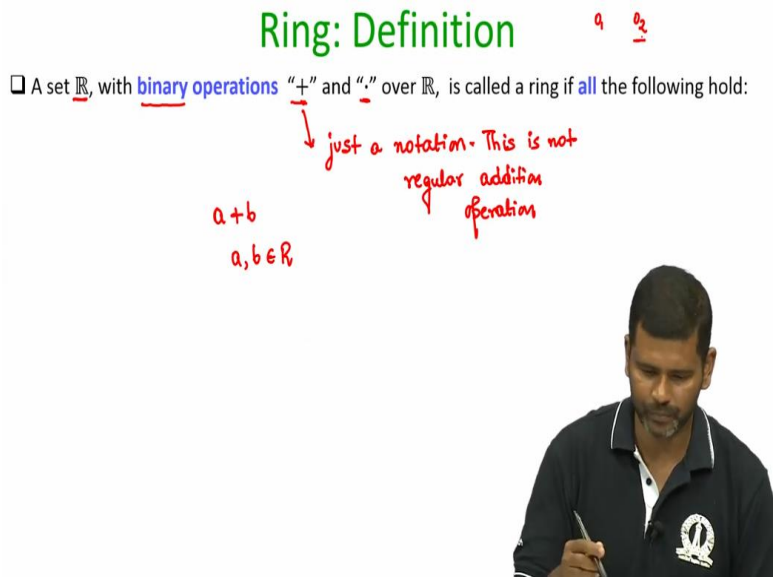
Secure Computation - Part I
Prof. Ashish Choudhury
Department of Computer Science
International Institute of Information Technology, Bangalore

Module - 1
Lecture - 5
Recap of Basic Concepts from Abstract Algebra Contd.

(Refer Slide Time: 00:32)

Hello everyone. Welcome to this lecture. So, the plan for this lecture is as follows: We will continue discussing some various facts from abstract algebra. In the last lecture, we discussed about groups. In this lecture, we will discuss about 2 other algebraic structures namely rings and fields, which will be useful when we will design MPC protocols.

(Refer Slide Time: 00:57)



So, what is a ring? So, remember, when we discussed groups, in group, the set G involved a single operation, namely the operation $\circ$. But when we consider a ring, we will be given a set $\mathbb{R}$, and now there will be 2 operations instead of 1 operation. I could have called them as operation o_1 and operation o_2, but, instead, we use the notation $+$ and the notation $\cdot$ for the operations o_1 and o_2.

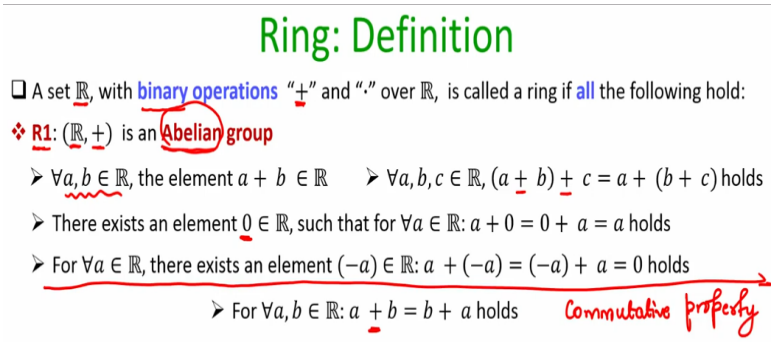
Both of them will be binary operations, namely, they will be operated on 2 elements at a time, from the set $\mathbb{R}$. And an important point to note here is that this $+$ is just a notation, means just a representation for your operation o_1. I could have used operation o_1, but instead I am using the $+$ notation here. And this is just a notation. This is not the regular addition operation.

So, whenever I write $a + b$ here, where a and b are elements of the set $\mathbb{R}$, you should not interpret it as the addition of the elements a and b in the integer sense. Even though I will say that I am going to add a and b, because I am using the notation $+$ here, that is not the usual addition operation. The addition operation will be defined as per the set $\mathbb{R}$. So, my addition operation, $+$ operation could be here, the $+_N$ operation.

Even though it is $+_N$ operation, I will be saying or I will be using the notation $+$ to denote that. So, that is just an abstract notation here. In the same way, this operation $\cdot$ is an abstract notation for multiplication operation or the operation number 2. But that need not be always the integer multiplication or real number multiplication. It is just an abstract notation.

So, for the groups, we require that the set G along with the operation $\circ$, should satisfy certain properties. Now, for $\mathbb{R}$ to be considered as a ring, with respect to this $+$ and $\cdot$ operation, some properties should be satisfied.

