Lecture - 63
Subgroups

(Refer Slide Time: 00:24)

Hello everyone, welcome to this lecture. So, the plan for this lecture is as follows. In this lecture, we will introduce the definition of subgroups and we will see some properties of subgroups. And then we will discuss about Lagrange's theorem in the context of subgroups and its applications.

(Refer Slide Time: 00:37)

So, let us start with the definition of a subgroup. So, imagine you are given an abstract group G with operation $\circ$, it may or may not be finite. And imagine I take a subset H for the set G.

Again it may or may not be finite. Of course, if G is finite any subset will be finite, but if G is infinite then I may take a finite subset or infinite subset. Now, if the subset H with the same operation ∘ satisfies the group axioms namely G_1, G_2, G_3, G_4 then I will call H along with the operation ∘ to be a subgroup of the original group.

So, an example of a subgroup will be the following. So, let group G be the set of real numbers with the operation integer addition then if I take the set of integers then that will be of course, a subset of the real numbers. So, my real number was the bigger set and my integer is a subset of the set of real numbers and I take the same operation plus here. So, it is easy to see that the set of integers is indeed a group, it satisfies the group axioms with respect to the integer addition and hence, I can say that this is a subgroup of the group of real numbers with integer addition.

Whereas, if I take the set of integers as my main group or the bigger group with the integer addition operation and now, if I take the subset namely the subset of non-negative integers with the plus operation then it does not constitute a subgroup. Because the set of non-negative integers does not satisfy all group axioms. Namely, the additive inverse is negative and it will not belong to the set of non-negative integers.

So now, an interesting question is, imagine you are given an abstract group and now, I give you a subset, how do I check whether it is a subgroup or not? There are 2 options, option one that you manually check whether all the group axioms are satisfied for the subset H that you are given. But that is not what we will prefer because if my subset H is very large then it might become very difficult to verify whether all the group axioms are satisfied or not.

Instead, what we are looking now, here, is the following. We are looking for a characterization, some kind of condition which should be sufficient to check and declare whether the given subset H satisfies the group axioms or not with respect to the operation.

(Refer Slide Time: 03:35)

Characterization of Subgroups

❑ Let $(\mathbb{G}, \cdot)$ be a group and let $\mathbb{H} \subseteq \mathbb{G}$, where $\mathbb{H} \neq \emptyset$, such that the following holds:

(S_1): $\forall x, y \in \mathbb{H}: x \cdot y \in \mathbb{H}$ $\qquad$ (S_2): $\forall x \in \mathbb{H}: x^{-1} \in \mathbb{H}$

Then $(\mathbb{H}, \cdot)$ is a **subgroup** of $(\mathbb{G}, \cdot)$

❑ Proof:

❖ From (S_1), the operation $\cdot$ satisfies the **closure property** in $\mathbb{H}$

❖ The operation $\cdot$ is **associative** in $\mathbb{H}$, since $\mathbb{H} \subseteq \mathbb{G}$ and operation $\cdot$ is associative in $\mathbb{G}$

❖ From (S_2), every element in $\mathbb{H}$ has a corresponding **inverse** in $\mathbb{H}$

❖ Consider an **arbitrary** $x \in \mathbb{H}$

➢ From (S_2), we have $x^{-1} \in \mathbb{H}$

➢ From (S_1), we have $x \cdot x^{-1} \in \mathbb{H}$ $\quad \Rightarrow 1 \in \mathbb{H}$

So, here is a very interesting characterization for subgroups. So, you are given a subset H, of course, a subset H has to be non-empty because if it is empty, it can never be a group because you need the identity element to be present at least in your group. So, definitely H cannot be empty; it has to be a non-empty subset. So, imagine you are given a non-empty subset, the characterization is the following.

You just verify whether the 2 properties S_1 and S_2 are satisfied. And if they are satisfied then you can declare that the subset H indeed constitutes a subgroup of the original group. Note that I am using the multiplicative notation here. So, what are these 2 conditions? The condition S_1 demands that, the closure property should be satisfied.

That means, you take any x, y value from your subset H, the result of the group operation should be a member of the subset H itself. And the second property here is that every element in the subset H should have multiplicative inverse present in the subset H itself. So, the claim here is that if these 2 properties are satisfied, that automatically ensures that all the group axioms are satisfied.

