

Secure Computation - Part I
Prof. Ashish Choudhury
Department of Computer Science
International Institute of Information Technology, Bangalore

Module - 1
Lecture - 4
Recap of Basic Concepts from Abstract Algebra

(Refer Slide Time: 00:32)

Lecture Overview

- Group
 - ❖ Definition and properties
 - ❖ Examples


Hello everyone. Welcome to this lecture. The plan for this lecture is as follows: In this lecture, we will recap some of the basic facts about algebraic structures. Specifically, we will consider groups. We will discuss the definition of groups, the properties of groups, and we will see some examples of groups. Looking ahead, these concepts will be used when we will design protocols for secure multi-party computation.

(Refer Slide Time: 01:02)

Group: Definition ↗ Group axioms

□ A set G , with some binary operation \circ over G , is called a group if all the following hold:

❖ Closure (G_1): for every $a, b \in G$, the element $a \circ b \in G$



So, let us begin with the definition of a group. Consider a set G with some binary operation small \circ . And when I say binary operation, by that I mean it operates over 2 operands, and both the operands will be from your set G . So, the set G along with this operation \circ will be called a group, if certain conditions are satisfied. So, let us see what those conditions are. Those conditions are often called group axioms.

So, let us see those group axioms. So, the first group axiom is the closure property, which I denote by G_1 . You can imagine G_1 to be property number 1. The closure property demands that you take any pair of elements a and b from the set; I stress - any pair of elements; so, that means, your a could be same as b as well, or your a could be different from b .

So, the closure property demands that if you take any pair of elements from the set G and you perform the operation small \circ , treating the elements a and b as the operands, then the result should be an element of the set G itself. That is why it is called closure property. Closure in the sense; imagine G is a big circle which has several elements. And you take any 2 elements from this circle, a and b , and you perform the operation $a \circ b$.

You will obtain some element $c = a \circ b$. That element c should also lie within the circle itself; it should not go outside the set capital G . That is why the term closure property. And this should hold for every pair of elements a and b from the set capital G . That is a closure property.

(Refer Slide Time: 03:26)

Group: Definition ↗ Group axioms

□ A set \mathbb{G} , with some **binary operation** \circ over \mathbb{G} , is called a group if **all** the following hold:

❖ **Closure (G_1)**: for **every** $a, b \in \mathbb{G}$, the element $a \circ b \in \mathbb{G}$

❖ **Associativity (G_2)**: for **every** $a, b, c \in \mathbb{G}$, $(a \circ b) \circ c = a \circ (b \circ c)$ holds



The second property is the associativity property, which says the following: You take any triplet of elements a, b, c . Again, any possible triplet; that means, it could be the case that a, b and c are all different; it could be the case that all of them are same; it could be the case that a and b are same, c is different and so on. So, the associativity property demands that it does not matter which triplet of elements you choose from the set capital G .

If you first perform the operation $a \circ b$, and then you take the result and apply the operation \circ with c , then you get a same element which you obtain by first performing the operation $b \circ c$, and then, applying the operation \circ with the result and the element a as the operands. That means, it does not matter in order to perform the operation \circ involving these triplets of elements, the result will be the same group element. So, if this property holds, then we say that associativity axiom is satisfied. So, that is a second requirement from a group.

(Refer Slide Time: 04:48)

Group: Definition ↗ Group axioms

□ A set G , with some **binary operation** \circ over G , is called a group if **all** the following hold:

- ❖ **Closure (G_1)**: for every $a, b \in G$, the element $a \circ b \in G$ $G = \{a_1, \dots, a_n, e\}$
- ❖ **Associativity (G_2)**: for every $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$ holds $a_1 \circ e = a_1$
 $a_2 \circ e = a_2$
- ❖ **Existence of identity (G_3)**: there exists a **unique element** $e \in G$, such that for **every** $a \in G$: $a_n \circ e = a_n$
 $e \circ e = e$

$a \circ e = e \circ a = \underline{a}$ holds

The third axiom that should be satisfied is the presence of a special element which we call as the identity element. So, there should exist some special element; let us call it e ; and that element should be a member of the set G itself. And that element will be called as the identity element. So, what do I mean by the identity element? By identity element, I mean that; you take any element a from the set G and you perform the operation $a \circ e$.

You should get back the element a . So, that means, if your G is $\{a_1, a_2, \dots, a_n\}$, and there is some special element e there. What we demand is that e should have the property that, if you perform the operation involving a_1 and e , you should get back a_1 . If you perform the operation between a_2 and e , you should get back a_2 . If you perform the operation between a_n and e , you should get back the element a_n .

And in fact, if you perform the operation involving e and e , you should get back e , because this requirement is for every a from the set G . So, even e will also be considered as an element. If such a special element e is present, then we say that it is the identity element. And the third group axiom demands that your set G should have the identity element with respect to your operation \circ .

