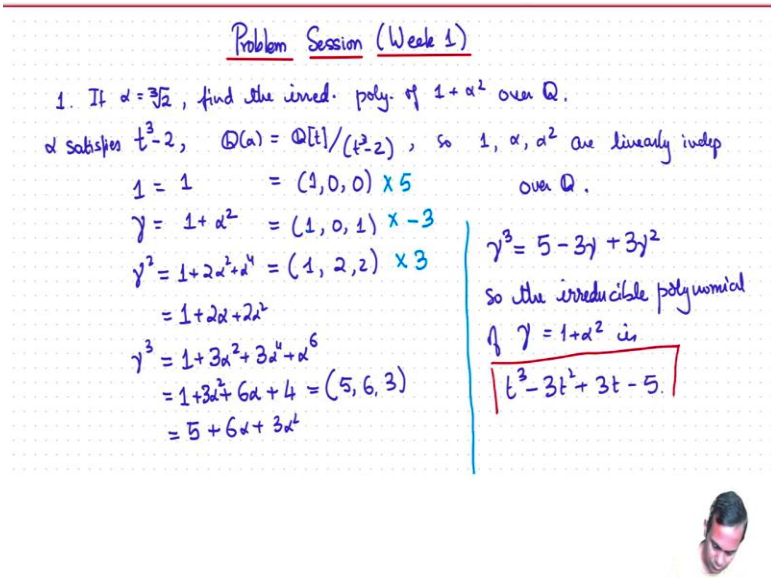
**Algebra - II**
**Professor Amritanshu Prasad**
**Mathematics**
**The Institute of Mathematical Sciences**
**Lecture 8**
**Solved Problems (Week 1)**

(Refer Slide Time: 0:15)




Let us solve some problems. So here is the first problem, if alpha is the cube root of 2 find the irreducible polynomial of 1 plus alpha square over Q. So alpha is cube root of 2 then what we know is that the irreducible polynomial of alpha is t cube minus 2. Alpha satisfies t cube minus 2 and t cube minus 2 is clearly irreducible over Q because it has no roots over Q, a cubic polynomial cannot be irreducible unless it has root.

So alphas satisfies t cube minus 2 and so Q alpha is a just Q t mod t cube minus 2 which means that 1, alpha and alpha squared are linearly independent over Q. So with that in mind let say gamma is 1 plus alpha squared. We want to find a polynomial which, any irreducible polynomial that gamma satisfies. So the strategies for all these problems, so basically if you have a polynomial say gamma satisfies a polynomial like gamma to the 4 minus 3 gamma square plus 1 equals 0.

Then essentially this if you think of gamma, gamma squared, gamma cube and also 1 as elements of Q alpha then you can think of them as vectors and expand them in the basis 1 alpha and alpha square. And this kind of equation is a linear relation between those vectors. So idea is we start with gamma and we could even think 1 so that just 1 and we can think of this as vectors one we expand them to the 1 alpha and alpha square.

So we just compute some powers of gamma and then look for the first time those vectors become linearly dependent. So in terms of the coordinates 1, alpha, alpha squared this is, this has 1, 0, 0 coordinates, this has coordinates 1, 0, 1. What about gamma squared? Well it is 1 plus 2 alpha squared plus alpha to the power 4. So this has coordinates well alpha to the power 4, we know that alpha cube is 2 so this is 1 plus 2 alpha plus 2 alpha square.

