Day 28 July 17, 2024

Yesterday:

- A polynomial is separable if it has no repeated roots. A field extension $E \supset F$ is separable if every element of E is a root of some separable polynomial over F.
- If $E \supset F$ is the splitting field of a separable polynomial, then $|G(E/F)| = [E:F]$ and

$$E_{G(E/F)} = F.$$

(Recall: For any $H \leq G(E/F)$,
$$E_H = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in H.\})$$

Def. Let $E \supset F$ be an algebraic field extension. We call E a normal extension if every irred. polynomial in $F[x]$ with at least one root in E splits over E.

Thm. Let $E \supset F$ be a field extension. Then TFAE:

1. E is a finite, normal, separable extension of F.
2. E is the splitting field of a separable polynomial in $F[x]$.
3. For some finite subgroup $G \leq Aut(E)$, $F = E_G$.

Thm [Fundamental Theorem of Galois Theory]
Let F be a field of characteristic zero and let $E \supset F$ be a finite, normal extension of F with Galois group $G(E/F)$. Then:

1. The map $K \mapsto G(E/K)$ is a bijection from the collection of subfields of E containing F to the subgroups of $G(E/F)$.
2. For any $E \supseteq K \supseteq F$,
$$[E:K] = |G(E/K)| \text{ \& } [K:F] = [G(E/F) : G(E/K)].$$
3. Subfields $K, L \subseteq E$ with $F \subseteq K, L$ satisfy $K \subseteq L$ iff $G(E/L) \leq G(E/K)$.
4. A subfield $K \subset E$ is a normal extension of F iff $G(E/K)$ is a normal subgroup of $G(E/F)$.
Moreover, $G(K/F) \cong \dfrac{G(E/F)}{G(E/K)}$.

Ex. Consider $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

$x^7 - 2$
Let $\zeta = e^{\frac{2\pi i}{7}}$.

1. The splitting field

$$\begin{aligned} x^4 - 2 &= (x^2 - \sqrt{2})(x^2 + \sqrt{2}) \\ &= (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}). \end{aligned}$$

So $x^4 - 2$ splits over $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$ and over no proper subfield.

② The order of the Galois group

$\mathbb{Q}(\sqrt[4]{2}, i) \supset \mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$.

The extension $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ has basis $\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3\}$, so $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

Similarly, $\mathbb{Q}(\sqrt[4]{2}, i) \supset \mathbb{Q}(\sqrt[4]{2})$ has basis $\{1, i\}$, so $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$.

$$\therefore [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$$
$$= 2 \cdot 4 = 8.$$

Since $x^4 - 2$ is separable,

$$|G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8.$$

③ Identifying the Galois group

the Galois group

We can define an element of G via its effect on $\sqrt[4]{2}$ and i. Consider

$$\sigma : \sqrt[4]{2} \mapsto i\sqrt[4]{2}, \quad i \mapsto i \qquad \tau : \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad i \mapsto -i.$$

Check: $G = \{id, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ by showing that these elements are distinct.

Check: $\sigma^4 = \tau^2 = (\sigma\tau)^2 = id$.

So $G = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = (\sigma\tau)^2 = id \rangle \cong D_4$.

④ The subgroups of the Galois group

$$
\begin{tikzcd}[column sep=small]
 & & \{id\} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\{id, \tau\} \arrow[dr, dash] & \{id, \sigma^2\tau\} \arrow[d, dash] & \{id, \sigma^2\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \{id, \sigma\tau\} \arrow[d, dash] & \{id, \sigma^3\tau\} \arrow[dl, dash] \\
 & \{id, \sigma^2, \tau, \sigma\tau\} \arrow[dr, dash] & \{id, \sigma, \sigma^2, \sigma^3\} \arrow[d, dash] & \{id, \sigma^2, \sigma\tau, \sigma^3\tau\} \arrow[dl, dash] & \\
 & & G \cong D_4 & &
\end{tikzcd}
$$

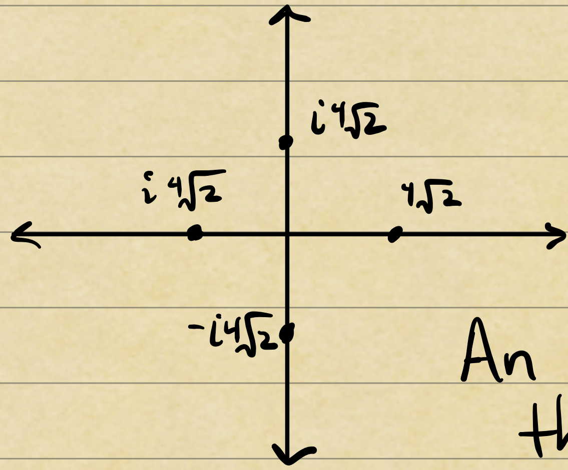
⑤ The fixed fields of the splitting field

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

all deg. 4

all deg. 2

Since $\{id, \tau\}$ is not normal in G,
$\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ is not a normal extension.
e.g., $x^4 - 2 \in \mathbb{Q}[x]$ is an irred. poly.
which has a root in $\mathbb{Q}(\sqrt[4]{2})$, but
does not split over $\mathbb{Q}(\sqrt[4]{2})$.



$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2}) \cdot (x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$$

An elt of G must permute these roots.

$\tau: \sqrt[4]{2} \mapsto \sqrt[4]{2}$
$\quad i \mapsto -i$
refl. across horiz.

$\sigma: \sqrt[4]{2} \mapsto i\sqrt[4]{2}$
$\quad i \mapsto i$
90° CCW rotation