

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

1. LECTURE 26 [FREE GROUPS I]

Today we are going to talk about, Free Groups. Now, this is not a topic that you usually encounter in first course on group theory for example. But, its nevertheless a very important notion and we will try to understand it as intuitively as possible initially, and then slowly work our way towards the formal definition ok.

So, here is the main motivation. So, firstly we know, what generators of a group mean ok? So, what is the set of generators of a group? So, given a set  $S$  so, if suppose  $G$  is a group. So, let  $G$  be a group and  $S \subseteq G$  be any subset of  $G$ , then we say  $S$  generates the whole group  $G$ , if the following is true. If so, what we will call the smallest subgroup generated by  $\langle S \rangle = G$  ok?

Now, what is the subgroup generated by  $S$ ? So, let us unravel that little notation there. So, this is what is called the subgroup generated by the subset  $S$ . So, let us define that so, this is just defined to be the smallest subgroup of  $G$  which contains the set  $S$ .

Free Groups

Generators of a group :  $G$  group &  $S \subseteq G$ . we say  $S$  generates  $G$  if  $\langle S \rangle = G$ .  
subgp generated by  $S$

def:  $\langle S \rangle := \bigcap_{\substack{H \text{ subgp of } G \\ H \supseteq S}} H$  . subgroup of  $G$

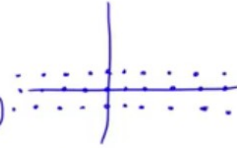
Eg : (i)  $G =$  cyclic group of order  $n$      $G = \{1, a, a^2, \dots, a^{n-1}\}$   
 $S = \{a\}$      $\langle S \rangle = G$



- (2)  $G = (\mathbb{Z}, +)$
- $S = \{1\}$      $\langle S \rangle = \mathbb{Z}$
  - $S = \{-1\}$
  - $S = \{2, 3\}$
  - $S = \{2\}$  does not generate  $\mathbb{Z}$   
 $\langle S \rangle = \{\text{even numbers}\}$

(3)  $G = (\mathbb{Z}^2, +)$      $(x, y) \in \mathbb{Z}^2$      $x, y \in \mathbb{Z}$

$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$



$S = \left\{ \underset{a''}{(1, 0)}, \underset{b''}{(0, 1)} \right\}$      $\langle S \rangle = \mathbb{Z}^2$

$ab = ba$



So, it is defined as follows so, here is definition this is just the:

$$\langle S \rangle = \bigcap_{H \text{ subgroup of } G, S \subseteq H} H$$

so, for all the the elements all the sub groups  $H$ . So, what is  $H$ ?  $H$  is a sub group of  $G$  its a intersection of all sub groups of  $G$ , which contain the set  $S$  itself ok.

And as its probably familiar to you this is in fact, a subgroup. So, if you define an an arbitrary intersection of subgroups is again a subgroup. So, this will always be a subgroup so, this is always a sub group of the group  $G$ . And this subgroup as you can check easily. So, this subgroup is what is called the subgroup generated by the set  $S$  ok.

So, here are some examples so, if I take for example, let us say  $G$  is the cyclic group,  $G$  is cyclic group of order  $n$  and cyclic group of order  $n$ . In this case just means the elements of the group look like

$$G = \{1, a, a^2, \dots, a^{n-1}\}$$

So, these are the the various elements of this group, and what we have is well if this is your group  $G$ . We know that the singleton if I take  $S$  to just be the element  $S = \{a\}$  itself for example.

Then the subgroup generated by this singleton  $a$  is of course, the entire group  $G$ . Because, once  $a$  is in the in the subgroup then so, is  $a^2, a^3, \dots$  and so on ok. So, all of these are in the subgroup. So, here its clear that the subgroup generated by the singleton is the whole group  $G$ .

Now, let us look for another example. So, here is example 2, let us take the group  $G = (\mathbb{Z}, +)$  to be the set of all integers with addition being the group operation. So, this as you know is an is an Abelian group. And here again we can find subsets which generate the whole group for example, if I take the subset  $S = \{1\}$  consisting of only the the number 1.

