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

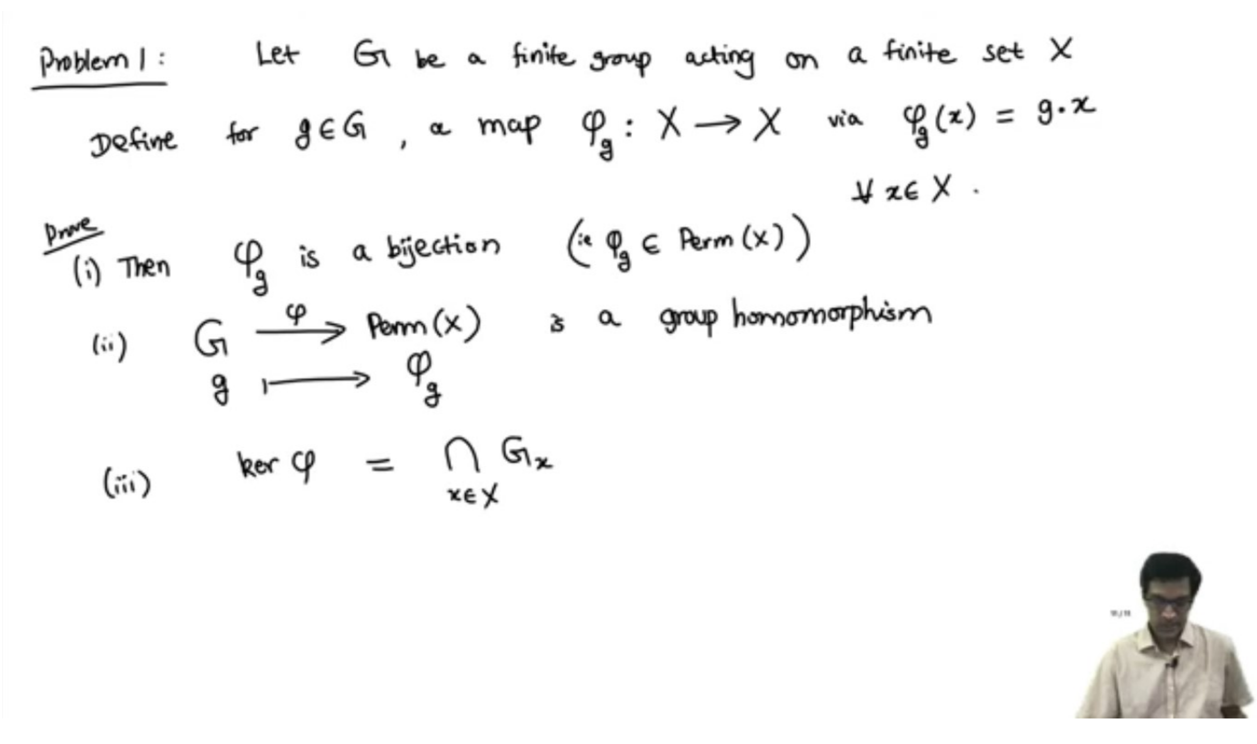
1. Lecture 21[Problem Solving II]

