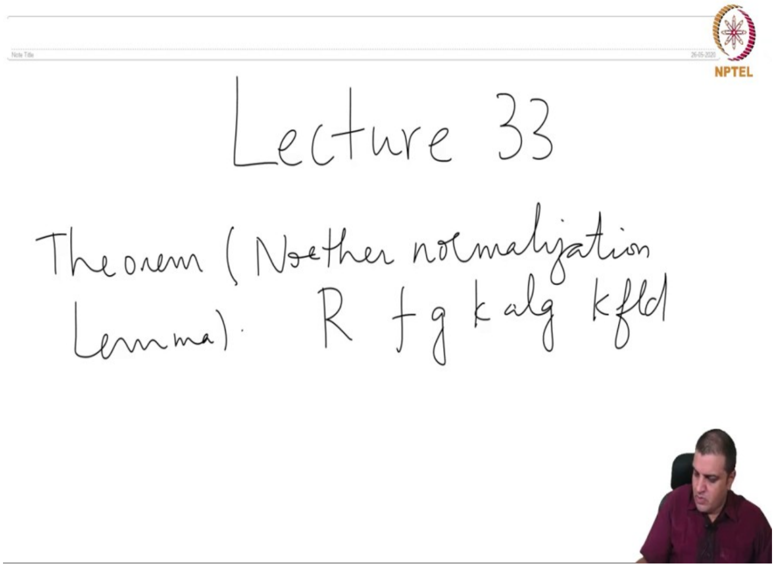
Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

Lecture - 33
Noether normalisation lemma - Part 2

(Refer Slide Time: 00:14)



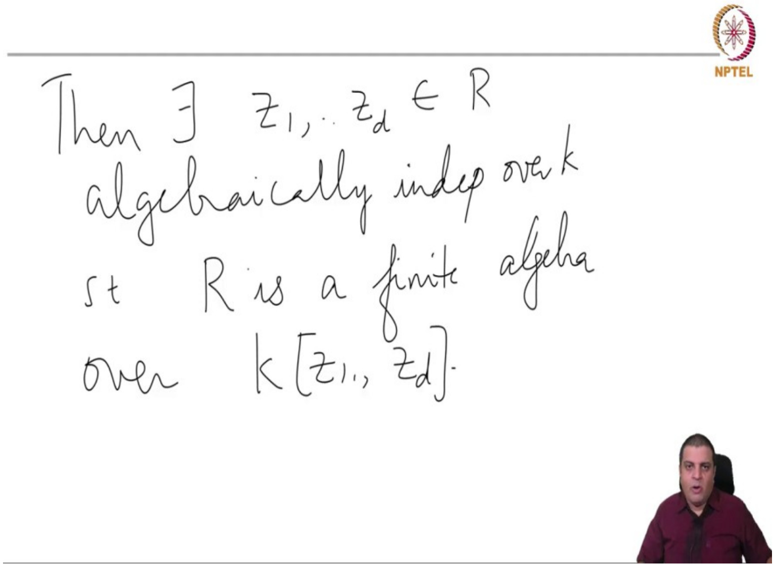
Note Title 26-05-2020

Lecture 33

Theorem (Noether normalization Lemma). R f g k alg k fld

Welcome, this is lecture 33. In this we give a proof of Noether normalisation lemma, which is the following. Let so, this is let us recall what Noether normalisation lemma was; so, theorem. This is Noether normalisation lemma. It says that if R is a finitely generated k algebra k field.

(Refer Slide Time: 00:58)



Then $\exists$ $z_1, .. z_d \in R$
algebraically indep over k
st R is a finite algebra
over $k[z_1,, z_d]$.

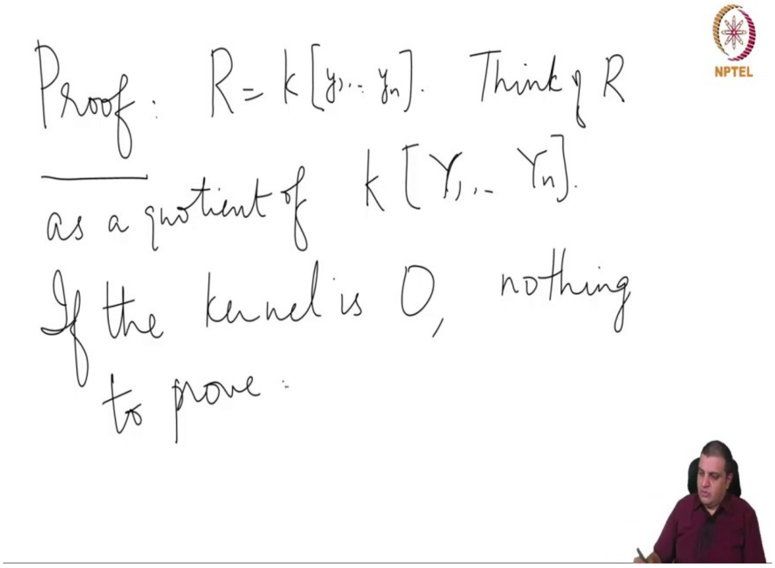
Then, there exist some finitely many $z_1,\ldots,z_d \in R$ algebraically independent over k, such that R is a finite algebra in other words as a module, which is finitely generated, finite algebra over this sub ring, which itself is a polynomial ring because this is algebraically independent.

So, we saw a proof of this last time for algebraically closed fields for infinite fields, where we did change of coordinates and the change of coordinates ensure that some element in a some relation among the generators of R can be written in a more in a monic polynomial form.

