Algebra - I

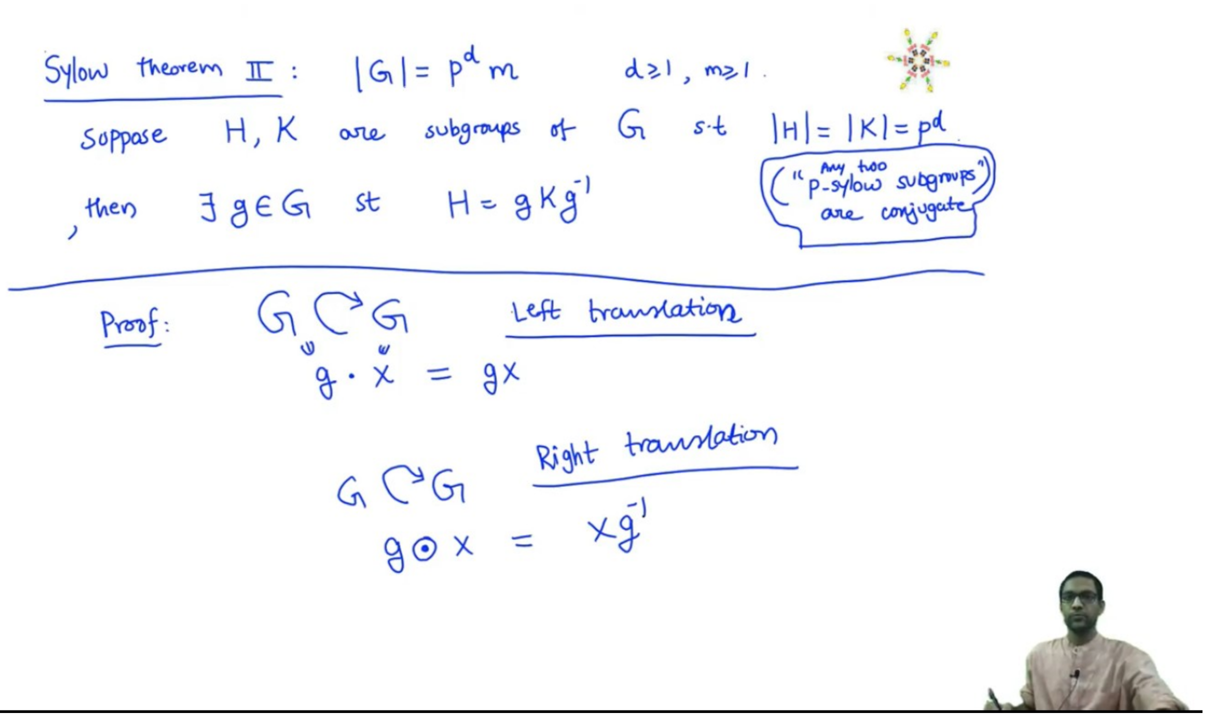
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

