6.7 The Galois correspondence

Let $\mathbb{F}$ be a field.

- The *automorphism group of* $\mathbb{F}$ is $\mathrm{Aut}(\mathbb{F}) = \{\sigma\colon \mathbb{F} \to \mathbb{F} \mid \sigma \text{ is an automorphsm}\}$.
- Let $\mathbb{E}$ be a subfeld of $\mathbb{F}$. Then define
$$\mathrm{Aut}_{\mathbb{E}}(\mathbb{F}) = \{\sigma \in \mathrm{Aut}(\mathbb{F}) \mid \text{if } e \in \mathbb{E} \text{ then } \sigma(e) = e\}.$$
- Let H be a subgroup of $\mathrm{Aut}(\mathbb{F})$.
$$\mathbb{F}^H = \{x \in \mathbb{F} \mid \text{if } \sigma \in H \text{ then } \sigma(x) = x\}.$$

Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[x]$. Let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$.

- The *splitting field of* f over $\mathbb{F}$ is the subfield $\mathbb{S}_f$ of $\overline{\mathbb{F}}$ such that
  (a) $\mathbb{F} \subseteq \mathbb{S}_f$ and there exist $\alpha_1, \ldots, \alpha_r \in \mathbb{S}_f$ such that $f(x) = (x-\alpha_1)\cdots(x-\alpha_r)$,
  (b) if $\mathbb{K}$ is a subfield of $\overline{\mathbb{F}}$ and there exist $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$ such that $f(x) = (x-\alpha_1)\cdots(x-\alpha_r)$ then $\mathbb{K} \supseteq \mathbb{S}_f$.
- A *Galois extension of* $\mathbb{F}$ is an extension $\mathbb{K} \supseteq \mathbb{F}$ such that there exists $f \in \mathbb{F}[x]$ such that $K = \mathbb{S}_f$ is the splitting field of $\mathbb{F}$.

Theorem 6.16. *Let $\mathbb{K}/\mathbb{F}$ be a Galois extension. Then the map*

$$\begin{array}{ccc}
\{\textit{field inclusions } \mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}\} & \longleftrightarrow & \{\textit{group inclusions } \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \supseteq H \supseteq \{1\}\} \\
\mathbb{E} & \longmapsto & \mathrm{Aut}_{\mathbb{F}}(\mathbb{E}) \\
\mathbb{F}^H & \longleftarrow & H
\end{array}$$

is an isomorphism of posets.

6.8 Splitting fields and algebraic closure

Let $\mathbb{F}$ be a field and let $S \subseteq \mathbb{F}[x]$. The **splitting field of** S **over** $\mathbb{F}$ is the field $\mathbb{K}$ such that

(a) $\mathbb{K} \supseteq \mathbb{F}$ and $\mathbb{K}$ satisfies the condition

$$\text{If } f \in S \text{ then there exist } \alpha_1, \ldots, \alpha_n \in \mathbb{K} \text{ such that } f(x) = (x-\alpha_1)\cdots(x-\alpha_n),$$

(b) If $\mathbb{E}$ is a field such that $\mathbb{E} \supseteq \mathbb{F}$ and satisfies the condition

$$\text{If } f \in S \text{ then there exist } \alpha_1, \ldots, \alpha_n \in \mathbb{K} \text{ such that } f(x) = (x-\alpha_1)\cdots(x-\alpha_n),$$

then $\mathbb{E} \supseteq \mathbb{K}$.

Theorem 6.17. *Let $\mathbb{F}$ be a field and let $S \subseteq \mathbb{F}[x]$. Then the splitting field of S over $\mathbb{F}$ exists.*

Corollary 6.18. *Let $\mathbb{F}$ be a field. Then the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$ exists.*