for a given a there must exist a b, which is basically called as a inverse such that if we multiply a with a, it will give us the identity element.

Now, if this 4 property satisfied for a set along with this operator, then it is called a group. So, if this 4 property satisfied then this along with this operator is called a group now we can take some example of a group.

(Refer Slide Time: 16:15)



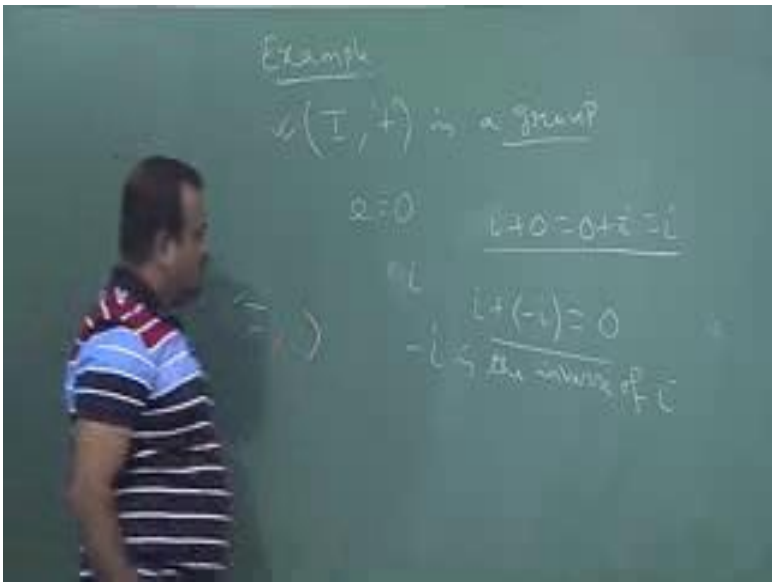
So, let us just come to this slide. So, this is the set G and with the operator dot, this dot it operator binary operator and these are the following properties this is closer property. So, for any 2 element a b, a dot b must belongs to G this is associativity property. So, a dot b dot c is equal to a dot. So, this we have already talked and this is the existence of identity. So, there must exist an element e which is called identity element and this is unique such that a dot e is equal to e dot a, is equal to a, and for each element should have the inverse. So, for a given a there must exist a b, which is basically called a inverse such that a operate with b, a inverse is equal to e, which is any side we can operate this. So, if this 4 property satisfied then I called a group.

(Refer Slide Time: 17:30)

Now, let us take an example of a group. So, example if we take the set as say set on natural numbers, this is our G and suppose our operator is plus the real number plus, a 2 plus 3 is 5 this plus operation. Now the question is whether under this operation N along with plus is a group, this is the question. So, what is the answer? Answer is no because why? Now let us check whether it is satisfying all the 5 properties we have. So, if you take 2 natural number say m and n, now first you have to check the closure property let us take 2 natural number m and n. So, m plus n is also natural number. So, closer property is ok. Now associativity so if you take 3 natural number m, n and k then this is also true m plus, n plus, k is equal to m plus, n plus, k, associativity is also satisfying. So, it is a semi group. So, these 2 tell us it is a semi group.

Now, the question is whether it is a group or not? So, for group we need to have a identity element, can you have a identity element for? So, if we take an n natural number then identity element means there should be a element on which we operate this and it should give us. So, that element is basically 0 element for real number. So, n plus 0 is n which is 0 plus n, but thing is 0 is not belongs to the natural number set. So, this is not a group and even if we include 0 with the natural number set, then also it will not a group. So, this is basically set of positive integral because then the inverse will not be having. So, because if we have take a any positive integer say 2 then the inverse under this additive operation is minus 2. So, minus 2 does not belongs to this set. So, it is not a group.

