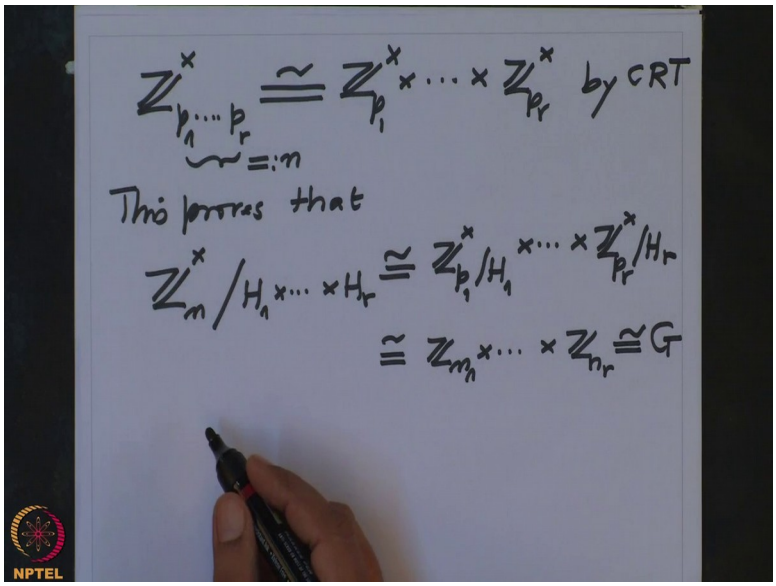
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science Bangalore
Lecture 43
Inverse Galois problem for Abelian Groups

Recall that in the last lecture we proved that under the Galois correspondence of a a Galois extension finite Galois extension, the Galois intermediary field extensions will correspond to the normal subgroups of the Galois group of the original extension. We want to use this to prove that every finite Abelian group will occur as a Galois group of Okay, Galois group of a number field over $\mathbb{Q}$ that means what? That means I want to find a finite Galois extension of $\mathbb{Q}$ such that the Galois group is the the given Abelian group and this problem is known as inverse Galois problem, so let me mention it here to start with.

(Refer Slide Time: 1:28)

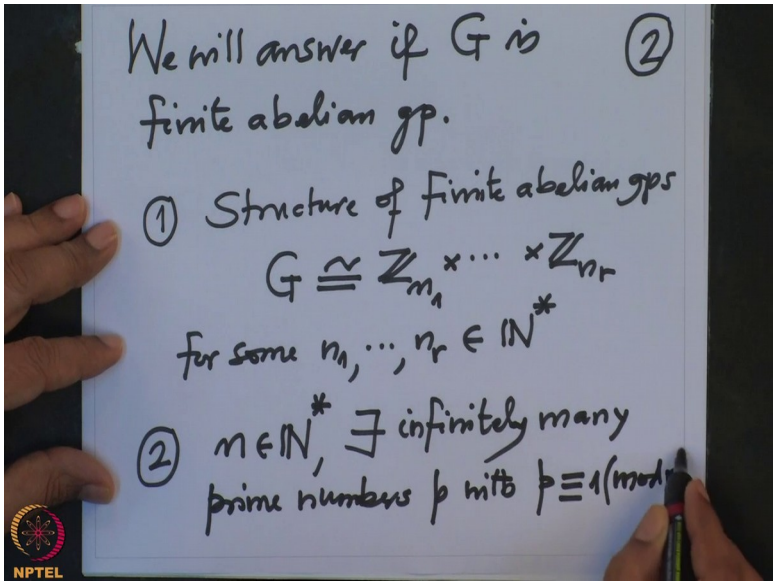


So this is known as inverse Galois problem, so given a finite group G… Question is, does there exist a finite Galois extension L over $\mathbb{Q}$ such that Galois group of L over $\mathbb{Q}$ is precisely the G or isomorphic, this is the problem in general. This problem is big problem and lot of research is done to answer this problem. It is expected that the answer is yes and lot of research is done in this direction and which uses as per topology as per geometry and so many other connections, also the theory of Riemann surfaces that is used in in this kind of problem so it is to be very difficult problem.

And I am going to answer this partially very very special case of this we will prove today namely if the given group given finite group is Abelian and I am going to construct finite

field extension L over $\mathbb{Q}$ such that the Galois group is precisely the given abelian group, so this is what I want to prove today.

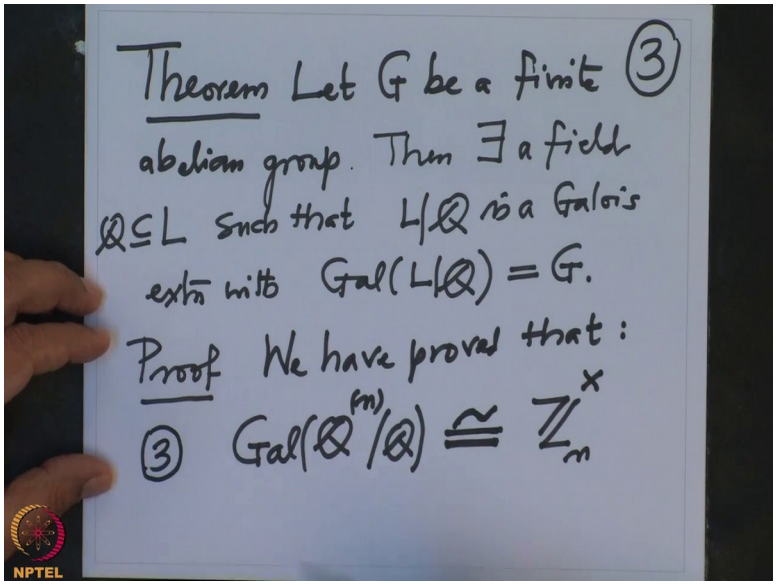
(Refer Slide Time: 4:03)



