



So, recall  $S$  was the alphabet and  $S'$  is just sort of the primed alphabet just got primes on top of the alphabets ok that is the augmented set  $\widehat{S}$ . Then starting point was the monoid which is the set of all words using the alphabet  $\widehat{S}$  both letters and their primes. So we considered this and we know that this is not quite a group. But it is got a very useful operation that of concatenation the same definition applies as before. And the concatenation has the following properties that it is an associative operation and it is got an identity element which in this case as before is just the empty word ok.

So, well what do we need to do next? We need to define an equivalence relation like we did in the case of the free group on 2 generators. So, this is what we achieved by means of what we called the basic rewriting rules. So, what were these? These rules are the the following if you recall what it was before it said you know  $aa'$  can be replaced with the empty word  $a'a$  similarly  $bb'$ ,  $b'b$  each of these can be replaced with the empty word ok.

So, here it is the same thing instead of  $a, b$  you have many more alphabets. So, let me write this out in general as follows, whenever I see an alphabet  $x$  next to the alphabet  $x'$ . I can replace this word of length 2 by the the empty word. Similarly if I see  $x'$  followed by an  $x$ . I am allowed to replace it with the empty word ok and in fact the way we wrote the basic rewriting rules, there are also rules in reverse. So,  $xx'$  is replaceable by the empty word  $x'x$ . I can replace it these are 2 rules.

And the opposite rules also are available I can replace the empty word with  $xx'$  or I can replace the empty word with  $x'x$ . So, there are in this case 4 basic rewriting rules for each alphabet in  $x$  ok and we defined the the following things. So, this is for every  $x$  and  $S$  and we defined an equivalence relation on words as follows. So, we have an equivalence relation which is the following that 2 words  $w_1$  and  $w_2$  are said to be equivalent or related to each other.

If I can go from  $w_1$  to  $w_2$ , so if there exists words  $z_1 \rightarrow z_2 \rightarrow \dots \rightarrow z_k$  between  $w_1$  and  $w_2$  in this way. So, let me write this as if there exists a chain of words such that each arrow is a basic rewriting rule is obtained. So, each of these arrows which connects these successive words is obtained via some basic rewriting rule ok. In other words by successively replacing  $xx'$  by empty or  $x'x$  by empty or the reverses of those rules you can go from the word  $w_1$  to the word  $w_2$  and just like what we saw in our earlier example.

And as before the definition of the free group  $G$  is defined to be the set of equivalence classes of the set of all words under the equivalence relation tilde ok. So, this as before is going to be our set  $G$ . And the operation is is the same thing, so if I take 2 words  $w_1$  and  $w_2$  and I look at their equivalence classes in  $G$ . So, I look at  $w_1 \in G$  well I look at the equivalence class of  $[w_1]$  that is an element of this set  $G$  this is an element of  $G$ , the product is defined as before to be you take the concatenation of the 2 words and then you look at the equivalence class of the concatenation ok.

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

Now since it is the verification of the properties is very closely analogous to what we have seen already for the case of 2 alphabets. So, I am just going to leave this as an exercise for you to try your hand at how these arguments work in general. So, here here are the various exercises, I suppose one is show that this is an really an equivalence relation is an equivalence relation. So, that is 1 and 2 that under this product that I have just defined. So,  $G$  with this product dot is a group ok.

In other words the product is associated it has an identity and most importantly it has inverses ok. And you will observe that like before if I take the word just a single alphabet

$$\begin{array}{ccc} [\omega_1] \cdot [\omega_2] & := & [\omega_1 * \omega_2] \\ \uparrow & & \uparrow \\ G & & G \end{array}$$

Exercises: (i)  $\sim$  is an equivalence relation  
(ii)  $(G, \cdot)$  is a group.

$$(iii) [x]^{-1} = [x'] \quad \forall x \in S$$

$$G = \text{Free group on the set } S \\ F(S)$$



$x$  coming from the set  $S$  and it is a word of length 1 I look at it is a equivalence class and somehow this is how we motivated the entire definition. So, we needed to find an inverse for this this word  $x$  and like in the earlier case this inverse is just the word  $x'$ , so this is for all  $x \in S$ .

