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

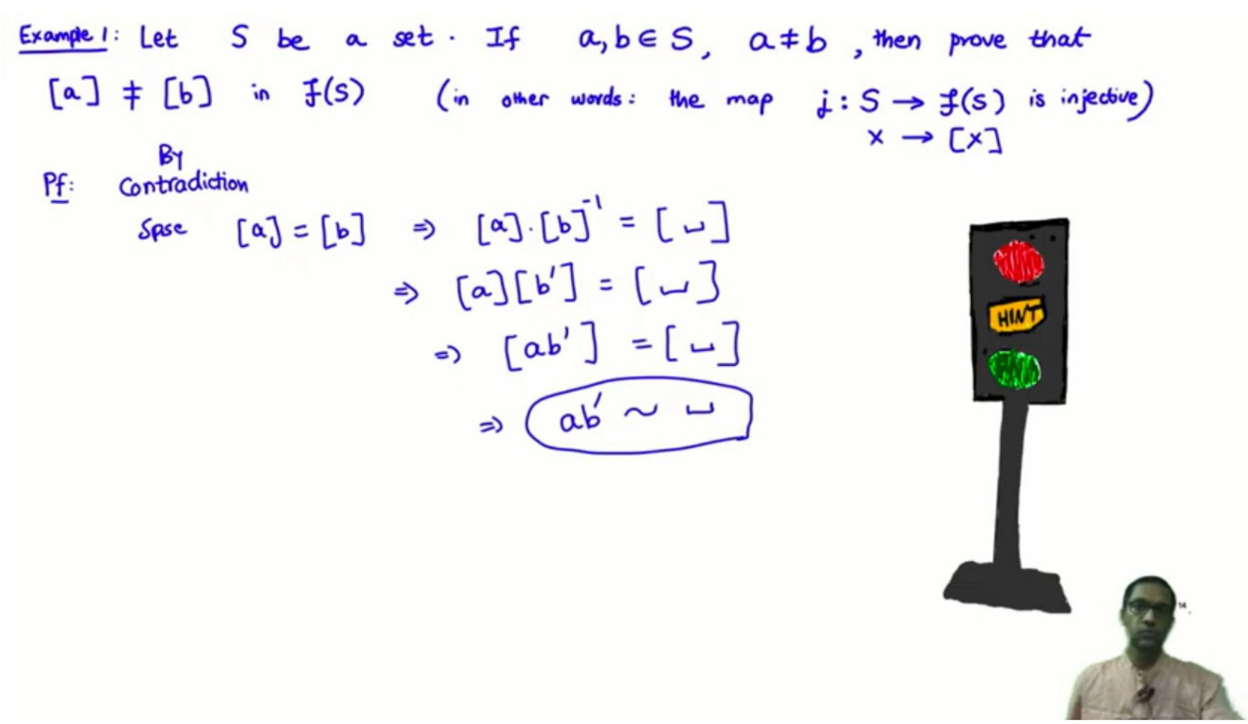
1. Lecture 31 [Problem Solving]

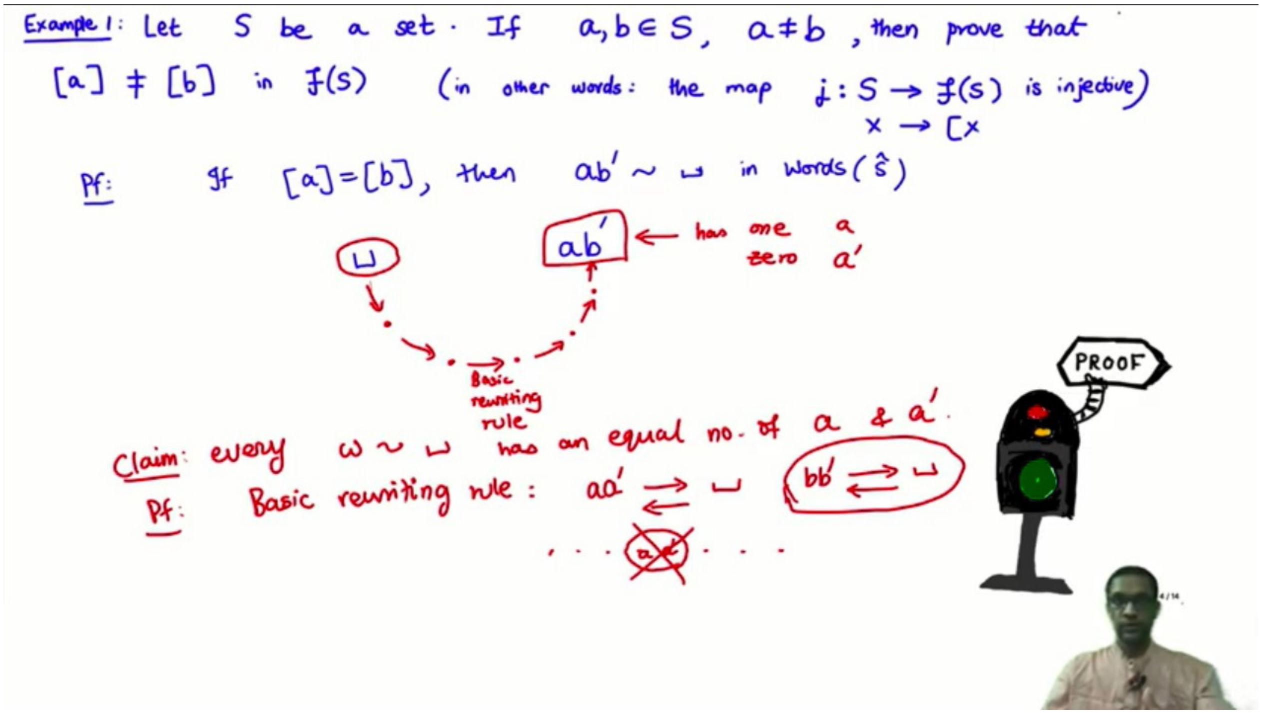
Today, we will talk about some examples and applications of the universal property of free groups ok. So, we will do 4 examples today. So, let me skip to the very first one . So, here is the example or a problem.Let S be a set and if we take two elements a and b in the set which are not equal to each other, then the problem is the following.

Example-1: Let S be a set. If $a, b \in S$, $a \neq b$, then prove that $[a] \neq [b]$ in $F(S)$.

Another way of saying this is that the map $j : S \to F(S)$ that we talked about in the universal property that map is in fact injective. So, this is the map $x \to [x]$ ok. So, at this point those of you who are sort of watching the video,I would encourage you very much to try andyou know try your handed this problem first;but you know maybe pause the video and and try it, but let me go on.

