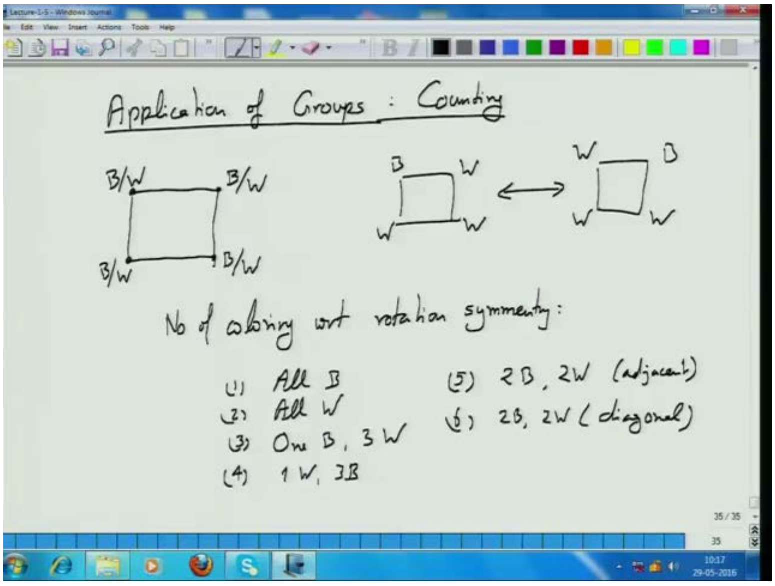
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture – 06
Groups: Applications

Today, I am going to show you one application of groups, and that is when it is very interesting application, clearly simple one also. There are large variety of problems on which groups can be applied, but we will respect our attention to just this one. And we will use groups in developing this abstraction further from the next lecture.

(Refer Slide Time: 00:43)



Application of Groups : Counting

No of coloring wrt rotation symmetry:

(1) All B
(2) All W
(3) One B, 3 W
(4) 1 W, 3B
(5) 2B, 2W (adjacent)
(6) 2B, 2W (diagonal)

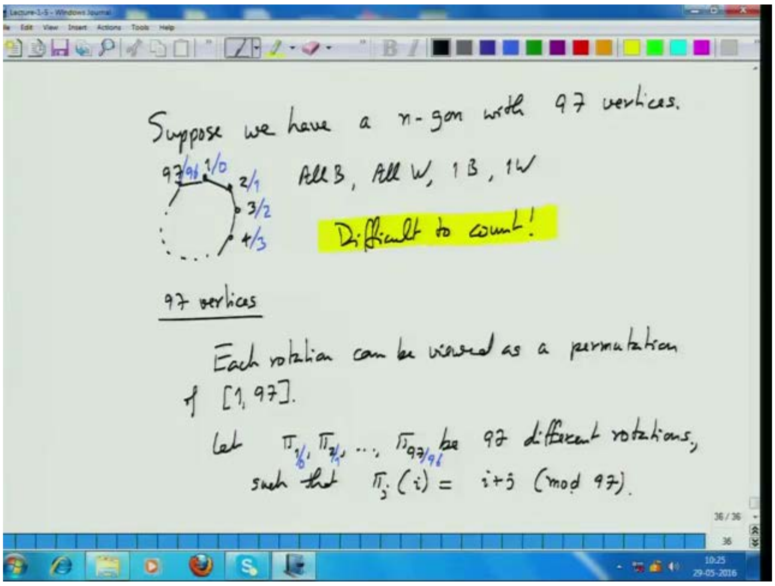
And this application is related to counting. So, let us start with an example. Suppose, we have a square and we want to color the vertices of this square with two colors, let say black or white. How many ways are there to color these vertices with these two colors. But then if you look at it this closely and that is where the complication set in, if there are certain symmetries of coloring.

For example, if you color this black, this white, white, white, and you color this black, and this white, white, white, then these two colorings are essentially the same, because you can rotate this square, and get to the other coloring or vice versa. So, we want to not just color, we also want to know that how many distinct ways are there to color a square in this fashion. And distinctness is counted with respect to this rotation there; if we compare the square I color the vertices I rotate that square, I get another coloring that is the same coloring. Now, how many colorings are possible?

We just count all black or gets number of coloring with respect to rotation symmetry. First is all blacks; another 1 is all white; third-one is 1 black, 3 white; and it does not matter which of this 4 vertices I color as black, because I can rotate it and get any other vertex colored as black and all other 3 as white. So, actually there is just one coloring with respect to rotation symmetries and which we can color vertex with black and all other three as white.

Correspondingly, there is 1 white and 3 black. Then how about 2 whites and 2 blacks, how many colorings are there? 2, right. We can adjacent vertices are black or with diagonal vertices where black, and then all other possible colorings can be extracted by symmetry. Adjacent 2 black, 2 white diagonal. So, we get 6 different colorings and that is it, there are no any other colorings possible. So, there is simple enough.

