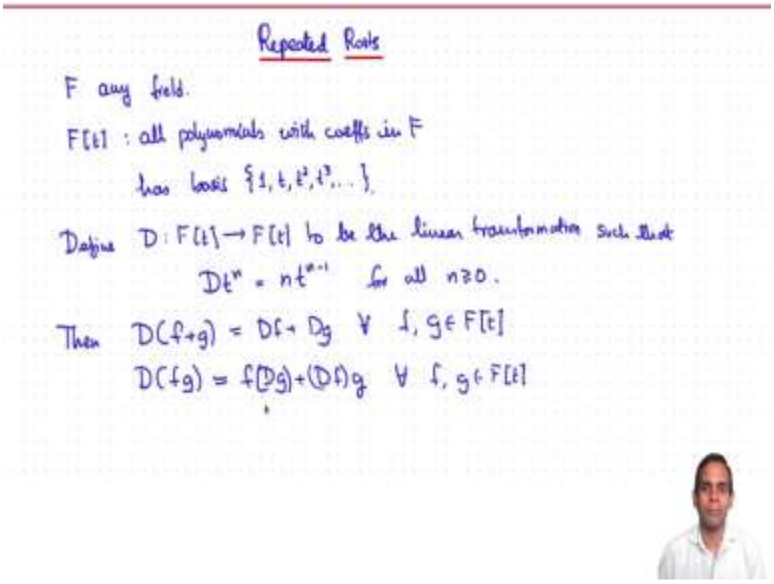
Algebra - II
Professor Amritanshu Prasad
Mathematics
The Institute of Mathematical Science
Repeated Roots

(Refer Slide Time: 0:15)



In this lecture we are going to see when polynomials admit repeated roots. This is going to be useful when we construct finite fields. Before we do that I would like to recall the derivative. So in calculus you have all studied the derivative of a function and a function is differentiable if a certain limit exists and then you can compute its derivative.

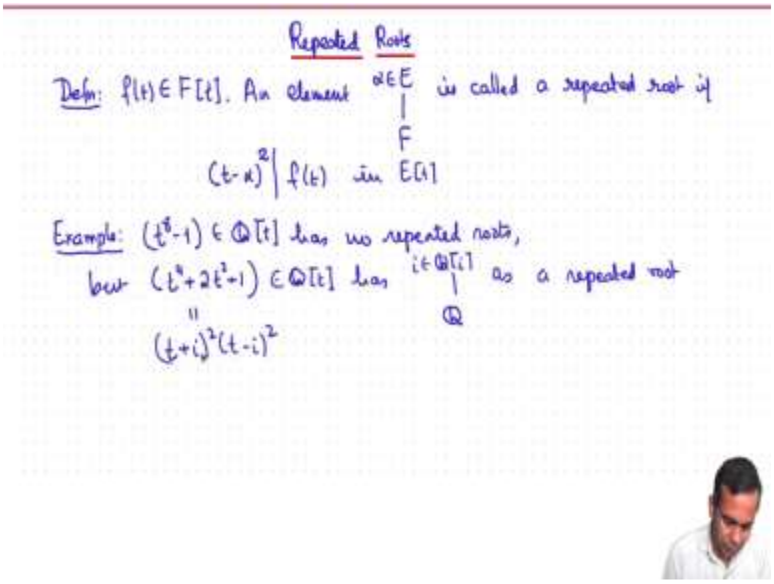
But we know that computing the derivative for polynomials is very easy. So at least the calculus theory of derivatives would work for polynomials with real coefficients because they would be functions of a real variable. However, even when you work over polynomials in any field you can still make sense of the derivative formally.

So let us take F to be any field and then you have the space Ft of all polynomials with coefficients in t in f and this has bases. It is an infinite dimensional vector space and it has bases given by 1, t, t square, t cube and so on. Now you define D from Ft to Ft to be the linear transformation. Well to define a linear transformation I just need to tell you what its values are on the basis such that D of t to the power n is n times t to the n minus 1 for all n greater than or equal to 0.