Now,for those who want a little bit more of a hint to you know try this problem, here is the the very first thing. So, observe what is it that we really want to prove. So, we are trying





to prove the following that if I have two elements. So, let us let us proceed by contradiction here.

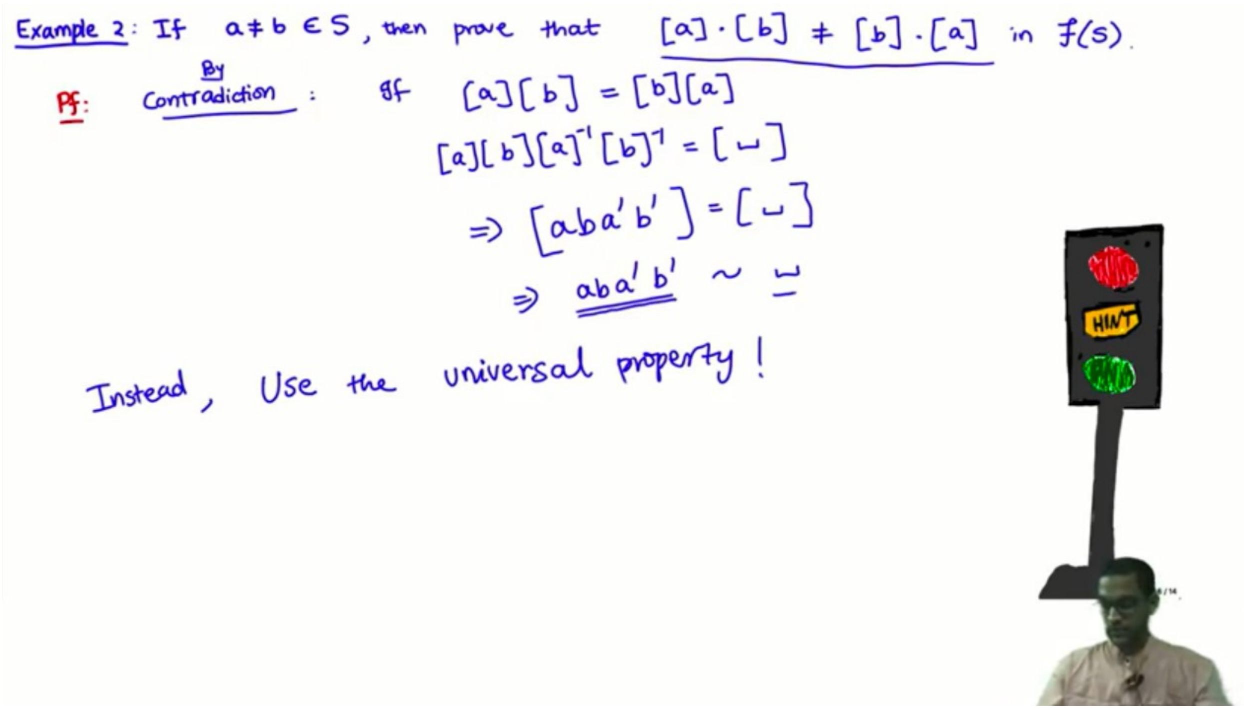
So, supposeone thing we could try is to try an argument by contradiction. So, suppose these two equivalence classes are actually equal to each other in the free group . What is that mean? It means that if we take $[a][b]^{-1} = [\_]$, I should get the identity in the free group ok.

Now, what is that mean? Well, if you recall what the $[b]^{-1}$ was, this is just $[b']$. So, this is the identity and now, this concatenation the product of $[a][b']$ is just the concatenation which is the word $[ab']$ is the identity. So, the final thing that you you really need to do is to derive a contradiction from this fact. So, what do we finally conclude that ab' is equivalent under that rewriting rules equivalence relation to the empty work ok. So, this is the this is what it means forthe equivalence class a and b to be equal to each other ok. So, at this point again those who would like to use this hint to try this problem, I would encourage you to pause the video and sort of try your handed ok.

So,let me move on. So, here sort of the final solution to this problem. So, recall from the hint that this is sort of what we we assumed that weproceed a by contradiction, if we assume that $[a] = [b]$; then, we concluded that $ab' = \_$ ok . So, this is of course, thought of both thought of as words in the augmented alphabet $\widehat{S}$. Now, why is this a contradiction? Where is the contradiction going to come from? So, observe what is this equivalence mean?

So, let me start with the empty word. So, I am saying the empty word is equivalent to the word a b ', which means that from the empty word, I can find a sequence of rewriting steps, basic rewriting steps or a chain which will finally, get me to the word ab' ok .

So, each of these these arrows is a basic rewriting rule, now I claim the following that when you apply a basic rewriting rule tothe empty word, what you get at every step? So, each of



these words here, each of the words in the in the chain has the following property that it has an equal number of a and a' ok; likewise b and b' .

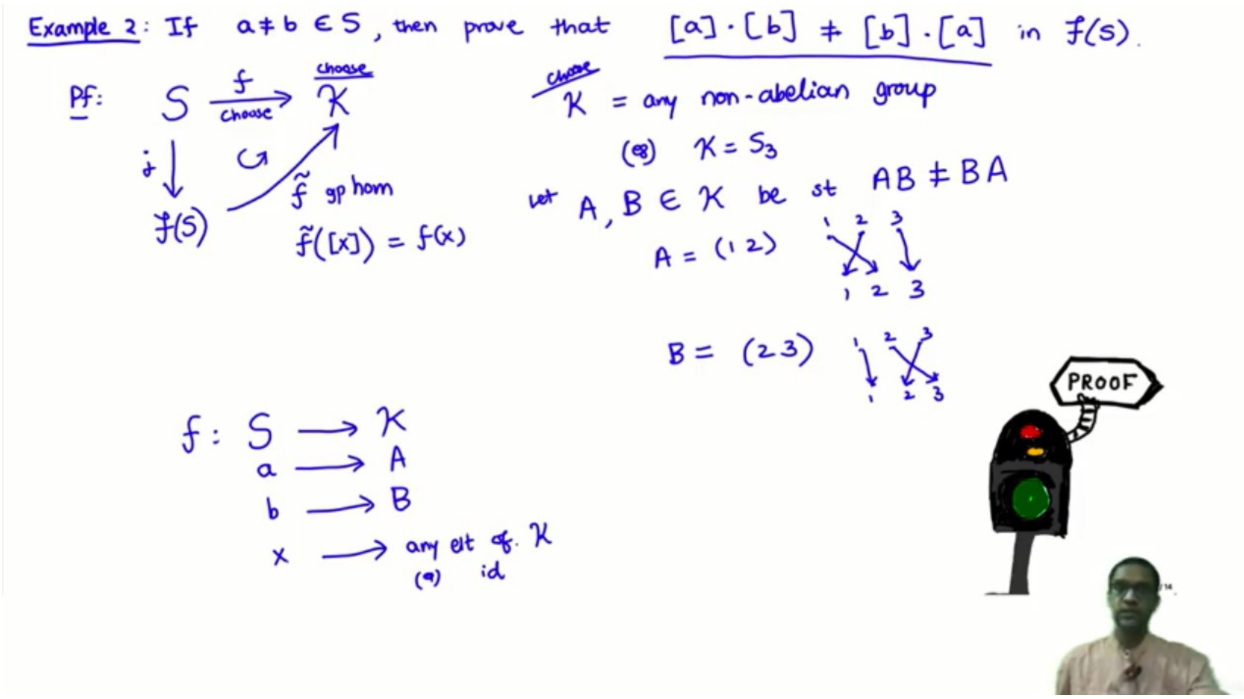
But let us focus on one of the alphabets. So, I claim that every $w = \llcorner\lrcorner$ that is equivalent to the empty word has an equal number of a and a' ok. a and a', there should be an the same number of these two in the word w ok and the proof is well more or less clear, we just have to look at what a basic rewriting ruled as; it either inserts . So, this just follows from what the basic rewriting rules where, it either takes aa', if you have an occurrence of aa', you can replace it by the empty word.

