Algebra - I

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

1. Lecture 33 [Generators and Relations of Symmetric Group - II]

So, last thing we talked about Generators and relations for the symmetric group S_3 . Now, more generally what if we had the symmetric group S_n where $n \geq 2$ now this is just a slight difference . So, here is the theorem. So, let $n \geq 2$. So, I want to give generators and relations .

So, let $n \geq 2$, then S_n symmetric group is isomorphic to the free group on $n-1$ generators ok. So, let me give them a name now $F(\{a_1, a_2, ..., a_{n-1}\})$. So, there are $n-1$ in all and modulo the normal subgroup N generated by where N equals the normal subgroup generated by a short list of relations.

So, what are the relations we need by the following elements ? First a_i^2 ok. So, this is like the a^2 and the b^2 that we had in the case of S_3. So, this is a_i^2 for $1 \leq i \leq n$. So, this is one set of elements I need The second collection of elements I need are like the ab whole cubed that we had in the case of S_3 . So, that is the following. I take each generator a_i and multiply it with sort of its adjacent generator the next one a_{i+1}. So, I look at $(a_i, a_{i+1})^3$. Now, here i

$\underline{S_n}$: $\underline{\text{gen. \& relations}}$

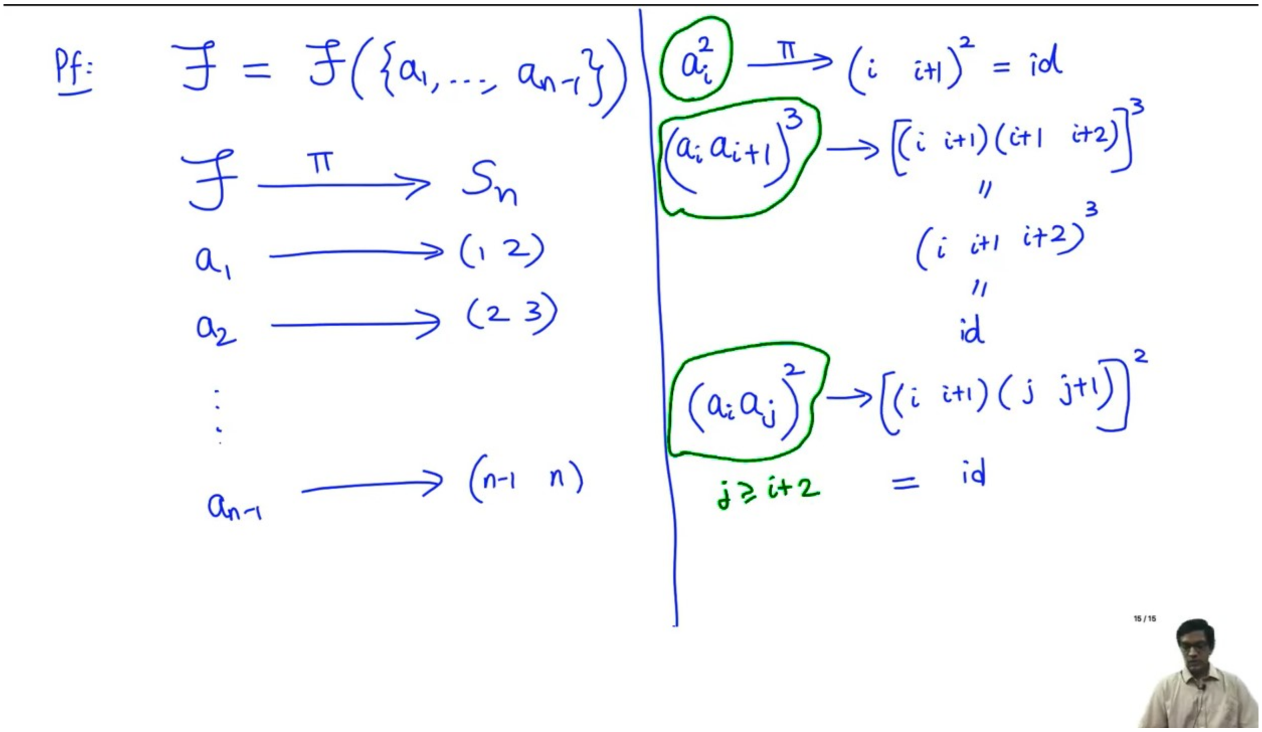
$\underline{\text{Thm}}$: Let $n \geq 2$. Then

