Mathematical Logic
Prof. Arindama Singh
Department of Mathematics
Indian Institute of Technology, Madras

Lecture - 1
Sets and Strings

What a set is, we will not define; what membership is, we will not define. But then it's difficult to not define anything and you are using a technical term; are you confident that you are using it correctly? That brings up all this question. In fact, it becomes correct because the properties it obeys, that is enough for us. Anything else if you said instead of set or membership? But, it has those properties; it is enough. That is how we will be proceeding; you become slightly accustomed to using the language you do not know exactly what it means.

But, it means something around this, it is enough; that is the idea. That happens in mathematics also. That is what membership is. We go for the operations on sets, say union, intersection; remember those things? Yes? You will define them. I am just brushing it up, now then difference of sets, then power set, then the properties of these operations, etc.

Power set always has more elements than the set itself; you can prove it. Can you? But it needs to define what is `the number of' means. Fine. For example, take the set of natural numbers. How many elements it has? Infinite elements? Take its power set. How many elements it has? How do you say it has more elements? It is also infinite; raise your hand.

Student: Elements... from each member of the set A all of them are present in the power set as, so power set at least has the same cardinality as the set.

Please continue.

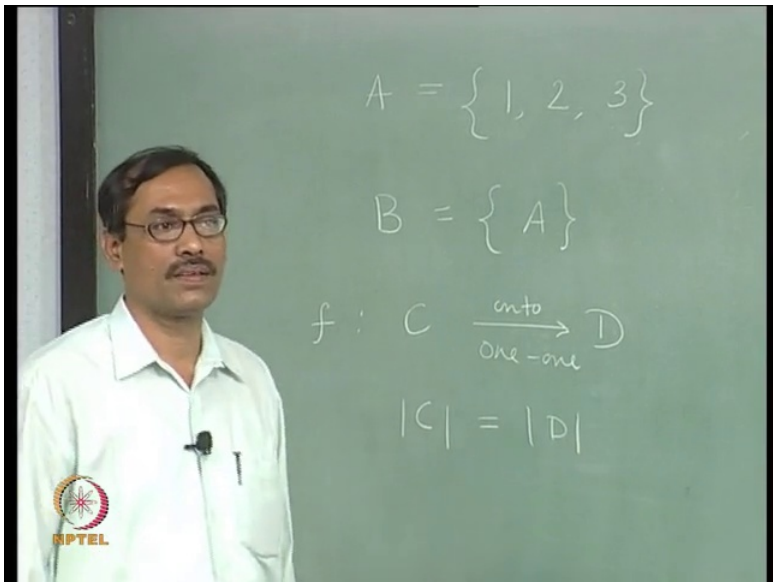
Student: Power set at least has the same number of elements as the set A which we looking at now. You can always consider one more element at least say as combination of just 1, 2 for a set of natural numbers, at least has it has at least one more than the number of elements in the set A, you can say, more elements.

That makes sense, but not exactly. Let us try to make it exact. First thing is `cardinality'; you have used, which we do not know, we know of course, we have not yet `brushed it up' till now. We have this `number of', `cardinality'; these are used synonymously. The problem is what is `number of', we can define for finite sets easily, perhaps for infinite sets it can become difficult to define. What we can do is, we can compare sets for their `number of', for their `cardinality'. How to compare? It remands a story.

See, there was one person in Africa, on a safari. He found one tribal, the tribal people had only 3 types of numbers. It was trying for him to accept. He found they have one, they have two, then they have many. If you ask somebody how many sheep he is having, he says it is `many'. It does not have a number for `how many', it is not 100, it is not 105 and so on, it has only `many'. The thing is, he is not missing one of his sheep. How? It is by comparison, it does not have a name for that number.

But, he knows how many. In a bag he just keeps a pebble for one sheep, when in the evening, they come, he allows one sheep and then puts out one pebble from his bag, and it continues. It is possible by comparison, even if you do not know the name of the number; that is the method we will use. One ship, one pebble; it defines a function a one-one function. If it is over, then an onto function.

