Secure Computation: Part II
Prof. Ashish Choudhury
Department of Computer Science and Engineering
Indian Institute of Science, Bengaluru

Lecture - 18
Recap of Basic Concepts from Abstract Algebra

Hello everyone. Welcome to this lecture.

(Refer Slide Time: 00:25)

Lecture Overview

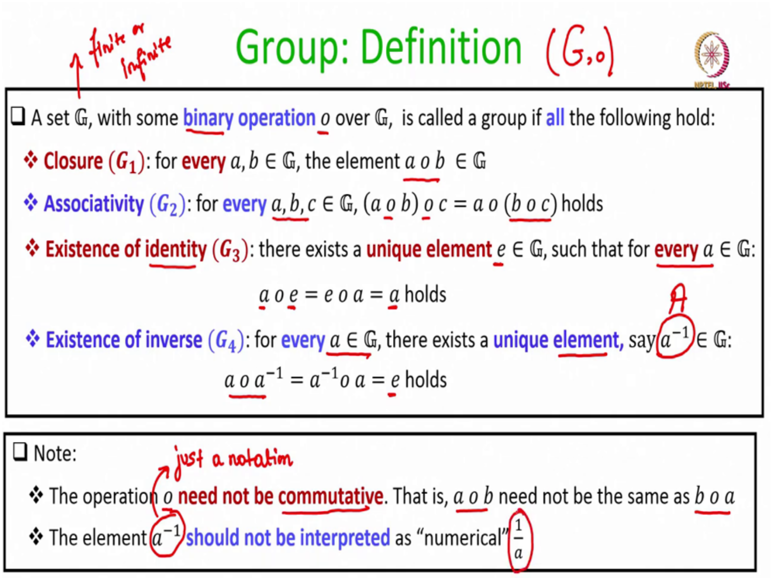
❑ Group
- ❖ Definition and properties
- ❖ Examples

❑ Rings and Fields

So, we will now start shifting our attention to other topics, other problems in Secure Distributed Computing. Remember that, our eventual goal is to design Secure Multi-Party Computation Protocols tolerating malicious corruptions. Towards that goal we have already spent quite a lot of time discussing Byzantine agreement and Broadcast protocols. We will now start looking into some other primitives which will be useful for designing MPC protocols.

Before going into those primitives, we have to brush up our knowledge, whatever information we have regarding Abstract Algebra. So, I will be quickly going over some of the topics from abstract algebra which we will require. So, in this lecture we will touch upon the basic properties of Groups, Rings and Fields.

(Refer Slide Time: 01:17)



finite or infinite

Group: Definition (G, o)

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

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

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

❖ Existence of identity (G_3): there exists a unique element $e \in \mathbb{G}$, such that for every $a \in \mathbb{G}$:

$$a\ o\ e = e\ o\ a = a \text{ holds}$$

A

❖ Existence of inverse (G_4): for every $a \in \mathbb{G}$, there exists a unique element, say $a^{-1} \in \mathbb{G}$:

$$a\ o\ a^{-1} = a^{-1}\ o\ a = e \text{ holds}$$

□ Note:

just a notation

❖ The operation o need not be commutative. That is, $a\ o\ b$ need not be the same as $b\ o\ a$

❖ The element a^{-1} should not be interpreted as "numerical" $\frac{1}{a}$

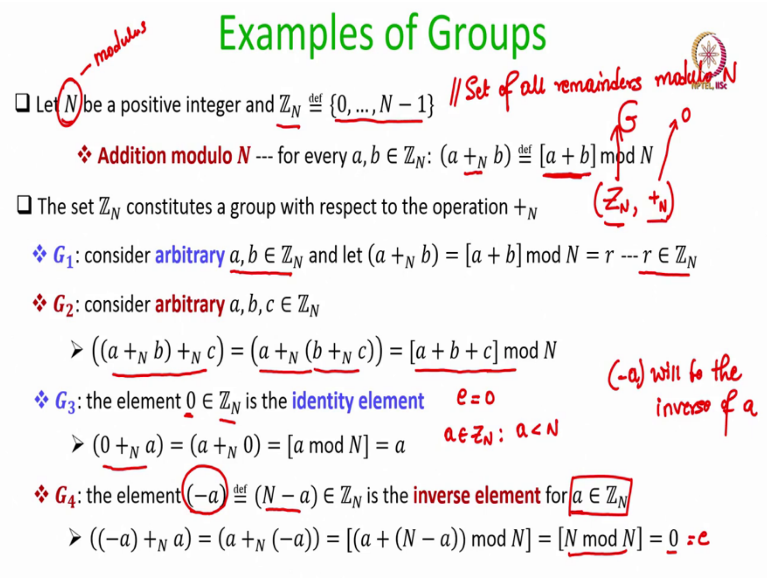
So, what is a group? It is some set with a binary operation, the set could be finite or infinite. It has some binary operation which I denote by o, which operates with two operands. And the set G along with the operation o will be called as a group, if some properties are satisfied. These properties are also called as Group axioms.

