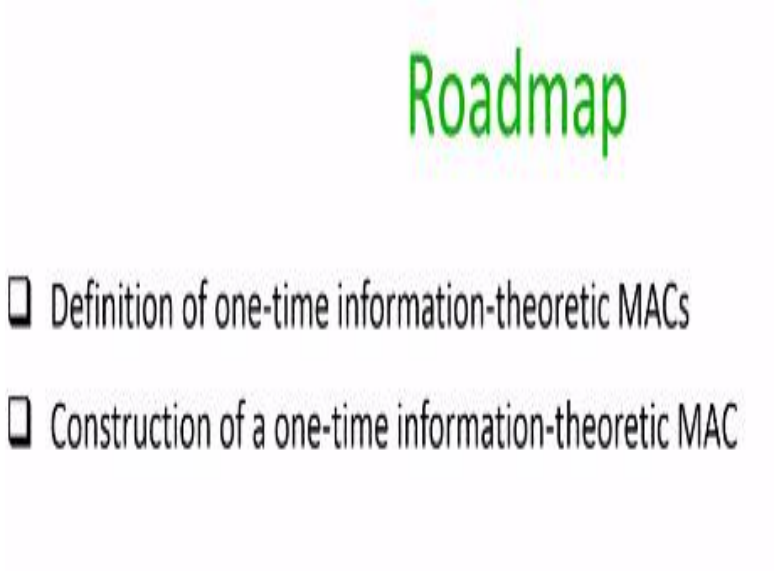
Foundations of Cryptography
Prof. Dr. Ashish Choudhury
(Former) Infosys Foundation Career Development Chair Professor
International Institute of Information Technology – Bangalore

Lecture – 25
Information – Theoretic MACs

Hello everyone, welcome to lecture 23. Just to recap, in the last lecture, we have seen how to construct message authentication codes for arbitrary long messages, basically we had seen how to construct pseudorandom functions for arbitrary long inputs and we have seen that once we have pseudorandom functions for arbitrary length inputs, we can directly plug in them to construct secure MACs for arbitrary length messages, right. However, the constructions that we had seen in the last lecture are computationally secure, namely they are secured only against an adversary whose running time is polynomially bounded.

An interesting question is can we design message authentication codes which are secure even against an adversary who are computationally unbounded right because that is a natural question that one can ask. Remember in the context of encryption process, we had seen that it is indeed possible to achieve the notion of perfect secrecy namely we can design perfectly secure encryption schemes which are secure even against a computationally unbounded adversary.

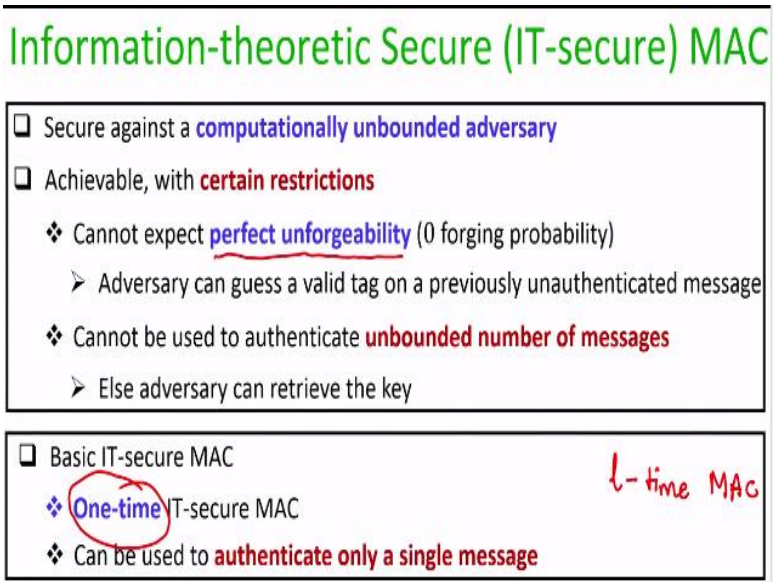
(Refer Slide Time: 00:31)



So at today's lecture, the focus will be how to construct secure MACs which are secure even against an adversary which is computationally unbounded and the plan for this lecture is as

follows. We will give the definition of one-time information-theoretic MACs and we will see a candidate construction for one-time information theoretically secure MAC, right.