$$S_n \approx \frac{\mathcal{F}(\{a_1, a_2, \ldots, a_{n-1}\})}{N}$$

N = normal subgroup generated by

$$\left\{ \boxed{\begin{matrix} a_i^2 \\ 1 \leq i \leq n-1 \end{matrix}}, \boxed{\begin{matrix} (a_i a_{i+1})^3 \\ 1 \leq i \leq n-2 \end{matrix}}, \boxed{\begin{matrix} (a_i a_j)^2 \\ 1 \leq i, j \leq n-1 \\ j \geq i+2 \end{matrix}} \right\}$$

14 / 14



can go from sorry, here it can go till $n-1$ here it can go until $n-2$ ok. So, this is the second sort of element I need in the kernel.

And, the third sort which we did not have in the case of S_3 because it is too small, but here we will have it in general is elements of the following form. So, let us take any a_i and multiply it by a_j and take the ^{2} of this element . Now, what are i and j here? $j \neq i+1$ ok. So, j has to be greater than i, but sort of farther than just one step apart ok. So, it is two steps or more from i. So, here we say thati and j well let us say i and j are firstly, between 1 and n $-$ 1 , but j is at least $i+$ 2 . So, this is the third collection of elements you need.

And, well between them they together they give you a collection of relations . So, they give you a set of elements and the normal subgroup generated by this set is exactly going to be the kernel of of the the map from the free group to this ok. So, let me sort of give you an indication of the proof which is almost along the same lines as for S_3 .

So, the first thing is from the free group, so let F denote the free group on these n $-$ 1 generators . From the free group we can define a map a homomorphism $\pi : F \to S_n$ as follows ; it takes, so this is a homomorphism π like in the case of $S_3 a_1 \to (12)$, $a_2 \to (23)$ and so on till $a_{n-1} \to (n-1, n)$, ok. And, as before thisthis defines a homomorphism by the universal property of of free groups, it is enough to specify it on these elements a_1 , a_2 , a_{n-1} ok .

But the fact that you are mapping it to these transpositions implies in particular so, observe that just like in the case of S_3 that each a_i^2 is going to map under π to this transposition $(i, i+1)^2$ ok and a transposition of course, has order 2 ok. So, each a_i^2 maps to the identity. So, a_i^2 is in the kernel, if I take a pair of consecutive elements (a_i, a_{i+1}) where does it map?

$N \subseteq \ker \pi$

$$\begin{tikzcd} \frac{F}{N} \arrow[r, two heads] \arrow[rr, bend left] & \frac{F}{\ker \pi} \arrow[r, "\sim"] & S_n \end{tikzcd}$$

$$gN \longrightarrow g(\ker \pi) \longrightarrow \pi(g)$$

Claim $\longrightarrow$ is an isoM.

Pf: Claim $\left|\frac{F}{N}\right| \leq n! = |S_n|$

Well, it maps to the product of these two consecutive transpositions , but that is just a three cycle $(i, i+1, i+2)$ whose cube is identity. So, therefore, this cubed is just cube of this product which is again the identity ok.

So, thus far it is like the the computation for S_3 and now, comes the newingredient if I take (a_i, a_j) two generators which are far apart meaning not just one step apart , but at least two steps apart, then their product maps to well what is it mapped to? It maps to $(i, i+1)(j, j+1)$. But, these are now two disjoint transpositions ok. There they have no elements in common because $j \neq i+1$ it is greater than $i+2$ greater than equal to $i+2$. So, this is like a product of two disjoint transpositions and this element still has order 2 . So, if you take the square of this, it is just going to give me the identity again .

So, that is where we we got those those relations . So, a_i^2 is surely in the kernel, $(a_i, a_{i+1})^3$ is in the kernel and $(a_i, a_j)^2$ is in the kernel this is for $j \geq i+2$ ok. So, we know for sure that the the subgroup N that we wrote out the normal subgroup generated by these these elements that is surely contained in the kernel .

So, what we know is that this normal subgroup N like in the case of S_3 is contained in the $\ker\pi$ and again one sort of proceeds in the same fashion as before . You know that $\frac{F}{ker\pi}$ is well there is an isomorphism to the group S_n and since $N \subseteq Ker(\pi)$ from $\frac{F}{N}$ to this I have a surjection ok . Just the usual the same maps that we wrote out before $gN \to g\ker\pi \to \pi(g)$.

