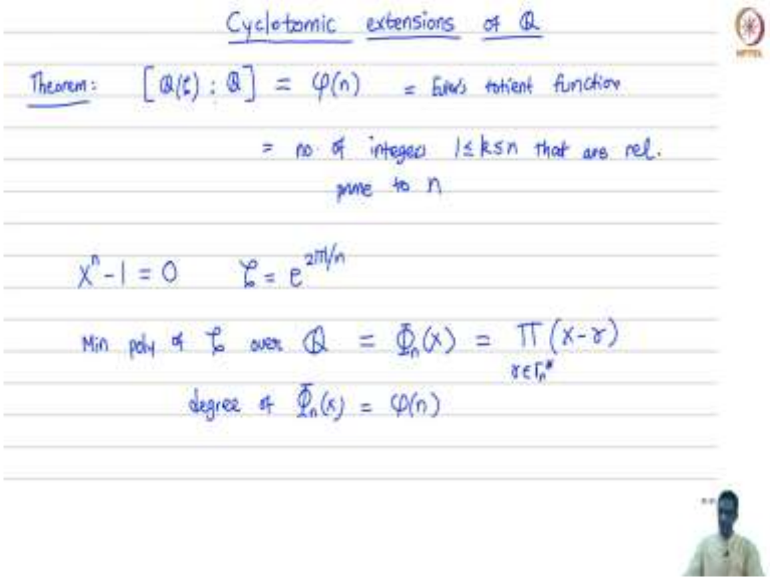
Algebra - II
Professor S Viswanath
Department of Mathematics
The Institute of Mathematical Science
Lecture 41
Application: Constructability of regular n – gons

(Refer Slide Time: 00:14)



Cyclotomic extensions of $\mathbb{Q}$

Theorem: $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ = Euler's totient function

= no. of integers $1 \leq k \leq n$ that are rel. prime to n

$x^n - 1 = 0 \quad \zeta = e^{2\pi i/n}$

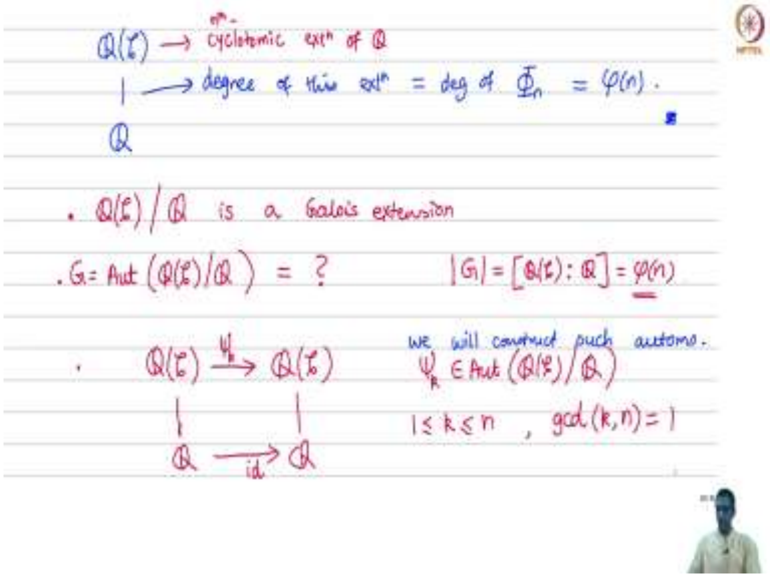
Min poly of ζ over $\mathbb{Q}$ = $\Phi_n(x) = \prod_{\gamma \in \Gamma_n^*} (x-\gamma)$

degree of $\Phi_n(x) = \varphi(n)$

Let us complete the proof of the theorem that we stated which is that if you take the cyclotomic extension, Q of zeta of Q, so recall what is zeta here? So I am looking at the polynomial x to the n minus 1 and looking at its roots and zeta here denotes the primitive nth root of unity e to the 2 pi i over n and what we have shown from, say the last 2 parts is the following, that the minimal irreducible polynomial, so the minimal polynomial of zeta over Q, the irreducible polynomial that zeta satisfies, is just the nth cyclotomic polynomial.

So recall that we had the nth of cyclotomic polynomial, which we said is just the product over all gamma primitive nth roots of unity x minus gamma and this has degree, degree of this polynomial, so degree of phi n, phi n of x is just the number of integers between 1 and n, which are relatively prime to n.

(Refer Slide Time: 01:45)



$\mathbb{Q}(\zeta) \rightarrow$ n^{th} cyclotomic ext^n of $\mathbb{Q}$

$|$ $\rightarrow$ degree of this ext^n = deg of Φ_n = $\varphi(n)$.

$\mathbb{Q}$

. $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension

. $G = \mathrm{Aut}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right) = ?$ $\quad |G| = [\mathbb{Q}(\zeta):\mathbb{Q}] = \underline{\varphi(n)}$

$$\begin{tikzcd}
\mathbb{Q}(\zeta) \arrow[r, "\psi_k"] \arrow[d, dash] & \mathbb{Q}(\zeta) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "id"'] & \mathbb{Q}
\end{tikzcd}$$

we will construct such automo.

$\psi_k \in \mathrm{Aut}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$

$1 \leq k \leq n$, $\gcd(k,n) = 1$

So that is what we call Euler's totient function and so now that proves this theorem because Q zai, sorry Q zeta over Q the degree of the extension recall. So I have Q and I adjoin a single element zeta to it, then the degree of this extension is just the degree of the minimal polynomial. So it is just the degree of phi n, which is fine.

So that completes the proof of the theorem. So recall now that, as we said in the beginning, that there is actually a Galois extension. So this field here is what we call the nth cyclotomic extension. So this is called a cyclotomic field or a cyclotomic extension of Q and maybe we will also say nth cyclotomic, to keep track of the fact that nth roots of unity that you are adjoining and we have already said that this is a Galois extension recall, Q zeta over Q is a Galois extension.

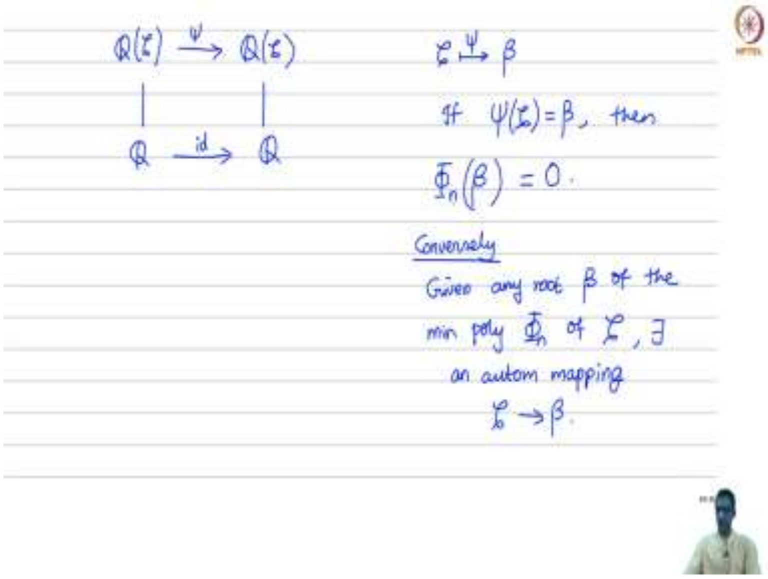
It was normal because it is just the splitting field of the polynomial x to the n minus 1. It is separable because Q has characteristic 0. So now given the fact that it is Galois, we want to understand its Galois group. In other words, what is the group of automorphisms of Q zeta over Q? So, what is this? What is the Galois group?

