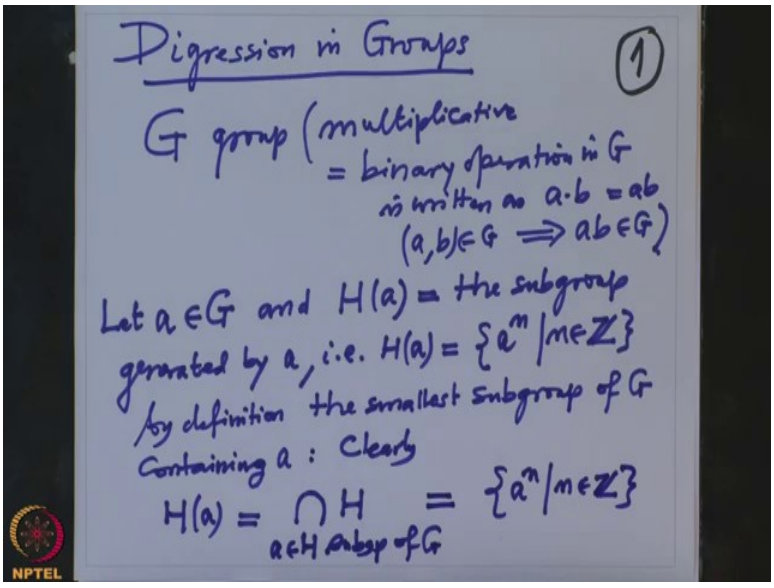
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Banglore
Lecture 19
Digression on Groups

In the last lecture we have use some basics results about groups especially order of an element in a group and in this lecture I will digress on the simple facts about groups.

(Refer Slide Time: 00:51)

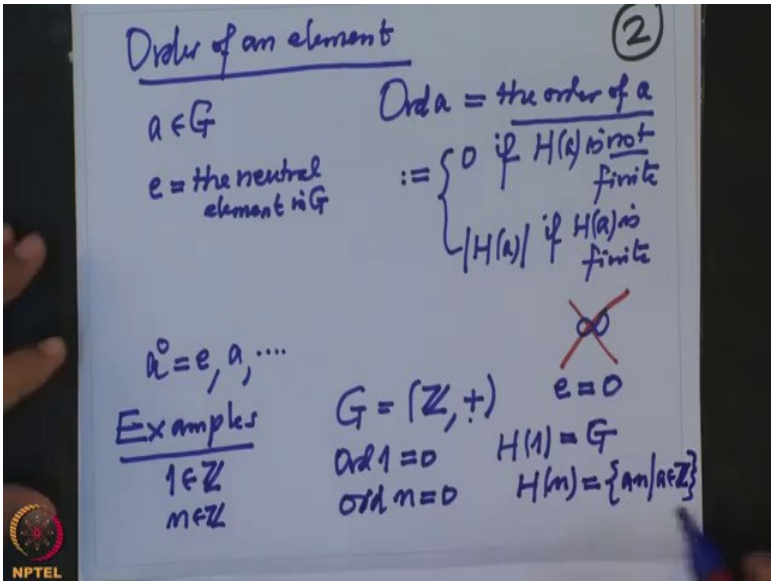


So let us do Digression in Groups alright, so we will as usual denote G group and we will use binary operation written multiplicative so will keep saying that G is a multiplicative group that means the binary operation in G is written as a times b or simply a b. So this is the binary operation in G a, b in G then we a b belongs to G that is the binary operation in G and now we want to define what is a order of an element in G.

So let a be an element in G and H a, H of a denotes the sub-group generated by a that means this H a so that is H a is power of a, a^m as m varies in $\mathbb{Z}$. This is clearly a sub-group of G and by definition this H a is the smallest sub-group of G containing the given element a and it is therefore clear. So clearly H a is therefore by definition intersection of all the sub-groups H where a belong to H and H is a sub-group of G and on the other hand this is one candidate a^n , n

in $\mathbb{Z}$ this is as I said this is clearly a sub-group and all the powers therefore are contained in every sub-group so therefore this equality here. So that is the smallest sub-group of G containing a.

