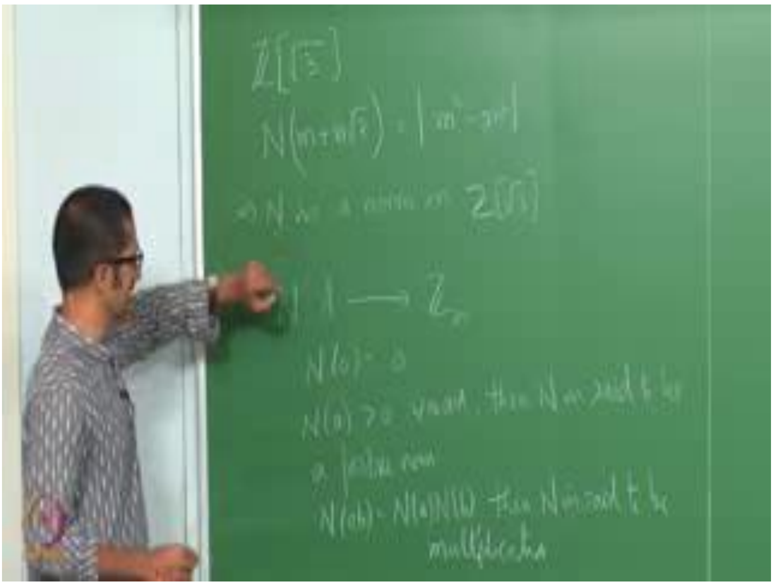
Commutative Algebra
Prof. A. V. Jayanthan
Department of Mathematics
Indian Institute of Technology, Madras

Lecture – 24
Lying Over and Going-up Theorems

Let me quickly talk about one example that we said yesterday.

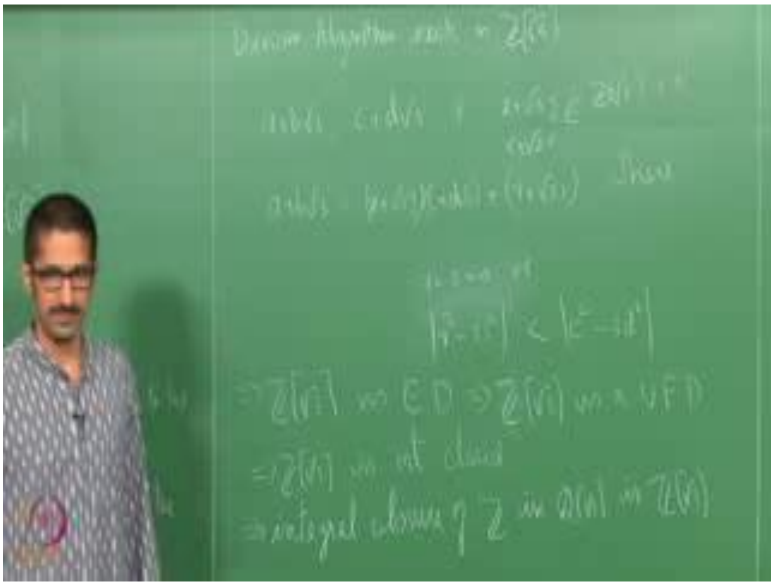
(Refer Slide Time: 00:28)



That Z root 3. So, if I look at this a plus b root; m plus N root 3 norm to be m square minus N root 3 n mod of this, then one can check that this is a norm on Z root 3. What is the norm? Norm is a map from A to if A is an integral domain a to Z non-negative such that N of 0 is 0 that is the only condition required; and if N of a is positive for all non-zero A in A then N is said to be positive said to be a positive norm, and more over N of if N of a b is equal to N a and b then N S multiplicative then N is said to be multiplicative.

So, in your first course this must have been discussed that n defined by this is a norm on Z root 3. So, this is specific to root 3, but if you take root 5 this is not really the norm that works on Z 5 Z root 5. So, one should be careful about that.