(Refer Slide Time: 01:15)



So what are exactly information-theoretic secure or IT secure MAC. So basically, they are MACs which are secured against a computationally unbounded adversary and it is indeed possible to construct such MAC but with certain restrictions. Namely first of all, you cannot expect to design information theoretically secure MAC which prevents forgeability meaning which gives you complete unforgeability right. That means there is always possible for an adversary to come up with a valid forgery, but what we could expect from the construction is that the probability of coming up with a valid forgery should be very less right.

So in the context of information-theoretic MAC, we cannot expect or achieve to obtain perfect unforgeability because there always exists an adversarial strategy where adversary can guess the value of a tag on a message which has which was never communicated by the sender, right. So this is unlike the perfectly secure encryption process where we had seen that indeed it is possible to design schemes where adversary obtains no additional information about the underlying message by seeing the ciphertext.

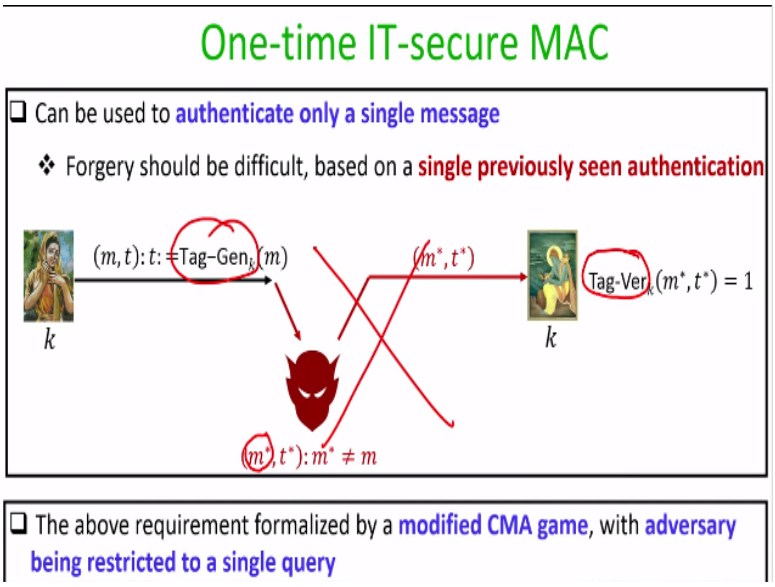
That means, adversary's advantage of learning the underlying message by seeing the ciphertext was absolutely 0, but similar guarantees we cannot achieve in the context of information-theoretic secure MAC because there always exists a guessing adversarial strategy. The second restriction that is imposed by information-theoretic secure MAC is similar to what was imposed by information theoretically secure encryption process.

So remember in the context of information theoretically secure encryption schemes or perfectly secure encryption schemes, one of the key restrictions was that we cannot reuse the same key to encrypt arbitrary large number of messages. One key can be used at most for one instance of encryption. So, the same restriction carrys over in the domain of information theoretically secure MAC, namely we can formally prove that if we are designing an information theoretically secure MAC, then we cannot authenticate arbitrary or unbounded number of messages using the same key.

So, the key reusability is again a restriction imposed by MAC in the information theoretic world, right. So in this lecture we will consider a very basic information-theoretic secure MAC, namely we will construct what we call as one-time information-theoretic secure MAC, that means it provides you unforgeability guarantee only if a key is used for authenticating a single message and whatever discussion we are going to make today that naturally generalizes to the case where you can define what we call as *l*-time information-theoretic secure MAC.

Namely message authentication code which is information-theoretic secure and where a key could be used to authenticate *l* number of messages, right.