(Refer Slide Time: 4:17)



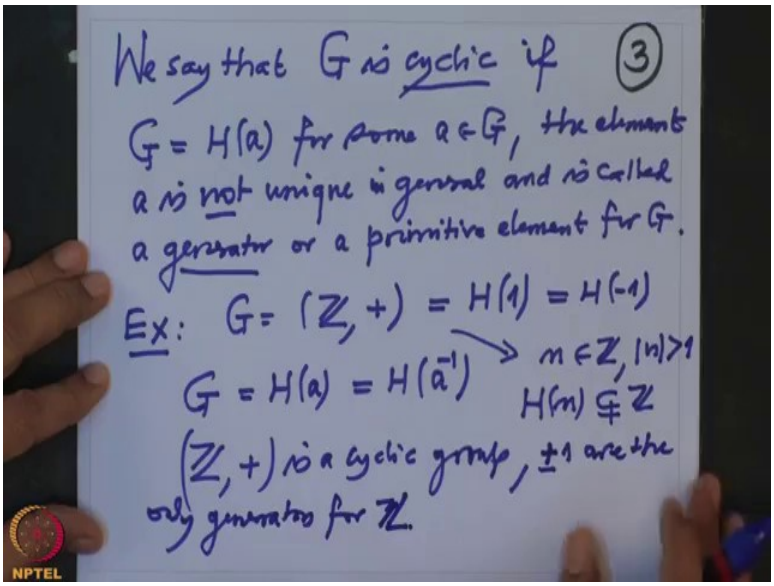
Now we define order of an element (order of an element) so a is in G and let us denote E to be the identity in G this is the neutral element neutral in G that is also called the identity element in G. So order of odd a this is the order of a, this definition is slightly different from the standard textbooks but it is more useful than the standard one and also it clarifies some ambiguity somewhere. So order of an element is by definition it is zero if H a is not finite (not finite) then it is order zero and cardinality of H of a if H of a is finite.

So order of an element in there we never say it is infinite for many reasons, we never write this symbol, this symbol is not written because of its first of all it is not defined also it is countable and countable all kinds of problems will crop so we never define an element of infinite order. So it is a power zero is identity always and a and so on. If this powers of a they don't come back to identity that means that a that means this H a is not a finite group and in that case we define order to be zero ok. So let us see few examples which will throw some light on our definition.

Let us take G to be the additive group of integers under addition, one is in $\mathbb{Z}$ remember identity (element) neutral element is zero here because we are taking the additive operation. So what is

order of one? Order of one is zero because what is a sub-group generated by one? That is a whole group G, this is a whole group G which is not finite therefore order of one is zero. Similarly if I take any integer n what is order of n? That will also be zero because if I take the sub-groups generated by n those are precisely the multiples of n so this are precisely ^{an} as a varies in integers, multiple because our group structure is addition. Therefore in both the cases the sub-group is infinite therefore order is zero alright, so further now.

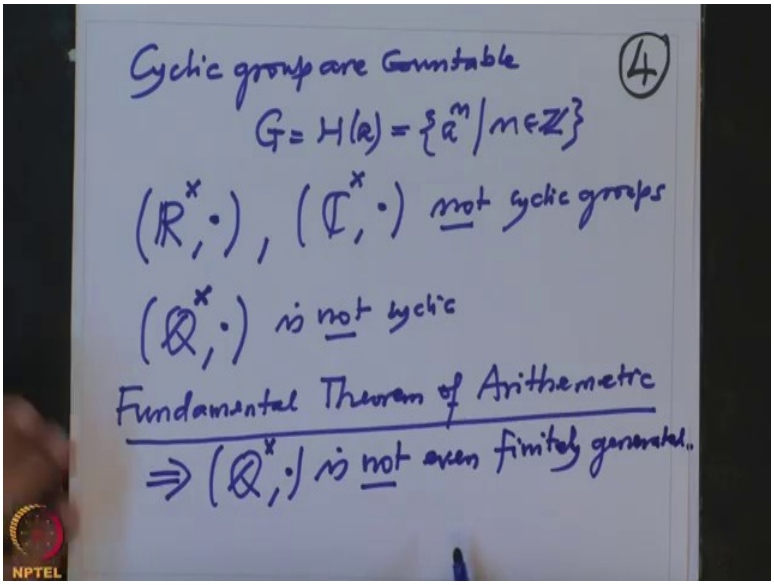
(Refer Slide Time: 8:15)



When does one we say that? We say that G is cyclic if G equal to G generated by one element G is equal to H a for some a in G and this element a, the element a is not unique in general and is called a generator or also called a primitive element, element for G. For example G is the group ($^{\mathbb{Z}}$,+) then G is generated by one also generated by minus 1. More generally if G is arbitrary group if G is generated by a then G is also generated by a inverse, this is multiplicative notation and this additive notation ok.

