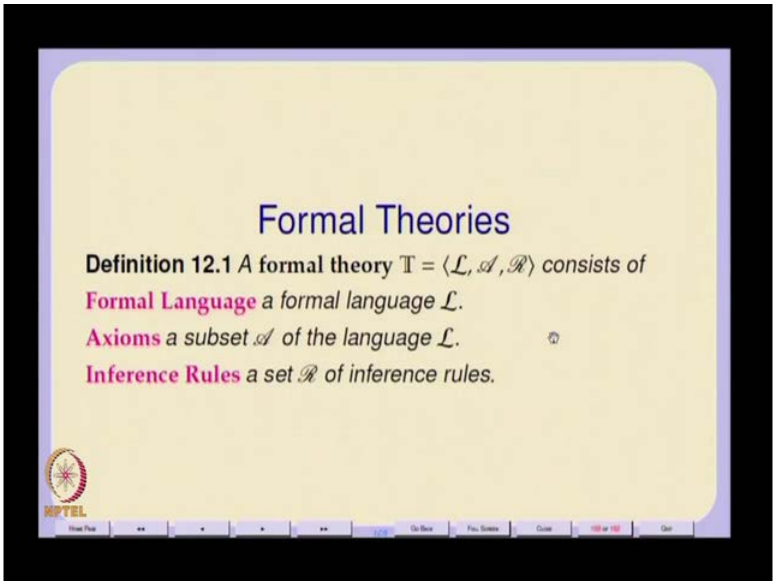
Logic for CS
Prof. Dr. S. Arun Kumar
Department of Computer Science
Indian Institute of Technology, Delhi

Lecture - 13
Proof, Theory: Hilbert-Style

So, will do Hilbert style will do a Hilbert style proof system in some more detail. There is an important theorem that we have to prove before we can do that. But, we will also look at other thing about Formal Theories.

(Refer Slide Time: 00:47)



Formal Theories

Definition 12.1 *A* **formal theory** $\mathbb{T} = \langle \mathcal{L}, \mathscr{A}, \mathscr{R} \rangle$ *consists of*

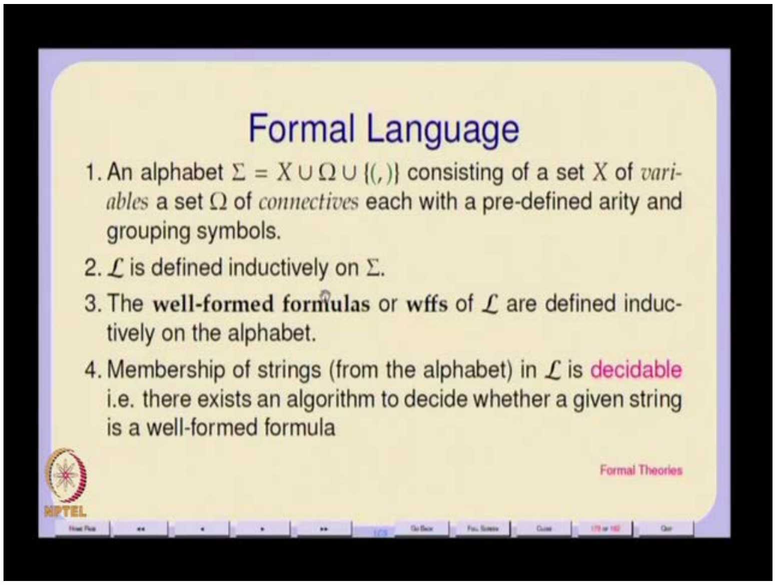
Formal Language *a formal language* $\mathcal{L}$.

Axioms *a subset* $\mathscr{A}$ *of the language* $\mathcal{L}$.

Inference Rules *a set* $\mathscr{R}$ *of inference rules.*

So, let us fist go to that so a formal theory basically consists of some language it is a Formal Language. And, a collection of axioms which are subsets of that language which is a subset of the language. Or of course in if you have an infinite subset of axioms for the theory then, you might want to think of them as axiom schemas which so that, they are finitely expressible and a set of inference rules.

(Refer Slide Time: 01:18)



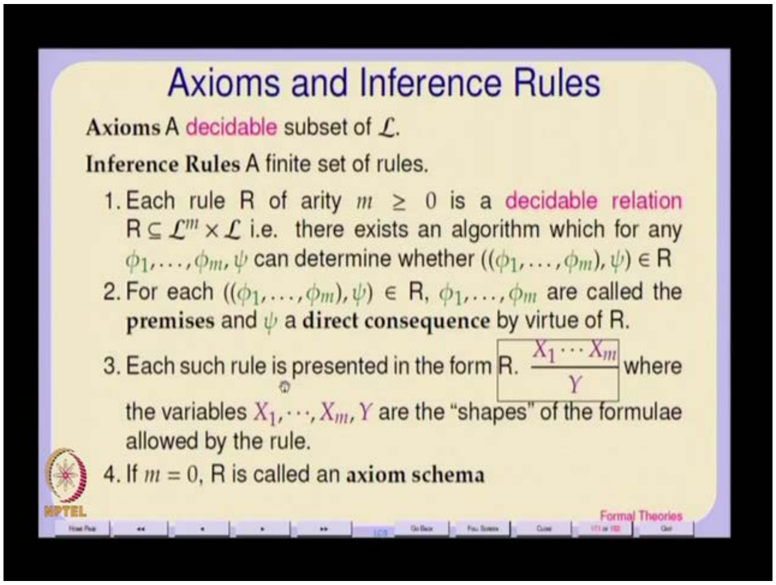
Formal Language

1. An alphabet $\Sigma = X \cup \Omega \cup \{(,)\}$ consisting of a set X of *variables* a set Ω of *connectives* each with a pre-defined arity and grouping symbols.
2. $\mathcal{L}$ is defined inductively on Σ.
3. The **well-formed formulas** or **wffs** of $\mathcal{L}$ are defined inductively on the alphabet.
4. Membership of strings (from the alphabet) in $\mathcal{L}$ is decidable i.e. there exists an algorithm to decide whether a given string is a well-formed formula

Formal Theories

So, that is so this is what so usually as I said this formal language is inductively defined. And, therefore membership in the language for any string is decidable. And, similarly the axioms should all be a decidable subset they could be infinite but it should be a decidable subset.

(Refer Slide Time: 01:33)



Axioms and Inference Rules

Axioms A decidable subset of $\mathcal{L}$.

Inference Rules A finite set of rules.

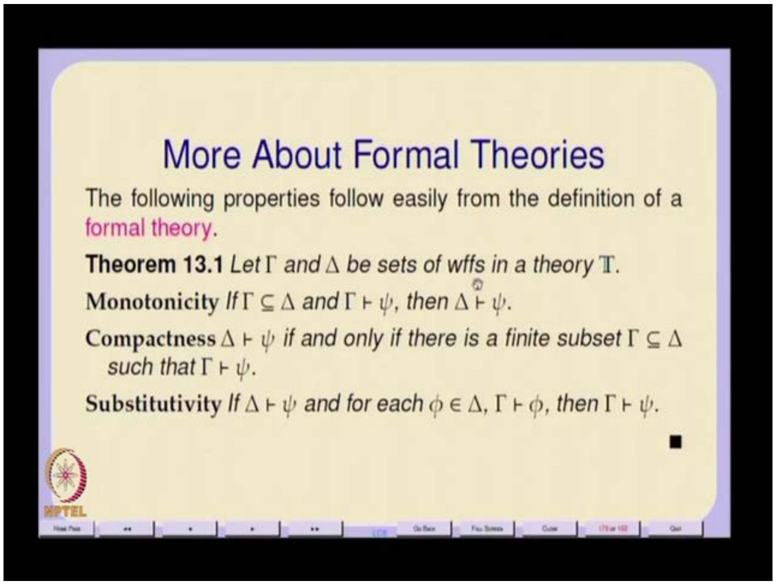
1. Each rule R of arity $m \geq 0$ is a decidable relation $R \subseteq \mathcal{L}^m \times \mathcal{L}$ i.e. there exists an algorithm which for any $\phi_1, \ldots, \phi_m, \psi$ can determine whether $((\phi_1, \ldots, \phi_m), \psi) \in R$
2. For each $((\phi_1, \ldots, \phi_m), \psi) \in R$, $\phi_1, \ldots, \phi_m$ are called the **premises** and ψ a **direct consequence** by virtue of R.
3. Each such rule is presented in the form $\boxed{R. \ \frac{X_1 \cdots X_m}{Y}}$ where the variables $X_1, \cdots, X_m, Y$ are the "shapes" of the formulae allowed by the rule.
4. If $m = 0$, R is called an **axiom schema**

Formal Theories

And, then a Inference rules are essentially written in this form essentially we look at. So, inference can often be represent infinite relations in which this one thing one statement is direct consequence of some one or more other statements. And, since it has to be a decidable relation even if it is infinite what we expect is that there will be some pattern matching in substitution way of expressing this infinite rule this infinitary relation.

So, you can think of these X so in a rule of the form X1 to Xm is Y. You can think of these X1to Xm and Y as shapes or skeletal shapes of the formulae. Which, have to follow certain structure and the structure is defined by the syntax of a language. So, there are some basic theorems which which might be called meta theorems about theories in general. One is and of course remember that formal theories of pure syntax. So, the question of how useful or applicable or consistent this theories are really depends on connecting up connecting them up with semantics. But that, will worry about that later. So, now we will just look at what is known as proof theory.

(Refer Slide Time: 03:19)



More About Formal Theories

The following properties follow easily from the definition of a formal theory.