So,or conversely you if you have the empty word, empty sub word you can replace it by aa'. Now, observe that these two processes what happens here is if I have a word. So, so for example, if a word has an equal number of a and a' and I take a sub word, so here is a word .

And let us assume this word has an equal number of a and a' and what this first basically writing rules as says I take say suppose, there is an a and an a dash which occur consecutively. Then, this rule says I am allowed to delete that from my word to obtain my new word right. Now, if my original word had say 10 a and 10 a', then the new word will have 9 a and 9 a'. So, it will continue to have an equal number of a and a' ok.

Now, the other rewriting rules even simpler; it says I can either replace bb' by the empty word or the empty word by bb dash. Here,since I am only focusing on the alphabet a, if my word has some number of a and a' and suppose, I apply this rewriting rule.

Then, the number of a and a' in the in the new word does not change because all I am doing here is taking a bb dash and making itempty or taking the empty word and making it bb' ok. So, I would encourage you to play with some examples to get a an actual idea of what we are doing. So, the key point here is that if you take the empty word and no matter which one of the basic rewriting rules you you apply and you keep applying it successively.



At every step, the number of every word you get has the following important property that the number of a and a' in that word are equal to each other ok. Now, that automatically implies that in this chain you cannot finally end up with this word ab' ok; why?

Because this final word that we have, it has one occurrence of a and 0 occurrences of a' right. So, this word has an unequal number of a and a'. So, this word could not possibly have arisen from a sequence of basic rewriting rules applied to the empty word ok.

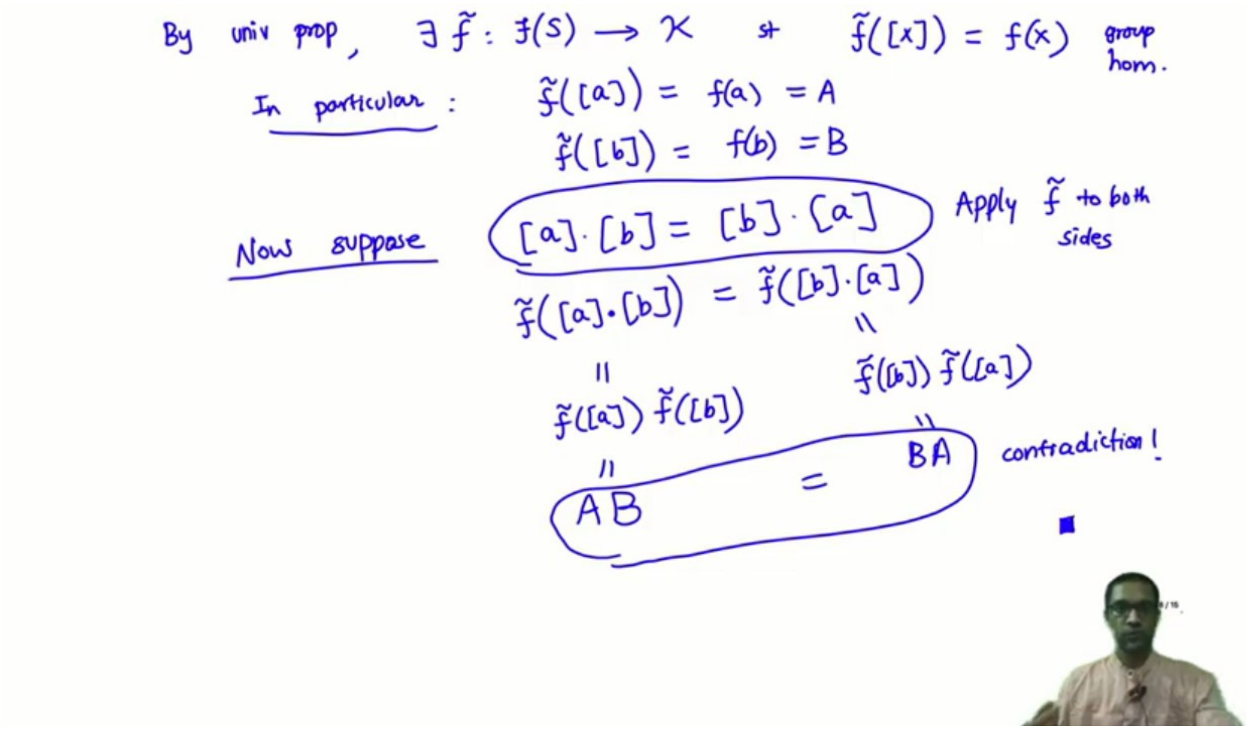
So, that is the the first example. So, this was a simple enough thing, we were just trying to understand what basic rewriting rules do to the number of a's and a dashes and in fact, this is related to the example in one of our earlier videos in which we said the free group on a single alphabet, single letter is isomorphic to the group of integers and if you remember the homomorphism there was just given a word, you associate to it, the $a - a'$ and this is more or less the same idea ok.

So, let us move on to the the second example.

Example-2: If $a \neq b \in S$, then prove that $[a][b] \neq [a][b]$ in $F(S)$.