So if in this case if n is integer and n is more than 1 modulus of n is bigger than 1 then H of n is a proper sub-group of $^{\mathbb{Z}}$, it can never be equal so this means there is no other generator than 1 and minus 1. So $^{\mathbb{Z}}$ this means this ($^{\mathbb{Z}}$,+) is a cyclic group and 1 and $^{-1}$ are the only generators (only generators) for $^{\mathbb{Z}}$. Ok so some more obvious remarks that now we know cyclic groups so what about non-cyclic group ?

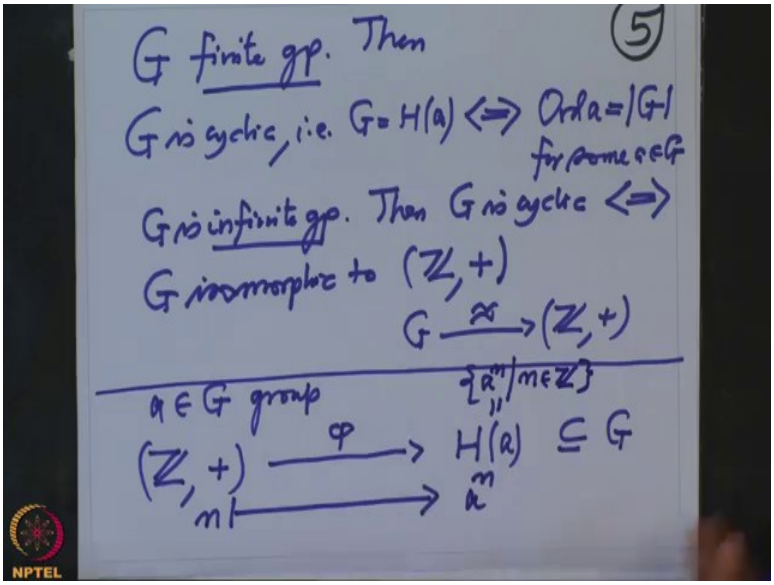
(Refer Slide Time: 11:11)



So cyclic groups first observation is cyclic groups are countable that is clear because cyclic means it generated by one element that is a smallest sub-group which contain this a but this is nothing but a^n as n where the integers. So therefore there are at most $\mathbb{Z}$ many elements in G so in particular G is countable. So now if you look at the group R cross under multiplication non-zero real numbers and their multiplication or non-zero element under multiplication non-zero complex numbers under multiplication this groups are obviously non-cyclic because simply they are not countable but now the group $\mathbb{Q}^x$ rational non-zero rational numbers under multiplication this group though it is a countable it is not cyclic this needs a proof.

But this proof is not obvious but also it is not so difficult, this follows from what is called Fundamental Theorem of Arithmetic (Fundamental Theorem of Arithmetic) which one learns in the school which says that every natural number is a product of prime numbers in a (unique) essentially unique way up to a permutation. So that one can use that to prove that actually more general than non-cyclic that $\mathbb{Q}^x$ under multiplication this group is not even finitely generated let alone one element generating the non-zero rational numbers but even finitely elements cannot generate $\mathbb{Q}^x$ away cyclic $\mathbb{Q}^x$ group under multiplication.