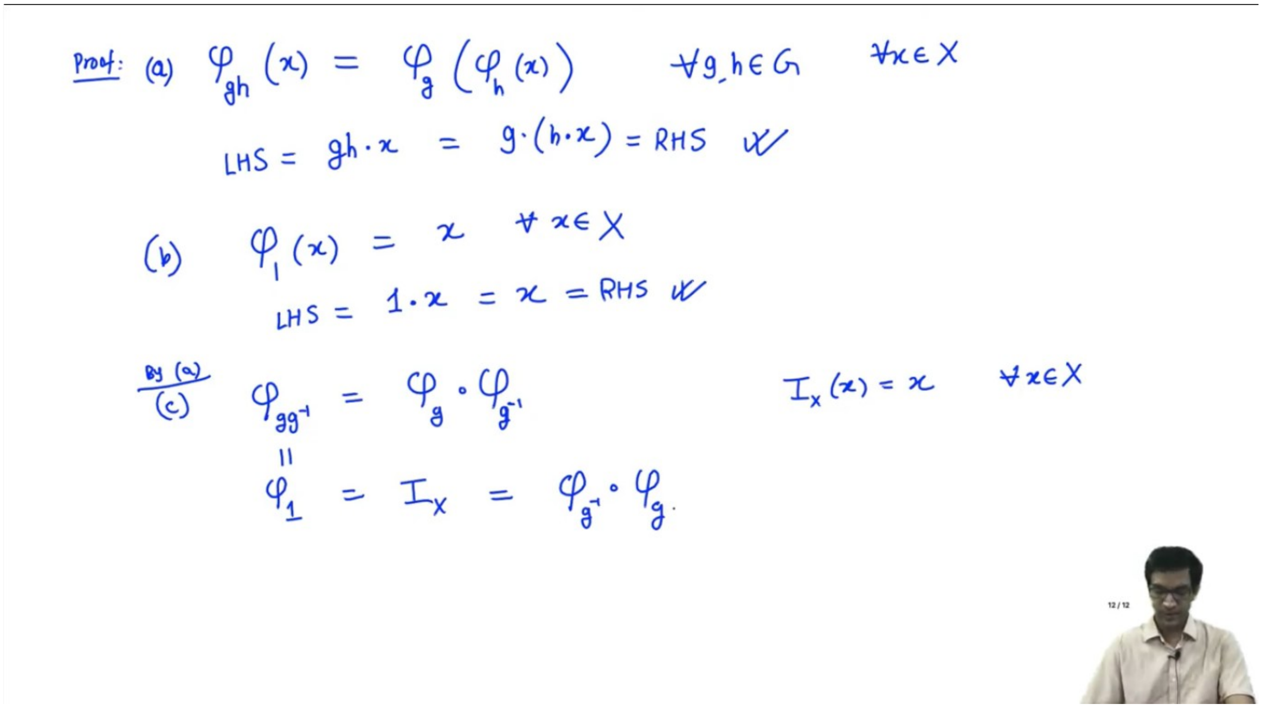
Let us do more problems on group actions. So, here is a somewhat general principle, so I am stating in the form of a problem here. So, suppose I have a group action. So, let G be a finite group acting on a finite set X . Define the following map define for $g \in G$ a map,

$$\phi_g : X \to X$$
$$\phi_g(x) = g \cdot x$$

So, this is for all $x \in X$ So, define a map like this. Now, sort of many many different things; then prove the following. So, these are all things we need to prove; prove number one, then this map ϕ_g is in fact a bijection , is a bijection , ok. And the set of all bijections we can, in other words ϕ_g belongs to we call this $Perm(X)$, the set of all permutations of this finite set x or the set of all bijections .

- Then ϕ_g is a bijection. (i.e. $\phi_g \in Perm(G)$)
- $G \to Perm(X); g \to \phi_g$ is a group homomorphism.
- $ker\phi = \cap_{x \in X} G_x$





So, here are three assertions we need to prove; you can view this as just being another way of thinking about group actions. So, let us prove these statements first. So, each of them is rather easy. So, if I have a map, if I have a group action. So, what is given? I have a group action ok and I construct from the group action; I construct maps ϕ_g a defined like this. So, first thing we need to show that ϕ_g is a bijection ok . And, also that this is a group homomorphism. So, let us prove the following fact. So, proof .

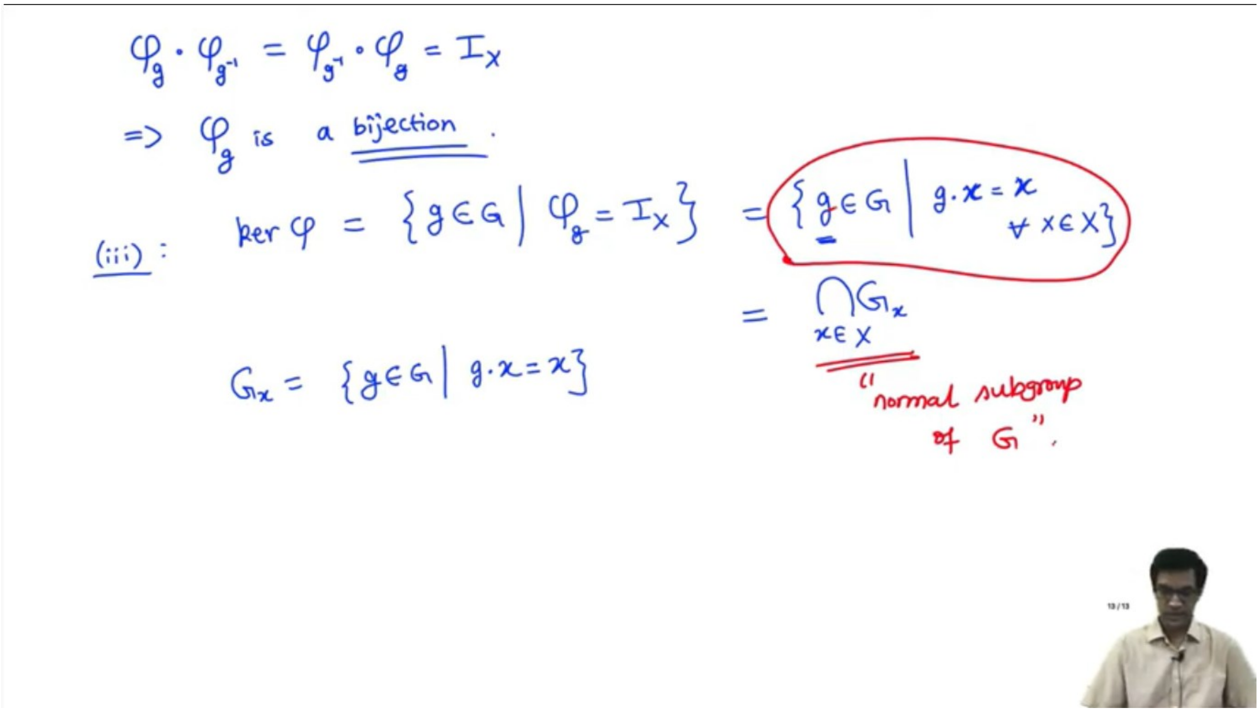
So, let us prove first, what is $\phi_{gh}(x)$? So, I claim