So then this formally derived derivative, there is no limit if you are working over say a finite field or over rational numbers because there is no clear notion of a limit. But this derivative does satisfy many of the same formal property, the ordinary derivatives satisfy. So then for example D of f plus g is Df plus Dg for all f, g in Ft.

That is just because we have defined it to be linear. So it is linear. But more interestingly the D of f times g is f time Dg plus Df times g for all fg in Ft. I will leave it as an exercise to prove this if you want to look at a detailed proof but it is not difficult. It is just a formal proof playing with symbols.

(Refer Slide Time: 3:11)



Now let us move on to our discussion of repeated rules so firstly the definition. Let ft be a polynomial in ft where f is some field and then an element alpha that lies in E where E is some field extension of f. So this notation here means that alpha lies in an extension of f, is called a repeated root if of course it should be a root. So that means that t minus alpha divides ft in the range Et because t minus alpha.

If alpha is in E then t minus alpha is a polynomial in Et and ft being a polynomial with coefficients in f it is also a polynomial with coefficients in E. So t minus alpha should divide ft. That is just the property of being a root. Repeated root means that t minus alpha squared divides ft.

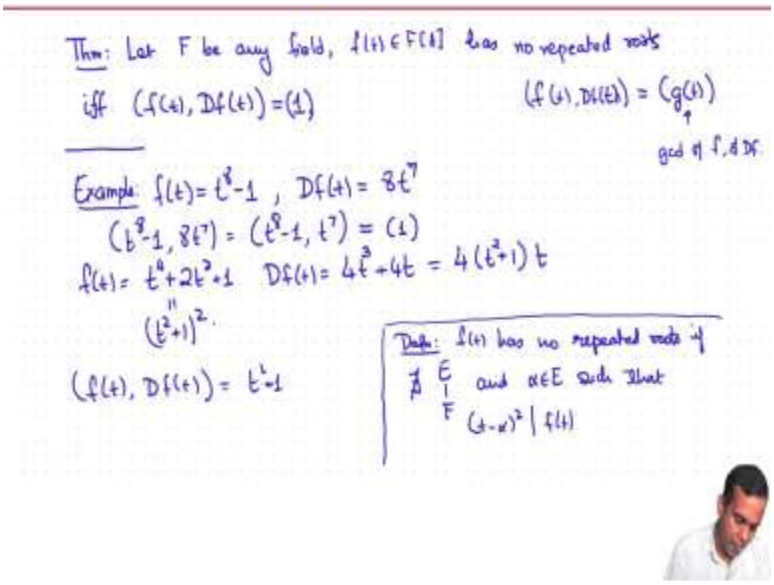
So note firstly that in this definition when I say repeated root I do not insist that the root lie in the field over which the polynomial is defined. It could lie in a larger field.

We have already seen that. Given any polynomial we can always construct a field in which it can be written as a product of linear factors. So you could for example work in that field. So let us just look at an example.

So last time we analyzed quite thoroughly the polynomial t to the power 8 minus 1 in Qt. This has no repeated roots. But the polynomial t to the power 4 plus 2t square plus 1, let us say this also in Qt has an element i in a Q adjoin i over Q as a repeated root. In the Gaussian numbers this ring Q adjoin i, the extension field at Q adjoin i we have a factorization of this polynomial as t plus i whole squared, t minus i whole square.

After all t plus i to t minus i is t squared plus 1 and this is manifestly the square of t squared plus 1. So the first polynomial has no repeated roots. That is the second one has repeated rules. Now let us come to the main theorem of this lecture.

(Refer Slide Time: 6:22)



So let F be any field and let us take a polynomial with coefficients in f. Then this has no repeated roots. So maybe I should clarify here. What does it mean for a polynomial to have no repeated roots? So let us just say that, ft has no repeated roots, if there does not exist any extension E over f and alpha belonging to t such that, t minus alpha squared divides ft.

So basically you are saying that repeated roots does not exist just to be extra clear here. As no repeated roots, so we want to decide whether or not a polynomial has repeated roots and the answer is actually very simple. If and only if ft, f prime t is equal to 1. So this is maybe I should write it as Dft. I mean the derivative of f.

