

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

1. LECTURE 16 [FIXED POINTS OF GROUP ACTIONS]

Today, we will start talking about fixed points of group actions ok. So let us make the definitions first. Now, we start with a group G acting on a set X . so, let us say G is a group and because this was our shorthand for saying that G , there is an action of G on the set X . so, this is set X , group G . And sometimes we say as a shorthand that X is a G -set, in other words it is a set with a group action, the action of the group G ok.

So, given this. given a group and a set on which it acts, a fixed point. so a point or a or an element an element x of X is said to be a fixed point, is said to be a fixed point or a G fixed point, said to be a G fixed point. If the following happens that. g acting on x gives me x , for all group elements $g \in G$. In other words, it is fixed. the element x is fixed by the action of every group element.

Now, we have a another way of saying this equivalently. another equivalent formulation is to say that the orbit of the element x is just the singleton x ok. Remember, the orbit just comprises all the elements of the form gx , as g varies over G , but here you only get the

Def: G group \curvearrowright X set " X is a G -set "

, an element $x \in X$ is said to be a G -fixed point if $g \cdot x = x \quad \forall g \in G$

(orbit(x) = $\{x\}$)

$X^G := \{ x \in X \mid g \cdot x = x \quad \forall g \in G \}$ the set of G -fixed points.

Def: p prime number . If $|G| = p^k$ for some $k \geq 1$, then G is a p -group.

FIGURE 1. Refer Slide time 3:13

Propⁿ: Let G be a p -group & X be a G -set st $p \nmid |X|$. Then $X^G \neq \emptyset$ (i.e. \exists a G -fixed point).

Proof: Need to prove: \exists an orbit \mathcal{O} st $|\mathcal{O}| = 1$.

let $a \in X$; $|\text{orbit}(a)| = |G|/|G_a|$ $G_a = \{g \in G \mid ga = a\}$
stabilizer of 'a'

G_a subgroup of $G \Rightarrow |G_a| \mid |G| = p^k \Rightarrow |G_a| = p^i$
 $0 \leq i \leq k$

$|\text{orbit}(a)| = p^{k-i}$ is either $\boxed{1}$ or $\boxed{\text{divisible by } p}$

$|X| = \sum_j |\mathcal{O}_j|$ \mathcal{O}_j distinct G -orbits in X .


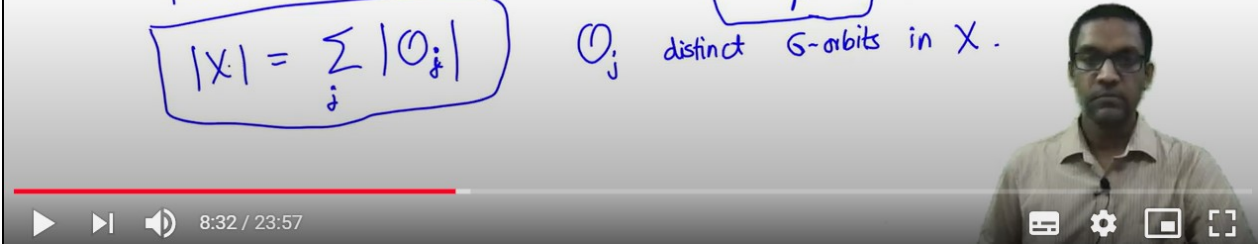



FIGURE 2. Refer Slide time 8:32

element x in the orbit. So, another way of saying that a point is fixed is to say that its orbit is a singleton ok. And here is the notation for the set of all fixed points. X^G is the set of all fixed points. set of all $x \in X$, such that $g \cdot x = x$, for all $g \in G$. so this is the set of fixed points ok. Now, here is another little definition. so this is regarding the group itself. So, we say that suppose p is a prime number. if the cardinality of the group is a power of p , if this looks like p^k for some $k \geq 1$. Then we say G is a p group. So, this again is a situation which will arise frequently enough to warrant its own terminology. So, shorthand we say that group G is a p group, if it is a finite group whose cardinality is some power of a prime p . so, the p is the same p here.