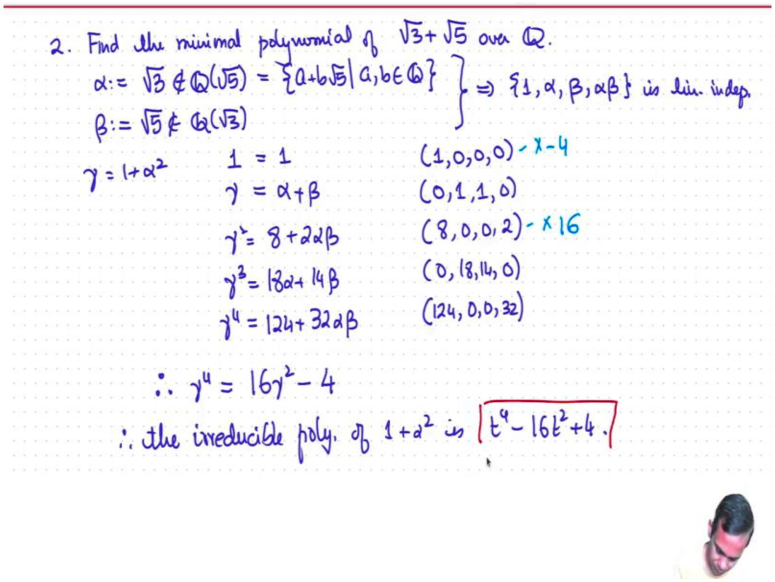
So this has coordinates 1, 2, 2 and let us look at gamma cube this has coordinates. So far this vectors look like they are linearly independent. If you take gamma cube now then we get that gamma cube is 1 plus 3 alpha square plus 3 alpha to the power 4 plus alpha to the power 6 which is 3 alpha squared is 6, 3 alpha to the power 4 is alpha cubed is 3 so this is 3 into 6 alpha and alpha cubed is 2 so alpha to the power 6 is 4. So we get, I am sorry, 3 alpha squared is not 6, it is just 3 alpha squared.

Alpha squared is not 2, alpha cubed is 2 so what we get is 5 plus 6 alpha plus 3 alpha square. So this has coordinates 5, 6, and 3. So now we look at these 4 vectors they must have a linear dependence because they are vectors in Q cube. So let us just figure out, how to write gamma cube expand gamma cube in terms of 1, gamma and gamma square.

Now if you look at these coefficients here, so if you look at the second coordinate for example. So the second coordinate here is 2, here it is 0. So the only way, so we are looking for a relation of the form a1 plus a2 times gamma plus a3 times gamma square is equal to gamma 3, gamma cube. So you look at the second coordinate the only possibility is that a3 is 3. So this has to be multiplied by 3.

And once you do that this becomes 6 but now let us look at the third coordinate. So if I do 3 times this I get 6 here and so I have to subtract 3 times 1 to get 3 back. So I have to do this times minus 3. And but then when I do that this 3 times 1 and minus 3 times 1 they cancel out and so to get 5 here I have to do 5. So anyway one way or the other I find out that gamma cube is equal to 5 minus 3 gamma plus 3 gamma squared. And so the irreducible polynomial of gamma which is this 1 plus alpha squared is t cube minus 3t square plus 3t minus 5 and that is your solution.

(Refer Slide Time: 6:34)




Here is the second problem. Find the minimal polynomial of square root 3 plus square root 5 over Q. Before we jump into the calculation, let us just note that square root 3 does not belong to Q adjoint square root 5. Because we know that this Q adjoint square root 5 consists of complex numbers of the form a plus b root 5 where a and b are rational numbers. And it is not difficult to show, so if you have a number like this its square a plus b root 5 square is going to be a square plus 5b square plus 2ab root 5.

And if you want this square to be 3 then you would need either a to be 0 or b to be 0, in fact for the square to be rational number you would need either a to be 0 or b to be 0. Otherwise this 2ab root 5 term will come to haunt you. But if a is 0 or b is 0 then you cannot have, so if for example if a is 0 then you are looking at b root 5 squared which will be 5 b squared but 3 is not a multiple of 5. So it cannot be that b root 5 squared is 3 and similarly of course a squared cannot be 3 because a is a rational number and square root of 3 is rational.

So we know that square root 3 does not lie in Q adjoint root 5 and very similarly we know that square root 5 does not lie in Q adjoint root 3. What this means is that 1 alpha, so let us give this names, so let say alpha equals let us call this alpha square root 3 and beta square root 5. So 1 alpha of course these are linearly independent over Q, 1 and beta are linearly independent over Q but alpha and beta linearly independent because beta is not in Q root 3 in not in the field obtained by adjoining alpha to Q.

And again alpha beta is linearly independent of both alpha and beta because alpha, beta is neither in Q root 3 not in Q root 5. It is not in Q root 3 because alpha is in Q root 3 but beta is not in Q root 3. So alpha, beta cannot be in Q root 3. So these are linearly independent. So this is linearly independent set and so now we take gamma to be 1 plus alpha squared and just like last time we start computing powers of gamma.