(Refer Slide Time: 04:43)



That means, we say that if a set C is there if a set D is there, I have a function f from C to D which is one-to-one and also onto, then I will say that C has same number of elements

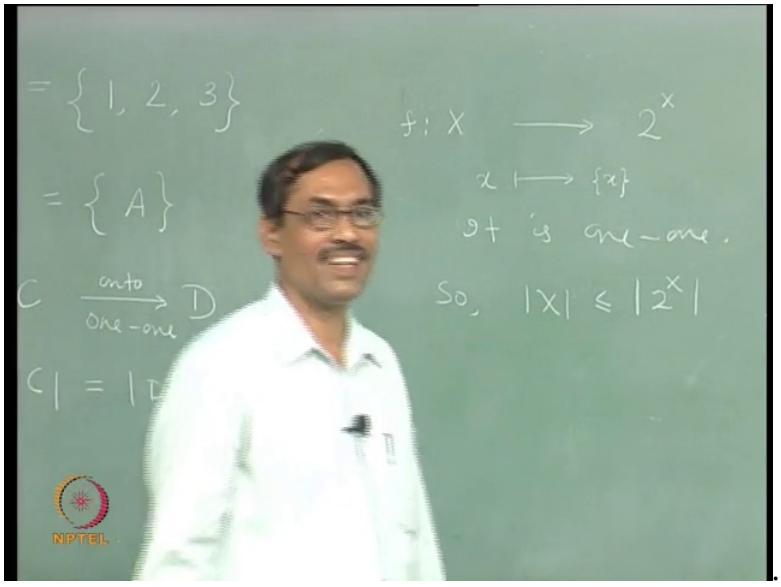
as D. Is that fine? Agreed? Now, you can think so many other things from this. If there is function g from C to D which is one-to-one, I do not have any information on its onto-ness, then what do I say? C has at least that many elements as D. Is that? If it is onto then, if there is a function h from C onto D, then C has no more elements than D. Yes? Is that fine?

You can have some by bifurcations there. But this is the standard way of comparing them in a way, by one-one onto functions; fine? Now, when do you say a set cannot have more elements than its power set? What do you need to show? We show that...

Student: Let us say one-to-one; we can say that it has one-to-one element.

We can say that, it is easy to show that, there is a one-to-one function because you have already done it by taking the? taking the single-ton sets.

(Refer Slide Time: 06:52)



You have a set X and you take its power set; we will write 2 to the power of X symbol. And you can always defined a function f from X to the 2 power of X by what? The x in X goes to the single-ton {x}. We can always define like this. Is it one-to-one? Yes, it is one-to-one, because, find two elements whose image is that single-ton. They will be the same; it is one-to-one. Therefore, always X will have at least, as many elements, as we cannot say, as many elements; at most that many elements as, in its power set.

Let us forget this at least, at most; it is confusing. We will say cardinality of X is less than or equal to cardinality of its power set.

Because of this one-to-one f, we say cardinality of X is less than or equal to cardinality of its power set. Clear? And the question is the other one: that is why I said it is easy to prove what you told.

But, it does not prove what you wanted to prove, even to show that X does not have that many elements as in the power set. Is that? It does not show that. It is still a possibility that there is one X whose number of elements is equal to the number of elements in its power set. All that you have, is less than or equal to; what is required to be proved?

Student: We know that power set contains the empty set, which is not an image of any element, it will always be greater than...

