

Lecture # 4 (Oct 2nd, 2024)

Theorem Consider a finite field extension L/K and a field homomorphism $\sigma: K \rightarrow F$. Then $\#\{\tau \in \text{Hom}(L, F); \tau(a) = \sigma(a) \forall a \in K\} \leq [L:K]$

$$\begin{array}{ccc} L & \xrightarrow{\tau} & F \\ \cup & \nearrow \sigma & \\ K & & \end{array}$$

Moreover, equality holds if and only if

(i) L/K is separable, and

(ii) if $f \in K[x]$ is equal to $\min_K(\alpha)$ for some $\alpha \in L$, then $\sigma(f)$ splits in $F[x]$.

Corollary Suppose that L/K is a finite field extension. Then

$$|\text{Aut}_K(L)| = [L:K] \iff L/K \text{ is both separable and normal}$$

Why? Take $F=L$ and $\sigma =$ inclusion in the theorem.

Note that since L/K is finite

$$\text{Hom}_K(L, L) = \text{Aut}_K(L)$$

More generally, we have the following.

~~Definition~~ / Proposition: For a finite field extension L/K , the following are equivalent

(i) $|\text{Aut}_K(L)| = [L:K]$

(ii) $L^{\text{Aut}_K(L)} = K$ ← fixed field under Aut

(iii) L/K is separable and normal

(iv) $L = \text{SF}_K(f)$ for some $f \in K[x]$
separable

If any (hence all) of these holds, we say that the extension is Galois and we write $\text{Gal}(L/K) := \text{Aut}_K(L)$.

This group is called the Galois grp. of the extension.

proof of theorem

Step 1: Take $\alpha \in L$ and consider

$$K_1 = K(\alpha) \subset L. \text{ Let } n = \deg \min_K \alpha := f$$

Then

$$\# \{ \tau_1: K_1 \rightarrow F; \tau_1|_K = \sigma \}$$

||

$$\# \{ \text{roots of } \sigma_* f \text{ in } F \} \leq \text{def} = [K_1:K]$$

----- interlude

Note that any $\tau_1: K_1 \rightarrow F$ defines a root of $\sigma(f)$, namely $\tau_1(\alpha)$. This is because

$$\sigma_* f(\tau_1(\alpha)) = \tau_1(f(\alpha)) = \tau_1(0) = 0$$

Conversely, any root β of $\sigma_* f$ gives

$$K_1 = K(\alpha) \cong K[x]/(f) \cong K(\beta) \hookrightarrow F$$

$$\begin{array}{c} \text{-----} \curvearrowright \\ \tau_1 \\ \alpha \mapsto \beta \end{array}$$

by construction, $\tau_1|_K = \sigma$.

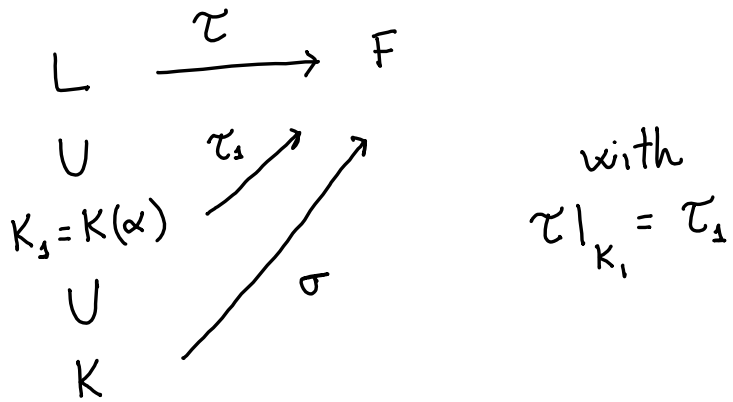
----- end interlude

Note that, moreover, we have equality iff

(a) α is separable $\Leftrightarrow f$ is separable,
and

(b) $\sigma_* f$ splits over F

Step 2 We now wish to count all τ 's fitting in a diagram like the one below



for each possible choice of τ_1 as in step 1.

Step 3

Put $\alpha = \alpha_1$ and write $L = K(\alpha_1, \dots, \alpha_d)$
 $= K_3(\alpha_2, \dots, \alpha_d)$

Using induction on d , we can deduce that for each τ_1 there are at most $[L:K_3]$ extensions.

Thus, the counting from step 2 gives

$$\#\{\tau\} \leq [K_3:K] [L:K_3] = [L:K]$$

Step 4 We need to check when do we have equality.

Note that ^{the} proof tells us it suffices to show that assuming (i) and (ii),

then K_1/K and τ_1 satisfy

(a) α is separable and

(b') $\tau_1(\min_{K_1} \alpha)$ splits over F

Now,

(a) follows from (i) and

(b') follows from (ii) since

$\min_{K_1} \alpha$ divides $f \Rightarrow \tau_1(\min_{K_1} \alpha)$
divides

$$\tau_1(f) = \sigma(f)$$

and $\sigma(f)$ splits / F .