Theorem 13.1 *Let Γ and Δ be sets of wffs in a theory $\mathbb{T}$.*

Monotonicity *If $\Gamma \subseteq \Delta$ and $\Gamma \vdash \psi$, then $\Delta \vdash \psi$.*

Compactness *$\Delta \vdash \psi$ if and only if there is a finite subset $\Gamma \subseteq \Delta$ such that $\Gamma \vdash \psi$.*

Substitutivity *If $\Delta \vdash \psi$ and for each $\phi \in \Delta$, $\Gamma \vdash \phi$, then $\Gamma \vdash \psi$.*

■

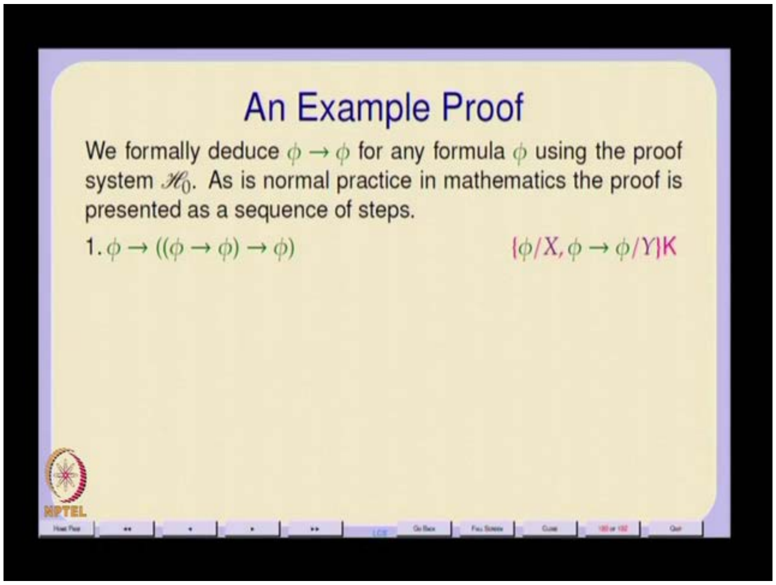
So, in general now Formal Theory we expect that theory is monotonic on the assumptions on the set of assumptions. So, if gamma is a subset of delta is a set of assumptions then, if whatever gamma can prove is also provable from delta. Because I need to use only whatever assumptions there in gamma and they are all there in delta. So, this compactness so this is an so this is not really a compactness theorem. But, because of its connection with the compactness theorem that we have already proved I am calling it compactness. But, the main point about this property is that when we talk about of proof or provability we are talking about provability in a finitary sets.

So, you cannot I mean there are only the proof of any statement psi from a possibly infinite set of assumptions delta. If there exist a proof it has to exist from a finite set of subset of that set of assumptions.

So, even if delta is infinite when we talk about our proof we say that it should be there should be a finite subset of assumptions from, which the proof is obtained. And, then substitutivity of course is just that this is a standard method of splitting of a theory into lemma's and theorems. So, if I have a set of assumptions delta from which I can prove some statement psi. And, each of those assumptions can be prove from a different set of assumptions gamma. Then, from gamma i can prove psi that is. So, psi is provable from gamma essentially because each of the assumptions in gamma is also provable from this each of the assumptions in delta is also provable. And, therefore I can split up my proofs into several such theorems or lemma's and so on so forth which is how formal theories and normally organized. Which is how normal mathematical theories are also organized we have lemma's theorems corollaries. They are all the same things it is just that in terms of provability they all mean the same thing on the name lemma or theorem or corollary just refers to certain value judgments firstly about the importance of the results. So, kenoics lemma probably kenoic did not think it was too important so he called it a lemma. But, the rest of the worlds seems to think it is very important. And, Tukey's lemma similarly seems to be important enough to be called a theorem. But, a corollary is of course something that directly follow from theorems but there also there also theorems in that sense.

So, there is only one ocean of a formal theorem though there are many different notions based on value judgments of whether something is a lemma or a fact. So I have a hierarchy fact which means it is completely trivially trivial to prove. A, lemma is something that is usually used to prove a theorem. And, a corollary is something that directly follows from a theorem. So, that is those are the kinds of value judgments we make while organizing a theory. But, in a in a formal sense all of them are the same notions. And, they actually allow us to organize formal theories and structure them in a certain way.

(Refer Slide Time: 07:24)



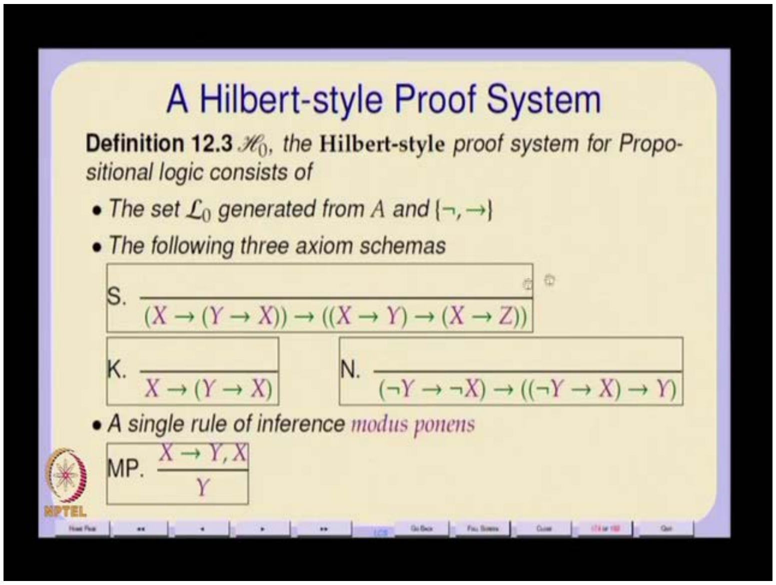
An Example Proof

We formally deduce $\phi \rightarrow \phi$ for any formula ϕ using the proof system $\mathscr{H}_0$. As is normal practice in mathematics the proof is presented as a sequence of steps.

1. $\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)$ $\{\phi/X, \phi \rightarrow \phi/Y\}$K

So, will do An Example Proof we also looked at we also looked at this Hilbert style proof system where we have this axiom schemas S K and N. And, this rule of inference called modus ponens.

(Refer Slide Time: 07:30)



A Hilbert-style Proof System

Definition 12.3 *$\mathscr{H}_0$, the* **Hilbert-style** *proof system for Propositional logic consists of*

- *The set $\mathcal{L}_0$ generated from A and $\{\neg, \rightarrow\}$*
- *The following three axiom schemas*

S. $\dfrac{}{(X \rightarrow (Y \rightarrow X)) \rightarrow ((X \rightarrow Y) \rightarrow (X \rightarrow Z))}$

K. $\dfrac{}{X \rightarrow (Y \rightarrow X)}$

N. $\dfrac{}{(\neg Y \rightarrow \neg X) \rightarrow ((\neg Y \rightarrow X) \rightarrow Y)}$

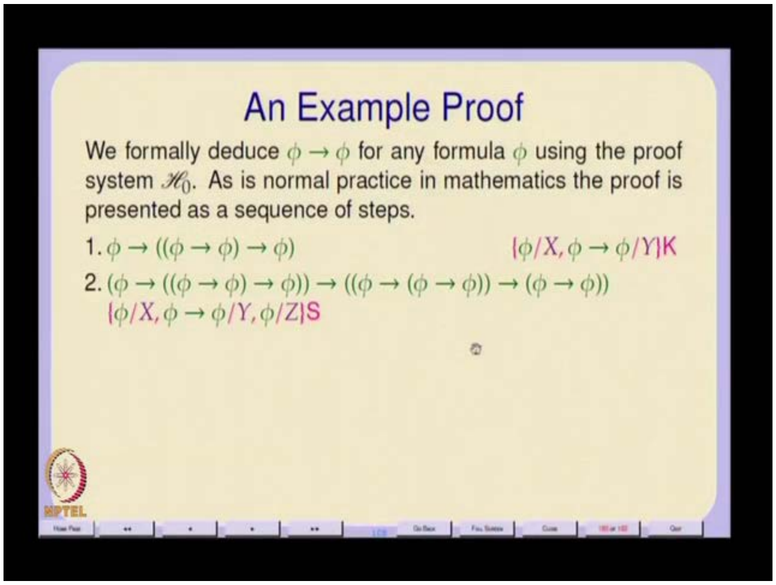
- *A single rule of inference modus ponens*

MP. $\dfrac{X \rightarrow Y, X}{Y}$

So, here is a simple theorem this is essentially the reflexivity if the conditional. So, you want to prove phi arrow phi from an empty set of assumptions. So, here this gamma is an empty set and you have to going to prove phi arrow phi. So, phi arrow phi then is a theorem if you can find a proof with. Then normal way we write proofs in mathematics and we should be writing it that way is that every step is somehow justified. So, well so you will find that this, Hilbert style proof systems initially are not very easy to understand. So, here this justification is another of those secular things that I use. Which, are not mostly used in most logic books I directly use the notion of substitutions that we are all familiar with in pattern matching and programming and so on and so forth.

And, I use substitutions to as just justification so that it is easy to specify how we got this step up otherwise how did we this steps. So, this step essentially comes from the axiom schema K and you are essentially looking for patterns to substitute for these variables X and Y. So, this so this step essentially says in the axiom schema K if I replace X by phi and replace Y by phi arrow phi then, I get this step. So, you can think of these axiom schemas and rules of inference as essentially like, Christmas tree templates. You know you take Christmas trees they have a lot of hooks on them. And, which the gifts are usually hung but we can go for the we can hang other Christmas trees on them for example. So, our formulae's our formulas of that kind we can we can hang. So, these patterns provide that structural templates on which larger trees can be built up from smaller trees by hanging those trees on the hooks.

