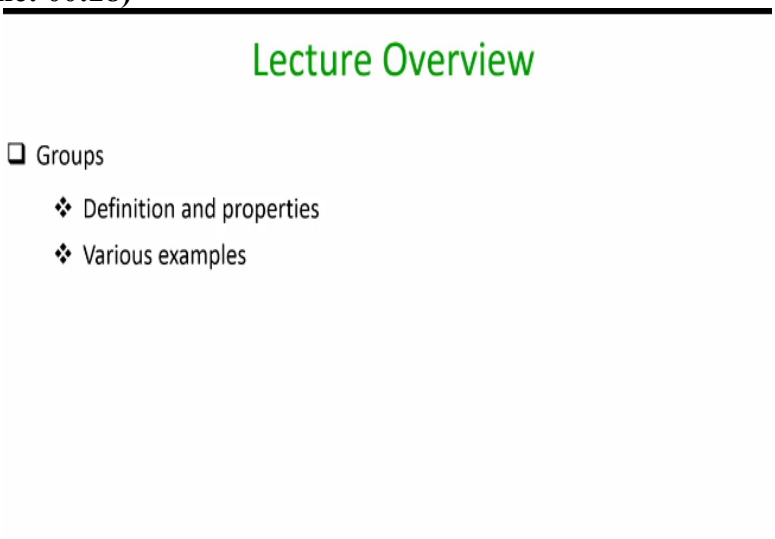
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology, Bangalore

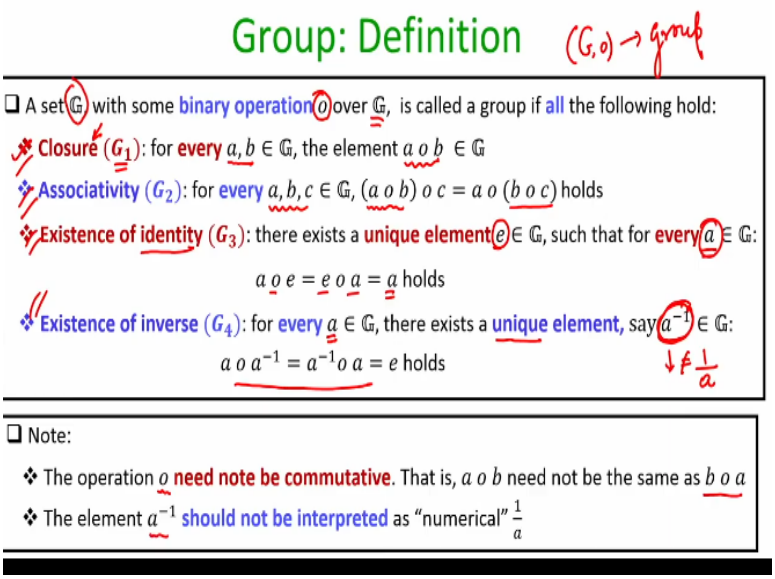
Lecture – 61
Group Theory

(Refer Slide Time: 00:28)



Hello everyone, welcome to this lecture. We will focus on abstract algebra for the next few lectures and we will start with group theory. So, the plan for this lecture is as follows: we will discuss the definition of groups and we will see various properties of groups. And we will also see various examples of groups.

(Refer Slide Time: 00:40)



So, let us start with the definition of group. So what is a group? Imagine you are given a set G, which may or may not be finite, and you are given some binary operation. By binary operation I mean it operates on 2 operands from G. So, G along with the operation $\circ$ will be called a group

if it satisfies certain properties, which we often call as group axioms. So, let us see what are the group axioms.

The first axiom which we call as G_1 is the *closure property* and the closure property demands that you take any 2 operands a, b from your set G, if you perform the operation $\circ$ on a and b the result should be an element of the set G itself. And hence the name closure. This is true for every a, b namely even when $a = b$ as well.

