3.3 The Galois correspondence

Def: L/K finite

$\mathrm{Aut}_K(L) = \{\sigma : L \xrightarrow{\sim} L \mid \sigma(a) = a \ \forall a \in K\}$, $\sigma \cdot \tau = \sigma \circ \tau : L \xrightarrow{\tau} L \xrightarrow{\sigma} L$

L/K is <u>Galois</u> if it is normal and separable.

In this case, we call $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ <u>the Galois group of L/K</u>.

Def: $H < \mathrm{Aut}_K(L)$ subgroup

The <u>fixed field of H</u> is

$$L^H = \{a \in L \mid \sigma(a) = a \ \forall \sigma \in H\}$$

Rem: Since

$$\sigma(a * b) = \sigma(a) * \sigma(b) = a * b$$

for all $a, b \in L^H$, $\sigma \in H$ and $* \in \{+, -, \cdot, /\}$, L^H is indeed a field.

Thm 1 (Fundamental theorem of Galois theory)

L/K finite Galois

$G = \mathrm{Gal}(L/K)$

Then

$$\begin{array}{ccc}
\{K \subset E \subset L\} & \xleftrightarrow{1:1} & \{H < G\} \\
E & \xmapsto{\Phi} & \mathrm{Gal}(L/E) \\
L^H & \xleftarrow{\Psi} & H
\end{array}$$

are mutually inverse inclusion reversing bijections.

Rem:

$$\begin{tikzcd}
L \arrow[d, dash, "\text{sep.\ \& normal}"] \\
E \arrow[d, dash] \\
K
\end{tikzcd}$$

sep. & normal

by Cor. 3.1.3 & Cor. 3.2.6

A subextension E/K is normal iff. $H = \mathrm{Gal}(L/E)$ is a normal subgroup of G. In this case, we have an isomorphism

$$\begin{aligned} G/H &\xrightarrow{\sim} \mathrm{Gal}(E/K) \\ [\sigma] &\longmapsto \sigma|_E \end{aligned}$$

$$\begin{tikzcd} L \arrow[d, dash, "H"] \\ E \arrow[d, dash, "G/H"] \\ K \end{tikzcd} \quad G$$

and a short exact sequence

$$1 \to \mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K) \to 1.$$
$$\sigma \longmapsto \sigma|_E$$

The proof requires a number of auxiliary results.

<u>Lemma 2:</u> $L^G = K$ and Φ is injective.

proof: • Let $a \in L^G$; <u>want</u>: $a \in K$

By Lemma 22.7, every K-linear $\sigma : K(a) \to \overline{L}$ extends to some $\sigma_L : L \to \overline{L}$. Since L/K is normal,

$$\begin{tikzcd} L \arrow[r, "\sigma_L"] & \overline{L} \\ K(a) \arrow[u, dash] \arrow[ur, "\sigma"] & \\ K \arrow[u, dash] \arrow[uur, dash] & \end{tikzcd}$$

$\sigma_L(L) = L$ and thus $\sigma_L \in G$.

Since $\tau(a) = a \quad \forall \tau \in G$, $[K(a):K]_s = 1$.

Since a is separable over K,

$[K(a):K] = [K(a):K]_s = 1$, i.e. $a \in K$.

Clearly, $K \subset \{a \in L \mid \sigma(a) = a \ \forall \sigma \in G\} = L^G$.

Thus $L^G = K$.

• Consider $K \subset E \subset L$ and $H = \mathrm{Gal}(L/E)$.

Then $E = L^H$. Thus if $H' = \mathrm{Gal}(L/E') = H$,

then $E' = L^{H'} = L^H = E$. Thus Φ is injective. $\square$

Thm 3 (Artin):

L field

$\mathrm{Aut}(L) = \{\sigma : L \to L\}$ group of field automorphisms

$G < \mathrm{Aut}(L)$ of finite order n

$K = L^G = \{a \in L \mid \sigma(a) = a \ \forall \sigma \in G\}$

Then $[L:K] = n$ and L/K is Galois with

Galois group G.

We use 2 lemmas for the proof:

Lemma 4: L/k separable

$a \in L$

$\deg_K(a) := [K(a):K] = \deg$ Mipoa

Then $[L:K] = \sup\{\deg_K(a) \mid a \in L\}$.

