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

Lecture - 22
Integral Dependence

(Refer Slide Time: 00:26)

So, today we will start the topic of integral dependence. So, let A be contained in a ring B. An element x in B is said to be integral over A, if there exists a 1 up to a n in A such that x power n plus a 1 x power n minus 1 plus it a n minus 1 x plus a n 0.

Student: A and B are;

A and B are rings. So, one says B is an extension of ring A. So, this is a concept that you know comes in.

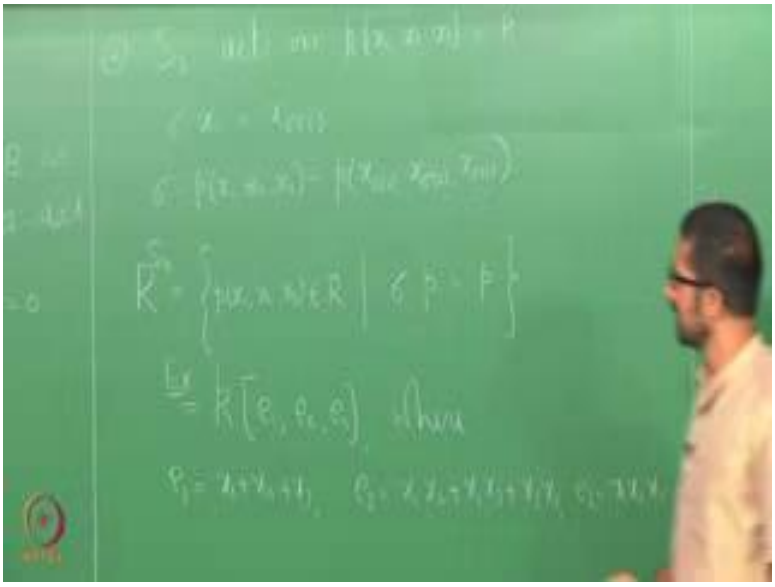
Student: subset of A sub ring of B.

If A, so this is by this notation I mean A and B are rings and when I say A contained in B, it means A is a sub ring of B as operations being the same, so that is the I mean the notation means that. So, this is a concept that comes in number theory as well as in algebraic geometry. It is a important concept that if you do a course in algebraic geometry, you will see relation between what is called the integral closure of a you know

ring in number fields that keeps coming in number theory and the integral closure property of certain rings. With that has close relation with algebraic curve, curve associated to or the ring which is associated to curve; the integral closedness of that ring has closures association with the ring being smooth or not; the curve being smooth or not.

We will see one example of such sometime, but you will see more such examples if you do a course in algebraic geometry next semester or course in algebraic number theory and so. So, let us look at some simple examples. One quick example is that if you look at k x square contained in k x; x is a variable; k is a field then. So, this is A, this is B, x and B is integral over A. It satisfies the equation y square minus x square; takes will satisfy this equation. So, if I take n to be 1, n to be 2, and a 1 to be 0 and a 2 to be this is 0, this is x square. So, this is integral over A.

(Refer Slide Time: 04:55)



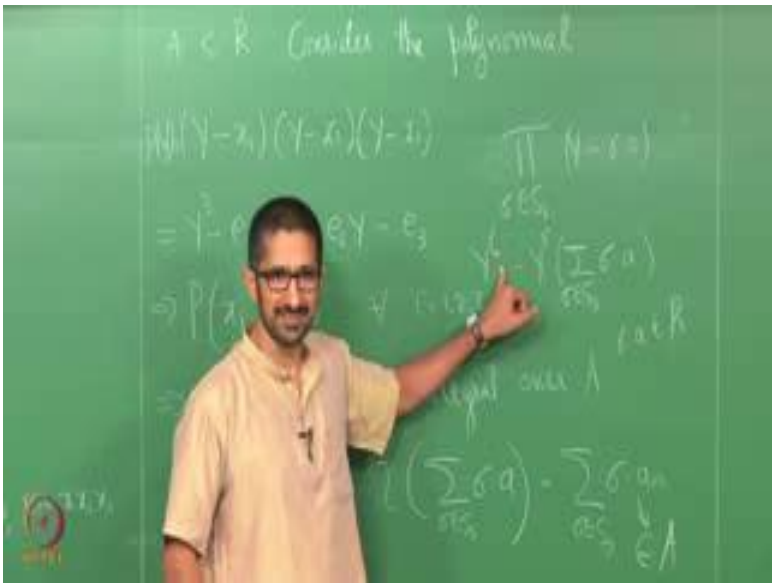
Let us look at another very interesting example. So, you must have seen in your algebra course that S 3 acts on k x 1, x 2, x 3, how does this S 3 act on this ring?

