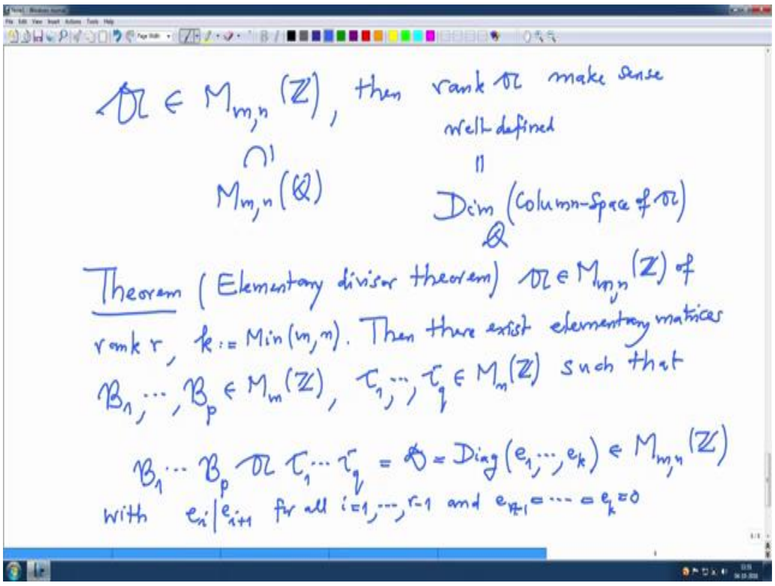
Linear Algebra
Prof. Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore

Lecture – 47
Elementary Divisor Theorem

So, first with this introduction, I want to state a theorem which is known as elementary divisor theorem and you will know also why is it called elementary divisor theorem. This is elementary divisor theorem.

(Refer Slide Time: 00:29)



$\mathfrak{A} \in M_{m,n}(\mathbb{Z}) \subseteq M_{m,n}(\mathbb{Q})$, then rank $\mathfrak{A}$ make sense well-defined $= \operatorname{Dim}_{\mathbb{Q}}$ (Column-Space of $\mathfrak{A}$)

Theorem (Elementary divisor theorem) $\mathfrak{A} \in M_{m,n}(\mathbb{Z})$ of rank r, $k := \operatorname{Min}(m,n)$. Then there exist elementary matrices $\mathfrak{B}_1, \cdots, \mathfrak{B}_p \in M_m(\mathbb{Z})$, $\mathfrak{C}_1, \cdots, \mathfrak{C}_q \in M_m(\mathbb{Z})$ such that

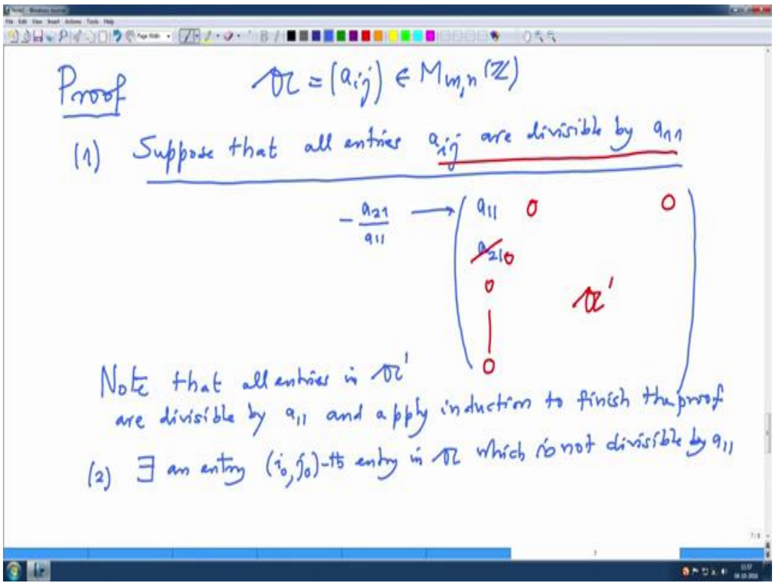
$$\mathfrak{B}_1 \cdots \mathfrak{B}_p \mathfrak{A} \mathfrak{C}_1 \cdots \mathfrak{C}_q = \mathfrak{D} = \operatorname{Diag}(e_1, \cdots, e_k) \in M_{m,n}(\mathbb{Z})$$

with $e_i \mid e_{i+1}$ for all $i = 1, \cdots, r-1$ and $e_{r+1} = \cdots = e_k = 0$