(Refer Slide Time: 10:26)



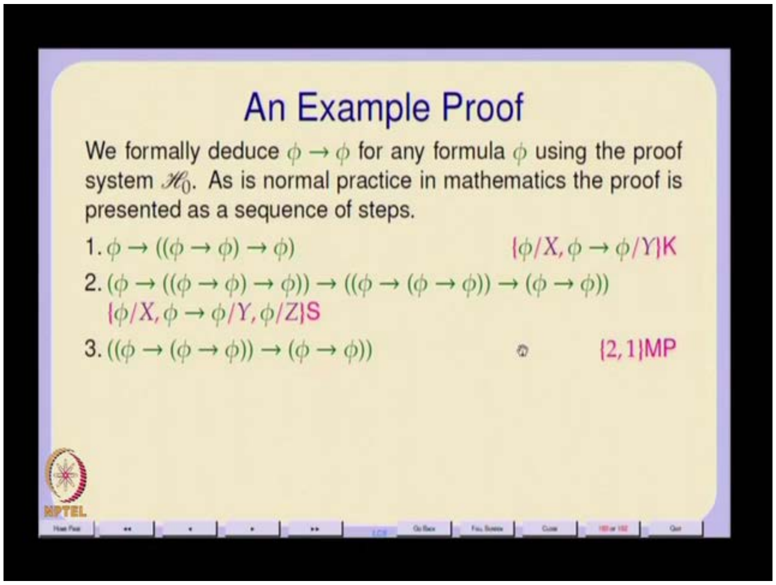
An Example Proof

We formally deduce $\phi \to \phi$ for any formula ϕ using the proof system $\mathscr{H}_0$. As is normal practice in mathematics the proof is presented as a sequence of steps.

1. $\phi \to ((\phi \to \phi) \to \phi)$ $\{\phi/X, \phi \to \phi/Y\}$K
2. $(\phi \to ((\phi \to \phi) \to \phi)) \to ((\phi \to (\phi \to \phi)) \to (\phi \to \phi))$
   $\{\phi/X, \phi \to \phi/Y, \phi/Z\}$S

So, the next step I mean so this kind of proof is going to be completely non-obvious and its going to leave you quite bit huddled but, will go through with it and will get used to it. The, next step is this horribly complicated step which is actually justified by the axiom schema S. So, if you lo at the axiom schema S besides its normal connection with the S combinatory in lambda calculus combinatory logic it also expresses. Basically, the fact that the conditional distributes over other conditionals. So, this X arrow Y arrow X is essentially implies X arrow Y arrow X arrow Z. So, the conditional distributes over the conditional it is a very interesting and a powerful way of looking at the conditional. And, this step is formed by replacing by replacing phi for X phi arrow phi for a Y and phi for Z. So, you get this phi arrow phi arrow.

(Refer Slide Time: 12:12)



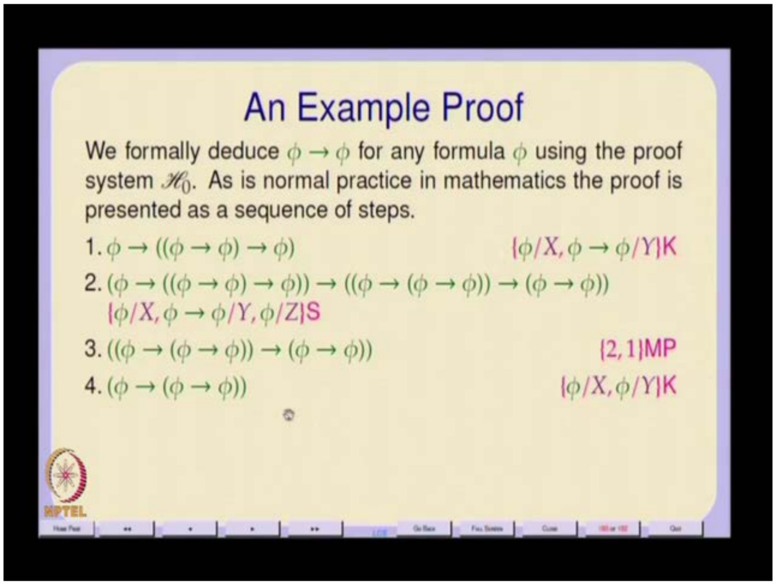
An Example Proof

We formally deduce $\phi \to \phi$ for any formula ϕ using the proof system $\mathscr{H}_0$. As is normal practice in mathematics the proof is presented as a sequence of steps.

1. $\phi \to ((\phi \to \phi) \to \phi)$ $\{\phi/X, \phi \to \phi/Y\}$K
2. $(\phi \to ((\phi \to \phi) \to \phi)) \to ((\phi \to (\phi \to \phi)) \to (\phi \to \phi))$ $\{\phi/X, \phi \to \phi/Y, \phi/Z\}$S
3. $((\phi \to (\phi \to \phi)) \to (\phi \to \phi))$ $\{2, 1\}$MP

So, and then of course then what I can do is I can notice that this one step 1 and step 2 are essentially too instances of the hypothesis for the modus ponens rule. So, which means I can apply the modus ponens rule. So, the modus so here I have taken a short cut. So, basically you if you have a if you have two formulae having this skeletal structure this pattern X arrow Y and X then, I can essentially infer Y. So, this is what the modus ponens rule does and from this formula is essentially of the form X arrow Y. Where, from here to here is X and from here to here is Y. And, this pattern as an abstract syntax-tree is exactly the same as this pattern. And, therefore the modus ponens rule can be applied and you will get this pattern as a result and that is what we had given.

(Refer Slide Time: 13:23)



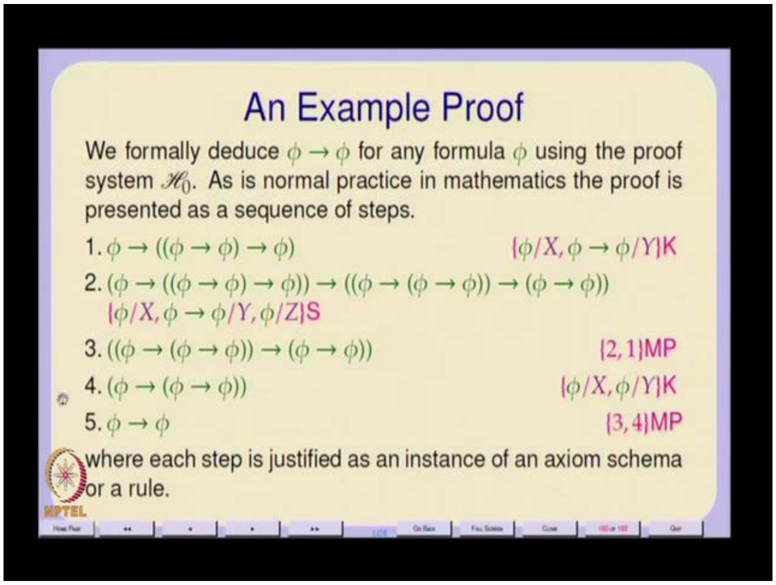
An Example Proof

We formally deduce $\phi \rightarrow \phi$ for any formula ϕ using the proof system $\mathscr{H}_0$. As is normal practice in mathematics the proof is presented as a sequence of steps.

1. $\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)$ $\{\phi/X, \phi \rightarrow \phi/Y\}$K
2. $(\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$ $\{\phi/X, \phi \rightarrow \phi/Y, \phi/Z\}$S
3. $((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$ $\{2, 1\}$MP
4. $(\phi \rightarrow (\phi \rightarrow \phi))$ $\{\phi/X, \phi/Y\}$K

Of course then, but then from the K rule by replacing phi for X and phi for Y I, do get this phi arrow phi arrow phi.

(Refer Slide Time: 13:36)



An Example Proof

We formally deduce $\phi \rightarrow \phi$ for any formula ϕ using the proof system $\mathscr{H}_0$. As is normal practice in mathematics the proof is presented as a sequence of steps.

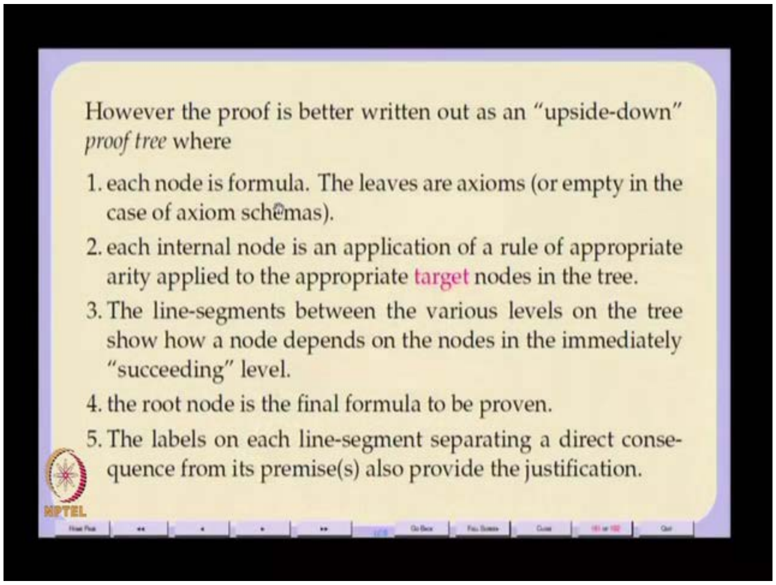
1. $\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)$ $\{\phi/X, \phi \rightarrow \phi/Y\}$K
2. $(\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$ $\{\phi/X, \phi \rightarrow \phi/Y, \phi/Z\}$S
3. $((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$ $\{2, 1\}$MP
4. $(\phi \rightarrow (\phi \rightarrow \phi))$ $\{\phi/X, \phi/Y\}$K
5. $\phi \rightarrow \phi$ $\{3, 4\}$MP

where each step is justified as an instance of an axiom schema or a rule.