So, we need to, well we know something about it definitely, we know from say, the fundamental theorem of Galois theory and so on, we know that the cardinality of the Galois group is just the degree of the extension. So this is just the degree of extension, which is phi of n. So that is the Euler's totient function of n.

So, what we will do next is to sort of construct explicitly these many elements phi n number of elements in the Galois group. So what is the Galois group mean? Recall, we are looking therefore, to construct auto morphisms of the field Q of zeta. So I am going to try and construct some maps which are called psi sub k, such that when I restrict it to Q, it gives me identity? It is the identity map on Q and what should psi k satisfy? Psi k should be an auto morphism, should be a field auto morphism of Q zeta.

So any field auto morphism is automatically identity on Q because it maps 1 to 1, therefore it automatically maps 2 to 2, 3 to 3 and so on. Then one can also show it maps p by Q to p by Q. So I am going to construct such auto morphisms one for each element. So what is k here? k is going to run from 1 to n and the g c d from k and n is 1. So for each such k, I am going to construct, so that is what I am going to do. We will construct such auto morphisms. So, how does one do this?

(Refer Slide Time: 05:17)



$$\begin{tikzcd} \mathbb{Q}(\zeta) \arrow[r, "\psi"] \arrow[d, dash] & \mathbb{Q}(\zeta) \arrow[d, dash] \\ \mathbb{Q} \arrow[r, "id"] & \mathbb{Q} \end{tikzcd}$$

$\zeta \xrightarrow{\psi} \beta$

If $\psi(\zeta) = \beta$, then

$\Phi_n(\beta) = 0$.

Conversely

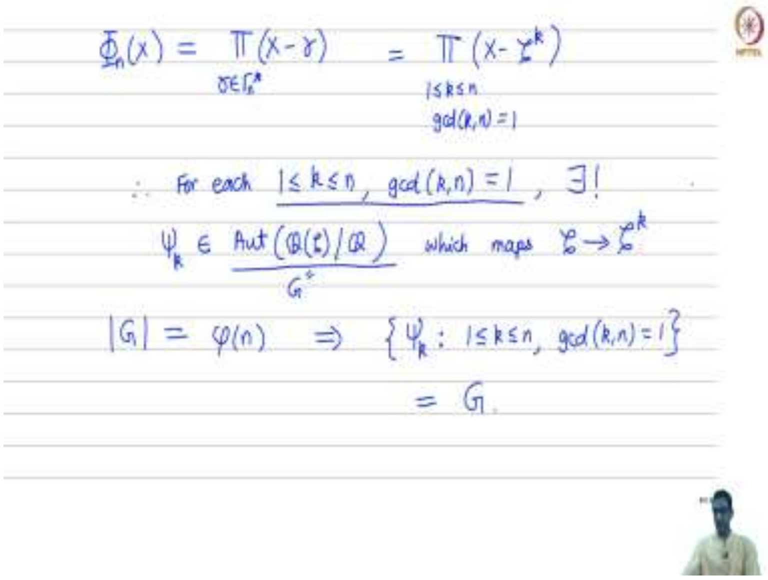
Given any root β of the min poly Φ_n of ζ, $\exists$ an autom mapping $\zeta \to \beta$.

Well, we already have the various ingredients required to construct such a map. So, recall from what we have done before, that when I have this extension Q zeta, how do we construct auto morphism? Well, what I can do is I can map zeta. So, an auto morphism recall is uniquely identified once I know the following.

So, I know its identity on Q in order to define an auto morphism what can I do? I have to say what zeta maps to. I must try and find a suitable candidate to map zeta. Now, recall from what we have said before that whatever zeta maps to has to be so, if I, if it is some beta then so, under this auto morphism psi then beta, so if psi maps zeta to beta then beta must also satisfy the same polynomial that zeta satisfies.

Then we must have that, this is 0 and also recall conversely given any such beta which satisfies the same minimal polynomial as zeta, you can always define such auto morphism. So, these are these are all facts that we have proved before conversely given any beta any beta, any root beta of the minimal polynomial, which in this case is phi sub n of zeta there exists such an auto morphism which maps, mapping should say that exists auto morphism mapping zeta to beat.

(Refer Slide Time: 07:28)



$$\Phi_n(x) = \prod_{\gamma \in \Gamma_n^*} (x-\gamma) = \prod_{\substack{1\le k\le n \\ gcd(k,n)=1}} (x-\zeta^k)$$

$\therefore$ For each $\underline{1\le k\le n,\ gcd(k,n)=1}$, $\exists!$

$\psi_k \in \underbrace{Aut(\mathbb{Q}(\zeta)/\mathbb{Q})}_{G}$ which maps $\zeta \to \zeta^k$

$|G| = \varphi(n) \Rightarrow \{\psi_k : 1\le k\le n,\ gcd(k,n)=1\}$

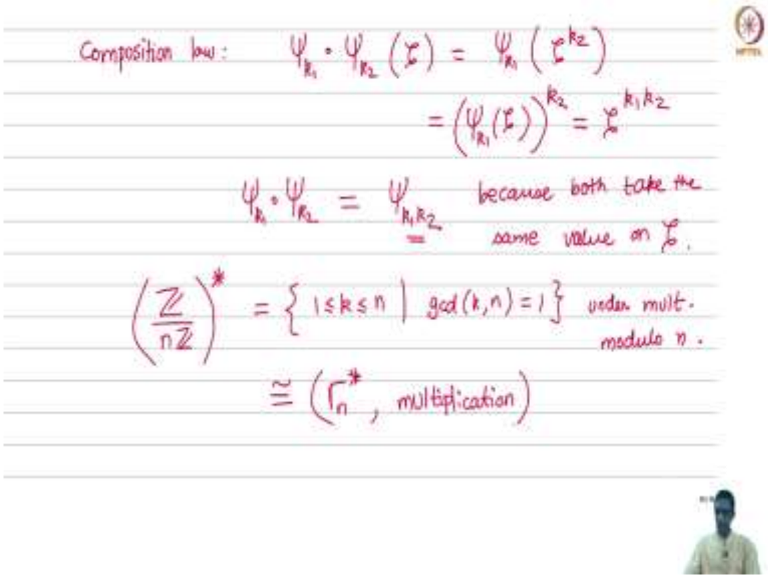
$= G.$

Now, what does this tell us? So, you know I just need to look for the other roots of the minimal polynomial phi sub n and what are the other roots? We already know what they are. So, phi sub n the cyclotomic polynomial is just the product of all the primitive nth roots of unity. So, what are the various choices? So, what do these look like? They are just x minus if you wish zeta power k, the various powers of k which are relatively prime to n.

Those are the elements of gamma n star. So, therefore for each such k I have therefore constructed an auto morphism. So, for each by this general principle for each k between 1 and n g c d, k with n is 1, there exists a unique in fact, because once you specify what zeta goes to the auto morphism is uniquely defined there exists a unique auto morphism psi k, just said there exists a unique psi in the Galois group which maps, well it has map Q to Q by identity that sort of forced which maps zeta to zeta power k

So, this is the description of psi k. Now, the point is how many psi k’s have we constructed? Well, we have constructed exactly phi of n the Euler’s totient function of n number of psi k’s. So because we know that the Galois group or the, this auto morphism group that is a Galois group is really g. Since we know that this has the correct cardinality implies that this collection of psi k’s is that we have constructed, this must be the entire group g, this must be the Galois group.

(Refer Slide Time: 09:44)



Composition law: $\psi_{k_1} \circ \psi_{k_2}(\zeta) = \psi_{k_1}(\zeta^{k_2})$

$$= \left(\psi_{k_1}(\zeta)\right)^{k_2} = \zeta^{k_1 k_2}$$

$\psi_{k_1} \circ \psi_{k_2} = \psi_{\underline{k_1 k_2}}$ because both take the same value on ζ.