Then clearly the subgroup generated by this group is just the whole group  $\mathbb{Z}$  right. Because, as soon as 1 belongs to you know the subgroup generated by  $S$ , you know 2, 3, 4, .. they all have to belong because, they are just obtained by repeated additions ok.

Now, similarly of course, this by no means is the only set which generates a whole group, you could look at for example, the singleton consisting of  $S = \{-1\}$  that again would generate the group.

Here is another example I could take two elements for example, the elements  $S = \{2, 3\}$ , this two element subset also generates a group. Because, once 2 and 3 belong then so, does their difference which is  $3 - 2 = 1$  and once you have 1 in a subgroup, then of course, all elements of  $Z$  belong to that subgroup ok.

But observe so, these are all generating subsets they all generate the whole group  $G$ , but here is an example of something which does not generate the group  $G$ . Which is just the singleton  $S = \{2\}$ , this guy does not generate  $\mathbb{Z}$ . Because, the smaller subgroup which contains the set  $S$  is just the so, in this case if you just think about it for a minute. The smallest subgroup of the integers which contains  $S$  is just going to be the set of all even numbers. So, these are all even numbers and so, that is of course, not equal to the entire group  $\mathbb{Z}$  itself ok.

Now, the the next example is very close to the previous one, we could look at  $G = (\mathbb{Z}^2, +)$  which is the set of all vectors if you wish. The typical elements here look like  $(x, y)$ , this is a typical element of  $\mathbb{Z}^2$  where  $x, y \in \mathbb{Z}$  both belong to integers. So, this is like pictorially you can think of  $\mathbb{Z}^2$  as just being you know just draw the the usual plane and just mark off the points, whose  $x$  and  $y$  coordinates are both integers so, for example, these guys.

So, what you get? Sometimes called the integer lattice. So, the origin is also there and so on. So, this collection of points is what is what we could think of as  $\mathbb{Z}^2$ ? And of course, here these are all vectors in the plane integer coordinate vectors. And you have the usual notion of addition, which is if I take

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

And the group of you know the group  $\mathbb{Z}^2$  has the following obvious set of generators, I could just take the vector  $S = \{a = (1, 0), b = (0, 1)\}$ . And again as one can check easily, if I take the smallest sub group of  $\mathbb{Z}^2$  which contains these two elements, then it must contain every other element of of set it must contain all elements ok.

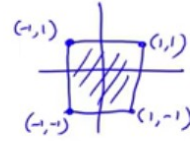
So, here is again an example of of a group which is generated by two elements  $a$  and  $b$  in this case. So, I will just call these these two elements I will denote them by as  $a$  and  $b$ . And observe in this case that because this group is Abelian the group  $\mathbb{Z}^2$  is Abelian, we actually have something something further here that these two generators  $a$  and  $b$  satisfy this relation that  $ab = ba$  in this case ok.

So, here is example 4. So, this is what we call the dihedral group again must be a very familiar example for all of you. So, the dihedral group with 8 elements. So, what I will call  $D_4 = \{Symmetries\ of\ a\ squar\}$  ok? So, this has 8 elements this as we are use to thinking about this this is nothing, but the set of all this is the group of symmetries of a square ok. So, that is the dihedral group and the the typical symmetry.

So, if you imagine the square as being as positioned in this manner so, this is a square of say some side length let us say side length 2. So, these are the 4 vertices  $(1, 1), (1, -1)$ , this is  $(-1, -1)$ . And this is the point  $(-1, 1)$ . So, imagine the square here of side length 2 drawn on the plane.

$$(4) \text{ Dihedral group } D_4 = \{\text{symmetries of a square}\}$$

$$= \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$$



$a = \text{rot}^n$  by  $\pi/2$

$b = \text{refl}^n$  about X-axis

$$S = \{a, b\}$$

$$\langle S \rangle = D_4$$

$$\text{Relations: } \underbrace{a^4 = 1, b^2 = 1, ab = ba^3}$$

$$(5) \quad G = S_n = \text{permutations of } 1, 2, \dots, n$$

$$S = \left\{ \begin{matrix} (1\ 2) \\ a_1'' \\ (2\ 3) \\ a_2'' \\ \dots \\ (n-1\ n) \\ a_{n-1}'' \end{matrix} \right\}$$

$$\langle S \rangle = S_n$$

$$a_i^2 = 1 \text{ and } (a_i a_j)^3 = 1 \text{ etc.}$$

And we sort of ask what are the this is the square? And what are the symmetries? So, what are the operations of the plane which preserve the square ok and so, the most obvious one is of course, the rotation. And there is another one which is reflection about the X-axis.