So we will answer this, if G is finite abelian group, so remember what is more important is Galois extension of $\mathbb{Q}$ rational numbers. If one allows Galois extension of arbitrary field then we can always do it this, so I will show you in later lectures and what I am going to use for this? The ingredients in this proof is the following; understanding the structure of a finite abelian group that is one, we will use these 2 facts, one structure of finite abelian groups namely If G is a finite abelian group, G is isomorphic to product of cyclic group. So G is isomorphic to $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$ for some n_1 to n_r nonnegative integers positive integers.

So this is very standard but we will also prove this, and remember that when I write this isomorphism, this is usually we are writing Galois groups as multiplicity group and this notation here on the right side is additive notation, so that one has to be little careful. This 2nd one 2nd ingredient I will use is, given any $n \in \mathbb{N}$ nonzero natural number, we know that there exists infinitely many primes prime numbers p with property that p is congruent to 1 mod n, this we have proved as a corollary to when we were studying cyclic cyclotomic fields over $\mathbb{Q}$ that time we have proved this and we will use it today.

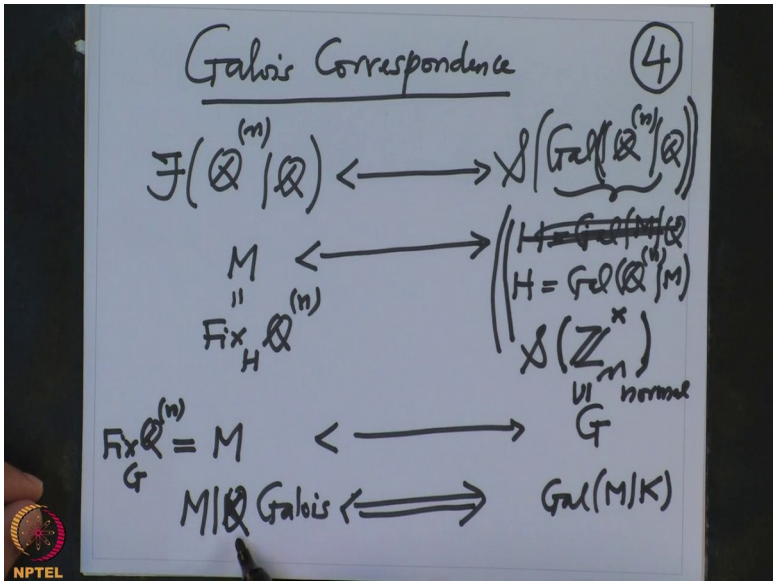
(Refer Slide Time: 6:56)



So let us now state it formally and prove it, so this theorem I am going to prove is. Let G be a finite abelian group then there exist a field L which contains $\mathbb{Q}$ such that L over $\mathbb{Q}$ is a Galois extension with Galois group is equal to the given G, this is what I want to prove, alright. So proof, note that we have proved that if I take the Galois group of the cyclotomic field extension, this is isomorphic to $\mathbb{Z}_n^x$, this is what we have proved and I am going to use this fact also. So this is what, this is the 3rd fact we are going to use, alright.

So, remember that in the last lecture I have also proved that if I take the subgroups here that is subgroups here and the intermediary field extensions, they are all they are in one-to-one correspondence, the Galois correspondence I am going to use the Galois correspondence. So what is that Galois correspondence which states that?

(Refer Slide Time: 9:27)



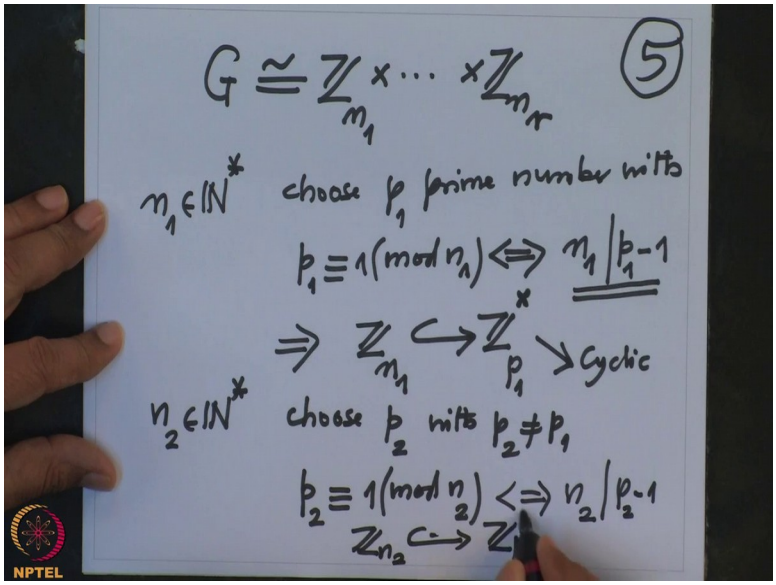
So Galois correspondence, this is also we have checked so on one side intermediary field extensions of the cyclotomic field extensions over $\mathbb{Q}$ and the subgroups of the Galois group this, there is a one-to-one correspondence given a field extension in between here that is M that corresponds to H $Gal\left(Q^{(n)} \vee M\right)$ is clearly from here and how do you recover M from H? This is the fixed field of H, this is it. So now the idea is the following, I have given a finite group G so I have given G, I want to realize this as a subgroup here, this I know this Galois group we know so this is same thing as subgroups of M.. mod n cross you need modular n.