And once can be once a relation among the generators can be written using a monic polynomial, it says that one of the generators is integrally dependent on the other and hence, the morphism is finite and, then using that we can do we can bring the number of generators down. So, that was what we did last time.

So, here also the idea is the same, but the proof is a little bit more involved and we will see an example after this proof that, if the field is finite one cannot really look there are situations, where one may not be able to find a linear change of coordinates like the one we did last time. Remember, that was just y_i went to some y_i minus some appropriately chosen constant from k times y_n, ok. So, that would not be possible, ok. So, now, let us do the proof in the general case.

(Refer Slide Time: 03:15)

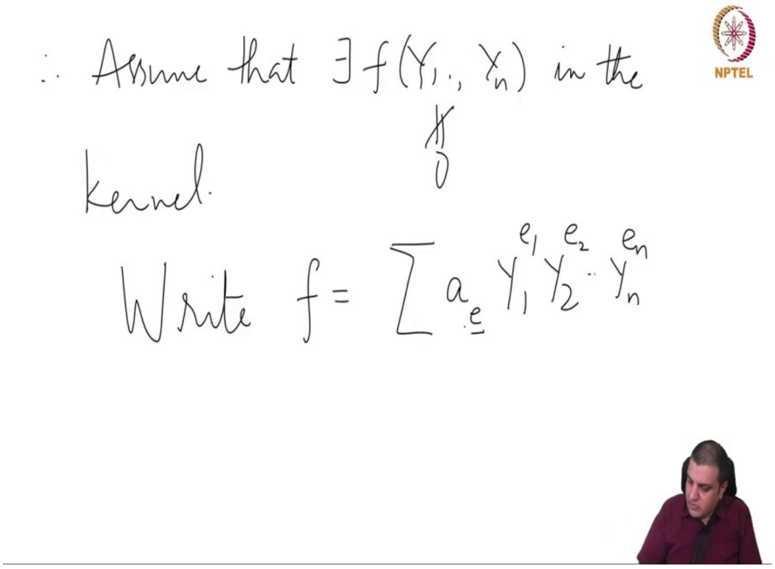


<u>Proof</u>: $R = k[y_1 .. y_n]$. Think of R as a quotient of $k[Y_1, .. Y_n]$.

If the kernel is 0, nothing to prove.

So, it is a same idea we so, let us say $R = k[y_1, .., y_n]$. And think of R as a quotient of polynomial ring $k[Y_1, \ldots, Y_n]$ in that many variables. And if this is an isomorphism the kernel is 0, then there is nothing to prove. So, all of this is the same approaches from the last time, if the kernel is 0. Then there is nothing to prove, because then this itself is a polynomial ring and it is finite over itself, so, that is nothing to prove. So, then for assume that.

(Refer Slide Time: 04:21)



∴ Assume that $\exists\, \underset{\neq 0}{f(Y_1, ., Y_n)}$ in the kernel.

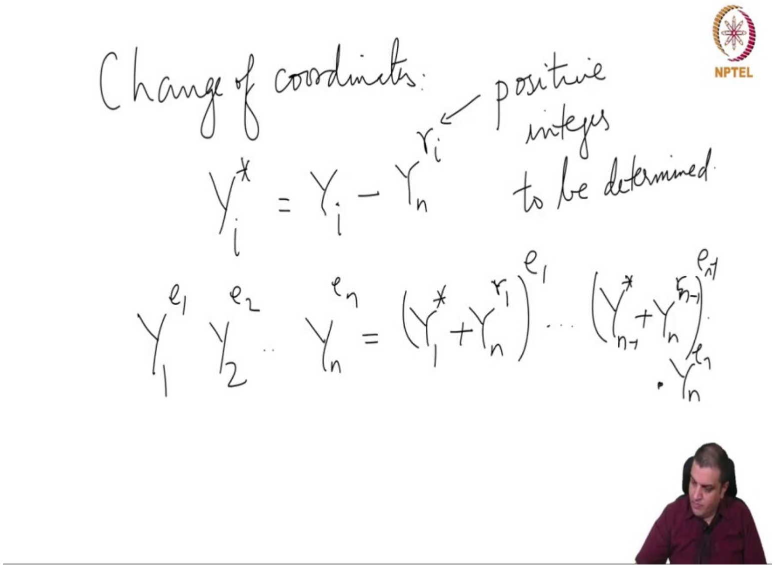
Write $f = \sum a_{\underline{e}} Y_1^{e_1} Y_2^{e_2} \cdots Y_n^{e_n}$

Therefore, assume that there exists some nonzero polynomial $f(Y_1, \ldots, Y_n)$ in the kernel. So, the idea is again to change coordinates that f takes the form of monic polynomial and that would introduce a relation of little y_n over some combination of the earlier ones, not necessarily the earlier wise.

Suppose let us write $f=\sum a_{\underline{e}} Y_1^{e_1} Y_2^{e_2} \ldots Y_n^{e_n}$. These are the variables, f is of this form.

So, now we do we would like to do a change of coordinates so, this polynomial will take the form of a monic polynomial with coefficients coming from I mean monic polynomial, and the coefficients of lower powers of Y_n may come from the earlier variables, those variables will change them a little bit. So, the change of coordinates that we will try to attempt is change of coordinates.

(Refer Slide Time: 06:14)



Change of coordinates:

$r_i \leftarrow$ positive integers to be determined.