And, I can apply modus ponens on these two steps 3 and 4 to obtain phi arrow phi. So, essentially I have proved the reflexive so the reflexivity of the conditional has been proven by with no assumptions by resorting to the axioms schemas and the rules of interest. And, this is how normally you can think of mathematics as being presented if it is presented formally. In fact when I was in school and we were taught Euclidian geometry we had to actually write it in this fashion you know. We, have to write each step and give a justification for each step sometimes a justification would just been there as an assumption other ways sometimes the justification would be that where. So, that it is some previous theorem or some previous definition or some such thing. But, they had to be a number of steps each numbered and each of them have to be justified and that is. So, we did not write in free flowing English we actually wrote in a two column format always all the proofs in geometry.

So that trends seems, to gone off now but that provides an important structure to the fact that each step does have a logical justification. But, of course as computer scientist this is lousy, actually the proof is not such a sequence. A, proof is actually a tree in facts it is what I would call an upside down tree. So, what we are going to do say is. So, essentially this proof what we refer to as a proof tree there is a certain dependency you apply a rule of inference on some previously obtained statements by doing a pattern matching. So, now this dependence can be expressed as essentially a directed edge. And, if your proof was indeed non-circular what you would get is a directed a cyclic graph or a tree. If, it say directed a cyclic the only difference between directed a cyclic graph and a directed tree is that some nodes in a directed a cyclic graph can have in degree more than 1. But, then what you do is if you replicate these nodes so that their in degree is 1 then you can actually get a tree. So, that is by replication you will actually by appropriately replicating this, such nodes. So, you will get you will get a tree so what we what we will look at are we will look at proofs as trees.

(Refer Slide Time: 16:53)

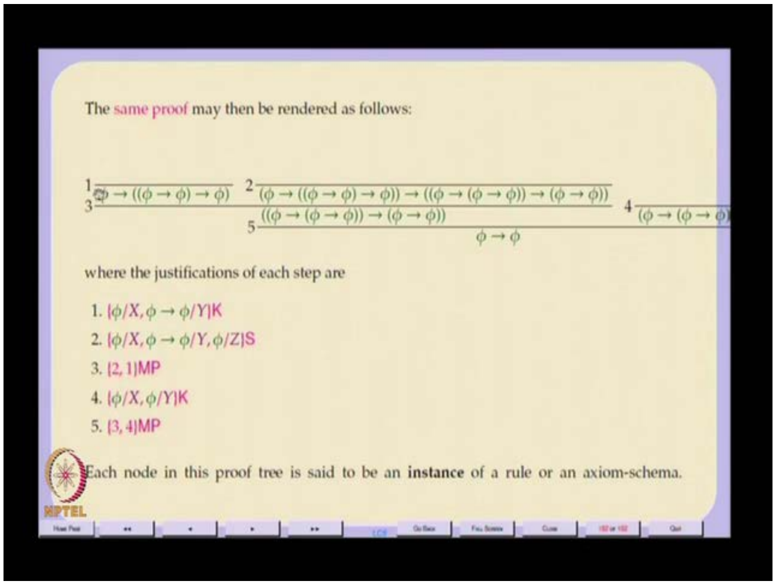


However the proof is better written out as an "upside-down" *proof tree* where

1. each node is formula. The leaves are axioms (or empty in the case of axiom schemas).
2. each internal node is an application of a rule of appropriate arity applied to the appropriate target nodes in the tree.
3. The line-segments between the various levels on the tree show how a node depends on the nodes in the immediately "succeeding" level.
4. the root node is the final formula to be proven.
5. The labels on each line-segment separating a direct consequence from its premise(s) also provide the justification.

So, essentially so each node is a formula in this proof tree and the leaves are either axioms or in case there were there was a non-empty set of assumptions. There could be one of the there could be drawn from the assumptions or there could be for example instances of axiom schemas. Each internal node is an application of a rule of inference on some target nodes by pattern matching and substitution. And, the final the root node of this proof tree is the formula that must be proved. And, of course standard things for book keeping and so on and so forth is that you have to provide justification sometimes as you can see even in a short proof like this justifications can be pretty complicated. If, there were if these justifications were not there you would be quite possible to see all these phi's hanging around in strange ways bracketed in strange ways. And, you would know how they were obtained so, you need justification. So, that will be provided by these so that is also something that be provided by a label let us say. So, a our typical proof will look like this.

(Refer Slide Time: 18:17)



The same proof may then be rendered as follows:

$$ {}^{5}\dfrac{{}^{3}\dfrac{{}^{1}\dfrac{}{\phi \to ((\phi \to \phi) \to \phi)} \quad {}^{2}\dfrac{}{(\phi \to ((\phi \to \phi) \to \phi)) \to ((\phi \to (\phi \to \phi)) \to (\phi \to \phi))}}{((\phi \to (\phi \to \phi)) \to (\phi \to \phi))} \quad {}^{4}\dfrac{}{(\phi \to (\phi \to \phi}}{\phi \to \phi} $$

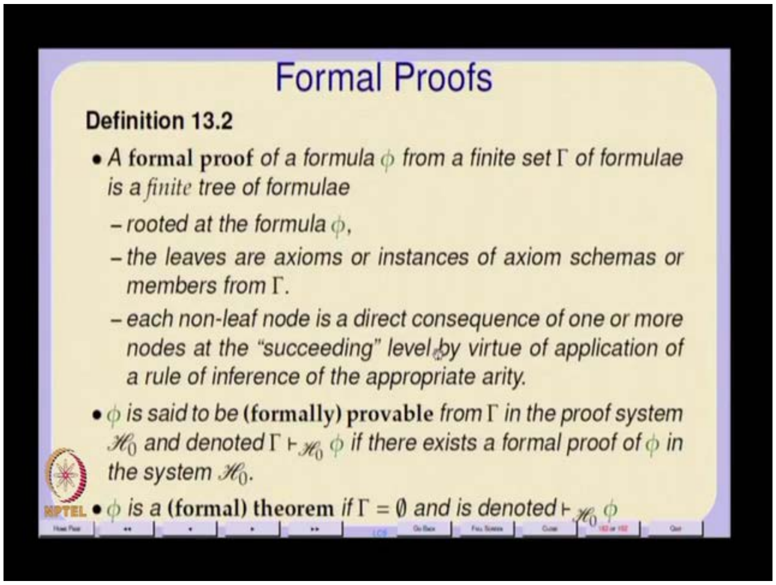
where the justifications of each step are

1. $[\phi/X, \phi \to \phi/Y]$K
2. $[\phi/X, \phi \to \phi/Y, \phi/Z]$S
3. [2, 1]MP
4. $[\phi/X, \phi/Y]$K
5. [3, 4]MP

Each node in this proof tree is said to be an **instance** of a rule or an axiom-schema.

So, the same proof so these are the steps 1and 2 and this step 3 which yields this formula is essentially is a is the line segment extends right up to all the hypothesis of the rule that are that are applicable. And, this below the line segment I get the conclusion this is a separate leave node. Which, was actually obtained as an instance of the axiom schema K. And, this line segment 5 which derives phi arrow phi. Essentially, spans these two steps from which the modus ponens rule was used. So, we will look at proofs essentially in this fashion.

(Refer Slide Time: 19:27)



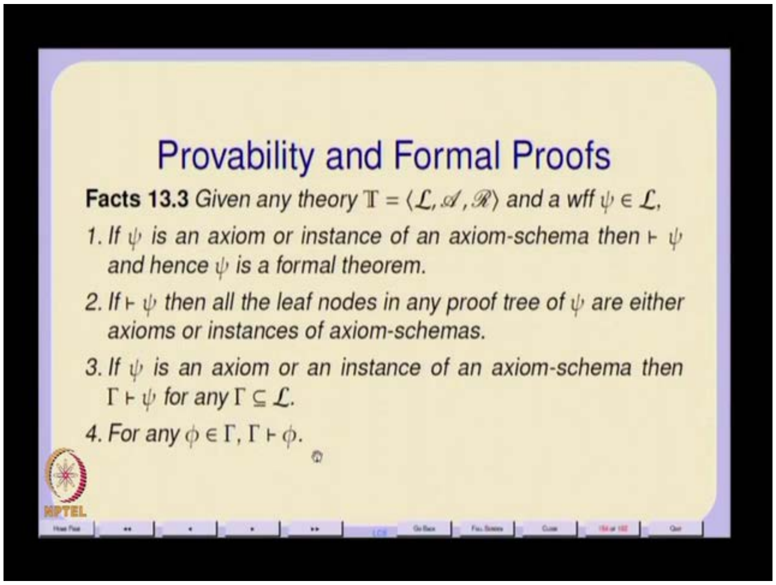
Formal Proofs

Definition 13.2

- *A* **formal proof** *of a formula* ϕ *from a finite set* Γ *of formulae is a finite tree of formulae*
  - *rooted at the formula* ϕ*,*
  - *the leaves are axioms or instances of axiom schemas or members from* Γ*.*
  - *each non-leaf node is a direct consequence of one or more nodes at the "succeeding" level by virtue of application of a rule of inference of the appropriate arity.*
- ϕ *is said to be* **(formally) provable** *from* Γ *in the proof system* $\mathscr{H}_0$ *and denoted* $\Gamma \vdash_{\mathscr{H}_0} \phi$ *if there exists a formal proof of* ϕ *in the system* $\mathscr{H}_0$*.*
- ϕ *is a* **(formal) theorem** *if* $\Gamma = \emptyset$ *and is denoted* $\vdash_{\mathscr{H}_0} \phi$

So, a Formal Proof as far as we are concerned of a formula phi is a tree is a proof tree rooted at the formula phi. Such that the leaves are axioms or instances of axioms each non-leaf node is a direct consequence one or more nodes at the well the succeeding level. I mean the way we defined trees was that the leaf nodes have a level greater than the root node right. So, in this case we are turning the tree upside down but still retaining the same notion of dependence. And, the directed edge essentially talks about is the dependence of the conclusion from the hypothesis. And, we would say that our formula phi is formally provable from gamma in the proof system this if, there exists of formal proof of phi in the system H naught. If, gamma is empty then we say that phi is a formal theorem of the system. So, this H naught is since we will be studying several different proof systems. This H naught is for the Hilbert style proof system whose axioms we are K S N and mp.