So I want to realize this G as a subgroup here, once I realise that I will get hold of extension M intermediary extension here so this will correspond to that M and when will M over K be Galois that is what we have checked last time, M over K this extension is Galois that will that if and only if the subgroup here should be normal but we have an abelian group so G is always normal here. So this M over K will be a fixed field of this and the G will be realised as therefore Galois group of M over K, so this is the fixed field of G of Okay n so that is how I will do it.

So therefore our problem is, given a finite abelian group I want to realise it as a subgroup of $\mathbb{Z}_n^x$, once I do that I will use this Galois correspondence and that will give me a fixed field and this fixed field is to check the fixed field over this is over $\mathbb{Q}$. This fix field is Galois over Okay, to check that we would have to go back and check this G is normal but normally it is obvious because our field extension our group Galois group of this cyclotomic field extension is abelian so that is a plan. Now given G, I want to realise this as a subgroup of $\mathbb{Z}_n^x$ that is the

main step in the proof okay. So that is how I will use that corollary that there are infinitely many primes.

(Refer Slide Time: 13:12)



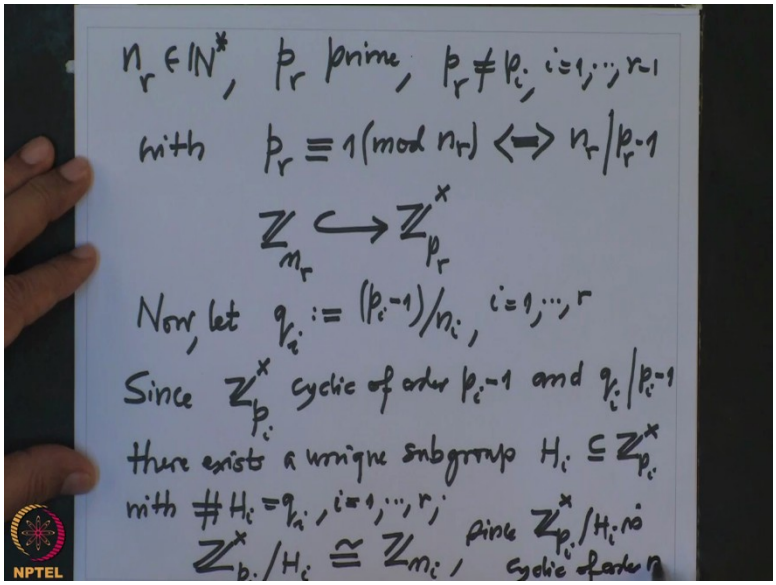
So 1st of all my 1st step I know because G is a finite group, G is a product of cyclic groups that is this, this I will prove after I finish this proof. So this I will prove, this is by this is the structure of the abelian group finite abelian groups okay. Now what do the second say, second say that given any integer any natural number n_1, I will find a prime number p_1 so that so given n_1, n_1 is a nonzero natural number so choose p_1 prime number with the property that p_1 is congruent to 1 mod n_1, but this is equivalent to saying n_1 divides $p_1 - 1$ so that means that means what?

That means if you look at this group so this is further this further implies, so if I look at the group $\mathbb{Z}_{p_1}^{x}$, this is a cyclic group and this $n_1 \vee p_1 - 1$ means the cyclic group has a cyclic subgroup, subgroup of cyclic is cyclic always because n_1 is the order of this group, there will be an element of order there. So that means there is a cyclic subgroup of orders n_1 inside this group so that means this cyclic subgroup of order n_1 is always isomorphic $\mathbb{Z}_{n_1}$ that means this is $\mathbb{Z}_{n_1}$ is subgroup of this.

This follows from this and the knowledge that this is cyclic so given any cyclic group and the divider of the order of that group there is a cyclic subgroup of that order and every cyclic subgroup of that order will look like $\mathbb{Z}_{n_1}$ so therefore this. Now given n_2, I want to choose a prime number, choose p_2 which is different from p_1 with p_2 not equal to p_1 and p_2 is

congruent to 1 mod n_2. This I can do it because I know there are infinitely prime numbers with this property therefore this is only one and I choose a different one now, I want to avoid this p_1. And this is equivalent to saying again n_2 divides $p_2 - 1$ and that will mean that $\mathbb{Z}_{n_2}$ is a subgroup of $\mathbb{Z}^x_{p_2}$, same argument as before and I keep doing this to this given n_1 to n_r.

