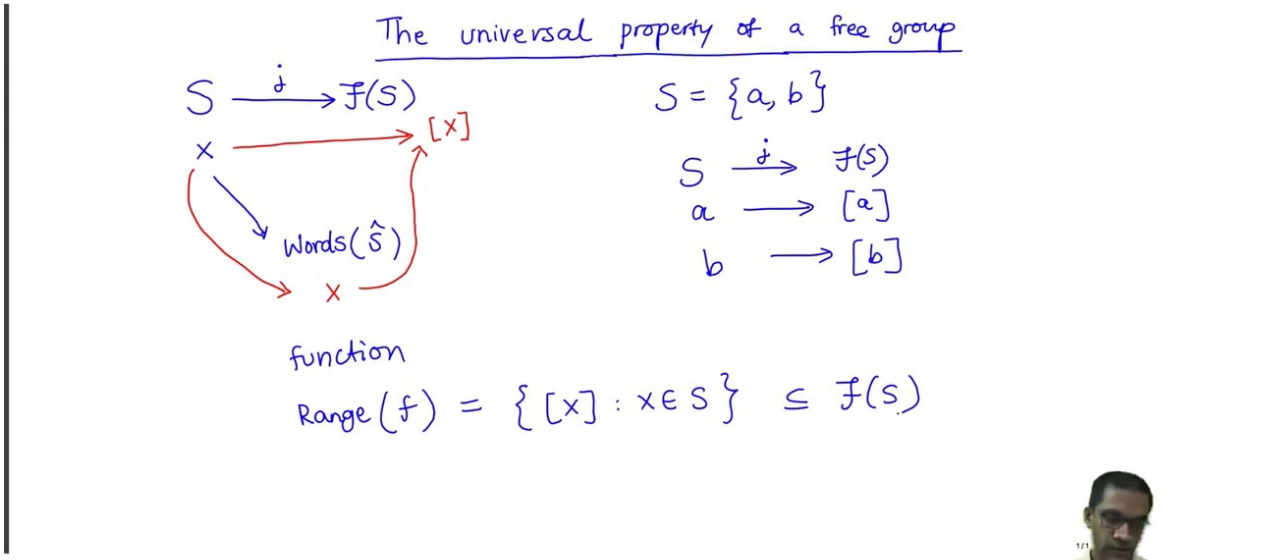
Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

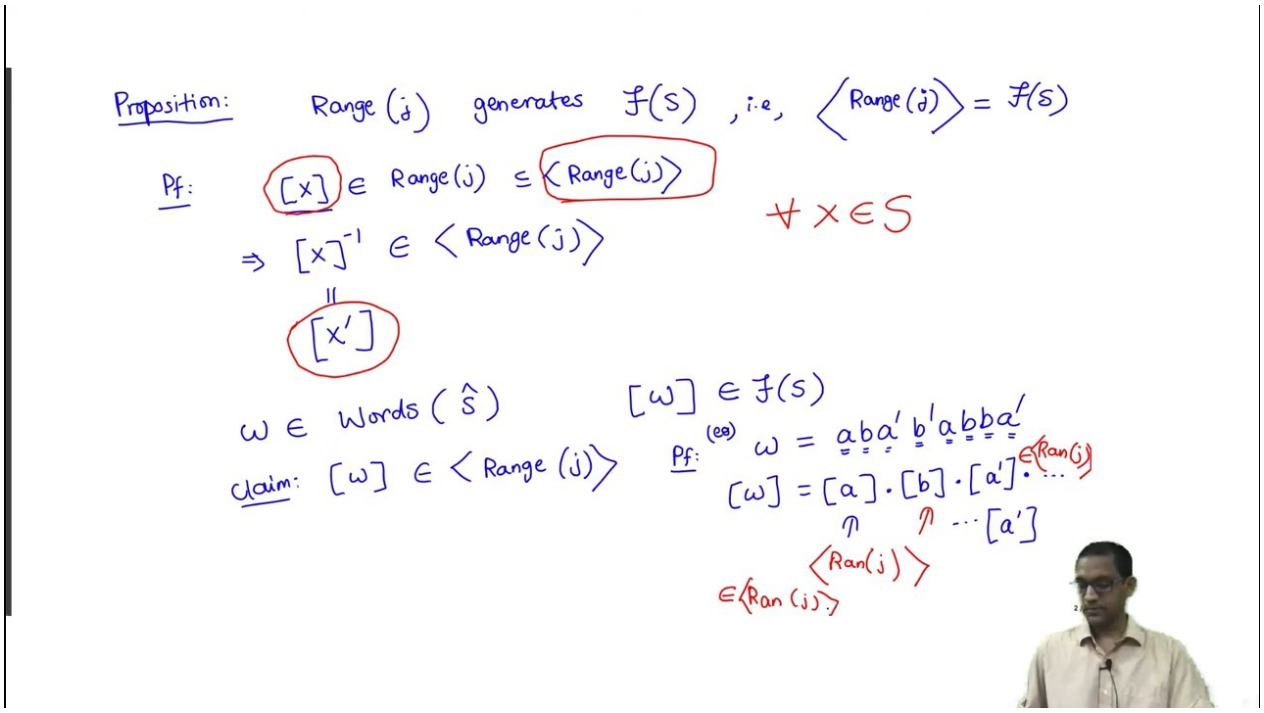
1. Lecture 30 [Free Groups IV]

So, what we will talk about today is what is called the universal property of a Free Group. So, what do we have, we have a set S and given the set S we have constructed something called the free group on this set S or generated by this set $S = \{a, b\}$.