(Refer Slide Time: 02:41)



So, that says that this is a Z and with this norm there exists division algorithm on Z root 3. So, exist in Z root that you can verify I would leave with you to verify; it is if you have not done this in your first course you can easily do it. So, what does this say given any a plus b root 3, I can write this as sum you know 2 integers a plus b root 3 and c plus d root 3, I can find a some x plus root y root 3 y in Z root 3, such that and are plus root 3 S both of them in this such that a plus b root 3 is equal to x plus root 3 y times c plus d root 3, and plus root 3 S where r square minus 3 S squares is this is this is 0. So, or r square minus 3 S square is less than c square minus 3 d squared.

With this, I mean this is a useful standard computation you take any element, then look at this I mean multiply divided by a minus root 3, and then look at this I mean closest integer to that and the standard practice that you have done in your first course, doing that you get this you can easily directly prove that there exists this r and s. So therefore, this says that Z root 3 is a Euclidean domain and that implies that Z root 3 is up UFD and that implies Z root 3 is integrally closed. So, therefore, that implies that the integral closure of Z in Q root 3 is Z root 3 that directly proves; without manipulating with integers prime factorization etcetera. So, let us continue with properties of more properties of extension integral extensions; suppose A contained in B bearings B integral over A.

(Refer Slide Time: 06:00)

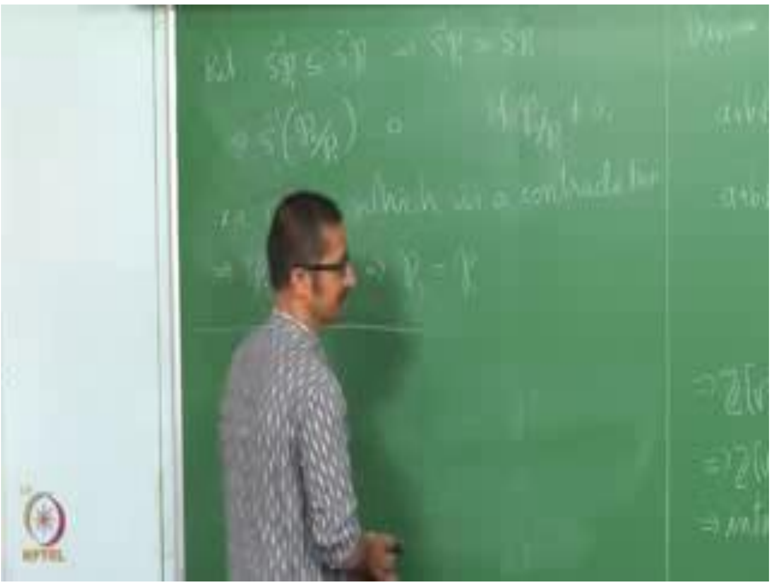
So, we were saying that. So, we were saying that if I start with a maximal ideal; if I have B integral over A and. So, I have A contained in B; if I take a maximal ideal here or if I take a prime ideal here and intersect contract to A then this is maximal if and only this is maximal. So, now, suppose I have you know now the question is suppose I have 2 ideals, you know can both of them contract to 1 ideal here.

So, I have a tower structure suppose I have a tower structure here, if I keep contracting it back will it follow strictly the tower structure here or you know in between there will be collapses; this is important because this tower determines what is called dimension of ring. So, let me state this first let P 1 and P 2 be prime ideals of P 1 contained in be prime ideals of B, if P 1 intersection A is equal to P 2 intersection A then P 1 is equal to P 2.

So, how do I do this? I have a is contained in B, B is integral over A I look at A. So, we can assume that. So, I have A contained in B. So, let me write this as q 1; q this equal to q what we know is that A localized that. So, S inverse A, S inverse B, where S is A without q this is integral. See we are saying that P 1 is contained in P 2, now what is the maximal ideal here this is this is A q.

