Lecture – 44

Proof of Jacobian Criterion

(Contd)

Gyanam Paramam Dhyeyam: Knowledge is Supreme.

All right, so what is $\frac{m}{m^2}$? That is we have to understand. So $\frac{m}{m^2}$, so this m is image of p after localization, right? And this is m square but remember image of p after localization not in the polynomial ring but in a mod , so therefore this is same as, I will write once only because it's not, this is $pK[X]$. X means n variables, then localized p and modulo you have to go and that image of a, right? So this is a $K[X]$ P. This is m, and now I have to go mod m square, that means, square of this ideal. But when you take square of that this p square may not contain a. So you will have to add that, right? So this means, the square of this is, square of this, so $p^2K[X]$, localized p plus a and mod of this. This is what we have to go mod. So when you go mod then this will get. So this is same as, allow me to write short form for this. So I will write a short form is P_p this is $p^2K[X]$ localized p. If you this short form, then this is nothing but p p mod a p and we are going mod p^2 $p+a$ and mod a. This is also same, suffix p, suffix p. I just copied it in this, notice. But this is same as P_p mod, so this will go away, so this is p^2p+ap. This will go away, now we want to compute the dimension of this. So the dimension of this. So you see here, p^2p if here, this is containing p^2p+ap and this is containing P_p. And this dimension you want to come. But this is better, right? So therefore this dimension, so I will write the dimension of as a L vector space m by m square is equal to this is what I want. This is what we want so the dimension will be this, minus this, right? So I just writing that, that is, dimension of P_p mod p^2p minus dimension of a localized $p+p^2p$ mod p^2p. I have not done anything grade. It's only complicated. We are interested in this dimension, so I have written this dimension equal to this dimension minus this dimension. All right, but what is this?

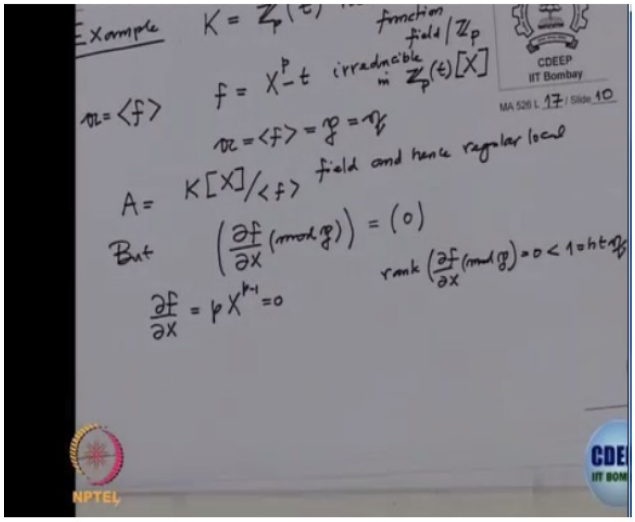
So even this bigger equal to height of p, this part. You see, because where is this? This is now, in a polynomial ring $K[X_1,\ldots,X_m]$ localized. And this ring, I know the dimension is height p. And this is the Lemma 1 dimension, so it is actually equal to. Minus and this one is height of q, bigger equal to you see, because this a is here containing q, containing p, so it is localized nothing is happening after that and before that only q. so q is one of the minimal prime. So the dimension will be a, this is minus n, so this is less equal to height. So it is this. This is clear. And when will equality will happen here? Precisely equality will happen here, so equality here, if and only if R is regular that is because, you see, we have noted here the dimension of $\frac{m}{m^2}$ is bigger equal to height p minus height q. So if equality happens here, that means, dimension of $\frac{m}{m^2}$ is equal to dimension of R. And therefore R is regular. Equality, if and only if R is regular. So therefore that, okay.

