

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

1. LECTURE 19 [SYLOW THEOREMS I]

Today we will continue talking about the Sylow theorems. So, we still have not actually stated any of the Sylow theorems. But recall from last time that we stated the following proposition B which was motivated by our understanding of how p -groups act on sets whose cardinalities are co prime to p ok. So, this was the converse to that p -group acting with fixed points proposition .

So, we had called it proposition B last time. So, let me just recall the statement in the contra positive form.

Proposition 1.1. *Let us say suppose I have a group G whose cardinality is divisible by p , but suppose G is not a p -group ok, then you can construct a finite G -set X , such that p does not divide the cardinality of X and such that there are no fixed points $X^G \neq \emptyset$.*

ok.

So, this is the in some sense, a statement about the existence of fixed point free actions with also satisfying that cardinality co prime to p condition ok and these are the blanket

Propⁿ B: Let $p \mid |G|$. If G is not a p -group, then

Recall \exists a G -set X such that $p \nmid |X|$ and $X^G = \emptyset$.
 (existence of fixed-point-free actions)


G, X finite
 p prime

↕

Sylow Theorem I: Let $|G| = p^d m$ $d \geq 1, m \geq 1$.
 Then \exists a subgroup H of G st $|H| = p^d$.

Proof: If G is a p -group (i.e, $m=1$), then $H=G$. done

otherwise: By Propⁿ B, \exists a G -set X st
 $p \nmid |X|$ and $X^G = \emptyset$.



assumptions G and X are always finite, p is some fixed prime number ok. Now, this is going to somehow be our starting point for the first Sylow theorem. So, let me state what is called Sylow theorem number 1 Sylow theorem I ok. What does it say?

Theorem 1.1 (Sylow Theorem 1). *Let $|G| = p^d m$ such that $d \geq 1, m \geq 1$. Then there exist a subgroup H of G such that $|H| = p^d$.*

It says let G be a finite group whose cardinality is divisible by p So, same assumption as above. So, I will assume that the cardinality of G is of the form $p^d m$. So, I am assuming the cardinality is divisible by p so, I will say d the power d is at least 1 and m is at least 1 ok. So, let G be a finite group whose cardinality is divisible by p that is all the statement is saying. Then, the Sylow theorem says that there exists a subgroup H such that cardinality of H is exactly p^d . So, take the maximum power of p which divides the cardinality of a group, you can find a subgroup of that exact cardinality ok. So, this is this celebrated theorem statement is called Sylow theorem number I and it will turn out that in some sense, this statement here is actually equivalent to proposition B ok. So, this is; this is the in fact, what we will talk about today ok. So, I will at least establish one side of the the equivalence and leave the other T.

So, let us prove the Sylow theorem. So, we have already proved proposition B. Let us use proposition B to show how the first Sylow theorem follows ok. So, let me prove proof of this Sylow theorem. So, first observe that if G is already a p -group; if G is a p -group what does that mean?

It means that G the cardinality is already a power of p in other words, the number $m = 1$, then this is trivial, the assertion is trivial I just take $H = G$ itself ok and so, the theorem is done, I mean the proof is done there is nothing to do ok, so done .

Otherwise , in other words, if m is at least two or in other words, there are other primes which divide the cardinality of the group , then let us use proposition B ok, now we are in the setting of proposition B which says that if a prime divides a cardinality of a group, but G is not a power of that prime. The cardinality of G is not a power of that prime , then I can manufacture a fixed point free action whose cardinality or fixed point free action on a G set whose cardinality is not divisible by p , ok.

So, otherwise ok so, now, let us use proposition B to conclude the following use proposition B or let us write it as using proposition B by proposition B there exists a G -set X with two properties such that p does not divide the cardinality and there are no fixed points , ok.

