We've seen before that $\Phi_p(x)$ is irreducible

In fact we have

Thm 6.5 The cyclotomic poly $\Phi_n(x)$ is a monic irreducible polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$

Proof Exercise.

Cor 6.6 $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$

Since $\Phi_n(x)$ is irreducible monic and ζ_n is a root, it is its minimal poly ...

Moreover we have

Thm 6.7 The Galois gp of the cyclotomic field $\mathbb{Q}(\zeta_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$

The isom is given explicitly by the map

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow Gal(\mathbb{Q}(\zeta_n):\mathbb{Q})$$

$$a \bmod n \longmapsto \sigma_a$$

where σ_a is the autom defined by

$$\sigma_a(\zeta_n) = \zeta_n^{\,a}$$

In particular $Gal(\mathbb{Q}(\zeta_n):\mathbb{Q})$ is an abelian group.

Note any autom σ of $\mathbb{Q}(\xi_n)$ is uniquely determined by its action on ξ_n.
This element, ξ_n, must be mapped to another primitive n-th root of unity
(These are the roots of the irreducible cyclotomic poly $\Phi_n(x)$)
Hence $\sigma(\xi_n) = \xi_n^{\,a}$ for some a, $1 \leq a < n$, $(a, n) = 1$

Defn: An extension $L : K$ is called an abelian extension if $L : K$ is Galois and $Gal(L : K)$ is abelian

One deep theorem says that any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension

$$\boxed{\begin{array}{l}\text{Thm (Kronecker–Weber) Let } L \text{ be a finite abelian extension of } \mathbb{Q}\text{. Then } L \text{ is}\\ \text{contained in a cyclotomic exten of } \mathbb{Q}\\ \text{ie } L \subset \mathbb{Q}(\xi_n) \text{ for some } n.\end{array}}$$

§7. Solvability by radicals and Solvable groups.

(insolvability of general quintic).

The main problem that motivated the development of Galois theory was the question of solutions of polynomials using the field operations and taking n-th roots.

ie given a poly $f = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Q}[x]$ we want a formula for zeroes of f in $\mathbb{C}$ in terms of the a_i's and field operations and n-th roots; ie in terms of a radical expressio

We first formulate the idea of "solvability by radicals" from the point of view of field extensions. We assume $\operatorname{char} K = 0$.

Defn An extension $L:K$ is called a radical extension if $L = K(\alpha_1, \dots \alpha_m)$ where for each $i = 1, \dots, m$, $\exists$ an integer n_i s.t $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1}) =: K_{i-1}$ $i \geq 2$

The elements α_i are said to form a radical sequence for $L:K$.

Note this says α_i is a zero of the polynomial $x^{n_i} - a_i \in K(\alpha_1 \dots, \alpha_{i-1})$ with $a_i \in K(\alpha_1 \dots \alpha_{i-1})$, $a_i = \alpha_i^{n_i}$

Rmk 1) A radical extention is finite and algebraic but not necessarily normal.
$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is radical but not normal

2) For a radical extention $L:K$ we have a chain of intermediate fields

$$K = K_0 \subset K_1 \subset \dots \subset K_m = L \qquad K_{i-1} = K(\alpha_1, \dots \alpha_{i-1})$$

s.t $K_{i-1}(\alpha_i) = K_i \quad \forall i = 1, \dots, m$ where α_i is a root of $x^{n_i} - a_i$ with $a_i \in K_{i-1}$

Defn A polynomial $f \in K[X]$ is <u>soluble by radicals</u> if there exists a radical extention $M:K$ s.t f splits into linear factors over M. ie $\exists$ a field M which contains a splitting field L_f of f s.t $M:K$ is a radical extention.

Rk. We have that if f is soluble by radicals then the roots of f are given by radical expressions over the ground field K.

Ex: $\gamma = (\sqrt[3]{5})(\sqrt[7]{2+\sqrt{3}}) + \sqrt[4]{1+\sqrt[3]{4}}$ is a radical expression

it lies in $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$

where $\alpha_1 = \sqrt[3]{5}$, $\alpha_1^3 = 5 \in \mathbb{Q}$, $\alpha_2 = \sqrt{3}$, $\alpha_2^2 = 2$
$\alpha_3 = \sqrt[7]{2+\alpha_2}$, $\alpha_3^7 \in \mathbb{Q}(\alpha_2) \subset \mathbb{Q}(\alpha_1, \alpha_2)$ $\in \mathbb{Q} \subset \mathbb{Q}(\alpha_1)$

$\alpha_4 = \sqrt[3]{4}$, $\alpha_4^3 = 4 \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$

$\alpha_5 = \sqrt[4]{1+\sqrt[3]{4}}$, $\alpha_5^4 = 1 + \alpha_4 \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$

and $\gamma \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_5)$ and

$\mathbb{Q}(\alpha_1 \ldots \alpha_5) : \mathbb{Q}$ is a radical extension.

The problem of solvability by radicals of f is closely related to the structure of its Galois group.

Recall

Defn A group G is called solvable if it has a finite series of subgroups

$$1 = G_0 \subseteq G_1 \subseteq G_2 \ldots \subseteq G_n = G \quad \text{s.t}$$

① $G_i \trianglelefteq G_{i+1}$ $i = 0, \ldots, n-1$

② G_{i+1}/G_i abelian for $i = 0, \ldots, n-1$

Rmk Note this does not say $G_i \trianglelefteq G$ since normality is not transitive

Ex ① Every abelian group is solvable.
$(1 \subseteq G)$

(2) S_3 is soluble, $1 \trianglelefteq A_3 \trianglelefteq S_3$
$A_3/1 \cong \mathbb{Z}_3$, $S_3/A_3 \cong \mathbb{Z}_2$

(3) S_4 is soluble
$1 \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$. $A_4/V_4 \cong \mathbb{Z}_3$
$S_4/A_4 \cong \mathbb{Z}_2$

We have that

Thm 7.1 S_n is not soluble if $n \geq 5$.

This follows from the following Propositions

Proposition 7.2 If G is a group, H s/gp $N \trianglelefteq G$. Then

(1) G soluble $\Rightarrow$ H soluble

(2) G soluble $\Rightarrow$ G/N soluble

(3) N solu, G/N solu $\Rightarrow$ G soluble

Proof This follows from isom. thms for groups.
See for example I. Stewart's book
Galois theory, Thm 13.2.

Prop. 7.3 A soluble group is simple $\iff$ it is cyclic of prime order.

Proof Thm 13.3 of Stewart.

Recall from Group theory.

Prop 7.4 If $n \geq 5$, A_n is simple.

Proof of Thm 7.1 If S_n were soluble then by Prop 7.2 (i) A_n would be soluble. By Prop 7.4 A_n is simple. By prop 7.3, this would imply that A_n is cyclic of prime order. But note that $|A_n| = \frac{n!}{2}$ is not prime if $n \geq 5$ ☒.

The main Thm that connects the solubility by radicals and soluble groups is

Thm 7.5 Let K be a field of char 0, L a finite normal (Galois) extension of K. Then $G = Gal(L:K)$ is soluble $\iff$ $\exists$ an extension M of L s.t. $M:K$ is a radical extension.

In particular

Thm 7.6 a poly f is soluble by radicals $\implies$ $Gal(f)$ is soluble.

(In fact we have $\iff$)