So, there are many rotations and we will sort of you know the usual way of writing out this group is to say well there are elements the following are elements of the group, I have  $\{1, a, a^2, a^3\}$ . So, what is this transformation  $a$  the symmetry  $a$ ? Let us think of  $a$  as being rotation about rotation through 90 degree angle ok, rotation by 90 degrees say anti clockwise ok.

And there are 4 more elements, which I will denote  $\{b, ba, ba^2, ba^3\}$ . Where  $b$  is the transformation which is reflection about the X-axis ok. And observe that this again preserves each of them preserves the square and  $a^2, a^3$  are just rotation by 180 degree angle and 270 degree angle respectively.

And again here observe that if I take  $S = \{a, b\}$ , my generating subset to just comprise the elements  $a$  and  $b$  then, just because the elements all have this form observe. If I look for what is the smallest subgroup of  $D_4$ ? Which contains this subset  $S$  which contains  $a$  and  $b$  then, there is no other way out it has to also contain every single element of  $D_4$  ok.

So, here is a generating set the set two element set  $a, b$  generates the group  $D_4$ . Now, again like we we observed in the earlier case that the generators  $a$  and  $b$  end up satisfying some relations in this group ok. So, earlier I said if I take  $a$  and  $b$  to be the generators of the group  $\mathbb{Z}^2$  then  $ab = ba$  because it was an Abelian group.

And in this case similarly the relations are  $a^4 = 1$  ok. So, I will i will denote the identity by 1. So, this is the identity element of the group  $D_4$ . So,  $a^4$  is just rotation by 360 degrees which is the same as doing nothing. So, that is the identity,  $b$  being a reflection if I do it twice I get back the identity. So,  $b^2 = 1$  and here is the non trivial relation which you must

have actually seen, which is if I take  $a \cdot b$ , then its not equal to  $b \cdot a$ , but rather  $b \cdot a^{-1} = ba^3$  ok.

So, here are some relations which are satisfied by these two generators  $a$  and  $b$  ok. And you know one has many examples of groups like this with some canonical set of generators, and the generators obeying some sorts of relations. So, here is another example which I will leave for you as an exercise. I can take  $G$  to be the the permutation group  $S_n$  the set of all permutations of the elements  $1 \rightarrow n$ . And in this case the rather beautiful generating set is the following, you can just take what are called the adjacent transpositions or the elementary transpositions. Which is you only look at the permutations, which permute 2 adjacent letters to adjacent numbers and do not do anything to any of the other numbers ok.

$$S = \{a_1 = (12), a_2 = (23), \dots, a_{n-1} = (n-1, n)\}$$

So, its its an interesting fact that its these these  $n - 1$  elements actually generate this entire group. This is the whole group  $S_n$  ok rather remarkable because there are only  $n - 1$  of them, but the group  $S_n$  itself is rather large there are  $n!$  factorial elements. But, its enough you know you can generate them with just these particular  $n - 1$  elements ok. There are other other even more economical sets of generators.

But again here notice that you know, if I call these there are  $n - 1$  of them. So, I will call them  $a_1, a_2, \dots, a_{n-1}$  observe then that I actually have some relations here as well. So, each of them satisfies the following relation  $a_i^2 = 1$  and for all  $i$  and there are other sorts of relations there are many others. So, if I take a product of two of these guys if I take  $a_1 a_2$ , then it is a product of 2 simple transpositions  $(12)$  and  $(23)$ . And that turns out to be the the three cycle  $(123)$  and therefore, its cube is actually the identity ok.

And there are many other such relations ok which I will I will leave for now. So, so an an exercise for you in some sense is to try and figure out. What are all the relations that hold among the  $a_i \in S$  ok. Now, intuitively when you have a group that is generated by some collection of generators so, in many of our earlier examples there were let us say 2 generators  $a$  and  $b$ .

