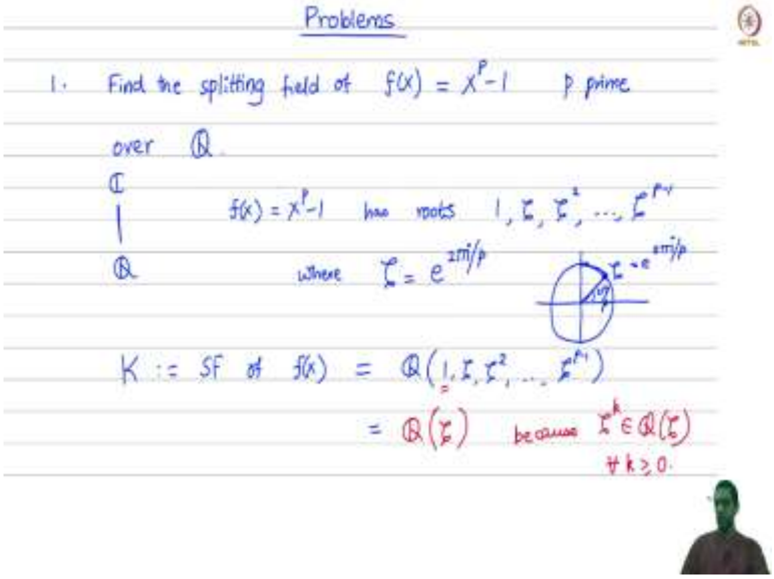
Algebra II
Professor – S. Viswanath
The Institute of Mathematical Sciences
Solved Problems, Part 2 (Week 3)

(Refer Slide Time: 00:14)



Problems

1. Find the splitting field of $f(x) = x^p - 1$ p prime over $\mathbb{Q}$.

$$\begin{tikzcd}\mathbb{C} \arrow[d, dash] \\ \mathbb{Q}\end{tikzcd}$$

$f(x) = x^p - 1$ has roots $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$

where $\zeta = e^{2\pi i/p}$

$K := SF$ of $f(x) = \mathbb{Q}(1, \zeta, \zeta^2, \ldots, \zeta^{p-1})$

$= \mathbb{Q}(\zeta)$ because $\zeta^k \in \mathbb{Q}(\zeta)$ $\forall k \geq 0$.

Let us do some problems on computing splitting fields and the degree of the the splitting field over the base field. So here is the first problem. So, compute or find the splitting field, find the splitting field of the polynomial, splitting field of the polynomial f of x equals x to the p minus 1, where p is now a prime. And I sort of want you to find the splitting field of this polynomial over the base field, which is the field of rational numbers.

So, let us recall what the definition of the splitting field was, or how one could find the splitting field of a polynomial. So, let us recall. So, what are we supposed to do here? So, take Q, base field. Now, in this case, there is this convenient field, the field of complex numbers on top of Q, which is algebraically closed. So, any polynomial has all its roots in C. So, what we could do is just take this this polynomial f of x, so what are its roots in in C?

So, if x equals x to the p minus 1 has complex roots. Well, what are they? They are 1, so let me call this zeta, zeta square, and so on till zeta to the p minus 1, where zeta is the, what we call the primitive pth root of unity. So, it is e to the 2pi i over p. So, if you think in terms of the complex plane, so this is just, so this is on the unit circle, and look at this angle here, which is 2pi divided by p. So, you are dividing the circle into p equal equal sectors.

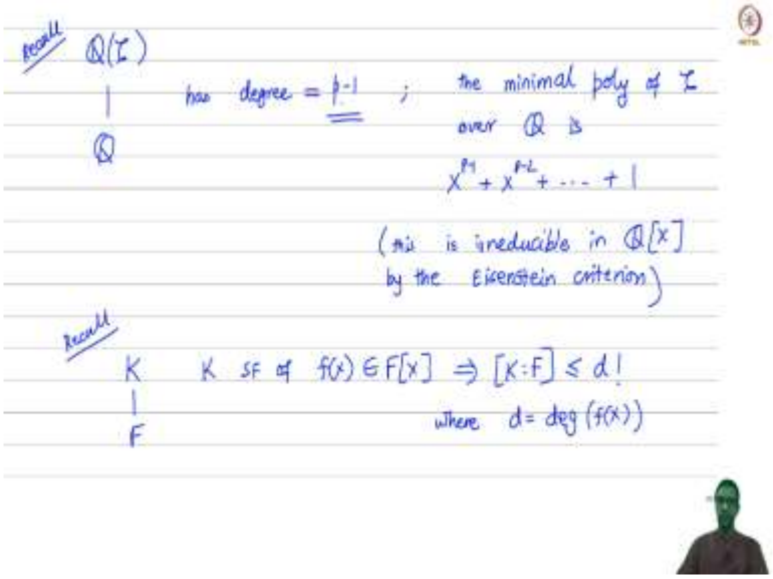
And this number here on the unit circle in the complex plane is what we call zeta, it is e to the 2pi i over p. So, these are the roots and then how is the splitting field itself formed? So, recall, let K denote the splitting field, which I have abbreviate to SF, the splitting field of f of x is well take Q and Q adjoined to it all the roots of this polynomial. So, look at 1, zeta, zeta square, till zeta to the p minus 1.

So, I need to take the subfield of C, which is generated by Q and the roots of this polynomial f. But observe of course when you adjoin elements, some of those elements do not really need to be adjoined, you do not get a new field. For example, if I adjoin the root 1 to the base field Q, I do not get anything new. That is just Q again, because 1 belongs to the base field. And well, so I do not really need to adjoin 1. So, I could just adjoin the next guy, which is zeta.

But observe that as soon as he observed, as soon as you as you adjoin zeta, then of course, Q of zeta is a field and because it is a field and zeta belongs to it, automatically zeta square, zeta cubed and so on all powers of zeta, automatically belong to this field. So, observe that because all powers of zeta, zeta power K are automatically inside this field Q zeta.

