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

1. Lecture 18 [Sylow Theorems: A Preliminary proposition]

Today, we will start talking about the Sylow Theorems. So, let me first recall two results that we spoke about in our previous videos. So, the first one was the proposition we started out with which is that,

Proposition 1.1. *if G is a group which acts on set X both G and X being finite. And if G turns out to be a p group, p is a fixed prime and the cardinality of X is not divisible by p, then there exists a fixed point for the action, $X^G \neq \emptyset$.*

So, this was the first thing that we proved by analyzing orbits and stabilizers and so on. The second one is was one of our applications of this basic fixed point principle,

Proposition 1.2. *Take any two numbers n and r natural numbers then:*

$$\binom{pn}{pr} \cong \binom{n}{r} (mod\ p)$$

.

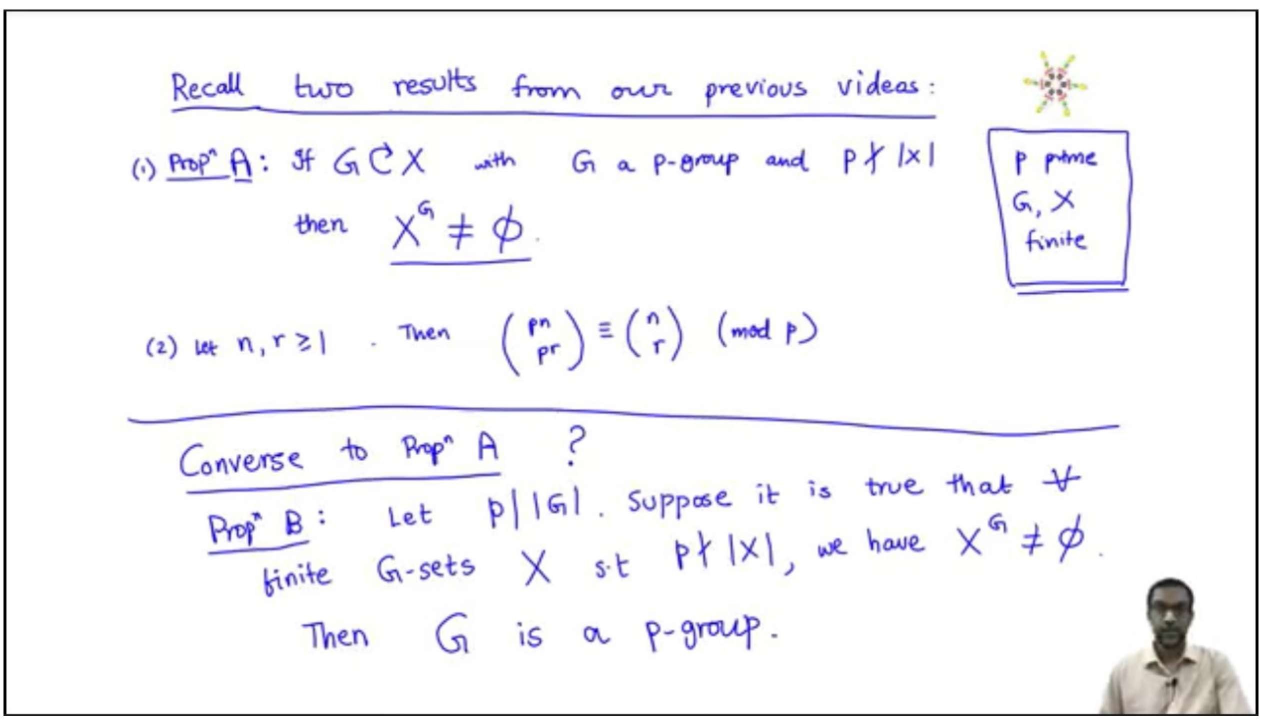


Figure 1. Refer Slide time 00:21

So, these were two results and I am sort of recalling them specifically because, I am going to use both of them together. So, let us begin. So, what I first want to ask is sort of the following converse, if you will to this this proposition here. So, here is a converse question. So, converse to this proposition. So, and we should just give this a name for now let me call this proposition A. So, I want to know what can I say about the converse to Proposition A? Is there, a converse ok. In other words can I say something about suppose I have so, ok. Let us let us try and formulate reasonable converse here. So, let me make some hypotheses. So, let me call this proposition B.

Proposition 1.3. *Let p be a prime such that p divides $|G|$. Suppose it is true that for all finite G-set X such that p doesn't divide $|X|$, we have $X^G \neq \emptyset$, then G is a p-group.*

Again I will make these blanket assumptions that p is a prime G and X are finite sets and G is a group acting on the set X. So, for proposition B let me formulate it as follows, let p divide the cardinality of G first ok. So, let me assume that the the group cardinality is divisible by p. Now, suppose we have the following property, that whenever this group G acts on a set X whose cardinality is not divisible by p, then it always has fixed points ok.

So, it acts in such a way that it always has every action on set whose cardinality is not divisible by p; every such action has a fixed point ok. So, suppose the group has this property. So, let p divide the cardinality of G, suppose it is true that for all finite sets X. So, let me call it finite G-sets recall; that means, that there is an action of the group G on the set X. Suppose it is true that for all finite G-sets X such that p does not divide its cardinality, we have X^G is not empty ok. In other words every such action has fixed points. Then can I conclude that G is a p group then G. I want to claim is in fact, a p group ok. So, observe if G is a p group then this is the Proposition A says exactly this I mean, it says that on every such set X whose cardinality is not divisible by p the action of G will have fixed points ok. So, we are sort of asking the converse question. If we know this property the fixed point property of actions, then is it necessarily true that G is a p group ok. And for this of course, I will assume that p divides the cardinality of $|G|$ that sort of the first main assumption ok.