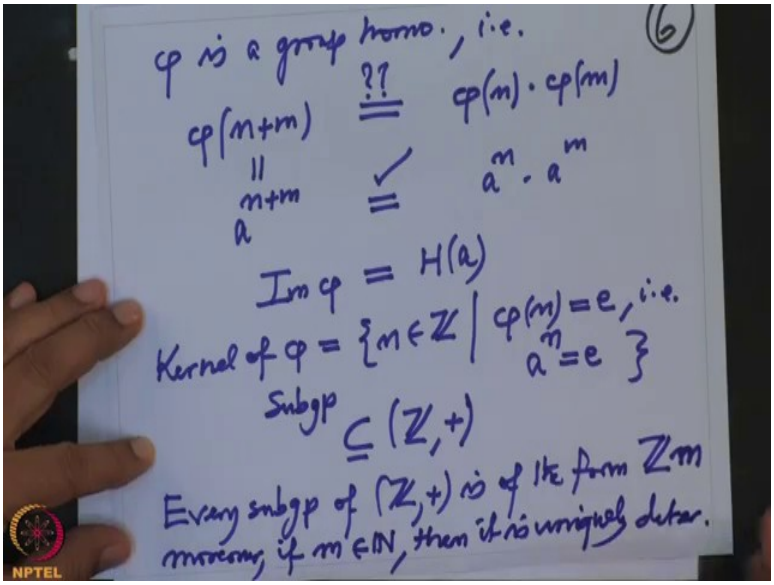
(Refer Slide Time: 13:55)



So there are two kinds of cyclic groups as we have seen, G is so G is a finite group let us say G finite group then G is cyclic that means G equal to H of a if and only if order of a equal to cardinality of G for some a and that a will be primitive element because this order by definition it is cardinality of this and therefore it is clear so that is in case of a finite group when G is infinite group then G is cyclic if and only if G is isomorphic to the additive group ($\mathbb{Z}$,+). So G to ($\mathbb{Z}$, +) there is an isomorphism then only it is cyclic this is so infinite case there is only one group upto isomorphism and finite case there are many more.

Alright so, so how is this isomorphism done? So that is done as follows, more generally what do the following. Given any group G and any element in the group G so this is arbitrary group and a is an arbitrary element there then we have a map from ($\mathbb{Z}$,+) to ϕ the map ϕ this goes inside H of a which is a sub-group of G and is the map any n goes to a^n . So a^n is obviously this H a by definition a^n , n varies in integers.

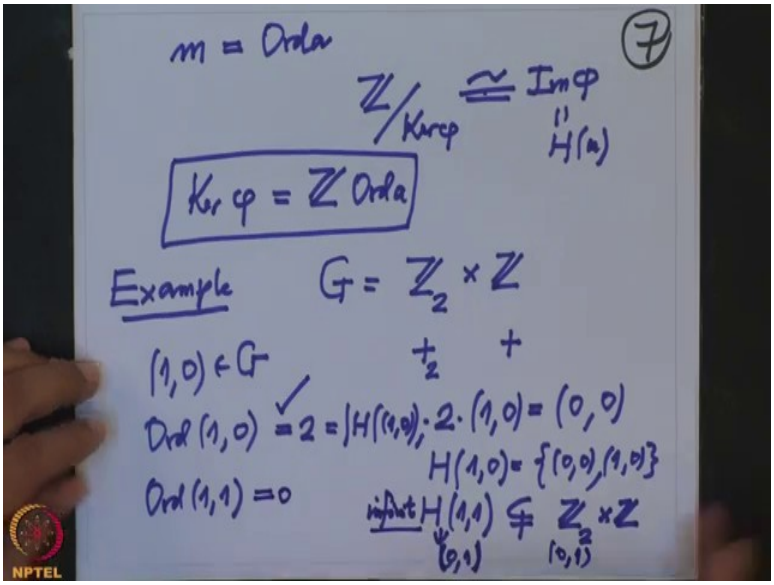
(Refer Slide Time: 16:39)



So therefore we have a natural map it is obvious that this ϕ is a group homorphism, to check that what do we have to check that ϕ respects the operations. So that means we need to check that equality $\phi(n+m)$ where we take two integers add them and then take the image of ϕ on the other hand you take image of ϕ image of n under ϕ and multiply them in a group G whether this result is same or not that is where one checks it is a group homorphism but what is this by definition? This is a^{n+m} and this is a^n this is a^m and the way we multiply elements in the group the associative to the group will tell we can (cal) and this is equality then.

So therefore image of ϕ this is a group homorphism and image of ϕ is nothing but the sub-group generated by a so H of a. So that is how so and what is the Kernel? Kernel of ϕ this is by definition all those elements n in $\mathbb{Z}$ such that ϕ of n is the identity element in the group G but this is same thing as saying that is a^n is identity element but this is Kernel is a sub-group of ($\mathbb{Z}$,+) this is a sub-group but we know all sub-groups of $\mathbb{Z}$ plus every sub-group of ($\mathbb{Z}$,+) is of the form they are $\mathbb{Z}$ multiplies of the fixed number n (m).