Then this for all K infinite, for all K greater than equal to 0, so we understand what the splitting field is, you can just get it by adjoining a single element to Q that element is just the complex number e to the 2pi i by p.

(Refer Slide Time: 04:11)



recall $\mathbb{Q}(\zeta)$ has degree $= \underline{\underline{p-1}}$; the minimal poly of ζ over $\mathbb{Q}$ is $\mathbb{Q}$

$x^{p-1}+x^{p-2}+\dots+1$

(this is irreducible in $\mathbb{Q}[x]$ by the Eisenstein criterion)

Recall K K SF of $f(x) \in F[x] \Rightarrow [K:F] \leq d!$

F where $d = \deg(f(x))$

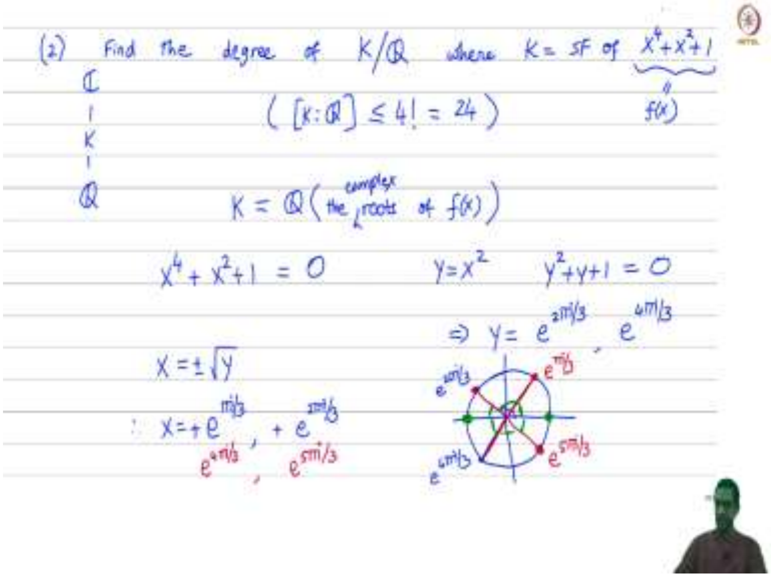
Now, of course, I want to understand what the degree of this extension is. So, you have seen this before. So, this is what we call the cyclotomic extension. So, Q zeta over Q and observe this has degree. So, recall from your earlier lectures on cyclotomic extensions that this has degree equal to p minus 1. And why was this? Because the the minimal polynomial or the irreducible polynomial, the minimal polynomial that zeta satisfies.

So, minimal polynomial of zeta over Q is just the polynomial x to the p minus 1 plus x to the p minus 2 plus dot dot dot till 1. So, and recall this, you know one showed that this was irreducible. So again, this is an irreducible polynomial in Qx. And to establish this one use this important thing called the Eisenstein criterion by the Eisenstein criterion.

And it involved a little bit more, one had to sort of replace x by x plus 1 and do a little trickery there. But anyway, it came from the Eisenstein criterion. Good. So that is the first problem. What it says is that the splitting field of the polynomial x to the p minus 1 is the cyclotomic field Q of zeta. And it has degree p minus 1.

So, recall, of course, the general fact we showed, the general upper bound we proved was that if I have a polynomial, so so let us say this is K, and I have some base field F. And suppose if K is the recall, or upper bound, K is the splitting field of some polynomial fx in FX, means that the degree of K or F, as we shown already is at most d factorial, where d is the degree of this polynomial f of x. So, in this particular example, it is at most p factorial, but in reality, it is much, much smaller, which is actually just p minus 1.

(Refer Slide Time: 07:00)



(2) Find the degree of $K/\mathbb{Q}$ where $K =$ SF of $\underbrace{x^4+x^2+1}_{f(x)}$

$$\begin{tikzcd} \mathbb{C} \arrow[d, dash] \\ K \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

$([K:\mathbb{Q}] \leq 4! = 24)$

$K = \mathbb{Q}(\text{the complex roots of } f(x))$

$x^4 + x^2 + 1 = 0$ $\quad y = x^2 \quad y^2 + y + 1 = 0$

$\Rightarrow y = e^{2\pi i/3}, e^{4\pi i/3}$

$x = \pm\sqrt{y}$

$\therefore x = +e^{\pi i/3}, +e^{2\pi i/3}$

$e^{4\pi i/3}, e^{5\pi i/3}$

Let us move on to the second problem. So again, let us compute the splitting field. So, let us again take the base field to be Q, and let us ask, find the splitting field. Find the degree in fact, of K over the base field Q, where what is K? K is just the splitting field of the polynomial x to the 4 plus x square plus 1.

So, I have K over Q, I have told you what K is, it is the splitting field of a fourth degree polynomial. Of course, the degree therefore, the, our upper bound says that KQ can be at most 4 factorial, which is 24. But like we saw in the earlier example, in practice, this is often much smaller. So, let us see what it is in this particular example.

So again, like we did in the earlier problem, we proceed similarly. We first take Q and to it, we adjoin all the complex roots of this polynomial. So, let us call this polynomial f of x. So, we will recall that I have C on top. And so, I can just think of K as Q adjoined all the roots of this polynomial. The roots, the complex roots of this polynomial fx. So, let us try and find out what the roots look like?

So firstly, f of x is x to the 4 plus x square plus 1. So, I need to solve the following equation x to the 4 plus x square plus 1 equals 0, to find the roots. So of course, it is easier to just put y equals x square and solve the equation y square plus y plus 1 is 0. So, this is just the I mean, we know the solution to this, these are the cube roots of unity. So, this is y is just what we would usually write as omega and omega square.

So, let me just write them out explicitly e to the 2pi i by 3 and e to the 4pi i by 3. So, these are the two cube roots of unity, other than one itself. So, this is my complex plane. So, omega is this fellow here, which makes 120 degree angle, e to the 2pi i by 3, omega square is the other root e to the 4pi i by 3. And of course, this is what y is. So, x, since x square is y.