(Refer Slide Time: 04:49)



So, let us begin with the discussion on one-time information-theoretic secure MAC. So as I said earlier, they are special type of MACs which can be used to authenticate only a single message and the security requirement here is that it should be difficult for a computationally

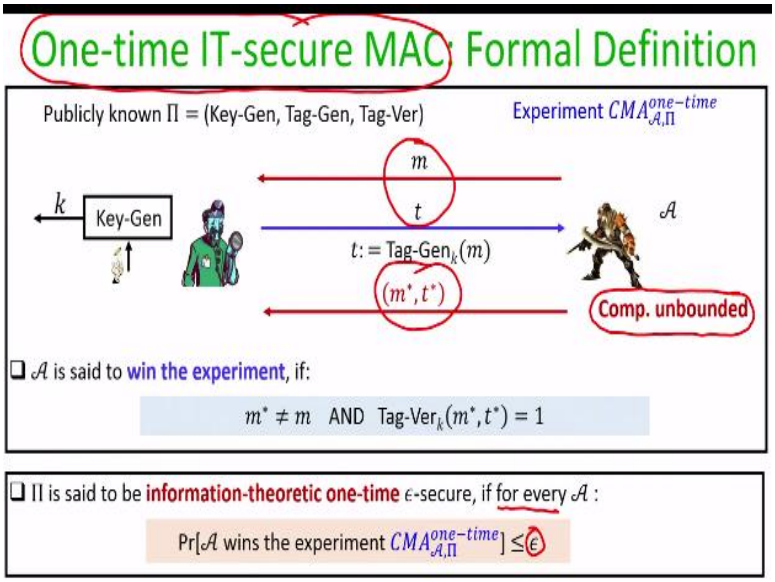
unbounded adversary to come up with a forgery based on a single previously seen authentication, right. So pictorially what exactly the security property that is achieved well by this primitive is as follows.

So imagine that we have an one-time information-theoretic secure MAC where the tag generation algorithm is Tag-Gen and the tag verification algorithm is Tag-Ver and imagine that we have a shared key which is uniformly random selected from the key domain of the underlying MAC and pre-shared between the sender and the receiver and for simplicity we assume that the message authentication code is a deterministic MAC.

So, imagine sender has authenticated one message and sent the (message, tag) over the insecure channel and say there is a malicious adversary which has seen the (message, tag) pair and the goal of the adversary is to come up with a forgery, namely by seeing the (message, tag) pair where the tag is generated with an unknown key k not known to the adversary. The goal of the adversary is to come up with a new message m* and a corresponding tag t* and forwarded to the receiver such that the verification of the message m* with respect to the tag t* is successful at the receiving end.

If this is the case if this is possible, then the adversary is able to do a forgery. So basically, the goal of the one-time information-theoretic secure MAC is to prevent this from happening, that means it should not be possible for an adversary to successfully come up with the message, tag pair m*, t* by seeing a previously authenticated message, tag pair even if the adversary is computationally unbounded. So this requirement we formalized by modified CMA game where the adversary is restricted to just make a single query, right.

(Refer Slide Time: 07:00)



So recall the CMA security game that we had seen in the context of message authentication code, right. So the game basically consists of a training phase where the adversary can ask for the MAC tag on several messages of his choice and based on the MAC, Tag pairs that it has seen, the goal of the adversaries to come up with a forgery, but now we are making some modifications in that experiment because we want to model the security of a one-time information-theoretic secure MAC.

So the changes that we have made in this experiment are as follows. The first change is that that instead of saying that adversary is computationally bounded, we allow a computationally unbounded adversary to participate in this game and the second restriction is that since we want to model security only against one-time authentication, the adversary can ask tag for a single message of its choice. We do not give the adversary to ask tag for arbitrary or polynomial number of messages because we are interested in only one-time authentication.

So, the adversary can ask for tag on any message of its choice and to respond to the adversary's query, the experiment of the verifier runs key generation algorithm, obtains a key and computes the tag on the message for which the adversary has asked for the tag and the tag is sent back to the adversary. So this basically models that adversary sitting between the sender and the receiver has seen a message, tag pair and now the goal of the adversary is to come up with a forgery.