(Refer Slide Time: 16:45)



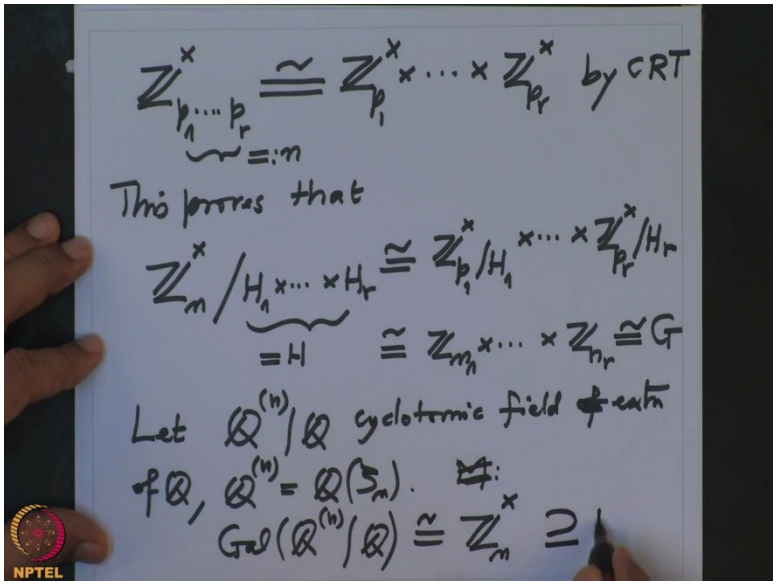
So therefore I have now further number n_r we find prime number p_r prime which is different from earlier chosen primes p_i, i is from 1 to r – 1 with the property that p_r is congruent to 1 mod n_r, this is possible because we had proved earlier that given anyh natural number n there are infinitely many primes so that p is congruent to 1 mod that natural number. This congruence is equivalent to saying that n_r divides $p_r - 1$, so this means in the cyclic group $\mathbb{Z}^x_{p_r}$, this is a cycling group of order $p_r - 1$ and this n_r is a divisor of this so it has a subgroup of order n_r so that is also cyclic because subgroup of the cyclic group is cyclic again that is additive notations so this this goes inside this.

Now, let q_i be the number $\frac{p_i - 1}{n_i}$, we know n_i divides $p_i - 1$, this is for i = 1 to r. And now since $\mathbb{Z}^x_{p_i}$ this is the multiplicative group of a finite field which is we have proved it is cyclic of order $p_i - 1$ and q_i divides $p_i - 1$ therefore, there exist a unique subgroup H_i of $\mathbb{Z}^x_{p_i}$ with cardinality of H_i is precisely q_i, this is for i = 1 to i. Therefore what do you get, this H_i is

subgroup of cyclic group therefore H_i is also cyclic and then we know that $\mathbb{Z}_{p_i}^x H_i$ this will be cyclic of order n_i precisely because $\frac{p_i - 1}{q_i}$ is precisely n_i so this is $\mathbb{Z}_{n_i}$.

This is because since $\mathbb{Z}_{p_i}^x H_i$ is cyclic of order n_i therefore this any 2 cyclic groups of the same order or isomorphic so therefore take this.

(Refer Slide Time: 20:31)

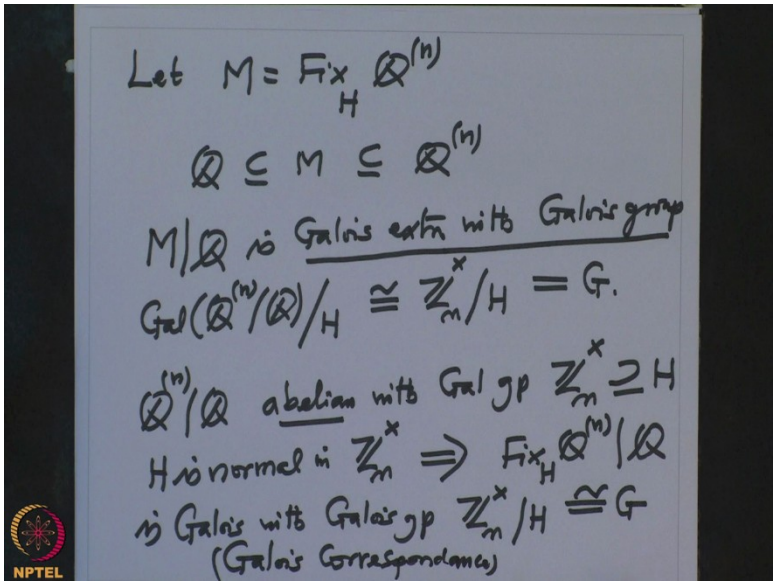


Now you look at $\mathbb{Z}_{p_1}^x$ to p_r, p_1 to p_r are the primes we have chosen, this is by Chinese remainder this is isomorphic to $\mathbb{Z}_{p_1}^x \times ... \times \mathbb{Z}_{p_r}^x$, this is by Chinese remainder Theorem. So this proves what? This proves that this proves that $\mathbb{Z}_n^x$… n is this product of distinct prime. So this modulo H n cross cross H r this is isomorphic to $\mathbb{Z}_{p_1}^x H_1 \times ... \times \mathbb{Z}_{p_r}^x H_r$, but this is precisely $\mathbb{Z}_{n_1}^x \times ... \times \mathbb{Z}_{n_r}^x$ this is precisely our group G given group G. So we have proved that for a given abelian group is isomorphic to the quotient of $\mathbb{Z}_n^x$ for sum n that is what we have proved, where n is product of these distinct primes.