So how do I compute x from here? Well, x is just a square root of y, x is just, well, there will be two possible square roots. So, I need to say, let us compute e to the 2pi i by 3. So, let me say x is like plus minus the square root of y if you wish. And here y is just e to the 2pi i by 3, so I pick one square root, which is therefore.

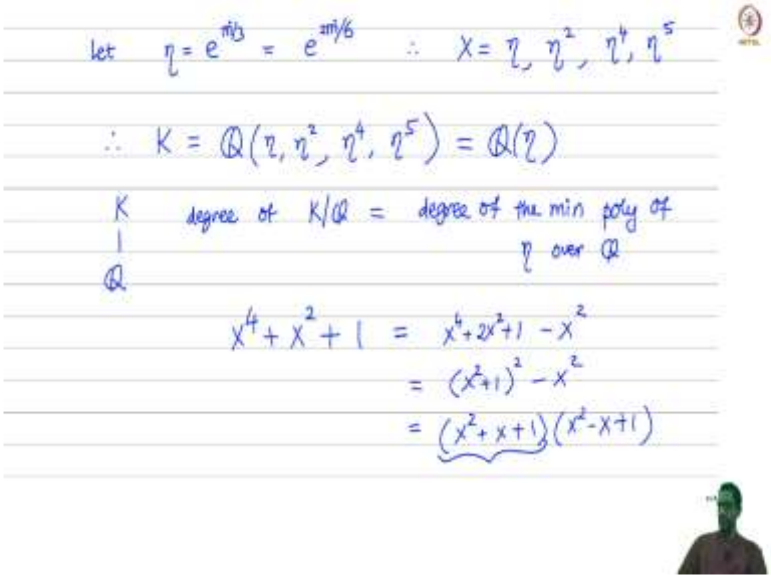
So, what are my solutions for x? It is the square root of 2pi i by 3 is just pi i by 3. So, it is plus minus pi i by 3, plus minus 4pi i by 3 square root is 2pi i by 3. So, I take plus minus 2pi i by 3. So, let us also locate these roots on the diagram. So, e to the 2pi i by 3, the square root is sort of something which makes half the angle.

So, this is e to the pi i by 3, e to the minus pi i by 3, I am sorry, minus e to the pi i by three is just the thing on the other end of the diagram, I mean, it is just diametrically opposite. So, this is actually the same as e to the 4pi i by 3. So, x equals minus e to the pi i by 3, so that minus, I can just think of as e to the 4pi i by 3.

And similarly, e to the 2pi i by 3 is this, this point, and negative of that is just something on the other end. So, what is this going to be? This is just going to be, so let us see, this is 1, 2, this is 4 and 5. So 5pi i by 3. So, what are these really? Well, you can see these are nothing but the sixth roots of unity.

So, what are the six, sixth roots of unity? There should be six of them in all, so there are two more, that is plus 1 and minus 1. So, if I add in those two points as well, then observe that these 6 points that I have, the 2 green and the 4 reds, they are the sixth roots of unity, because you know the angle between each of them is a 60 degree angle.

(Refer Slide Time: 12:15)



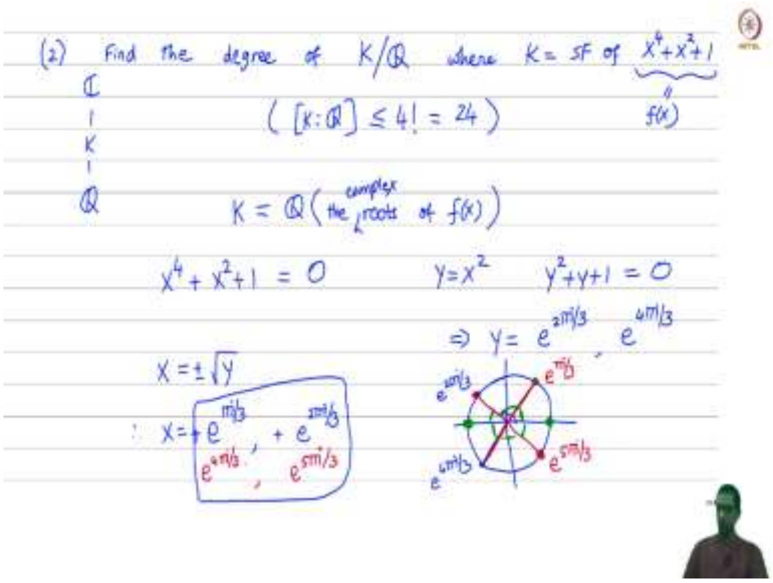
let $\eta = e^{\pi i/3} = e^{2\pi i/6}$ $\therefore$ $X = \eta, \eta^2, \eta^4, \eta^5$

$\therefore$ $K = \mathbb{Q}(\eta, \eta^2, \eta^4, \eta^5) = \mathbb{Q}(\eta)$

$$\begin{tikzcd} K \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

degree of $K/\mathbb{Q}$ = degree of the min poly of η over $\mathbb{Q}$

$$\begin{aligned} x^4 + x^2 + 1 &= x^4 + 2x^2 + 1 - x^2 \\ &= (x^2+1)^2 - x^2 \\ &= \underbrace{(x^2+x+1)}(x^2-x+1) \end{aligned}$$



(2) Find the degree of $K/\mathbb{Q}$ where $K =$ SF of $\underbrace{x^4+x^2+1}_{f(x)}$

$$\begin{tikzcd} \mathbb{C} \arrow[d, dash] \\ K \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

$$\left([K:\mathbb{Q}] \leq 4! = 24 \right)$$

$$K = \mathbb{Q}\left(\text{the complex roots of } f(x)\right)$$

$x^4 + x^2 + 1 = 0$ $\quad y = x^2 \quad y^2+y+1 = 0$

$\Rightarrow y = e^{2\pi i/3}, \ e^{4\pi i/3}$

$x = \pm\sqrt{y}$

$\therefore\ x = \boxed{\pm e^{\pi i/3}, \ \pm e^{2\pi i/3}, \ e^{4\pi i/3}, \ e^{5\pi i/3}}$

So, where are we? Let us, let us give this a name. So, I will just call this this very first guy, something. So, let us call that very first root, so that is e to the pi i by 3, or the same as e to the 2pi i by 6, forms a 60 degree angle. So, this is, let us call it eta. Therefore, the other roots, so what are the choices? What are the roots? x, x is eta, eta square, eta cube is not there, instead eta to the 4 and eta to the 5.

