Lec 22 March 3, 2021

Last time:

Thm. - $[K:F]<\infty$ K/F Galois

There is a bijection

$$\left\{\begin{array}{c}\text{Intermediate fields}\\ F\subseteq E\subseteq K\end{array}\right\} \underset{\Phi = \mathrm{Fix}(-)}{\overset{\Gamma = \mathrm{Gal}(K/\_)}{\rightleftarrows}} \left\{\begin{array}{c}\text{subgroups } H\\ \text{of}\\ G=\mathrm{Gal}(K/F)\end{array}\right\}$$

which reverses inclusions

i.e. if $E_1 \subseteq E_2$ then

$$\mathrm{Gal}(K/E_2) \subseteq \mathrm{Gal}(K/E_1)$$

if $H_1 \subseteq H_2$ then

$$\mathrm{Fix}(H_2) \subseteq \mathrm{Fix}(H_1).$$

$$|\mathrm{Gal}(K/E)| = [K:E]$$

Also E/F is normal iff $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$.

<u>Ex.</u> K = Splitting field of $x^4 - 2 =: f$ over $\mathbb{Q}$. Let $\alpha = \sqrt[4]{2}$, $i = \sqrt{-1}$.

Then roots of f in $\mathbb{C}$ are

$$\{\alpha, \alpha i, -\alpha, -\alpha i\}$$

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

f is irr. by Eisenstein, so

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = \deg f$

$i \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, i is a root of x^2+1

So $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$

$[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8$.

$K/\mathbb{Q}$ is a splitting field for f so is Galois. So $|\mathrm{Gal}(K/\mathbb{Q})| = 8$.

Now if $\sigma \in G = \mathrm{Gal}(K|F)$ then

$\sigma(\alpha)$ is a root of f

$\sigma(i)$ is a root of x^2+1.

8 choices total, and σ is determined by where it sends α and i. So all occur.

Let $\sigma: \alpha \mapsto i\alpha$ $\quad$ $\tau: \alpha \mapsto \alpha$
$\qquad i \mapsto i$ $\qquad\qquad\quad i \mapsto -i$

$|\sigma| = 4$. $\quad |\tau| = 2$.

$|\langle\sigma\rangle\langle\tau\rangle| = 8 \qquad \langle\sigma\rangle \cap \langle\tau\rangle = 1$

So $G = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$

$$\tau\sigma(\alpha) = \tau(i\alpha) = -i\alpha$$
$$\tau\sigma(i) = -i$$

$$\sigma^3\tau(\alpha) = \sigma^3(\alpha) = -i\alpha$$
$$\sigma^3\tau(i) = -i$$

So $\tau\sigma = \sigma^3\tau = \sigma^{-1}\tau$.

So $G \cong D_8$.

Let's find all subgroups of $G = D_8$
$= \langle \sigma, \tau \rangle$

$$\begin{tikzcd}
 & & G \arrow[dll, dash, "2"'] \arrow[d, dash] \arrow[drr, dash] & & \\
\langle \sigma \rangle \arrow[d, dash] & & \langle \sigma^2, \tau \rangle \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] & & \langle \sigma^2, \sigma\tau \rangle \arrow[dllll, dash] \arrow[dl, dash] \arrow[d, dash] \\
Z(G) = \langle \sigma^2 \rangle \arrow[drr, dash] & \langle \tau \rangle \arrow[dr, dash] & \langle \sigma^2\tau \rangle \arrow[d, dash] & \langle \sigma\tau \rangle \arrow[dl, dash] & \langle \sigma^3\tau \rangle \arrow[dll, dash] \\
 & & 1 & &
\end{tikzcd}$$

Apply $\mathrm{Fix}(-)$

$$\begin{tikzcd}
 & & \mathbb{Q} \arrow[dll, dash, "2"'] \arrow[d, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(i) \arrow[d, dash, "2"'] & & \mathbb{Q}(\sqrt{2}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] & & \mathbb{Q}(\sqrt{2}\,i) \arrow[dllll, dash] \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}, i) \arrow[drr, dash] & \mathbb{Q}(\sqrt[4]{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt[4]{2}\,i) \arrow[d, dash] & \mathbb{Q}(\sqrt[4]{2}(i+1)) \arrow[dl, dash] & \mathbb{Q}(\sqrt[4]{2}(i-1)) \arrow[dll, dash] \\
 & & K = \mathbb{Q}(\sqrt[4]{2}, i) & &
\end{tikzcd}$$

$\mathbb{Q}(i) \subseteq \mathrm{Fix}(\langle \sigma \rangle)$

$[\mathbb{Q}(i) : \mathbb{Q}] = 2$

What about normality?