Student: (Refer Time: 05:27).

So, sigma of x i is x sigma i. This is in general sigma acting on any p x 1, x 2, x 3 is p x sigma 1, x sigma 2, x sigma 3 then this is a group action. Now, let me call this ring a; call this ring R. Look at this ring R S 3. This is set of all p x 1, x 2, x 3 in R such that sigma

acting on p is same as p. Then what do you know about this ring? Do you; well this might not be known to you, but this one can easily show that this is equal to e 1, e 2, e 3. Where e 1 is x 1 plus x 2 plus x 3; e 2 is x 1 x 2 x 1 x 3 x 2 x 3, and e 3 is x 1 x 2 x 3. What is this R S 3? They are all symmetric polynomials. These elements of this are called symmetric polynomials. How are you change x i to x j? They are unchanged. These e 1, e 2, e 3 are called elementary symmetric polynomials, this equal to this. It is not very difficult to show, I will leave it to you as an exercise this, complete this. Now, can you see that x 1 is integral over, so let me call this A.

(Refer Slide Time: 08:19)



So, now, we have A contained in (Refer Time: 00:00), can you tell me whether x 1 is integral over? So, I want to get a polynomial. So, what is the idea? So, when would you say that x 1 is integral over A, if I can find the polynomial let say p y such that you put y equal to x 1 it is 0. Now, if I look at this polynomial consider the polynomial y minus x 1 times y minus x 2 times y minus x 3. What is this polynomial y cube minus, what is the coefficient of y square, y square times minus x 3 then y square times minus x 1 and y square minus y square times minus x which is e 1 times y square. What is the coefficient of y?

Student: (Refer Time: 10:02) e 2.

E 2, e 2 times y minus e 3. So, therefore, p y I take p y to be this. Then p of x 1 is 0 in fact, p of x i is 0 for all i from 1 I mean i equal to 1 to 3 because its if you put x 1 equal

to 0, y equal to x 1 or x 2 or x 3 this is going to be 0 which means, we have an in we have an integral equation for x 1 over A. Similarly, for x 2, and similarly for x 3, so this says that x 1 x 2 x 3 are integral over A. So, what have we really done here we have taken one x, one element we have taken one element and looked at all possible and the orbit of x 1.

So, we have taken an element from the polynomial ring looked at y minus that element times y minus all the products possible products, we are looking at y minus a then y minus sigma a. So, or in other words what we have done is we have looked at y minus sigma dot a sigma in S 3. We did not take the entire product, but if I take any A in R, this will work. And every coefficient is going to be, each coefficient is going to be inside the ring A. What will be the, suppose this is this has to be of degree if I take this polynomial, what will be its degree.

Student: 3.

How many elements in S 3?

Student: 6.

6, so this will be of degree 6. We did not take this here we took A, we sensibly took a smaller polynomial, but in generally if I had for any A, if I take this, this will have degree 6. What does coefficient of y power five it will be summation sigma dot a sigma in S 3 minus of this. This polynomial will be y power six minus this one. Is this symmetric? These are all symmetric. If I apply this is a polynomial sigma dot a will again be a polynomial in R, but if I apply some tau, if I apply tau on this sigma a; this is?

Student: (Refer Time: 13:59).

This will be same as this one right tau sigma acting on a tau varies over S 3, but that is same as this element itself. Therefore, this is fixed by all elements in S 3 and hence this is in.

Student: a.