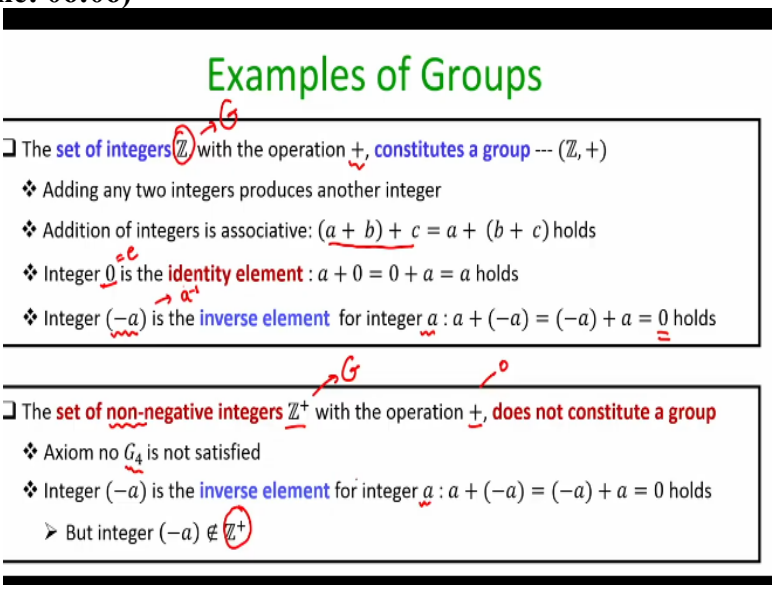
The second property or axiom is the *associativity property*, denoted by G_2, which demands that your operation $\circ$ should be associative i.e., the order of the operands does not matter. Namely, for every triplet of values a, b, c from G, $(a \circ b) \circ c = a \circ (b \circ c)$.

The third property or the axiom is the *existence of identity* denoted by G_3 which demands that there should be a unique element denoted by e present in G called as the *identity element* such that the identity element satisfies the following property for every group element. If you perform the operation $\circ$ on the element a and the identity element, you will obtain the same element a. And this holds even if you perform the operation on a and e or if you perform the operation on e and a i.e., $a \circ e = e \circ a = a$.

The fourth property and the last property which you require from a group is that of *existence of an inverse element*, which demands that corresponding to every element from the set G there should exist a unique element in G, which we denote by a^{-1}, such that the result of the group operation on a and a^{-1} (or vice versa) is the identity element i.e., $a \circ \mathrm{a}^{-1} = a^{-1} \circ \mathrm{a} = e$. I stress here that a^{-1} does **not** mean $\frac{1}{a}$. Rather it is just a notation for a special element which is required to be present in the group for this property to hold. So, if G along with the binary operation $\circ$ satisfies all these 4 axioms, then $(G,\circ)$ is a group.

Even if one of these 4 properties is violated, the set G along with operation $\circ$ would not be constitute a group. An important point to note here is that the axioms do not require the operation $\circ$ to be commutative. The group axioms only demand the operation $\circ$ be associative. That means, the result of performing the group operation on a and b need not be the same as the result of performing the group operation on b and a. Moreover, as discussed earlier, the element a^{-1} should not be interpreted as the numerical $\frac{1}{a}$.

(Refer Slide Time: 06:06)

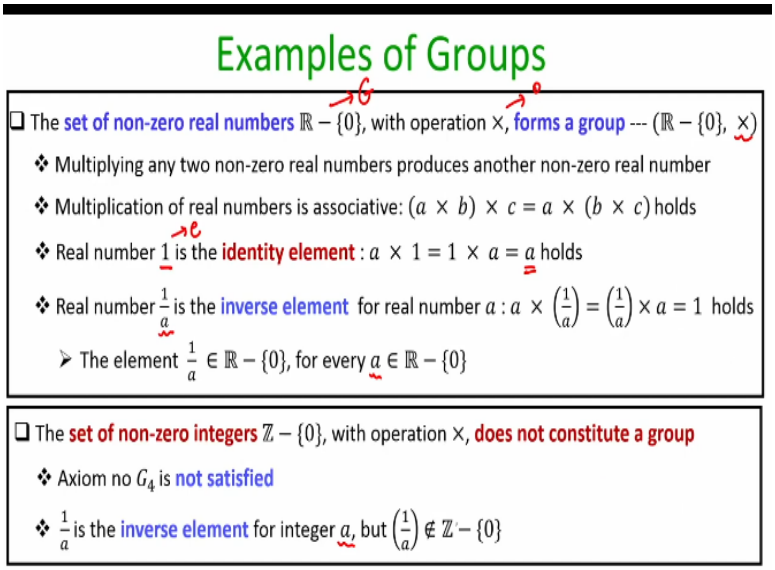


So now, let us see some examples of groups. So, the set of integers $\mathbb{Z}$ which is an infinite set along with the operation $+$ constitutes a group. So, let us see whether all the 4 properties are satisfied or not. So, the closure property is of course satisfied; you take any 2 integers a and b and add them you will again obtain an integer. The operation is associative over the integers too since if you take any 3 integers, it does not matter in what order you add them, the result will be the same.

