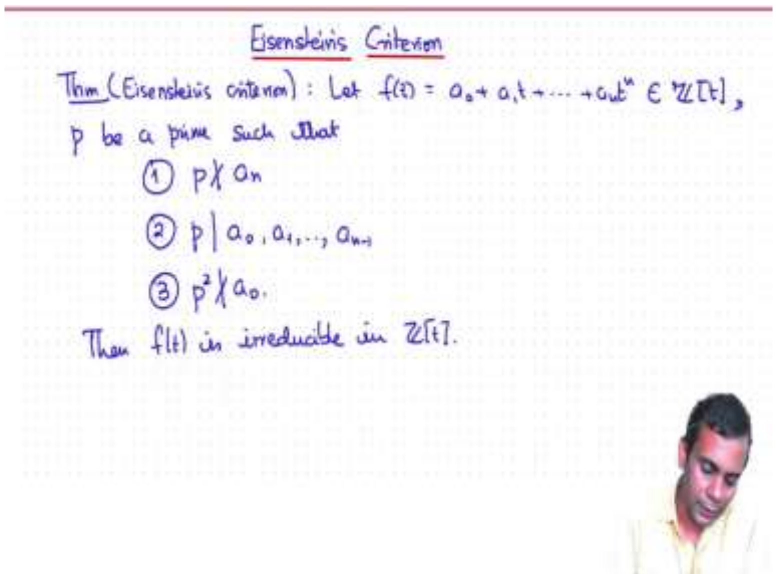
Algebra – II
Professor Amritanshu Prasad
Mathematics,
The Institute of Mathematical Sciences
Lec13
Eisenstein's Criterion

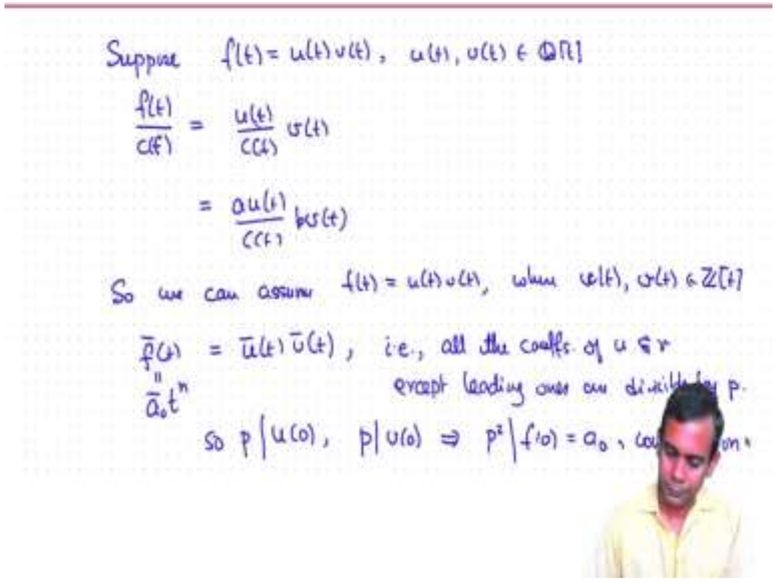
(Refer Slide Time: 00:15)



In general, it can be quite difficult to prove that a polynomial is irreducible over the rational numbers; however there is 1 useful trick that works for many important polynomials and that is Eisenstein's criteria. So here is the statement, suppose you have a polynomial ft equals a0 plus a1t plus ant to the n.

And let us assume that the coefficients are in integers zt, and suppose p is a prime such that the first condition is that p does not divide an, so p does not divide the leading term of this polynomial f and the second condition is p divides all the other coefficients, p divides a0, a1 up to an minus 1, and the third condition is that p square does not divide a0 then the theorem says that ft is irreducible in Zt. The proof will use reduction modulo p and proceeds by contradiction.

(Refer Slide Time: 02:04)