So you have these these maps and to prove that N equals $\ker\pi$ is the same as showing that this this whole composite map is is an isomorphism . So, if we can take this composition here and show that this composite map is an isomorphism, then we are done ok . So, that is what we are we still have to prove andto prove that so, need to prove that this green arrow .

<u>Pf:</u> Proceed as in the case of S_3

$$\{[\omega]N : [\omega] \in \mathcal{F}\}$$

<u>HINT:</u> <u>Do it for S_4</u>

$$\begin{array}{ccc} a_1, & a_2, & a_3 \\ \| & \| & \| \\ a & b & c \end{array}$$

$$T = \{ \_N,\ aN,\ bN,\ abN,\ baN,\ abaN \}$$

$$cT = \{ cN,\ caN,\ cbN,\ \dots \}$$

So, this green arrow is an isomorphism that is the claim ok. And, to prove that I mean the proof is still indirect like before which is we show that $\frac{F}{N}$ has at most the number of elements in in S_n . So, claim the proof proceeds via counting argument we show that this can have at most n factorial elements and recall that is the cardinality of S_n .

Once you show this, because there is a surjection it has to have at least n factorial elements and the claim now . So, the claim further claim is to say it has at most n factorial elements. So, together it will show that it has exactly $n!$ elements and then you know you proceed like in the case of S_3 .

So, now, I am I am sort of just going to indicate how how to do this. You have to proceed as in the case of S_3 . So, the proof proceed as in the S_3 case as in the case of S_3 ok which is that you have to write out all the the different possible cosets of elementsof this kind look at $[w]N$ and write out what are the all the possible cosets. So, look at all this $\{[w]N : [w] \in F\}$ and now you will have to countthe cosets and show that there can be at most $n!$ of them .

So, I wouldsort of say the hint is first do it for S_4 do it for S_4 and that will sort of tell you how to how to do the general case . And, for S_4 let me just tell you what is it that you have to prove . So, here I have three generators in the case of S_4 . So, recall I had a_1 , a_2 , a_3 these are the three generators .

So, maybe it is easier to let us just rename them as a, b and c in the case of S_4 . So, what we had in the case of S_3 was the following . We said look at the following six cosets. So, those those very same cosets will also be required here aN, bN, cN sorry there is no c here $\{N, aN, bN, abN, baN, abaN\}$. So, these six cosets were what you need in the case of S_3 . Now, in the case of S_4 we will need 24 cosets. ok What are the 24? Well, these 6 certainly are there in addition we also need this look at what I call cT which is the very same 6 cosets with c multiplied on the left dot dot dot. Same thing with so, look at bcN and $abcN$ ok this will again give me a list of six bcN sorry, bcT, I am sorry T was my set of six cosets . So,

$bcT = \{ bcN, \ bcaN, \ \dots \}$

$abcT = \{ abcN, \ abcaN, \ \dots \}$

Applications:

Allows us to construct Homomorphisms from $S_n \longrightarrow G$

Prop^n: Let $g_1, g_2, \dots, g_{n-1} \in G$ satisfying

$g_i^2 = id$, $1 \leq i \leq n-1$, $(g_i g_{i+1})^3 = id$, $1 \leq i \leq n-2$ and $(g_i g_j)^2 = id$ $\forall j \geq i+2$.

bcN then there was so, you have aN look at $bcaN$ dot dot dot six of them . $abcT$ again is I take $abcN$. So, I had aN, so, I just put $abcaN$ dot dot .

So, I have $6 + 6 = 12$ on this page and 12 on the earlier page . Show that these 24 cosets are all you need . Any other word that you write out in the a, b and c will always reduce to one of these these 24 ok. And the way to do it is sort of also an an inductive process only look at words which have a's and b's to start with ok and that is like the S_3 calculation which we have already done and now, insert the c.

And, now put the extra cN and see what happens ok. So, I am going to leave this for you to explore and play with. So, it it is a_i t is a very good exercise because it sort of gives yousome facility in working with free groups and so on , ok. But let me now move on to what is the application of of this generators and relation procedures . So, here are some applications. If you can realize a group by way of generators and relations what it gives you is a way of constructing homomorphism's that is the key key use of having generator simulations . If I want to construct homomorphism's from my group S_n ok S_n is the group which I now understand in terms of generators and relations I can construct homomorphism's from $S_n \to G$ ok.