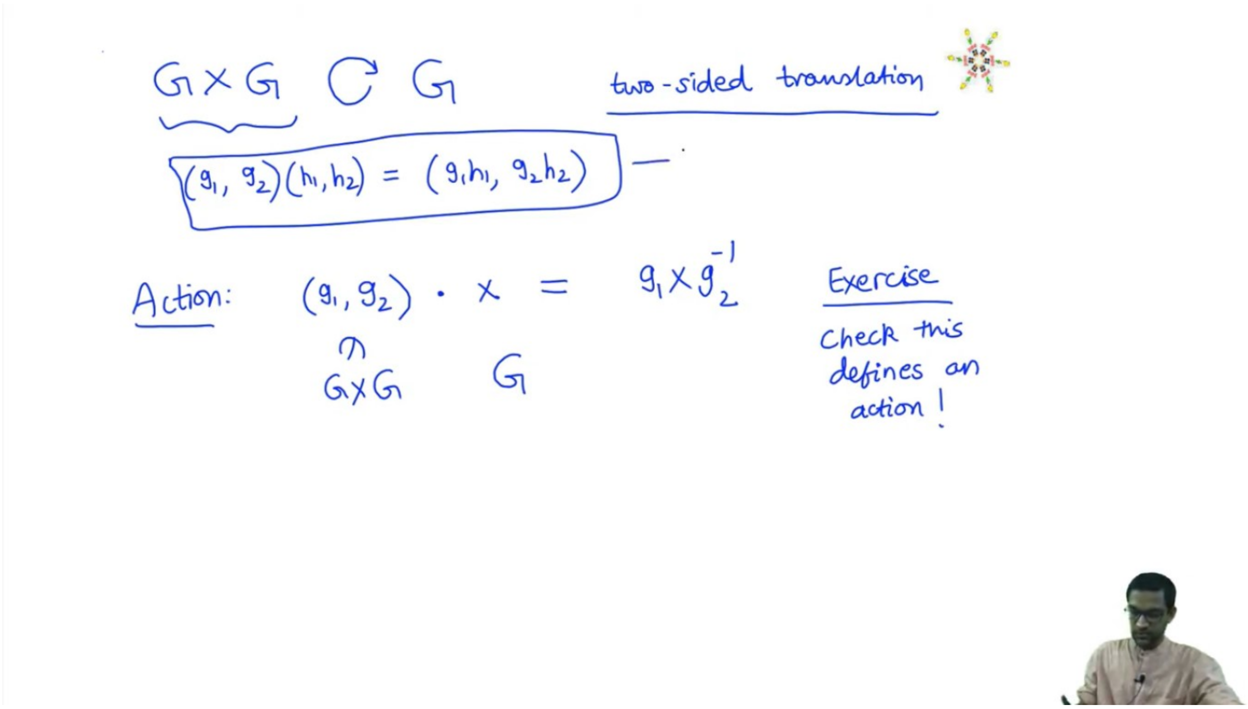
1. Lecture 22 [Sylow theorem II]

Today, we will prove the second Sylow Theorem. Here is a statement of Sylow theorem number 2. It says in words that any two p-Sylow subgroups of a group g are conjugates of each other, ok. More precisely:

Theorem 1.1 (Sylow theorem II)**.** *Let G be a group such that $|G| = p^d m$ where $d \geq 1$, $m \geq 1$. Suppose two subgroups H and K of G such that $|H| = |K| = p^d$, then there exist $g \in G$ such that $H = gKg^{-1}$.*

In other words, H and K are conjugates of each other, ok.
Now, let us prove this this theorem. And for the proof we will recall something that we talked about in in one of the earlier videos on on group actions. So, recall, we have an action of a group G on itself this is the translation action, but recall there are actually two such actions, ok. So, this is, remember there is something called left translation which is the following action the group element g acting on well the element x. So, I think of x again as





being an element of the group G. But now it is the set on which the action is taking place. This is defined as $g \cdot x = x$. So, this is called the the action by left translation.

