Lecture No. 58

Fractionary Ideals and Dedekind Domains

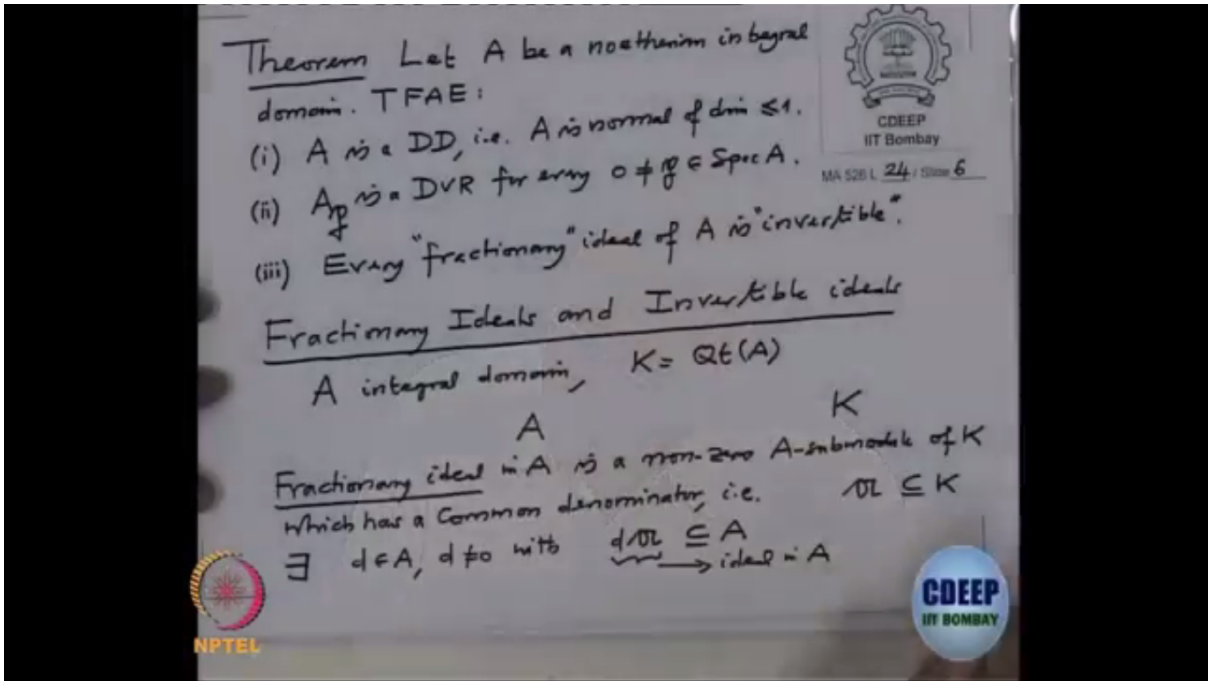
Gyanam Paramam Dhyeyam: Knowledge is Supreme.

Okay, so now the theorem I want to prove about Dedekind Domains is the following. We will go little bit backwards. So this is the theorem I want to prove. This will characterize and this will also. Yeah, is the characterization of Dedekind Domains, so let A be a noetherian integral domain in the following or equivalent. One, A is DD, Dedekind Domain, that is normal of dimension less equal to 1. Two, AP, every localization, A localized P is a DVR for every non-zero prime ideal. And third, these are the new terms, every factionary ideal of A is indivertible. So I will define these terms. And then we will prove the equivalence of this. And as a corollary we will deduce the theorem that I mentioned that every ideal is a product of prime ideals. You know, essentially in [02:40 inaudible] in a Dedekind Domain.

Okay, so let us [02:44 inaudible] a little bit about Fractionary Ideals and Invertible Ideals. So Fractionary Ideals and Invertible Ideals. So we will assume always A is an integral domain and K is its coefficient field. So we have K here, we have A here. Fractionary Ideal means, so this should correspond to the fractions in the usual integers. So that means they are elements of, and fractions are elements. So fraction is ideals, it should be the ideals corresponding to the fractions, right. So, fractionary A ideal means, fractionary ideal in A is a non-zeros of module, A sub-module of K which has a common denominator which has a common denominator. That simply means that is, it's a sub-module. I keep writing a, this is not an ideal.

