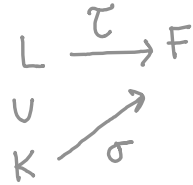
Lecture #4

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

$$\leq [L:K]$$



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

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

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

Note that since L/K is finite

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

More generally, we have the following.

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

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

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

(iii) L/K is separable and normal

(iv) $L = SF_K(f)$ for some $f \in K[x]$ separable

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

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

proof of theorem

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

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

Then

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

$$\| $$

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

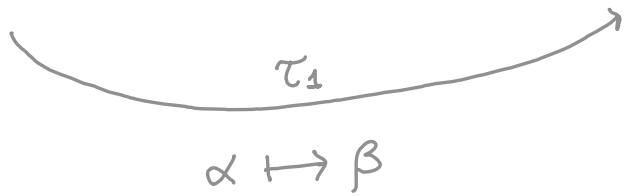
- - - - - - interlude

Note that any $\tau_1 : K_1 \to F$ 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

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



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

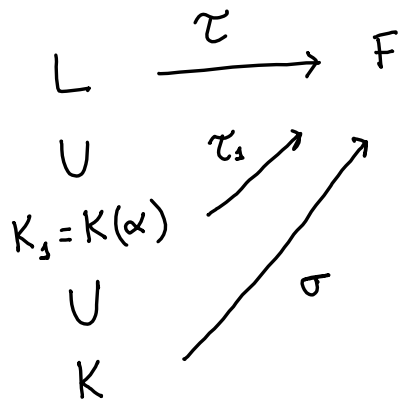
---------- end interlude

Note that, moreover, we have equality iff

(a) α is separable $\iff$ 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



with $\tau|_{K_1} = \tau_1$

for each possible choice of τ_1 as in step 1.

Step 3

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

$= K_1(\alpha_2, \dots, \alpha_d)$

Using induction on d, we can deduce that for each τ_1 there are at most $[L : K_1]$ extensions.

Thus, the counting from step 2 gives

$$\#\{\tau\} \leq [K_1 : K]\,[L : K_1] = [L : K]$$

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

Now,
(a) follows from (i) and

(b') follows from (ii) since

$\min_{K_1}\alpha$ divides $f \Rightarrow \tau_1\left(\min_{K_1}\alpha\right)$ divides $\tau_1(f) = \sigma(f)$

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

Consider now $K \subset L \subset \overline{K}$ (finite). What is the smallest Galois extension of K that contains L?

Rmk.: If $K \subset L$ is finite we can always embed L in $\overline{K}$

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

Proposition If L/K is a finite and separable field extension with $L \subset \overline{K}$, 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 $L^{Gal} = SF_K(\{\min_K \alpha_i\})$

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

RmKs

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

(2) Given $K \subset L \subset \overline{K}$ with L/K normal, we have that the separable extension $L^{sep,K}/K$ is normal (hence Galois) as well. In the case $L = \overline{K}$, 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 $G = \mathrm{Aut}_K(L)$.

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

The inverse map is given by

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

and this correspondence is inclusion-reversing:

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

Moreover, (Part II)

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

(A) $|H| = [L:F]$ and $[F:K] = [G:H]$

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

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

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

(C) F/K is Galois $\iff H \trianglelefteq G$

In which case, $G = \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$

$$\sigma \mapsto \sigma|_F$$

is surjective with kernel H. Thus,

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

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 $\mathrm{Aut}(F)$. Then F/F^H is finite Galois and $\mathrm{Gal}(F/F^H) = H$.

proof Let $K = F^H$. Since $H \subset \mathrm{Aut}(F)$ and $K = F^H$, we have that

$H \subset \mathrm{Aut}_K(F) \Rightarrow |H| \leq |\mathrm{Aut}_K(F)|$

And if F/K is finite, then $|\mathrm{Aut}_K(F)| \leq [F:K]$ (1st thm of today)

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 $f_1, \ldots, f_{|H|+1} \in F$ 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 $\tilde{f}_m = 1$.

<u>Claim</u> Given any $h \in H$,

$$\left(\tilde{f}_1 - h(\tilde{f}_1), \dots, \tilde{f}_{m-1} - h(\tilde{f}_{m-1}) \right)$$

is a solution to L_{m-1}.

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

But then

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

(this comes from one of the equations in (*) taking $h = id_F$)

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:

$\forall h' \in H$,

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

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

$\forall g \in H$

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

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