(Refer Slide Time: 19:31)



Moreover if you choose moreover if n is a natural number then it is unique (then it is uniquely) determined then that is a unique generator and this unique generator is called the order of this is nothing but this m unique m is precisely the order of the element a and we know if I take $\mathbb{Z}$ go modulo as a Kernel is quotient group is isomorphic to the image of ϕ this is precisely H of a so the Kernel of ϕ is generated as a sub-group of $\mathbb{Z}$ by order of a. Alright so let us see some examples, so just to get acquainted with how does one complete the order.

So let us take G to the product group $\mathbb{Z}_2$ with a modulo 2 operation cross $\mathbb{Z}$ additive group of $\mathbb{Z}$. So remember the operation here is modulo 2 operation and here the operation is usual addition. So one look at the element 1, 0 this is an element in G and what should be the order of 1, 0? I claim order of 1,0 is 2 that is because see what is the 2 types now additive group so I will write 2 times 1, 0 this is by definition adding this element itself with itself so this is 1 plus 1 but it is a modulo 2 operation so the first component is zero and second component is 2 times zero that is zero. So 2 times that element is zero and this element is non-zero this element is not identity element because identity element of the product group is identity in each component.

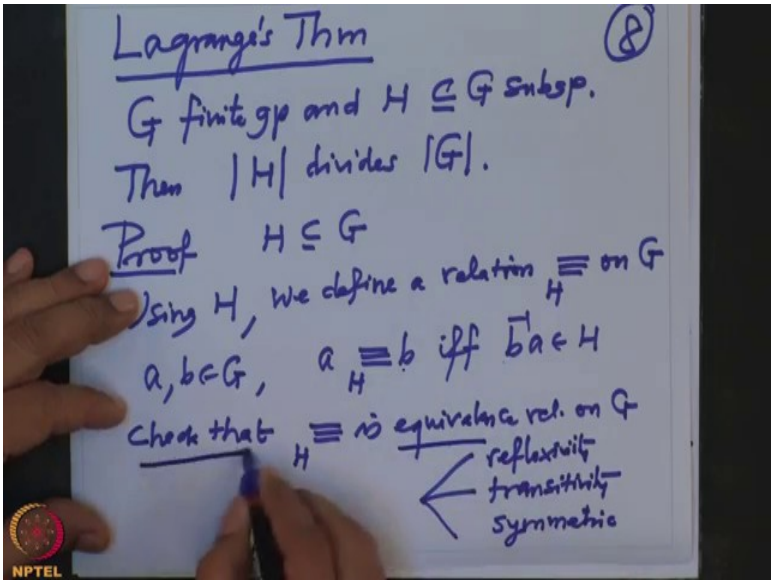
So what is a sub-group generated by 1, 0? This is nothing but only two elements 0,0 and 1, 0 so the this sub-group has cardinality to therefore order of this is 2, this is precisely the cardinality of sub-group generated by 1, 0. What is the element of order 1, 1? So for that again we will

compute the sub-group generated by 1, 1 what will this be? So obviously I claim the sub-group cannot be the whole group simply because the element 0,1 0, 1 is an element here and 0, 1 can never be an element here because to get 0, 1 we will have to multiply this element by some integer but when you multiply this element the second component can never be 1 again.

So therefore this sub-group is actually infinite the sub-group is infinite because we can keep multiplying the m so you can get different the second component is always different. So therefore this element has order zero because this is this sub-group generated by that is infinite order. So with this I will ok, so then in the next lecture where would I have discussed what is the structure of the unit group of a field? That we wanted to prove that if you have a finite sub-group of the unit group of a field then it is cyclic, this is proved in couple of lectures later.

Ok, alright so next thing I want to do now is (eight) now another thing I have used in my last lecture was what is called Lagrange's theorem.