So, we have a matrix A, M m n; m cross n matrix with integer entries of rank r, this means rank has a q matrices; a as a q matrix it has a rank r and as usual in earlier theorem I will use similar notation k is the minimum, min m comma n then there exist elementary matrices B 1 to B p with integer entries Z and also C 1 to C q with integer entries square matrices elementary is always square matrices such that when I multiply the given matrix a on the left by B 1 to B p; that means, I am making a row operations on a according to these elementary matrices and if I multiply by from the right by C 1 to C q, this makes sense; these multiplication makes sense because I have taken correct order. So, that; that means, making a row column operations on a and then there is (Refer Time: 02:44) matrix I give it to the diagonal matrix D which has the diagonal entries e 1 to e k.

Which is an integer entries M n Z this is (Refer Time: 03:09) matrix is M n m m cross n because correct orders n. So, this e 1 to e k are integers with you can say even more with each e i divides a next 1 e r plus 1 for all i from 1 to r minus 1 and the remaining guys are 0 e r plus 1 e k r 0 because the ranks are equal now. So, the rank will not change if I multiply it by elementary matrices on the left or right because elementary matrices are actually having determinant 1. So, they are actually invertible matrices are integers. So, these e's are called elementary and then I will explain this after we prove this theorem. So, this is what we want to do so; that means, again what are we looking for we are looking for elementary column and row and column operation are given matrix a to make it a diagonal matrix and now you see we are not allow to cancel we are not allowed to invert make a use of the fact that dividing by integers that is not allowed because we want to remain within integers all right. So, what is the procedure? Let us start.

(Refer Slide Time: 04:59)



Proof $\mathfrak{A} = (a_{ij}) \in M_{m,n}(\mathbb{Z})$

(1) Suppose that all entries a_{ij} are divisible by a_{11}

$$-\frac{a_{21}}{a_{11}} \rightarrow \begin{pmatrix} a_{11} & 0 & & 0 \\ \cancel{a_{21}}0 & & & \\ 0 & & \mathfrak{A}' & \\ | & & & \\ 0 & & & \end{pmatrix}$$

Note that all entries in $\mathfrak{A}'$ are divisible by a_{11} and apply induction to finish the proof

(2) $\exists$ an entry (i_0, j_0)-th entry in $\mathfrak{A}$ which is not divisible by a_{11}

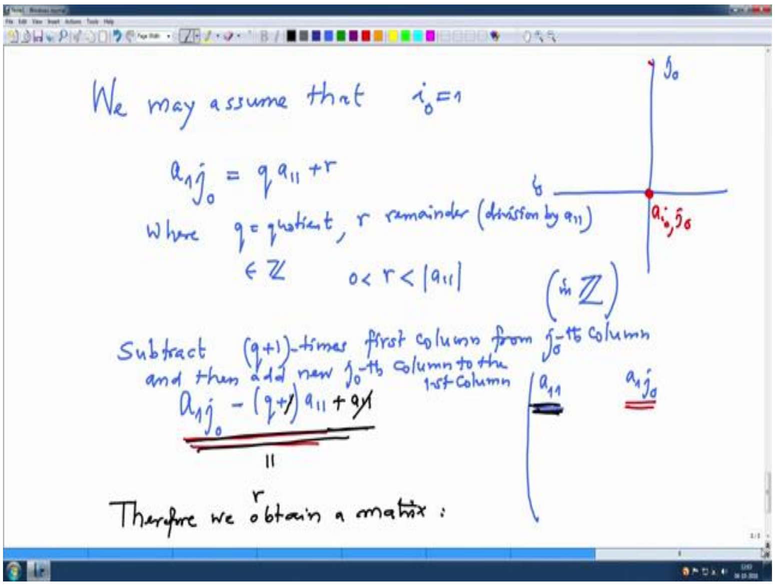
So, I will first. So, proof is very easy if you do it with a systematic care. So, the first thing I will make some assumption on the entries. So, suppose that all entries. So, given matrix A is a i j; a i j where integers suppose that all entries a i j are divisible by the top entry a 11, we are making under this assumption now and later on we will relive this assumption.