Now,between these two objects the set and the free group generated by that set there are in fact, is a certain natural map ok. So, what map is this? So, we will give this map a name I will call it j, what does this map do? Take any alphabet take any element x of the set S. So, for example, for the free group on two generators we had called them $\{a, b\}$. So, X is say a or B in that case. So, more generally X can be any element of the set S.

Now, how do we associate to this an element of the free group . So, we do the following we first think of. So, maybe it is best to think of this in the following waylet us map S to the set of all words in s hat the augmented alphabet. What map is this, well the element X first is going to map to the word X . So, think of this as just the word X it is got length 1. Now, from the set of words in s hat to the free group I have the following obvious map given any word I can associate to it the equivalence class corresponding to that word ok.





So,the net result is that this map j that I have talked about is the following it sends X to the equivalence class of just the singleton word X ok. So, that is sort of a natural map.

So, for instance if we take the free group on two generators that we talked about. So, this is let us illustrate this phases a, b. I have the free group on two generators this natural map just does the following it takes a and maps it to the equivalence class of $[a]$, b to the equivalence class of $[b]$ ok. So, map to the free group.

Now, observe that$S$ is just a set $F(S)$ is a group, butfrom a set to a group, you have a function you really cannot talk about other extra properties that the function can have right. For example, if you have a map between two groups, as we have seen before we can talk about homomorphisms sub groups ah, but in this case one of them is just a set. So, it is justa map of sets or in other words it is just a function ok.

So, this is a function so, just a map. And, what is the image of this map. So, what is the range of this function if you wish? So, let me call this the range of this function f , well. What is this by definition this is just the set of all equivalence classes of the singletons X as X ranges over S ok. So, this is some subset of the free group and here is the firstimportant observation that this subset range of S. So, here is the let us call this a proposition. So, here is a proposition , this particular subset the range of this function range of this function j in fact, it is a subset of the free group which generates the free group ok.

Proposition: Range(j) generates $F(S)$, i.e $\langle Range(j)\rangle = F(S)$

In other words, if you recall we had this notation which said given any subset this case the $Range(j)$, the subgroup generated by that subset which means the intersection of all sub groups of $F(S)$ which contain the subset that subgroup the subgroup generated by this is in fact, the whole group that is what we mean by saying it generates this ok.

So, the proof well rather easy there are some obvious elements which belong to the range for example, by definition this belongs to the range and hence to the sub group generated by

the range . Now, whenever an element in this case X singleton belongs to a subgroup the inverse of that element. So, this means that the inverse of X also belongs to that subgroup ok. But observe the $[X]^{-1}$ as we have already seen is nothing, but the equivalence class of the word $[X']$ ok. So, what does this mean, this means that $[X'] \in Range(j)$ ok. So, we have identified two very important classes of elements one is X itself, the other is X' . So, all of these guys belong to the range of j ok and this is true for every X in the alphabet S. So, in particular if your alphabet only had two elements $\{a, b\}$, what we are saying is that the a, b as well as $\{a', b'\}$ all four of these belong to the subgroup generated by the range of this function ok.

Now, that is more or less all we need as soon as you have these four types of elements, I mean we have these two types of elements X and X' . This automatically means that everything else belongs ok. So, what are all the other, what is the typical element of $F(S)$ going to look like? Well, it is going to look like the following you take a word take w to be a word in the augmented alphabet then the typical element. So, look at the equivalence class of $[w]$ this is an element of the free group . So, every element of the free group is of this form the equivalence class of some word, I claim that this equivalence class of $[w]$ also belongs to the subgroup generated by sorry that that is going to be edited out .