So it's a sub-module of K and it has a common denominator means, if I multiply by that it should goes inside A. So there exit d, non-zero. d in A, d non-zero with d times this [05:15] a is contained in A actually. So that means this d times a is actually an ideal in A. So this A is may not be an ideal, it's a sub-module of K, but if I multiply by 1, non-zero element it becomes an ideal [05:34 inaudible]. So this is ideal in A.

(Refer Slide Time: 05:38)



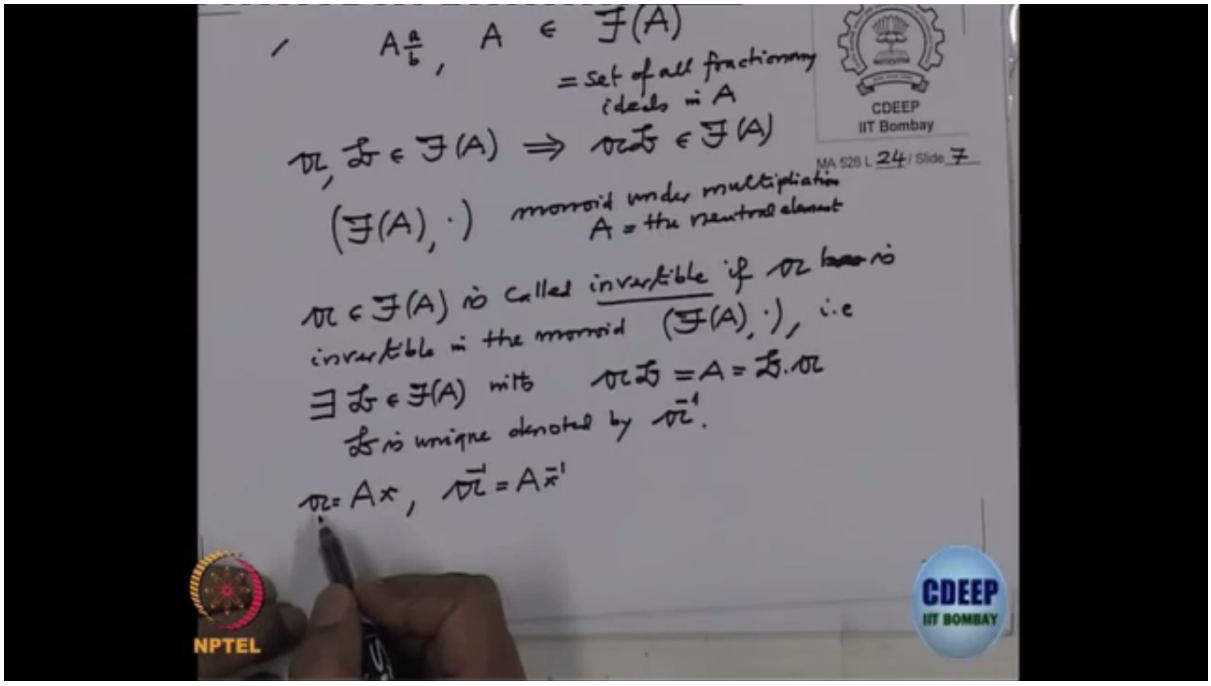
All right. So that is a fractionary ideal. Now there is, look at [05:46 inaudible] properties of the fractionary ideals. First of all, if A is a fraction, so I will introduce a notation fraction, ideals usually denoted by F of A, this is a set of all fractionary ideals in A. All right. So obviously the principle, the sub-module of K generated by one element there obviously fractionary ideal because that denominator really the denominator. Also the ideal, the sub-module A, A sub-module A is also fractionary. So A is an element here, also the principle sub-module, the cyclic sub-modules, a by b. This is also fractionary because this b is a really denominator.

More generally if I have two fractionary ideals a and b then their product is also fractionary ideal. a times b is also fractionary ideal. A times B makes n because everything is happening in the field K, so the product is the, see, normally you cannot multiply two sub-module, a two modules. But these are very special module that contained in K. So if d is a common denominator of A, d prime is a common denominator of B then d times, d prime will be common denominator of the product. Okay, so the product. Okay, so therefore this one, this F(A) with the product, this becomes semi-group. Semi-group simply means that this product operation and it is associative. But it is more than a semi-group, it also have the identity element, namely A is an identity element. So this is indeed a monoid under multiplication. A is an identity element or it is a neutral element.