(Refer Slide Time: 03:48)



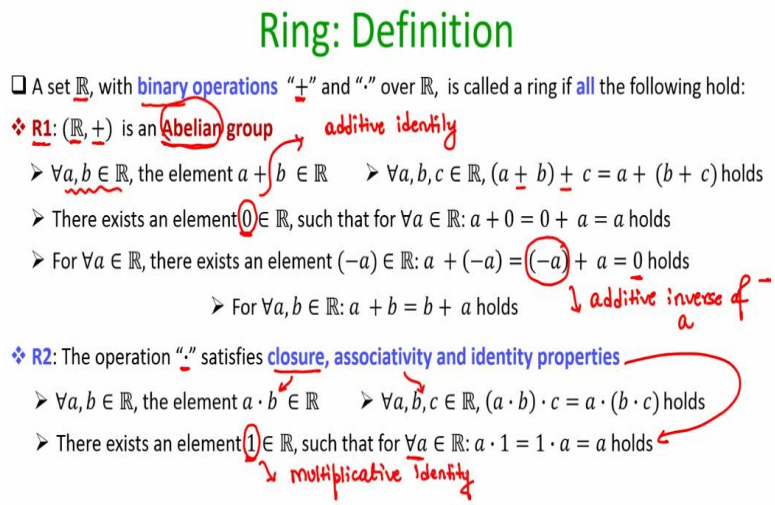
So, let us see what the properties are. So, the first ring axiom is that, if I consider the set $\mathbb{R}$ along with the $+$ operation, it should constitute an abelian group. Now, what is this abelian group? It is a special type of group. Since the operation $+$ should satisfy the group axioms, that means the closure property should be satisfied. That means, you take any pair of elements a and b from the set $\mathbb{R}$; add them; you should obtain back an element from the set $\mathbb{R}$ itself.

The plus operation in your set $\mathbb{R}$ should be associative. There should be some special element 0 from the set $\mathbb{R}$, which should be the additive identity element. And there should be an additive inverse element for every element a. So, up to this point, we have just considered group axioms. Now, what is an abelian group? It is a special type of group where a fifth property is satisfied, namely the commutative property.

So, remember, when we discussed the properties of groups, there I stressed that it is not necessary that if your operation $\circ$ is associative, it should be commutative. That may or may not be the case. So, that is why, every group need not be an abelian group. It will be considered as an abelian group if the operation $\circ$, which in this specific case is the $+$ operation, also satisfies the commutative property.

If it does not satisfy the commutative property, then it will be not considered as an abelian group. So, my first ring axiom is that, if I perform the $+$ operation; again I stress, by $+$ I mean whatever way I define the $+$ operation. I am right now considering it as an abstract operation. So, the first ring axiom is that the $+$ operation over the set $\mathbb{R}$ should constitute an abelian group. That is the first requirement.

(Refer Slide Time: 06:12)



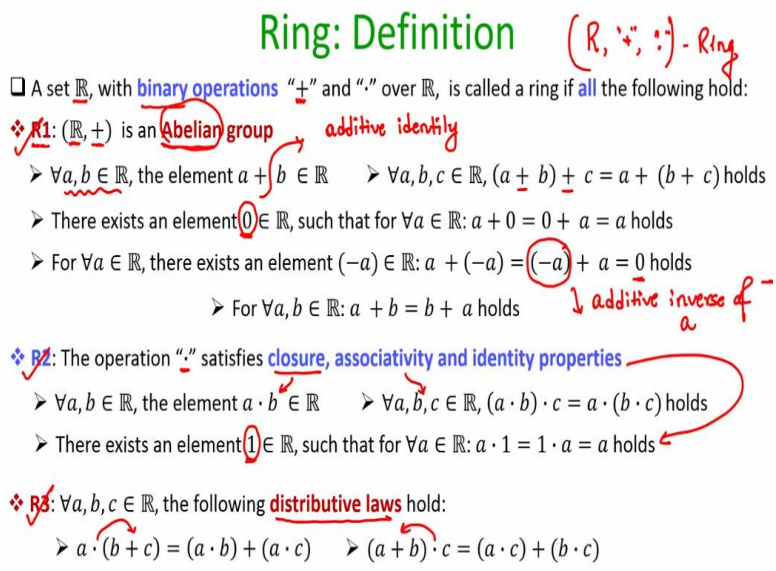
The second requirement is that if I consider that the · operation over the set ℝ, then it should also satisfy certain properties. Namely, it should satisfy closure property; that is, if you take any pair of elements from the set ℝ; perform the · operation; you should get back an element of the set ℝ. The · operation should be associative over the set ℝ. And the · operation should have an identity element.