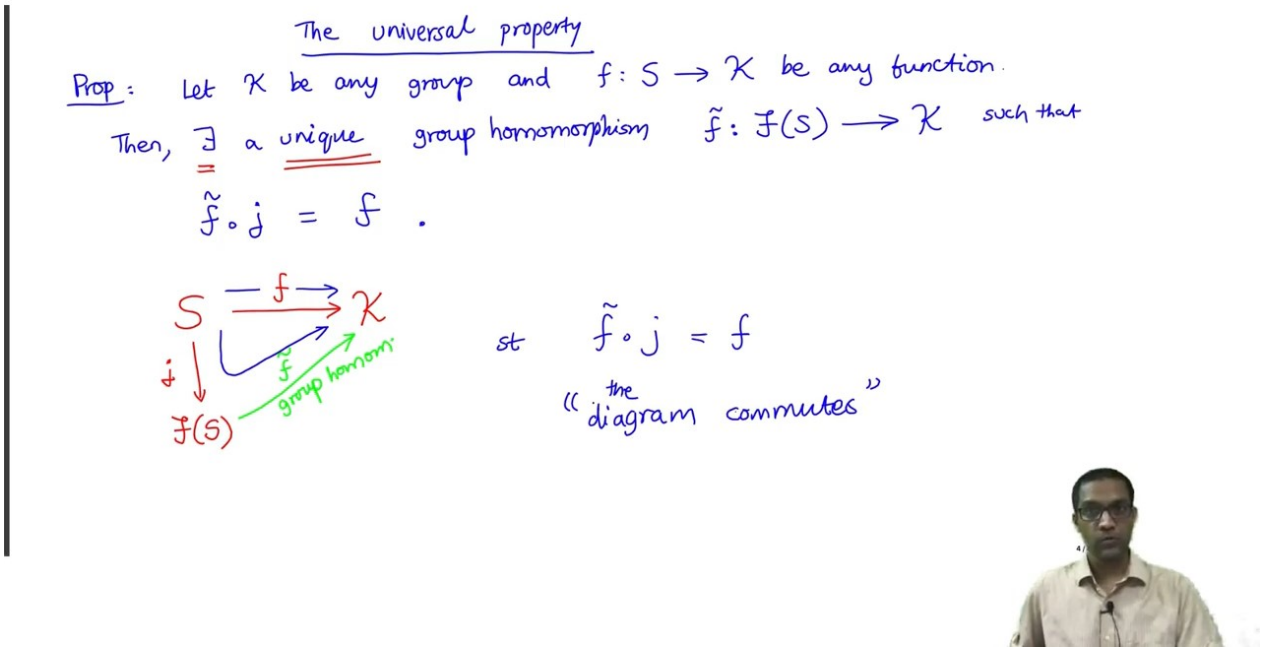
So, let me start again from the claim. So, the claim is that the equivalence class of $[w]$ belongs to the image of or the range of this function . The subgroup generated by the range ok and why is this, what does a typical word look like. So, there is a proof of the claim. So, imagine, what does a word look like? So, let me just describe the basic idea and leave the formal writing out of this argument to you ah. So, for example,if we were in the the free group on two generators case here is the. So, here is an example , say maybe this is a typical word may be the word looks like this ok.

So, if this is what your word looks like, then observe the equivalence class of $[w]$ is by definition. So, w itself is a concatenation of all the singletons right w can be thought of as the singleton a that is a word concatenated with the word, the singleton b concatenated with this word, with the next one with a with b with b and a'ok.

$$[w] = [a][b][a']$$

So, when you look at the definition of the product in the free group it is just this multiplied by dot dot dot all the way till the last alphabet which is a'ok. So, the equivalence class of $[w]$ is nothing, but the product of equivalence classes of singletons just words of length one and each singleton is of the form either a or a'or b or b'right. So, more generally if you would write this proof out for the case of an arbitrary set S, each w would be written as a productsimilar product in which each alphabet which occurs each letter which occurs is either an element X of the alphabet or of the form X' for some X' in the alphabet ok, just like what we see here.

So, what does that mean, but now observe each of these guys we have just proved that a belongs to right. So, we have just shown that a is an element of the image of j or the range of j b the singleton belongs to the range, a'belongs to the range , b'if it occurs belongs to the range and so on right. So, in this case we have shown that each one of the singletons is an element of the subgroup generated by the range. And so, if each element is in the subgroup the product is of course, in the subgroup ok. So, this means that because it is a product it belongs to the subgroup generated by the range of j ok. So, the key idea here is really the first step. So, this is this is more or less a once you show that the singletons are there in the



subgroup generated by the range then every word is automatically there because a word is really a product of singletons ok.

