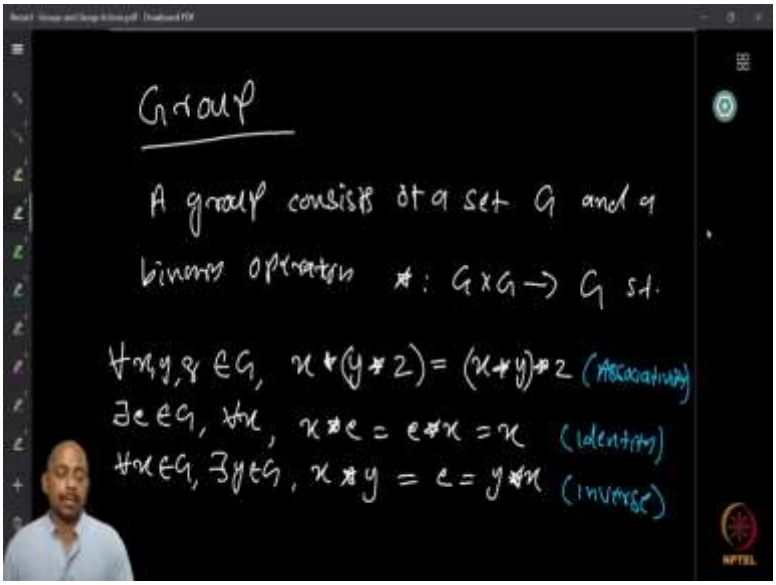
**Combinatorics**
**Professor Doctor Narayanan N**
**Department of Mathematics**
**Indian Institute of Technology, Madras**
**Lecture 46**
**Introduction to Group Actions**

(Refer Slide Time: 00:30)



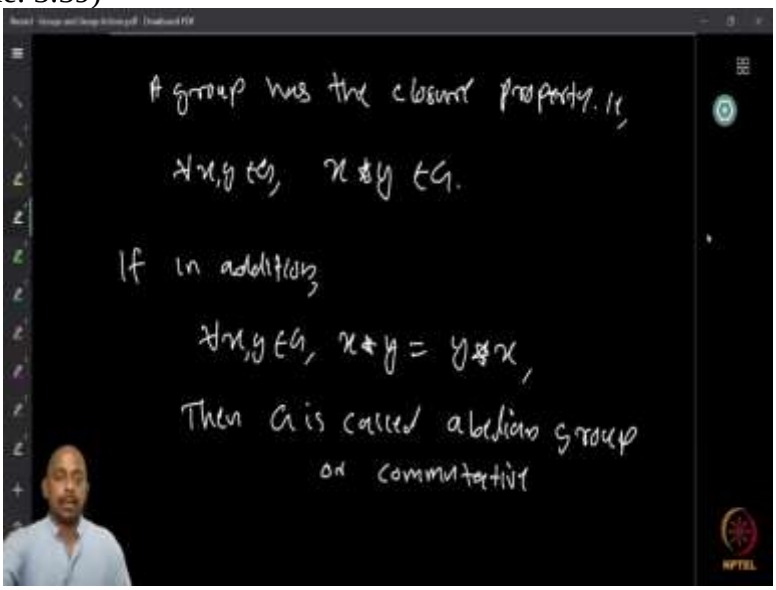

Now, I will give a very short introduction to groups and group actions, which we will need when we are discussing Polya's theory counting. Most of you must be familiar with groups and in case not, here is a very short introduction about it. So, a group is basically a set with a binary operation like addition or multiplication, such that, the set is closed under this operation. So, all the pair of elements under this operation gives rise to elements in the same set and it satisfies the properties like associativity and it must have an identity element with respect to the operation and every element has an inverse.

So, if these properties are true, then the set together of this operation, the binary operation is called a group. So, what is the associativity like for any three elements in the set G, here if star is the operation, x *( y * z). So, you take the operation y * z, the element corresponding to that and then with respect to x and y * z , you do the operation again. What you get must be the same element as you first do x * y and then take star with z. So, this is the associativity.

Then you have the identity element that, if you apply star with this identity e, and then x * e = e * x = x, for every x and for the identity element e. So, you should have such an identity element and then that if you take any element in the group G, then you can find an element which is called the inverse where if x is the element and y is an inverse of x, if x * y = e = y * x. So, any element commutes with the identity element. These are called the group axioms. So,

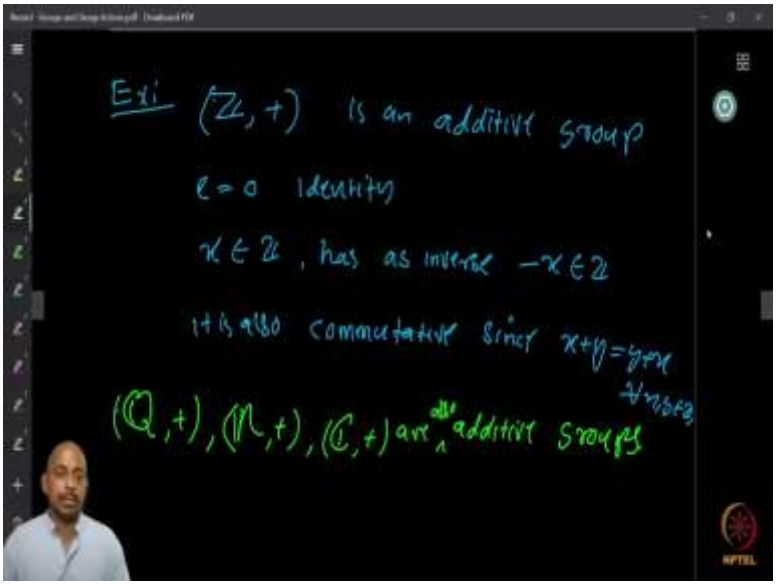
if all these three properties are true, then the set is a group with respect to the binary operation. Now, several examples of group occur naturally, in fact, all these ideas actually come from everyday mathematical objects like natural numbers or integers and all we are considering.

(Refer Slide Time: 3:39)




So, this idea comes from the usual mathematics that we do. So, we can find several examples, so we will see some of them soon. So, I mentioned this before, that the group has closure the property; that any two elements, if you take the operation *, x * y also is an in element in the group. Now, if any two elements have this commutativity that is, if x * y = y* x, then the group is called abelian or it is a commutative group.