So let me just recall we discussed in algebra 1 what these things are. The rank of polynomials, they form a principle ideal domain. In fact they form a Euclidean domain and since it is a principle ideal domain, if you take the ideal generated by ft and Dft that is going to be a principle ideal.

So you would have ft and Dft, this would be a principle ideal and this could either be the whole ring or it could be something smaller. So by this I mean 1 in parentheses or it could be generated by some, this should be Dft. It could be generated by some polynomial gt. That polynomial has degree greater than 1, then this is a proper sub ring of ft and this polynomial gt, this is called the gcd of f and Df.

And we have seen in Euclidean domain, you can compute the gcd of 2 elements by repeated application of Euclid's division algorithm with remainder. But for now it is just enough to say that f has no repeated roots if and only if its gcd with its derivative is trivial. That means it has no common factors with its derivative.

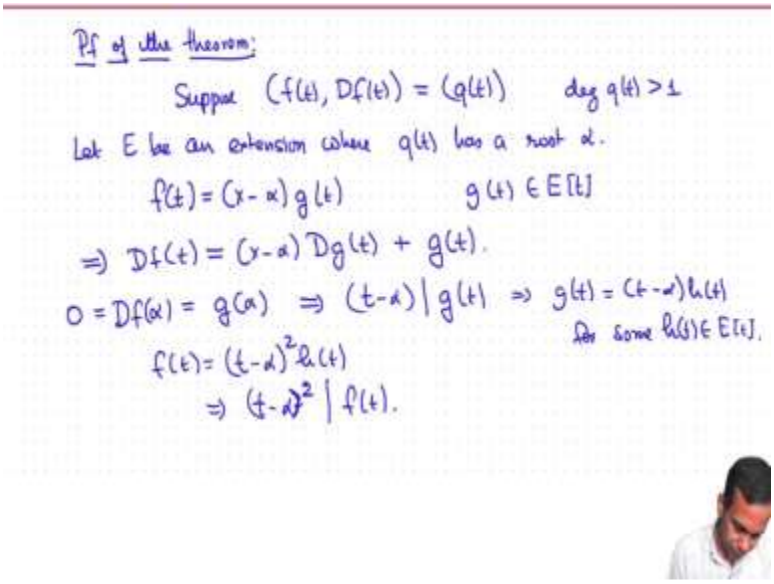
So that is the statement and if you want we can look at the examples. So if we go back to this example. Let us take t to the power 8 minus 1. If this is ft, then f prime t or Dft the derivative of t is 8 t to the power 7. Now these integers we are working over qt. These integers 8 and so on these are just units in the ring. So we can ignore them.

So that we have is t to the 8 minus 1 8t to the power 7. This is just the gcd of the t to the 8 minus 1 and t to the power 7. Now any common factor of the t to the 8 minus 1 and t to the power 7 must be a power of t because it has to be a factor of t to the power 7 and the only factors of t to the power 7 are powers of t.

But this thing has constant terms 0 t to the 8 minus 1. So it is not divisible by any factor power of t. So these 2 polynomials generate the entire ring. And now let us look at the other example that we had. We had ft equals t to the power 4 plus 2t square plus 1. Then Dft is 4t squared plus 4t which we can write as sorry 4t cube plus 4t which we can write as 4 times t squared plus 1 times t.

This polynomial is t squared plus 1 times whole squared. So what we have is that the gcd of ft and Dft is actually t squared plus 1 in the polynomial ring qt. And so you see this polynomial actually has repeated roots and the first polynomial t to the 8 minus 1 has no repeated roots, illustrating this theorem here.

