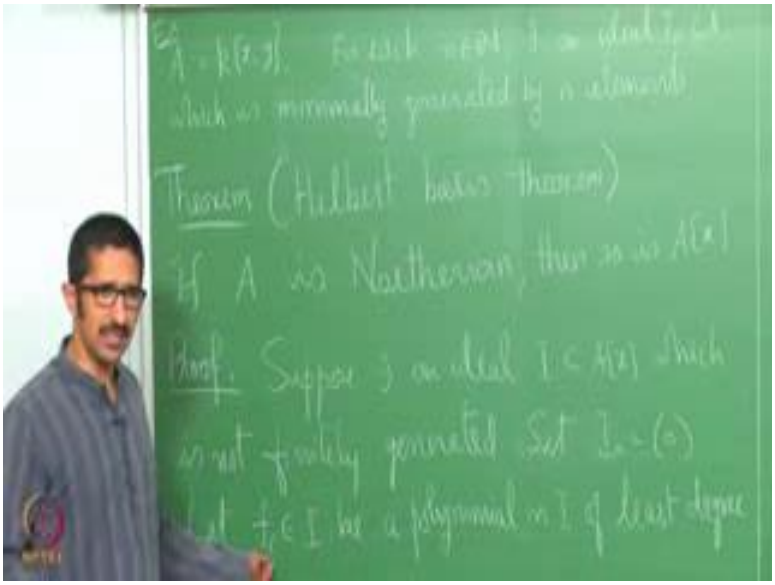
Commutative Algebra
Prof. A. V. Jayanthan
Department of Mathematics
Indian Institute of Technology, Madras

Lecture - 31
Hilbert Basis Theorem and Primary Decomposition

(Refer Slide Time: 00:25)



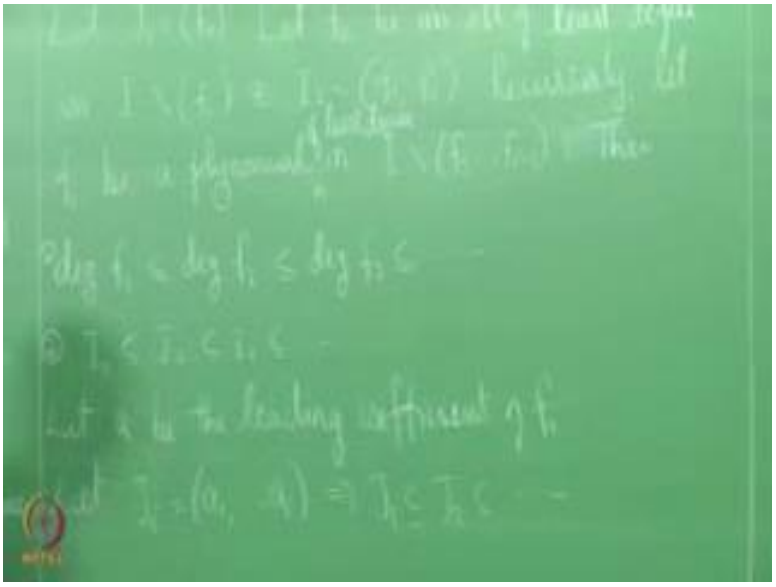
So did you think about the question that I asked you yesterday. So take A to be k x y and take I n, for each n in N, there exists an ideal I n in A which is generated by n elements. So when I say generated by I mean minimally generated by, because otherwise you can add many elements to generating set which is minimally; did you think about this question? So I will still leave this as an exercise. So what we are going to see is that, this does not really say that ideals of k x, k x y is not finitely generated. So this is famous theorem of Hilbert, this is called Hilbert basis theorem. Hilbert did not prove this in this a did not state this state the result in this manner or proved this like this. He was studying rings of invariance and he wanted to prove that it is finitely generated k algebra.

So but the idea was used later to prove something like this. So the statement is, if a is Noetherian then, so is A x where x is an indeterminate over A. That is A x is also Noetherian. So you want to prove that every ideal of A x is finitely generated. Suppose there exists an ideal which is not finitely generated. There exists an ideal I in A x which

is not finitely generated. We want to arrive at a contradiction. So what we do is, see we want to make use of the fact that A is Noetherian.