So those are these four guys. The four roots that I have here, are just eta, eta square, eta power 4and eta power 5, as you can see directly. Now, what is Q of eta? So, let us see. So, so, so what is the splitting field? So therefore, K is just, I need to take Q and I need to adjoin these four roots. But as we saw in the earlier example, we do not need to adjoin all of them.

If you adjoin eta, then you automatically get the rest, because powers of eta are definitely in this field. So now the question finally is, so we understand what the splitting field looks like, just take K and adjoin a single element, just e to the pi i by 3 to Q, with questions, what is the degree of this extension?

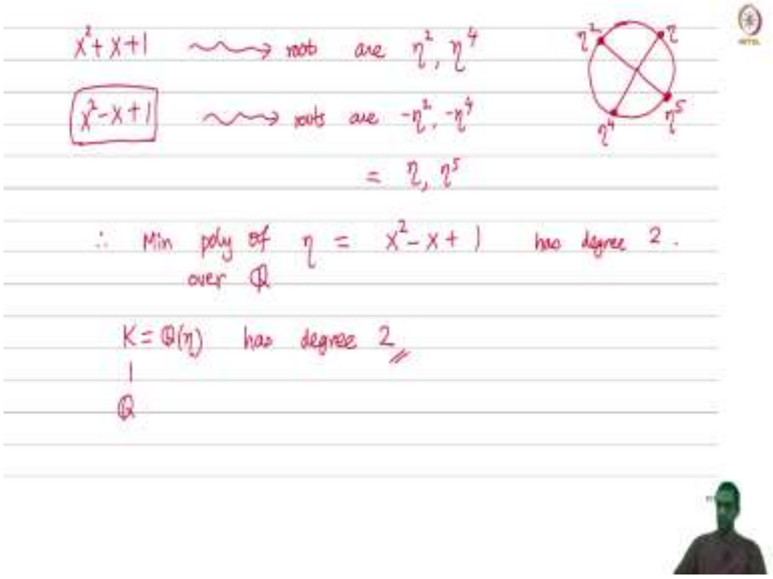
In other words, so K over Q, so then observe, the degree of this extension, degree of this extension is just nothing but the degree of the minimal polynomial that eta satisfies. So, this is just the degree of the minimal polynomial of eta over the rational numbers. So, let us see what is this this minimal polynomial that eta satisfies?

So, what are these four roots eta, eta square and so on? They were roots of which polynomial? Well, it was, let us go back to the original polynomial, x to the 4 plus x square plus 1. So of course, eta satisfies this polynomial. It was the root of this polynomial. But is this polynomial irreducible? That is the first thing we need to ask ourselves is x to the 4 plus x square plus 1 irreducible.

Well, one has to sort of play with it a little bit to see what can be done to it. But if you sort of use a little manipulation, so here is something you can do, x to the 4 plus 2 x square plus 1 minus x square. And now this is just x square plus 1, the whole square minus x square. And now I used identity. So that is a square minus b square. So that is a plus b into a minus b.

So, in fact, this factorises into a product of these two elements. Now, each of these factors is sort of familiar. So, what are the roots of x square plus x plus 1 equal to 0? Well, those are just the cube roots of unity. So, we know the roots of this. So, I should say, so maybe let us just go to the next slide.

(Refer Slide Time: 15:32)



$x^2+x+1 \rightsquigarrow$ root are η^2, η^4

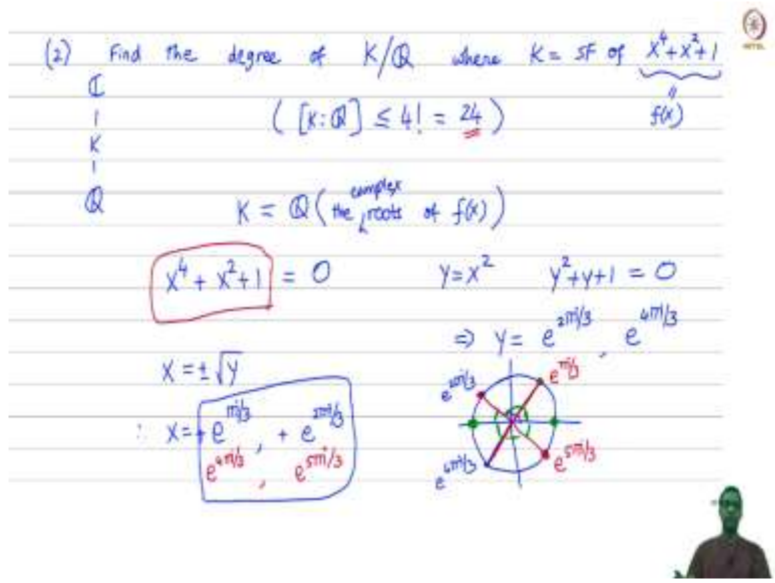
$\boxed{x^2-x+1} \rightsquigarrow$ roots are $-\eta^2, -\eta^4$

$= \eta, \eta^5$

$\therefore$ Min poly of η over $\mathbb{Q}$ $= x^2-x+1$ has degree 2.