(Refer Slide Time: 11:46)



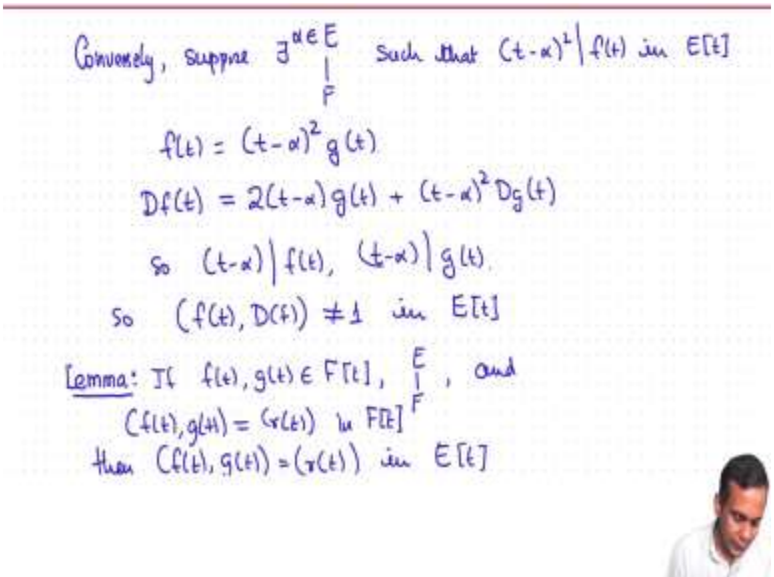
Okay, so let us move on to the proof of the theorem. So let us suppose the gcd of f and its derivative is not 1. So suppose, ft and Dft, their gcd is generated by some polynomial qt where degree of qt is greater than 1. So it is not an constant polynomial. So, then take E to be an extension where qt has a root.

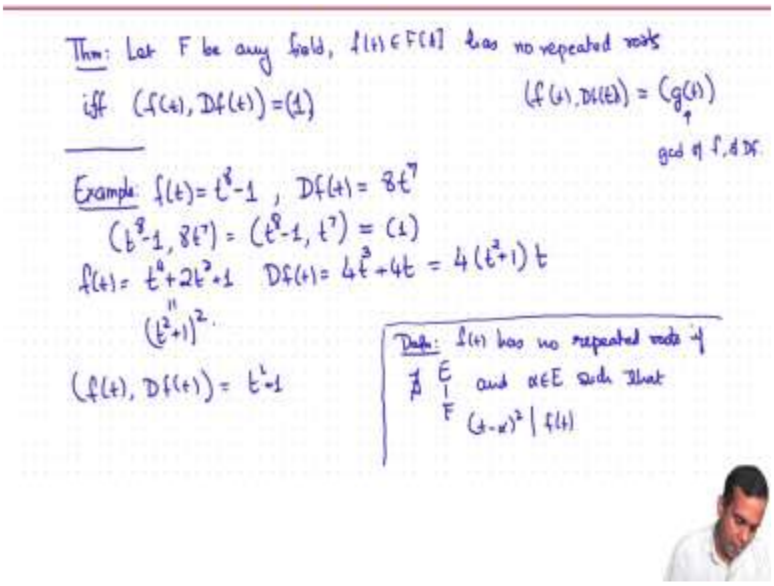
Let us call that root alpha. We have already seen that such extensions exist. In fact you can find an extension where qt is a product of linear factors. So then both ft and Dft have a root alpha in E. So since qt is a factor of ft, ft also has a root alpha. So ft can be written as x minus alpha times gt. This implies that Dft using product rule for derivative this is x minus alpha times Dgt plus just gt.

But Dft also has a factor qt which vanishes at alpha. Therefore, df alpha is equal to 0. But if I substitute here, alpha minus alpha that becomes 0. So I get g alpha which implies that t minus alpha in fact divides gt because g of alpha is 0. So together with this, this implies that f of t equals, so t minus alpha divides gt. So I can write gt as t minus alpha times ht for some polynomial belongs.

So all this here is happening gt belongs to Et in this extension right. That is where this factorization is happening because alpha itself is in Et. So what we have is, t minus alpha squared times ht in Et which implies that t minus alpha squared divides ft. So this proves the result in one direction. That if gcd of a polynomial and its derivative is not 1 then the polynomial has a multiple roots. Now let us prove the converse.