So whenever we have a monoid we look at the elements in that monoid which are invertible. So those guys are called invertible ideals. So the name also is very clear. So and fractionary ideal in F(A) is called invertible if a is invertible in the monoid F(A) under multiplication. So what does that means, so that is there exist an element b here, so that the product is a, so that is their exit. Another fractionary ideal b in F(A) with a times b equal to A also it is b times a. And such a 'b" will be unique then and that unique is denoted by a inverse. So that b is unique denoted by a inverse.

So we want to guess who is this b in terms of a and that will be, so for example, if your fractionary ideal where principle generated by x, let me call it. Suppose this has a principle fractionary ideal. Then who will be the inverse of A, then obviously a inverse will be generated by x inverse. x inverse make [10:49 inaudible] this x is a non-zero element. So a, the zero ideal cannot be fractionary ideal.

(Refer Slide Time: 10:57)



So therefore this is the, so you want to guess a will be the inverse, so obviously, so we have given this a fractionary ideal. So note that, so we want somebody whose product with that is equal to A. So look at this colon operation, (A:a), this is what, this is by definition, all those elements in the coefficient field, this is happening in the coefficient field, because A is a sub-module of Q, so all those elements in the field such that when I multiply by this ideal will get inside A.

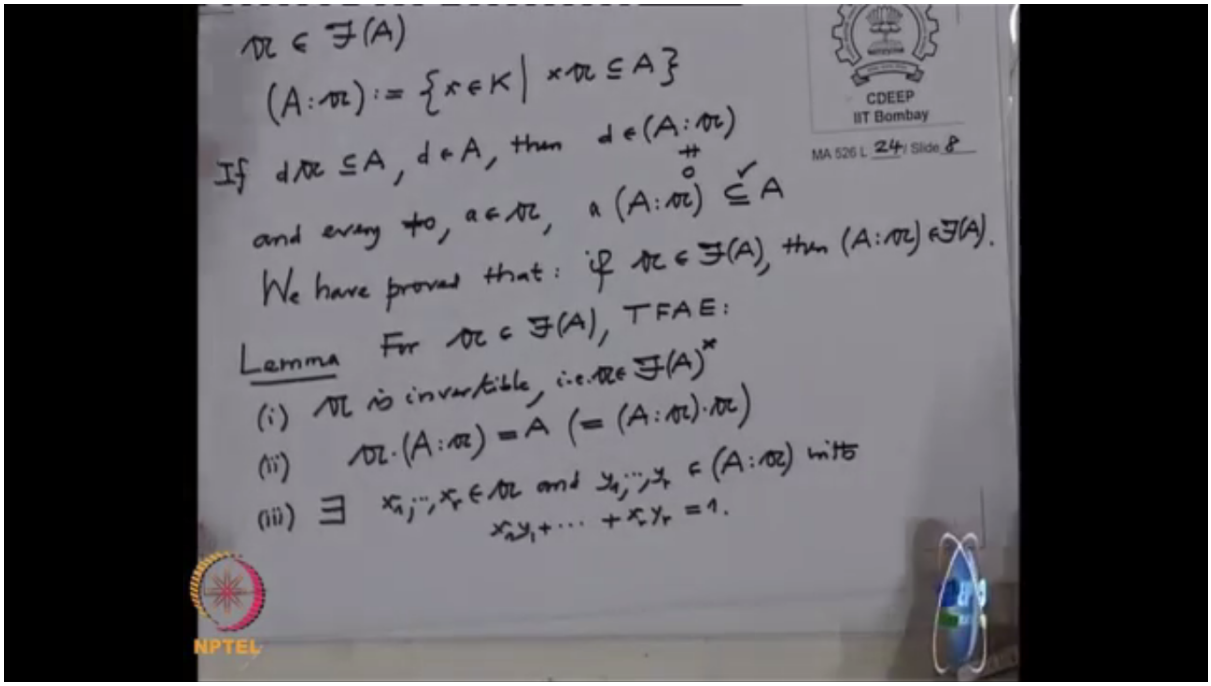
So x times a is contained in A. This is the colon ideal. So first of all note that this is again fractionary. So to say that it is again fractionary, what we have to show, it also has a common denominator. So give a common denominator of "a". We want to find a common denominator for this. So that is, suppose you have given d which is a common denominator for A, that means, d times a is contained in A. So suppose if for some d in A is, then what does it means? So that means, this d will belong to this colon ideal and then this is non-zero in particular this colon ideal is non-zero because d is there. Now element of A [13:05 inaudible] it is a common denominator for this colon ideal.