The integer 0 is the identity element e because adding 0 to any integer a will result in the same integer a. And the integer $-a$ will be considered as the inverse of the integer a. So, this $-a$ is actually a^{-1} as per the notation and you can see that you take any integer a, its inverse is $-a$ because if you add $-a$ to a then the result will be 0, which is the identity element.

Here the set G was the set of integers. Now, let G be the set of non-negative integers $\mathbb{Z}^+$ i.e., negative integers are not included. The operation is still the same, namely $+$. Now, it is easy to see that this G along with the $+$ operation does not constitute a group. Which property is violated? Here the closure and associative properties are still satisfied and the identity element 0 is still present in G. The issue is that the fourth group axiom is not satisfied, because the inverse of an integer a will be $-a$, but $-a$ is not an element of $\mathbb{Z}^+$ because $-a$ is a negative integer.. Whereas the group axiom says that the inverse element also needs to be a member of the set G itself. So, that is why the set of non-negative integers along with the addition operation does not constitute a group.

(Refer Slide Time: 08:56)

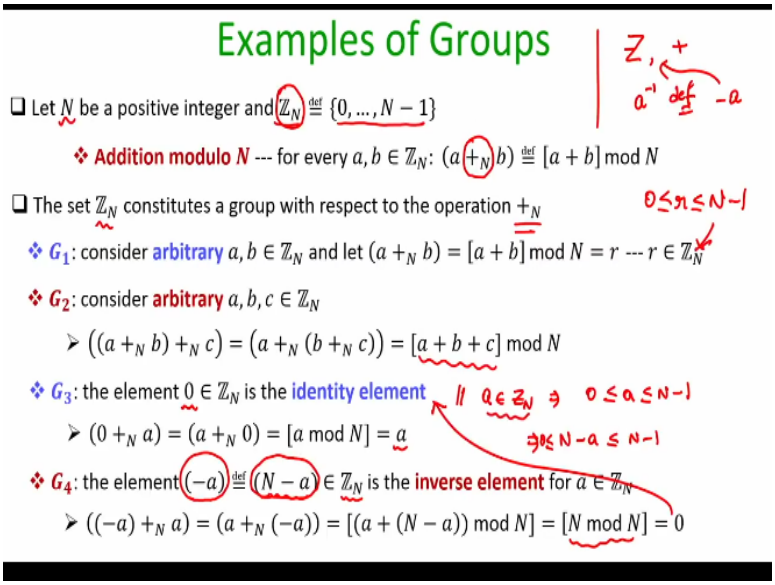


So, we have seen now a group with respect to the $+$ operation now let us see a group with respect to the multiplication operation. So, now my set G is the set of all real numbers excluding 0 and my operation $\circ$ is the multiplication operation and now you can see that all the 4 properties of group are satisfied.

Multiplying any two real numbers will give you a real number and multiplication is associative over the real numbers. The real number 1 is the identity element because you multiply 1 with any non-zero real number a, you will obtain the same non-zero real number a. And you take any non-zero real number a, its multiplicative inverse will be $\frac{1}{a}$. And $\frac{1}{a}$ is well defined because a is non-zero. So, $\frac{1}{a}$ indeed exists and it belongs to the set of non-zero real numbers. So all my 4 group axioms are satisfied and hence this set constitutes a group.

Whereas if I take the set of non-zero integers, then it does not constitute a group with respect to the multiplication operation. Now, let us see which property gets violated. So the closure property is still there, associativity property still satisfied, the identity element 1 is indeed present in the set of non-zero integers. The problem is that the existence of inverse is not guaranteed, because the inverse of an integer a will be $\frac{1}{a}$, but $\frac{1}{a}$ may be a real number, it might not be an integer. So that is why the fourth property is violated due to which this does not constitute a group.