$$\begin{tikzcd} K=\mathbb{Q}(\eta) \arrow[d, no head] \\ \mathbb{Q} \end{tikzcd}$$

has degree 2



(2) Find the degree of $K/\mathbb{Q}$ where $K =$ SF of $\underbrace{x^4+x^2+1}_{f(x)}$

$\mathbb{C}$ | K | $\mathbb{Q}$

$\left([K:\mathbb{Q}] \leq 4! = \underline{\underline{24}} \right)$

$K = \mathbb{Q}\left(\text{the } \overset{\text{complex}}{\text{roots}} \text{ of } f(x)\right)$

$\boxed{x^4 + x^2 + 1} = 0$ $\qquad y = x^2 \qquad y^2+y+1 = 0$

$\Rightarrow y = e^{2\pi i/3}, e^{4\pi i/3}$

$x = \pm\sqrt{y}$

$\therefore x = \boxed{\begin{matrix} + e^{\pi i/3}, & + e^{2\pi i/3} \\ e^{4\pi i/3}, & e^{5\pi i/3} \end{matrix}}$

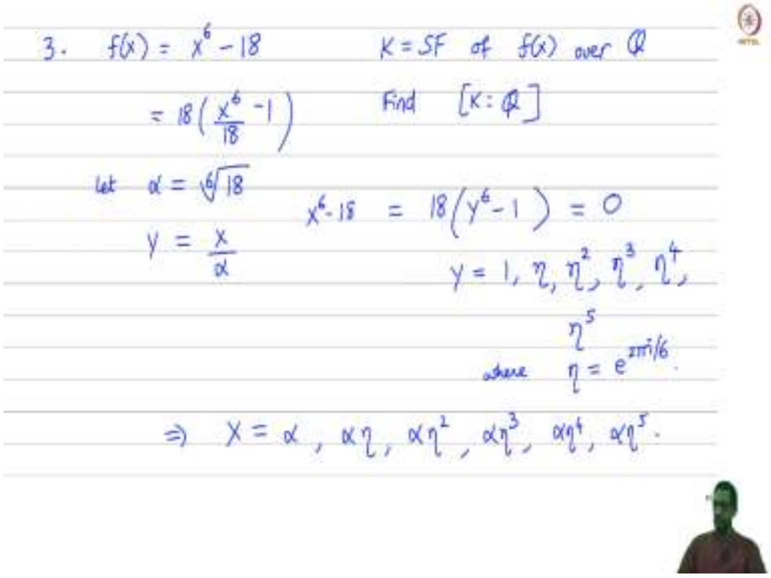
So, observe now x square plus x plus 1, its roots are the cube roots of unity. So, which in our figure, what were they? So that this guy was called eta, this fellow was called eta square, eta to the 4 and eta to the 5. So, the cube roots of unity were these two fellows, eta square and eta to the 4. And x square minus x plus 1 is 0.

Well, its roots are just the negatives of the, of these these guys, because observe the, the bottom polynomial is just obtained from the one on the top by replacing x by minus x. So, the roots of this are the negatives. And well, what is that? That is just the other two roots eta and eta to the 5. So, these two fellows are the roots of the other polynomial.

So, in fact, we now know what the minimal polynomial of eta is, so observe that the minimal polynomial of eta, so eta satisfies this polynomial x square minus x plus 1 is 0. So, this is just x square minus x plus 1. So, this is the minimal polynomial over Q. And it is easy to see it is irreducible. You cannot factor it any further.

Well, just because the the roots are not rational numbers. So therefore, this has degree 2. So, what does that mean? That, well, this extension K over Q that we were looking at K is Q of eta, this has degree 2. So, recall to start with, we said it is at most degree 4 factorial, which is 24. But it turns out that, you know, it is actually much much smaller. It is just a simple quadratic extension.

(Refer Slide Time: 17:31)



3. $f(x) = x^6 - 18$ $K = SF$ of $f(x)$ over $\mathbb{Q}$

$= 18\left(\frac{x^6}{18} - 1\right)$ Find $[K : \mathbb{Q}]$

let $\alpha = \sqrt[6]{18}$

$y = \frac{x}{\alpha}$ $x^6 - 18 = 18(y^6 - 1) = 0$

$y = 1, \eta, \eta^2, \eta^3, \eta^4, \eta^5$

where $\eta = e^{2\pi i/6}$.

$\Rightarrow x = \alpha, \alpha\eta, \alpha\eta^2, \alpha\eta^3, \alpha\eta^4, \alpha\eta^5$.

So, let us move on to the next problem. So, this is problem three, which is to compute, again, splitting field, but slightly harder one this time. So, let us take my polynomial f of x be the polynomial x to the 6 minus 18. And now again, I ask the same question, let K be its splitting field, splitting field of f of x over Q, find the degree of the extension?

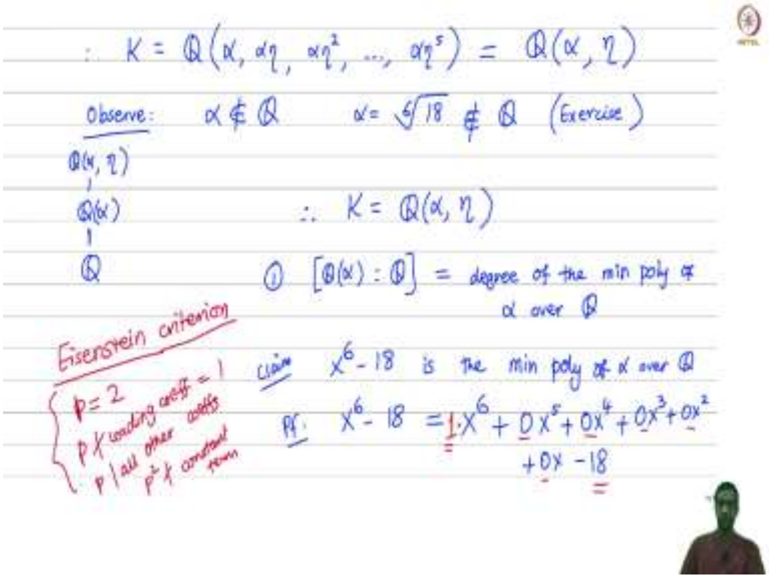
So, let us do this. So, let us rewrite it as follows. I pulled the 18 out, write it as x to the 6 by 18 minus 1. And let me just call this the first time as as y to the 6. So, let us do one thing. So, I mean, clearly there is an obvious root of this polynomial that I can write out, which is just the 6th root of 18. It is a real root. So, let alpha denote that real root, the 6th root of 18. And therefore, and, let me also change variables.