Then and every non-zero element a in A is common denominator for this. That means, what should I check? That this A times a colon ideal should be contained in A but that is obvious. So therefore, every non-zero element is a common denominator. So what did we proved? We proved that assuming A fractionary ideal, this colon ideal is also a fractionary ideal. So it is, so we have proved that if a is a fractionary ideal then colon A is also a fractionary ideal. So obviously we want to now check that this guy is the right inverse. This A colon, [14:18 inaudible] ideal, this A colon [14:19 inaudible] a, this is

the inverse of this. This is what we would like to check. Because this is a candidate and also the product is contained in A, so therefore we will prove the following lemma.

All right. So for fractionary ideal the following are equivalent. One, a is invertible. So just to remember that, that is F(A), A belongs to F(A) cross A. Remember that was our standard notation to denote units in a monoid in general. This one, two is this gothic a times the colon A, this product is actually equal to A. If you prove this then this has to be the inverse of this because the operation is commutative, so this will also become equal to this or you can use, instead of a you can replace this a by the colon ideal a and then it is the colon of colon A colon a will be a. So this two, three is. So what does this mean, this equality should mean what? This product is A that means, one should be a combination of this. So there exit some elements, x1 to xr in the gothic a and y1 to yr in colon with the product x1y1 plus, plus, plus xr yr equal to 1.

(Refer Slide Time: 16:52)



So further, just to summarize of this three and then we will prove all the equivalent. So further, if any one of one, two, three holds then a inverse equal to A colon a and a is generated as a module by this x1 to xr and inverse is generated by y1 to yr. This is generated by y1 to yr. So proof, we will prove one implies, two implies, three implies one. All right, so one means it's invertible. And two means, A times the colon, A colon gothic a is equal to a. So a is invertible given, suppose a is invertible in F(A) that means, there is a inverse there, so that is, there exit a inverse in F(A) with a times a inverse equal to A. The other equality, we don't have to write because we are in a commutative case.

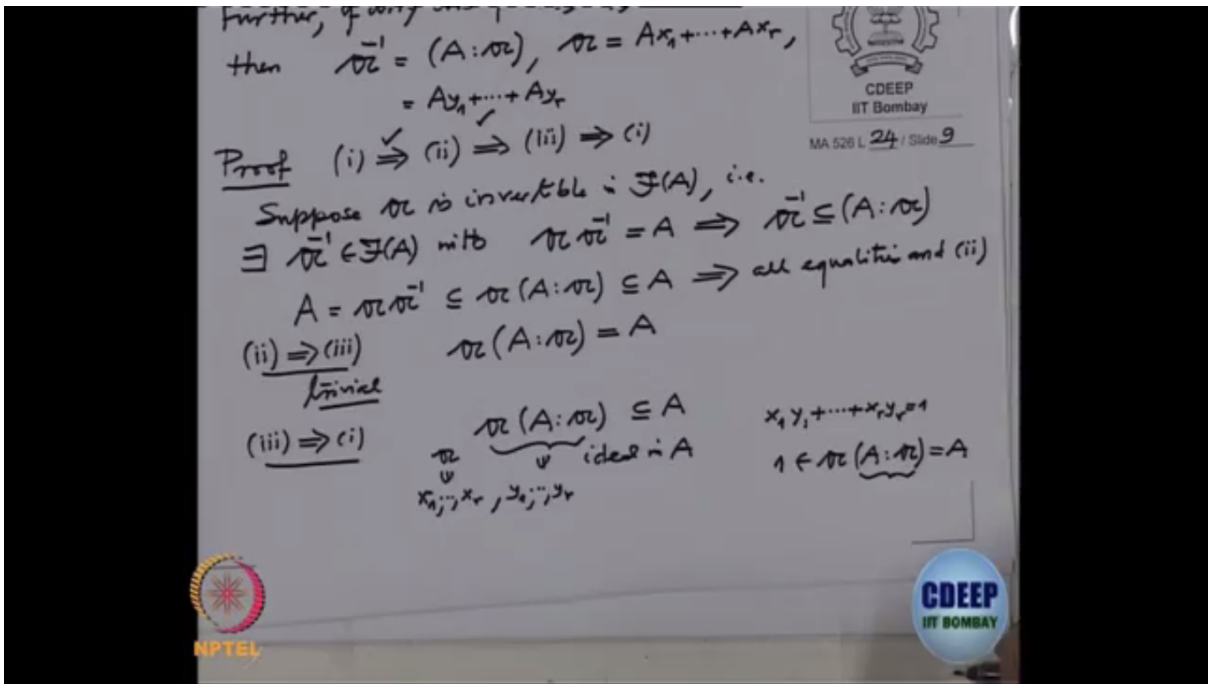
But this means what, this will mean, if we want to rewrite this or this you will have to related this a inverse with the colon. So in a colon notation this means, a inverse is contained in the A colon a. So therefore, look at A which is a a inverse. This is the definition of the inverse and now I am going to replace this with this containment. So this is contained in a, contained in A colon a which contained in