Now, what does this get us? Here is the first observation. So, suppose I have a set X on which the group X recall that there are the the action of the group splits this into equivalence classes which are the different orbits, so let me just draw a picture these are let us say the different orbits of the various elements , ok. So, I have my orbits ok G orbits in X ok that is what the picture is. Now, observe that the sum of all these orbits so, let us give these orbits names may be O_1, O_2, \dots there are some finitely many of them. Observe that the sum of the orbit cardinalities is of course, the cardinality of the whole set X ok . So, this cardinality plus this plus this plus this plus this and so on just going to give you the full cardinality.

$$\sum_i |O_i| = |X|$$

Now, since the whole cardinality is not divisible by p at least one of these O_i 's there exists an orbit whose cardinality is not divisible by p right otherwise, every if every single orbit had cardinality divisible by p , the total sum would also be divisible by p ok. So, let us pick that



G -orbits in X $\mathcal{O}_1, \mathcal{O}_2, \dots$

$$\sum |\mathcal{O}_i| = |X|$$

Since $p \nmid |X|$, \exists an orbit whose cardinality is not divisible by p .

Suppose $G \cdot a = \text{orbit}(a)$ has the property that $p \nmid |G \cdot a|$

Recall: $|\text{orbit}(a)| = |G| / |G_a|$

$$G_a = \text{stabilizer of } a \\ = \{g \in G \mid g \cdot a = a\}$$




orbit so, let us take an element in that orbit maybe so, in my picture, let us just say maybe this this green fellow has cardinality which is not divisible by p so, I will take this orbit and let me pick a particular element in this orbit ok. So, let me take an element inside . So, let me call that element something a ok, so let um; let a belong to that orbit. So, suppose so, let us say so, suppose a is that kind suppose the orbit of a so, this is remember this is a notation $G \cdot a$ just means the orbit of a has the property that p does not divide the orbit cardinality ok . Suppose the orbit of a has the property you should say has the property ok.

So, consider that particular orbit the one that is marked in green there. Now, let us recall the the counting statement which says that recall: the counting theorem which says that the cardinality of an orbit is just the cardinality of the full group divided by the cardinality of the stabilizer ok. So, what is G_a here? $G_a = \{g \in G \mid ga = a\}$ is nothing, but the stabilizer of a which just means its all group elements of G which fix a ok. So, this is just the counting theorem.

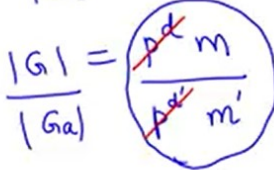
So, what is this this mean? So, what is this this G_a here? So, what are our conclusions? So, here are various conclusions. Consider this new subgroup. So, remember the Sylow theorem says that we are trying to find a subgroup with some properties ok.

So, consider this subgroup G_a ok. So, this is sort of going to be my candidate for my Sylow subgroup or my subgroup H whose thing is a power of p So, let me call it H^1 . Consider the subgroup H^1 which is the stabilizer of G . So, this is a subgroup ok. So, this is just my notation for now. I am just calling $G_a = H^1$. What do I know about it ok? Consider this now let me try and figure out some facts about it.

$$\frac{|G|}{|G_a|} = |\text{orbit}(a)|$$

So: Consider $H' := G_a$ subgroup of G . 


(1) $\frac{|G|}{|G_a|} = |\text{orbit}(a)|$ is not divisible by p

$\frac{|G|}{|G_a|} = \frac{p^d m}{p^{d'} m'}$  ← no powers of p divide this quotient.

$|G_a| = p^{d'} m'$ $d' \geq 0$
 $m' \geq 1$
 $p \nmid m'$

$\Rightarrow d' = d$

$\Rightarrow |G_a| = p^d m'$ $|H'| = p^d m'$ $m' \geq 1$
 $p \nmid m'$



which is not divisible by p that was our assumption ok. So, now, what does that mean? So, let us write this cardinality of $|G| = p^d m$. Cardinality of $|G_a| = p^{d'} m'$. So, d prime is some power so, I do not know could be 0 as well, m prime is some number which is 1 or more ok. Now, let us divide $\frac{|G|}{|G_a|}$. So, observe any any number, any natural number can always be written in this form as p to the some power times some natural number ok uniquely where p does not divide m prime ok. So, this is $p^d m$. Now in this quotient, what is it that I know that finally, there are no powers of p occurring ok.