The the group was generated by them, but there were nevertheless some relations meaning some equations between the generators of the form, you know either  $a^2 = 1$  some power of as identity, or some multiple of  $a$  and  $b$  in some order turns out to be the same as some other product of  $a$  and  $b$ . You know with some powers some other order and so, on right. So, things like  $ab = b^3 a$  in the dihedral group is an example of relation ok.

Now, what we want to do now? When we talk about free groups ok so, let me sort of explain this try to do all of this the free group on just two generators ok. So, in general I have a notion of what is called the free group generated by a set  $S$  ok. So, this is the general notion given any set  $S$ , we can talk about the free group generated by that set  $D$ , but let us illustrate everything for the special case, when the set only has two elements  $a$  and  $b$  ok. So, we will try and explain, I will try and explain what the free group on 2 generators looks like ok. So, this set sometimes its called the the alphabet or the set of generators ok. So, you should think of these as as some formal symbols so,  $a$  and  $b$  now are just some alphabets in some sense.

So, they are just some formal symbols ok. So, I am just given two symbols  $a$  and  $b$  ok. And what I want to do? Is to try and generate a group from these 2 guys. So, this is called the free group. So, I will denote it like this  $F(S)$ . So, what is this? This  $F(S)$  supposed to be well. Firstly, this should be a group. So, what what are the properties that I want for  $F(S)$

Free group generated by a set  $S$

Eg.  $S = \{a, b\}$  alphabet (formal symbols)

$\mathcal{F}(S)$  :

- group
- $\langle \{a, b\} \rangle = \mathcal{F}(S)$
- ("free") There should be no "relations" between  $a$  and  $b$ .



number one this should be a group of course, it should contain these generators  $a, b \in F(S)$ , but of course, even more I want  $a$  and  $b$  to generate the whole group. So, these two elements  $a$  and  $b$  the subgroup of  $F(S)$  generated by them is in fact, the whole group  $F(S)$ . In other words the set  $S$  generates the whole group, but so, we have already seen many instances of where this property holds that I have say a couple of elements in the group which generates the group. But, here is where the the the new thing happens. So, this is the what it means for a group to be free? So, here is the freeness so, I want so, here is the third property which I want my group to satisfy that there should be no relations between  $a$  and  $b$  ok.

There should be no relations now whatever; that means, between  $a$  and  $b$ . So, all the examples that we have looked at already are not examples of free groups because, I had generators no doubt, but those generators always satisfied some relations in the group ok. Now, at the moment I am still talking little loosely little intuitively. So, we will we will get to the precise definition later ok, but broadly this is the idea.

So, let us talk about a candidate. So, I said I want to construct a group like this. So, there is sort of a natural candidate for this group. So, let me talk about that so, I can actually talk about a candidate for for this free group  $F(S)$ . So, again remember I am only going to do everything for the case when the set has these two elements  $a$  and  $b$ . So, what is the you know what all can I definitely conclude about my group  $F(S)$  right, I said it must have these two elements  $a$  and  $b$  and it must be generated by them. Now, what I want to do? Is to try and see what elements must definitely belong to the group right. What can I say about the elements that are definitely there?

So, here are some elements which I can I can surely say are there in the group, the element  $a$  must surely  $b$  in the group its almost the element  $b$ . So, these are both of course, the generators. So, they both belong to the groups earlier ok. Now, because  $a$  and  $b$  are both there I know that  $aa$  or  $a^2$ , if I multiply  $a$  with itself the element which I will write as  $aa$

Candidate for  $\mathcal{F}(S)$        $S = \{a, b\}$

---

$a, b$

---

$aa, bb, ab, ba$

---

$aaa, aab, aba,$   
 $baa, abb, bab,$   
 $bba, bbb$

---

$aaaa, aaab, \dots$

Words( $S$ ) = { words in  $a, b$  }

- Infinite set
- Multiplication operation on words

$w_1 * w_2 = \text{concatenation of } w_1, w_2$   
 $= \text{write } w_1, \text{ then write } w_2$

$(aba) * (baa) = ababbaa$   
 $(baa) * (aba) = bbaaaba$



must be there, if I multiply  $b$  with itself an element  $b^2$  or  $bb$  must be there the element  $ab$  must be there. And of course, I am not assuming my group is Abelian or anything. So,  $ab$  and  $ba$  are both in general different elements and I want both of them of course, must belong to my group ok. So, I managed to to figure out some more elements. So, let us write this out.