So; that means, what let me draw day a picture here of a matrix. So, a 11 is here and this guys divides all the entries then from I want to kill this. So, that is very easy now because this guy divisible by this. So, this entry is a 21. So, this one it divisible by this, so I am going multiply this column this row by a 21 divided by a 11 by this minus of that and add it to the next row. So, that way I will make this entry to be 0 and similarly all these entries; I will make it 0 and this assumption is very very important because this is; I get only integers if that does not divide then I cannot use this operation because then in that case I will not remain in integer matrices, I will go out of that. So, this and similarly I will make a column operation. So, that these guys are 0 and therefore, we will get matrix here a prime, a primes order is reduced, 1 row is reduced, 1 column is reduced and also note that in all entries what will happen to the entries of a prime they will be the combination of the entries of these and this guys. So, they will again be. So, a further note that all entries in a prime I have also the same property are divisible by a 11.

And therefore, I will apply induction and apply induction to finish the proof what proof that by row and columns operation we can make a given matrix over integers into a diagonal matrix and then we will worry about those conditions on the diagonal entries of a see we still have some condition to check the diagonal entries we have these properties. Now, therefore, we are in next case that is the case where this is not true; that means, there is some entry in a matrix who is not divisible by a 11. So, this means there is an entry say call it i naught j naught th entry.

In the matrix a which is not divisible by a 11, some entries somewhere which is not divisible by a 11 then what you do in that case? So, it is somewhere here. So, I want to bring it to this position first I will inter change that to the row the first row and it will come in the first row that means.

(Refer Slide Time: 10:30)



We may assume that $i_0 = 1$

$a_{1j_0} = q a_{11} + r$

where q = quotient, r remainder (division by a_{11})

$\in \mathbb{Z}$ $\quad 0 < r < |a_{11}|$ $\quad$ (in $\mathbb{Z}$)

Subtract $(q+1)$-times first column from j_0-th column and then add new j_0-th column to the 1-st column

$$\underline{\underline{a_{1j_0} - (q+1)a_{11} + a_{11}}}$$

$$\|$$

$$r$$

Therefore we obtain a matrix :

So, we may assume that i naught is 1 that was any entry in i naught th row and j naught th column, here this was this was a entry here which means a i naught j naught. So, I will inter change this i naught through the first row and I would bring it here that is allowed because we are allowed to do row and column operations. So, that entry has become now in the new notation i naught is 1. So, it is a 1 j naught and these entry is not divisible by 11. So, what can I do? I divide; I use a divisional algorithm to divide this entry by a 11 and take a quotient and remainder. So, write this as q times a 11 plus r where q is a quotient and r is a remainder.

Of the division by division by when you perform division by a 11 and both are this is integer both are integers and normally that the I can assume this r is in between 0 r cannot we 0 because a 11 does not divide r is less, then it is bigger than 0 and less then the modulus of a 11, this is how the division algorithm is used in the ring Z, similar these an algorithm you can use it for the polynomial ring (Refer Time: 12:45) ring etcetera, etcetera more generally the (Refer Time: 12:48).