So and remember what we want to do is, we want to find an abelian extension and we want to find a Galois extension of $\mathbb{Q}$ with precisely Galois group G. So now you take you have got hold of this group H, this is our group H which is a product of this group which is a subgroup of $\mathbb{Z}_n$. So let $Q^{(n)}$ over $\mathbb{Q}$ this is a cyclotomic field extension of $\mathbb{Q}$, these are precisely $Q^{(n)}$ is precisely $\mathbb{Q}[\zeta_n]$ where ζ is the root of unity and in that we are taking M to be the fix field of

we know that the Galois group of $Q^{(n)}$ over $\mathbb{Q}$ this Galois group is precisely $\mathbb{Z}_n^x$ and in this there is a subgroup H so we can take fix field of that.

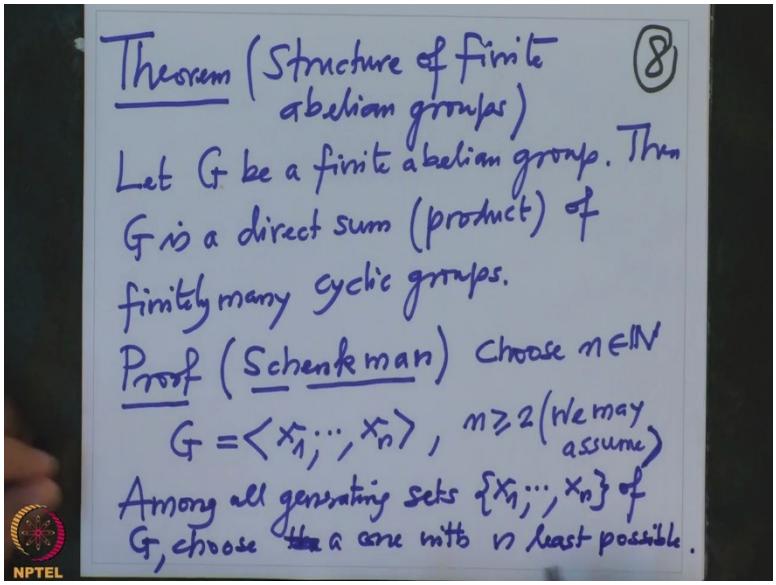
(Refer Slide Time: 23:31)



So let M be the fix field with respect to H of this $Q^{(n)}$ and this M is intermediary field and I want to prove now that M over $\mathbb{Q}$ is Galois extension with Galois group $Gal\left(\mathbb{Q}^{(n)} \vee \mathbb{Q}\right)H$ which is nothing but $\mathbb{Z}_n^x H$ which is the given group G. So we have to justify this is a Galois extension with Galois group, but that is immediate because we know this $\mathbb{Q}^{(n)}$ over $\mathbb{Q}$, this is an abelian extension abelian with Galois group $\mathbb{Z}_n^x$ and H is subgroup here therefore H is normal in $\mathbb{Z}_n^x$ because it is abelian. And therefore we know that this is what the criteria for fix field H $Q^{(n)}$ over $\mathbb{Q}$ is Galois with Galois group $\mathbb{Z}_n^x H$ which is our given group G.

For this we have used Galois correspondence, namely the normal subgroups will correspond to the Galois sub extensions. So that proves that given any finite abelian group we have Galois extension of $\mathbb{Q}$ for which the Galois group is the given abelian group so this was part of the inverse Galois problemh for finite abelian group. Here one can also invoke the big theorem structure of finitely generated abelian group but in this case we did not really necessary and the proof is really simple so I want to indicate this proof so alright, so the theorem I want to prove that theorem

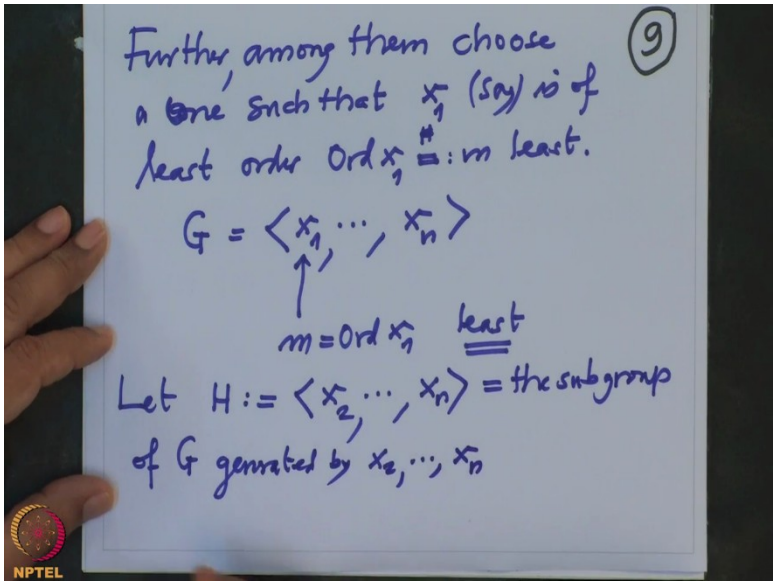
(Refer Slide Time: 26:29)