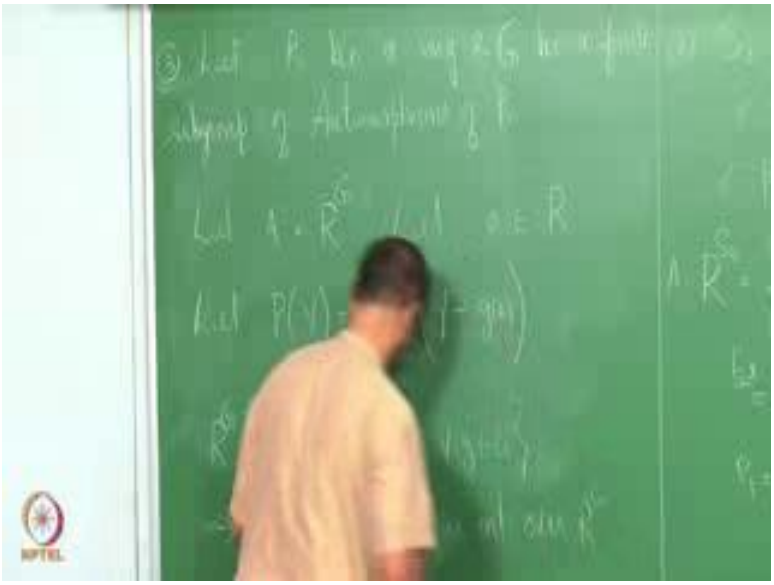
In A. This will be sigma dot a sigma in S 3. S 3 is a finite group you look at tau sigma, where sigma varies of over S 3 is same as sigma varies over S 3. So, therefore, this

implies this element is in A. Similarly, look at coefficient of y power 4, we will have sigma 1 a sigma 2 a and products like that. So, therefore, each of these coefficient will be in A, and hence this will be this will give me a integral equation for A.

Student: (Refer Time: 15:20)

Not really a special case, this is a smaller polynomial in fact. Because if I take for example, if I take the take sigma to be 2, 3 and apply on x 1 it will remain x 1.

(Refer Slide Time: 15:49)



So, if I take this one, this will be square, square, square. See, if I take, so I take this y minus sigma x 1 product sigma in S 3, what would this be, this will be y minus 1 square y minus x 2 square y minus x 3 square. Because this will see what does this I am looking at y minus sigma acting on x 1; for sigma equal to identity acting on x 1, there will be y minus x 1; sigma equal to 2, 3 acting on x 1 will again be x 1. Now, in this one, if I take 1, 2, 3 this will be x 1 will be sigma of x 1 will be x 2 and if I take; so yeah the transposition 1, 2 that will also give me x minus y minus x 2. So, there are 2 of them similarly here. So, this will be this one. So, in general you might not require whole of S 3 to get a polynomial integral equation, but this is a safe one if I take this that is going to serve as a polynomial for the integral equation.

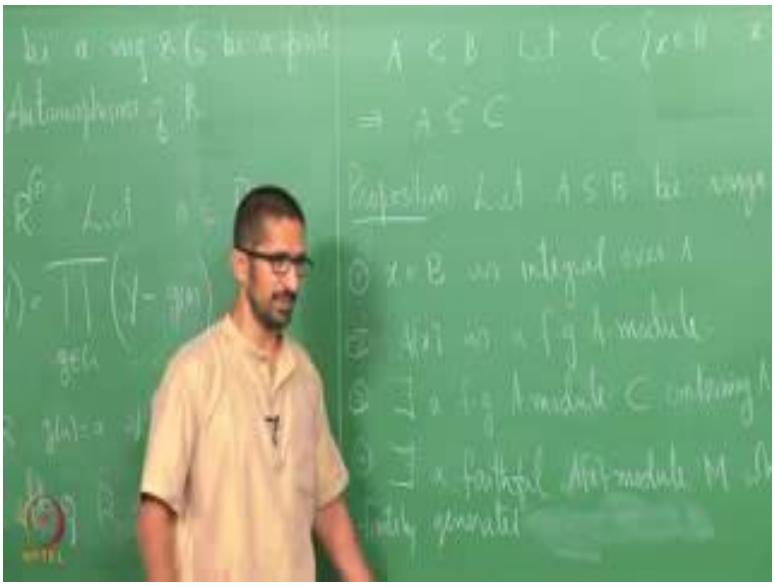
So, now what we have done is this is a very particular interesting case, but we can replicate this in a much more general situation. What is that I take a ring? Let R be a ring

and G be a finite subgroups of automorphisms of R. I take a finite subgroup of automorphisms of R, isomorphisms from R to R, they are called automorphisms. This is in particular, this is an automorphisms permutation of variables is an automorphisms of k x 1, x 2, x 3. So, we take a finite subgroup of automorphisms of R. And look at A to be equal to R G. Now, can you tell me whether R is integral over A. I look at this a be in R. Can you tell me whether this is integral over A, can you give me a polynomial which will serve as, which will give us integral equation for A. Take p y to be, we are doing exactly what we did there, not doing anything other than it.