So let set I naught equal to 0. Then let f 1 in I be a polynomial in I of least degree. If I take this collection of all elements in I and look at the degrees of each polynomial, that will be a subset of set of all natural numbers, that always set of all natural numbers always have a least element. So take a least element and look at a polynomial corresponding to that. And let I 1 be the ideal generated by f 1.

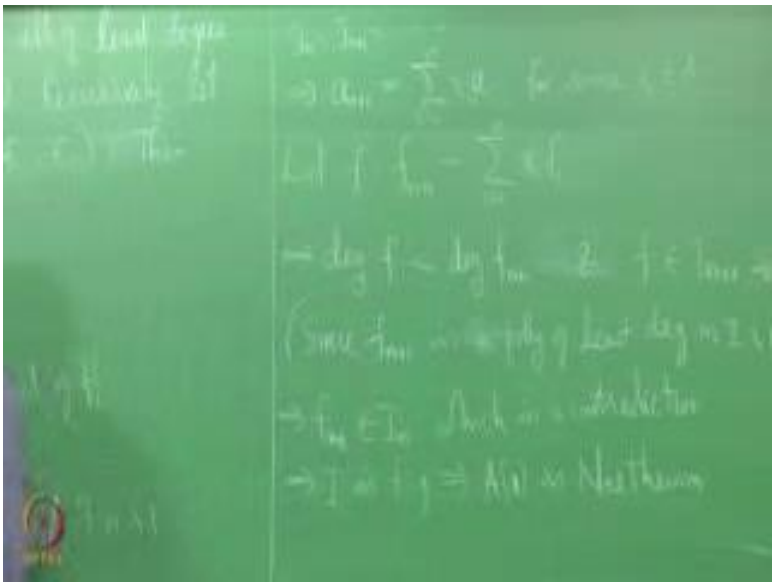
(Refer Slide Time: 05:21)



Now, let f 2 be an element of least degree in I without the ideal generated by f 1. And I 2 be the ideal generated by f 1 and f 2. Keep doing this. Recursively, let f i be a polynomial in I without f 1 up to f i minus 1 ideal generated by a f 1 up to f i minus 1, which is of a polynomial of least degree in this set. So first thing that you can observe is that degree of f 1 is less than or equal to degree of f 2 less than equal to degree of f 3 and so on. That is one observation. Another observation is I 1 contained in I 2 contained in I 3 and so on.

Now, we want to say that you know. So let us look at let a i be the leading coefficient of f i. See from here we have to obtain some ideal in A and use the fact that the ideal there is finitely generated. And consider let J i be the ideal generated by a 1 up to a i, then again of course, you have ideal generate by J 1 contained in J 2 and so on. This chain is in is happening in A, and A is Noetherian which means this terminates at some point. Since this is a chain of ideals in A there exist n.

(Refer Slide Time: 09:19)



Such that J n is equal to J n plus 1 and so on. Which means that this element a n plus 1 which is the leading coefficient of f n plus 1, it belongs to J n, or in other words I can write this as, summation r i a i I from 1 to n for some r i in A.

Now, let f be equal to f n plus 1 minus summation r i f i I from 1 to n. Now what can you say about this?

Students: (Refer Time: 10:38).

Degree of f will be degree of f is strictly less than degree of f n plus 1. What does that mean? See now look at this element f, f is in i n plus 1, f is in i n plus 1 because it is a linear combination of f 1 up to f n plus 1. F n plus 1 was chosen as an element in.

Student: (Refer Time: 11:30).

I 1 up to?

Student: (Refer Time: 10:34).

I mean I without f 1 up to f n of least degree, f is in I n plus 1 and degree is less than?

Student: (Refer Time: 11:46).

Degree of f n plus 1; that means, f has to be in I n, but if f is in I n I can write f n plus 1 as linear combination of f and this, which means f n plus 1 is in?

Student: I n.