(Refer Slide Time: 06:35)

(G, \circ) : group **Group: Definition** *Group axioms*

□ A set \mathbb{G} , with some **binary operation** \circ over \mathbb{G} , is called a group if **all** the following hold:

- ❖ **Closure (G_1)**: for **every** $a, b \in \mathbb{G}$, the element $a \circ b \in \mathbb{G}$ $G = \{a_1, \dots, a_n, e\}$
- ❖ **Associativity (G_2)**: for **every** $a, b, c \in \mathbb{G}$, $(a \circ b) \circ c = a \circ (b \circ c)$ holds $a_1 \circ e = a_1$
 $a_2 \circ e = a_2$
- ❖ **Existence of identity (G_3)**: there exists a **unique element** $e \in \mathbb{G}$, such that for **every** $a \in \mathbb{G}$:
 $a \circ e = e \circ a = a$ holds \rightarrow identity element with respect to operation \circ
- ❖ **Existence of inverse (G_4)**: for **every** $a \in \mathbb{G}$, there exists a **unique element**, say $a^{-1} \in \mathbb{G}$:
 $a \circ a^{-1} = a^{-1} \circ a = e$ holds

□ Note: a^{-1} is not same as $\frac{1}{a}$

- ❖ The operation \circ **need not be commutative**. That is, $a \circ b$ need not be the same as $b \circ a$
- ❖ The element a^{-1} **should not be interpreted** as "numerical" $\frac{1}{a}$

So, this element e will be considered as the identity element with respect to operation \circ . And the fourth group axiom demands the presence of an inverse element for every element small a in your set G . So, what does it mean? The demand here is that, you take any element a from the set G , corresponding to this element a , there should exist some element from the set G . Let us use the notation a^{-1} for that element.

And the property of that element a^{-1} should be the following: If you perform $a \circ a^{-1}$, you should get back the identity element e . If that is the case, then we say that a^{-1} is the inverse element for the element a with respect to the operation \circ . So, if your set G is such that operation \circ satisfies the closure property, associativity property, the existence of identity is guaranteed and the existence of inverse is guaranteed, then the set G along with the operation \circ will be considered as a group.

Whereas, even if one of these 4 properties is violated, then G is not be considered as a group. So, before I proceed further, few remarks here. The operation \circ need not be commutative. That means, it is not necessary that the result of $a \circ b$ and the result of $b \circ a$ is the same group element. Of course, there will be some group element because of the closure property, but that does not mean that $a \circ b = b \circ a$, even though the associativity property is true.

That is a first thing to note here. And a second important thing to note here is that this notation a^{-1} is just a notation for a special element denoting the inverse of the element a . You should not consider it as a^{-1} in the numerical sense, namely, you should not consider a^{-1} to be same

as $\frac{1}{a}$. Because, at the first place, the element a need not be an integer value, it is just an abstract element from an abstract set G . It is just a representation.

(Refer Slide Time: 09:54)

Examples of Groups

$G = \mathbb{Z}$
 $\circ = +$

□ The set of integers \mathbb{Z} with the operation $+$, constitutes a group $(\mathbb{Z}, +)$

- ❖ Adding any two integers produces another integer - closure if $a, b \in \mathbb{Z} \Rightarrow a+b \in \mathbb{Z}$
- ❖ Addition of integers is associative: $(a + b) + c = a + (b + c)$ holds + operation is associative
- ❖ Integer 0 is the identity element: $a + 0 = 0 + a = a$ holds $a^{-1} = (-a)$
- ❖ Integer $(-a)$ is the inverse element for integer a : $a + (-a) = (-a) + a = 0$ holds

$\mathbb{Z}^+ = \{0, 1, 2, \dots\}$

□ The set of non-negative integers \mathbb{Z}^+ with the operation $+$, does not constitute a group

- ❖ Axiom G_4 is not satisfied \times if $a = 2 \Rightarrow$ inverse of a will be $-2 \notin \mathbb{Z}^+$
- ❖ Integer $(-a)$ is the inverse element for integer a : $a + (-a) = (-a) + a = 0$ holds
- But integer $(-a) \notin \mathbb{Z}^+$

So, now, let us see some examples of groups. We will start with the groups which all of us are familiar with, and then we will introduce some of the interesting class of groups which we will encounter in this course. So, all of us are familiar with the set of integers which I denote by this notation \mathbb{Z} , and you consider the operation $+$. So, that means, I am considering my set G , the abstract set G in the previous slide, to be the set of integers. And, I am considering the operation \circ to be the plus operation.

Now, let us see whether all the group axioms are satisfied with respect to this set of integers and the plus operation. So, the closure property is guaranteed, because, you take any 2 integers a and b , then their summation will also be an integer and will be a member of the set \mathbb{Z} . The associative, the plus operation, namely the integer addition operation is associative. That means, it does not matter in what order you add a, b and c , you will obtain the same result, same answer.

The integer 0 will be the identity element, because, you add 0 to any element a , any integer a , you will get back the integer a . And the integer $-a$ will be the inverse element for the integer a , because if you add $-a$ to the integer a , you will get back the identity element which is 0 . So, here, a^{-1} is nothing but $-a$, as per our notation for inverse of a .

So, now, if you are wondering that why I am considering the set of integers, why can't I take the set of non-negative integers? By non-negative integers, I mean all the positive integers along with 0. So, that set is denoted by this notation. Now, let us consider this set \mathbb{Z}^+ and the operation to be the integer addition, and let us see whether all the 4 group axioms are satisfied or not.

So, of course, closure property will be satisfied, because, you take any 2 positive integers, add them, you will again obtain a positive integer. Addition of integers is anyhow associative.