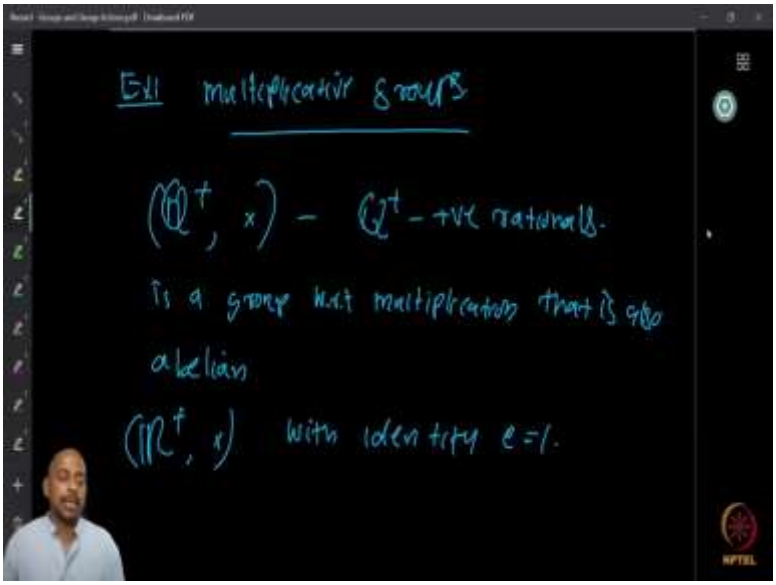
(Refer Slide Time: 4:18)




So, as I mentioned ℤ, the set of all integers with respect to addition is a group, so we call it an additive group, where 0 is the identity element. If I take any integer and then add 0 to it, it does

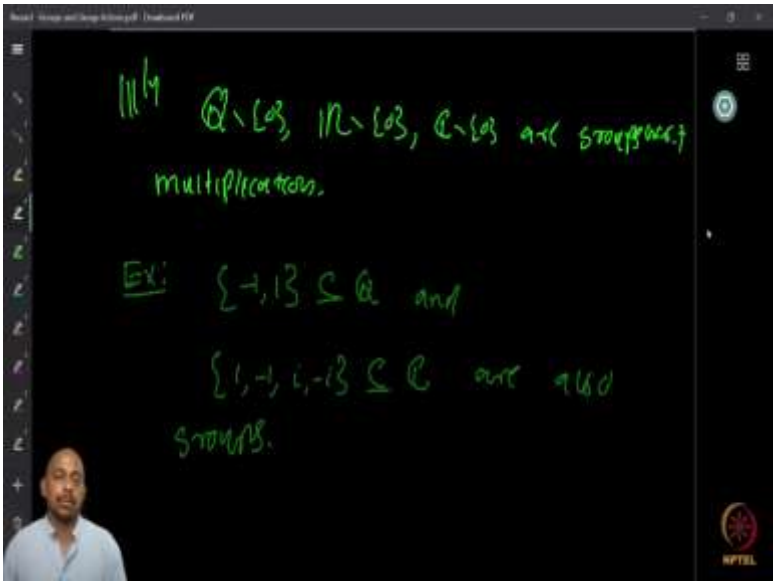
not change the value and you can add a number with 0 or 0 with the number, you will still get the number that you started. Then you have for any number it is negative, is the inverse. And it is also commutative because x + y = y + x for any two elements. And other examples that occur naturally are the set of rational numbers, set of real numbers with respect to addition. Set of complex numbers, all these are additive groups. So, we have several natural examples.

(Refer Slide Time: 5:19)




Then there are multiplicative groups, because the binary operation can be multiplication instead. So, if you take the non-zero rational numbers or positive rational numbers, it forms a group with respect to multiplication, where 1 is the identity. It is a group with respect to multiplication and it is also abelian again, you know multiplication in our natural settings are all usually commutative. Then you have the positive real numbers with respect to multiplication. Similarly, if you take all these $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc and look at just the non-zero elements, that also forms multiplicative groups.

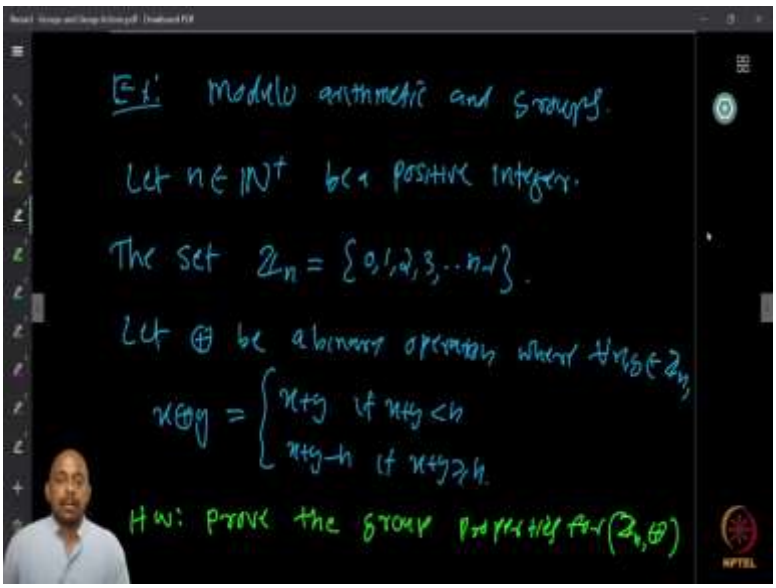
(Refer Slide Time: 6:12)




So, $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, and $\mathbb{C}\setminus\{0\}$ are all groups under multiplication. Now, other than this we have finite groups. For example {-1, 1}. They form a group with respect to multiplication and because any 2 elements if you multiply, it belongs to the set itself.

Every element has a multiplicative inverse which is itself and then you have the identity element which is 1, also you have this associativity. Then you have {1, -1, i, -i} this also is a subset of $\mathbb{C}$ because i and -i are complex numbers. This is also an example of a multiplicative group, so we can verify all these things. So, I insist if you are not familiar with groups, you should work out this, try to verify each of them, is actually a group with respect to the operation that we are discussing.

(Refer Slide Time: 7:29)



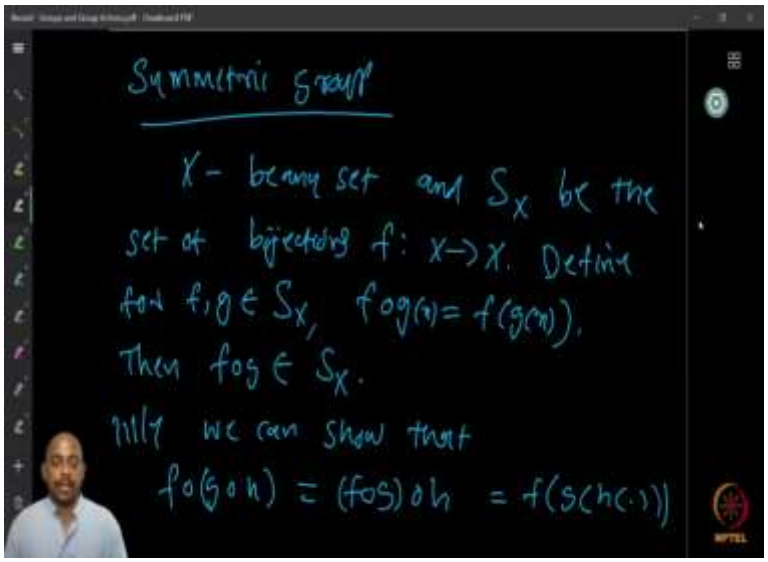
Then another example is the numbers under modularity, positive natural numbers if you take any positive natural number n, then you can look at the numbers {0, 1, 2, …, n – 1} and this set, we usually denote by $\mathbb{Z}_n$, is the group with modulo of arithmetic where we are looking at the modulo n arithmetic.

So, if, I take x and y then x * y is x + y mod n. That is you look at the remainder when divided by n that is what this is. Let $\oplus$ be a binary operation. For all x, y $\in \mathbb{Z}_n$

$$x \oplus y = \begin{cases} x + y, & If\ x + y < n \\ x + y - n, & If\ x + y \geq n \end{cases}$$

And one can show that this is actually the modulo arithmetic. So, now prove that the group property is all satisfied for $Z_n$ and this you should take as a homework and then do it, one can show this easily.

