

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

1. LECTURE 28 [FREE GROUPS IIB]

Now, the key thing that one needs to prove is really well definedness ok. The key point here is that this definition is well defined and why does one need to worry about that because we are picking representatives from these classes  $w_1$  and  $w_2$  if .

So, its not a priori clear that suppose I changed my representative. So, here is what we will need to show what if I pick different representatives. So, if  $x_1$  is another representative it belongs to this equivalence class ok and I pick a different representative  $x_2$  from the equivalence class  $[w_2]$  ok. Then so, what does that mean? I have instead of taking  $w_1$  as my representative I am thinking of  $x_1$  as my representative of that class and similarly ok. So, I am I am changing my representative then. So, suppose I do this, then I need to show that my right hand side will be the same answer whether I do  $[w_1 * w_2]$  and take the concatenation or I take  $[x_1 * x_2]$  and and take their concatenation, the answers should be the same. its ok. Then um we need ok we must show that  $x_1 * x_2$  the equivalence class is the same answer as what you would get if you took  $w_1 * w_2$  ok. So, this is what showing well definedness

Proposition:  $G$  has a well-defined binary operation given by

$$[w_1] \cdot [w_2] := [w_1 * w_2]$$

Proof: Need to show:  $\forall x_1 \in [w_1] \quad \& \quad x_2 \in [w_2]$

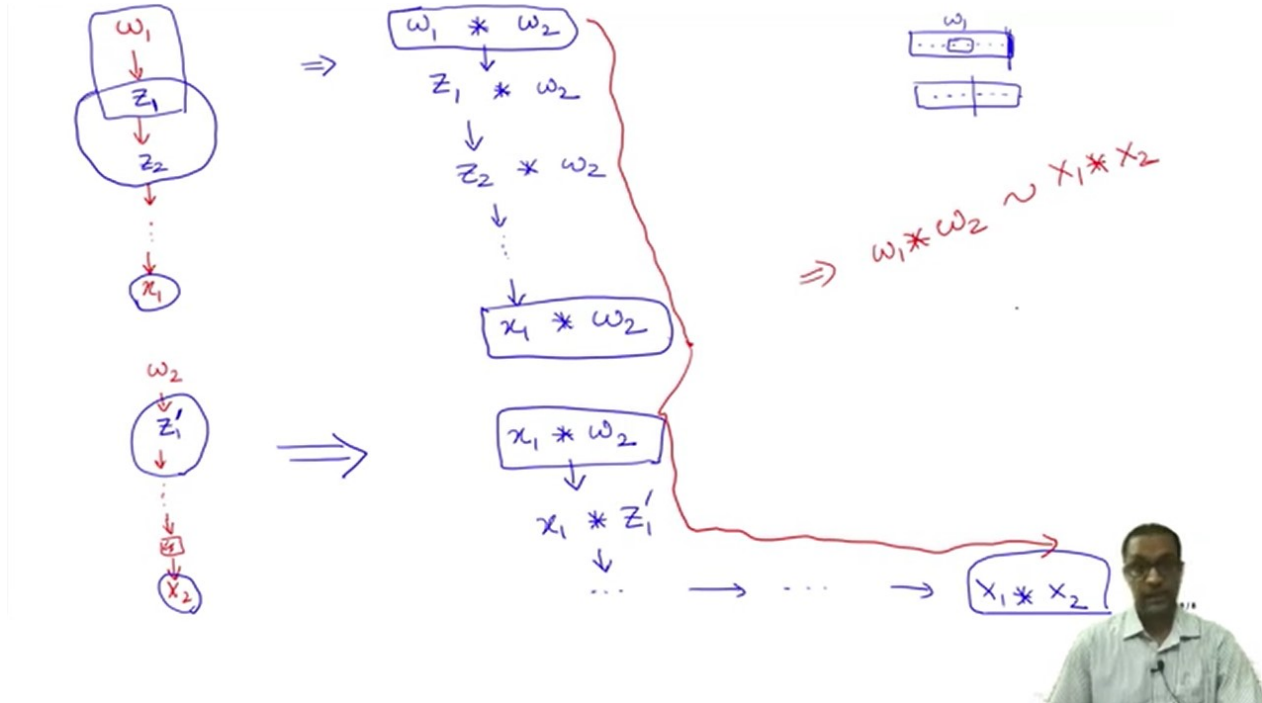
(i.e.),  $[w_1] = [x_1] \quad , \quad [w_2] = [x_2] .$

Then: we must show:  $[x_1 * x_2] = [w_1 * w_2]$

Given:  $x_1 \sim w_1 \quad \& \quad x_2 \sim w_2$

Need:  $x_1 * x_2 \sim w_1 * w_2$





means ok. So, let us prove this. Again it comes about from the special way in which the equivalence class or the equivalence relation was defined.