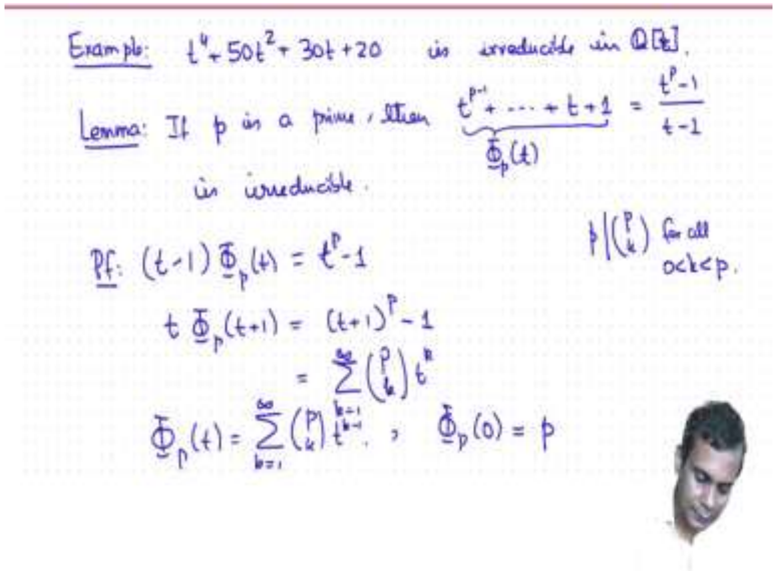
So suppose we have a factorization ft equals ut times vt, where ut vt, well we need to prove that there is no factorization in Qt, so we need to take ut and vt and Qt, but then to apply reduction modulo p we would need these factors to actually have integer coefficients. So, we fix that by using Gauss's lemma.

So you look at the polynomial ft by ct, where cf, where cf is the content of f that is the gcd of all its coefficients, then this is ut by cf vt, we can take it like that, so ut by cf and vt are both polynomials with rational coefficients, and then by Gauss's lemma well this ft by cf is a primitive polynomial and so by Gauss's lemma we can write this as a times ut by cf times vt where a times ut by cf and vt are integer polynomials.

So, we can assume that ft is ut vt where ut and vt are have integer coefficients, just by replacing u by aut by cf and v by bvt I guess, and now we have f bar t, this is just this is just a0 bar t to the n, no other term survive because of our hypothesis on f all the coefficients of f except the leading term are divisible by n, is equal to u bar t times v bar t, but this means that all but the leading coefficients of u and b are divisible by p all the coefficients of u and v except leading coefficient are divisible by P.

In this factorization were assuming that u and v are non-constant polynomials, so in particular that means that u of 0 which is the constant term of u is divisible by p and also v of 0 is divisible by P, but this implies that f of 0 which is u of 0 times, v of 0 is divisible by p square, p square divides f of 0 but that is just a0 which contradicts this last hypothesis that p square does not divide a0, and so we conclude that f must be irreducible contradiction.

(Refer Slide Time: 05:36)



Let us look at some examples so here is a simple example, just take the polynomial t to the 4 plus 50t square plus 30t plus 20, now if you take p equals 5, then you see that p divides all but the leading coefficient of this polynomial, p square does not divide 20, so this is irreducible in Qt. But more interesting are examples a very interesting class of examples is this, lemma, if p is a prime then t to the power p minus 1 plus t plus 1, so this is the polynomial t to the power p minus 1 divided by t minus 1 is irreducible.

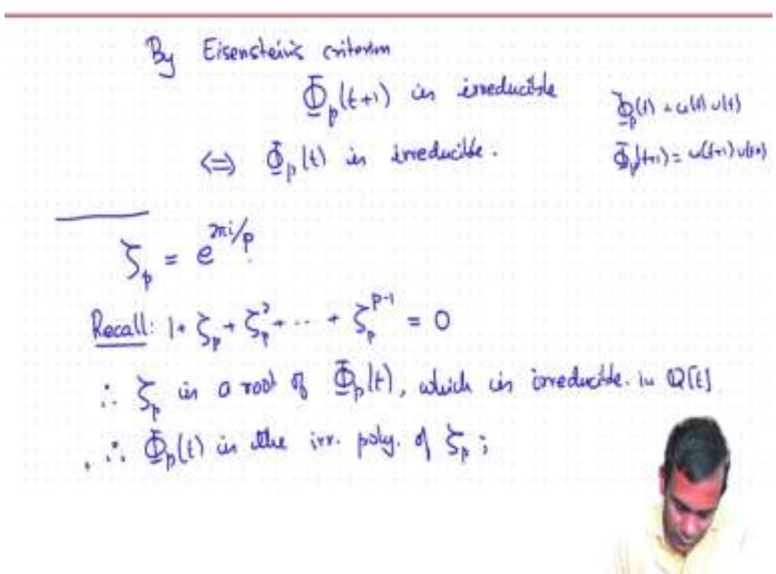
You may look at this and say, well all the coefficients here are 1, so how could I apply Eisenstein's criterion, so the trick is apply Eisenstein's criterion after substituting for t, t plus 1. Now the thing is, if you take a polynomial and transform the variable like that, if the original polynomial was irreducible then the transformed polynomial would also be irreducible.