(Refer Slide Time: 20:17)



So, now the question is whether set of integer is a group or not along with this plus operator? So, this is the set of integer plus is a group, because we know this satisfying the semi group property and if we take identity element is 0, 0 is basically over here, because if we take any integer i plus 0 is equal to 0 plus i is equal to i. So, this is the existence of identity and inverse is also there because if we take an integer say k or say i then the inverse is basically minus i. So, i plus or minus i is equal to 0. So, minus i is the inverse of i under this addition operation. So, this is a group, now the question is whether this along with this multiplication, real number multiplication is a group or not? This is not a group because what is the. So, this is having this property like closer property is ok, because if we multiply 2 integer it will give as an integer. So, closer property is ok, associativity is it coming from the associativity for a law of the real number and then existence of identity; what is the identity element for multiplication? That is 1 basically.

(Refer Slide Time: 22:03)

So, that is also 1 belongs to, so this is identity element. So, this is also Ok. Now the problem is with the inverse. So, if you take an integer say 3, now what is the multiplicative? So, this is this operation is multiplicative sense. So, what is the inverse? Inverse is 1 by 3 because if you multiply 3 with 1 by 3, it will give us the identity element. So, this is the basically 3 inverse, but this does not belongs to the I, so that is why this is not a group. So, now, the question is. So, is there any group under this dot? Yes. So, if you take the set of the rational number.

(Refer Slide Time: 23:24)

If you take set of rational number Q, this is a rational number then this will form a group with the multiplication is a group, you can easily verify this because inverse is also there because if we take a rational number, then inverse is just 1 by x. So, if it is p by q then that 1 by x will be q by p, this again a rational number. So, this is a group.

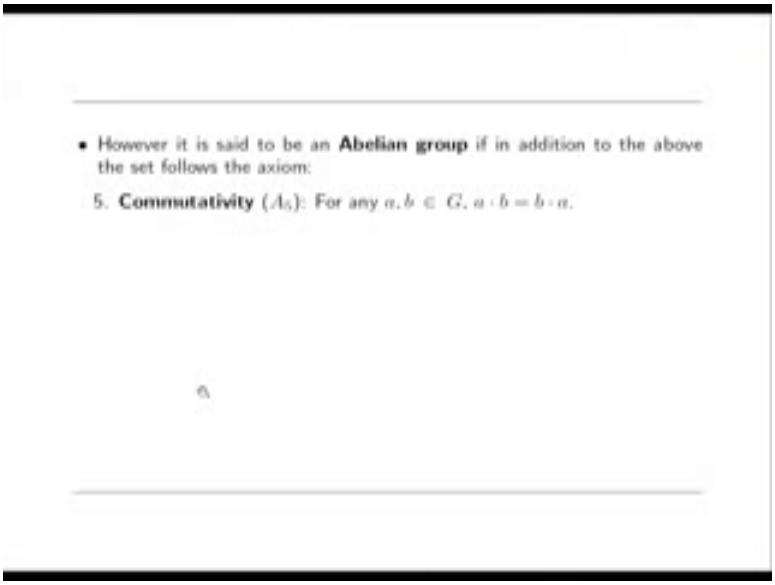
Now, even set of real number along with this, is a group. Set of real number with this is also a group. So, these are the example of group. So, these are all infinite group like infinite with the order of a group is basically, if you have a group suppose G is a group then the order of this group is basically number of cardinality of this set, order of this group is the cardinality of this set, the size of this set. So, if it is finite then it is called finite group; if it is infinite then it is called infinite group.

(Refer Slide Time: 25:16)

Now, we talked about what is called Abelian group or commutative group; when it says G along with the operator, binary operator is a Abelian group. First of all it has to be a group. So, this is the first condition is a group; that means, it must satisfy all the 4 properties. So, A 1 to A 4 all the 4 properties it may satisfied and then it should satisfy the Abelian property, Abelian or commutative property; this property is telling if you take any 2 element a b then for all a b belongs to G, a dot b is b dot a then it is called sorry Abelian l then it is called and if this is true for all a b then it is called Abelian group or the commutative group.

So, for the group we have seen like R plus, this is the Abelian group because the plus operation is real number plus operation is Abelian operation because if you take 2 real number a b (Refer Time: 26:37) a plus b, b plus a; even the dot is also a Abelian operation commutative operation, so R dot is also a an Abelian group or the commutative group because this operation has to be a commutative operation.

