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

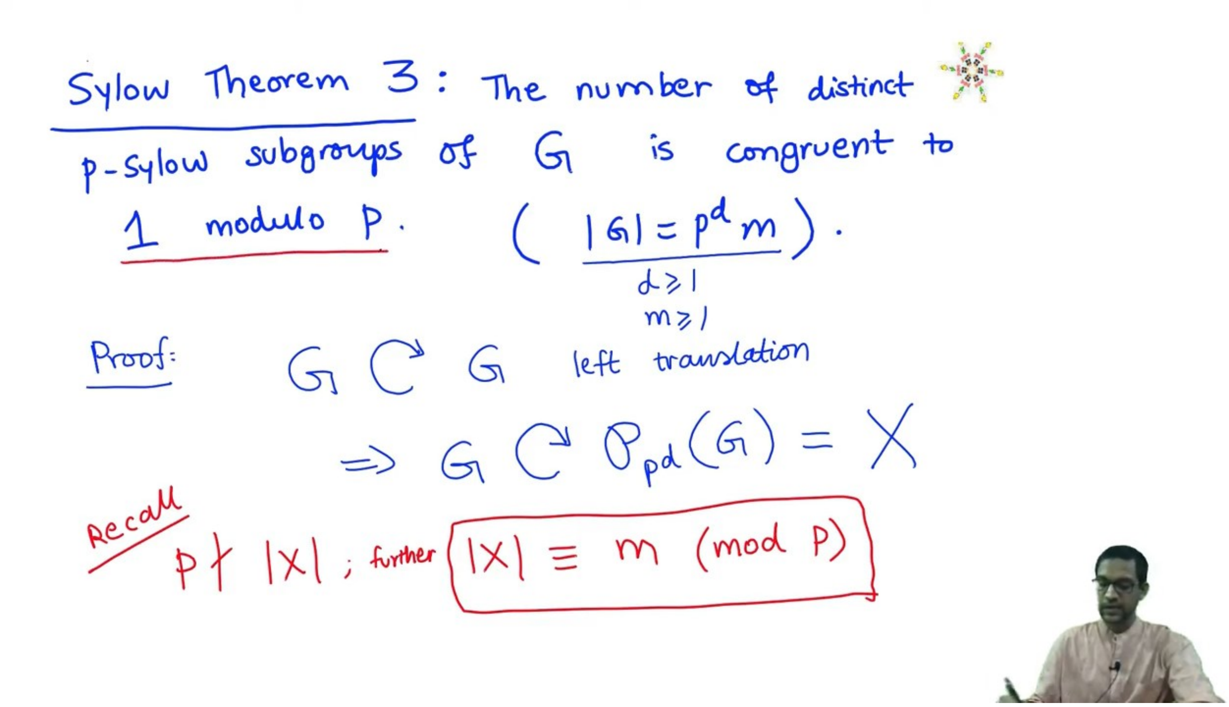
1. Lecture 23 [Sylow theorem III]

Let us prove the third Sylow theorem. So, this is the last of the Sylow theorems part 3.

Theorem 1.1 (Sylow Theorem 3:)**.** *Le G be a finite group of cardinality $|G| = p^d m$, where p is a prime and $d \geq 1, m \geq 1$. The number of distinct p-Sylow subgroups of G is congruent to 1 modulo p.*

and the notation is more or less what we used in all the earlier theorems as well earlier parts of the theorem that we assume p divides the cardinality of the group. let us prove with third Sylow theorem . Now, this again involve some some very interesting ideas and as before it uses the the set X that we have been looking at repeatedly . So, here is the proof .

So, let us go back to the action of G on itself . So, G acts on itself by just left translation . So, recall we used both left and right translations in the earlier proof of Sylow 2 . Now, we will go back to just the left translation . So, G acts on it itself by left translation and therefore, by the action on subsets G acts on the set of all subsets of G of cardinality p^d and we called the set $P_{p^d}(G) = X$.

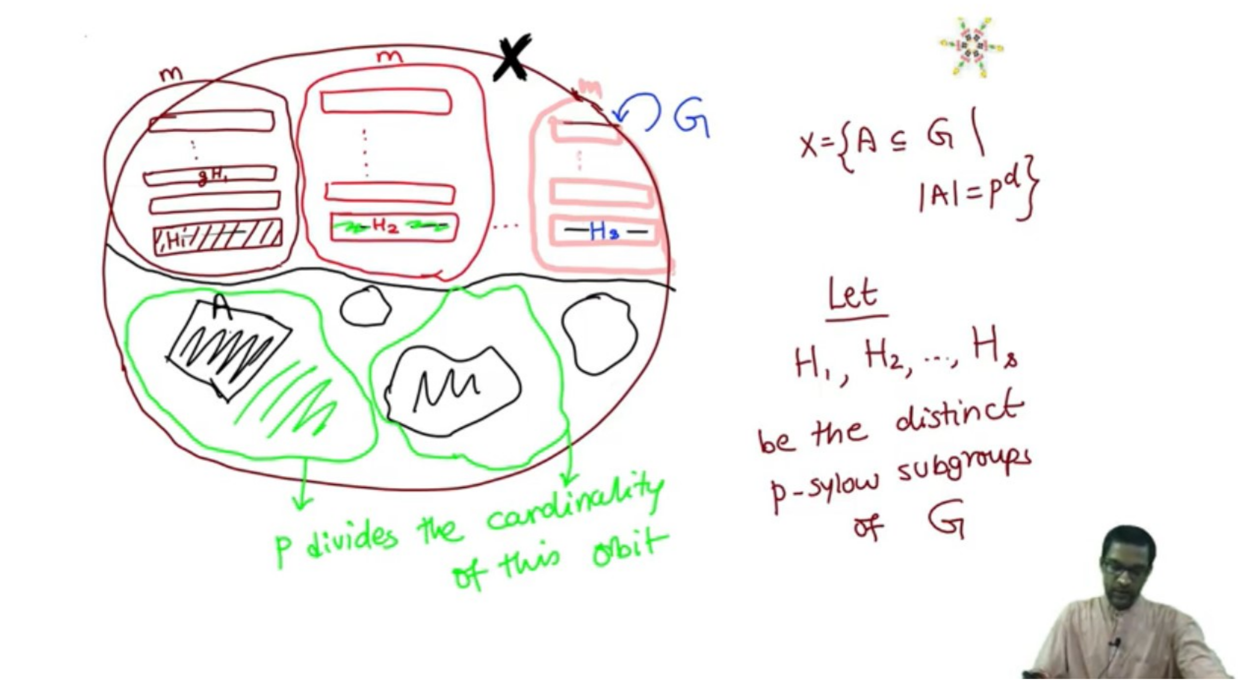


Sylow Theorem 3: The number of distinct p-Sylow subgroups of G is congruent to 1 modulo p. $\left(\underset{\substack{d \geq 1 \\ m \geq 1}}{|G| = p^d m} \right)$.