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* = \{1 \leq k \leq n \mid \gcd(k,n) = 1\}$$ under mult. modulo n.

$$\cong \left(\Gamma_n^*, \text{multiplication}\right)$$

Now, these auto morphisms which map zeta to zeta power k. So what are these? They are actually you know, they are they are familiar; we sort of know what they are. Well, to understand what these auto morphisms do, let us understand the group structure. So what is the composition law here? What happens when you compose to such auto morphisms? Well, if I compose psi k 1, psi k 2 where k 1 and k 2 are both relatively prime to n.

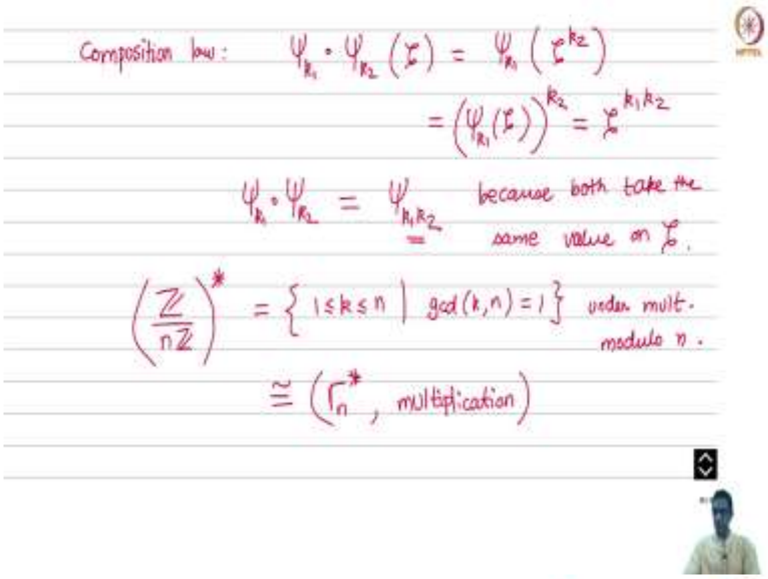
What does this give me? Well, let us see what it does to zeta. So this maps, so this is psi k 1 zeta power k 2. Now psi k 1 is a homomorphism; so field homomorphism. So this is just if I know what it does to zeta, then I just raised that to the power k 2. So, this is just zai to the k 1, k 2. So, what is this?

Well, therefore, it means that the composition psi k 1, psi k 2 must be the same as psi of the product k 1, k 2 because they match on because they have, they take the same value on zeta because both take the same value on zeta k and of course on Q there, they are both necessarily the identity. So what is this? Well, this looks exactly like the usual multiplication rule. So, of course, here I only have to look at the values of k, which are relatively prime to n.

So, what exactly is this? Well, this is just the group. So let us take the group Z mod, the cyclic group, if you wish Z mod n Z star, what does this mean? This is just integers modulo n, but I am just going to take the units is in this ring. So this is maybe, let us just say it is all numbers. Well, one way of saying it is it is all numbers from 1 to n, which are relatively prime to n and this is thought of as a group under multiplication modulo n.

Another way of saying it is that this is just the group; well, this is isomorphic if you wish to the group gamma n star of primitive nth roots of unity under multiplication. So you should think of this primitive nth roots of unity as a group under multiplication.

(Refer Slide Time: 12:19)



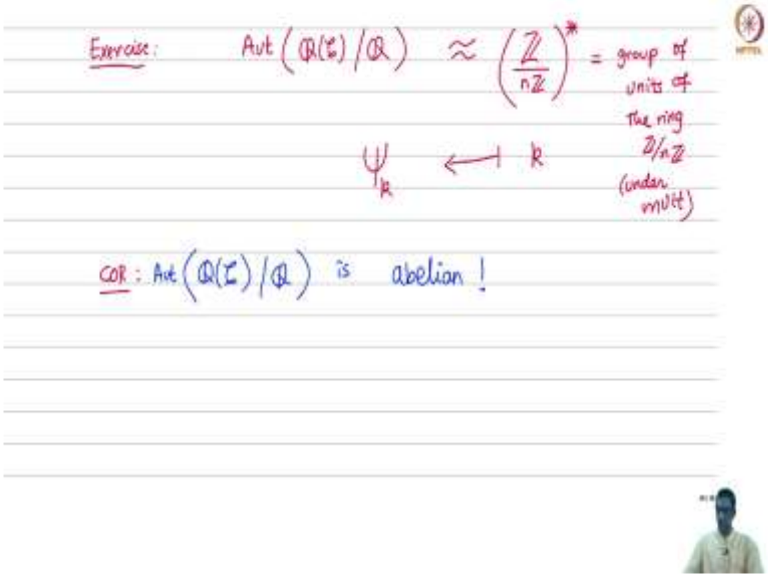
Composition law: $\psi_{k_1}\circ\psi_{k_2}(\zeta) = \psi_{k_1}(\zeta^{k_2})$

$= (\psi_{k_1}(\zeta))^{k_2} = \zeta^{k_1 k_2}$

$\psi_{k_1}\circ\psi_{k_2} = \psi_{\underline{k_1 k_2}}$ because both take the same value on ζ.

$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* = \{1 \le k \le n \mid gcd(k,n)=1\}$ under mult. modulo n.

$\cong (\Gamma_n^*, \text{multiplication})$



Exercise: $Aut(\mathbb{Q}(\zeta)/\mathbb{Q}) \approx \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ = group of units of the ring $\mathbb{Z}/n\mathbb{Z}$ (under mult)

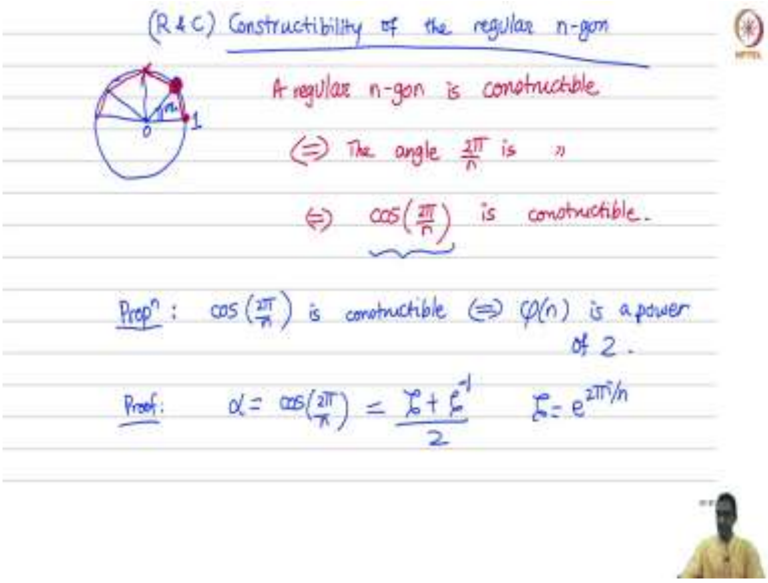
$\psi_k \longleftarrow k$

COR: $Aut(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian!

So they are all some complex numbers and if you multiply 2 primitive nth roots of unity, what you get again is a primitive nth root of unity. So, this is this is the group structure. So, now, it is an easy exercise from all that we have said. So, observe that the Galois group, the group of auto morphisms is nothing but this group Z mod n Z star. So, the group of units of this ring if you wish, this is just nothing but the group of units if you wish to think in terms of the ring of, the ring Z mod n Z.