(Refer Slide Time: 05:11)


Lecture-1-5 - Windows Journal
File Edit View Insert Actions Tools Help
97/96
1/0
2/1
3/2
4/3
36 / 36
36
10:25
29-05-2016

Suppose we have a n-gon with 97 vertices.

All B, All W, 1 B, 1 W

Difficult to count!

97 vertices

Each rotation can be viewed as a permutation of [1, 97].

Let $\pi_{1/0}, \pi_{2/1}, \ldots, \pi_{97/96}$ be 97 different rotations, such that $\pi_j(i) = i+j \pmod{97}$.

But now let us may propose a more difficult for coloring. Let us say suppose we have a n gon with say 97 vertices which is basically similar structure with 97 vertices. Now how many colorings are possible? Same 2 colors - black and white; how do you count, 16? Distinct colorings with respect to this rotational symmetry; we do not want to, so again all black is clearly 1 all white is another, 1 black is another one, 1 white is another one, and then rotationally they are all same.

How about 2 blacks? It will be determined by the gap between the 2 blacks, there will be some number you can count easily. But then 3 blacks, 4 blacks, 27 blacks, now if you have to count 27 blacks, you have to worry about how many what are the gaps between these 27 blacks and with respect to that count is that going to be easy? No, there is not going to easy at all.

Now, by the end of this lecture, we will derive a very convenient way of counting such numbers, have we use groups as I just said. So, how do we use the groups? Well, let us stay with this particular example, although we will generalise it very soon. We have two factors out in the sense the rotational symmetries.

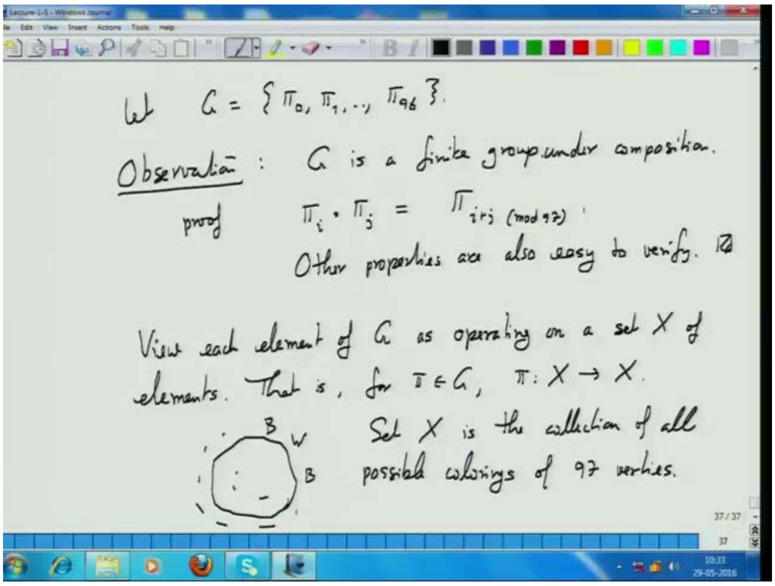
Let us try to represent the rotational symmetries in an abstract way. When I say rotational symmetry, what does it really mean, a rotation is a mapping of or a rotation of by certain number, they are 97 vertices so how many different notations will there be, 97 with different notations, you can take these vertices and keep it to itself that is a trivial rotation. There is no rotation or send it to the first one or second one or third one. Once you fix mapping of a vertex to the other vertex all other are automatically fixed, so therefore 97 notations possible.

Each rotation can be viewed as a permutation of 1 to 97 correct. So, if that is if I start labelling this vertices by numbers, so 1 to 97, each rotation I can represent as sending this number 1 to 97 to a permutation of these numbers and that permutation will be determined by where 1 is mapped to say 1 is mapped 4, then 2 would be mapped to 5, 3 would be mapped to 6, 4 would be mapped to 7 and so on, 97 would be mapped to 2 and so on right, it is very simple.

But this abstraction now allow me to view these rotations as maps, and these are not just maps, collectively these rotations form a group. Such that pi j of any i is i plus j minus 1, I think. So, pi 1 gives does not rotate at all pi 2 shifts by 1 or I can name it any which way, but this is and this when I say this of course, I mean that when I map 97 and add something to this, I will reduce it by taking out that folding back.

For mod 97, I will need to do this numbering slightly differently, I should have number this with 0, is exactly, I should have started with let us say the number not 1, but 0, 1, 2, 3 and up to 96. Then I would say that instead of 1, I will call it pi 0, pi 1, up to pi 96. In that case, I can now say that pi j of I is I plus j mod 97, now it makes sense i plus j minus 1, no, now you have pi 0 we start with, so it is i plus j mod 97.

(Refer Slide Time: 11:51)



Let $G = \{ \pi_0, \pi_1, .., \pi_{96} \}$.

Observation : G is a finite group under composition.

proof $\pi_i \cdot \pi_j = \pi_{i+j \ (\mathrm{mod}\ 97)}$

Other properties are also easy to verify. ☒

View each element of G as operating on a set X of elements. That is, for $\pi \in G$, $\pi : X \to X$.