So, the first axiom is that the operator o should satisfy the closure property. Namely if you perform the group operation with any pair of elements a, b including the case where a and b are same, then the result should be an element from the set G itself. The second property is the associativity property; which demands that the operation o should be associative; that means, it does not matter in what order you perform the group operation, you do the operation with involving a and b first and then involve c, the result should be the same, as what you obtain if you do the group operation over b and c first and then with the result and the operator o and operand a, yeah. This should hold even if a, b, c are identical, if they are different so on. There should be a special element, a unique element small e from the set G, which we often call as the Identity element such that, you take any element a from the set G and perform the group operation with e, you should get the element a only. And this should be the case for every element small a in the set G.

And the fourth property is the existence of the inverse which demands that you take any element a from the set G corresponding to that there should be some element denoted by a^{-1}, such that the result of the group operation between a and a^{-1} is the identity element. If all these four properties are satisfied, then the set G along with the operation o is called as a Group.

So, few things which we have to note here is that, the operation o need not be commutative even though it is associative; that means, the result of a operation b need not be the same as the result of b operation a. And, this notation a^{-1} is just a notation, ok. You can use any notation say big A, whatever you are comfortable with. It should not be interpreted as $\frac{1}{a}$.

(Refer Slide Time: 04:37)



Examples of Groups

modulus

❑ Let N be a positive integer and $\mathbb{Z}_N \overset{\text{def}}{=} \{0, \ldots, N-1\}$ // Set of all remainders modulo N

- ❖ **Addition modulo N** --- for every $a, b \in \mathbb{Z}_N$: $(a +_N b) \overset{\text{def}}{=} [a + b] \bmod N$

G o

$(Z_N, +_N)$

❑ The set $\mathbb{Z}_N$ constitutes a group with respect to the operation $+_N$

- ❖ G_1: consider **arbitrary** $a, b \in \mathbb{Z}_N$ and let $(a +_N b) = [a + b] \bmod N = r$ --- $r \in \mathbb{Z}_N$
- ❖ G_2: consider **arbitrary** $a, b, c \in \mathbb{Z}_N$
  - ➢ $((a +_N b) +_N c) = (a +_N (b +_N c)) = [a + b + c] \bmod N$
- ❖ G_3: the element $0 \in \mathbb{Z}_N$ is the **identity element** $e = 0$
  - ➢ $(0 +_N a) = (a +_N 0) = [a \bmod N] = a$ $a \in Z_N : a < N$
- ❖ G_4: the element $(-a) \overset{\text{def}}{=} (N - a) \in \mathbb{Z}_N$ is the **inverse element** for $\boxed{a \in \mathbb{Z}_N}$
  - ➢ $((-a) +_N a) = (a +_N (-a)) = [(a + (N - a)) \bmod N] = [N \bmod N] = 0 = e$

(-a) will be the inverse of a

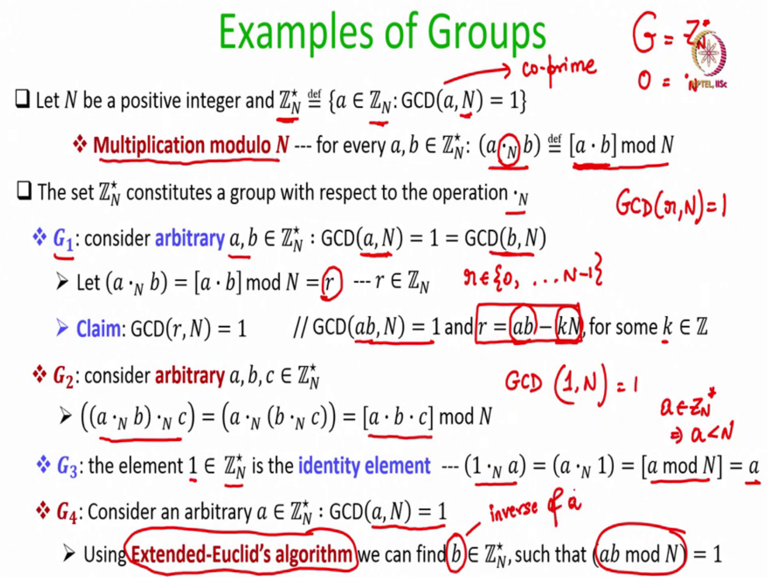
Let us see some examples of groups. So, imagine N is a positive integer. Then consider the set $Z_N = \{0, \cdots, N-1\}$. So, you can imagine that this is the set of all remainders modulo N; that means, you take any integer and you divide it by this number N, this N you can imagine as a modulus. So, you take any integer and divide it by this modulus, you will get a remainder in this collection Z_N.