This is G is a finite group. So, this is a polynomial of degree equal to the cardinality of G one of them is identity. So, therefore, P a is 0; and every coefficient of this polynomial will be fixed by this. Is this clear? What this is R G is set of all a in R such that g of a is yeah, g of a is a for every g in G.

Now, if I take summation g a for a fixed A, summation g a, g varies over G is fixed by if I apply g prime on that g prime g as g varies over g is same as g varies over g, it will be whole group again. So, therefore, every coefficient of this will be in R G. So, therefore, this will give me an integral equation for A. So, this says that every element of R is integral over R G. We will see more examples little later.

(Refer Slide Time: 21:40)

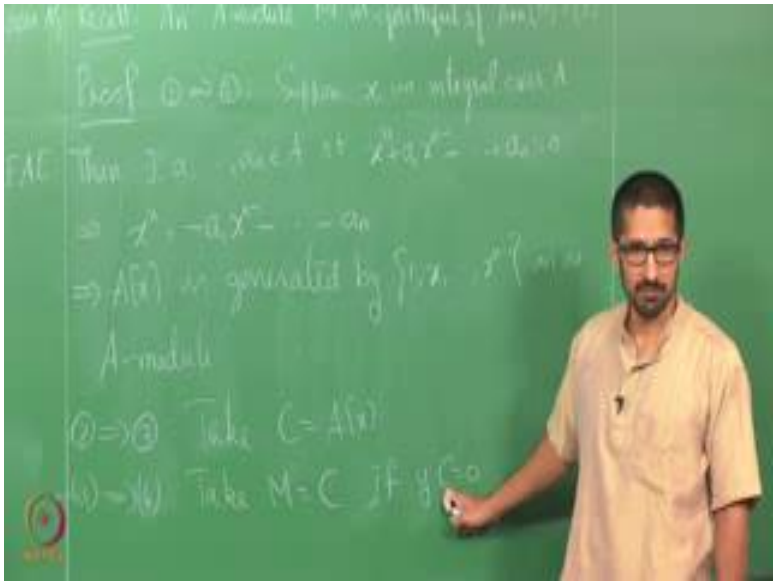


So, now suppose I have a ring extension A contained in B. I look at all elements in B, which are integral over A. Can you give me some elements from that set? So, let C be set of all x in B such that x is integral over A. Can you tell me some elements of c?

Student: (Refer Time: 22:17)

All elements in A will be in C, then C is I mean A is contained in C. So, this is C is containing A and contained in B. Naturally, one tend to ask if C has some additional structure, is it a sub module, is it a sub ring is it an ideal what is it, does it have some structure nice structure compared to the structures of A and B. So, this is obtained by observing some you know equivalent conditions for the integrality. So, let B rings A contained in B be rings. Then the following are equivalent x in B is integral over A, A x is a finitely generated A-module, there exists a finitely generated A-module C containing A and x. There exists faithful A-module faithful A x module M, which is generated by n elements finitely generated over A.

(Refer Slide Time: 24:52)