(Refer Slide Time: 15:23)





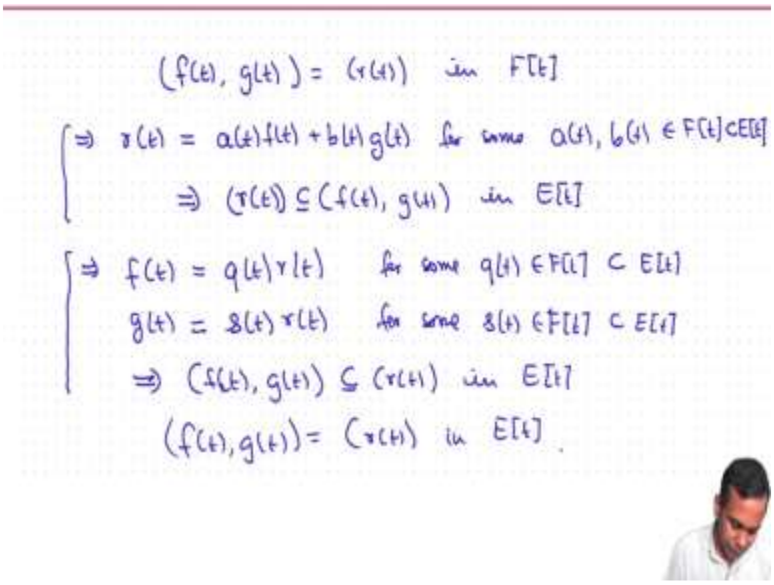
So conversely suppose we do have an extension, E over f and an element alpha in E such that t minus alpha squared divides ft in the polynomial ring Et. So in this theorem this gcd is taken in ft. But here we have this in Et. So let us just see what happens now. So what we have is f of t equals t minus alpha squared times gt.

Now let us compute Dft. So using the product rule for derivative we get 2 t minus alpha gt plus t minus alpha squared Dgt. So t minus alpha divides both ft and gt which means that the gcd of ft and Dft is not equal to 1 in Et. This is the gcd in Et. But in this theorem I do not want to worry about the extension. I just want to compute the gcd of ft and Dft in ft. So the point is it does not really matter.

It turns out it does not matter. So here is the lemma. If ft gt are 2 polynomials in Ft and E is an extension of F and the gcd of ft and gt is rt for some polynomial r in Et. So in ft let us say. So suppose the gcd of f and g is r in this ring of polynomials in the smaller field f. Then I claim that the gcd of ft and gt is r even in the big ring of polynomials with entries in a larger ring.

It is possible that you may since you are allowing more polynomials you may find more common factors between ft and gt. But what this lemma is saying, no that this rt will generate the ideal of ft and gt even in Et. The proof of this is not very hard.

(Refer Slide Time: 18:52)



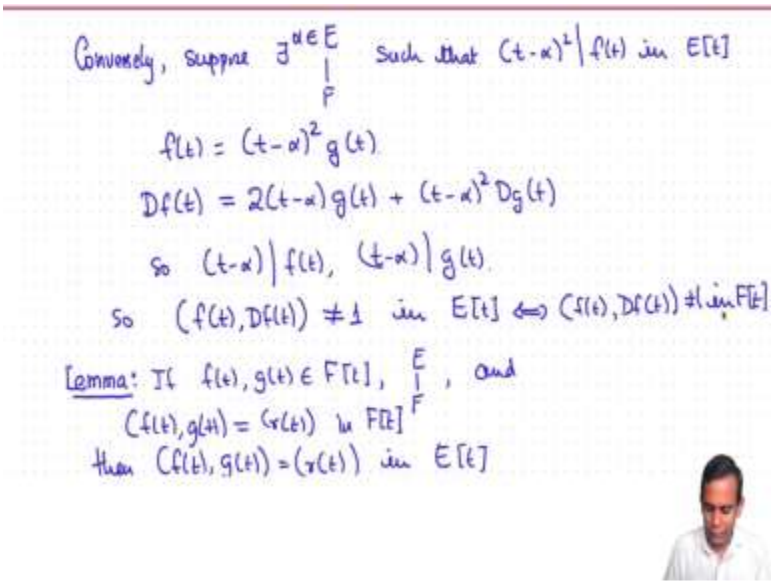
It mostly just proceeds by thinking about what it means for these 2 ideals to be equal. So what we have is that, we know that ft, gt is equal to rt in Ft in the smaller field and we want to establish the same result in Et. So what does this mean? This is the same as saying that rt lies in the ideal generated by ft and gt. So this is equivalent to, maybe I will just do 1 way.