The group of units means the invertible elements and they are a group under multiplication. So this is under multiplication and what is the isomorphism given any k here, we just map it to the corresponding sides of k and we have more or less shown the calculation we just did on the composition rule, just says that the multiplication on the Z mod n Z level translates into the composition of maps like, so we exactly understand the cyclotomic extension and its Galois group.

(Refer Slide Time: 13:57)



(R & C) Constructibility of the regular n-gon

A regular n-gon is constructible

$\Leftrightarrow$ The angle $\frac{2\pi}{n}$ is "

$\Leftrightarrow$ $\underbrace{\cos\left(\frac{2\pi}{n}\right)}$ is constructible.

Propn : $\cos\left(\frac{2\pi}{n}\right)$ is constructible $\Leftrightarrow$ $\varphi(n)$ is a power of 2.

Proof: $\alpha = \cos\left(\frac{2\pi}{n}\right) = \frac{\zeta + \zeta^{-1}}{2}$ $\zeta = e^{2\pi i/n}$

The corollary is that the Galois group is abelian. So, observe the Galois group of the cyclotomic extension is actually an abelian group, just the group of units of this ring, this commutative ring. Now what does this have to do with a problem that we considered earlier? So this is ruler and compass construction.

So let me say R and C, ruler and compass constructability of the regular n-gon. So the problem is as follows. We know the regular polygons. Now, can you construct using ruler and compass the regular polygon with n sides? So, what is a regular n-gon? Well, it is vertices you can think of as being, they form equal angles 2 pi by n, 4 pi by n and so on.

So this angle here is 2 pi by n and so this is if you think of this as the unit circle in the complex plane. These vertices are exactly the roots of Unity but we will think of it on just the usual plane or 2. So observe that to construct the regular n-gon, well remember this point is assumed to be given, when you do ruler and compass constructions you assume 0 and 1 are given.

Now, if you can construct this point here, then of course you can construct the regular n-gon because you can draw the unit circle and if you can construct this first point, then I can construct all the other points as follows: I just keep my compass here, I measured this distance and now I put the centre of my compass at the next point and then I cut out the same distance here.

So, that will give me the next vertex. Again I measure the same distance and so on. So once you know what the correct distance is of a side of a regular n-gon, you can just measure that everywhere and construct the full regular n-gon. So the first observation is that a regular n-gon is constructible, regular n-gon is constructible if and only if this angle 2 pi by n, the angle 2 pi by n is constructible.

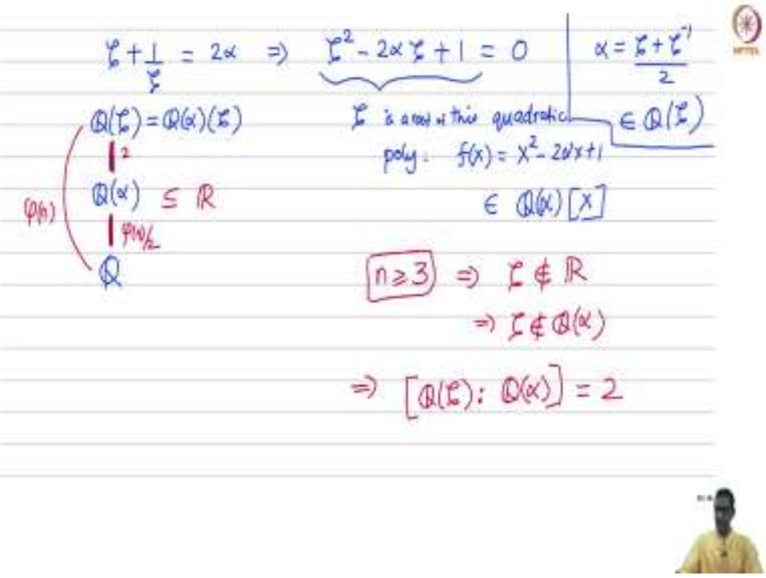
You can construct that angle somehow using ruler and compass and recall again, we have looked at this before; constructing an angle is the same as sort of constructing this point here on the unit circle and that point has coordinates cos and sine of 2 pi by n. So this is the same as saying cos of 2 pi by n is a constructible real number.

So, we have seen this before already. Now, I mean if cos can be constructed then sine can also be construct. Because once you know cos, you sort of draw a right triangle and so on. Now, the point is you know, let us prove the following theorem. So remember, what is this cosine here?

So what does this got to do with the whole analysis of cyclotomic extensions that we have been doing? So observe the following. So maybe I will just write the theorem down first. Proposition: that cosine of 2 pi by n is constructible or in other words, the regular n-gon is constructible if and only if phi of n, the Euler’s totient function is a power of 2.

So let us prove this this proposition. Proof: so first, let us call this number something alpha, which is cosine of 2 pi by n. This is just zeta plus zeta inverse by 2. What is zeta? Zeta is our complex nth root of unity and if you just compute this plus, minus of this I mean e to the minus 2 pi n by 2 that is one of the definitions of cosine.

(Refer Slide Time: 18:09)



$$\zeta + \frac{1}{\zeta} = 2\alpha \Rightarrow \underbrace{\zeta^2 - 2\alpha\zeta + 1 = 0}$$

ζ is a root of this quadratic poly: $f(x) = x^2 - 2\alpha x + 1$

$\in \mathbb{Q}(\alpha)[x]$

$\alpha = \frac{\zeta + \zeta^{-1}}{2} \in \mathbb{Q}(\zeta)$

$\mathbb{Q}(\zeta) = \mathbb{Q}(\alpha)(\zeta)$

2

$\mathbb{Q}(\alpha) \subseteq \mathbb{R}$

$\varphi(n)/2$

$\mathbb{Q}$

$\varphi(n)$

$\boxed{n \geq 3} \Rightarrow \zeta \notin \mathbb{R}$

$\Rightarrow \zeta \notin \mathbb{Q}(\alpha)$

$\Rightarrow [\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2$

So alpha is just zeta plus zeta inverse by 2. So what that means is that so if we just simplify, that is just zeta plus 1 by zeta is 2 alpha. In other words, zeta square minus 2 alpha zeta plus one is 0. In other words, if you think of Q and if you look at the cyclotomic extension Q zeta and you look at Q of alpha here, so observe alpha is zeta plus zeta inverse by 2 means, of course that alpha belongs to Q zeta.

This is certainly an element which is in the field Q zeta. Because if zeta is there zeta inverse is there; so it is sort of an intermediate field Q alpha is between Q and Q zeta and this equation here says that zeta square, so zetas, sorry zeta satisfies this quadratic equation, this quadratic polynomial. So, what quadratic polynomial?

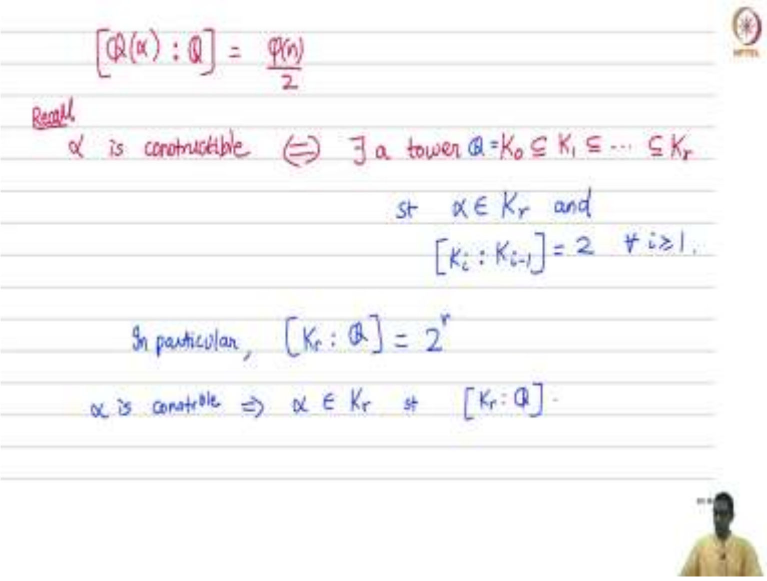
Let us call it F of x is x squared minus 2 alpha x plus 1. It is the root of this quadratic polynomial, zeta is a root of this quadratic polynomial and this quadratic polynomial has coefficients in Q alpha. So, what that means is that zeta Q zeta, if you think of it as an extension of Q alpha, so this extension here, it has degree utmost 2 because zeta is just I mean, I can think of this as first you adjoin alpha and then you adjoin zeta to it.