So, now in this set Z_N, I define an operation which I call as addition modulo N denoted by $+_N$, and the result of this operation is a + b modulo N; that means, you add a and b that is a regular addition, but that is not the answer that is not the result of a plus b modulo N. The result is the remainder which we obtain after dividing a plus b by N.

Now, the claim is that the set Z_N, along with the operation plus modulo N constitutes a group. So, my Z_N serves the role of big G and this operation plus modulo N serves the role of operation o in the previous definition. Let us see whether all the group axioms are satisfied or not. So, the first group axiom is satisfied because, you take any two remainders a and b from the collection Z_N, you add them and take modulo N you will again obtain a remainder r which will be a number in the range 0 to N - 1. So, the closure property is satisfied. The operation addition modulo N satisfies the associativity property. Because, it does not matter whether you do first a plus b modulo N followed by c modulo N or you first do b plus c modulo N and then to that you add a and do modulo N. The result will be the same as what we get by adding a, b and c and then taking modulo N. So, the associativity property is satisfied. The element 0, the integer 0 belongs to the set Z_N and that serves as the identity element e. Because, if you add 0 to any element a from the set Z_N, the result will be a only and the effect of mod N will not be there. Because, if a is in Z_N, then a is strictly less than N. And, corresponding to every element small a, I can define an element −a, which is same as N - a, which is the inverse of the element a. Because, if I add minus a to this −a and take modulo N, the result will be N modulo N and N modulo N will be the 0 which is the identity element.

So, −a will be the inverse of a. So that means, this collection Z_N along with the operation addition modulo N satisfies all the group axioms.

(Refer Slide Time: 08:40)



Examples of Groups

$G = \mathbb{Z}_N^*$

$0 = \cdot_N$

co-prime

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

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

❑ The set $\mathbb{Z}_N^\star$ constitutes a group with respect to the operation $\cdot_N$

$\text{GCD}(r, N) = 1$

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

➢ Let $(a \cdot_N b) = [a \cdot b] \bmod N = r$ --- $r \in \mathbb{Z}_N$ $r \in \{0, \ldots N-1\}$

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

❖ G_2: consider **arbitrary** $a, b, c \in \mathbb{Z}_N^\star$

$\text{GCD}(1, N) = 1$

➢ $((a \cdot_N b) \cdot_N c) = (a \cdot_N (b \cdot_N c)) = [a \cdot b \cdot c] \bmod N$

$a \in \mathbb{Z}_N^*$
$\Rightarrow a < N$

❖ G_3: the element $1 \in \mathbb{Z}_N^\star$ is the **identity element** --- $(1 \cdot_N a) = (a \cdot_N 1) = [a \bmod N] = a$

❖ G_4: Consider an arbitrary $a \in \mathbb{Z}_N^\star$: $\text{GCD}(a, N) = 1$

inverse of a

➢ Using **Extended-Euclid's algorithm** we can find $b \in \mathbb{Z}_N^\star$, such that $(ab \bmod N) = 1$

Now, let us see another group, ok. I define now a set $Z_N^\star$; where I take only those elements from Z_N which are co-prime to my modulus N; that means, the GCD of that a and my modulus N is 1. And now, in this set I define a variant of the multiplication operation which I denote by this notation $\bullet_N$. This is called Multiplication modulo N operation.

And let us see how do we get the result of multiplication modulo N operation. So, if you want to apply this operation on two numbers a and b which are from the set $Z_N^\star$;, then you first do the regular multiplication regular integer multiplication you multiply a and b, but that will not be the answer, the answer will be what you get after you do a mod N. And now we can prove that the collection $Z_N^\star$ along with this operation multiplication modulo N is a group, it satisfies all the group axioms.