How do I construct them? Well, here is the the proposition . So, I should say applications of of the generators and relation procedure, it allows us to constructallows us to construct group homomorphism's from S_n to any other group ok. So, what is the the procedure? How do you construct a group homomorphism? Well, here is what you need to do .

You need to find $n - 1$ elements in your group G which sort of obey the same relations as the generators of S_n ok. So, let $\{g_1, g_2, ..., g_{n-1}\} \in g$ satisfying the following properties that g_i^2 is the identity for all $1 \leq i \leq n - 1$. So, this is identity of the group G .

Then $\exists$ a group hom $\varphi: S_n \longrightarrow G$ st $\varphi(\sigma_i) = g_i$

where $\sigma_i = (i \;\; i+1)$ $\quad 1 \leq i \leq n-1$.

Proof: $\exists$ a homomorphism $\mathcal{F}(\{a_1, a_2, \dots, a_{n-1}\}) \xrightarrow{\pi} G$

$$a_i \longrightarrow g_i \quad \forall\, 1 \leq i \leq n-1$$

Let $N =$ normal subgp gen by $\{a_i^2, (a_i a_{i+1})^3, (a_i a_j)^2\}$

Then: $N \subseteq \ker \pi$ by the given hypotheses

Now, $(g_i g_{i+1})^3 = id$ in the group G this is for all $1 \leq i \leq n-2$ and the third set of relations which is $(g_i g_j)^2 = 1$ is the identity for all $j \geq i+2$ ok and between $1 \leq i \leq n-1$. So, in other words, I find $n-1$ elements of my group G which satisfy the same relations in the group G that my generators of S_n are supposed to satisfy .

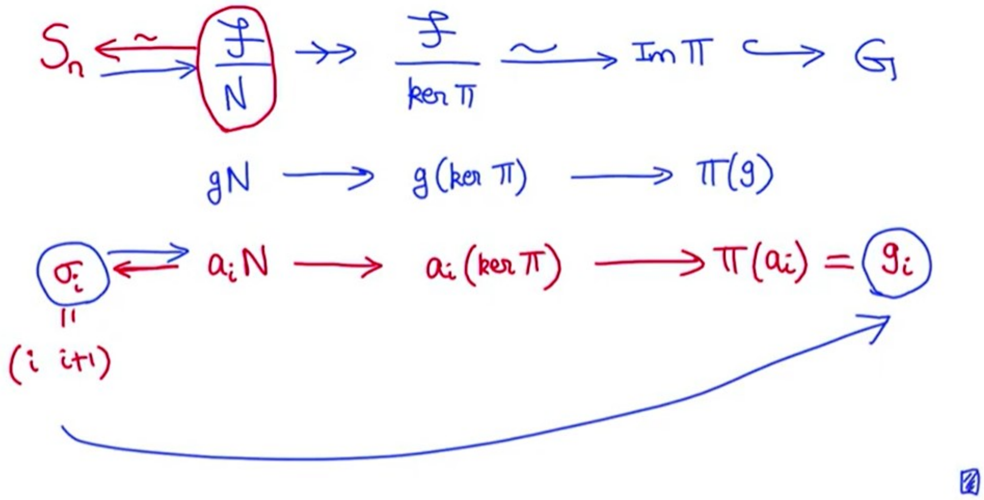
If I can do this then I am guaranteed there exists a group homomorphism from S_n to my group G such that which sendsthe the corresponding elements of S_n . So, what elements? The elements $\sigma_i \rightarrow g_i$ ok where σ_i is are the the transpositions where $\sigma_i = (i, i+1)$ ok.

So, if you want to map the transpositions to any elements of the group G those elements must satisfy the same relations that the transpositions do and conversely that is all you need if you have that then automatically there exists a well defined group homomorphism ok. So, let us prove this proof . Where do we get this from? Well, from from the we need to go to the free group to get this ok. We cannot just work with S_n itself to to prove this fact. So, observe that from my free group on n $-$ 1 generators .