So, this additional adjunction of zeta, the zeta satisfies only a quadratic polynomial. So, this can be at most degree 2 but it is in fact exactly degree 2. Why is it 2? Observe that Q of alpha is actually a subset of the real numbers. Alpha is after all a real number. So Q alphas is purely real, whereas zeta is not real.

So if n is at least 3, so let me assume here that n is at least 3 because I am trying to construct a polygon, so n must be at least 3 for it to be a polygon. So since n is at least 3, then this element zeta is definitely not a real number. So that implies that zeta cannot live inside, which implies z cannot be an element of Q alpha.

So, what we have just said implies that Q zeta, this field over this field Q alpha has to have degree exactly 2. So, what we know now is that this is a degree 2 extension and this is the cyclotomic field over Q and that we know is a degree phi n extension. Now, let us look at what that implies. Well, that says in particular that Q alpha over Q is of degree phi n by 2.

(Refer Slide Time: 21:17)



$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{\varphi(n)}{2}$

Recall

α is constructible $\Leftrightarrow$ $\exists$ a tower $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$

st $\alpha \in K_r$ and

$[K_i : K_{i-1}] = 2 \quad \forall i \geq 1.$

In particular, $[K_r : \mathbb{Q}] = 2^r$

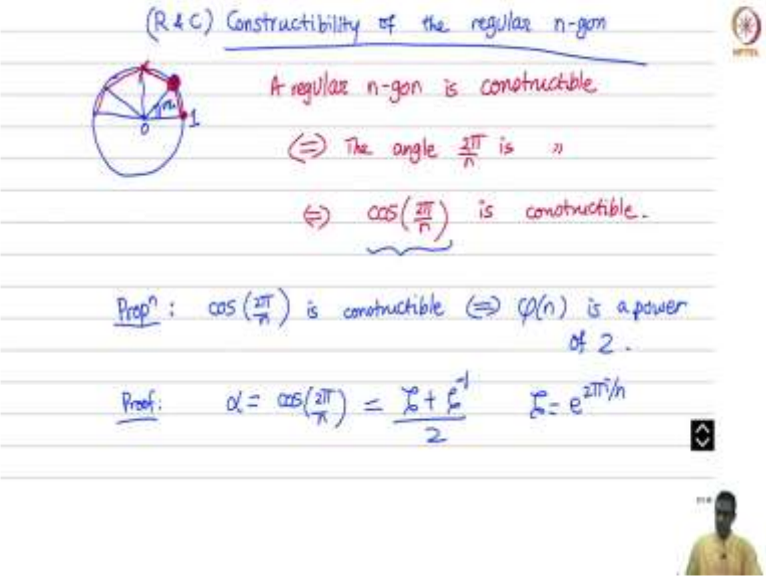
α is constrctble $\Rightarrow$ $\alpha \in K_r$ st $[K_r : \mathbb{Q}]$.

So, that is the conclusion we wanted. So, if I look at the extension Q alpha over Q its degree is phi n by 2. Now recall, constructability of a real number, when is it possible to construct a real number? So, we have seen all this; recall alpha is constructible so alpha is a real number is constructible if and only if it belongs to a tower of extension, so there exist a tower of extensions.

So, let me call this K 0 contained in K 1 contained in some K r is a tower such that well, this bottom tower is just Q, Q is this and this top tower, this is a tower such that alpha belongs to the last element of the tower and each extension is of degree 2. K i K i minus 1 is a quadratic extension for all i greater than or equal to 1. So you can get it inside a tower of successive quadratic extensions. So this was the theorem on constructability.

So in particular, this means so what does it mean? In particular, this means that K r, K 0, which is Q it is just a product of the degrees of the intermediate extensions. So this is just 2 power r in this case. So it is a power of 2. So, what does that mean? Therefore, alpha is constructible implies, alpha is constructible implies that the degree of this extension in particular, it means that alpha belongs to some K r, so it belongs to some K r, which is an extension of Q such that K r Q is some power of 2.

(Refer Slide Time: 23:24)


(R & C) Constructibility of the regular n-gon

A regular n-gon is constructible

$\Leftrightarrow$ The angle $\frac{2\pi}{n}$ is "

$\Leftrightarrow$ $\underbrace{\cos\left(\frac{2\pi}{n}\right)}$ is constructible.

Prop^n: $\cos\left(\frac{2\pi}{n}\right)$ is constructible $\Leftrightarrow$ $\varphi(n)$ is a power of 2.

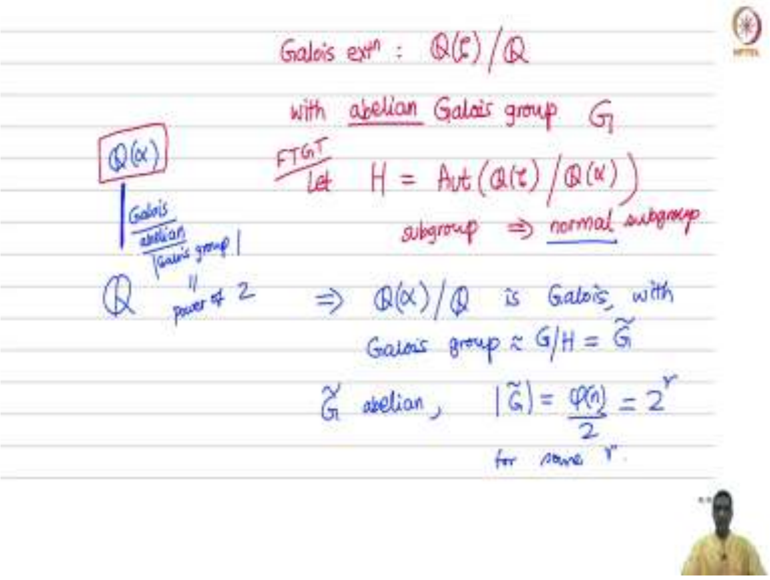
Proof: $\alpha = \cos\left(\frac{2\pi}{n}\right) = \frac{\zeta + \zeta^{-1}}{2}$ $\zeta = e^{2\pi i/n}$

So, here is the setting K r s here, Q is here, alpha belongs to K r. So, I can look at alpha as an element here. So, I can just look at Q alpha. I just adjoin alpha to Q and look at this whole thing, what I know is that this overall guy is some power of 2. This has degree which is a power of 2. So these intermediate extensions must have degree which divides this overall degree, which implies that Q alpha Q divides this degree to power r which implies it is also a power of 2.

So Q alpha Q is therefore a power of 2 and we have already said Q alpha Q is just phi by 2. So, this is a power of 2 means that phi n is a power of 2. That is exactly what we wanted to prove, phi n is a power of 2. So one direction is proved; so let us prove the converse. So let us go back. What did we want to prove?

Cosine is constructible if an only if phi n is a power of 2, so we have shown one way implication. Now let us do the converse, if phi n is a power of 2, so converse; so if phi n is a power of 2 then so is well, let us look at, so phi n by 2 is also power of 2 of course.