Namely, there should exist some special element which I denote by 1, such that it constitutes an identity element for every element a from your set ℝ. That is a second ring axiom. So, the element 0 here, I will call it additive identity if it exists. And again, this is just a representation of some special element, namely the identity element. That need not be the integer 0.

And the inverse of a with respect to the plus operation, it will be called as the additive inverse of a, denoted as $-a$. Again, this should not be interpreted as the negative of a. It is just a representation of the element. So, property of this $-a$ element is that, if you perform the $+$ operation involving this element $-a$ and the element a, you will get back the 0 element which is the additive identity element.

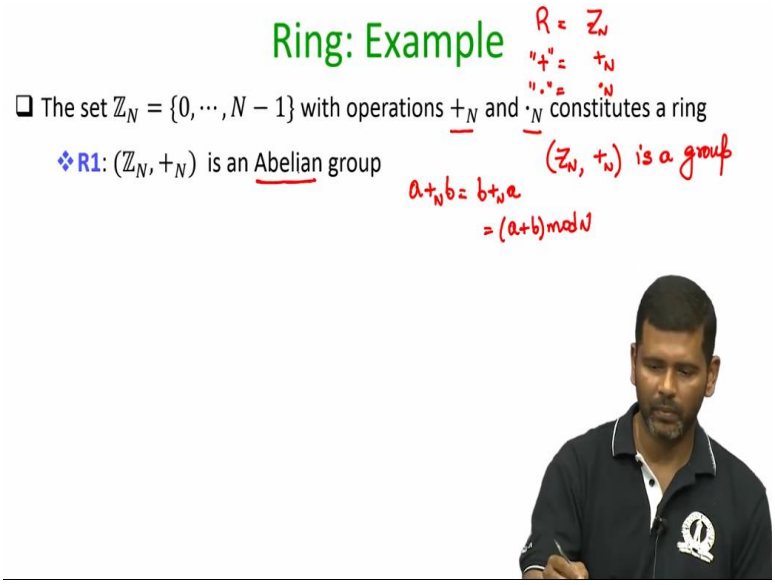
In the same way, this element 1, if it exists, this need not be the integer 1. It is just a representation of a special element from your set ℝ. And if such a special element exists, then I will call it as the multiplicative identity or the · identity. That means, it constitutes the identity element with respect to your dot operation.

(Refer Slide Time: 08:40)



The third property which the + and the · operations should satisfy over the set ℝ is the following: It should satisfy the distributive laws. What are the distributive laws? The requirement here is that, the · should be distributed over +, in these 2 ways. If all these 3 properties are satisfied, R_1, R_2 and R_3, then I will say that the set ℝ along with this abstract + operation and the abstract · operation constitutes a ring. If any of these 3 properties is violated, then I would not be calling ℝ as a ring.

(Refer Slide Time: 09:33)



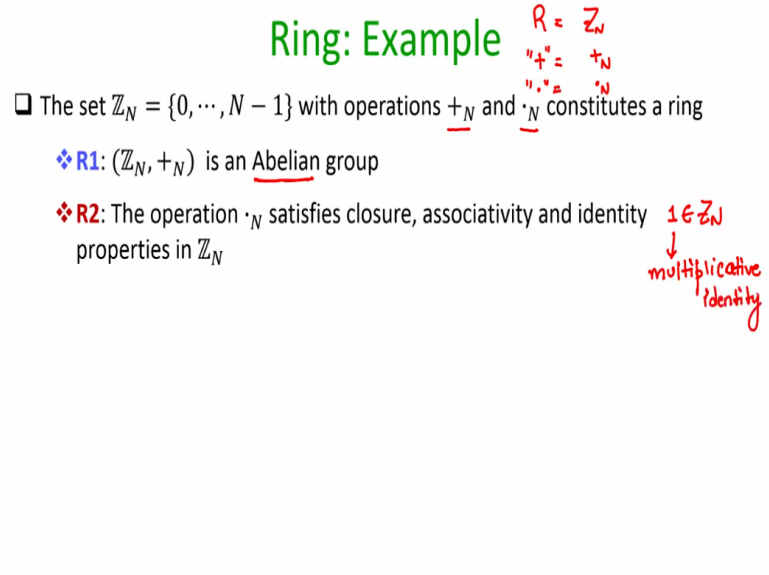
So, let us see some examples of rings. So, let us consider the set $\mathbb{Z}_N$ which we have defined in the last lecture. It is a set of all possible remainders which you can obtain by dividing any integer by a modulus N. And now, I consider the addition modulo N operation and the multiplication modulo N operation. So, basically, what I am saying here is now, my abstract set ℝ is $\mathbb{Z}_N$.