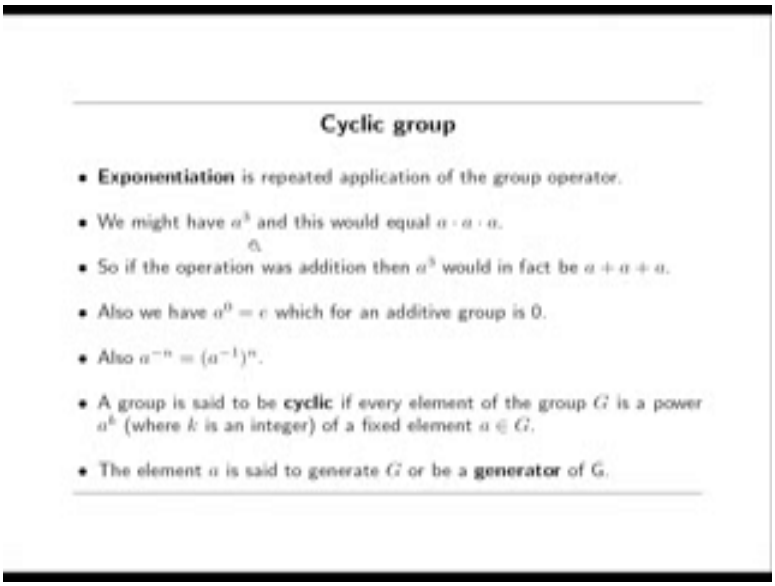
(Refer Slide Time: 27:16)



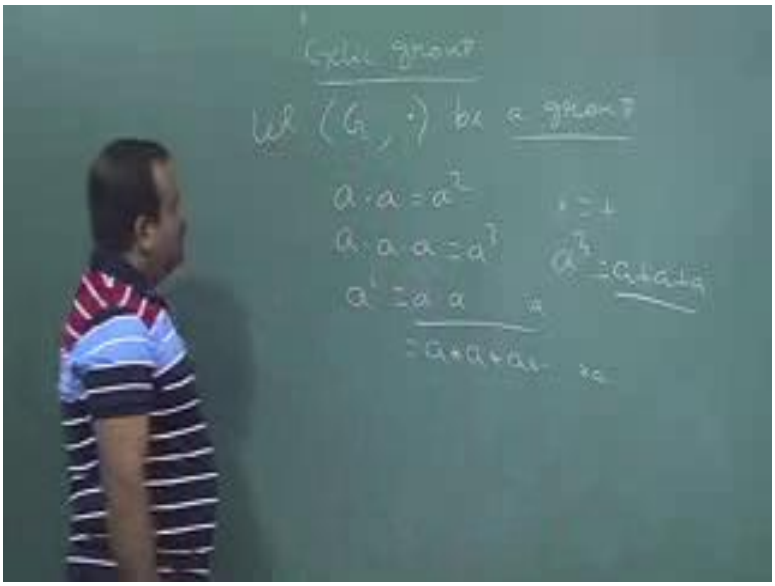
Now we will talk about cyclic group. So, let us come to the slide. So, this is the Abelian group, this is the extra property commutative property, if this property satisfied then we call a group is Abelian group, this is another property.

So, now we talk about cyclic group.

(Refer Slide Time: 27:29)