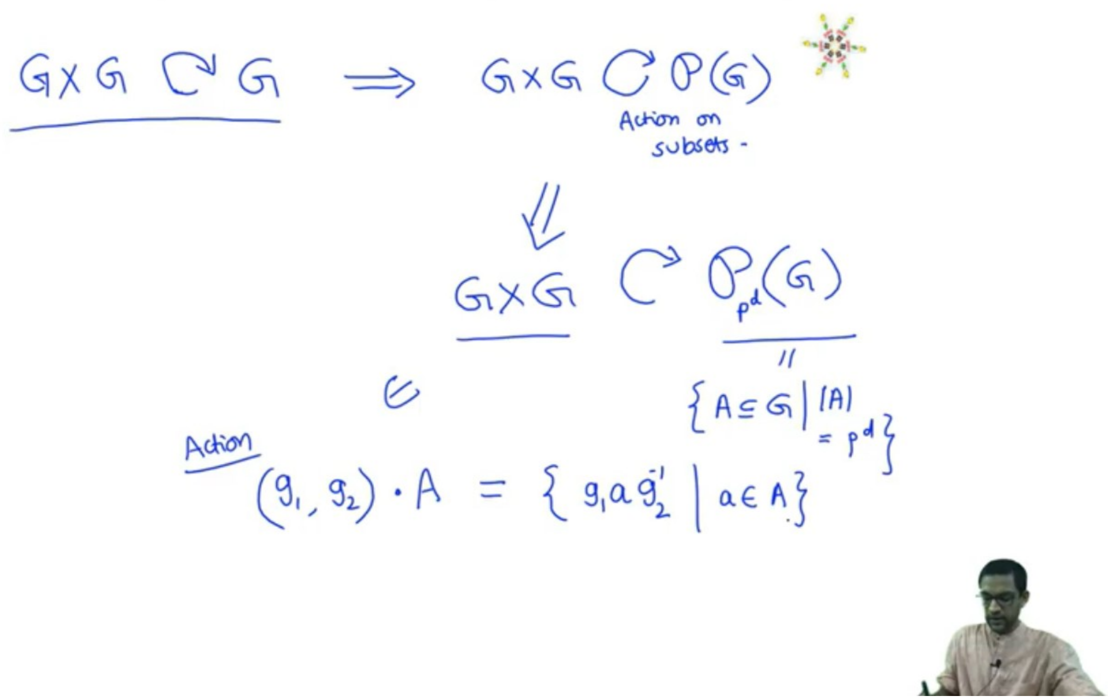
And there is similarly an action by what is called right translation. And if you recall this involves a little twist. So, G acts on G as follows, G this is the right translation action. So, maybe I will put a different symbol for now. $g \odot x = xg^{-1}$, ok and remember that it is important to put the inverse, otherwise this does not satisfy the the compatibility axiom for an action, ok. So, there are actually two translation actions, the left translation and the the right translation action of a group G on itself. And in fact, it is probably sometimes more powerful or more advantageous to put them both together, ok. So, in fact what the left and right translation actions do is the following interesting thing.

They actually define an action on the cross product $G \times G$. So, remember the definition of cross products of groups, the direct products;. If I have two elements, so what what is this this new group? The elements are of course, pairs (g_1, g_2) and the multiplication operation is just component wise. So, I take $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$. So, this is the definition of the cross product.

And, we actually can define an action of the cross product $G \times G$ on G and this is maybe what should most appropriately be called the two-sided translation action. So, what is this double sided or two-sided translation? The action is the following, ok. So, this is just recalling what the multiplication operation on the cross product is. So, here is the definition of the action.

So, how do I make $G \times G$ act on G ? So, I take a pair $(g_1, g_2) \in G \times G$, and I take a point x in the set well here the set is G itself. So, let me define the action the pair (g_1, g_2) acting on the element x gives me; well I use the first g_1 to do a left translation and the the g_2 to perform a right translation, ok. So, the action definition is this