So, if I take P 1, S inverse P 1 is inverse P 1 contract to let me write S inverse P 1 is an ideal in S inverse B, and S inverse P 1 intersection A is equal to sorry S inverse q which is you know q A q this is a maximal ideal right; this is a maximal ideal therefore, this is maximal and that implies that S inverse P 1 is maximal ideals, because in integral extensions that is what we proved yesterday or I indicated here. A contained in B is integral extension if I take a prime ideal and contract here than this 1 is maximal if and only if the other is maximal. So, therefore, this is a maximal ideal.

(Refer Slide Time: 11:41)



But we already know that S inverse P 1 is contained in S inverse P 2; P 1 is contained in P 2. So, what does that mean? This implies that S inverse P 1 is equal to S inverse P 2. So, the see what we want to say is that P 1 is equal to P 2 right. So, what we know is that S inverse P 1 is equal to S inverse P 2. So, this implies that S inverse of P 2 mod P 1 is 0. When does and this is if P 1 P 2 mod P 1 is non-zero what does this mean?

Student: (Refer Time: 12:48).

No when is? So, if I take a module M when is S inverse M 0.

Student: (Refer Time: 12:59).

Either 0 belongs to S which is not the case because we have taken S to be A minus this, but when is this true.

Student: (Refer Time: 13:07).

S contains an element of the annihilator of M right S should contain an element of the annihilator. So, here what does that mean? It means that I can find an x in annihilator of this; what does annihilator of this? Precisely P 1; so what it says is that there exists x which is in P 1 intersection S, but what is P 1 and what is S? S complement of q in a; so q is I mean q is a smaller set I mean subset of P 1 and we are taking compliment of that in a. So, this is a contradiction which is a contradiction; that is says that S inverse I mean P 1 P 2 mod P 1 is non-zero I mean that is P 2 mod P 1 is 0, or in other words P 2 is equal to P 1.

Student: Sir, why this (Refer Time: 14:39).

This is what is the; this is the local ring right if you take a.

Student: (Refer Time: 14:46) prime ideal (Refer Time: 14:46).

Q is the prime ideal P is a prime ideal therefore.

Student: Contraction.

Contraction q is a I mean P is a prime ideal here therefore, its contraction here is A prime ideal. So, q is always I mean q is certainly a prime ideal.

Student: Q a 2 can be prime ideal.

What is we have already shown this right if I take a prime ideal P, and see if you take a prime ideal P, and look at A P and then if I look at any element x by S which is not in P A p then x by S is a unit; that means, x is not in P which means x is in s. So, therefore, I can I mean x is in S means I have this S by x is also there. So, every element which is not in P A p.

Student: Is a unit.

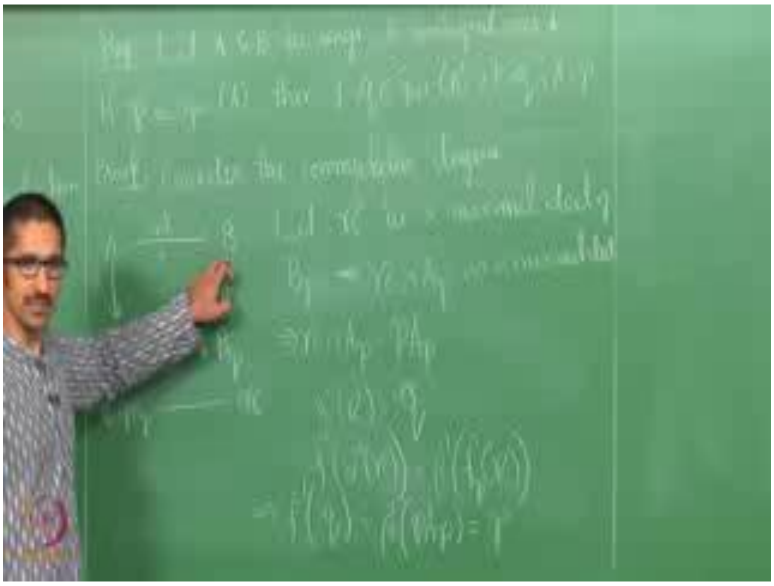
Is a unit which means all non-units are collection of all non-units is P A p which means it is a maximal ideal it is the maximal ad. So, therefore, this is a local ring with P A p as a maximal ideal, as the maximal ideal; this is something that we have seen already. So, this is a maximal ideal therefore, these S inverse P 1 as well as in S inverse P 2 both are maximal ideals therefore, they are equal; once they are equal and from here there are many I mean you can start.