So, maybe that is part 3 of the exercise show that in this group  $G$  the inverse of the the singleton word, the word of length one  $x$  is in fact the word  $x'$  ok also a word of length 1 ok. In fact, that will be one of the things you will show when you show it is a group ok. So, this is sort of how you define free groups in general. So,  $G$  is what is called the free group on the set  $S$  and the notation we introduced was this sort of curly  $F(S)$  ok. So, let us get our hands on an example.

So, here is sort of something even simpler than the free group on 2 alphabets we could look for the free group on a on a single alphabet or a single generator. So, suppose my set  $S$  has just a single element  $a$  and so now I try to understand what the free group on this single alphabet  $a$  looks like. And here is my claim this free group on a single alphabet is actually isomorphic to the group of integers under addition. In other words it is an infinite cyclic group ok. So, so let us prove this so I am going to prove my claim . So, observe what is it that the the free group I mean how do we constructed we will first have to look at words in the alphabet  $a$  and  $a'$ .

So, the typical word here will look like some  $a$ s and then some  $a'$  and some  $a$ s again and some number of  $a'$  and so on and so forth right. So, this is this is all the word can have can have  $a$ s and  $a'$  which occur in some order some number of times and so on. Of course, the words all words are finite so it it ends somewhere.

So, this is a typical word in  $\hat{S}$  and then the free group itself is obtained by looking at the equivalence relation on the set of words in which you are allowed to sort of collapse and  $aa'$  and make it empty or expand an empty word and make it  $aa'$  or  $a'a$  and so on.

Example:  $S = \{a\}$  Claim  $\mathcal{F}(S) \approx (\mathbb{Z}, +)$


Proof:  $\hat{S} = \{a, a'\}$  a'a'

Want  $\mathcal{F}(S) \rightarrow \mathbb{Z}$  isomorphism

Words( $\hat{S}$ )  $\xrightarrow{\phi}$   $\mathbb{Z}$   
 $\omega$   $\rightarrow$   $(\text{No. of } a \text{ in } \omega) - (\text{No. of } a' \text{ in } \omega)$   
 $\parallel$   
 $aa \dots a'a' \dots$

Observation  $\omega_1 \xrightarrow{\text{basic rewriting}} \omega_2 \Rightarrow \phi(\omega_1) = \phi(\omega_2)$

Cor:  $\omega_1 \sim \omega_2 \Rightarrow \phi(\omega_1) = \phi(\omega_2)$





So, we however our need to show that the free group is actually isomorphic I claim to the just the ordinary group of of integers ok. And intuitively it is sort of clear why because, whenever you you see a string like this of  $a$  and  $a'$ . What is of course going to happen is that you know every time you see an  $a$  and  $a'$  together. So for example, this  $a$  and  $a'$  the basic rewriting rule will say you can actually erase it right. So, this this sort of goes away, now again an another  $a$  and  $a'$  end up being together. So, you can get rid of them using the basic rewriting rule . So, every time you see  $a$  and  $a'$  of of they go  $aa'$  ok. So, let me just complete this word to something. So, let us suppose these last few letters were  $a'a'a'a$  ok. So, again I scan this and I notice that here is an  $a'a$  which again can be made into an empty word, so get rid of all these.

So, observe that every time an  $a$  and  $a'$  occur together and you can get rid of them and finally after you have done this process sufficiently many times. I mean as many times as you can you will find that the word that you finally get has only as or has only  $a'$  ok. It has some number of as or it has some number of  $a'$  and so that number of as that you are left with that is really the integer that we are going to map that word to ok. So, observe to construct an isomorphism what we need to do is to construct a map from the free group to the integers or from the integers to the free group ok.