(Refer Slide Time: 10:52)



Now let us see some other interesting examples of groups. So let N be a positive integer and let $\mathbb{Z}_N$ be the set of integers 0 to $N-1$. Basically, it is the set of all possible remainders which you can obtain by dividing any integer, it could be either positive or negative, by N.

Now I define a new form of addition over this set called *addition modulo* N, which is denoted by $+_N$. So, addition modulo N of a and b is defined as follows: I add a and b and then take modulo N, the result will be called as the result of addition of a and b modulo N i.e., $a+_N b = [a+b] \bmod N$. So, now my claim is that this set $\mathbb{Z}_N$, which is a finite set because N is a positive integer, constitutes a group with respect to this operation of addition modulo N.

So, let us see whether the 4 properties are satisfied or not. So the closure property is indeed satisfied. You take any integer a and b in the range 0 to $N-1$, you add them and then if you take modulo N, the result will be r. And r of course, will be in the range 0 to $N-1$, so hence it is a member of $\mathbb{Z}_N$. So, closure property is satisfied. It is easy to see that the operation of addition modulo N is indeed associative because it does not matter in what order you perform the addition modulo N over 3 values a, b, c the result will be the same as $a + b + c$ modulo N.

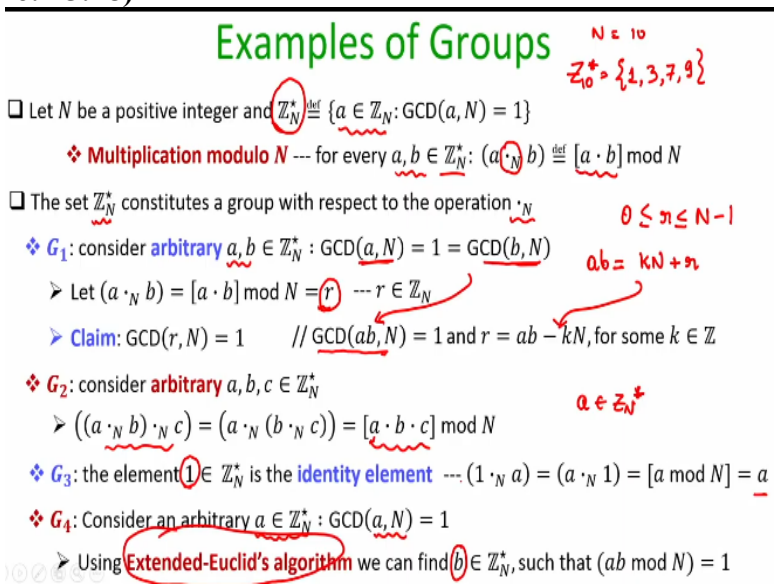
The element 0 which is indeed present in $\mathbb{Z}_N$ and will be the identity element because if I add 0 to any element a from $\mathbb{Z}_N$ and take modulo N the result will be a itself because a is a member of $\mathbb{Z}_N$ and is in the range 0 to $N-1$. Now, if I add 0 to a, the value of a does not get incremented, it remains the same. And now if I take modulo N the effect of mod will not

actually take place, because my value a at the first place itself is less than $N - 1$, so the result will be a.

Now, what about the inverse? So, my claim is that the number $-a$ which is defined to be $N - a$ in the context of this operation addition modulo N, constitutes the inverse for any element a. Recall that when the group was taken to be the set of integers and the operation was regular addition then a inverse was defined to be $-a$ and $-a$ indeed belongs to the set of integers. So, the $-a$ in the context of set of integers modulo N will be defined to be $N - a$ and it is easy to see that $N - a$ is again an element of $\mathbb{Z}_N$ because if a belongs to $\mathbb{Z}_N$ that means a is in the range 0 to N-1 then that automatically implies that $N - a$ is also within the range 0 to $N - 1$. Thus the inverse is a member of $\mathbb{Z}_N$ and property of this $-a$ is that if you add it with any a and then if you take modulo N the result will be N modulo N which is 0, the identity element.

So, this is now an interesting example of a variation of addition operation with respect to a set and together they constitute a group.