We will prove this this statement by sort of first rephrasing it. So, it turns out that this is in fact true and let us prove this to prove this let us rephrase it in its contra positive form. So, what does that mean? We will show suppose G is not so, in some sense proof by contradiction if you wish suppose G is not a p group ok.

But, remember the cardinality of $|G|$ was divisible by p. So, if you write out what the cardinality of $|G|$ looks like? p will be one of the factors ok. And of course, it can occur to some power right cardinality could be divisible by $p, p^2, p^3, ...$ and so on. There will always be some highest power of p which divides the cardinality. So, let me call that d. So, what is d here? d is the highest power, highest power of p such that p^d divides the cardinality of the group.

And of course, if I write out the prime factorization of G of the cardinality of G in addition to p^d, then what I will start seeing next is a bunch of you know powers of other primes not not p itself, but other primes. So, let me not write out the entire prime factorization, let me just call the that product of powers of other primes as the number m ok. So, what is m here well $m \geq 2$. And observe m is essentially the product of prime powers other than p. So, of course, m is co prime to p in other words p does not divide the number m ok.

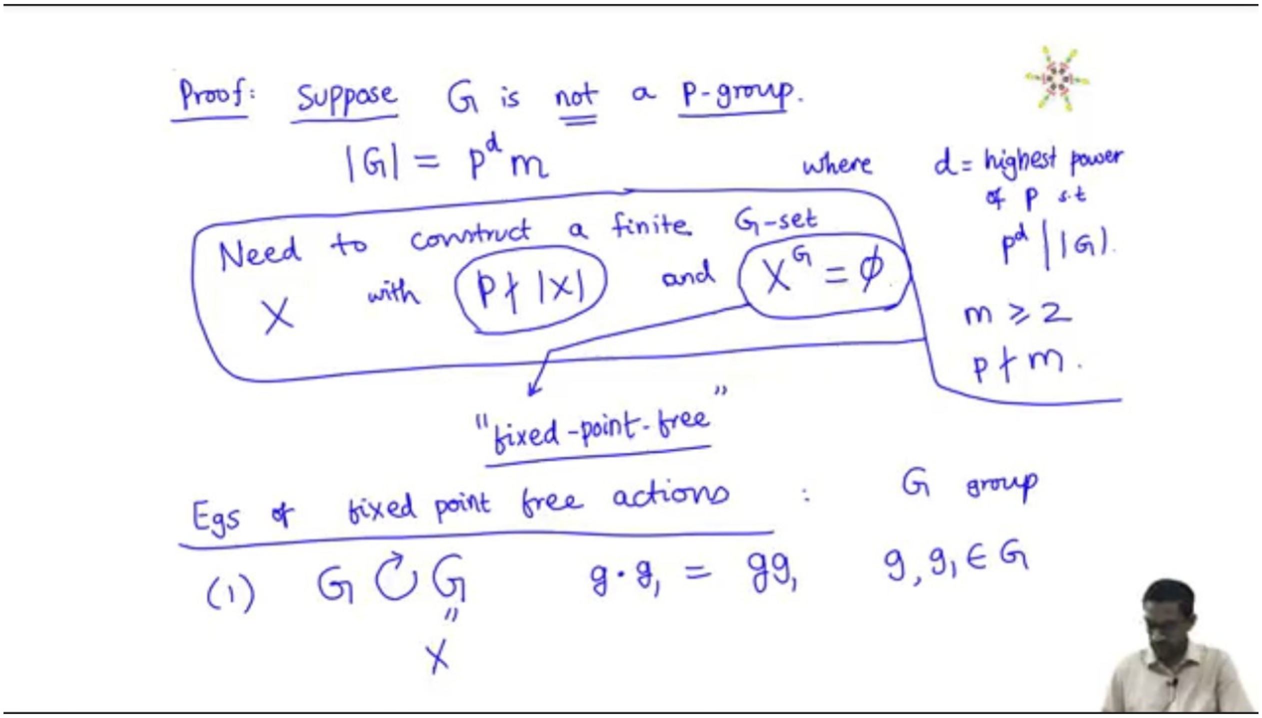


Figure 2. Refer Slide time 00:21

So, any any number can always be written in this way, but I still have not incorporated this assumption, I am saying suppose G is not a p group. So, what does that mean? It says when I write the cardinality of G in this way, the number $m \neq 1$ cannot be 1 ok. So, if the number $m = 1$ then of course, it just means that the cardinality of G is p^d ok. So, here is what I know? That $m \geq 2$ ok. So, this is what we conclude from the fact that from the assumption that G is not a p group ok. Now, let see what do we need to do? In order to prove the proposition. So, let me go back to the statement of proposition B ok. So, it says suppose it is true that for all finite G-sets X such that p does not divide the cardinality, we have $X^G \neq \emptyset$ then G is a p group right. So, to prove this I am saying suppose G is not a p group. Then what I will do? Is I will produce finite G-set X. What we need to do? Is to produce a finite G-set X, whose cardinality is not divisible by p such that $X^G = \emptyset$ ok. So, this is what we would need to do in order to complete the proof. So, need to construct a finite G-set X with p not dividing its cardinality and such that there are no fixed points ok. If I can do this, then I would have obtained a contradiction and therefore, my original assumption would have been wrong. And therefore, the proof would be complete ok.