This is structure of finite abelian groups, so let G be a finite abelian group. Then G is a direct some, remember because we are dealing with finite direct sum so G is a finite abelian group, finite direct sums and finite direct products they are same. Direct product of finitely many cyclic groups, this is what we want to know alright. So that means all the cyclic groups will be isomorphic to $\mathbb{Z}_{n_1}$, $\mathbb{Z}_{n_2}$, et cetera therefore that proves our assertion that we had assumed so I have to prove this. So proof alright, this proof is very interesting proof, this is due to Schenkman. There is a very nice book by Schenkman group theory but it is little unusual book because it is quite difficult to read.

Alright so because G is a finite group, chose a natural number n such that G is generated by these elements x_1 to x_n. If G itself is cyclic than I could choose n = 1 and G is cyclic and we have nothing to proof. So we could always we could assume that n is at least 2 this is we went as you alright so G is generated by x_1 to x_n. Now I am going to choose the generating sets so choose among all generating sets x_1 to $x_n$of G, choose one with n least possible. There may be many generating sets, among them you choose the one which has the least number of elements okay.

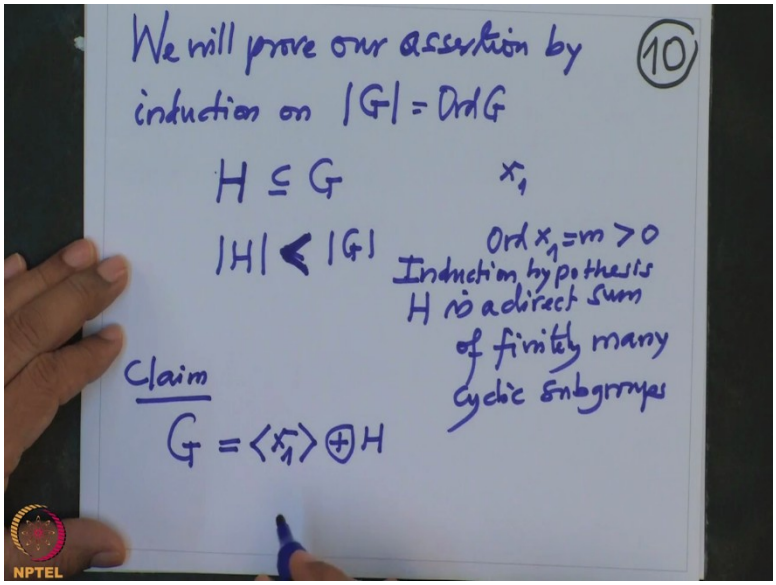
(Refer Slide Time: 30:20)



Now among them choose one such that the first element such that x_1 say is of least order. So we have this we have chosen a generating set which are n elements and n is at least 2 so look at the generators x_1, x_2, etc so on, you get their orders so one of them will have the least order and among all the generating sets we have chosen, choose the x_1 which has the least number of orders. So the order of x_1 which is let us call this as m least, right. So G is generated by x_1 to x_n and this one has order m and this one is the least.

Remember, according to our convention of order of an element, order of an element is always a positive nonnegative integer and in this particular case because G is a finite group obviously the order of all elements are positive, no elements will have order 0. Remember order 0 means the subgroup generated by that has the infinite order, which is not possible here because G we are working and she is a finite group only alright. And what do we want to prove? We want to prove that G is direct sum of cyclic groups so I want to, let H be equal to subgroup generated by x_2 to x_n, this is the subgroup of G generated by x_2 to x_n alright.

(Refer Slide Time: 33:14)