$$\phi_{gh}(x) = \phi_g(\phi_h(x)); \forall g, h \in G; \forall x \in X$$

So, this is the first statement we will prove a ok; why is this? Well, this is more or less the definition of the action.

So, what is the left hand side now? The left hand side by definition was just the product $gh \cdot x$. But if you remember the one of the axioms of the group action says that, $g \cdot (h \cdot x)$; but that is exactly the right hand side, which is ϕ_g evaluated on $\phi_h(x)$ by definition is exactly this ok.

So, this done. Property b, ϕ_1 is a identity of x . So, the identity element which I will denote as 1 as we have done before is I claim just X . Now, in other words ϕ_1, where 1 identity element of the group acts as the identity permutation of the set X , ok. Why is this true? Well, that is the another axiom of group actions which is that; so the left hand side here is just 1 acting on x and by definition and by the axiom that is just $1 \cdot x = x$ itself . So, it is also true, ok. So, what is this? This imply in particular it says that, observe if I take $\phi_{gg^{-1}}(x)$ of x or another way of rewriting the first axiom $\phi_{gg^{-1}} = \phi_g \phi_{g^{-1}}$. So, by, so this is by a , special case in which I take $h = g^{-1}$. But observe that this is just ϕ_1 and part b says that this is just the identity map of I_x ok. This is identity of x , this is just a map which sends $x \to x$ for all $x \in X$. This is a, this is an element of per max, it is a map from $x \to x$