My abstract $+$ operation is actually the addition modulo N operation $+_N$, which I have defined in the last lecture. And my abstract $\cdot$ operation here is the multiplication modulo N operation $\cdot_N$, which also I had defined in the last lecture. And now, let us see whether all the ring axioms are satisfied or not. In the last lecture, we already proved that $\mathbb{Z}_N$ along with the operation of $+_N$ is a group. We already proved that in the last lecture.

It satisfies your closure property; the operation of $+_N$ is associative; the integer element 0 which is a member of the set $\mathbb{Z}_N$ is actually the additive identity element; and $N - a$, if a is an element of $\mathbb{Z}_N$, then the element $N - a$ will be the additive inverse element; and that is why all the 4 group axioms are satisfied. But it satisfies the additional property that the addition modulo N operation is also commutative.

Because, if you perform $(a + b)\%N$, the result will be same as $(b + a)\%N$, because both of them will give you the result $(a + b)\%N$. So, that is why your $+_N$ operation is commutative. And that is why the first ring axiom is satisfied. That means, with respect to the abstract $+$ operation, where the abstract $+$ operation in this case is the addition modulo N operation, the set $\mathbb{Z}_N$ is an abelian group.

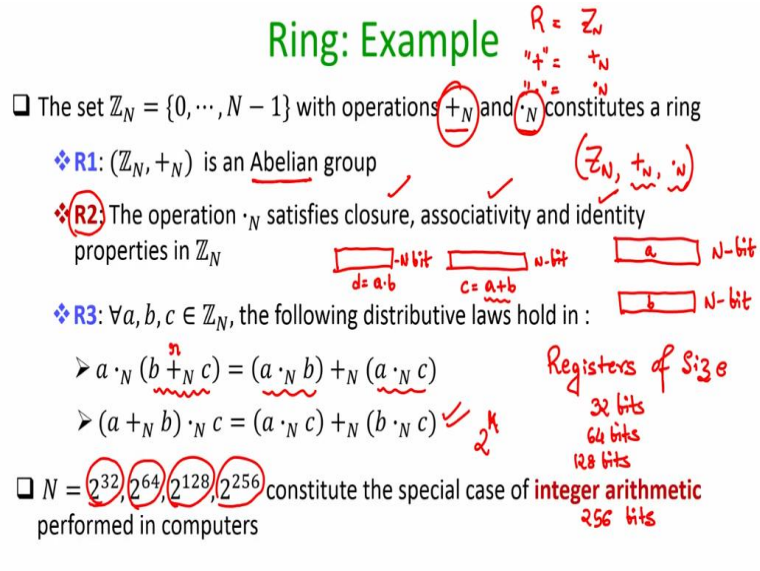
(Refer Slide Time: 11:58)



Now, let us consider the multiplication modulo N operation and see whether it satisfies the closure, associative and identity properties. The closure property is guaranteed. Because, you take any 2 numbers in the set $\mathbb{Z}_N$; multiply and then take modulo N; the result will be an element

of the set $\mathbb{Z}_N$. The operation multiplication modulo N is associative and integer 1 which is belonging to $\mathbb{Z}_N$ will be the multiplicative identity. That means, in this case indeed, 1, it should be, 1 is actually the integer 1, multiplicative identity.

(Refer Slide Time: 12:51)



Now, let us see whether the distributive properties are satisfied with respect to the addition modulo N and multiplication modulo N. And it is easy to verify that indeed the distributive laws are satisfied. So, I leave it as an exercise for you. You can easily prove that. If you add b and c and then take modulo N and call that number as r, and then if you multiply a and r and then take modulo N, the result will be same as if you first multiply a and b modulo N and then multiply a and c modulo N and then add the individual remainders and then take modulo N.

The result will be the same. And same way, you can prove the second distributive property as well. So, that shows that the set $\mathbb{Z}_N$ along with the operation of addition modulo N and multiplication modulo N constitutes a ring. Now, this is a very interesting ring. Because, if I consider the moduluses of the form 2^{32}, 2^{64}, 2^{128}, 2^{256}, then basically this captures the special case of integer arithmetic performed inside your computers.