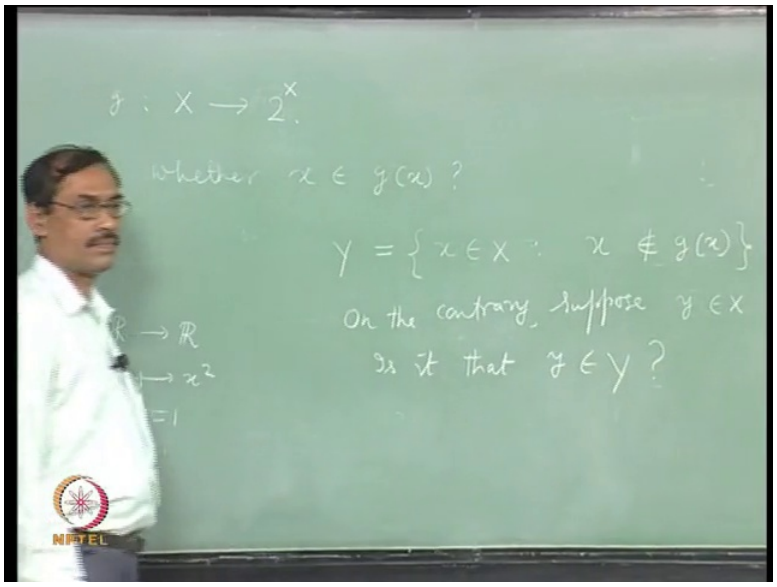
You want to say that this function what we have defined is not an onto function, agreed. This is not onto function. It is clear. Either you take the empty set in this, or you take a set having two elements. It is not an image of any element, provided there are at least two elements in it; if there are not, then you cannot do that. But that argument is fine. The empty set is there which is never an image. But, this does not prove that for any X, X has less elements than its power set; it only proves that this function which is one-to-one, is not onto. There can be another function which is one-to-one and onto. Is the issue clear? First, you must understand the issue, then try for the solution. Is the issue clear? We have tried to construct the function which is one-to-one, we find that it is not onto.

It may be giving us some push for our belief; yes, perhaps we are correct, but not yet. We can try some other one-to-one functions, constructing them, see whether they are onto or not. That is your experimental stage which mathematicians never reveal. Any one-to-one function there, you will see that it is never onto. Will that prove? Will that prove even you say there is no function which is onto? Will that prove? Let us try one of these, whichever where it goes will have to try to discover the proof, now, right, we have two options open.

Here, we kept a 1one-to-one function and prove that it can never be onto, or in general, you take any function so that it can never be on to, right? It is easy to construct one function which is not onto, but we are not interested in that. We are interested in the

other question: you give me any function I will show that it is not onto. This is the contention, is it clear? Now, how to proceed, that is the problem.

(Refer Slide Time: 12:13)



Let us take a function g from X to 2 to the power X. we want to show that it is not onto. That means, there are some elements in the power set which are not images of any elements in X wherever this g goes it does not matter. This sends elements of X to elements of the power set , which are subsets of X; is that clear? g sends elements of X to subsets of X which are in the power set. Now, you have to see that there is one element here which is not an image of any of these elements in X. Clear? This is what our aim is. Fine. That is easy to get if you have some X or its size before it.

But, I will give you one other way of looking at it. There is a temple in south India where you go and through a coin to reach the top of the temple. If you see that it never comes back, your wish is fulfilled. God has accepted, if it comes back, your wish is not fulfilled; that is the way people there believe. Now, as a student of IIT you want to disprove it; you want to show that it is not correct. So, what wish you have while throwing the coin?

Now, prove it, your wish, what? Continue. Oh, can do it? Anybody else? Just try to think of it. You do not have produce immediately. He says, what is your name? Shekhar, says that you wish the coin should come back right and then, now what will happen if wish is

fulfilled. But, the people believe that if it comes back which is not fulfilled that part is wrong, in the other case.

Student: If it stays then your wish is not fulfilled.

But, people say that, anyway you have proved. It has something to do with this proof. That is way I told you to look at the elements in X and look at its images. Here, we have one function g which is taking x to singleton x; this x is a member of its image. Will it always happen for any function you take? Will it happen that the element on the left side and its image on the right side will have this relation “x belongs to that image”? May be, may not be, right, because any arbitrary function we are taking, it is meaningful to ask this question whether x belongs to g of x; is that right?

See, g of x can be empty set also; in that case it does not belong; but other cases we can say. We need to know what this g is. Fine, we do not have any information, but you will use it. The question, the question now is, whether x belongs to g of x? Answer can be anything: x may belong to x may not belong to; it depends on g, it depends on this particular x. Now, let us look at one set. Let us say Y which is equal to the set of all elements of x which satisfy some property; the property is that x does not belong to g of x. It takes some time to understand because we are not giving any construction, taking that you are matured enough.