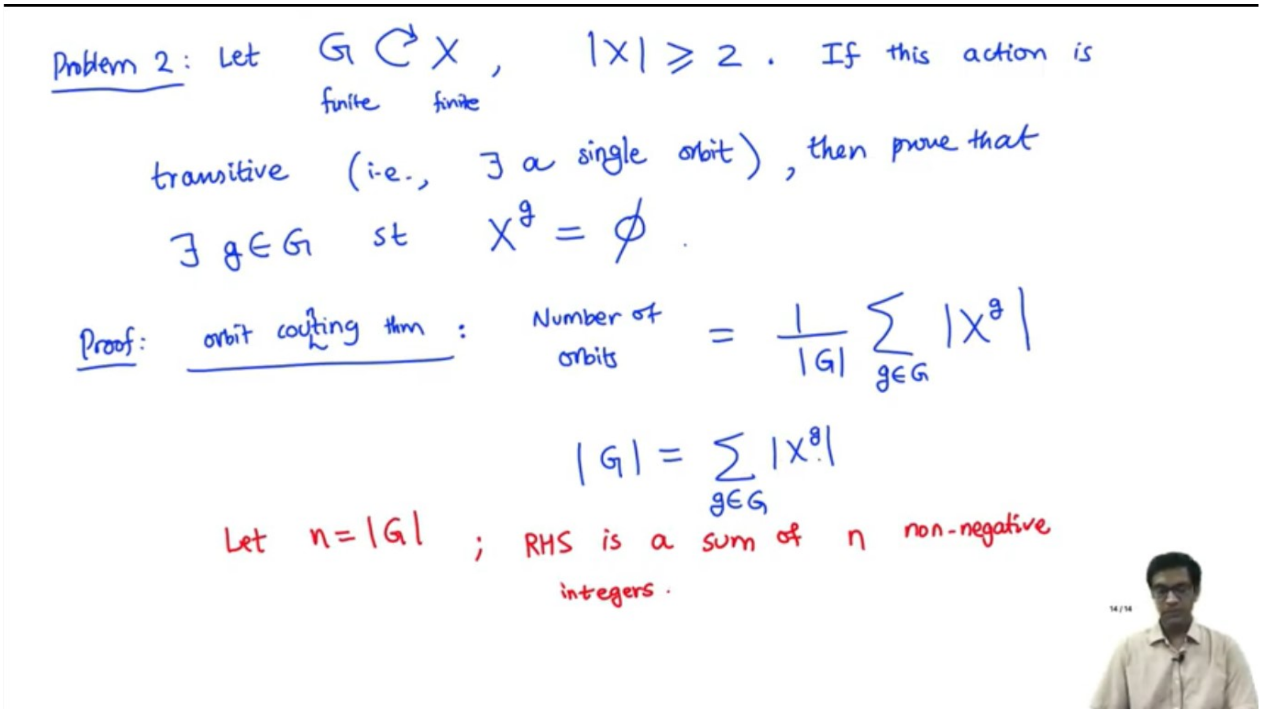


, ok. So, what does this mean? It says that if I take the composition of $\phi_g \cdot \phi_{g^{-1}}$, I just get identity, ok. And similarly you know, similarly this is also equal to $\phi_{g^{-1}g}$ ok, just repeat the same argument that I just did, ok.

So, what is this give us, why are we doing all this? Well, this says that the map ϕ_g now in other words ϕ_g has a two sided compositional inverse, ϕ_g has the following property that when I compose it with this map $\phi_{g^{-1}}$ on the left or on the right, it gives me back the identity map on I_X , ok. What does that mean? It means ϕ_g is a bijection right; a bijection is exactly maps, I mean you can think of it as a map which has left or right inverse . I mean which has both left and right inverses; here for finite sets of course, you sort of it is enough to check one, but from the more general point of view let us just look at both.

So, we have ϕ_g, $\phi_{g^{-1}}$ is sort of the both the left and the right inverse of the map ϕ_g, ok. So, it is a bijection. So, that proves part a of the proposition. But in fact, along the way we have proved all the other parts as well. So, observe that, so sorry what did we need to prove? This is part one of the proposition is done, which says that ϕ_g is a bijection. But in fact, we have also proved this that, it is a group homomorphism; because that is exactly these properties a and b ok, because it says that $\phi_{gh} = \phi_g \cdot \phi_h$ ok, and ϕ_1 goes to identity. So, that is exactly the properties a and b, exactly are the second point that we need to prove, ok. So, let us prove the last of the assertions that, the kernel of this map is just the intersection of the stabilizers, ok. So, let us see, what is the kernel of this map? So, I just now need to prove part 3 of this problem . To do this, I need to understand what the kernel of this map phi is ? By definition it is all those g in the group G such that phi sub g maps to the identity map, ok. But, what does that mean? That is its all those group elements g in G which have the property that g acting on x equals x for all x in the set X , ok.

$$Ker\phi = \{g \in G | \phi_g = I_X\} = \{g \in G | g \cdot x = x; \forall x \in X\} = \cap_{x \in X} G_x$$



$$G_x = \{g \in G | g \cdot x = x\}$$

But, then observe there is another way of thinking about this; I can say let me fix an x in my set capital X , then a group element g which belongs to the kernel. So, this g here must satisfy the property that g stabilizes x right, $gx = x$, ok. So, this means that, this element g certainly belongs to the stabilizer $g \in G_x$, ok.

So, this this element x here. So, G_x recall is a stabilizer G_x is group elements which stabilize that fixed x , ok. But then I want those group elements which stabilize x for every $x \in X$; well that is another way of saying that, this is just the intersection of all the stabilizers, ok. So, write this out in full by checking that you know what I wrote here; this guy is a subset of this side and conversely that the thing on the other side is a subset of this, ok . So, in any case, this is more or less more or less from the definitions, ok. So, here is an interesting thing that we have formulated that, if you take the intersections of the stabilizers of all the elements of the set X ; then what you get is actually a normal subgroup ok, because it is the kernel of a homomorphism, ok.

So, recall this must necessarily be a normal subgroup , ok. And this is sometimes a very useful construction, ok. So, that is the first problem. And the point here is that, you can actually view actions of well rather here. So, this part of the problem can often be thought of as an equivalent formulation of group actions ok; you can define if you wish a group action to be a homomorphism from the group g to the group of permutations of a set, ok.

Now, let us move on to problem 2 ok, which is the following; it say suppose I have an action of a finite group on a set . So, let G act on X ; everything is finite here G is finite, X is finite . And suppose $|X| \geq 2$, it is not a singleton; it is got at least 2 elements. Now, if this action is transitive , if this action is transitive; which means that , what does transitive mean? I e there exists a single orbit for this action; every element of X is in the same orbit some sense it all, they are all mutually you can get one from the other by acting some group element, ok. If the action is transitive, then prove, then prove that there exists at least one group element $g \in G$ which has no fixed points, such that $X^g = \emptyset$. So, recall X^g just means, a set of fixed points, ok .