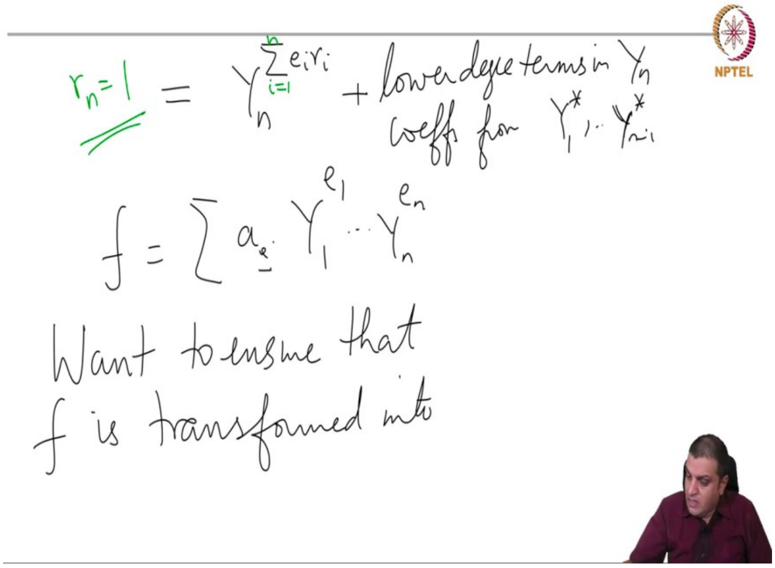
$$Y_i^* = Y_i - Y_n^{r_i}$$

$$Y_1^{e_1} Y_2^{e_2} \cdots Y_n^{e_n} = (Y_1^* + Y_n^{r_1})^{e_1} \cdots (Y_{n-1}^* + Y_n^{r_{n-1}})^{e_{n-1}} \cdot Y_n^{e_n}$$

We write $Y_i^{¿}=Y_i-Y_n^{r_i}$, but these are integers to be determined, and we will see what we have to determine.

So, then a monomial of the form $Y_1^{e_1}Y_2^{e_2}\ldots Y_n^{e_n}=\left(Y_1^{¿}+Y_n^{r_1}\right)^{e_1}+\ldots+\left(Y_{n-1}^{¿}+Y_{n-1}^{r_{n-1}}\right)^{e_{n-1}}Y_n^{e_n}$, under this change of coordinates. So, this is the expression that we get. So, this we will have a term.

(Refer Slide Time: 07:44)



$r_n = 1$ $= Y_n^{\sum_{i=1}^{n} e_i r_i}$ + lower degree terms in Y_n coeff from $Y_1^*, .., Y_{n-1}^*$

$f = \sum a_{\underline{e}} Y_1^{e_1} \cdots Y_n^{e_n}$

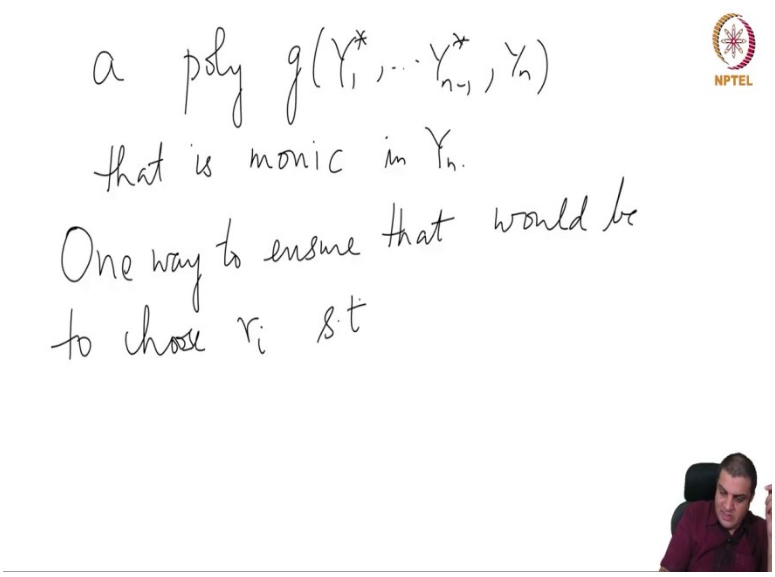
Want to ensure that f is transformed into

So, just this monomial itself will have a term $Y_n^{\sum e_i r_i} + ¿$lower degree term in Y_n coefficient from $Y_1^{¿}, \ldots, Y_{n-1}^{¿}$, this for this monomial this term here would be this monomial will get converted into some polynomial, where this coefficient here is 1. And then some lower degree terms lower degree terms. Here the coefficient is from k and it is 1 so, this looks like this.

So, recall that $f = \sum a_{\underline{e}} Y_1^{e_1} \ldots Y_n^{e_n}$ was some coefficient times this one. And we can assume that $a_{\underline{e}}$ is a non-zero, otherwise they will not appear in sum anyway. So, we would like to give these choose these r_i's. So, that each of these monomials will give a term and this monic term that we get here with unit coefficient are distinct so, that they will never cancel each other.

And therefore, f will get transformed to a monic polynomial. So, this is just to ensure that whatever f gets more transformed to has leading, if you write it as a polynomial in Y_n the leading coefficient is a unit. So, we want to choose r_i. So, one way to so, we want to ensure that f is transformed into a polynomial.