So, I hope the question is clear. If we take two elements of S which are not equal, then the corresponding elements in in the free group, the the equivalence classes of a and b do not commute with each other and again, this is a good place to stop and stop the video and sort of try your hand at this problem. So, I would very much encourage you to do that ok. Now, here is a hint. So, let us sort of proceed the way we did earlier, which is to try and see what we can get by a contradiction argument. Suppose, we we proceed by contradiction . So, let us do contradiction .

So, suppose, we assume that $[a][b] = [b][a]$ ok. Then, by the same reasoning as before, the left hand side is $[a][b]$, the equivalence class of the word ab; the right hand side is the



equivalence class of the word ba and if those two equivalence classes are the same, it means ab and ba are equal to each other or are equivalent each other.

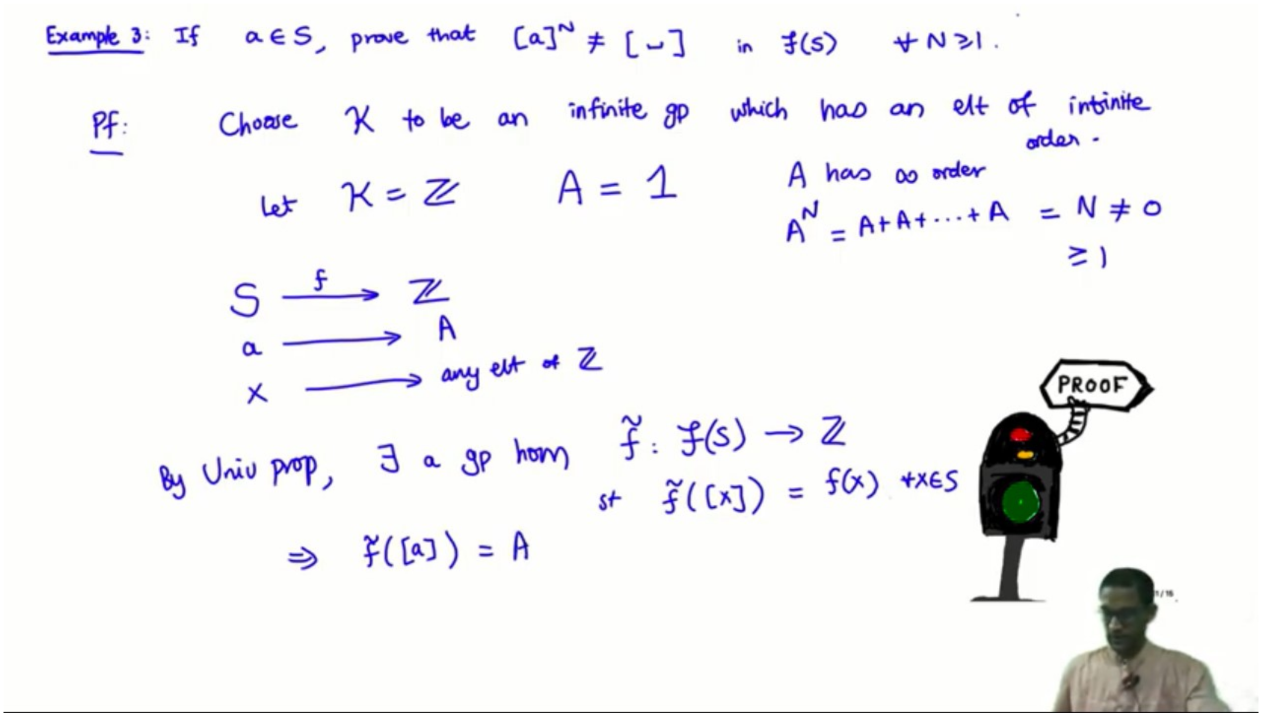
In fact, we can sort of do the same thing that we did before, since I have rewriting it in this way. Let me do what I did to the earlier problem which is sorry if a b equals b a let me do it in the next step.

ah I can replace the right hand side, I I put them both onto the left hand side as inverses. So, this means $[a][b][a]^{-1}[b]^{-1}$ is the identity ok. And now, again as before $[a]^{-1}$ and $[b]^{-1}$ are just the equivalence classes of the words a' and b'. So, this means that this is the identity and that in turn implies that $aba'b'$ is equivalent to the empty word ok.

So, we are sort of in a similar situation as an example one, we have a word which is equivalent to the empty word ok. But observe unlike the earlier example, we do not get an automatic contradiction. Because this word here $aba'b'$ has an equal number of a's and a'; it has one a and one a', it has one b and one b' ok. So, at least it satisfies that primary requirement for a word to b e equivalent to to the empty words. It is a necessary condition, b ut we still somehow need to get a contradiction out of this ok. So, we will turn out we have to prove that this cannot b e the case that a b a $'$ b $'$ cannot b e equivalent to the empty word ok and since, what I am trying to do here is to give you a hint to do this problem. Use instead, so here is the way to proceed. We will use the universal property ok.

So, try to come up with a way of using the universal property of free groups to prove that a b a $'$ b $'$ cannot b e equivalent to the the to the empty word or equivalently, that a b cannot b e the same as b , I mean whatever we need to prove ok. So, let me move on to the solution next. Again, I would encourage everyone to pause here and try your handwritten ok.

So, here is the here is the proof which uses a very nice application of the universal property . So, what we do is the following. So, recall what does the universal property look like? It says the following, take any group K. So, what all do you have to choose? You must choose



