Lec 24  3/8/2021

Root extensions.

Look at a field $F$ and an extension $F \subseteq K$ and $\alpha \in K$ s.t. $\alpha^n \in F$.
(So $\alpha$ is a root of $x^n - \alpha \in F[x]$.)

Then $F \subseteq F(\alpha)$, that is, $\alpha = \sqrt[n]{\alpha}$.

Prop. Let $F$ be a field s.t. $x^n - 1$ splits in $F$ with distinct roots. Suppose $F \subseteq K$ such that $\alpha \in K$ s.t. $\alpha^n \in F$.

Then $F(\alpha)/F$ is Galois and $\text{Gal}(F(\alpha)/F)$ is cyclic of order $d | n$.

Pf. By assumption, the set of roots of $x^n - 1$ is a subgroup of $F^x$ of order $n$. So it is cyclic by an earlier theorem.
Let \( y \) be a generator, so \( 1, y, \ldots, y^{n-1} \)
= set of all roots of \( 1 \).

Let \( \alpha = y^i \in \mathbb{F} \), so \( \alpha \) is a root of \( x^n - \alpha \in \mathbb{F}(\alpha) \).

The \( \alpha, y, \ldots, y^{n-1} \) are all roots of \( x^n - \alpha \), and they are distinct.

So \( x^n - \alpha = (x - y)(x - y^i) \ldots (x - y^{n-1}) \)
in \( \mathbb{F}(\alpha) \).

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

If \( \sigma \in \text{Gal}(\mathbb{F}(\alpha)/\mathbb{F}) \) then \( \sigma(\alpha) \) is another root of \( x^n - \alpha \)
\( \sigma(\alpha) = y^j \) for some \( j \) and \( \sigma \)
is determined by \( \sigma(\alpha) \).

We have a map
\[
\phi : \text{Gal}(\mathbb{F}(\alpha)/\mathbb{F}) \rightarrow (\mathbb{Z}_n)^+
\]
\( \sigma \rightarrow \bar{i} \)
\[ \text{Ann } \alpha_{21} = 2 \mathbb{Z}^i. \]

Claim: \( \phi \) is a homomorphism - if \( \tau(\alpha) = \alpha \delta_1^i \) then

\[ \tau(\gamma_2 \alpha) = \tau(\delta_1^i) = \tau(\gamma_2 \alpha) \]

\[ = \tau(\alpha) \delta_1^i = \alpha \delta_1^i \delta_1^i = \alpha \delta_1^i \]

\( \phi \) is injective since \( \alpha \) is defined by where it sends \( \alpha \).

Finally, \( \text{ker}(\Phi) / \langle \tau \rangle \) is isomorphic to a subgroup of \( \mathbb{Z}_n \), so it is isomorphic to \( \mathbb{Z}_d \) for some \( d | n \).

\[ \text{Ex. } f = x^8 - 2 \in \mathbb{Q}(x). \]

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

Let \( \alpha = \delta \sqrt{2} \). \( K = F(\alpha) = \mathbb{Q}(\sqrt{2}, \gamma) = \alpha \mathbb{Q}(\delta) \)
of form $\mathbb{Q}$.

Apply prop 1: $F \leq F(x) = \mathbb{K}$

So $K/F$ is Galois and $\text{Inv}(K/F)$ is cyclic, but it is $\mathbb{Z}_4$ not $\mathbb{Z}_8$.

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

Thus $\Omega(\gamma) = \Omega(\sqrt{2}, i)$

So $K = \Omega(\sqrt{2}, i)$

\[
\Omega(\sqrt{2}, i) = \Omega(\sqrt{2}, i + \sqrt{2}) = \Omega(\sqrt{2}, i) \
\]

$[K: \mathbb{Q}] = 8$

\[
[K: \mathbb{Q}(\sqrt{2})] = 4
\]

\[
[K: \mathbb{Q}(i)] = 4
\]

\[
[K(\sqrt{2}): \mathbb{Q}] = 4
\]

\[
2 \mid \text{Inv}(K/F) \implies 24
\]
Prop. \( E \subseteq K \) with \( (K:F) < \infty \)
Assume \( F \) contains \( n \) roots of \( x^n - 1 \). Suppose \( K/F \) is Galois and \( \text{Gal}(K/F) \) is cyclic of order dividing \( n \).
Then \( K = E(\alpha) \) where \( \alpha^n \in F \).

Pf. \( \sigma = \text{Gal}(K/F) \) is cyclic of order \( d \), \( d \mid n \). Let 
\( \sigma \) generate \( \sigma \) so \( \sigma^d = 1 \).
Think of \( \sigma \) as an \( F \)-linear transformation of \( K \).

(If \( a \in F \) then \( \sigma(a) = \sigma(a) \sigma(b) \)
\( = \sigma(ab) \) because \( \sigma \) fixes \( F \)).

\( (K:F) = d \). Think of \( K \)
\( \sigma a \in E(\alpha) - \)module where \( \alpha \)
acts as \( \sigma \), and consider invariant factors + elementary divisors.

Notice \( \alpha \) satisfies \( x^d - 1 \in F(x) \) so its minimal polynomial divides \( x^d - 1 \). Since \( x^d - 1 \) factors with distinct roots in \( F \), so does \( x^d - 1 \).

So \( x^d - 1 = (x - \omegarier) \cdots (x - \omegarier) \) where \( \omega \) is a primitive \( d \)th root.

min poly \( \omega \) \( | x^d - 1 \) so it already splits in \( F(x) \) with distinct roots. All invariant factors split with distinct roots.

Since min poly \( (\omega) \) is largest invariant.

So elementary divisors all have degree 1. So \( \sigma \) is diagonalizable.
Let $\alpha$ be an eigenvalue in $K$ for eigenvalue $\beta$, i.e.,
\[ \sigma(\beta) = \beta \alpha. \]
Then $\sigma(\alpha^k) = \beta^k \alpha^k$.

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

So they are a basis of $K$ over $F$.

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

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

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

Since $K/F$ is Galois,

so $\alpha^d \in F$. Since $d | n$. 
Thm. $F \leq K \land x^n - 1$ splits with distinct roots in $F$.

TFAE

1. $K/E$ is abelian and $\text{Gal}(K/E)$ is cyclic of order dividing $n$.
2. $K = E(\alpha)$ for $\alpha \in K$ with $\alpha^n \in F$.

Def. A field extension $FSK$ is a root extension if

$F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K$

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

Say $f \in F(x)$ is solvable by radicals if there is a root extension $F \leq K$ s.t. $f$
split in $k(a)$. 

Idea: if it is solvable by radicals if it roots can be expressed using elements of $F$, $\pm \sqrt[3]{a}$ and $\sqrt{-}$ e.g. $\sqrt{5} + \sqrt[3]{2}$ would lie in a root extension over $\mathbb{Q}$.

**Thm. (Ludolff)**

If characteristic 0.

If $f \in F[x]$ is solvable by radicals if and only if $(K/E)$ is solvable when $K$ is the splitting field of $f$ over $F$.

**Note.** Not a finite group $G$ is solvable if there is a chain
of subgroups

1 \triangleleft H_0 \triangleleft H_1 \triangleleft H_2 \ldots \Rightarrow H_n \triangleleft H_{n+1} \triangleleft \ldots \\
5. \text{ } H_n/H_i \text{ is cyclic.}

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

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