So, after I consider this quotient here, after I have cancelled out all the common factors, what I know is that no p is occur; no powers of p are left over ; no powers of p divide this quotient , well when can that happen? It can only happen if every power of p on the denominator everything here canceled out everything on top right only then, can you not have any p 's remaining. So, remember m and m' are relatively prime to p right, they have no p 's in them they are products of powers of other primes. So, what is this mean? This means that the only way this could have happened is if this power d prime was actually equal to this power d' ok. In other words, what have we done we have constructed a subgroup G_a which has the following property that its cardinality looks like this it is $p^d m'$ ok the d being the same d as what we had for the original group ok ok.

So, this subgroup. So, maybe let me call this subgroup not as H^1 , but as H' ok. So, H' is this this subgroup here and what I conclude is that H' has so, it is; it is just another name for G_a , this is has cardinality which also looks like this $p^d m'$, ok for the same power $p^d m'$, p does not dividem'ok. Now, so we are almost there in other words, H' is almost the subgroup we are looking for what is it that the Sylow theorem says here is a statement it says that I can find a subgroup H of G whose cardinality is just p^d ok just that maximum power p^d . This is an almost so, by the way this such a subgroup H is called a Sylow subgroup or a p -Sylow subgroup.

$$(2) \quad \begin{array}{c} G \\ p^d m \end{array} \not\cong \begin{array}{c} H' \\ p^d m' \end{array}$$



$$m \geq m'$$

observe: $m > m'$; in other words

$$H' \neq G.$$

Why not?

$$\text{If } H' = G \Rightarrow G_a = G$$

$$\Rightarrow \text{orbit}(a) = \{a\}$$

$$\Rightarrow a \in X^G.$$

contradiction!




What we have manufactured now is something which is almost a p -Sylow subgroup. Its cardinality is it and the maximum power of p is the same still p^d . But then, there is some additional factor m' here ok which could be 1 or more. If $m' = 1$, then we are done, ok ok.

So, we are almost there. So, this is see. So, let me observe the following that to start with I had my original group G whose cardinality was $p^d m'$ sorry $p^d m$. Now, inside G , I manufactured this G a subgroup which we will call H' whose cardinality is also the form p to the d times something ok. Now, observe this G is of course, bigger than than H' . H' is a subgroup of G . So, observe certainly that m has to be greater than or equal to m' ok because the cardinality of H' is less than or equal to the cardinality of G ok. But in fact, this is strictly smaller ok, but observe something more m is actually strictly bigger than m' ok.

In other words, this is a proper subgroup, this is not the whole guy, it is actually a proper subgroup. In other words, H' cannot be the whole thing ok why not? Because if H' this subgroup we have constructed is the whole group G , then it means that well what was H' ? It was the the stabilizer of that element G . If the stabilizer of that element is the whole group well that just means that every element of the group stabilizes that element a . In other words, $\text{orbit}(a) = \{a\}$ itself right or if you want to think in terms of cardinalities, the cardinality of the orbit is just 1 ok. Now, what does that mean? It means a is a fixed point ok. But that is a contradiction remember this was a fixed-point free action. So, that is why, we are using that property.

That, since it was a fixed-point free action, the subgroup the stabilizer of that element G_a is a proper subgroup of the p -group ok. So, we have manage to to sort of reduce the size of the problem instead of the original group G , we now have a proper subgroup H' ok and both G and H' have the same power of p , the same highest power of p dividing both ok.


Now, it is all we have to do is really repeat the argument. Now, here is the next step. If H' is a p group; if H' is a p -group what does that mean? It means that that power m prime is

If H' is a p -group (i.e. $m'=1$) then $H=H'$  done

If not, repeat the above arguments using Propⁿ B.

$$\begin{array}{cccc}
 G & \supseteq & H' & \supseteq & H'' & \supseteq & H''' \\
 p^d m & & p^d m' & & p^d m'' & & p^d m''' \\
 (m > 1) & & (m' > 1) & & (m'' > 1) & &
 \end{array}$$

If $m''=1$, then $H=H''$ done; else repeat argument.

$$m > m' > m'' > m''' > \dots \geq 1 \Rightarrow \text{The process has to stop.}$$


exactly 1 I am; I am sorry the number m prime is 1 let us go up again which means that this is already just the cardinality is p to the d ok there is no m prime in it then, we are done.