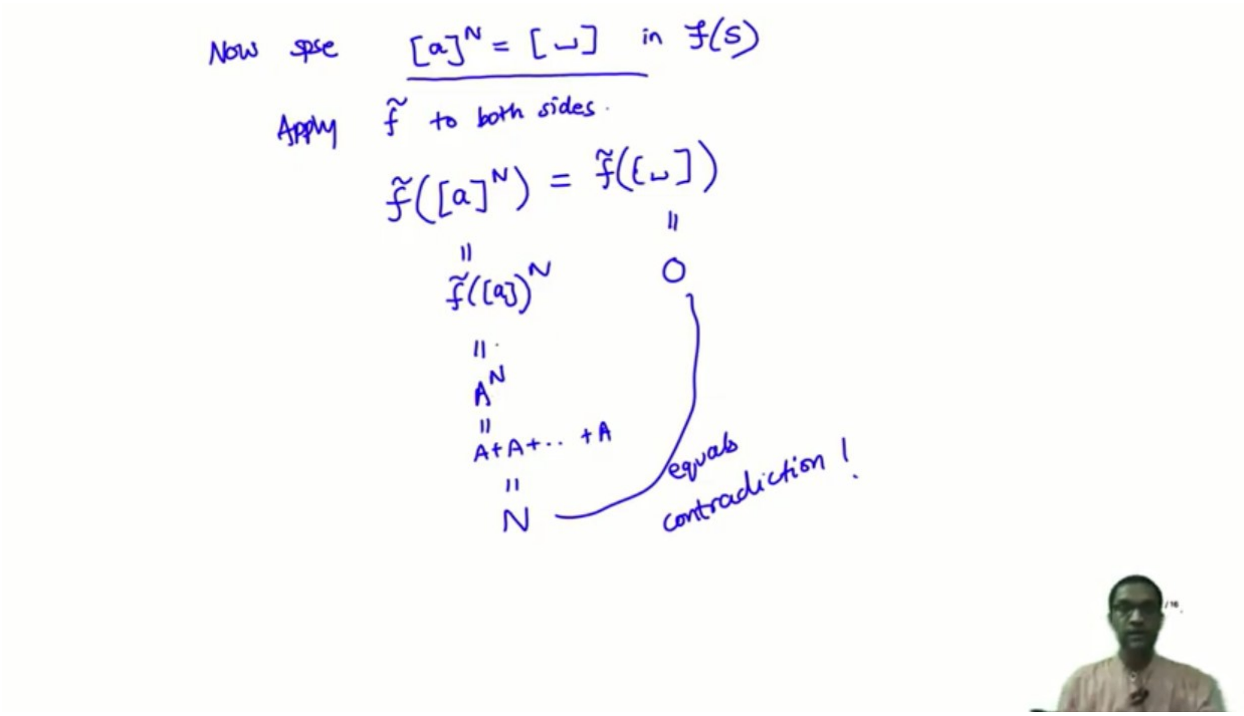
a group K and you must choose *a* map. This is another choice here, you must choose *a* function any set map from the set $f : S \to K$ ok.

So, you choose these two things K and f and having done that, what the universal property says is I have *a* map from the free group to K. It is *a* group homomorphism. So, main property is it is *a* group homomorphism ok and further, $widetilde f$ has its related to f in the following way $widetilde f(j(x)) = f(x)$.

In other words, the diagram commutes right. So, this is diagram commutes that was what the universal property say and there is *a* uniqueness as well which we won $'$ t really need in this example ok. So, if you choose K and f, cleverly enough you should be able to prove what we need to prove, in this case that these two are not the same ok. So, let us do that. Let us make the following choices. So, for K, I will choose K to be any non-abelian group ok. So, let us pick *a* non-abelian group and well, what is one of the easiest examples, well you can pick K to be say the symmetric group S_3 ok.

So, for concreteness, let us pick an actual group. I take K to be S_3 is *a* symmetric group ok. Now, I need to define my map f. So, to define my map f, let me pick the following. I will pick two auxiliary elements. So, I have *a* non-abelian group K. Now. let me pick two elements A and B from this group K. Let $A, B \in K$; be non-commuting, be such that $AB \neq BA$. So, I have picked *a* group S_3 and now, I have to pick two non commuting elements from this group. So, let me pick them as follows. So, I take A to be the two cycle which means it is; so, it written in cycle notation, it is (12) and if you recall or *a* notation in terms of permutations, its 1 2 3, 1 2 3. So, one it is *a* *b* ijection of the set 1 2 3; 1 goes to 2, 2 goes to 1 and 3 goes to 3. So, this is the permutation A.

The permutation B is *a* similar thing its (23). So, again in terms of our diagram it is 2 and 3 are exchanged and 1 goes to 2 ok. So, 1 2 3; 1 2 3 ok. So, that is the definition of A and



B. Now, having chosen these two non commuting elements, let us define this this function f next . So, what is f? f is as follows from the set $S \to K$.

So, S has these two distinguished elements a and b . So, let me map $a \to A$, this element here; $b \to B$ ok and of course, there are lots of other elements potentially in S and I do not really care what I do to them. So, I I can send them to any element you know to different elements even of K. So, I can send each of them to any element of K ok. So, if you want something concrete example, I can take I can send all of them to the identity of K if you wish ok.

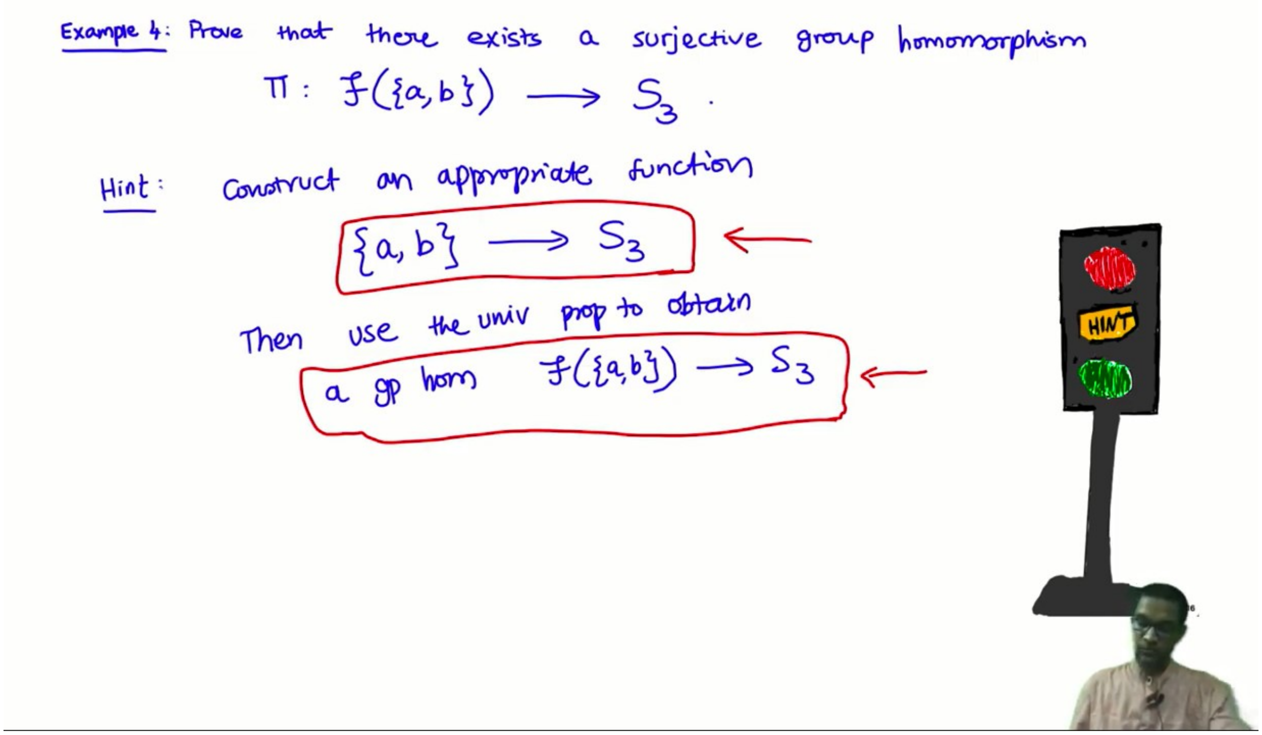
So, this choice really does not matter, you can do what you want ok. So, I hope this is clear so far. I picked the group of, in general I can pick any non-abelian group, I can pick any two non commuting elements a and b in that non non-abelian group and I will define my function f to *b*e the one which sends small $a \to A$, small $b \to B$ and it it does whatever it wants to the remaining elements of myself ok.