(Refer Slide Time: 25:06)



Galois ext^n : $\mathbb{Q}(\zeta)/\mathbb{Q}$

with abelian Galois group G

FTGT

Let $H = \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}(\alpha))$

subgroup $\Rightarrow$ normal subgroup

$\Rightarrow \mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, with

Galois group $\approx G/H = \tilde{G}$

$\tilde{G}$ abelian, $|\tilde{G}| = \frac{\varphi(n)}{2} = 2^r$

for some r.

Let us think in terms of fields. So I have these cyclotomic extension Q zeta over Q, the sum power of 2 and what I have in the middle is this extension Q alpha over Q. So they are all powers of 2, all the extensions involved, we have assumed their powers of 2. So this is some power of 2, so 2 to the something. Therefore, each of these must also divide it must also be the form 2 power something.

Now, what else did we know? We know that this is a Galois extension. So what is the Galois extension? Q zeta, Q zeta over Q is a Galois extension. But we actually know something more with abelian Galois group. We already proved this. It is just a group of units of the rings at mod n Z. So it is got an abelian Galois group G.

Now, let us use this this fundamental theorem of Galois Theory, what does it say? It says that intermediate subfields for example, this one are in one to one correspondence with some groups of G. So, in this case Q alpha is some intermediate subfield. So, that will correspond to some subgroup. So, let us call that H. Let H denote the subgroup corresponding to so, I am using the fundamental theorem of Galois Theory here.

So, let H denote the subgroup auto morphisms of zeta over Q alpha. That was the association the fundamental theorem. So, we know that this is a one to one correspondence. Now, what do we know here, we know the following: this is an abelian Galois group, G is abelian, H is a subgroup which automatically implies it is a normal subgroup because G is abelian and what does that give us?

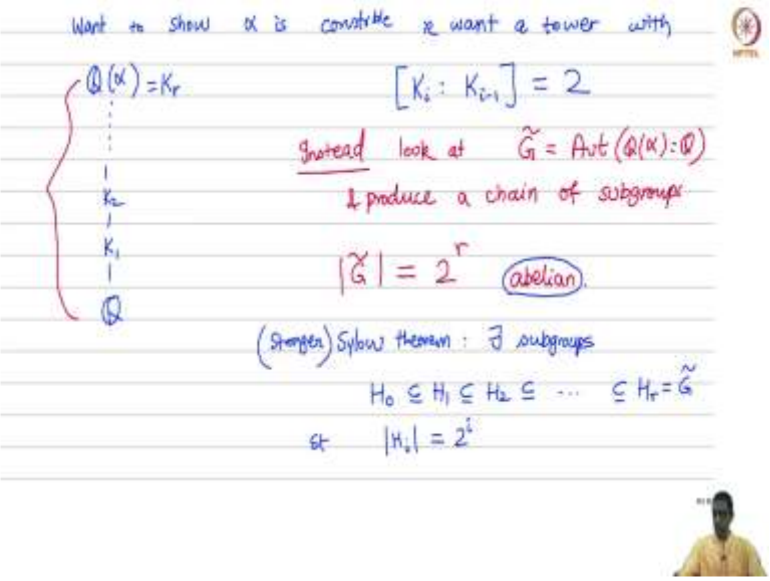
It tells us so, recall the second part of the fundamental theorem, it says if your subgroup is normal, then in fact the subfield that it corresponds to, which in this case Q alpha is Galois over the base field. So this therefore, implies I am using the sort of follow up to the fundamental theorem, which says that, if H is normal then the subfield that it corresponds to which in this case was Q alpha over Q is Galois and what is the Galois group?

Well, it is just G mod H, with Galois group, G isomorphic to G mod H. So maybe we will call this something G tilde; this is the Galois group of Q alpha over G. Good. So now we are in good shape, we can now forget about the cyclotomic extension. Now, we really only wanted to get something about Q alpha over Q. We have concluded it is a Galois extension. Its Galois group is an abelian group. So g tilde is also abelian.

So this is Galois, it is got an abelian Galois group and further the Galois group has cardinality which is a power of 2, cardinality of G tilde is phi n by 2, that is also some power of 2. So, these 2 power r for r. So, this is what we know and Galois group cardinality is a power of 2. Now, what is it that we need to prove? We need to show that alpha is constructible.

In other words, I can realise alpha can realize alpha inside an extension which is obtained from Q by a sequence of you know by a successive tower of quadratic extensions. So, I want to be able to find an intermediate tower like this.

(Refer Slide Time: 29:24)



Want to show α is constrble ⇒ want a tower with

$\mathbb{Q}(\alpha) = K_r$

$[K_i : K_{i-1}] = 2$

K_2

K_1

$\mathbb{Q}$

Instead look at $\tilde{G} = \mathrm{Aut}(\mathbb{Q}(\alpha) : \mathbb{Q})$

& produce a chain of subgroups

$|\tilde{G}| = 2^r$ abelian.

(Stronger) Sylow theorem : $\exists$ subgroups

$H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_r = \tilde{G}$

st $|H_i| = 2^i$

So recall this, what we want to show that alpha is constructible. What does that mean? I should be able to do the following between Q alpha and Q, I should be able to put up a bunch of subfields. So that this a last fellow, this let us call K r, i.e one tower like this with each successive extension of degree 2.

Now, how are we going to construct a tower? Well, we use the fundamental theorem of Galois Theory again. I know that this is a Galois extension. I know a lot about its Galois group, Galois extension with Galois group which is abelian and whose cardinality is a power of 2. How do I get a tower of extensions?

Well, I look instead for a tower of subgroups and such that the successive quotients I mean the; or the cardinalities of the subgroups. The successive quotients of the cardinalities are just 2. So, we will instead look at the level of; instead let us look at the Galois group instead of subfields. Instead, consider the Galois group g tilde which is Q alpha over Q.

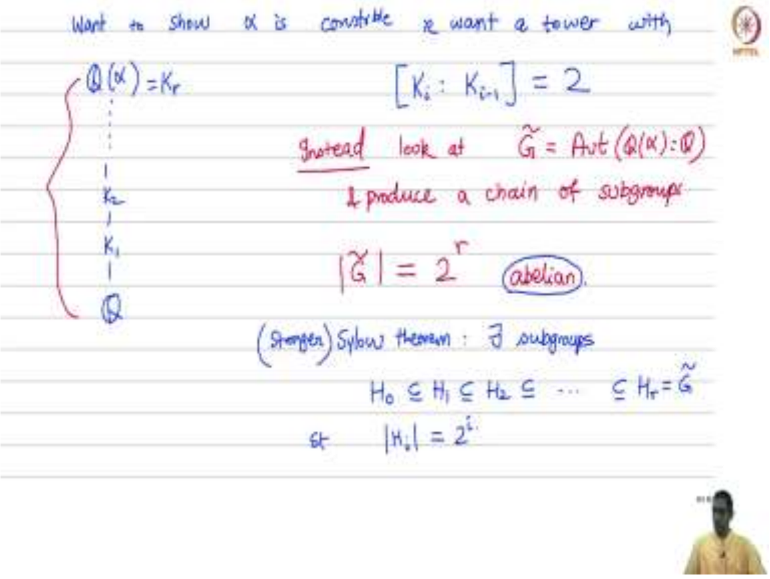
Now, what do we know about this and we will produce and produce a number of subgroups if you wish, or a chain of subgroups. Now, how are we going to do this? Well, recall that cardinality of G is some power of 2. Now, what does that imply? Well, it is also abelian, if you wish but if you have you know, group which is the P group, which is just 2 power r, if you wish, say you know by using sort of the stronger form of Sylow theorem, for example, so what does Sylow theorem tell you?