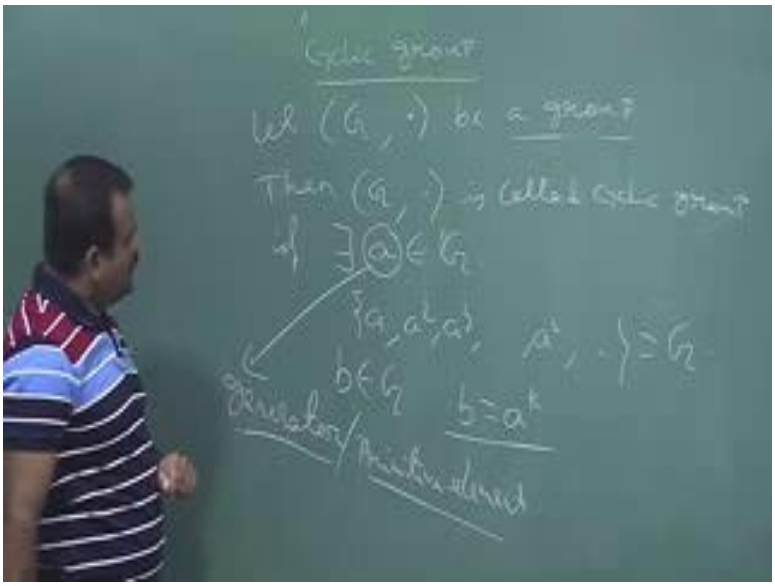


(Refer Slide Time: 27:33)



Now suppose we have a set a along with a operator, suppose let G this be a group. Now we are operating the operator is dot. So, a dot a we refer as a square, a dot a dot a we refer as a cube like this. So, this is in this multiplicative sense, but if it is plus then if the operator is plus, if the dot is plus, then a cube is basically a plus a plus a. So, this is I mean just a symbol, it is telling us we operate a 3 times like this. So, a to the power k is basically, a to the power i is basically a dot, a operate 5 times. So, if it is plus sense it is plus, if it is multiplicative sense in to like this, if it is star basically in general if the operator is star a star, a star, like this.

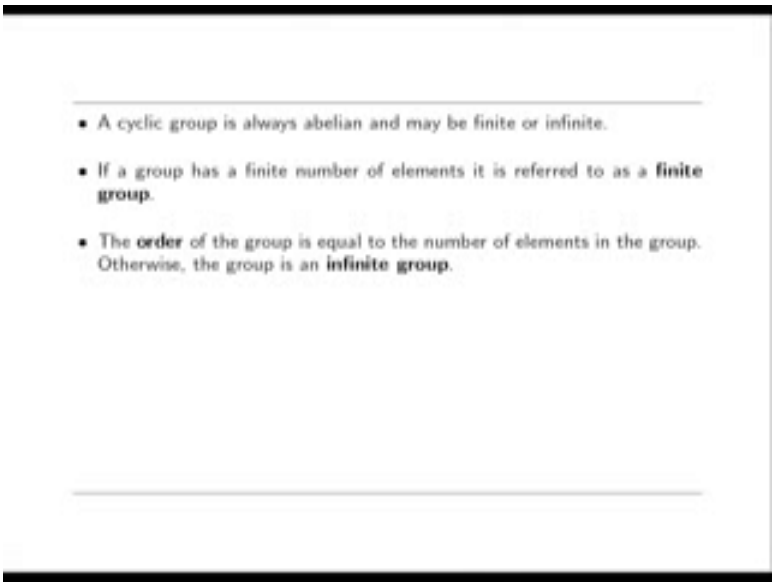
(Refer Slide Time: 29:08)



So, we call a group is a cyclic group, if there exists a element which is called the primitive element or generator of the group is called a cyclic group then G is called cyclic group, cyclic group if there exists an element a from G such that it generates the group. So, that means, if you take a, a square, a cube, a to the power i this set will be basically G.

So, that means, any element from G will be written as some sort of a to the power k; then this a is called generator of that group or generator or it is also called primitive element, primitive element of the group. If there exists a with generates this group, then we called this is a generator of this group and we call this group as a cyclic group if such a exist. So, this is the definition of cyclic group, and this is the convention we take a to the power 0 is basically e and a to the power minus n is basically referred as n times a inverse, and this we know if a group is cyclic if every element is written as a to the power k and then this is a is called the generator or the primitive element of the group.

(Refer Slide Time: 30:59)



And it can be shown that easily the cyclic group is always Abelian and but it could be finite or infinite, we see that if it is finite that will be useful for our computer, computer has a finite memory, finite I mean there is some constant on this and cyclic group has a important role in our cryptography.

Thank you.