

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

1. LECTURE 17 [SECOND APPLICATION: FIXED POINTS OF GROUP ACTIONS]

So, now, we will do a Second Application of ah the principle that we talked about earlier, the Fixed point principle. So, the proposition let me recall the fixed point principle this time.

$G$  is a finite group acting on a finite set  $X$  and  $G$  is a  $p$  group.  $|X| \equiv |X^G| \pmod{p}$ .

So, this was the principle. And now we had one nice application of this last time which was the a proof of Fermat's little theorem . Now, here is the second application of this, again sort of a number theoretic statement. So, it says the following ah let  $n$  and  $r$  be some natural numbers ,  $p$  is a prime the same prime that we have fixed throughout ; then the binomial coefficient

$$\binom{pn}{pr} \equiv \binom{n}{r} \pmod{p}$$

So, ah recall the binomial coefficient;  $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ , number of ways of choosing  $r$  out of  $n$  distinguishable objects from which you have to pick  $r$  , ok.

Prop<sup>n</sup>:  $G \curvearrowright X$ ,  $G$   $p$ -group  $\Rightarrow |X| \equiv |X^G| \pmod{p}$

Application 2: let  $n, r \geq 1$ . Then  $\binom{pn}{pr} \equiv \binom{n}{r} \pmod{p}$

$\binom{n}{r} = \frac{n!}{r!(n-r)!}$  = # of ways of choosing  $r$  objects from  $n$  objects.

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

$p$   $\left\{ \begin{array}{c} \dots \\ \dots \\ \dots \end{array} \right.$   $n$

$pn$  dots  $Z := \{\text{dots in this grid}\}$

FIGURE 1. Refer Slide time 00:21

So, now, ah the statement here is really something about ah you know the fact that these two numbers are always congruent to each other, number of ways of picking  $pr$  things from  $pn$  things and the number of ways of choosing  $r$  from  $n$ , they turn out; well they would not be equal of course, but they are congruent to each other when you look at them modulo the prime  $p$ , ok.

So, let us prove this again as an instance of this fixed point principle. So, what I mean going to try and do? Well, the same thing we did earlier; we will try and construct a set  $x$  whose cardinality is the left hand side,  $\binom{pn}{pr}$ . And we will construct a group  $p$  group action on it, such that the set of fixed points gives you the right hand side  $\binom{n}{r}$ , ok. So, we have to manufacture ah the following two things; we need to manufacture a group  $G$  and we need to manufacture a set  $X$ . such that its cardinality is  $\binom{pn}{pr}$  that is the first step. And then we must hope that the fixed point set turns out to be the right hand side, ok. So, let us do this. So, for a start again, ah like last time I will just in the previous example let us just pick the simplest cyclic group of cardinality  $p$  as our  $p$  group.

So, this is just  $C_p = \{1, \sigma, \sigma^2, \dots, \sigma^{(p-1)}\}$ . So, of course, this is a  $p$  group. And now I need to construct a set whose cardinality is  $\binom{pn}{pr}$ , ok. So, how am I going to choose that set? Well, ah first let us construct a set of cardinality  $pn$  as follows. So, I will ah think of it in the following manner. So, let us construct a rectangle, a rectangular grid of dots.

So, I imagine I have a grid like this ok and you know. So, some number of rows, some number of columns. So, let me assume it is got  $p$  rows and  $n$  columns, ok. So, I have a rectangular grid of dots.


So, of course, this has  $pn$  dots in all, ok. So, I am going to take my  $Z$ , ah set  $Z$  to be the set of all the dots in this diagram. So, first my set  $Z$  is the set of all dots in this grid and that is my set, the elements are the dots, ok. So, we will try and give some sort of geometrical construction. And then of course, having done that, ah the set  $X$  itself can be chosen to be you know all subsets of the set  $Z$  of cardinality  $pr$ , ok. So, that is the next step. So, maybe we should just do this uh you know by way of example, just to get a better handle on what is going on. So, the proof is best illustrated by an example.