Now, so. what do I mean the definitions of fixed points and p groups have sort of been given one after the other for the following reason?

We have the following proposition which concerns the actions of p groups on sets and what their fixed points look like and so on. So, if G is a p group; so let G be a p group; so I fixed the prime p here and let X be a G -set, it is got an action of the group G such that the cardinality of X is not a multiple of p .

So, notice that G and X are of very different types; G has cardinality of power of p and X has cardinality which is not even divisible by p ok. They are sort of the opposite ends of the spectrum in some sense.

But, if you do have such situation and you have the group G acting on the set X ; then something very interesting happens, then this action must necessarily have a fixed point. In other words, a set of fixed points cannot be empty; i.e., there exists a fixed point or a G -fixed point.

So, it is a theorem which asserts the existence of fixed points ok; so, let us prove this proposition. So, what is it that we need to prove? We need to prove that there exists a

singleton orbit right; so, remember that is what fixed points are. So, I need to show to prove that at least one orbit has cardinality one, there exists an G -orbit; let us call it O , such that the cardinality of that orbit is 1 ok.

There is an orbit of some element a ; I mean the orbits remember, partition the set X into a disjoint union; I mean the disjoint union of orbits is just the whole set X . Now, let us try and find this orbit or prove that such an orbit must necessarily exist. So, let us take a typical element of X and ask what can its orbit look like or what cardinality can its orbit have.

So, let $a \in X$; now let us look at the orbit of a and observe the cardinality of this orbit is given by the counting formula recall which says that this is the cardinality of the full group divided by the cardinality of the stabilizer of that element ok; G_a is just a stabilizer. So, G_a is nothing, but the set of all elements of the group, so that $ga = a$; so that is the stabilizer ok.

Now, what is G_a here? G_a recall is a subgroup of G , so by Lagrange's theorem; the cardinality of this subgroup must divide the cardinality of the group. But remember, I have assumed G is a p group, in other words the cardinality of G is some power of p . This means the cardinality of G_a is therefore, also a power of p , this must look like some p^i ok; these are the only divisors of p^k .

So, this exponent $0 \leq i \leq k$. Now, observe what does this tell us? This says that the orbit cardinality is also a power of p ; this is just p^{k-i} .

so this is some power of p . Of course, $k = i$; so this power could just be $p^0 = 1$, but it could be any of the other parts; $1, p, p^2, \dots$

So, now, what does that mean? So, this is therefore, what is it? This is either 1 or some higher power of p or well any power of p ; p, p^2, p^3, \dots are all divisible by p .

So, there are only two possibilities; it is either the orbit cardinality can either be 1; if its p^0 or if its p, p^2, p^3 ; then those numbers are all necessarily divisible by p ok. And now observe that the cardinality of the whole set X is just the sum of the cardinalities of the different orbits. So, let me give the orbit some name O_j s, let us say j you know running over, how many other disjoint orbits I have.

So, what are the O_j 's? O_j 's are the distinct orbits, G -orbits in X ok. Now, this equation here; on the left hand side, I have a number which is not divisible by p ; that was my hypothesis that p does not divide the cardinality of X , whereas, on the right hand side; I have a sum of numbers each of which is either 1 or divisible by p .

So, what does that mean? This equality can only appear, I mean the fact that this equality holds means that the right hand side must have some 1's right; otherwise all the summands on the right hand side are necessarily multiples of p , which would also imply that the left hand side must be a multiple of p ok.

So, by what we have just said; so, this property star here that orbit cardinalities I_j are either 1 or a multiple of p , we conclude; so by star and the fact that the left hand side which is cardinality X is not divisible by p . We conclude there must be at least one orbit O_j ; such that its cardinality is not divisible by p , but; that means, the cardinality is 1, I mean that is by star in some sense; so, star is really being used here to say that the cardinality is 1 which means there exists a fixed point which is exactly what we are talking about.