So this implies that rt is equal to at, ft plus bt gt for some at, bt in ft. But ft is contained in Et. So that means that rt is at ft plus bt gt for some at and bt in Et. So this implies that the rt lies in the ideal generated by ft and gt in Et which can be restated as the ideal generated by rt is contained in the ideal generated by ft and gt in Et.

And on the other hand we also have that this implies that at, ft and gt belong to the ideal generated by rt. So ft is some qt times rt for some qt in ft and gt is equal to st times rt for some st in ft. Now again ft is contained in Et and ft is contained in Et.

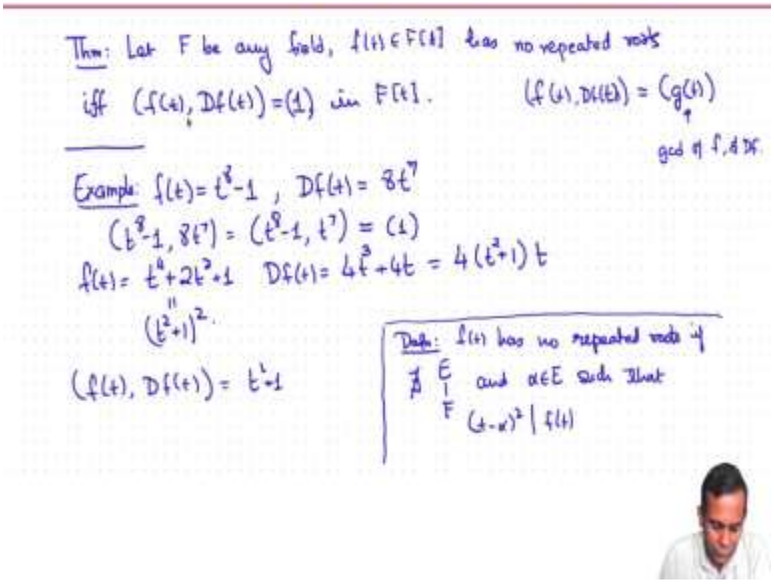
So what we have is that this implies ft, gt is contained in rt, in also the larger polynomial ring. So putting these together what we get is that ft, gt is equal to rt in also the larger polynomial ring Et. So if the gcd of the 2 polynomials is non-trivial in ft, it is non-trivial in at. And that is all we need here.

(Refer Slide Time: 21:53)



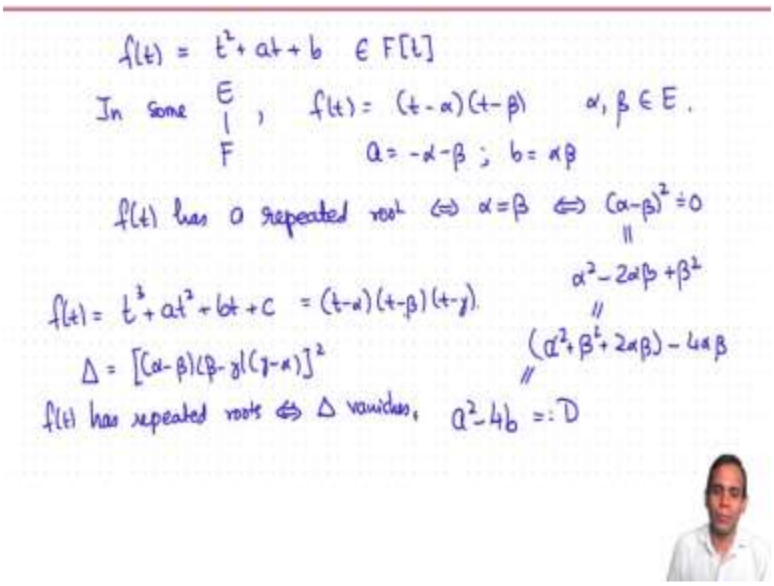
So if we go back, we showed that ft and Dft, maybe I should write it, Dft, their gcd is non-trivial in Et but their gcd in Et is the same as their gcd in ft. And that is all we needed to prove.