(Refer Slide Time: 24:06)

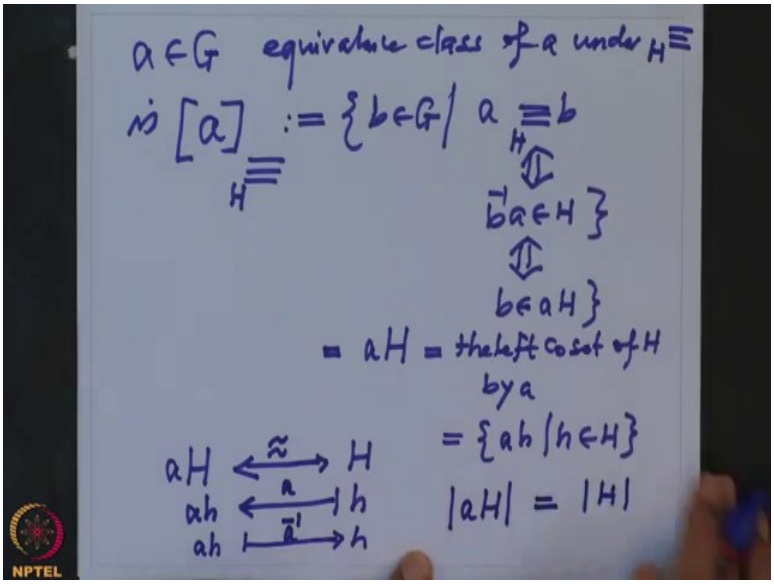


So let me state it first, so G be a finite group and H is a sub-group of G then the order of H divides order of G this is how it is stated how the theorem appears like this in normally in every textbook on the elementary book theory. However, Lagrange then can be this statement in this way, Lagrange came to the statement by computing the fixed points of some group action. So but this very easy to prove this is more of a set theory than a group theory. So how does that prove?

So proof, so given a sub-group H using H we define a relation on G, what is the relation define? That means suppose I have two elements a and b in G then I will say that a and b are related under this if and only if this is the definition b inverse a belong to H. Now one really easily verify that check that this is an equivalence relation on G equivalence relation means you have to check three things mainly reflexivity, transitivity and symmetric and I will not go into this detail so reflexivity is simply mean that a is related to a that means a inverse a belongs to H which is very clear because a inverse a is identity element.

Similarly, symmetry and similarly the transitivity, so I will leave it for you to check this so this is a check that it is a equivalence relation on G ok. Now once we have equivalence relation one talks about the equivalence classes. So what are the equivalence classes?

(Refer Slide Time: 27:22)

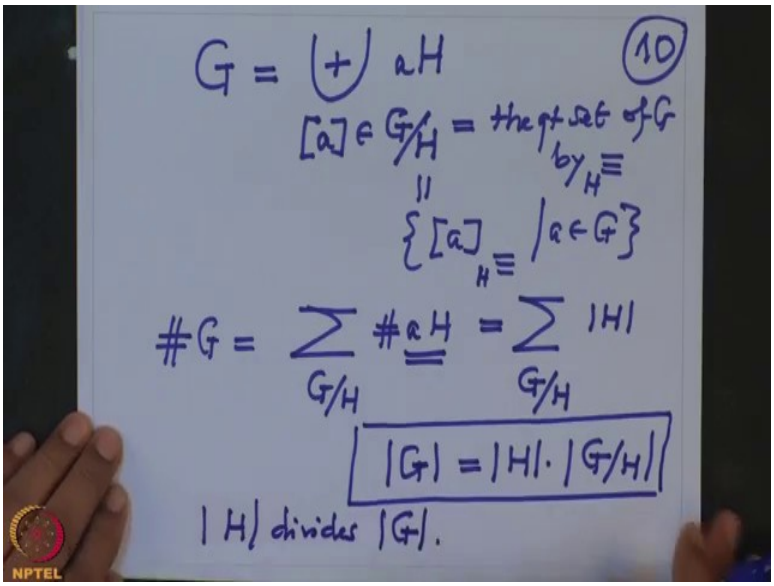


So what is a equivalence class of a? given a in G equivalence class of a under this equivalence relation is also denoted by a suffix this notation of the relation this is that definition all those elements b in G such that a is related to b but this is equivalent to checking that b inverse a belonging to H but is the same thing as b belonging to the coset a H therefore this equivalence class is nothing but the left coset by H, this is the left coset of H by a this is precisely all those elements of the form a times h, h is in H.