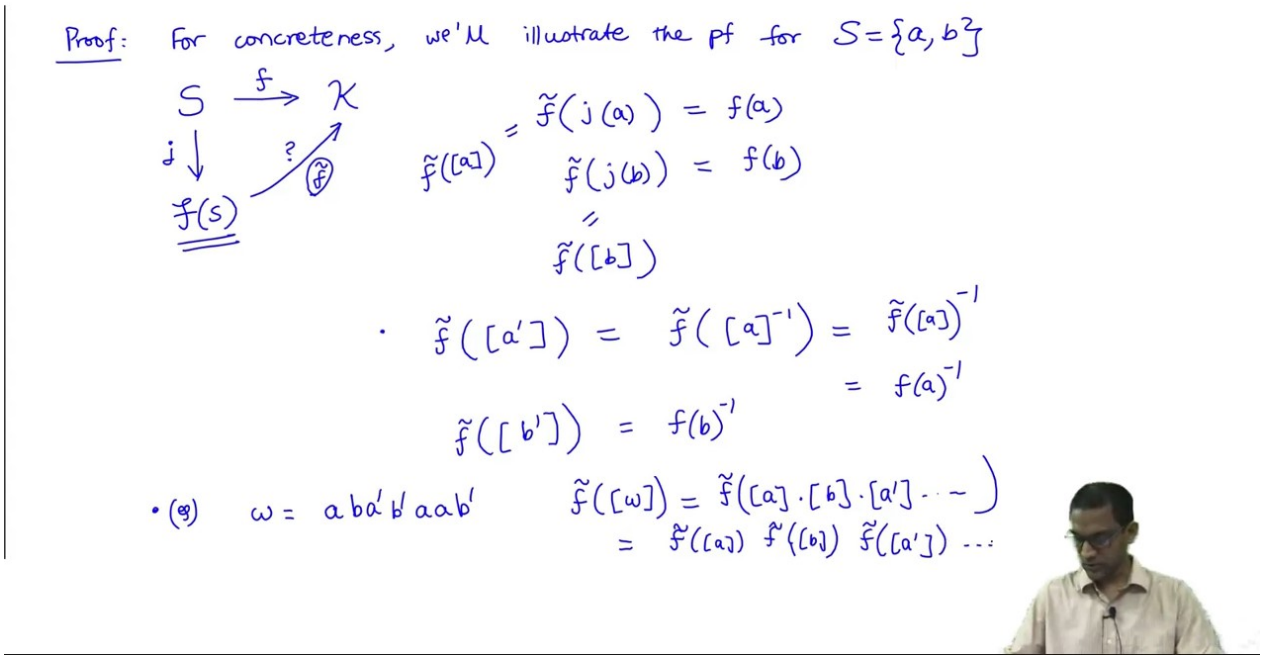
So, what does that mean; that means, that finally, we have shown thatw belongs to the subgroup generated by the range of j and so; that means, every element of the free group itself is contained in the range ah, but of course, the subgroup sorry the subgroup generated by the range. But the reverse inequality is of course, true the subgroup generated by the range is always I mean after all by definition it is a subgroup of the free group. So, this is obvious and so we have inequalities or ratherthe subset sign going both ways which means these two are actually equal. So, the free group is equal to the the subgroup generated by the range of this special map j ok and in some sense this is the sense in which this we say that the free group is the group generated bythe set S we identify the set S in some sense with the range of this this map j ok.

Now let us go on to the the the universal property itself. So, this is sort of the first step in some sense. Now let us move on to the universal property. So, call this ok. Now let us formulate this in the form of a proposition . So, it says:

Proposition: let K be any any group and, $f : S \to K$ be any function just a map of sets. Then, there exist a unique group homomorphism $\widetilde{f} : F(S) \to K$ such that $\widetilde{f} \circ j = f$

So, this is thethis is the statement of the universal property of the free group.

So, let us just try and understand this what it saysa little bit more ok, for this it is easiest if we just draw diagram. So,recall what is given is your set s a group K and a function between them f . Now, j as we saw earlier is a certain distinguished map from the set to the free group generated by the set. Now what is being ascertained here is that there exists a group homomorphism. So, f and j are not group homomorphisms, they are just maps of sets, but the claim is that there is a group homomorphism ok. So, the existence of this map which we will call $\widetilde{f}$ is the content of the proposition. So, that is a group homomorphism ok.



