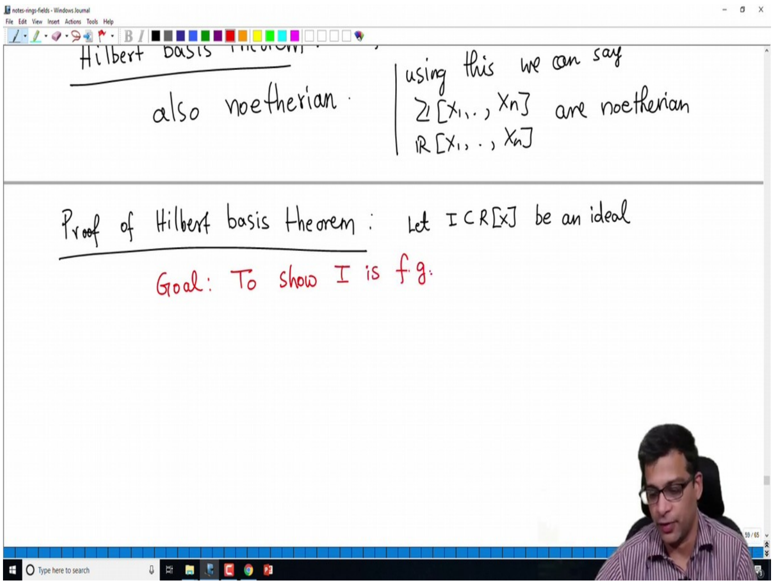
Introduction To Rings And Fields

Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 22
Hilbert Basis Theorem

(Refer Slide Time: 00:18)



Let us continue now, in the last two videos we have looked at Noetherian rings. These are rings where every ideal is finitely generated or alternatively these are rings where every ascending chain of ideals stabilizes. We looked at various examples of Noetherian rings, that we know integers, polynomial rings, over fields in one variable, even in polynomial ring in one variable over the integers.

And, we also looked at a couple of examples of rings that are not Noetherian, a polynomial infinitely many variables or a field for example, or the ring of continuous functions from R real numbers to real numbers. And, we also observed that if a ring R is Noetherian any quotient ring R mod I is Noetherian for every ideal I.

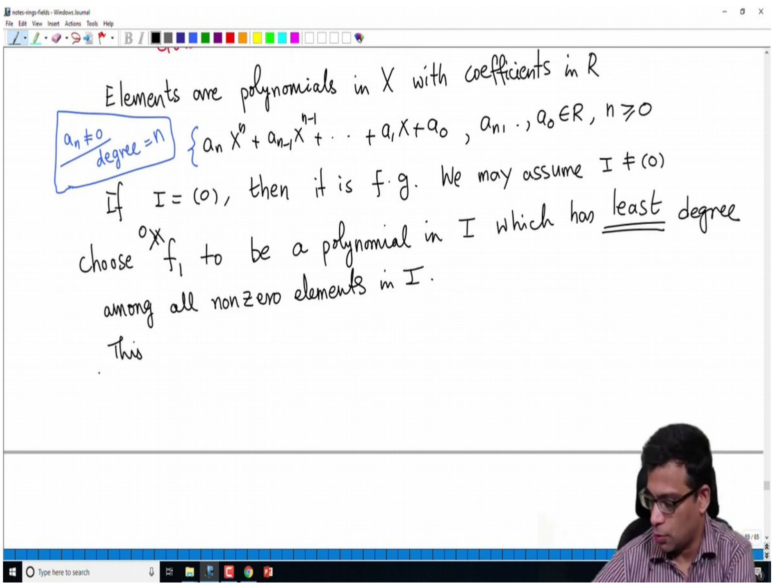
So, now the main theorem in the study of Noetherian rings is called the Hilbert basis theorem. So, that is on your screen now, it says that if you have a ring which is Noetherian, then a polynomial ring over it in one variable is Noetherian also ok.

So, let us prove this and using this of course, we can apply induction to prove that ring polynomial ring in finitely many variables over a Noetherian ring is also Noetherian. So, after proving the theorem I will remark on how to apply it. So, this is the proof of Hilbert basis theorem.

So, today's video is dedicated to proving Hilbert basis theorem. So, we are going to use the original definition of Noetherian rings and we will show that if I is an ideal in R x, then every ideal it is finitely generated. So, let us start with that let I be an ideal so, an arbitrary ideal. So, remember the goal is so, I will write that here goal is to show I is finitely generated.

So; that means, we have to exhibit a finite set of elements of I, which generate it as an ideal ok. So, what we will do is the following; so, among all elements in I remember: what are elements in I these are polynomials with coefficients in R in 1 variable x.

(Refer Slide Time: 02:37)



So, elements of I indeed elements of R X it is itself are polynomials in X with coefficients in R right. These are all how elements of the polynomial ring look like. So, in particular they are exact they will right in mathematical symbols, they are of this form where x is of course, a symbol an through a 0 are elements of R and n is a non negative integer. So, n is 0 1 2 3 and so on ok.

So, these are elements of R. So, now, I being an ideal consists of some of some such polynomials if I is 0, if I is the 0 ideal then it is certainly finitely generated. So, we may assume I is not the 0 ideal right, 0 ideal is certainly a finite ideal, it consists of only the 0 element.