So, let me actually choose concrete numbers here; let me take  $n$  to be 4, let me take  $r$  to be 2, and let me take my prime to be 3, so that I can actually draw a nice figure here.

So, let me draw ah the first thing which is my set  $Z$ . So, what does  $Z$  look like?  $Z$  is all points in a  $4 \times 3$  grid of dots. So, this is my four guys in the first, let us see where are we, yellow, ok. So, this grid of dots is going to be my set  $Z$ . So, it is got exactly  $pn$  dots. So, observe this is a three columns and I mean four columns and three rows. So, this is a 3 cross 4 grid of dots, ok. So, the dots themselves are they form the elements of my set  $Z$ , ok. So, I have my set  $Z$  here. So, let us copy this; here is my set  $Z$ , ok. Now, ah what is it that I want to define as my set  $X$ ? So,  $X$  of course, remember has to have cardinality  $\binom{pn}{pr}$ , ok.

So, that is what I know about. So,  $Z$  has cardinality 12 which is  $pn$  in this case. The set  $X$  that I am interested in in constructing should have cardinality  $\binom{pn}{pr}$  right, which is the number of ways of choosing  $pr$  objects out of  $pn$  objects. So, this is the number of ways of choosing 6 objects out of 12 objects, so 6 dots out of these 12 dots.

So, I am going to think of all these 12 dots as being distinguishable objects here; I just colored them with three colors to say these are the three rows that is it, ok. So, what should my set  $X$  look like? This is just going to be the collection, the set of all  $A$  subset of  $Z$ . So, subsets of the dots, some collections of dots such that the cardinality of  $A$  is 6; in other

Example:  $n=4$   $r=2$   $p=3$  

$Z$   $3 \times 4$  grid of dots  $|Z| = pn = 12$

$X = \{ A \subseteq Z \mid |A| = 6 \}$   
 $= \{ \text{collections of 6 dots among the 12} \}$

$|X| = \binom{pn}{pr} = \binom{12}{6}$






FIGURE 2. Refer Slide time 04:53

words this is the set of all collections of 6 dots out of these 12 collections of sets, ok. So, set of all such collections, and observe the cardinality is exactly  $\binom{12}{6}$ ; because that is a definition of the binomial coefficient, ok. So, what are some examples of elements of  $A$  for example, ? So,  $A$  is in this case, I need 6 dots, right. So, let us see suppose I take the four guys in the top, this one green, this. So, this is an example of a subset  $A$  of cardinality 6. So, this subset  $A \in X$ , ok. Similarly maybe I could take these three and these three together; this is another, this is another choice of  $A$  and so on. So, you get the idea here. So, I can take these 6 dots or any any collection of 6 dots among these 12, all such collections put together that is my set  $X$  that I am going to talk about, ok. So, I have a set of the correct cardinality, we are only trying to match cardinalities so far. Now, the set  $X$  of course is more complicated than the set  $Z$ .

So, remember the set  $Z$  was well, what was it? It was just the, well it was just this grid, right. So, this is your set  $Z$ , just single dots;  $X$  is more complicated, the elements of  $x$  are now collections of six dots at a time, ok. So, we will come to  $X$ ; but what is it that we eventually want to do? We want to define an action of the group and remember the group in this case is the cyclic group. So, in this case  $p$  was 3 in our example.

So, let me try and construct an action of the cyclic group of three elements on the set  $X$ ; but before I do that, let us first work with  $Z$  as a starting point. So, this is what I eventually want to understand how to define an action on  $X$ ; but for start, let us define an action on  $Z$ . So, how do you make the cyclic group of three elements act on this set  $Z$  of 12 dots? Well, there is one obvious action, what is the obvious thing you can do?

Well, what does  $C_3$  look like?  $C_3 = \{1, \sigma, \sigma^2\}$ , ok.  $\sigma$  is the generator,  $\sigma^3 = 1$ . How do you make this group act on  $Z$ ? Well, it can sort of cyclically permute the rows of this diagram ok, by cyclically permuting rows. So, what do I mean by that, ok? So, let us come back to this

$C_3 \subset Z$      $C_3 = \{1, \sigma, \sigma^2\}$   
 $\sigma^3 = 1$   
 by cyclically permuting rows.