(Refer Slide Time: 15:28)



Now let us see a corresponding variation of the multiplication operation, which we call as multiplication modulo N. So, let $\mathbb{Z}_N^*$ be the set of all integers a in the set $\mathbb{Z}_N$ which are co-prime to the modulus N. So for instance, if $N = 10$ then $\mathbb{Z}_{10}^* = \{1,3,7,9\}$ since the remaining set of elements in $\mathbb{Z}_{10}$, namely $\{0, 2, 4, 5, 6, 8\}$, are not co-prime to 10.

And now, we define a new operation called multiplication modulo N which is a variation of multiplication over the elements of $\mathbb{Z}_N^*$ and denoted by $\cdot_N$. So, the result of a multiplication

modulo N with b will be the following: I multiply a with b and then take modulo N i.e., $[a \cdot b] \bmod N$. And my claim is that this set $\mathbb{Z}_N^*$ with respect to this operation of multiplication modulo N constitutes a group.

So, let us see whether the closure property is satisfied or not. So, for closure property I have to prove that the product of any pair of integers a, b from the set $\mathbb{Z}_N^*$ modulo N is also a member of $\mathbb{Z}_N^*$. Since a and b are members of $\mathbb{Z}_N^*$ they are individually co-prime to N. Now let r be the result of ab modulo N that means, I multiply a with b and then take mod N, I get the remainder r. Of course, r will be in the range 0 to $N - 1$, but that does not show the closure property because I have to show that r belongs to $\mathbb{Z}_N^*$. Namely, I have to show that r is also co-prime to my modulus N. And indeed my claim is that r is co-prime to the modulus N because since a is individually co-prime to N, b is individually co-prime to N, I get the conclusion that ab is also co-prime to N. Because if ab is not co-prime to N that means, if there is some common prime factor p which divides ab and N then I get a contradiction that either a is not co-prime to N, namely the same prime is a common factor of a and N, or b is not co-prime to N which is a contradiction. So, ab is co-prime to N and from the rules of division I know that r is ab minus some multiple of N because r is the remainder which you obtain by dividing ab by N i.e., $r = ab - kN$ where k is an integer. So, now since ab is co-prime to N and r is $ab - kN$, we get the conclusion that indeed r is co-prime to N. So that shows the closure property.

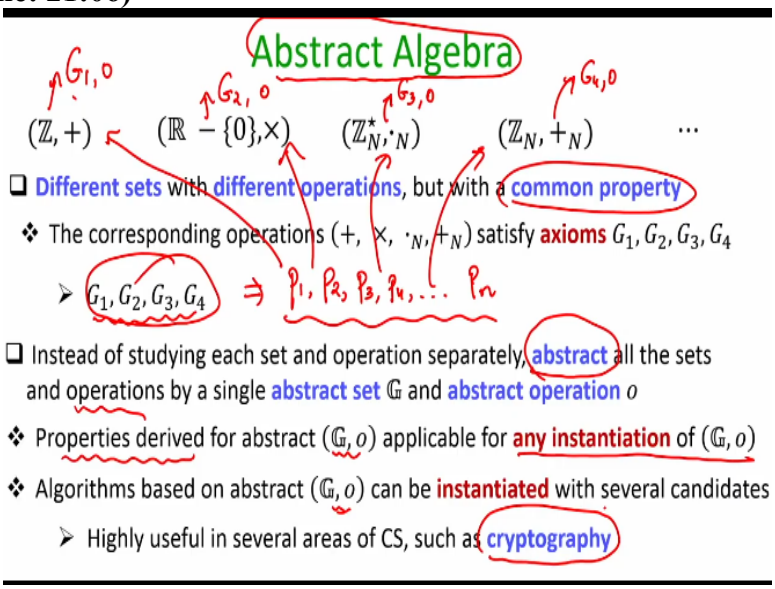
Now, let us see whether the operation multiplication modulo N is associative or not. And it is associative because if you take a triplet of integers a, b, c from $\mathbb{Z}_N^*$ it does not matter in what order you perform multiplication modulo N the result will be the same that you will obtain by multiplying a, b, c and then taking modulo N.

The element 1 is always present in $\mathbb{Z}_N^*$ and it is the identity element because you take any element a belonging to $\mathbb{Z}_N^*$ and multiply 1 with a then if upon taking modulo N the result will be a itself because a is member of $\mathbb{Z}_N^*$ and is thus strictly less than N so the effect of mod will not take place.