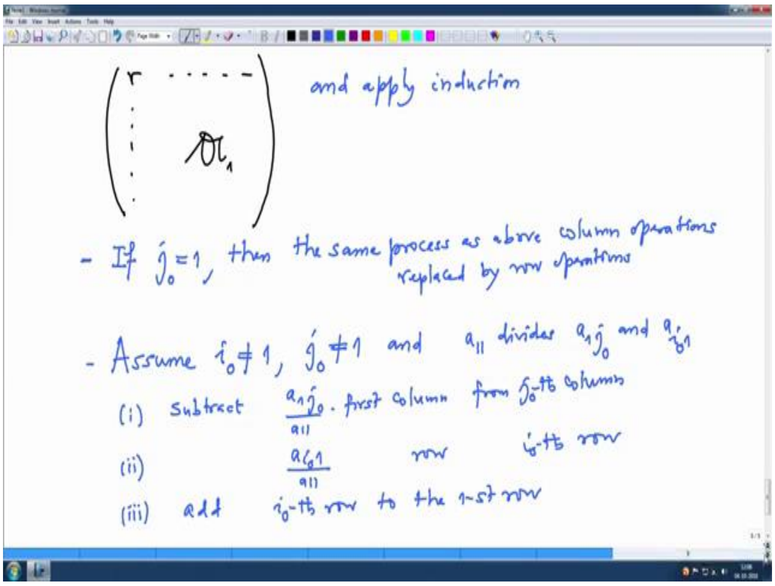
Now, what is the next procedure? Now I want to subtract. So, subtract q plus 1 times first column from j naught column, I want to use this operation.

So, what does; what will these do? So, what is the first column is the entry here is. So, let me write again the first column entry here is here was a 11 and here is somewhere a 1 j naught. So, we are going to multiply this column the first column by q plus 1. So, and subtract it from here. So, these entry here what will it become a 1 j naught minus q plus 1 a 11. So, I will get this entry here. So, this entry will become this entry, if I do this operation, but after this I will write here and then add new; I will get a new column here.

This new column; this new j naught th column; I will add it to the first one and then add new j naught th column to the first one to the first column. So, let me repeat what did you do we are multiplied this column by q plus 1 and subtract from the j naught th column, now you get a new j naught th column that new j naught th column, I am going to add it the first column; that means, the new entry in the first column here this entry, let me use the black color, this entry will become further here I will add it to a 11, this will be the new the entry here, but these entry is what this is precisely r the remainder because this is because of this equation this is a 11 these will get cancelled with this and we are left to this and that is precisely the r. So, therefore, I have reduced this size, I reduce the modulus of this a 11 is clear

So, therefore, what do we obtain let us write their result therefore, we obtain a matrix following form r is here somebody is in the first column first column here and there is matrix a 1 here.

(Refer Slide Time: 17:10)



$\begin{pmatrix} r & \cdots \\ \vdots & \mathcal{A}_1 \end{pmatrix}$ and apply induction

- If $j_0 = 1$, then the same process as above column operations replaced by row operations

- Assume $i_0 \neq 1$, $j_0 \neq 1$ and a_{11} divides a_{1j_0} and a_{i_01}

(i) subtract $\frac{a_{1j_0}}{a_{11}}$. first column from j_0-th column

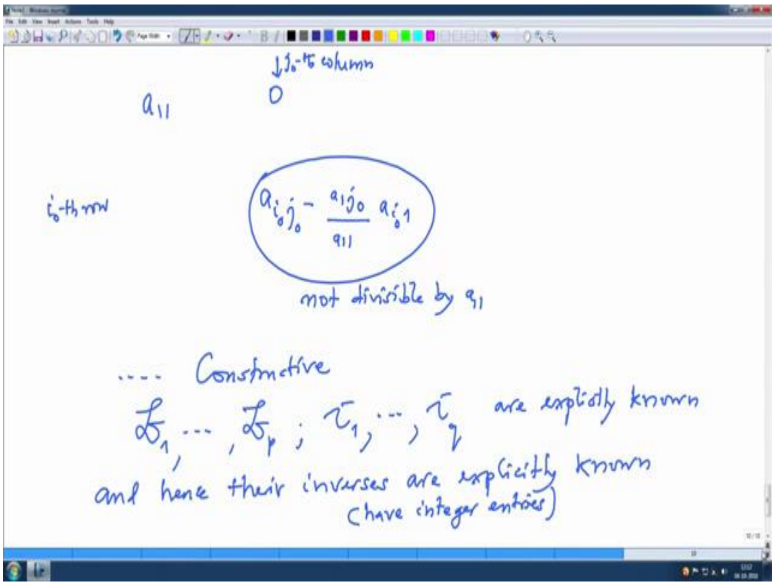
(ii) $\frac{a_{i_01}}{a_{11}}$ row i_0-th row