So, now in this example my set big G is $Z_N^\star$. And my abstract operation o is the multiplication modulo N operation. So, let us see whether all the properties are satisfied or not all the group axioms to be more specific. So, closure property is satisfied. So, to prove the closure property let us take two arbitrary elements a and b from the set $Z_N^\star$. So that means, individually a is co-prime to N and b is co-prime to N. We want to show that a multiplied with b modulo N is also an element of $Z_N^\star$, ok.

So, imagine that ab modulo N is r. We already know that r is in Z_N, because r will be a number in the range 0 to N - 1, because we are multiplying a and b and then taking a mod N. But that is not our goal; we want to show that r is a member of $Z_N^\star$. We want to show that GCD of r and N is 1 and that is very simple to show. Since a and b are relatively prime And, what can we say about the remainder r here? Remainder r is what you obtain after dividing ab by N; that means, it is the result of subtracting some multiple of N from ab, for some k from the set of integers.

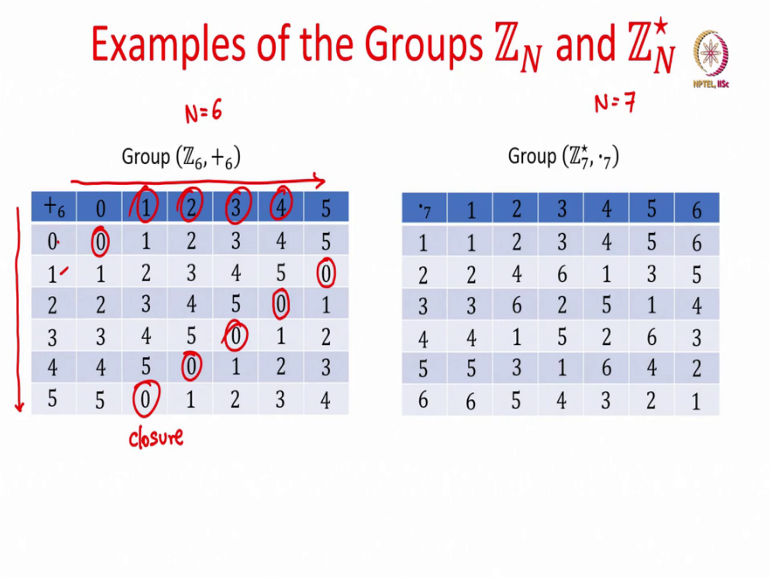
So, now if the GCD of r and N is not 1, then we basically end up showing that the GCD of ab and N is not 1 which is a contradiction. So, that shows that the closure property is satisfied.

The operation multiplication modulo N satisfies the associativity property. It does not matter in what order you perform the operation multiplication modulo N involving 3 numbers a, b, c from the set $Z^{\star}_{N}$, the result will be same as the product of a, b, c modulo N.

The integer 1 is an a member of $Z^{\star}_{N}$ because, 1 is always co-prime to N. And it serves as the identity element because you take any element small a from the set $Z^{\star}_{N}$, you multiply 1 with a and take modulo N, you get the number a only, because since a is a member of $Z^{\star}_{N}$, it implies that a is strictly less than N and that is why a modulo N will be a only.

And, if we take any element a from the set $Z^{\star}_{N}$ such that the GCD of a and N is 1, its coming from the definition of $Z^{\star}_{N}$, then, there is a very well-known algorithm in number theory called as Extended Euclid's Algorithm, which is basically just the extension of the simple Euclid's GCD algorithm, which allows you to find out another number b from the set $Z^{\star}_{N}$ corresponding to this number a, such that ab modulo N is 1. So, b will be the inverse of a, ok.

(Refer Slide Time: 14:53)