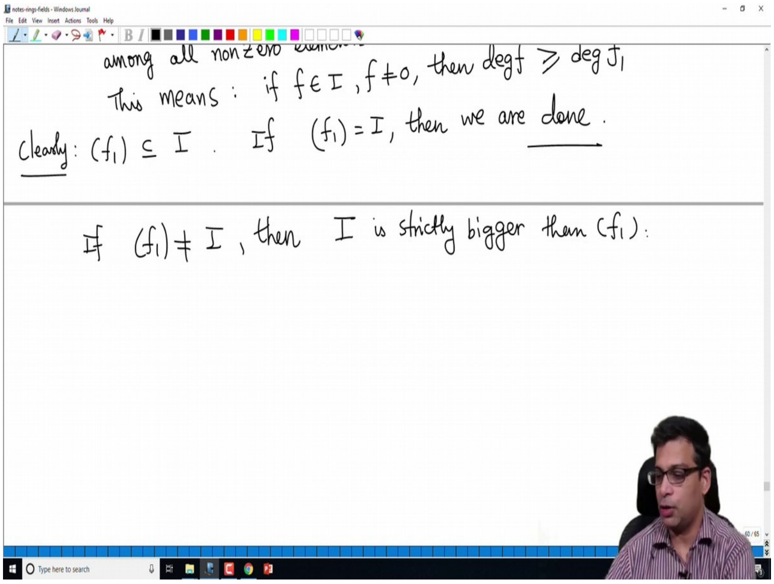
So, it is surely finitely generated. So, we may assume I is not 0; that means, it contains nonzero polynomials and for every nonzero polynomial we have what is called the degree right. So, what is the degree of this? So, if a n is nonzero we always assume that otherwise we will not even write that term. So, degree of this is n. So, this is the largest power of x that you see in the polynomial. So, this is defined for every nonzero polynomial. So, we look at degrees of all non-zero polynomials in x in I.

So, choose f, f 1 to be 1 the following, choose f 1 to be a polynomial in I which has least degree. So, choose f 1 to be a nonzero polynomial, f 1 is nonzero to be a polynomial in I which has least degree among all elements, all of course, non-zero elements; so, that I will forget maybe sometimes among all nonzero elements in I ok. So, of course, you can avoid you separating out nonzero elements by declaring the degree of the 0 polynomial to be 0.

So, I want to take the polynomial which is least degree among all non-zero elements. So, I remove 0 element. What am I doing. So, f I of course has infinitely many elements typically. So, we look at degrees of each nonzero element of I. So, these are all non-negative integers it can be 0. For example, if I consists contains a nonzero constant it is degree is 0 so, potentially 0, but there are non-negative integers.

So, among all these non-negative integers there will be 1 with which is smallest, non-negative integers have this property that any set of non-negative integers has a least element. So, we identify that maybe it is 3, maybe 3 is the least degree of polynomials in I. There would be lots of polynomials of degree 3 in I perhaps, but I am just going to pick one of them. So, f 1 is not unique definitely, but there is some such polynomial.

(Refer Slide Time: 06:32)



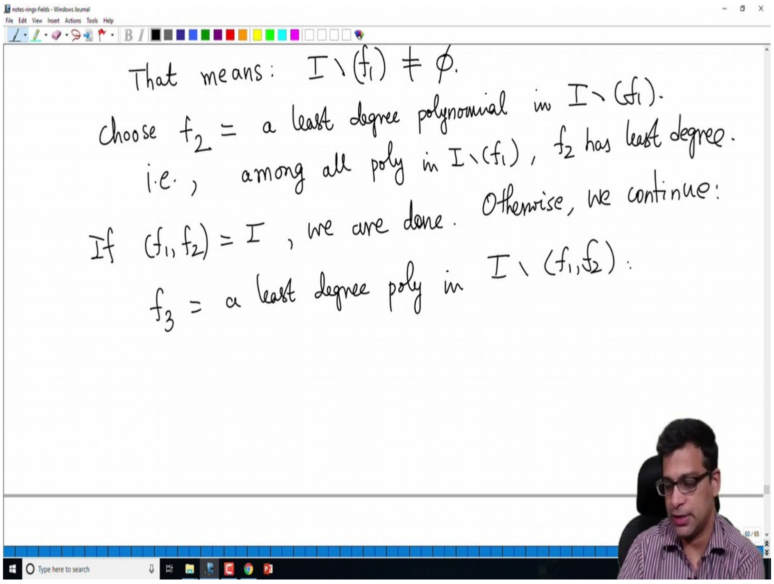
This means so, I am going to spell this out because it is an important fact, important property of how we are choosing f 1. So, this means that if f is any non-zero element, then degree of f is greater than or equal to degree of f 1, because of the choice of f 1 maybe it is equal to degree of f 1 that is allowed, but it can be strictly smaller. Because, if it is smaller than the degree of f 1 is not the smallest degree of an element in I, it has smaller degree elements.

So, we would pick that or even something smaller. So, if f is in I and it is non-zero then degree is at least degree f 1 ok. So now, we have chosen the first element. So, like in a previous proof in the previous video where we were doing proving that ascending chain condition implies Noetherian S. We are going to can construct an infinite chain, sequence of elements of I and this is our first element f 1 is the first one.

Now, consider the ideal generated by f 1. So, of course, it is contained in I clearly. So, clearly the ideal generated by f 1 is an I, because f 1 remember is in I. So, I emphasize that here f 1 is a I or ideal generated by f 1 is in I. If, it is actually equal to I, then we are done, we are done because what is the goal which I wrote here we want to show that I is finitely generated.

If, I is actually generated by f 1 it is generated by a single element, which is what we want which we want in fact, you have finite set of generators. So, if f 1 is I we have done. If not in other words if the ideal generated by f 1 is not I, then I is of course, strictly bigger because certainly it contains f 1, but if it is not equal it is strictly bigger.