Set X is the collection of all possible colorings of 97 vertices.

Now this tells means let G be this collection of pi 0, pi 1 to pi 96. This is a finite group under the usual operation, which is works for permutations that is the composition. And this is simple proof pi i compose with pi j equals pi, i means rotate pi i shift by i essentially if pi j shifts by j which is same as pi i plus j mod 97. So, there is a closure property this shows it has associativity trivially, it is not commutative. How does it, it is commutative also in this case it is commutative as well (Refer Time: 13:09), then there is identity which is pi 0, and there is inverse. What is inverse of pi i? 97 minus i or is this 97 minus i; 96 minus i.

Student: (Refer Time: 13:31)

97 minus i plus not plus i plus 1.

Student: pi i and pi 97 minus i.

Yes.

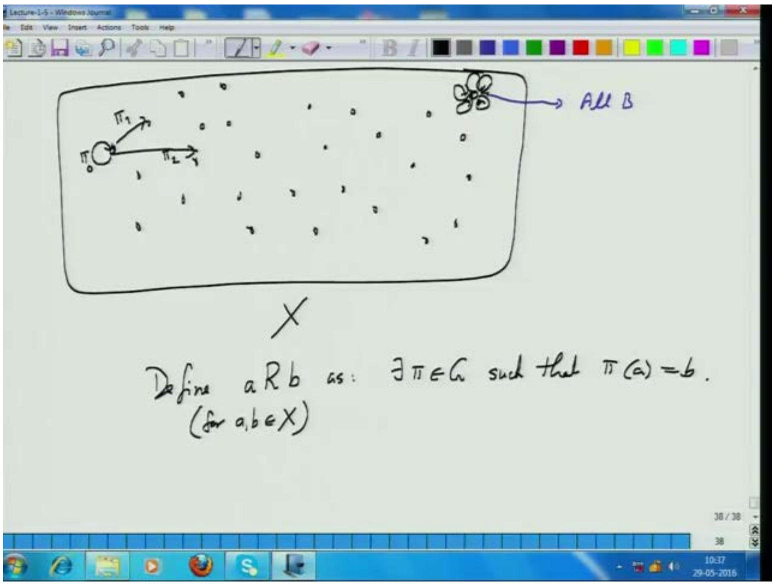
Student: 97 minus i plus i.

So, you get 0 that is right, so 97 pi I is mapped to pi 97 minus i that is sorry the inverse is pi 97 minus i. So, for these reasons, now we are seeing some interesting structure emerging. Now we can apply our knowledge about groups to understand the number of symmetries or adjust number these are we know that these are so many symmetries each group elements here captures a one type of symmetry, and then we can use it to count, requires a little bit of cleverness. So, let me describe that. What is it that this so the we have this group elements, these group elements, each one of them we apply it to a picture like this, and rotate it, so each group that is the we apply to this and we get another such figure that am I making sense here?

So, let me explain (Refer Time: 15:27). So, we have this group of symmetries. These each one of this, I am going to view it as follows. I am going to view each of these elements as operating on a set of elements we call X which is notationally I write it as pi which is in G takes in element of X and produces another element of X. What are these elements? These are the elements which we really want to count. What are the elements you want to count, we have this n gon, 97 gon, we color each vertex, give some coloring to vertices.

How many distinct coloring you just counted this, you write it in the beginning, set X is the collection of all possible colorings of 97 vertices that is 2 to the 97, each vertex can be either black or white, there are 97 vertices. So, there are 2 to the 97, so that is my set X. When I apply a pi in G on one element of this that just rotate it and produces another element of set X. This is an important point or rather important view is not very difficult to understand, where its important view to keep in mind that this symmetry which are pi the rotations, I will view as taking one coloring of this 97 vertices and sending it to another coloring of this 97 vertices. Any question on this, no?

(Refer Slide Time: 18:47)



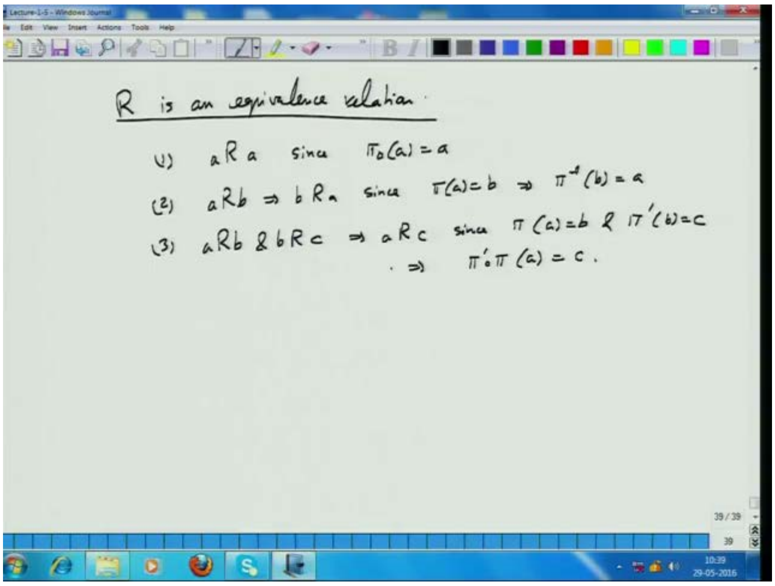
Define aRb as: $\exists \pi \in G$ such that $\pi(a) = b$.
(for $a, b \in X$)