(iii) add i_0-th row to the 1-st row

And apply induction I will say and apply induction similar process if that j naught see there was a j naught also know if. So, this are this are the cases we have to put them altogether. So, if j naught is also one then. So, here in case of just let me remained you in case of i naught i 1, we have performed column operations if this was the first column the j naught was first and somewhere entry below if i naught is 1, apply these if j naught where one then it will be the entry in the row and then I will apply row operations. So, j naught is 1 then the same process as above columns replaced by rows column operations column operations replaced by row operations in any case the top entry will be will be smaller, then a 11 magnitude also now if assume both i naught is not 1 and j naught is also not 1 and a 11 divides both this entry a 1 j naught and a i naught 1, there I will make three possibilities three possibilities are 1, 2, 3.

What are the possibilities? Again I will subtract. So, subtract because of this what will a 1 j naught divided by a 11 times first column from j naught th column and this one is now instead of rows and I have to write the corresponding statement here a i naught 1 divide by a 11 first row form i naught th row and add i naught th row to the first row. If you do this if do this operation then what do you get? So, let us write the result and may be which is here to you see what do get?

(Refer Slide Time: 21:57)



$$a_{i_0 j_0} - \frac{a_{1 j_0}}{a_{11}} a_{i_0 1}$$

not divisible by a_{11}

.... Constructive

$\mathcal{L}_1, \dots, \mathcal{L}_p ; \tau_1, \dots, \tau_q$ are explicitly known

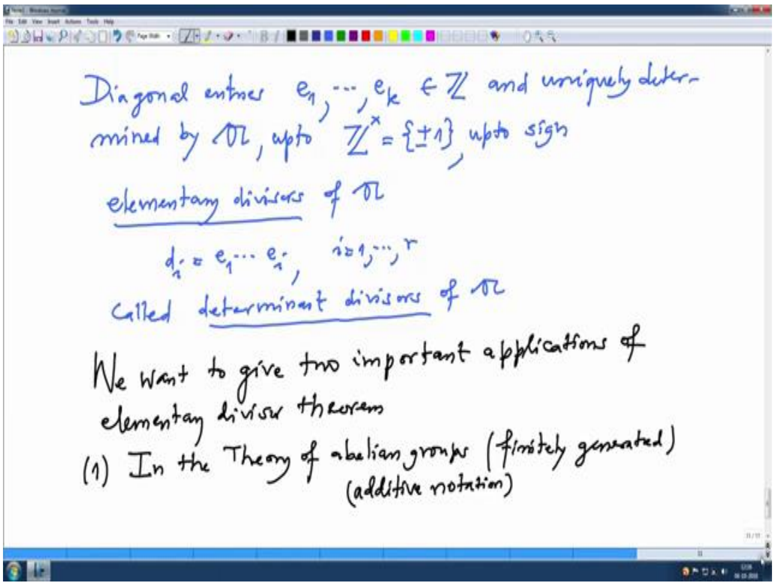
and hence their inverses are explicitly known (have integer entries)

So, I will write a final answer. So, we will get; so original entry was a 11 here and we will get 0 here this is a j naught column and similarly you will get.

So, what will be the entry here v in i naught th row the entry here will be here it is a i naught j naught minus a one j naught divided by a 11 and a i naught one and now this entry here is not divisible by not divisible by a 11, since a 11 does not divide this and divide this. So, we will the matrix with this here that will become a case one that it does not divide and then we are we will apply induction. So, you see the i d i is to reduce the magnitude of the entries and which is this prove is. So, whatever after that we are going to get after this operation we are going to get a diagonal matrix this process here is very constructive.

In particular, we will also know this operation very precisely namely we will know this matrices says B 1 to B p and C 1 to C q this matrices says this elementary matrices are explicitly known are explicitly known because a only one entries of diagonal we have to know it and that we know that exact procedure we are applying. So, once we know them we also know their inverses explicitly and hence their inverses are explicitly known because inverse of the elementary matrix is very easy by whichever entries of diagonal the inverse is want to find just replace that entry by minus of that and then it become the inverse of that elementary matrix and all these inverses also have r, r matrices have integers entries because the inverses are nothing, but which ever entry was non 0 you replace by that minus of that.