So apply Eisenstein's criterion to t plus one, so let us let us call this polynomial, well it turns out that this polynomial is actually the pth cyclotomic polynomial. I will explain that to you in a moment, so this is certainly a polynomial that is satisfied by a primitive pth root of unity and its irreducible, so it is the pth cyclotomic polynomial, so apply Eisenstein's criterion to after shifting the variable to t plus 1.

So, what we have is t minus 1 times Phi pt by definition is t to the power p minus 1, and now let us just change the variable from t to t plus 1, so if I put that then I get Phi pt plus 1 is t plus 1 to the power p minus 1, but now if you look at this t plus 1 to the power p, this is summation k goes from 1 to p I am removing the k equals 0 term because it will cancel out with this minus 1, p choose k by t raised to k times t raised to k.

But now note that p divides p choose k for all k between except for zero and p, and so what we get is that, this all all but the leading term of this polynomial, but now maybe I should look at divide by this t, so let me just, so what we get is Phi pt plus 1 is summation k goes from 1 to infinity p choose k t to the power k minus 1. Now this is a polynomial of degree p minus 1, its leading coefficient is 1, and all the remaining coefficients are divisible by p, and what is Phi p0, the constant term is just p, so that is not divisible by p square.

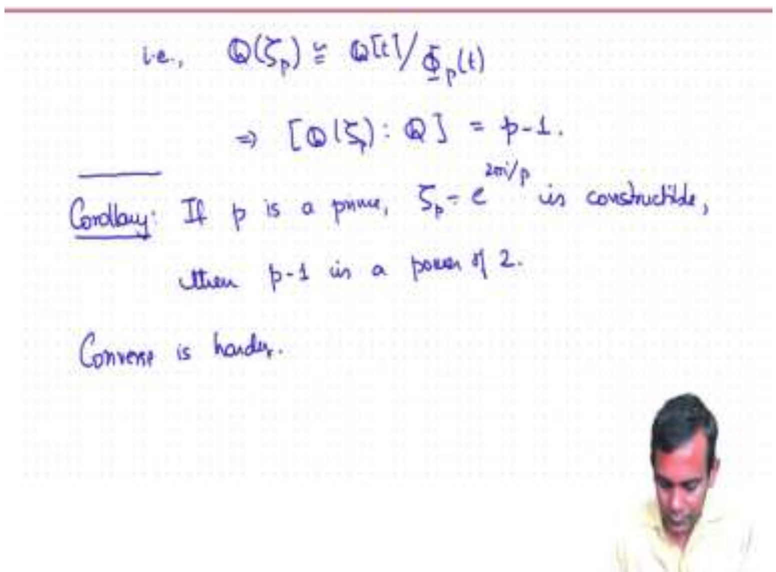
(Refer Slide Time: 09:49)



And hence by Eisenstein's criterion Phi pt plus 1 is irreducible, which means that, it is equivalent to saying that Phi pt is irreducible. See if you have a factorization of Phi pt say Phi pt equals ut vt then Phi pt plus 1 equals ut plus 1 vt plus 1, so you can get a factorization of Phi pt plus 1, and you can do the reverse by substituting t minus 1. So, the irreducibility of these two polynomials is equivalent so what we get is that Phi pt is irreducible.

Now recall that we were defining zeta p to be the primitive pth root of unity so this is e to the 2 Pi i by p and this satisfies zeta p 1 plus zeta p plus zeta p square plus zeta p to the power p minus 1 you can use a geometric series to sum this if you like is equal to 0. So, use the formula for geometric series to check this. Therefore, zeta p is a root of this polynomial Phi pt which is also irreducible in qt, so what this means is Phi pt is the irreducible polynomial of zeta p.

(Refer Slide Time: 12:10)