Now, what is rate that I want to count I can re put it across in a very nice way. Let us say here are all the circle, these are all elements of the set X each of the point here represents one coloring of the 97 vertices. Now each coloring, if you look at it, an apply a pi on it, it would be map to another coloring, let say this is map by pi 1 to this, may be by pi 2 to this and so on. Keep in mind that is there are some pi's, which will map this point to itself. For example, pi naught will map an element to itself, it does not change the element, but that is not the only pi that may map an element to itself.

For example, if you look say this element is all black. And you apply pi on it, where does it go to it stays here, no matter which pi apply you just stay here right. So, all pi, so we will just take it keep it to itself. So, this will look different, so for different elements here, we will get different structure that some pi will take it to some other notes some pi will map it to itself. Now let me define, so we create this picture, we keep this picture in mind this is what we have these element, so then we create this arrows corresponding the different pi taking that element or node to another node.

And now let us define a relation. There exist a pi in G, such that pi a equals b, this is for a b in X. So, when 2 nodes a and b in X are related, what does it say about a and b. It says that there is a rotation of a that gives me b fine, and therefore a and b are from this rotational symmetry perspective are the same. So, we do not want to count in our regional counting, we do not want to count a and b separately. We want to count them together a just one element. So, this relation is what we want to enforce on this set, and then count how many distinct unrelated elements are there, so exactly that is what I am driving at but for that we have to first show that R is an equivalence relation and that is easy.

(Refer Slide Time: 22:46)



Lecture-1-5 - Windows Journal
File Edit View Insert Actions Tools Help
39 / 39
10:39
29-05-2016

R is an equivalence relation.

(1) $a R a$ since $\pi_0(a) = a$

(2) $aRb \Rightarrow bRa$ since $\pi(a) = b \Rightarrow \pi^{-1}(b) = a$

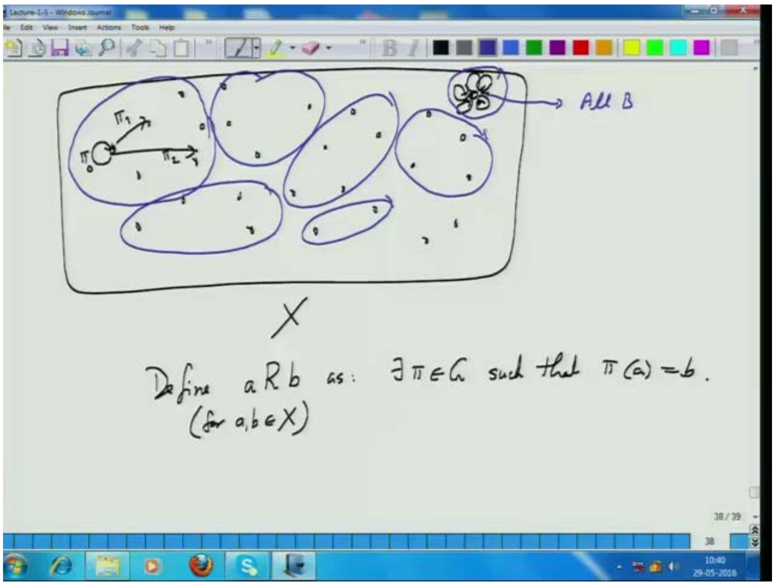
(3) aRb & $bRc \Rightarrow aRc$ since $\pi(a) = b$ & $\pi'(b) = c$

$\Rightarrow \pi' \circ \pi(a) = c$.

Well, firstly a is related to a, pi 0 is a. Second a related to b implies b related to a, since pi a equals b implies pi inverse b equals a. We know that pi 0 belongs to the group G, it is an identity map. We know that if pi is in the group G then pi inverse is also in the group G that we why they group property.

And 3 a related to b, and b related c, implies a related to c, since pi 1 a equals b; and pi 2 a, I do not want to use index 1 and 2, because I used it is slightly differently pi equals b and pi prime b equals c implies pi prime compose with pi a equals c. And pi prime compose pi is again by the closure of the property belongs to the group. So, there is another elements that there. Here another demonstration that there is a close relationship between equivalence relation and group so this group G induces an equivalence relation on these elements.