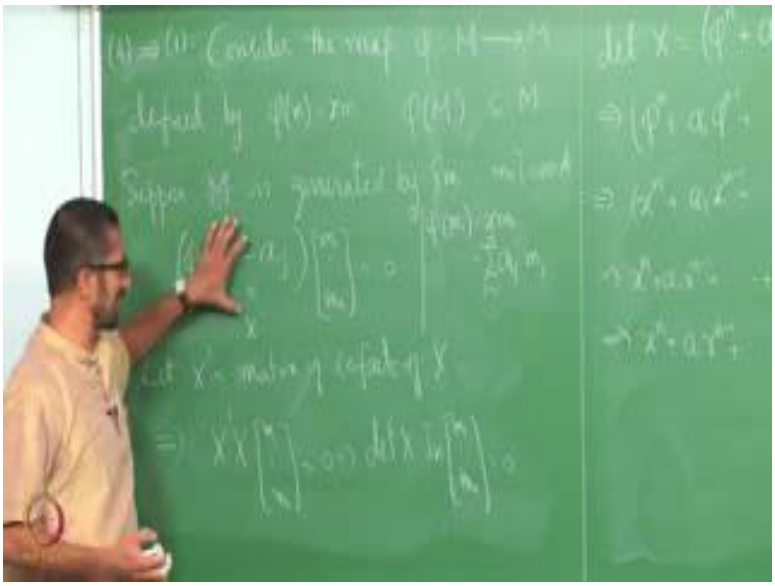
What is faithful module? So, an A-module M is faithful if annihilator of M is 0. There are no elements that kill M. So, let us prove this. 1 implies 2, if x is integral over A, suppose x is integral over A, then x power n there exists a 1 up to a n in a such that x power n plus a 1 x power n minus 1 plus a n is 0. Can you tell me an A module generating set for a x now?

Student: (Refer Time: 26:22).

1 x up to x power n minus 1. So, this will imply that. So, there are many ways of saying this. This implies that x power yeah n is equal to minus a 1 x power n minus 1 minus a n and that implies that a x is generated by 1, x, x power n minus 1 as an a module. Any higher power you can substitute x power n, this for x power n and reduce to a, an equation of degree n minus 1 so that proves the second statement.

Now, 2 implies 3, I am given that a x is a finitely generated A-module. And here I have to prove that there exists a finitely generated A-module C containing a and x just take c to be equal to a x. And 3 implies 4, I know this, and I want to prove that there exists. So, I should probably here write instead of which is finitely generated, I do not really, since I am not really talking about elements here. In fact, one can state this as a x is generated by 1, x, x square up to x power n minus 1, and this generated by n elements, and here also generate. So, that n if I can add in these 3 or I can just omit in 3. 3 implies 4, again I can take M to be equal to C. Why would it be faithful? Take M to be equal to C. Now, see the A module C is containing a. So, if I have some y, if y times C is 0, C contains a, which means C contains 1, which means y times 1 is 0, which is y is 0.

(Refer Slide Time: 29:37)



So, now let us look at 4 implies 1. What we are given is a module M which is a faithful a x module and which is finitely generated as an A-module. We need to prove that this x is integral over a or in other words I need to produce an integral equation of the form x

power n plus a 1 x power n minus 1 and so on so forth. So, therefore, let us look at consider the map phi from M to M defined by phi of m equal to x m this is the multiplication map, now, yeah?

Student: (Refer Time: 30:49).

No, this is this is for the fixed x, x in B is integral implies A x. So, all these x are same x here, x here, x here, x here all of them are same x. If for an element x in B, if that is integral then this is true; if for an x in B, if A x is a finitely generated A-module then the third statement is true. Similarly, if there exists a C containing A and x then this is true. Similarly, if I have a A x module with this property then x is integral over here that is what we are trying to prove. So, the x here is fixed. The x here, here, here, here all are the same.

Now phi is an endomorphism of M phi of M is contained in M; obviously. Now, what I do is I just now apply the Cayley Hamilton theorem which what does it say there exists. So, here let me write it clearly. Suppose M is generated by m 1 up to m n then I can write this phi delta i j minus you know see each x m i is an element of M, and hence I can write it as a finite a linear combination of m 1 up to m n generate by over A. What we are given is that M is a finitely generated sorry over A.

So, if this is I can write this a i j acting on this m 1 up to m n, this is 0. So, I take I mean this is my matrix let us say yeah, if I call this matrix X, and if I take X prime be the cofactor matrix with cofactors of X. Then what do we have X, X acting on this matrix on this vector m 1 up to m n, this is 0. We are just going through the you know Cayley Hamilton theorem in some sense, but this is determinant of this matrix X times I n acting on m 1 up to m n. Now, we need to use that the module is faithful over A x more generally see this will be a polynomial some phi power n.