Now, I can start looking at products of 3 things at a time. So, for example, I can look at the element  $a^3$  just  $aaa$  and I can look at  $aab$ , I can look at  $aba$ , I can look at  $baa$ ,  $abb$ ,  $bab$ ,  $bba$  and  $bbb$ . So, these are all in some sense products of elements 3 at a time. And you can imagine this goes on I can look at products of things 4 at  $aaaa$  as  $aaab$  etcetera etcetera ok. So, these are all words of length 4 in some sense then, I look at words of length 5 words of length 6 and so on ok.

Now, so, what have I; what have I done? Well at the moment remember I said  $a$  and  $b$  are just two formal letters right, they are like an alphabet. They just do formal symbols. And what I am trying to do here really? Is to write down words using these two as my alphabet ok. So, let us look at all the words which you can form with  $a$  and  $b$  as your alphabet and in some sense what I have done here is really write down those words. So, here for example, these are these two are the words of length 1, these are the words which have two letters in them. Here are the words with length of length 3, here are the words of length 4 length 5 length 6 and so on ok.

So, given two elements  $a$  and  $b$  formal symbols, well one thing I seem to be able to do is to construct the set of all words in this alphabet ok. And the set of all words. So, this is the set of all words in these two letters  $a$  and  $b$  ok. So, look at this this set of all words. Now what all do I know about this? Firstly, remember its an infinite set so, one thing I surely know is that is that this is an infinite set ok.

But, here is the question can this be made into a group is this maybe a reasonable candidate for the free group itself here is a list of all words. So, I that is that is going to be the attempt we will try and make this into a group, but in order to do this we have remember we need to be able to define a multiplication operation. So, I need a multiplication.

So, the question is what is the multiplication operation on words? And we look for the multiplication operation on words and there is one obvious operation. So, if I have a word  $w_1$  and a word  $w_2$ . So, let me define their product so, maybe we will put a  $*$  for the product  $w_1 * w_2$  is the following this is what is called the concatenation of words. So, this is the concatenation of the two words  $w_1, w_2$  ok.

Now, what is concatenation mean? It just means you first write the word  $w_1$ , then write  $w_2$  ok in that order. So, whatever comes first comes first. So, for example, if  $w_1$  is the word *aba* and I want to figure out what I get when I multiply it by the word *bbaa*, then the concatenation operation is just the following just write them all out one after the other *ababbaa* ok. And notice that this concatenation operation is not commutative because, if I write these in the opposite order then of course, the answer is going to be you know I have *bbaa \* aba*. So, I first write *bbaa* and then follow it up by follow it up with *ab* ok.

So, this is this is the definition of an operation. Now, its not commutative as as we just observed here. But what is interesting is that? This is actually an associative operation ok. So, that is the that is the next thing we will we will talk about. So, observe this was not commutative. So, that was the observation. So, this is not a commutative operation ok, but it is associative ok.

So, let us see why is this; why is this associative the reason is rather straight forward this is; however, associative. Because, if I take three words which is what associativity involves I need to take three words  $w_1, w_2$  and  $w_3$  so, if I first concatenate words  $w_1$  and  $w_2$  and then concatenate, it with the word  $w_3$ . Then what is this? This is just going to be one long word, which is obtained by first write  $w_1$ , then write  $w_2$  then write  $w_3$  right.

So, it is just going to be these these 3 guys written out one after the other. And if you did the same thing in the other order which is I first multiply  $w_2$  and  $w_3$ . And then multiply the answer on the left by  $w_1$ , then well as you can see the answer is quite the same thing. Because, you would have written  $w_2$  and  $w_3$  first concatenated them together and then followed it up by concatenating  $w_1$  on the left ok. So, these are these are actually the the same answer.

So, even though this operation of concatenation is not a commutative operation, it certainly is associative ok. So, that is that is already rather promising. Now let us ask, ourselves what about the the other, properties is this a group with respect to this operation. Now, for it to be a group we also need identity and inverse right.