$$(g_1, g_2) \cdot x = g_1 x g_2^{-1}$$

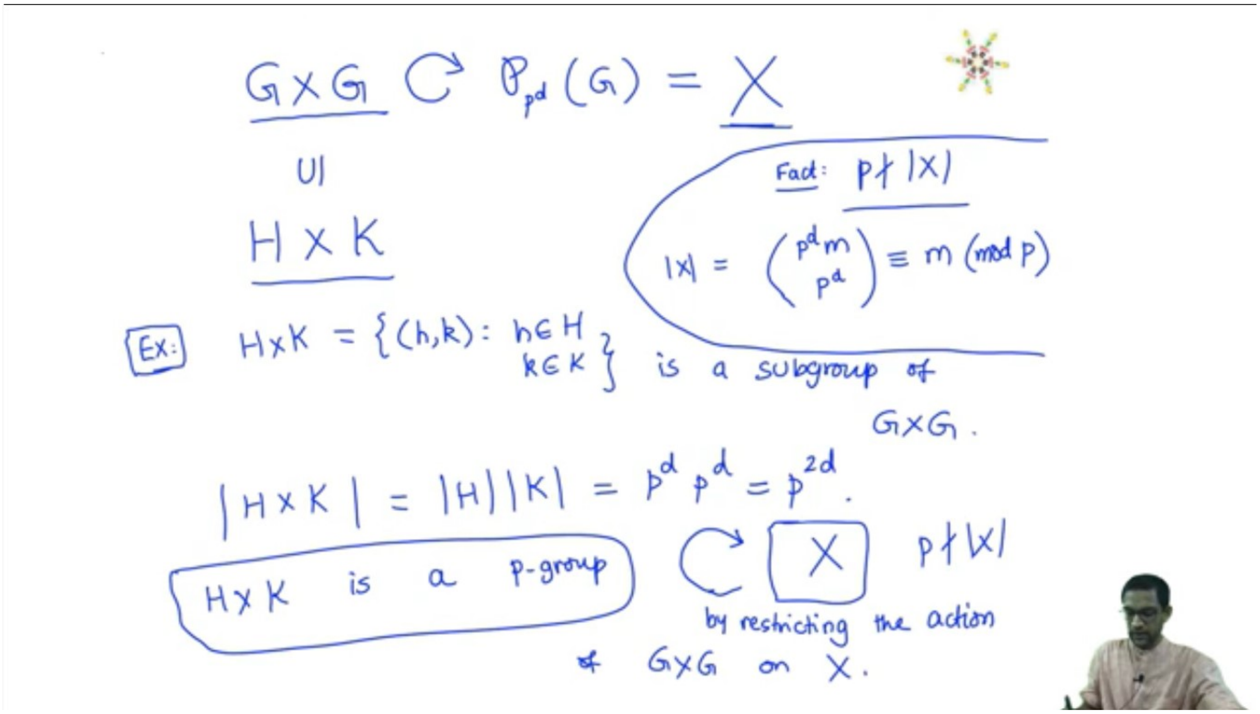


So, this is a two-sided translation. And, here is a little exercise which I urge you to do, which is to check that this is an action check that this is an action, this defines an action, ok. So, you know this involves first looking at what the definition of the product on the cross product is and so on. So, this is a nice little exercise which puts together all the things you have learned until now, cross products, definitions of actions and so on, ok.

So, in fact what we have is not just right and left translation, but really you should stitch them together and think of it as giving you an action of the group $G \times G$ on G by means of this this two-sided action, ok. So, that is that is maybe the most general way of thinking about translations. Now, why is this relevant to our proof of the second Sylow theorem? Well, that comes from the following, ok. So, when I have an action of a group in this case the group $G \times G$, when I have an action on a set, so when $G \times G$ acts on a set, in this case the set is just the group itself. Then, recall whenever I have a group action it automatically defines an action on subsets, ok. So, I can make the group G act in fact on the power set of the set $P(X)$. So, here the set X on which the action takes place is G itself.

So, this is the action on subsets that we define, ok. And in fact, we refined this a little bit, we said we do not need to look at the entire power set, in fact it defines an action on subsets of any given cardinality, ok. So, I can look at $P_k(G)$ for any cardinality G , ok, but recall that the value of K that was somehow relevant to our situation is; so, let me just not confuse notation here. Let me just keep G . So, recall that the cardinality that was most relevant to our situation was somehow this number p^d, ok.