(Refer Slide Time: 08:50)

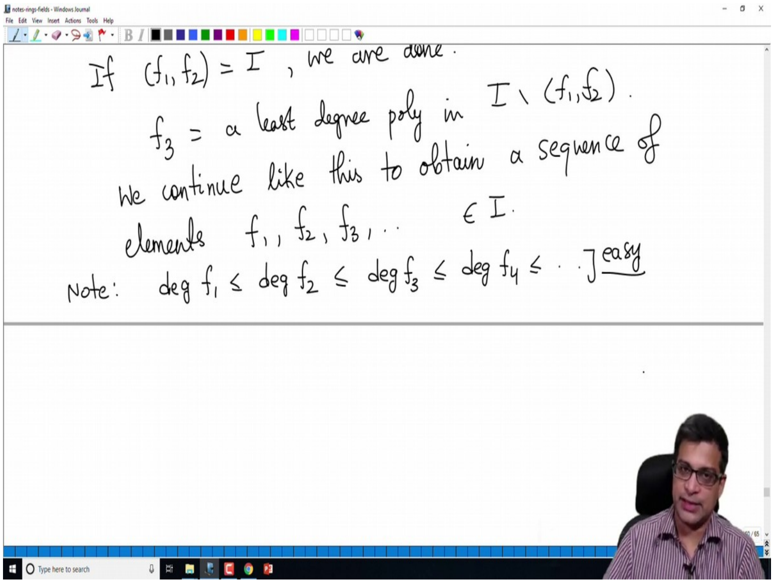


That means, yet another way of saying that is that the set I minus f 1 is not empty. In other words elements in I that are not in f 1 is a non-empty set. There are elements in I that are not inside the ideal generated by f 1. Now, choose f 2 to be exactly as before, how did we choose f 1, f 1 to be a least degree polynomial among all elements in I. Now, I do not do it among all elements in I, but I choose f 2 to be a least degree polynomial in I minus f 1. So, this means among.

So, that is: among all polynomials in I minus f 1, f 2 has least degree. So, said another way if f some other polynomial f is in I minus f 1 it is degree is at least the degree of f 2. So, again remember f 2 is not unique with this property, there is perhaps lots of polynomials which have least degree, but I am going to just choose 1 I do not care how I chose this I just choose f 2 to be that, now we continue. If, f 1 f 2 is equal to I, we are done again, meaning we have shown that I is finitely generated by these two elements.

Otherwise, we continue and how do we continue? We simply take f 3 to be a least degree polynomial in I minus f 1 f 2 now, right. I if I is not equal to the ideal generated f 1 f 2 it must be strictly bigger than ideal generated by f 1 f 2; that means, there are elements in I that are not in ideal generated by f 1 f 2 lots of them infinitely many may be, but I am going to choose the one which has the least degree. And, of course everywhere I am taking nonzero, but that is me I do not need to write that here because 0 is in the ideal generated by f 1 f 2. So, only elements in I minus f 1 f 2 will be non-zero.

(Refer Slide Time: 11:27)



So, we continue like this to obtain a sequence of elements f 1, f 2, f 3 and so on in I. And, just to repeat for you the procedure of how to choose these. Suppose, you have chosen 100 of them, f 100 is chosen, how do you choose f 100 and 1 you choose it in the following way you look at the ideal generated by f 1 f 2 f 3 up to f 100 this is a finitely generated ideal which sits inside I. So, if it is equal to I we stop we are done there is no more work to do, but if I is strictly bigger than the ideal generated by f 1 f 2 f 100.

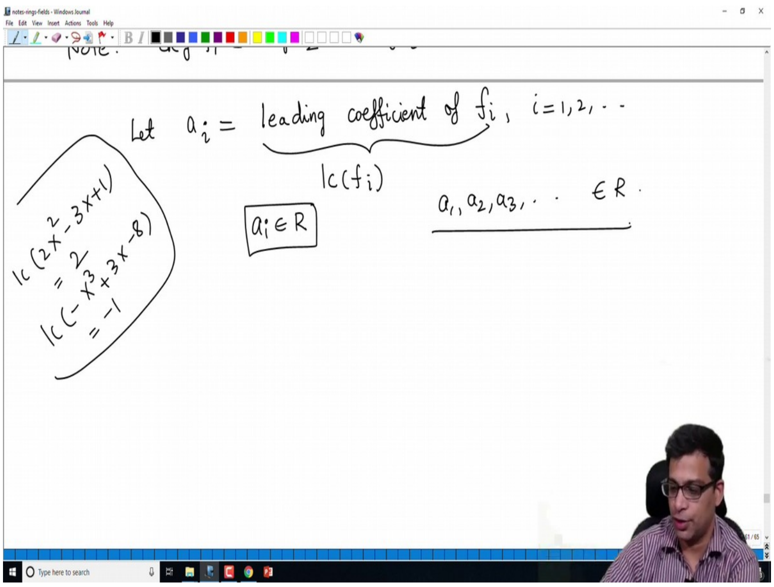
There are nonzero elements in I minus the ideals generated by f 1 f 100. Among all those elements we pick a polynomial with the least degree which we call f 100, f 101. And, then we continue, remember that if this process stops at any point we achieved our goal which is that I is finitely generated. So, we have to rule out the possibility that this process continues forever. And, we have now constructed this and I will only remark now, this is something we will use later. Note that degree of f 1 is less than degree of f 2, less than degree of f 3, less than degree of f 4, and so on.