In particular, $[L:K]$ is finite if there is an $n \in \mathbb{N}$ s.t. $\deg_K(a) \leq n$ for all $a \in L$.

proof: • Clearly $[L:K] \geq \deg_K(a)$ for all $a \in L$

$\Rightarrow [L:K] \geq \sup\{\deg_K(a) \mid a \in L\}$.

Thus "=" if $\sup\{-\} = \infty$.

• Assume that $n = \sup\{-\} < \infty$. Then $n = \deg_K(a)$ for some $a \in L$.

• claim: $L = K(a)$

Consider $b \in L$. By the thm. of the prim. elt. (Thm. 3.2.10), $K(a,b) = K(c)$ for some $c \in L$, and thus

$$K \subset K(a) \subset K(a,b) = K(c).$$

Since $[K(c):K] = \deg_K(c) \leq n$, we have

$$K(a,b) = K(c) = K(a),$$

and thus $b \in K(a)$. Thus $L = K(a)$ as claimed. //

- We conclude that

$$[L:K] = [K(a):K] = n = \sup\{-\}.$$

$\square$

<u>Lemma 5</u>: L/K finite

Then $\# \mathrm{Aut}_K(L) \leq [L:K]_s$, and "=" iff. L/K is normal. In particular, $\# \mathrm{Aut}_K(L) = [L:K]$ iff. L/K is Galois.

<u>proof</u>: • $\mathrm{Aut}_K(L) \longrightarrow \left\{ L \xrightarrow{\hat\sigma} \bar{L} \text{ over } K \right\}$

$$\left(L \xrightarrow{\sigma} L\right) \longmapsto \left(L \xrightarrow{\sigma} L \xrightarrow{\iota} \bar{L}\right)$$

is injective, thus $\# \mathrm{Aut}_K(L) \leq [L:K]_s$.

- "=" $\iff$ every $\hat\sigma : L \to \bar{L}$ (over K) comes from a $\sigma : L \to L$ (over K)

$\iff$ $\hat\sigma(L) = L$ for all $\hat\sigma : L \to \bar{L}$ (over K)

$\iff$ L/K normal.
(Thm. 3.1.2)

- Thus we have $\# \mathrm{Aut}_K(L) \underset{\text{"=" iff. normal}}{\leq} [L:K]_s \underset{\text{"=" iff. separable}}{\leq} [L:K]$,

with equalities iff. L/K is Galois. $\square$

Thm 3 (Artin):

L field

$\mathrm{Aut}(L) = \{\sigma : L \to L\}$ group of field automorphisms

$G < \mathrm{Aut}(L)$ of finite order n

$K = L^G = \{a \in L \mid \sigma(a) = a \ \forall \sigma \in G\}$

Then $[L:K] = n$ and L/K is Galois with Galois group G.

proof: • Consider $a \in L$.

Let $\{\sigma_1 \_ \sigma_r\} \subset G$ be a maximal subset s.t. $\sigma_1(a) \_ \sigma_r(a)$ are pairwise distinct.

Then $\tau \circ \sigma_1(a) \_ \tau \circ \sigma_r(a)$ are pairwise distinct for all $\tau \in G$, and thus by the maximality of $\{\sigma_1 \_ \sigma_r\}$, we conclude that $\{\tau \circ \sigma_1(a) \_ \tau \circ \sigma_r(a)\} = \{\sigma_1(a) \_ \sigma_r(a)\}$.

• Thus

$$f = \prod_{i=1}^{r} (T - \sigma_i(a)) \quad \in L[T]$$

is separable and $\tau(f) = f$ for all $\tau \in G$, i.e. $f \in K[T]$. Since $id_L(a) = a$, a is a root of f. Thus a is separable over K and $\deg_K(a) \leq \deg f = r \leq n = \# G$.

$$\Rightarrow \# \mathrm{Aut}_K(L) \underset{\text{(Lemma 5)}}{\leq} [L:K] \underset{\text{(Lemma 4)}}{\leq} n = \# G$$

Since $G < \mathrm{Aut}_K(L)$, we have "$=$" & L/K Galois (by Lemma 5) $\square$

Thm 1 (Fundamental theorem of Galois theory)

L/K finite Galois

$G = \mathrm{Gal}(L/K)$

Then

$$\begin{array}{ccc} \{K \subset E \subset L\} & \overset{1:1}{\longleftrightarrow} & \{H < G\} \\ E & \overset{\Phi}{\longmapsto} & \mathrm{Gal}(L/E) \\ L^H & \overset{\Psi}{\longleftarrow\!\shortmid} & H \end{array}$$

are mutually inverse inclusion reversing bijections.