So, in other words, because there is this two-sided action on the group G on the set G , there is also a two-sided action of $G \times G$ on the set of all subsets of cardinality P^d. So, recall this is just a subsets of G , whose cardinality is exactly p^d. So, there is an action on all such subsets. And just to recall what is that action? If I give you a pair (g_1, g_2), so this is the action. If I give you a pair $(g_1, g_2) \in G \times G$ its action on the subset A is just given by well



it just gives me a new subset whose elements look like this. It takes every element of A, and it it applies the two-sided action to it, ok.

$$(g_1, g_2) \cdot A = \{g_1 a g_2^{-1} | a \in A\}$$

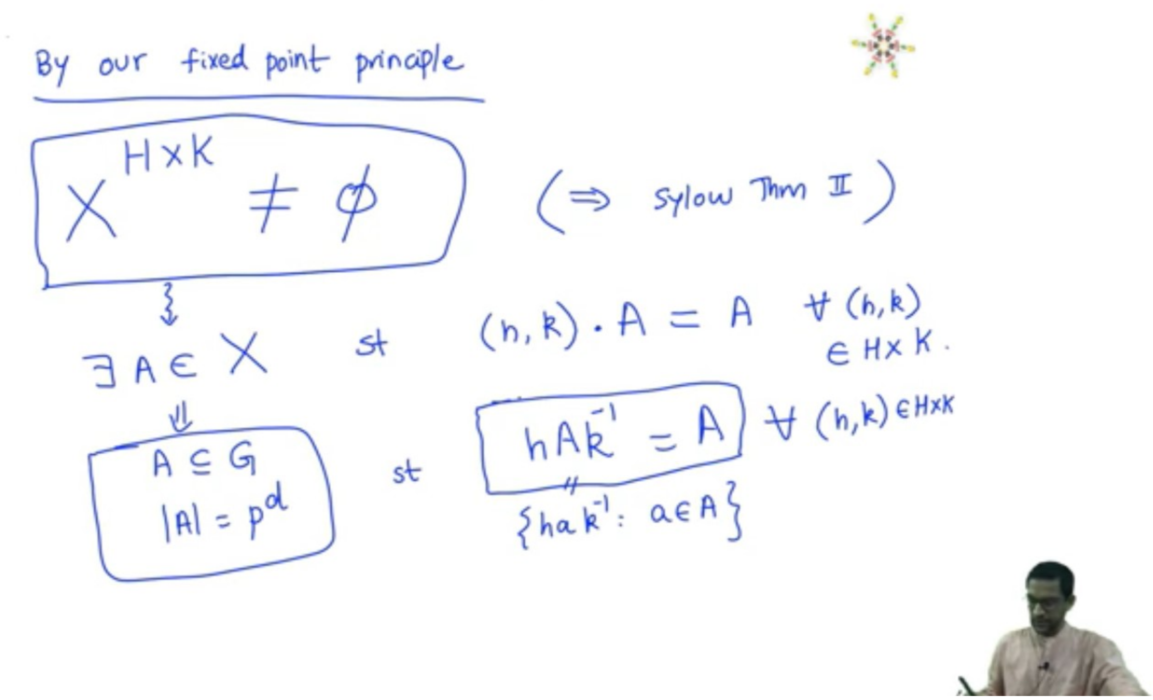
And take the collection of all such elements that will be another subset whose cardinality is p power d that subset is what you define the action to give you that subset, ok. So, that is the definition of these; I am just recalling the action on subsets definition, ok.

Now, let us let us go back to let us let us just look at the hypothesis of Sylow theorem 2 again, what is it that we need to prove. We need to show the following if I have two Sylow subgroups H and K then I can somehow relate them by a conjugation, one is obtained from the other by a conjugation. So, I will use the same notation. I have two subsets H and K.

So, observe; so, what is it that we just said? I have $G \times G$ acting on the set of all subsets of cardinality d $P_{p^d}(G) = X$, ok and let me call this as me as my set X now, ok. Now, since $G \times G$ acts on X so recall the the very important fact about X that we we proved which is that the cardinality of X is not divisible by p, ok p cannot divide the cardinality of X. This is the very interesting thing we proved.