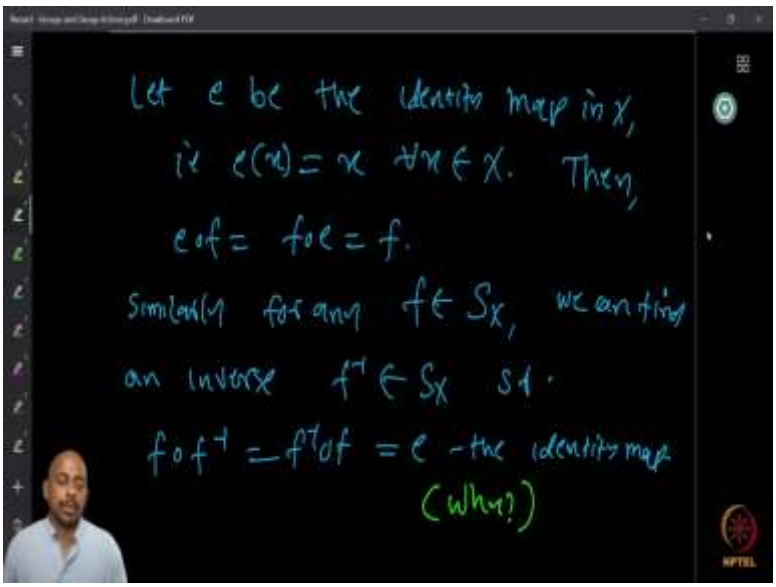
(Refer Slide Time: 9:03)




Now, a very important group that we will come across many times in the next few lectures is the symmetric group. So, symmetric group is the set of all permutations of a set X. So take any set look at all possible permutations of the set then this forms the group of symmetries or symmetric group. So, why is it called symmetric group is because if you take for example combinatorial objects which also have some geometric representations like polygons or high-dimensional polytope or things like that, you can define certain symmetries of this. For example, symmetry under rotation, symmetry under reflection and this kind of things and all these symmetries can be represented in terms of permutations of the vertices or phrases.

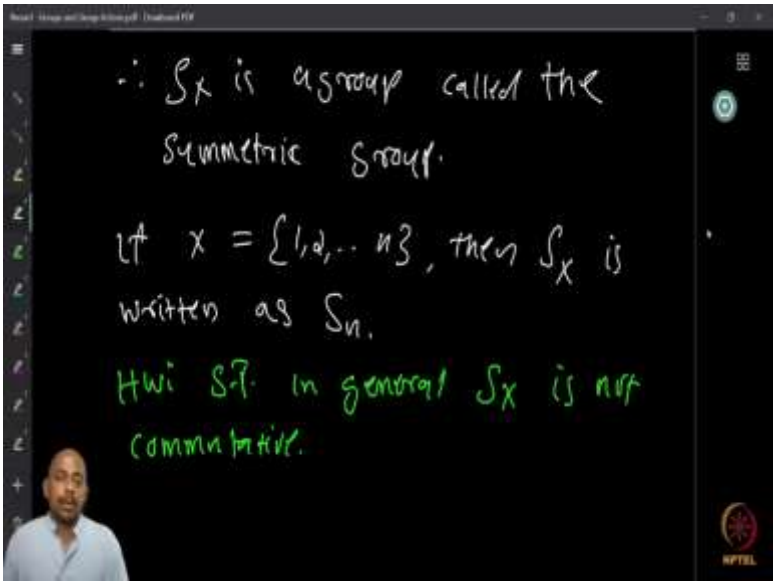
And therefore, one can see permutations themselves as a kind of symmetry and it just depends on what we want to consider as a symmetry or not and therefore set of all permutations is called the symmetric group. So, if you take any set X and then $S_X$ is called set for bijection from X to X which are the permutations and we define for any two permutations in $S_X$, the composition, f ∘ g (x) = f(g(x)). So, g(x) is basically the map of x under the permutation g, then f(g(x)) is the map of g(x) under the permutation f. So, therefore one can show that f ∘ g is also a permutation, one can show this, you can take it as an exercise if you want and similarly one can show that, this composition is basically associative also.

(Refer Slide Time: 11:22)



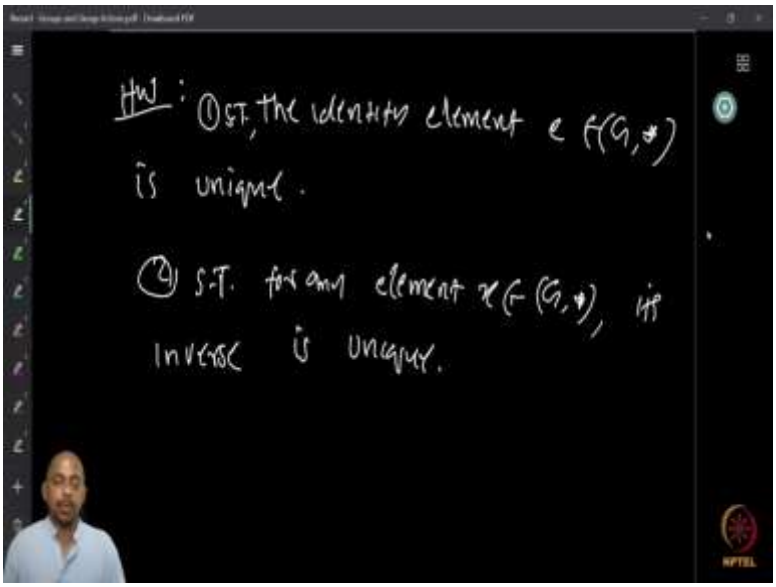

Now, if e is the identity map, right? Because any element is mapped to itself is the identity then e is an identity for the symmetric group also. So, one can show this by taking e ∘ f = f ∘ e = f. It is again trivial to verify immediate. Then we have inverse. If you take any permutation then you can also find the inverse permutation, so that the composition gives you the identity permutation. And again, I know that the inverse permutation will give you identity permutation when you composite with the f that you started with and one can verify this. I request you to go through this and then verify this to be the case.

(Refer Slide Time: 12:23)




Now, as we mentioned $S_X$ is called a symmetric group. Now, if X is a finite set let us say {1, 2, … n}, then $S_X$ is usually written as $S_n$, and this is the n is symmetric group. Then show that as a homework in general, $S_X$ is not a commutative. So, you know because most of the natural examples that we saw earlier were all commutative, now let us look at some group which need not be commutative. This $S_X$, the symmetric group, the set of all permutations of a set, need not be commutative.