So, having done this, let us see where does that put us the universal property now says *b*y the universal property of free groups, we conclude that there is *a* map $widetildef$ group homomorphism from the free group to the group K satisfying the following property that $widetildef$ maps the equivalence class of $[x]$ to whatever f does to x ok.

Now, in particular so this is the important property here, it is *a* group homomorphism. Now, in particular, let me see what ; so, I will take x to *b*e a and b those two specific elements. So, $widetildef([a]) = f(a) = A$ $widetildef([b]) = f(b) = B$.

Now, let us apply let us get our contradiction. Let us go *b*ack to the original question. Now, suppose it were true that $[a][b] = [b][a]$, we will see how our map $widetildef$ is going to help us. Let us do the following. Let us apply $widetildef$ to *b*oth sides ok.

So, these these two elements here, I mean these two sides of the equality, they are *b*oth elements of the free group. I apply the homomorphism $widetildef$ to each of them. So,



$widetildef$ will take the left hand side to an element of K and the right hand side to an element of K. So, let us see what is $widetildef$ of of the left hand side. So, ok; so, I am going to apply $widetildef$ to both sides and this is what I get.

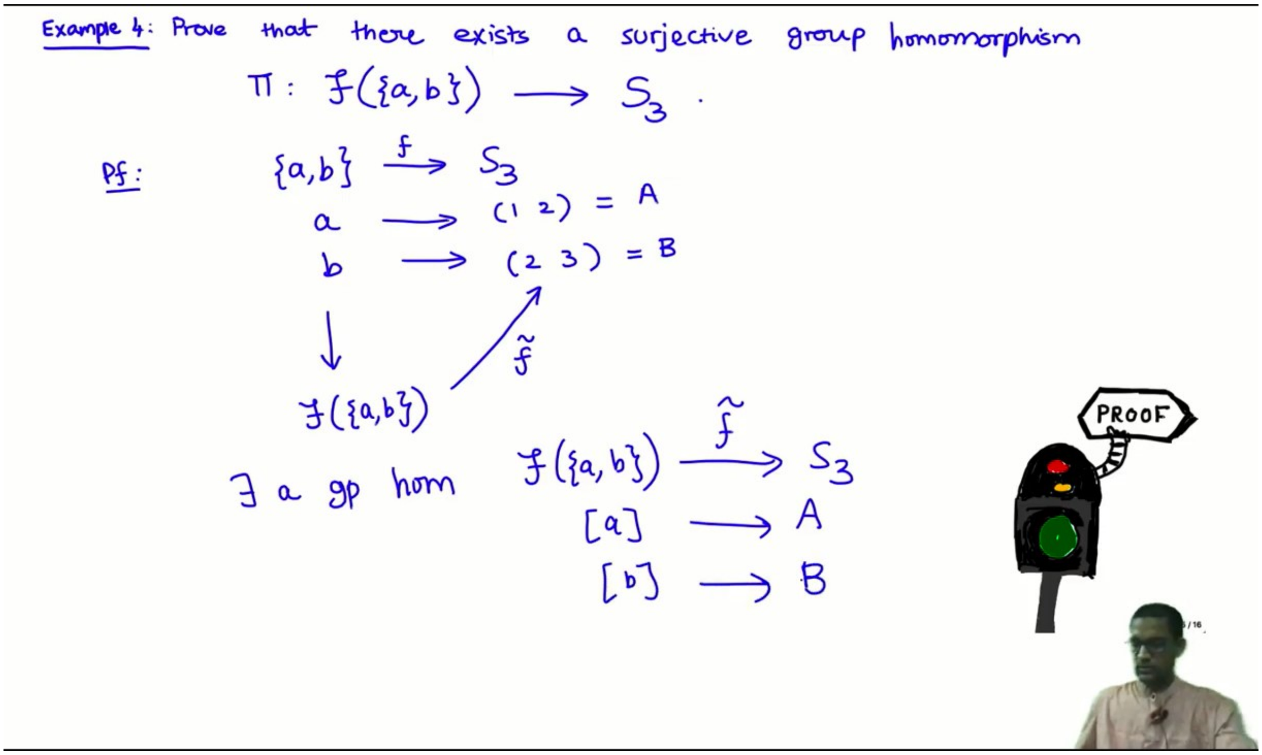
And now, comes the important thing remember $widetildef$ also homomorphism ok and this is now a product of elements. So, this is going to be $widetildef([a])widetildef([b])$ and that of course, by choice is AB. If you do it to the other side, it is going to give you $widetildef([b])widetildef([a])$ and that of course, by choice is BA. ok. So, what do we conclude, if this equality holds; then, it must also be true that AB is the same as BA ok. But that is a contradiction $b$ecause we specifically chose two elements A and B which are a non commuting ok.

So, in some sense the so that completes this proof here. In some sense, the $b$road idea of of these sorts of proofs is the following. Any property that you want to show holds in the free group for example, that a and b do not commute, you try and and produce a concrete group in which you and certain elements in that concrete group which do not have that property ok.

So, I have to show if if I have a show for example, the $AB \neq BA$ one way of doing it is this we know find a group in which there are two elements a and b , where AB is not equal to BA and then, you know you just map these elements small a and small b to capital A and capital B ok . So, we will we will see another example of this kind and hopefully, things will b ecome clearer.

Example-3: If $a \in S$, prove that $[a]^N \neq [\_\_]$ in $F(S), \forall N \geq 1$.

in other words, the element a is not a finite order claim is it as infinite order ok and again, pause the video, think about it .



And in this case, the hint is well the same thing use the universal property ok and sort of study how example two worked ok and see if you can prove this in a similar way ok.

Moving on, so here is the the proof. Again, similarly, I just need to pick a group K . So, I choose K to be an infinite group, to *b*e an infinite group which has an element of infinite order ok, which has an element of infinite order .

And it can *b*e this general if you want, *b*ut let us let us *b*e very concrete here suppose I take K to *b*e, so let me choose K to *b*e the group of integers under addition and let me take an element of infinite order in this group . So, I will take A to *b*e the number 1 ok. So, observe that this number A has infinite order has infinite order *b*ecause you know what what is A^N in this group?