So, my axiom G_3 is also satisfied, because the integer 0 will be the identity element. But, the fourth requirement, namely, the fourth group axiom is not satisfied, because, if you take any positive integer, say $a = 2$, then the inverse of a will be the integer -2 . But -2 does not belong to the set \mathbb{Z}^+ , because the set \mathbb{Z}^+ is not allowed to include the negative integers. So, even though the inverse is there, the inverse is not present in the set \mathbb{Z}^+ .

Whereas, the requirement of the inverse is that, it should be a member of the set itself. So, that is why, the axiom number G_4 , the fourth group axiom is not satisfied, and that is why the set of non-negative integers with respect to the integer addition does not constitute a group.

(Refer Slide Time: 14:31)

Examples of Groups

$G = \mathbb{R} - \{0\}$
 $\circ = \times$

□ The set of non-zero real numbers $\mathbb{R} - \{0\}$, with operation \times , forms a group --- $(\mathbb{R} - \{0\}, \times)$

- ❖ Multiplying any two non-zero real numbers produces another non-zero real number
- ❖ Multiplication of real numbers is associative: $(a \times b) \times c = a \times (b \times c)$ holds
- ❖ Real number 1 is the identity element: $a \times 1 = 1 \times a = a$ holds
- ❖ Real number $\frac{1}{a}$ is the inverse element for real number a : $a \times \left(\frac{1}{a}\right) = \left(\frac{1}{a}\right) \times a = 1$ holds

➤ The element $\frac{1}{a} \in \mathbb{R} - \{0\}$, for every $a \in \mathbb{R} - \{0\}$

□ The set of non-zero integers $\mathbb{Z} - \{0\}$ with operation \times , does not constitute a group

- ❖ Axiom G_4 is not satisfied
- ❖ $\frac{1}{a}$ is the inverse element for integer a , but $\left(\frac{1}{a}\right) \notin \mathbb{Z} - \{0\}$

If $a = 2$ then
 $a^{-1} = \frac{1}{2} \notin \mathbb{Z} - \{0\}$

So, now, let us see another very simple example of a group. So, consider the set of non-zero real numbers. So, the set of real numbers is denoted by this notation our capital \mathbb{R} , but I am excluding 0 from it. And my operation is now the multiplication operation, usual multiplication operation. And now, let us see whether all the group properties are satisfied. So, the closure is

satisfied, because, you take any 2 non-zero real numbers, you multiply them, the result again will be a non-zero real number.

The multiplication operation is anyhow associative. So, it does not matter in what order you multiply three non-zero real numbers a, b, c , you will get the same result. The real number 1, which is a non-zero real number, will be the identity element for every non-zero real number. Because, you take any non-zero real number a , and multiply it with the element 1, you will get back the element a . And what will be the inverse element?

So, if you consider a real number a , its inverse will be $\frac{1}{a}$, because, when you multiply $\frac{1}{a}$ with a , you will get back the identity element which is 1. And the element $\frac{1}{a}$ is well-defined. Why it is well-defined? Because, since a is a non-zero real number, a cannot take the value 0. And that is why $\frac{1}{a}$ is well-defined. And $\frac{1}{a}$ is also going to be a non-zero real number.

And it will be a member of your set $\mathbb{R} - \{0\}$. So, in this case, the abstract set G is the set of real numbers excluding 0. And your abstract operation small \circ is basically the multiplication operation. And we have shown that all the 4 properties are satisfied. That is why it constitutes a group. So, now, you might be wondering what happens if I include 0 as well in this. That means, if I consider the full set of real numbers and my operation is multiplication, will it constitute a group?

Well, the answer is no, because the inverse element is not defined for the element 0. Because, the inverse will be $\frac{1}{0}$, and $\frac{1}{0}$ is not well-defined, it is not a member of the set of real numbers. So, that is why we are excluding 0 here, and then only we can prove the group axioms. So, now, let us discuss why we have considered the set of real numbers, why not the set of non-zero integers.

Can we say that the set of non-zero integers constitute a group with respect to the multiplication operation? So, let us see which properties are satisfied. So, the closure will be satisfied, because, you take any 2 non-zero integers, multiply them, the result will be again a non-zero integer. Multiplication operation is anyhow associative. The integer 1 will be a member of this

set and will be the identity element, but the problem is that the inverse for an integer is not well-defined.

Say for example, if $a = 2$, then the inverse of a will be $\frac{1}{2}$, but $\frac{1}{2}$ is not a member of the set of non-zero integers, it belongs to the set of real numbers. So, that is why axiom 4 is not satisfied. And hence, the set of non-zero integers do not satisfy the group axioms. So, we have seen till now, examples of groups which we are familiar with, namely the set of integers, real numbers and so on.