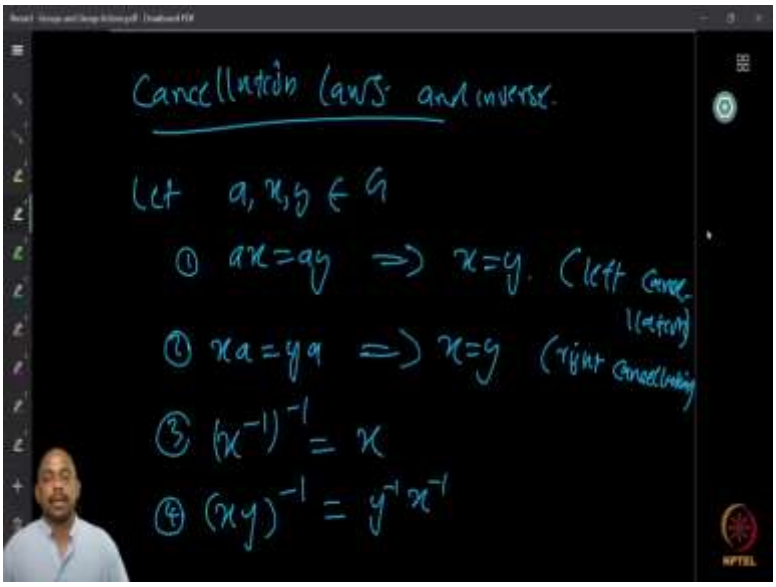
(Refer Slide Time: 13:12)




Then as homework you can show that the identity element is unique in the group, again this is quite lazy exercises. Then for any element, its inverse is also unique. So, the group has these

two properties that it has inverse of an element and there is an identity element so that these are unique.

(Refer Slide Time: 13:45)




Then once you show this, you can show the cancellation laws. So the cancellation laws are the following. Let us say a, x, y are elements of the group G, then

(1) $ax = ay \Rightarrow x = y$, which means that we have the left cancellation law. If the left side of an identity where you have a multiplication by the same element on the left, then you can cancel that.

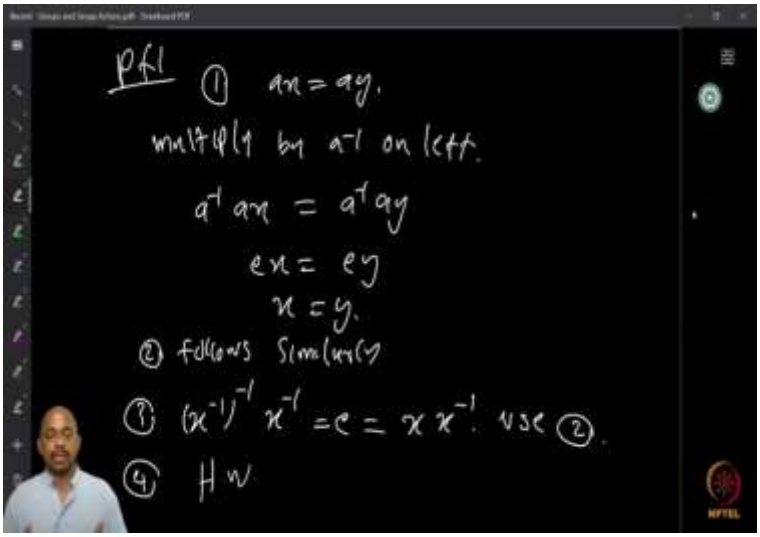
(2) $xa = ya \Rightarrow x = y$, again the right cancellation law.

(3) $(x^{-1})^{-1} = x$

(4) $(xy)^{-1} = y^{-1}x^{-1}$

This all holds for our arbitrary group. If the group is commutative because xy = yx so you can write it differently but otherwise we have this, true for everything.

(Refer Slide Time: 14:53)




Now, the proofs are again very simple,

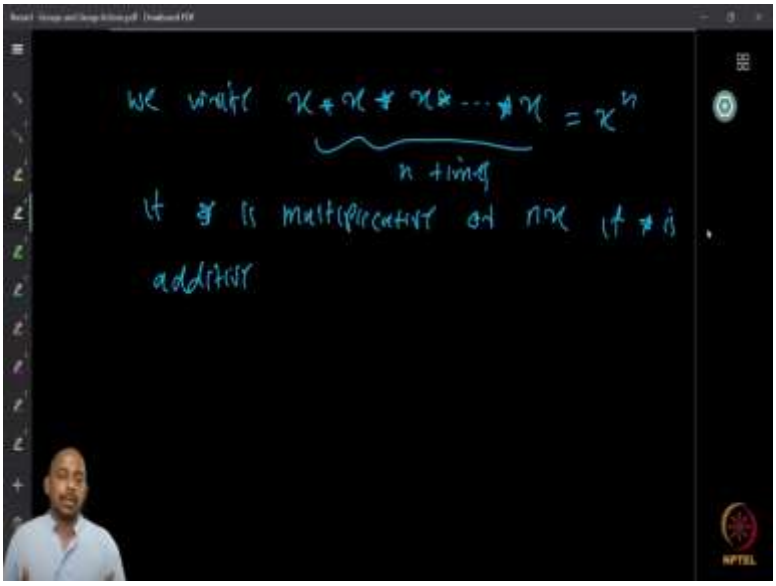
(1) $ax = ay$

multiply by $a^{-1}$ on the left, we get $a^{-1}ax = a^{-1}ay$ .

Since $a^{-1}a = e$, we get $ex = ey$. Therefor $x = y$.

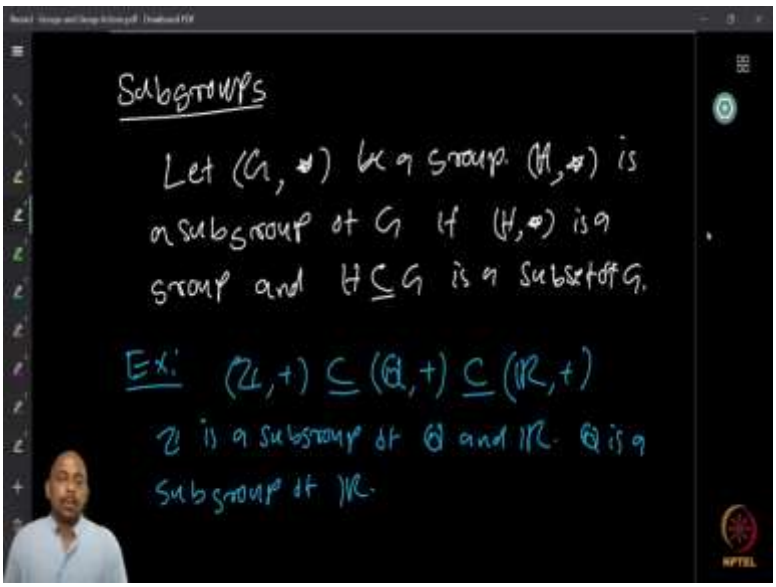
And similarly, (2) follows, from the right cancellation also. And if you want to show $(x^{-1})^{-1} = x$ , what you do is you take $(x^{-1})^{-1}$ and multiply with $x^{-1}$ on the right. Then by definition it is the identity also $xx^{-1} = e$. So $(x^{-1})^{-1} = e = xx^{-1}$. Since $x^{-1}$ is on the right side of both so right cancellation gives you $(x^{-1})^{-1} = x$ ,. Similarly, you can show the fourth one also, I leave it as a homework to do.