Proof: $G \circlearrowright G$ left translation

$\Rightarrow G \circlearrowright P_{pd}(G) = X$

Recall $p \nmid |X|$; further $\boxed{|X| \equiv m \pmod{p}}$



$X = \{A \subseteq G \mid |A| = p^d\}$

Let

$H_1, H_2, \ldots, H_s$ be the distinct p-sylow subgroups of G

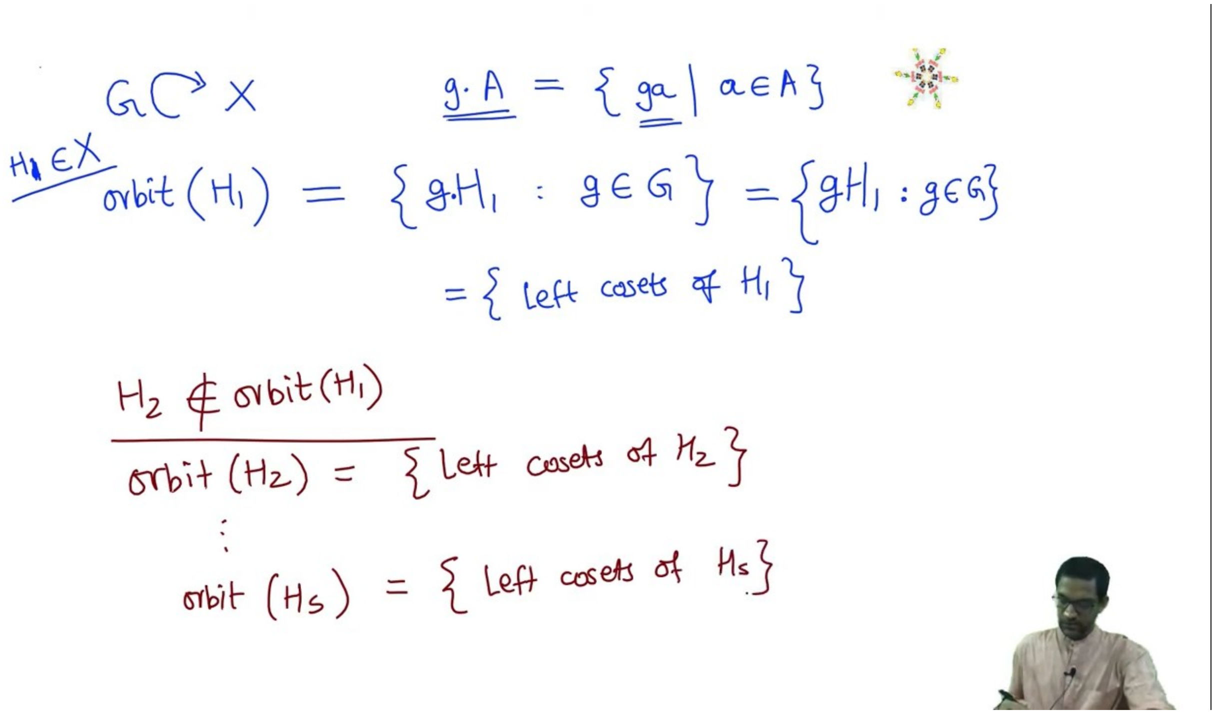
And again to recall the the key property of X was that it was it had a cardinality which was not divisible by p. And for this Sylow theorem 3 we will recall one additional fact about X . We actually knew a little bit more about the cardinality of $|X|$ further recall

$$|X| \cong m(mod\ p)$$

So, this this little fact has never been used in it is full power until now. We only use the fact that the cardinality of $|X|$ is not divisible by p, we have never used the exact congruence modulo p that the cardinality satisfies ok . And since of course, this particular statement here in Sylow 3 is a statement about something being congruent to something modulo p I will turn out that this is exactly the fact that that will play a role ok. So, let us move on . So, observe that this set X that we keep talking about is actually interesting for the the following reason .

So, what is this set X really. So, the set X let us draw a picture of the set X it is the set of all subsets . So, what what are elements of X ? So, it is X is nothing, but all subsets of G whose cardinality is p^d . And so in particular the p Sylow subgroups that we are looking at the H or K that appeared in the earlier one. So, any p Sylow subgroup for example is in fact an element of X . So, let me let me give them names. So, let us say that let let us assume that the p Sylow subgroups are the following H 1, H 2 till some number H s be the distinct p Sylow sub groups .

So, recall by the second Sylow theorem we know they are all conjugates of each other . Be the distinct p Sylow sub groups of G and so in fact they are all elements of of the set X . So, H_1 the subgroup is somewhere in X . So, maybe we will just put them in different colors . So, I have H_2 another subgroup and so on till I finally get my subgroup hs just write here . So, this is a last subgroup H_s ok . Now, um H_s ok.



$G \curvearrowright X$ $\quad \underline{\underline{g\cdot A}} = \{ \underline{\underline{ga}} \mid a\in A\}$

$\underline{H_1 \in X}$

$\text{orbit}(H_1) = \{ g\cdot H_1 : g\in G\} = \{ gH_1 : g\in G\}$

$= \{ \text{left cosets of } H_1 \}$

$\underline{H_2 \notin \text{orbit}(H_1)}$

$\text{orbit}(H_2) = \{ \text{Left cosets of } H_2 \}$

$\vdots$

$\text{orbit}(H_s) = \{ \text{Left cosets of } H_s \}$

Now, here are some subsets of cardinality p^d no doubt . Now, let us do the following let us ask the following question since they are all elements of X after all what do their orbits look like. So, recall the set X is a G-set. It is got an action of the group G the action on subsets right . So, recall what is the action ? G acts on X.