A, so a is contained in A, so are equalities and therefore we have done. So all equalities and hence that proves true. [20:06 inaudible] early this equality.

Okay, two implies three, this is proved, two implies three. We have given that a times A gothic a colon is equal to A. That is given to us and from here we want to conclude that. What do we want to conclude? We want to conclude, there exit elements x1 to xr are here, y1 to yr are here which is 1. But that is [20:39 inaudible] because this product of these sub-modules is, so one belong there, so one is a combination of the product. So, three is, this is trivial. Three implies one, so this we have proved. Three implies one, three, what is given? We have given that there are elements x1 to xr in A and y1 to yr in A colon gothic a with the x1 y1 et cetera, xr yr equal to 1, then we want to prove A is invertible.

So look at the colon, a times A colon a, this we know it is contained here by definition of this colon. So therefore this is an ideal in A because it's a sub-module contained inside A. So it's an ideal, so therefore and also we have given that there is x1 to xr. Three says, we have x1 to xr in a and y1 to yr in this colon, such that there this sums of the products. This is one, that is give in three to us. Therefore this sub-module, this ideal will contain 1. So 1 belongs to a colon A, a. So we have an ideal where 1 belongs, so therefore, that ideal [22:35 inaudible] will be the unit ideal which is the [22:37 inaudible]. So that proves this is equal to A. So that proves that A is invertible and this is the inverse of a, and the remaining thing is, it's clear.

(Refer Slide Time: 22:49)



For that statement it just re-organization, so that proves three implies one. All right, so let me deduce you consequences from here for the future views. So corollary 1, so remember this F(A) is the set of all fractionary ideals and we have taken an a here. We have characterized when will this sub-module of K has a inverse and the condition three say that in particularly finitely generated. Finitely generated, because you see the third this moreover part, further part says, if a has inverse then it is finitely generated by those x1 to xr. So therefore what we have proved that I want to know to corollary every fractionary ideal which is invertible is finitely generated. So an invertible fractionary

ideal in A is finitely generated. See there are many fractionary ideals which are not invertible in general.

All right. Next, another corollary which we will use that, let (A, m) noetherian local domain then A is a DVR if and only if m is invertible, m belongs to F(A) cross, that is, m is invertible in F(A). So let's prove this. So proof. So, this show that we don't have to check, even if you check only the maximal ideal is invertible then from there only you can conclude it's a DVR. Okay, so first we prove this way, assume it is a DVR, then I want to prove m is invertible. If it is a DVR, then the maximal is principle. But the principle ideals are invertible. Inverse is generated by the inverse of the generator.