So, we know that this is contained here. So, you can start with an element in P 2 and you know either using elements or using directly using this properties one can direct.

Whatever we have proved so far here we said you know if this is prime then this is prime; if that is maximal then this is maximal, if I have you know a tower like this then it translates to a tower like that, but there is a fundamental question I start with the I mean if I take a prime ideal I always have a prime ideal because its contraction is a primary ideal certainly.

But if I start with the prime ideal here, can I always find a prime ideal here which contracts. In general that is not true right if you have any ring extension forget about integrality; start with an arbitrary ring extension for example, Z 2 q. I start with the prime ideal in Z I do not have a prime ideal in q which intersects Z and give me the give is prime ideal that we start with. So, in general if I have an ring extension A to B and I start with the prime ideal there need not exist a prime ideal which contracts to P.

(Refer Slide Time: 17:57)



But the ring extension is integral things are slightly different. Let be rings B integral over A if p. So, if P is in spec of A then there exists q in spec B such that q intersection A is P; and the extension is integral we do have we do not have situation like Z N q of course, we know Z N q is not an integral extension. So, let us prove this is pretty straight forward I start with. So, consider the diagram the commutative diagram A to B, A p this B p you do not know. What is q as of now what we know is that this is a local drink with unique maximal ideal P A p and this is integral. So, this is an integral extension this is integral.

So, let me call this map the natural map f, this is f P, I call this map alpha and call this beta. I know that this is a local ring, but I do not know anything about this P is. So, I am looking at S inverse B, where S is the multiplicative set in A which is a complement of P. So, I do not know whether this is integral or not I sorry this is local on, but of course, this always have a maximal ideal. So, is start with let N be a maximal ideal of B p.

This is integral over here now if I take. So, if I take its contraction to Ap that will be a maximal ideal here right. N contracted to A p will be prime ideals, but this is an integral extension. So, if I have a prime ideal here and its contraction here then one is maximal if and only the other is maximal. So, therefore, this would imply that N contracted to A p is a maximal ideal, but this in Ap how many maximal ideals are there.

Student: Only one.

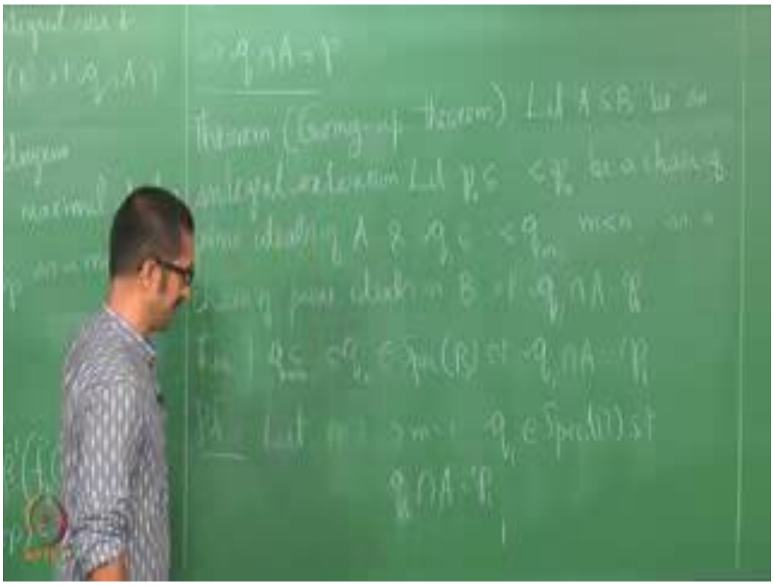
There is only one which is?

