Lec 24 3/8/2021

Root extensions.

Look at a field F and an extension $F \subseteq K$ and $\alpha \in K$ s.t. $a = \alpha^n \in F$.
(so α is a root of $x^n - a \in F[x]$)
Then $F \subseteq F(\alpha)$ think of $\alpha = \sqrt[n]{a}$.

<u>Prop.</u> Let F be a field s.t. $x^n - 1$ splits in F with distinct roots. Suppose $F \subseteq K$ where $\alpha \in K$ s.t. $\alpha^n \in F$.
Then $F(\alpha)/F$ is Galois and $Gal(F(\alpha)/F)$ is cyclic of order $d \mid n$.

<u>Pf.</u> By assumption the set of roots of $x^n - 1$ is a subgroup of $F^\times$ of order n. So it is cyclic by an earlier thm.

Let ζ be a generator, so $\{1, \zeta, \ldots, \zeta^{n-1}\}$ = set of nth roots of 1.

Let $a = \alpha^n \in F$, so α is a root of $x^n - a \in F[x]$.

Then $\alpha, \alpha\zeta, \ldots, \alpha\zeta^{n-1}$ are all roots of $x^n - a$, and they are distinct.

So $x^n - a = (x-\alpha) \cdots (x - \alpha\zeta^{n-1})$ in $F(\alpha)$

Thus $F(\alpha)$ is a splitting field for $x^n - a$ over F, so $F(\alpha)/F$ is Galois.

If $\sigma \in \mathrm{Gal}(F(\alpha)/F)$ then $\sigma(\alpha)$ is another root of $x^n - a$

$\sigma(\alpha) = \alpha\zeta^i$ for some i and σ is determined by $\sigma(\alpha)$

We have a map

$$\phi : \mathrm{Gal}(F(\alpha)/F) \longrightarrow (\mathbb{Z}_n, +)$$

$$\sigma \longmapsto \bar{i}$$

where $\sigma(\alpha) = \alpha \zeta^i$.

Check ϕ is a homomorphism -

if $\tau(\alpha) = \alpha \zeta^j$ then

$\tau\sigma(\alpha) = \tau(\alpha\zeta^i) = \tau(\alpha)\tau(\zeta^i)$

$= \tau(\alpha)\zeta^i = \alpha\zeta^j\zeta^i = \alpha\zeta^{i+j}$

ϕ is injective since σ is determined by where it sends α.

Finally $\mathrm{Gal}(F(\alpha)/F)$ is isomorphic to a subgroup of $\mathbb{Z}_n$, so it is isomorphic to $\mathbb{Z}_d$, some $d \mid n$.

<u>Ex.</u> $f = x^8 - 2 \in \mathbb{Q}[x]$.

Let ζ primitive 8th root of 1 in $\mathbb{C}$. Take $F = \mathbb{Q}(\zeta)$

Let $\alpha = \sqrt[8]{2}$. $K = F(\alpha)$

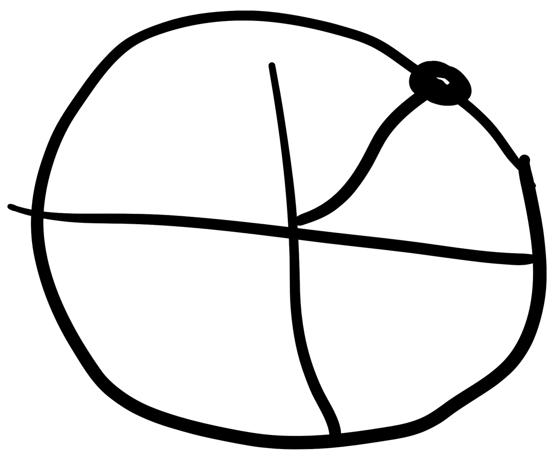
$= \mathbb{Q}(\alpha, \zeta)$ = splitting field of f over $\mathbb{Q}$.

Apply prop to $F \subseteq F(\alpha) = K$

So K/F is Galois and

$\mathrm{Gal}(K/F)$ is cyclic, but it is

$\mathbb{Z}_4$ not $\mathbb{Z}_8$.