So, that completes the proof; so, that central proof here, we have shown at least one orbit is a singleton ok, but. In fact, we have shown a little bit more. So, if you have if you sort of look at you know what the proof shows; so, the proof establishes a little stronger result.

By (*) and $p \nmid |X|$, $\exists O_j$ s.t. $p \nmid |O_j|$
 $\Rightarrow |O_j| = 1 \Rightarrow \exists$ a fixed point ■

Propⁿ: $G \curvearrowright X$ G p -group $p \nmid |X|$
 Then $|X^G| \equiv |X| \pmod{p}$

Pf: $|X| = \sum |O_j| = \underbrace{\sum_{j: |O_j|=1} |O_j|}_{|X^G|} + \underbrace{\sum_{j: |O_j|>1} |O_j|}_{\substack{\text{divisible by } p \\ \left(\begin{smallmatrix} \text{Recall} \\ m \equiv n \pmod{p} \\ \Leftrightarrow p \mid m-n \end{smallmatrix} \right)}}$

$\Rightarrow p \mid |X| - |X^G|$ ■


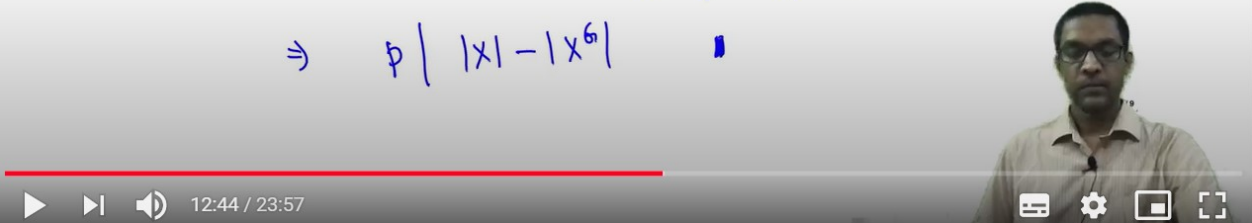



FIGURE 3. Refer Slide time 8:32

So, let us call this proposition um; well let us call it proposition for now. So, this is a slight strengthening of the earlier one.

So, under the same hypothesis; under so, let us write the hypothesis again, G finite group acting on a finite set X , G is a p group, X does not have, is not divisible by p ; the cardinality. Then, we have just shown that there definitely exists some fixed points, but in fact, what we are shown is that, if you look at how many fixed points there are; the number of fixed points, the cardinality of $X^G \cong X \pmod{p}$. So, recall what congruence means, we say two numbers are congruent to each other. So, recall when do you say two numbers are congruent to each other; you say $m \cong n \pmod{p}$, if $m - n$ divisible by p ; I mean they both leave the same remainder when divided by p .

In other words, we say m is congruent to n when if p divides their difference right. So, here again I am saying that the cardinality of the subset X^G is congruent to the cardinality of the whole set X modulo p and prove well the same observation as before, that on the one hand; I have the cardinality of X , on the other hand I have the cardinalities of the different orbits.

Now, some of these; so I will rewrite this sum as the sum over the singleton orbits. So, I can say let us first take the cardinalities of only those O_j 's which are singleton; orbits only those j 's which are the fixed points plus the cardinality of those orbits which are non singletons; sum over j such that the cardinality of $O_j \geq 1$.

Now, observe that; what is this? When you sum over the orbits whose cardinality is exactly 1, what you are doing is just summing over the fixed points, so here this sum will just give you X^G . And now the sum over the orbit cardinalities which are greater than 1, these remember are all some proper higher powers of p . So, this sum is going to be divisible by p ok.

$G = C_p = \{1, \sigma, \sigma^2, \dots, \sigma^{p-1}\} \quad \sigma^p = 1$

Define $G \curvearrowright X$ by: cyclic permutation of entries
 $1 \cdot (y_1, \dots, y_p) = (y_1, \dots, y_p)$
 $\sigma \cdot (y_1, y_2, \dots, y_p) = (y_p, y_1, y_2, \dots, y_{p-1})$
 $\sigma^2 \cdot (y_1, y_2, \dots, y_p) = (y_{p-1}, y_p, y_1, y_2, \dots, y_{p-2})$
 \vdots

Exercise: This is an action.