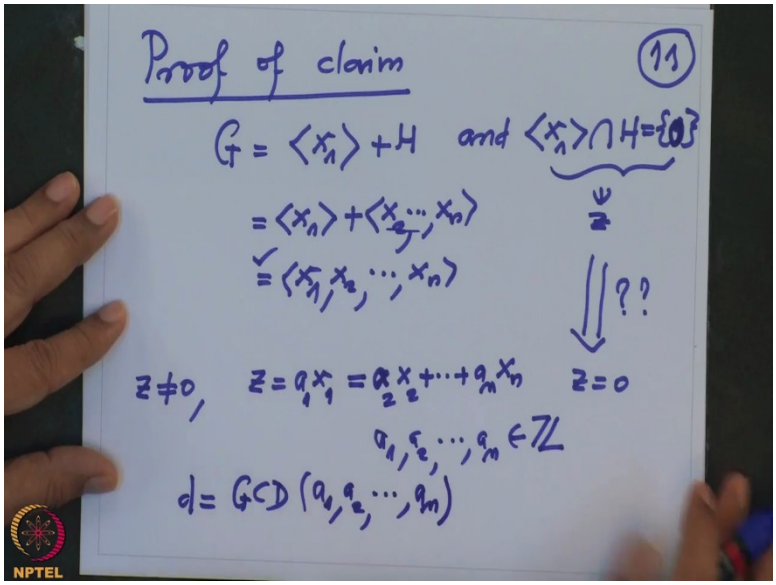


And I am going to prove the assertion so what assertion? We are going to prove, we will prove our assertion by induction on the order of G cardinally we have G, this is the order of G. What assertion, that G is a direct finite direct sum of cyclic groups, this assertion I am going to prove it by induction on the order. Now remember that this the H the subgroup H, H is a subgroup here and what we have dropped is the element of least order and that is that cannot be so the least order element x_1 order is x_1 is m.

This least order m element cannot be identity because if it were identity element then our set is not a minimal generating set for G but we have chosen first a minimal generating set and among them the orders of the generators, then order of x_1 is the least element so therefore this m is positive and therefore this cardinality of H is strictly smaller than cardinality of G because x_1 is not in H and therefore the theorem is true for H therefore H is a direct sum of cyclic, H is a direct sum of finitely many psychic sub-groups. This is induction hypothesis therefore if I prove that the G is direct sum of cyclic group generated by x_1 direct sum H if I prove this so this is what we will claim.

If I prove this claim then we are done because this is cyclic already by notation, this is cyclic group generated by x_1 and H is the direct sum of cyclic finitely many cyclic subgroups so G will be altogether direct sum of finitely many cyclic subgroups so G will be altogether direct sum of finitely many cyclic subgroups so only I have to prove the claim.

(Refer Slide Time: 36:03)

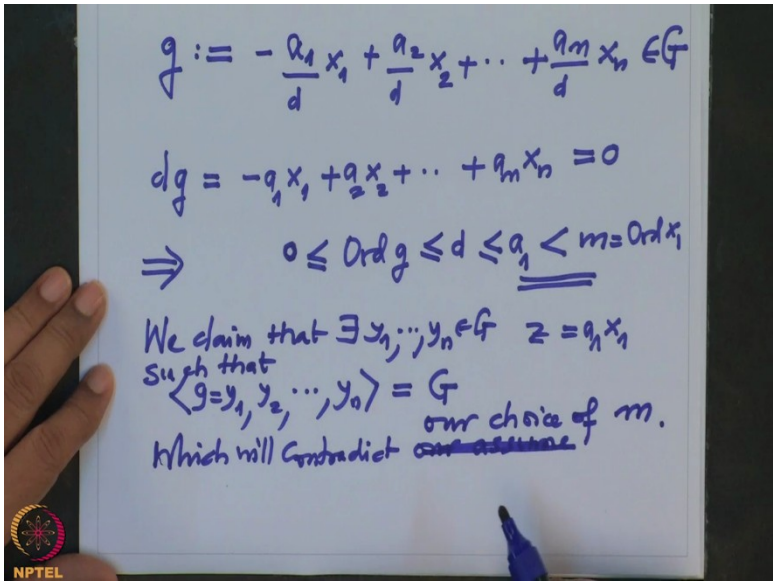


So proof of the claim, this is proof of the claim. So I have to prove 2 things; G is the sum of these 2 groups and I have to prove that they do not intersect other than identity. $\langle x_1 \rangle$ intersected with H is only the identity element which I am denoting by 1, this is what I have to prove. So this one is obvious because H is generated by x_2 to x_n and G is also generated by this is same thing as generated by $x_1, x_2, \ldots, x_n$, this was given to us already we have chosen like that so I have to prove only this. So let us take element which is common so let us take z belongs to here and we want to show that this z is actually 0 element, this is what we have to show.

So look at z, on 1 end if z is nonzero we should get a contradiction. So on one end z is a multiple of x_1. Oh I have written the groups as additive groups so therefore this identity I should write it 0 not 1. So if z was nonzero, on one end it is a multiple of x_1 so z will be $a_1 x_1$, adding x_1 cyclic so group generated by x_1 means adding $x_1 a_1$ times. On the other hand, it will also be an element of H so it will be a z linear combination of elements from x_2 to x_n, so $a_2 x_2 + \ldots + a_n x_n$, where $a_1, a_2, \ldots, a_n$ they are integers, alright.

Now let us take d with a GCD of integers $a_1, a_2, \ldots, a_n$ and divide, so once I take this then what do I get?