(Refer Slide Time: 09:53)



a poly $g(Y_1^*, \dots Y_{n-1}^*, Y_n)$

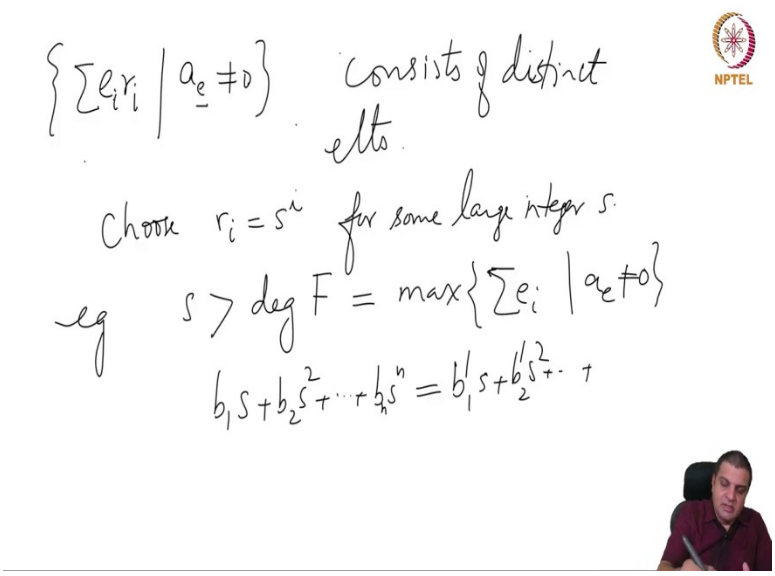
that is monic in Y_n.

One way to ensure that would be

to choose r_i s.t

Let us say $g(Y_1^{¿},\dots,Y_{n-1}^{¿},Y_n)$ that is monic in Y_n. So, this is what we want this is the idea is the same from the other proof, but it is just one requires little bit more work to handle this. So, one way to ensure that would be to ensure that all these degrees are different for each one of these $\underline{e}$, where $a_{\underline{e}}$ is non-zero this sum is different. So, one way to ensure that would be and ensure that would be to choose r_i.

(Refer Slide Time: 10:58)



$\{\sum e_i r_i \mid a_{\underline{e}} \neq 0\}$ consists of distinct elts.

Choose $r_i = s^i$ for some large integer s.

eg $s > \deg F = \max\{\sum e_i \mid a_e \neq 0\}$

$b_1 s + b_2 s^2 + \cdots + b_n s^n = b_1' s + b_2' s^2 + \cdots +$

such that this collection is distinct I mean consist of distinct elements, for all I mean this collection is I mean this is collected overall e such that, $a_{\underline{e}}$ is non-zero, maybe sorry I will write this set in this. So, this collection $\{\sum e_i r_i | a_{\underline{e}} \neq 0\}$ because they will anyway come into consideration when we expand y those are the only terms of f, so, distinct elements.

So, you know one easy way to do that would be, choose $r_i = s^i$ for some large integer s. For example, $s > degree\, F = max ¿ \sum e_i \vee a_{\underline{e}} \neq 0 \} ¿$.

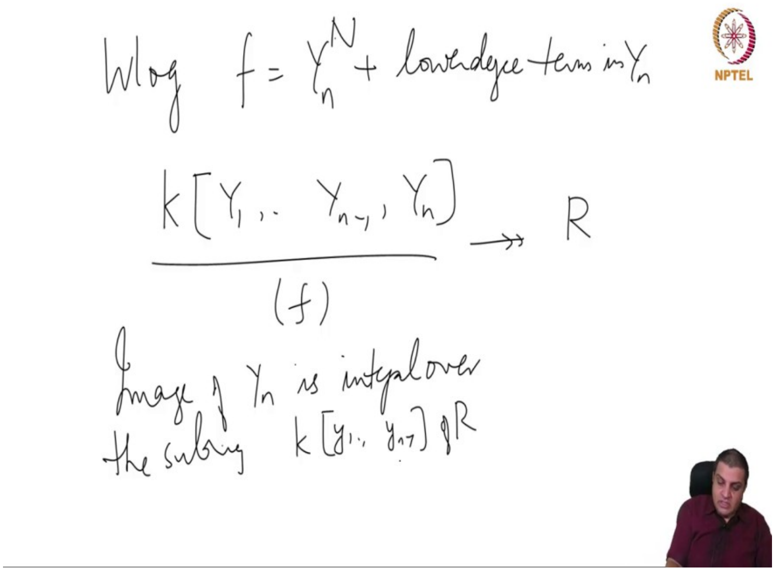
So, these are the actual terms appearing in it and in that the degree is the largest term, that we would we would get the sum is the largest so, if you choose an s large enough, then each one of these e_i will be strictly less than s.

And then if you take something of the form let us say, $b_1 s + b_2 s^2 + \ldots + b_n s^n$ this term will be for various values we every integer which will come as in that form, if the this is different from with this property this will be different from some other $b'_1 s + . b'_2 s^2 + \ldots$ So, this is such similar term.

So, the various these sums will be distinct elements and hence in this sum when we expand out this sum precisely one of those terms will dominate.

So, this sum is over 1 through n and $r_n = 1$ recall that is how the sum will come. So, just keep this in mind and. So, one way to ensure this would be to choose a very large s and, then choose r_i to be s^i and then we will get all of them to be distinct and exactly one term in the terms of F written as Ys, exactly one term will when we do this and therefore, the that would ensure that F is a monic polynomial.