(Refer Slide Time: 18:56)

Examples of Groups

- Let N be a positive integer and $\mathbb{Z}_N \stackrel{\text{def}}{=} \{0, \dots, N-1\}$ / As the set of integers modulo N
- ❖ Addition modulo N --- for every $a, b \in \mathbb{Z}_N$: $(a \oplus_N b) \stackrel{\text{def}}{=} [a + b] \bmod N$
- The set \mathbb{Z}_N constitutes a group with respect to the operation \oplus_N $G = \mathbb{Z}_N, 0 = \oplus_N$
- ❖ G_1 : consider arbitrary $a, b \in \mathbb{Z}_N$ and let $(a \oplus_N b) = [a + b] \bmod N = r$ --- $r \in \mathbb{Z}_N$
- ❖ G_2 : consider arbitrary $a, b, c \in \mathbb{Z}_N$
 - $((a \oplus_N b) \oplus_N c) = (a \oplus_N (b \oplus_N c)) = [a + b + c] \bmod N$
- ❖ G_3 : the element $0 \in \mathbb{Z}_N$ is the identity element $a \in \{0, \dots, N-1\}$
 $a + 0 = a$
 $a \bmod N = a$
 - $(0 \oplus_N a) = (a \oplus_N 0) = [a \bmod N] = a$

Now, we will introduce 2 interesting groups, which we will encounter later when we design MPC protocols. So, the first group I define here is the set \mathbb{Z}_N . And what is the set \mathbb{Z}_N ? It is a collection of integers 0 to $N - 1$. And basically, you can interpret this set \mathbb{Z}_N as the set of integers modulo N . What does that mean? You take any integer. So, you have the set of integers.

We have the number line 0, 1, 2; then in the positive direction you go towards ∞ , and in the negative direction you go towards $-\infty$. This is your set of integers \mathbb{Z} . You take any integer and divide it by the number N , you will obtain a remainder. And the remainder will be in the range $\{0, \dots, N - 1\}$. You divide any integer, the remainder will be in the range $\{0, \dots, N - 1\}$.

So, that is why you can imagine that set \mathbb{Z}_N is basically the entire infinite set of integers reduced modulo N . So, basically, I am collapsing an infinite set to a finite set by taking modulus with

respect to N . So, that is the interpretation of your set \mathbb{Z}_N here. And I am going to define a special plus operation here. So, this is called addition, but modulo N . And the notation that we use for this special plus operation is $+_N$.

So, you have the usual plus operation, and then, in the subscript you have the modulus N . And how this addition operation is performed? So, if you have 2 numbers a and b in this set $\{0, \dots, N - 1\}$. And if you want to obtain the result of $+_N$, what you do is, you first add the 2 numbers a and b , as per the usual addition operation, and then you take the modulo N . That will be the overall result of $(a + b) \% N$.

That is my definition of addition modulo N . Now, my claim is that if I consider my abstract G to be \mathbb{Z}_N , and if I consider the abstract operation to be this operation of $+_N$, then all the group axioms are satisfied. Let us see. So, you take any pair of elements a, b from the set \mathbb{Z}_N , namely a is some element in the range 0 to $N - 1$, b is also an element in the range 0 to $N - 1$.

And then, if you perform the addition of these 2 elements $(a + b) \% N$, whatever is the result of $a + b$, as soon as you perform modulo N , the remainder will be in the range 0 to $N - 1$. Let that remainder be r . And the remainder will be in the range 0 to $N - 1$. Hence it will be an element of the set \mathbb{Z}_N . So, that is why the closure property is satisfied. Now, let us see whether the associative property is satisfied or not.

And it turns out that, it does not matter what your elements a, b, c are; if you pick them from the set \mathbb{Z}_N , then it does not matter in what order you perform the operation of addition modulo N , the final result will be the same as $(a + b + c) \% N$. You can verify that very easily. The integer 0 which is a member of the set \mathbb{Z}_N ; will be the identity element.

Because, if you take any element a in the range 0 to $N - 1$ and if you do $a + 0$, basically you are still having the element a only. And now, if you take $a \% N$, the result will be same as a . So, that is why the element 0 constitutes the identity element here. Now, what about the inverse?

(Refer Slide Time: 23:50)

Examples of Groups

- Let N be a positive integer and $\mathbb{Z}_N \stackrel{\text{def}}{=} \{0, \dots, N-1\}$ *As the set of integers modulo N*
- ❖ Addition modulo N --- for every $a, b \in \mathbb{Z}_N$: $(a \oplus_N b) \stackrel{\text{def}}{=} [a + b] \text{ mod } N$
- The set \mathbb{Z}_N constitutes a group with respect to the operation \oplus_N *$G = \mathbb{Z}_N, 0 = \oplus_N$*
- ❖ G_1 : consider arbitrary $a, b \in \mathbb{Z}_N$ and let $(a \oplus_N b) = [a + b] \text{ mod } N = r$ --- $r \in \mathbb{Z}_N$
- ❖ G_2 : consider arbitrary $a, b, c \in \mathbb{Z}_N$
- $((a \oplus_N b) \oplus_N c) = (a \oplus_N (b \oplus_N c)) = [a + b + c] \text{ mod } N$
- ❖ G_3 : the element $0 \in \mathbb{Z}_N$ is the identity element *if $a \in \{0, \dots, N-1\}$
 $\Rightarrow N-a \in \{0, \dots, N-1\}$
 $a \oplus_N N-a = [a+(N-a)] \text{ mod } N$*
- $(0 \oplus_N a) = (a \oplus_N 0) = [a \text{ mod } N] = a$
- ❖ G_4 : the element $(-a) \stackrel{\text{def}}{=} (N-a) \in \mathbb{Z}_N$ is the inverse element for $a \in \mathbb{Z}_N$ *$\hat{=} N \text{ mod } N = 0$*
- $((-a) \oplus_N a) = (a \oplus_N (-a)) = [(a + (N-a)) \text{ mod } N] = [N \text{ mod } N] = 0$

Imagine that your element a is some element in the range 0 to $N - 1$. Now, I consider an element $-a$, and this is not a usual $-a$; $-a$ here is defined to be the element $N - a$. That is the interpretation of this notation. When I say equal to, and on top of that define I write, that means, I am now defining a new way or new interpretation for $-a$.