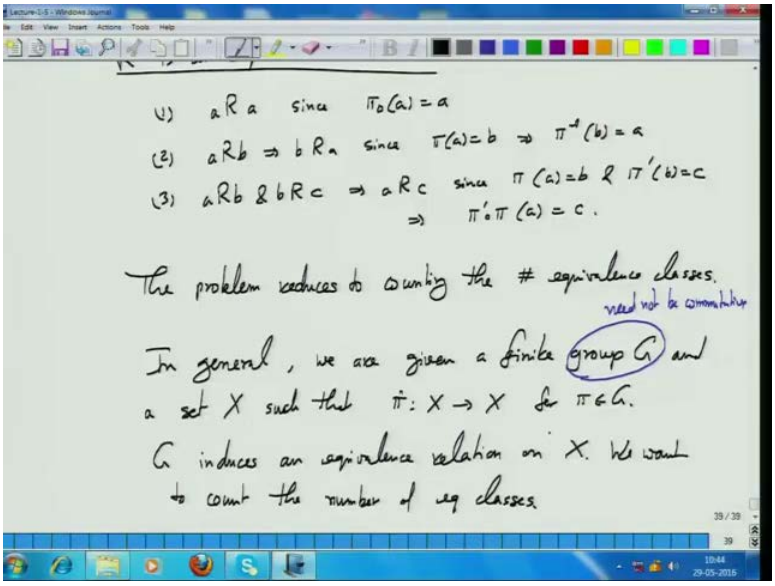
(Refer Slide Time: 24:41)



Define aRb as: $\exists \pi \in G$ such that $\pi(a) = b$.
(for $a, b \in X$)

So, now the picture looks much nicer, because now we have that there are equivalence classes there with respect to this relation. By the way, this is an equivalence class of its own, this all blacks, because every element in G takes it to itself, so this is a solitary equivalence class.

(Refer Slide Time: 25:15)



(1) aRa since $\pi_0(a) = a$

(2) $aRb \Rightarrow bRa$ since $\pi(a) = b \Rightarrow \pi^{-1}(b) = a$

(3) aRb & $bRc \Rightarrow aRc$ since $\pi(a) = b$ & $\pi'(b) = c$

$\Rightarrow \pi' \circ \pi(a) = c$.

The problem reduces to counting the # equivalence classes.

need not be commutative

In general, we are given a finite group G and a set X such that $\dot{\pi} : X \to X$ for $\pi \in G$.

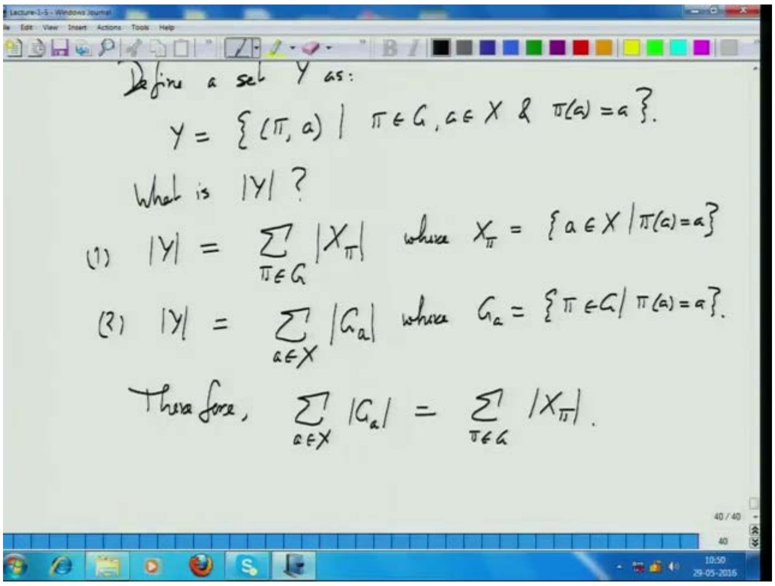
G induces an equivalence relation on X. We want to count the number of eq classes.

And, now the problem is the number of equivalence classes each equivalence class gives me one distinct element, because a element of an equivalence class can be transformed to each other via this rotations. So, we just need to count, how many distinct equivalent classes are there that will give me exactly the number of different colors.

Are you with me so far? There is a slight problem because equivalence classes, where define equivalence classes, we will have different number of elements you saw example here is an equivalence class that are just one element in it, whereas some other equivalence class, we will have many more. So, we have to do a slightly careful counting, you cannot count very easily. So, how do we count well, here is a trick we use.

So, in general, we are given a finite group G and a set X such that pi is a mapping X to X for pi and G, then G induces we just saw an equivalence relation on X and we want to count the number of equivalence classes. So, now, let I am removing this connection with this rotation group take I am saying take any finite group and. In fact, this group need not even be commutative could be any group we are given a finite group and a collection of elements X so that every elements of every elements of finite group maps elements of X to X this induces an equivalence relation on X and then you want to got the number of equivalence classes.

(Refer Slide Time: 28:25)


Lecture-1-5 - Windows Journal
File Edit View Insert Actions Tools Help
40 / 40
10:50
29-05-2016

Define a set Y as:

$$Y = \{ (\pi, a) \mid \pi \in G, a \in X \ \& \ \pi(a) = a \}.$$

What is $|Y|$?

(1) $|Y| = \sum_{\pi \in G} |X_\pi|$ where $X_\pi = \{a \in X \mid \pi(a) = a\}$

(2) $|Y| = \sum_{a \in X} |G_a|$ where $G_a = \{\pi \in G \mid \pi(a) = a\}$.