I n; that is a contradiction, since f is in I n plus 1, this implies that degree of f is strictly less than f n plus 1 and f is in I n plus 1 implies that f is in I n. Because since this and f n f is in I n plus 1 implies f is in I n, since f n plus 1 is a polynomial of least degree in I without f 1 up to f n. So therefore, f is in I n implies, f n plus 1 is in I n, and that is a contradiction because f n plus 1 is chosen to be in I; the complement of I n in I n plus in I. So therefore, that is a contradiction.

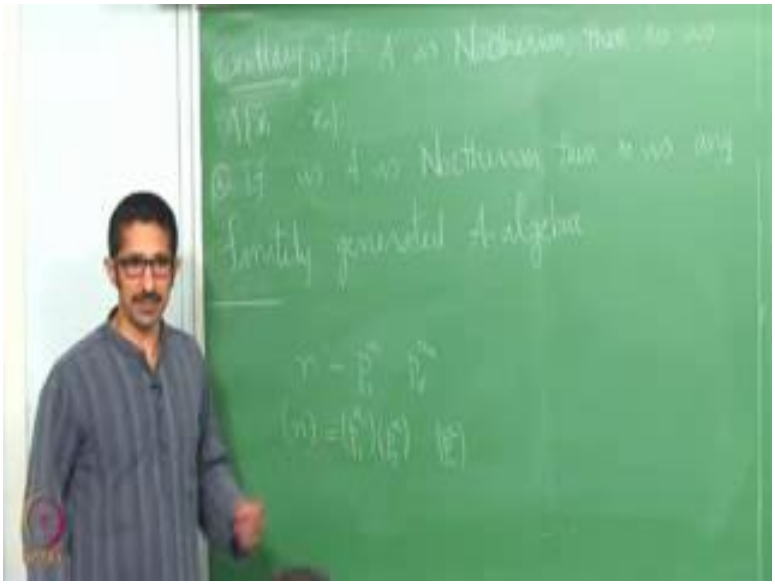
So what does that contradiction say? That our assumption that we have made that the ideal I is not finitely generated is wrong. Which means I is finitely generated and that implies A x is Noetherian.

There is a proof given in Atiyah MacDonald which is a constructive proof from, so starting with an ideal I in A x, one constructs a generating set. It is like an algorithm. You look at; for each n, look at the; look at a construct an ideal in A and use the fact that ideals of A are finitely generated to get a generating set finite generating set for I in A x. So do go through the proof and try to understand that. That is slightly lengthier, but it is a constructive proof it is it gives a concrete generating set for a given ideal in A x. So that is also a nice proof. This is, but that is more slightly more lengthy and it is yeah know techniques are similar, but it is slightly more lengthy and a constructive proof. So do go through that proof as well.

So this says that you know k x y is Noetherian, in k x y there exists given any n there exists an ideal which is generated minimally generated by n elements, but there are no elements which are infinitely generated; however, large n is every ideal is finitely generated. This is again I will I mean I can give you I n for each n, but you know try to construct on your own try to see if we can construct. I can even give you a hint saying that you can think of ideal generated by monomials. What are monomials polynomial is a you know some of you know monomials. So a monomial in polynomial ring is of the form x 1 power alpha 1 to x n power alpha n. So here it will be some x power a y power b try to think of ideals generated by monomials.

So the this says that every polynomial ring with finitely many variables is a polynomial is Noetherian.

(Refer Slide Time: 17:04)



So if A is Noetherian then so is more generally if A is Noetherian then, so is any finitely generated A algebra. How does any finitely generated A algebra look like? Quotient of A x 1 up to x n. So if a is Noetherian, this is Noetherian therefore, any coefficient is Noetherian. Therefore, any finitely generated a algebra is Noetherian this is a you know very important result that goes into you know I mean finite generation of ideals in in polynomial ring is something that is one of the most basic thing required in algebraic geometry. Because when we are considering a set in k n, and look at all the polynomials which vanish on all the points, all the polynomials whose 0s are this given set this this there will be infinitely many polynomials, but when we have to look at the properties, we only have to look at only finitely many of them the generating set it is. So there are you know I mean this is something that is very basic required in an algebraic geometry.