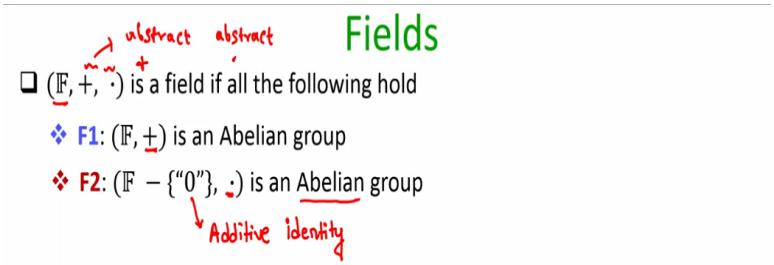
Because, typically inside your computers, you have registers which are typically of size 32 bits or 64 bits, well 128 bits or even if you have a very powerful machine, then the registers will be of size 256 bits; they can store any integer of length n bits. And now, if you have a register where you have stored an integer a, another register which has stored the value b, and both of them are n bit registers.

And then, there is another register c which is also an n bit register. And this register stores basically the result of adding the values which are stored in the a register and b register. Then, basically, since c register can also store an n bit number; that means, if the result of addition of a and b cannot be stored in an n bit number, then basically you have to; that means an overflow has occurred; and that means, you have to reduce that value to $c \% N$, so that it can fit an n bit register itself.

So, basically, internally what computer is doing is, it is actually doing an addition modulo N operation. Similarly, if you have a d register which is also an n bit register, and where you want to store the result of product of the values stored in the a and b register, then again, if the result of multiplying a and b crosses an n bit number, then you have to do a modulo N operation so that the result can be kind of truncated and stored as an n bit number.

So, there you are actually performing a multiplication modulo N operation. And that is why, depending upon the size of registers which are there inside your CPU, which are typically of the form, some 2^K; this ring $\mathbb{Z}_N$ with respect to the addition modulo N operation and multiplication modulo N operation actually constitutes or it mimics the integer arithmetic performed inside your computers.

(Refer Slide Time: 16:56)



Now, let us introduce our third algebraic structure which are called as fields. And here also, you have abstract $+$ operation and abstract $\cdot$ operation as it was the case for rings. And now,

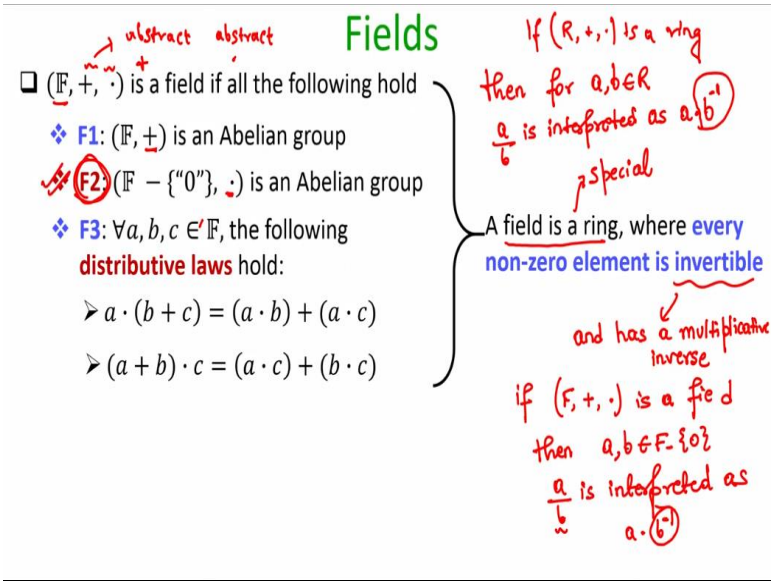
you demand some additional axioms over the ring axioms. So, when we will say that a set $\mathbb{F}$ constitutes a field with respect to this abstract plus an abstract $\cdot$? If the following conditions are satisfied.

So, the first field axiom is that a set $\mathbb{F}$ along with the abstract $+$ operation should be an abelian group. Well, this was the requirement even for the case of ring. For the rings, whatever was the set, the plus operation with respect to that set should constitute an abelian group. Now, the second requirement here is that, if I exclude the additive identity which I often call as the 0 element; by 0 element, I mean the additive identity.

That does not mean that the integer 0 is a member of $\mathbb{F}$. No. Remember, 0 is just a representation. So, the demand here is the following: If I consider the non-zero elements from the set $\mathbb{F}$, then with respect to the $\cdot$ operation, that truncated set should also constitute an abelian group. Now, this is a new property. Because, if I go back to the requirements of ring, then in the second ring axiom, there was no demand with respect to the dot operation.