Therefore, $\sum_{a \in X} |G_a| = \sum_{\pi \in G} |X_\pi|$.

How do we do that for that define a set Y as pi Y is a set of pairs, one component of a pair is pi and G, and second component to the pair is a and X. And pi a pair belongs to the set Y, if pi of a is a; that means, this elements pi of the group G does not disturb a. It keep since a to itself; pi need not be identity, pi could be mapping some other element to a third element that is possible, but it just so happens that it keeps the element a to itself.

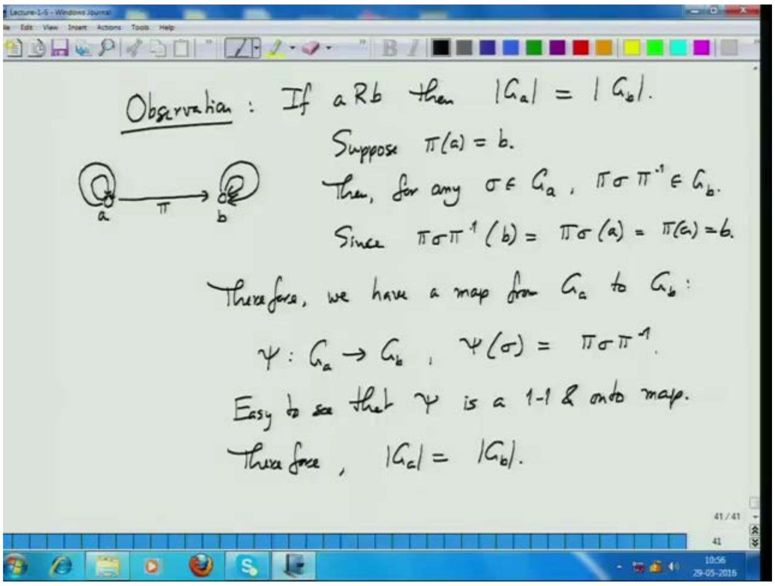
What is a size of Y, well, I will write it in two ways. Size of Y, first way I will write it as it is sum over pi in G X pi, where X pi is set of elements a in X, so that pi a sends to a too itself. This is trivial to observe so I am doing something special here, I am just saying that (Refer Time: 30:25) a pi contains a pairs pi sorry Y contains a pair pi and a, for all pi and always that is find this equation, you just split that and write it as sum over all pi's in G and X pi where X pi is all the elements a and X, so that pi is in.

So, this set Y, I am dividing it into subsets one corresponding to each pi, and then summing over oops sorry size of X not a size. The other way I will write size of Y as sum over a and X we can guess G a so that is a other split you fix one for each a and X, you just count again this is a size, count the number of pi's that map to itself so that is a slightly different split of Y. Now as splitting Y in subsets, one for each a in X and then counting how many pi's map that a to itself, and clearly both or though is summations give me the same number which is size of Y.

Therefore, we can write equality between these two sums, pretty straight-forward so far, but the cleverness here is already used which is to define this set Y and count it into two different ways. Once we said this equation enough, the rest is pretty straight-forward, keep in mind the final target. What is the final target, I want to count the number of equivalence classes. Let us focus on this sum.

This sum I am going to write slightly differently and for that let us go back to the picture. Keep this sum in mind, what is the sum, this is sum of for every element a of X the number of mappings or number of pi's of G that keep a to itself. If you go back to this picture, what we are talking about is how many here is an element a, how many of G's map, how many of pi's map, this element to itself, so that is how many arrows are in this picture going from this element to itself that is G a. If this element is a, G a is in this picture the number of arrows that send a to itself, correct. Feel free to stop me and ask a question for clarification.

(Refer Slide Time: 34:03)


Lecture-1-5 - Windows Journal
File Edit View Insert Actions Tools Help
a
π
b
41 / 41
10:56
29-05-2016

Observation: If $a R b$ then $|G_a| = |G_b|$.

Suppose $\pi(a) = b$.

Then, for any $\sigma \in G_a$, $\pi \sigma \pi^{-1} \in G_b$.

Since $\pi \sigma \pi^{-1}(b) = \pi \sigma(a) = \pi(a) = b$.

Therefore, we have a map from G_a to G_b:

$\psi : G_a \to G_b$, $\psi(\sigma) = \pi \sigma \pi^{-1}$.

Easy to see that ψ is a 1-1 & onto map.

Therefore, $|G_a| = |G_b|$.

Now, I will just make one final observation, and then we are done. If a is related to b, then size of G a is same as size of G b that means, if I draw a sub picture of that picture say this is a, and this is b, a is related to b, so that mean there is a pi that maps a to b. And now I want to see my target is see how many self loops are there in this picture, which are arrows which send a to itself. Similarly, I want to count how many self loops are there on b and I want to related these pronouns and the relationship is that the numbers are the same. Why, well, let us prove this. Suppose, pi a equals b, then for any sigma in G a take a map which send a to itself, and I am going to transform this map into a map that is map b to itself. How do I transform it?