So and we expand those powers in terms of this basis. So firstly take the 0th power. So 1 is equal to 1 in terms of this basis it correspond to the vector 1, 0, 0, 0. Now let us look at gamma this is just alpha plus beta. So this is the vector 0, 1, 1, 0 in terms of this basis gamma squared is alpha squared plus beta squared which is 8 plus 2 alpha, beta. So this corresponds to 8, 0, 0, 2 in this basis.

And you can see so far this vectors are all linearly independent. And let us look at gamma cubed for its 8 plus 2 alpha beta into alpha plus beta. So what we get is, so let us just do it some rough work here 8 plus 2 alpha beta into alpha plus beta that works out to 8 alpha plus 8 beta. Now 2 alpha beta into alpha is 2 alpha squared beta but alpha squared is 3, so that is 6 beta and 2 alpha beta into beta is 2 alpha beta squared but beta squared is 5, so this becomes 10 alpha.

So what we get here is that this is 18 alpha plus 14 beta. And this again see this vectors are very nice they either have non zero coordinates in the two middle coordinates as in gamma and gamma cubed or they have non zero coordinates in the first and last coordinates as in 1 and gamma square. So it is very easy to see that this are linearly independent you just check that this vector and this vector are linearly independent, this vector and this vector are linearly independent, obviously all 4 of them are linearly independent.

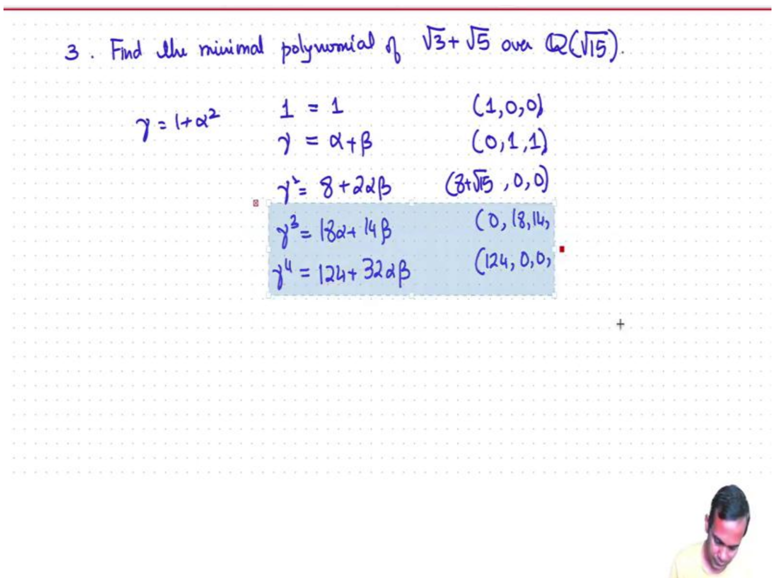
What about gamma to the power 4? So we have 18 alpha plus 14 beta let us just use the space here to do the calculation. 18 alpha plus 14 beta into alpha plus beta. So what we get is 18 alpha squared, 18 alpha squared but alpha squared is 3. So that is 18 into 3 which is 54 plus 14 beta squared. So beta squared is 5, so 14 into 5 that is 70 plus 18 alpha beta plus 14 alpha beta. So that is 18 plus 14 which is a 32 alpha beta.

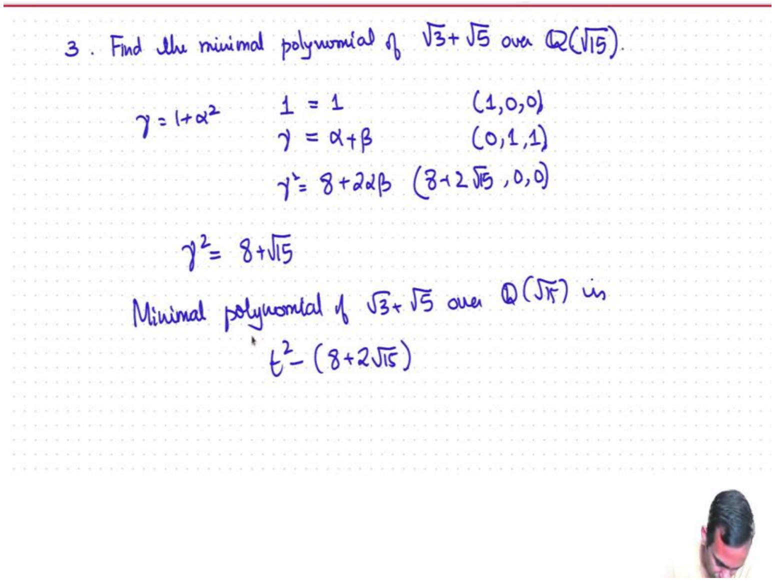
So 54 plus 70 that is 124. So we get 124, 0, 0, 32 these are the first 5 powers of gamma starting with gamma to the power 0. And now we can find a linear dependence between these vectors. Now this gamma to the power 4, we want to express it as a linear combination of 1 gamma,