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

N=6

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

$+_6$	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

closure

N=7

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

$\cdot_7$	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

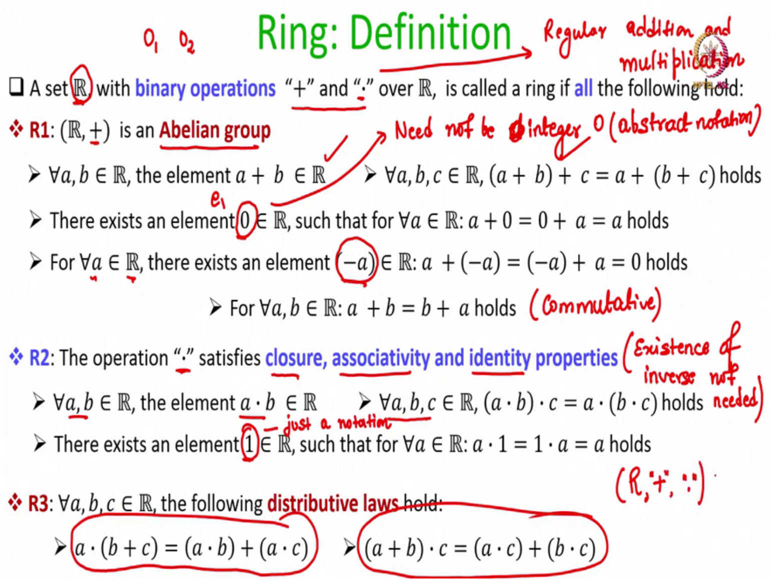
So, let me demonstrate this group Z_N and $Z^{\star}_{N}$with an example. If I take N is equal to 6 and then if I take the operation plus modulo 6 then, here is the group table. Along the rows I have the elements of Z_6 and along the columns also I have the elements of Z_6 and now we can fill the table. So, 0 plus 0 modulo 6 will be 0; 0 plus 1 modulo 6 will be 1; 0 plus 2 modulo 6 will be 2 and like that 0 plus 5 modulo 6 will be 5.

The next row will be 1 2 3 4 5 0. So, for instance 1 plus 4 is 5; 5 modulo 6 will be 5. But, 1 plus 5 will be 6 and 6 modulo 6 will be 0. So, like that you can fill the other rows as well. Now, you can see the closure property is satisfied. Because, in this table none of the elements are from outside the set 0 to 5, all the elements are from the set 0 to 5 only.

The operation plus modulo 6 is anyhow associative. The element 0 is the identity element because, if you see the column under 0, then 0 addition 0 is giving you 0; 1 addition 0 is giving you 1; 2 addition 0 is giving you 2; 3 addition 0 is giving you 3; 4 added with 0 modulo 6 giving you 4 and 5 added to 0 modulo 6 giving you 5 that is the additive identity, namely the element 0 is the identity element and now let us try to find out the inverse, ok.

So, inverse of 0 will be 0 only; inverse of 1 will be 5 because, 1 added to 5 gives you the identity element 0. The inverse of 2 will be the element 4. The inverse of 3 will be the element 3. The inverse of 4 will be the element 2 and the inverse of 5 will be the element 1. So, you have the inverse present as well. In the same way, I can draw the table of group $Z_7^{\star}$, I can take N equal to 7 and then I can fill the rows and the columns and then you can check whether all the properties are satisfied or not.

(Refer Slide Time: 17:47)



O_1 O_2

Ring: Definition

Regular addition and multiplication

□ A set $\mathbb{R}$ with binary operations "+" and "·" over $\mathbb{R}$, is called a ring if all the following hold:

❖ R1: $(\mathbb{R}, +)$ is an Abelian group

Need not be integer 0 (abstract notation)

- $\forall a, b \in \mathbb{R}$, the element $a + b \in \mathbb{R}$ ✓
- $\forall a, b, c \in \mathbb{R}$, $(a + b) + c = a + (b + c)$ holds
- There exists an element $\overset{e_1}{0} \in \mathbb{R}$, such that for $\forall a \in \mathbb{R}$: $a + 0 = 0 + a = a$ holds
- For $\forall a \in \mathbb{R}$, there exists an element $(-a) \in \mathbb{R}$: $a + (-a) = (-a) + a = 0$ holds
- For $\forall a, b \in \mathbb{R}$: $a + b = b + a$ holds (Commutative)

❖ R2: The operation "·" satisfies closure, associativity and identity properties (Existence of inverse not needed)

- $\forall a, b \in \mathbb{R}$, the element $a \cdot b \in \mathbb{R}$
- $\forall a, b, c \in \mathbb{R}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ holds
- There exists an element $1 \in \mathbb{R}$, such that for $\forall a \in \mathbb{R}$: $a \cdot 1 = 1 \cdot a = a$ holds

just a notation

$(R, "+", "\cdot")$

❖ R3: $\forall a, b, c \in \mathbb{R}$, the following distributive laws hold:

- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Now, let us go to our next algebraic structure which we call as Ring and now we have a set with two binary operations denoted by plus and dot and they are not regular addition and multiplication operations, they are not the regular addition and multiplication operations. So, in fact, you could have used the operations o1 and o2, but typically in textbooks we use the operation plus and dot to denote the operations o1 and o2.