(Refer Slide Time: 20:57)



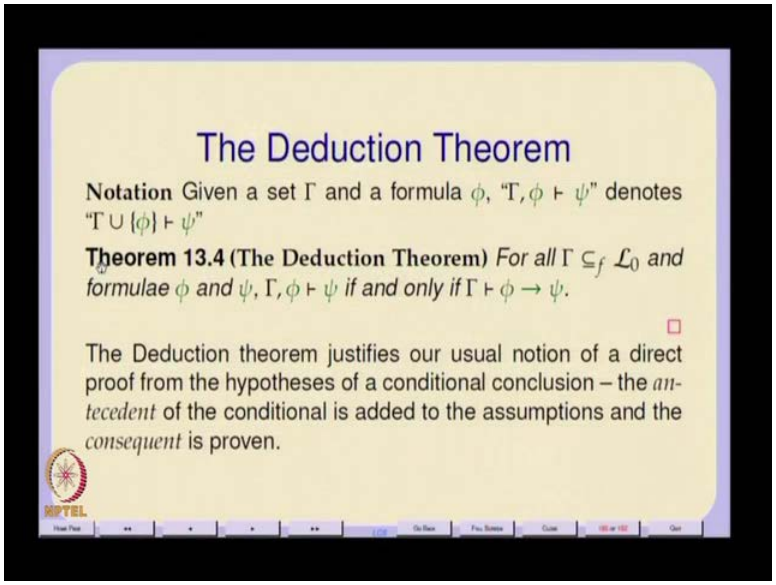
Provability and Formal Proofs

Facts 13.3 *Given any theory* $\mathbb{T} = \langle \mathcal{L}, \mathscr{A}, \mathscr{R} \rangle$ *and a wff* $\psi \in \mathcal{L}$,

1. *If* ψ *is an axiom or instance of an axiom-schema then* $\vdash \psi$ *and hence* ψ *is a formal theorem.*
2. *If* $\vdash \psi$ *then all the leaf nodes in any proof tree of* ψ *are either axioms or instances of axiom-schemas.*
3. *If* ψ *is an axiom or an instance of an axiom-schema then* $\Gamma \vdash \psi$ *for any* $\Gamma \subseteq \mathcal{L}$.
4. *For any* $\phi \in \Gamma$, $\Gamma \vdash \phi$.

And, we will study other proof systems also. Now, we come to an important so will come to an important thing about. So, the notion of Provability Formal provability is just that I mean if, phi is an axiom or instance of an axiom schema. Then, if then phi is formal theorem if, phi is provable or is psi is provable. Then, all leaf nodes in any proof tree of psi or either axioms or instances of axioms schemas with they could not applications of rules unless there were some succeeding nodes preceding it. And, if psi and axiom or an instance of an axiom schema. Then, it does not matter what assumptions you make psi is still provable from that assumptions except that you are not going to use any of those assumptions probably. And, if I have an assumption if I have a non-empty set gamma and I have an assumption phi inside gamma I will claim that phi is formally provable from gamma. I mean those is this is just sort of from the assumptions gamma I can prove I mean this is sort of trivial statement.

(Refer Slide Time: 22:20)



The Deduction Theorem

Notation Given a set Γ and a formula ϕ, "$\Gamma, \phi \vdash \psi$" denotes "$\Gamma \cup \{\phi\} \vdash \psi$"

Theorem 13.4 (The Deduction Theorem) *For all $\Gamma \subseteq_f \mathcal{L}_0$ and formulae ϕ and ψ, $\Gamma, \phi \vdash \psi$ if and only if $\Gamma \vdash \phi \rightarrow \psi$.*

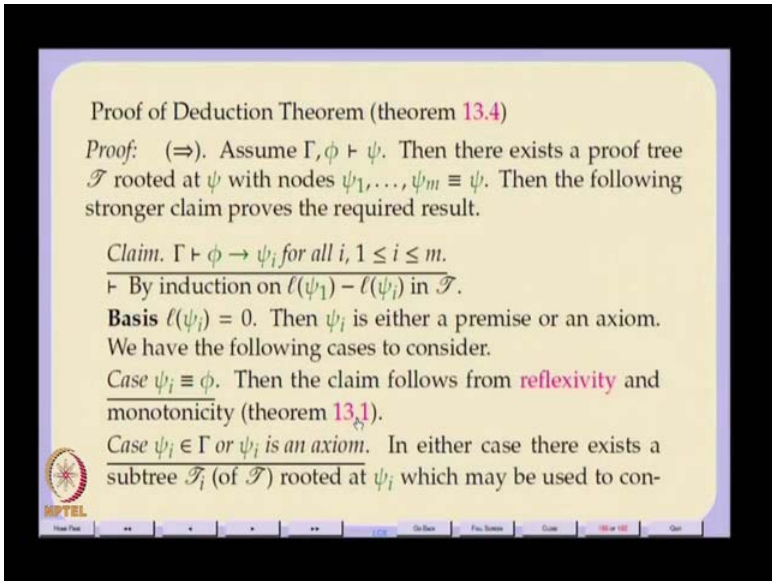
□

The Deduction theorem justifies our usual notion of a direct proof from the hypotheses of a conditional conclusion – the *antecedent* of the conditional is added to the assumptions and the *consequent* is proven.

So, next we come to this important theorem called The Deduction Theorem. And, this actually epitomizes most of the way we go about proving theorems in mathematic. So, the deduction theorem so the notation most logicians do not like all these set union and set brackets and so on and so forth. So, if you want to add to some assumptions we just put a comma and add those assumptions I mean. So, this is so gamma comma of phi proof psi is just mean this gamma union phi proof psi. So, the Deduction Theorem essentially says that, if I have that if there is a conditional statement of the form phi arrow psi that is provable from a set of assumptions gamma. If and only if I after adding phi to the assumptions the new set gamma union phi can prove psi alone.

This is exactly what happens if you see the most of the direct theorems that we prove in mathematics you given a set of hypothesis and, then you have a conditional conclusion. So your first step in any direct proof is to assume all the hypothesis and also assume the left side of the condition. And your last statement usually is the right side of the conditional and effectively you are using the deduction theorem to justify it. So, you are proving a different theorem. So, you are you had to prove this gamma proves phi arrow psi but what you are actually proving is gamma comma phi prove psi right in any direct proofs. Now, the proof of this is not easy so let us go about it in some detail. So, those of you are doing other things besides logic I think should wakeup now.

(Refer Slide Time: 24:40)



Proof of Deduction Theorem (theorem 13.4)

Proof: (⇒). Assume $\Gamma, \phi \vdash \psi$. Then there exists a proof tree $\mathscr{T}$ rooted at ψ with nodes $\psi_1, \ldots, \psi_m \equiv \psi$. Then the following stronger claim proves the required result.

Claim. $\Gamma \vdash \phi \rightarrow \psi_i$ *for all i*, $1 \leq i \leq m$.

$\vdash$ By induction on $\ell(\psi_1) - \ell(\psi_i)$ in $\mathscr{T}$.

Basis $\ell(\psi_i) = 0$. Then ψ_i is either a premise or an axiom. We have the following cases to consider.

Case $\psi_i \equiv \phi$. Then the claim follows from reflexivity and monotonicity (theorem 13.1).

Case $\psi_i \in \Gamma$ *or* ψ_i *is an axiom.* In either case there exists a subtree $\mathscr{T}_i$ (of $\mathscr{T}$) rooted at ψ_i which may be used to con-

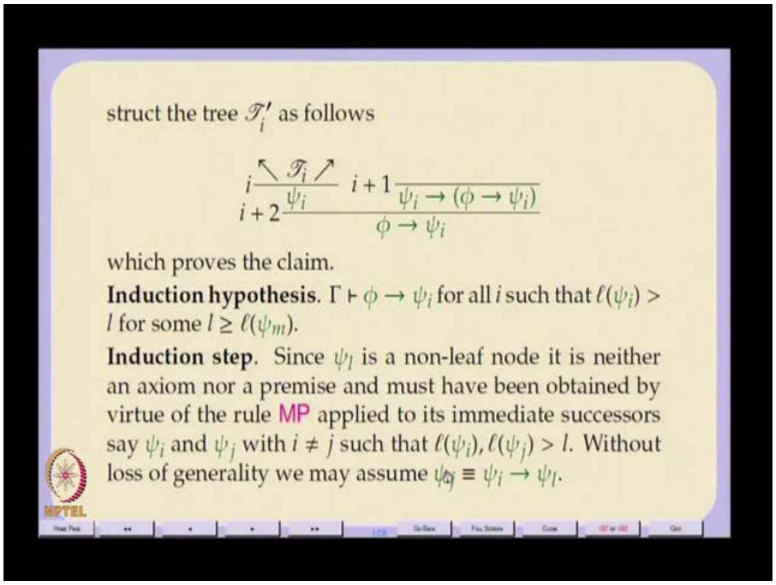
So, this is and if and only if, theorem it is a characterization theorem. So, which means that well there are parts to it one thing to do. Let us go through this parts I have tried to split it up into claims so, that the proof is easier but let us see how it goes. So what I am going to assume is that by putting in phi including phi in the assumptions. I, can prove psi given that assumptions. So, if I assume that psi is provable from gamma comma phi that means there exist a proof tree possibly consisting of m different nodes rooted at psi. Let these m different nodes be psi1 to psi m. By the way there is no there is no proof tree which is empty if you are concluding something. Then there is at least a root which is also the leaf. So, now what will prove is will prove this much stronger claim.