My $-a$ is now interpreted as if the difference of the modulus and the element a . And if your element a belongs to 0 to $N - 1$, then it is easy to see that $N - a$ will also be an element of 0 to $N - 1$. And what can you say about the result of addition modulo N involving a and $N - a$? Well, it will be same as $a + N - a$; you add them and then you take a mod as per our definition of \oplus_N .

But $a + N - a$ at the first place will give you N . And now, $N \% N$ will give you the element 0, which is your identity element. So, that is why the inverse element also exist, and the inverse element will be $N - a$. So, now you can see that this is a special type of addition operation defined over a special set \mathbb{Z}_N , and it satisfies all your group axioms.

(Refer Slide Time: 25:49)

$$\mathbb{Z}_N: \{0, \dots, N-1\}$$

Examples of Groups

□ Let N be a positive integer and $\mathbb{Z}_N^* \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_N : \text{GCD}(a, N) = 1\}$

→ a is co-prime to N

3, 6 are not
Co-prime

4, 7 are coprime



Now, let us define a special form of multiplication over a special set and we will prove that, that constitutes a group as well. And this is a very interesting group, which we will encounter later. So, earlier, we had defined a set \mathbb{Z}_N , which consists of all the remainders that you can obtain by dividing any integer by the modulus N , namely it has the elements 0 to $N - 1$. Now, \mathbb{Z}_N^* is the collection of all the elements from \mathbb{Z}_N , which are co-prime to N .

So, $\text{GCD}(a, N) = 1$ means that a is co-prime to N . And GCD means the greatest common divisor. So, co-prime means, there is no common integer other than 1 which divides a and N ; that is the greatest common divisor here. So, for instance, 3 and 6 are not co-prime, because their GCD is 3. 3 divides 3 as well as 6, so, and that is not equal to 1; so, their GCD is more than 1, it is not 1; that is why they are not co-prime.

But if I consider say 4, 7 are co-prime, because their GCD , namely the greatest common divisor is 1. So, what is my definition of \mathbb{Z}_N^* ? So, \mathbb{Z}_N had the elements 0 to $N - 1$. Among all these elements, I am focusing on only those elements which are co-prime to my modulus. That means, I am considering now; so, if this is your \mathbb{Z}_N , I am focusing on a subset of \mathbb{Z} , which I am calling as \mathbb{Z}_N^* , which basically consists of only those elements from \mathbb{Z}_N which are co-prime to my modulus N .

(Refer Slide Time: 28:49)

$\mathbb{Z}_N = \{0, \dots, N-1\}$ **Examples of Groups** 3, 4, 7 are co-prime

□ Let N be a positive integer and $\mathbb{Z}_N^* \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_N : \text{GCD}(a, N) = 1\}$

❖ **Multiplication modulo N** --- for every $a, b \in \mathbb{Z}_N^*$: $(a \cdot_N b) \stackrel{\text{def}}{=} [a \cdot b] \bmod N$ m

□ The set \mathbb{Z}_N^* constitutes a group with respect to the operation \cdot_N $G = \mathbb{Z}_N^*$ $0 = 1$

❖ G_1 : consider arbitrary $a, b \in \mathbb{Z}_N^*$: $\text{GCD}(a, N) = 1 = \text{GCD}(b, N)$

➤ Let $(a \cdot_N b) = [a \cdot b] \bmod N = r$ --- $r \in \mathbb{Z}_N$ $r \in \mathbb{Z}_N^*$

➤ **Claim:** $\text{GCD}(r, N) = 1$ // $\text{GCD}(ab, N) = 1$ and $r = ab - kN$, for some $k \in \mathbb{Z}$

If $\text{GCD}(ab, N) = x \neq 1$ $ab = kN + r$
 \Rightarrow either x divides both a, N
or x divides both b, N

And now, analogous to addition modulo N , I define the operation of multiplication modulo N . And how it is defined? So, first of all, the notation is this. So, we use \cdot typically for multiplication, but now, we are going to do multiplication with respect to a modulus namely capital N , so, in the subscript we have that modulus and the operation is denoted as \cdot_N . And if you have 2 elements a and b in the set \mathbb{Z}_N^* , then the result of multiplication modulo N of a and b will be computed as follows:

You first multiply a and b as it is, as per the integer multiplication, and then you take mod with respect to the modulus N . That will be the result of $a \cdot_N b$. So, now, we can prove the following. If I consider my set G , the abstract set G to be \mathbb{Z}_N^* , and my abstract operation \circ to be the operation of \cdot_N , then all the group axioms are satisfied. So, let us prove that.

Well, let us prove first the closure property. So, imagine you take a pair of arbitrary elements a, b from \mathbb{Z}_N^* . I have to show that, if I perform $a \cdot_N b$, then again I obtain an element from \mathbb{Z}_N^* itself. So, since a is an element of \mathbb{Z}_N^* , that means a is co-prime to N . That means, their GCD is 1. And similarly, b is an element of \mathbb{Z}_N^* . That means, b is co-prime to N , their GCD is 1.