Again worth recalling once more

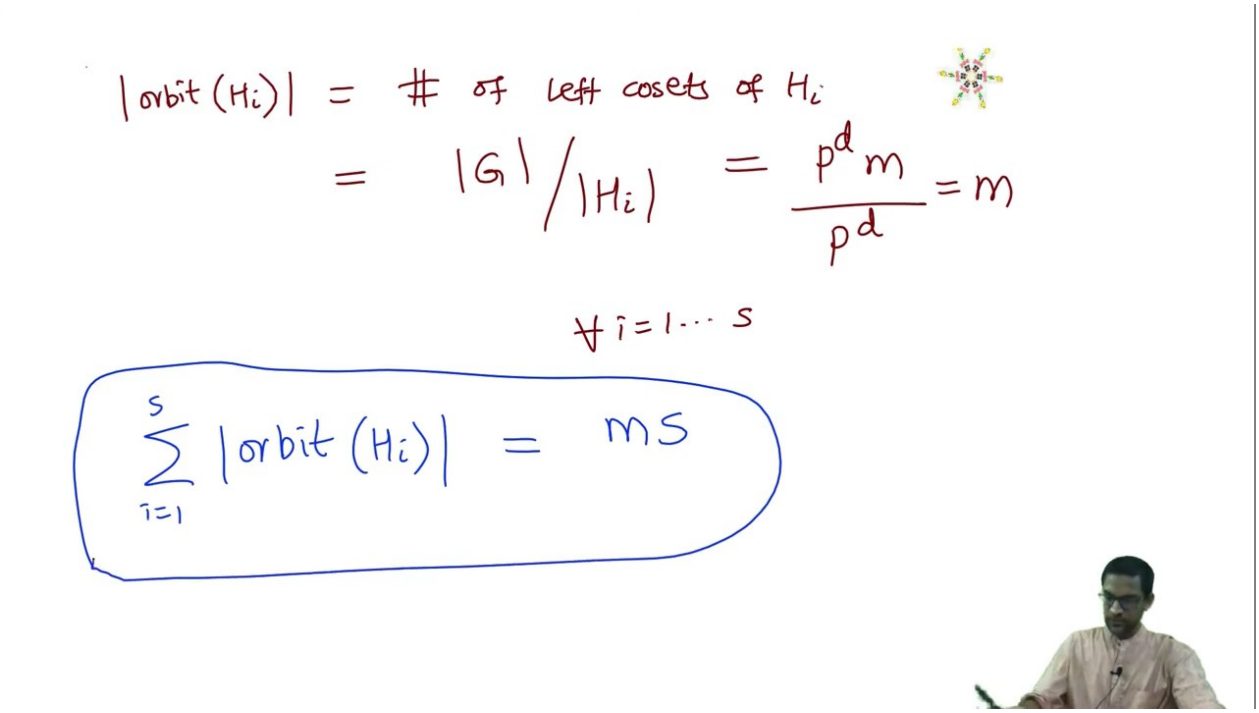
$$g \cdot A = \{ga|a \in A\}$$

. So, in particular we can ask well look at these p Sylow sub groups and let us ask what are their orbits under this action ok .

So, take the p Sylow sub group H_i for example, or let us start with the H_1 is an element of X . It is a subset of carnality p^d . So, it is a valid question to ask what is the orbit of this point. This this you know it is now just a single point in the set X . So, what is its orbit under the group action? Well, by definition this is just going to be all elements of the form uh gH_1 ok .

$$Orbit(H_1) = \{g \cdot H_1|g \in G\} = \{gH_1|g \in G\}$$
$$= \{left\ coset\ of\ H_1\}$$

So, what is this? The sets the subsets you get in this way are exactly the left cosets . In other words, these are just the left cosets of the set H_1 ok . So, this is an first interesting fact here that when I look at H_1 it is orbit under the group is just going to be it is various left cosets . So, let me just mark them here . So, these are the various left cosets of H_1 ok. So, various gH ones . So, this is the orbit of H_1 ok. Now, uh let us move on to H_2 now. So, observe H_2 is not in this orbit ok. This this H_2 being a distinct p Sylow sub group. So, note that in in the orbit of H_1 what you have are H_1 and its various cosets. Among these so observe a coset can never be a subgroup except for the the identity coset meaning the coset of the original subgroup itself.



$$|\text{orbit}(H_i)| = \#\text{ of left cosets of } H_i$$

$$= |G|/|H_i| = \frac{p^d m}{p^d} = m$$

$$\forall\, i = 1 \cdots s$$

$$\boxed{\sum_{i=1}^{s} |\text{orbit}(H_i)| = ms}$$

All the other guys are not sub groups they are not closed under multiplication . So, this guy is the only subgroup here and since H_2 is assumed to be different from H_1,H_2 cannot cannot live inside this orbit right it . The only subgroup among these cosets is the one that I have shaded. And so if at all H_2 lives in this orbit it has to equal that guy, but H_2 is not equal to H_1 ok. So, observe H_2 is not in the orbit of H_1. So, that is all I am I am trying to say here. So, observe H_2 is in a separate orbit ok. So, look at orbit of H_2 . What is that? Well, by the same token this is just the set of all left cosets of H_2 and so on . So, you keep going this way.

So, you observe that at every step the orbit of . So, these these left cosets here. This is the orbit of H_2 under the group action and so on till you reach the very end and the orbit of H_s will just be its left cosets ok . Because, that is the last orbit ok and these are all disjoint I mean they are all more or less by definition of orbits they are all disjoint sets. So, I have I have produce some number of elements of the set X ok.

So, let us write X separately here again . So, X is my my ambient set ok on which the action takes place ok . Now, so what have we done so far we have produce some elements of X or rather we have produce some orbits inside the set X . Now, how many elements of X are accounted for in this way ok. In other words, how many elements are there in each orbit? What is the cardinality of each orbit ? So, observe so and so on. So, this holds all the way till orbit of the last guy he is just going to give me the set of all left cosets of H_s ok . Now, observe we know how many left cosets there are of of any subgroup right.

So, observe that the cardinality of the orbit of any one of the H_i is by,

$$|Orbit(H_i)| = \#of\ left\ coset\ of\ H_i$$

So, let us go back to our picture of X . So, what does that mean it means that there are m elements here . So, the cardinality of this set is m, the cardinality of this set is m , the cardinality of the last every one of them is m ok and there are s of them. So, there are you know how many total elements of X are accounted for in these orbits there are ms elements that lie in these s orbits ok .