So, degrees keep increasing why is that? Because, when you are choosing f 1 you are choosing a polynomial with the least degree right. So, in other words when I wrote earlier if f is any element of I non-zero then degree of f is greater than equal to degree f 1, f 2 is one such element right because f 2 is being chosen later. So, degree of f 2 will be greater than equal to f 1. Now, f 3 will be chosen after f 2. So, if f 3 has strictly a smaller degree than f 2, we would not have chosen f 2 in step 2.

So, degrees keep increasing like this is very easy point, think about it for a minute pausing the video, think about it for a minute if it is not clear to you. At each stage we are picking the lock a picking a polynomial with the least degree and if we have chosen f 100, f 101 is to be chosen in the next step. So, if f 101 has smaller degree than f 100, why would we choose f 100 now. We would have actually chosen something which has a smaller degree.

So, f 1 f 100 and 1 which is actually chosen at a later stage will have a bigger degree than f 100, when I say bigger it could be equal, but it will not be less than it could be less than or equal to we have this relation now. So far we have not used hypothesis remember we cannot in general wrote that R x is Noetherian for arbitrary rings R. We want to use the fact that R is Noetherian and that is done in the following way ok.

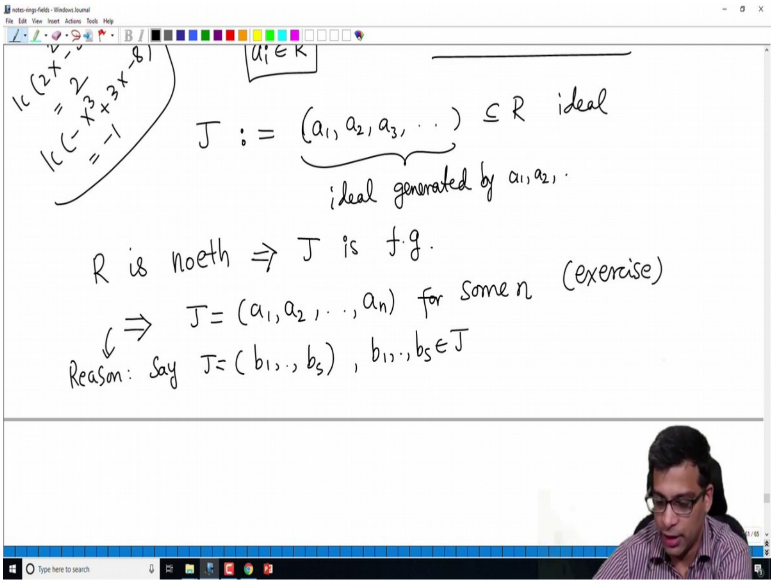
(Refer Slide Time: 14:47)



So, what we do is let a i. So, now, I have constructed f 1, f 2, f 3 and so on. So, we going to work with these now let ai, be the leading coefficient leading coefficient of f i. So, we do this for every i, what is the leading coefficient. So, remember I will simply say this by saying lc of fi, lc of f i simply the coefficient of the largest degree term you have.

So, lc of 2 x squared minus 3 x plus 1 is 2, lc of minus x cubed plus 3 x minus 8 is minus 1. So, the leading coefficient is simply the coefficient which is in front of the largest power of x in your polynomial. So, certainly a i is in R and this is where we will go to R now and use the hypothesis. So, we have now a 1, a 2, a 3 and so on these are all elements of R. So, we have an infinite sequence potentially infinite sequence of polynomials and we are now forgetting the polynomial except the leading coefficient we take the collection of leading coefficients.

(Refer Slide Time: 16:05)



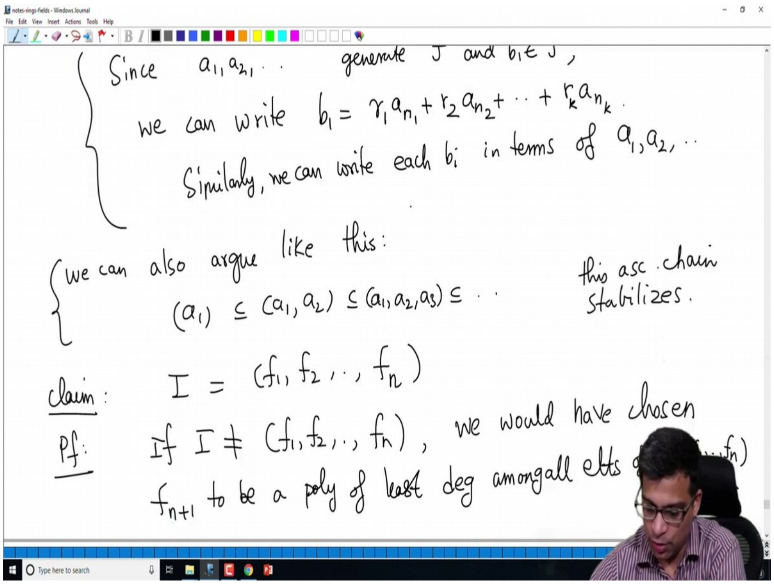
And, define now J to be the ideal generated by all these leading coefficients. So, this is an ideal by definition right. I am not taking the set of these leading coefficients of course, that is certainly not an ideal I am taking the ideal generated by. So, these ideal these are notation remember generated by a 1, a 2 and so on.

Now, my hypothesis is R is Noetherian correct, this implies J is finitely generated, because R is Noetherian, every ideal of R is finitely generated in particular J is finitely generated. Now, I claim that we know that there is in fact, a finite set of generators.

