

3.3 The Galois correspondence

Def: L/K finite

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

L/K is Galois if it is normal and separable.

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

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

The fixed field of H 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)

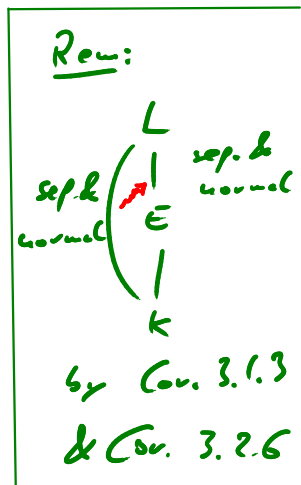
L/K finite Galois

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

Then

$$\begin{array}{ccc} \{ K \subset E \subset L \} & \xleftrightarrow{\quad \uparrow \downarrow \quad} & \{ H < G \} \\ E & \xleftrightarrow{\quad \Phi \quad} & \text{Gal}(L/E) \\ L^H & \xleftrightarrow{\quad \Psi \quad} & H \end{array}$$

are mutually inverse inclusion reversing bijections.



A subextension E/K is normal iff. $H = \text{Gal}(L/E)$

is a normal subgroup of G . In this case, we

have an isomorphism $G/H \xrightarrow{\sim} \text{Gal}(E/K)$
 $[\sigma] \mapsto \sigma|_E$



and a short exact sequence

$$1 \rightarrow \text{Gal}(L/E) \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(E/K) \rightarrow 1.$$

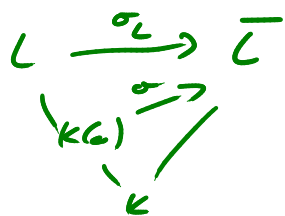
$\sigma \mapsto \sigma|_E$

The proof requires a number of auxiliary results.

Lemma 2: $L^G = K$ and Φ is injective.

proof: Let $a \in L^G$; want: $a \in K$

By Lemma 2.2, every K -linear $\sigma: K(a) \rightarrow \bar{L}$ extends to some $\sigma_L: L \rightarrow \bar{L}$. Since L/K is normal,



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

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

Since a is separable over K ,

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

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

Thus $L^G = K$.

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

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

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

Thm 3 (Artin):

L field

$\text{Aut}(L) = \{\sigma: L \rightarrow L\}$ group of field automorphisms

$G < \text{Aut}(L)$ 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

$a \in L$

$$\deg_K(a) := [K(a):K] = \deg \text{Mip}_a$$

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

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 " \geq " iff $\sup \{ - \} = \infty$.

• 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

$$K \subset K(\alpha) \subset K(\alpha, S) = K(\alpha).$$

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

$$K(\alpha, S) = K(\alpha) = K(\alpha),$$

and thus $\beta \in K(\alpha)$. Thus $L = K(\alpha)$ as claimed. \square

• We conclude that

$$[L:K] = [K(\alpha):K] = n = \text{sup} \{ \dots \}.$$

\square

Lemma 5: L/K finite

Then $\# \text{Aut}_K(L) \leq [L:K]_s$, and " $=$ "

iff. L/K is normal. In particular,

$\# \text{Aut}_K(L) = [L:K]$ iff. L/K is Galois.

proof: $\text{Aut}_K(L) \longrightarrow \left\{ L \underset{K}{\xrightarrow{\hat{\sigma}}} \bar{L} \right\}$

$$L \xrightarrow{\sigma} L \longmapsto L \xrightarrow{\sigma} L \xrightarrow{\hat{\sigma}} \bar{L}$$

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

• " $=$ " \Leftrightarrow every $\hat{\sigma}: L \underset{K}{\rightarrow} \bar{L}$ comes from a $\sigma: L \underset{K}{\rightarrow} L$

$$\Leftrightarrow \hat{\sigma}(L) = L \text{ for all } \hat{\sigma}: L \underset{K}{\rightarrow} \bar{L}$$

$$\Leftrightarrow L/K \text{ normal.}$$

(Thm. 3.1.2)

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

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

Thm 3 (Artin):

L field

$\text{Aut}(L) = \{\sigma: L \rightarrow L\}$ group of field automorphisms

$G < \text{Aut}(L)$ 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 $\{\sigma_1, \dots, \sigma_r\} \subset G$ be a maximal subset s.t. $\sigma_i(a) - \sigma_j(a)$ are pairwise distinct.