Why? $\zeta = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$

means $\mathbb{Q}(\zeta) = \mathbb{Q}(\underline{\sqrt{2}}, \underline{i})$

So $K = \mathbb{Q}(\zeta, \alpha) =$

$\mathbb{Q}(\underline{\underline{\sqrt{2}}}, i, \sqrt[8]{2})$

$= \mathbb{Q}(\underline{\sqrt[8]{2}}, \underline{i})$ so $[K:\mathbb{Q}] = 16$.

but $[K : \underline{\mathbb{Q}(\zeta)}] = 4$

$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

so $|\mathrm{Gal}(K/F)| = 4$ so $\cong \mathbb{Z}_4$

Prop. $F \subseteq K$ with $[K:F] < \infty$. Assume F contains n roots of $x^n - 1$. Suppose K/F is Galois and $\mathrm{Gal}(K/F)$ is cyclic of order dividing n.

Then $K = F(\alpha)$ where $\alpha^n \in F$.

Pf. $G = \mathrm{Gal}(K/F)$ is cyclic of order d, $d \mid n$. Let σ generate G, so $\sigma^d = 1_K$.

Think of σ as an F-linear transformation of K.

(if $a \in F$, $b \in K$, $\underline{\sigma(ab)} = \sigma(a)\sigma(b)$
$= \underline{a\sigma(b)}$ because σ fixes F)

$[K:F] = d$. Think of K as an $F[x]$-module where x

acts as σ, and consider invariant factors + elementary divisors.

Notice $\underline{\underline{\sigma}}$ satisfies $x^d - 1 \in F(x)$ so its minimal polynomial divides $x^d - 1$. Since $x^n - 1$ factors with distinct roots in F, so does $x^d - 1$.

So $x^d - 1 = (x-1)(x-\rho)\cdots(x-\rho^{d-1})$ where ρ is a primitive dth root.

$\text{minpoly}(\sigma) \mid x^d - 1$ so it already splits in $F(x)$ with distinct roots. All invariant factors split with distinct roots since $\text{minpoly}(\sigma)$ is largest inv. factor.

So elementary divisors all have degree 1. So σ is diagonalizable (over F)

the eigenvalues of σ are dth roots of 1, and one is a primitive dth root (otherwise $\sigma^i = 1$ for $0 < i < d$))

Assume ρ is an eigenvalue.

Let α be an eigenvector in K for eigenvalue ρ, so

$\sigma(\alpha) = \rho\alpha$.

Then $\sigma(\alpha^i) = \rho^i \alpha^i$.

So $1, \alpha, \ldots, \alpha^{d-1}$ are eigenvectors with distinct eigenvalues $1, \rho, \ldots, \rho^{d-1}$.

So they are a basis of K over F.

So $F(\alpha) = K$.

Finally, $\sigma(\alpha^d) = \rho^d \alpha^d = \alpha^d$

so $\alpha^d \in \mathrm{Fix}\langle\sigma\rangle = F$

since K/F is Galois.

So $\alpha^n \in F$. since $d \mid n$.

Thm. $F \subseteq K$, $x^n - 1$ splits with distinct roots in F.

TFAE

① K/F is Galois and $\mathrm{Gal}(K/F)$ is cyclic of order dividing n.

② $K = F(\alpha)$ for $\alpha \in K$ with $\alpha^n \in F$.

Def. A field extension $F \subseteq K$ is a root extension if

$$F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m = K$$

where $K_{i+1} = K_i(\alpha_i)$ $\alpha_i^{n_i} \in K_i$ for all $i \geq 0$.

Say $f \in F[x]$ is solvable by radicals if there is a root extension $F \subseteq K$ s.t. f

Split in $K[x]$.

Idea: f is solvable by radicals if its roots can be expressed using elements of F, $\pm$, $\cdot$, $/$ and $\sqrt[n]{-}$

e.g. $\sqrt[3]{5+\sqrt{2}}$ would lie in a root extension over $\mathbb{Q}$.

Thm. (Galois)
F characteristic 0.
$f \in F[x]$ is solvable by radicals iff $\mathrm{Gal}(K/F)$ is solvable where K is the splitting field of f over F.

Rmk. Note a finite group G is solvable iff there is a chain of subgroups

$$1 \subseteq H_0 \trianglelefteq H_1 \trianglelefteq H_2 \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

s.t. H_{i+1}/H_i is <u>cyclic</u>.

(use that a finite Abelian group is a direct product of cyclic groups.)

So it is plausible that solvable groups correspond to root extensions.