Now, I have to show the following: I have to show 2 things. I have to show that, when I perform, when I perform $a \cdot_N b$, then I obtain something; it should be of course in the range $\{0, \dots, N - 1\}$, plus it should be co-prime to your modulus N . So, 2 things I have to prove. So, the first thing is easy to prove. If I multiply a and b and then take modulo N , of course, the remainder r will be a value in the range $\{0, \dots, N - 1\}$.

But I also need to prove that this remainder r , which is the result of $a \cdot_N b$ is co-prime to your modulus N . Then only I can show that r is actually a member of \mathbb{Z}_N^* , because that is my definition of \mathbb{Z}_N^* . How do I prove that r is co-prime to N ? Well, that is very simple. So, I can write r to be the difference of $a \cdot b$ and some multiple of your modulus N .

Why so? What is r ? r is the result or r is the remainder which you obtain by dividing $a \cdot b$ by the modulus N . That means, it is the leftover portion. That means, I can say that $a \cdot b = KN + r$ by your division property. If $a \cdot b$ is completely divisible by N , then the remainder r will be 0. But if $a \cdot b$ is not completely divisible by N , then there will be a leftover remainder, that is your remainder r , and K is basically your quotient.

So, that is why K is some integer; it could be 0; it could be 1; it could be some integer. And since $GCD(a, N) = 1$; that means, there is no common divisor of a and N apart from 1; and since $GCD(b, N) = 1$, because both a and b are co-prime to N ; then, I can conclude that $a \cdot b$ is also co-prime to N . Why? Because, if $GCD(a \cdot b, N)$ is some x which is not equal to 1, then it implies that either x divides both a and N or x divides both b and N .

But if x divides both a and N , that means the $GCD(a, N)$ is not 1 but rather x ; and x is not equal to 1. But that is a contradiction, because $GCD(a, N)$ is 1. In the same way, x cannot divide both b and N , because if that would have been the case, then $GCD(b, N)$ would have been x but not 1. But that is again a contradiction to this fact. So, that is why, since both a and b are co-prime to N , I can say that their product is also co-prime to N .

(Refer Slide Time: 33:42)

Examples of Groups

- $\mathbb{Z}_N: \{0, \dots, N-1\}$
- Let N be a positive integer and $\mathbb{Z}_N^* \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_N : \text{GCD}(a, N) = 1\}$
 - ❖ **Multiplication modulo N** --- for every $a, b \in \mathbb{Z}_N^*$: $(a \cdot_N b) \stackrel{\text{def}}{=} [a \cdot b] \text{ mod } N$
 - The set \mathbb{Z}_N^* constitutes a group with respect to the operation \cdot_N
 - ❖ G_1 : consider arbitrary $a, b \in \mathbb{Z}_N^*$: $\text{GCD}(a, N) = 1 = \text{GCD}(b, N)$
 - Let $(a \cdot_N b) = [a \cdot b] \text{ mod } N = r \quad \dots r \in \mathbb{Z}_N$
 - **Claim:** $\text{GCD}(r, N) = 1 \quad // \text{GCD}(ab, N) = 1$ and $r = ab - kN$, for some $k \in \mathbb{Z}$

And by the divisibility property, I get that r will be the difference of $a \cdot b$ and some multiple of N . So, now, combining these 2 facts, I can conclude that the $\text{GCD}(r, N) = 1$. That is very simple. So, that shows that r is a member of \mathbb{Z}_N^* as well and r is the result of $a \cdot_N b$.

(Refer Slide Time: 34:19)

Examples of Groups

- Let N be a positive integer and $\mathbb{Z}_N^* \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_N : \text{GCD}(a, N) = 1\}$
 - ❖ **Multiplication modulo N** --- for every $a, b \in \mathbb{Z}_N^*$: $(a \cdot_N b) \stackrel{\text{def}}{=} [a \cdot b] \text{ mod } N$
- The set \mathbb{Z}_N^* constitutes a group with respect to the operation \cdot_N
 - ❖ G_1 : consider arbitrary $a, b \in \mathbb{Z}_N^*$: $\text{GCD}(a, N) = 1 = \text{GCD}(b, N)$
 - Let $(a \cdot_N b) = [a \cdot b] \text{ mod } N = r \quad \dots r \in \mathbb{Z}_N$
 - **Claim:** $\text{GCD}(r, N) = 1 \quad // \text{GCD}(ab, N) = 1$ and $r = ab - kN$, for some $k \in \mathbb{Z}$
 - ❖ G_2 : consider arbitrary $a, b, c \in \mathbb{Z}_N^*$
 - $((a \cdot_N b) \cdot_N c) = (a \cdot_N (b \cdot_N c)) = [a \cdot b \cdot c] \text{ mod } N$
 - ❖ G_3 : the element $1 \in \mathbb{Z}_N^*$ is the **identity element** --- $(1 \cdot_N a) = (a \cdot_N 1) = [a \text{ mod } N] = a$
 - ❖ G_4 : Consider an arbitrary $a \in \mathbb{Z}_N^*$: $\text{GCD}(a, N) = 1$
 - Using **Extended-Euclid's algorithm** we can find $b \in \mathbb{Z}_N^*$, such that $(ab) \text{ mod } N = 1$

So, the closure property is satisfied. Now, let us see associativity property is satisfied or not. So, if you take any triplet of elements a, b, c , all of which are individually co-prime to N and multiply them together, and you perform the multiplication modulo N operation, I have involving 2 elements at a time, then it does not matter in what order you perform the multiplication modulo N operation, the result will be the same as if you do $a \cdot b \cdot c$ and then you take modulo N .