Namely, it was not required that the $\cdot$ operation should constitute a group. We needed only the closure property, associative property and the existence of the identity element. It was not required in the second ring axiom that the dot operation should also satisfy the group axioms. But now, when I come to the field, the demand here is that, if I consider the non-zero elements of the set $\mathbb{F}$, then, along with the $\cdot$ operation, they should satisfy the requirements of abelian group. Namely, the closure property should be there, associative property should be satisfied, identity element should be there and the inverse element also should be there.

(Refer Slide Time: 19:42)



And of course, like we had the distributive law for the rings, we demand that the $\cdot$ should be distributive over $+$ in the case of fields as well. So, if we closely compare rings with fields, what we can say is the following: A field is a special type of ring where every non-zero element is also invertible. That need not be the case just for a ring. Because for a ring, if I consider an element from the set $\mathbb{R}$, that may or may not have a multiplicative inverse.

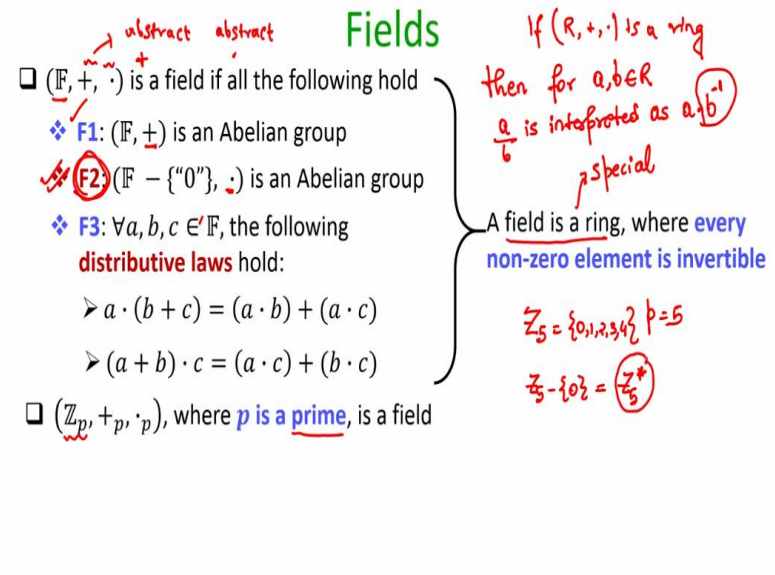
But the axiom number F_2 demands that every non-zero element is invertible and has a multiplicative inverse. That is why field is a special kind of a, more powerful algebraic structure compared to ring. Because, in ring, since every element need not have a multiplicative inverse, you may not be able to do the division operation. What do I mean by division operation in a ring?

So, if $(\mathbb{R}, +, \cdot)$ is a ring, then, for $a, b \in \mathbb{R}$, $\frac{a}{b}$ is interpreted as$a \cdot b^{-1}$. That is the interpretation of a divided by b in an abstract ring. But at the first place, this element b^{-1} may not be present in the ring $\mathbb{R}$, because ring does not give you the guarantee that every element has its multiplicative inverse. But if I consider a field, then, for any $a, b \in \mathbb{F}$, $\frac{a}{b}$ is interpreted as$a \cdot b^{-1}$.

And now, because of this second field axiom, b^{-1} is guaranteed to exist, because $a, b \in \mathbb{F} - \{0\}$. So, if both a and b are non-zero elements, then $\frac{a}{b}$ should be interpreted as $a \cdot b^{-1}$. And since b is a non-zero element because of this second field axiom, it will be guaranteed that b^{-1} exists. So, that is what the interpretation of division operation is over rings and fields.

So, basically the idea is that you now are given the flexibility to do both multiplication, addition, subtraction, as well as division. In rings, you may or may not be always able to perform the division operation, because the multiplicative inverse need not exist. But over a field, you can always perform division involving the non-zero elements.