Now, let us look at the other elements of course, this does not exhaust all the elements of X because these are all very special subsets of cardinality p^d. These are either the p Sylow sub groups themselves or their left cosets ok. So, these are some very very special kinds of subsets of cardinality p^d , but the of course, there will be lots of other random subsets right. So, there are many many other subsets here of cardinality p^d in in the group G . So, of course, I have to look at all of them next ok. So, let us look at any one such guy. So, let me pick some not so special subset a which is not of this form and ask .

So, here is a subset of cardinality p^d I can ask the same question what is its orbit going to look like ok. Again a very very interesting question if I take a random element of cardinality random subset of cardinality p^d and ask what is its orbit under the action of the group. In other words, if I keep hitting it on the left by different group elements it produces new subsets of cardinality p^d .

What can I say about that orbit how many new subsets will I produce for example. These p Sylow guys are very nice and regular in the sense that we know exactly what you will get when you you know what their orbit looks like when you keep left multiplying these sub groups by elements of G you just produce the different cosets ok.

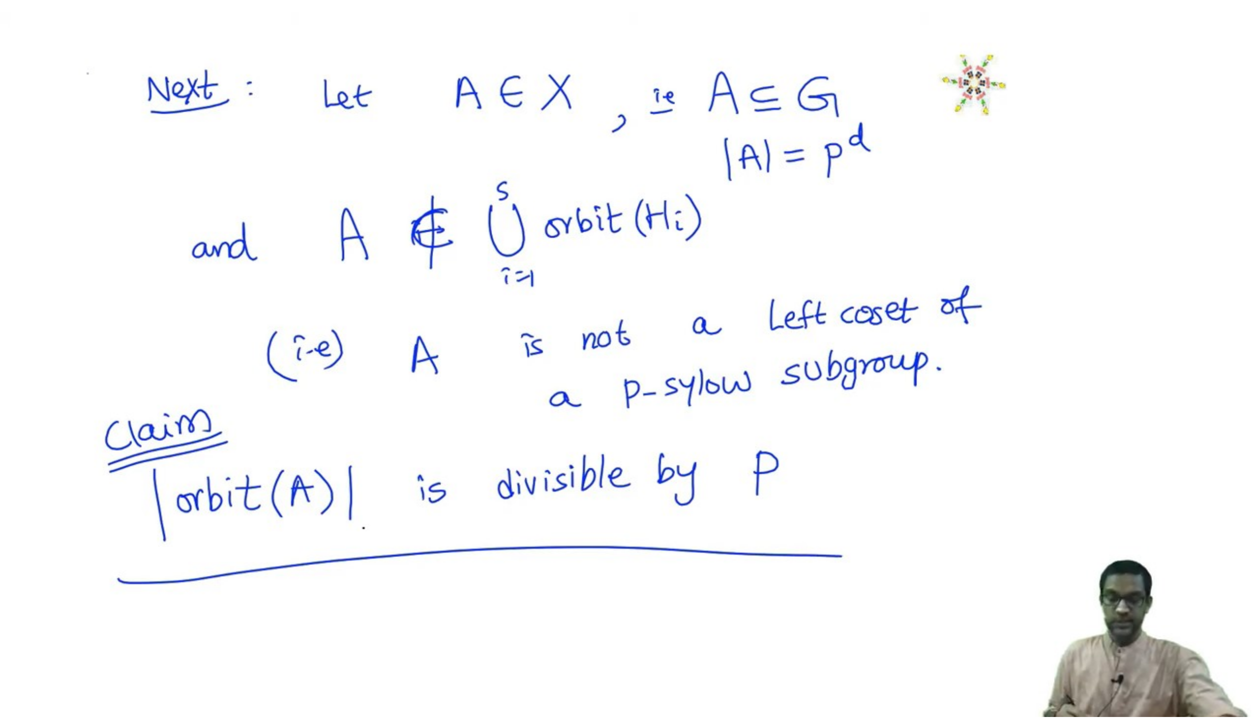
But, if a is not a subgroup for example, then it is not clear it is it is somewhat trickier it is not so easy to figure out what happens ok . So, I want to now next try and understand what is the $Orbit(A)$ look like ok. So, what is A now. So, let us pick . So, I want to say now consider ok. So, let us let us just note this this fact down as well. The sum of the orbits of these H is orbit cardinalities for these guys is m times s ok. So, so many elements are are nice in some sense ok . So, this is done now let us move on to the other orbits ok . Next let us pick suppose $A \in X$ in other words i e $A \subseteq G$ of cardinality p^d and A is not in any of these orbits and A is. So, how should I write it A does not belong to the orbits that we have already looked at ok.

$$A \notin \cup_{i=1}^{s} Orbit(H_i)$$

What does that mean ? i e A is not a left coset of a p Sylow subgroup ok . This is my this is now my assumption on A that it is not a left coset of a p Sylow subgroup . Now, under this assumption I want to ask what can I say about the cardinality of the orbit of A ok and here is my claim here is an important observation for all such A the cardinality of the orbit is divisible by p . This is the important claim.

Observe this does not hold for the the other nice orbits that we have already looked at . So, the orbits that we have looked at their cardinalities what was the cardinality was m right . So, these are the the cardinalities of the the p Sylow subgroups .

So, those guys have orbit cardinalities which are not divisible by p because m is of course, not divisible by p by assumption. But, if you are not one of these nice orbits any other orbit has cardinality which is a multiple of p ok. So, that is our claim ok . So, let us prove the claim first . So, proof of claim . Well, as always we will use the counting formula. If you want to understand how many elements there are in a given orbit you will have to understand what the stabilizer looks like ok. So, let me just called this the stabilizer of A ok . So, what is the stabilizer of A ?



Next : Let $A \in X$, ie $A \subseteq G$

$|A| = p^d$

and $A \notin \bigcup_{i=1}^{s} \text{orbit}(H_i)$

(i.e) A is not a Left coset of a p-sylow subgroup.

Claim

$|\text{orbit}(A)|$ is divisible by P

So, let me give that a name . So, let L denote the stabilizer of a it is a certain subgroup remember the stabilizer is always a subgroup . What is it? It is a set of all group elements which stabilize A. In other words, when you hit it on the left I mean when you act it on A you should get back in ok . So, this is the the definition of the stabilizer . All those elements of the group such that you take A, you hit it on the left by g, you still get back the same set A.