Student: P A p.

P A p, so this implies that n intersected with A P is nothing but P A p. So, I have N here and then its contraction is n contraction which is same as P A p. So, this I can I start with this prime ideal here n, alpha inverse of n I take it as q intersecting with B or taking alpha inverse whatever you want to say. Alpha inverse of n b q then what can you say about f inverse of alpha inverse of n? See this is a competitive diagram. So, if I go from here in to here this root or this root both are same. So, alpha f inverse alpha inverse of n is same as beta inverse f p inverse of n, but what is f p inverse of n? F p inverse of n is P A p and its contraction to A is P itself.

So, this is f inverse of q; I take this to be q this is equal to beta inverse of P A p which is same as P; f inverse of q is nothing but intersecting.

(Refer Slide Time: 24:23)



So, that says that q intersection A P. And q is clearly a prime ideal because its inverse image of a maximal ideal. So, it has to be a prime ideal therefore, this is. So, we have obtained the prime ideal which contracts to beta to p. So, when the extension is integral I start with a prime ideal here, I do get a prime ideal here which contracts to this one.

This is a very strong property that distinguishes integral extension from the normal usual you know ring extensions. So, therefore, I have a question, I have you know an integral extension; I start with a prime ideal here I have a prime ideal here. Now I do this one, I start with a prime ideal here, can I have a prime ideal, here can I extend this? I have a chain here can I have a chain here such that each q i contracts to P i.

This an answer to this is called what is called going up theorem, there you can go up you know sorry you start with something down you can go up and you can construct a change to the top; this is called going up theorem. So, let me write it which is a straightforward application of this proposition, yes.

Student: Given a P (Refer Time: 27:12).

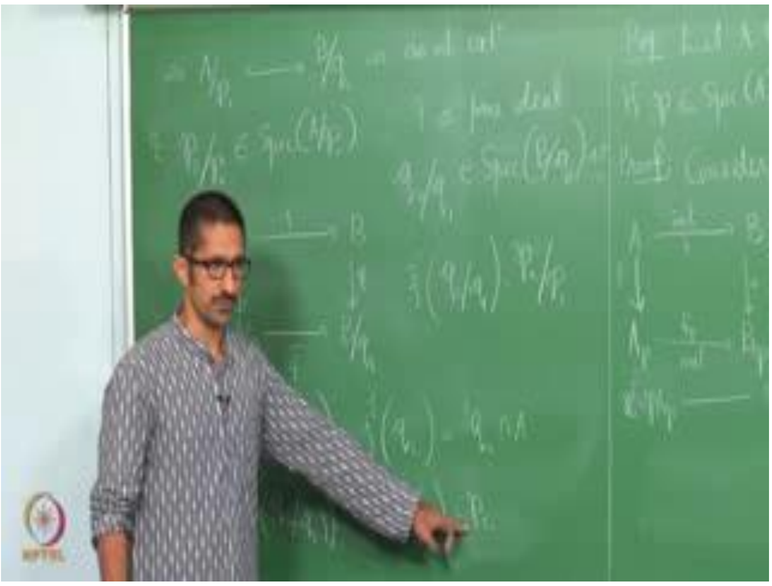
Given a q you see if I take a q here, if I contract here that will always be a prime ideal right. So, if I start with the prime ideal here I always get a prime ideal, but the question is if I start with the prime ideal here, can we get a prime ideal here which contracts to this right? In the usual ring extension this is not the case right if I look at Z to q, I start with 2

Z there is nothing here that no ideal here that contracts to 2 Z right. So, in general it is not there, but when the extension is integral, what we have shown is that they do exist.

Let A content in B be an integral extension, let P 1 to P n be a chain of prime ideals of A and q 1 to q m, m strictly less than n is a chain of prime ideals in B such that q i intersection a is P i then there exists q m plus 1 up to q n prime ideals of B such that q i intersection a is P i. So, there exists tower in spec such that q i intersection A is P i. So, first we look at the case N equal to 2 and once you prove N equal to 2 and m equal to 1 you can always push it. So, let us first do that let n be equal to 2 and m be equal to 1 given chain P 1 contained in P 2 its always I mean there exists there exists q 1. So, I and we know there exists q 1 here given as well.

