14.1 Galois Theory.

Goal. Study K/F via the group

$$\mathrm{Aut}\,(K/F) := \{\varphi\colon K \to K \ :\ \varphi \text{ is an isomorphism}, \varphi|_F = \mathrm{id}_F\}.$$

Lemma. *Let $G = \mathrm{Aut}\,(K/F)$, $f(x) \in F[x] \setminus F$ and $Z = \{\alpha \in K \ :\ f(\alpha) = 0\} \neq \emptyset$. Then*

(1) *G acts on Z.*
(2) *If $K = F(Z)$, then G embeds into S_Z.* (group of permutations on Z, i.e. action is faithful)
(3) *If K is the splitting field of $f(x)$, which is irreducible, then G is transitive on Z.*

Recall. If $f(x)$ is also separable in (3), then $|G| = [K : F]$.

Proof. 1) Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$ with $a_i \in F$

Let $\varphi \in \mathrm{Aut}(K/F)$, $\alpha \in Z$. Then

$f(\varphi(\alpha)) = a_0 + a_1 \varphi(\alpha) + \dots + a_n \varphi(\alpha)^n = \varphi(\underbrace{f(\alpha)}_{=0})$ since $\varphi(a_i) = a_i$

Hence $\varphi(\alpha) \in Z$.

2) $h: G \to S_Z$ is group hom.
$\varphi \mapsto \varphi|_Z$

If $\varphi \in \ker h$, then $\varphi|_Z = \mathrm{id}_Z$ and $\varphi|_F = \mathrm{id}_F$. Hence $\varphi|_{F(Z)} = \mathrm{id}_{F(Z)}$.

3) For $\alpha, \beta \in Z$

$$\begin{tikzcd} K \arrow[r, "\exists \varphi \in G"] & K \\ F(\alpha) \arrow[u, phantom, "\cup"] \arrow[r, "\varphi_{\alpha\beta}"] & F(\beta) \arrow[u, phantom, "\cup"] \\ F \arrow[u, phantom, "\cup"] \arrow[r, "\mathrm{id}"] & F \arrow[u, phantom, "\cup"] \end{tikzcd}$$

extends to splitting fields.
($\varphi: \alpha \to \beta$ always possible by previous Lemma)

$\square$

Example. (1) $\tau \in \mathrm{Aut}\,(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ satisfies $\tau(\sqrt{2}) = \pm\sqrt{2}$

Hence $\tau(a + b\sqrt{2}) = a \pm b\sqrt{2}$ Splitting field of $x^2 - 2$.

$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_2$

2) $\varphi \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is uniquely determined by $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$

Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$.

Not the splitting field of $x^3 - 2$.

Subfields and subgroups.

Definition.

$$\begin{aligned} \mathrm{Fix}\colon \{H \leq \mathrm{Aut}\,(K/F)\} &\to \quad \{L : F \leq L \leq K\} \\ H \quad &\mapsto \{\alpha \in K : \varphi(\alpha) = \alpha \ \forall \varphi \in H\} \end{aligned}$$

Fix(H) is a subfield of K, the *fixed field* of H.
Dually

$$\begin{aligned} \mathrm{Aut}\,(K/.)\colon \{L : F \leq L \leq K\} &\to \{H \leq \mathrm{Aut}\,(K/F)\} \\ L \quad &\mapsto \quad \mathrm{Aut}\,(K/L) \end{aligned}$$

Aut (K/L) is a subgroup of Aut (K/F), the stabilizer of L in Aut (K).

$$\begin{array}{ccc} K & \xrightarrow{\mathrm{Aut}(K/.)} & \mathrm{Aut}(K/K) = 1 \\ \rotatebox{90}{$\leq$} & & \rotatebox{90}{$\geq$} \\ \mathrm{Fix}(\mathrm{Aut}(K/L)) & \longleftarrow & \\ \rotatebox{90}{$\leq$} & & \\ L & \longrightarrow & \mathrm{Aut}(K/L) \\ \rotatebox{90}{$\leq$} & & \rotatebox{90}{$\geq$} \\ F & \longrightarrow & \mathrm{Aut}(K/F) \end{array}$$

Fix and Aut $(K/.)$ are *order reversing.*

$H_1 \leq H_2 \leq \mathrm{Aut}(K/F) \Rightarrow \mathrm{Fix}(H_1) \geq \mathrm{Fix}(H_2)$

$E \subseteq L \Rightarrow \mathrm{Aut}(K/E) \geq \mathrm{Aut}(K/L)$

Fix Aut $(K/.)$ **and** Aut $(K/\mathrm{Fix}(.))$ **are closure operators.**

[Closure ops cl satisfy $A \subseteq cl(A)$ $\qquad A_1 \subseteq A_2 \Rightarrow cl(A_1) \subseteq cl(A_2)$]

$cl(cl(A)) = cl(A)$

Lemma. *Let* $G = \mathrm{Aut}\,(K/F)$*, Then*

(1) $\mathrm{Fix}(\mathrm{Aut}\,(K/\mathrm{Fix}(H))) = \mathrm{Fix}(H)$ *for all* $H \leq G$.
(2) $\mathrm{Aut}\,(K/\mathrm{Fix}(\mathrm{Aut}\,(K/L))) = \mathrm{Aut}\,(K/L)$ *for all* $F \leq L \leq K$.

Proof. 1) Let $H \leq G$.