Student: Composition with pi.

Composition with pi and that would be sufficient. I want to go pi sigma pi inverse is in G b. Why, just this is another map in the set rather group G. What happens when you apply this map on b, apply on b, pi inverse will take b to a, then sigma will take a to itself and that pi will take a to b. Since pi sigma pi inverse of b is pi sigma of a, which is pi of a, which is b. So, we have established a mapping from G a to G b therefore, we have a map from G a to G b and that (Refer Time: 37:03) give it a name plus call it psi.

Student: (Refer Time: 37:25).

Yes.

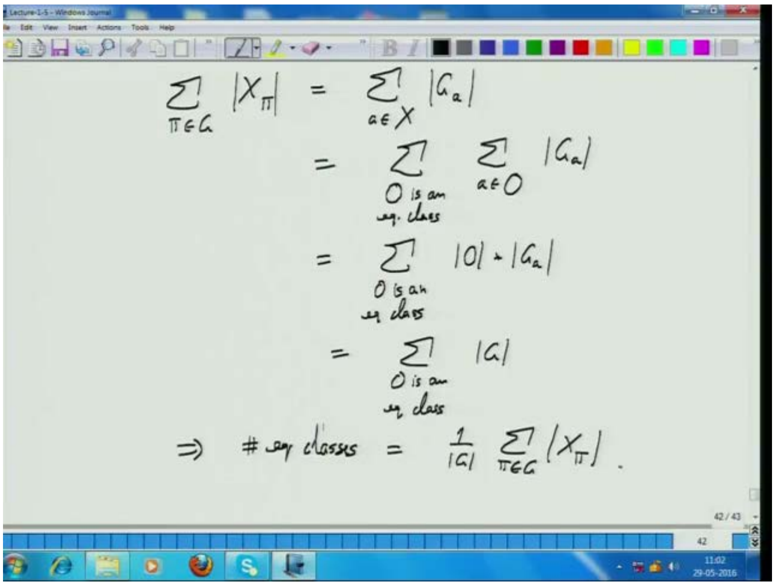
Student: (Refer Time: 37:29).

Colors, the relative position the colors are the same, you are right?

Student: (Refer Time: 37:39).

The same thing give a very right that is an intuition, and I am just putting their intuition in formal symbols that is all otherwise there is nothing very special happening here. You can see I think instead of you know giving further details, I think is easy to see that psi is a 1 to 1 and on to map. Therefore, size of G a is same as size of G b, psi maps G a to G b is a 1 to 1 and on to map, both are finite sets to their size are the same. And once we have the same sizes I am done just we will let us go back to this.

(Refer Slide Time: 38:35)


Lecture-1-5 - Windows Journal
File Edit View Insert Actions Tools Help
42 / 43
42
11:02
29-05-2016

$$\sum_{\pi \in G} |X_\pi| = \sum_{a \in X} |G_a|$$

$$= \sum_{O \text{ is an eq. class}} \sum_{a \in O} |G_a|$$

$$= \sum_{O \text{ is an eq class}} |O| \cdot |G_a|$$

$$= \sum_{O \text{ is an eq class}} |G|$$

$$\Rightarrow \# \text{ eq classes} = \frac{1}{|G|} \sum_{\pi \in G} |X_\pi| .$$

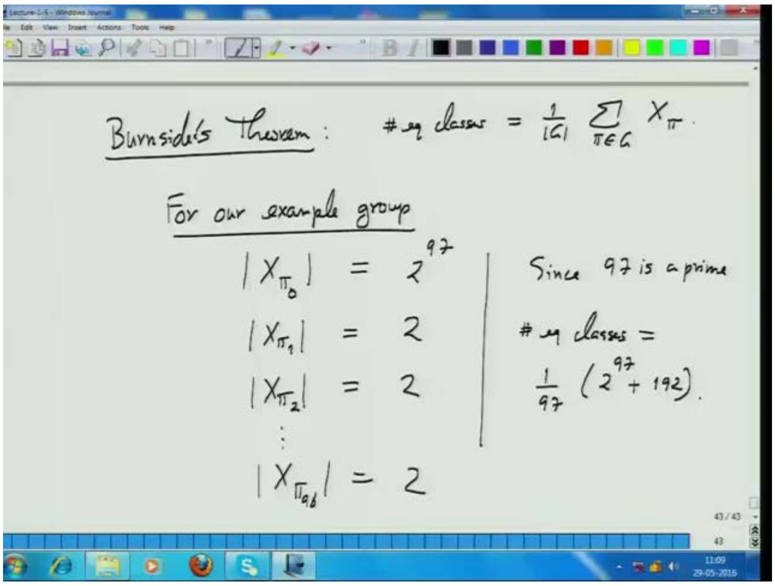
Let us we write this as splitting this further into equivalence classes. So, O is an equivalence class summation a, is in O size of G. So, I am writing this sum and splitting it. First, I am going over all equivalence classes and then next I am going over all elements within the equivalence class, so in the inner sum size of G a is the same for every element, so this is I can write as size of O times size of G.