So, we are suppose to prove that gamma from gamma you can prove phi arrow psi m but will prove gamma proves phi arrow psi i for all i. So, that is a so if you can prove this claim then essentially we have we have proved the implication in the theorem. So, will do this by induction this induction this is because of this upside down proof tree. So, the upside down proof tree and because of our definition of tree and levels of a tree the root of the tree has a level 0. The leaves of the tree have the levels of much some positive integer greater than the root of the tree. So, which means that but, our inference actually starts from the leaves and goes down to the root. So, this induction is essentially because of that so the first the very first step I am assuming is going to assuming is going to be a leaf node. So, psi1 is a leaf node if so then essentially each of these, psi i is has some level which is essentially given by the level of psi1 minus its level.

So, I do this induction so this is my measure of induction precisely because of the fact that I am using an upset of an proof tree if I had actually turn the tree upwards to the right way. Then, it would have been any induction on level of psi i. So, this should have been level of psi1 minus level of psi i equal 0. That is the basis of induction that means we are looking at a leaf node. So, think of it right the basis is that you are looking at a leaf node. If, it is a leaf node then clearly it is not obtain by application of any rule of inference. So, it is either an axiom or an assumption or an instance of an axiom schema. In the case of our Hilbert style proof system there are no axioms there are only 3 axiom schemas. So, but of course all each instances each instance of each of those axiom schemas is also an axiom that's there are no separate axioms.

So, then we have three cases to consider. One is that this psi i belongs to gamma or it is the same as phi or third that it is an axiom. So, we can we can club we can separated the case when psi i is phi from the other two cases. If psi i is phi then this reflexivity theorem that we proved already shows phi arrow phi i means it is always it always holds. So, there is there is really nothing to be show. So, the only case so the only interesting part of this case is when psi i is either an assumption for an axiom or that is or an instance of an axiom schema. So, that means so corresponding to each psi i there is a sub-tree of the original proof tree. Which, I will call Ti so this Ti is rooted at psi i.

(Refer Slide Time: 29:44)



struct the tree $\mathscr{T}_i'$ as follows

$$ {}_{i+2}\dfrac{{}_{i}\dfrac{\nwarrow \mathscr{T}_i \nearrow}{\psi_i} \qquad {}_{i+1}\dfrac{}{\psi_i \to (\phi \to \psi_i)}}{\phi \to \psi_i} $$

which proves the claim.

Induction hypothesis. $\Gamma \vdash \phi \to \psi_i$ for all i such that $\ell(\psi_i) > l$ for some $l \geq \ell(\psi_m)$.

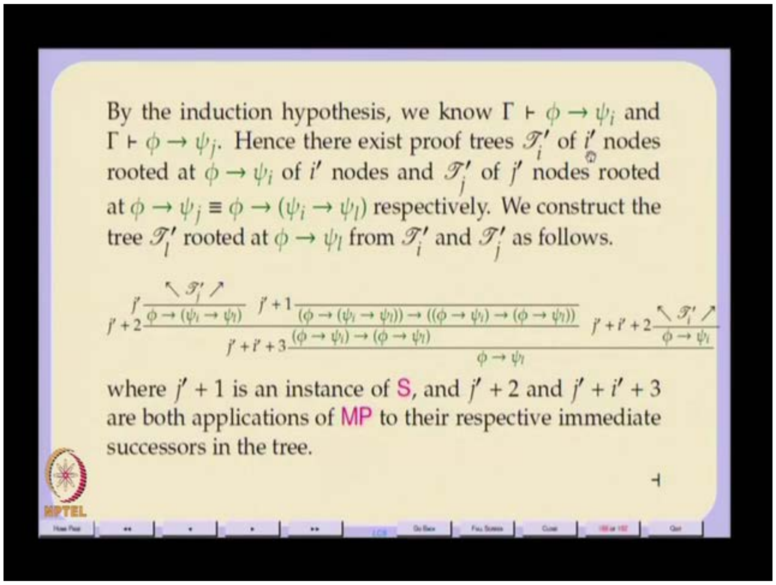
Induction step. Since ψ_l is a non-leaf node it is neither an axiom nor a premise and must have been obtained by virtue of the rule MP applied to its immediate successors say ψ_i and ψ_j with $i \neq j$ such that $\ell(\psi_i), \ell(\psi_j) > l$. Without loss of generality we may assume $\psi_j \equiv \psi_i \to \psi_l$.

Now, what I will do is, so this is this is how I am going to represent this Ti. Now I am going to construct another proof tree Ti prime from using this proof tree Ti. So, this whole thing is the proof tree Ti. And let us assume it is some step higher or some such thing or i prime if you like. And, then what I do is I create a new leaf node essentially by appealing to the axiom schema K. So, this leaf node with this so this trivially follows axiom schema K psi i arrow phi arrow psi i it exactly matches the patterns given in defined in K. So, this must be true but now from this two steps I can infer phi arrow psi i by modus ponens. So, now let us assume the induction hypothesis that we have done this all for some up to some l or for all measures below that level l. Let us say and that we have got we have got to prove for some psi l we have to prove that phi arrow psi l is provable from gamma. So, this psi l is a non-leaf node it is neither.

So, therefore it cannot be an axiom or a premise or a, or an instance of an axiom schema there is only one rule of inference in the Hilbert system. And, so therefore that psi l that step psi l should have been obtain by an application of this rule. If, it was obtained by an application of this rule modus ponens then it must have, then the only way you could have concluded psi l is if therefore some target steps i and j. Which, enable to do a pattern matching in substitution according to the rule mp. So, there are some psi i and psi j such that they actually without loss of generality I am just assuming that psi j is of the form psi i arrow psi l. Otherwise you could not have concluded psi l using modus ponens.

So, you concluded from these two nodes i and j if, you concluded psi l then, one of the nodes let us say psi i was just some formula of psi i. And, the other node psi j was of the form psi i arrow psi l only then you could have applied this rule of inference and concluded psi l. So, now but what we have to prove is gamma prove and this is in the tree gamma comma phi proves psi l. So, we are looking at we have we started with the assumption that gamma comma phi proves psi. And, we have gamma comma phi proves psi i all of each for each i there sub-trees of this tree. So, this is what we are going to assume so we are going to assume that psi j is of the form psi i arrow psi l in that proof tree.

(Refer Slide Time: 33:58)



By the induction hypothesis, we know $\Gamma \vdash \phi \to \psi_i$ and $\Gamma \vdash \phi \to \psi_j$. Hence there exist proof trees $\mathscr{T}_i'$ of i' nodes rooted at $\phi \to \psi_i$ of i' nodes and $\mathscr{T}_j'$ of j' nodes rooted at $\phi \to \psi_j \equiv \phi \to (\psi_i \to \psi_l)$ respectively. We construct the tree $\mathscr{T}_l'$ rooted at $\phi \to \psi_l$ from $\mathscr{T}_i'$ and $\mathscr{T}_j'$ as follows.

$$j'+i'+3\ \cfrac{j'+2\ \cfrac{j'\ \dfrac{\nwarrow \mathscr{T}_j' \nearrow}{\phi \to (\psi_i \to \psi_l)} \qquad j'+1\ \dfrac{}{(\phi \to (\psi_i \to \psi_l)) \to ((\phi \to \psi_i) \to (\phi \to \psi_l))}}{(\phi \to \psi_i) \to (\phi \to \psi_l)} \qquad j'+i'+2\ \dfrac{\nwarrow \mathscr{T}_i' \nearrow}{\phi \to \psi_i}}{\phi \to \psi_l}$$

where $j'+1$ is an instance of S, and $j'+2$ and $j'+i'+3$ are both applications of MP to their respective immediate successors in the tree.

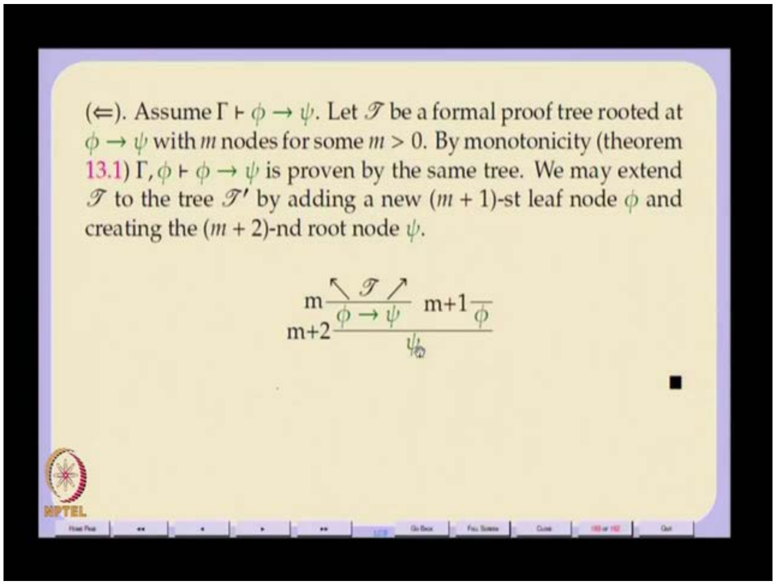
⊣

And, since i and j belong to some target levels less than this level or higher than this level l. So, therefore by induction hypothesis they do exist proof trees Ti prime and Tj prime. Which, proof from gamma which proof phi arrow psi i and phi arrow psi j respectively. These are separate proof trees because, these are different proofs with a different some assumptions. So, now what this means is now each of these proof trees Ti prime and Tj prime let us assume they have i prime nodes and j prime nodes respectively. So, Ti prime is rooted at i prime rooted phi arrow psi i and Tj prime is rooted at phi arrow psi j. But, psi j of course is psi arrow psi l so Tj prime is rooted at phi arrow psi arrow psi l. Now, what I am going to do is I am going to form a new proof tree T prime l from the proof from the two proof trees T prime i and T prime j.