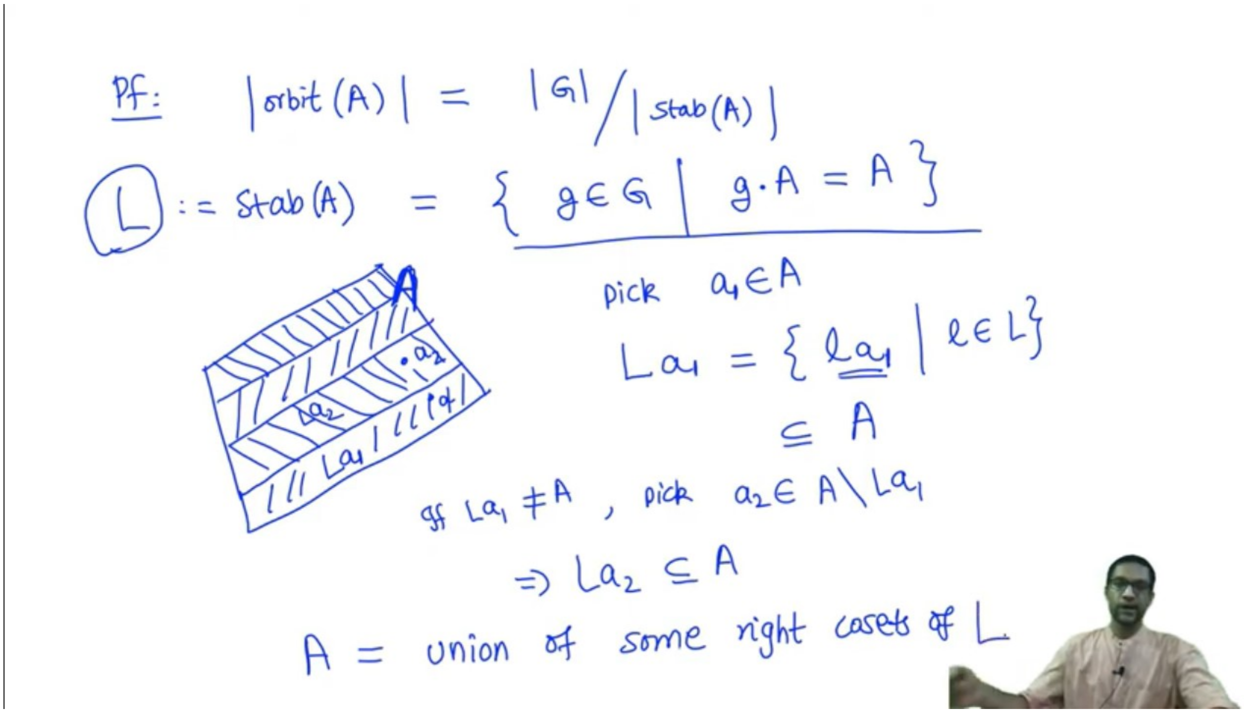
$$L := Stab(A) = \{g \in G | g \cdot A = A\}$$

I mean of course it can permute the elements of amongst A, but you should you should just get back the set A again. It should not take an element of A and move it to an element that is outside A ok .

So, this is the this is the property of the I mean this is the definition of the stabilizer . So, let us try and understand what the relationship is between A and its stabilizer ok. So, let me draw the set A now . So, maybe I will draw it the way I did in the the inside the set X . So, suppose my set a looks like this like a diamond. So, let us say this is my set A ok . Now, let us do the following. Let us pick an element $a \in A$. So, let us pick an element first $a \in A$ ok . So, take some element. So, I have taken some element$A$. Now, look at this stabilizer. So, what is the stabilizer? The stabilizer is A is a certain subgroup with this property ok .

Now, observe if I take an element. So, consider the right coset La ok. L is a subgroup, a is an element I can look at the right coset La . What is this? This is just all elements of the form la where l comes from L ok, but observe that La. So, according to this formula if I take an element of A I mean according to this definition if we take an element of A and multiplied by an element from the stabilizer the answer should again be inside A .

So, observe that every element of the form La must again be inside A by definition of the stabilizer ok . So, what is that mean I take A and if I look at this left coset L a well that entire thing is a subset of A. So, as soon as an element belongs to A it is entire right coset



Pf: $|\text{orbit}(A)| = |G| / |\text{stab}(A)|$

$L := \text{Stab}(A) = \{ g \in G \mid g \cdot A = A \}$

pick $a_1 \in A$

$La_1 = \{ \underline{la_1} \mid l \in L \}$
$\subseteq A$

if $La_1 \neq A$, pick $a_2 \in A \setminus La_1$

$\Rightarrow La_2 \subseteq A$

A = union of some right cosets of L

of La belongs to A ok . So, this entire thing is there ok . Now, we keep going suppose this exhausts A, then we are done. If not there is another element inside A ok . So, maybe we should call this a_1 pick an element $a_1 \in A$. If $la_1 \neq A$ stop otherwise look for an element a_2 which is not in la_1 which is an A ok. Apply the same reasoning. So, pick $a_2 \in A$.