(Refer Slide Time: 14:42)



Wlog $f = Y_n^N +$ lowerdegree term in Y_n

$$\frac{k[Y_1,.. Y_{n-1}, Y_n]}{(f)} \twoheadrightarrow R$$

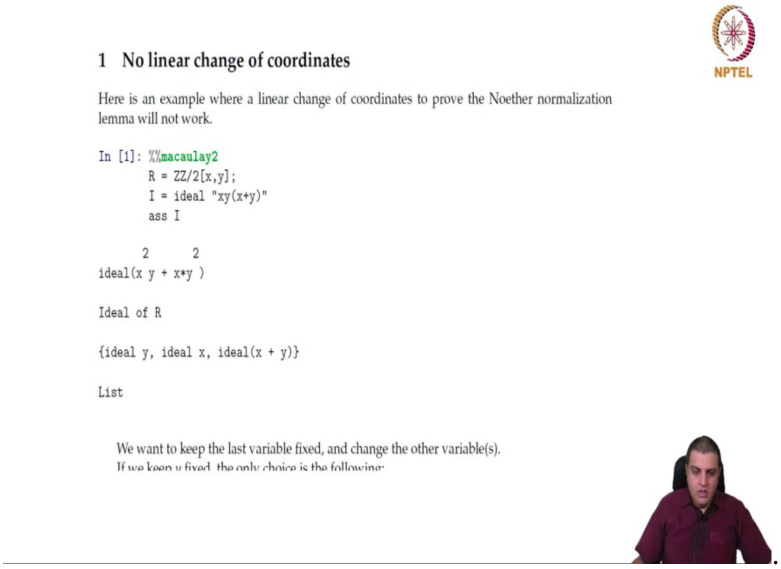
Image of Y_n is integral over the subring $k[y_1,.. y_{n-1}]$ of R

So, without loss of generality f is of the form $f = Y_n^N +$¿lower degree term in Y_n. So, what do we have? We have $\frac{k[Y_1,\ldots,Y_{n-1},Y_n]}{(f)}$. So, now we may as well call we can drop the star in the notation, we may as well call them $Y_1,\ldots,Y_n$.

So, this surjects on to R, f is just in the kernel so, the surjects on to R. And in this ring Y is integral over the sub ring. So, image of Y_n is integral over the sub ring $k[y_1,\ldots,y_{n-1}]$ of R.

Hence, it suffices to prove the theorem for smaller ring and then we can bring it down till we actually get that there is no relation among them. So, this is the proof of the general version of Noether normalisation lemma and so, let us do an example and then we will come back to this question about finiteness and how to use it or why is it relevant.

(Refer Slide Time: 16:35)



1 No linear change of coordinates

Here is an example where a linear change of coordinates to prove the Noether normalization lemma will not work.

```
In [1]: %%macaulay2
        R = ZZ/2[x,y];
        I = ideal "xy(x+y)"
        ass I

       2       2
ideal(x y + x*y )

Ideal of R

{ideal y, ideal x, ideal(x + y)}

List
```

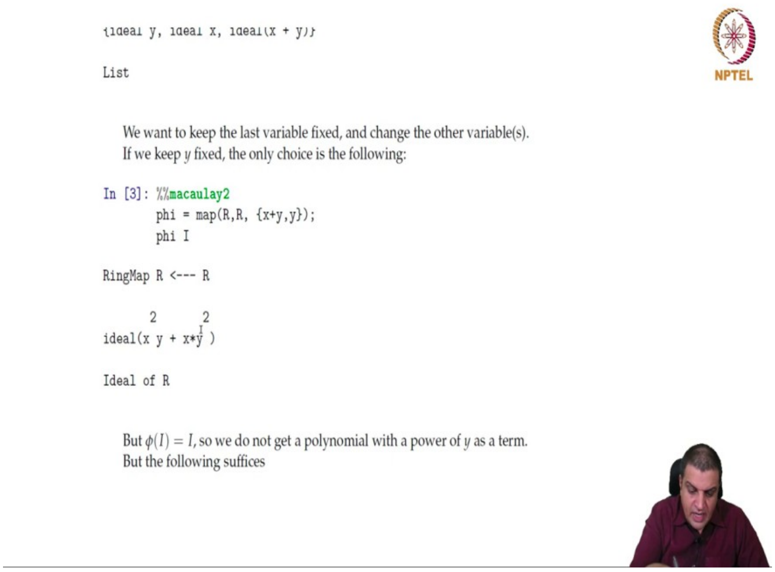
We want to keep the last variable fixed, and change the other variable(s).
If we keep y fixed, the only choice is the following:

So, here is an example so, in the proof in the first proof Noether normalisation lemma for arbitrary for infinite field we observed that a linear change of coordinates would work. So, here is an example where linear change of coordinates would not work in the proof.

So, later after we understand dimension a little bit we will try to come up with an example, where there is no the algebraic independent elements are not even linear. So, that will requires a some of understanding to be able to calculate something. So, that we will revisit after we understand dimension a little bit better.

So, here we are taking a polynomial ring in two variables over finite field of 2 elements and then we look at the ideal $(xy(x+y))$. So, it is and then we ask for its associated primes it is expected, it was just ass. So, this is the command to compute associated primes. So, it is as expected because these are irreducible elements, they are all distinct primes and if you take a product like this it will not have any other associated primes requires a little bit of thinking, but in the polynomial ring one can show that.

(Refer Slide Time: 17:53)



```
{ideal y, ideal x, ideal(x + y)}

List
```

We want to keep the last variable fixed, and change the other variable(s).
If we keep y fixed, the only choice is the following:

```
In [3]: %%macaulay2
        phi = map(R,R, {x+y,y});
        phi I

RingMap R <--- R

       2       2
ideal(x y + x*y )

Ideal of R
```

But $\phi(I) = I$, so we do not get a polynomial with a power of y as a term.
But the following suffices

So, we would like so, in our proof we change the first n-1 variables and then we changed the we did not change the last variable. So, we would like to change x, but not y well, this is a finite field and x has to go into a non-zero vector; a nonzero linear polynomial something of the form $x+\alpha y$ remember, that is what we did in the proof.