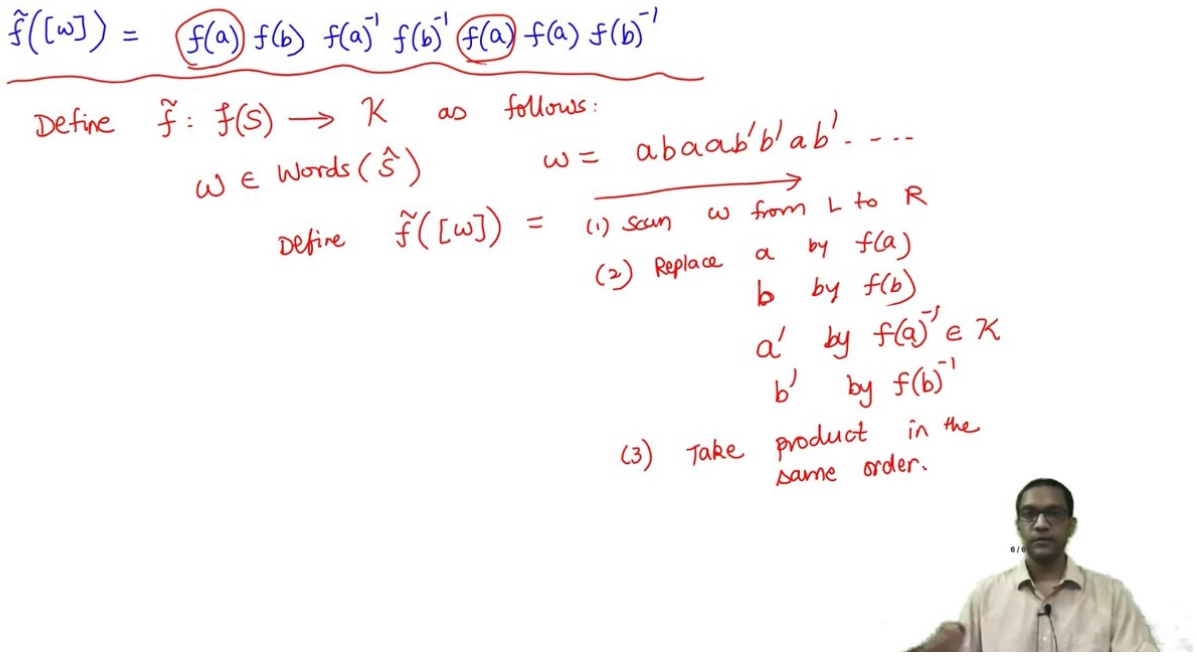
And further its unique so, there is also an additionalthing of uniqueness such that, this what we usually express as such that this diagram commutes. So, if you see what thisidentity says it is $\widetilde{f} \circ j = f$, which means that if you sort of go from S downwards and then like this. So, that is your $\widetilde{f} \circ j$ or you just go straight to K that is your f ok, such that whether you go down like this or straight like this you get the same answer and this is what we usually express by saying such that the diagram commutes ok which diagram the one that I have just drawn ok.

So, the the key assertion here is the existence and uniqueness of a group homomorphism which makes this diagram commute ok. So,let us try and prove this, the proof itself is rather easy some sense everything about the proof is already forced it is all determined. So, we just have to follow what is required to be satisfied by the function $\widetilde{f}$

So, let us let us start here. So, maybe for concreteness let me illustrate the proof again for the case. So, let me just say for concreteness , I will illustrate the proof for for the free group on two generators, but you should be able to extend it without any difficulty to arbitrary free groups. So, what is it that we need, we need from the set $S$to K you are given a map f I have to construct a map like this right. So, this is this is the thing that I still do not know this is the original map j ok.

So, let me see what properties my $\widetilde{f}$ has to satisfy this this map $\widetilde{f}$. So, observe that $\widetilde{f}(j(X))$. So, so here I just have S is $\{a, b\}$. So, let us just see what this does to $\{a, b\}$ first. So, observe this is equal to $f(a)$, similarly $\widetilde{f}(j(b))$ is supposed to be the same as $f(b)$ ok. So, this is just by the definition I mean this is the requirement $\widetilde{f} \circ j = f$.

Now, what is this mean $\widetilde{f}(j(a))$ is by definition, $\widetilde{f}([a])$ ok $\widetilde{f}(j(b))$ again by definition is $\widetilde{f}([b])$ ok. So, what is it that I have to start with, I already know what values $\widetilde{f}$ must take on the range of j ok. I know what value takes on the the singleton equivalence class of $[a]$, I



know what value takes on the equivalence class of $[b]$ ok. So, $\widetilde{f}$ is partially determined it is determined it is given to me on the range of this function j that is more or less what it said ok.

But that is really enough because if you remember what we just did the range of j generates the free group right it is a generating set for the free group. So, if I know my homomorphism $\widetilde{f}$ on this generating set, I can deduce its values on all the elements of my free group ok and we will do it in just a second. So, this is what I am I know I must have . So, for now just treat all this as sort of heuristics we are trying to see what all information we can deduce about $\widetilde{f}$.

Now, so let us do the next thing what is $\widetilde{f}$, what do you think $\widetilde{f}$ should be on let us say a', well again as before. So, this is almost like the calculation we just did. So, recall $a'$is nothing, but a inverse by definition and a homomorphism since $\widetilde{f}$ is a homomorphism, if I know the value on a then the value on a inverse is just the inverse of that value ok. But now again $\widetilde{f}([a])$ I already know what it is it is $f(a)$ and so this should be $f(a)^{-1}$ ok.

So, what this means is I also know the value of $\widetilde{f}([a'])$ similarly by the same logic I know the value of $\widetilde{f}([b'])$ it is nothing, but $f(b)^{-1}$ ok. So, what we have done is, we have managed to find four pieces of information about $\widetilde{f}$ its value on a, its value on b, its value on a' , its value on b' ok.

And, now recall that any word you know I am trying to find out how to define $\widetilde{f}$ on all of $F(S)$ ok, but any word in $F(S)$ is well it is a word. So, I mean see equivalence class of $[a]$ word it can be written as a product of $[a] \cdot [b]$, $a'$and b'ok. So, that will tell me how to define $\widetilde{f}$ on any word .