So, now what do we do? What we know is that q 1 is a prime ideal in B such that q 1 intersection A is P 1. So, now, there is a integral extension involving quotients, what is that can you think of that? See q 1 is in spec B such that q 1 intersection A is P 1.

(Refer Slide Time: 31:13)



Therefore, A mod P 1 to B mod q 1 this is an interval extension right. Now do you see a prime ideal here? Do you see a prime ideal on this one what is that we need to prove we need to prove that there exists a prime ideal q 2 in be containing q 1, and q 2 intersection a is P 2. So, for that I need to start with a prime ideal here and then use the existence property, what are the what is the prime ideal here which is useful in this?

Student: If I (Refer Time: 32:09).

If I take this is an integral extension and P 2 mod P 1 this is a prime ideal in A mod P 1 therefore, there exists a prime ideal. So, I have A here B here quotient A mod P 1 here, this is B mod q 1 here; again if I look at this is f this is f bar, this is phi let me just use phi and psi. So, there exists the prime ideal q 2 mod q 1 I mean I can write it in this form because of the correspondence theorem. This in spec B mod q 1 such that f bar inverse of q 2 mod q 1 is P 2 mod P 1. This is the natural maps of phi inverse of q 2 mod q 1 is a prime ideal will denote by q 2 q 2 in B; so f inverse of phi inverse of q 2 mod q 1. This is nothing but f inverse of q 2, f inverse of q 2 is same as.

Student: Q 2 intersection.

Q 2 intersection A with this is q 2 intersection A at the same time this is equal to psi inverse of.

Student: F bar inverse.

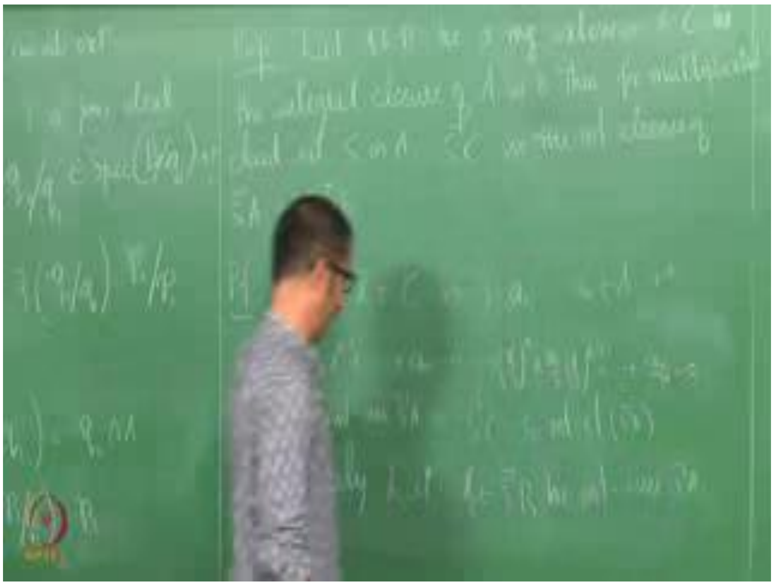
F bar inverse of q 2 mod q 1; but f bar inverse of q 2 mod q 1 is.

Student: (Refer Time: 34:49).

Psi inverse of P 2 mod P 1 psi inverse of P 2 mod P 1 is P 2. So, q 2 intersection A is P 2. So, we obtained the prime ideal q 2 in B, which is containing q 1 and q 2 intersection A is P 2. Now if you want to have you know at each stage if you have a let us say P 3 here do the same thing replace q 2 by P 2 sorry I mean P 2 by P 3 and go through the whole process. So, in the case of you know you have seen that in the case of the spectrum of A ring a spec of A; I guess you have attempted that is the first chapter exercises in which there is a topology defined on spec of A right it is called a risky topology. So, therefore, there is a you know 1 can talk about dimension of a ring using you know there are various ways, one way is a chain of you know length of a chain of maximal length of maximal chain of prime ideals in spec.