Well, there is a Sylow subgroup in this case; the group itself is 2 power r. So, the Sylow subgroup is just the whole group itself. But there is also a strengthened version of Sylow' theorem, which says that, you also have subgroups of every order of the form 2 power K, where K is any number from 0 to r.

So you could use that or if you wish, you could use the fact that this is abelian and then use the fundamental theorem of finite abelian groups. So, there is two different ways of concluding this. So, let me just say for example, the stronger form of Sylow theorem says that there exists subgroups.

In fact, there is a chain of sub groups so, there exists subgroups of the following form H not contained in H 1, contained in H 2 and so on. Such that the cardinality of so, this is the final group g tilde, the cardinality of each H i is just 2 power i. Now, once you have this, then you are done because from a tower of subfields or from a chain of subgroups, you just have to construct the corresponding tower of subfields by taking the fixed fields.

(Refer Slide Time: 33:12)



Want to show α is constrble $\Rightarrow$ want a tower with

$\mathbb{Q}(\alpha) = K_r$

K_2

K_1

$\mathbb{Q}$

$[K_i : K_{i-1}] = 2$

Instead look at $\tilde{G} = \mathrm{Aut}(\mathbb{Q}(\alpha) : \mathbb{Q})$

& produce a chain of subgroups

$|\tilde{G}| = 2^r$ abelian.

(Stronger) Sylow theorem : $\exists$ subgroups

$H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_r = \tilde{G}$

st $|H_i| = 2^i$

So now define, we will call them L sub i to be the field corresponding to H sub i. So, what is this? This is just so this is the top field here. So, maybe that is Q alpha. So, I just take this to be the fixed field of H sub i by which I mean, I have taken Q have alpha, the top field and then look at the elements which are fixed by H i.

Now, what would you get? You just get something which goes in the opposite direction. So, in other words the, I have g tilde here and I have identity at the other end. So this is H naught, contained in H 1 contained in a blah, blah, this is H r. Now, at the level of fields, it just goes in the other order.

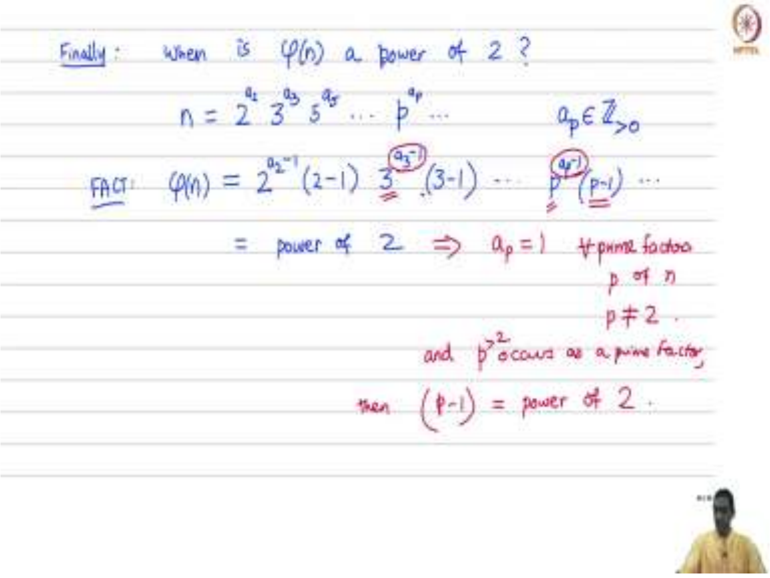
So L r, which is the fixed field of H r would be well that would just be Q, because that is the Galois group, H r is the whole Galois group and then L 0 would just be the whole because it is identity, it is the whole field and now these go in the other order, L 1 is a sub of L 0, sub 2 and so on.

So any case I just I mean, the numbering is sort of the opposite, if you wish, but the key point here is that, if you look at the degrees of these extensions, L I, L i plus 1 observe this again by the fundamental theorem of Galois theory, if you will is, so L i corresponds to which subgroup? L i corresponds to the subgroup H i.

So, I have an L i somewhere, L i plus 1 comes after it. So, L i corresponds to some H i L i plus 1 corresponds to H i plus 1. So, it goes in the opposite order, this is just the cardinality of H i plus 1 divided by cardinality of H i.

This is from the fundamental theorem again and now, the way we have chosen it, this is just 2. So, that completes the proof. So, that says that you can actually construct such a tower of successive quadratics, which finally alpha belongs to the topmost guy in the tower. So, this completes the proof, this implies that alpha is constructible.

(Refer Slide Time: 35:55)



Finally : when is $\varphi(n)$ a power of 2 ?

$$n = 2^{a_2} 3^{a_3} 5^{a_5} \cdots p^{a_p} \cdots \qquad a_p \in \mathbb{Z}_{>0}$$

FACT: $\varphi(n) = 2^{a_2 - 1}(2-1)\, \underline{\underline{3}}^{\boxed{a_3 - 1}}(3-1) \cdots \underline{\underline{p}}^{\boxed{a_p - 1}}\underline{\underline{(p-1)}} \cdots$

$= \text{power of } 2 \Rightarrow a_p = 1$ ∀ prime factors p of n $p \neq 2$.

and $p^{\geq 2}$ occurs as a prime factor, then $(p-1) = \text{power of } 2$.

Now, finally to complete this, this whole analysis, so sort of an aside or finally is it possible at all that when is phi n a power of 2? That is a question that one wants to understand. Now, can it even be a power of 2? Now well, what is phi n, there is a simple formula for phi n. So, if you write n as a product of primes, so n looks like say 2 power a 3 power, let us get these names, this is n, 2 power n sorry, it is called m 2 or maybe a 2.

2 power a 2, 3 power a 3, 5 power a 5 and so on. So, take all primes p power a p n is, n has some prime factorization. So, I just call the exponents as a p's are all non-negative integers. Now phi of n is, let me use this little fact about phi of n. It is I just have to take you know it is a product of all these phi of each of them and in each case, it is 2 to the a 2 minus 1 into 2 minus 1 then 3 to be a 3 minus 1, 3 minus 1 and so on.

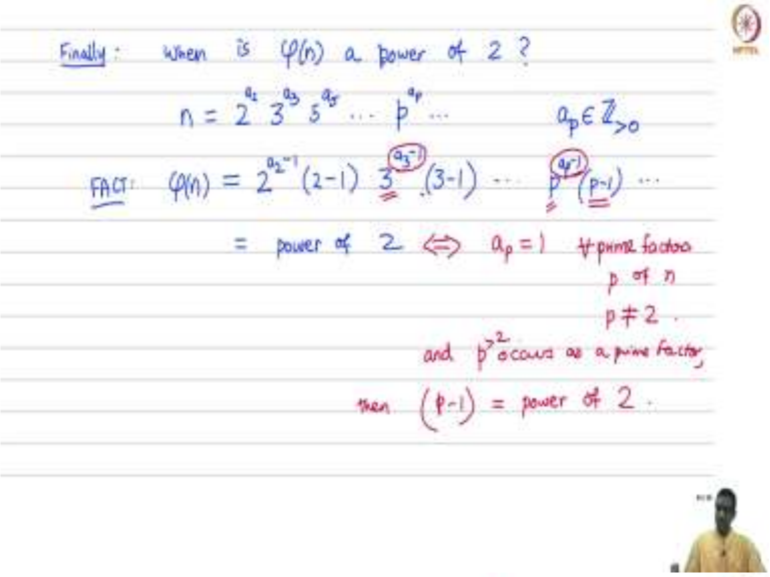
So, in general p to the a p minus 1 to p minus 1. So, this is only for the a p's which actually occur in in the decomposition. So I should not write this for all numbers. So, let me assume that I only write those prime factors which actually occur in the decomposition. If it is 0 then I do not want to write that.