So, let me call y as x by alpha. So then observe that f of x can be rewritten as follows, if it was 18 times y to the 6 minus 1. So, I have changed variables to y and now it has this this nice form. So now let me think of my polynomial as a polynomial in y rather than a polynomial in x. So, to start with, I had this.

So, let me find its roots. Well, what are its roots? Well, this this polynomial has the obvious roots, which are the, the 6, 6th roots of unity. So, y is just 1, so I will just use the the notation of the previous problem, which is, I will call it eta, eta as the 6th root, eta to the 4, eta to the 5, where eta just denotes the 6th root of unity, so same notation as the previous problem.

So therefore, what is x? Well, x is just alpha times these possibilities. So, the roots x are just alpha, alpha times the 6th root of unity, alpha times cubed, 4 and 5. So these are the 6, 6th roots of I mean these are the 6 roots of this polynomial f of x.

(Refer Slide Time: 20:05)



$\therefore\ K = \mathbb{Q}(\alpha, \alpha\eta, \alpha\eta^2, \dots, \alpha\eta^5) = \mathbb{Q}(\alpha, \eta)$

Observe: $\alpha \notin \mathbb{Q}$ $\quad \alpha = \sqrt[6]{18} \notin \mathbb{Q}$ (Exercise)

$$\begin{tikzcd} \mathbb{Q}(\alpha,\eta) \arrow[d, dash] \\ \mathbb{Q}(\alpha) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

$\therefore\ K = \mathbb{Q}(\alpha, \eta)$

① $[\mathbb{Q}(\alpha) : \mathbb{Q}] =$ degree of the min poly of α over $\mathbb{Q}$

Eisenstein criterion

$p = 2$

$p \nmid$ leading coeff $= 1$

$p \mid$ all other coeffs

$p^2 \nmid$ constant term

Claim $x^6 - 18$ is the min poly of α over $\mathbb{Q}$

Pf. $x^6 - 18 = \underline{\underline{1}} \cdot x^6 + \underline{0}x^5 + \underline{0}x^4 + \underline{0}x^3 + \underline{0}x^2 + \underline{0}x - \underline{\underline{18}}$

Therefore, as before, what is the splitting field? I just take K, I take Q and adjoin to it these 6 fellows alpha, alpha eta, alpha eta square and so on till alpha eta to the 5 and observe as before that well I have to adjoin alpha definitely because alpha is not in Q. So, observe quick observation here, observe that alpha is not in Q, the 6th root of 18 is and what is alpha? Alpha is just a 6th root of 18.

So, what is the 6th root of 18? Well, I mean one has to just show this is not a rational number. So, I will leave that as an, as an exercise. Similar to showing for example, that square root of 2 is irrational and so on. Similarly, you can show that this is, this is not rational. Now, so, so, definitely I have to adjoin alpha at least. So, I take Q and when I adjoin alpha, I get something strictly more than Q, a bigger field.

And now, of course, I need to adjoin the next guy which is alpha eta, but adjoining alpha eta is the same as just adjoining eta itself, because alpha is already there. So, I can multiply alpha eta by alpha inverse and, so, if I adjoin alpha and alpha eta, that also means that eta belongs to the the the adjunction. So, observe that Q alpha, alpha eta is actually the same as Q of alpha, adjoin eta.

And once I have eta, then well I do not need to adjoin any further roots. Because once I have alpha and eta, I have alpha eta square, alpha eta cubed, every one of those other roots already belongs to this, this extension Q alpha, eta. Therefore, I have understood what my splitting field looks like. It is obtained by adjoining alpha and eta.

So, now we need to understand how to find the degree of this extension? So, let us let us do it in two steps using our, what we know about degrees of towers of extensions. So, I will think of this as my tower of extensions. So, first step, what is the degree of the the bottom most step of the tower? So, what is the degree of this? Well, I am adjoining a single element alpha.

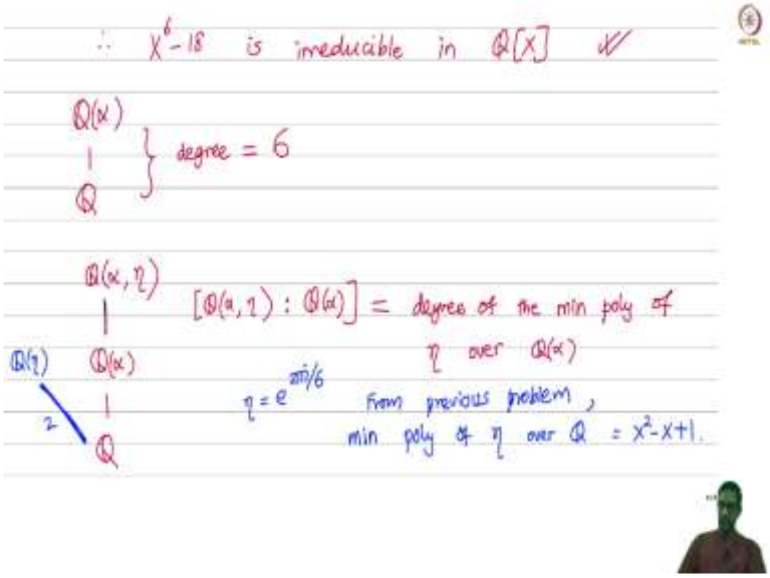
So, the degree of this extension as you have seen before is just nothing but the degree of the minimal polynomial, minimal polynomial of alpha over Q. So, what is the minimal polynomial that alpha satisfies? Well, observe alpha certainly satisfies the original polynomial, x to the 6 minus 18. So alpha is, this is certainly one possibility. So, claim, I claim this is the minimal polynomial of alpha over Q. Why is this?