So, this represents T prime j so now I am assuming that step numbers have to be different in each case. So, now I am assuming that this proof tree Ti prime has i prime nodes and this proof tree has j prime nodes. And, if I am going to combine them I have to make step number unique and so on and so forth. There is a basic there is at basic book keeping which has to be done. So, let us assume that this tree Tj prime is rooted at phi arrow psi i psi l. And, there is this tree Ti prime rooted at phi arrow psi i. Now, I am going to take my j plus j prime plus 1th step to be a leaf node which is an instance of the axiom schema S.

So, look at this j prime plus 1 it is an instance of the axiom schema S. Because, phi arrow psi i arrow psi l can arrow this arrow distributes over this arrow. So, you get phi arrow psi i arrow phi arrow psi l these two steps j prime and j prime plus 1 are instances of the hypothesis of modus ponens. And, so I can get the step j prime plus 2 by an application of modus ponens which will essentially give me phi arrow psi i arrow phi arrow psi psi l. The tree Ti prime is already rooted at phi arrow psi i. So, the steps 1 to i prime i rename them i renumber them as j prime plus i prime plus 2 to j prime plus j prime plus 3 to j prime plus i prime plus 2and I have this root here. And, these two steps essentially are instances of the modus ponens rule can be applied on these two to yield phi arrow psi, Is there anybody who followed it is fine. So, this proof tree is my proof tree T prime l. And, that proofs that from gamma it proves phi arrow psi l and let so the induction step is over and, therefore the first part of the theorem is over.

(Refer Slide Time: 38:47)



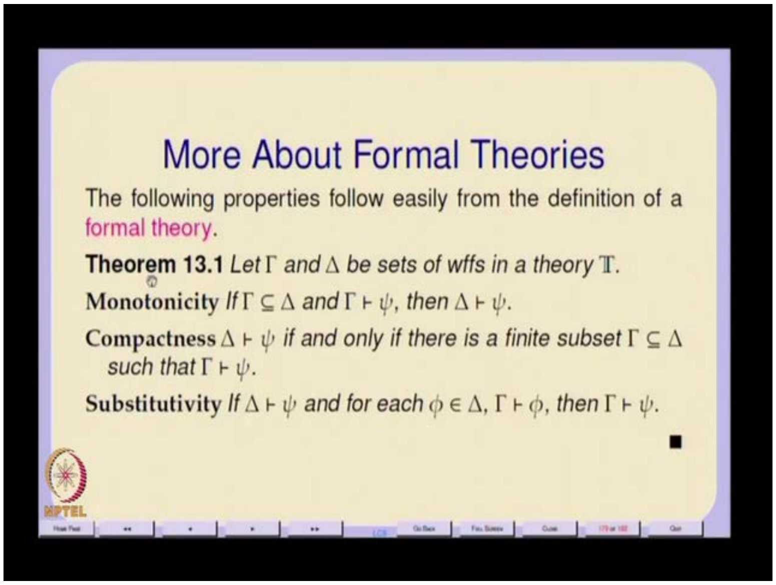
(⇐). Assume $\Gamma \vdash \phi \rightarrow \psi$. Let $\mathscr{T}$ be a formal proof tree rooted at $\phi \rightarrow \psi$ with m nodes for some $m > 0$. By monotonicity (theorem 13.1) $\Gamma, \phi \vdash \phi \rightarrow \psi$ is proven by the same tree. We may extend $\mathscr{T}$ to the tree $\mathscr{T}'$ by adding a new $(m+1)$-st leaf node ϕ and creating the $(m+2)$-nd root node ψ.

$$\text{m+2}\,\frac{\text{m}\,\dfrac{\nwarrow \mathscr{T} \nearrow}{\phi \rightarrow \psi} \qquad \text{m+1}\,\dfrac{}{\phi}}{\psi}$$

■

So, the second part is the converse and that is much simpler actually. So, here of course we Assume that we have proofs of phi arrow psi. So, let T be this formal tree may be consisting of m nodes for some m greater than 0 then, by monotonicity.

(Refer Slide Time: 39:12)



More About Formal Theories

The following properties follow easily from the definition of a formal theory.

Theorem 13.1 *Let Γ and Δ be sets of wffs in a theory $\mathbb{T}$.*

Monotonicity *If $\Gamma \subseteq \Delta$ and $\Gamma \vdash \psi$, then $\Delta \vdash \psi$.*

Compactness *$\Delta \vdash \psi$ if and only if there is a finite subset $\Gamma \subseteq \Delta$ such that $\Gamma \vdash \psi$.*

Substitutivity *If $\Delta \vdash \psi$ and for each $\phi \in \Delta$, $\Gamma \vdash \phi$, then $\Gamma \vdash \psi$.*

■

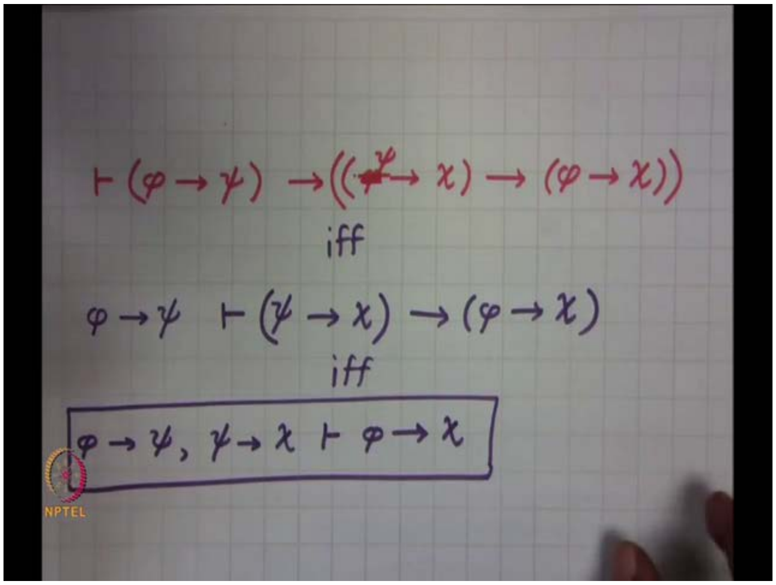
So that, is there are this we had this three properties which essentially said if you keep adding extra assumptions. The previously proven conclusions still continue to hold the there is a question of supposing my extra assumption was a negation of some previous conclusion, Does that previous conclusion still hold? When that is valid and legitimate question But, the answer to that is yes it holds it, still continues to hold. So, we will define provable inconsistency in terms of that. So, in fact what we will do is we will define that a, set of assumptions is inconsistent if and only if every formula and the language can be proven from that.

So, in that sense it still consistent with monotonicity. So, by this monotonicity theorem I can add this extra assumption phi and i still have my conclusion phi arrow psi. So, the proof tree does not change so the original proof tree for gamma proofs phi arrow psi continues to hold also for gamma comma phi proves phi arrow psi. But, what we can do is we can add this so this proof tree has m nodes you added in extra assumption you can also add an extra leaf node.

So, I take this original proof tree T rooted at phi arrow psi add this extra assumption phi and i get a conclusion psi by a simple application of modus ponens. So, this is actually a very powerful theorem. In fact without in any Hilbert's style proof system without first proving this theorem it is almost impossible to proceed further. Because, what it does is it greatly simplifies the proofs of several other kinds of theorems. So, though almost but notice that I had to use reflexivity somewhere I had to use reflexivity somewhere. So, this proof was absolutely essential and it had to be done without the use of deduction theorem. If, you look at the deduction theorem it is essentially about conditionals whereas reflexivity is also about conditional.

And from the deduction theorem it actually, if I dint require to use reflexivity in the deduction theorem. And I had that deduction theorems stand alone then I could have prove reflexivity trivially by saying phi proves phi i mean that is it. But, unfortunately I did require reflexivity and therefore it is necessary to do that proof before actually proving the deduction theorem. But, once you have the deduction theorem lots of things become much easier. So, one of the so let us take so reflexivity is one aspect. Let us look at something else so one other possibility is transitivity.

(Refer Slide Time: 45:25)



$$\vdash (\varphi \rightarrow \psi) \rightarrow ((\overset{\psi}{\cancel{\varphi}} \rightarrow \chi) \rightarrow (\varphi \rightarrow \chi))$$

iff

$$\varphi \rightarrow \psi \ \vdash (\psi \rightarrow \chi) \rightarrow (\varphi \rightarrow \chi)$$

iff

$$\boxed{\varphi \rightarrow \psi, \ \psi \rightarrow \chi \ \vdash \varphi \rightarrow \chi}$$

So, you can look at this so essentially phi arrow psi, comma psi arrow Kai proves phi arrow Kai. So, this is essentially transitive of the conditional. And, if it had been written as a theorem as a formal theorem then what one would have done, is one would not have bother to write these commas. Instead actually one would have written it like this. So, if I had to write it as a theorem as a formal theorem this is how I would have written it, is it clear or should I.