So, again let us do it do this by example for concreteness, if I take the word w which looks like a, b, a' , b' , a, a for example, a a b'ok. If this is my w then observe how will I. So, I am

going to ask the following question; what should what value should $\widetilde{f}$ take on the equivalence class of $[w]$? Well, just like the computation we did the value should be $\widetilde{f}$ of I first write w as a concatenation of singletons. So, I think of w as being a into b into a' etcetera etcetera ok.

And, now I use the fact that $\widetilde{f}$ must be a homomorphism. So, if it is a homomorphism what does that mean, it says thatthis is $\widetilde{f}$ of. So, let us maybe just do it on this page. So, this should look like this should look like $\widetilde{f}([a])$, $\widetilde{f}([b])$ this is just the homomorphism property, $\widetilde{f}([a'])$ etcetera ok, but then each of those we know, we know the answers to those right.

So, for example, this is justlet us do this. So, the answer is going to be $\widetilde{f}([a]) = f(a)$, $\widetilde{f}([b]) = f(b)$, $\widetilde{f}([a']) = f(a)^{-1}$, $\widetilde{f}([b']) = f(b)^{-1}$, next was $f(a)$ let us go back up and check. So, this was $aba'b'aab$. So, the last guy is $a\ b'$. So, this is $f(b)^{-1}$ ok.

So, you can sort of see how I deduced the value that $\widetilde{f}$ should take on this word and this this final answer here $\widetilde{f}([w])$. So, this sort of tells us how we should define this this map $\widetilde{f}$ now in general ok. So, now, now that we sort of have an intuitive idea of how$\widetilde{f}$ should be acting , let us just go back and use this as our definition of $\widetilde{f}$ ok. So, this this last thing here is going to begoing to becomeour definition in some sense.

So, now we go back and define $\widetilde{f}$ formally . So, define $\widetilde{f}$ formally as follows , from the free group to K as follows take any element w well take any word w, if you wish s hat. Now write this as a product of a is b is a s and b sa b a a etcetera that is what w is going to look like in general. Now, the definition so then, define $\widetilde{f}([w])$ using the following prescription. So, let me just describe it you scan. So, here is the procedure you scan w from left to right. So, step one scan w from left to right , every time you see an a. So, what will you see when you scan it you will see either an a or $a\ b$ or an a'or $a\ b'$, whenever you see an a you replace a by f of a .

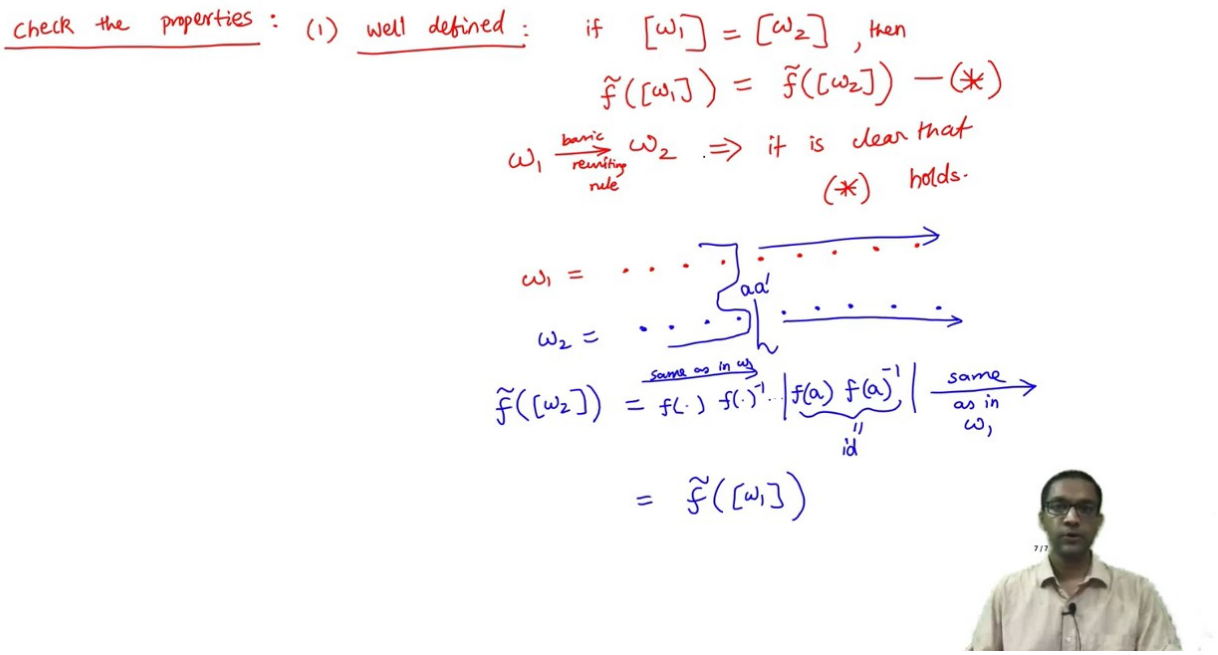
So, you will notice that is what we have done here right all the as have become f as replaceb by f b and if you see an a'you have to replace it by f of a inverse ok. Observe, f of a is an element of K so f of a inverse of course, makes sense it is also an element of the group K and similarly you replace any occurrence of $b'$by f of b inverse again an element of K ok.