And recall the way we proved this was by observing that the cardinality of $|X|$ is in fact nothing but the binomial coefficient $\binom{p^d m}{p^d}$, and again by our group actions principle we managed to show that or our fixed point principle we managed to show that this number is $\cong m(mod\ p)$. And since, m is not divisible by p cardinality of $|X|$ is also not divisible by p, ok. So, this was how we showed that X has cardinality which is not divisible by p, ok.

So, now we have the following interesting thing we have a group acting on a set whose cardinality is not divisible by p and inside this group let us consider the following subgroup. So, remember I had H and K as part of my; so, this is what I need to prove I am now going



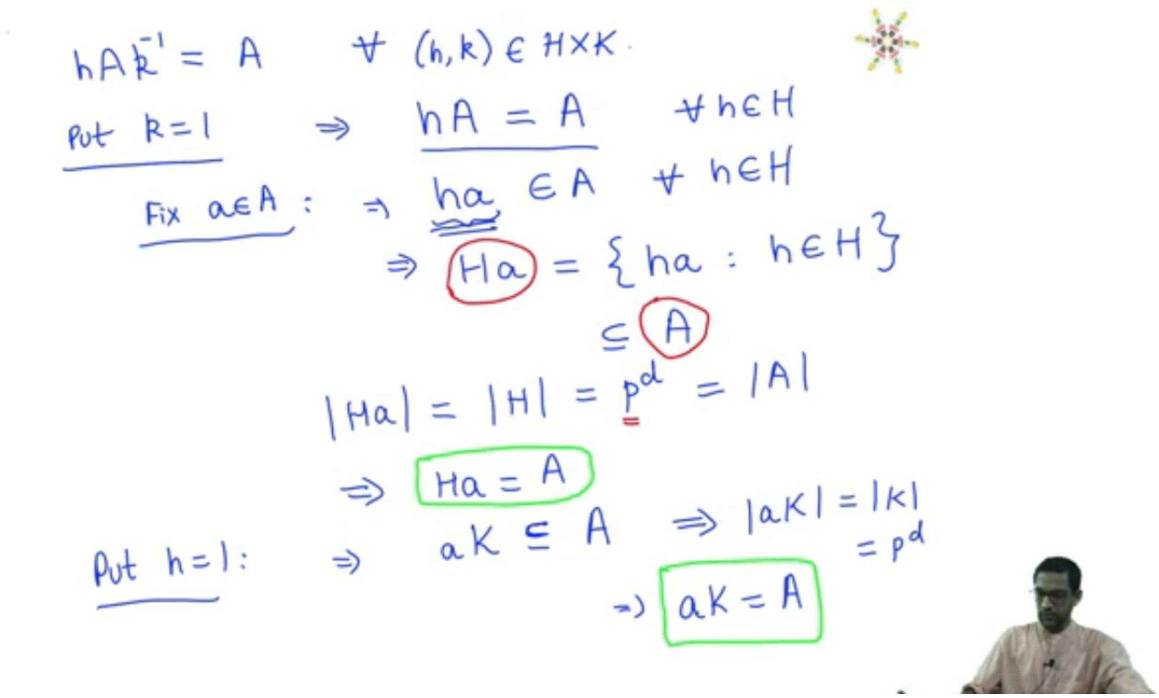
to prove the the second Sylow theorem. So, recall that H and K were both subgroups of G that implies that the cross product $H \times K$ is actually a subgroup of the group $G \times G$, ok.

So, verify again here is another little exercise. Check that $H \times K = \{(h,k)|h \in H, k \in K\}$. Check that this is actually a subgroup of the group $G \times G$, is a subgroup of the group $G \times G$, ok. Now, having done this; so, I mean assuming you have done this exercise what is it that you get, now, observe what is the cardinality of of this this group $|H \times K|$. Well, by definition it is just it is all ordered pair. So, it is cardinality of $|H \times K| = |H||K| = p^d p^d = p^{2d}$. So, what does that mean? It means that $H \times K$ is in fact a p-group. So, in other words $H \times K$ is a p-group. It is cardinality is a power of a prime p, ok.