So, here what we are in some sense what we are saying is that, if I have a chain here I have a corresponding chain on the top. So, if I have an integral extension this dimension is at least sorry it will be at most the dimension of B, we will in fact, prove the converse also. So, there is we will of course, in the course we will see most likely will define what is dimension and so on.

(Refer Slide Time: 37:26)



But now this is another you know property of integral extension, suppose I have you know let this B an integral be an extension.

Student: Sir (Refer Time: 37:42).

So, that is what we may have a bigger chain there, but we have proved that we do not really have a bigger chain, because if 2 of them contracts to 1 prime ideal they have to be equal, but what we I am this this is not enough to say that the dimensions are equal; if I start with see in the maximal chain of prime ideals you have to start, if I start with the maximal ideal can we always come down and get to a place where this is you know we have maximal saturated chain both up and down you need little more work.

So let A contained in B be an integral domain sorry be a ring extension be a ring extension, will and C be the integral closure of A in B then for any multiplicative set multiplicatively closed set S in A,S inverse C is the integral closure of S inverse A in S inverse B. So, I have A to B ring extension and C is the integral closure of A in integral closure of A in B. So, correspondingly I have an interval I have an extension S inverse A to S inverse B, what this result says is that the integral closure of S inverse A in S inverse B is nothing but integral closure of A, the S inverse of integral closure of A and B. And so pretty easy to prove let x by S in S inverse C if the other way is easy to see let x B and C.

Student: (Refer Time: 41:12).

Then x by, so therefore there exists a 1 up to a N in a A, such that x power N plus a 1 x power n minus 1 plus etcetera a n is 0. So, therefore, x by s whole power n plus a 1 by s x by s whole power n minus 1 plus etcetera a n by s power n is 0 that means.

Student: X by s.

Sorry x by s is integral over S inverse A; that means, S inverse C is contained in the integral closure of S inverse a in S inverse b.

(Refer Slide Time: 42:34)

Conversely, suppose I take an element in S inverse. So, let us start with let x by S in x inverse B be integral over S inverse; that means, I have an equation there exist a 1 by S 1 a N by S n in S inverse A such that x power n by S power n plus a 1 by S 1 n minus 1 by S nminus 1 a n by S n this is 0. See what I want to do is I want to say that x by s is equal to some you know it is in S inverse c or in other words I have a representation for this in c or in other words I can you know for some you u x by u s is in S inverse C. So, If I know that for some u in S u x is integral over a then I am through now can you think of some u s u x for some; how can I clear all the denominators of this equation? If I multiply S 1 up to S n and.

Student: S power n.

S power n what do I get; here it will be S 1 up to S n, x n power n and so on, but then see if I have something like this this need not be some u power u x power n. So, how do I make it u x power n?

Student: (Refer Time: 44:19) x power n.

I multiplied by power of all these. So, let me right like that. So, let us u b equal to S t, t is S 1 up to S N does not really matter; u is S 1 up to S , S then u power n multiplying by and multiply by u power n we get. So, this is if I call this t that is easier, t x whole power n plus. So, there will be an S coming from here.

Student: (Refer Time: 45:30).

So, I can take the appropriate quantities inside, there will be a 1 prime t x n minus 1 plus etcetera a n prime is 0; what is a 1 prime? It will be a 1 times S and then there will be S 1 power n minus 1 up to then S 2 power n up to S n power n; a 1 prime see its simple image is this multiplied by u power n here what is that. So, therefore, this this implies that t x is, t x in B is integral over A. That means, t x is in C. So, that implies that t x divided by t s is in S inverse C and that implies x by S is S inverse. So, the integral closure of S inverse A in S inverse B there is nothing but S inverse of the integral closure of A and B.