But, I can assume that J is actually equal to a 1, a 2, a n for some n ok. This is a little exercise for you: what we actually get from the statement that J is finitely generated is that there is a finite set of generators. They need not be to begin with maybe the finite set of generators you are given are not a 1, a 2, a they are not they are not actually is, but you take any of the generators. So, maybe I will just quickly write the reason.

So, reason for this reason for this implication is that let J be generated by let us say b 1, b s ok; b 1 through b s are inside J right. We know that J is finitely generated; that means, J belongs sorry J is generated by some finitely many elements of it contained in J. Now, we know that a 1 through a n and so on I mean infinitely many a i's potentially infinitely many a i's generate J.

(Refer Slide Time: 18:19)



So, since a 1, a 2 and so on generate J and b 1 is in J let us use first b 1, we can write b 1 as some r 1 a 1 plus I do not know what actually it need not b 1. So, r 1 a n 1 plus r 2 a n 2 plus r k a n k, remember that even though J has infinitely many generators does any particular element of J can be written as a finite sum like this.

Similarly, we can write each bi in terms of a i or a 1, a 2; the point is maybe b 1 will require the first 1000 a ns b 2 requires first 1 million a i s, b 3 may require first billion, but I do not care I will because b 1 through bs is a finite set, I will look at all the a i's that appear in b 1, all the a i's that appear in b 2, all the a i's that appear in bs and look at the largest index of a that appears in those and take those up to that index a 1 a 2 an.

So, the point is J could be maybe generated by 10 bis, but if I include a i's maybe I have to go to 1 million, because maybe b 10 requires up to a million, but I do not care about what n is it does not matter to me, if n is very big I am not looking to find an efficient set of generators, I am only interested in finding generators. So, that I can say first n of them generate J.

So, this is just an argument to explain that, again please pause the video and think about it if it is not clear to you and you can ask questions if it is something is not clear to you still. Another way to see this is we can also argue like this. So, we can consider the chain like this so, a 1, a 2, a 1, a 2, a 3, and so on right. So, this chain this ascending chain stabilizes because it is an ascending chain of ideals in Noetherian ring R.

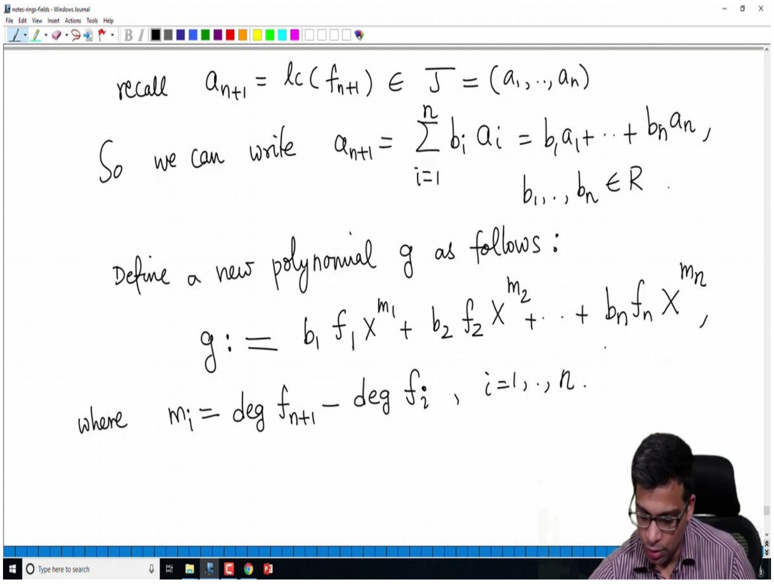
So, it stabilizes; that means, it is equal beyond some point they are all equal, but they must all equal J because if it is not equal to J we would have continued ok. So, this is another argument to show that J is equal to the ideal generated by a 1 through a n. Now, finally, to finish the proof I claim that, I now go back to the ideal I in r x. In fact, will be generated by remember that just to recap the proof, I have started with an arbitrary ideal in R x, I is an arbitrary ideal in R x, I have constructed an infinite sequence by describing the by the process described at the beginning of the proof.

And, I have taken the leading coefficients each of each of them; the ideal of the leading coefficients which is actually an ideal J inside R is finitely generated. So, it is finitely generated in fact, by the first n leading coefficients now to finish the proof I am claiming that I is in fact, generated by those n polynomials, we do not need to continue.

And, the proof of this is the following. Remember how we were constructing these f i's, if I is not equal to f 1 f 2 f n, we would have chosen f n plus 1 remember; remember the construction of f i's. If, the ideal generated by the first n of them is not equal to I we would have chosen f n plus 1 to be a polynomial of least degree among all elements of I minus the ideal generated by f n ok.

So, now, we have f 1 through f n which is not equal to I and then we continue the process that I described at the beginning of this proof. So, f n plus 1 has a least degree of all elements.