That means I do not need to check separately for the existence of the identity element. And I do not have to check for the associative property. So, let us see the proof of this characterization. So, I have to prove that, if indeed S_1 and S_2 are satisfied then all the group axioms are satisfied in my subset H. We observe that the closure property follows directly from S_1.

So, if indeed S_1 condition is satisfied that means, the closure property is satisfied. The operation dot or abstract operation ∘ was indeed associative in the G itself because G satisfies the group axioms. So, it will be associative in H as well because the elements of H are nothing but elements of G. And closure property is anyhow satisfied guaranteed in H, so that means, the operation ∘ or the operation dot will be associative in H as well.

The axiom number S_2 guarantees you that every element in H has its inverse in H present. And now, I have to show that identity element is also a part of my subset H, if the condition S_1 and S_2 are satisfied. So, for that, consider an arbitrary element x belonging to your subset H. I can apply the axiom number S_2 and claim that x^{-1} is also present in H.

And from the first axiom S_1, I know that the result of x operation x^{-1} will be an element of H because the axiom number S_1, says that the closure property is satisfied. So, x is an element of H, x^{-1} is also an element of H. So, the result of group operation of x and x^{-1} should be also a member of H. But what is the result of group operation being performed on x and x^{-1}? It will be the identity element and this shows that identity element is guaranteed to be present in my subset H. So that shows that if S_1 and S_2 are satisfied, all the group axioms are satisfied.

(Refer Slide Time: 07:23)

Characterization of Subgroups of Finite Groups

❑ Let $(\mathbb{G},\cdot)$ be a group and let $\mathbb{H} \subseteq \mathbb{G}$, where $\mathbb{H} \neq \emptyset$, such that the following holds:

(S_1): $\forall x, y \in \mathbb{H}: x \cdot y \in \mathbb{H}$ $\qquad$ (S_2) $\forall x \in \mathbb{H}: x^{-1} \in \mathbb{H}$

Then $(\mathbb{H},\cdot)$ is a **subgroup** of $(\mathbb{G},\cdot)$

Corollary: If $\mathbb{G}$ is finite then (S_1) is alone is sufficient for $(\mathbb{H},\cdot)$ to be subgroup of $(\mathbb{G},\cdot)$

❑ **Proof:** we will show that if $\mathbb{G}$ is **finite**, then condition $(S_1) \Rightarrow (S_2)$ $\quad$ $x \in \mathbb{G}$
Let $O(x) = m$
$x^m = 1$

❖ If $\mathbb{H} = \{1\}$, then clearly $(\mathbb{H},\cdot)$ is a subgroup of $(\mathbb{G},\cdot)$

❖ Else, let $x \in \mathbb{H}$ where $x \neq 1$, such that $Order(x) = m$ where $m > 1$

$x^m = 1$ $\quad \Rightarrow \quad$ $x^m \cdot x^{-1} = x^{-1}$ $\quad \Rightarrow \quad$ $x^{m-1} = x^{-1}$

❖ To show that $x^{-1} \in \mathbb{H}$, we need to show that $x^{m-1} \in \mathbb{H}$

➤ But $x^{m-1} \in \mathbb{H}$, by **repeated application** of (S_1) on $x \in \mathbb{H}$

So that is a very nice characterization. Now, an interesting corollary here, is the following. The corollary says that, if your original group G is finite then no need to check even for the second axiom; just check whether the first axiom is satisfied or not. Namely, just check whether the closure property is satisfied or not in your subset H. If the closure property is satisfied in the

subset H that automatically guarantees you that all the remaining group axioms are also satisfied in your subset H.

So, the proof for this corollary will be the following. We have to show that if your bigger group G is finite and if your condition S_1 is satisfied in H, I have to show that, condition S_2 is also satisfied in H because we had already proved that if both S_1 and S_2 are satisfied in H then all the 4 properties of group hold in H. Right now, it is not given to me whether S_2 is satisfied or not, it is just given to me that G is finite and S_1 is satisfied in H.