So, I had the free group $F(a_1, a_2, ..., a_{n-1})$. From that free group I always have a map $F(a_1, a_2, ..., a_{n-1}) \rightarrow G$ ok. What map is this?Maybe we should call it something π this map just sends the generators $a_i \rightarrow g_i$ ok for all $1 \leq i \leq n-1$.

So, there exists a homomorphism there exists a homomorphism like this. Why does it exist? Well, from the universal property of free groups I can always specify arbitrarily where I want to map my a_i 's and that always defines the homomorphism ok. But, recall thatthe the g_i is satisfy those special relations .

So, let N be the normal subgroup generated by those relations normal sub group generated by the set $\{a_i^2, (a_i a_{i+1})^3, (a_i a_j)^2\}$. So, here I am I am just suppressing the the the bounds by I mean the ranges for i's and j's, but I mean we have we have looked at this before . So, normal subgroup generated by that set of relations.

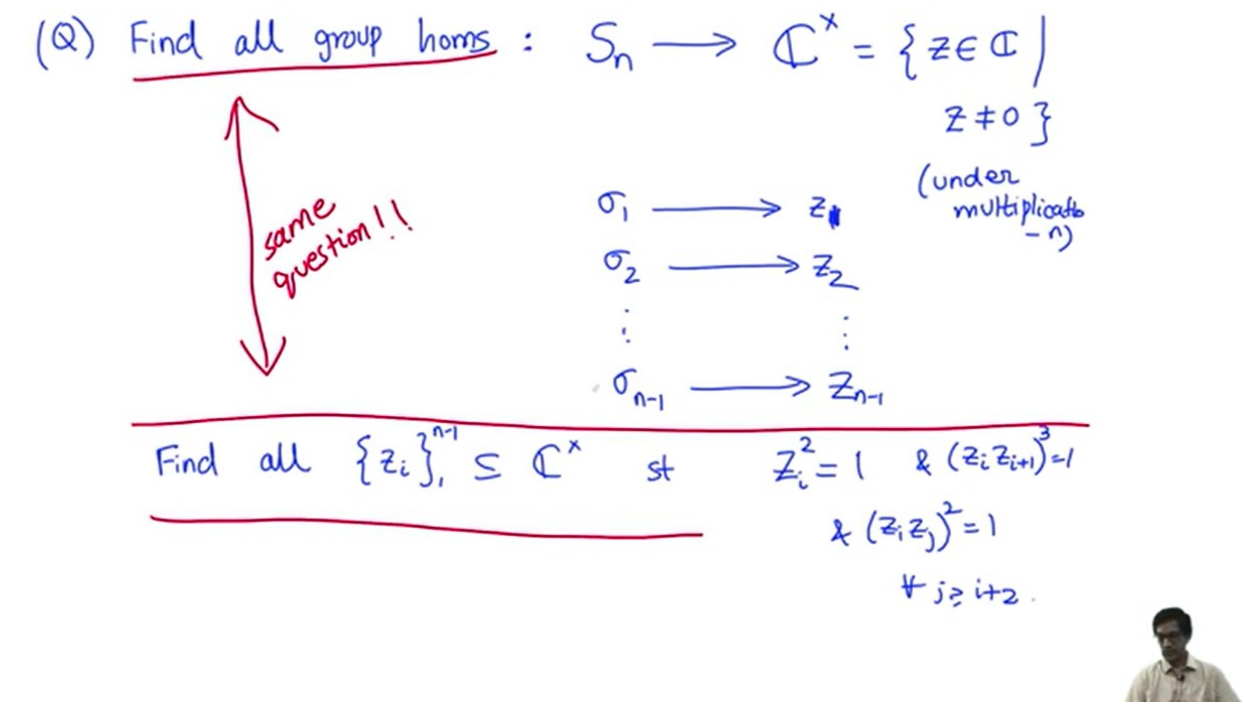


Then observe that then observe that since g_i satisfy the same relations it is clear that each of these generators and a_i^2 will map to g_i^2, but that g_i^2 is the identity ok and so on . $(a_i ai + 1)^3$ will map to $(g_i g_{i+1})^3$ but then that was assumed to be the identity in the group ok. So, in other words all thesethese relations are actually satisfied in G, in other words each of them lies in the kernel of this homomorphism π ok by the hypothesis by the given hypothesis on the elements g_i .