(Refer Slide Time: 15:57)



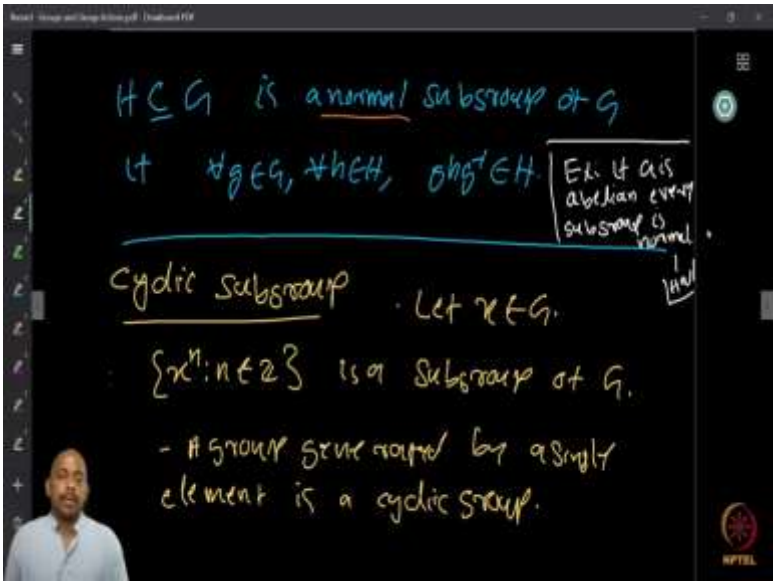
Now, when you have an element, you multiplied it with itself several times let us say. Then, we write it as $x^n$, if the group is multiplicative. And if the operation * is additive operation, then we can also write it as $nx$. In rare cases, one also writes group using the multiplicative notation, the additive groups also. Sometimes it is easier to discuss both cases, in that case one can use the multiplicative notation for the additive groups as well but we will not worry about that, we will not go into that, I think at the moment. But in this case, we can just say that, if * is multiplicative then n times $x * x * \ldots$ is written as $x^n$ and if it is additive then you write it as $nx$. This is the natural way to say this.

(Refer Slide Time: 17:11)




Now, a subgroup of a group. So given a group G and subset let us say H of G, we say that H with respect to the same operation * is a sub group of G, if H with respect * is a group by itself. So if $H \subseteq G$ and (H, *) is a group by itself, then we say H is a sub group of G. Examples are, $(\mathbb{Z}, +)$, so the integers with the addition is contained in the rational numbers with addition and we know that it is the same rules of addition that we use and in $\mathbb{Q}$, we see that set $\mathbb{Z}$ is just a subset with the same addition becomes a group by itself. Therefore, it is a sub group of ($\mathbb{Q}$, +). Now, ($\mathbb{Q}$, +) is sitting inside ($\mathbb{R}$, +) because again real numbers with respect to addition contains rational numbers with respect to addition. Then $\mathbb{Z}$ is a subgroup of both $\mathbb{Q}$ as well as $\mathbb{R}$. And $\mathbb{Q}$ is a subgroup of $\mathbb{R}$.

(Refer Slide Time: 18:38)



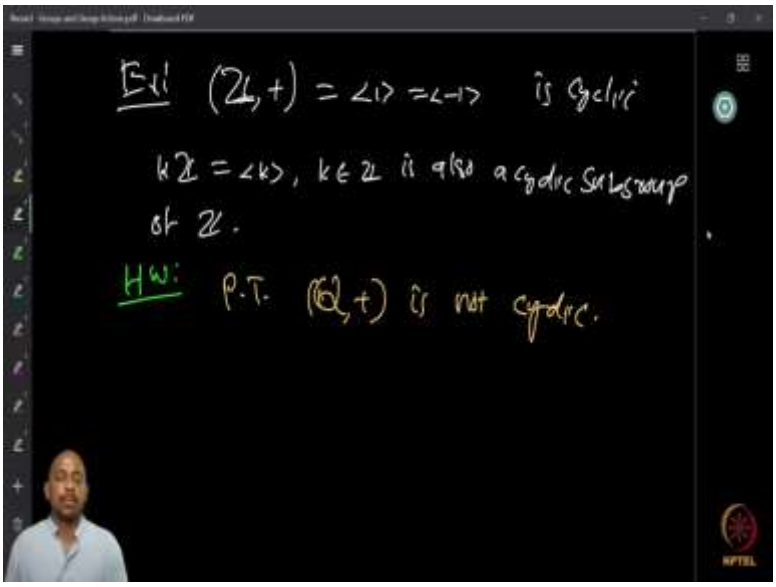

A subgroup is said to be normal, we probably will not need too much of knowledge in this course, but just for completion we just mentioned this. The subgroup is normal, if for every group element of g of G and then very element of h of H, $ghg^{-1}$ is an element of H. Now, if you look abelian group, one can show that sub group if abelian groups are all normal subgroups. You can take it as a homework and show, why it should be the case, if G is abelian, then every sub group of G is a normal subgroup. That will give you several examples as well, so work on this and try to come up with some good examples. Now, given a group G, you can take an element and then as we did before, we can take the powers of this element. Again multiply with itself or add with itself, either way and you can do this several times, then you look at these $x^n$ for every $n \in \mathbb{Z}$.

So, $\{x^n : n \in \mathbb{Z}\}$ is a subgroup of G. If you take an element and multiply with itself or look at the powers, whenever n = 0, for example, you will get the identity and whenever any other numbers you will get the numbers in the group itself and this forms a subgroup because it is always staying inside. One can see that this is a group by itself because, for any number you can find an inverse because if I take $x^n$, $x^{-n}$ is an inverse, because, $x^n x^{-n} = x^0 = e$.

This you can verify and then, if you have a subgroup which is generated by the single element it is called a cyclic subgroup. Now, any group which is generated by a single element is called a cyclic group and therefore such an example shows that every group has a cyclic subgroup. Because you take any element multiply with itself, find $x^n$ for every n, you will get the

subgroup which is cyclic. And $x^{-n}$ can be defined by taking as inverse of a $x^n$. To identity, if you look that is exactly what you are going to get, $x^0 = e$ and therefore you can show this.

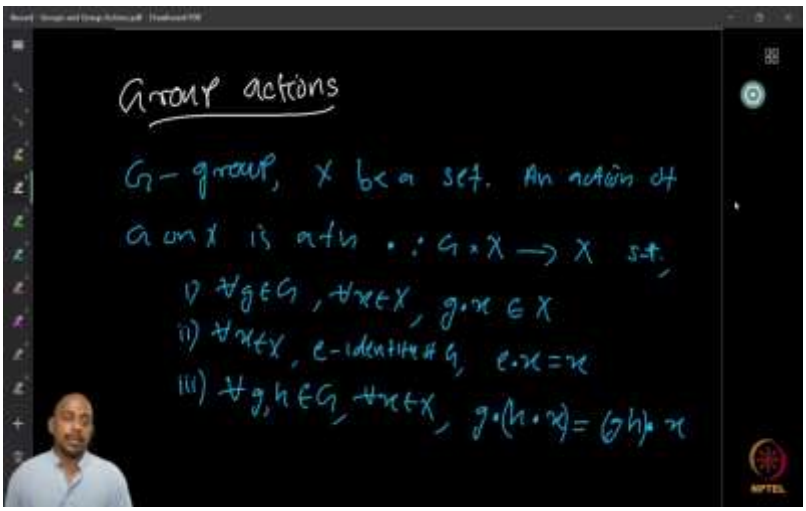
(Refer Slide Time: 22:25)




Then another concrete example is $(\mathbb{Z}, +)$ is generated by 1. $\mathbb{Z}$ is also generated by the single element -1. Therefore, $(\mathbb{Z}, +) = < 1 > = < -1 >$

Now $k\mathbb{Z}$ for any k is a cyclic subgroup of $\mathbb{Z}$. Because when you have k larger than 1, then $k\mathbb{Z}$ will only give multiples of k and this forms an additive subgroup which is also cyclic because you can see that $k\mathbb{Z}$ is generated entirely by k and if you add any of two of them, you will get again an element of the type $k\mathbb{Z}$. So, one can show all these things and then show that $(\mathbb{Q}, +)$ is not cyclic, this is another nice exercise.