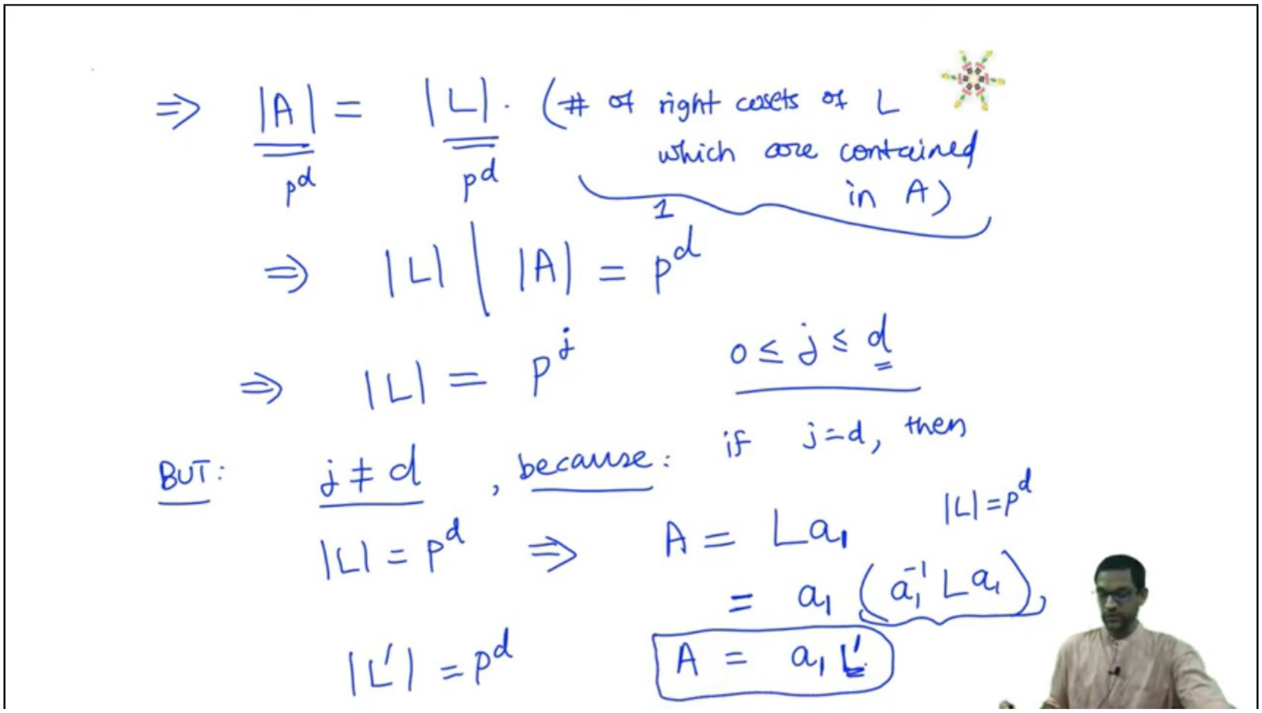
So, if La_1 is not the whole set A pick $a_2 \in A$, but not in la_1 and now again by the same reasoning conclude that la_2 is also a subset of A ok . Again by the definition of the stabilizer. So, this this entire coset la_2 is inside A and so on.

So, you keep going that way till you observe that as soon as some element is there it is entire right coset is there ok which means finally, this process has to stop because everything is a finite set . And finally, when this process stops what would you have obtained you would have realized A as a union A can therefore, be written as a union of some right cosets of L right .

Some finitely many right cosets of L. They are all disjoint necessarily that union of those many some finitely many of them should give you the set A ok . So, this is just we are just applying the definition of the stabilizer ok and the action on subsets. So, what does that mean in particular.

It says in particular this means that the cardinality of A has to equal cardinality of L times the number of right cosets which are contained the number of right cosets which of L which are contained in A . In other words, this means that the cardinality of L whatever it is must divide the cardinality of A ok because this is some number of course.

So, it means that the left hand side is A multiple of the cardinality of L ok, but observe the cardinality of A was p^d to begin with. So, what this means is therefore, the cardinality of L must also be some of a prime. It must look like some p^j where $0 \leq j \leq d$ ok . So, we have concluded that the stabilizer is also p group, but observe that, but the key point here



$$\Rightarrow \underset{p^d}{\underline{|A|}} = \underset{p^d}{\underline{|L|}} \cdot \underbrace{(\#\text{ of right cosets of } L \text{ which are contained in } A)}_{1}$$

$$\Rightarrow |L| \;\Big|\; |A| = p^d$$

$$\Rightarrow |L| = p^j \qquad \underline{0 \le j \le d}$$

BUT: $\underline{j \neq d}$, because: if $j = d$, then

$$|L| = p^d \Rightarrow A = La_1 \qquad |L| = p^d$$

$$= a_1 \underbrace{(a_1^{-1} L a_1)}_{},$$

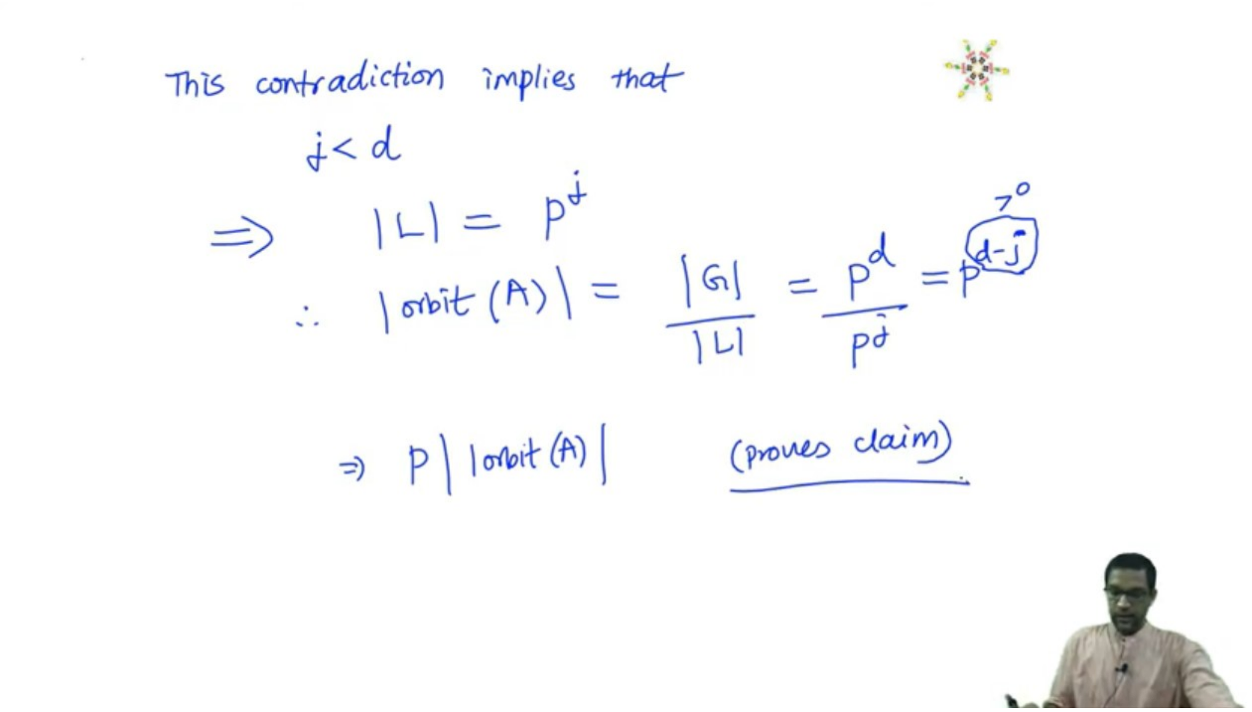
$$|L'| = p^d \qquad \boxed{A = a_1 L'}$$

is that L cannot have cardinality p^d, but observe that j cannot equal d ok . This maximum value is not allowed.