$\langle \sigma \rangle$, $\langle \sigma^2, \tau \rangle$, $\langle \sigma^2, \sigma\tau \rangle \trianglelefteq G$
$\langle \sigma^2 \rangle$

The others are not normal.

So all fields are normal (and Galois) over $\mathbb{Q}$ except.

$\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[4]{2}i)$, $\mathbb{Q}(\sqrt[4]{2}(1+i))$
$\mathbb{Q}(\sqrt[4]{2}(1-i))$

e.g. $\sqrt[4]{2}$ is a root of x^4-2 but x^4-2 does not split over $\mathbb{Q}(\sqrt[4]{2})$.

$\sqrt[4]{2}(1+i)$ is a root of x^4+8 which does not split over $\mathbb{Q}(\sqrt[4]{2}(1+i))$.

Also $\langle \sigma^2 \rangle = \mathrm{Gal}(K/\mathbb{Q}(\sqrt{2}, i))$

Fund. Theorem says

$$G/\langle \sigma^2 \rangle \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}).$$

both are $\cong$ to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Another example.

Ex. $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ $\alpha = \sqrt{2+\sqrt{2}}$

$\mathrm{minpoly}_{\mathbb{Q}}(\alpha) = x^4 - 4x^2 + 2$

roots are $\pm\alpha, \pm\beta$ $\beta = \sqrt{2-\sqrt{2}}$

check K = splitting field of $x^4 - 4x^2 + 2$

since $\alpha\beta = \sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}}$

$= \sqrt{4-2} = \sqrt{2} \in K.$

$(\alpha^2 - 2 = \sqrt{2} \in K)$

$[K:\mathbb{Q}] = 4$, $K/\mathbb{Q}$ is Galois.

What is $\mathrm{Gal}(K/\mathbb{Q})$? Group of size 4.

Any $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$ is determined by where it sends α, which is in $\{\pm\alpha, \pm\beta\}$.

Choose $\sigma(\alpha) = \beta$.

then $\sigma(-\alpha) = -\beta$.

Since $\alpha\beta = \sqrt{2}$

$\sigma(\alpha\beta) = \underline{\sigma(\alpha)}\,\sigma(\underline{\beta}) = \sigma(\underline{\sqrt{2}})$

Since $\alpha^2 - 2 = \sqrt{2}$, $\sigma(\sqrt{2}) = \sigma(\alpha^2) - 2$

$= \sigma(\beta^2) - 2$

$\sigma(2+\sqrt{2}) - 2 = \sigma(2-\sqrt{2}) - 2$

$\sigma(2+\sqrt{2}) = \sigma(2-\sqrt{2})$

$\sigma(\sqrt{2}) = -\sqrt{2}$

this forces $\sigma(\beta) = -\alpha$.

$$\begin{aligned} \sigma:\ \alpha &\to \beta \\ \beta &\to -\alpha \\ -\alpha &\to -\beta \\ -\beta &\to \alpha \end{aligned} \qquad |\sigma| = 4 \quad \text{and } G \cong \mathbb{Z}_4.$$

$$\begin{array}{ccc} G = \langle \sigma \rangle & & \mathbb{Q} \\ | & \xrightarrow{\mathrm{Fix}(-)} & | \\ \langle \sigma^2 \rangle & & \mathbb{Q}(\sqrt{2}) \\ | & & | \\ 1 & & K \end{array}$$

Next time: Cyclotomic polynomials

Galois group of splitting field

of $x^n - 1$ over $\mathbb{Q}$.