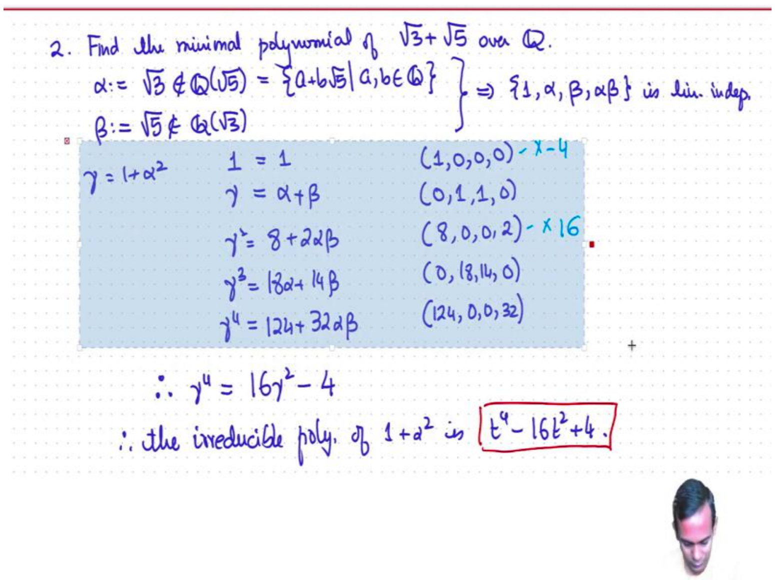
gamma squared and gamma cubed. Well two middle coordinates of gamma to the power 4 are 0. So we only need to worry about, we will only use these two vectors in our expansion.

We will only use 1 and we will use gamma square and luckily for us here this coordinate is 0. So we know that this vector gamma squared must occurs 16 times to get this. But if this occurs 16 time then here we have 8 into 16, what is 8 into 16 so 16 into 4 is (()) (13:15) 128. So we would have 124 minus 128, and so we would have to, we would have 128 so we would have to subtract 4. So this into minus 4 so what we get is, gamma to the power 4 equals 16 gamma square minus 4. Therefore, the minimal polynomial, the irreducible polynomial of 1 plus alpha squared is t to the power 4 minus 16 t squared plus 4 that is the solution.

(Refer Slide Time: 14:12)





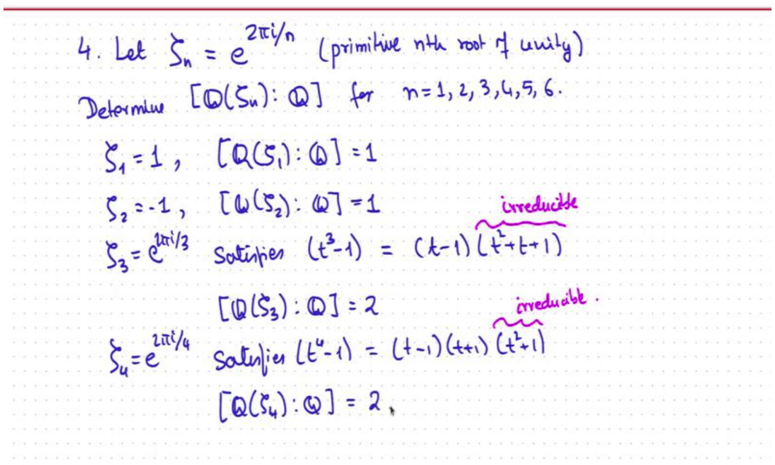

Now I am going to take the previous problem and change it just a little bit firstly instead of problem 2 I am going to call it problem 3 and instead of finding the minimal polynomial of root 3 root plus 5 over Q, I am going to ask for the minimal polynomial of root 3 plus root 5 over Q square root of 15. Now this is actually our old alpha beta. So alpha beta is no longer, is no longer linearly independent of 1 and alpha and beta because alpha beta is already in the field.