So, what I really need to do is the following? So, if G is not a B group, then I should be able to construct an action of G, you know on a set X such that there are no fixed points. In other words I need to construct a fixed point free action ok. So, such an action let us just give this a name. So, I I would like to say that this sort of action is what is called fixed point free? Meaning there are no fixed points here ok or fixed point less if you wish ok. So, let us let us analyze such actions for little while. So, notice the key point here is we also need this condition there are two conditions, we need to satisfy number 1 the cardinality should not be divisible by p and secondly, there should be no fixed points ok.

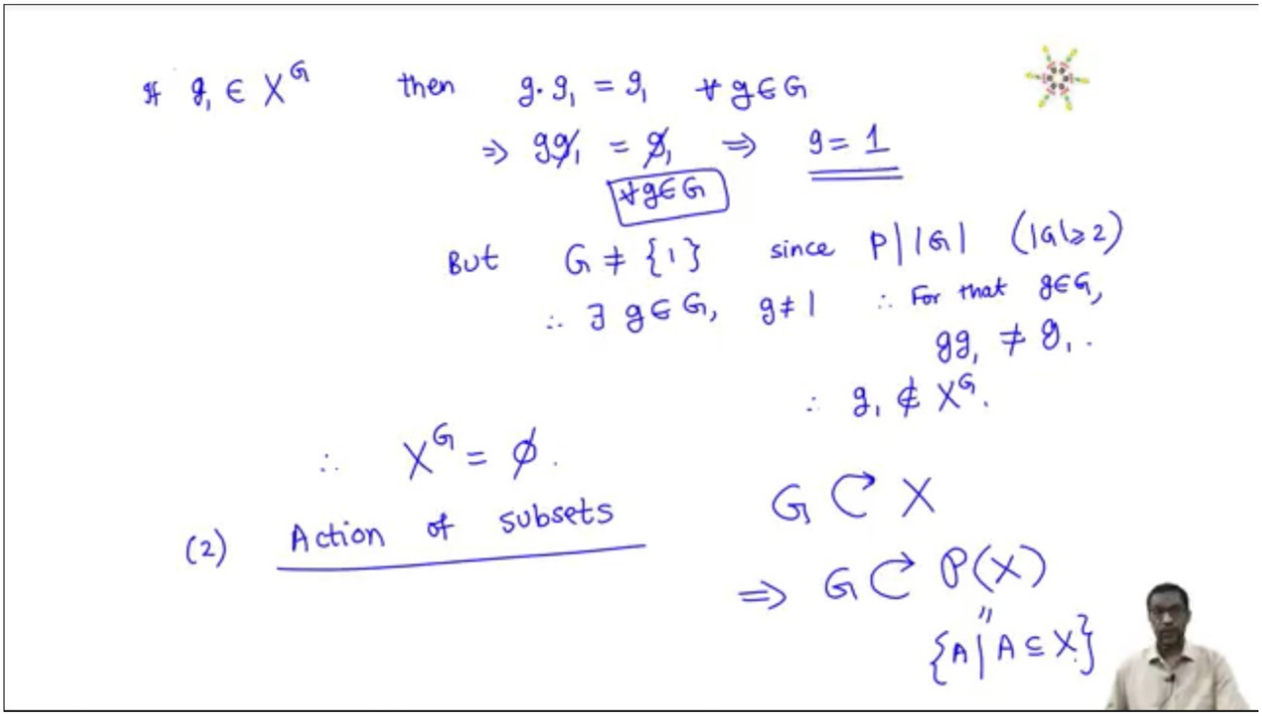


FIGURE 3. Refer Slide time 10:54

Now, so, sorry this condition is what is what I want to call fixed point freeness ok? Now, what is the next thing? Let us show that ok. So, let us let us analyze fixed point free actions for little bit. So, what are some examples of fixed point free actions? Examples of fixed point free actions ok. So, let me assume my group G is fixed so, G is my given finite group. Now, there is always a very nice action which we have looked at before which is a group acting on itself, by sort of left multiplication by multiplication. So, how does the group g act in this case? g acting on the group element g_1 is just the product $g \cdot g_1 = gg_1$ ok. So, here g and g_1 are both elements of the group. So, the the group and the set are in some sense the same. So, I think of this as my set X on which my group acts, this acts by left multiplication and the interesting thing about this is that this is a fixed point free action ok.

So, let us check that what are the fixed points for this action? So, if I have a fixed point. So, suppose I let me call an element g 1 let us say, if it is a fixed point for this action. If I have a fixed point then what does that mean, it says that $g \cdot g_1 = g_1$ for all group elements $g \in G$ ok. But, that just means that the product $gg_1 = g_1$, but this necessarily means and remember this should hold for all group elements $g \in G$. Now, what does that mean? That just means that well I can after all its a group. So, I can cancel I have cancellation on both sides so, it means $g = 1$ ok. But, remember this this equation is supposed to hold for all group elements $g \in G$ ok, but what we have just shown is it can only possibly hold for the identity element of G ok. So, observe, but remember we know that G is not the identity group remember, that G is not just the group with a single element. Since we have already assumed that it is divisible by some prime number right.