Now, we are slowly bringing things into the the formalism of our fixed point principle. Here is a p-group, ok and here is a set X whose cardinality is not divisible by p, ok. So, I have the two ingredients that I want I have a p-group, I have a set X and in fact there is an action of this p-group on this set X. Why is there an action? Well, observe that the entire big group $G \times G$ acts on X, ok. And this is after all the subgroup of the big group, ok.

So, when you have an action of of the ambient group the bigger group acting on a set, you automatically get an action of any subgroup by just restricting the action. In other words, you just say if I take an element from the subgroup it, it acts the same way as it would act as an element thought of as an element of the big group, ok. So, this is just by restricting the action. So, you can make $H \times K$ act on X by restricting the action of $G \times G$ on X ok.

So, we have all the right ingredients. So, by our fixed point principle, from one of the earlier videos, by our fixed point principle, fixed point principle what we obtain is the following that $H \times K$ action on X must have a fixed point. There must be. So, what is the correct notation? X was the set, $H \times K$ is the group acting on it, so this is the set of fixed points. This set is non-empty, ok. The set of $H \times K$ fixed points in X is non-empty, ok.



Now, what does that imply? So, let us just unravel the the definition. So, this basically is now well let me just skip ead this is going to tell us that Sylow theorem 2 holds, ok. So, Sylow theorem 2 is essentially just this fact that is all. It is the, it is the same its if you wish its equal into saying this this statement here, ok. So, why does the $H \times K$ fixed points, I mean why does that imply Sylow theorem 2? Right. So, this is what I need to prove.

So, let us unravel this definition a little bit. So, $X^{H\times K} \neq \emptyset$ is not empty means there exists a fixed point. In other words, there is a subset, so there is an element $A \in X$ such that A is fixed by every element of $H \times K$. So, such that $H \times K$ acting on A gives me A for every pair $(h,k) \in H \times K$, ok.

Now, what does this mean? A is an element of X means that A is a subset of the group whose cardinality is p^d. So, that is those are the elements of X ok. So, A is a subset of cardinality p power d such that the action of $(h,k) \cdot A = A$. Now, remember what is the action of (h,k)? It is left multiplication by h, right multiplication by k^{-1}. This gives me A for all elements, for all pairs $(h,k) \in H \times K$ ok.

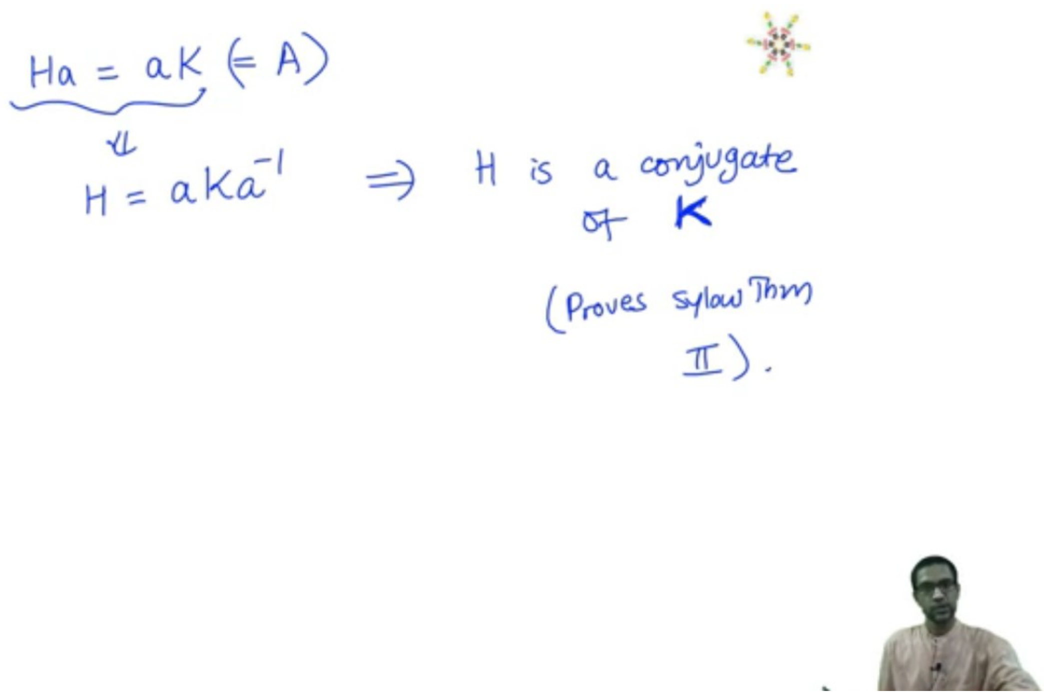
So, this is this what is meant. So, if I if I multiply, so if you recall $\{hah^{-1} | a \in A\}$, ok. So, that is equal to capital A. So, now, let us look at this this statement here. Now, let us do the following. Let us put for example, so let me pick any element of A, ok. So, let me skip to the next page. So, let me just rewrite that equation again,