That means based on the knowledge of m, t and without knowing the key k, the goal of the adversary is to come up with a pair m*, t* and we say that the output of the experiment is 1 or

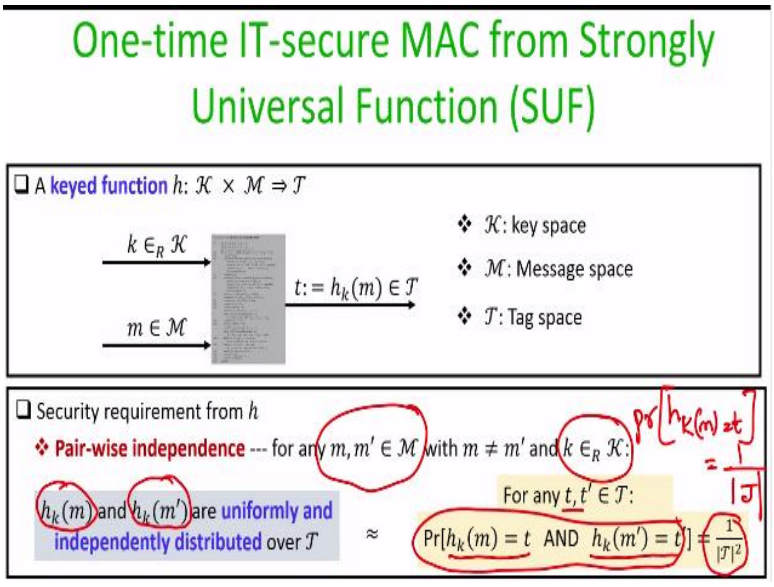
we say which is interpreted as adversary has won the experiment if the following 2 conditions hold. First the message m* should be different from m and the tag verification of the message m* with the tag part t* under the unknown key k should be equal to 1.

That means if the adversary has successfully produced a forgery, m*, t* such that m* is different from m, then we say that adversary has won the experiment and our security definition is we say that this publicly known message authentication code Π is information-theoretic one-time ε-secure if for every adversary A, right. I stress for every adversary, not only polynomially bounded adversary, but it could be even an adversary whose running time is computationally unbounded.

So the security definition is we say that the scheme Π is information-theoretic one-time ε-secure if the probability that adversary participating in this experiment is successfully able to come up with a forgery is upper bounded by the quantity ε, right, where the probability is taken over the random coins of the experiment, namely the randomness of the key generation algorithm and over the randomness of the message which has been queried by the adversary.

So that is our definition of one-time information-theoretic secure MAC. If we want to model the security of *l*-time information-theoretic secure MAC, then basically the modification here will be that adversary is now allowed to query for tag up to *l* number of messages right, so but for this lecture, we keep our discussion simple and we just focus on the one-time information-theoretic secure MAC.

(Refer Slide Time: 10:26)



So now we have the definition of what exactly we want to construct, namely we want to construct a one-time information-theoretic secure MAC and now let us see a generic construction of one-time information-theoretic secure MAC from another interesting cryptographic primitive, which we call as strongly universal function or SUF, right. So what exactly is an SUF? So it is a keyed function, so it takes a key from the key space where the key will be selected uniformly randomly and it will take a message as an input and it will produce a keyed output right.

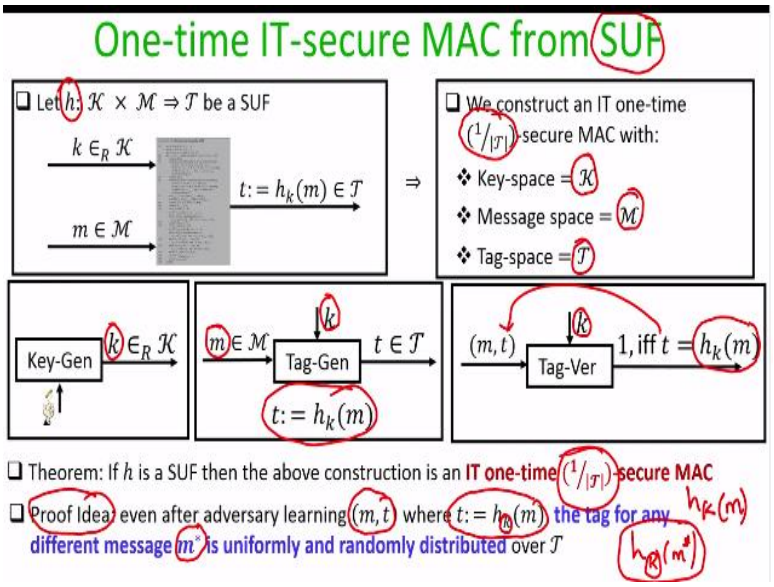
So the SUF is denoted by h which is a two input function, but once we fix the key, then the input is m and the output of the keyed function on the input m is denoted as t and the output t belongs to a bigger space which is called as the tag-space $\mathcal{T}$. So, syntactically this is same as the syntax of keyed pseudorandom function where we have a key as an input, block as an input and block and one possible output, but propertywise this SUF has different properties and security requirements compared to pseudorandom function.