Well, $A^N = A + A + A + ... + A$ because the operation is just addition. In that by definition, its $1 + 1 + 1 + ... + 1$ N times which is the number N ok and the number N can never equal to 0 which is the the additive identity in the group set right. So, one the element one inside has infinite order ok. So, we have found *a* group with an element of infinite order and now, let us just use the the universal property as follows.

So, I take my set S and to the group K, I define my function f as follows. This special element a that I am looking at, I will map it to this element of infinite order and all the other elements, I do not really care. I can map it to any elements of I mean different elements of $\mathbb{Z}$, different x ′ s can map to different elements for example ok.

So, I do not care about the rest. So, I define *a* function $\widehat{f} : F(S) \rightarrow \mathbb{Z}$ and by the universal property, what does that give me it gives me there exists *a* group homomorphism $\widetilde{f}$ from the free group to Z such that $\widetilde{f}([x]) = f(x)$ for all $x \in S$.

And as you can imagine in particular, all we are going to do is just take this particular value of x which is a . So, in particular, if I look at $\widetilde{f}([a]) = A$, this is going to give me capital A ok . And now, we will derive the contradiction in much the same way that that we did earlier as follows.

So, now, for the contradiction. Now, suppose $[a]^N = [\_\_]$ in the free group and let us do the following. We will apply $\widetilde{f}$ to $b$oth sides ok. Now, $\widetilde{f}$ on the left hand side, again we have to use the fact that $\widetilde{f}$ as a homomorphism . So, $\widetilde{f}([a]^N) = \widetilde{f}([\_\_])$. Now, on the left hand side $\widetilde{f}([a])^N$ because it is a homomorphism is the same as $\widetilde{f}$ of a whole thing power N which in turn is just A power N ok; where this is of course, the operation in the . So, this is 0 in Z. So, this is the the the operation in if you wish the the operation of the integers.

So, this is actually ok. So, let us let us do it this way $A^N = A + A + ... + A$ N times which $b$ecause A is 1, this is just the number N ok and now, here is your contradiction. So, what we are really using here is that the element A has infinite order, it cannot have finite order.

So, the contradiction now is this. So, we have shown that N equal 0 ok and that is a contradiction ok. So, we have proceeded b y contradiction, we have assumed that the element a has finite order and concluded that this element capital A would have to have finite order and that is the contradiction ok. So, now for the last example:

Example-4: Prove that there exist a surjective group homomorphism $\Pi : F(\{a, b\}) \to S_3$.

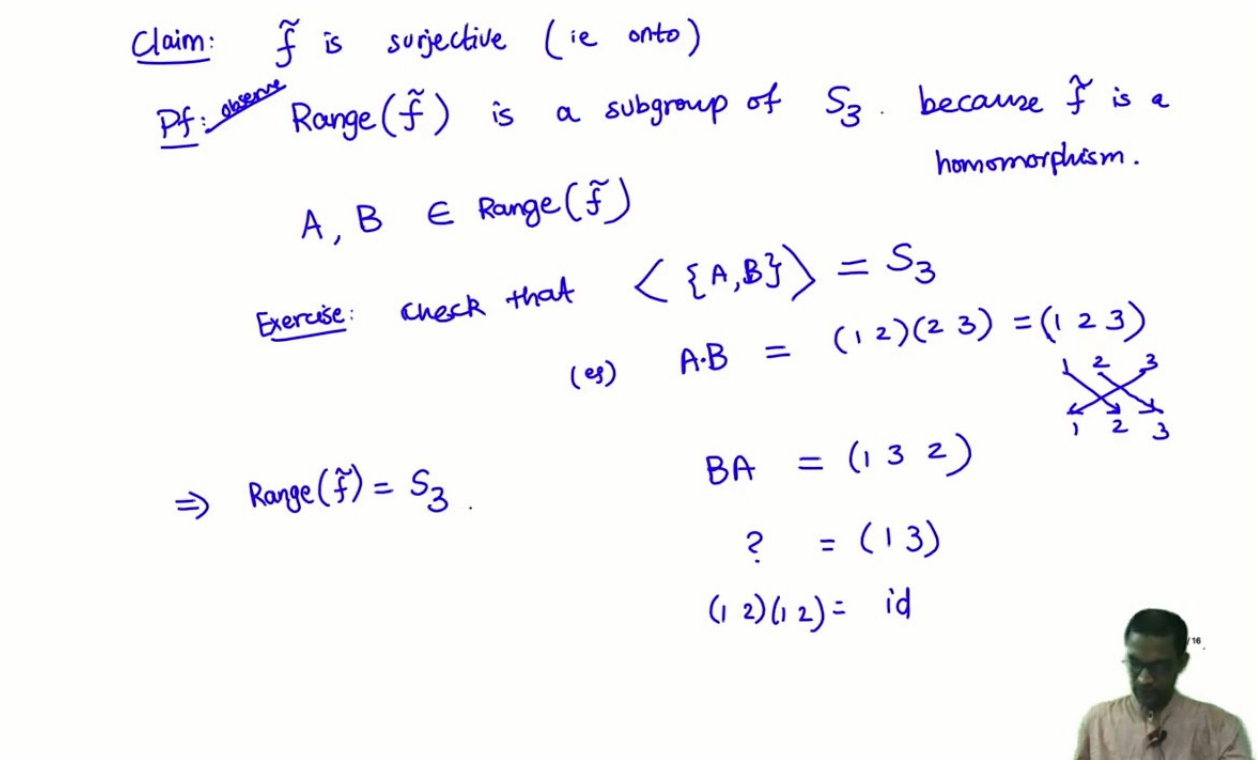
So, again think about it, pause the video here. Now, here is a hint how do you construct homomorphisms from free groups. So, hint how does one construct homomorphisms from free groups to other groups? Well, all you have to do is to just construct just to set map construct an appropriate function from just the set $\{a, b\} \to S_3$. It is just it has no additional property; it is just a function. If you construct an appropriate function, then use the universal property; use the universal property to obtain a group homomorphism from the free group ok. So, in some sense, a group homomorphism from the free group to another group, this information is really in some sense the same information as just map of sets from the set $\{a, b\} \to S_3$ ok.

So, if you are asked to construct this guy, then it sort of enough to construct the guy on top ok. Of course, you should do it in such a way that the the resulting homomorphism has the properties you want ok. So, focus on this, try to find an appropriate function from the set $\{a, b\} \to S_3$ ok . So, again pause and think about it using this hint .