$\sigma \cdot a = a'$  ,  $\sigma \cdot a' = a''$  etc  
 $\sigma^2(\cdot) = \cdot$  etc

Ex: check this defines an action of  $C_3$  on  $Z$

FIGURE 3. Refer Slide time 08:53

next, let us first figure out how to define an action on  $Z$ ? So, how do we cyclically permute rows? What do I mean by that? If I take my element  $\sigma$  and it acts on this dot here, this red dot  $a$ ; well I will define it to be the dot that is right below that dot here. So, I am moving a dot in the first row, the action of  $\sigma$  just takes it to the corresponding dot in the second row. So, this guy is my  $a$  dash for example,  $a'$ . So, similarly how does  $\sigma$  act on this dot? Well, it just moves it down to this other kind,  $a''$ , ok.

Now, how does  $\sigma$  act on dots in the second row? What does it do to a green dot? It just moves it to the corresponding  $a''$  dot on the row below. So, this dot here under  $\sigma$ . So, if we call this  $b$  dash, it will just move to this dot  $b''$ , ok.

So, if I call the dots on the first guy as  $a, b, c, d$  these are all dashes, these are double dashes maybe; then the action of  $\sigma$  is the following, it moves the first row to the second row, the second row elements to the third row and it moves the third row elements back to the first row, ok.

So,  $\sigma \cdot a = a'$ ,  $\sigma \cdot a' = a''$  etcetera. So, I have sort of just visually defined what  $\sigma$  does for you; it moves the red dots to the corresponding green dot below it, it moves the green dots to the corresponding yellow dot below it, and it moves each yellow dot to the red dot which is sort of cyclically below it. Meaning if you sort of think of it as being on a circle or a cylinder; then the yellow dot sort of moves to the corresponding  $a''$  red dot that is going to be in the first row, ok.

So, this is what I mean by cyclically permuting rows. So, this is the action of  $\sigma$  and of course,  $\sigma^2$  will just have to do this twice. So, what will  $\sigma^2$  do? Well, it will sort of do  $\sigma$  two times; in other words how will it act on a red dot? Well, it will move it to the yellow dot which is two steps below it etcetera, right. So, it is I hope it is visually clear, I tried to you know not make it overly formal.

$C_3 \curvearrowright X = \{ \text{6-elt subsets of } \mathbb{Z} \}$   
 General fact  
 $G \curvearrowright X \Rightarrow G \curvearrowright P(X)$   
 by  
 $g \cdot A = \{ g \cdot a \mid a \in A \}$   
 $\forall A \subseteq X$   
 "Action on subsets"

$C_3 \curvearrowright \mathbb{Z} \Rightarrow C_3 \curvearrowright X$   
 $\binom{m}{r} = \binom{12}{6}$

FIGURE 4. Refer Slide time 14:09

So, if you of course, you want you can sort of write this all out in very formal language; but for now let us try and understand the main idea here. If I have a grid of dots like this, then I can make the cyclic group of cardinality three act on it by sort of moving my . So, here is my grid of dots, I act  $\sigma$  does this; it moves each row one row below to the row that is below it, ok. So, this action of  $\sigma$ , ok .

Now, again exercise check that this is an action. So, check this defines an action of the group  $G$  in this case  $C_3$  on the set  $Z$  which is this set of twelve dots, ok. And of course, you can see here, there is nothing special about three and twelve and so on; I could have done this with general  $n$  and  $p$  and  $r$ . I mean  $r$  has not entered the picture yet; but I could have done this with any  $n$  and any  $p$ , the corresponding cyclic group  $C_n$ , the grid now has  $n$  rows right or rather  $p$  rows and  $n$  columns .