So we got when is R regular, in terms of this height p and height q and equality holds here. Okay, now therefore you only have to tie-up with the rank of the matrix. Okay, that is and I will remind you what did we prove in Lemma 1, and what did we prove in Lemma 2. Okay, so in the Lemma 1, we

approved the following . This was precisely contained of the Lemma, it's not exactly but it will be, this will be the outcome of that. So this ring polynomial ring localized p. This is regular. If and only if height of p that is the dimension. And Lemma 1 dimension that means localize that means, this should be equal to dimension of L of pp mod $p^2 p$. That is when, this is regular. This is only a definition. This is what we have by Lemma 1. And Lemma 2 was rank of this matrix Jacobian $\frac{df_i}{dx_j}$ mod p. This rank was less equal to the dimension of, because you see, this is a q, $a_p + p^{2p}$ module p square p, which is less equal to height q. That is what we have proved in Lemma 2. And also we have proved equality. Here, if and only if R is regular. So equality if and only if R is regular. So that precisely what we want. You see, here because this one is bounded by this. This one bounded, when equality holds here, that means equality hold here and this equality holds that means, the equality hold here will mean that R is regular. So just tie-up both these things and then you get the answer. So that proves your A and everything.

Now let me just discuss couple of examples. So first of all, I want to show example where this separability issues. Okay, so example, let us take K to be the prime field $\mathbb{Z}_p$ and the rational function will be non-variable. Rational function field over $\mathbb{Z}_p$. Let me take only one polynomial S, this is our ideal A. So f is the polynomial, $X^p - t$, where p is this. All right, what I would give you also p and we are testing at p. So p I want and also I want Q so a is ideal generated by f that is also p and that is also q. Let us take this. Note that p is a prime ideal because f is irreducible. F is irreducible because f doesn’t have, t doesn't have p through. So this is irreducible in $\mathbb{Z}_p(t)[X]$. This field is not perfect, this $\mathbb{Z}_p(t)$ because you see, if you take the p power map that t doesn’t have p through. Okay, so that is this. So now, what is our ring A? A is $\frac{K[X]}{\langle f \rangle}$. f is zero decibel. This is a pid, therefore this is actually a field. Ring is the field. But the field that regular local. And hence regular local. Fields are local because 0 is maximal ideal. The only ideal and this is regular local. So A is regular local, now let us the Jacobian matrix and the rank. So but Jacobian matrix is now, df , there is only one equation so only one matrix. So this one-cross-one matrix. And this I have to read mod p, right? But what is this? What is first of all, $\frac{df}{dx}$, I have to differentiate with respect to x that means, this is $X^p - 1$. And t is a quantum but this is 0. Becuaes p is catalytic. So actually this is zero matrix. Zero matrix says rank, so the rank is. The rank of this matrix rank is 0. And what is the height? Height of q? It's a principle ideal in a polynomial ring so height is 1. So this is strictly less than 1 which is height of q. So therefore the c part, that converse of p doesn’t hold because this is example.

(Refer Slide Time: 14:49)