So alpha beta is a scalar, so what we do is we go back to the previous problem and we look at this powers but now what we have is alpha beta is over here. So let me just, let me just copy this whole thing and bring it over to the next slide. So this are the calculations in Q but now this alpha beta is part of the first coordinate. So we no longer have this third coordinate. And this rather fourth coordinate and so what we are saying is that this is 1, 0, 0.

This is well still alpha plus beta but this was a 8 plus 2 alpha beta. So what we get is here we would write 8 plus root 15 because now that is in the field. But this gamma squared is already now a scalar multiple of 1, 0, 0. So this two steps we do not need at all. So we do not need this bit here. So we will just remove it and so what we get is gamma squared.

Since we are working over Q root 15, we get gamma squared is 8 plus root 15 and so what we have is that the minimal polynomial of root 3 plus root 5 over Q root 15 is t square minus 8 plus root 15 and that is the solution. I am sorry this should be I think there was a 2 there right? yeah that is a 2, so there should be 2 root 15. 8 plus 2 root 15 and so this should be 8 plus 2 root 15 and that is the solution to our problem.

(Refer Slide Time: 17:37)




Now come to problem 4 which is a very interesting class of a numbers was minimal polynomial we shall seek. Let zeta n be e to the power 2 pi i by n. So this is a complex number and if you raise this number to the power n then you get 1. So this is, this is called a primitive nth root of unity. The powers of this number are all the nth roots of unity in the complex number. All the numbers which if you raise the power to n you get 1.

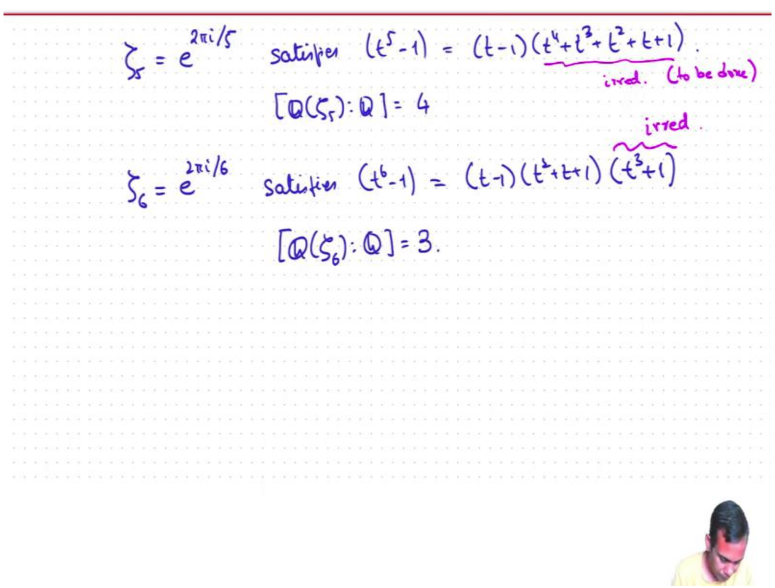
And a very interesting problem is to determine the degree Q zeta n over Q for, well you so this is known for all n but today we will just do n equals 1, 2, 3, 4, 5, 6. So we will try this, we may not succeed in solving all of them but what we know right now. So let us give it a shot. So what is zeta 1, so zeta 1 is just 1 it is a rational number. So Q zeta 1 over Q has degree 1. In fact, the minimal polynomial the irreducible polynomial of zeta 1 is just t minus 1.