So let us see the security requirements that we expect from this SUF. So the main property that we require from this SUF or the security property that we expect from this SUF is the pair-wise independence and what exactly we mean by pair-wise independence is that we require that for any message pair m, m' from the message space which are distinct and for any key k from the key space k, the tag value or the function value on input m and on input m' should be uniformly and independently distributed over the tag-space.

That means the value of $h_k(m)$ should be completely independent of $h_k(m')$ and both $h_k(m)$ and $h_k(m')$ would take any value from the tag-space with equal probability. Stated differently what it means is that for any tagpair t, t' from the tag-space, the probability that $h_k(m)$ takes the value t and $h_k(m')$ take the value t' is equal to $1/(|\mathcal{T}|)^2$ because if $h_k(m)$ and $h_k(m')$ are uniformly and independently distributed over the tag-space.

Then the probability that $h_k(m)$ takes the value t will be $1/(|\mathcal{T}|)$ and in the same way the probability that $h_k(m')$ takes the value t' will also be $1/(|\mathcal{T}|)$. So jointly the probability that $h_k(m)$ takes the value t and $h_k(m')$ takes the value t' will be $1/(|\mathcal{T}|)$ multiplied by $1/(|\mathcal{T}|)$ which is same as $1/(|\mathcal{T}|)^2$. So that is what the security requirement from SUF okay.

(Refer Slide Time: 13:32)



So for the moment, assume that we have an SUF right, we will soon see a candidate construction for SUF, but assume for the moment that you have an SUF whose description is publicly available, then using SUF we see how to construct generically one-time information-theoretic secure MAC right. So you have the public description of SUF and what we will construct is an information-theoretic secure MAC where the success probability of forgery for an adversary who is computationally unbounded is $1/|\mathcal{T}|$.

So the property of the MAC that we are going to construct is as follows. The key space will be the same as the keys space of SUF. The message space of the MAC, namely the messages which could be authenticated by the MAC that we are going to construct will be the same as the message space of the SUF and the tag-space will be the tag-space of the output space of our SUF. So the key generation, the tag generation, and the tag verification algorithm of the MAC that we are going to construct is as follows.

The key generation algorithm outputs a uniformly random k, k from the key space and the tag generation algorithm is a deterministic algorithm where to compute a tag on a message m with a key k, we basically compute the value of the SUF namely h with the key k and m as the input and that is the tag for the message m under the key k and the tag verification algorithm is canonical in the sense that if you are given a message,tag pair as input, then to verify a message,tag pair with respect to a key k, what you do basically is you re-compute the value of the tag under the key k for the message. Namely you evaluate or you compute the value of the SUF on the message as the input with respect to the key k and verify whether the