So note that the left coset a H and the sub-group H they are in bijective correspondence with each other and the bijection is simply given by h going to a times h this is clearly bijective

because the inverse is given by a inverse. So inverse is given by any a h here, multiply by a inverse so you will get to h so this is multiplies by a inverse this is multiplied by a. So therefore they are inverses so in particular cardinality of the left coset and cardinality of the sub-group they are same. So alright once you have this then Lagrange's theorem proof is more or less clear because look so what does a equivalence relation and equivalence classes do?

(Refer Slide Time: 29:51)

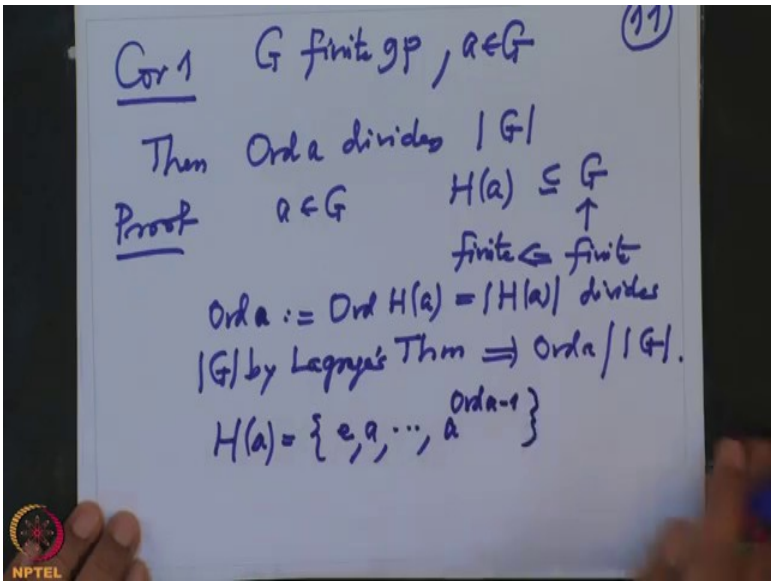


Therefore, this G is decomposed as a disjoint union into the equivalence classes, equivalence classes are the left coset. So this (that) union disjoint union is varying over all the elements a which are in the this is a number of cosets of H in G this is precisely the quotients set of G by the relation this. So $\frac{G}{H}$ is precisely equivalence classes and the only take the different collect only those elements which have the different equivalence classes. So therefore cardinality G is finite so this is a finite set and this is the partition of the finite set.

Therefore cardinality of G will be equal to the sum, sum is running over the set quotient set $\frac{G}{H}$ and the cardinality of the cosets but we have seen cardinality in the coset is same thing as cardinality of H and this is this sum is varying over $\frac{G}{H}$ and this is a constant so I can take it out

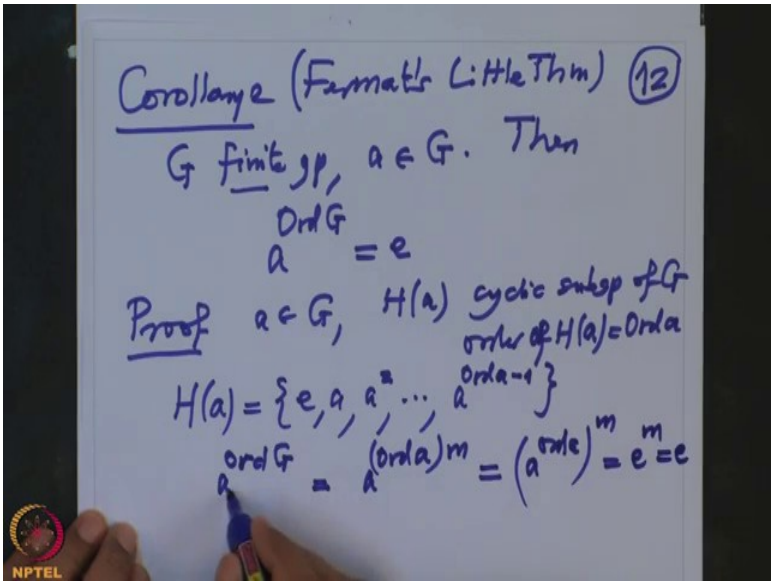
and so therefore this is equal to cardinality of H times cardinality of the quotients at $\frac{G}{H}$ so we get a formula cardinality of G equal to this but from this formula it is very clear that order of H divides order of G. So that proves Lagrange's theorem ok now only two observations I have to record for the future use.