So, now we need some properties to be satisfied with respect to the first operation namely the plus operation and some properties should be satisfied with respect to the second operation o2 or the multiplication, so that the underlying algebraic structure or the set R along with these 2 operations is called as a Ring. So, the first property is that, if I take the plus operation in the set R that should constitute an Abelian group. Now, what is an Abelian group?

Well, it is a group; that means, the closure, associativity property, existence of the identity element and existence of inverse should be guaranteed. On top of that, the operation plus should be commutative. If that is the case, then we say that the set along with the operation is an Abelian group, ok. Now, notice that here to denote the identity element with respect to the plus operation I am using the notation 0. This need not be the integer 0. It is just an abstract notation.

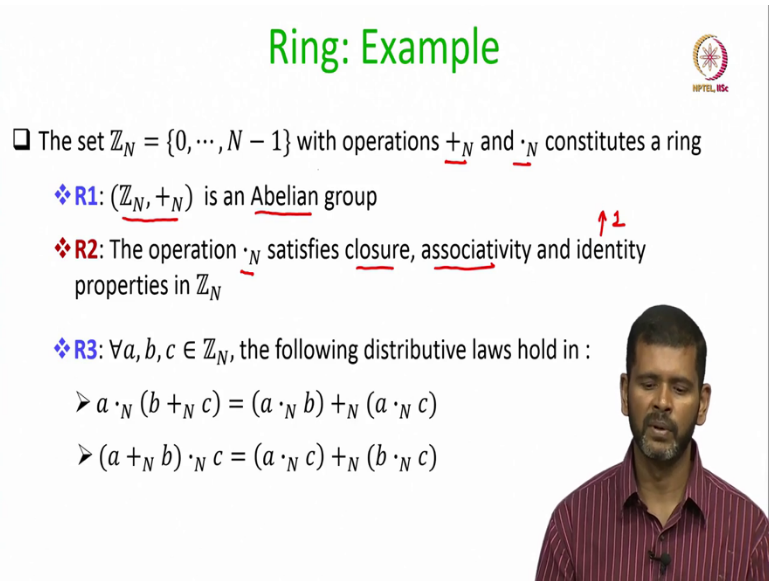
In fact, you could have used the notation e sub 1 to denote the identity element with respect to the plus operation. And in the same way, this element minus a is not the negative a in the sense that it is not the minus of integer a because, element a is an abstract element from an abstract set it need not be always an integer, ok. So, that is the first property. The second property is that the second operation namely the dot operation in the set R, should satisfy the closure property, associativity property and there should be an identity element, ok.

However, existence of inverse is not needed. Closure means you take any pair of elements, you do the dot operation the result should be an element from the set R. You take any triplet of elements a, b, c and do the dot operation in any order, the result should be the same. And there should be a special element which I denote by 1 which constitutes the identity element.

Again, this is just a notation. It need not represent the integer 1. Because, my set R is an abstract set and its element need not be integers. My set R could be a collection of matrices. My set R could be a collection of vectors, right, it could be anything. And, the third property which we require is that the dot operation and the plus operation they should be distributive over each other. Namely they should satisfy two distributive laws. This is the first distributive law; namely the dot should be distributive over plus and this is the second distributive law.

If all these three properties R1, R2, R3 are satisfied, then the collection R along with the abstract operation plus and abstract operation dot will be called a ring

(Refer Slide Time: 22:52)