So this says that Noetherian rings are kind of special, they are nice see we in in Z in Z or in even in any. So let us when we wanted to talk about analogues we always start with Z. In Z if you take any integer n I can write this as p 1 power alpha 1 up to p n power alpha n where p 1 up to p 1, p 2 up to p n are sorry. So p r, alpha r they are different distinct primes; that means, it has a unique prime decomposition.

Now, the question is how far we can push this. So one thing like say if I look at the ideal generated by n, I can write this as ideal generate by p 1 power alpha 1 times ideal generated by p 2 power alpha 2 ideal generated by p r power alpha r. These are not prime ideals. The ideal is not a prime ideal if alpha 1 is bigger than 2 bigger than or equal to 2. This ideal will not be a prime ideal, but it is radical is a prime ideal. So in general Noetherian rings there is what is called a primary decomposition.

(Refer Slide Time: 21:33)

So let us look at, what is mean by primary decomposition? Let us begin with definition of primary ideals. This is you know for the definition of primary ideals and so on, we do not need any noetherianness and it is Noetherian you know things are much more nice, you know many properties are nice when the ring is Noetherian.

So let us start with a commutative ring A be a commutative ring. Did we define a primary ideal earlier? No. An ideal proper ideal A is said to be a primary ideal if, so I is said to be a prime ideal if x y is in I implies either x is in I or y is in I, equivalently A mod I is a an integral domain. So here we say this is said to be a primary ideal if, for x comma y in a x y is an I implies either x is in I or a power of y is in I. Or in other words if a product is in I and one of them is not in I the other one need not be in I, but some power of this belongs to I.

This will be more clear if you look at the equivalent statement. This is equivalently if I look at A mod I, if I look at A mod I, x y is in I if you translate into A mod I, it says x

bar y bar is 0, x bar y bar is 0 and suppose x is not in; that means, y is a non zero divisor in A mod I. If it is a non zero divisor; that means, there exists some x, with not in I such that x bar y bar is 0, but then in that case this should be true; that means, y bar power n should be 0; that means, every non zero divisor is a nilpotent, y will be a non zero divisor. If I assume that x y is in I and x is not in I implies y power n is in I for some n.

Student: sir is this condition equivalent to x y belongs to implies either some power of x belongs to I or something.

I mean these 2 are;

Student: yeah but equivalent as an if some power of x or some power of y n comes to I

Yeah.

Student: then if we take, suppose some power of y does not belong to n then it says that x should belong to n.

So see that is what here x and y they do not really distinguish between each other. I mean x y is same as y x. So you can switch the roles of x and y. I mean what it says is that, if there is a product with you know if there is a product with one of them not in I, then some power of the other element should be in I.

That is exactly what I what we are seeing in the equivalent form here, that when do you say x y is in I with one of them not in I, which means we have x bar y bar is 0 with x bar non zero; that means, y bar is a 0 divisor. It is a 0 divisor in A mod I, but then the conclusion is that it should be nilpotent, y n is in should be in I, or in other words y bar power n should be 0; that means, y is y bar is nilpotent in A mod I. Or in other words the equivalent form is every non zero 0 divisor is nilpotent. Every I mean 0 is also of course, every 0 divisor is nilpotent in A mod I. So can you give me a first example of a primary ideal, can you give me an example of a.