So, this is the product only corresponding to the terms which occur. Now, the point is; when can this possibly be a power of 2? So I want this to just be a power of 2. So that is a very restrictive condition because you see, this number here is clearly not a power of 2 this is not a power of 2. So unless somehow this power here becomes 1.

So if these powers become 0, so if this is a power of 2, then when is that possible? Well, this implies that all these higher power, so a p has to be 1 for all primes p which occur which are not 2 for all prime for p not equal to 2, for all prime factors p of n, for all we write it like this, for all prime factors p of n other than 2

Only then these powers will all vanish and further, what more do you want? And you need something more that if a prime p occurs, if p occurs as a prime factor, p greater than 2 occurs as a prime factor, then what more do you want? You also want p minus 1 to be a power of 2; this should be a power of 2 because that is the other term which occurs in the formula for phi n.

(Refer Slide Time: 39:37)



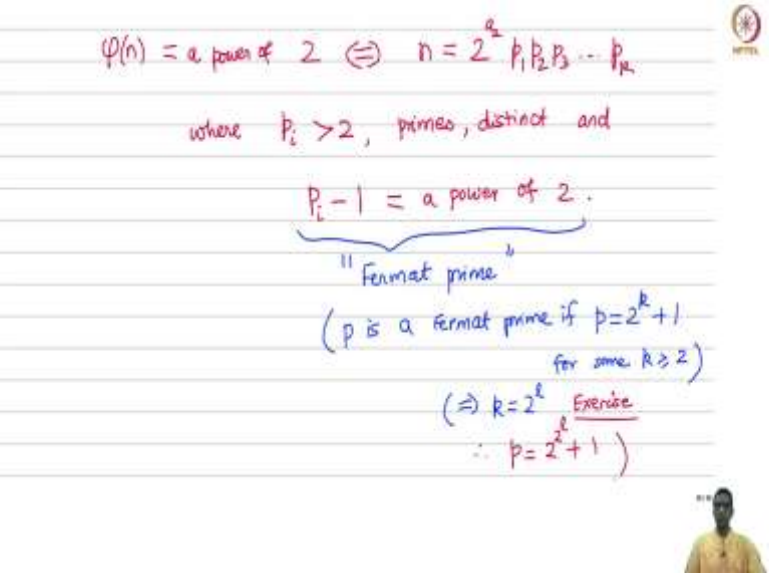
Finally: when is $\varphi(n)$ a power of 2 ?

$$n = 2^{a_2} 3^{a_3} 5^{a_5} \cdots p^{a_p} \cdots \qquad a_p \in \mathbb{Z}_{>0}$$

FACT: $\varphi(n) = 2^{a_2 - 1}(2-1)\, \underline{\underline{3}}^{\boxed{a_3-1}}(3-1) \cdots \underline{\underline{p}}^{\boxed{a_p-1}}\underline{\underline{(p-1)}} \cdots$

$= \text{power of } 2 \iff a_p = 1 \;\; \forall$ prime factors p of n, $p \neq 2$.

and $p > 2$ occurs as a prime factor, then $(p-1) = \text{power of } 2$.



$\varphi(n) = \text{a power of } 2 \iff n = 2^{a_2} p_1 p_2 p_3 \cdots p_k$

where $p_i > 2$, primes, distinct and

$$\underbrace{p_i - 1 = \text{a power of } 2.}_{\text{"Fermat prime"}}$$

(p is a Fermat prime if $p = 2^k + 1$ for some $k \geq 2$)

($\Rightarrow k = 2^l$ Exercise

$\therefore p = 2^{2^l} + 1$)

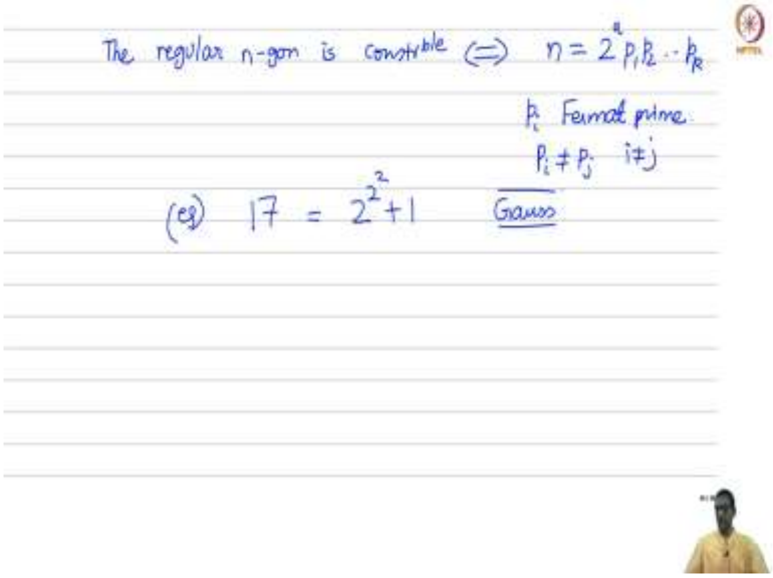
So that is already very, very restrictive. So what does this mean? So, we have concluded and observe this is if and only if, so if these conditions all hold then definitely phi n is a power of 2, because we have taken care of both the kinds of terms which can appear. So what does this mean? This says that phi n is a power of 2, is a power of 2 means is the same as saying n looks the following; n is some power of 2 does not matter which power times some product of prime powers the other primes.

Now the other primes which occur must all occur with a p equal to 1. So, each of the other primes which occurs, occurs with coefficient 1. So, let me just say there are other primes p 1, p 2, p 3, p k where what are the p i's? p i's are greater than 2. They are primes, they are all distinct and they are very special primes.

They are primes which have the following property that p i minus 1 is also a power of 2. So these are very special type of prime and this is, this has a name. This is called a Fermat prime. A Fermat prime p, a prime p is called a Fermat prime if p is of the form some power of 2 plus 1. So Fermat prime p is a Fermat prime if p is of the form some power of 2 plus 1 for some k and it is in fact, not too hard to see that if (2) some power of 2 plus 1is prime then in fact it implies that k itself must be some power of 2.

So this is again k must be a power of 2. This is a sort of a simple exercise. You can show that, if k is not of this form then p cannot be prime, you can find a common factor if there is some odd factor, if k has an odd number dividing it, then you can easily pull out a divisor of p. So, exercise show that k must look like 2 power n.

(Refer Slide Time: 42:18)



The regular n-gon is Constible $\Longleftrightarrow$ $n = 2^a p_1 p_2 \cdots p_k$

p_i Fermat prime

$p_i \neq p_j$ $i \neq j$

(eg) $17 = 2^{2^2}+1$ Gauss

So, in fact a Fermat prime is something of the following form; it is 2 to the 2 to the l plus 1 for some l and p is prime. So what we have finally shown is this very classic result whose special case, so example is, so finally to conclude, what did we say? We said that the regular n-gon is constructible.

So finally we have shown that the regular n-gon is constructible if and only if the following happens, n looks like a power of 2, 2 power something multiplied by a product of distinct Fermat primes. Now, and P i is not equal to P j or i not equal to j. Now, what is an example of Fermat prime? Well, 17 is sort of the classic example.

Observe this is just 2 power 4 which is 2 to the 2 square plus 1. That is a Fermat prime and this is sort of a famous result due to Gauss who discovered that the 17 sided polygon was actually constructible using ruler and compass and here is more general result on constructability of regular n-gon.