So, it has  $p$  rows, the cyclic group of cardinality  $p$  just moves, the generator  $\sigma$  moves each row of dots to the corresponding row below it, ok . So, it is again easy to check that this defines an action that, the the two properties of an action are satisfied. Now, let us come to the question we are interested in; how does, ah how do we define an action of the cyclic group on the set  $X$  here ok ?

So, I need an action of  $C_3$ , not on  $Z$  itself, but I want to understand how to define an action on  $X$ . And what was  $X$ ? If you remember this was just a set of all six element subsets of  $Z$  right, all collections of 6 dots . So, how do I do that? Well, there is again the obvious thing; if I have a set of dots, so here is my set of dots. And ah let us say I have a collection of six dots. So, for instance, uh what shall we do ?

So, suppose I take these four and these two, here is a collection of six dots . So, if this is my subset  $A$  , the collection of 6 dots; then there is again an action of the cyclic group on this by what is called the element wise action , ok. So, if I have. So, this is maybe it is worth

writing out as a general thing ; a general fact to observe that suppose a group acts on a set  $X$  , then the group in fact acts on, given this I can make the group act on what is called the power set of  $P(X)$  right, which is the set of all subsets of  $X$  .

And how do I make it act? As follows by, if I take group element  $g$  and if I take a subset  $A$  of the set  $X$ ; then the definition of the action is just, it just acts element by element, take each element of  $A$  . So, this is this action is defined for every subset of  $X$ ; in other words for every element of the power set, ok. So, this this action here again check it is an action, this is called the action on subsets , ok .

So, this is the action on subsets of  $X$  and this action is just the element wise action; it just acts on every single element of the subset, and each element will now be transformed to some other element and you take the new collections of elements. So, let us do this by example; if  $A$  is this collection of six dots that I have just marked here , then what is  $\sigma$  acting on  $A$  for example, ok? So, by definition, what does  $\sigma$  do to these six dots? Well,  $\sigma$  will take , draw this separately .

So, what will  $\sigma$  do to each of these dots? Sigma will take this red dot to this green dot that is right below it, right . So, this element goes here, this element goes here, this goes here. Well, in fact this goes here and this green guy goes to the thing below it; this yellow fellow in  $A$  goes to the one above it, ok . So, if I act  $\sigma$  on each of these elements, what are the new elements I get? Well, I get these three green dots, I get this green dot, I get this yellow dot and the yellow dot goes to the red dot above . So, I also get this red dot.

So, this new set here, which has let us try it, clean this up a little bit. So, the action of  $\sigma$  on  $A$  is just obtained by acting  $\sigma$  on every element of  $A$  and seeing what are the new dots that you get . So, that is the set  $\sigma(A)$ , it is those four green dots one, two, three, four ; there is a red dot on top , there is a yellow dot on the bottom .

So, this collection of six dots is exactly  $\sigma(A)$  , where  $A$  was the original subset,  $A$  was this thing , the thing I had marked originally in blue , ok. So, I hope the definition is clear, you just add element by element, you act that group element on each element of the subset , ok.

So, this is called the action on subsets . And so, what have we done here? To recall we said, we have an action of  $C_3$  on the set  $Z$  of all dots in the grid, and from here we have an action on the subsets .

Well, there is an action on all subsets ; but in fact you can also restrict this to get an action on subsets of a given cardinality, ok. So, ah I mean as is clear if I have a collection of , if I have a subset of  $Z$  which has six elements and I act a group element on that subset ; the new subset also has six elements, ok.

So, this is the action of on subsets of a given cardinality . So, anyway this is, this is something that you should check in this case; that because I have an action of  $C_3$  on  $Z$ , I also have an action of  $C_3$  on  $X$ , which was the collection of six elements subsets of  $Z$ .


So, we have we are closed now, we already have a  $p$  group and we have an action of that  $p$  group on the set  $X$  , whose cardinality is exactly  $\binom{pn}{pr}$ , this cardinality is  $\binom{pn}{pr}$  , ok. Now, the question is the; I mean now we are we are ready to apply our fixed point principle.