So, of course the result will be an element in the range $\{0, \dots, N - 1\}$; and at the same time, it will be co-prime to N . Namely, if r is the remainder obtained by dividing $a \cdot b \cdot c$ by N , then r has to be co-prime to N . Because, if r is not co-prime to N , then you get a contradiction that either a is not co-prime to N , or b is not co-prime to N or c is not co-prime to N , which is not true. The element 1 will be a member of \mathbb{Z}_N^* , because $GCD(1, N) = 1$.

This implies the element 1 belongs to \mathbb{Z}_N^* . And now, you perform the multiplication modulo N involving any element a from \mathbb{Z}_N^* , and the element 1. The result will be the element a itself. And now, what about the inverse. So, if you are given an element a from \mathbb{Z}_N^* ; that means, the $GCD(a, N) = 1$; then there is the wonderful result from number theory which says that if a is relatively prime or co-prime to your modulus N , then there always exist another integer b also from your set \mathbb{Z}_N^* , such that the result of $a \cdot_N b$ will give you the identity element namely 1.

So, the element b will be considered as the multiplicative inverse a modulo N . And it is easy to see that if b is the multiplicative inverse of a modulo N , then a will be considered as the multiplicative inverse of b modulo N . That means, they are inverse of each other. So, that means, $a^{-1} = b$, and $b^{-1} = a$; because of the fact that when you multiply a and b and take modulo N , you get back the identity element 1.

(Refer Slide Time: 37:35)

Examples of the Groups \mathbb{Z}_N and \mathbb{Z}_N^*

$\mathbb{Z}_6 = \{0, \dots, 5\}$
 $N = 6$

Group $(\mathbb{Z}_6, +_6)$
 → elements of \mathbb{Z}_6

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$1 +_6 5 = 6 \pmod 6 = 0$

elements of \mathbb{Z}_6^*

$1^{-1} = (-1) = 6 - 1 = 5$
 $2^{-1} = (-2) = 6 - 2 = 4$



So, now, let us see some concrete examples of the 2 special groups \mathbb{Z}_N and \mathbb{Z}_N^* that we have encountered. So, here, let us see first $N = 6$; and with respect to the addition modulo 6

operation. So, I have drawn a table here. Along the columns, you have the elements of \mathbb{Z}_6 , and along the rows, you have the elements of \mathbb{Z}_6 . So, you can imagine that along the columns, you have the candidate values of a ; along the rows, you have the candidate values of b ; and then, the various entries will denote the result of performing $a+_6b$.

So, for instance, if I take 0 and 0, add them and take modulo 6, the result will be 0. If I take 0 and 1 and then add them and take modulo 6, I will obtain 1 and so on. In the same way, now, if I take the element 1 and add it with 0, I will obtain 1, and 1 modulo 6 will be 1 and so on. So, this entry, let us verify. So, if I add 1 to 5, and then if my operation is modulo 6, this will be 6 modulo 6. And 6 modular 6 is 0. So, that is why we get the result 0 here.

In the same way, the third row will be this; fourth row will be this; fifth row will be this; sixth row will be this. So now you can see that it does not matter what is the value of a , what is the value of b , the result is always an element of the set \mathbb{Z}_6 . Remember, my set \mathbb{Z}_6 will have the elements 0 to 5. Nowhere we obtained an element which is outside the set 0 to 5. The associativity property is always satisfied. The element 0 is the identity element.

Because, you add 0 with 0, you get 0; you add element 0 and 1, obtain the element 1; you add 0 and 2, you obtain 2; you add 0 and 3, you obtain 3; you add 0 and 4, you obtain 4; you add 0 and 5, you obtain 5. So, that means, if you want to find out the identity, just focus on the row involving 0. And if you want to find out the inverse of various elements, then you can verify here that the inverse of 0 is 0; the inverse of element 1 is element 5, because $5 + 1$ will be 6.

So, basically, 1 inverse will be considered as -1, and as per our definition of -1, it will be $6 - 1$, which is 5. And indeed, if you add 5 to 1 and take modulo 6, you will obtain the identity element namely 0. In the same way, the inverse of element 2 will be element 4. Because, 2 inverse is basically -2 in the set \mathbb{Z}_6 , and -2 is nothing but $6 - 2$, and $6 - 2$ is 4 and so on.