So, which means g actually has no fixed points at all, ok. Again rather interesting statement in some sense it says that, when a group acts transitively on a set; so, of course, this cannot be true if the set only has one element; because then that element is fixed by all elements of the group ok necessarily. But, if you have at least two elements in your set and the group somehow acts transitively on this set; then at least some group element must cannot you know has to act in this interesting way that, it moves all elements of the set X ok, it does not fix any element, it moves all of them in some way, ok. So, let us prove this again , and through this we will just use the orbit counting theorem again.

So, recall the orbit counting theorem , which says counting theorem which says that, the total number of orbits, so the number of orbits is the same as 1 by the cardinality of the group $|G|$ summation the cardinality of the fixed points. Now, we have assumed that this is a transitive action, which means there is a single orbit, ok.

$$No\ of\ orbits = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

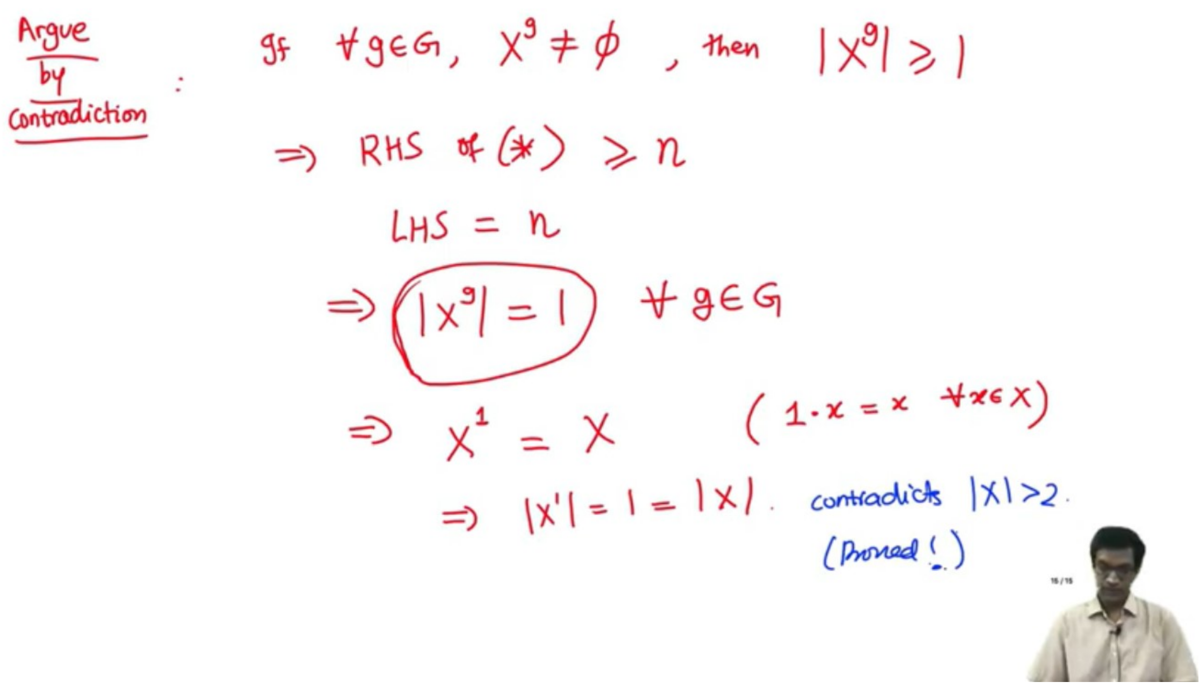
$$|G| = \sum_{g \in G} |X^g|$$

So, now, let me do also one thing, let me move the cardinality $|G|$ over to the other side. So, there is only one orbit. So, 1 into the cardinality of $|G|$; therefore is the sum of the numbers of fixed points for all group elements. Now, this is the equation we need to understand, ok. Now, let us look at the left hand side; the left hand side is the cardinality of the group itself. The right hand side, how many summons are there right? It is a sum of how many terms.

Well, if the cardinality of the group is let us call it some number; if you if the cardinality of the group is $|G| = n$, then the right hand side is a sum of n terms, ok. So, let us just give this a name, let n be the cardinality of the group; then we observe that the right hand side is a sum of n terms , ok. Now, what do we know about these n terms? They are all nonnegative numbers, ok. So, it is a sum of n nonnegative integers, because it is the cardinality of the set of fixed points. So, it is either 0, 1, 2, 3 and so on. So, it is a sum of n nonnegative integers , ok. Now, you know when I sum up n nonnegative integers and I have to get n as my answer; well then what does it mean? Well, if all these guys on the right hand side are to be positive, ok.