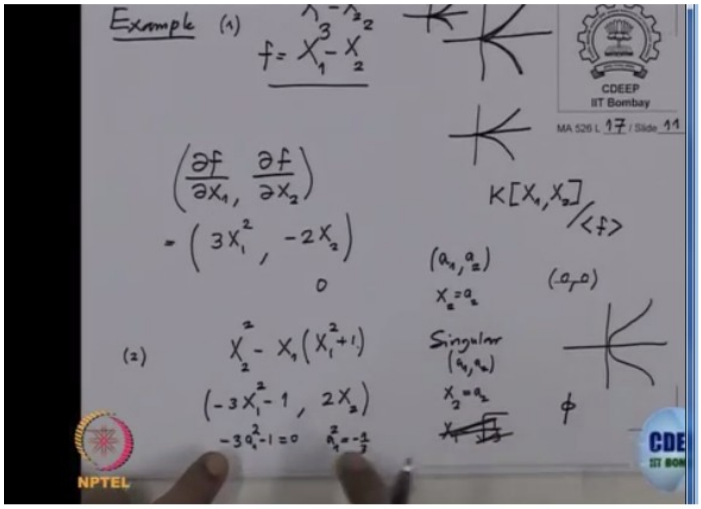


Okay, now let us take some more examples so that one will realize that how important it is for the calculation. Okay, let us take next example. Okay, let us take this first, remember the first that is looping at equation f which is $X_1^3 - X_2^2$. See this example. This is called a Cusp. And if you increase the power here that will go more and more touching. For example, if you go $X_1^5 - X_2^2$, this diagram should become more close to the axis. If you go higher power it is even more. And so if you go larger power the picture will look like this. If we get closer and closer. Okay, so we are looking at this, same thing will happen for the other example also. I want to compute exactly how many points are singular and which are they? So for that we'll have to compute the Jacobian matrix and the rank. So what we are doing? So first we have to compute the Jacobian matrix. Okay, the Jacobian matrix will be the partial derivative. So d is only one equation so it will be $\frac{df}{dX_1}, \frac{df}{dX_2}$. This 2, right? And then we have to read them mod somebody. Right, the prime ideal which want to test whichever is singular or not? So and we are working in this ring. This are fine ring. $\frac{K[x_1, X_2]}{\langle f \rangle}$. In many case this is one dimension. So therefore and 0 is the prime ideal ring and the maximal ideals. There is no in between. Okay, so this partial derivative are what? This R, this is $3X_1^2 - 2X_2$. So we now looking for solutions so also we want to look for. So they are only, lets also assume. It's not necessary.

So let us take a point, testing a whether the point (a_1, a_2) whether these singular or not? So when I plug it here, it should become, the rank should become zero, right? So that means, x_2 is already 0. This coordinate is. At this point the rank should be 0 or 1, that is only the question. At this point this

a_2, and the rank is 0. Then this coordinate is 0, means, x_2 is a_2. And this one, if it is 0, then x_1 is also 0. Right, and that is going to these, right? So you have to check all those things. So the only possibility is $(0,0)$. Because if you take any other than $(0,0)$ point, either x_1 coordinate non-zero and x_2 coordinate in non-zero. Then one of them is non-zero. And therefore rank will become 1. And then that criterion will tell you then it is regularly. Therefore the only singular point is $(0,0)$. Okay, one more. So for example, if you take now the other example, that is $x_2^2 - x_1$, $x_1^2 + x_1$. This one. Remember this picture was like this. Something like this. So in the picture, you can see, there is no singular point. So the singular loop was should be empty here, right? So that also you can see it by differentiate. So differentiate it, then what is the matrix you will land up into? Fist the differentiation with x_1, that is this. So that is minus $3x_1^2 - 1$ that is the first entry and the next one is 2 x 2. Okay, so when you get singular if I take the point (a_1, a_2) and if it is singular then that means, x_2 is a_2. Looking at the singular point. Singular means, rank is, strictly follow. So the x_2 will be a_2 and then this also I want non-zero. This also you want zero but that will get solved for x_1. So the singular point x_1 will be then equal to, you shifted to that side $\frac{1}{3}$ and $\sqrt{\frac{1}{3}}$. This should be 0. See, if it is non-zero it will be non-singular because the rank will be 1 and it will be therefore non-singular by the criterion. So in order that the point, these point to be singular both this should vanish at this point. At this point they vanish from x_2 is a_2 and this is, when I plug it x_1 equal to a_1 it should become 0, so that means x_1 is $\sqrt{\frac{1}{3}}$ but it doesn't pass through that curve. So I need $3a_1^2 - a_1$ is 0, right? This means, $a_1^2 = \frac{1}{3}$, isn't it? This go to the minus. So it depends on the field. Even if you would have worked on complex numbers, it is something. But then, this point will not pass through this curve because see, when you're putting . Here you put a 2 and here you put something this or this, so the only singular point is, nobody singular, therefore singular loop is empty. Just check that these solution which we got by taking the Jacobian matrix to be zero matrix that will not pass through the curve.

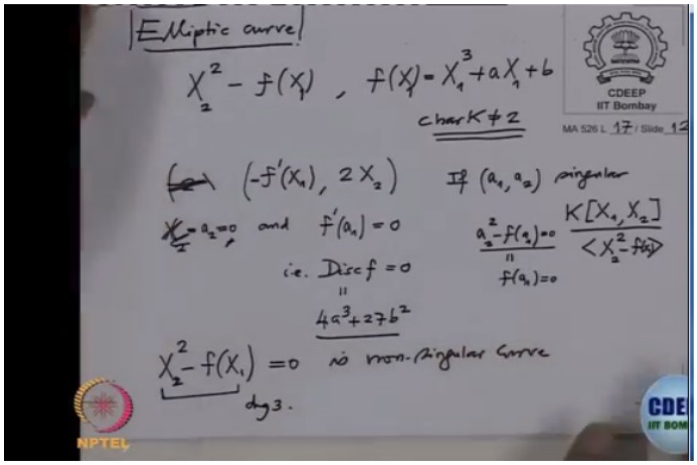
(Refer Slide Time: 22:48)