21:00 / 23:57

FIGURE 5. Refer Slide time 8:32

So, because there I was trying to conclude that X^G is not empty, in the second one is more general. So, you know one should erase that from the hypothesis. So, let me restate the second proposition again; this says that if a group, finite group acts on a finite set and if the group G is a p group, then it is true that the set of fixed points is congruent to the original group modulo p ok.

So, I do not really need to assume that p does not divide the cardinality of X ; so, I could have zero fixed points in this case. So, now let me go back to this; so, what am I trying to do? I am trying to construct a p group g which will act on a finite set X and in order to for this conclusion to the set, let me try and find; so, we will try to do this, try to find a finite set X ; whose cardinality is a power p ; so, that is the left hand side here and whose fixed point set has cardinality a ok.

So, that is the plan trying to find something whose fixed point set is a and the original set is a power p and the group must be a p group which acts on it. So, let us try and do this; so, what is this number a here? a is just some natural number. So, how do we find a set whose cardinality is a^p ? Well, the simplest thing to do is let us just take first a set of cardinality a .

So, the simplest set is $Y = \{1, 2, 3, \dots, a\}$, $|Y| = a$ and how do I construct something of cardinality a^p ? I will just take many copies of this. So, let us take $X = Y \times Y \times \dots \times Y$; I mean by copies I mean the cross product, this is just the Cartesian product Y^p and observe this has the correct cardinality now; cardinality of $|X| = a^p$.

Now, what are elements of X ? If you think about it, it is just all elements of the following form; it is $\{y_1, y_2, \dots, y_p \mid 1 \leq y_i \leq a\}$; so, that is what my set X looks like, all p tuples of numbers between 1 and a . So, I have a set with the correct cardinality, now I must try and concoct a group G , which is a p group which acts on this set. Now, the easiest p group in some sense is just a cyclic group of cardinality p .

So, let us do that next. So, for my group I will choose just a cyclic group C_p of cardinality p . So, let me write its elements as follows; one is the identity element of this group $\{\sigma, \sigma^2, \dots, \sigma^p\}$ where sigma is the generator of the cyclic group; so, $\sigma^p = 1$.

So, here is a; this is definitely a p group does cardinality exactly p here and I need to make this cyclic group, act on this set X , which if you recall from the previous page; this is just all p tuples of elements $\{y_1, y_2, \dots, y_p\}$. So, how do we make a cyclic group act on p tuples? That is the question.

So, we need to define an action; so, let us define this as follows. So, let us try to figure out how this generator σ of the cyclic group will have to act; σ when it acts on this p tuple of elements, I am going to take a typical element $\{y_1, y_2, \dots, y_p\}$, let me take $\{y_1, y_2, \dots, y_p\}$; this is an element of X , I need to make this into another element of X . There is sort of one obvious thing I can do, let it act by cyclic permutation or cyclic permutation of the entries of y . So in other words, I will push everything one step to the right. So, I move y_1 to the second position, y_2 to the third position and so on; the end I put y_{p-1} and y_p gets cyclically rotated and sort of moves up to the first of this tuple ok. So, this is how I define the action of σ ; takes the tuple $\{y_1, y_2, \dots, y_p\}$ and cyclically rotates the entries; of course, sigma square therefore, will perform a cyclic rotation by two steps.

So, I will have to define it in the obvious fashion; I will move y_{p-1} and y_p to the first, move y_1 two steps to the right and so on ok. The higher powers of sigma will all have to act likewise and it is an easy exercise to check that this in fact, defines an action, this is an action. In other words, you have to check the axioms of an action; the identity acts trivially, so you also define the identity action, as just doing nothing $\{y_1, y_2, \dots, y_p\}$ just gives you back $\{y_1, y_2, \dots, y_p\}$.