And now, I can claim that for every integer a belonging to $\mathbb{Z}_N^*$, since the GCD of a and N is 1 then recall that in one of the earlier lectures we proved that if a is co-prime to N then multiplicative inverse of a modulo N exists; that means there always exist an integer b which

will be a member of $\mathbb{Z}_N^*$ such that if you multiply a with b and then if you take mod N the result will be 1. And that b you can always find out using extended Euclid's algorithm. So that shows that this $\mathbb{Z}_N^*$ along with this variation of multiplication namely multiplication modulo N constitutes a group.

(Refer Slide Time: 21:06)



So, now we have seen examples of several groups. Namely we have seen examples of 4 groups, each group has a different structure; namely their elements were different and the operations were also different. And these are not the only examples of groups, I can give you infinitely many examples.

Now, the point is that even though they are different sets with different operations they have a common property, and what is the common property? All of them satisfy the 4 group axioms. So, what we can now do is instead of studying and deriving properties for each of these sets individually and separately, we will abstract out all these sets by a common template. And all the operations that were available with respect to the individual sets, they are also abstracted by a single operation $\circ$.

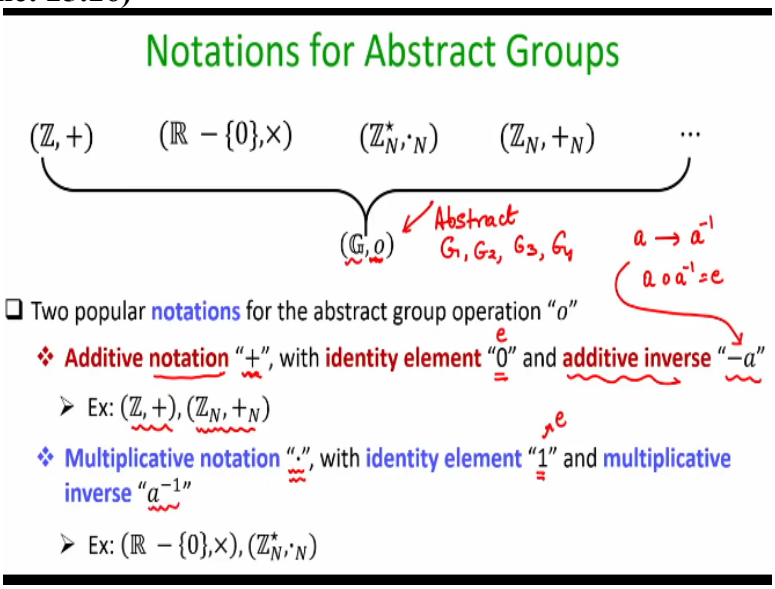
And then, we will study the abstract set and along with the corresponding abstract operation assuming that they satisfy these 4 properties and we will derive whatever interesting properties that we can derive for the abstract set and the abstract operation. And now, I can say that whatever properties that I have derived for the abstract G and abstract $\circ$, they hold for any instantiation of the abstract G and abstract $\circ$.

What I mean by that is, assuming that the properties G_1, G_2, G_3, G_4 are satisfied for this abstract G and $\circ$ and say based on these properties, I derived several interesting properties say $p_1, p_2, p_3, p_4, p_5 \ldots p_n$. Then I can say that all these properties $p_1, p_2, p_3, p_4, \ldots, p_n$ holds for any instantiation of the group.

And this is very interesting, because I am not deriving these properties separately and individually for each set but rather deriving it once and for all for this abstract group G with the abstract operation $\circ$. So, that is why abstract algebra is a very interesting topic in computer science because once we do this abstraction and derive algorithms or properties for this abstract group and abstract operation, then depending upon our requirement and our application, we can instantiate the group and operation with some concrete set and concrete operation and then apply these properties that we have derived on those corresponding concrete instantiations. And this is very helpful in several areas of computer science, especially in cryptography which we will see later.

So that is why when we say abstract algebra, it might look very abstract to you, because we are talking about an abstract set and abstract operation and keep on deriving properties, but when we instantiate those sets and operations by a concrete group and concrete operation and then fit it in an application, then you will see the real application of the theory that we are developing in the abstract algebra.