Now, we are almost back to our our usual situation so, what does this mean? So, I have now a map from $\frac{F}{N} \to \frac{F}{Ker(\pi)}$ and $\frac{F}{Ker(\pi)} \cong Im(\pi)$ by the first isomorphism theorem this is isomorphic to the the image of π. The imageπ is some subgroup of my original group G .

So all this is just repeating the same arguments we did before. So, I can get a sequence of homomorphisms like this this is just $gN \to g\ker\pi \to \pi(g)$ ok πg is a subset of G. So, this is for all g_i n my free group F ok. So, I get this this sequence of homomorphisms . Now,what is it that we have? Well, we wanted to get a map from the symmetric group $S_n \to G$ ok, but observe that this $\frac{F}{N}$. So, now, comes our our the use of our theorem this last guy $\frac{F}{N}$ remember is exactly isomorphic to the symmetric group right from $\frac{F}{N}$ recall I actually have an isomorphism to S_n ok and what is this this isomorphism do now we just have to unravel what this isomorphism does ?

So, let me write out this this isomorphism just on those special elements . So, what was this isomorphism doing? Well, if I take the special generator $a_i N$ it was mapping it to those the the transposition σ_i right. This is how we defined that map how did we prove the isomorphism between $\frac{F}{N}$ and S_n we defined a map from $F \to S_n$ which takes $a_i \to \sigma_i$ ok and so, the coset $a_i N$ therefore, was mapping to $\sigma_i N$ just by the first isomorphism theorem . So, now, we we are all set because now we know what $a_i N$ goes to. It goes to a_i kernel π which



in turn goes to π of a_i , but πa_i by definition was g_i ok. So, we just have to stare hard at this equation .

So, of course, this this isomorphism is is defined as going in this direction , but all I have to do is just think of the the the reverse isomorphism I just take the map from S_n to this which is the inverse of this map . So, this map σ i maps to $a_i N$ maps to a_i kernel π maps to g_i . In other words, what I have done is to show that I have constructed a homomorphism from S_n to the group G and this homomorphism takes the element σ_i exactly to the given element g_i ok and that is that is what we set out to prove that finishes the proof.

So, if you give me g_i 's with the correct properties, then I can construct for you a homomorphism from the group $S_n \to G$ ok which maps the the the σ i's to the element which maps these σ i's to the elements g_i ok. So, that is the the crux of this this proposition .

So,in particular so, here is one one simple application of this So, so here is a question what are homomorphism? So, find all group homomorphisms from the symmetric group S_n to? What I will call $\mathbb{C}^\times$. So, this is just the set of nonzero complex numbers under multiplication $Z \neq 0$, thought of as a group under multiplication ok this forms a group because I have inverses and so on . So, the question is uh what are all the group homomorphisms that you can define from S_n to this group? Well, I let us think of it as an application of our earlier principle . So, what did we say in order to define a group homomorphism from S_n to to $\mathbb{C}^\times$ what I need to do is give you elements . So, I I know that I have these $n-1$ generators of S_n and if I stipulate their images . So, $\{Z_1, Z_2, ...Z_{n-1}\}$, if I tell you where they map then,that sort of determines my homomorphism . So, we needfind all group homomorphisms is the same as saying fine.

So, I am rewording the question find all collections of Z_i $1 \leq i \leq n-1$ of complex numbers non zero complex numbers satisfying the following relations that all $Z_i^2 = 1$. So, 1 is the identity for the multiplication operation and $(Z_i, Z_{i+1})^3 = 1$ and $(Z_iZ_j)^2 = 1$ for all j greater than or equal to $i + 2$ ok.

So, these two problems are actually equivalent. It is it is enough to do this . So, so this thing that I wrote here is the same as the original question ok, that is the that is the beauty of this . So, just homomorphisms are just these n $-$ 1 tuples of special elements which satisfy the correct relations . Now, it is easy we just have to find such complex numbers . So, observe Z_i^2 equals 1 for all i means of course, that what are the the conditions. We conclude Z_i can only be + or $-$ 1 for all i, ok. Now, if Z_i is say $-$ 1 for all i.

So, here are two cases either Z_i equals 1 + 1 for all i ok that gives me one obvious homomorphism which is that the identity homomorphism everything maps to the identity. So, this is this is a valid choice because σ_i maps to 1 for all i means the homomorphism from S_n to C star is just every every permutation maps to 1 . Because I can write any permutation as a product of these simple transpositions and if every transposition maps to 1, then every element has to map to 1. So, that is case 1.