So, let us let us do it in this order. So, we will try and construct a map from the free group to the integers ok. Now of course a free group is so this is what I want I want to construct a isomorphism of groups ok. So, I want to construct a group isomorphism . But as an intermediate step let me try doing this on at the level of words, so let me look at all words in  $a$  and  $a'$  and define a map from that to the integers ok. So, I will call that map  $\phi$  and here is my my map. So, I write my word  $w$  it is some as and  $a'$  primes  $a'$ s. I said some bunch of  $a'$ s and some bunches of bunch of  $a'$ . Now my map does the following it maps  $w$  to the number of  $a'$ s in  $w$ , so it is a

(number of  $a$  in the word  $w$ )-(the number of  $a'$  in  $w$ ) ok.

So, I do not want to put that also in quotes sorry probably get confused so let me get rid of this. So, let us do one thing let me just put this in a different color. So, I will say it is a number of the alphabet a number of occurrences of the alphabet  $a$  minus the number of occurrences of the alphabet  $a'$  ok.

So this is of course an integer it could be a positive or a negative integer and let us see what properties this map has. So observe if I have a word  $w$ , so here is the first key observation that suppose I have a word  $w$  and suppose I perform a basic rewriting rule on  $w$  ok. So, I transform  $w$  to some other word so maybe let us say if I have a word  $w_1$  and I perform a basic rewriting rule. So, let us say basic rewriting which means whatever I have done I have either collapsed and  $aa'$  and made it empty or you know  $a'a$  empty or expanded an empty into an  $aa'$ . Observe the basic rewriting rule always has the same number of  $a$  as it either collapses it either removes the you know 1  $a$  and 1  $a'$  or it increases the number of  $a$ 's by 1 and number of  $a'$  by 1 ok. In other words the basic rewriting rule does not change this difference that we are talking about, the number of  $a$  minus  $a'$  remains constant ok.

So, if  $w_1$  and  $w_2$  are related like this then certainly this is number  $\phi(w_1)$  and the number  $\phi(w_2)$  are necessarily the same ok. Now as a corollary to this observation if I have 2 words which are equivalent under the equivalence relation, which means I can go from  $w_1 \rightarrow w_2$  by means of a sequence of basic rewriting rules. I may not be able to go in one step still the same property holds because it holds at every step ok. So, what is this mean 2 equivalent words necessarily have the same value of  $w$ .

So, I can in fact define a map. So, what this means is that I can think of  $\phi$  as actually giving me a map from the set of equivalence classes ok, which is what we call the free group. In other words given a word  $w$  look at it is equivalence class I can associate to this equivalence class the number  $\phi(w)$  ok and this new map I will call  $\bar{\phi} : F(S) \rightarrow \mathbb{Z}$  ok. So, observe this is well defined. In other words it does not depend on the representative  $[w]$  that it picked for the equivalence class ok. Why? Because of what we just said what we just said about, if instead of  $w_1$  I had picked  $w_2$  as my representative or maybe here if I had instead of  $w_1$ . I picked something equivalent to  $[w_1]$ , then the value of  $\phi$  would have remained the same ok. So, I can just go ead and pick any representative of my class and I define my map to just be  $\phi$  of that ok.

So, this is a number of  $a$  minus number of  $a'$ ; this defines gives me a well defined map from the free group on  $S \rightarrow \mathbb{Z}$ ,  $S$  remember is just a singleton here. So firstly it is well defined and now I claim that this is actually the isomorphism that we want ok. So, first let us show that it is a group homomorphism . So, recall what does homomorphism mean, I must take 2 elements  $w_1$  and  $w_2$  in my group  $F(S)$ . I should multiply them out in the group and then my answer should equal  $\bar{\phi}([w_1] \cdot [w_2])$ , but times is the product on the right hand side is computed in the group  $\mathbb{Z}$  it is computed in the the range of this map.