Now, what is size of O times size of G a. Go back to this picture, here is an equivalence class size of G a, is all pi is that map a to itself that is the number of pi. How many elements are there in all in the equivalence class that number we do not know, but what we now is that if we take any pi in G, it will send keep either a to itself or send a to some other elements in the equivalence class.

And so the there are size of G different elements in G. Each one of those elements corresponds to one arrow in this equivalence class; and size of G a times size of O, this is a equivalence class O is exactly equal to number of arrows in this equivalence class, why is that. This I am going to saying is O is an equivalence class size of G. To prove this, I will just appeal to you to think about the last lecture or the even the lecture before and observe the following.

G is a group, first observation is a G a is a sub group of G. And we then when we quotient G with G a, you get equivalence classes, each of this equivalence class corresponds to one elements here. There is this is a G a, these are G a's here as the sub group then there is a other group. If you look at G, and quotient it with G a, you will get exactly the number of distinct elements in an equivalence class. I leave you to proof this, it is not difficult just need to observe that. And now I have number of equivalence class just look at this, this sum is running over all equivalence classes; and inside the sum, we all have the same number which is size of G. So, number of equivalence classes is precisely 1 over size of G times the sum.

(Refer Slide Time: 42:54)



Lecture-1-5 - Windows Journal
File Edit View Insert Actions Tools Help
43 / 43
43
11:09
29-05-2016

Burnside's Theorem : # eq classes $= \frac{1}{|G|} \sum_{\pi \in G} X_\pi$.

For our example group

$|X_{\pi_0}| = 2^{97}$

$|X_{\pi_1}| = 2$

$|X_{\pi_2}| = 2$

$\vdots$

$|X_{\pi_{96}}| = 2$

Since 97 is a prime

eq classes $=$

$\frac{1}{97}(2^{97} + 192)$.

What we just proved is call Burnside’s theorem that number of equivalence classes equals 1 over size of G times sum over pi in G X pi. This theorem is applicable in general for all groups and all X’s where G operates all though X’s here finite groups. Of course and it is a very useful tool in counting, why? let us get back to our original example of 97 vertices. How many pi’s are there? 97 in the group G, there are 97 X. Let us count X pi for each one of them. What is the X pi 0 size of this? Pi 0 maps an element to it each node to itself, there are 97 nodes in that figure each pi maps each node to itself. So, how many distinct colorings are there, how many colorings are there which are preserved by pi 0, all what is all what is that number?

Student: All 97.

All 97; how about X pi 1, X pi 1, pi 1 sends one vertex to the X 1 and then next, next, next, next. How many colorings would be preserved by pi? Is the first vertex vertex number zero as say color black, pi 1 will map 0 to 1 in order for that colors to be preserved one also must have colored black; one is goes to 2, the 2 also must have the color black, 2 goes to 3, so all of them must have the color black or all white, so that just 2. How about X pi 2, here 0 goes to 2; 1 goes to 3. So, 0 and 2 must have same color, 1 and 3 must have same color. So, 0 2, 2 goes to 4, 0, 2, 4, 6, 8 - this even number must have the same color; 1, 3, 5, 7, 9 - odd number must have the same color create counted mod 97.

So the next observation is there it will one, when you start moving from 0, 0 to 4, 8 when you come to 98, that is just as one, sorry?

Student: (Refer Time: 46:44).

And then.

Student: (Refer Time: 46:47).

No, see it would I am claiming there it is all white or all black only, because 0 suppose 0 is black, then 2 must be black, 4 must be black, 6 must be black and so on 94 must be black 96 must be black, 98 must be black 98 is 1. 1, if 1 is black then 3 must be black, then 5 must be black, 7 must be black, so all we have gone through; sorry?

Student: (Refer Time: 47:16)

So mod of 97 the question is yeah how many can you cover all the elements so this is also two. And in fact, all of them are 2, and this falls out of the fact there since 97 is a prime number. In case 97 was not prime, suppose we had in 9, then there should be different because 0, 3, 6, 9, 0 that would be one.

Student: That is what I was saying.

That is what you are saying, OK perfect, so that I did not understand that and that is it. We have now our count so the number equivalence classes is 1 by size of G which is 97, and this sum inside is how much 2 power 97 plus 2 times 96 that is 192. So, therefore, we have an exact count of the number of equivalence classes.

Student: (Refer Time: 48:43)

Yes, number of elements, sorry number of elements in G; if the G as a large number of elements, then you have more difficulty in counting.

Student: (Refer Time: 49:01).

Then you would have to do a little more involve counting, but that still would not be it will depend on number of factorization of would that number is. The key game here is that this count is now one for each elements of G, G will typically which is set of symmetry, we will have a small number of elements. So, you can do this counting much more easily compare to earlier where we looking at all possible ways that is we will took.

So, we have done with the groups and I will mail you the assignment also the second one on groups today, and (Refer Time: 49:44) submission deadline.