(Refer Slide Time: 35:14)

This is a polynomial in phi determinant X, X will be some phi power n minus some I will just write now as a 1 phi power n minus 1 plus a n minus 1 phi plus a n this acting on. So, this is the determinant therefore, phi power n plus a 1 phi power n minus 1 n minus 1 phi plus a n acting on any m i is 0; for all i from 1 to n. But what is phi power n acting on m i phi is an A-module homomorphism.

Student: x power.

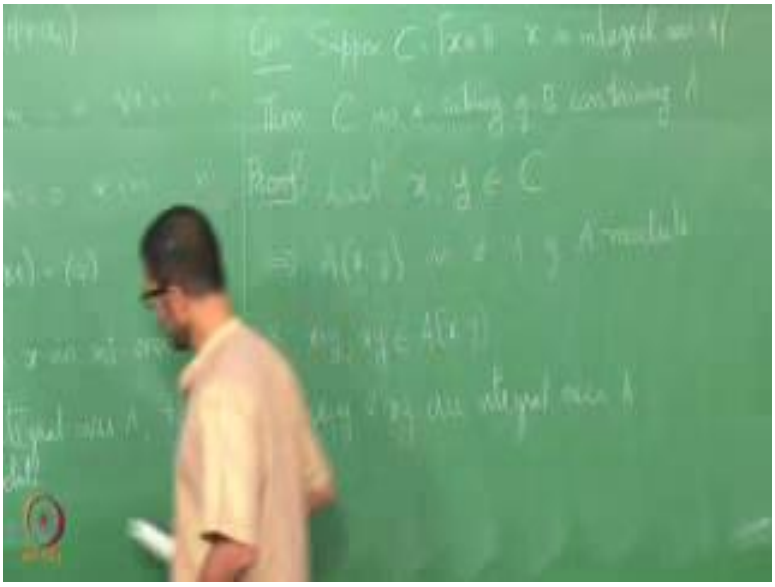
It will be x power n m i. So, this implies that x power n plus a 1 x power n minus 1 plus etcetera a 1 a n minus 1 x plus a n acting on m i is 0 for all i from 1 to n. Or in other words, this element is in the annihilator of M, because it annihilates all m i's. So, this implies x power n plus a 1 x power n minus 1 plus etcetera a n this belongs to annihilator of M, but since annihilator, this is an element in a x and M is a faithful A x module this is 0. So, that implies x power n plus and that implies that x is integral over A. Is the proof clear? What is 0?

So, I am writing phi m 1 this is x m 1. What are this be I am just writing it as summation a i j a 1 j m j, j from 1 to n. Similarly, for each i m i is this and these are these coefficients this is this is the same matrix that we considered while proving Cayley Hamilton theorem or you know the lemma before Nakayama lemma. So, the matrix is same as that. We were just see from here I could have directly from here I could have

directly come to this one, because by directly applying the determinant trick lemma, but I just went through the proof completely that is it.

So, there are some nice corollaries one of which is the question that we started with. So, first we observe something that if b 1 up to b n in B are integral over A then A b 1 up to b n is a finitely generated A-module because A b 1 will be a finitely generated a module by the preposition. Now, A b 1 b 2 will be a finitely generated module over A b 1, but A b 1 is a finitely generated module over A. So, if you take the corresponding generating sets and look at all the products that will be an A generating set for A b 1 b 2 and keep going on like this. So, therefore, this is a finitely generated A-module. Write down a proof for this. So, if you have, so this is more generally true that if A is contained in B contained in C, they are all rings and if B is a finitely generated A-module and C is a finitely generated B-module then C is a finitely generated A module.

(Refer Slide Time: 40:06)