So, by our proposition or the fixed point principle; let me call it that , I know that the

$$|X| \cong |X^G|(\text{mod } p)$$

Now, let us again do it in this example. So, what is our set  $X$  ?  $X$  is the collection of all six elements subsets . So, its cardinality is as we know  $\binom{12}{6}$  . Now, what is the, what are the

By f.p. principle,  $|X| \equiv |X^G| \pmod{p}$

$$\binom{12}{6} \equiv$$


$A \subseteq Z, |A| = 6$

$A \in X^G \Rightarrow ?$

$\Rightarrow \sigma \cdot A = A \Rightarrow$

$\Rightarrow A$  must be a union of columns in  $Z$ .

$A$  is a collection of 6 dots which remains invariant under "cyclic rotation"

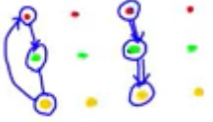




FIGURE 5. Refer Slide time 19:19

fixed points? So, that is the question. So, let us try and understand, what the fixed points of this look like? So, here is a grid again, ok. So, here is the question, suppose I have a six element subset of these twelve dots.

So, let us take  $A$  to be a subset of this grid of dots and  $A$  let us say has 6 elements, ok. Now, the question is when does  $A \in X^G$ ? What does it mean to say that  $A$  is a fixed point, ok? So, let us try and figure that out. If  $A$  is a fixed point in particular,  $A$  is fixed this means that  $A$  is actually fixed by  $\sigma$  the generator of the group; in fact this is enough if it is fixed by  $\sigma$ , then it is also fixed by  $\sigma^2$ ,  $\sigma^3$  and so on.

So, but let us just look at this condition,  $A$  is fixed by the element  $\sigma$  of the group. Now, what is this mean? So, if you recall, what ah the action of  $\sigma$  was; it moved ah dots in a given row to the corresponding dots in the row below it, ok. So, which, how can I choose six dots? So, this is my question; how can I choose six dots from this diagram, so that when I move that configuration of six dots, one unit down sort of cyclically; the new configuration of six dots coincides with the original configuration of six dots, ok.

So, the question is, how to choose a configuration? Well, a  $\sigma$  is  $A$  just means that  $A$  is a configuration. So, let me write it that way; this means  $A$  is a collection of 6 dots, which remains invariant under cyclic, under the operation of under the action of  $\sigma$ , right. So, which is under cyclic permutation or cyclic rotation whatever the word is, ok.

So, let us just try and look for examples, what does that mean, right?  $A$  must contain some 6 dots. So, let us see, suppose  $A$  contains this red dot, suppose this dot is in  $A$ , ok. Now, what can I say about the other five dots? Well, observe firstly that  $A$  must be invariant under this cyclic rotation; means as soon as I have this this red dot here, this green dot and this yellow dot must both be in  $A$ , ok.

$|A|=6 \Rightarrow A$  is a union of 2 columns  
 $\text{"pr}$

$\therefore X^G = \{ A \subseteq Z \mid A \text{ is a union of } r \text{ cols of } Z \}$

$|X^G| = \binom{4}{2}$  (general:  $|X^G| = \binom{n}{r}$ )

$\Rightarrow G \curvearrowright X$   
 P-OP     ↓ cardinality  
 (pn, pr)