(Refer Slide Time: 23:49)



Now, what we want is the group actions. So, what is a group action? Consider a group G and X be any set, then we can say that the group G acts on the set X by way of the following function. So, we will define a function let us say dot (.) which takes G × X to X

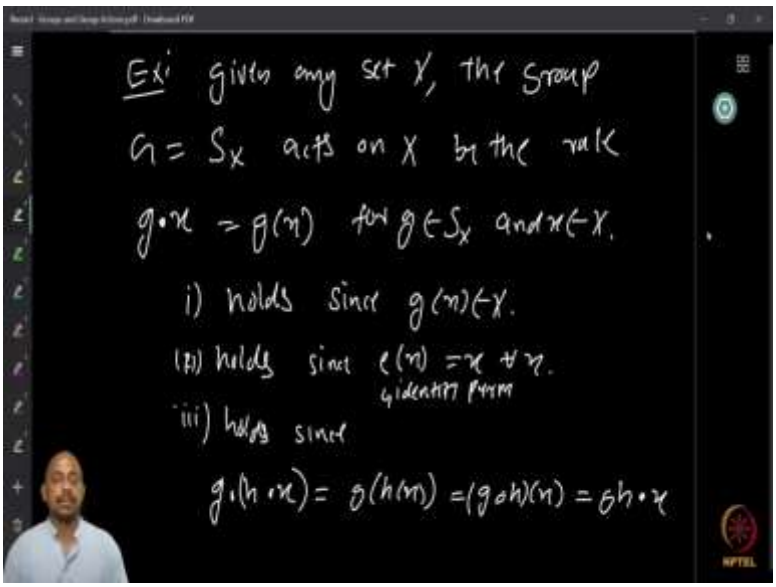
So, basically the elements of X are being permuted by the action of the group, because elements of X can be mapped to X by the action of elements of the group G. So, if G has $g_1, g_2$ as elements, then $g_1$ will take some element let us say $x_1$ of X to some $y_1$, then it can take $x_2$ to $y_2$ and $g_2$ can take $x_1$ to $y_2$ maybe and $x_2$ to $y_3$ or something like that. So, this way we have the group which acts on X.

Now, when do we say that this function defines a group action that is only when

(1) for every element $g \in G$ and for every $x \in X$, $g.x \in X$
(2) for every $x \in X$, and identity element $e \in G$, $e.x = x$
(3) for every $g, h \in G$, for every $x \in X$, $g.(h.x) = (gh).x$

So, if these three properties are hold true then we say what we have defined the function is the group action.

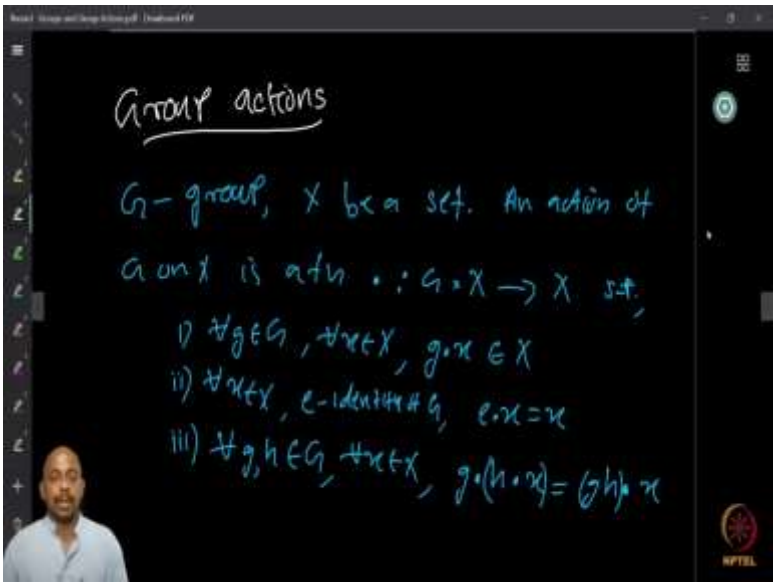
(Refer Slide Time: 27:15)




Some examples here, so if you take any set X, the group of symmetries of X, the permutations of elements of X of course naturally acts on X. Because any element of a set SX is just a permutation of the elements in X and we know that the product of permutations is a permutation and then one can show that all these three properties holds true. So, if you take the first property, first property says that we want for every g in G for every x in X, g.x must be in X. Now, g(x)

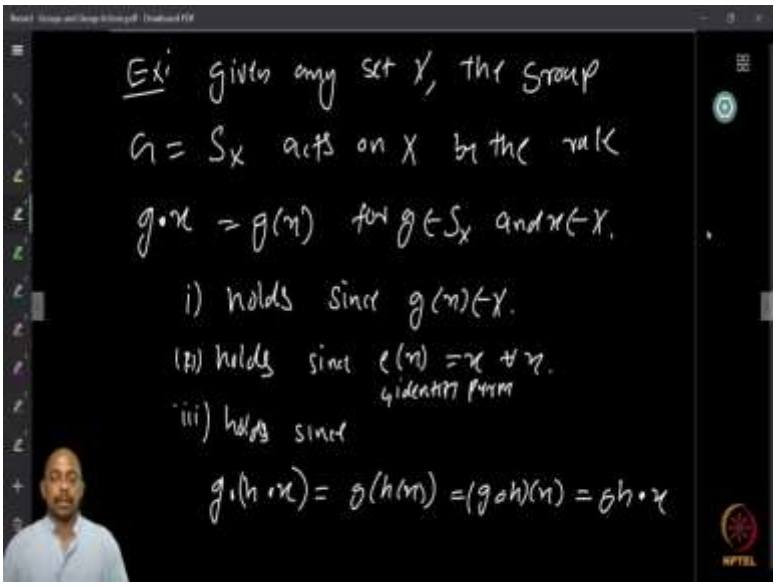
belongs to X for any permutation g and then because of this we have this first property gx belongs to X.

(Refer Slide Time: 28:27)




What is second property? Second property says that for every x in X the e identity, then e.x = x. Now, that is true because e is identity permutation of $S_X$. So that this is true.