(Refer Slide Time: 25:26)



So now, what we will do is from now onwards, we will not be focusing on concrete groups and the corresponding operation but rather we will be focusing on an abstract group and

corresponding operation. So, I will say that, my G is a group, I do not care what exactly are the elements of my group G, I will just give them some names. I would not know whether they are integers, whether they are real numbers, whether they are vectors, whether they are matrices, I will not go into the exact instantiation.

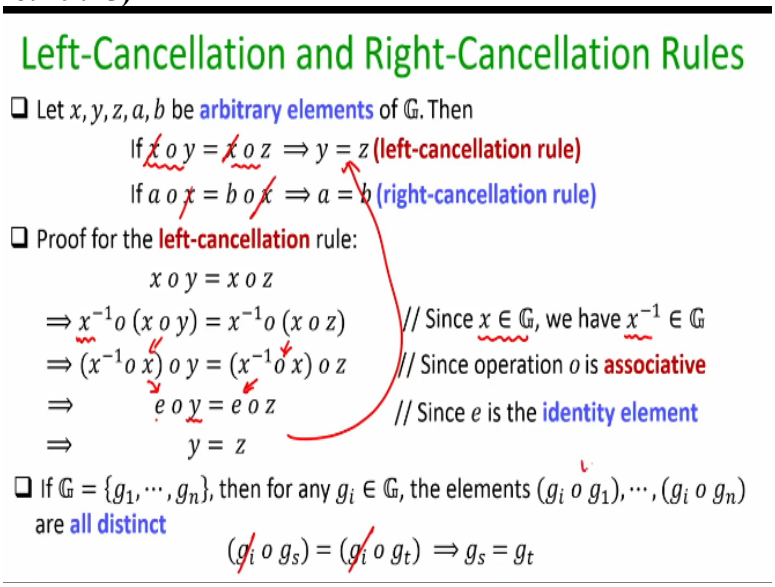
And in the same way, I will denote my corresponding group operation by $\circ$, I will not go into the details whether my operation $\circ$ is the numerical addition, numerical multiplication or whether it is addition modulo N or whether it is multiplication modulo N or whether it is matrix multiplication or whether it is dot product of vector or scalar product of vector and so on.

And then I will just assume that my group axioms G_1, G_2, G_3, G_4 are satisfied, and derive whatever interesting properties I can derive for the groups. So, it turns out that there are 2 popular notations which are used for the abstract group operation $\circ$. The first notation is the *additive notation*, and I stress that this is just a notation, where instead of $\circ$ we will use the plus $(+)$ symbol and the identity element e will be denoted by 0. So I stress here that this plus is not a numerical plus and 0 is not the numerical 0; it is just a notation that we are following. If you do not want to bring the plus and 0, you can just stick to your operation $\circ$ itself and you can use e as your identity element. But since we are very much habituated to plus and 0 that is why sometimes we find it convenient to use instead the additive notation. In the additive notation the *additive inverse* of any element a in the group, namely the inverse of a under the group operation, is denoted by $-a$.

So, examples of groups which come under the umbrella of additive notations are $(\mathbb{Z}, +)$ and $(\mathbb{Z}_N, +_N)$. So, you can recall that the set of integers with the operation plus was actually an additive group, the set of integers modulo N along with the operation addition modulo N forms under the umbrella of additive group and so on.

Whereas another popular notation, which is used for abstract group operation is the *multiplicative notation* where the operation $\circ$ is instead represented by the dot $(\cdot)$. But this dot does not mean numerical multiplication, this is just a representation for convenience. And if I am following the multiplicative notation, then the identity element e will be represented by 1. And the multiplicative inverse of a will be represented by a^{-1}. Again, a^{-1} does not mean $\frac{1}{a}$ it is just a representation if I am following the multiplicative notation.

(Refer Slide Time: 29:15)



So, now let us derive some nice properties that are true for any abstract group. So the first property that I am going to derive are the *left cancellation rule* and the *right cancellation rules*. So, the left cancelation rule says the following: if you take any arbitrary group elements x, y, z, a, b from the group and if it is the case that that $x \circ y = x \circ z$ then I can conclude that $y = z$ and this is called as the left cancellation rule. Why cancellation? Because from the implication I can say that this has the same effect as if I am cancelling out x.