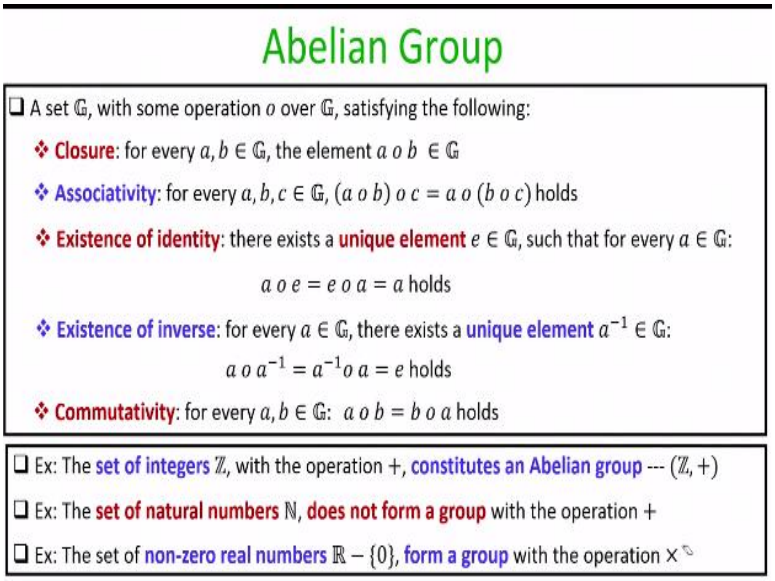
recomputed tag matches the tag that you have seen in your input. If that is the case, then the verification is successful and the output is 1, otherwise the output is 0. So that is the generic construction of one-time information-theoretic secure MAC from SUF. Now we want to prove that if the candidate h function that you are taking here is an SUF, then the MAC that we have constructed is information-theoretic secure for authenticating a single message where the success probability of forgery is $1/(|T|)$. That means an adversary who has seen a single message,tag pair authenticated as per the tag generation algorithm, then by seeing one message,tag pair the probability that an adversary could come up with a successful forgery is upper bounded by $1/(|T|)$.

The basic proof idea here is that imagine there is an adversary who is computationally unbounded and who has seen an authentication of a message m, that means say it has queried for the tag on a message m and it has seen the tag t and it knows that as per the construction the tag t that it has seen is the value of the SUF on the message m, but under the unknown key k. So the key is not known to the adversary and from the viewpoint of the adversary, the key is a uniformly random element from the key space and now the goal of the adversary is to come up with a forgery.

Basically, now it has a new message m* and its goal is to compute a tag on this new message m* with respect to the unknown key k and for that basically the adversary has to compute the value of $h_k(m^*)$, but since $h_k(m)$ and $h_k(m^*)$ are independent of each other right, that is a security property guaranteed from the underlying SUF since $h_k(m)$ and $h_k(m^*)$ are independent and uniformly distributed over the tag-space, the probability that a computationally unbounded adversary without knowing the key k could successfully come up with the output of the SUF on the input m* is of course $1/(|T|)$.

So that is the success probability with which a computationally unbounded adversary could come up with a forgery, so that is a proof idea. I am leaving the full formal details here, but you can very easily formalize the proof idea that we have discussed here intuitively.

(Refer Slide Time: 18:03)



So now we have a generic construction of one-time information-theoretic secure MAC given that you are having a SUF. So now the question is how do we construct a candidate SUF, and there could be several possibilities to construct an SUF. What we are going to do is now we will see a candidate construction based on group theory and finite field arithmetic. So let us see the definition of abelian group first. So what exactly is an abelian group?

So a group basically consists of a set which could be either finite or infinite, it has certain number of elements and along with that set you have an operation o and we say that the set $\mathbb{G}$ along with the operation o constitutes a group if the following properties are satisfied. The first property is the closure property which states that if you take any two elements from the group, say a and b and perform the group operation o those two elements, then the result should again be a member of the group and that is why the name closure property.

That means by performing the operation little o on any two group elements, you would not go outside or you would not get an element which is outside the group. You will still get an element which belongs to the group. So that is why the name closure property. The second property that we require from the set $\mathbb{G}$ and operation o is as follows. It is called associativity property and which basically demands that if you take any 3 elements a, b, c from the group right, then it does not matter whether you perform the group operation on a and b and then following by performing the group operation on c.

You will get the same answer if you first perform the group operation on b and c and then you perform the group operation on the result on the element a. That means the operation o

satisfies the associativity property. The third property that we require is the existence of identity element, namely there should exist a unique element which we denote as say e belonging to the set $\mathbb{G}$ which satisfy a magical property.

Namely it should satisfy the condition that if you take any element a from the group $\mathbb{G}$ and if you perform the group operation or the operation o on the element a and on the element e, then you should get back the element a and that is why we call that special element e as the identity element. That means you perform that operation o with e and any element a from the group, you will end up getting back the element a. The next property that we require from the set $\mathbb{G}$ and operation o is as follows.