$\& |X^G| = \binom{n}{r}$

FIGURE 6. Refer Slide time 24:55

Why is that? Because if either of them is missing, then when I perform  $\sigma$  on  $A$ ; you will see that the new configuration is not the same as the old configuration, ok. For example, if  $A$  has this this red dot here and suppose it does not have this this green dot, ok. So, imagine this red dot is in  $A$ , but this this green dot is not ok; then what will happen if I perform  $\sigma(A)$  then the new set  $\sigma(A)$  will contain the green dot, ok. But the original set  $A$  does not contain the green dot, ok. So, this property here that this  $A$  must be a collection of dots which is invariant under cyclic rotation; means the following, as soon as  $A$  contains any dot say the red dot, then it must contain the other dots in that column. So, this automatically means this is there, this automatically means this is there, ok. So, all three guys in a column are automatically there, ok. So, we have figured out three elements. Now,  $A$  has six elements, let us look, let us assume some other element belongs to  $A$ . Let us say this dot was in  $A$ , ok. By the same reasoning, if I apply  $\sigma$  to  $A$  to that yellow dot, when I apply  $\sigma$ , it will become the red dot ok; which means since the yellow dot is in  $A$  and  $A$  is invariant here under the cyclic rotation, it means that this red dot must also be in  $A$  and by the same token the green dot must also be in  $A$ , ok.

So, as soon as any dot in any columns is in  $A$ , every other dot in that column is also automatically in  $A$ , ok. In other words, we conclude that  $A$  must be a union of columns in  $Z$ ; you take this grid of dots and you take some columns, take the unions of the full columns, you cannot have partial columns, ok. So, think about this final conclusion little bit and convince yourself by looking at a few examples that this is indeed the case. So, the only way in which  $A$  can be a fixed point is, if it is a union of columns, ok. And observe the reverse inclusion is obvious that, if it is a union of columns; then of course it is invariant under the action of  $\sigma$ , ok.



By f.p. principle: 
$$\binom{pn}{pr} \equiv \binom{n}{r} \pmod{p}$$

$$|X| \equiv |X^G| \pmod{p} .$$



FIGURE 7. Refer Slide time 28:01

Now, what does that mean?  $A$  had six elements remember and if it has six elements; then since the cardinality of  $|A| = 6$  and it is a union of columns.  $A$  must be a union of how many columns? Well, each column has size 3, so it must be a union of 2 columns, ok. So, observe this, this is exactly the number  $r$  that we are talking about, 6 is the number  $pr$ , ok. If you did this in general, each column has  $p$  dots and  $A$  was a subset of cardinality  $pr$ ; that means  $A$  must be a union of  $r$  columns in general ok, in our example it is a union of 2 columns.

So, therefore, what have we concluded? What are the possible elements, what are the elements of the fixed point set? Well, it is all those subsets of  $Z$  such that  $A$  is a union of some 2 columns of the grid, ok; like I said in general  $r$  columns of the grid. Well, what does that mean? How many ways, how many different ways can you choose? So, in general the grid has here for example, the grid has four columns. So, what are all the various possibilities for  $A$ ? It can be a union of the first two columns for example, or it can be the union of this and this or the union of say this column and the third column and so on and so forth, right. So, the number of different ways of choosing 2 columns out of the 4 columns. So, this is as you can see, it is just take the 4 columns that we have and choose any 2 out of them. So, that is going to be the total number of ways of a manufacturing elements  $A$ , which satisfy this this required condition, ok. And again I have demonstrated all this by example; but in general if I did this, in general with  $n$  and  $p$  what we are going to do is, you have  $n$  columns in  $z$  and you have to choose  $r$  columns out of that, ok.

So, just repeat the argument for the general case, ok. So, all this is sort of I mean I am trying not to do this overly formally and so on; just try to give you a visual geometrical idea of what is going on. But finally, I hope you will convince yourself that, we have in fact proved the following that. So, what have we done in the end? We have constructed a set  $X$ , which is acted upon by a  $p$  group which in fact is just a cyclic group here,  $X$  has cardinality.

So, this set has cardinality  $\binom{pn}{pr}$  which is all configurations of  $pr$  points and the cardinality of the fixed point set is exactly  $\binom{n}{r}$ , ok. So, we have managed to manufacture this and so, by finally by the fixed point principle ; what this means is that,  $\binom{pn}{pr}$  that is the cardinality of  $X$  is congruent to the cardinality of the fixed point set which is  $\binom{n}{r}$ , ok.

So, that is sort of the second example and this will sort of come back when we start talking about Sylow's theorem and so on; but until then ah you know just think of this as a nice number theoretic consequence of the fixed point principle .