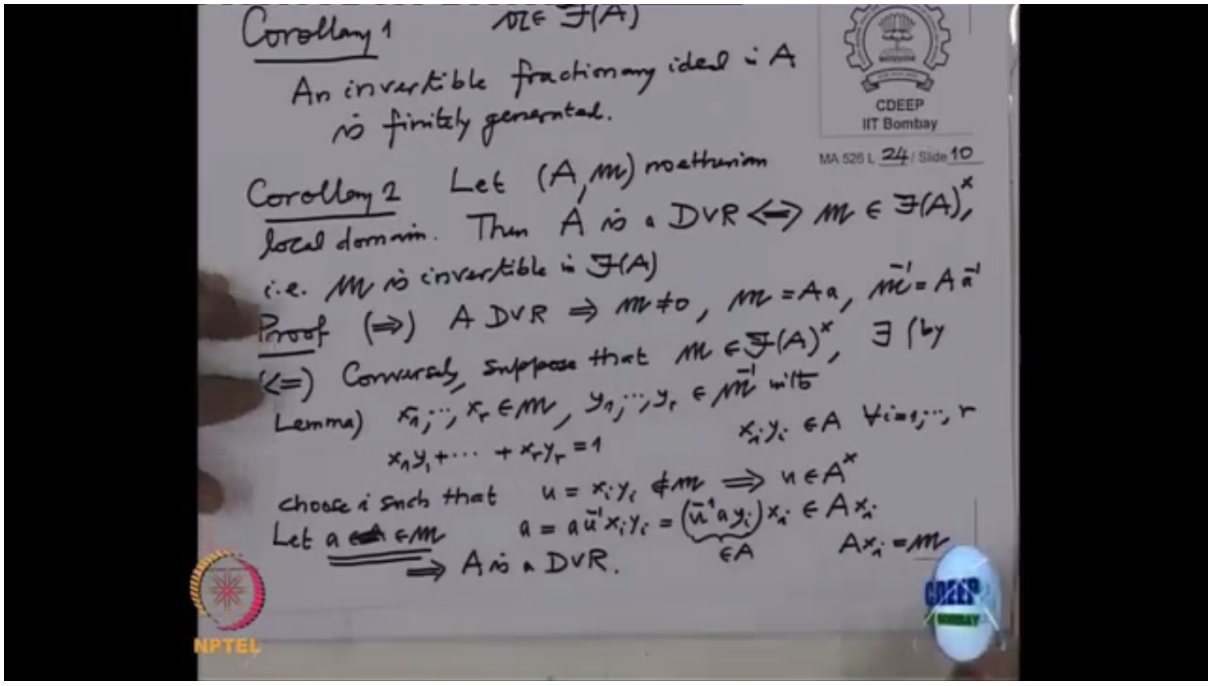
So A DVR, first of all A DVR that will imply m is non-zero and principle A times a and therefore m inverse will be actually A a inverse. so this is easy. Now this way, we want to check it is a DVR, given that (A, m) is invertible. What does that mean? That means conversely, suppose that m is invertible. So by the earlier lemma that means what? That means there are elements here, r elements, so there exit by lemma x1 to xr in m and y1 to yr in m inverse with x1 y1 plus, plus, plus xr yr equal to 1. But note that this xi times yi, this is in A for all i, because x1 is m and say for example, x1 is m and y1 is in m inverse.

That means their product has to be go inside A. So xi yi are in A. So and we know this sum is 1, so that means at least one of them cannot belong to the maximal ideal. So choose, because if all these products belong to the maximal ideal then this sum will also belong to the maximal ideal but 1 is not there. So choose i such that, let's call it u which is xi yi this is not in m, but we are in a local ring. This element u is not in m, so that will mean that u belongs to actually a unit, u is a unit.

Now let us take any a. So let a, what do you want to prove? We want to prove A is a DVR, so that means we want to prove that this maximal ideal has to be generated by a non-zero element, principle ideal, non-zero element. So let, I am looking for a generator for m. So let us take arbitrary a in A or in m. Okay, now a equal to a u inverse and u inverse is, the inverse of this xi yi, so I just multiply this. So this inverse, this is a. But this is same as, this u inverse is, I have taken out and then u inverse a, and come out of this yi and then xi. Whereas this element, obviously this element, I claim that it is in the principle ideal generated by xi because for that I only have to check this is in a. This is in a is obvious because a is where, a was in m, u inverse of the unit in a, therefore this make sense in a, and this I multiplied by yi, but yi is an element in m inverse.

So elements of m times elements of m inverse goes inside A. So therefore this element has gone inside A. So this A is a multiple of this xi. So therefore, and I have proved this for every a. So that means this principle ideal generated by xi is m. So it's a principle ideal, therefore A is a DVR. So A is a DVR.

(Refer Slide Time: 31:20)



All right, I think the next, we will prove the theorem next time.