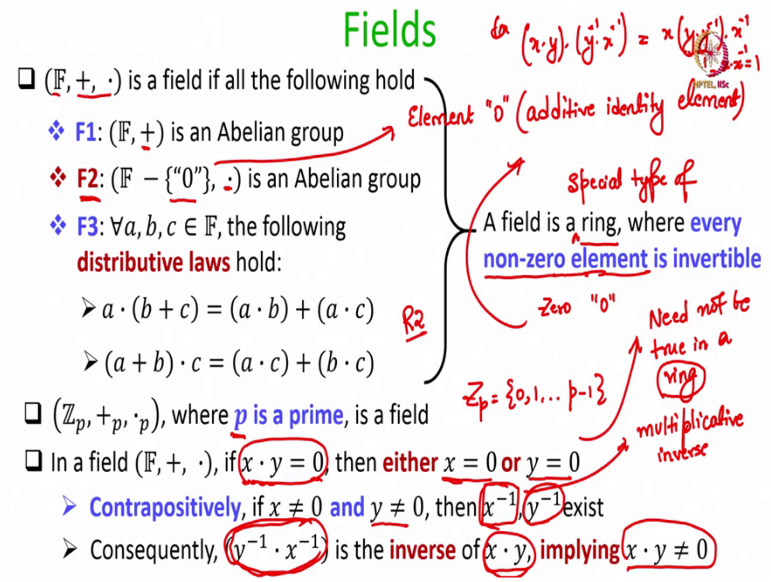
Ring: Example

❑ The set $\mathbb{Z}_N = \{0, \cdots, N-1\}$ with operations $+_N$ and $\cdot_N$ constitutes a ring

- ❖ **R1**: $(\mathbb{Z}_N, +_N)$ is an Abelian group
- ❖ **R2**: The operation $\cdot_N$ satisfies closure, associativity and identity ↑1 properties in $\mathbb{Z}_N$
- ❖ **R3**: $\forall a, b, c \in \mathbb{Z}_N$, the following distributive laws hold in :
  - ➢ $a \cdot_N (b +_N c) = (a \cdot_N b) +_N (a \cdot_N c)$
  - ➢ $(a +_N b) \cdot_N c = (a \cdot_N c) +_N (b \cdot_N c)$

So, let us see some examples. The set ZN along with the operations addition modulo N and multiplication modulo N constitutes a ring. So, we have already shown that the addition modulo N operation satisfies the group axioms. Well, it is also constitutes an Abelian group because, the addition modulo N operation is commutative. The multiplication modulo N operation satisfies the closure property, its associative and the identity element will be the integer 1. And it is easy to verify that the distributive laws hold. So, that is why this is an example of a ring.

(Refer Slide Time: 23:48)



Fields

❑ $(\mathbb{F}, +, \cdot)$ is a field if all the following hold

- ❖ **F1**: $(\mathbb{F}, +)$ is an Abelian group
- ❖ **F2**: $(\mathbb{F} - \{\text{“}0\text{”}\}, \cdot)$ is an Abelian group
- ❖ **F3**: $\forall a, b, c \in \mathbb{F}$, the following **distributive laws** hold:
  - ➢ $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
  - ➢ $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

A field is a ring, where **every non-zero element is invertible**

❑ $(\mathbb{Z}_p, +_p, \cdot_p)$, where **$p$ is a prime**, is a field

❑ In a field $(\mathbb{F}, +, \cdot)$, if $x \cdot y = 0$ then **either** $x = 0$ **or** $y = 0$

- ➢ **Contrapositively**, if $x \neq 0$ **and** $y \neq 0$, then x^{-1}, y^{-1} exist
- ➢ Consequently, $(y^{-1} \cdot x^{-1})$ is the **inverse** of $x \cdot y$, **implying** $x \cdot y \neq 0$

$(x\cdot y)\cdot(y^{-1}\cdot x^{-1}) = x\cdot(y\cdot y^{-1})\cdot x^{-1}$
$x\cdot x^{-1} = 1$
Element "0" (additive identity element)
special type of
R2
Zero "0"
$Z_p = \{0, 1, \ldots p-1\}$
Need not be true in a ring
multiplicative inverse

Now, the last algebraic structure which we will be using in this course now is a Field. And like ring, field also has a set and two binary operators, plus and dot again they are abstract plus and abstract dot operators. We will call this triplet a field if the following axioms hold; with respect to the plus operation the set F should be an Abelian group. And now, with respect to the dot operation also we require F to constitute an Abelian group if we exclude the element 0 which is the additive identity element.

If we exclude the additive identity element from the set F, then the resultant set along with the operation dot should constitute an Abelian group. So, it should have it should satisfy the closure property, the operation should be associative, there should be an identity element and every element from this small subset namely the subset where the element 0 is not present should have an inverse. And, the distributive law should be satisfied.

So, if we closely compare the definition of a ring and a field what we get here is that, a field is a special type of ring, where every non-zero elements is invertible and when I say non-zero, I do not mean the values which are different from 0. By non-zero I mean, every element different from the additive identity element because 0 in this context stands for the additive identity element.

So, some examples of field. If we take the modulus p, where p is a prime then the collection Z p which will be the set 0, 1 up to p minus 1 is a field. We can prove that, But I will we will not be going through the proof. And one final property which we require which holds in the field which we will require later is the following. That in the field, if the product of any two elements x and y is 0; and when I say 0, I mean to say the additive identity element. If the product of any two elements x and y is the additive identity element then, either x is the additive identity element namely 0 or the element y is the 0 element.