So, this is in other words cardinality of $|G| \geq 2$ or more. So, surely there exists an element other than the identity in the group ok. Therefore, I can always find an element $g \in G$ other than the identity ok. And also for that element I get a contradiction here ok. So, therefore, I can't have so, what what do I mean? There exists an element $g \in G$. So, that $g \neq 1$ for that $gg_1 \neq g_1$ok. So, therefore, g_1 cannot be a fixed point therefore, g_1 cannot be ok. So, in other words I cannot have any fixed points for this action ok. So, therefore, we conclude that under the hypothesis, that the group is not the identity group. The left multiplication action is fixed point free ok. So, this is one example. Now, um here is another important example that will that will come up again. So, this has already occurred in our our previous video. So, this is what we had called action on subsets ok. So, what is the general setting here? If I have a group which acts on a set X then, from this I can construct a new action of the group G on subsets of X ok. So, on the power set what we call the power set of X, this is the set of all $\{A|A \subseteq X\}$ ok. So, I can construct an action on subsets and what is the action well it is just the element wise action.

So, recall again that the action on subsets is defined like this g a group element acting on a subset A. So, here A is assumed to be a subset of the original set X. How does g act on this subset A? It just acts element wise you its just set consisting of $\{ga|a \in A\}$ ok. So, this is going to be a new subset and this is the this is the action g acting on a produces, this new subset which is just the element twice action on the original subset. And observe we had used this in fact, to prove that the congruence that $\binom{pn}{pr} \cong \binom{n}{r}(mod\ p)$, by sort of analyzing the action on dots in a grid and looking at subsets of dots and so, on. So, this is the general formalism whenever you have an action on a set you also have automatically an action on subsets of that set.

So, let us apply this to the to the particular case. So, let us take the example of the previous action. Suppose I take my set X to also be the group G ok, in other words I look at G acting on G by the multiplication by left multiplication. Now, this action well what are its well ok now I want to look at the action now on subsets of G. So, for the action on G, I just said there cannot possibly be fixed points. But what about for the action on subsets of G? Can I have fixed points there ok.

So, let us analyze that action. So, let us call this this new set as Y maybe now let us ask. What is $Y^G =$? In other words which subsets of G are invariant under this action ok? So, let us observe what what what do we have? So, suppose I have a subset.

So, suppose I have a fixed point. Then what property must that fixed point satisfy? Then, it means $g \cdot A = A$, this should be true for all group elements $g \in G$ ok. In other words on the left hand side I have the product $\{ga|a \in A\}$. And on the right hand side I just have the original set a itself ok. Now, what does this mean? So, this is the property I want to be true. So, maybe its easiest to just draw a figure here. So, let me imagine this is my group G ok and I have a certain subset A of the group so, here is my subset A. Now, what I am saying? Is that if I take these elements of A and I multiply all of them by a single group element G no matter which one. The answer is again the same dots ok meaning when I when I hit this dot by an element of G it probably, it could become some other dot ok. But, it does not leave the group so, it does not leave the subset A ok. So, when I when I multiply G with elements of A, I just get back elements of A again ok. So, that is sort of what what this is saying ok? Now, observe again that this is not this is very easy to to violate. For example, suppose I take an element b here ok. So, suppose so here is my here is my conclusion, let us analyze this suppose $A \neq G$ ok. Then pick some element $b \notin A$ ok. So, that is that is in this green dot in the picture a point which is not in A.