Why not because of the following reason . If j equals d because if j equals d then what that means is that L has cardinality p^d which means if you look at the the earlier or look at this this equation here the cardinality of $|A| = p^d$ the cardinality of $|L| = p^d$ which means that there should be exactly 1 right coset of L which is contained in A ok . So, what that means is that I mean or if you look at this earlier picture the at the very first step the very first right coset that you form that already exhausts the entire set A because the cardinality of that right coset is already p^d ok. So, what this means is that A looks like this.

Its just a single right coset just La_1 alone will do the job the very first one will do the job ok . So, A is a is a single right coset and L remember has cardinality p^d . So, what does that mean? Well, it means L ofcourse is therefore a p Sylow subgroup and A is a right coset of a p Sylow subgroup. But, observe that because of Sylow theorem number 2 here something we can do. Let me rewrite this as follows $a_1(a_1^{-1}La_1)$ ok . So, I will write this as a_1 times this guy here is just a conjugate of L' is is is a conjugate of L. So, I will call this L' maybe ok . So, what is L'? L' dash is another subgroup whose cardinality is p^d ok. So, what have I finally, concluded. I have concluded that my set A is therefore, a left coset of a p Sylow subgroup ok .

So, well because you know all these p Sylow subgroups are I mean conjugate of a p Sylow subgroup is a p Sylow subgroup. So, the right coset of a p Sylow subgroup is also the left coset of a different p Sylow subgroup that is all we are saying here ok. Now, but that recall is a contradiction because we assumed to begin with that the set A was not where was this assumption. We assume that A is not a left coset of a p Sylow subgroup. It was such an a that we are looking at . So, if $j = d$; however, we conclude that A does look like that. A has to have that form ok. So, this contradiction.



This contradiction implies that

$j < d$

$\Rightarrow \quad |L| = p^j$

$\therefore \quad |\text{orbit}(A)| = \frac{|G|}{|L|} = \frac{p^d}{p^j} = p^{\overset{>0}{\boxed{d-j}}}$

$\Rightarrow \quad p \mid |\text{orbit}(A)|$ (proves claim)

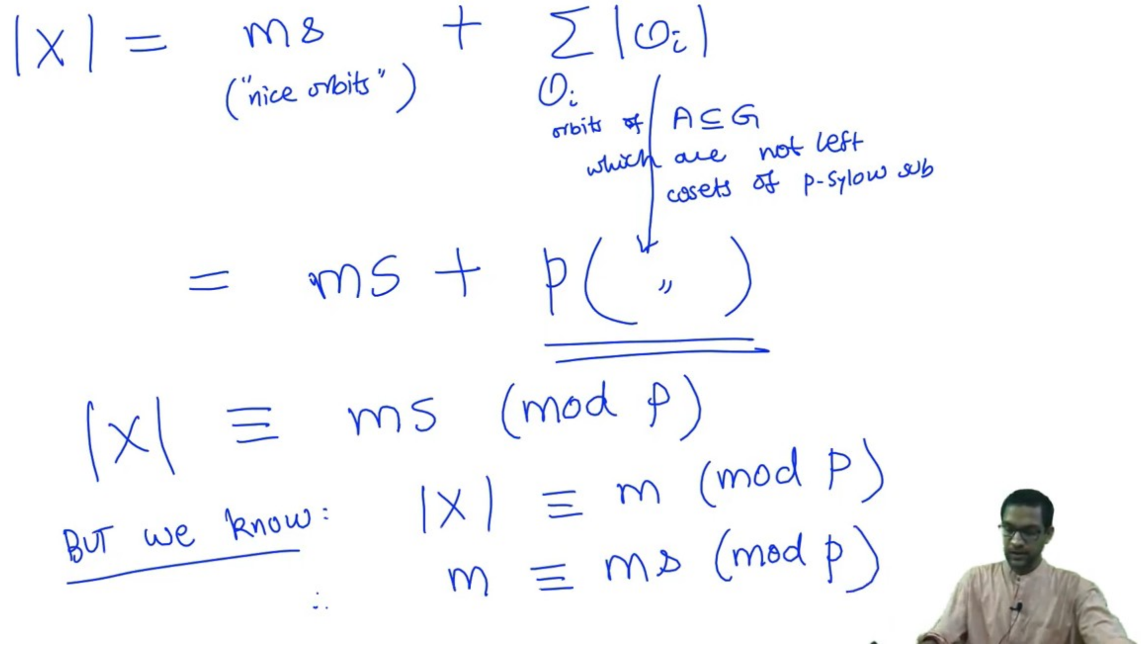
This contradiction implies that our assumption was wrong $j < d$ has to be strictly smaller than d cannot equal d . But, if j is strictly smaller than d well what does that mean cardinality of $|L| = p^j$ recall . So, j is strictly smaller than d therefore, the orbit cardinality the orbit of the set A that we looked at its cardinality looks like cardinality G by the cardinality of the stabilizer which is p^{d-j} which is some strictly positive power of p ok. So, this is this is divisible by p because this $d - j > 0$. So, p therefore, divides the orbit cardinality ok as required as claim. So, this proves our claim ok. So, let us take stock. Where are we now? We have gone back to our let us go back to this picture that we drew right in the beginning. So, we have the set X . We have these nice regular orbits ok which are the cosets of Sylow subgroups and then we have sort of all these other irregular orbits .

Now, these orbits are orbits of other subsets A which are not uh cossets of Sylow subgroups and what we have just shown is that this orbit you know the the the different the number of subsets that you get . So, this orbit cardinality is divisible by p . So, p divides the cardinality of this orbit ok and the same holds for the other subsets as well.

So, if I pick some other arbitrary subset A which is not in this orbit and I look at its orbit you know how many other subsets are obtained by left translating this by G that orbit again will have cardinality which is a multiple of p and so on ok ok . So, finally where does this this lead us . So, now, let us look at this big subset X and ask how many elements are there in X . So, there are these 2 types of elements. On the one side, we said that these nice orbits they account for m s elements, but the total size of X . So, now, let me compute the total size of X which is these nice orbits and these not so nice orbits .