(Refer Slide Time: 25:51)



Diagonal entries $e_1, \ldots, e_k \in \mathbb{Z}$ and uniquely deter-mined by $\mathfrak{A}$, upto $\mathbb{Z}^{\times} = \{\pm 1\}$, upto sign

elementary divisors of $\mathfrak{A}$

$d_i = e_1 \cdots e_i$, $i = 1, \ldots, r$

called determinant divisors of $\mathfrak{A}$

We want to give two important applications of elementary divisor theorem

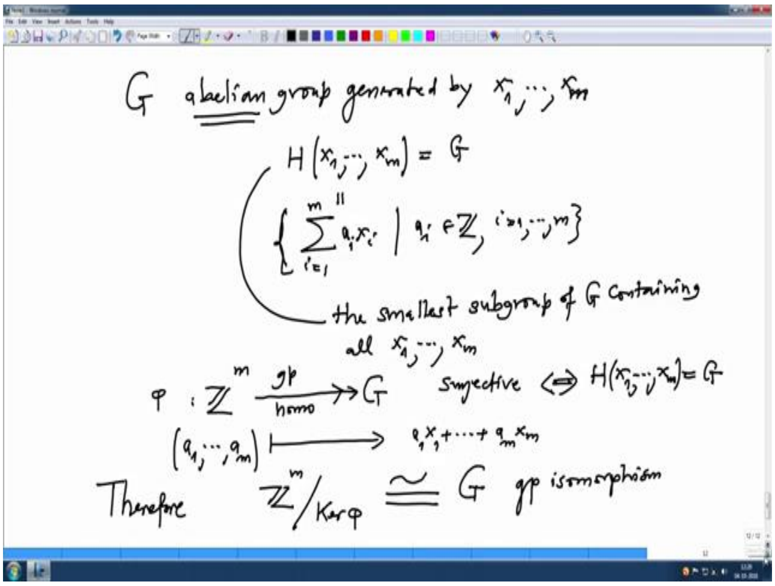
(1) In the Theory of abelian groups (finitely generated) (additive notation)

Then what did we do? So, therefore, the integers that diagonals the diagonal entries which we are calling it e 1 to e k their integers and also they are uniquely determined by the matrix a possibly up to element in Z cross which is plus minus 1 that is up to sign up to sign this e 1 to e k uniquely determined up to the sign and this e 1 to e k.

They are called elementary divisors of a and the products their products d i is their products up to i e 1 to e i and that can be up to i from 1 to r because the later products are 0. These products are called; these are called determinant divisors of a this, what determinant will be explained, later when we have introduce the determinants. So, again the explicit the precise proof of the statements with all the case, I will write in the notes where one can check all the details more precisely, but now I want to give 2 applications 2 important applications we want to give 2 important applications of elementary divisor theorem.

So first one this is in the theory of Abelian groups in the theory of Abelian groups and finitely generated. So, I will write Abelian groups as additive groups additive notation.

(Refer Slide Time: 29:24)



G abelian group generated by $x_1, \dots, x_m$

$$H(x_1, \dots, x_m) = G$$

$$\Big\| $$

$$\left\{ \sum_{i=1}^{m} a_i x_i \;\middle|\; a_i \in \mathbb{Z}, i = 1, \dots, m \right\}$$

the smallest subgroup of G containing all $x_1, \dots, x_m$

$$\varphi : \mathbb{Z}^m \xrightarrow[\text{homo}]{\text{gp}} G \quad \text{surjective} \Leftrightarrow H(x_1, \dots, x_m) = G$$