So, suppose I argue by contradiction; why should there exists at least one group element whose fixed points it is empty ? Suppose not, suppose every element had some fixed point set, non-empty fixed point set . So, let us argue by contradiction . If for all group elements $g \in G$ the fixed point set is now empty $X^g \neq \emptyset$. What does it mean? Then all these summons on the right hand side that I talked about over here right was the sum of all these numbers; each number is at least 1, because there is at least 1 fixed point, ok .

And if each number is at least 1, then since there are n terms on the right hand side; the right hand side is therefore at least, let us called the equation star. The right hand side of the equation star; which means the right hand side of equation star will automatically be at least n, because every summoned gives contributes at least a 1, ok. But, recall the left hand side is exactly n right that is the cardinality of the group, ok. Now, what does that mean? It



means that every summoned on the right hand side has to be exactly 1, that is the only way in this in which this equation can possibly hold , ok. So, is this this I hope this argument is, ok. All the summons on the right hand side are 1 or more, but 1 is the only possible choice; because even if one of them is 2, then the right hand side, the sum on the right hand side will become strictly bigger than n, ok. But we know it has to equal n, ok. So, that is a very strong requirement.

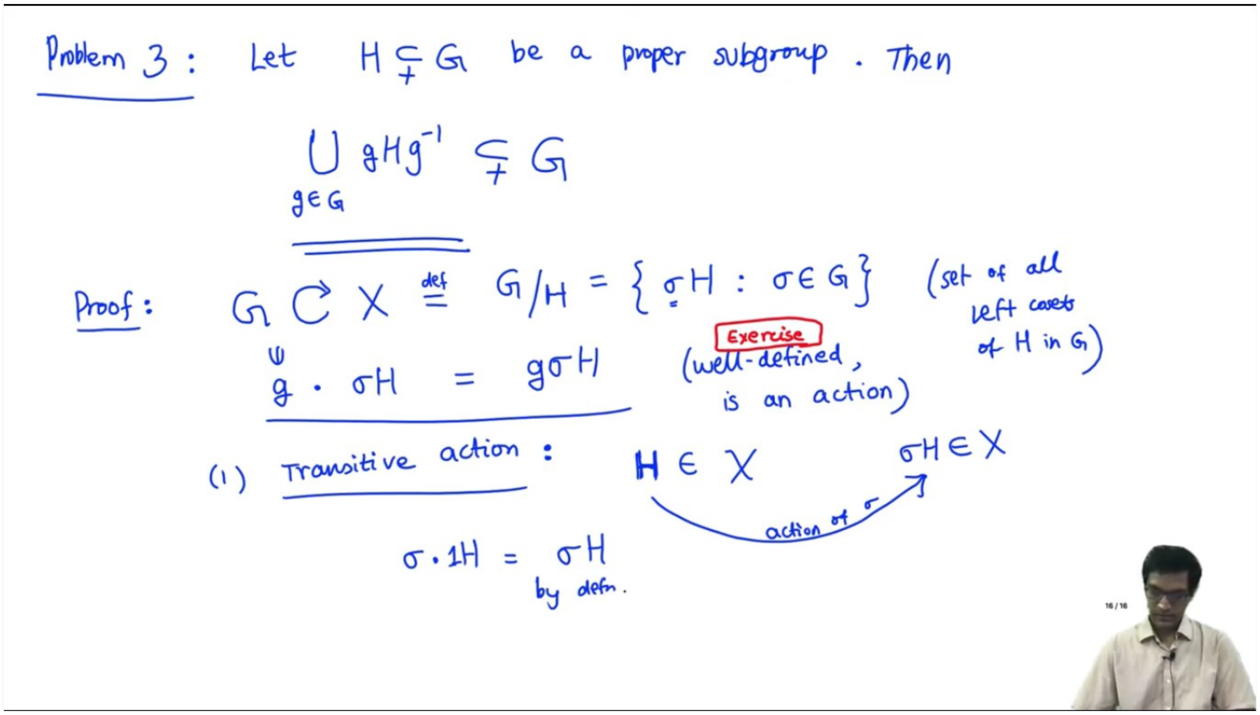
So, it says that the fixed point set; if every group element has a fixed point, then every group element must have a unique fixed point, ok. But this is already a problem, because there is one very special element in the group which is the identity itself. So, let us take the identity element of the group ; that guy has the following property that, what are the fixed points for the identity element? Well, the identity fixes every element of the set X right; recall the axiom for group actions says the identity of the group acting on a set element $x \in x$ for all $x \in X$; which means that the every element is a fixed point of identity .