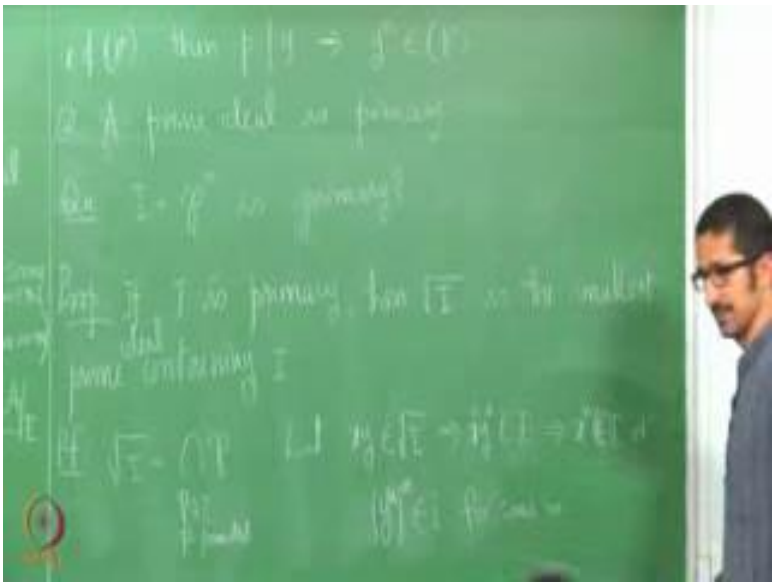
Student: (Refer Time: 28:18).

Yeah in Z or you know slightly in general. So let me write this. So example, p power n in Z, why is this primary? How do you justify this?

Student: some where it is p power n with power n divided.

If x y belongs to the ideal generated by p power n; that means, p power n. So x y will be of the form some m times p power n; that means, p divides either x or y. So if x is not in p power n; that means, p cannot divide p power n does not divide x. So p will divide yeah p power n has to divide y in this case, some power of p, p has to divide y.

(Refer Slide Time: 29:48)



If x is not in p power n then p divides y because p power n is on the right hand side. So that that much power at least that much power of p should be there in this product, p power n is not there in x. So therefore, some p will be there in the prime decomposition of y; that means, p divides y and that would imply that y power n will be in p power n, at least there could be some smaller power there, but y power n has to be.

Now, can you read this line once again and give me an example of a primary ideal in general so.

Student: p x and x in.

No I will just start with a commutative ring A. What if there are no 0 divisors? You said something? It is true. If the ideal is maximal slightly more general. If it is a prime ideal right. If ideal is prime, then there are no non zero 0 divisors. So this is vacuously true, for that ideal any prime ideal if x y is in I that will imply either x in I or y is in I. So therefore, this is true with n equal to 1. So therefore, every prime ideal is; a prime ideal is primary.

Student: Sir.

Yeah.

Student: x y belongs to I then x primary is equal to 0 a mod I.

Sorry?

Student: if x y belongs to I then x bar y is equal to 0 for any a mod I.

Yeah.

Student: but a mod I is in integral domain.

Yeah.

Student: x y is not o then (Refer Time: 32:35).

Y bar has to be 0; that means, why is in I if I is prime, you are talking about I being prime?

Student: they showed is it that resulting y power n belongs to I.

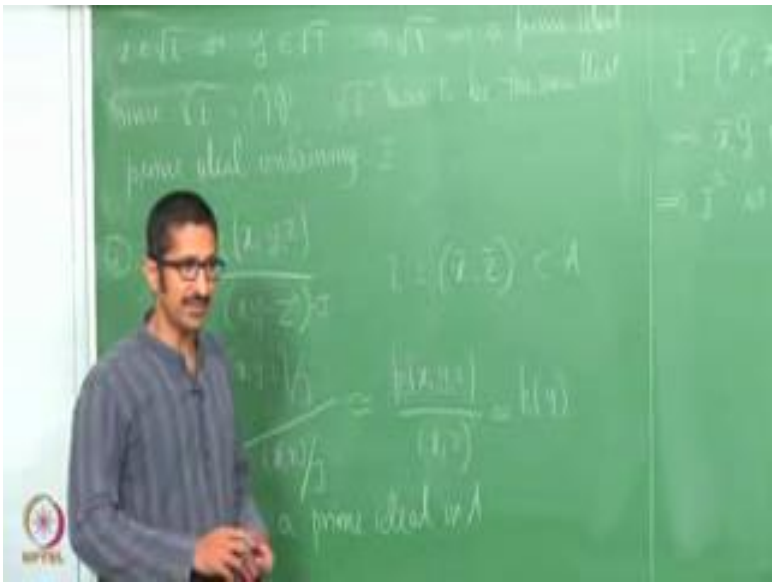
For some n, so for n equal to 1 this is true if yeah.