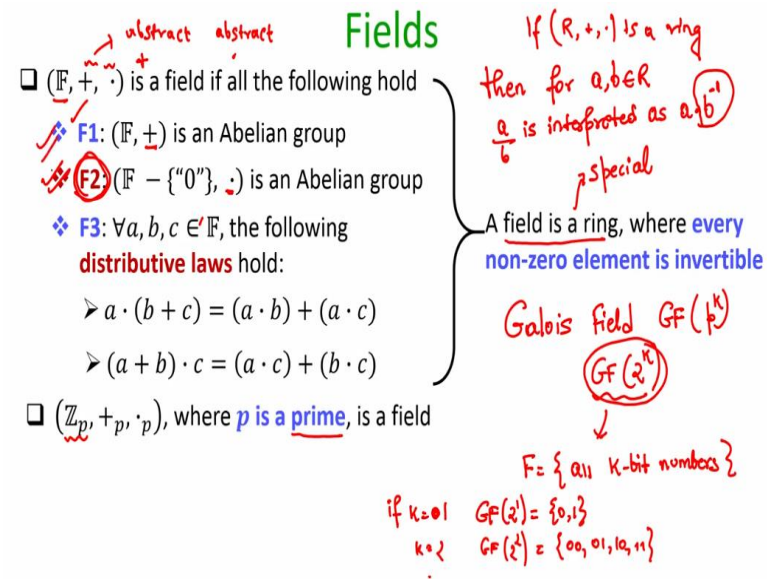
(Refer Slide Time: 23:29)



So, what could be an example of a field? The simplest example is the set $\mathbb{Z}_p$, where p is a prime number. So, for instance, if I consider the set $\mathbb{Z}_5$. Because, if I take $p = 5$ which is a prime number, then$\mathbb{Z}_5 = \{0,1,2,3,4\}$. Then, you can verify that field axiom 1 is satisfied. And if I take$\mathbb{Z}_5 - \{0\}$, then, as per our definition of $\mathbb{Z}_p^*$; this is $\mathbb{Z}$; because, as soon as I exclude the element 0 from the set $\mathbb{Z}_5$, I get all the elements which are co-prime to 5.

So, 0 cannot be co-prime to 5. So, I have excluded it. Now, I have $\mathbb{Z}_5^*$. And now, you can check that every element in this set $\mathbb{Z}_5^*$ will have its multiplicative inverse. And of course, with respect to the $+_p$ and $\cdot_p$ operations, the distributive properties are satisfied. So, that is why, this is a very nice example of a field. Of course, we can have other kinds of field as well.

(Refer Slide Time: 24:45)

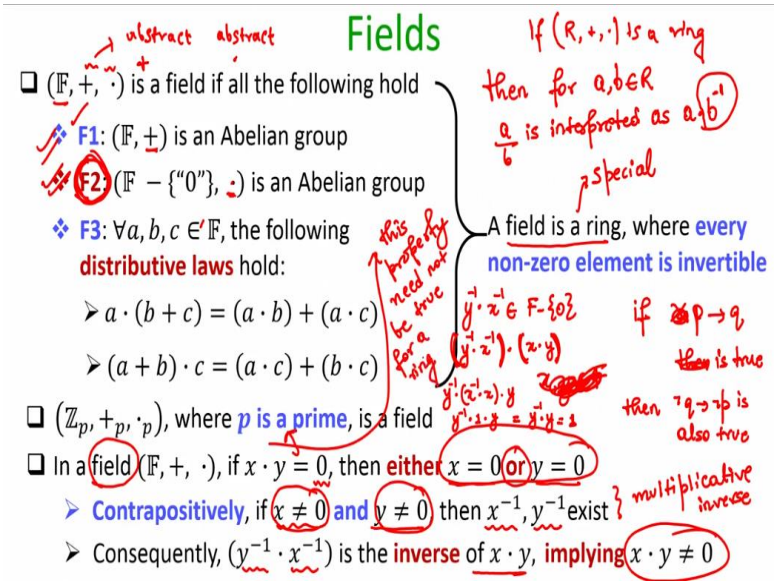


We encounter what we call as Galois field, which is typically of the form, some prime p raised to power K, denoted as $GF(p^K)$. But a popular one which we use for implementation purpose is Galois field of size 2^K. What is this field? Basically, this is a field. Here, $\mathbb{F}$ is a collection of all K bit numbers, where K is some parameter. So, for example, say if $K = 1$, then $GF\ (2^1)$ will consist of all 1 bit numbers.

If $K = 2$, then $GF(2^2)$ will have the bit strings 00, 01, 10, 11 and so on. And the $+$ operation and the $\cdot$ operation over this Galois field is not the usual $+$ operation or the$\cdot$ operation. They are defined in a special way. So, when we will encounter Galois field, we will see the details, what exactly are the $+$ operation and $\cdot$ operation; and they will satisfy all these field axioms. So, that is another popular field which we use.