So, that is what I have written like this; this fixed point set of identity is the whole set X , ok. So, what does this this statement therefore tell us? This means that $X^g = 1$; this means that the set $|X| = 1$ itself must have cardinality 1, ok. But that is a contradiction, because we assume to begin with that; so contradicts our initial assumption that there are at least 2 elements in X , ok. So, therefore, we have proved this fact . So, that is a that is a proof that at least one element must act without any fixed points, ok.

Now, let us do one more problem which is very closely related to this one . So, problem 3 ; so it says the following, suppose I take a group and I take. So, let $H \subset G$ be a proper subgroup , ok . In fact, for all this you do not even need finiteness for H and G and so on.

But I mean if you wish you can assume that they are all finite . Let $H \subset G$ be a proper subgroup; then

$$\cup_{g \in G} gHg^{-1} \subset G$$



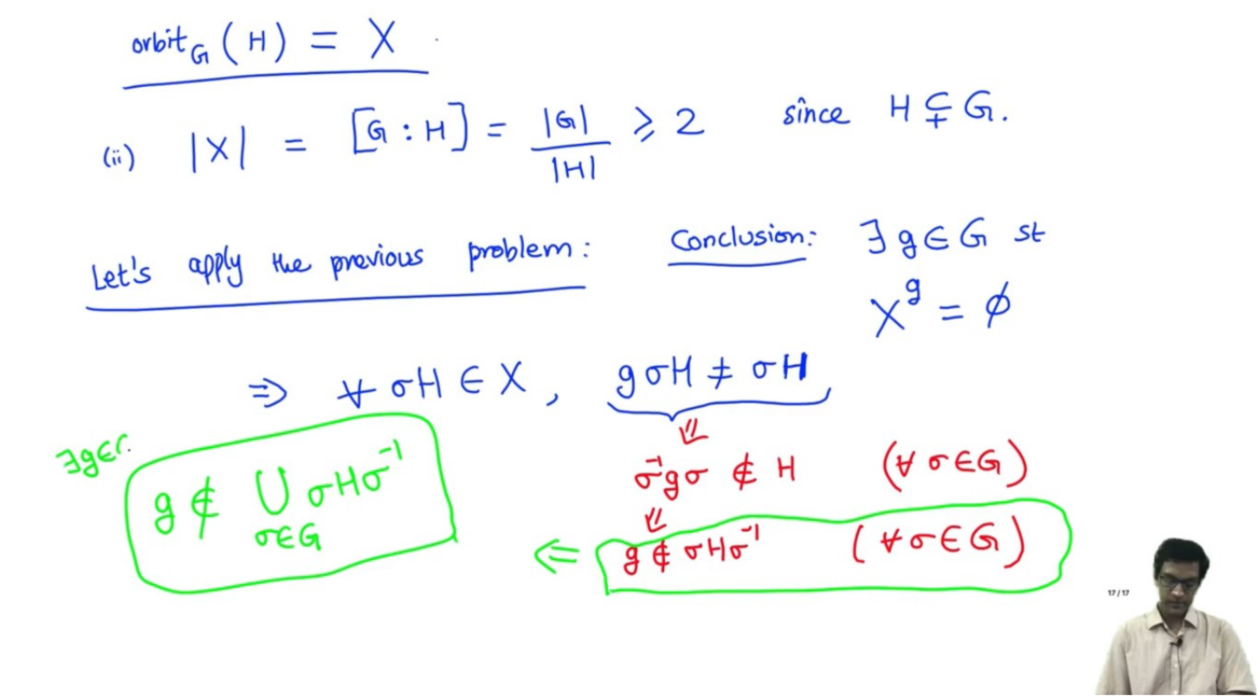
See the left hand side here is only a subset of G ; but the assertion here is that, this must still be a proper subset of G , you cannot somehow by taking unions of conjugates, you cannot get every element of the group just from that, ok. So, let us try and prove this, this is seemingly nothing to do with group actions ; a does not seem to be a problem about group actions, more a problem about sub groups and group and the group itself. But let us reformulate it into the language of group actions, and we will see that in fact it is actually the previous problem in disguise ok; it is it is going to involve the previous problem just problem 2, ok.

So, let us do this. So, to do this we first have to construct a group action , ok. So, I am going to take the action of a group G of the given group G on a set X . So, how will I construct the set X ? So, here is the first thing to note, I will define this set X as follows; I take the set which I will denote $G/H = \{\sigma H : \sigma \in G\}$. So, H is not a normal subgroup here. So, when I say G/H , I do not mean, it is not a group or anything; but I can think of it as a set certainly, this is just the set of all left cosets.