$\supseteq$ Let $\alpha \in \mathrm{Fix}(H)$, $\varphi \in \mathrm{Aut}(K/\mathrm{Fix}(H))$.
Then $\varphi(\alpha) = \alpha$. So $\alpha \in \mathrm{Fix}(\mathrm{Aut}(K/\mathrm{Fix}(H)))$.

$\subseteq$
$$\begin{array}{ccc} \mathrm{Aut}(K/\mathrm{Fix}(H)) & \to & \mathrm{Fix}(\mathrm{Aut}(K/\mathrm{Fix}(H))) \\ \cup & & \cap \\ H & \to & \mathrm{Fix}(H) \end{array}$$

2) similar, try. $\square$

Galois extensions.

Definition. An algebraic extension K/F is Galois if

$$F = \mathrm{Fix}(\mathrm{Aut}\,(K/F))$$

i.e., F is closed under FixAut $(K/.)$.

Example.
$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois $\qquad \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \langle \tau \rangle, \quad \tau(\sqrt{2}) = -\sqrt{2}$
$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ not Galois $\qquad \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$

Definition. An algebraic extension K/F is normal if every irreducible $f(x) \in F[x]$ with some root in K splits in $K[x]$.

Theorem. *For K/F of finite degree TFAE:*
(1) *K/F is Galois.*
(2) *K/F is normal and separable.*
(3) *K is the splitting field of some separable $f(x) \in F[x]$.*
(4) $|\mathrm{Aut}\,(K/F)| = [K : F]$.

Proof. 1) ⇒ 2) Assume K/F is Galois.
For $\alpha \in K \setminus F$ show $m_{\alpha,F}(x)$ splits in K.
Let $G := \mathrm{Aut}(K/F)$. Then the orbit $G(\alpha) \subseteq$ roots of $m_{\alpha,F}(x)$.
$p(x) := \prod_{\beta \in G(\alpha)} (x - \beta) \in K[x]$
For $\sigma \in G$, $\sigma(p(x)) = p(x)$ $\qquad \sigma(a_0 + a_1 x + \dots + a_n x^n) = \sigma(a_0) + \sigma(a_1)x + \dots + \sigma(a_n)x^n$
So $p(x) \in \underbrace{\mathrm{Fix}(G)}_{=F}[x]$
Thus $p(x) = m_{\alpha,F}(x)$ is irreducible and separable.

2) ⇒ 3) Assume K/F is normal, separable, finite.
Let $\alpha_1, \dots, \alpha_n$ a basis of K/F.
Then K is the splitting field of lcm$(m_{\alpha_1,F}(x), \dots, m_{\alpha_n,F}(x))$.

3) ⇒ 4) done in section on separability.

4) ⇒ 1) Assume $|\mathrm{Aut}(K/F)| = [K:F]$
Let $\mathrm{Fix}(\mathrm{Aut}(K/F)) =: E$
Then $F \subseteq E$.
$\mathrm{Aut}(K/E) = \mathrm{Aut}(K/\mathrm{Fix}(\mathrm{Aut}(K/F))) = \mathrm{Aut}(K/F)$ by previous Closure Lemma.

Note $\mathrm{Fix}(\mathrm{Aut}(K/E)) = E$ implies K/E is Galois.

So by 1) ⇒ 4) $\quad [K:E] = |\mathrm{Aut}(K/E)| = |\mathrm{Aut}(K/F)| = [K:F]$

Hence $F \subseteq E$ implies $F = E$; i.e. K/F is Galois. $\square$

Corollary. *Splitting fields of separable polynomials are separable.*

Proof. part of 3) ⇒ 2) of Thm above. □

Corollary. *If K/F is Galois, then K/E is Galois for all $F \leq E \leq K$.*

Proof. by 1)⇔3) of Thm above □

$$\text{Galois}\left\{\begin{array}{l} K \\ \,|\; \Big\}\ \text{Galois} \\ E \\ \,| \\ F \end{array}\right.$$

Example.

1)
$$\begin{tikzcd} \mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}
\qquad
\begin{array}{l} \Big\}\ \text{Galois} \\[1ex] \Big\}\ \text{Galois} \end{array}
\qquad \Bigg\}\ \text{not Galois (not normal, not splitting field)}$$

2) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2-2)(x^2-3)$, hence Galois over $\mathbb{Q}$.

$\varphi \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ is uniquely determined by

$\varphi(\sqrt{2}) = \pm\sqrt{2}$ $\qquad \varphi(\sqrt{3}) = \pm\sqrt{3}$ $\qquad$ $\varphi(\sqrt{2})$ is a root of $\varphi(m_{\sqrt{2},\mathbb{Q}}(x)) = x^2-2$

Let $\sigma(\sqrt{2}) = -\sqrt{2}$, $\quad \sigma(\sqrt{3}) = \sqrt{3}$

$\tau(\sqrt{2}) = \sqrt{2}$ $\quad \tau(\sqrt{3}) = -\sqrt{3}$

Then $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

subgroups $\qquad\qquad$ fixed fields

$$\begin{tikzcd}[column sep=small] & 1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle\sigma\rangle \arrow[dr, dash] & \langle\sigma\tau\rangle \arrow[d, dash] & \langle\tau\rangle \arrow[dl, dash] \\ & \langle\sigma,\tau\rangle & \end{tikzcd}
\qquad\qquad
\begin{tikzcd}[column sep=small] & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$