I will show that if G is finite and S_1 is satisfied in H, I can draw the conclusion that even S_2 is satisfied for my H. And now if S_1 and S_2 are satisfied for my H, I had already proved that all the group axioms will hold for H as well. So, everything boils down to this proof. So, the proof will be divided into 2 cases depending upon what is the cardinality of the subset H. If the subset H is a singleton set then it only has the identity element.

So, consider the case when indeed the subset H is singleton and it has the identity element then I do not have to check S_1 holds, S_2 holds or not. Indeed, they hold because the subset H which has only the identity element present in it along with the group operation is indeed a subgroup. The closure property is satisfied because if you perform the group operation on the identity element with itself, you will obtain the identity element which is again a member of H.

The operation ∘ will be associative anyhow in H, the inverse element of the identity element will be the identity element itself and anyhow the identity element is present in H. So, it trivially constitutes a subgroup, I do not have to check about S_1, S_2. On the other hand, imagine that your subset H is not a singleton set. So, imagine that it has some other elements and consider one such element x which is different from your identity element. Now, since x is a member of H, x is a member of G as well.

So, let the order of x be m. And when I say order of x, it means, order of x in the context of the group G. That means, if the order of x is m that means, m is the smallest positive integer such that, x^m is the identity element. Now, if x^m is the identity element, if I multiply both sides of this equation with x^{-1} and again x^{-1} is a group element as per my definition of the group

exponentiation. If I multiply both sides of this equation with x^{-1} then the identity element operated with x^{-1} will give me x^{-1} only.

That means, I can say that $x^{-(m-1)}$ is same as x^{-1}. Now, what is my goal? My goal is to show that, if S_1 holds in my subset H then, S_2 also holds. So that is what I am trying to do here. I have taken an arbitrary x here, different from the identity element whose order is m and right now, I have derived that x^{-1} is same as x^{m-1}. My goal is to show that x^{-1} indeed belongs to the subset H.

So, to show that x^{-1} indeed belongs to the subset H, I have to equivalently show that x^{m-1} belongs to the subset H because, I have already proved here that x^{-1} is same as x^{m-1}. And now, how do I prove that x^{m-1} is a member of this subset H? I can repeatedly apply the fact that axiom S_1 holds in my subset H on the element x.

So, remember x is a member of the subset H and if S_1 holds, it holds for x as well. So, x^2 will be a member of H, x^3 will be a member of H, x^4 will be a member of H and hence x^{m-1} also will be a member of H and x^{m-1} is nothing but x^{-1} and that shows that x^{-1} is automatically guaranteed to be present in H, if the axiom number S_1 is satisfied.

So now, you might be wondering where exactly the fact that G is finite is used here. Well, the fact that G is finite is used here is when I use the fact that the order of x is m. Because if G is infinite and I cannot say necessarily what exactly is the order of x, it may not be defined at the first place. So that is why this proof holds only for the case when my group G is a finite group. So that means, if I am given a finite group G and a subset of G then to check whether the subset H constitutes a subgroup or not it is just sufficient to check the closure property.

Just check whether the closure property holds in the subset or not, if it holds then you can conclude that all the remaining group axioms will also hold, a very nice characterization.

(Refer Slide Time: 14:02)

Cyclic Subgroup Generated by a Group Element

- Let $x \in G$ such that $\text{Order}(x) = m$ $x^m = 1$

$$\mathbb{H} \stackrel{\text{def}}{=} \{x^0 = 1, x^1, \cdots, x^{m-1}\}$$

- Then $(\mathbb{H}, \cdot)$ is a **cyclic subgroup** of order m, **generated** by x

$$\mathbb{H} = \langle x \rangle$$

- Let $(\mathbb{G}, \cdot)$ be a group and let $\mathbb{H} \subseteq \mathbb{G}$, where $\mathbb{H} \neq \emptyset$, such that the following holds:

$$(S_1): \forall x, y \in \mathbb{H}: x \cdot y \in \mathbb{H}$$

$$(S_2): \forall x \in \mathbb{H}: x^{-1} \in \mathbb{H}$$

Then $(\mathbb{H}, \cdot)$ is a **subgroup** of $(\mathbb{G}, \cdot)$

- **Proof**: we will show that (S_1) and (S_2) hold for $\mathbb{H}$

  ❖ For **any** $x^i, x^j \in \mathbb{H}$, we have $x^i \odot x^j = x^{i+j} = x^{[i+j \bmod m]} \in \mathbb{H} = x^{(i+j) \bmod m} \quad // x^m = 1$