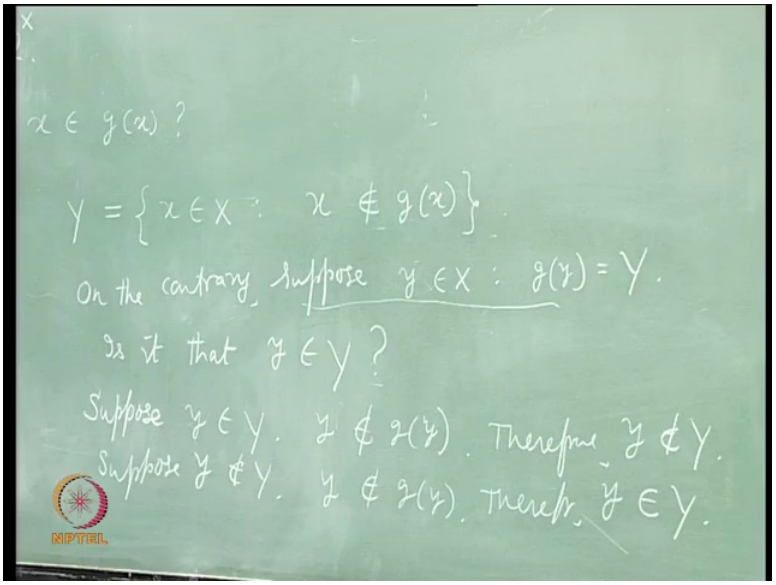
Let us look at it, it has relation to that story. We are peeking up all the elements (which contradicting that your law, some law one of the laws we have peeked up): find out the collection of all those elements. Now, we are going to prove that it is not possible that the belief is tenable, here the procedure is: show that this Y is never an image of any element in x, if it is, then there is some problem. Is it clear? Now, suppose on the contrary, suppose I have an element y which is in X such that g of y is equal to this set . Notice that I am not writing everything. There exists one y in X, in fact there exists some element whose name I am writing y, if I write there exists y, that y you cannot use, it can be something some other name as alpha, beta.

In that sense we are not writing every detail, here we are telling: there exists one element call it y, which has this property g of y is this set. Because you want to show that it is not possible to have any y of which this one is the image. On the contrary this will be assumption, now you have to see some contraries happening. It is not correct to assume

like this, this is the proof by contraries. Well, once this y exists which is in X such that g of y is equal to Y, we ask the same question, now what happens to this Y and that g of y?

Our question is that, have you gone on scout sometime? You would formed knots and then how to un-thread the knots and so on. It is naughty affair, now we are proceeding slowly, but they have already two knots not many. First, what we have done? We have asked a question which look meaningful. From there, we constructed a set: take all those which are not in their images, then you formed set, there is this set and you say a subset of X, it can be empty, you do not know. But, it does not matter whatever it is, it is subset of X. Then we are telling: suppose there is an element whose image is this set. Then that element is a member of this set or it is not. Too curios? Let us find out what happens again.

(Refer Slide Time: 20:47)



Suppose y belong to Y; then what happens? What happens is, y satisfies this property because that is the definition of Y, that means y does not belong to g of y. Is that? But, g of y is what? Y. Therefore, what happens, y does not belong to Y. Do you get a contradiction? Here contradiction to what? Which assumption - get the contradiction?

Student: Suppose y belongs to Y.

Suppose y belongs to Y. Then you get y does not belong to Y. It is not that this has been contradictory. Because there is the other case y may not belong to Y. This proves that y

does not belong to Y, do you see the proof? But anyway, we are not worried about what it says, that probably y does not belong to Y, there is another case; let us take it. Now, suppose y does not belong to Y (and what is y capital Y), g of y, this is y does not belong to g of y, Y is equal to g of y; just replace that. Hence, y does not belong to Y. Now this Y is equal to g of y, by replacing that, I just get y does not belong to Y, but now y does not belong to g of y is defining a property of Y. Therefore, y belongs to Y. Now, we have contradiction. Look at it we have a contradiction. Now it says if I assume y belongs to Y then y does not belong to Y, if I assume (small) y does not belong to Y, then (small) y belongs to Y. Both of them gives the contradiction that “y belongs to Y if and only if y does not belong to Y”. That is a contradiction; then and for that contradiction, responsibility goes here. Fine?