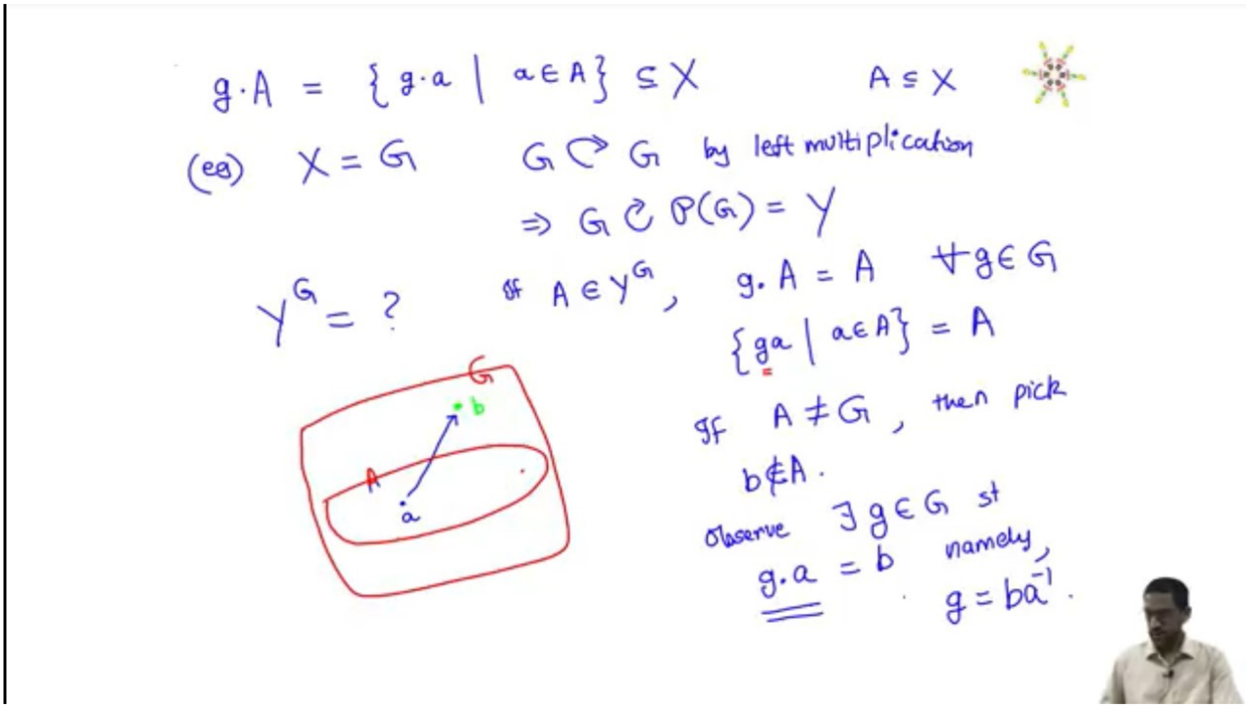


FIGURE 4. Refer Slide time 00:21

Now, observe that suppose I take any point $a \in A$. I can always map it to b. So, let us call this take any one point $a \in A$, I claim you can find group element which will when acting on a it will give you b ok.

Now, observe there always exists a group element $g \in G$ such that $ga = b$ ok. And why well that element is namely? The element $g = ba^{-1}$ right because, recall this action of g on a was just the action by left multiplication. So, if I multiply a on the left by ba^{-1} of course, the answer is b ok. So, if I take this particular group element g, it maps a to this element b which is outside a ok. So, what is that mean? It says that there cannot really exist any subset A which is a fixed point for this action ok. Because, I can always find an appropriate group element which will take a point a which is inside this subset to a point b which is outside the subset ok.

So, what does that mean? This means observe a cannot be a fixed point ok. So, this was under the assumption that a was not the whole set right. So, this analysis you can try and convince yourselves, that this analysis actually proves the following.

So, here is our conclusion it says that if I have any proper non empty subset $A \subseteq G$, it cannot be a fixed point for this action. In other words the only fixed points are well the empty set $\emptyset$ is necessarily the empty set is a subset and its a fixed point of course, because if it if it is empty to begin with when you act by group. The group elements there is nothing you can act on. So, the result is again empty ok. And the whole set G that is again invariant because uh that is a fixed point because, when you hit every element of the group G, by some fixed element small g. What you get is again elements of the group G ok? So, its trivial that the the whole set is necessarily a fixed point ok. So, here is a conclusion there are only two fixed points, for the action on the power set which is the empty set and the whole set ok. So, this is almost fixed point free its not quite fixed point free, there are these two sort of

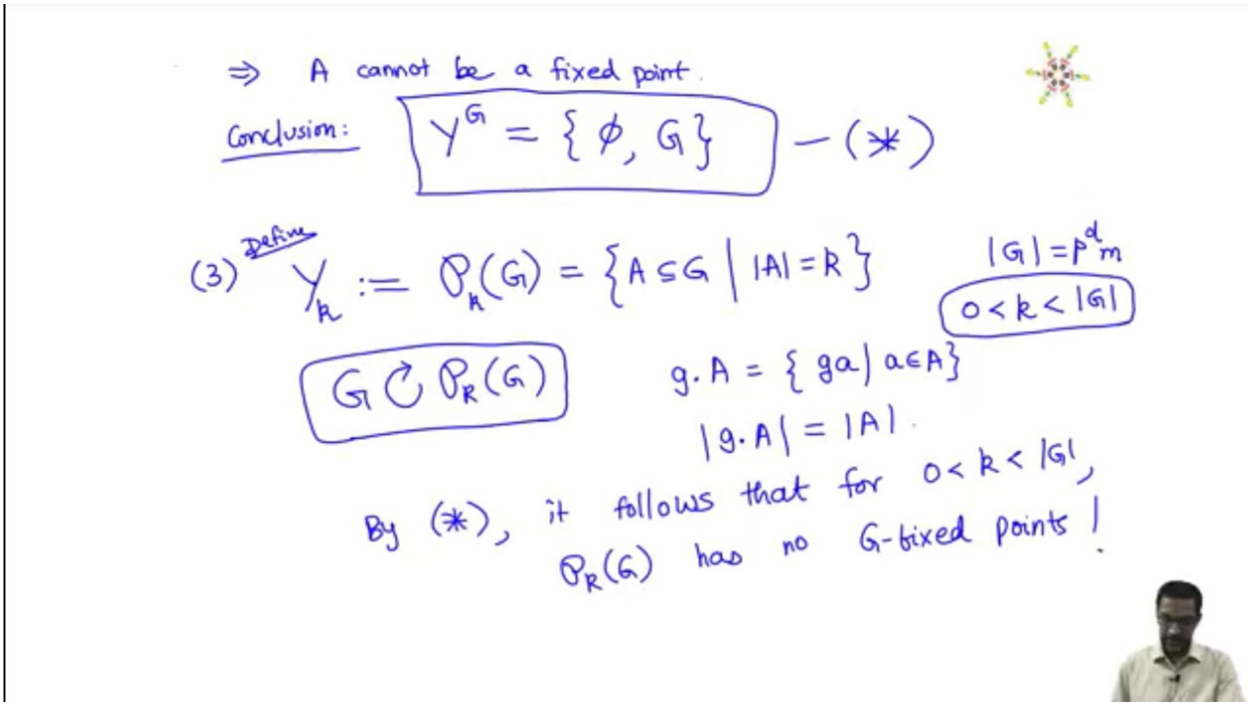


FIGURE 5. Refer Slide time 19:03

trivial fixed points. But, there is this sort of example three is slight modification of of this this earlier argument. Let us consider not the entire power set. So, let me call this this set instead of the set Y, uh let me fix also a number ok. What shall we we call it? Let us call it um so ok.