  ❖ Consider **any arbitrary** $x^i \in \mathbb{H}$, where $i > 0$ $0 < i \leq m-1$ $x^{m-i} \in \mathbb{H}$

  ➤ $x^i \odot x^{m-i} = x^m = 1$

  ➤ Since $x^{m-i} \in \mathbb{H}$, the **inverse** of x^i is x^{m-i}

So, now, based on this we will generate various cyclic subgroups of a group. So, you might be given a group which need not be a cyclic group but by using the previous result I will try to now derive cyclic subgroups of my original group. So, I have retained the result that I have just proved. Namely, the characterization for the existence of a subgroup. That means, if you are given a non-empty subset, how do you check whether that non-empty subset is a subgroup or not.

So, now, imagine you are given a group G and an element x, whose order is m. Its order is m means x^m is the identity element; that means m is the smallest positive integer such that x^m gives you the identity element.

Now, let me define subset H which is obtained by raising or by computing m distinct powers of x namely, $x^0, x^1, \ldots, x^{m-1}$. So, these m elements are distinct; we had already proved that in one of our earlier lectures. Now, my claim is that this subset H is a cyclic group, whose generator is x. And it is a cyclic subgroup of your original group. So, how do we prove? First of all x is a generator; that is easy to see because all the elements of H are generated by different powers of x. So, indeed, x is a generator. Now, I have to prove that indeed, the group axioms are satisfied for my subset H.

And for that, I have to show that both property S_1 as well as property S_2 holds for H. If I can prove S_1 and S_2 holds for my subset H that I have computed like this then that shows that it is indeed a cyclic subgroup. So, let us first prove the closure property. So, let us take 2 different

elements from the set H. Since they are 2 different elements of H, they are basically some distinct powers of the generator x, say the i-th power and the j-th power.

Then I have to show that the group operation performed on x^i and x^j will also give me an element of H. And that is very trivial to prove because the group operation performed on x^i and x^j will give me an element x^{i+j}. Now, this x^{i+j} is same as $x^{(i+j)\bmod m}$. Why so? Because, since the order of x is m, that means $x^m = 1$, so I can rewrite x^{i+j} as several blocks of x^m; and the last block which may not be a full block of x^m but rather it will be $x^{(i+j)\bmod m}$.

Now, I know that each block of x^m will give me the identity element and the last block which has $x^{(i+j)\bmod m}$ that will remain. Now, the identity element being multiplied to itself several times will give me the identity element. So, this will be same as identity element being multiplied with $x^{(i+j)\bmod m}$.

And hence the result of x^{i+j} is same as the result of $x^{(i+j)\bmod m}$. But then $(i+j)\bmod m$ will give you a remainder in the range 0 to $m - 1$. So, this will be a value in the range 0 to $m - 1$ because the possible remainders that you can obtain by dividing $i + j$ by m will be either 0, 1, $\ldots$, $m - 1$. That means this is nothing but some power of x in the range where the exponent is in the range 0 to $m - 1$ and that will be definitely an element of H because any power of x where in the exponent you have something in the range 0 to $m - 1$ will give you an element of H. So that shows the closure property or S_1 is satisfied.

Now, I have to prove the S_2 property. That means if I take any arbitrary element from the subset H that I have computed, it has an inverse present in the subset H as well. So, I take some arbitrary element where the arbitrary element is x^i and $i > 0$. Why greater than 0? Because if $i = 0$ then x^i is nothing but the identity element and the inverse of the identity element will be the identity element only. So, S_2 will be of course, satisfied for the identity element. I want to prove that it is satisfied for any other non-identity element as well. So that is why I am taking x^i where i is not zero. And I have to show that for this x^i element, the corresponding inverse is also present in H.