We require that there should exist for every element a from the set $\mathbb{G}$, there should exist a special element which we denote as a inverse or a raise to power -1 such that if you perform the operation o on the element a and this element a^{-1}, you should get back the identity element. So I stress that even though we are using the notation a raise to power minus -1, numerically it is not equal to 1/a because we are constructing where we are actually treating the set $\mathbb{G}$ in abstract terms.

That means your set $\mathbb{G}$ could consist of any type of element, it need not be numbers or integers or so on, it could be consisting of say vectors, matrices and so on. So do not get confused that a to the power -1 stands for the numeric 1/ a, it is just a notation. What we are basically demanding here is that if you take any candidate element a from the set G, then corresponding to that you should also have a candidate element from the set G itself which I am denoting by this notation a^{-1} such that if you perform the operation o on the element a and on this special element a^{-1}, you should get back the identity element, right.

So if my set G along with operation o satisfies these 4 properties, then I say that G, o is a group and on top of these 4 properties if my set G along with the operation o satisfies an additional condition namely that of commutativity property which requires that for any pair of elements a, b from the set G, it does not matter whether you perform the operation on a and b or on b and a, you get back the same answer, then that special group is called as an abelian group.

So in the absence of commutative property, what we obtain is a group, but on top of that if the group also satisfies the commutativity property, then the group is called as an abelian group, right. So that is the definition of an abstract abelian group. Now let us see some candidate examples for an abelian group. So if you consider a set of integers which I denote by $\mathbb{Z}$ which is an infinite set and if I take the operation plus namely the integer addition.

So my operation o in this case is plus and my set $\mathbb{G}$ is nothing but $\mathbb{Z}$, then the set of integers along with the integer addition satisfies the closure property, associativity property, existence of identity, existence of inverse and commutative property. You can verify that, right. So let us verify the closure property. If you take any two integers and add them numerically, you will again obtain an integer, so closure is satisfied. It is easy to verify that the operation integer addition satisfies the associativity property

Because it does not matter that whether you add a and b first and followed by adding c, you get the same answer which you have by performing the addition of b and c first and then adding the answer to a, so the associativity property is satisfied. The element 0 belonging to the set of integers constitutes your identity element because a+0 for every integer a is going to give you back the element a and for every element a or for every integer a, you have the corresponding integer -a also belonging to the set of integers such that a + -a is going to give you the identity element namely 0.

And it is easy to verify that for any two integers a and b, a+b is same as b+a, so the commutativity property is also satisfied. That means the set of integers $\mathbb{Z}$ along with the operation plus satisfies all the 5 axioms that I require from an abelian group and that is why the set of integers along with the integer addition operation constitutes a candidate abelian group okay right. So we have seen an example of abelian group. Now let us see whether the set of natural numbers which I denote by $\mathbb{N}$ along with the operation plus constitutes a group or not.

So it satisfies the closure property, if you take any two natural numbers and add it, you will get a natural number, the addition operation satisfies the associativity property over the set of natural numbers. The problem here is that you do not have the identity element right because you do not have the element 0 present in the set $\mathbb{N}$, so this axiom is not satisfied and it turns

out that every natural number does not have an inverse in the set of natural numbers. So if you take for instance the element 2, its inverse should be ideally -2.

So first of all the identity element is not at all there, so the inverse is not at all well defined, so this axiom is also not satisfied. So since two of the axioms are not satisfied, the set of natural numbers along with the operation plus does not constitute a group. In the same way if we take the set of nonzero real numbers right, so it constitutes a group with respect to the multiplication operation. So if you take any 2 nonzero real numbers, multiply it, you again obtain a nonzero real number, multiplication satisfies associativity property.

The element one will constitute the identity element and for every element a belonging to the real number you have a corresponding real number 1/a present in the set of real numbers such that 1/a multiplied by a will give you the identity element 1, right and 1/a is indeed well defined because my a cannot be 0 because I am considering the set of elements which consists of all the real numbers except 0, so a cannot be 0.

So the inverse element is also well defined and of course multiplication operation satisfies the commutativity property and that proves that the set of nonzero real numbers constitute a group with respect to the multiplication operation. So that is the definition of group right. I hope you enjoyed this lecture. Thank you.