Now, replace these and take this product in the same order left to right. So, take the product of those elements. So, take product in the same order . So, notice K may not be in abelian group. So, I cannot change the order of my factors, if I see an a before $a\ b$ then when I apply my $\widetilde{f}$ it should be $f(a)f(b)$, cannot be $f(b)f(a)$ ok.

So, here is the prescription here is my definition of of $\widetilde{f}$ ok. Now, having defined it in this way it is just a question of checking the various properties , so that is the the main definition.

So,let us check the the key properties check properties ok. So, what all will we have to check. Firstly, there is well definedness ok. We have to check well definedness because, remember we have defined $\widetilde{f}$ on the equivalence class of a word $[w]$. So, well definedness just means the following. I need to check the following that if two words $w1$ and $w2$ are equivalent to each other. In other words, if one of them can be obtained from the other by a sequence of rewriting rules . Then, my $\widetilde{f}$ the value on $w1$ will give me the same answer as if I compute it on using $w2$ as my representative ok . And so, let me just sketch the proof again I will leave this as the formal writing as an exercise to you.

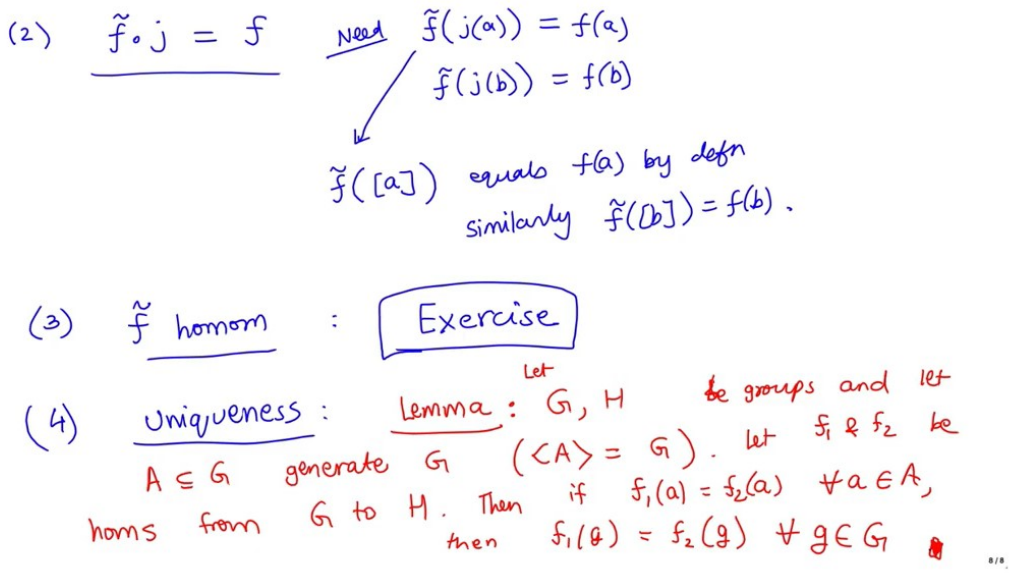
So, observe if $w1$ and $w2$ are just directly related by a basic rewriting rule. Suppose, this is a basic rewriting rule , which means I can get $w2$ from $w1$ in one step by just either inserting



an a a'or $a'a$ or deleting an a a'or $a'a$ or b $b'$and so on, if you can do that in one step then this is this is clear ok. Then, it is clear that they both must have the same $\widetilde{f}$ ok, then it is clear that this equation. So, let us call this equation star it is clear that this equation star holds , why is that because what does $w1$ look like it is a product of a's, b's, a' 's, and b' 's in some order right. Let me assume thatI obtained $w2$ from $w1$ by let us say insertinga pair a a'somewhere ok. So, let us assume this was $w1$ and let us assume $w2$ was the same thing as $w1$ except somewhere here in the middle I inserted an additional a a'ok, the rest is the same .

Now suppose this is how I got $w2$ from $w1$, it is now got length 2 more, but now if you see what our prescription was, how did we compute $\widetilde{f}([w2])$, the definition is you just apply you know you look at each of these dots from left to right if it is an a you replace it with f a, if it is a'you replace it by with f a inverse likewise for b ok. So, you will you will keep scanning it from left to right it will become either f of something or f of something inverse dot dot dot and now so far it will be the same whether you do it on $w2$ or on $w1$ thus far both are going to give you the same answer. The only difference can arise when you see the a a'in w 2, now for thatwhat is the prescription say, when I see an a I am supposed to replace it with an f a, when I see an a'I am supposed to replace it with an f a inverse ok.