So, this is all σH as σ ranges over G . So, this is just the set of all left cosets ok, the thought of only as a set. But in fact, it is a set on which the group G acts ok that is the interesting bit, what is the action that is the most natural thing; if I take a group element $g \in G$ and I take an element from X .

What is an element of X ? Well, it is a left coset. Well, how do I make it act? I just say it is a new left coset , the left coset of the element $g\sigma$ ok. So, it is easy to check that this is a well-defined . So, well definedness remember comes up, because in some sense I am choosing a representative of my coset while writing this definition; but it does not depend on which representative I pick of the coset .

So, this is well defined and in fact is a group action, is an action . So, I leave these two for you to check; exercise please do check that this is a well-defined action of the group G on this set X of left cosets, ok . Now, I have an action, now let us try to figure out; what the



properties of this action are? So, I claim the first property is that this is actually a transitive action ; in other words what are the orbits? Well, there is a single orbit, everything is in the same orbit. So, how do we prove this? Well, the easiest is to say; let us pick a particular coset, let us take this special coset H . So, look at this element H which is the coset inside my set X , it is a single element. I claim that every other coset can be obtained from this particular special coset by a suitable action of a group element. Well, how do I do that? It is more or less from the definition itself. What do other cosets look like? Any other coset looks like σH , every coset looks like this.

Now, how do I get σH from H ? Well, if you just see what this definition is, all it says is you just multiply on the left by the appropriate group element. So, this I can get σH from H by acting by σ, because σ acting on H . So, here it means I am sort of picking identity as my representative of H if you wish. So, σ acting on identity H is just σH by definition , ok.

So, what does that mean? It means that every coset lives in the orbit of this element H ; which means that the orbit under this group action G for this element H is in fact the whole set X , ok. So, therefore, it is a transitive action, there is only a single orbit, ok. Now, I am going to use my previous statement. So, I am going to use my previous problems; so let me just recall what the statement of the previous problem was. I needed a group acting on a set X , the cardinality of the set $|X|$ has to be at least 2 . And if this action is transitive, then we needed to prove that; then we proved that there is at least some group element which has no fixed points, ok.

So, let us verify the hypothesis, first we have checked its transitive; the second hypothesis I need is to check that the cardinality of the group of the set $|X|$ is at least 2. But observe the cardinality of the set $|X|$ is nothing, but the cardinality or the index of $[G : H]$ if you wish , ok. The number of co sets and that is just cardinality of $\frac{|G|}{|H|}$ when they are all finite.

And I have assumed that H is a proper subgroup of G ; so which means that, this is at least 2, since H is assumed to be proper , ok. So, the second hypothesis is also there, it is also satisfied, ok.

Now, let us apply the previous problem . Let us apply the previous problem. What does that allow us to conclude? We conclude therefore that, so the conclusion of the previous problem was the following that there is at least one group element, there exists an element $g \in G$ whose fixed point set is empty $X^g = \emptyset$ ok. Now, let us see what that means for this particular action? So, this means that; so what is the fixed point set for g? So, this is for all. So, fixed point set; so which means for all co sets, for all $\sigma H \in X$ for all cosets, g does not fix that element , ok. This is another way of saying that the fixed point set is empty; I am just rewriting it as saying that for every element of X , g does not fix that element ok, g maps that coset to a different coset .

Well, what does this statement mean in terms of cosets? It says that, if $g\sigma H \neq \sigma H$; this means that, so I can push the sigma over to the other side, this as $\sigma^{-1}g\sigma \notin H$, ok. And remember this is $\forall \sigma \in G$ if you wish right, this is for all cosets. So, this is true $\forall \sigma \in G$; that $g \notin \sigma H \sigma^{-1} H$. Now, again this last equation can be written, rewritten again I can push the σ over to the other side; this says that $g \notin \sigma H \sigma^{-1} H$, again this is true for all $\sigma \in G$, ok.

And, now the last conclusion, let us stare at that a little harder. So, it says that this particular special element g which has no fixed points; that works out to the same thing as saying that $g \notin \sigma H \sigma^{-1} H$, this particular conjugate of H for every $\sigma \in G$, ok, which means .

$$g \notin \cup_{\sigma \in G} \sigma H \sigma^{-1}$$

And that was exactly we need to, what we needed to prove. Because we have concluded that there exists a group element which does not belong to the union of all the conjugates, ok. Now, if you look back on the statement of the problem, we need to say the union of all the conjugates cannot give you the entire group G ; it is a proper subset that has at least one element which lies outside this set and that is exactly what we have produced, ok. So, that completes this problem , ok .