Then $\tau \circ \sigma_i(a) - \tau \circ \sigma_j(a)$ are pairwise distinct

for all $\tau \in G$, and thus by the maximality of $\{\sigma_1, \dots, \sigma_r\}$, we conclude

$$\{\tau \circ \sigma_i(a) - \tau \circ \sigma_j(a)\} = \{\sigma_i(a) - \sigma_j(a)\}.$$

• Thus

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

is separable and $\tau(f) = f$ for all $\tau \in G$,

i.e. $f \in K[T]$. Since $\text{id}_L(a) = a$, a is

a root of f . Thus a is separable over K

and $\deg_K(a) \leq \deg f = r \leq n = \#G$.

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

(Lemma 5) (Lemma 4)

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

Thm 1 (Fundamental theorem of Galois theory)

L/K finite Galois

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

Then

$$\begin{array}{ccc} \{K \subset E \subset L\} & \xleftrightarrow{\quad \cong \quad} & \{H \subset G\} \\ E & \xrightarrow{\quad \Phi \quad} & \text{Gal}(L/E) \\ L^H & \xleftarrow{\quad \Psi \quad} & H \end{array}$$

are mutually inverse inclusion reversing bijections.

A subextension E/K is normal iff $H = \text{Gal}(L/E)$

is a normal subgroup of G . In this case, we

have an isomorphism $G/H \xrightarrow{\sim} \text{Gal}(E/K)$

$$[\sigma] \mapsto \sigma|_E$$

$$G \begin{pmatrix} L \\ | \\ H \\ | \\ E \\ | \\ G/H \\ | \\ K \end{pmatrix}$$

and a short exact sequence

$$0 \rightarrow \text{Gal}(L/E) \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(E/K) \rightarrow 0.$$

$\sigma \mapsto \sigma|_E$

proof: Φ is injective by Lemma 1.

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

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

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

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

$$\Rightarrow \pi: \text{Gal}(L/K) \longrightarrow \text{Gal}(E/K).$$

$$\sigma \longmapsto \sigma|_E: E \rightarrow E$$

Since every $\tau: E \xrightarrow{\cong} E \rightarrow \bar{E} = \bar{L}$ extends

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

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

we see that π is surjective.

Since $\ker(\pi) = \{ \sigma: L \rightarrow L \mid \sigma|_E = \text{id}_E \}$

$$= \{ \sigma: L \rightarrow L \}_{E'} = \text{Gal}(L/E) = H$$

we conclude that $H \triangleleft G$ and

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

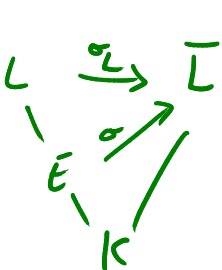
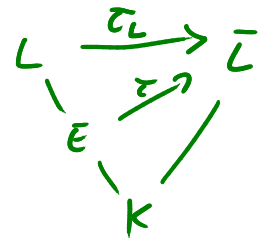
is exact, and thus $\bar{\pi}: G/H \rightarrow \text{Gal}(E/K)$
 $[\sigma] \mapsto \sigma|_E$
 an isomorphism.

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

Consider $\sigma: E \rightarrow \bar{L}$, $E' = \sigma(E)$.

By Lemma 2.2.7, σ extends to $\sigma_L: L \rightarrow \bar{L}$,
 and $\sigma_L(L) = L$ since L/K is normal.

\Rightarrow Consider $\sigma_L: L \xrightarrow{\cong} L$ as autom. in $\text{Gal}(L/K)$



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

$$\text{Let } H' = \text{Gal}(L/E').$$

We obtain an isom.

$$\begin{array}{ccc} H & \longrightarrow & H' \\ L \xrightarrow{\sigma} L & \longmapsto & L \xrightarrow{\sigma_{L'}} L \xrightarrow{\sigma} L \end{array}$$

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

Since $H \triangleleft G$, $H' = H$ and $E' = \sigma(E) = \bar{E}$.

Thus E/K is normal. \square