$$hAk^{-1} = A \forall (h,k) \in H \times K$$

. Now, let us do the following. Let us put $k = 1$, ok. What this means is that if I take $hA = A$ because right multiplication by k^{-1} is does nothing, ok. So, what this means is that

$$hA = A, \forall h \in H$$

.



So, in particular what this means let us fix an element A. So, let us pick any element, fix an element $a \in A$, ok. So, what do I conclude? This means that $ha \in A, \forall h \in H$, ok. So, that is really the statement here. If I take this element a which comes from capital A, and I multiply it on the left by h the answer is again in A, ok,. But, what does that mean? Well, what is this this; now look at this elements of the form $Ha = \{ha | h \in H\}$ So, this is exactly the right coset Ha, ok. So, observe the right coset Ha is nothing but the that is exactly the set of elements of this form h coming from H, ok. So, saying that every such product $Ha \subset A$ just means that this entire right coset is in A, ok,. But observe the following the right coset $|Ha| = |H|$.

So, right cosets have the same cardinality as the subgroup themselves and that is that is the cardinality is p^d and in fact that is also the cardinality of $|A|$, ok. So, what that means is that this right coset here Ha and this set a here both have the same cardinality, both their cardinalities are p^d, ok and one is a subset of the other which can only happen if they are actually equal to each other, ok. So, this means that Ha must actually equal the setting, ok.

Now, similarly, so we we can do the thing on the other side as well. We can put h to be 1 and conclude by a similar token that if I take this element a and you multiply it on the right by elements of K, then this is a subset $ak \subseteq A$, for the same reason. And again because the cardinality of $|ak| = |K| = p^d$. This again means that the the right coset aK and a have the same cardinality this means that $aK = A$, ok. So, we have made the two conclusions that we are looking for, one is that $Ha = A$, the other is that $aK = A$, ok.

So, this this right coset, a certain right coset of H is equal to sort of the corresponding left coset of K, Ha is the same as aK. Both are equal to the set A, ok. Now, we are done because observe what does this say, the right coset Ha is the same as well both are equal to A. But what does this mean? This just says that $H = aKa^{-1}$. Now, in other words H is a conjugate of G , sorry conjugate of K, ok. So, this proves, so this proves Sylow 2, ok.

So, again as you see this the the Sylow theorems are all instances of just one basic principle that a p-group acting on a set whose cardinality is not divisible by p will have to act by fixed points. And this property characterizes p-groups in the sense that the converse is also true, right. So, the converse is what was used in in Sylow 1 and sort of the forward principle is what is used in the proof of Sylow 2, ok.

Next time we will prove Sylow theorem number 3 which is again again an application of the same principle.