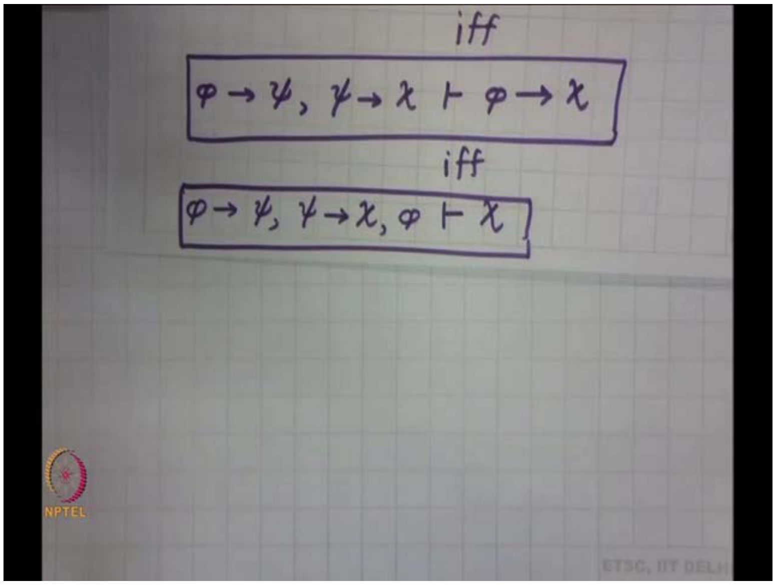
So, as a formal theorem what I would have written is this phi arrow psi, arrow psi arrow Kai, arrow phi arrow is this bracket no. This is not so, I would have write it as a formal theorem I would have written it as phi arrow psi arrow phi arrow psi arrow Kai arrow phi arrow chi this would have been the formal theorem. So, supposing you have to prove this here. Now, it is actually very simple this whole theorem can be proven write it I prove.So, this is a formal theorem by the deduction theorem if and only iff from the assumption phi arrow psi I can prove psi arrow Kai arrow phi arrow Kai. And, this holds if and only iff phi arrow psi comma psi arrow Kia proves phi arrow Kai. So, in fact so it suffices to prove this by the deduction theorem. Now, how I will prove this?

Student: deduction phi arrow phi (Refer Time: 47:22)

That is what we are going to use. So, can somebody tell me, How to proceed with this using phi?

Student: (Refer Time: 47:36)

(Refer Slide Time: 47:44)



iff

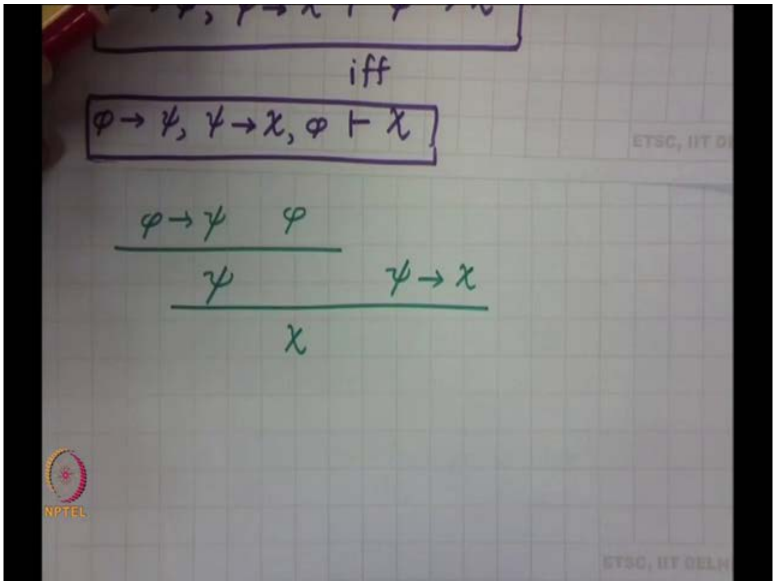
$\boxed{\varphi \to \psi, \psi \to \chi \vdash \varphi \to \chi}$

iff

$\boxed{\varphi \to \psi, \psi \to \chi, \varphi \vdash \chi}$

So, we are going to you are going to assume phi. So, if and only iff phi arrow psi, phi arrow psi, psi arrow Kai comma phi Kia that is all. So, if you prove this it is actually sufficient and how do we go about proving this we just we start with this assumptions.

(Refer Slide Time: 48:34)



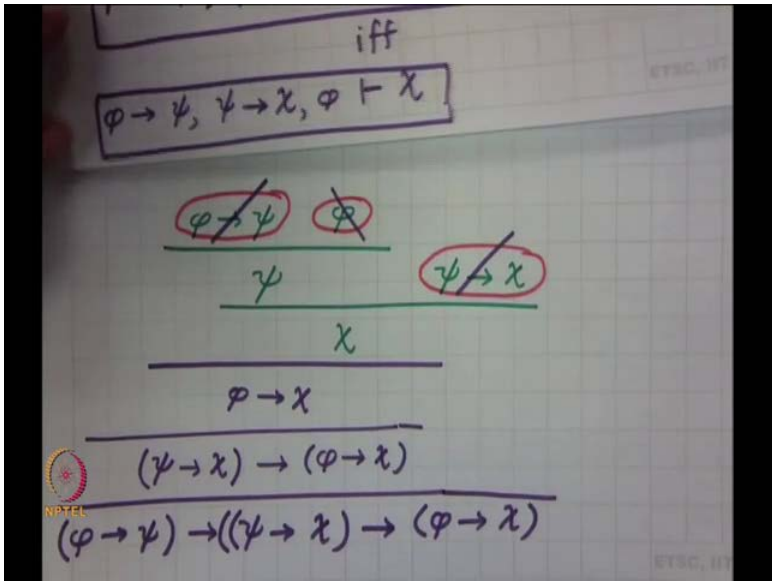
iff

$$\boxed{\varphi \to \psi, \psi \to \chi, \varphi \vdash \chi}$$

$$\dfrac{\dfrac{\varphi \to \psi \qquad \varphi}{\psi} \qquad \psi \to \chi}{\chi}$$

And, essentially from so you have you have this you have one leaf node this require some complicated manner calculation. Which, I have this as a leaf node I have this is another leaf node from which I can infer psi. And, then I have this as a leaf node and I already have this from which I can infer Kai and, that is a three step proof. So this, the deduction theorem will considerably simplify a large number of proofs. There is also a connection that this deduction theorem gives you. So, let us take this let us take all this together so what we are saying now is that we have what are known as direct conditional proofs in which certain assumptions can be made. So, what we are essentially going to do is, we are going to look at this deduction theorem. So, we are going to so assume so this, much assume you got this. These are all you can think of these assumptions.

(Refer Slide Time: 50:24)

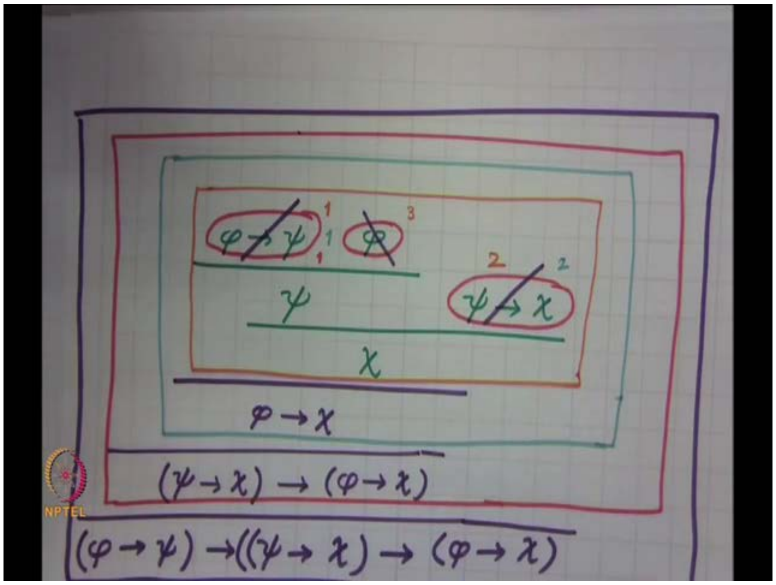

iff
$\varphi \to \psi, \psi \to \chi, \varphi \vdash \chi$
$\varphi \to \psi$ φ
ψ $\psi \to \chi$
χ
$\varphi \to \chi$
$(\psi \to \chi) \to (\varphi \to \chi)$
$(\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi)$
NPTEL

So, these are assumptions from gamma. So, our gamma consisted of this, something else was this something else psi arrow Kai also no psi arrow chi phi. Now, these are the assumptions we used. So, from these assumptions you prove Kai and essentially what you are going to do is so you have a proof like this, from these assumptions. And, then essentially the deduction theorem allows you to discharge these assumptions. So, if you look at this purple stuff here the deduction you can actually backwards on this on this step. So I can actually think of this as from here I can actually discharge the assumption.

So I am using at different colored to show that I am discharging in assumption. And, this discharge this assumption phi essentially means that I have phi arrow Kai here. And, then I can go one step further and discharge this assumption and get psi arrow Kai arrow phi arrow Kai. Then, I can go another step further and discharge this assumption to give me essentially phi arrow psi arrow psi arrow Kai arrow phi arrow Kai. So what this, the connection with programming language is and programs in general is merely this. That, in order to prove this I am essentially making some assumptions those assumptions are create new scope for those assumptions.

Student: what is the discharging (Refer Time: 53:17)

(Refer Slide Time: 53:33)



I tell you what I am looking for a suitable way of presenting it in terms of trees. But, so essentially what I am saying here is so this is an inner most scope. Which has these assumptions 3, 2 and 1 having discharge this as this assumption phi i get an outer scope. Which has these two assumptions 2 and 1 in which this assumption it has this two assumptions 2 and 1 and then when I discharge this psi arrow Kai I get another scope. Which has essentially the assumption in which this is gone and there is only the assumption 1. And, the outer most scope for which I have run out of colors is essentially this outer most scope. Which, has no assumptions this connection with scope is not I mean is not just incidental or trivial. There, is a scope of the assumption so if you look at this, tree you are looking at increasing nesting of scope levels exactly like we see in our program. Further this, scope levels now actually what will happen is the next important theorem will prove is a proof by contradiction. And, there what assumptions are taken in order to get a contradiction become important. And, so therefore the scope of these assumptions becomes important.