(Refer Slide Time: 23:39)



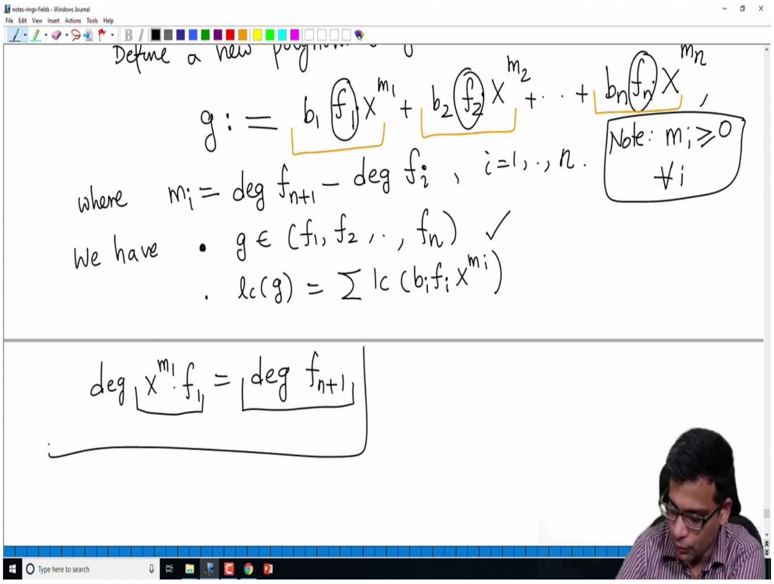
But, now let recall an plus 1 is the lc of f n plus 1, because I have defined a I to be lc of f i for every I, but this belongs to J, remember J is ideal generated by all the leading coefficients.

So, an plus 1 belongs to J, but I have just argued using the Noetherianness of R such that a 1 through an generate J. So, a n plus 1 is an ideal generated by a 1 through a n. So, we can write a n plus 1 as summation bi a i, i equal to 1 to n. So, just for clarity I will write it like this. And, what are b i's where b i's are some arbitrary elements of R I do not care what they are they are just elements of R.

Now, I forgot in the polynomial ring. I am actually now arguing inside the ring itself the coefficient ring; because J is generated by this a n plus 1 can be written like this. Now, I am going to define a new polynomial g as follows. So, g is defined as b 1 f 1 times x power m 1, I will tell you what m 1 is, b 2 f 2 x power m 2 and all the way up to bn f n X power mn, where mi is degree of f n plus 1 minus degree of f i for each i from 1 to n ok.

So, remember I remarked earlier that degrees of f i's keep increasing; degree of f 1 is less than equal to degree of f 2, less than equal to the degree of f 3, less than equal to degree of f 4 and so on.

(Refer Slide Time: 25:58)



So, these are all non-negative integers. So, note that mi is greater than equal to 0 for all i. So, I can. In fact, consider x power m 1 x power m 2 x power mn these are if they were negative of course, this will not be a polynomial x power minus 1 is not allowed inside a polynomial, but because m i's are non-negative I can put a coefficient exponent like that and it is a polynomial. So, f 1 times x 1 power m 1, f 2 times x power m 2, f n times x power mn; what kind of polynomial is g?

So, first note the following about g, we have first that g belongs to the ideals generated by f 1, f 2, f n right, that is obvious because g is actually written as f 1 times something plus f 2 time something right.

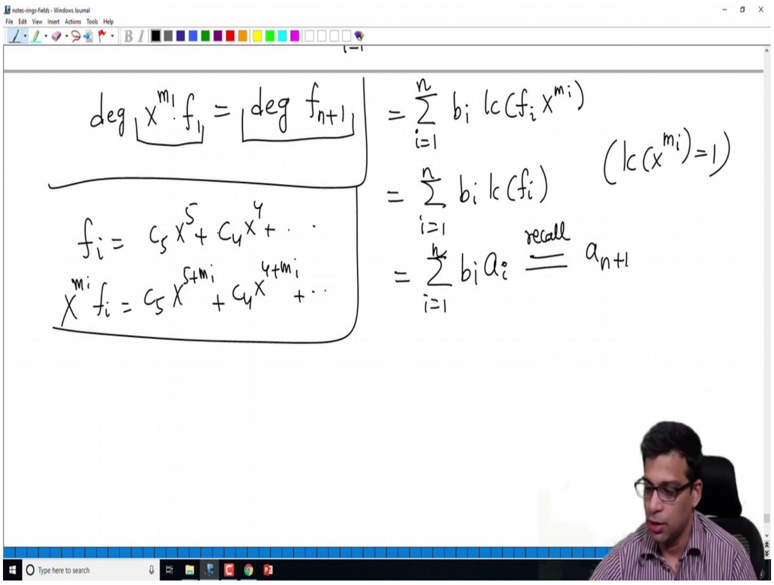
Because, f 1 is here, f 2 is here, f 1 is here. So, it is f 1 times something plus f 2 times something plus f n times something. So, it is in the ideal generated by f 1 through f n. Moreover, we also know that leading coefficient of g is equal to what, what are the degrees of these terms.

So, whatever is the leading coefficient of f 1? So, I am going to separately look at each term that appears in g. Let us look at let us look at this term, this term, this term separately. So, remember that, the reason I am multiplying by x 1 x power m 1 is. So, that the degree of x power m 1 times f 1 is actually equal to a degree of f n plus 1 right. Degree of f 1 is potentially smaller than degree of f n plus 1 by, but I am providing the remaining x.

So, by multiplying by x power m 1 this term now will have equal degree equal to a degree of f n plus 1 ok. Similarly, this term now will have degree equal to degree f n plus 1. This term will have degree equal to degree f n plus 1. So, what is the leading coefficient of b 1 through of g? So, I can certainly write this as summation lc of bi f i x power mi.

So, you have a sum of polynomials the leading coefficient all this polynomials have the same degree right, because this degree is degree f n plus 1, this degree is degree f n plus 1, this degree is degree f n plus 1. So, the leading coefficient of the sum is simply the sum of the leading coefficients; leading coefficient of g is the leading coefficient of the first one, plus leading coefficient of the second one, plus leading coefficient of the third one.