Therefore, g is not onto, any function you define from x to its power set, it will never be onto. This is your famous Cantor's theorem, which says that cardinality of any set is always less than the cardinality of its power set. This does not prove that. This, along with, such an x goes to singleton x proves it. Any function which is not onto might tell you that there is a possibility that the other set which is the co-domain may have more elements. But, it does not prove it, the proof only says that any function you take, that is never onto. Therefore, X always has less than or equal to elements than power set of X, but `it has less than' is proved by the one-to-one function.

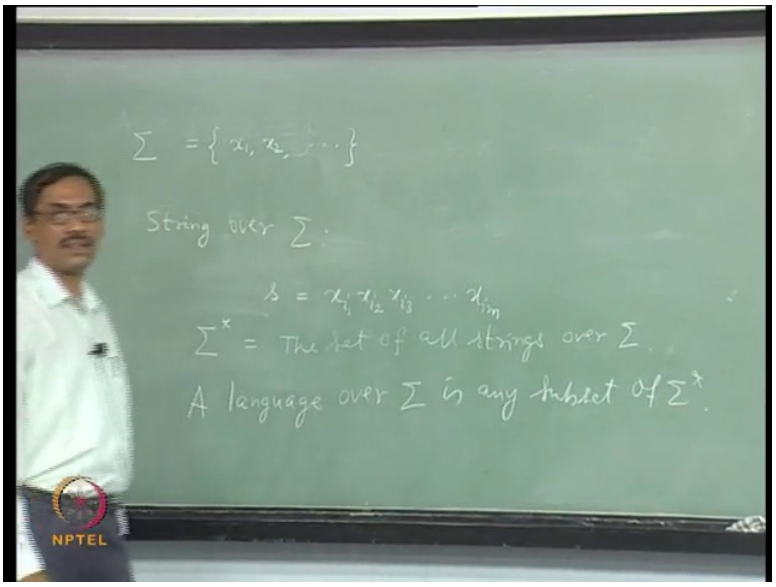
This will be helpful later when you come to comparing cardinalities, now because (the set of) natural numbers is countable, 2 to the power set of natural numbers is having more elements than the natural numbers. We have to give a name for it, it is uncountable when you count. Because of natural number, even if it is infinite we say it is still countable. Countable is not a name for having finite things it is finite. Countable can be finite or it can be infinite, but like natural numbers.

Countable is in one-to-one correspondence with natural numbers or it is in one-to-one correspondence with an initial fragment of natural numbers, which is finiteness; Is that clear? And, every other set is called uncountable. We are not going again do the details of that countability-unaccountability theory. In unaccountability itself, there can be many types of uncountability. Like power set of power set of natural numbers, it will have more elements than the power set of natural numbers, but all of them are termed as

uncountable. It is too big for us to handle, now if you like, then we can give them some names.

This is about something we need about the countability and uncountability. You will need something about formal languages. There again, a countable set; you might have already some exposure, but will just again brush up.

(Refer Slide Time: 27:23)



Suppose I take one set having some symbols in it and so on. So, x1, x2, and, so on; there are symbols, they are just elements, we are calling them symbols in this context. But when you say symbols, there is another connotation to it, that no symbol is a part of another symbol. This is funny, in Tamil character you might find this symbol is in, is a part of the other symbol, for example a straight line that might be a part, it can be symbol. It can be again part of symbol that is possible. Here, we are taking them away. We are telling that our symbols will have such characteristics: none is a part of anther symbol.

For example, you cannot get this (ab); and this has two different symbols. We will not call this as a symbol. This a is a symbol and again this is another symbol b. Then ab can be concatenation of two symbols one is this one (a), the other is this (b). But, it (ab) is not independently a symbol; that is your understanding. You are not formality defining what a symbol is, anyway. Now, let us take this alphabet of some symbols this is called an alphabet just like our usual languages. Then you define a string over this alphabet