So, I have the cardinality of the group here. So, remember the cardinality of the group was something we assume the cardinality of the group looks like this $p^d m$ ok. So, let me pick some number $0 < k < |G|$. Or maybe the sort of a symmetrical way to write, it is I take k to be a natural number which is strictly between $0 < k < |G|$ ok. Then look at what I will call Y_k ok? So, let us define this set called $Y_k := P_k(G) = \{A \subseteq G||A| = k\}$ well what is this?So, maybe another notation so, let me also give another name for this it is the p. So, the power set of G with k as my my subscript $P_k(G)$. So, what is $P_k(G)$? It is the set of all subsets of G whose cardinality is k ok of a fixed cardinality. And again remember this is again something, we have seen in the the earlier video on the congruence problem where we took all dots. So, we took a grid of 12 dots and we looked at all subsets of 6 dots out of the 12 dots ok.

So, we fix the cardinality of the subsets and observe that there is of course, a group action also on$P_k(G)$ ok. So, observe G acts the action on subsets, also gives you an action of the group G on the set $P_k(G)$ ok. So, there is an action of G on $P_k(G)$ why the same thing. So, how does it act? When g acts on the subset a it just gives you the element wise action, which in this case is just left multiplication.

So, let us just write it as g a the product as a belongs to A. And this new set of course, has the same cardinality as the original set because, I have just taken element by element and acted on them by you know left multiplied by group element g. So, this is just going to give me the original thing ok. So, if the original set had k elements the new set will have k

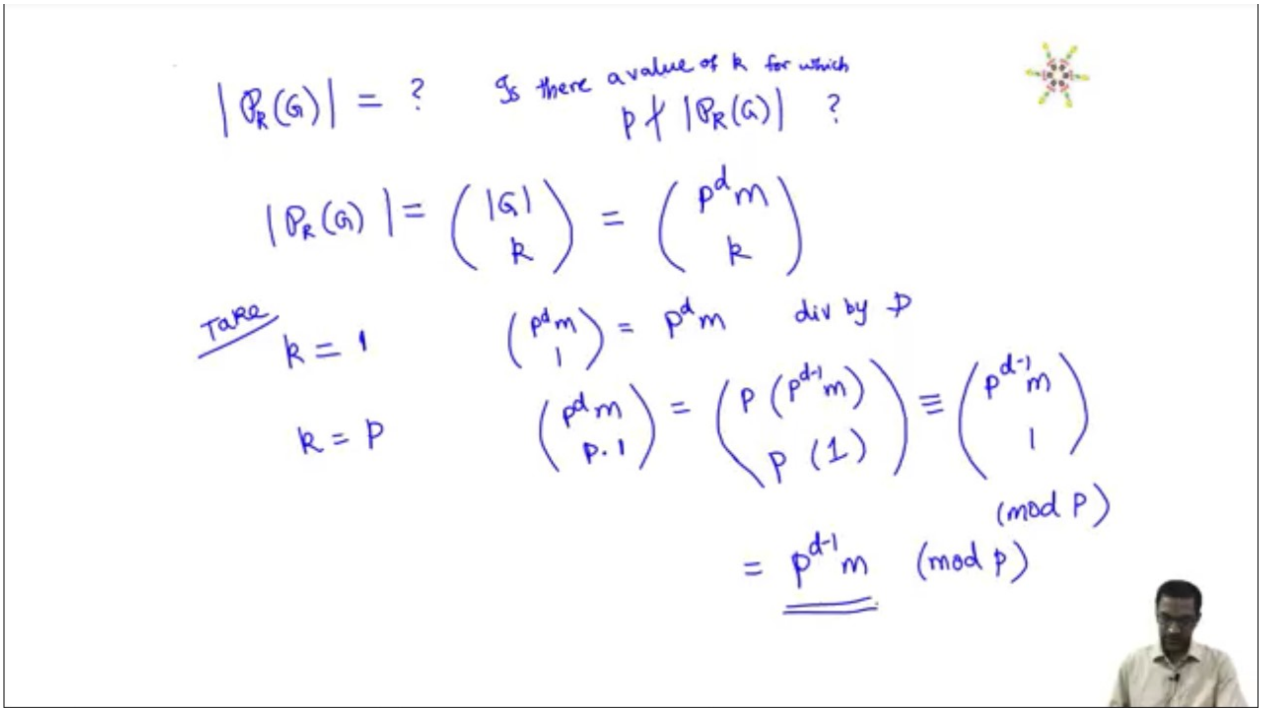


FIGURE 6. Refer Slide time 25:11

elements also. So, it will be another element of $P_k(G)$ ok. So, what I have now is the action of a group on subsets of cardinality k ok. And now observe that if k is strictly between 0 and cardinality G ok. Then what does that mean? It means that the subsets a that I am considering here. So, $P_k(G)$ the subsets A. I am not I mean if I took $k = 0$, then $P_0(G)$ is just the it contains only the empty set. And if I took k to be the other end mod G itself, then the only subset in $P_k(G)$ will be the full set ok. Now, for k strictly between these two bounds I have $P_k(G)$ consists of subsets which are you know non empty and not the whole proper subsets and we have just seen that none of those can be a fixed point ok. So, observe by what we have just said. So, by this observation before by observation star, it follows that for k strictly between these two numbers $P_k(G)$ has no fixed points ok.