Well, all I have to show is that this polynomial is irreducible. Because I already know that alpha is, I already know that alpha satisfies this polynomial is the root of this polynomial. So proof, just need to show this is irreducible. So, x to the 6 minus 18, I claim is irreducible by a simple application of well, the Eisenstein's criterion. So, let us apply the Eisenstein's criterion as follows. So, observe all coefficients are zeroes, 0 x square 0x minus 18.

And what does the Eisenstein's criterion tell us? It says, so let us recall Eisenstein criterion, it says if you can find a prime p, now in this case, I am going to take the prime p to be 2, which has the following property that this prime does not divide the leading coefficient, so this leading coefficient in this case is 1. So, this prime does not divide the leading coefficient, so leading coefficient. So that is all right, in this case, that is true.

And what is the next condition? The prime should divide all the other coefficients, all other coefficients should be divisible by p, that is also true because they are all zeroes. And the last guy is 18, which is also divisible by 2. Finally, the constant term should not be divisible by p squared. You know, the constant term is 18. And 18 is not divisible by the square of 2, which is 4. So, all the three conditions are satisfied of Eisenstein's criterion. So, what this implies in particular is that, this polynomial is irreducible.

(Refer Slide Time: 25:02)



$\therefore \ x^6 - 18$ is irreducible in $\mathbb{Q}[x]$ ✓

$$\begin{tikzcd}[row sep=small] \mathbb{Q}(\alpha) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd} \Bigg\} \text{degree} = 6$$

$$\begin{tikzcd}[row sep=small] & \mathbb{Q}(\alpha, \eta) \arrow[d, dash] \\ \mathbb{Q}(\eta) \arrow[dr, dash, "2"'] & \mathbb{Q}(\alpha) \arrow[d, dash] \\ & \mathbb{Q} \end{tikzcd}$$

$[\mathbb{Q}(\alpha, \eta) : \mathbb{Q}(\alpha)]$ = degree of the min poly of η over $\mathbb{Q}(\alpha)$

$\eta = e^{2\pi i/6}$

From previous problem, min poly of η over $\mathbb{Q}$ $= x^2 - x + 1$.

So therefore, x to the 6 minus 18 is irreducible in Qx. And we are done. So therefore, it must be the minimal polynomial of the element alpha. So, so done. So, what does that mean? At least the first step is done Q alpha over Q, this extension has degree equal to the degree of the minimal polynomial of alpha over Q and that degree is just 6. So, this is a degree 6 extension.

Now, let us go back. What, what did we need? We also need to adjoin a second element, which is eta. So, let us try adjoining eta to this, to this previous extension. So now I want to say I already have Q alpha. And to that I add an additional element eta, I adjoin an additional element. So, the question is, what is the degree of this extension?

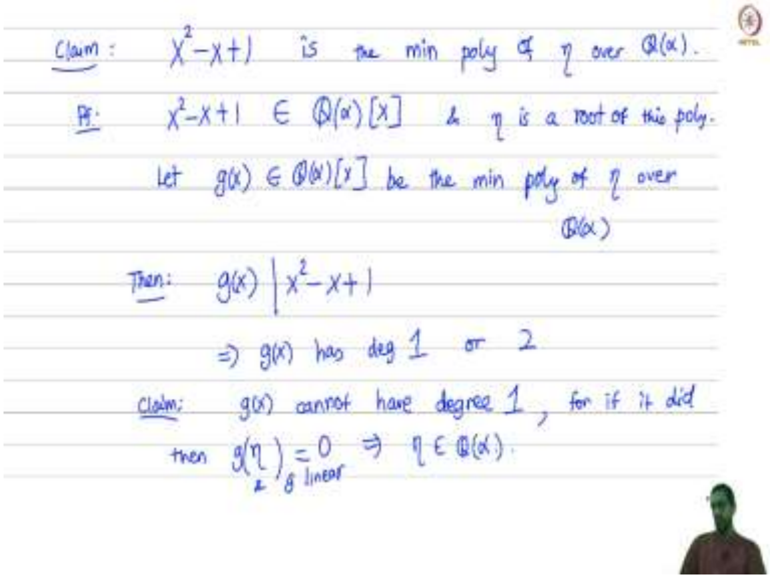
Well, again, by the same same reasoning, the degree of this extension, so Q alpha, adjoined one more element over Q eta is just the degree of the minimal polynomial, the degree of the minimal polynomial of this new element eta. But the degree I mean, the minimal polynomial is now to be computed over sorry, what what did I, sorry, this should be an alpha. So, this, this minimal polynomial of eta is over the field Q alpha.

So, observe, it is not over Q, but rather over a bigger field. So, I had to be a little careful, see whether I am computing the minimal polynomial over the correct field. So how does one find the minimal polynomial? Well, one tries to find at least one candidate polynomial. So, what is the candidate polynomial here? So, observe what was eta? Eta was just e to the 2pi i by 6.

And recall that from the previous problem, we already know, what the minimal polynomial of eta over Q is, we know this, that the minimal polynomial of eta over Q, meaning with coefficients in Q was just a polynomial x square minus x plus 1. So, look back on the previous problem, we showed that this is exactly the minimal polynomial of eta over the field Q. Well, what does that mean?

That does not automatically mean that this is the minimal polynomial of eta over this, this bigger field Q alpha. So at least it means the following that if I if I just adjoined, eta to Q, that would give me a degree to extension. So, let us let us think of it like this, I have Q to eta, if I just adjoined it, I would get something of degree 2. That is all this shows, in some sense.