So, these are the two extra terms that I get in $w2$ and again the rest of the terms to the right of that are the same in both $w1$ and w 2. So, this part agrees ok . So, these terms are the same as those in w 1, similarly these terms are also the same as in w 1, the extra is only in the middle. But observe the extra is just the product f a times its inverse so of course, that is just the identity element of K. So, this is nothing, but the identity element in K. And so, this product is just going to give you the same terms that you had in in w 1 times identity

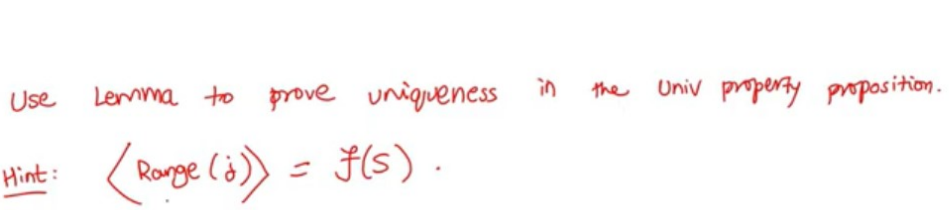


times the same terms that you had in w 1. So, net result is of course, the same answer as what you would have gotten for w 1 ok.

And of course, this is the proof for a single basicrewriting rule, but if it is true when you apply a single rule then of course, it is true even if it is a chain of rules, if you can go from $w1$ to $w2$ by a sequence of steps at each basic step this fact holds that $\widetilde{f}$ gives the same answer. So, of course, even if you have many steps the first beginning and the end of the the stepthey will still have the samevalues of $\widetilde{f}$ ok. So, this is the well definedness . Now,the other properties are also very easy. So, if you show what do we need to show, we need to show that $\widetilde{f} \circ j = f$ that is the important one, but that is obvious because of the way I mean in fact, that was really how we figured out what $\widetilde{f}$ should look like.

So, observe this just means the following I should show that I need to prove this that $\widetilde{f}(j(a)) = f(a)$ and $\widetilde{f}(j(b)) = f(b)$ ok, but this is true because $\widetilde{f}(j(a))$ observe is nothing, but $\widetilde{f}(j(a))$ is just this a by definition right and $\widetilde{f}([a])$ is of course, equal to $f(a)$. So, this equals $f(a)$ by definition and the same holds for f b ok. So, similarly for f b ok. So, that is this property now of course, the other important ones are to show it is a homomorphism ok. So, this one isjust question of figuring out how this works under concatenation.

So, I am going to leave this you as an exercise show that if I take two words $w1$ and $w2$ and try to compute $\widetilde{f}$ on their product, then it will just give me f tilde of the first guy times $\widetilde{f}$ of the second one ok. So, again an easy exercise from the definition and finally, what we need to show. So, with this we are really done with the existence of $\widetilde{f}$ right, we have shown it is a homomorphism, it is well defined, it satisfies the diagram commutes property. Now, what we need to do is really to show uniqueness ok, that there exists a unique $\widetilde{f}$ which satisfieswhich makes a diagram commute which is a group homomorphism . Now, again uniqueness I am I am going to state a little lemma and then let you deduce the uniqueness from that lemma ok.



So, this is a general lemma really about homomorphism between two groups. So, suppose I have two groups G and H ok.

So, let G and H be groups and suppose so well I do not really have anything between them yet let G, H be groups and suppose I have a generating set for G ok. So and let A subset of G generate G . So, again recall; that means, that the subgroup generated by A is going to be the entire group G ok. Now, let suppose I have two homomorphisms. So, let $f1$ and $f2$ be homomorphisms homs from $G \to H$, then if $f1$ and $f2$ agree on A if $f1(a) = f2(a)$ for all $a \in A$, then they agree on all of G then $f1(g) = f2(g)$ for all $g \in G$ ok. So, if I have two homomorphisms which agree on a generating set then they must agree on the whole group ok. So, that is a little lemma. So, the proof of the lemma is also an exercise again a very easy exercise.

Now, what I want you to try and do is to see how this lemma can be used to show a uniqueness ofthe map $\widetilde{f}$ that we have ok. And the the little hint is so use this lemma to prove uniqueness in the in the main proposition in the universal property proposition ok.

And the hint here recall is the hint is the following recall that the range of the map j . So, that is the important thing here , this guy generates the free group this is what we proved first. So, heres a generating set and if two homomorphisms agree on a generating set then they must agree everywhere ok. So, show that for uniqueness what you will have to try and show is that, if I have two homomorphisms $\widetilde{f1}$, $\widetilde{f2}$ both of whichmake the diagram commute then those two homomorphisms agree on the range of j ok and hence by this lemma they agreed together ok ok.

So, we will talk about applications of this this universal property next time .