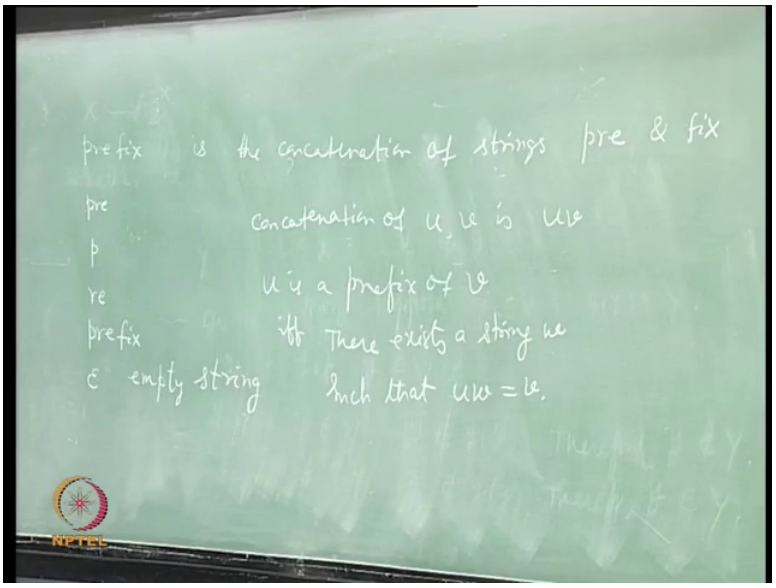
'Sigma', a string over Sigma is just a finite sequence of symbols from Sigma. We will be writing it as something like s equal to xi1, xi2, xi3, . . . ,xim, there are m symbols, here, which (symbols) are not fixed not x1, x2, . . . , xm; any symbol they can be this xij; they can be from anywhere in Sigma.

But, it looks like this `any string from Sigma' is a finite sequence of symbol. Then by Sigma star we will write `the set of all strings over Sigma'. Then, when we say `a language over Sigma' it is just a subset of Sigma star. We say the language over Sigma is any subset of Sigma star. Which means, the language over sigma is some set of strings over Sigma. They are finite strings not infinite. We are using string, in that sense, always keeping ourselves to finite sequence of symbols.

These are the basic things of formal languages. You want to describe a formal language with some number of symbols; then find some strings, take a set of strings. This depends on that set of symbols, that set of symbols is called an alphabet, so it is wrong to tell A is an alphabet, B is an alphabet, C is an alphabet, or in the Roman alphabet A, B, C are alphabets. It is wrong to tell like that the alphabet is the Roman alphabet which is the set containing A to Z, a to z, 0 to 9, all those things; that, is it right?

That is the way it is being used, here Sigma is called an alphabet, all others are symbols from the alphabet or alphabet letters. Then you take the strings, take a subset of strings; that is a language over sigma. We might use this language over some definite symbols. Take some symbols, define a language then give some conventions over that language. This is what we will be doing later. For that we may need one or two more concepts like the concept of prefix. See, they are just some technical words which we will be using later, that we are explaining.

(Refer Slide Time: 32:44)



For example take the word prefix, here, pre is a prefix of prefix, p is a prefix of prefix, ri is not a prefix of prefix; fine. Also, prefix is a prefix of prefix. If there is nothing I write, here that is also prefix of prefix. But, it is difficult to leave it like that. Is it not that if I write nothing and say that as a prefix of prefix, it will not make sense? We will not be able to talk about it, that is, the problem probably makes sense: we will not be able to talk about it. Let us give a name to it, say, the empty string, which will write as epsilon. There are no symbols (in it), so the empty string is also prefix of any string, now what is a prefix? Yes, can someone define?

Student: A consecutive set of symbols from the beginning of a string is a prefix starting from the beginning of the string.

Well, we define it a better way. We will define only one idea which is called concatenation of strings, prefix is a concatenation of two strings pre and fix this is the concatenation we are using, the concatenation which we simply use.