Student: what about power of n sir?

Yeah. So the question is, if I take p power n I in general I take p power n, is this is primary? So there is this example which says that I will come back to this. This question makes sense. I mean it has it is slightly more interesting after you know we prove one basic result, that if I is primary, then radical of I is the smallest prime containing I. See we know that radical of I is prime ideal. We know that radical of I is equal to intersection of prime ideal p prime. We are saying that if I is primary, you can pin down to one prime ideal which is the smallest one which contains I. So let us let us look at x y be in the radical of I; that means, some power x n power x n y n belongs to I by definition of radical.

Now, I is primary; that means, either x power n belongs to I, x power n belongs to I or y power m y power n whole power some m belongs to I for some m.

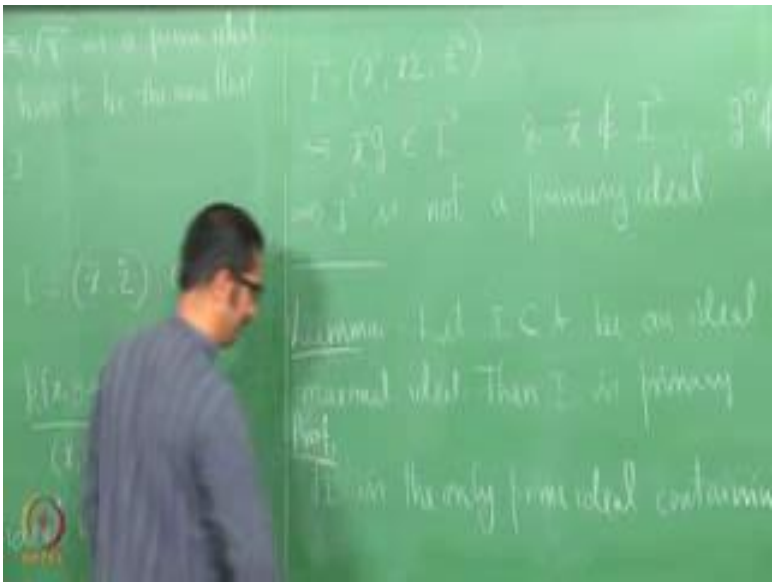
(Refer Slide Time: 36:21)



What does that say x belongs to radical of I, or y belongs to radical of I right y power n whole power m is same as some power of y, some power of y belongs to y means y is into the radical. So what we have shown is that x y is in the radical implies either x is in the radical or y is in the radical. Which means radical of I is a prime ideal, and by their in a definition it has to be the smallest prime ideal the smallest prime ideal.

So if I is primary the radical is prime. So now, let us look at this question, p n this is an ideal with whose radical is p. So this question asked if the converse of this is true, that the radical is a prime ideal can we say that I is primary or not. Unfortunately this is not true. Look at this ring A equal to k x y Z mod x y minus Z square. And look at I equal to x Z, x bar Z bar in A. Then this is a prime ideal in A. Why is it a prime ideal? What is A mod I see this is an ideal containing this right call this J. Then what is A mod I, A mod Is k x y Z mod J modulo x Z mod J which is isomorphic to k x y Z mod x Z and this is isomorphic to k y this is an integral domain. So therefore, this is a i is a prime ideal in A.

(Refer Slide Time: 40:04)



Now, let us look at I square. What happens to I square? Can you write down what is I square? I square is the ideal generated by x square x bar square x bar Z bar and Z bar square, but now in A what is Z bar square? Z bar square is same as x bar y bar, x bar y bar minus Z bar square is 0 in A. So therefore, x bar y bar and Z bar square is same as x bar y bar. So this means that x bar square sorry x bar y bar belongs to I square. Right and x bar is not in I square, for this to be a primary ideal some power of y should be in I square. Do we have that?

So x bar is not in I square and y bar power n is also not in I square for any n. So that implies that I square. So here I should first remark that I is a prime ideal in A. So this is not a primary ideal. I is a prime ideal, but I square is not a primary ideal. So power of prime need not be a primary ideal, is that clear? If you take a prime ideal and look at it is powers that need not be a primary ideal. In the case of Z, it is true, but in general that is not true. In Z primary ideals are precisely the ideals which are product of I mean powers of prime ideals. I be an ideal such that radical of I is maximal.