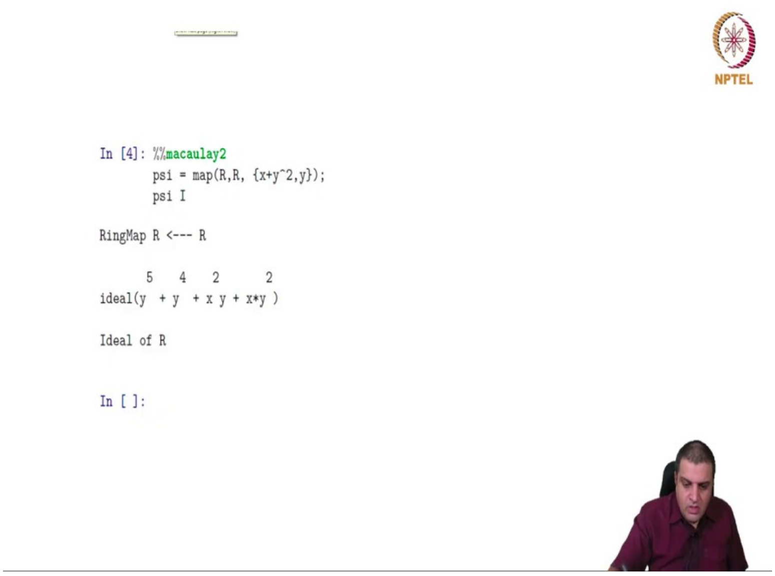
But there is only one choice then x. So, we want to define a change of coordinates so, change of coordinates is a ring homeomorphism it is ring automorphism. So, there is only if you want to keep y fixed, there is only one choice and x has to go to $x+y$. So, this is a map from R to R and x goes to x+y and y goes to y fixed. And we ask what happens to the I. So, we are trying to find whether linear change of coordinates of this variables x and y will give us a suitable Noether normalisation for $\frac{R}{I}$.

So, if you do that here then we see that I does not change, I is this is same as that right $(x^2 y+x y^2)$, but in the proof if you remember the kernel needed to have something monic in y after the change of coordinates or the change of coordinates this is affected so, that we get a monic polynomial in y.

But here there is only one change of coordinate that is possible and that yields same f, and there is not going to be any monic polynomial in this ideal monic in y in this ideal and so, then we cannot do anything.

So, this is an example of a case where over a finite field we are unable to find a linear change of coordinates, which introduces or which gives us a monic polynomial in the kernel of that surjective ring map. So, surjective ring map again what I mean is R surjects on to $\frac{R}{I}$, but just the proof that we just saw if you instead of taking x goes to x+y or if you take x goes to x plus some power of y it might work.

(Refer Slide Time: 20:30)



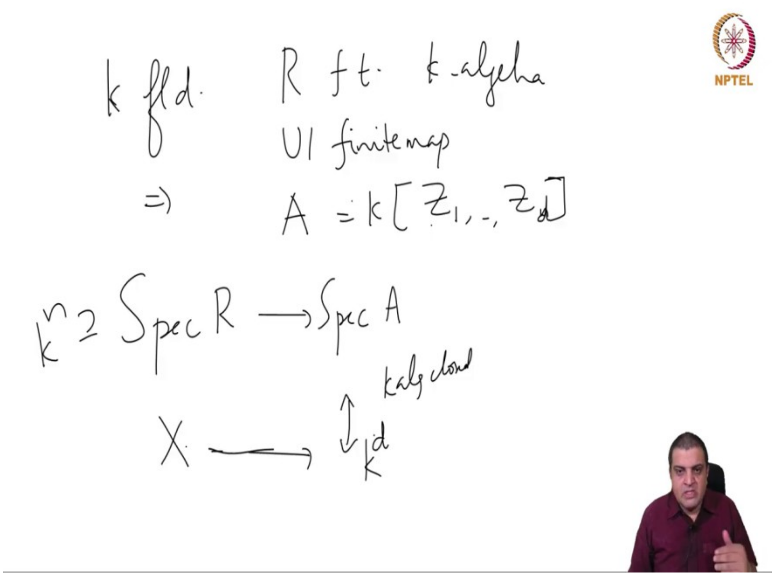
```
In [4]: %%macaulay2
        psi = map(R,R, {x+y^2,y});
        psi I

RingMap R <--- R

       5    4    2      2
ideal(y  + y  + x y + x*y )

Ideal of R

In [ ]:
```

And so, let us check that so, here we change x goes to $x+y^2$ squared and y is fixed. So, let us call that ψ and here is a monic polynomial in y.

So, this is what this proof does, I mean this proof says that this is always possible. And if you think about how we constructed this polynomial which I want to explain, but if you think about why is it that if you take this I, we are unable to get a monic polynomial that there is only one ϕ, and $\phi(I)$ is itself ϕ of the generator of I is itself. Then you would be able to do this in other fields also finite fields also.

So, that is the proof of Noether normalisation lemma. So, this is proceed by induction, sorry. So, now, what we want to understand is.