So, observe now the cardinality of $|X| = ms.$ So, these come from the nice orbits left cosets of Sylow subgroups and so on plus these other orbits.

$$|X| = ms + \sum O_i|O_i|$$



$$|X| = \underset{(\text{"nice orbits"})}{ms} + \sum_{O_i} |O_i|$$

orbits of $A \subseteq G$ which are not left cosets of p-Sylow sub

$$= ms + \underline{\underline{p(\quad " \quad)}}$$

$$|X| \equiv ms \pmod p$$

BUT we know: $|X| \equiv m \pmod p$

$$\therefore \quad m \equiv ms \pmod p$$

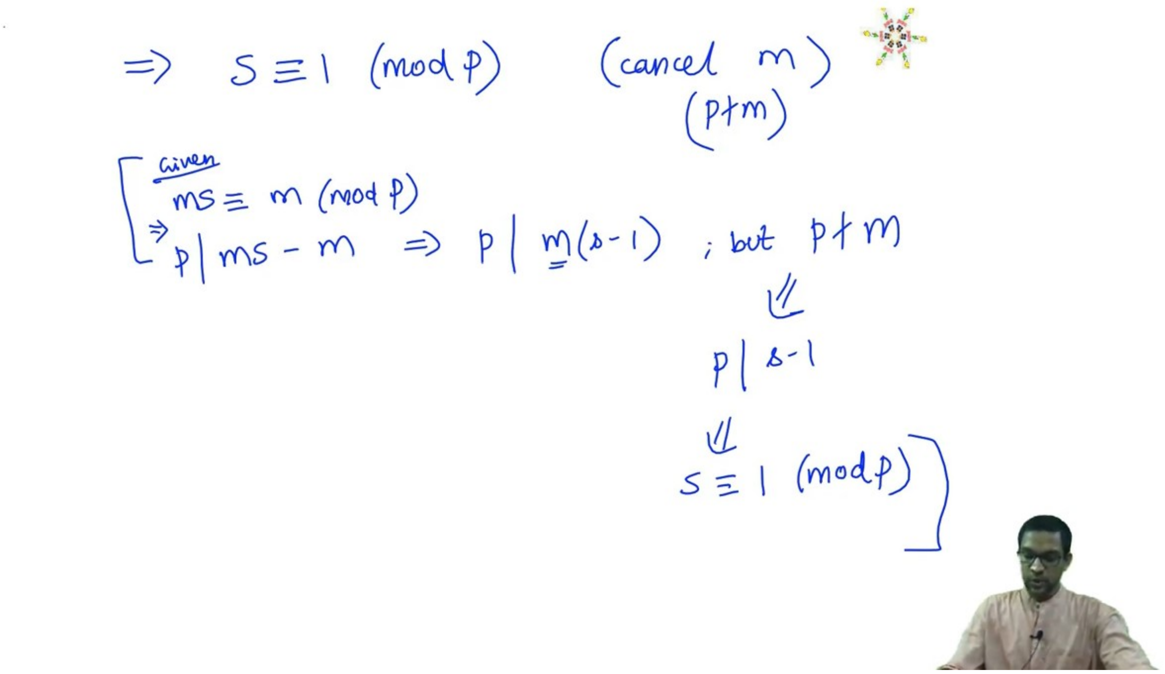
. So, let me just call it O_i for now where what is O_i. $O_i's$ are these not so nice orbits. If you wish whose cardinalities are divisible by p .

So, this is orbits of subsets A which are not left cosets which are not left cosets of p Sylow subgroups . So, these are the not so nice orbits and so what this gives us is ms plus what we have here we have just shown is divisible by p right . So, this is a multiple of p. Each orbit here is has cardinality which looks like p time something .

So, the net answer is congruent. So, this this part is divisible by p . So, I can ignore it when I am looking at congruence modulo p. So, I conclude that the cardinality of $|X| \cong m(mod\ p)$ is therefore, $m \cong ms(mod\ p)$ where s is the number of Sylow subgroups ok. But, observe we already know something, but we know and this is the fact I recall right in the beginning that the cardinality of $|X|$ by our other arguments is already congruent to m modulo p ok.

So, therefore, we conclude that the number m and ms had better be congruent to each other modulo p . And well we are almost there you can observe if you cancel the m from both sides it implies that $s \cong 1(mod\ p)$ Ok and so that is the end of the proof . Just a little aside on this this cancellation of m. So, remember I can cancel m because m is not congruent to 0 modulo p ok . If m is not divisible by p, I can cancel m from both sides of a congruence and why is that because. So, recall what is given is this I know I am given that ms is congruent to m modulo p . This just means that their difference $ms - m$ is divisible by p. This is what a congruence means . But, this means in particular that p divides $m(s-1)$ and if p divides a product.

But, recall when p divides a product, but p does not divide one of the terms right. This this factor m has no powers of p in its prime factorization then it means that p must divide the other term that is the only way out. In other words, s must be congruent to 1 mod p ok. So, this is just a little proof of why cancellation is is valid ok .



$\Rightarrow \; s \equiv 1 \pmod p$ (cancel m) ($p \nmid m$)

Given

$$ms \equiv m \pmod p$$

$$\Rightarrow p \mid ms - m \Rightarrow p \mid \underline{m}(s-1) \; ; \text{ but } p \nmid m$$

$$\Downarrow$$

$$p \mid s-1$$

$$\Downarrow$$

$$s \equiv 1 \pmod p$$

So, again so to to broadly summarize the idea of the proof here it it again comes back to the to the very same thing as as before this this action on cosets is what we we study here . So, the key point is really in understanding this this figure here on this on the screen which is when you look at all the subsets of X and you look at the left translation action on subsets the Sylow subgroups and their cosets they form a bunch of nice regular orbits ok .

Each orbit has cardinality m and if there are s Sylow subgroups the total total number is ms and then all the other orbits are the not so nice orbits which are orbits of subsets a which are not of this form, but those orbits all have cardinalities which are divisible by p ok. So, all those orbits will be divisible by p whereas, each of these orbits are are are not divisible by p and and then that coupled with the what we know about the cardinality of X completes the proof ok .