In other words that operation here is just a plus the usual addition in the integers. So, this is  $\bar{\phi}([w_1]) + \bar{\phi}([w_2])$  this is what I need to prove. So, this is what it means to say that phi bar is a homomorphism ok. So, let us compute each side and see whether this equality holds. So, let us check what the left hand side is by definition this is  $\bar{\phi}$  evaluated on the product is the concatenation of these words. Now look at this concatenated word  $\bar{\phi}([w_1 * w_2])$ ,  $\bar{\phi}$  of this equivalence class is just going to be the number of  $a$ 's minus the number of  $a'$  in the concatenation ok. But observe the concatenation of 2 words is just put  $w_1$  first and then write  $w_2$  next to it right.

$$\begin{aligned}
 & \mathcal{F}(S) \xrightarrow{\bar{\varphi}} \mathbb{Z} \\
 & [w] \longrightarrow \varphi(w) \text{ is well-defined.} \\
 \text{a) } & \text{homomorphism} \xrightarrow{\text{Need}} \bar{\varphi}([w_1] \cdot [w_2]) = \bar{\varphi}([w_1]) + \bar{\varphi}([w_2]) \\
 & \text{LHS} = \bar{\varphi}([w_1 * w_2]) = \text{No. of } a \text{ in } w_1 * w_2 \\
 & \quad \quad \quad - \text{No. of } a' \text{ in } w_1 * w_2 \\
 & \quad \quad \quad \boxed{\dots} \boxed{\dots} = \bar{\varphi}([w_1]) + \bar{\varphi}([w_2]) \\
 \text{b) } & \text{one-to-one: } \text{iff } \bar{\varphi}([w]) = 0, \text{ then need to prove} \\
 & \quad \quad \quad [w] = \text{identity elt of } \mathcal{F}(S) \\
 & \quad \quad \quad = [ ]
 \end{aligned}$$

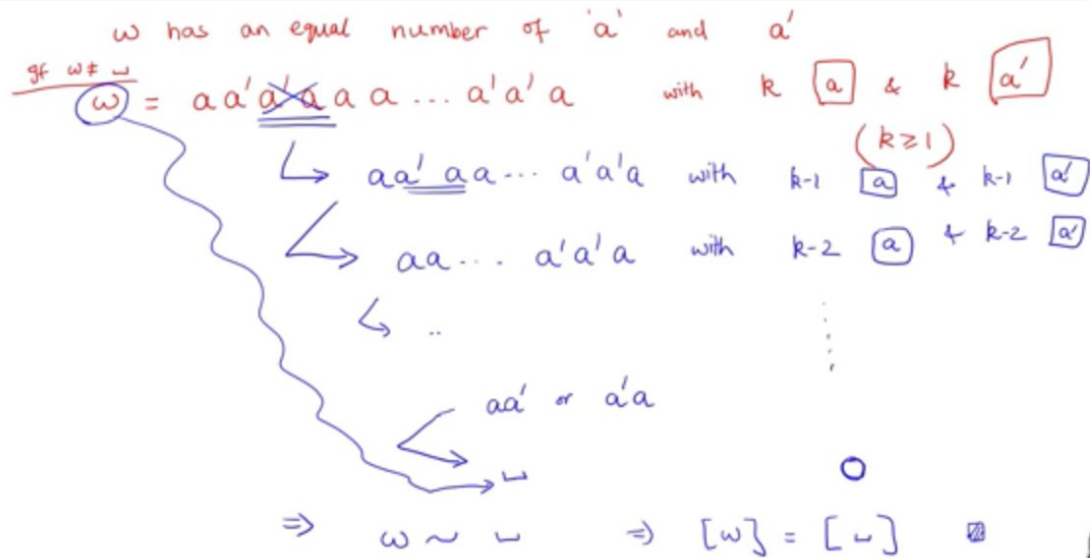


So, if I am trying to count how many  $a$ 's occur in the concatenation well I just have to see how many  $a$  occur in  $w_1$ , I may see how many  $a'$  occur in  $w_2$  and it is just the sum of those 2 numbers ok. Similarly the number of  $a'$  in the concatenation is just the sum of the number of  $a'$  in  $w_1$  and  $w_2$  ok ok. So, what this means is that this answer is nothing but  $\bar{\varphi}([w_1])$  which means is the number of  $a$  minus  $a'$  and  $w_1$  plus  $\bar{\varphi}([w_2])$  the number of  $a$  minus  $a'$  in  $w_2$  ok. So, that is that is the proof of the homomorphism property ok.