Consider now $K < L < \bar{K}$. What is the smallest Galois extension of K that contains L ? ^{finite}

Definition Given $K < L < \bar{K}$, the normal closure of L (in \bar{K}) is the smallest normal extension of K containing L . Notation: L^{Gal}

Proposition If L/K is a finite and separable field extension with $L < \bar{K}$, then the normal closure of L is also separable (hence Galois) over K .

proof Write $L = K(\alpha_1, \dots, \alpha_n)$. Since L/K is separable, $\{\min_K \alpha_i\}$ is a collection of separable polynomials.

The claim then follows from observing that $L^{\text{Gal}} = \text{SF}_K(\{\min_K \alpha_i\})$

$$= K\left(\bigcup_{\substack{\text{roots of } \min_K \alpha_i \\ \downarrow \\ \text{in } \bar{K}}} \right)$$

RmKs

① Even when L/K is NOT Galois, we often call the group $\text{Aut}_K(L^{\text{Gal}})$ the Galois grp. of the finite separable extension L/K .

② Given $K \subset L \subset \bar{K}$ with L/K normal, we have that the separable extension

$L^{\text{sep},K}/K$ is normal (hence Galois)

as well. In the case $L = \bar{K}$, the corresponding Galois group is called the absolute Galois group of K .

The Galois correspondence

Theorem Let L/K be a (finite) Galois extension with Galois group $G = \text{Aut}_K(L)$.

The map $F \mapsto \text{Gal}(L/F)$ defines a bijection between intermediate fields $K \subset F \subset L$ and subgroups of G .

The inverse map is given by

$$H \mapsto L^H = \{ \ell \in L; \sigma(\ell) = \ell \ \forall \sigma \in H \}$$

and this correspondence is inclusion-reversing:

$$\begin{array}{ccc}
 & L & \{ \text{id} \} \\
 & \cup & \cap \\
 & F' & \text{Gal}(L/F') \\
 & \cup & \cap \\
 & F & \text{Gal}(L/F) \\
 & \cup & \cap \\
 L^G = K & \longmapsto & G
 \end{array}$$

Moreover, (Part II)

If $F = L^H \mapsto H = \text{Gal}(L/F)$, then

$$(A) |H| = [L:F] \text{ and } [F:K] = [G:H]$$

$$(B) F \underset{K}{\simeq} F' \Leftrightarrow H \text{ and } H' \text{ are conjugate}$$

In particular, for $\sigma \in G$ we have

$$\text{Gal}(L/\sigma(F)) = \sigma \text{Gal}(L/F) \sigma^{-1}$$

$$(C) F/K \text{ is Galois} \Leftrightarrow H \trianglelefteq G$$

In which case, $G = \text{Gal}(L/K) \rightarrow \text{Gal}(F/K)$
 $\sigma \mapsto \sigma|_F$

is surjective with kernel H . Thus,

$$G/H \simeq \text{Gal}(F/K)$$

To prove the main theorem, we will use the following lemma by E. Artin.

Lemma (Artin) Let F be any field and let H be any finite subgroup of $\text{Aut}(F)$. Then F/F^H is finite Galois and $\text{Gal}(F/F^H) = H$.

proof Let $K = F^H$. Since $H \subseteq \text{Aut}(F)$

and $K = F^H$, we have that

$$H \subseteq \text{Aut}_K(F) \Rightarrow |H| \leq |\text{Aut}_K(F)|$$

Note $\text{Aut}_K(F) \subseteq \text{Aut}(F) \rightarrow \leq [F:K]$

Thus, to prove F/K is Galois, it suffices to show $|H| \geq [F:K]$.

By contradiction, assume $[F:K] \geq |H| + 1$ and choose $f_1, \dots, f_{|H|+1} \in F$ linear independent / K .

For each $m \leq |H| + 1$ consider the linear system of $|H|$ eq. on the var. X_1, \dots, X_m

$$(*) \quad L_m : \left\{ \sum_{i=1}^m h(f_i) X_i = 0, \quad h \in H \right.$$

Fix the smallest m for which $(*)$ admits a (non-trivial) solution.

Fix a solution $(\tilde{f}_1, \dots, \tilde{f}_m) \in F^m$

with $\tilde{f}_m = 1$.

|| Claim Given any $h \in H$,
 $(\tilde{f}_1 - h(\tilde{f}_1), \dots, \tilde{f}_{m-1} - h(\tilde{f}_{m-1}))$
is a solution to L_{m-1} .

Thus, by minimality of m , this is the trivial solution and $\tilde{f}_i \in K \quad \forall i$

But then

$$\sum_{i=1}^m f_i \tilde{f}_i = 0$$

(this comes from one of the equations in (*) taking $h = \text{id}_F$)

is a non-trivial K -linear combination of the f_i 's, which is an absurd since $m \leq |H| + 1$



Sketch of the proof of claim:

$\forall h' \in H,$

$$\textcircled{\text{I}} \quad h'(f_m) = h'(f_m) \cdot 1 = - \sum_{i=1}^{m-1} h'(f_i) \tilde{f}_i$$

we can apply any $h \in H$ to both sides, and "change variables" $g = hoh'$. Thus,

$\forall g \in H$

$$\textcircled{\text{II}} \quad g(f_m) = - \sum_{i=1}^{m-1} g(f_i) h(\tilde{f}_i)$$

So, matching the h's with the g's,
subtracting $(II) - (I)$ gives the claim.