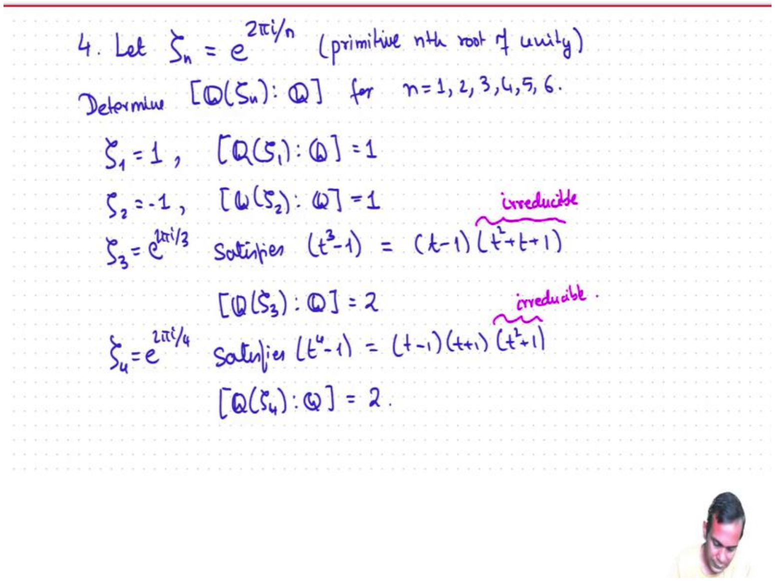
Zeta 2 is minus 1 again it is rational, so Q zeta 2 over Q is equal to 1. What about zeta 3? So zeta 3 turns out to be a well e to the 2 pi i by 3 it is a cube root of unity. So it satisfies the polynomial t cube minus 1 which is t minus 1 into t squared plus t plus 1. But of course we know that t minus 1 does not vanish at zeta 3. So t squared plus t plus 1 must vanished at zeta 3. And t squared plus t plus 1 is irreducible over Q. So this must be the irreducible polynomial of zeta 3.

And so this part is irreducible and satisfy and vanishes at zeta 3. So what we get is that Q zeta 3 over Q is just 2, this is the irreducible polynomial. Let us look at zeta 4. So zeta 4 is a e to the 2 pi i by 4 which we also know to be the number i. The square root of minus 1 and this satisfies t to the power 4 minus 1 which I can write as t minus 1 into t plus 1 into t squared plus 1. Now this factors do not vanish at zeta 4.

So we are only left with this factor and this is irreducible again. So for quadratic polynomials easy to check that they are irreducible, you just use the formula for the root of a quadratic polynomial the discriminant is negative then they are irreducible. So this is irreducible and so again we get Q zeta 4 over Q is equal to 2.

(Refer Slide Time: 21:26)






And now let us go to zeta to the power 5. So zeta power 5 is e to the 2 pi i over 5 and this satisfies t to the 5 minus 1 which I can write as t minus 1 into t to the 4 plus t squared plus t plus 1. Now t to the power 4 sorry there is one more term missing plus t cube plus t square plus t plus 1. And well it turns out that this polynomial is irreducible but showing that it is irreducible may not be that easy I will differ it to next week.

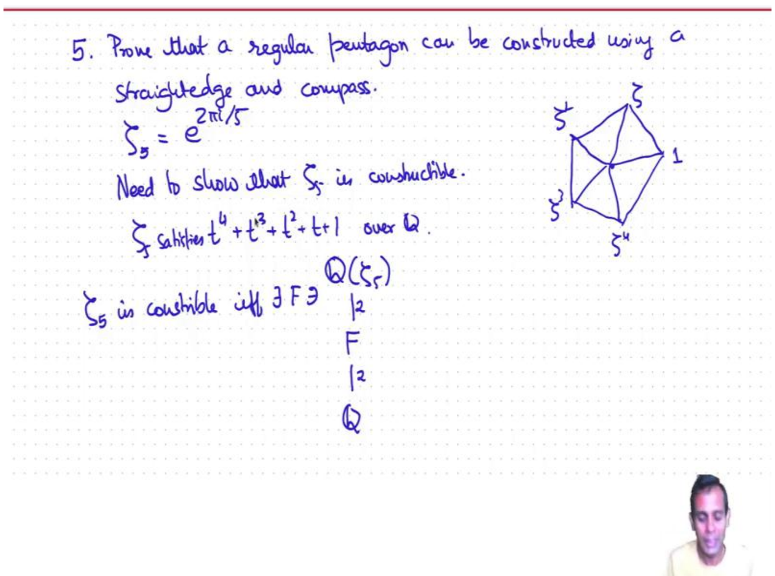
And the you will see this when we through Eisenstein criterion for irreducibility but anyway it turns out that this guy is irreducible. And in any case zeta 5 does not satisfy this. So this, so this is to be done. So we have not technically fully solved this problem you can try it proving that it is irreducible with how much you know right now like by looking for a factorization. We know it has no roots but we need to know that it does not have any quadratic factor.