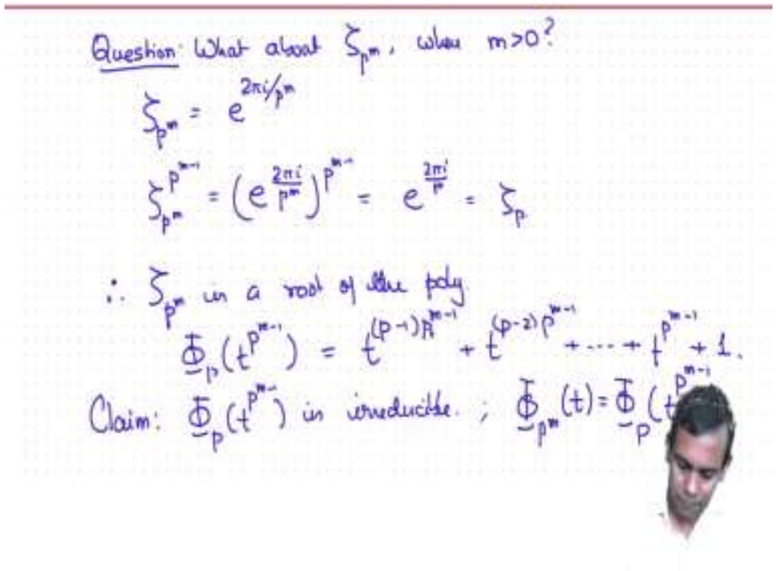


In other words, if I look at the subfield of the complex numbers generated by, so this is inside the complex numbers generated by zeta p this is isomorphic to Qt mod Phi pt which implies that, the degree of this extension is equal to the degree of this polynomial Phi pt which is p minus 1. So primitive pth root of unity lies in is lies in a field extension generates a field extension of degree p minus 1 over Q.

We can just tweak this method a little bit to get in fact more cyclotomic polynomials, so but before that, one more corollary if p is a prime and zeta p is e to the 2 Pi i by p is constructable, then p minus 1 is a power of 2, why is this well, of course we have already seen that if you have a constructable number, then it generates a field extension of degree equal to a power of 2.

So, p minus 1 has to be a power of 2, by this earlier calculation. So, the converse of this theorem is also true but that is harder to prove, that is if p minus 1 is the power of 2 then zeta p is constructive.

(Refer Slide Time: 14:19)



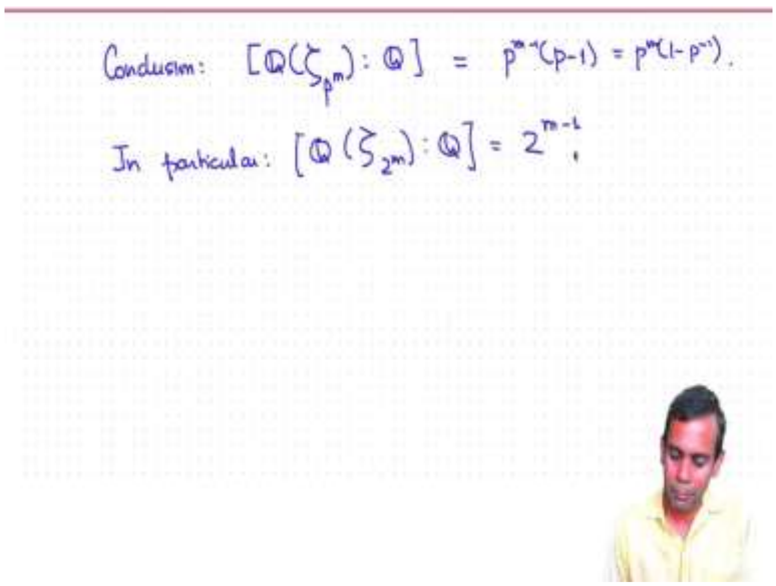
Now well try to get some further mileage out of Eisenstein's criterion. Let us ask what about so we have looked at pth roots of unity, what about prime power roots of unity, what about zeta p to the power m, where m is a positive integer. Now let us see we can guess something here, so what is zeta p power m? this is e to the 2 Pi i by p power m. What we have is that zeta p power m to the power p to the power m minus 1 is, e to the 2 Pi i by p power m whole to the power p to the m minus 1 is just e to the 2 Pi i by p, which is just zeta p.

So zeta p to the power m raised to the p power m minus 1 is zeta p and so this will satisfy the irreducible polynomial for zeta p therefore zeta p to the power m satisfies is the root of the polynomial Phi pt to the power p to the power m minus 1 which is just the polynomial t to the power p minus 1 times p power m minus 1 plus t to the power p minus 2 p to the power m minus 1 plus dot dot dot plus t to the power p to the power m minus 1 plus 1.

And so the question is, is this really the irreducible polynomial of zeta p to the m or not? and the claim is that, this is irreducible. The proof is exactly the same apply Eisenstein's criterion after replacing the variable by t plus 1 slightly you know it is it is a different polynomial so obviously, you need to check it again but the proof is the same in all respects I will leave it to you as an exercise to check.

So, what we are saying is that this is in fact the irreducible polynomial of the p to the nth root of unity. So what we get is phi p to the m the p to the m cyplo cyclotomic polynomial is the pth cyclotomic polynomial evaluated at t to the power p to the power m minus 1 and so what is the degree here, the degree is p minus 1 times p to the power m minus 1.

(Refer Slide Time: 17:24)



So, we have that, the degree of the field extension generated by p to the power mth root of unity over Q is p power m minus 1 into p minus 1, which I like to write as p power m times 1 minus p inverse. In particular if you take powers of 2 then you just get 2 to the power m minus 1 the p minus 1 part goes away.