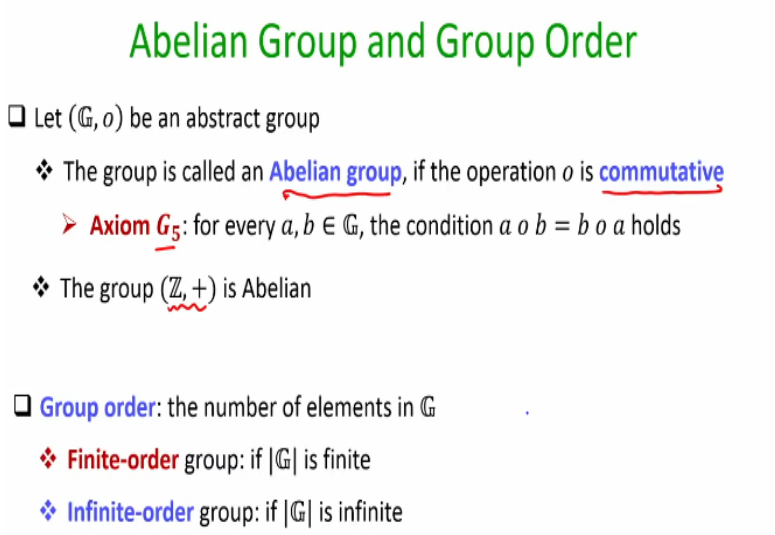
And in the same way you have a corresponding right cancelation rule. Namely, the rule says that if $a \circ x = b \circ x$ then you can cancel out x and conclude that $a = b$. So, let us prove the left cancellation rule, the similar proof you can give for the right cancellation rule. And I will give the proof for any abstract group G along with the corresponding abstract operation $\circ$. And I will give a direct proof. So imagine that your premise for the left cancelation rule is true, namely, $x \circ y = x \circ z$.

Since x is an arbitrary element of the group, the inverse of x is also present in the group. Thus the result of $x^{-1} \circ (x \circ y)$ will be the same as $x^{-1} \circ (x \circ z)$. And now, since my operation $\circ$ is associative, I can rearrange the terms here on the left hand side as well as on the right hand side but from the property of inverse we get $x^{-1} \circ x = e$ which is the identity element. Since the property of the identity element is that if you perform the operation on the identity element and any element y you will obtain the same element y, we arrive at the conclusion that $y = z$, proving the left cancellation rule. A similar proof can be given for the right cancellation rule.

Now, an interesting corollary of the left cancellation rule and the right cancellation rule is the following. Imagine you take a group which has say n number of elements, $g_1, \ldots, g_n$ and you take any group element g_i. Now, if you perform the group operation on g_i and various elements of the group, say you perform the operation on g_i and g_1, g_i and g_2 and so on till g_i and g_n; of course, from the closure property all of them will be elements of the group itself. The question is whether the results that are obtained will be same or different. So, I will obtain n elements, so call the first value that I obtained as a_1, call the second value that I obtained as a_2 and call the last result that I obtained as a_n.

The claim here is that the result that I will obtain, namely a_1 to a_n, are all distinct. This is because, suppose the result of $g_i \circ g_s = g_i \circ g_t$ then from my left cancelation rule, I come to the conclusion that $g_s = g_t$. So, contra positively, if g_s and g_t are different then the result of $g_i \circ g_s$ is different from $g_i \circ g_t$, which shows that each of this results are distinct.

(Refer Slide Time: 33:25)



A group is called as an *Abelian group*, if it is a group and it satisfies an extra axiom, namely a fifth axiom, which says that operation $\circ$ is commutative. So, it is not the case that every group is Abelian because the operation $\circ$ may or may not be commutative, but if the operation $\circ$ is commutative, then my resultant group is called as an Abelian group. So, for instance, the set of integers with respect to the plus operation is Abelian and there are other examples of Abelian group as well.

The *group order* is basically the number of elements in the group G. Now, depending upon whether the number of elements is finite or infinite; namely, whether the cardinality is finite or infinite, the group order is either finite or infinite.

So with that, I conclude today's lecture. Just to summarize in this lecture, we started our discussion on abstract algebra. We discussed about the definition of groups, abelian groups we saw various examples and we also saw left cancellation rule and the right cancellation rule. Thank you.