So, my claim is the following. That, x^{m-i} which is also an element of the subset H constitutes the inverse of x^i. So, it is easy to see that indeed x^{m-i} belongs to H. Why? Because i is some

power, of course, i is greater than 0 but i is also less than equal to $m - 1$. That means, $m - i$ will also be now a power in the range 0 to $m - 1$. So that is why it is a member of H. And what will be the result of performing the group operation on x^i and element x^{m-i}? Well, it will be the same as identity element.

So that is why I can now conclude that you take any non-identity element in the subset H, its corresponding inverse is also present in the subset H. And since S_1 and S_2 is satisfied for the H that I have built that means, H indeed constitutes a group. And it is cyclic because its generator is x. By the way, you might be wondering that why I am verifying both S_1 and S_2 here for the subset H. Why cannot I just verify S_1? Because I just proved some time back that it might be sufficient to just check the condition S_1.

Well that is the case when your group G would have been a finite group but here I am proving the property for a group G which may or may not be finite. So, if your group G is not finite then I have to check for both condition S_1 as well as condition S_2. That is why I am checking for both S_1 and S_2.

(Refer Slide Time: 21:21)

Left and Right Coset of a Subgroup

❑ Let $(\mathbb{G},\cdot)$ be a group, $(\mathbb{H},\cdot)$ be a subgroup of $\mathbb{G}$ and let $g \in \mathbb{G}$

Left coset of $\mathbb{H}$ with respect g: $\quad g\mathbb{H} \triangleq \{g \cdot h \mid h \in \mathbb{H}\}$

Right coset of $\mathbb{H}$ with respect g: $\quad \mathbb{H}g \triangleq \{h \cdot g \mid h \in \mathbb{H}\}$

❑ If $(\mathbb{H},\cdot)$ is a finite subgroup, then for any $g \in \mathbb{G}$, we have $|g\mathbb{H}| = |\mathbb{H}g| = |\mathbb{H}|$

❖ Let $\mathbb{H} = \{h_1, \cdots, h_n\} \implies g\mathbb{H} = \{gh_1, \cdots, gh_n\}$

❖ From the right-cancellation rule, all $gh_1, \cdots, gh_n$ are distinct

❑ Ex: Consider the subgroup $\mathbb{H} = \{1, 10\}$ of $\mathbb{G} = \mathbb{Z}_{11}^* = \{1, 2, \ldots, 10\}$, where operation is $\cdot_{11}$

❖ $1\mathbb{H} = \{1, 10\}$ ❖ $3\mathbb{H} = \{3, 8\}$ ❖ $5\mathbb{H} = \{5, 6\}$ ❖ $7\mathbb{H} = \{7, 4\}$ ❖ $9\mathbb{H} = \{9, 2\}$

❖ $2\mathbb{H} = \{2, 9\}$ ❖ $4\mathbb{H} = \{4, 7\}$ ❖ $6\mathbb{H} = \{6, 5\}$ ❖ $8\mathbb{H} = \{8, 3\}$ ❖ $10\mathbb{H} = \{10, 1\}$

❑ Any two left cosets are either the same or disjoint

Now, let us next define what we call as left and right *coset* of our subgroup. And this notion of cosets is very important when we perform error correction in coding theory. Of course, we would not be discussing coding theory this course, but people who are familiar with error correcting codes they might be knowing that when we perform error correction then we use this concept of left and right cosets. So, let us define what exactly is coset.

So, imagine you are given a group and a subgroup for the group. Again, they may be finite, infinite and so on because the definition does not put any restriction. And imagine you are given a group element g from the bigger group. The cosets are defined with respect to your subgroups. But they are defined with respect to elements which are chosen from the bigger group.

So, it might be the case that element is g may not be a member of H; it may be present in G but not in H. So, definition does not put any restriction that element is g should present in the set H; it may or may not be present. But the cosets are defined with respect to your subgroups. So, the left coset of the subgroup H is denoted by gH. And it is basically the collection of all group elements which I obtained by performing the group operation between the g that I have chosen here and all the elements of my subgroup H.

Let the elements of H be denoted by $\{h_1, ..., \}$. Note that it might have infinite number of elements. So, you perform $g \cdot h_1, g \cdot h_2, ..., g \cdot h_i$; you perform g operation every element of subgroup H. Of course, from the closure property you will obtain group elements. The collection of those group elements is your left coset.