(Refer Slide Time: 22:32)



So the upshot is that a polynomial has no repeated roots if and only if its gcd with its derivative is 1. Let us look at this illustrated in the case of quadratic polynomials. So that is a very simple case and it is also very possible to work out the case for higher degrees.

(Refer Slide Time: 22:50)



But let us ask, suppose we have a polynomial ft equals t squared plus at plus b. We could have taken at squared plus bt plus c but it does not really matter because multiplication by scalars. Scalars are units. So we can just take a monic polynomial belonging to ft. F is any field whatsoever.

Now in some extension we have ft is t minus alpha into t minus beta. So alpha beta belongs to E. And ft has repeated roots if and only if alpha is equal to beta has a repeated root if and only if alpha is equal to beta. So ft has a repeated root, if and only if alpha is equal to beta which can be written as if and only if alpha minus beta the whole squared is equal to 0.

But this can be written as alpha squared minus 2 alpha beta plus 2 beta squared. Now note if we compare t minus alpha and t minus beta with t squared plus at plus b what we get is that a is minus alpha minus beta and b is alpha beta. Using that we can expand this in terms of a and b.

This polynomial here is alpha square plus beta squared plus 2 alpha beta minus 4 alpha beta and that is the same as a squared minus 4b. This is the discriminant. This is you know when we solve quadratic equation, we call this the discriminant. So a quadratic polynomial has repeated roots if and only if a square minus 4b is equal to 0.

So you can express the condition for having a repeated root in terms of the vanishing of a polynomial in the coefficients. Of course you could have done this using the formula for the roots of a quadratic polynomial as well. But the nice thing about this method is that you can apply the same thing to higher degree polynomial.

Suppose I had a cubic polynomial, t cubed plus at squared plus bt plus c. Then I can take delta to be the polynomial. Suppose it has roots in some extension t minus alpha, t minus beta, t minus gamma. Then I can take this polynomial, alpha minus beta, beta minus gamma, gamma minus alpha whole squared.

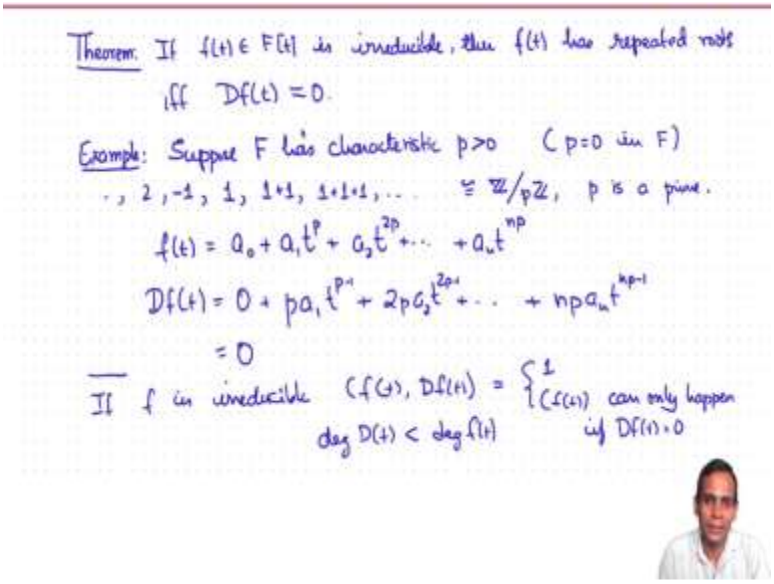
This is going to be a symmetric polynomial in the roots alpha, beta, gamma. It is going to be a degree 3 symmetric polynomial in the root alpha, beta and gamma and therefore it can be written as a polynomial in a, b and c and this polynomial has repeated roots if and only if delta vanishes.