Now let us look at property (b) which is one to one. So, let us prove one to one now and then we will prove on to. So, why is this map one to one? Since it is a homomorphism we just need to check the following property that if a word maps if the equivalence class of a word maps to the identity element of  $\mathbb{Z}$ . So, the identity under the addition remember is 0. So, suppose some equivalence class maps to 0, then we need to prove then we need to prove that this equivalence class must be the identity element of the free group. And remember so this should be the identity element of  $F(S)$  which if you remember and which you probably checked is nothing but the equivalence class of the empty word ok. So, let us prove this. So, let us analyze what this means for a second. So, we are trying to understand what it means for  $\bar{\varphi}$  of a word to be 0 ok. By definition phi bar is the number of  $a$ 's minus  $a'$ , so the fact that  $\bar{\varphi}$  of a word is 0 just means that the word has an equal number of  $a$  and  $a'$  ok.

So, let us go here the word  $w$  has as many  $a$ 's as  $a'$ 's has an equal number of  $a$  the alphabet  $a$  and the alphabet  $a'$  ok. So, what is that mean? It means that if you scan this this word from left to right just like we were doing before. So, let me write over like this  $a'a'a$  something like this maybe. So, this is what the word looks like it has an equal number of  $a$  and  $a'$ . So, it has at least one  $a$  and  $a'$  ok.

Let us assume that the word is not empty ok. If the word is already empty then you are done because, you have to prove that finally this word the equivalence class of  $[w]$  is just the equivalence class of the empty word ok. So, if  $w$  is not the empty word then  $w$  looks like this



in which there are at least with let us say  $k$  occurrences of  $a$ 's and  $k$  occurrences of  $a'$  ok, now where  $k$  is at least 1. Now you scan word from left right ok there is got to be at least one place where an  $a$  and an  $a'$  occur next to each other they occur consecutively right.

That is you really cannot avoid that if you have got  $k$   $a$ 's and  $k$   $a'$  and you know where I mean any word which has both  $a$ 's and  $a'$  already must have at least one position where  $a$  and  $a'$  come next to each other ok. One way of saying it is you scan the word from left right, you look at the first letter if it is an  $a$  then at some point you must get to  $a'$  right. So, the place where it transitions from  $a$  to  $a'$  that place will have  $aa$  sub word of the form  $aa'$  ok.

So, you pick the the  $a$  and  $a'$  coming next to each other, it could be  $aa'$  or  $a'a$ . So, let us do this for examples so find a place where I have  $a'a$  and using the basic rewriting rule I get rid of that entirely ok. So, from this I can form an another word in which, so using a single basic rewriting rule what I have been able to do is to find another word in which still it has an equal number of  $a$ 's and  $a'$ 's. But that number has come down by 1 it is  $k-1$   $a$  and  $k-1$   $a'$  s ok. Now repeat the argument again if  $k-1$  is at least 1, then it means this word is not the the empty word; that means surely it has both  $a$ 's and  $a'$  s.

And again find any one location where a and an  $a'$  come next to each other and you get rid of them using the basic rewriting rule. So, again I can do this ok. So, what have I generated another word but now it is got  $k-2$  occurrences of  $a$  and  $k-2$  occurrences of  $a'$  s ok and so on. So, you can see that as long as this number  $(k-1)$ ,  $(k-2)$  etcetera, as long as these numbers are at least 1 you can keep doing this.

So, what it means is at some point you will be left with the case when this number becomes 0. This number keeps decreasing by 1 each time and at some point it is got reached to 0 ok. What does that mean? When it is reaches 0 it just means that the resulting word at the last step that you have has 0  $a$ 's and 0  $a'$  s, in other words this is just the empty word ok. In



$$\begin{aligned}
 \text{(3) } \bar{\phi} \text{ ONTO : } & \quad f(S) \xrightarrow{\bar{\phi}} \mathbb{Z} \\
 & \quad [w] \longrightarrow n \\
 & \quad \text{if } n \geq 1, \quad w = \underbrace{aa \dots a}_{n \text{ times}} \\
 & \quad n \leq -1, \quad w = \underbrace{a' a' \dots a'}_{(-n) \text{ times}} \\
 & \quad n = 0, \quad w = \epsilon
 \end{aligned}$$

$$\begin{aligned}
 f(\{a\}) & \approx (\mathbb{Z}, +) \\
 f(\{a, b\}) & \not\approx (\mathbb{Z}^2, +) \\
 & \quad \text{Non-abelian} \quad [ab] \neq [ba]
 \end{aligned}$$



fact, in the one preceding step the word must have had a single  $a$  and a single  $a'$ . So, that word must have looked like either  $aa'$  or  $a'a$  ok, that was the one preceding step.