So, here is a fixed point free action has no G fixed points ok. So, we have we have managed to find an example of of something which has no G fixed points. And remember; however that. So let us go back to what we wanted to prove? We wanted to prove um that there exists a subset need to construct a finite G-set X such that it there are no fixed points.

So, that we have managed to do now right take a group G and look at $P_k(G)$ for example, where $0 < k < |G|$k that is a fixed point free action. But, remember there is this additional condition I also want my set to have cardinality that is not divisible by p ok. So, now let us look at this the set that we have managed to construct right here. Which is what I call$P_k(G)$?

So, now, what can I say about the cardinality of $P_k(G)$? Is it divisible by p or not. I would like it not to be divisible by p right, if I can find the value of k, for some value of k if this is not divisible by p then I have done I have proved my proposition ok.

For let let just say for what value of k is not divisible by p is there a value of k. So, is there a value of k for which the cardinality of $P_k(G)$ let us make ourselves more space. So, is that a value of k for which the cardinality of $P_k(G)$ is not divisible by p ok. And to answer this we need that second observation that we talked about. So, let us ask ourselves. What is the cardinality ?

$$|P_k(G)| = \binom{|G|}{k} = \binom{p^d m}{k}$$

Now, what I want to do? Is to try and use that that proposition. So, let me take the following value of k. So, let me take k to be let us say p for instance ok. So, I mean we could start with various choices of k, but let us take k to be well maybe how about $k = 1$ that is the most obvious choice right. So, let us try a few values of k, if I take $k = 1$. Then this is

$$\binom{p^d m}{1} = p^d m$$

well this is divisible by p. Because, there is of course, a p^d in front right so, that is no good that value of k is not going to help me. Let me try the next one which is p itself well I am going to try p now look at this so

$$\binom{p^d m}{p} = \binom{p(p^{d-1}m)}{p} \cong \binom{p^{d-1}m}{1}(mod\ p)$$
$$= p^{d-1}m(mod\ p)$$

. So, I will put this into the form of the the earlier result. So, it is p to the dm choose p into 1. So, I will write it as p times p to the d minus 1 m choose p times 1 ok and which by the earlier result is congruent to p to the d minus 1 m choose 1 mod p ok. Now, let us look at this its p to the d minus 1 m choose 1, but that is just by definition p to the d minus 1 m mod p ok. And now this again is well this is could be 0 mod p because, p to the d minus 1 is probably still some you know some power of p. But, its already better than the original right the original guy was p to the d m, now I managed to get it down to p to the d minus 1 m ok.

And now you can see that all it takes now is to repeat this argument. So, let us repeat this argument the value of k that will do the trick for us is $k = p^d$. So, here is the chain of computation.

$$\binom{p^d}{p^d} = \binom{p(p^{d-1}m)}{p(p^{d-1})} \cong \binom{p^{d-1}m}{p^{d-1}}(mod\ p)$$
$$\cong \binom{p^{d-2}m}{p^{d-2}}(mod\ p)$$
$$\cong .... \cong \binom{m}{1}(mod\ p) \cong m(mod\ p)$$

So, if I have p to the d m choose p to the d, I can think of it as I will pull out a p from both p to the d minus 1 m p to the d minus 1.

And by that proposition by that result its p to the d minus 1 m choose p to the d minus 1 ok mod p. Now, again this is this is in the same form as the original I can keep going therefore, again I will pull out a p from both the thing on the top and on the bottom and I will get this to be p to the d minus 2 m choose p to the d minus 2 mod p and so on and so, forth till all the p's have been pulled out 1 by 1.

And what is on top is m and what is on the bottom is 1. So, this is m choose 1 mod p which is of course, just m ok. So, observe this is nothing, but m mod p ok. So, what are we