(Refer Slide Time: 38:32)

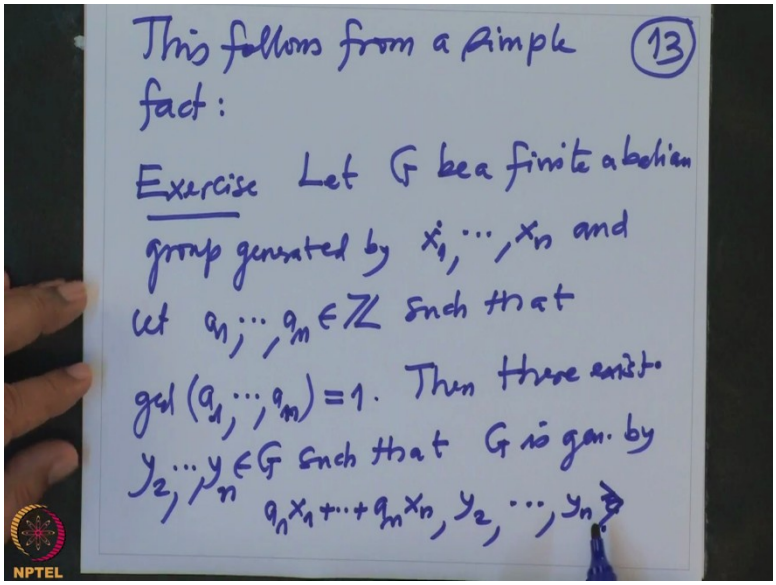


Let us call g element g which is by definition and I am writing it as –… I want to shift this term to this side so that will become $-\frac{a_1}{d}x_1+\frac{a_2}{d}x\,2+...+\frac{a_n}{d}x_n$, consider this expression this is an element in the group g, alright. And if I multiply by d what happens, that means if I add g d times what happens, d times g is nothing but $-a_1x_n+a_2x_2+...+a_nx_n$, this element is 0 because we have taken this as z and then I have subtracted, this is 0 that means what? That means the order of this element g what can it be?

It has to be smaller than equal to d, this is smaller than equal to d, this is smaller equal to d and d is smaller equal to a_1 and a_1 is strictly smaller than m because z is a_1x_1 and this m is order of x_1 so therefore this a_1 is bigger, then I could always reduce it to the smaller element so therefore we have this a_1 is smaller than this and order of g is bigger equal to 0. So therefore, I found an element g in the group g whose order is strictly smaller than that m, so now if I could check that if I could check that there is an element with.

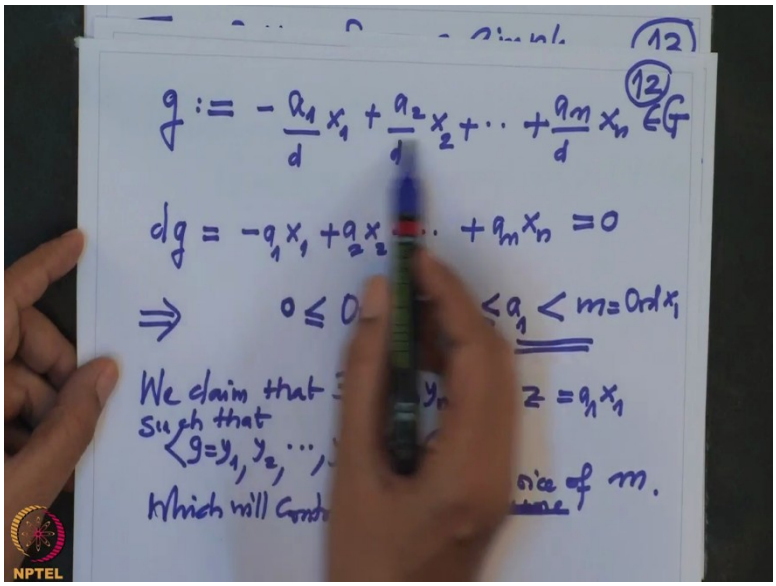
If I can find a generating set with g here, g is $y_1, y_2, \ldots, y_n$, if I can find such a generating set I will get contradiction to our choice of generating set where one of the elements has order strictly less I found, so we claim that now. We claim that there exist $y_1, y_2, \ldots, y_n$in G such that this is a generating set for G, which will contradict our choice of that m, m is the least among all the orders of the elements which the generating set for G. And what is this? This is very simple, I have will just treat it as a result and then one can prove it very easily, so the result is the following which follows from the following.

(Refer Slide Time: 42:20)



This follows from a simple fact, so what is the fact? So that is I want to write it as an exercise. Let G be finite abelian group generated by $x_1,\ldots,x_n$ and let a 1 to a n are integers such that GCD of $a_1,\ldots,a_n$ is 1, then there exist $y_2,\ldots,y_n$ in G such that G is generated by 1st element is this linear combination $a_1x_1+\ldots+a_nx_n$, $y_2,\ldots,y_n$, this is G generated by this.

(Refer Slide Time: 44:02)



So that is precisely what we wanted to prove because in our case G is this linear combination and GCD is 1 because G is GCD of $a_1,\ldots,a_n$ and therefore the GCD of this coefficient is 1 therefore I will find a generating set where G is one of the elements that is what we wanted to claim. So this is a very simple exercise, this follows from the fact that when you have n integers, if the GCD is 1, 1 is a linear combination of those elements, 1 is z linear

combination of $a_1,\ldots,a_n$ that is precisely the minimum GCD is one. So using that one can prove this exercise very easily by induction on m, so I will leave that proof for you to check and with this I will end this lecture and in next we will continue our discussion on the Galois groups in the next one. Thank you.