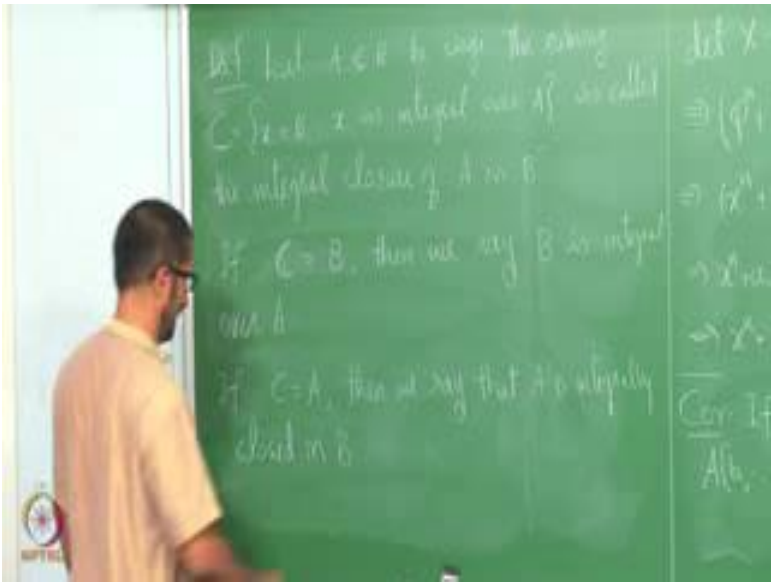
Just take if this b 1 up to b n is A generating set for B, and c 1 up to c m is a B generating set for c then b i c j is an A generating set for C. So, this is using this result one can prove that this is a finitely generated A-module. Suppose, c is set of all x in B such that x is integral over A, then C is a sub ring of B containing A. So, here if I know that x is integral over A, and y is integral over A, how do I know x plus y is integral over A. I mean from the integral equations of x and y, I cannot possibly get a integral equation for x plus y, there will be entirely different. So, therefore, we use the result that we proved.

See here to prove that it is a sub ring we only need to prove that it is closed under addition and multiplication. Once they are there then all other all other properties are associativity, distributivity etcetera, they are all part of ring you know B itself. So, therefore, we do not need to worry about them, we only need to prove that this is closed under addition and multiplication. So, if I take x in x comma y in C integral, so they are integral over A so.

Student: (Refer Time: 42:42) finitely generated.

Yeah. So, this implies that A x comma y is a finitely generated A-module. And x plus y comma x y belongs to this one by the third property that we proved in the last proposition. If there exists a finitely generated a module containing x then x is integral over A. So, here I have a finitely generated a module containing x plus y as well as x y, therefore x plus y and x y are integral over A, so that proves that it is a sub ring.

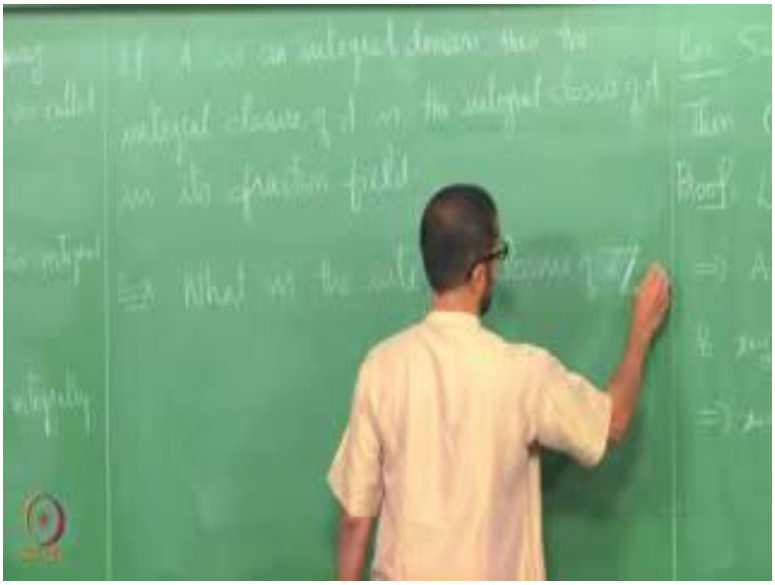
(Refer Slide Time: 43:57)



So, the collection of all integral elements of B over A is a sub ring. So, this let A contained in B be a rings. The set the sub ring C equal to set of all x in B such that x is integral over A is called the integral closure of A in B, if C is equal to B, then we say B is integral over A, C is equal to A then we say that A is integrally closed in B. And if A is a domain, if A is an integral domain then the integral closure of A. See, here the terminology is integral closure of A in the super ring, but if A is a integral domain then

we say that the integral closure of A is a notion that represents the integral closure of A in its fraction field.

(Refer Slide Time: 46:06)



So, if A is an integral domain then the integral closure of A is the integral closure of A in its fraction field. What is the integral closure of?