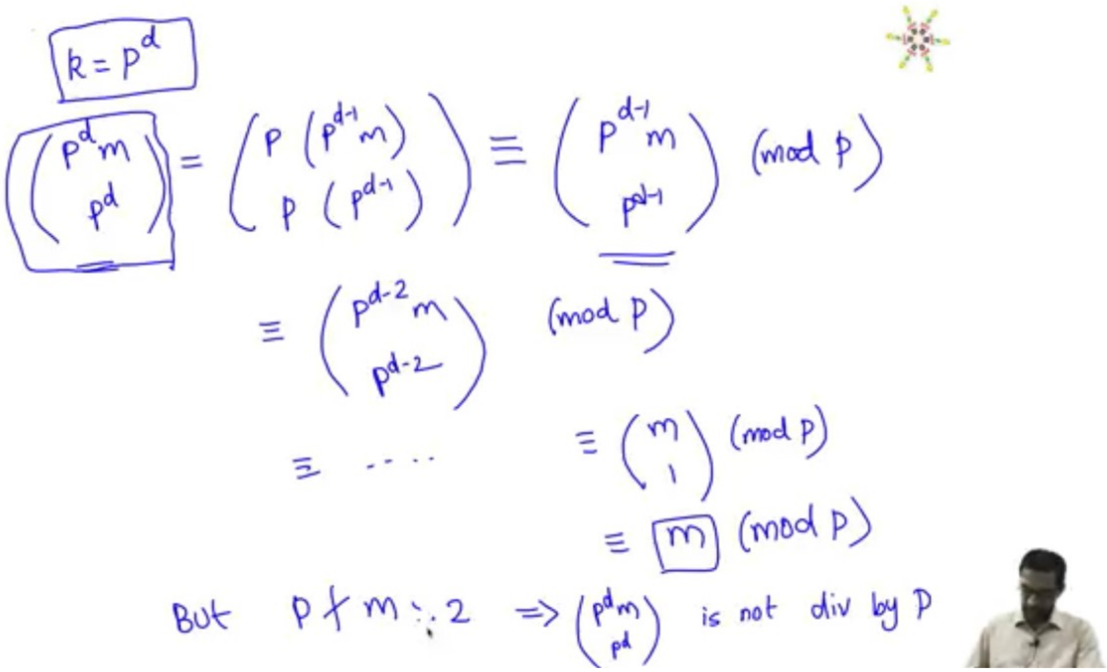


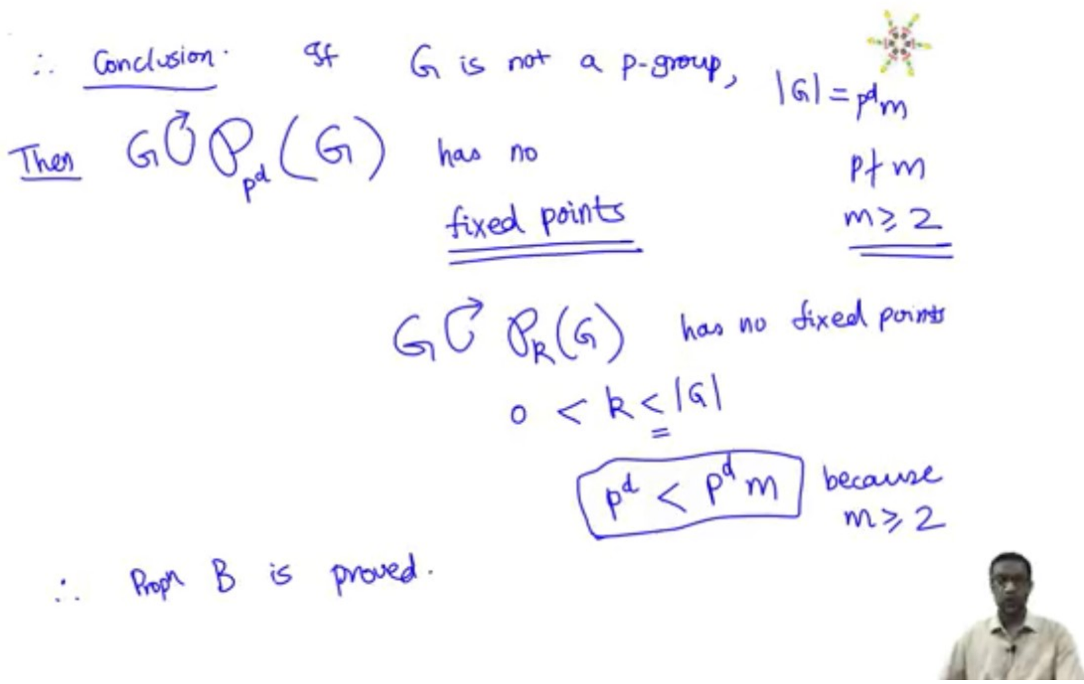
FIGURE 7. Refer Slide time 28:30

we proved p to the d m choose p to the d is congruent to m mod p. And m remember was a number that is not divisible by p ok so, but p does not divide m that was our assumption that is what m was and m was a number that was 2 or more ok. So, what does that mean? I mean I do not really care about no I do. So, let us say m here is a number that is that is 2 or more that was our assumption that G was not a p group. So, this means that this this number $\binom{p^d m}{p^d}$ is congruent to a number that is not. So, its not congruent to $\cong 0(mod\ p)$ its not divisible by p, I mean at the moment let me not worry about this m greater than equal to two business. So, all I know all I care about is that m is not divisible by p and; that means, that neither is this $\binom{p^d m}{p^d}$ ok.

So, what have we done? We have we have actually managed to do what we wanted that we have constructed, we seem to have constructed uh a set on which this group G acts without fixed points ok.

Therefore final conclusion is the following that under the assumption. So, if G is not a p group look at the set the power set of G subsets of G of G of cardinality exactly p^d ok. So, let us say cardinality of G looks like $p^d m$ ok p does not divide m, then what we have shown is that the action of G on this set has no fixed points ok.

But, we seemingly have not used the fact that $m \geq 2$, but we actually have used it so, observe that I I also assumed. So, G can be written in this way p not dividing m, m is at least 2 right. Because, it is not a p group where have we used it. So, observe this has no fixed points that that requires that you know remember what did I say before, I said the power set $P_k(G)$ the action of G on the on the power set $P_k(G)$ has no fixed points. provided $0 < k < |G|$ ok. So, I I need this strict inequality here ok. Now why is that inequality strict



in this case? So, if I take $k = p^d < |G| = p^d m$ this inequality is strict because $m \geq 2$ ok, that is why its true.

So, I am I am actually looking at proper subsets subsets of cardinality of p^d are actually proper subsets of the group. They cannot they are not the entire group itself because, p to the d is in fact strictly smaller than the the full cardinality of the group ok. So, therefore, we have managed to prove therefore, this proves proposition B; proposition B is proved in other words we have managed to prove a nice converse to our to our original result. So, let me go back and show you the statement of proposition B. So, here is what we have managed to prove ok, which is that if a prime divides the cardinality of a group and suppose its true that for all G-sets X such that p does not divide its cardinality there is a fixed point, then this group had better be a p group ok.