Why left coset? Because g is the left operand and the elements of the subgroup H are occurring as your right operands. Whereas the right coset is defined similarly but what you now do is the elements of subgroup H will occur as your left operand and each of them will be operated with g. That will be your right coset and our notation for that will be Hg.

Now, if you change your element g that will give you a different left coset and a different right coset. So it is not the case that you will obtain the same left coset and right coset every time, it depends on g.

So, the first thing that we can prove here is the following. If H is a finite subgroup then you take any element from the bigger group, the corresponding left coset, right coset they have the same cardinality as the cardinality of your finite subgroup. And the proof is very simple. So, imagine your finite subgroup H has n number of elements and the left coset will have the elements $\{g \cdot h_1, g \cdot h_2, ..., g \cdot h_n\}$; where we are using the multiplicative notation for the group.

From the right cancellation rule, all this elements $g \cdot h_1, g \cdot h_2, \ldots, g \cdot h_n$ are distinct. Namely, you cannot have $g \cdot h_i = g \cdot h_j$ where h_i and h_j are distinct because if that is the case, you can apply the left cancellation rule and come to the conclusion that $h_i = h_j$, which is a contradiction.

So that is a trivial proof. Now, let us see a very nice property here, regarding the coset. So, let me first demonstrate the property and then we will prove it for any general group and general coset. So, let me take this group G which is the set $\mathbb{Z}_{11}^*$ and remember the set $\mathbb{Z}_{11}^*$ will have all the integers in the range 0 to 10 which are co-prime to my modulus 11. So basically, you will have all the integers 1 to 10, except 0 because 0 is not co prime to 11.

And my operation is $\cdot_{11}$; multiplication modulo 11. That is my concrete group operation. And suppose I take the subgroup consisting just of elements $\{1, 10\}$. If you are wondering whether this is a subgroup or not, well, you can apply your characterization S_1 on this subset H and then you can verify that indeed the property S_1 holds for this subset H. Now, let us compute the various left cosets of this H.

By various left cosets mean, I will keep on changing my g. I will take g to be 1 first, and then I will take g to be 2 next, and then finally I will take g to be 10. So, the left coset of H with respect to 1 will be $\{1, 10\}$. The left coset of H with respect to the group element 2 will be $\{2, 9\}$. Why? So, this will be because of the following reason. So, if I take g to be 2 then gH will be basically $2 \cdot 1 \bmod 11 = 2$ and $2 \cdot 10 \bmod 11 = 9$ because my operation is multiplication modulo 11.

So that is why this left coset is consisting of the elements $\{2, 9\}$. In the same way, you can compute the left coset with respect to the element $g = 3, g = 4$. So, you will have 10 cosets. Because you have 10 possible values of g. But now you can see here, it is not the case that all my 10 cosets that I have obtained here they are all distinct.

Some of them are same completely or otherwise they are completely disjoint. So, for instance, the left coset of H with respect to the element 1 and the left coset of the same H with respect to the element 10 are same. Whereas, if I consider the left coset of H with respect to element 1

and a left coset of H with respect to 2 they are completely disjoint, they have nothing common. So, now, you might be tempting to prove whether this is the case with respect to any coset or not, or is it the case that it is happening only for this G and only this subgroup?

(Refer Slide Time: 29:11)

Well that is not the case, we will prove that this is a general result. So, what we are going to prove here is the following. If you are given any group and its subgroup then you take any 2 elements from the parent group, call it g_1, g_2 then the left coset of H with respect to the elements g_1, g_2 will be either completely same or they will be completely disjoint. That is a statement here.

And before going into the proof idea, let us try to recall a concept that we had earlier seen in our course where we come across a similar situation. Where we proved something of the following form that you have many subsets and either 2 subsets are exactly same or they are completely disjoint. Namely, we proved that result in the context of equivalence classes. So, if we have an equivalence relation and we formed a corresponding equivalence classes then we know that 2 equivalence classes will be either completely same or they will be completely disjoint.

Something similar is happening here. So that is why we are now going to prove this result by defining an equivalence relation and proving that left cosets are nothing but equivalence classes with respect to that equivalence relation that we will define. So, my equivalence relation that I am defining here is the following. I say that element x is related to the element y, if the element y is present in the left coset with respect to the element x.