(Refer Slide Time: 41:38)

Examples of the Groups \mathbb{Z}_N and \mathbb{Z}_N^*

$\mathbb{Z}_6 = \{0, \dots, 5\}$
 $N = 6$

Group $(\mathbb{Z}_6, +_6)$
elements of \mathbb{Z}_6

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\mathbb{Z}_7 = \{0, \dots, 6\}$
 $N = 7$

$\mathbb{Z}_7^* = \{1, \dots, 6\}$
 $N = 7$

Group $(\mathbb{Z}_7^*, \cdot_7)$

\cdot_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$2 \cdot_7 1 = 2 \bmod 7 = 2$
 $2 \cdot_7 4 = 8 \bmod 7 = 1$
 $2 \cdot_7 2 = 4 \bmod 7 = 4$
 $2 \cdot_7 3 = 6 \bmod 7 = 6$

Now, let us take the example of \mathbb{Z}_N^* and I take here $N = 7$. So, your \mathbb{Z}_7 will have the elements 0 up to 6. Now, \mathbb{Z}_7^* will have all those elements from \mathbb{Z}_7 which are co-prime to 7. So, it turns out that 0 is not co-prime to 7. Because, if I take GCD of 0 and 7, then it turns out to be 7. That is the largest number which divides both 0 as well as 7, and that is not 1. So, that is why 0 will not be included in \mathbb{Z}_7^* .

But if you take the remaining elements, all of them are going to be co-prime to your modulus 7, because 7 is a prime number. And that is why, \mathbb{Z}_7^* will have elements 1, 2, 3, 4, 5, 6. So, again, I have done the same thing. Along the columns, I have denoted the candidate values of a ; along the rows, I have denoted the candidate values of b . Well, you can interpret it other way around.

You can imagine that along the rows, you have the candidate a 's; and the columns, you have the candidate b 's. And now, let us see the result of performing $a \cdot_7 b$. So, 1 multiplied with any number; after performing modulo 7 will give back the same number. So, the row under a is not interesting. Let us consider the row under 2. See, if you perform $2 \cdot_7 1$, that will be same as $2 \% 7$, and hence 2.

If you multiply 2 with 2 and take modulo 7, that will be 4 modulo 7, which is 4. But now, if you perform multiplication of 2 and 3 modulo 7, that will be 6 modulo 7. That will be 6. But as soon as you perform 2 multiplication 4 modulo 7, that will be 8 modulo 7. And 8 modulo 7 is 1. So, you can see now. And similarly, 2 multiplied with 5 will be 10. 10 modulo 7 will be 3 and so on. The same way, you can find out the remaining rows.

You can see the closure property is satisfied, because you always obtain a result which lies within the set 1 to 6. The integer 1 will be the identity element.

(Refer Slide Time: 44:47)

Examples of the Groups \mathbb{Z}_N and \mathbb{Z}_N^*

$\mathbb{Z}_6 = \{0, \dots, 5\}$
 $N=6$

Group $(\mathbb{Z}_6, +_6)$

elements of \mathbb{Z}_6

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\mathbb{Z}_7 = \{0, \dots, 6\}$
 $N=7$

Group (\mathbb{Z}_7, \cdot_7)

$\mathbb{Z}_7^* = \{1, \dots, 6\}$
 $N=7$

\cdot_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5 <td>3</td> <td>1</td> <td>6</td> <td>4</td> <td>2</td>	3	1	6	4	2
6	6	5	4	3	2	1

$2^{-1} = 4$

And the inverse of 1 will be 1; inverse of 2 will be 4. Because, when you multiply 4 with 2 and then take modulo 7, you get the identity element 1. So, the inverse of 2 is 4. And now, let us check the inverse of 4. The inverse of 4 will be 2. Because, this particular entry is the identity element; so, under the column 4, under the row 2, you obtain the element 1; that is why the inverse of 4 is 2.

So, that is why, what I said earlier is correct. You can verify that. If b is the multiplicative inverse of a , then a will be the multiplicative inverse of b and so on.

(Refer Slide Time: 45:38)

Examples of the Groups \mathbb{Z}_N and \mathbb{Z}_N^*

$\mathbb{Z}_6 = \{0, \dots, 5\}$
 $N=6$

Group $(\mathbb{Z}_6, +_6)$

elements of \mathbb{Z}_6

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\mathbb{Z}_7 = \{0, \dots, 6\}$
 $N=7$

Group (\mathbb{Z}_7, \cdot_7)

$\mathbb{Z}_7^* = \{1, \dots, 6\}$
 $N=7$

\cdot_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

□ What will be the cardinality of the group \mathbb{Z}_p^* , if p is a prime number?

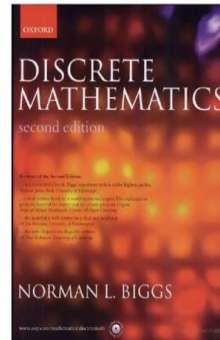
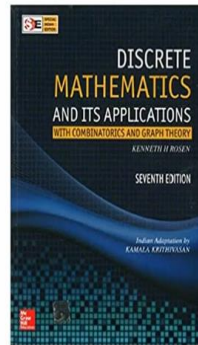
$$\mathbb{Z}_p^* = \{1, \dots, p-1\} = \mathbb{Z}_p - \{0\}$$

$\text{GCD}(0, p) \neq 1$

So, what will be the cardinality of the group \mathbb{Z}_p^* , if p is a prime number? So, as we have demonstrated here, \mathbb{Z}_p^* will have all the elements from \mathbb{Z}_p except the element 0, because the GCD of 0 and p will not be equal to 1, because it is p . Other than that, all other elements in the set \mathbb{Z}_p will be co-prime to your p .

(Refer Slide Time: 46:05)

References for Today's Lecture



So, with that, I end today's lecture. These are the references used for discussing today's concepts. Of course, they are very basic facts about groups. You can find them in any online resource. Thank you.