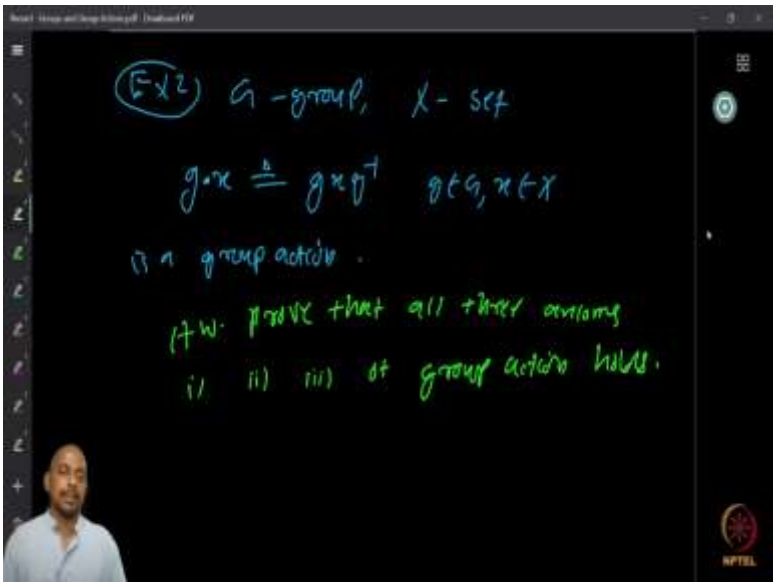
(Refer Slide Time: 28:44)




Then three third holds, it says that the composition must be also true, so g(h . x) is basically g(h(x)). Because h( x ) is the permutation of x then g(h(x)) is the permutation of h( x ) and we know that the composition has the property. Therefore, (g ∘ h) (x) is also equal to gh(x) because gh is the composition of g and h in the symmetric group. This one can show easily. So, all these three properties hold and therefore the symmetric group acts on the set. So, this is our most

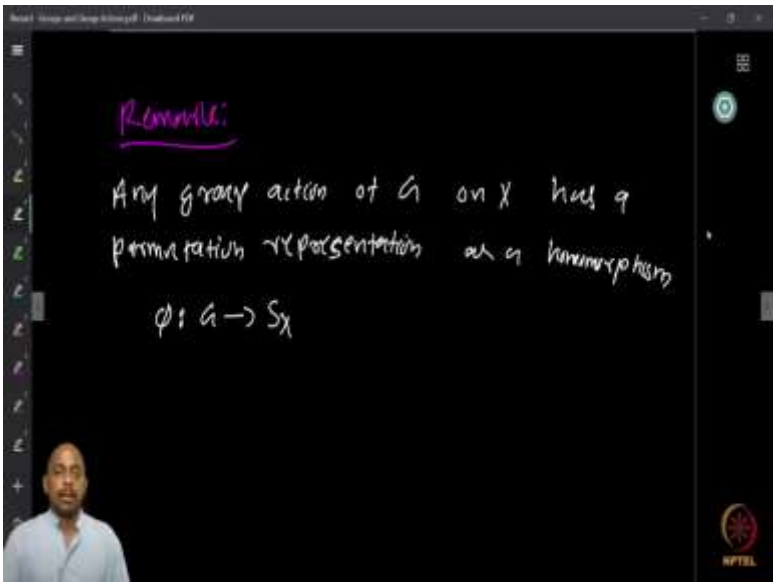
important example because one can show easily that, any group action can be represented by action of a symmetric group.

(Refer Slide Time: 29:37)




So, if you take a group G and a set X, then let us define $g.x := g\,x\,g^{-1}$ where $g \in G,\ x \in X$. Now this is a group action, so this is the claim and I want you to show that all the properties of the action, all the three axioms hold true in this case. So, this is the very good example, I want you all to try this.

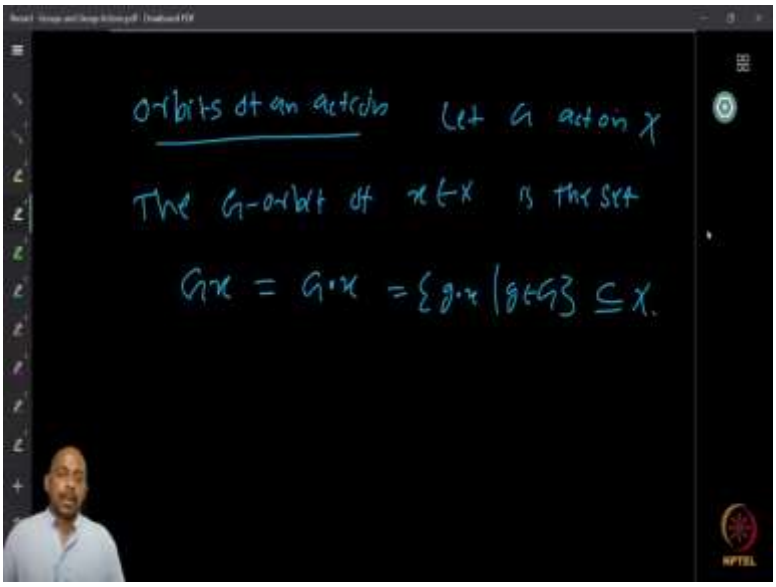
(Refer Slide Time: 30:06)




Now a remark. Any group action of G on X has a permutation representation as a homomorphism from $\phi: G \to S_X$. So, I want you to think about this, this is not very difficult

to show but I am not going to work out the details in this short introduction, but it would be a nice exercise to try and if you have any difficulties get back to me.

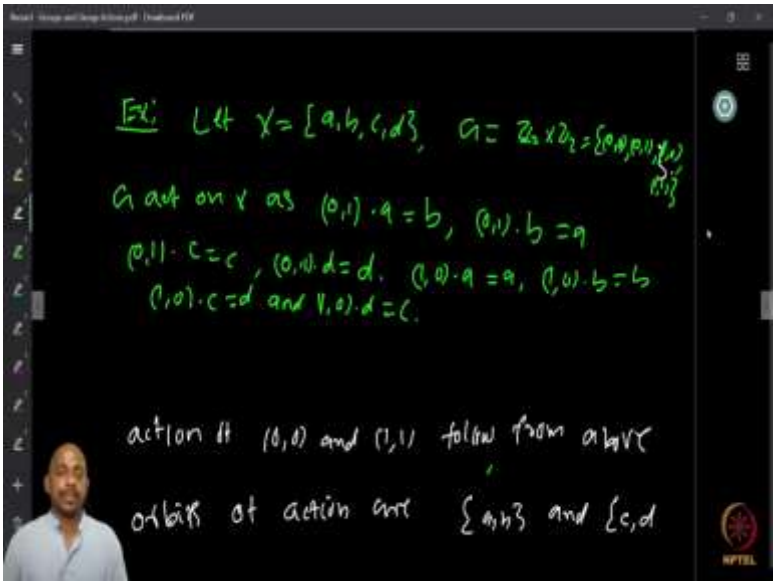
(Refer Slide Time: 30:38)




Now, another important notion that we want is, what happens under the action of a group. So, to an element what happens that is represented by the idea of an orbit. So take elements of this set X and see what happens to the elements under the action of the elements of the group G.

So, take all the elements in the group G, see where it takes a fixed element of X. So if a small x is an element of the set X, then $Gx = G.x = \{g.x \mid g \in G\}$. And this is of course a subset of X because Gx takes elements of X to elements of X. So, therefore it is a subset of X and this is called orbit of x ∈ X. So, for a fixed element its orbit is all the elements of X including x that to which x can be taken by the action of G.