If that is the case, I will say x is related to y, otherwise x is not related to y. And I will prove very soon that indeed this relation is an equivalence relation. Namely, it satisfies the reflexive property, symmetric property and transitive property. Assume for the moment that it is indeed the case, that means, this relation is an equivalence relation. Then what can I say about the equivalence classes of this relation?

Well, I can use the property that equivalence classes constitute a partition of the original set. So, the original set over which the relation is defined is the set G. Because x and y are elements of G, I have defined a relation over the elements of the group G. I say element x and element y of the group G are related if y is present in the left coset of x. So, if at all this relation is an equivalence relation then the equivalence classes will constitute a partition of this group G.

And it is easy to see that the equivalence classes here are nothing but the cosets. Because that is how I have defined the relation. And that automatically proves that the theorem statement holds; that means, either 2 cosets will be completely different or they would not have any overlap and will be identical because they constitute your equivalence classes. So, now proof boils down to proving that this relation is indeed an equivalence relation.

So, let us prove that this relation is an equivalence relation by proving the reflexive, symmetric, and transitive properties. So, let us first prove that the relation R is reflexive. That means, we have to prove that every x is related to itself. That means, we have to prove that every x is always present in its left coset where x is a element of your parent group. So, this simply follows from the fact that x is always the result of group operation being performed on x and the identity element.

And this identity element is of course, an element of your subset H because H is a subgroup. So that means when I will be forming the left coset of x, I will be encountering the element x operated with identity element and that will give me the element x itself. Hence, I get the conclusion that x is related to x showing that my relation is reflexive.

Now, let us prove my relation is symmetric. So, imagine x is related to y. x is related to y means when I operated x with all the elements of H, I must have encountered some h_1 such

that $x \cdot h_1 = y$. Now, upon multiplying both sides by h_1^{-1} we get $x = y \cdot h_1^{-1}$. Note that since h_1 is a member of subgroup H, h_1^{-1} also will be a member of subgroup H.

That means x is nothing but y operated with some element of the subgroup H, say, h_2 i.e., let $h_1^{-1} = h_2$. But $y \cdot h_2$ is a member of the left coset of y by definition. So, what I have shown here is that, the element x belongs to the left coset of y. And if element x belongs to the left coset of y then that is equivalent to showing that y is related to x, as per my definition of relation R. So, I have proved that my relation is symmetric as well, and in the same way I can prove it, it is transitive.

So, imagine x is related to y and y is related to z. I have to show that x is related to z. So, if x is related to y that means, y is a member of left coset of x. That means, y is $x \cdot h_1$ where h_1 is a member of the subgroup H. And if y is related to z that means, z is a member of left coset of y and $z = y \cdot h_2$ where h_2 is a member of my subgroup.

Substituting the value of y in the second equation gives $z = x \cdot h_1 \cdot h_2$. Since both h_1 and h_2 are members of H, we can apply the closure property and say that $h_1 \cdot h_2 = h$ is some other element of the subgroup H. Hence, $z = x \cdot h$ will be a member of my left coset of x. That means, x is related to z as well. So that shows my relation R is transitive as well.

(Refer Slide Time: 36:32)

So, now, given the definitions of cosets we will give a very nice theorem which we call Lagrange's theorem which will be useful later on. The Lagrange's theorem in the context of group is the following. If you are given a finite group whose order is n, namely there are n

elements in the group G. And say H is a subgroup, of course, it has to be finite because my parent group is finite.

And say the order of the subgroup is m. Namely, there are m number of elements in my subgroup H. Then the Lagrange's theorem says that m divides n. Why this theorem is for finite group? Because if it is not for finite group, I cannot say anything how many elements are there in G and my H also could be an infinite subgroup. So, basically Lagrange's theorem says that, the order of any subgroup divides the order of parent group if your parent group is finite order.

And the proof is very simple assuming that we have already proved our result regarding our cosets. Now, since my subgroup size is m; that means, the cardinality of H is m, the size of each coset will be m. Because, we proved already that the size of each left coset is same as the size of your subgroup and since the size of subgroup is m, the size of each coset will be m and we had already proved that the cosets constitute a partition as per the relation that I have defined here.