So, observe what are we given we given that  $x_1$  and  $w_1$  are equivalent to each other. So, let us prove this given what is given is the following these two are equivalent and what we need to prove is that the concatenations are equivalent  $x_1 * x_2 \sim w_1 * w_2$  ok. So, what is equivalent mean? It means there is a chain starting with  $w_1$  ending at  $x_1$  in which each intermediate step is obtained from the preceding one by an application of a basic rewriting rule ok.

So, let us write that down. So, step 1; I started  $w_1$  ok and I use my basic rewriting rule, I get some word, I use again one of the other rules it becomes some other word, etcetera etcetera till I finally, am able to reach  $x_1$  ok. This is what it means to say  $w_1$  and  $x_1$  are equivalent to each other ok. Similarly, I have  $w_2$  and  $x_2$ . So, I can start at  $w_2$ , I can follow my rules successively till I reach well ok. So, that is what the definition says.

Now, given this we need to show that if it start with  $w_1 * w_2$ , I can reach  $x_1 * x_2$  by means of my basic rewriting rules ok. Now, the way we do this is just via this simple observation that look at this this initial chain, starting from  $w_1$  and going to  $x_1$ . What does the basic rewriting rule do? The basic rewriting rule has the following form. So, for instance if this is my word  $w_1$ , I look through the letters in  $w_1$ , I either find a successive pair of the form  $aa'$  etcetera which I delete or I take my word  $w_1$ . I look through the letters, I pick some position and there I insert a pair  $aa'$  ok. So, the transformation that I perform has this very specific form. You either collapse or you sort of expand at a certain location in the word.

So, if I go from let us look at the very first step of the chain I go from  $w_1$  to whatever is the next word in the sequence by means of some basic rewriting rule then here is what it means, it means that look at  $w_1$  and the next guy. Now, to  $w_1$  on the right hand side, I can


Theorem:  $G$  is a group

Pf: a)  $\cdot$  is associative

$$\begin{aligned}
 ([w_1] \cdot [w_2]) \cdot [w_3] &= [w_1 * w_2] \cdot [w_3] \\
 &= [(w_1 * w_2) * w_3] \\
 &= [w_1 * (w_2 * w_3)] \\
 &= [w_1] \cdot ([w_2] \cdot [w_3])
 \end{aligned}$$

b) Identity  
 $e = [ ]$   
 $[w] \cdot [ ] = [w * ] = [w] = [ ] \cdot [w]$

c) Inverses exist!  
 $[a] \cdot [ \dots ] = [ ]$



let me try doing this. Let me concatenate  $w_1$  on the right hand side with the word  $w_2$  ok and the next step in the chain I will do the same thing to it. I concatenate  $w_2$  to that word.

Now, if this second guy can be obtained from the first one by some basic rewriting rule, then it follows that  $w_1 * w_2$  will lead to that word  $x_1 * w_2$  ok. I can take the second guy and I do  $w_2$  to it. So, maybe I should give this give this a name. So, this intermediate step suppose, I call it  $z_1$  that is my word, then here is what I mean that if from  $w_1$  to  $z_1$  I can go by means of a basic rewriting rule. I can also go from  $w_1 * w_2 \rightarrow z_1 * w_2$  by the same rule really ok, because I only need to apply that rule to the  $w_1$  portion of my word now and so on.

So, the next step again, because I can go from  $z_1$  to the next fellow  $z_2$  by means of some rule, it means I can also go from  $z_1 * w_2 \rightarrow z_2 * w_2$  by using the same rule, but only applying into the  $z_1$  portion and so on ok. So, keep doing this till you reach the end. So, the end here is  $x_1$ , but of course, remember I have starred every one of them with the  $w_2$  ok.

So, I have started at  $w_1 * w_2$  which is what I need to start with ok. So, we have managed to go from  $w_1 * w_2$  which is what we wanted, but we have only reached  $x_1 * w_2$  ok, but that is already a very good start, because now we do the same thing with the with the other sequence. We know that we can start at  $w_2$  and reach  $x_1$ . So, now let us do the same thing here this implies. Now, I will sort of concatenate on the left of  $w_2$ . So, starting at at  $w_2$ , I can reach the next step whatever this this word is. So, let us call this  $z'_1$  now, what I do is to concatenate  $x_1$  on the left of  $w_2$  and, because I can go from  $w_2 \rightarrow z'_1$  it also implies that I can go from  $x_1 * w_2 \rightarrow x_1 * z'_1$  in the same manner and you know by the same logic as before.