(Refer Slide Time: 31:58)

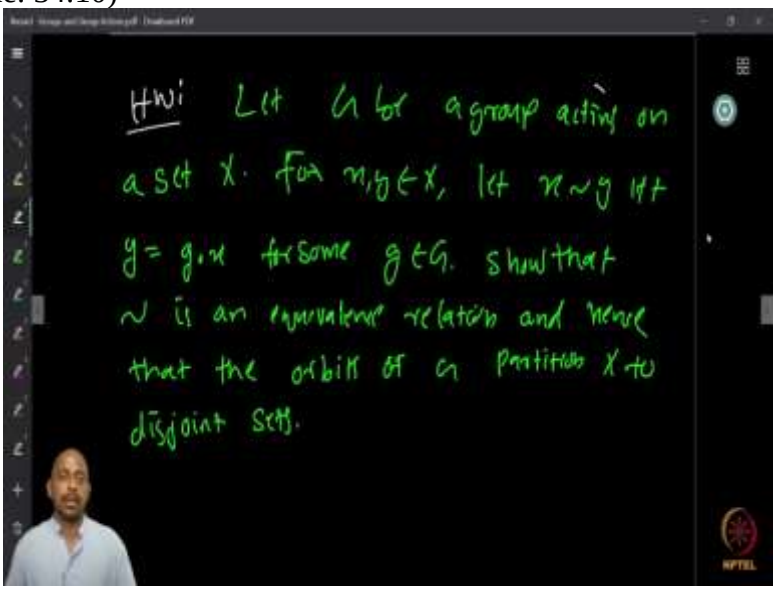



Now, here is a concrete example. Let X = {a, b, c, d} be the set and G = $Z_2 \times Z_2$= { (0, 0), (0, 1), (1,0), (1, 1) }. Now, let us see what happens to a, b, c, d under this action. So, we are going to define an action so G act on X as follows (0, 1)a = b. (0,1) is just an element of an element of G, it takes a to b and it takes b to a and similarly (0,1) takes c to c and (0, 1) takes d to d.

Now (1, 0) takes a to a. (1, 0) takes b to b. (1, 0) takes c to d and (1, 0) takes d to c. Now, I have not defined what (0, 0) does or (1, 1) does but since (0, 1) and (1, 0) can generate whole of G, you can show that this also defines the other actions. What happens when (0, 0) acts on a or (1, 1) acts on a etcetera. So, this one can verify in fact you should verify, what happens to this and then once you have all this thing you can show that the orbits of the action are a, b and c, d.

Now a, b so a is always taken to b and b is, I mean a is taken to either a or b and by the elements of G and b is taken to a or b itself and similarly c will be going to d or c and then d will be going to c or d itself. And one can verify that, a never goes to c or b never goes to d etcetera. So, these properties one can we can verify it.

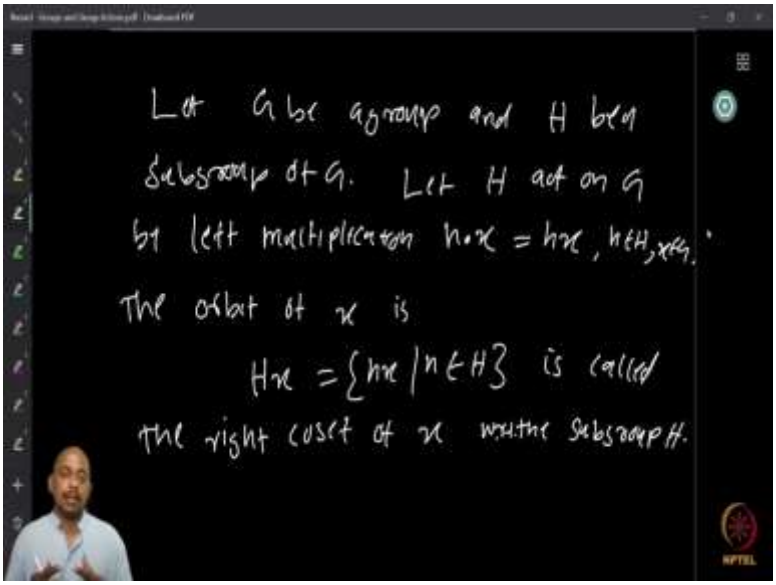
(Refer Slide Time: 34:10)




Now, you should check out all these. Then as a homework you can do the following. If G is a group acting on a set X, for two elements x and y in X, let $x \sim y$ , if and only if $y = g.x$ for some group element g, if y is in the orbit of x. Now show that this relation is an equivalence relation. In fact, if y is in the orbit of x then x is also in the orbit of y. It is an equivalence relation and hence show that the orbits partition X into disjoint sets, because equivalent relation, the equivalence class is basically from a partition of the partition of the set in which it is defined.

So, therefore one can observe or one can show that the orbits are basically the equivalent classes under this equivalence relation that we have defined and hence they basically partition the set X to disjoint sets and this property is very important, we will use it quite often in the next few lectures.

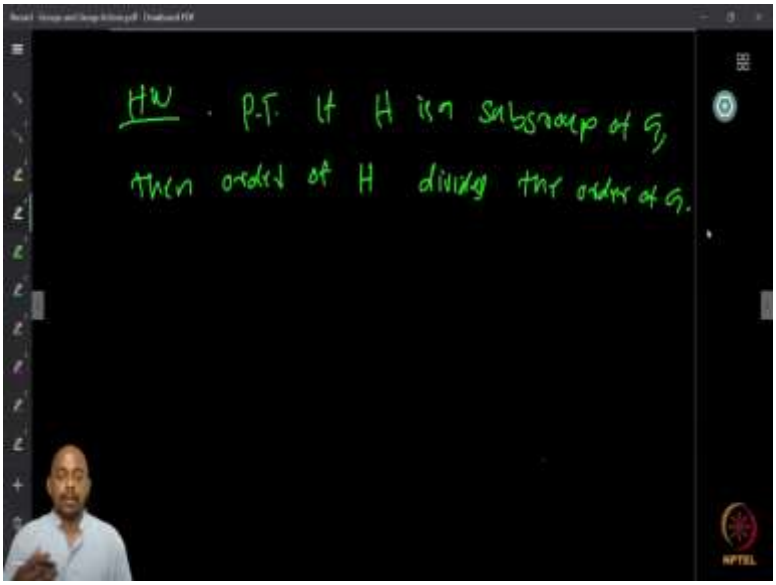
(Refer Slide Time: 35:29)




Now, given a group G and a subgroup of G, let us say H, we can let H act on G by left multiplication. So, you take the subgroup H then act on G by left multiplication, so we are looking at elements of H, with multiplied to elements of G. So, x is an element of G and h is an element of H, then h.x = hx which defines the left multiplication. Now, this left multiplication by h, one can show that it is actually a group action and show that it is a group action by showing all the three properties holds and then find the orbit of an element and this orbit of element which is basically Hx that we defined earlier.

We denoted by Gx, the action of G on the set X with the element x is going where that is the orbit of x. So Hx = {hx | h ∈ H }and this is called the right cosets of x with respect to the subgroup H. So, this idea of cosets are also important. Again, cosets come from the group actions but it has independent importance as well.

(Refer Slide Time: 37:16)




So, we will see this and as a homework I want you to try out and show that if H is sub group of G then order of H divides the order of G. This is very immediate, once you show these properties that you can show and show that this is an equivalence relationship and one can immediately show that this is actually true. This is a very famous result; order of subgroup divides the order of the group and with that we can stop this very short introduction to groups and group actions. We will need a few more things but that we will introduce when we discuss Polya's Theory.