And it is very easy to check that this satisfies the definitions of the axiom; definitions of an action The key point is somehow if you do $\sigma^p = 1$, that is really all the checking involves ok. So, I will leave this for you to check, but having done this; let us see if this gives us what we want.

So, we have managed to define an action of a p group on a set X and like I said, I do not need any assumption on p dividing the cardinality of X or not dividing the cardinality of X ; on this guy in this case.

So, in this setting; I know the following that the cardinality of X and the cardinality of its fixed points are congruent to each other modulo p ok. Now, the left hand side; as we know is a^p in this case because that is a ; that is how we chose the set. So, let us look to see what the right hand side looks like which is the cardinality; I mean I need look at the fixed point set first. So, what are the fixed points for this action? So, that is a question right. So, suppose I have a certain p tuple; $\{y_1, y_2, \dots, y_p\}$; in X^G and this p tuple is fixed under the action. So, I take $\{y_1, y_2, \dots, y_p\} \in X^G$ what does it mean? This means that in particular its fixed by sigma right, every element of the group fixes it; particular sigma fixes it the generator, but observe the left hand side is just a cyclic permutation of the entry. So, this is $\{y_p, y_1, y_2, \dots, y_{p-1}\}$.

Now, how can these two possibly be equal? So, the fact that these are equal; it is only possible if all the entries are equal right. Because you just look at the second entries of these two tuples, you observe in this case its y_1 and the other case it is y_2 ok, so y_1 must be the same as y_2 . Now, compare the third entries y_2 and y_3 and so on.

So, unless all the entries are equal to each other; you cannot get the cyclic rotation being equal to the original ok. Now, what does that mean? It means that the only possible fixed

$$G \curvearrowright X \Rightarrow |X| \equiv |X^G| \pmod{p}$$

\downarrow
 $a^p \equiv$

$$X^G \ni (y_1, y_2, \dots, y_p) \Rightarrow \sigma \cdot (y_1, \dots, y_p) = (y_1, y_2, \dots, y_p)$$

\parallel
 $(y_p, y_1, \dots, y_{p-1})$

$\underbrace{\hspace{10em}}_{\text{equal}} \Rightarrow y_1 = y_2 = \dots = y_p$

$$X^G = \{ (y, y, \dots, y) : 1 \leq y \leq a \} \Rightarrow |X^G| = a$$


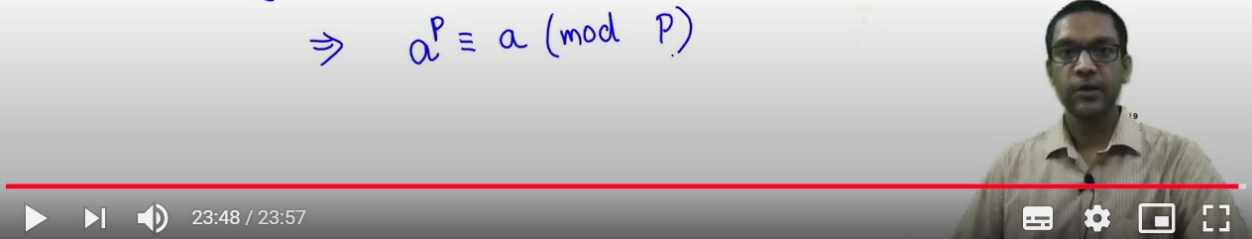
$$\Rightarrow a^p \equiv a \pmod{p}$$



FIGURE 6. Refer Slide time 8:32

points have the following form. So, what does X^G look like? Well, X^G looks like this; it is $\{y, y, y, y, \dots, y\}$; all numbers y are the same, but what are the possible values of y ? y can be any number from 1 to a ok, this in particular means that you know it is all 1s or all 2s or all 3s and so on; till all a s and this means that this is exactly a ; there are just a fixed points ok.

So, what does that mean? It means we have proved Fermat's little theorem, as a corollary of our fixed point principle, the more in general fixed point principle ok. So, in the next video; we will look at a slightly more complicated application of this which will also turn out to appear in our proof of the Sylow theorem.