(Refer Slide Time: 21:49)



k fld. $\quad$ R f.t. k-algebra

$\cup|$ finitemap

$\Rightarrow \quad A = k[z_1, .., z_d]$

$k^n \supseteq \operatorname{Spec} R \longrightarrow \operatorname{Spec} A$

k alg closed

$X \longrightarrow \updownarrow k^d$

So, let us say k is a field, we will come back to algebraically closed in little later and R is a finite type k algebra. And this means that by Noether normalisation, there is some polynomial ring some $z_1, \ldots, z_d$ polynomial ring such that this is a finite map. In particular its integral.

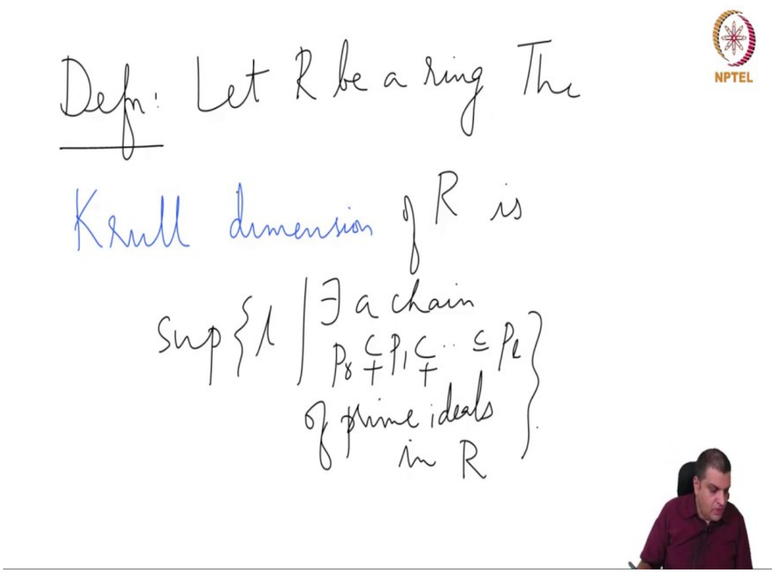
So, now we would like to understand. So, this gives a map from Spec R to Spec A. In this particular case it will also give a map from maximal Spec of R to maximal Spec of A, but that is a difficult theorem which we will not attempt to prove or at least in specific examples maybe we can work it out in the exercises, but in general it is not is I mean one that needs a proof.

But it gives us a map like this and. So, we will continue our discussion about integral extensions and finite map, which will prove that fibers of such a map are finite. They are so, this is so, if you think of the, if k is algebraically closed then we can think of Spec of A by it is maximal ideals and maximal ideals corresponds to a point. So, we can think of this as some space k^d. So, at least k algebraically closed, this is, and this is some X. So, X maps to this is what the picture is.

The points in this one is some subset of let us say k^n. So, some subset of k^n variety maps on to k^d we will prove in this lecture or the next that this is actually a finite at the point fibers are finite we will prove also that this is surjective. And so, then we would like to understand. So, we could use this as a way of understanding X.

So, that we want to pursue now a little bit. So, morphisms and then if you are finite or integral morphisms what do the fibers behave I mean what can we say about their about their fibers that is the next topic. So, before that we need to introduce definition.

(Refer Slide Time: 24:56)



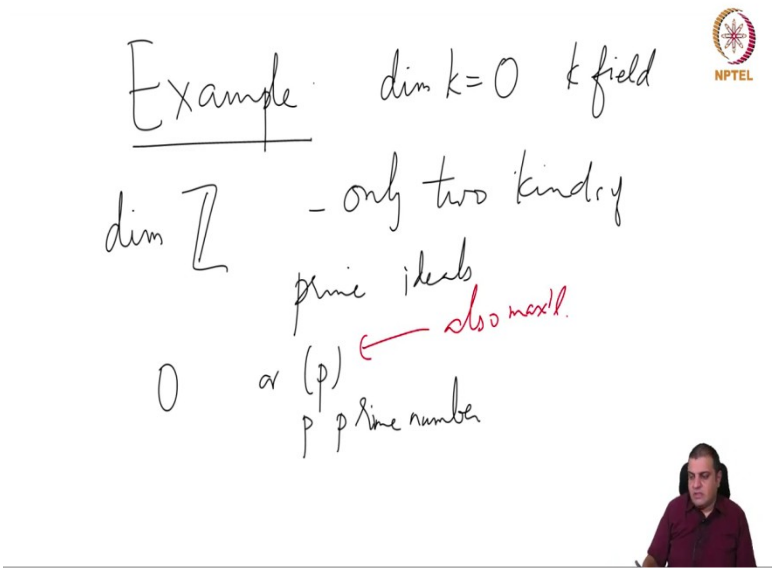
Defn: Let R be a ring The Krull dimension of R is

$$\text{Sup}\left\{ l \;\middle|\; \begin{array}{l} \exists \text{ a chain} \\ P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_l \\ \text{of prime ideals} \\ \text{in } R \end{array} \right\}.$$

Let R be a ring the Krull dimension of R is ¿$\{l|\exists$a chain $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_l$ of prime ideals in R}. So, this is what a Krull dimension is. So, let us look at a couple of examples.

So one of the things that we will study is the how dimension behaves under integral extensions. So, we need to develop a few more definitions, but let us quickly look at example.