So, let us check whether this group has an identity element. So, recall what is an identity element? So, let us call it *id* does does there exist an identity element, it is an element which satisfies the following property it should be a special word, which when I concatenate with any word  $id * w = w$ . And this should also equal  $w$  concatenated with the special word *id*. And this should hold for all words  $w$  right.

Now, observe what word can possibly have this this property. So,  $w$  for example, is already some word right. So,  $w$  already has some some alphabets you know as or bs and I am saying I take this this word  $w$  and I concatenated with this this special word *id*. And when I look at this concatenation the answer is just whatever was there in  $w$  already right. And to get this there is really just one way this word *id* must have no alphabets whatsoever right. So, this says actually the following that this word, *id* must be what we will call the empty word



a, b  
aa, bb, ab, ba  
 aaa, aab, aba,  
 baa, abb, bab,  
 bba, bbb  
aaaa, aaab, ....

- Infinite set
- Multiplication operation on words  
 $w_1 * w_2 = \text{concatenation of } w_1, w_2$   
 $= \text{write } w_1, \text{ then write } w_2$

$$(aba) * (baa) = ababbaa$$

$$(baa) * (aba) = bbaaaba$$

not commutative



ok. So, this is the empty word in in the alphabet  $ab$ . So, what does that mean? It has no  $a$ 's or  $b$ 's has no  $a$ 's or  $b$ 's another way of saying it is that its length is 0 the length of the word is 0 or another thing, we could say is well maybe not another thing, but another notation for the for the empty word is the following.

So, we will just put this this little placeholder here to say with with nothing in it to say that you know there are no letters. So, here is the notation for the empty word. So, this is the notation for the empty word  $\epsilon$ . So, we have managed to get the set of all words has these two properties associativity and identity. And let us just check the last axiom, which is inverse the existence of an inverse. Now what does existence of an inverse mean?

Given any element any word  $w$ , I should be able to find another word  $w^{-1}$ , which we will call  $w^{-1}$  such that  $w \cdot w^{-1} = id$  should give me the the identity element right. This is what existence of inverse would mean? Now, observe in this case the identity element as we we just observed must just be the empty word  $\epsilon$ . So, that is the notation. So, what am I asking for here? I want this element  $w$  to be concatenated with some word, suitably suitable word, such that the the the overall concatenation just turns out to be empty right. So, I mean as should be clear this thing can only be done. If  $w$  is already empty other than for the empty word  $w$ , you are never going to be able to do this right. So, if  $w$  is empty we can do this of course, right observe if  $w$  is the empty word then  $\epsilon$ . Then,  $w$  concatenated can we find an inverse well the empty word concatenated with the empty word is of course, the empty word right because there are no letters whatsoever.

But, for any non-empty word if  $w$  is anything other than the identity, then  $w$  already has some letters and there is just no way you can concatenate it with anything, and ensure that the answer has no letters in it  $\epsilon$ . So, this basically cannot be done for the the words whose length is one or more. So, that is sort of bad news in some sense that inverses do not exist ok so, this inverses do not exist. So, what we have here the set of all words with the

• Associative :  $(w_1 * w_2) * w_3 =$  first write  $w_1$ , then write  $w_2$ , then write  $w_3$ .

$$w_1 * (w_2 * w_3)$$

• Identity :  $id * w = w = w * id \quad \forall w \in \text{Words}(S)$

$$\boxed{\dots} \boxed{\dots} = \boxed{\dots}$$

$\Rightarrow id =$  empty word (has no a's or b's  
• length = 0)

$$\boxed{\_} \text{ notation}$$

• Inverse :

$$w * \boxed{\dots} = id = \_$$

Inverses do not exist.

$$\begin{aligned} w &= \_ \\ \_ * \_ &= \_ \\ w &\neq \_ \\ w * \_ &= \_ \end{aligned}$$

concatenation operation has the identity and the associativity properties, but it fails to have the inverse property ok.

So, we have already made a start so, this is a good beginning, but we are sort of not quite, where we want to be we have not managed to construct a group starting with with  $a$  and  $b$  ok. And this is something that we will take up in the next lecture.