And of course, the possibilities for each step prior to that are many more ok. But at the very end you are going to necessarily reach the empty word ok. So, what is that mean? You can reach the empty word from the original word  $w$  right, I have gone through a sequence of basic rewriting rules and I have gotten to the empty word. Which means that  $w$  is in fact a equivalent to the empty word, in other words the equivalence class of  $w$  is the same as the equivalence class of the empty word ok. Which is what I wanted to prove, so this proves one to one.

And let us finally prove the onto. So, part 3 of the proof of isomorphism I need to show that this map  $\bar{\phi}$  is onto ok. What does that mean? I need to show that so recall  $\bar{\phi}$  as a map from  $F(S) \rightarrow \mathbb{Z}$ . Given any integer  $n$  I must show that there is some word some pre image right, I am assured that there is some word  $[w] \rightarrow n$  ok. So, this is very easy to manufacture. So, observe if  $n \geq 1$  then what is this word which maps to to the number  $n$ . I can take  $w$  to be so let us write this out here if  $n \geq 1$ . I can take  $w$  to be the word which has  $aa \dots a$  occurring  $n$  times ok. If  $n$  is negative if  $n = -1$  or lower. I can take the word which which looks like  $a' a' a'$ . So now I should take  $(-n)$  times or modulus of  $n$  times ok. So, observe this is the first word has if I look at  $\bar{\phi}$  which is number of  $a$ 's minus  $a'$ 's it is  $n$  for the first word.

And because it is  $n = 0$  there are no  $a'$ 's, for the second word it is  $0 - n$  because there are no you know it is not  $0 - n$ , but rather  $0$  minus modulus of  $n$  ok. So, in this case mod  $n$  is the same as  $(-n)$ . So, maybe I should write it as it occurs  $(-n)$  times. So, if you compute  $\bar{\phi}$  you will again see this  $n$  and then finally if  $n = 0$ . Of course, that is the easiest case I can just take  $w$  to be the empty word and  $\bar{\phi}$  the empty word is of course just  $0$  ok.



So, we have managed to show that this is an isomorphism and so that is sort of a nice tractable example. But sort of a thing to keep in mind is that as soon as you are so this this is done proves our claim that  $f(a)$  singleton the free group is just isomorphic to the group of integers. But as soon as the set  $S$  has 2 or more generators this becomes a vastly more complicated group ok. If I take the the free group on 2 generators  $a$  and  $b$ , then this is a much much more complicated group than the group of integers for example ok.

In particular this is not going to be the group of you know it is not the group  $\mathbb{Z}_2$ . For example, so observe while this is isomorphic to  $\mathbb{Z}$  of this is very far from being true ok. So, this is not at all the case ok. So, these groups are you know  $\mathbb{Z}_2$  is in fact an abelian group it is got sort of got 2 generators, but it is an abelian group  $f(\{a, b\})$  the free group on 2 generators is of course non abelian. The word  $a b$  and the word  $b a$  in this free group will turn out not to be in the same equivalence class ok.

So in order to sort of better understand some properties like this of the free group. So for example, I just mentioned this is a non abelian group, in other words if I take the word  $ab$  in this group and I look at the word  $ba$  in this group, then the equivalence class of  $[ab] \neq [ba]$ . So, I am talking about the the free group here on 2 generators ok.

So, to prove things like this even basic facts about free groups, I mean you could prove it just from the definition. For example, that there are no basic rewriting rules which will help you go from here to there. But there is sort of a nice conceptual way of of understanding these free groups and that is the notion of it is universal property and that is something that we will take up in the next lecture .