(Refer Slide Time: 26:16)



Example dim $k = 0$ k field

dim $\mathbb{Z}$ - only two kinds of prime ideals

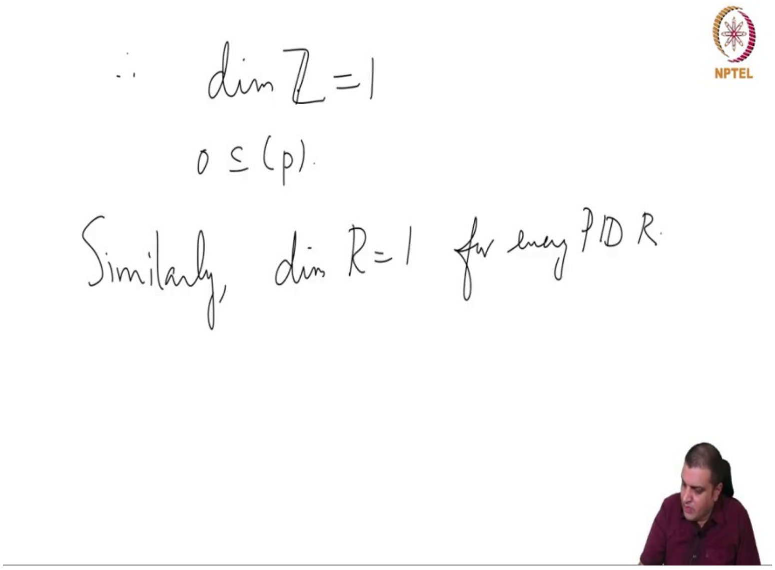
0 or (p) ← also max'l.

p p prime number

Dimension of a field is 0, this is k field, because there is only one prime the maximal ideal which is 0. And hence it is 0. Dimension of Z, the only to start with the only sort of rings that we know are Z_q and maybe fields that at least we know exists.

At least and dimension we have to start counting from I mean, if you want to build up something we are for algebra, we were start measuring it from somewhere. So, now, what about dimension Z? So, there are only 2 kinds of prime ideals 0 or the ideal generated by p; p a prime number and these are also maximal ideals are exactly this.

(Refer Slide Time: 27:41)



$\therefore$ dim $\mathbb{Z} = 1$

$0 \subsetneq (p)$.

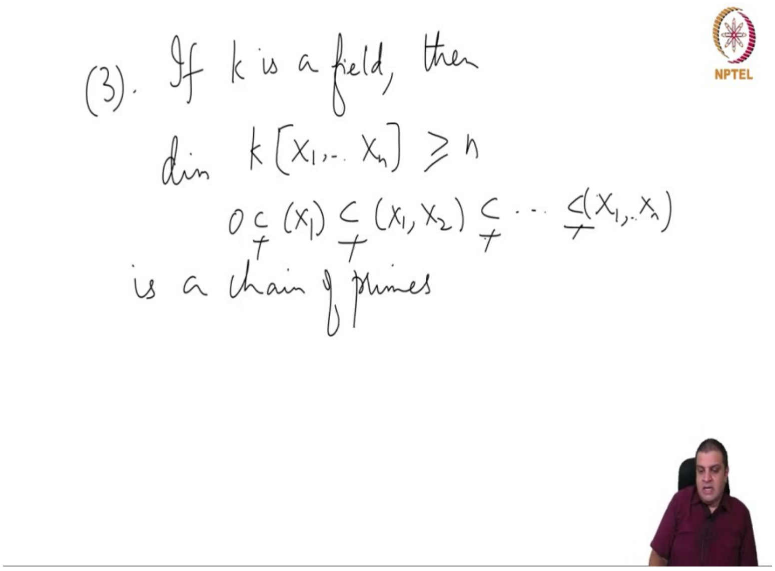
Similarly, dim $R = 1$ for every PID R.

And hence therefore, dimension of Z is 1. So, Krull dimension is a just written dimension and now, there will be a little confusion often we will have to look at k algebras and we will have to use the word dimension to mean it is vector space dimension or Krull dimension.

So, in that case I will try to be consistent with the following usage where for vector space dimension I will call rank, and dimension would be Krull dimension. In any case if there is a confusion I will clarify, so dimensions Z is 1.

So, which means this is always a chain and you cannot do anything better I mean you cannot insert more elements here or the here or in the middle. So, cannot extend it any further. So, similarly dimension of R equals 1 for every PID, same argument; maximal ideals are generated by irreducibles and though the only prime ideals are either maximal or the 0. So, any chain will look like this. So, this is one definition I mean, one example.

(Refer Slide Time: 29:03)



(3). If k is a field, then

$\dim k[X_1,.. X_n] \geq n$

$0 \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1,.. X_n)$

is a chain of primes

And another so, just half example the other half is, what we will struggle quite a bit to prove. So, we will if k is a field, then dimension of $k[X_1,..,X_n]$ is at least n, the reason is the following that $0\subsetneq(X_1)\subsetneq(X_1,X_2)\subsetneq\ldots\subsetneq(X_1,\ldots,X_n)$ the ideal is generated by all the variables this has length n.

So, this is a chain of primes. And there is no immediate way that one can insert things in between or extend or anything to that is this is already a maximal ideal. So, you cannot add anything here, you cannot add anything to the left, if this is already 0 and these have so, these are not we in between this there is no one cannot insert anything.

But remember the definition is of dimension is supremum of such chains. So, we will work a little bit to prove that dimension of this is equal to n, but that requires some work that there is no some other chain of primes, that will go in to some other maximal ideal with greater length.

And so, one of the there is some difficulty we will face some difficulty in proving it partly, because we do not actually know the structure of Spec we do not yet know the structure of a spectrum of this ring.

So, that is the so, this is the end of this lecture. In the next lecture we will discuss start further properties of integral extensions and then we will slowly so, then we will have to spend time understanding Krull dimension more properly and that is what we will do.