Now, radical of I is a prime ideal, need not necessarily imply that I is primary. Suppose your radical is a maximal ideal, can we say I is primary? Let us look at A mod I, what are the ideals of A mod I?

Student: ideals containing I.

Ideals containing I?

Student: J mod I.

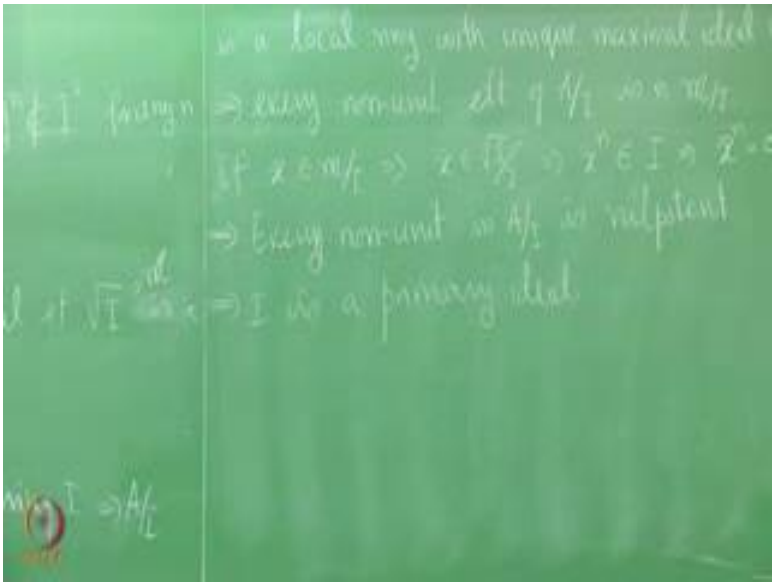
J mod I where J is an ideal content, what are the prime ideals of A mod I? Prime ideals of a containing I. Now radical of I, what is radical of I?

Students: (Refer Time: 44:34).

It is by definition or characterization it is the intersection of all prime ideals containing I. And that is a maximal ideal right. Intersection of all primer ideals containing is a maximal ideal. Therefore, the only prime ideal containing I is the maximal ideal which is the radical of I, that is the only prime ideal containing I.

So radical of I is the only prime ideal containing I. That means, A mod I is a local ring with unique maximal ideal M mod I. What does that say all the; you know elements look at the elements of A mod I, either they are unit is or they are in M mod I.

(Refer Slide Time: 45:51)



So this implies A mod I is a local ring with unique maximal ideal M mod I. So what is m here I will call this m. So elements of A mod I either they are in M mod I or in the complement of M mod I. If it is not in M mod I it is a unit. If it is in M mod I it means that x bar belongs to m, which is the radical of I. So; that means, some power of that belongs to I which means x bar power n is 0; that means, every non unit is nilpotent.

Now, the equivalent statement for primary ideal says that every 0 divisor is nilpotent. Here we are proving that every non-unit is nilpotent. Non unit cannot be a 0 divisor. So anything that is non zero divisor is nilpotent here. In particular, every 0 divisor is nilpotent. Therefore, this is ideal I is primary ideal. So let me write this. This implies every non unit element of A mod I is in M mod I. If x bar belongs to M mod I; that means, x bar belongs to radical of I mod I which means x bar power n belongs to x power n belongs to i; that means, x bar power n is 0. Which means every non unit in A mod I is nilpotent. And that implies that I is a primary ideal. So what we have proved here is, then I is primary.

Radical of I is a prime ideal does not imply that I is primary, but what we are proving here is that if the radical is a maximal ideal, then yes, the ideal is a primary ideal. Now we will you know continue with; so in the case of Z, we had we can say that it is like a primary decomposition. You take an ideal n Z, it is like decomposition into a primary ideals. We will see such a similar decomposition in the case of Noetherian rings.