Now you can try this at home. If you try this symmetric polynomial, alpha will be minus beta, beta minus gamma, gamma minus alpha whole squared and express it in terms of a,b and c, you will get a polynomial expression in variables a, b, and c whose vanishing will be equivalent to the cubic polynomial having repeated roots.

So there is, I am not deriving it. It takes a little more work to derive it but there is a formula from which you can read of whether or not a cubic polynomial has a repeated root or not. And you can do the same thing with polynomials of any degree.

There is always a discriminant from which you can read off whether or not it has a repeated root. So mostly in older books on the theory of equations, you will find these things computed in great detail. It is a lot of fun. So you can take a look at the internet or other references for the discriminant of a polynomial.

(Refer Slide Time: 27:40)



We now come to a very surprising result about when irreducible polynomials have repeated roots theorem. If ft is a polynomial with coefficients in a field capital F is irreducible, then ft has repeated roots if and only if its derivative is identically 0. Very strange you might see right.

How can a polynomial which is non-trivial have derivative 0? Well okay maybe it is constant and so it has derivative 0. But then that is not irreducible. That is a unit. So what are we really talking about here? Well the example that we are really interested in is the polynomial like this. So suppose we have F is a field of characteristic p.

So suppose F has characteristic p. This means that, in F you start with 1 which definitely is the multiplicative unit of F. You take 1 plus 1. 1 plus 1 plus 1 and so on. So this generates monoid and you can also take minus 1, minus 2 and so on. So this, it could be either isomorphic to z or it could be isomorphic as an abelian group to z mod pz where p is a prime.

So if you keep adding 1 to itself and you never get 0 then you say that the field has, well you could say infinite characteristic. But usually for some perverse reason we say the field has characteristic 0. So the rational numbers have characteristic 0. But suppose f has characteristic p greater than 0 where we mean p is a prime number then f is an extension of the field z mod pz where p is a prime number.

So suppose f has characteristic p that means that p is equal to 0 in F. That means if you take 1 and add it to itself p times you get 0 in F. Then you can look at the polynomial, ft equals a naught plust a 1 t to the p plus a 2 t to the power 2p plus a n t to the power np. In short we are looking at polynomials where the only powers of t that occur are powers that are multiples of p. Then you compute Dft.

Then a naught when its derivative is 0, a 1 t it will be p times a 1 to the p minus 1. This will be 2p 2 t to the 2p minus 1 and so on n p an t to the n p minus 1. But these p's are all equal to 0. So this is equal to 0. So here is your example of a polynomial which is non-zero but its derivative is identically 0.

So these are the polynomials in positive characteristic. In characteristic 0 you really cannot have this. If you have a polynomial which is of degree greater than 0 and its derivative is 0 then it has to be the 0 polynomial itself. So when the characteristic of the field is 0, we are saying that if a polynomial is irreducible then it cannot have repeated roots.

In positive characteristic we are saying that if a polynomial has is irreducible and it has repeated roots then it must be a polynomial of this form. But the only powers of t that occur are multiples of p. Let us see how to prove this theorem. We will just use the criterion for the existence of repeated roots that we showed few minutes ago. So suppose f is irreducible, then what can be the value of ft and Dft.

So then ft Dft has to be a factor of, has to be generated by a factor of ft. So this has to be 1 or this has to be ft. The only 2 possibilities because only 2 factors of, there is only 2 divisors of the polynomial ft. So this has to be 1 or ft. Now but this Dft, the degree of Dft is strictly less than the degree of ft.

So you cannot have a ft diving Dft because the degree of Dft is smaller than the degree of ft unless of course Dft is identically 0. So this can only happen if Dft is 0. In fact if Dft is 0, this is exactly what happens. The ideal generated by ft and 0 is the ideal generated by ft and so that proves the theorem that a polynomial is irreducible then it has repeated roots if and only if its derivative vanishes identically.

And this is something which never happens in characteristic 0. So this is primarily of interest in positive characteristic and this is where we are going to next. We are going to construct finite fields which are all fields of positive characteristic.