So you can try to do that with your bare hands comes out more easily where the Eisenstein criteria. So this needs to be shown to be irreducible. But then if we accept the fact that is irreducible then what we get is Q zeta 5 over Q has degree 4. Because this polynomial is of degree 4. Interesting one zeta 6 e to the 2 pi i by 6. So this satisfies t to the power 6 minus 1 and this has a nice factorization.

So it is a t cube minus 1 into t cube plus 1 but t cube minus 1 is t minus 1 into t squared plus t plus 1. And then there is another thing which is t to the power 4 plus t squared plus, no that is just t cube plus 1. So these two give t cube minus 1 and this is t cube plus 1, t cube minus 1 into t cube plus 1 is t cube minus 6. Now this does not vanish at zeta 6, this also does not vanish at zeta 6 we know what its roots are, its roots are zeta 3, zeta 3 squared.

So this does not vanish at zeta 6, so this must be, so this polynomial vanishes at zeta 6. And this polynomial is irreducible again for cubic polynomial we know it is irreducible if it does not have a root. So this guy is irreducible and so what we get is that the degree of Q zeta 6 over cube is equal to 3. So we have an interesting sequence here 1, 1, 2, 2, 4 and 3. See if you can guess what the pattern is, this is a very important class of field extensions, these are the cyclotomic extensions and we will keep revisiting them during this course.

(Refer Slide Time: 25:03)




A last problem, prove that a regular pentagon can be constructed using a straightedge and compass. Now you can construct a regular pentagon if you can construct a fifth root of unity. So like zeta 5 as before the e to the 2 pi i by 5 and if you can show that this point is constructible then its powers will also lie in the same field Q adjoints zeta 5 and you can realize a regular pentagon as having corners of given by the, so if I draw a regular. It is not a great drawing but straight in through it a bit.

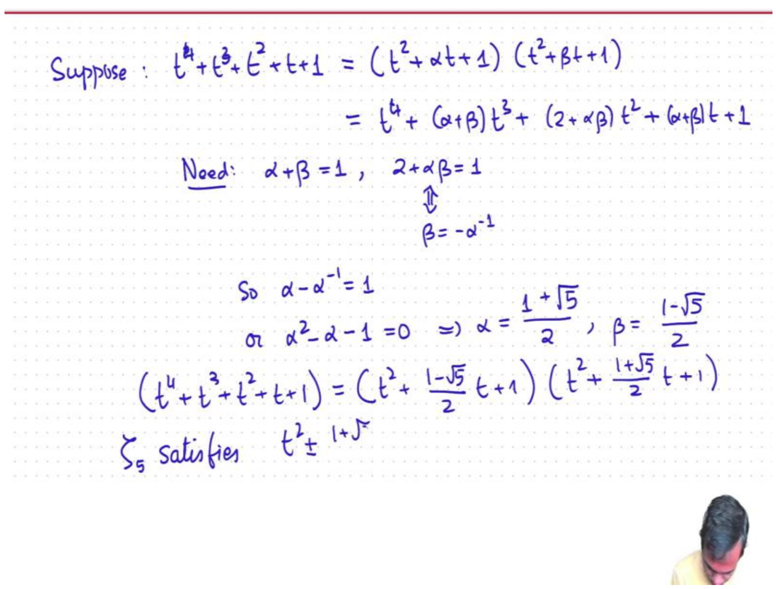
That is the best I can do. So this is 1, this is zeta, this is zeta squared, this is zeta cubed and this is zeta power 4. And these will all have the same angle related to each other at the center. So this will be a regular pentagon, so we just need to show that we can construct the point zeta is constructible. And then its powers will automatically be constructible by our criterion for constructability.

So we need to show that a zeta 5 is constructible. Well we have already seen that zeta 5 probably has degree 4 over Q. It satisfies a polynomial of degree 4 at any date. So let us just see that, so in fact we have a zeta 5 satisfies t to the power 4 plus t cube plus t squared plus t plus 1 over Q. And to show that it is, so the degree of zeta 5 is 4 Q, Q adjoint zeta 5 is probably 4 well we have not quite prove that but it become clear by the time I solve this problem.

So what we have is this, you have this Q zeta 5, zeta 5 does not satisfies any quadratic polynomial over Q. So what we are asking is, you know can we find a field here F between Q zeta 5 and Q such that F is of degree 2 over Q and Q zeta 5 is of degree 2 over F. So zeta 5 is constructible if and only if we can find this. F such that this holds, i. e., F lies between Q zeta 5 and Q and F is degree 2 over Q and Q zeta 5 is degree 2 over F.