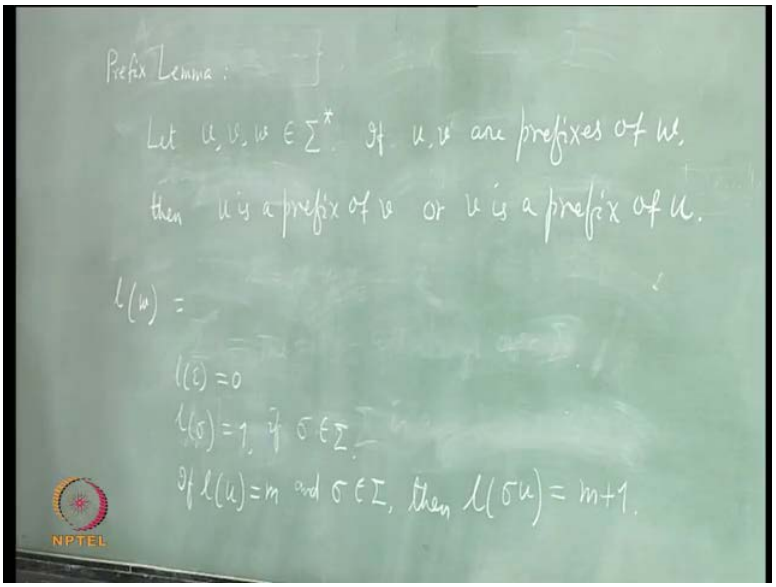
It means if u is a string of symbols say x1 x2 x3 . . . xm and then v is a string symbols y1 y2 y3 . . . yn, then x, sorry u concatenated with v gives a string which looks like x1 x2 . . . xm y1 y2 . . . yn. Is that clear? That is the idea of concatenation. Now, using the word concatenation can you define prefix?

Student: Strings, A is a prefix of B if it is possible to get B by concatenating string.

Is that clear? u is a prefix of v if there exist a string w such that uw is equal to v, we are saying uw means concatenation of u and w; is that so? Just following these we will write concatenation without putting on any symbol in between the strings. That means, we will write concatenation of u, v as uv. We will write like this. Then what we say is u is a prefix of v if and only if there exists a string w such that v equals uw. Prefix is defined, now let us take two strings we do not know whether one is a prefix of the other or not.

Let us think of two strings arbitrary, take a prefix of first one prefix of a second one, connection they may have, but not necessary; nothing can be there. One is epsilon another is u then there is something. But, if I take x1 x2 another is y1 y2 no connection. Right? But if I take same string and two prefixes of it, then? Yes, you are correct. Is it clear what I am telling? Right. Take prefixes u and v of the same string. Now, you may say there is a connection between u and v, what connection? It is: either u is a prefix of v, or v is a prefix of u, or u is equal to v; right? Only the prefix of the other; just so, we write it first.

(Refer Slide Time: 38:43)



Here implicitly using an alphabet, the alphabet is Sigma, write it. Now, especially, well, you know the result. You want to show the result. Can you suggest which proof method really does that; in mathematics there are so many ways of proving. One method: you use always for a known result; if you know the result then you can use that proof if you do not know it, you cannot proceed on the beginning. Induction, mathematical induction.

Once you know what is there to be proved, you can prove; before that nothing can be done, you cannot use anything.

Now, suppose we use induction, what will happen? Induction on what? there is a first question, induction on what? Let us have induction on the right string. But, w is not a number how do you have induction on it, how big it is, induction on that. That is called the length of string. What is the length? Now, length of a w is number of input, the number of occurrence of symbols, that is important, very important; because your alphabet can have only one symbol 0 still you can have a length of string 10 all of them are zeros.

Length is the number of occurrence of symbols in w. But again we have to define this occurrences; repetitions? We are too fussy, so what we do, we use concatenation. Since you know what concatenation is, we will use it. How do you use it? Again, define it by induction because concatenation slowly increases the lengths of the strings; you can visualize that; where, you can use it to define what is the length of a string? Fine.

Length of empty string is 0, length of any symbol is 1; then go to the next stage, find out one symbol either as a prefix or as suffix and then define the length; what we are doing? We will say length of the empty string is 0, length of a symbol is 1, now if length of u is equal to m and take a symbol sigma from Sigma, then length of `sigma u' or you could have written `u sigma', either way, you define, is equal to m plus 1. Is it? This is a definition, by induction. You can use induction as a proof method or as a definition method also, fine? This implicitly defines length, it has to be a natural number.

Now onwards, natural numbers will include 0, otherwise we will always have to say non-negative integers; that is very awkward to speak always, we are natural people, we will take 0 as a natural number; fine? Agreed. Length is a function from the set Sigma star to natural numbers; just define this one; is it clear? Now then, you can use length for a prefix, now length of w.