(Refer Slide Time: 28:18)



Claim : x^2-x+1 is the min poly of η over $\mathbb{Q}(\alpha)$.

Pf: $x^2-x+1 \in \mathbb{Q}(\alpha)[x]$ & η is a root of this poly.

Let $g(x) \in \mathbb{Q}(\alpha)[x]$ be the min poly of η over $\mathbb{Q}(\alpha)$

Then: $g(x) \mid x^2-x+1$

$\Rightarrow g(x)$ has deg 1 or 2

Claim: $g(x)$ cannot have degree 1, for if it did

then $\underset{\& \ g \text{ linear}}{g(\eta) = 0} \Rightarrow \eta \in \mathbb{Q}(\alpha)$.

But I claim that well, this this very same polynomial is also the minimal polynomial of eta over Q alpha. Let us make that claim the same polynomial x square minus x plus 1 is also the minimum polynomial of this element eta over the base field, Q of alpha. Well proof, at least this polynomial is satisfied by the, I mean, this polynomial certainly has coefficients in Q eta.

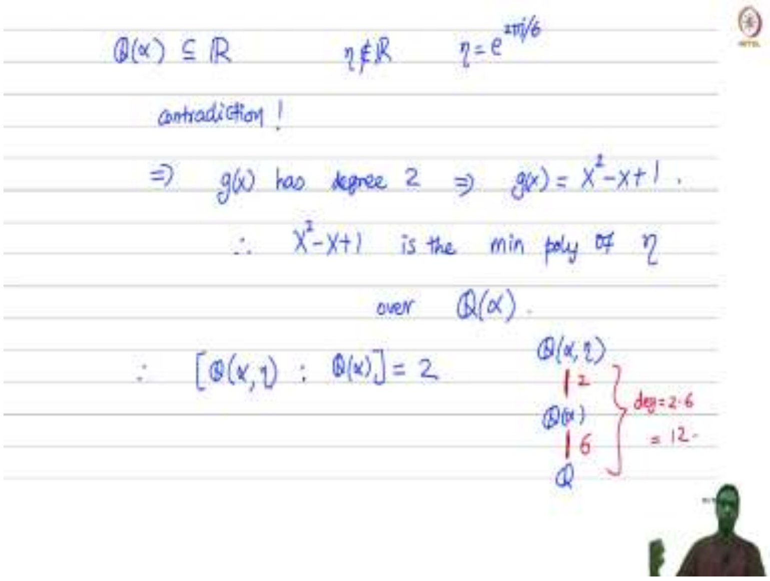
So observed this polynomial certainly Q alpha of x, its coefficients come from Q alpha. Why? Because in particular, the coefficients are in Q, so they are surely in Q alpha. Now, what does this mean? So, suppose let g of x denote the minimal polynomial. So, let gx be the minimal polynomial of eta over Q alpha, then g must divide this polynomial at least, and alpha sorry eta is the root of this polynomial that much I know.

So, the minimum polynomial has to divide every other polynomial of which alpha is the root. Well, what does that mean? There are not too many possibilities. This means that either gx has degree 1 or gx has degree 2. So, this means that either gx is linear has degree 1 or 2, there are only these two possibilities. So that, well, if gx has degree 2, then it means it is just the same as this polynomial x square minus x plus 1.

So that is more or less all, we have to show that gx cannot be of degree 1. So observed claim gx is not linear cannot have degree 1, for if it did, then what would it mean? You know, it is a, it is a linear polynomial and observe eta as a root of that polynomial. What it would mean is that g of, g of eta is 0, would just mean and and the fact that it is linear, and g is linear, just means that eta would actually have to be in the field Q alpha itself.

So, this is also because g is linear, so g eta is 0 and g is linear polynomial. The any root of a linear polynomial is in the base field itself. So, this would mean that eta must have belonged to the base field Q of alpha. But this is not possible. Why?

(Refer Slide Time: 31:23)



$\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ $\eta \notin \mathbb{R}$ $\eta = e^{2\pi i/6}$

contradiction!

$\Rightarrow$ $g(x)$ has degree 2 $\Rightarrow$ $g(x) = x^2 - x + 1$.

$\therefore$ $x^2 - x + 1$ is the min poly of η over $\mathbb{Q}(\alpha)$.

$\therefore$ $[\mathbb{Q}(\alpha, \eta) : \mathbb{Q}(\alpha)] = 2$

$$\begin{tikzcd}\mathbb{Q}(\alpha,\eta) \arrow[d, dash, "2"] \\ \mathbb{Q}(\alpha) \arrow[d, dash, "6"] \\ \mathbb{Q}\end{tikzcd}$$

$\deg = 2 \cdot 6 = 12.$

Well, because Q of alpha is a subset of the reals, observe that alpha is the real root. It was the 6th root of 18, the real number, so this is a real number, but eta is definitely not real. Eta is e to the 2pi i by 6. So, if you wrote it out, it will have an imaginary part, cosine of 60 degrees plus i sin 60 degrees, for example.

So that is a contradiction. So, this, this is a contradiction. So, what does that mean? It just says that gx cannot have degree 2, which implies gx has, sorry gx cannot have degree 1, so gx has degree 2, which implies that it is just the same as the original polynomial itself. Well, what does that tell you? Well, that tells you that this is exactly the minimal polynomial.

So, therefore done, x square minus x plus 1 is in fact, the minimum polynomial of eta, even over a larger field, Q of alpha. Say, a priori, the minimal polynomial over a larger field only divides the minimal polynomial over a smaller field. But in this case, because somehow the degree is very small, it turns out that these two are the same. So, what that means finally, is that the degree of this extension Q of eta, sorry, alpha, gamma eta Q of alpha is 2.

And so, we will put these two things together, Q of alpha eta, Q alpha Q. So, we already showed that this extension had degrees 6, we showed that this extension had degree 2 and the tower therefore has total degree 2 into 6 which is 12 by using this theorem on degrees of a tower of extensions.