So I want to do more conceptual examples. For example, Elliptic curve. So Elliptic curve means what? It is curve like this. $X_2^2 - f(X)$, where $f(X)$ is cube. $f(X_1) = X_1^3 + aX_1 + b$. Cubic like this. And now, and let us assume also the characteristic of the field is not 2. This is needed because otherwise you don't have good formulas the quadratic equations through. If we have quadratic 2 field, how do you write zeros of the quadratic equation. So what is the Jacobian matrix here, Jacobian matrix is, is differentiating with respect to, first one is x_1, right? So that is $f'(X_1)$, minus and the second coordinate is 2 x 2. This is Jacobian matrix. And we are now, suppose (a_1, a_2) is singular, point (a_1, a_2) is singular if (a_1, a_2) is singular that means the Jacobian matrix should have become 0. Because see, we are in which ring? We are in the ring, Polynomial ring two variables (x_1, x_2) mod this equation. $X_2^2 - f(X_1)$, right? The dimension is one of this ring. So only possibility is that the Jacobian matrix is $(0,0)$ matrix. So when do singular point take this, that means, when plug this should become zero that means the condition is x_2 equal to a_2, and a_2 should be 0. Because this coordinate should be 0, characteristic is not 2, therefore a_2 should be 0. And $f'(a_1)$ should also be 0. Again we are using characteristic not 2 because it's plus and minus. So this is 0. But this condition is what? This means, this is a cubic equation and derivative is vanishing here. So this is equivalent to saying, this means, so that is. (a_1, a_2) should also pass through this curve. So that means $a_2^2 - f(a_1)$ should be 0. This also there. And this is 0, so a_2 is 0, therefore $f(a_1)$ is also 0. So $f(a_1)$ is 0, and $f'(a_1) = 0$. also that means the discriminate of f is 0. Because common roots of f and f prime are precisely the. Okay, so discriminate is 0, but what is discriminate? Discriminate is $4a^3 + 27b^2$. That is the discriminate of the cubic equation. So such a curve is called a Elliptic curve. So that means, you probably learn somewhere that Elliptic curves are precisely (x_1, x_2) square cubic polynomial with a distinct zeros.

But how that is because we want a non-singularity. It's a non-singular. So what we checked is this curve is has no singular point. So that means the curve is, non-singular. So that means, this curve $x_2^2 - f(x_1)$ is equal to 0 is non-singular curve. And you see the degree of this polynomial, as polynomial in x_1 and x_2 degree is 3. So the degree of this is 3. So such curves are called Elliptic curves.

(Refer Slide Time: 28:18)



There is abstract definition of Elliptic curves and then one say, that if you put them in the coordinate it will become this one. Another example, so these are geometric example but also it is interesting to compute. So if you look at the ring A, this is not fine algebra $\mathbb{Z}[\sqrt{-3}]$. Question is, what is singular looks, Sing A. That means, what are all those prime ideals P, so this is all those p such that A_p is not regular. Like, this is one dimensional ring. So again it only. I will not complete the calculation here, it's not so difficult but what we'll keep handy is note that this ring $\mathbb{Z}[1 \pm \sqrt{2}]$. So this is content here. Why this ring important? This is precisely the normalization. This is A bar. This is the integral closure of A in it's quotient field. What is the quotient field? Quotient field is precisely $\mathbb{Q}[\sqrt{-3}]$. So this is integral quotient that is not too difficult to see. This integral closure, and we have seen in one dimensional place normal and regular is same. So this is regular actually. This is regular. It's not local but so what might help you now, if you do beside, what is the singular lookness of A is not that $\overline{A}$. Euclidean domain. If you use that then you have to check your prime ideal which are singular. The answer you'll get is the following. Sing A is precisely only one point, namely the ideal generated by 2 and $1+\sqrt{-3}$. This check that this is prime ideal and this is the only prime ideal when you localize this ring there it becomes an non-zero. This is not too difficult to check but it will be very handy for you if you use this. Just I leave for you to check it. This is interesting calculation.

(Refer Slide Time: 31:59)