Case 2, suppose $Z_i = -1$ for some i just a single i then I need to figure out what are my choices is this a valid choice of Z_i . Well, at the moment I only used 1 relation I still have other relations which is $(Z_iZ_{i+1})^3 = 1$, . So, it is trying to use the cube relation . So, let us look at Z_iZ_{i+1} . So, if if i is not $n - 1$, then I I will have something next to it the next guy . So, observe $(Z_iZ_{i+1})^3 = 1$ is supposed to be 1. Well, what does that this mean if $Z_i = -1$ and the product cubed is 1, then the only way out. And and $Z_{i+1} = -1$, right. So, there is only 1 choice both Z_i and Z_{i+1} must have the same sign; they have opposite signs their product is -1 . So, this means that Z_i and Z_{i+1} have the same sign .

In other words, since $Z_i = -1$ this means that $Z_{i+1} = -1$ a ok. Likewise, so I can replace i by $i-1$ and conclude that $Z_{i-1} = -1$ ok because it is the adjacent guides the previous guy I can apply the same relation with $i-$ 1 in place of i ok and and we keep going. Since $Z_{i-1} = -1$ the one before it which is adjacent to it must also be the same sign; since $Z_{i+1} = -1$ the one after it must also be the same sign and so on.

So, on the 1 hand you keep going forward and on the other hand, you sort of keep going backward and this this argument says as soon as one of the Z_i 's is $-$ 1 everybody after it is $-$ 1 and everybody before it is $-$ 1 ok. So, this finally, implies that every single Z_i 's so, Z_j has to be $-$ 1 for all j .

So, this is the only other possible homomorphism and again what does this homomorphism look like at the level of the what does it do to the other elements of the symmetric group? So, if I take S_n to 2 C hash. So, I have said σ_1 , σ_2 , σ_{n-1} all the simple transpositions map to -1 that is what this homomorphism does , but what what about the other elements? What if I take an arbitrary permutation in S_n what does it map to? Well, what am I supposed to do? I take that arbitrary element and I write it as a product of the simple transpositions , ok. And, this map phi is well, what is it? phi g_i s + 1 well, it is it is always + or $-$ 1, but it is + 1 if g_i s a product of an even number of transpositions of an even number of simple transpositions .

These simple transpositions are just the σ_i's and it is $-$ 1 if well if this is an odd number of simple transpositions, ok and recall this is exactly the thing that you have seen before this is the sign map, this is the sign of a permutation which is if you write it as a product of transpositions whether you have an even or an odd number ok. So, what we have proved therefore, is that there are just two possible homomorphism's . So, the question was find

$z_i = \pm 1 \quad \forall i$

(1) $z_i = 1 \quad \forall i$

$\Rightarrow \sigma_i \mapsto 1 \quad \forall i$

means the hom.

$S_n \to \mathbb{C}^\times$

$g \to 1$

(2) $z_i = -1$ for some i

$(z_i z_{i+1})^3 = 1$

$\Rightarrow$ z_i & z_{i+1} have same sign

$\Rightarrow z_{i+1} = -1 \Rightarrow z_{i+2} = -1$

$\Downarrow$

$\vdots$

$\Rightarrow z_{i-1} = -1$

$\Rightarrow z_{i-2} = -1$

$\Rightarrow \cdots \qquad \Rightarrow z_j = -1 \quad \forall j$

$S_n \xrightarrow{\varphi} \mathbb{C}^\times$

$\sigma_1 \longrightarrow -1$

$\sigma_2 \longrightarrow -1$

$\vdots$

$\sigma_{n-1} \longrightarrow -1$

$$\boxed{\varphi(g) = \operatorname{sign}(g)}$$

g = product of the σ_i's

$$\varphi(g) = \begin{cases} 1 & \text{if } g \text{ is a product of an even number of simple transpositions} \\ -1 & \text{if } \ldots\ldots \text{ an odd } \ldots\ldots \end{cases}$$

all homomorphism's from $S_n \to \mathbb{C}^\times$ turns out there are exactly two of them ok which is the identity which takes everybody to 1 and the other which takes everything to a -1 .