So, I keep applying it to the next um to the next step of the chain and so on. So, I keep doing this till I reach the very last step and the last step is  $x_2$ , but concatenated on the left by  $x_1$  ok. So, what this means is if I start at  $x_1 * w_2$  by applying left concatenation to the

second chain I can reach  $x_1 * x_2$  ok. So, now I just put these together. So, what have I managed to do? I have managed to start at  $w_1 * w_2$ . I am following this chain of rewriting rules. So, at this point this and this are the same now I follow after that this chain of rules and finally, I reach my destination ok. So, what this means is that  $w_1 * w_2$  is in fact, equivalent to  $x_1 * x_2$  ok as required. So, what this means is that my um on my group  $G$  or at the moment my set  $G$  the um binary operation that have defined is at least it it makes sense its well defined ok, but we called it  $G$  for a reason we are going to make this into a group .

We are going to show that it actually becomes a group under this operation and that is really our our in some sense our main theorem that is going to be the free group. So,  $G$  is a group under the binary operation that we just defined ok proof well what all do we need to show we need to show that the binary operation is associative ok. Why is it associative? So, will show that first observe the definition said if I take  $[w_1]$  multiplied by  $[w_2]$  ok, let us just write out the definition of associativity here. This by definition is  $[w_1 * w_2]$  the equivalence class of the concatenation multiplied by the equivalence class of  $[w_3]$  ok which by definition again is the equivalence class of  $[(w_1 * w_2) * w_3]$  ok.

But observe that the what is inside, the representative of the class that I get here is just the concatenation of these three guys  $[w_1 * (w_2 * w_3)]$  and the concatenation operation is of course, associative. So, I can replace this triple with say  $[w_1]([w_2][w_3])$  and that by the definition of the multiplication in  $G$  will just become this product ok and that is exactly the the verification of associativity ok.

Now, the identity is also easy. So, there is an identity element what should the identity element be? Well, so, let us call it  $e$  maybe , the identity element of this group  $G$  well I claim its nothing, but you take the equivalence class of the empty word ok. So, that is the the empty word in words of  $\widehat{S}$  the equivalence class of the empty word by the ways it has lots and lots of words remember right. So, we um looked at for example,  $aa'a'a$ , those basic rewriting guys they are all. In fact, in the equivalence class of the empty word so this is in fact, the set of all words which if you keep applying rewriting rules will finally, come down to the empty word.

The claim is that that serves as an identity again by definition, because the multiplication just says for any word  $e$ , if I multiply it with the equivalence class of the empty word, I just have to concatenate  $w$  with the empty word, but that is just  $w$  ok and observe the same logic holds in the other order. If I hit the equivalence class of the empty word with  $w$  on the right then of course, it gives me  $w$  ok. So, in some sense these two properties just follow from the corresponding properties of the  $*$  operation. So, no surprises so far, but the reason we were doing all this is, because the  $*$  does not admit inverses ok, but the important property here is that this does have inverses ok. In other words it is a group.

So, let us verify this, let us check that given any element of  $G$ . I can construct an inverse of that element with respect to this this new operation that we have defined. So, for a start let us let us just look at the the two basic generators  $a$  and  $b$ , the alphabets um if I just take the single , if I take the equivalence class of the the word  $a$ , the question is what is the inverse of this guy.

So, in other words what equivalence class will you take such that you know what should I put here. So, that this product gives me the identity element and remember the identity element just means it is the equivalence class of the empty word ok and observe that well by definition we already know something . So, let us just throw that in let us let us perform a simple computation here. So, observe if I take  $a$  and I multiply it with the equivalence class

$$[a] \cdot [a'] = [a * a'] = [aa'] = [e] = e$$

$$[a'] \cdot [a] = e = [b] \cdot [b'] = [b'] \cdot [b]$$

(eg)  $w = abbaa$        $[w] \cdot [a'a'b'b'a']$   
 $\overline{w} =$  read  $w$  in reverse // & replace each letter by its dash.

$$[w * a'a'b'b'a']$$

$$[abbaaa'a'b'b'a']$$

$abbaaa'a'b'b'a'$



of the element  $a'$ , then by definition this is the equivalence class of the concatenation . The word  $a$  with  $a'$  which again by definition is just  $aa'$  the word of length 2, but remember  $aa'$  by the rewriting rule is the same as the empty word  $ok$ .

So, in other words it says that a equivalence class multiplied by the equivalence class of  $a'$  is in fact, the identity element of this group  $ok$  and of course, in the other order as well  $a'$  multiplied by  $a$  would also give you identity, you know you can also check that the same is true of  $b$  and  $b'$ .