A subextension E/K is normal iff. $H = \mathrm{Gal}(L/E)$ is a normal subgroup of G. In this case, we have an isomorphism

$$\begin{array}{ccc} G/H & \xrightarrow{\sim} & \mathrm{Gal}(E/K) \\ [\sigma] & \longmapsto & \sigma|_E \end{array}$$

$$\begin{tikzcd} L \arrow[d, dash, "H"] \\ E \arrow[d, dash, "G/H"] \\ K \end{tikzcd} \quad G$$

and a short exact sequence

$$\begin{array}{ccccccc} 0 \to \mathrm{Gal}(L/E) \to & \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(E/K) \to 0. \\ & \sigma & \longmapsto & \sigma|_E \end{array}$$

proof: • Φ is injective by Lemma 1.

• Given $H < G$, L/L^H is Galois with Galois group H by Thm. 3.

$\Rightarrow$ Φ and Ψ are mutually inverse bijections; it is clear that

$H \subset H' \iff L^{H'} \subset L^H$.

• If E/K is normal, then $\sigma(E)=E \;\forall \sigma\in G$;

$$\rightsquigarrow \quad \pi : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K).$$
$$\sigma \longmapsto \sigma|_E : E \to E$$

Since every $\tau : E \xrightarrow{\tilde{\tau}} E \to \bar{E}=\bar{L}$ (over K) extends

$$\begin{tikzcd} L \arrow[rr, "\tau_L"] \arrow[dr, dash] & & \bar{L} \\ & E \arrow[ur, "\tau"] \arrow[d, dash] & \\ & K \arrow[uur, dash] & \end{tikzcd}$$

to $\tau_L : L \to \bar{L}$ by Lemma 2.2.7,

and $\tau_L(L)=L$ (L/K normal), $\Rightarrow \tilde{\tau} = \tau_L|_E = \pi(\tau_L)$

we see that π is surjective.

Since $\ker(\pi) = \{\sigma : L \xrightarrow[K]{} L \mid \sigma|_E = \mathrm{id}_E\}$

$$= \{\sigma : L \xrightarrow[E]{} L\} = \mathrm{Gal}(L/E) = H$$

we conclude that $H \triangleleft G$ and

$$1 \to \underbrace{\mathrm{Gal}(L/E)}_{=H} \to \underbrace{\mathrm{Gal}(L/K)}_{=G} \xrightarrow{\pi} \mathrm{Gal}(E/K) \to 1.$$

is exact, and thus $\bar{\pi} : G/H \to \mathrm{Gal}(E/K)$, $[\sigma] \mapsto \sigma|_E$

an isomorphism.

• Conversely, assume that $H \triangleleft G$ and let $E = L^H$.

Consider $\sigma : E \xrightarrow[K]{} \bar{L}$, $E' = \sigma(E)$.

$$\begin{tikzcd} L \arrow[rr, "\sigma_L"] \arrow[dr, dash] & & \bar{L} \\ & E \arrow[ur, "\sigma"] \arrow[d, dash] & \\ & K \arrow[uur, dash] & \end{tikzcd}$$

By Lemma 2.2.7, σ extends to $\sigma_L : L \to \bar{L}$,

and $\sigma_L(L) = L$ since L/K is normal.

$\rightsquigarrow$ Consider $\sigma_L : L \xrightarrow{\sim} L$ as autom. in $\mathrm{Gal}(L/K)$

- Since L/K is normal, L/E' is normal by Cor. 3.1.3.

$$\begin{tikzcd}
L \arrow[d, dash, "\text{normal}"] \\
E' \arrow[d, dash] \\
K \arrow[uu, phantom, bend left, "\text{normal}"]
\end{tikzcd}$$

Let $H' = \mathrm{Gal}(L/E')$.
We obtain an isom.

$$\begin{array}{ccc}
H & \longrightarrow & H', \\
L \xrightarrow{\tau} L & \longmapsto & L \xrightarrow{\sigma_L^{-1}} L \xrightarrow{\tau} L \xrightarrow{\sigma_L} L
\end{array}$$

i.e. $H' = \sigma_L H \sigma_L^{-1}$ is conjugate to H in G.

Since $H \lhd G$, $H' = H$ and $E' = \sigma(E) = E$.

Thus E/K is normal. $\square$