So, now, if there are k distinct cosets which you can form all together. So, your G will have n number of elements; so, called elements as $g_1, g_2, ..., g_n$ and you may form the coset $g_1 H, g_2 H, ..., g_n H$. It may not be the case that you obtain n distinct cosets, some of them may be repeated, but they might be same or it might be the case and or otherwise the 2 cosets will be completely different.

So, imagine that all together they constitute k distinct cosets. Now, in each coset you have m number of elements and if you have all together k distinct cosets, since the union of all the coset, distinct cosets, will give you the parent group G, I can say that km is nothing but the number of elements in your parent group n. And that shows that m divides n. A very simple proof. There are other ways of proving the Lagrange's theorem but they might be slightly long.

But once we have proved the general result regarding cosets, the proof is just 2 line argument here. Now, let us see some interesting conclusions of this theorem. So, imagine if your G is a finite group of order n and if you take any element from the group then the order of that element G will divide order of the group namely n. The second conclusion here is that g^n is also the identity element.

And the proof again is very simple. So, imagine we construct a cyclic subgroup H by taking different powers of the element g. Why it will be cyclic subgroup? We already proved few slides back that if you take any group element from the parent group and compute different powers of that element, it will give you a cyclic group. So, imagine I constitute the subgroup H by taking different powers of the element g, that will give me a subgroup. And say the order of the element is g is m.

Well, if the order of the element g is m then the number of elements in the subgroup H that I have constructed will also be m. Because I have constructed H by computing g^0 up to g^{m-1}; that is my cyclic subgroup that I have constructed. But what exactly the Lagrange's theorem says? If you have finite group and a subgroup of that then the order of the subgroup always divides the order of the parent group.

So, what is the order of the subgroup? I have m. And what is the order of the parent group? I have n. So, from the Lagrange's theorem I obtain that n is completely divisible by m. And that shows that the order of my element g has to divide the order of the bigger group. Now, the order of the element g might be m where m can be strictly less than n but the second result that we want to prove here is that, g to the power order of the group will give you the identity element.

And once we have derived this fact it is very easy to prove that. So, let us see what exactly we will obtain if I compute g^n. g^n will be nothing but g^{km} and since the order of the element is g is m, I note that g^m will give me the identity element and identity element raised to power k will give me the identity element. So that is an implication of the Lagrange theorem.

And if I apply this implication in the context of a prime order group, namely a group where I have prime number of elements then I get the fact that it will be cyclic and every element except the identity element will be a generator for that cyclic group, if my group G is a prime order. Why so? Because if my group G has prime number of elements, and if I consider and arbitrary element x and try to generate the subgroup through that element x, the order of that subgroup has to divide the order of the parent group.

But the parent group has order p which is a prime value and the only divisors of a prime number are 1 or p but since the x that I have chosen is not the identity element, the only option that is left is the order of the x is the prime number p itself. And if the order of the x is the prime number p itself that means the subgroup that I have generated through x is nothing but the whole parent group.

Because if the order of x is prime number p and the parent groups order is also prime p that means, through x I have generated all the p distinct elements of my group. So that is a very powerful result that means, if you want a cyclic group where you do not want to worry about searching for the generators then try for a group which has a prime order.

(Refer Slide Time: 43:56)

References for Today's Lecture
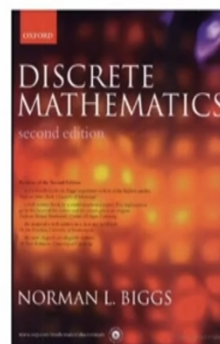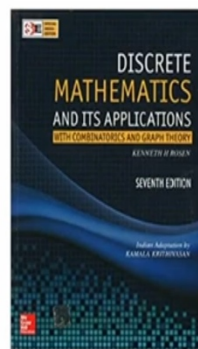
So, with that I end today's lecture. These are the references just to summarize in today's lecture. We discussed about left cosets, right cosets, we derived several properties for the cosets. And we also discussed about subgroups. We gave a characterization for subgroup. And we also discussed properties regarding the order of the subgroup, namely, the Lagrange's theorem. Thank you.