(Refer Slide Time: 32:01)



So corollary one, G finite group and I have an element a in G then order of a divides order of G. Proof, what is order of a? So given any a in H will form a sub-group generated by a which is H a and G is finite given therefore any sub-group is finite therefore order of a is by definition order of H of a this is a cardinality of H of a but then Lagrange's theorem says that this divides order of G by Lagrange's theorem so that means order of a divides order of G. So then in this case what will be H of a? H of a is clearly identity a it can go on till a power order of a minus 1 and then next power will be identity, so this is precisely the sub-group generated by a.

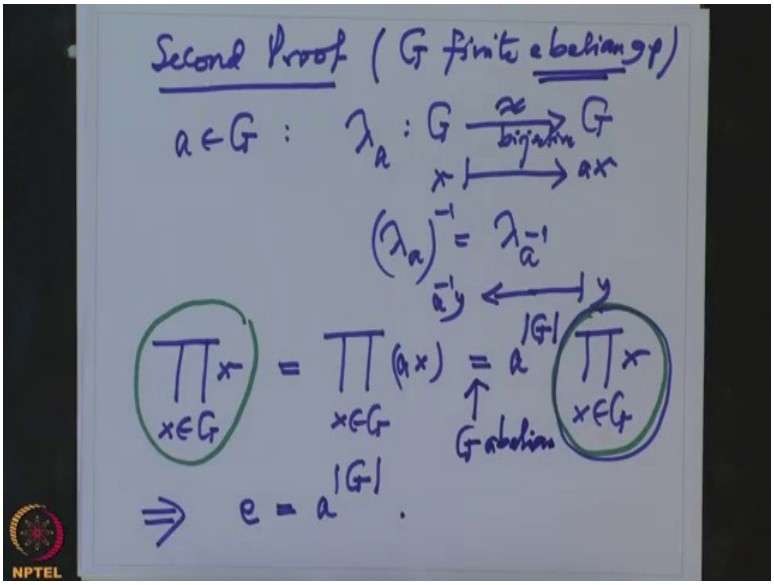
(Refer Slide Time: 33:56)



Alright so second corollary, second corollary is what is known as Fermat's Little Theorem ok, what does it says if G is a finite group, a is an element in G or a is element in G then a power order of G equal to identity. Proof, so let a be in G then as usual we know what is H of a, H of a is a sub-group generated by a this is obviously cyclic subgroup of G because it is generate by a and order of this group order of H of a is by definition order of a because we are in a finite group so H is also finite.

Therefore, as I said H of a is nothing but e, a powers of a going on until a power order of a -1 this is precisely H of a and what is a power the next a power order G that is what we want to prove but order of a divides order of G so a power order a times integer m but a power order a is already identity (a power order a) this power m but this is already identity so it is e^m which is e. So we have proved a power order a is identity.

(Refer Slide Time: 36:06)



So just one little one can also prove this in a slightly different way so second proof , ok so G is this I give proof is in that proof doesn't use that fact that G is abelian but this proof is for finite abelian group so G is finite abelian ok and a is an element is given then I consider the map lambda a on G this is a left multiplication by a so this is any x going to a x this is clearly a bijective map this is bijective because the in ways of this map infact we can write it down this is nothing but lambda suffix a inverse, inverse is given by that. So any y going to left multiplication by a inverse, a inverse y this is the inverse map for this lambda y.

So now let us compute the product, product x, $^{x\in G}$ this is same thing as product $^{x\in G}$ instead of x I will write a x because it is a bijective map this product has not changed so it is a bijective map and because (a is) G is obliged with this a is convenient as many times a G so this is a power order of G times product x, $^{x\in G}$ but this element and this element they are same, this element equal to this element they are same therefore and they are element in a group so I can cancel it. So that will prove that when I cancel this element I will prove that one gets e equal to a power order G this is what we wanted to prove.

So this proof uses the obviously the fact that G is abelian because I have taken out so many times to write this so here I have used the fact that G is abelian alright so with this I will stop this digression on the groups and it is further continued to study a more groups later on and I will

prove later that if I have a finites subgroup of a multiplicative group of a field then it is cyclic in particular $\mathbb{Z}_p^x$ this group is cyclic this is proved later in the lecture, thank you.