So, this is what I meant when I said in the beginning that you know a prime and b prime will eventually perform the roles of the the inverses  $ok$ . That is only we have only constructed inverses for these special one letter words if you wish. Ah, What about a general word? That is that is also very easy. So, let us just do it by example and you will you will see the general picture very quickly. Suppose, I take the word  $w = abbaa$  for example,  $ok$ . So, the question is what should the inverse? So, maybe I should make it slightly asymmetric. So, let me put two  $a$ 's on the end. So,  $abbaa$  for example,  $ok$ . So, take this word  $w$ , I want to know what is the inverse of this , this word  $ok$ .

So, I claim here is a simple prescription , you just look at this this string of letters you read them in reverse  $ok$  and when you read them in reverse you you just change all the  $a$  is to  $a'$  and  $b$  is to  $b'$ . So, here is the prescription the inverse of  $w$  so, let me call it  $\overline{w}$  for now. This is just read  $w$  in reverse and replace any any symbol that you see by its dash  $ok$ . So, maybe I should call it replace each letter by its dash  $ok$ . So, in other words here, I I apply this prescription , I read this in reverse and I see two  $a$ 's from the end. So, I make them dashes I make  $b$ 's into dashes . So, heres my claim is that this this new word will serve as the inverse. So, let us check. So, how should we check by definition this product is just  $w$  concatenated with this new word  $a'a'b'b'a'$  , which as we know is  $abbaaa'a'b'b'a'$ . So, here is

$$\omega = aba'a \quad [\omega]^{-1} = [a'a'b'a'] \quad \text{check!}$$


←

$$\omega = x_1 x_2 \dots x_k \quad x_i \in \{a, b, a', b'\}$$

$$[\omega]^{-1} = [y_k y_{k-1} \dots y_1] \quad \text{where } y_i = \text{"the dash" of } x_i$$


---

Defn  $(G, \cdot)$  is called the free group on  $a, b$ .



some some long word, but I claim that if I keep applying my rewriting rules successively I can convert this word into the the empty word ok.

So, let us just do this sort of right there. So, let me write down this this word and I will convert it into the the empty word. So,  $abbaaa'a'b'b'a'$  ok. So, let us just do it right right there. So, I have this pair  $a$  and  $a'$  right over here. So, I know that that pair can be erased. I can make it into the identity into the empty word. So, I erase that from a word ok. Now, I look at what is left. Now, again in what is left I see that an  $a$  and an  $a'$  are paired up. So, I can erase them ok. Now, I look at what is left, I see that this  $b$  and this  $b'$  are paired up. So, I erase them ok.

What is left the  $b$  and this  $b'$  are paired up, this  $a$  and this  $a'$  are paired up ok. So, you see that is exactly how we we constructed the inverse. We just read the word in reverse and for every symbol we just took its its dash ok and the reason for doing this is, because exactly this sort of pair wise cancellation is going to happen ok.

And in fact, this is this was just a particular example , but more generally the word can have dashes as well ok. So, here is the maybe here is another example. So, if I have  $aba'a$  for example, then I claim that the inverse of that equivalence class is just read the same thing in reverse, but put dashes. If you see  $a$  put it put an  $a'$  dash, if you see an  $a'$  you convert that to an  $a$ . So, that is it is in some sense  $a'$  is like an  $a$  . So, claim its this element ok and I leave this for you to check ok.

And it is easy to write a general prescription as well, if you wish that if  $w$  is a word which looks like  $x_1 x_2 \dots x_k$  each  $x_i \in \{a, b, a', b'\}$ , then the inverse of  $[w]$  is just given by the equivalence class of well read in reverse. So,  $y_k$  and I will change all the  $x$ 's  $\rightarrow$   $y$ 's where what is  $y_i$  is just the of  $x_i$  ok. So, this being a bit loose here, but you you know what I mean. Each  $x_i$  if it is an  $a$ , then  $y_i$  is  $a'$ , if it is  $a'$  then it is an  $a$  ok.

So, what have we done we have therefore, proved that this group. So, finally, we have managed to do what we set out to do. We have constructed a group  $G$ , with respect to this binary operation. So,  $G$  with respect to this binary operation is called so definition, this is called the free group on the two symbols  $a$  and  $b$  ok. So, observe it is it certainly contains in some sense the elements  $a$  and  $b$  and next time, we will start looking at some of its other properties ok.

For now at least the the motivation for this this terminology, I mean it is not yet fully clear, but we at least said let us start with  $a$  and  $b$ , let us not put any relations just sort of let  $a$  and  $b$  be arbitrary symbols. Let them generate look at all possible products and so on and in some sense what we did by this enlargement procedure is to say let us not just take products of  $a$ 's and  $b$ 's, let us sort of also take their inverses, let us also throw in two formal symbols which are like the inverses of  $a$  and  $b$  and sort of take all possible products, all words with  $a$  in which  $a$ 's,  $b$ 's are  $a^{-1}$  and  $b^{-1}$  occur ok and in some sense that is really what the what the free group is capturing ok. So, more on this next time .