Of course, there could be other kinds of fields as well. You can define a field where the elements are polynomials. And then, your $+$ operation is defined to be addition of polynomials; $\cdot$ operation is defined to be multiplication of polynomials and so on. So, that is a field.

(Refer Slide Time: 26:33)



An interesting property of the field is the following, which we will encounter, which will be useful when we will design MPC protocols. So, if you have 2 elements x and y which belong to this set , and $\mathbb{F}$ is a field, and if the result of $x \cdot y$ is the 0 element, namely the additive identity element, then it has to be the case that either $x = 0$ or $y = 0$. When I say $x = 0$, by that I mean that it is either the case that either your x is the additive identity element or y is the additive identity element.

So, you can quickly verify that this indeed is the case for the; this statement is indeed true for the case when yours field $\mathbb{F}$ is the set $\mathbb{Z}_p$, but this property in general holds for any field. How we can prove it? We can prove it by contrapositive. What do I mean by a proof by contrapositive? So, by proof by contrapositive, I mean the following: If you want to prove that if $p \rightarrow q$ is true, then $\sim q \rightarrow \sim p$ is also true.

So, one way of proving $p \rightarrow q$ to be true is, show that $\sim q \rightarrow \sim p$ is true. So, this is your q part of the statement. So, the negation of the statement ($x = 0$ OR $y = 0$) will be ($x \neq 0$ AND $y \neq 0$). This OR gets converted into AND. So, I want to show that if $x \neq 0$ and$y \neq 0$, then even $x \cdot y \neq 0$. How do I show that? If $x \neq 0$ and $y \neq 0$, that means they are the non-zero elements of the field $\mathbb{F}$.

Then, definitely their multiplicative inverse exists. Why the multiplicative inverse exists? Because of this field axiom number 2. Now, consider this element, namely the element $y^{-1} \cdot$

x^{-1}. Because of the closure property, since the $\cdot$ operation satisfies the closure property and y^{-1} and x^{-1} are non-zero elements, the result of $y^{-1} \cdot x^{-1}$ will also be an element of $\mathbb{F}$.

That means, I can say that, $y^{-1} \cdot x^{-1}$ is an element of $\mathbb{F} - \{0\}$, because of the closure property. However, this is a special element. If you see closely, then this element $y^{-1} \cdot x^{-1}$ constitutes the multiplicative inverse of $x \cdot y$. Why that is the case? Because, if you take $y^{-1} \cdot x^{-1}$, this will be a field element which is not 0. And then, if you multiply it with the element $x \cdot y$, and $x \cdot y$ is also a non-zero element from the field, you will get $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y)$

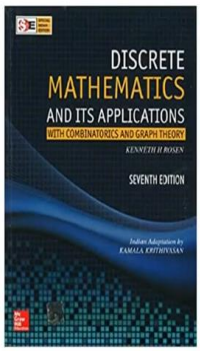
As per our assumption, $x \neq 0$ and $y \neq 0$. Since they are non-zero elements and since the $\cdot$ operation satisfies the closure property, $x \cdot y$ is also a non-zero element. But now, what will be the result of performing the $\cdot$ operation on these 2 elements? So, I can apply the associative property and then say that this is same as $(y^{-1} \cdot (x^{-1} \cdot x) \cdot y)$.

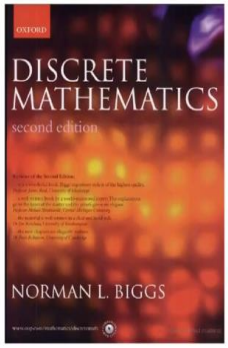
But the result of $x^{-1} \cdot x$ will be the multiplicative identity element, namely 1. So, this will be same as $y^{-1} \cdot 1 \cdot y$. And since 1 is the multiplicative identity, it being multiplied with y will give you the element y itself. So, you will get $y^{-1} \cdot y$. And $y^{-1} \cdot y$ will give you again the multiplicative identity element, namely 1. That means, indeed this element within the bracket, constitutes the inverse of another element.

And as per the field axiom F_2, the inverse element exists only for non-zero elements. So, that shows your $x \cdot y \neq 0$. So, that means, in a field, I can always say that if the $\cdot$ of 2 elements is the element 0, then definitely one of them has to be 0. But this property need not be true for a ring. You can verify that. I leave it as an exercise for you. This property need not be true for a ring. It is true only over a field.

(Refer Slide Time: 32:00)

References for Today's Lecture





So, with that, I conclude my discussion over the algebraic structures that we need for this course. Thank you.