(Refer Slide Time: 29:18)

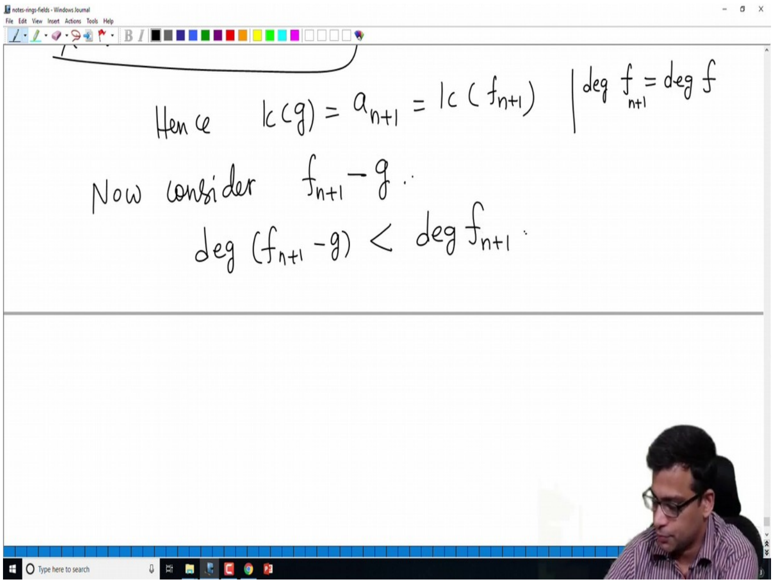


But, now continuing here, what is leading coefficient of this? This is summation leading coefficient of I can pull out bi right; bi is actually a constant term, bi is an element of R. So, this is summation. So, of course, summation goes from 1 to n, summation from 1 to n, bi times leading coefficient of f i times x power mi correct, but leading coefficient of f i times x power mi, see f I could be I am just giving an example so, f I could be sum a 5 x power 5 and so on. So, not a 5 let us say c 5 x power 5 and c 4 x power 4 and so on.

So, the leading term coefficient is c 5 and I multiply by x mi f i I get c 5 x 5 plus mi c 4 x 4 plus mi plus and so on. So, the leading coefficient does not change. From f i when I multiply by x power mi, because the leading coefficient of x power mi is 1 in general when you multiply 2 polynomials leading coefficients get multiplied also.

Here leading coefficient of f i mi is just leading coefficient of f i times leading coefficient of x power mi, but leading coefficient of x power mi is 1 so, I can omit this. So, bi times leading coefficient of f i, but what is leading coefficient of f i? Leading coefficient of f i is by definition a i. So, I have summation bi a i , but remember, what is summation bi a i , it is actually a n plus 1. So, this is from before this is actually an plus 1.

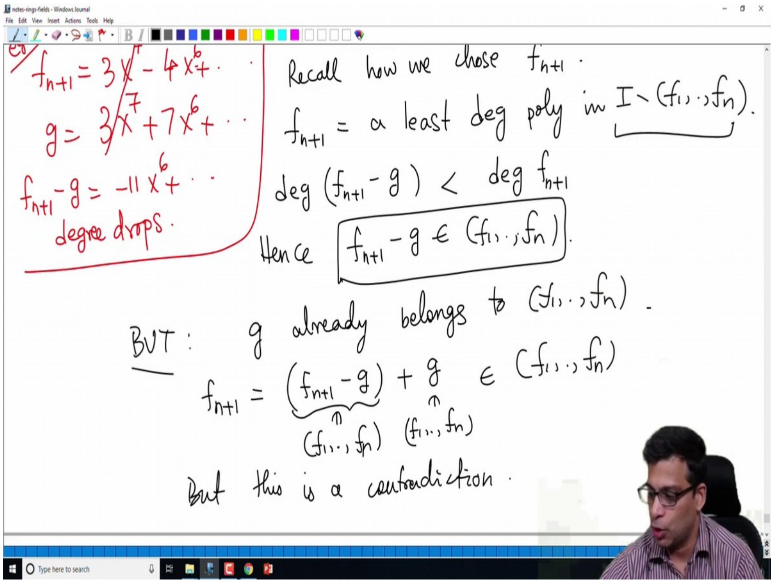
(Refer Slide Time: 31:13)



So, all this calculation proves that leading coefficient of g is an plus 1, which remember is also leading coefficient of f n plus 1. Now, consider f n plus 1 minus g. So, you have 2 polynomials, but their leading coefficients are. So, they are first of all equal degree, degree of f is equal to degree sorry degree of f n plus 1 is equal to degree of f and the largest degree in each of them is same and moreover the coefficients are also same.

So, when I subtract this degree of f n plus 1 minus g is strictly less than degree f n plus 1 right because, you have 2 polynomials as an example.

(Refer Slide Time: 32:09)



So, let us look at an example. So, you have f n plus 1 could be 3 x power 7 minus and so on so, minus 4 x power 6 I do not care what it is; what we know is that g. So, this is just an example g also has the same degree and has the same leading coefficient; so, but other terms may very well be different. What now I am doing is f n plus 1 minus g. So, when I do that this goes away.

So, what I have is actually minus 11 x power 6 and so on. So, the degree of this drops, what I mean is when I subtract one polynomial from another polynomial these two column will have they say these two polynomials have same degree and same leading coefficients. The first term will cancel out and what you are left with has a smaller degree.

But, this now tells me that degree of this is strictly less than degree f n plus 1. So; that means, and now recall how we chose, chose f n plus 1. We chose f n plus 1 to be a least degree polynomial, in I minus the ideal generated by f n right. We chose this to be the least degree polynomial. And, degree of f n plus 1 minus g is strictly less than degree f n plus 1.