Now here is the the solution proof. So, let us do the following. So, let us construct a function from $f : \{a, b\} \to S_3$ first. let me say a and b . So, let us do the following; let me map $a \to (12)$ and $b \to (23)$ ok. These were the very same two things that we call capital $A = (12)$ and capital $B = (23)$ in example 2 ok .

So, let me map a in b to these two guys and let me look at the the let us call this f and let us use the universal property. This therefore, induces a group homomorphism from here to S_3 which is called $\widetilde{f}$ ok . So, there exists a group homomorphism from the free group to S_3. Let us call this $\widetilde{f}$ and what does this guy do? It sends $a \to A$ and $b \to B$ ok. So, I know the existence of this by means of the universal property. Now, here is the important thing our claim is that this is the map we want; claim $\widetilde{f}$ is surjective. So, recall surjective just means on to. So, we claim $\widetilde{f}$ is an onto function ok. Why should $\widetilde{f}$ be onto?

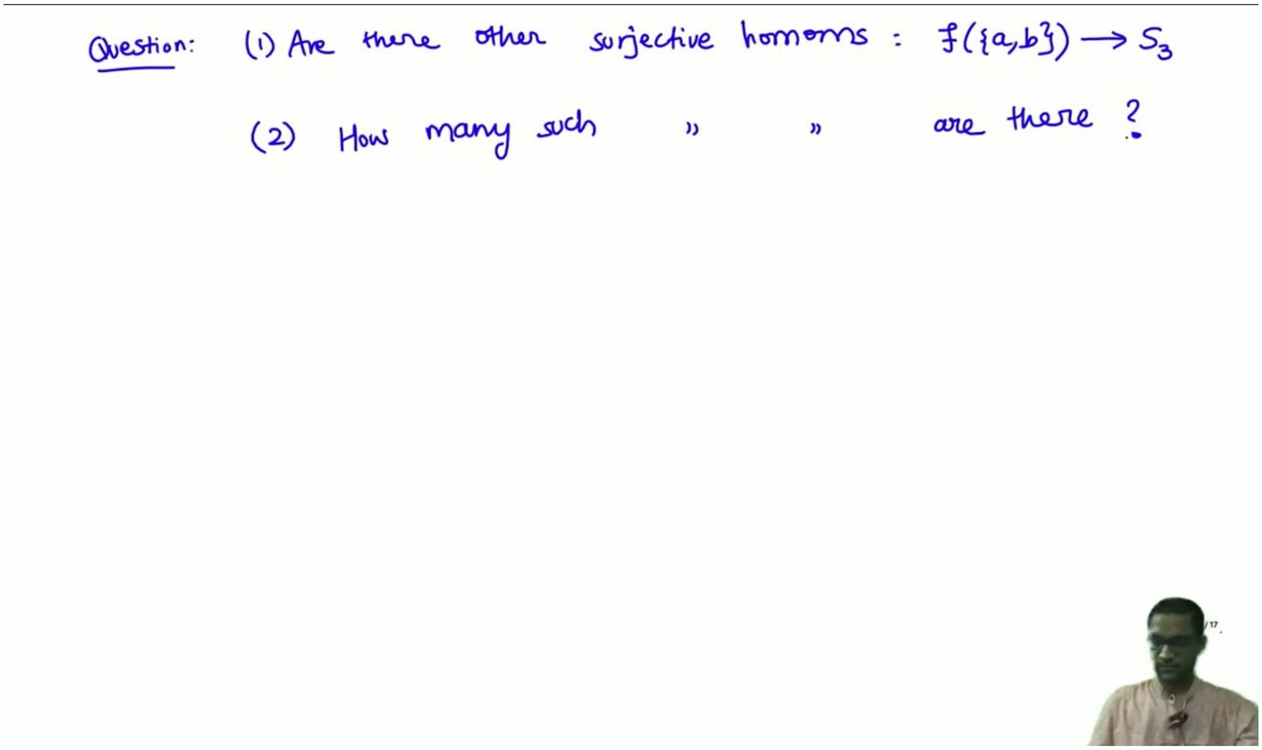
Well, here is what we know, what does it mean to say that $\widetilde{f}$ was onto? It means at the range of $\widetilde{f}$ is the entire group S_3 ok, b ut observe here is what we know about the range



at least. So, observe that b ecause $\widetilde{f}$ is a homomorphism, the range of $\widetilde{f}$, the range of homomorphism is always a subgroup; it is the subgroup of the the group on the right the co-domain ok. So, if I have a homomorphism $b$ecause $\widetilde{f}$ is a homomorphism ok. So, a simple exercise if you have not seen this b efore. Now, what more do we know? We know that this element capital A and capital B, $b$oth $b$elong to the range ok. So, the range is a subgroup of S_3, it contains capital A and capital B, well then all you have to check is that you can it it has to contain all the other elements of S_3 as well. In other words, I can get every other element of S_3 by sort of taking products for example of of elements a and b ok .

So, well, let me leave that little b it as an exercise. So, exercise check that well another way of saying it is that the subgroup generated by capital A and capital B in S_3, the subgroup of S_3 generated by these two elements is actually the entire group S_3 ok and how do we how do we check this? Well, you you sort of have to keep taking various products and so on to see that you get every element. So, here is one example if I take $AB = (12)(23)$, then you know we just have to check using the the diagrams for example. What this does is so the it is a composition of these two maps. So, 2 goes to 3 under the second map; 3 goes to itself. So, this is 2 goes to 3. So, I claim this is just a three cycle, 1 2 3. In other words, this is the map, it sends 1 goes to 2, 2 goes to 3 and 3 goes to 1.

So, it is this cycle ok. Similarly, if you if you sort of look at BA, then you will get (123) and you know you sort of have to see what you will do to get the other element. So, here is a little exercise what products of a $'$ s and b $'$ s will give you the the element $(13) \in S_3$ ok. So, the identities similarly, how will you get identity if you wish? Try write in terms of a. Well, identity is easy I suppose, you can just say identity is a square in other words, I just take a with itself what I get is the identity ok.



So, this just is another way of saying that every element of S_3 is in the subgroup generated *b* y these two elements capital A and capital B . So, of course, this means that the range has to *b* e the entire group S_3 ok. So, that completes the proof. So, we have we have used the universal property to construct *a* map and then, we have shown that this map has full range ok. Now, here is *a* sort of some additional questions for you to think about is there any other such function or are there other other such functions. Are there other surjective homomorphisms from the free group onto generate to S_3?

So, we we constructed one, *b*ut are there other other way of constructing them and maybe sort of related, *b*ut maybe slightly harder question. How many such homomorphisms are there? How many such surjective homomorphisms are there ok? It is *a* finite number ok, there are only finitely many of them. Your task is to try and find out exactly how many there are ok. So, we will stop here .