And this can be proved through a contraposition. Namely we can show, that if x is either not 0 or if y is either not 0; then x dot y is also not 0. Let us see how we can prove that. So, if x is not 0; then x inverse exist. The multiplicative inverse basically, which is the inverse of the element x with respect to the dot operation. And in the same way, since y is not 0; then there exists an inverse of y with respect to the dot operation let us denote it by y power minus 1.

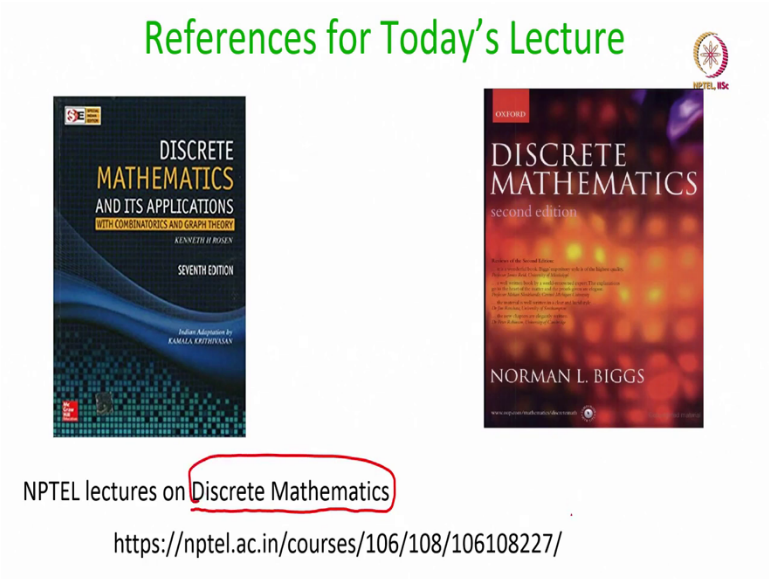
Now, what we can say about y power minus 1 product x power minus 1. Well, it is going to be the inverse of x dot y. Because, if we multiply x dot y, with y inverse dot x inverse, then that is going to give us x dot y dot y inverse dot x inverse. Now, y dot y inverse gives me the element 1 and x multiplied with 1 will be x. So, this becomes as x multiplied with x inverse and x multiplied with x inverse will be 1 which is the identity element; that means, the element y inverse dot x inverse is the inverse of x dot y.

But from the definition of field, we know that it is only the non-zero elements which have the inverse; that means, if at all there is an inverse of x dot y that x dot y has to be an element different from 0. But that is a contradict, but that is what we want to show through the contraposition, ok. So, we ended up showing that if either x is not 0 or y is not 0, then x dot y is also not 0 which actually is equivalent to showing that if x dot y was 0 then either x is 0 or y is 0, ok.

However, this property need not be true in a ring; that means, in a ring, we can find non-zero x, non-zero y, but their product being 0 that is possible, ok. And, where exactly the proof fails; whatever proof we have given for the case of field. The proof fails down because we use the fact that x inverse and y inverse exist in the case of field and that comes from the field axiom F2. Because, if x is not 0 and y is not 0 then as per the definition of field or axiom F2 x inverse and y inverse exist.

But if we take a ring instead of a field; then the ring axiom R2 does not guarantee us that x inverse and y inverse exist. Because in ring, it is not necessary that every element has a inverse with respect to the dot or the multiplication operation

(Refer Slide Time: 30:25)



References for Today's Lecture

NPTEL, IISc
DISCRETE MATHEMATICS AND ITS APPLICATIONS
WITH COMBINATORICS AND GRAPH THEORY
KENNETH H ROSEN
SEVENTH EDITION
Indian Adaptation by KAMALA KRITHIVASAN
OXFORD
DISCRETE MATHEMATICS
second edition
NORMAN L. BIGGS

NPTEL lectures on Discrete Mathematics

https://nptel.ac.in/courses/106/108/106108227/

So, these are the basic things regarding our Abstract Algebra which we will be using now for the rest of the course. There are several well-known references to know more about the Abstract Algebra - groups, rings and fields. I have taken I have followed the discussion which is available as part of the NPTEL lectures on Discrete Mathematics course offered by me, those videos you can access from this link.

Thank you.