So we are looking for this kind of a field. So in these fields since this is the quadratic equation zeta 5 would satisfy a quadratic polynomial over F. So what we would try to do is take this polynomial of degree 4 and see if we can write it as a product of two quadratic polynomials over some intermediate field.

(Refer Slide Time: 28:21)




So we would have to have factorize t to the power 4 plus t squared plus t cube plus squared plus t plus 1 and we want to factorize this we would have two quadratic factors. And let us just try this with t squared plus alpha t plus 1 and t squared plus beta t plus 1. Let us try to find a factorization like this. And alpha beta need not be rational numbers, they just need to lie in a quadratic extension of Q.

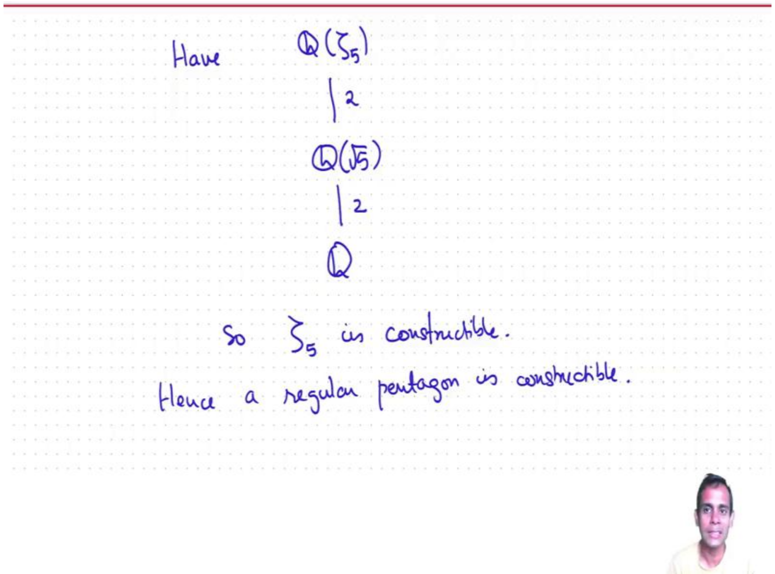
So if we expand this, what we get is t to the power 4 then the coefficient of t cube is so alpha plus beta t cubed and then the coefficient of t squared is 2 plus alpha beta t squared. And then the coefficient of t is again alpha plus beta t and then plus 1. So what we need to is alpha plus beta is equal to 1 and 2 plus alpha beta is equal to 1. Well alpha, 2 plus alpha beta is equal to 1 is the same as saying that beta is minus alpha inverse.

And substituting that in here we have alpha minus alpha inverse is equal to 1 multiplying by alpha and bringing everything to the left hand side, we get alpha squared minus alpha minus 1 is equal to 0. Which means that alpha has to be 1 plus or minus square root 5 over 2, 1 plus square root 5 over 2 is the golden issue. This is a very famous quadratic equation and well so beta, so maybe we can take alpha to be 1 plus square root 5 over 2.

And we can take beta to be 1 minus square root 5 over 2 and you will find that all your conditions are satisfied. So what we get is t to the power 4 plus t cube plus t squared plus t plus 1 is equal to t squared plus 1 minus root 5 over 2 t plus 1 and t squared plus 1 plus root 5 over 2 plus 1. So what we have is now the field generated by 1 plus root 5 over 2 contains 1 minus root 5 over 2 and the field generated by 1 minus root 5 over 2 contains 1 plus root 5 over 2.

These are the same field and so what we have is that zeta 5 satisfies the quadratic equation t squared plus or minus one of these equations 1 over root 5 by 2 plus 1. So maybe it satisfies one of these over Q adjoint root 5. So that is our intermediate field Q adjoint root 5.

(Refer Slide Time: 31:51)




So we have Q zeta 5 lies over Q adjoint root 5 lies over Q and each of this is of degree 2. And so zeta 5 is constructible, it is a constructible point and hence a regular pentagon is constructible. Now it could be an interesting project for you to take this idea and try to translate it into an actually straightedge and compass construction for a regular pentagon. I hope you have fun doing that but I will just leave you with this challenge as for now.