$$(a_1, \dots, a_m) \longmapsto a_1 x_1 + \dots + a_m x_m$$

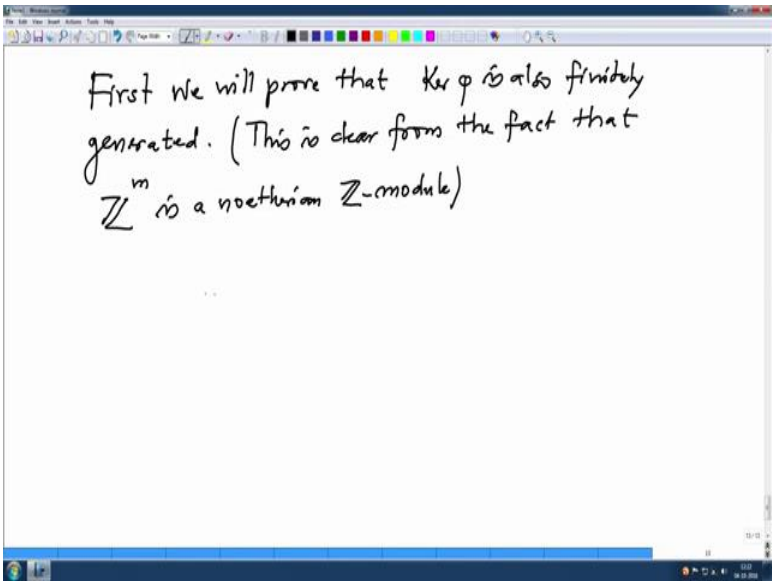
Therefore $\mathbb{Z}^m / \text{Ker}\,\varphi \cong G$ gp isomorphism

So, let us start with an Abelian group G. So, G Abelian group generated by finitely mini elements, let me call it x 1 to x m, this means this means the smallest subgroup generated by this x 1 to x m is G and the smallest subgroup which contain all the x 1 to x m are precisely the Z linear combinations of this x one to x m with integer coefficients a 1 a i x i i is from 1 to m where a i's are integers. This is the smallest the smallest subgroup same terminology, what we have been using for vectors spaces of G containing all x 1 to x n, this is the meaning of G generated by x 1 to x m; that means, very element of G in G is of combination of x 1 to x m with integer coefficients what does that mean that mean let us convert it to maps.

So, this means we have a group here the product group Z n Z m and we have a group G here and we have a natural map here these map is given by this excise. So, where the m tuple go x 1 to x m, a 1 to a m integer tuple m tuple goes to the combination a 1 x 1 plus, plus, plus, plus, plus, plus a m x m.1 This is a group of homomorphism that you can easily check from the fact that it is an Abelian group and because it is generated, this is G generated by x 1 to x m; that means, this map is surjective. Surjective is equivalent to saying that the smallest subgroup is G. So, we have a map from Z m to G, this is a group, this is an Abelian group which has a basis namely the standard basis G may not have a basis. So, we cannot talk about rank etcetera and so on. So, this map is surjective whenever we have a surjective map there is a kernel and the isomorphism. So, therefore, if I go mod the kernel, so let us call this map as phi.

So, Z power m module the sub group kernel is isomorphic to the image, but the image is G this is a group isomorphism so; that means, we have proved that any finitely generated Abelian group is a isomorphic to the quotient group of Z; Z power m module the kernel. Now first I want to note that this kernel is also finitely generated. So, and once it is finitely generated, I will choose generating set for that and do something with the generating set.

(Refer Slide Time: 33:52)



First we will prove that Ker φ is also finitely generated. (This is clear from the fact that $\mathbb{Z}^m$ is a noetherian $\mathbb{Z}$-module)

So, first we will prove that kernel phi is also finitely generated in group there is a no reason for a subgroup to be finitely generated there are examples of non Abelian groups and subgroups where the groups may not subgroups may not be finitely generated. Even if the group is finitely generated, but an Abelian group in this is very special situation well this also is clear form. So, this is those who know little bit more algebra this is clear from the fact that (Refer Time: 34:50) Z power m is a Noetherian Z module because if it is Noetherian means finitely generated and all sub modules are also finitely generated and kernel is a sub module of a Z power m and Z power I mean Noetherian. Therefore, kernel is finitely generated, but I want to give a proof which is simpler, this we will do it next time.

Thank you very much.