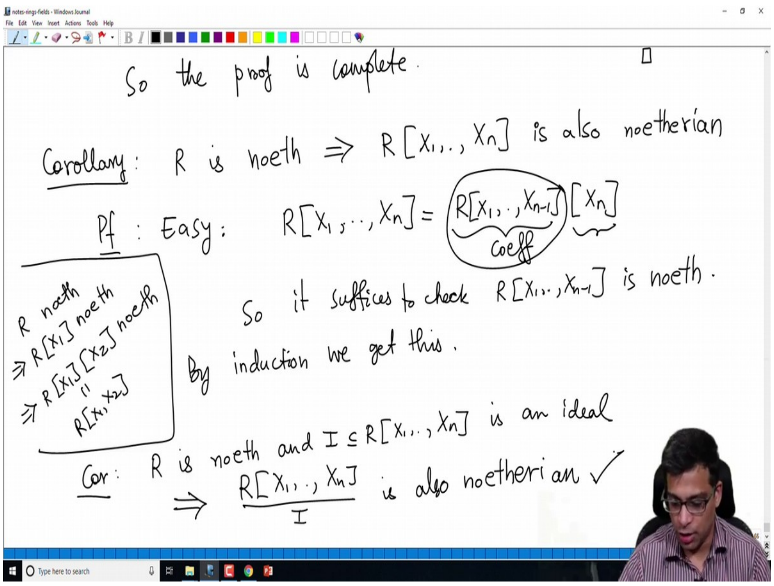
So, in fact, this tells me that hence f n plus 1 minus g is inside f 1 through f n right, is that clear, because f n plus 1 minus g is certainly an element of the ideal, because everything is happening within the ideal I. So, f n plus 1 minus g is an element of the ideal, if it was not in the ideal generated by f 1 through f n. So, suppose this is not true, suppose what is in this box is not true; that means, this polynomial f n plus 1 minus g is not in the ideal generated by f 1 through f n; that means, it is an I minus f 1 through f n.

Because, if it is not in the ideal generated by f 1 through f n it says it is in its complement; that means, it is inside this, but it then because it has smaller degree than f n plus 1 that violates how we chose f n plus 1, because that was supposed to be least degree polynomial in this compliment. So, there is no choice, but for this to belong to this.

But, g already belongs to right, g belongs to this because the way I defined g it certainly belongs to, I commented that here, g is already written as a linear combination of f 1 through f n. So, g belongs to this, now we can write f n plus 1 as f n plus 1 minus g plus g. This belongs to I sorry this belongs to f 1 through f n this belongs to f 1 through f n, g by definition belongs to this difference belongs to this because of this argument. So, this belongs to f 1 through f n, but this is a contradiction.

But, this is a contradiction because, this is a contradiction because, if f n plus 1 belongs to this we would not choose this, f n plus 1 is chosen to be a least degree element in the compliment in particular by definition, it does not belong to f 1 through f n. So, there is a contradiction. So, the proof is complete.

(Refer Slide Time: 36:15)



So, we have proved that R x is Noetherian ok. So, this is the Hilbert basis theorem. The proof is not difficult, but it could be confusing if you are seeing this for the first time. So, please go over this video as many times as you have, to make sure that you understand this argument this is a very nice argument to show that if R is Noetherian, the polynomial ring in one variable over R is also Noetherian.

So, corollaries: if R is Noetherian this implies that the polynomial ring in n variables is also Noetherian. The Hilbert basis theorem actually talks about adjoining 1 variable. But, I get the case of finitely many variables easily, because if you remember how we talked about polynomial rings for first time.

If, I do this R polynomial ring in 1 variable n variables is like this. It is actually can be thought of as a polynomial ring in X n with coefficients coming from this is just a matter of perspective right. Here variables are X 1 through X n coefficients in R here variable is X n coefficients are in this ring, but now this is become the becomes a polynomial ring in 1 variable over this ring.

So, it suffices to check R adjoined is Noetherian, because by Hilbert basis theorem if this is Noetherian by adjoining an extra variable this is Noetherian, and we keep doing this by induction we get this ok. So, this is clear right. So, all I am saying really is going from R to bigger polynomial rings, R Noetherian implies R x 1 Noetherian by diff by the statement of Hilbert basis theorem.

So, R x 1 adjoined x 2 is Noetherian. So, this is a ring it adjoined it is a Noetherian ring adjoined an extra variable is Noetherian, but this is nothing but this is just different notation for the same ring. So, polynomial ring in 2 variables is Noetherian and you keep going. As long as you are only attaching finitely many variables you get Noetherian s.

Remember of course, that if you attach infinitely many variables we know that it is not Noetherian. And finally, I will end the video with this corollary if R is Noetherian and I in R polynomial ring in n variables is an ideal this implies, the quotient ring of the polynomial ring R x 1 through xn modulo I is also Noetherian. This is because R is Noetherian by the previous corollary the polynomial ring is Noetherian and by a proposition that we did in the previous video any Noetherian ring modulo an ideal is also Noetherian.

So, this is an important statement. So, in a lot of most of the course we will only deal with polynomial rings and their quotients among other rings, but this is an important class of rings for us and these are all Noetherian because of Hilbert basis theorem. So, in this video we proved a very important theorem this is one of the most important theorems in the whole course called Hilbert basis theorem. And, from next video onwards we are going to study a special class of rings two special class of rings called principal ideal domains and unique factorization domains.

Thank you.