Then H' itself is your Sylow group right is the p Sylow subgroup because its cardinality is exactly p^d ok. Then again, we are done. Then take H the p Sylow subgroup in the theorem to just p H' and we can stop the proof right there ok. If not; if not, well then let us repeat the above set of arguments, repeat the above arguments using proposition B. So, remember proposition B is really the key statement that we need. It says if you have a non p -group, then you can construct a nice, fixed-point free action ok. So, if you see what we have done? If G is not a p -group, it had cardinality $p^d m$ and if $m \neq 1$, it is not a p group then, we are able to construct a subgroup H' whose cardinality now looks like $p^d m$ prime. If m prime is 1, then you are done. If m prime is greater than 1, which means that this is also not a p group, then you can repeat the argument and construct another subgroup H' and this subgroup H' also has. So, the subgroup H' has cardinality which is again of the same form which is the power of p is still the same and the the number m is now the number m' or rather m'' in this case ok. So, let us call it m'' . Now, if $m'' = 1$ which means if H double prime is a p group, then again, we are done ok. So, now, again you know it is now a question of the just repeating the argument again and again.

So, observe if $m'' = 1$, then we are done, if $m'' = 1$, then the Sylow group you are looking for is just H double prime you are done else repeat the argument again ok ok. So, else would mean m'' is also positive strictly bigger than 1, you can construct another guy and so on. So, observe that this sequence of subgroups that we are constructing, they all have the following property that they all have cardinalities of the form p power d into something. That p power d is the same throughout and these numbers m, m', m'', m''' are all you know m is strictly bigger than this, is strictly bigger than this, is strictly bigger than this and so on. They are all at least 1 of course, ok. Why is this strictly inequality is because at every step, you have

$\Rightarrow H^{m''}$ has cardinality $p^d \cdot 1 = p^d$.
 (proof is complete).

Exercise: Show that Sylow Theorem I \Rightarrow Proposition B.

a proper subgroup right. So, the cardinality of G is strictly bigger than the cardinality of H' which means that since p^d factor is the same m had better be bigger than m prime ok.

So, I construct such a strictly descending chain, but all of them are at least 1 right. So, this means that the process has to stop somewhere, you cannot keep going on forever the process has to stop and at some point, it stops you you have to reach 1 which means that there is some subgroup at some m'' has cardinality p^d into the corresponding $m'' = 1$.

So, in other words its cardinality is p^d ok. So, you you cannot keep going on and on here. At some point, the process has to stop which means that you must have reached a p -group ok and that is really the the proof of the theorem ok. So, this is proof complete ok. So, if you have seen may be the proof of of Sylow's theorem from you know prior courses and so on this is it looks slightly different, but it is the proof has been arranged in this manner primarily to to focus on the fact that Sylow's theorem itself is actually you know just a consequence of a statement about the existence of fixed point free action. So, this is really what underlies Sylow's theorem that is what is going on in the background ok. Now, so, I hope you will sort of look through this proof again and try to understand the the basic idea here. It is; it is a rather simple idea that at every step, if you have a p group you are done.

If it is not a p group, you can construct a fixed point free action, take one of the orbits in that; in that action which is not divisible by p , the cardinality not divisible by p and the stabilizer of an element there will give you a proper subgroup and you know keep going on and on and on at some point that stabilizer will have to become a p - group ok. Otherwise, this process goes on forever which is a contradiction ok. Now, that is; that is an interesting uh consequence of proposition B, but what is extremely interesting is that in fact, the first Sylow theorem also implies proposition B ok. So, we have proved one implication, but in fact, one can show that you can now assume the statement of Sylow theorem I and deduce proposition B from it ok.

So, I am going to leave this as an exercise for you, but please do try this exercise. Show that Sylow theorem I implies the statement of proposition B. So, assume this statement and prove the other statement. So, which means that so, what is proposition B state? If it is not a p group, then you should somehow construct a set X on which the group acts without fixed points. And to do that, you have to use the Sylow subgroup now. So, if G is a given to be a non p group, look at the p Sylow subgroup of that group and use the group and the subgroup to somehow construct the set X on which the group acts without fixed points, ok. So, it is a; it is a very interesting and useful exercise and I hope you will; you will try your hand at it.